



UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería del Diseño

CREACIÓN DE CONTENIDOS TÉCNICOS PARA LA FORMACIÓN EN REDES DE ÁREA LOCAL

TRABAJO FINAL DEL

Grado en Ingeniería Electrónica Industrial y Automática



REALIZADO POR

Olga M^a Minguet Mocholí

TUTORIZADO POR

Joaquim Francesc Arlandis Navarro

CURSO ACADÉMICO: 2020/2021

Índice

1	Introducción	6
2	Contextualización	7
2.1	La formación en Ciclos Formativos	7
2.2	La formación en empresas.....	9
2.3	La formación de post-grado.....	10
3	Objetivos	11
3.1	Objetivo general del curso.....	11
3.2	Objetivos específicos	11
4	Estructura del curso	12
4.1	Bloques, unidades didácticas y secuenciación.....	12
4.2	Distribución de contenidos e instrumentos de aprendizaje	15
4.2.1	Bloque 1: Introducción a las redes locales	15
4.2.2	Bloque 2. Instalación y configuración de las redes locales.	19
4.2.3	Bloque 3. Resolución de incidencias en redes locales y redes mixtas integradas.	24
5	Sistema de evaluación	27
5.1	Tipos de evaluación	28
5.2	Instrumentos de aprendizaje evaluables	29
5.2.1	Cuadernos de Actividades (CA) y Cuadernos de Prácticas (Pract).....	29
5.2.2	Trabajos de investigación (TI)	29
5.2.3	Pruebas escritas (PE).....	31
5.2.4	Actividades de refuerzo y ampliación (CR)	31
5.3	Sistema de calificaciones	31
5.4	Evaluación del funcionamiento del curso	32
6	Metodología	34
6.1	Clase magistral participativa	34
6.2	Aprendizaje basado en juegos	35
6.3	Resolución de problemas	35

6.4	Aprendizaje colaborativo.....	36
6.5	Píldoras educativas	36
7	Recursos didácticos y espacios	37
7.1	Recursos didácticos	37
7.2	El aula y el taller	38
8	Contenidos	39
8.1	Unidad didáctica 1	41
8.1.1	Presentación teórica	42
8.1.2	Cuaderno de actividades	73
8.1.3	Cuaderno de prácticas	79
8.1.4	Trabajo de investigación	89
8.2	Unidad didáctica 2	91
8.2.1	Presentación teórica	92
8.2.2	Cuaderno de actividades	120
8.2.3	Cuaderno de prácticas	128
8.2.4	Trabajo de investigación	159
8.3	Unidad didáctica 3	161
8.3.1	Presentación teórica	162
8.3.2	Cuaderno de actividades	184
8.3.3	Cuaderno de prácticas	192
8.3.4	Trabajo de investigación	201
8.4	Unidad didáctica 4	209
8.4.1	Presentación teórica	210
8.4.2	Cuaderno de actividades	229
8.4.3	Cuaderno de prácticas	234
8.5	Unidad didáctica 5	252
8.5.1	Presentación teórica	253
8.5.2	Cuaderno de actividades	265
8.5.3	Cuaderno de prácticas	270

8.6	Unidad didáctica 6	294
8.6.1	Presentación teórica	295
8.6.2	Cuaderno de actividades	306
8.6.3	Cuaderno de prácticas	308
8.6.4	Trabajo de investigación	319
8.7	Unidad didáctica 7	321
8.7.1	Presentación teórica	322
8.7.2	Cuaderno de actividades	343
8.7.3	Cuaderno de prácticas	347
8.7.4	Proyecto final de redes	372
9	Bibliografía	375
10	Anexo: Presupuesto	377

Índice de Ilustraciones

Ilustración 1: Imagen de taller y aula genérico.....	8
Ilustración 2: Agrupación de las unidades didácticas (UD) en bloques de contenidos y su secuencia de impartición.....	12
Ilustración 3: Estructura de contenidos.....	13
Ilustración 4: Modelo de evaluación de la actividad docente por parte de los estudiantes.....	33

Índice de Tablas

Tabla 1: Secuenciación de las unidades didácticas distribuidas en los bloques de contenidos	14
Tabla 2: Relación de actividades y prácticas de la Unidad Didáctica 1	15
Tabla 3: Organización secuencial de la Unidad Didáctica 1	16
Tabla 4: Relación de actividades y prácticas de la Unidad Didáctica 2	17
Tabla 5: Organización secuencial de la Unidad Didáctica 2	18
Tabla 6: Relación de actividades y prácticas de la Unidad Didáctica 3	20
Tabla 7: Organización secuencial de la Unidad Didáctica 3	20
Tabla 8: Relación de actividades y prácticas de la Unidad Didáctica 4	22
Tabla 9: Organización secuencial de la Unidad Didáctica 4	22
Tabla 10: Relación de actividades y prácticas de la Unidad Didáctica 5	23
Tabla 11: Organización secuencial de la Unidad Didáctica 5	23
Tabla 12: Relación de actividades y prácticas de la Unidad Didáctica 6	24
Tabla 13: Organización secuencial de la Unidad Didáctica 6	25
Tabla 14: Relación de actividades y prácticas de la Unidad Didáctica 7	26
Tabla 15: Organización secuencial de la Unidad Didáctica 7	26
Tabla 16: Ejemplo de rúbrica de evaluación.....	30
Tabla 17. Relación costes bloque de contenidos 1	377
Tabla 18. Relación costes bloque de contenidos 2	377
Tabla 19. Relación costes bloque de contenidos 3	378
Tabla 20. Relación costes totales	378

1 Introducción

Ha sido escaso el trabajo realizado en Trabajos Final de Grado que se haya dirigido a la formación, aplicando los conocimientos técnicos adquiridos en los estudios universitarios. En particular, el dirigido a la formación de profesionales fuera del contexto universitario: trabajadores de empresas de distintos sectores, estudiantes de formación profesional, cursos de formación de post-grado, etc.

Debido a la creciente implantación en múltiples ámbitos de nuestra sociedad de las tecnologías relacionadas con la teleinformática en general, nos planteamos un reto en éste trabajo: la creación de contenidos técnicos para la formación en redes, y, más específicamente, en redes de área local, utilizando a tal fin el conocimiento aplicado de informática industrial y comunicaciones, aprendido en el periodo de los estudios universitarios de Grado.

El presente documento se organiza en dos partes. Una primera parte introductoria, donde se detallan los objetivos de un curso de formación especializada en redes de área local y las competencias a adquirir. Asimismo, se define una metodología de enseñanza-aprendizaje a utilizar y, se plantea un sistema de evaluación, definiendo los instrumentos correspondientes.

En una segunda parte, se presentarán con detalle los contenidos creados dirigidos a caracterizar técnicamente una red de área local, objetivo central del trabajo. Para ello, la distribución de contenidos del curso propuesto se ha realizado en siete unidades didácticas, las cuales se describirán en este documento. Ello incluirá toda la serie de actividades y prácticas que se trabajarán, así como el material teórico de soporte utilizado en las clases. Teniendo en cuenta que es un curso principalmente práctico, se destinarán muchas horas de actividades en el taller o laboratorio.

Por otro lado, la situación producida por la pandemia de la COVID-19 ha inducido a la creación de recursos y materiales para la difusión telemática (online y offline), como vídeos auto-didácticos y de apoyo, así como actividades y prácticas de simulación más variados y explicados con mayor detalle.

2 Contextualización

Tal y como hemos indicado en la [introducción](#), este curso pretende ser de aplicación en distintos ámbitos formativos fuera del contexto universitario. Trabajadores de empresas de distintos sectores que, debido a la creciente implantación de la tele-informática, precisan ampliar y actualizar sus conocimientos en materias referentes a las tecnologías de la información. Estudiantes de formación profesional, que deben especializarse en informática y comunicaciones. O también post-graduados, con o sin trabajo, que, una vez finalizados sus estudios universitarios, han decidido ampliar sus conocimientos en pro de una mejor competencia laboral, realizando un curso de especialización.

Se presenta así un grupo bien distinto de alumnado, pero con una característica común, todos ellos iniciándose en materia de informática y comunicaciones, con perspectivas de alcanzar un nivel de especialización profesional en redes de área local.

2.1 La formación en Ciclos Formativos

Los Ciclos Formativos ya especializados (de grado medio o grado superior), se nutren, generalmente, de alumnos de edades comprendidas entre 17-20 años, los cuales han sido dirigidos para encaminar su formación hacia ciclos, puesto que con las habilidades que presentan creen que se pueden desarrollar o cumplir mejor sus expectativas técnicas. También hay que tener presente que los estudios de ciclos abren las puertas a profesiones que requieren este mínimo de estudios para su acceso (policías locales, bomberos...) y bastantes de estos alumnos acabaran en ese camino. En muchos de ellos nos encontraremos que no están estudiando este ciclo por vocación sino por otros motivos que quizá no provoquen un nivel de esfuerzo y atención necesario para superarlo.

Se puede presentar así un grupo de muy variada procedencia en un aula de formación profesional. Desde alumnos que han cursado estudios de secundaria o bachiller, alumnos que detuvieron sus estudios en un periodo de su vida para trabajar y ahora deciden retomarlos, o alumnos que, no pudiendo superar la educación secundaria obligatoria, decidieron tomar el camino de los ciclos formativos desde la formación profesional básica, tomando desde el principio una carrera técnica.

Añadido a todo esto, nos podemos encontrar estudiantes con serias dificultades de aprendizaje (TDA, con o sin hiperactividad, Asperger, Discapacidad neuronal, Dislexia, ...), pero también, estudiantes con altas capacidades. Se deberán, por tanto, tener siempre actividades de refuerzo, para los alumnos con más dificultades, así como actividades extra para que aquellos alumnos con altas capacidades puedan llegar un poco más lejos en el conocimiento de la materia. Es por ello que, uno de los puntos de atención en el desarrollo del curso, es la creación de grupos para la realización de las prácticas donde intentamos mezclar esa variedad de alumnos, para que los alumnos que tienen más agilidad en el aprendizaje puedan ayudar a los que tienen más dificultades, y los que encuentran más dificultades puedan apoyarse en los que tienen más facilidad en la comprensión, en reciprocidad.

La puesta en marcha de este curso deberá realizarse en centros educativos donde se disponga de unos mínimos de espacio y materiales para garantizar la eficacia del mismo. Debe contar con espacios distribuidos en aulas de informática y taller.

El centro educativo debe estar equipado con proyector y pizarra blanca en el aula y en el taller. Siendo muy conveniente, que todos los puestos de alumnos posean un ordenador de sobremesa o portátil individual o, en caso necesario, un dispositivo por parejas. El ordenador es herramienta fundamental de trabajo para el desarrollo del curso. Se muestra una imagen genérica del aula y del trabajo en el taller en la Ilustración 1.



Ilustración 1: Imagen de taller y aula genérico

2.2 La formación en empresas

La formación técnica en empresas tiene como finalidad preparar a los trabajadores para el desempeño cualificado de las diversas profesiones que puedan requerirse en la misma, formando parte del departamento informático de la organización en entidades de cualquier tamaño y sector productivo que utilicen sistemas microinformáticos y redes de datos para su gestión.

En la actualidad, las organizaciones modernas necesitan estar interconectadas continuamente a través de una infraestructura TIC funcional y de alta disponibilidad. Para ello, es imprescindible que dispongan de trabajadores técnicos profesionales que garanticen una correcta transmisión de los datos, permitiendo de esta manera, mantener satisfactoriamente los activos de la empresa.

Desde el Servicio Público de Empleo Estatal (SEPE)¹, y en la Comunidad Valenciana desde el Servei Valencià d'Ocupació i Formació (LABORA)², se ofrecen cursos tanto para desempleados como para trabajadores, a través de lo que se conoce como formación profesional dual. Esta formación mixta, de empleo y formación, tiene por objeto la cualificación profesional de los trabajadores en un régimen de alternancia de actividad laboral en la empresa con la actividad formativa. En éste sentido, existen en la actualidad cursos de administración y diseño de redes³, y de operación de redes⁴.

El montaje de redes locales cableadas, inalámbricas y mixtas, junto al mantenimiento de dicha infraestructura serán el resultado aplicado del conocimiento y aptitudes que proporcionará este curso.

Será muy importante, por tanto, la adquisición de habilidades técnicas basada en la experimentación de las situaciones que se encuentran en su contexto laboral. Clave en este curso, la realización de muchas actividades de simulación práctica y actividades de taller, proponiendo la resolución de

¹ Servicio Público de Empleo Estatal (10 de junio de 2021) <https://sede.sepe.gob.es/portalSede/es/>

² Servei Valencià d'Ocupació i Formació (10 de junio de 2021) <https://labora.gva.es/va/ciudadania>

³ Curso de Administración y Diseño de Redes (10 de junio de 2021)

<https://sede.sepe.gob.es/especialidadesformativas/RXBuscadorEFRED/DetalleEspecialidadFormativa.do?codEspecialidad=IFCT0410>

⁴ Curso de Operación de Redes (10 de junio de 2021)

<https://sede.sepe.gob.es/especialidadesformativas/RXBuscadorEFRED/DetalleEspecialidadFormativa.do?codEspecialidad=IFCT0110>

problemas y el trabajo colaborativo, que es como habitualmente desarrollan su actividad los equipos de trabajo.

2.3 La formación de post-grado

Las redes se han convertido en la columna vertebral de casi todas las tecnologías modernas en el mundo actual y esto ha provocado que la realización de cursos de post-grado en esta especialidad sea altamente demandada. Los puestos más solicitados en las empresas son los profesionales relacionados con la informática, administradores de redes y sistemas informáticos.

En la formación de post-grado, este curso está destinado a complementar el conocimiento de los ingenieros en la implementación y el mantenimiento de redes eficientes. Otorgando al alumno una sólida formación como especialista, capacitándolo para desempeñarse en el ámbito profesional con eficiencia y con un alto nivel de destreza. Actualmente, y en constante crecimiento, las redes de comunicaciones precisan de profesionales altamente cualificados.

3 Objetivos

3.1 Objetivo general del curso

El objetivo general pretende conseguir que el estudiante adquiera conocimientos básicos sobre el diseño, la configuración y el mantenimiento de una red de área local. Adquirir conocimientos en materias básicas y tecnológicas que lo capacite para el aprendizaje de nuevos métodos y teorías y lo dote de versatilidad para adaptarse a nuevas situaciones, aplicando los protocolos de calidad, seguridad y respeto al medio ambiente establecidos.

Cabe reseñar la adquisición de competencias basadas en la experimentación de las situaciones que se encuentran en las instalaciones de redes actuales. Por ello, se plantea el desarrollo formativo como una fase de aprendizaje de habilidades profesionales basada en la práctica, (se realizarán muchas actividades de simulación práctica y actividades en el taller) así como una fase de aprendizaje de competencias sociales y personales que son necesarias tanto para poner en valor el trabajo que han realizado, como para colaborar con otros compañeros para la consecución de los objetivos. Es por ello que tendrán mucha importancia todas aquellas acciones formativas que propongan la resolución de problemas y el trabajo colaborativo.

3.2 Objetivos específicos

Los objetivos específicos del curso se enumeran a continuación:

- Reconocer los principios de funcionamiento de las redes locales.
- Identificar los distintos tipos de redes existentes.
- Identificar los protocolos básicos en la comunicación.
- Describir los elementos de una red local y su función.
- Identificar y clasificar los distintos tipos de medios de transmisión.
- Reconocer e interpretar el mapa físico de una red local (topología física).
- Diseñar y calcular el plan de montaje lógico de una red (topología lógica).
- Configurar los parámetros básicos de dispositivos finales e intermedios en una red local.
- Aprender a utilizar un programa de simulación (Cisco Packet Tracer) de redes.
- Comprobar la conectividad entre dispositivos, cableados e inalámbricos.
- Aplicar mecanismos básicos de seguridad en la red.

- Identificar incidencias y comportamientos anómalos.
- Identificar si la disfunción es hardware o software.
- Resolución de incidencias físicas y lógicas de la red local.
- Aprender a utilizar herramientas de diagnóstico de redes en línea de comandos.
- Aprender a monitorizar las señales visuales de los dispositivos de interconexión.
- Aprender a monitorizar los protocolos de comunicaciones.

4 Estructura del curso

4.1 Bloques, unidades didácticas y secuenciación

El curso se dividirá en tres bloques de contenidos. El primer y el tercer bloque estarán compuestos por dos unidades didácticas (UD) y el segundo bloque, por tres unidades didácticas. Los diferentes bloques y unidades didácticas se imparten secuencialmente de acuerdo a su numeración, como se indica en la *Ilustración 2*.

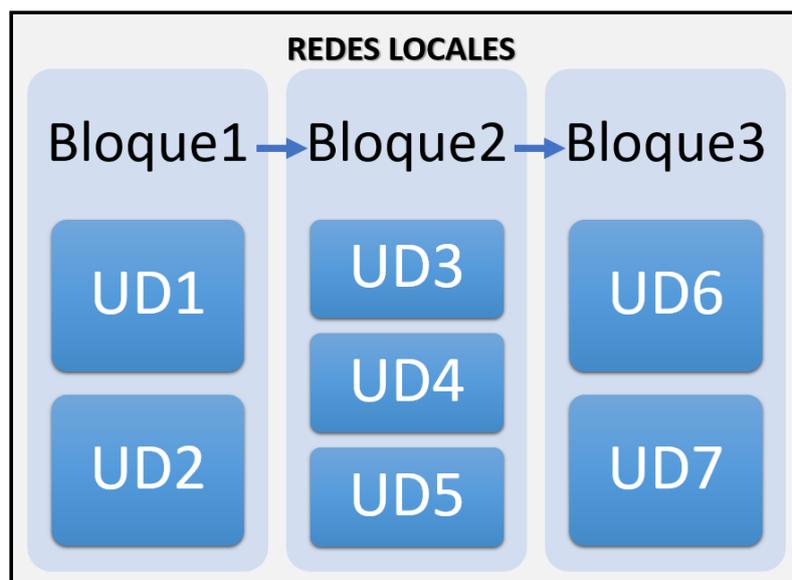


Ilustración 2: Agrupación de las unidades didácticas (UD) en bloques de contenidos y su secuencia de impartición.

La secuenciación viene determinada por el hecho de que, aunque los diferentes bloques tienen diferentes contenidos, estos mantienen una relación de dependencia por lo que algunos contenidos del primer bloque son necesarios en el segundo bloque y de forma similar, algunos de los contenidos del segundo bloque también son necesarios para el desarrollo del último bloque de contenidos. Del mismo modo, el desarrollo de las actividades prácticas va creciendo en complejidad, tomando como base las herramientas aprendidas en el recorrido secuencial. Se muestra la estructura de contenidos en la Ilustración 3.

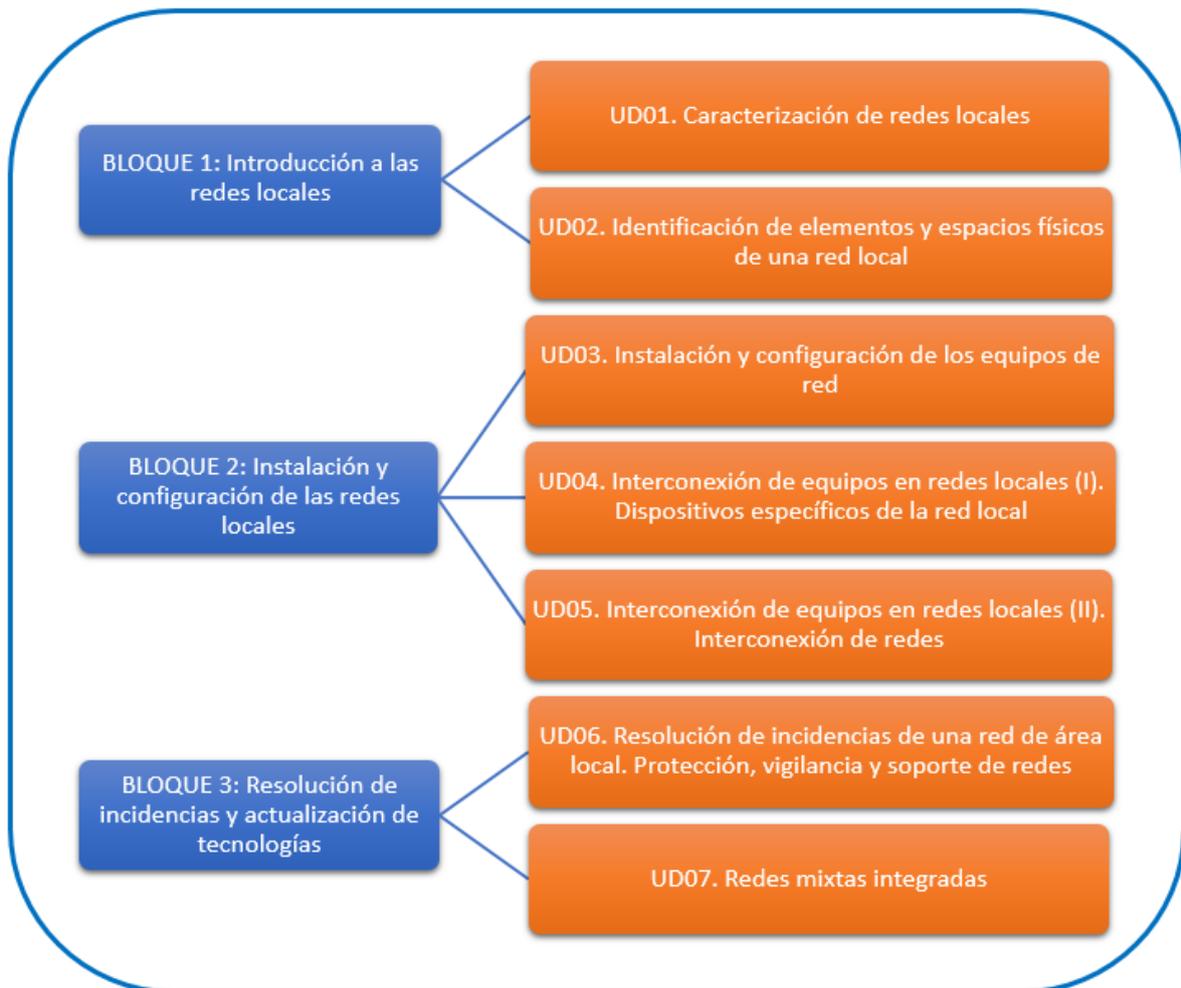


Ilustración 3: Estructura de contenidos

El curso tendrá un total de 224 sesiones. Cada sesión tendrá una duración de 55 minutos, de forma que exista un pequeño descanso de 5 minutos entre las mismas, o bien, se puedan organizar descansos de 10 o 15 minutos aunando sesiones.

La distribución en tres bloques de contenidos pretende agrupar los contenidos abordando las redes desde sus distintos aspectos y de forma progresiva, quedando una división de las sesiones como sigue:

Tabla 1: Secuenciación de las unidades didácticas distribuidas en los bloques de contenidos

Bloque de contenidos 1: Introducción a las redes locales. (84 sesiones)	
Unidades Didácticas	Sesiones
UD01. Caracterización de redes locales	42
UD02. Identificación de elementos y espacios físicos de una red local. Medios de transmisión	42
Total	84
Bloque de contenidos 2: Instalación y configuración de las redes locales. (77 sesiones)	
Unidades Didácticas	Sesiones
UD03. Instalación y configuración de los equipos de red	42
UD04. Interconexión de equipos en redes locales (I). Dispositivos específicos de la red local	21
UD05. Interconexión de equipos en redes locales (II). Interconexión de redes	14
Total	77
Bloque de contenidos 3: Resolución de incidencias en redes locales. (84 sesiones)	
Unidades Didácticas	Sesiones
UD06. Resolución de incidencias de una red de área local. Protección, vigilancia y soporte de redes	35
UD07. Redes mixtas integradas. Proyecto.	49
Total	84

Será conveniente poder impartir, al menos, dos sesiones seguidas de clase, porque esto nos facilita la ejecución de prácticas, tanto en el taller como en el aula, ya que el desarrollo de la mayoría de las prácticas ocupa aproximadamente un mínimo de sesión y media o dos sesiones.

4.2 Distribución de contenidos e instrumentos de aprendizaje

A continuación, se relacionarán los contenidos de cada unidad didáctica, indicando el número de sesiones que se propone para su desarrollo y situando los instrumentos de aprendizaje que se plantean como adecuados en cada punto, esto es, las actividades y prácticas propuestas. Al final de cada unidad didáctica se propone la realización de una prueba escrita, con el fin de evaluar los contenidos adquiridos por el estudiante durante el curso.

4.2.1 Bloque 1: Introducción a las redes locales

En el primer bloque de contenidos de 84 sesiones se pretende realizar una introducción a las redes en general y a las redes de área local en particular, teniendo en consideración que los posibles estudiantes del curso pueden ser de muy distinta índole, y con grados de conocimiento de partida muy variados.

UNIDAD DIDÁCTICA 1

En la primera unidad didáctica se presentan conceptos básicos fundamentales para comprender la evolución de las redes desde sus principios. Distintos tipos de red y distintos modelos de arquitectura que conforman las redes híbridas que existen en la actualidad.

A continuación, se muestra la Tabla 3 donde se relacionan la secuencia de contenidos de la Unidad Didáctica 1 con el número de sesiones que se considera convenientes para el adecuado desarrollo, junto con los instrumentos de aprendizaje referenciados en la Tabla 2.

Tabla 2: Relación de actividades y prácticas de la Unidad Didáctica 1

REFERENCIA	NOMBRE
CA1	Cuaderno de Actividades 1
CR1	Cuaderno de Actividades de Refuerzo 1
Pract1.1	Práctica 1.1_Mi red local
Pract1.2	Práctica 1.2_Mi día en línea
Pract1.3	Práctica 1.3_Dibuja tu concepto de Internet
Pract1.4	Práctica 1.4_Construyendo una red sencilla
TI1	Trabajo de investigación 1: Investigación de redes
TI2	Trabajo de investigación 2: Modelo OSI
PE1	Prueba escrita 1

Tabla 3: Organización secuencial de la Unidad Didáctica 1

Unidad Didáctica 1. Caracterización de redes locales (42 sesiones)			
Secuencia	Contenidos	Sesiones	Instrumentos de aprendizaje
0	Presentación del curso Presentar las unidades didácticas, la temporalidad y los criterios de evaluación. Prueba de valoración de nivel inicial.	2	-
1	Introducción: La comunicación Introducción a los sistemas de comunicación. Evolución de los mismos. Internet. El proceso de la comunicación. Tipos de señales	2	Pract1.1
2	Las redes de ordenadores Cómo se hace posible esta comunicación. Por qué. Redes en el mundo empresarial. Redes para los usuarios domésticos.	2	Pract1.2
3	Clasificación de las redes Clasificación atendiendo a la titularidad de la red Clasificación atendiendo a la topología Clasificación atendiendo a la localización geográfica Clasificación atendiendo a la tecnología Clasificación atendiendo a la relación funcional	9	CA1 Pract1.3
4	Elementos de la red Dispositivos finales, servidores, medios de transmisión, dispositivos intermedios, tarjetas de interfaz de red y software	2	CA1 TI1
5	Arquitectura de redes Topología física vs lógica Protocolo de red y familias de protocolos Arquitectura basada en niveles o capes	6	CA1
6	Modelo de referencia OSI Principios teóricos Niveles y agrupación en bloques Por qué es necesario OSI Unidad de Datos de Protocolos Niveles orientados a la red Nivel de transporte Niveles orientados a la aplicación Modelo OSI vs TCP/IP	6	CA1 Pract1.4
7	Trabajo de investigación	9	TI2

	Creación de un esquema de cada nivel OSI, partiendo de un sinóptico con hipervínculos		
8	Repaso de la unidad Repaso completo de la unidad con los esquemas que se han ido realizando y realización de un Kahoot	2	CR1
9	Prueba Escrita Prueba escrita que permitirá evaluar los conocimientos adquiridos por el estudiante del curso.	2	PE1

UNIDAD DIDÁCTICA 2

En la segunda unidad didáctica comenzamos a adentrarnos en las redes de comunicaciones desde una vista específicamente física, lo que se conoce como plano físico de una red. Se presentarán los distintos tipos de medios de transmisión que existen en la actualidad y las principales perturbaciones que afectan a cada medio, de modo que el estudiante adquiera la habilidad para distinguir en qué aplicaciones será mejor un tipo u otro. Se identificarán elementos y espacios para una red de área local.

La relación de instrumentos de aprendizaje se referencian en la Tabla 4, y la interrelación existente entre entre secuencia de contenidos, sesiones planteadas y actividades en la Tabla 5.

Tabla 4: Relación de actividades y prácticas de la Unidad Didáctica 2

REFERENCIA	NOMBRE
CA2	Cuaderno de Actividades 2
Pract2.1	Práctica 2.1_ Introducción a Packet Tracer
Pract2.2	Práctica 2.2_ Creando y cableando dispositivos en Packet Tracer
Pract2.3	Práctica 2.3_ Configurando dispositivos
Pract2.4	Práctica 2.4_ Creación de una red sencilla
Pract2.5	Práctica 2.5_ Conexión de una LAN por cable y una LAN inalámbrica
Pract2.6	Práctica 2.6_ Verificar la conectividad de la red con Ping y PDU's
Pract2.7	Práctica 2.7_ Vista física de Packet Tracer
Pract2.8	Práctica 2.8_ Crimpado RJ45: directo/cruzado y verificación
TI3	Trabajo de investigación 3: Medios de transmisión
PE2	Prueba escrita 2

Tabla 5: Organización secuencial de la Unidad Didáctica 2

Unidad Didáctica 2. Identificación de elementos y espacios físicos de una red local. Medios de transmisión (42 sesiones)			
Secuencia	Contenidos	Sesiones	Instrumentos de aprendizaje
1	Transmisión de señales Amplitud, frecuencia y fase de una señal Medidas del S.I. Herramienta web de medida. Señales analógicas Señales digitales. Principios fundamentales.	2	CA2
2	Perturbaciones de la transmisión Atenuación, interferencia electromagnética, diafonía y dispersión. Modulación (AM-FM-PM). Canal de comunicación: banda base, banda ancha y throughput.	4	CA2 Pract2.1
3	Los cables de pares y metálicos UTP, FTP y STP. UTP vs STP. Clasificación: categorías y clases. Cableado horizontal y cableado vertical.	5	CA2 Pract2.2
4	Cable coaxial Coaxial de banda base y coaxial de banda ancha. Conectores	2	CA2
5	Sistemas de fibra óptica Componentes. Partes. Tipos: Monomodo y multimodo. Modo de transmisión. Protección y soporte. Ventajas e inconvenientes. Conectores. UTP vs F.O.	4	CA2 Pract2.3
6	Sistemas inalámbricos Alteraciones: reflexión, difracción y dispersión. Frecuencias de propagación. Formas de transmisión. Ondas de radio. Microondas. Ondas infrarrojas. Ondas de luz.	2	CA2
7	Dispositivos de conexión de cables Conectores para redes.	2	CA2 Pract2.4

	Conectores para fibra óptica. Herramientas utilizadas en la conexión. Componentes utilizados en la red.		
8	El cableado de la red El proyecto de instalación. Elementos de la instalación: armarios, canaletas, suelos y techos técnicos. La instalación eléctrica y de aire acondicionado. Elementos de conectividad: Patch panels y latiguillos, conexiones a rosetas RJ45, confección de latiguillos RJ45 y etiquetado de los cables.	5	CA2 Pract2.5
9	Cableado estructurado y certificado Estructuración del cable. Certificación de la instalación.	3	CA2 Pract2.6
10	Instalación del CPD Caracterización.	1	Pract2.7
11	Gestión de residuos Gestión de residuos, políticas de tratamiento.	1	CA2
12	Trabajo de investigación Medios de transmisión y simulación de un CPD	8	TI3
13	Repaso de la unidad Repaso completo de la unidad con los esquemas que se han ido realizando y realización de un Kahoot	1	Pract2.8
14	Prueba Escrita Prueba escrita que permitirá evaluar los conocimientos adquiridos por el estudiante del curso.	2	PE2

4.2.2 Bloque 2. Instalación y configuración de las redes locales.

Este segundo bloque, de 77 sesiones, presentará el diseño lógico de las redes locales, incluyendo la clasificación y configuración de los distintos dispositivos que las componen.

UNIDAD DIDÁCTICA 3

La Unidad Didáctica 3 comenzará con conceptos básicos necesarios, como los sistemas de numeración binario, decimal y hexadecimal, y las posibles conversiones entre los mismos, para desarrollar completamente el método de obtención del cuarteto de parámetros básicos que definen una red (identificador de red, primera dirección útil, última dirección útil y difusión).

Una vez presentados conceptos como las clases de redes, la notación CIDR, y los parámetros que definen una red, se continuará con la creación de subredes dentro de una red local, utilizando técnicas de *subnetting* con máscara fija y variable.

A continuación se interrelacionan en la Tabla 7 la secuencia de los contenidos de la unidad, con el número de sesiones que se proponen, y los instrumentos de aprendizaje referenciados en la Tabla 6.

Tabla 6: Relación de actividades y prácticas de la Unidad Didáctica 3

REFERENCIA	NOMBRE
CA3	Cuaderno de Actividades 3
CR2	Cuaderno de Actividades de refuerzo y ampliación 2
Pract3.1	Práctica 3.1_ Diseño de una red de clase C con 3 subredes aplicando Subnetting
Pract3.2	Práctica 3.2_ Diseño de una red de clase C con 8 subredes aplicando Subnetting
Pract3.3	Práctica 3.3_ Diseño de una red de clase B con 4 subredes aplicando Subnetting
Pract3.4	Práctica 3.4_ Simulación y Verificación del diseño de una red Clase C con Packet Tracer
Pract3.5	Práctica 3.5_ Diseño de una red de clase C aplicando la técnica de VLSM
TI4	Trabajo de investigación 4: Utilidades propias de TCP/IP
PE3	Prueba escrita 3

Tabla 7: Organización secuencial de la Unidad Didáctica 3

Unidad Didáctica 3. Instalación y configuración de los equipos de red (42 sesiones)			
Secuencia	Contenidos	Sesiones	Instrumentos de aprendizaje
1	Los protocolos básicos en TCP/IP La familia de protocolos TCP/IP. Descripción de los protocolos básicos en TCP/IP: IP, ICMP, TCP, UDP, ARP y RARP.	3	CA3
2	Conversión (binario-decimal) Conversiones binario-decimal y decimal-binario.	2	CA3

3	El direccionamiento de red en TCP/IP El sistema de direccionamiento IPv4. Redes de clase A, clase B, clase C, clase D y clase E. Usos específicos. IPv4 vs IPv6. Máscaras de subred. Notación CIDR.	10	CA3
4	Cálculo de direcciones IP Obtención de los parámetros básicos	3	CA3
5	Subnetting Concepto de Subnetting. Casos prácticos.	10	CA3 Práctica 3.1 Práctica 3.2 Práctica 3.3 Práctica 3.4
6	Subnetting con VLSM Casos prácticos.	4	Práctica 3.5
7	Protocolos de nivel superior Descripción de los protocolos: FTP, HTTP, SNMP, RPC, SMTP, POP, IMAP.	2	CA3
8	Utilidades propias de redes TCP/IP Utilidades nslookup, ping, arp, ipconfig, netstat, traceroute, route, ftp y tftp, telnet y ssh	2	CA3
9	Trabajo de investigación Utilidades propias de TCP/IP	2	TI4
10	Repaso de la unidad Repaso completo de la unidad con los esquemas que se han ido realizando y realización de un Kahoot	2	CR2
11	Prueba Escrita Prueba escrita que permitirá evaluar los conocimientos adquiridos por el estudiante del curso.	2	PE3

UNIDAD DIDÁCTICA 4

La Unidad Didáctica 4 y la siguiente se centrarán en la interconexión de equipos en redes locales. Para ello, se considera conveniente dividir dichos dispositivos según su modo de interacción en la red. En la Unidad Didáctica 4 se presentan los dispositivos que actúan en los niveles 1 y 2 del modelo OSI, correspondientes a la capa física y a la capa de enlace de datos, respectivamente.

Se presentan las referencias de actividades y prácticas de la Unidad Didáctica 4 en la Tabla 8, y se relacionan con los contenidos en la Tabla 9.

Tabla 8: Relación de actividades y prácticas de la Unidad Didáctica 4

REFERENCIA	NOMBRE
CA4	Cuaderno de Actividades 4
Pract4.1	Práctica 4.1_ Configurar una red local básica con punto de acceso y hub
Pract4.2	Práctica 4.2_ Enlace de redes híbridas
Pract4.3	Práctica 4.3_ Configuración de VLAN's en Packet Tracer
TI5	Trabajo de investigación 5: Configuración básica del switch y prueba de conectividad en red local.

Tabla 9: Organización secuencial de la Unidad Didáctica 4

Unidad Didáctica 4. Interconexión de equipos en redes locales (I). Dispositivos específicos de la red local (21 sesiones)			
Secuencia	Contenidos	Sesiones	Instrumentos de aprendizaje
1	El acceso remoto a la red Tecnología DSL Módems de cable Módems de fibra	2	CA4
2	Repetidores y concentradores Repetidores Hub o concentradores El punto de acceso (AP)	4	CA4 Pract4.1
3	Puentes Puentes locales y remotos	4	CA4 Pract4.2
4	Conmutadores Switch o conmutadores	4	CA4 Pract4.3
5	Tecnologías específicas de los conmutadores Redes de área local virtuales, VLAN Enlaces entre conmutadores	3	CA4
6	Trabajo práctico de investigación Configuración básica del switch y prueba de conectividad en red local	4	TI5

UNIDAD DIDÁCTICA 5

El router es el dispositivo de comunicación utilizado para la interconexión de redes. La Unidad Didáctica 5 se centrará en caracterizar dicho dispositivo y desgranar su modo de funcionamiento. Al finalizar ésta unidad, el estudiante deberá ser capaz de diseñar y construir una red local sencilla con, al menos, dos dispositivos de los expuestos en el curso.

A continuación, se presenta la relación de instrumentos de aprendizaje de la Unidad Didáctica 5 en la Tabla 10, y la interrelación correspondiente con la secuencia de contenidos y sesiones propuestas en la Tabla 11.

Tabla 10: Relación de actividades y prácticas de la Unidad Didáctica 5

REFERENCIA	NOMBRE
CA5	Cuaderno de Actividades 5
Pract5.1	Práctica 5.1_ Red híbrida controlada por un router inalámbrico
Pract5.2	Práctica 5.2_ Red WAN entre tres ciudades
Pract5.3	Práctica 5.3_ Configuración de un firewall
Pract5.4	Práctica 5.4_ Visualización de las tablas de enrutamiento de host
TI6	Trabajo de investigación 6: Construcción de una red local sencilla con switch y router
PE4	Prueba escrita 4

Tabla 11: Organización secuencial de la Unidad Didáctica 5

Unidad Didáctica 5. Interconexión de equipos en redes locales (II). Interconexión de redes (14 sesiones)			
Secuencia	Contenidos	Sesiones	Instrumentos de aprendizaje
1	El acceso a las redes WAN Protocolos de acceso remoto Servicios de acceso remoto	4	CA5 Pract5.1 Pract5.2
2	El encaminador o router Características generales de los routers Tipos de encaminadores Protocolos de encaminamiento Configuración del enrutamiento Configuración de la tabla de rutas	4	CA5 Pract5.3 Pract5.4
3	Trabajo practico de investigación Creación y configuración de una red local sencilla con switch y router	3	TI6

4	Repaso de la unidad Repaso completo de la unidad con los esquemas que se han ido realizando y realización de un Kahoot	1	
5	Prueba Escrita Prueba escrita que permitirá evaluar los conocimientos adquiridos por el estudiante del curso.	2	PE4

4.2.3 Bloque 3. Resolución de incidencias en redes locales y redes mixtas integradas.

En este tercer y último bloque están incluidas las unidades didácticas 6 y 7, que pretenden completar, con 84 sesiones, los conocimientos sobre las redes de área local. Son dos unidades independientes.

UNIDAD DIDÁCTICA 6

En la Unidad Didáctica 6, se presentarán los contenidos relacionados con la resolución de incidencias en la red de área local. Identificando medidas de protección, vigilancia y soporte de redes. Material complementario fundamental en la labor de cualquier técnico especialista en redes locales. A tal fin, se presenta la Tabla 12 con la relación de actividades y prácticas propuestas, y la Tabla 13 con la interrelación planteada entre secuencia de contenidos, sesiones e instrumentos de aprendizaje.

Tabla 12: Relación de actividades y prácticas de la Unidad Didáctica 6

REFERENCIA	NOMBRE
CA6	Cuaderno de Actividades 6
Pract6.1	Práctica 6.1_ Uso de Wireshark
Pract6.2	Práctica 6.2_ Configuración de contraseñas seguras y SSH
Pract6.3	Práctica 6.3_ Herramientas de administración de redes
TI7	Trabajo de investigación 7: Amenazas de seguridad en la red
PE5	Prueba escrita 5

Tabla 13: Organización secuencial de la Unidad Didáctica 6

Unidad Didáctica 6. Resolución de incidencias en una red de área local. Protección, vigilancia y soporte de redes (35 sesiones)			
Secuencia	Contenidos	Sesiones	Instrumentos de aprendizaje
1	Condiciones físicas y ambientales de la instalación Ubicación de los armarios de cableado Tamaño de los armarios de cableado Temperatura y humedad Ruidos e interferencias electromagnéticas Inundaciones, iluminación e incendios Estrategias: parámetros de rendimiento	4	Pract6.1
2	Incidencias físicas e incidencias lógicas en redes locales Incidencias físicas más comunes Incidencias lógicas más comunes	4	CA6
3	Monitorización de redes cableadas e inalámbricas Monitores de rendimiento Monitores de red Protocolo básico de gestión de red (SNMP) Analizadores de red Logs del sistema	4	Pract6.2
4	Herramientas de diagnóstico Herramientas para el hardware Herramientas software	7	Pract6.3
5	Vigilancia y mantenimiento de la red Del tráfico de red Del rendimiento Visor de eventos Consolas de gestión remota Firewall	5	CA6
6	Trabajo de investigación Amenazas de seguridad en la red	9	TI7
7	Prueba Escrita Prueba escrita que permitirá evaluar los conocimientos adquiridos por el estudiante del curso.	2	PE5

UNIDAD DIDÁCTICA 7

La Unidad Didáctica 7 es la última unidad de este tercer bloque y del curso. Se pretende ahondar en contenidos técnicos más avanzados, desde el estudio de la versión 6 del protocolo de Internet hasta las exponencialmente crecientes tecnologías inalámbricas. La relación de actividades y prácticas de esta unidad 7 se referencia en la Tabla 14. La propuesta secuencial de contenidos, con las sesiones correspondientes y los instrumentos de aprendizaje de la unidad 7 se interrelacionan en la Tabla 15.

Tabla 14: Relación de actividades y prácticas de la Unidad Didáctica 7

REFERENCIA	NOMBRE
CA7	Cuaderno de Actividades 7
Pract7.1	Práctica 7.1_Creación de un diagrama de flujo
Pract7.2	Práctica 7.2_Configuración de la seguridad inalámbrica en una red doméstica
Pract7.3	Práctica 7.3_Fuentes de datos abiertas
Pract7.4	Práctica 7.4_Examinar NAT y resolver problemas de conexión
Pract7.5	Práctica 7.5_Configuración de direccionamiento en IPv6
TI8	Trabajo de investigación 8: PROYECTO Diseño y simulación de una red de área local

Tabla 15: Organización secuencial de la Unidad Didáctica 7

Unidad Didáctica 7. Redes mixtas integradas (49 sesiones).			
Secuencia	Contenidos	Sesiones	Instrumentos de aprendizaje
1	Introducción La evolución de la transformación digital La digitalización transforma los negocios Conexión global El futuro de las redes	6	Pract7.1
2	Redes inalámbricas Bluetooth Wi-Fi: funcionamiento, seguridad, estándares. Integración Wi-Fi con red cableada El estándar WiMAX Wi-Fi vs WiMAX WWAN Cableado vs inalámbrico	9	CA7 Pract7.2
3	Big Data y Cloud computing Grandes conjuntos de datos, datos masivos La nube y la computación en la nube	6	Pract7.3

	Tipos de gráficos Análisis de datos masivos para el uso eficaz en la empresa. La red intuitiva		
4	Inteligencia artificial Inteligencia artificial y aprendizaje automático (ML) Aprendizaje automático e IoT Redes basadas en la intención (IBN)	6	CA7 Pract7.4
5	IPv6 Necesidad de IPv6 Técnicas de migración de IPv4 a IPv6 Direccionamiento IPv6: representación Tipos de direcciones IPv6: unicast, multicast, anycast. Direcciones especiales	7	CA7 Pract7.5
6	Trabajo de investigación PROYECTO Diseño y simulación de una red de área local	15	TI8

5 Sistema de evaluación

En el curso se deberán evaluar competencias profesionales, y, en este sentido, es importante distinguir entre capacidad y competencia. Tener capacidades no significa ser competente. La competencia no reside en los recursos (capacidades) sino en la movilización misma de los recursos.

Las actividades de evaluación, presentarán una situación o problema, cercano a la realidad, con la finalidad de evaluar el nivel de conocimientos y habilidades adquiridas para la resolución de dicha situación. Añadido a esta práctica en la resolución, será muy importante saber gestionar la incertidumbre, y aprender a adaptarse a situaciones cambiantes, que aparecen continuamente en la realidad cotidiana de un técnico especialista en el diseño, montaje, y mantenimiento de redes.

La evaluación nos debe mostrar cómo actúa el estudiante y cómo ha usado los recursos disponibles para conseguir los objetivos. Estas situaciones serán complejas, y se deberán gestionar desde la total autonomía al estudiante, orientadas a la aplicación en el ámbito laboral.

Además, las actividades deberán ser atractivas para los alumnos, de modo que les motive a superarse. El papel del docente ha de ser meramente el de acompañar y orientar al alumnado, nunca el de llevarlo de la mano, pues en este curso estamos preparando a técnicos, ya titulados o no, para una especialidad profesional.

5.1 Tipos de evaluación

El sistema de evaluación principal que vamos a seguir es el de evaluación continua, sobre todo por tratarse de un curso muy práctico. Este sistema de evaluación continua deberá tener en cuenta la participación activa de los estudiantes, a partir del trabajo activo en las actividades propuestas, y la calidad de las soluciones aportadas.

A parte de este sistema de evaluación, durante todo el curso, se van a realizar otros tipos de evaluación:

Evaluación inicial: se realizará a partir de una prueba oral conjunta en la que se evaluarán varios aspectos que tienen relación con nuestra materia. Será importante validar los conocimientos de matemáticas (cálculos en diferentes bases numéricas), así como los conocimientos generales que se disponen de informática tanto a nivel físico (hardware) como lógico (sistemas operativos, software). Con esta evaluación inicial tendremos una visión clara de cuál es el nivel del alumnado, y nos dará una primera guía de los aspectos a los que deberemos dedicar más tiempo. Debemos tener en consideración el tipo de estudiantes del curso, ya que puede ser de muy distinta procedencia, tal y como se ha mencionado en el apartado 2 del trabajo.

Evaluación continua: de los cuadernos de actividades de aplicación de la teoría y de las prácticas, de cada una de las unidades didácticas. Las prácticas irán creciendo en dificultad con el recorrido secuencial de los contenidos. Estas actividades nos deberán permitir medir el nivel de competencia profesional alcanzado. Todas las actividades de aplicación teórica se resuelven oralmente en el conjunto, dando opción a la interacción continua de los estudiantes. Las actividades que realizarán son muy numerosas e importantes.

Evaluación final: por cada unidad didáctica está previsto realizar una prueba final para validar los conocimientos de forma individualizada, formando parte de la calificación final del curso. Además, al finalizar el mismo, se realizará un Proyecto en el que los alumnos realizarán un diseño completo y simulación de una red de área local propuesta.

Coevaluación: en cada bloque de contenidos se plantea la resolución de, al menos, un trabajo de investigación. Cada estudiante o estudiantes (si es posible se realiza en grupos de dos) expone su trabajo de investigación a los compañeros de curso y son los propios compañeros quienes puntúan el trabajo a través de un formulario (coevaluación).

5.2 Instrumentos de aprendizaje evaluables

Para la realización de la evaluación utilizaremos los siguientes instrumentos de aprendizaje:

- Cuadernos de actividades (CA) y Cuadernos de Prácticas (Pract)
- Trabajos de investigación (TI)
- Pruebas escritas (PE)
- Actividades de refuerzo y ampliación (CR)

5.2.1 Cuadernos de Actividades (CA) y Cuadernos de Prácticas (Pract)

Para cada unidad didáctica dispondremos de un Cuaderno de Actividades y de un Cuaderno de Prácticas, donde se incluirán todas las prácticas, tanto de simulación como de taller a realizar. Estas actividades estarán interrelacionadas entre ellas, pues en cada una de ellas se irán descubriendo elementos que son necesarios para completar las siguientes a realizar.

El Cuaderno de Actividades se compone de actividades de aplicación práctica de la teoría vista en clase. Tras cada explicación teórica con interacción, se dedica un espacio de tiempo a desarrollar de modo individual las actividades subyacentes de la sección de teoría. Y posteriormente se ponen en común las soluciones propuestas por ellos, permitiendo el debate.

El Cuaderno de Prácticas (en el aula se trabajarán como prácticas individuales) son actividades de simulación de redes (con Packet Tracer, ver apartado 7.1) o actividades de taller (con Tera Term o Wireshark, ver apartado 7.1), donde cada estudiante debe configurar los dispositivos con alguna singularidad diferente al resto de sus compañeros de curso. Por ejemplo, nombrando todos los dispositivos con sus credenciales de NombreApellido, o utilizando direcciones lógicas distintas. Con esta técnica tratamos de fomentar que cada uno realice su propio trabajo.

En el apartado 8 del presente trabajo se pueden consultar con detalle las actividades y prácticas de cada unidad didáctica.

5.2.2 Trabajos de investigación (TI)

Junto a estos cuadernos de trabajo, también tiene un peso singular la exposición y trabajo de investigación que realizan en cada bloque. En estas exposiciones se trabajan, no solamente los

conocimientos técnicos adquiridos y que han tenido que profundizar, sino aspectos clave como hablar en público, defender su trabajo, colaborar en equipo, creatividad para presentar su producto, etc.

En el mundo de la informática y particularmente en el mundo de las redes, no existe una solución única para la resolución de un problema, sino que nos podemos encontrar varias igual de válidas. Es por ello que será importante establecer una rúbrica de evaluación de aquellas actividades que lo precisen, especialmente las prácticas y trabajos, donde el alumno tenga claro cómo se le va a evaluar. Dichas rúbricas por ejemplo pueden tener en cuenta, la simplicidad de la solución, la calidad de la presentación, la exposición oral, etc. Un ejemplo de rúbrica para el proyecto de simulación de una red local será como se muestra en la Tabla 16:

Tabla 16: Ejemplo de rúbrica de evaluación

	Insuficiente (<5)	Bien (5-6)	Notable (7-8)	Excelente (9-10)
Exposición (25%)	No ha habido una presentación ordenada y básica de objetivos, contenidos y conclusiones	La presentación de los contenidos no ha sido clara ni ordenada. No se han mencionado objetivos, contenidos y conclusiones.	La presentación de los contenidos ha sido adecuada. No se han expuesto conclusiones o no han estado de acuerdo con el objetivo propuesto	Se ha realizado una correcta y ordenada presentación de los objetivos, contenidos y conclusiones del trabajo
Contenido (20%)	Los contenidos no son suficientes, faltan contenidos importantes	Los contenidos son suficientes pero faltan contenidos relevantes	Los contenidos son adecuados	Los contenidos son adecuados, se centran en los aspectos relevantes y pueden incluir detalles de interés
Material de soporte (15%)	Es poco visual y poco trabajado. La información del soporte se lee en su práctica totalidad	El material no es adecuado, aunque es visualmente creativo y original. O es poco visual aunque el material es adecuado	Bien trabajado visualmente pero no muestra los contenidos más importantes. O es adecuado al contenido y está bien trabajado visualmente pero hay exceso de texto	Muy bien trabajado y adecuado a los contenidos
Lenguaje no verbal (10%)	El lenguaje utilizado no es correcto	Hay errores de expresión y de vocabulario	El lenguaje es correcto y adecuado en general	Muy buena locución, adecuación y uso de vocabulario técnico
Respuesta a las preguntas que se formulan (10%)	No ha sabido responder correctamente las preguntas después de la exposición	Solo ha contestado a parte de las cuestiones	Sí, pero faltan argumentos	Si ha contestado correctamente
Adecuación temporal	Demasiado corto o demasiado largo. Distribución irregular del tiempo entre los miembros del grupo	Distribución equitativa, pero el tiempo total no es adecuado. O tiempo total adecuado pero distribución irregular	Pequeña desviación del tiempo, parcial o total	Distribución equitativa y tiempo total adecuado
Ortografía y sintaxis del contenido (5%)	El contenido tiene muchos errores de ortografía y errores sintácticos o lingüísticos. Formato irregular	Contenido con algunos errores sintácticos o lingüísticos.	Contenido sin errores sintácticos o lingüísticos pero con algunos errores de ortografía	Contenido bien estructurado sintácticamente y sin errores de ortografía. Formato uniforme

5.2.3 Pruebas escritas (PE)

Tras finalizar cada unidad didáctica procederemos a hacer una prueba escrita. A excepción de la última unidad didáctica, en la que se desarrollará un proyecto de simulación de una red local completo, a modo de recopilación de todo lo aprendido en las unidades anteriores.

En la situación de que el curso propuesto se concrete en un Ciclo Formativo, la prueba escrita podrá consistir en un examen. Estos exámenes o pruebas escritas se realizarán en el aula, y se compondrán de una parte de test, sobre cuestiones teóricas que deben conocer, y otra parte de desarrollo, donde deberán resolver problemas del tipo de resolución matemática de asignación de subredes, o de planteamiento de una solución para una situación real concreta, etc.

Si la prueba escrita se dirige a un alumnado procedente de empresas, la prueba escrita se podrá plantear como una actividad práctica escrita donde se plantee la resolución de un problema de redes intercalando cuestiones teóricas.

5.2.4 Actividades de refuerzo y ampliación (CR)

Tanto las actividades de refuerzo como las de ampliación de conocimientos estarán abiertas a todos los estudiantes del curso, aunque dependerá de ellos usarlas o no. Las actividades de refuerzo serán actividades que principalmente se facilitarán a aquellos estudiantes que necesiten de una ayuda para llegar al nivel del resto del grupo, bien porque tengan una falta de conocimiento de base, como para reforzar aspectos de la materia de redes que les cueste asumir. Las actividades de refuerzo y ampliación no tendrán implicación en la nota, si ésta define aprobar o suspender, pero sí que se considerarán en el momento de la evaluación final, como nota extraordinaria, para redondear la nota final.

5.3 Sistema de calificaciones

Aspectos importantes a considerar en la calificación:

- Para superar el curso completo será necesario que las notas de todas las unidades didácticas sean iguales o superiores a 5.
- La calificación final del curso se calculará usando la siguiente fórmula:

$$Q_T = 0,3*Q_{B1} + 0,3*Q_{B2} + 0,4*Q_{B3}$$

Siendo,

Q_T la calificación final del curso

Q_{B1} la calificación del Bloque de contenidos 1

Q_{B2} la calificación del Bloque de contenidos 2

Q_{B3} la calificación del Bloque de contenidos 3

La nota final de cada bloque de contenidos Q_{Bi} se calculará a partir de la siguiente fórmula:

$$Q_{Bi} = 0,4 * NA_{Bi} + 0,4 * PE_{Bi} + 0,2 * TP_{Bi}$$

La **Nota Actividades (NA_{Bi})**, se calculará haciendo la media de todas las actividades del bloque i , Cuadernos de actividades teóricas y prácticas, que se han realizado en el recorrido de las unidades que componen el bloque de contenidos. Tanto actividades de aplicación práctica de la teoría, como prácticas, de simulación o taller. Para poder aplicar esta nota a la ecuación de la nota final del bloque es necesario que el resultado sea igual o superior a una puntuación de 5.

$$NA_{Bi} = \text{Promedio } (NA_{UDi})$$

La nota de **Prueba Escrita (PE_{Bi})**, se calculará haciendo la media ponderada de las pruebas escritas realizadas tras cada unidad didáctica i , dentro de un mismo bloque de contenidos. Bien sea la realización de un examen o una propuesta práctica, según el grupo en cuestión. Será necesario que cada nota de prueba escrita sea igual o superior a 4 para poder aplicar la ecuación. Se incluirá como nota de examen el resultado obtenido del Proyecto final, a modo de prueba escrita de la Unidad Didáctica 7.

$$PE_{Bi} = \text{Promedio } (PE_{UDi})$$

La nota de **Trabajo Personal (TP_{Bi})**, se obtendrá de la valoración del trabajo y de la actitud del estudiante en el desarrollo de las clases. El trabajo en equipo, la puntualidad, la implicación en el curso, las actividades que se realizan no evaluables, serán criterios para la obtención del porcentaje total de ésta nota.

5.4 Evaluación del funcionamiento del curso

Esta propuesta de curso fija unos objetivos de aprendizaje, pero es una propuesta que puede y debe revisarse y cambiarse para adaptarse a las diferentes situaciones que nos vamos a encontrar. Para la evaluación de su funcionamiento, propongo estos métodos:

- Una autoevaluación donde el docente podrá valorar si la programación se está adaptando a los usuarios. Se podrá ver objetivamente en función de si los estudiantes están siguiendo las actividades, las clases magistrales participativas, las prácticas, ..., en definitiva, si se está siguiendo el ritmo previsto del curso.
- Una evaluación por parte de los estudiantes, en formato cuestionario anónimo, donde se evaluará también la tarea docente. Esta evaluación se deberá realizar tras finalizar completamente el primer bloque de contenidos. Un ejemplo de éste cuestionario podría ser como el que se muestra en la Ilustración 4.

VALORACIÓN DE LA ACTIVIDAD FORMATIVA Y DOCENTE						
Valora los siguientes aspectos de la formación que recibes en una escala de 1 a 5, siendo 1 "nada de acuerdo" y 5 "muy de acuerdo". Marca con una X.						
1. Organización		1	2	3	4	5
1.1. Se me ha informado de la planificación del curso						
1.2. Se me ha informado de los criterios de evaluación						
2. Contenidos y metodología						
2.1. Se me han explicado los contenidos						
2.2. Los contenidos se ajustan a lo que me esperaba						
2.3. La forma de trabajar en clase ayuda a aprender						
2.4. Me queda claro lo que hay que saber para aprobar						
2.5. La distribución de teoría y práctica es adecuada						
3. Sobre el Docente						
3.1. Su forma de impartir me ayuda a aprender						
3.2. El docente conoce el tema de trabajo						
3.3. Responde a las cuestiones que se le plantean						
3.4. El clima que genera en la clase ayuda a aprender.						
3.5. Me atiende de acuerdo con mis capacidades.						
4. Medios y recursos						
4.1. El material de estudio que facilita el profesor/a sirven de ayuda						
4.2. El material de estudio está actualizado						
4.3. Los diferentes medios utilizados por el profesor (vídeos, juegos interactivos, etc.) me han ayudado						
5. Valoración general						
5.1. Considero que he adquirido los conocimientos y capacidades de éste primer bloque						
5.2. Creo que el curso evoluciona adecuadamente						
5.3. En la clase existe cohesión y las relaciones con mis compañeros son buenas						
5.4. Mi grado de satisfacción general es bueno						
6. Observaciones (respuesta libre)						

Ilustración 4: Modelo de evaluación de la actividad docente por parte de los estudiantes

6 Metodología

Sobre las metodologías que vamos a utilizar, intentaremos dejar atrás aquellas en las que se consideraba al aprendiz como un recipiente vacío de conocimiento, y apostaremos por aquellas donde el estudiante construye su propia enseñanza a partir de los conocimientos y destrezas acumulados y de la propia experiencia.

Las metodologías que se van a utilizar en este curso son las que se describen a continuación.

6.1 Clase magistral participativa

La clase magistral participativa⁵ fomenta la participación del alumnado usando diferentes técnicas como la utilización de preguntas, el planteamiento y resolución de problemas, fomentar algún tipo de debate puntual, etc. Este tipo de metodología se basa en tres pilares: motivar al estudiante, organizar los contenidos y facilitar la información y comprensión. Ayuda a incrementar las capacidades para resumir, interpretar, aplicar, analizar, diferenciar lo importante, integrar, valorar, desarrollar la memoria y el pensamiento lógico, etc.

Dado que nuestro curso es principalmente práctico, sólo se utilizará esta metodología para la exposición de los contenidos más teóricos. En ella se incentivará la participación de los estudiantes, lanzando preguntas sobre determinados aspectos, o simulando situaciones. Además, se utilizarán ejemplos y se propondrán y resolverán problemas. También se apoyará la explicación de los contenidos con herramientas TIC, con la visualización de vídeos y/o tutoriales, todo ello con la intención de captar la atención del alumnado. Estas clases magistrales participativas estarán enfocadas para que sean realizadas en fracciones de tiempo relativamente cortas, a ser posible inferiores a 50 minutos, puesto que a partir de ese tiempo cuesta captar la atención de los estudiantes.

⁵ Valcárcel Pérez, M. V. (2009). Plan FIPRUMU VII. *La clase magistral*, 15. (U. d. Murcia, Ed.).
https://www.um.es/c/document_library/get_file?uuid=6a9e9620-b306-42c8-91e5-cef7198d39e4&groupId=316845

6.2 Aprendizaje basado en juegos

El aprendizaje basado en juegos⁶ es una técnica en la que se utilizan elementos propios de los juegos en ambientes no lúdicos. Su finalidad es transmitir mensajes, contenidos e incluso modificar comportamientos, mediante experiencias significativas y lúdicas con la intención de aumentar la motivación, y, por tanto, el interés y el compromiso de los estudiantes. Entre estos elementos propios del juego destacan la competitividad y los premios al margen de una estética más atractiva.

Algunos ejemplos serían las actividades lúdicas, los sistemas de recompensa, las barras de progreso, los logros. Existen plataformas y aplicaciones como Classcraft, Education minecraft, Glogster, Make it, CrossWord Labs, Decktoys, Mentimeter o Kahoot, que permiten llevar esto al terreno práctico.

Este tipo de aprendizaje utiliza juegos ya creados o inventados para la ocasión, con el fin de poder aprender y consolidar conocimientos a través de ellos. Existen algunos creados con el mero objetivo de divertir (suelen tener contenido académico) y aquellos pensados para enseñar algo concreto.

Resumiendo, podemos usar el juego como elemento de entretenimiento para el estudiante de una forma más o menos consciente aprenda conceptos, resuelva problemas, use estrategias, e incluso entrene su capacidad para superar ciertos retos bajo una determinada presión.

Nosotros, de entre los recursos disponibles, usaremos Kahoot⁷ y los juegos facilitados por el fabricante CISCO⁸. Kahoot es una herramienta para crear juegos de preguntas multijugador y así dinamizar los test, muy útil para revisar contenidos y preparar exámenes de una manera amena. Normalmente lo aplicaremos al final de cada Unidad Didáctica y con objeto de asentar lo visto.

6.3 Resolución de problemas

El aprendizaje basado en la resolución de problemas⁹ sitúa al estudiante en el centro del aprendizaje de forma que sea capaz de resolver de forma autónoma un problema o reto. La enseñanza desde esta

⁶ Gómez-Martín, M. A., Gómez-Martín, P. P. y González-Calero, P. A. (2004). Aprendizaje basado en juegos. *ICONO 14*, 2(4), 6.

⁷ Kahoot!. (2013). *Aplicación móvil educativa*. <https://create.kahoot.it>

⁸ Cisco Learning Network. (13 de febrero de 2020). *Games Arcade*. <https://learningnetwork.cisco.com/s/article/games-arcade>

⁹ Coronel, M. y Curotto, M. (2008). La resolución de problemas como estrategia de enseñanza y aprendizaje. *Revista Electrónica de Enseñanza de las Ciencias*, 7(2), 464.

perspectiva pretende poner el acento en actividades que plantean situaciones problemáticas cuya resolución requiere analizar, descubrir, elaborar hipótesis, confrontar, reflexionar, argumentar y comunicar ideas. Se centra fundamentalmente en aplicaciones de simulación, como Packet Tracer.

6.4 Aprendizaje colaborativo

Una de las competencias que tiene gran relevancia en las TIC es la capacidad de trabajo en equipo y colaborativo¹⁰, debido a que normalmente todos los proyectos son multidisciplinares y necesitamos poder colaborar y compartir con otros compañeros para poder conseguir desarrollar los proyectos de una manera óptima. Esta metodología fomenta la responsabilidad individual y grupal, las habilidades interpersonales y la interacción estimuladora. Para incentivar la colaboración entre los alumnos se realizan actividades en grupos. Se hará un seguimiento de las actitudes de trabajo y cooperación entre los miembros del grupo para asegurar que hemos conformado realmente grupos de trabajo cooperativo y no un grupo de alumnos trabajando de forma individual. En este sentido se identifica a un grupo cooperativo cuando a los estudiantes se les indica que trabajen juntos y ellos lo hacen de buen grado.

6.5 Píldoras educativas

Ésta es una metodología estrechamente relacionada con el uso de las TIC. Las píldoras se basan en los llamados Objetos de Aprendizaje, definidos como cualquier recurso digital que puede ser usado como soporte para el aprendizaje. En concreto las píldoras educativas¹¹ son recursos multimedia, habitualmente vídeos didácticos, que sirven como lecciones breves de algún tema específico.

Las actividades en las que se utilizará esta metodología son aquellas en las que se pretende que los estudiantes conozcan, amplíen y profundicen algunos conceptos que podrán ser de gran utilidad para la resolución de algunas de las actividades planteadas. Incluso algunos de los recursos multimedia pueden servir para consolidar o ampliar los conocimientos dados en clase. En este sentido se

¹⁰ Johnson, D., Johnson, R., y Holubec, E. (1994). *El aprendizaje cooperativo en el aula*. (G. Vitale, Trad.) Editorial Paidós.

¹¹ Serrano, E., M, R. y Russo, C. (sin fecha). *Píldoras educativas como instrumento de enseñanza universitaria*. http://educacaoaberta.org/wp-content/uploads/2017/07/IVWREA_serrano.pdf

proporcionará a los estudiantes algunos vídeos didácticos que se centran en temas específicos, serán vídeos de corta duración sobre conceptos específicos.

7 Recursos didácticos y espacios

7.1 Recursos didácticos

En este curso de redes de área local, la práctica tiene una gran importancia, por lo que dedicaremos gran parte de nuestro tiempo y de nuestros recursos didácticos a este tipo de actividades. En el mundo de las redes también es importante conocer bien las posibles soluciones, así como los dispositivos de los principales fabricantes, por lo que muchos de los recursos didácticos estarán enfocados en familiarizarnos con esas tecnologías de fabricante, y en nuestro caso usaremos recursos de CISCO por ser el mayor fabricante mundial de equipos de red, y porque muchos centros son centros asociados y certificadores, por lo que se facilitan equipos, manuales y soporte recurrentemente a los centros educativos para que los alumnos los puedan usar para aprender.

Los principales recursos propuestos para ser utilizados durante las unidades didácticas en el aula son:

1. Ordenador personal en el aula para el docente.
2. Pizarra y proyector.
3. Ordenador para cada uno de los estudiantes.
4. Una plataforma de trabajo centralizada en la nube, por ejemplo Office 365. Esta plataforma web es un paquete con Word, Excel, Stream, Teams, SharePoint, OneDrive, aplicaciones de trabajo habitual en el aula. Existen otras plataformas, como en Entorno G-Suite de Google, con utilidades similares.
5. Herramientas de edición de texto, presentaciones, o hojas de cálculo, que podrían estar incluidas en el paquete de Office 365.
6. Herramientas para la simulación, configuración y análisis de una red:
 - a. **Cisco Packet Tracer**¹²: programa de simulación de redes que permite a los estudiantes construir desde cero una red, configurar sus dispositivos para comunicarse, verificar las conexiones y experimentar con el comportamiento de la red sin necesidad de una instalación física de los elementos.

¹² Cisco Packet Tracer. (2020). *Software simulador de redes*. <https://www.netacad.com/courses/packet-tracer>

- b. **Wireshark**¹³: programa para monitorizar los paquetes de información que viajan por la red. Es un analizador de protocolos que se utiliza para analizar y solucionar problemas en redes, además de herramienta didáctica.
- c. **Tera Term**¹⁴: emulador de terminal de código abierto, utilizado para configurar dispositivos de interconexión como routers o switches.

Los recursos didácticos que se deben utilizar para el desarrollo de las unidades didácticas en el taller son:

1. Elementos de cableado estructurado: cable UTP, bastidores, canaletas, conectores.
2. Herramientas para la conexión del cableado: alicates, destornilladores, bridas, pelacables, crimpadoras, herramientas de impacto en parcheo, testers.
3. Dispositivos de red: switches, routers, puntos de acceso WIFI del fabricante CISCO.

7.2 El aula y el taller

El curso de redes locales se deberá impartir en el contexto de un aula y de un taller de informática.

A nivel de equipamientos, será conveniente que el aula sea grande, con mesas compartidas de, al menos, dos alumnos. La mesa del profesor deberá estar equipada con un ordenador de sobremesa, que controle el proyector y el equipo de sonido del aula, y cada estudiante deberá poseer su propio ordenador personal, que, pueden ser portátiles. Además, el aula deberá contar también con una pizarra blanca.

El taller deberá tener unas dimensiones mínimas de unos 100 m² y en él tendremos el espacio suficiente para la realización de las prácticas. El taller deberá contar con una zona de mesas altas con sillas de taller, cercanas a la mesa del profesor que comandará un proyector y una pizarra blanca, y otra zona, con armarios bajo llave y estantes donde se encuentre el material necesario bien organizado.

¹³ Wireshark. (2020). *Software analizador de protocolos*. www.wireshark.org

¹⁴ Tera Term. (2020). *Software emulador de terminal*. <https://g.co/kgs/PWmq9L>

En el aula el modo de funcionamiento es sencillo porque cada estudiante dispone de su ordenador personal y se pueden realizar las prácticas correspondientes de simulación de forma individual o, incluso, la formación de grupos online, sin necesidad de realizar ningún cambio.

En el taller la organización es diferente, es preferible que las prácticas de taller se realicen de modo grupal, no solamente por el aspecto pedagógico, sino también por el incremento de dispositivos que implica una práctica individual.

Para la realización de las prácticas será muy importante seguir las indicaciones de seguridad que dará el docente, debido al uso de herramientas cortantes/punzantes, herramientas eléctricas, etc. Y, al finalizar la actividad, todo deberá quedar en las mismas condiciones en que se ha encontrado, puesto que los talleres normalmente son de uso compartido.

8 Contenidos

En este punto del trabajo se presentan todos los contenidos técnicos que se han creado para cada unidad didáctica, conformando el curso de redes de área local completamente. Se distribuirán los contenidos de cada unidad en el siguiente orden:

- ✓ Presentación teórica¹⁵, donde se presentarán en formato de 2x2 todas las diapositivas con el desarrollo de la teoría correspondiente. Entre las diapositivas se intercalan espacios para el trabajo de actividades relacionadas con la misma. Las diapositivas serán utilizadas por el profesor en las explicaciones y estarán a disposición de los estudiantes como material de estudio.
- ✓ Cuaderno de actividades¹⁶. En formato de dos páginas por hoja se muestran todas las actividades que se propone realizar para asentar, por secciones, la teoría expuesta en las diapositivas.

¹⁵ Valdivia, C. (2019). *Sistemas informáticos y redes locales*. Madrid: Paraninfo.

Molina, F. J. (2009). *Redes Locales*. Madrid: RA-MA.

Abad, A. (2012). *Redes Locales*. Madrid: McGraw-Hill Interamericana.

Cisco Network Academy. (28 de julio de 2019). *CCNA R&S: Introduction to Networks v6*. Curso para instructores. <https://www.netacad.com/portal/learning>

¹⁶ Abad, A. (2012). *Redes Locales*. Madrid: McGraw-Hill Interamericana.

Cisco Network Academy. (28 de julio de 2019). *CCNA R&S: Introduction to Networks v6*. Curso para instructores. <https://www.netacad.com/portal/learning>

- ✓ Cuaderno de prácticas¹⁷, en el mismo formato que los cuadernos de actividades. Se realizarán en modo conjunto o individual, y se pretende situar casos de aplicación práctica, en modo simulación o de laboratorio (taller).
- ✓ Trabajos de investigación. Con el fin de ahondar en los contenidos técnicos vistos y de favorecer la creación de herramientas de búsqueda, se presentan trabajos de investigación al finalizar la exposición teórica de los contenidos.

Adaptación de contenidos en línea con la aparición de la COVID-19

El periodo correspondiente a la entrada en vigor de las leyes referentes a las restricciones de movilidad, consecuencia de la pandemia producida por la COVID-19, ha favorecido la creación de contenidos autodidactas, como video-tutoriales, y la ampliación en el desarrollo de los enunciados de las prácticas de simulación, así como el aumento en número de dichas prácticas de simulación, quedando el conjunto de materiales tal y como se desarrollará en este punto 8. Se observará en cada unidad didáctica la inserción de videos explicativos, reforzando la parte teórica, y el desarrollo del paso a paso detallado en las simulaciones, e incluso, la inclusión de grabaciones propias con las explicaciones del docente sobre las mismas.

¹⁷ Cisco Network Academy. (28 de julio de 2019). *CCNA R&S: Introduction to Networks v6*. Curso para instructores. <https://www.netacad.com/portal/learning>
Cisco Network Academy. (1 de septiembre de 2017). *Introduction to Packet Tracer v1.0*. Curso para instructores. <https://www.netacad.com/portal/learning>
Cisco Network Academy. (28 de marzo de 2017). *Networking Essentials v1*. Curso para instructores. <https://www.netacad.com/portal/learning>
Cisco Network Academy. (19 de diciembre de 2017). *IoT Fundamentals: Connecting Things v2.0*. Curso para instructores. <https://www.netacad.com/portal/learning>
Cisco Network Academy. (8 de septiembre de 2017). *Big Data & Analytics v2.01*. Curso para instructores. <https://www.netacad.com/portal/learning>
Cisco Network Academy. (22 de marzo de 2018). *Introduction to Cybersecurity v2.1*. Curso para instructores. <https://www.netacad.com/portal/learning>

8.1 Unidad didáctica 1

Al inicio de ésta primera unidad didáctica se presenta el índice global del curso.

Se describe la importancia de la transmisión de información entre computadores y cómo ha influido en la aparición y desarrollo de las redes. La base de cualquier comunicación es una transmisión de señal. Las redes de ordenadores vienen a cubrir estos dos aspectos: transmisión y comunicación.

Una vez conocidos los antecedentes de las redes se explican los aspectos que afectan al concepto, aplicaciones y clasificaciones de las redes de ordenadores, permitiendo la comunicación de equipos y ordenadores de aplicaciones y fabricantes dispares.

Para posibilitar y facilitar la comunicación, estudio y comprensión de las redes, se estudia la importancia de la existencia de modelos de referencia estandarizados, que todas las organizaciones y fabricantes deben aceptar. Con fin a comprender, cómo ha sido posible la expansión y desarrollo de las redes.

En esta unidad didáctica estudiamos algunos modelos básicos de redes de área local, así como algunas de sus implementaciones, especialmente de las redes TCP/IP como núcleo tecnológico de Internet y del modelo de referencia internacional estándar OSI.

8.1.1 Presentación teórica

CURSO

Redes de Área Local

UNIDAD 1- PARTE 1^a

Caracterización de Redes Locales

Redes de Área Local
Olga Minguet
1

UD1. Caracterización de Redes Locales


ÍNDICE

- [1. Introducción](#)
- [2. Las redes de ordenadores](#)
- [3. Clasificación de las redes](#)
- [4. Elementos de la red](#)
- [5. Arquitectura de redes](#)
- [6. El modelo de referencia OSI](#)

Redes de Área Local
Olga Minguet
2

UD1. Caracterización de Redes Locales


1. INTRODUCCIÓN

*El funcionamiento de todas las comunidades animales y humanas es posible gracias a la **comunicación**.*

Ésta consiste en un acto por el cual un individuo establece un contacto con otros que le permite intercambiar información.

Para que esa comunicación sea posible, los individuos que se comunican deben usar un lenguaje común que represente los mensajes. Así mismo hace falta que esos mensajes se transporten de un punto a otro.

La gran cuestión es cómo transportar esa información de un punto a otro.

Redes de Área Local
Olga Minguet
3

UD1. Caracterización de Redes Locales


1. INTRODUCCIÓN

A lo largo de la historia la **comunicación** ha representado un elemento esencial para la vida.

De hecho, la comunicación es casi tan **importante** para nosotros como el aire, el agua, los alimentos y un lugar para vivir.



Redes de Área Local
Olga Minguet
4

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN

Los métodos que utilizamos para compartir ideas e información están en **constante cambio y evolución**.

Mientras la red humana estuvo limitada a conversaciones cara a cara, el avance de los medios ha ampliado el alcance de nuestras comunicaciones. **Desde la prensa escrita hasta la televisión**, cada nuevo desarrollo ha mejorado la comunicación.



Al igual que con cada **avance** en la tecnología de comunicación, la **creación e interconexión de redes de datos sólidas** tiene un profundo efecto.

Redes de Área Local Olga Minguet 5

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN

Las primeras redes de datos estaban limitadas a intercambiar información basada en **simples secuencias de caracteres** entre sistemas informáticos conectados. Las redes actuales evolucionaron para agregarle voz, flujos de video, texto y gráficos, a los diferentes tipos de dispositivos.

Además, las formas de comunicación individuales y diferentes se unieron en una **plataforma común**. Esta plataforma común, **Internet**, alienta la formación de comunidades globales. Estas comunidades motivan la interacción social que depende de la ubicación o el huso horario.



Redes de Área Local Olga Minguet 6

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN

Es increíble la rapidez con la que **Internet** llegó a ser una parte integral de nuestra rutina diaria.

La compleja interconexión de dispositivos y medios electrónicos que abarca la red es evidente para los **millones de usuarios** que hacen de ésta una parte personal y valiosa de sus vidas.



Redes de Área Local Olga Minguet 7

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN

Las redes de datos que fueron alguna vez el transporte de información entre negocios se replanificaron para mejorar la calidad de vida de todas las personas.

En el transcurso del día, los recursos disponibles en Internet pueden ayudarnos a:



- *decidir cómo vestirse,*
- *buscar el camino menos congestionado,*
- *consultar su estado de cuenta bancario y pagar electrónicamente,*
- *recibir y enviar correo electrónico o realizar una llamada telefónica a través de Internet,*
- *obtener información sobre la salud y consejos sobre nutrición de todo el mundo,*
- *enviar y compartir fotografías, videos y experiencias con amigos o con el mundo.....*

Redes de Área Local Olga Minguet 8

UD1. Caracterización de Redes Locales

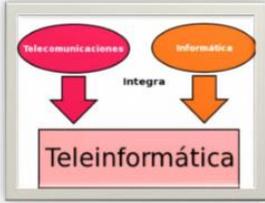


Redes de Área Local Olga Minguet 9

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN: El proceso de comunicación

Las tecnologías de la información y la comunicación (TIC) y en concreto la teleinformática o, más conocido como **telemática**, viven actualmente su mayor auge. La sociedad no puede avanzar sin información y la telemática trata del modo de acceso a la misma.

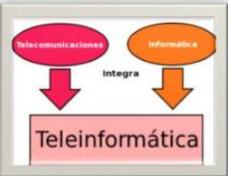


Redes de Área Local Olga Minguet 10

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN: El proceso de comunicación

Podemos definir la teleinformática como la técnica que trata la **COMUNICACIÓN remota** (a distancia) entre sistemas informáticos. Debe ocuparse de los siguientes aspectos:

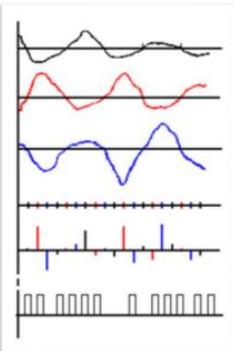


- **Interconectabilidad física:** forma del conector, tipo de señal, parámetro eléctricos, etc.
- **Especificaciones lógicas:** protocolos de comunicación, detección y corrección de errores, compatibilidad de distintas redes etc.

Redes de Área Local Olga Minguet 11

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN: El proceso de comunicación



La base de cualquier comunicación es la **transmisión de una señal**. La transmisión es el proceso telemático por el que se transporta señales de un lugar a otro.

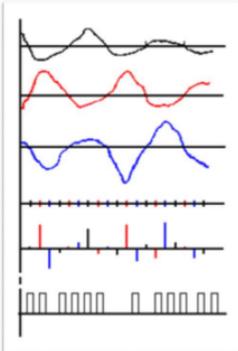
Las señales son principalmente: **luminosa, eléctrica y magnética**, capaces de transportar información.

Representan lo transmitido.

Redes de Área Local Olga Minguet 12

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN: El proceso de comunicación



Pero, **no siempre que existe transmisión de señales se opera una comunicación.**

Pongamos como ejemplo la *radiación estelar* que constantemente llega a la tierra. Las señales luminosas que nos llegan de las estrellas se transmiten a través del espacio interestelar y, sin embargo, no nos sentimos en absoluto participantes en comunicación alguna.

Redes de Área Local Olga Minguet 13

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN: El proceso de comunicación

Por tanto podemos concretar la comunicación como el proceso telemático por el que se **transporta INFORMACIÓN, viajando sobre una SEÑAL** que se transmite.

El emisor y receptor se ponen de acuerdo en una serie de **normas** por las que se entienden. Gracias a esto se produce la comunicación.

Si se diera el caso, por ejemplo, de que los interlocutores no compartieran el mismo idioma, seguiría habiendo transmisión de señales, pero no existiría comunicación de información: los interlocutores no se entenderían.

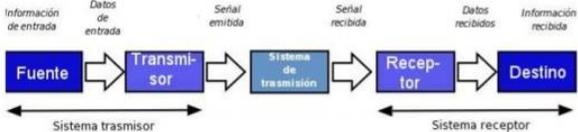


Redes de Área Local Olga Minguet 14

UD1. Caracterización de Redes Locales

1. INTRODUCCIÓN: El proceso de comunicación

Para que se produzca una comunicación deben intervenir una serie de **elementos** que tienen como objetivo el intercambiar información entre dos entidades. Tenemos el modelo sencillo de sistema de comunicación mostrado en la siguiente figura en la que se propone un diagrama de bloques.



Redes de Área Local Olga Minguet 15

UD1. Caracterización de Redes Locales

2. LAS REDES DE ORDENADORES



Desde que el ser humano tiene capacidad de comunicarse ha desarrollado mecanismos y sistemas que les permiten establecer esta comunicación a distancias superiores de las alcanzadas por sus propios medios.

Al poco de aparecer los ordenadores, se sintió la necesidad de **interconectarlos** para que se pudiesen comunicar entre sí como lo hacemos los humanos.

¿Quién hace posible esta comunicación?

Redes de Área Local Olga Minguet 16

UD1. Caracterización de Redes Locales

2. LAS REDES DE ORDENADORES

Las empresas necesitaban una solución que resolviera con éxito las tres preguntas siguientes:

- ✓ ¿Cómo evitar la duplicación de equipos informáticos y de otros recursos de forma innecesaria?
- ✓ ¿Cómo comunicarse con eficiencia?
- ✓ ¿Cómo configurar y administrar un conjunto de equipos informáticos?



Redes de Área Local Olga Minguet 17

UD1. Caracterización de Redes Locales

2. LAS REDES DE ORDENADORES

Las empresas se dieron cuenta de que podrían ahorrar mucho dinero y aumentar la productividad con la tecnología de red.



Empezaron agregando redes y expandiendo las redes existentes casi tan rápidamente como se producía la introducción de nuevas tecnologías y productos de red.

Como resultado, a principios de los 80, se produjo una tremenda expansión de las redes.

Redes de Área Local Olga Minguet 18

UD1. Caracterización de Redes Locales

2. LAS REDES DE ORDENADORES



Una **red de datos** es un conjunto de dos o mas equipos (ordenadores, impresoras, y dispositivos periféricos y de interconexión) **conectados entre sí** por medio de cables, señales, ondas o cualquier otro método de transporte de datos, **que comparten** información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos), **incrementando la eficiencia y productividad** de las personas.

Redes de Área Local Olga Minguet 19

UD1. Caracterización de Redes Locales

2. LAS REDES DE ORDENADORES

¿Por qué razón se han desarrollado las redes?

1.- **Redes en el mundo empresarial:**

- *Compartir recursos* (ordenadores, impresoras, conexión a internet, programas, datos,...) de forma que estén disponibles para cualquiera en la red sin importar la localización física de los usuarios y de los recursos.
- *Mejorar la seguridad* al contar con fuentes alternativas de recursos.
- *Ahorro de dinero* al no tener que duplicar recursos al estar disponible a través de la red.
- *Escalabilidad*, es decir la capacidad para incrementar su rendimiento de la red gradualmente cuando la carga de trabajo crece añadiendo o mejorando los recursos.
- *Medio de comunicación* de los empleados que se encuentran distantes.



Redes de Área Local Olga Minguet 20

UD1. Caracterización de Redes Locales

2. LAS REDES DE ORDENADORES

¿Por qué razón se han desarrollado las redes?

2.- **Redes para los usuarios domésticos:**

En los años 90 las redes empezaron a prestar servicios que se extendieron a particulares. Tres son las grandes razones de esta evolución:

- **Acceso a información remota.** Por ejemplo plataformas de formación on-line, navegación web, información multimedia, prensa, exploración de lugares de forma interactiva, FTP (transferencia de ficheros), etc.
- **Comunicación persona a persona.** Por ejemplo hablar por teléfono o videoconferencias, mensajería instantánea, correo electrónico, redes sociales, foros, planificación y colaboración en proyectos comunes, etc.
- **Entretenimiento interactivo.** Por ejemplo juegos en línea o competir con los amigos en general.



Redes de Área Local Olga Minguet 21

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

1. Clasificación de las redes atendiendo a la **titularidad de la red**
2. Clasificación de las redes atendiendo a la **topología**
3. Clasificación de las redes atendiendo a la **transferencia de la información**
4. Clasificación de las redes atendiendo a la **localización geográfica**
5. Clasificación de las redes atendiendo a la **tecnología**
6. Clasificación de las redes atendiendo a la **relación funcional**

Redes de Área Local Olga Minguet 22

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.1. Atendiendo a la titularidad (propiedad) de la red

- 1) **Redes dedicadas o privadas:** Tienen un propietario no público. Todo su recorrido es propiedad del poseedor de la red. También puede ocurrir que determinadas redes sean alquiladas a compañías de comunicaciones (públicas o privadas) para su uso exclusivo.
- 2) **Redes compartidas o públicas:** Son redes de titularidad pública. Normalmente en poder de compañías telefónicas o de cable. Las líneas de comunicación soportan información de diferentes usuarios. Se trata en todo caso de redes de servicio público ofertadas por compañías de telecomunicaciones bajo cuotas de alquiler en función de la utilización realizada. Pertenecen a este grupo las redes telefónicas conmutadas y las redes especiales para transmisión de datos.

Redes de Área Local Olga Minguet 23

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

Esta clasificación tiene en cuenta la arquitectura de la red, es decir, la forma en la que se interconectan los diferentes equipos informáticos o usuarios a ella:

- 1) **Bus:** Utiliza un único cable para conectar los equipos. Esta configuración es la que requiere menos cableado, pero tiene el inconveniente de que si, si falla algún enlace, todos los nodos quedan aislados.



Redes de Área Local Olga Minguet 24

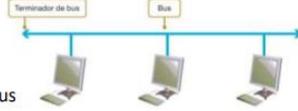
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

1) Bus

- ✓ Las redes de área local con topología en bus son las más **sencillas de instalar**.
- ✓ No requieren dispositivos complicados para realizar las conexiones físicas entre nodos.
- ✓ El medio de transmisión que forma la red es un único bus **multiacceso** compartido por todos los nodos.
- ✓ Se debe establecer una **competencia** para determinar quién tiene derechos de acceso a los recursos de comunicación en cada instante. Por lo tanto es muy sensible a **problemas de congestión** de tráfico si la red crece.
- ✓ La **rotura del cable** implica que la comunicación se detendrá.



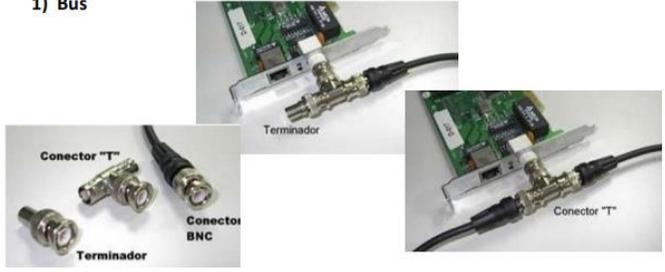
Redes de Área Local Olga Minguet 25

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

1) Bus



Redes de Área Local Olga Minguet 26

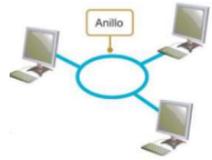
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

2) Anillo

- ✓ Una red en anillo conecta todos sus equipos en torno a un anillo físico.
- ✓ No presenta problemas de congestión de tráfico, a diferencia de las redes en bus.
- ✓ Sin embargo, una rotura del anillo produce en la red un fallo general.
- ✓ La ventaja es que cada equipo actúa como repetidor, regenerando la señal y enviándola al siguiente equipo, conservando la potencia de la señal.
- ✓ Es muy utilizada para conectar edificios entre sí.



Redes de Área Local Olga Minguet 27

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

2) Anillo

Las redes en anillo utilizan protocolos libres de colisiones con técnicas de paso por testigo (token ring). **Token Ring** evita la colisión de datos entre dos equipos que desean enviar información al mismo tiempo. Funciona así:

1. *Frames vacíos de información circulan continuamente en el anillo.*
2. *Cuando un equipo tiene un mensaje que enviar, introduce un símbolo en un frame vacío (suele consistir en un simple cambio de un 0 a un 1) e inserta un mensaje y el destino de un identificador en el frame.*
3. *El frame es examinado por cada estación de trabajo sucesivamente. Si la estación de trabajo considera que es el destino del mensaje, copia el mensaje desde el frame y cambia el token a 0.*



Redes de Área Local Olga Minguet 28

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

2) Anillo

To send data on a Token Ring network, a workstation must wait for the token to become available. A packet is then attached to the token and circles around the network until it reaches its destination.

This workstation attached a packet to the token.

This workstation sees its address on the packet and detaches the data from the token.

Redes de Área Local Olga Minguet 29

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

2b) Anillo doble

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí. Es análoga a la topología de anillo, con la diferencia de que, **para incrementar la confiabilidad** y flexibilidad, hay un segundo anillo redundante que conecta los mismos dispositivos.

Los enlaces conectados al mismo dispositivo de networking

La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales **se usa solamente uno por vez.**

Redes de Área Local Olga Minguet 30

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

3) Estrella

- ✓ En las redes que tienen su topología en estrella, las estaciones se conectan entre sí a través de un **nodo** especialmente privilegiado que ocupa la **posición central de la red**, y que forma con el resto de las estaciones una estrella.
- ✓ A este **nodo central** se le denomina **estación concentradora de la estrella**.

Redes de Área Local Olga Minguet 31

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

3) Estrella

- ✓ Puesto que a cada nodo le llega un único cable de red, las conexiones suelen ser más **estructuradas** que en el caso de otro tipo de cableados.
- ✓ Sin embargo, el problema de la topología en estrella se presenta en el entorno del concentrador ya que todos los segmentos deben terminar en él, lo que produce una **importante madeja de cables**.
- ✓ El uso de tanto cable **encarece** mucho la instalación de la red.
- ✓ Además, si **perdemos el nodo central**, perderemos la comunicación entre el resto de nodos.

Redes de Área Local Olga Minguet 32

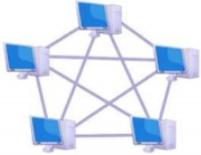
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

4) Malla

- ✓ Es una **interconexión total** de todos los nodos
- ✓ Tiene la ventaja de que, si una ruta falla, se puede seleccionar otra **alternativa**.
- ✓ Este tipo de red es **más costosa** de construir, ya que hace falta más cable.



Redes de Área Local Olga Minguet 33

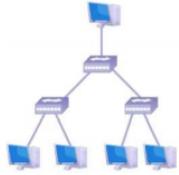
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

5) Árbol

- ✓ Es una forma de conectar nodos como una estructura **jerarquizada**. Esta topología es la menos utilizada, y se prefiere la topología irregular, ya que el fallo de un nodo o enlace deja a conjunto de nodos incomunicados entre sí.
- ✓ Desde una visión topológica, es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un **nodo de enlace troncal**.
- ✓ Con esta estructura es fácil solucionar problemas o fallos en la red.
- ✓ Si se **rompe un segmento** de un nodo de la red, **todos los que dependen de él dejan de funcionar. El resto siguen funcionando.**
- ✓ Si se **cae el segmento principal toda la red también cae.**



Redes de Área Local Olga Minguet 34

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología

6) Irregular



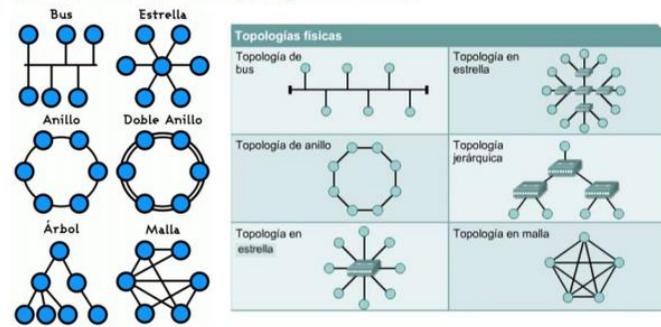
- ✓ En esta topología cada nodo debe estar conectado, como mínimo, por un enlace, pero no existen más restricciones.
- ✓ Esta topología es la más utilizada en redes que ocupan **zonas geográficas amplias**.
- ✓ Permite la **búsqueda de rutas alternativas** cuando falla alguno de los enlaces

Redes de Área Local Olga Minguet 35

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.2. Atendiendo a la topología: Resumen



Redes de Área Local Olga Minguet 36

UD1. Caracterización de Redes Locales

Realiza las siguientes **ACTIVIDADES DE TEORÍA**:

- Actividad 1
- Actividad 2
- Actividad 3
- Actividad 4
- Actividad 5

Redes de Área Local Olga Minguet 37

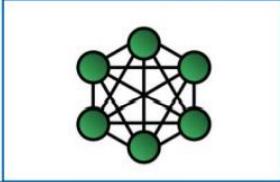
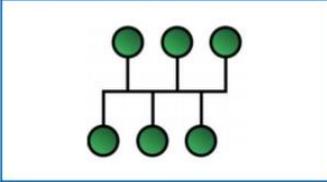
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.3. Atendiendo a la transferencia de información

Esta clasificación tiene en cuenta la **técnica empleada para transferir la información desde el origen al destino**. Por lo tanto, también depende de la topología de la red y, si se ha separado de la clasificación anterior, ha sido porque existen diferentes topologías que comparten el mismo método de transmisión.

Redes conmutadas (punto a punto) Redes de difusión (multipunto o broadcast)

Redes de Área Local Olga Minguet 38

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.3. Atendiendo a la transferencia de información

Redes conmutadas (punto a punto)

- ✓ En este tipo de redes, un equipo origen (emisor) selecciona un equipo con el que quiere conectarse (receptor) y la red es la encargada de habilitar **una vía de conexión entre los dos equipos**. Normalmente pueden seleccionarse varios caminos candidatos para esta vía de comunicación que puede o no dedicarse exclusivamente a la misma.
- ✓ Existen tres métodos para la transmisión de la información y la habilitación de la conexión:

Redes de Área Local Olga Minguet 39

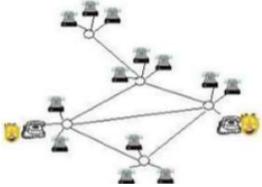
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.3. Atendiendo a la transferencia de información

Redes conmutadas (punto a punto)

1) Conmutación de circuitos: Se establece **un camino dedicado**. La ruta que sigue la información se establece **durante todo el proceso de conexión**, aunque existan tramos de esta ruta que se compartan con otras rutas diferentes. Una vez finalizada la comunicación, es necesario liberar la conexión. *Ejemplo: el teléfono.*



Redes de Área Local Olga Minguet 40

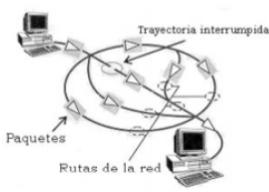
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.3. Atendiendo a la transferencia de información

Redes conmutadas (punto a punto)

2) Conmutación de paquetes: En este caso, el mensaje a enviar **se divide en fragmentos**, cada uno de los cuáles es enviado a la red y circula por ésta hasta que llega a su destino. Cada fragmento denominado paquete, contiene parte de la información a transmitir, información de control además de los números o direcciones que identifican el origen y el destino. *Ejemplo: Internet.*



Redes de Área Local Olga Minguet 41

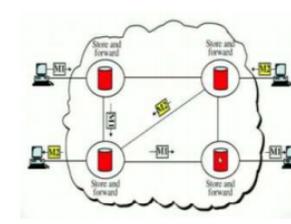
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.3. Atendiendo a la transferencia de información

Redes conmutadas (punto a punto)

3) Conmutación de mensajes: origen y el destino. Conmutación de mensajes: La información que envía el emisor se aloja en un único mensaje con la dirección de destino y se envía al siguiente nodo. Éste almacena la información hasta que hay un camino libre, dando lugar a su vez al envío al siguiente nodo hasta que finalmente llegue al destino. *Ejemplo: el telégrafo.*



Redes de Área Local Olga Minguet 42

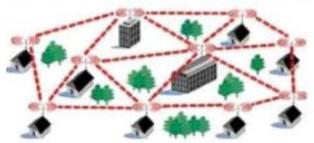
UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.3. Atendiendo a la transferencia de información

Redes de difusión (multipunto o broadcast)

- ✓ En este caso **un equipo o nodo envía la información a todos los equipos** y es el destinatario el encargado de seleccionar y captar esa información.
- ✓ Esta forma de transmisión de la información está condicionada por la topología de la red, ya que ésta se caracteriza por disponer de un **único camino o vía de comunicación** que debe ser compartido por todos los nodos o equipos.
- ✓ La red debe tener una topología en **bus o anillo** o debe estar basada en enlaces por **ondas de radio**.



Redes de Área Local Olga Minguet 43

UD1. Caracterización de Redes Locales

 Realiza las siguientes **ACTIVIDADES DE TEORIA:**

➤ **Actividad 6**

Redes de Área Local Olga Minguet 44

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.4. Atendiendo al tamaño

La **localización geográfica** de la red es un factor a tener en cuenta a la hora de diseñarla y montarla.

No es lo mismo montar una red para un aula de informática que interconectar las oficinas de dos sucursales que la misma empresa tiene instalada en diferentes países.



Redes de Área Local

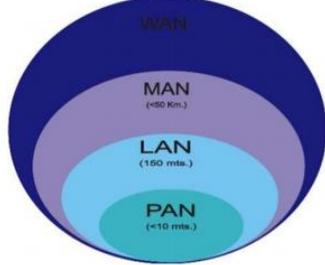
Olga Minguet 45

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.4. Atendiendo al tamaño

- Red de área personal (PAN)
- Red de área local (LAN)
- Red de área metropolitana (MAN)
- Red de área extensa (WAN)



Redes de Área Local

Olga Minguet 46

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.4. Atendiendo al tamaño

- Red de área personal (PAN)

Las redes PAN (**Personal Area Network**) tienen algunas características que las hacen peculiares:

- ✓ La **configuración** de acceso a la red debe ser muy **sencilla o incluso automática**.
- ✓ El radio de acción de la red debe ser geográficamente **muy limitado**, con objeto de que dos redes no colisionen fácilmente entre sí
- ✓ El medio de transmisión por excelencia, aunque no de modo exclusivo, es el **inalámbrico**, utilizando tecnologías bluetooth (radio) o IrDA (infrarrojos).
- ✓ Los costes de la red, tanto de instalación como de explotación, deben ser pequeños y en algunas ocasiones **sin coste**, como en el caso de la conexión de ratones inalámbricos, impresoras por infrarrojos, Bluetooth o Wi-Fi, etc.



Redes de Área Local

Olga Minguet 47

UD1. Caracterización de Redes Locales

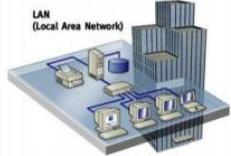
3. CLASIFICACIÓN DE LAS REDES

3.4. Atendiendo al tamaño

- Red de área local (LAN)

Una red de área local **LAN (Local Area Network)** es un conjunto de elementos físicos y lógicos que proporcionan interconexión entre dispositivos en un **área privada y restringida**. La red de área local tiene, entre otras, las siguientes características:

- ✓ **Una restricción geográfica:** el ámbito de una oficina, de la planta de un edificio, un edificio entero, e incluso, un campus universitario con los edificios próximos: depende de la tecnología con que esté construida (par trenzado, fibra óptica). Desde 10m a 1Km.



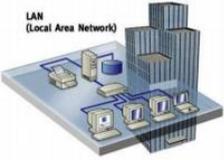
Redes de Área Local

Olga Minguet 48

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES
3.4. Atendiendo al tamaño
 ➤ Red de área local (LAN)

- ✓ La **velocidad de transmisión** debe ser relativamente elevada (de 10Mbps a 10Gbps).
- ✓ La **red** de área local debe ser privada, toda la red pertenece a la misma organización.
- ✓ **Fiabilidad** en las transmisiones. La **tasa de error** en una red de área local debe ser muy **baja**.
- ✓ Las LANs más conocidas y extendidas son la **Ethernet**, Token Ring, LAN inalámbrica (Wi-Fi), etc.
- ✓ Topologías: **Bus, estrella y anillo**.



Redes de Área Local Olga Minguet 49

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES
3.4. Atendiendo al tamaño
 ➤ Red de área metropolitana (MAN)

Una red de área local **MAN (Metropolitan Area Network)** generalmente está confinada dentro de una misma ciudad y se haya sujeta a regulaciones locales.

Puede constar de varios recursos públicos o privados, como el sistema de telefonía local, sistemas de microondas locales o cables enterrados de fibra óptica (redes de cable).



Las MAN más conocidas son la **FDDI, ATM, WiMax** (inalámbricas).

Redes de Área Local Olga Minguet 50

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES
3.4. Atendiendo al tamaño
 ➤ Red de área extensa (WAN, Wide Area Network)

A medida que el uso de los ordenadores en las empresas aumentaba, pronto resultó obvio que incluso las redes locales (LAN) no eran suficientes.

En un sistema LAN, cada departamento o empresa, era una especie de isla electrónica. Lo que se necesitaba era una forma de que la información se pudiera **transferir** rápidamente y con eficiencia, no solamente dentro de una misma empresa sino **de una empresa a otra**.



Redes de Área Local Olga Minguet 51

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES
3.4. Atendiendo al tamaño
 ➤ Red de área extensa (WAN)

Entonces, la solución fue la creación de redes de área metropolitana (MAN) y redes de área amplia (WAN). Como **las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas**, permitieron que las empresas se comunicaran entre sí a través de grandes distancias.

Una red de área extendida (WAN) abarca varias ciudades, regiones o países. Los enlaces WAN son ofrecidos generalmente por empresas de telecomunicaciones públicas o privadas que utilizan enlaces de fibra óptica, microondas o vía satélite.



Redes de Área Local Olga Minguet 52

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.4. Atendiendo al tamaño

➤ Red de área extensa (WAN)

Así pues, una red de área extensa es una red que interconecta equipos en un **área geográfica muy amplia**.

- ✓ Las transmisiones en una WAN se realizan a través de **líneas públicas**.
- ✓ La capacidad de transmisión (velocidad) de estas líneas suele ser **menor** que las utilizadas en las redes de área local.
- ✓ Son **compartidas por muchos usuarios a la vez**, lo que exige un acuerdo en los modos de transmisión y en las normas de interconexión a la red.
- ✓ Las **tasas de error** en las transmisiones en las redes de área extensa son **mayores** (unas mil veces superior) que su equivalente en las redes de área local.

Redes de Área Local Olga Minguet 53

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.4. Atendiendo al tamaño

➤ Red de área extensa (WAN)

Las **posibilidades** de las redes de área extendida son **enormes**:

- ✓ distintos tipos de redes de área local que interconectan,
- ✓ equipamientos de diversos fabricantes,
- ✓ multitud de protocolos de comunicación,
- ✓ posibilidad de diferentes líneas de transmisión, etc.

Las tecnologías también son muchas: **Red Digital de Servicios Integrados (RDSI o ISDN), Frame Relay, ADSL** o redes de **satélites**.

Internet es un ejemplo de red de servicios estructurada sobre una red de área extensa de alcance mundial que utiliza todas las tecnologías indicadas en el párrafo anterior.

Redes de Área Local Olga Minguet 54

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.4. Atendiendo al tamaño

➤ OTROS: Computación en la nube



La **computación en la nube (cloud computing)** es un nuevo modelo de utilización de los recursos informáticos de una **red de área extensa (Internet)** de modo que todo se brinda como servicio deslocalizado.

Por ejemplo, aunque se esté trabajando desde un ordenador personal, el espacio de almacenamiento de donde se guardan los ficheros puede estar en un proveedor de almacenamiento al otro lado de Internet (en la nube).

Si en un momento dado cambiamos de PC, **los datos** seguirán estando disponibles en la nube puesto que **no residen en el PC local**.

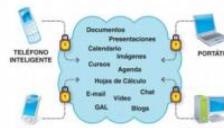
Redes de Área Local Olga Minguet 55

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.4. Atendiendo al tamaño

➤ OTROS: Computación en la nube



Un ejemplo parecido lo tendríamos si ponemos en la nube no solo el almacenamiento, sino también las propias **aplicaciones y las bases de datos**.

El objetivo funcional de la nube es que los usuarios puedan **utilizar los recursos** desde **cualquier dispositivo** electrónico (Smartphone, portátil, PC, etc.) situado en cualquier lugar, utilizando como herramienta un **navegador** de Internet o una aplicación local similar y como medio de acceso **Internet**.

Redes de Área Local Olga Minguet 56

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES
3.4. Atendiendo al tamaño

➤ **OTROS: Computación en la nube**

Las nubes pueden ser:

- ✓ **Privadas**, en donde toda la infraestructura necesaria es propiedad del propietario.
- ✓ **Públicas**, en donde la infraestructura se contrata con proveedores externos a la corporación que proporcionan servicios públicos.
- ✓ **Híbridas**, en las que se dispone de infraestructuras privadas complementadas con otras públicas.

Redes de Área Local Olga Minguet 57

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES
3.4. Atendiendo al tamaño

➤ **OTROS: Redes de área local inalámbricas (WLAN)**

Las redes de área local inalámbricas (**WLAN, Wireless Local Area Network**) representan otra mejora importante de las redes locales (cableadas) en las que el enlace entre equipos informáticos no se lleva a cabo por medio de cables, sino **por medio de enlaces radioeléctricos (ondas de radio)**. Las ventajas de este tipo de enlaces, en cuanto a **movilidad y facilidad de instalación**, son evidentes.



Las WLAN mas conocidas son las redes **Wifi**.

Redes de Área Local Olga Minguet 58

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES
3.4. Atendiendo al tamaño

➤ **OTROS: Redes de área local inalámbricas (WLAN)**

Una WLAN tiene muchas ventajas pero también inconvenientes:

VENTAJAS	INCONVENIENTES
Coste. La instalación sin cables y la facilidad de instalación y mantenimiento hace que sea una opción económica.	Seguridad. Al ser aéreo el medio de transmisión, las redes inalámbricas exponen una mayor superficie de ataque, lo que brinda más posibilidades a los crackers.
Disponibilidad. Se puede acceder a la red desde cualquier lugar, dispositivo y de forma más cómoda.	Velocidad. Como el canal de transmisión es compartido por todas las estaciones, los sistemas inalámbricos tienen que multiplexar las señales de transmisión (repartir el ancho de banda del canal) entre todas las estaciones inalámbricas, lo que frecuentemente produce situaciones de congestión.

Redes de Área Local Olga Minguet 59

UD1. Caracterización de Redes Locales

 Realiza las siguientes **ACTIVIDADES DE TEORIA:**

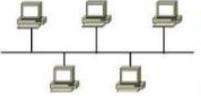
- **Actividad 7**
- **Actividad 8**
- **Actividad 9**
- **Actividad 10**
- **Actividad 11**
- **Actividad 12**

Redes de Área Local Olga Minguet 60

UD1. Caracterización de Redes Locales

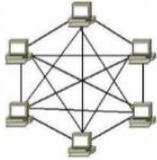
3. CLASIFICACIÓN DE LAS REDES

3.5. Atendiendo a la tecnología



Redes broadcast (multipunto o multidifusión). Medio de transmisión compartido por todos ordenadores interconectados. Caracteriza las primeras LAN.

Redes punto a punto. Se construyen por medio de conexiones entre pares de entidades, también llamadas líneas, enlaces, circuitos o canales. Una vez un paquete es depositado en la línea el destino es conocido de forma unívoca y no es preciso en principio que lleve la dirección de destino.



Redes de Área Local Olga Minguet 61

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.6. Atendiendo a la relación funcional

La principal función de las redes consiste en que los ordenadores de la red puedan **compartir recursos** entre todos los usuarios autorizados del sistema, mediante el intercambio de tramas de datos entre los distintos equipos conectados a las líneas de transmisión.

La capacidad ofrecida por un ordenador a otros en una red se llama **servicio o recurso**. Los ordenadores que usan un servicio se llaman *clientes* y los que lo ofrecen se denominan *servidores*.

Hay **dos maneras fundamentales de establecer la conexión** de los ordenadores en la red **según la ubicación de los recursos**.

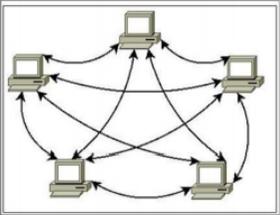
Redes de Área Local Olga Minguet 62

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.6. Atendiendo a la relación funcional

Modelo P2P



Redes ENTRE IGUALES o Peer to Peer (P2P): Cualquier ordenador puede ser cliente y/o servidor. No está claramente definida tal función. Todos los ordenadores ponen a disposición de los demás los recursos que disponen, fundamentalmente discos e impresora.

Esta estructura es muy simple pero se hace difícil el control de los recursos.

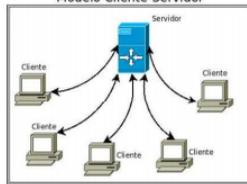
Redes de Área Local Olga Minguet 63

UD1. Caracterización de Redes Locales

3. CLASIFICACIÓN DE LAS REDES

3.6. Atendiendo a la relación funcional

Modelo Cliente-Servidor



Redes CLIENTE-SERVIDOR: En este tipo de distribución está claramente definido los ordenadores que son servidores y cuáles clientes. En este caso se privilegia a uno o varios ordenadores confiriéndoles capacidades añadidas en forma de servicios, denominándose servidores o servers.

El resto de los ordenadores solicitan servicios a estos servidores que estarán altamente especializados en la función para la que fueron diseñados creando así una estructura centralizada. Este tipo de organización es mucho mas fácil de administrar.

Redes de Área Local Olga Minguet 64

UD1. Caracterización de Redes Locales 

 Realiza las siguientes ACTIVIDADES DE TEORIA:

- Actividad 13
- Actividad 14

Redes de Área Local Olga Minguet 65

CURSO
Redes de Área Local

UNIDAD 1- PARTE 2^a
Caracterización de Redes Locales

Redes de Área Local Olga Minguet 1

UD1. Caracterización de Redes Locales 

ÍNDICE

- 1. Introducción
- 2. Las redes de ordenadores
- 3. Clasificación de las redes
- 4. Elementos de la red
- 5. Arquitectura de redes
- 6. El modelo de referencia OSI

Redes de Área Local Olga Minguet 2

UD1. Caracterización de Redes Locales

4. ELEMENTOS DE LA RED

Para construir una red local, se precisan básicamente dos cosas:

- **Elementos físicos o hardware:** Está formado por equipos informáticos (ordenadores y dispositivos de naturaleza variada) y medios de transmisión que posibilitan implementación física de la red. Como ejemplo tendríamos ordenadores, estaciones de trabajo, servidores, tarjeta de red, módem, dispositivos de interconexión, dispositivos de impresión, cables, etc.
- **Elementos lógicos o software:** Ofrece los recursos necesarios para que los usuarios y sus aplicaciones puedan acceder y utilizar los recursos o servicios de la red. Normalmente estas capacidades se integran en forma de programas en los propios sistemas operativos. Tampoco podríamos olvidar los propios **recursos o servicios** como por ejemplo las aplicaciones de red, los datos, los mensajes, etc.

Redes de Área Local Olga Minguet 3

UD1. Caracterización de Redes Locales

4. ELEMENTOS DE LA RED

A modo de ejemplo describimos algunos elementos que podemos encontrarnos en una red:

A) Dispositivos finales:
La mayoría de los componentes de una red media son los ordenadores individuales, también denominados **host o nodo final**; generalmente son sitios de trabajo o servidores.

Cada ordenador conectado a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos.

Asimismo, los ordenadores se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo no comparte sus propios recursos con otros ordenadores.



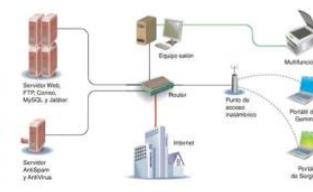
Redes de Área Local Olga Minguet 4

UD1. Caracterización de Redes Locales

4. ELEMENTOS DE LA RED

B) Servidores:
Son también dispositivos finales. Son aquellos ordenadores **capaces de compartir sus recursos con otros**. Los recursos compartidos pueden incluir impresoras, unidades de disco, directorios en disco duro e incluso archivos individuales.

Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web, servidor de correo, etc.



Redes de Área Local Olga Minguet 5

UD1. Caracterización de Redes Locales

4. ELEMENTOS DE LA RED

C) Medios de transmisión:
La LAN debe tener un **sistema de cableado** que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos.

Hay muchos tipos de cableado, cada uno con sus propias características en cuanto al costo y capacidad. Ejemplos de cables usados en la red local son el **par trenzado, coaxial y fibra óptica**. Tampoco debemos olvidar el desarrollo de los medios de transmisión sin cables (inalámbricos).



Redes de Área Local Olga Minguet 6

UD1. Caracterización de Redes Locales

4. ELEMENTOS DE LA RED

D) Dispositivos intermedios:
También conocidos como **dispositivos de interconexión**. Se encargan de implementar el direccionamiento y administración de los mensajes en la red de forma que los equipos informáticos se puedan comunicar entre sí. Ejemplos de dispositivo de interconexión son los **hubs, switches, routers, etc.**

Redes de Área Local Olga Minguet 7

UD1. Caracterización de Redes Locales

4. ELEMENTOS DE LA RED

E) Tarjeta de interfaz de red o Network Interface Card (NIC):
Para comunicarse con el resto de la red, **cada ordenador debe tener instalado una tarjeta de interfaz de red**. Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto USB. La tarjeta de interfaz obtiene la información del PC, la convierte al formato adecuado y la envía a través del medio de transmisión a otra tarjeta de interfaz de la red local. Esta tarjeta recibe la información, la traduce para que el PC pueda entenderla y la entrega al PC.

Redes de Área Local Olga Minguet 8

UD1. Caracterización de Redes Locales

4. ELEMENTOS DE LA RED

F) Software base y Software de aplicación:

- **Software base:** También conocido como Sistema operativo de red o Network operating system (NOS). Después de cumplir todos los requerimientos de hardware para instalar una LAN, se necesita instalar un sistema operativo de red, que administre y coordine todas las operaciones de dicha red. *Ejemplo:* Windows 10.
- **Software de aplicación:** Son el conjunto de programas a través de los cuáles los usuarios utiliza los recursos de la red tanto locales como remotos. Este software puede ser tan amplio como se necesite ya que puede incluir procesadores de texto, hojas de cálculo, clientes de correo electrónico, etc. *Ejemplo:* Internet Explorer.

Redes de Área Local Olga Minguet 9

UD1. Caracterización de Redes Locales

Realiza las siguientes ACTIVIDADES DE TEORÍA:

- **Actividad 15**

Redes de Área Local Olga Minguet 10

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

La arquitectura de una red viene definida por **tres características fundamentales**, que dependen de la tecnología que se utilice en su construcción:

- **Topología:** la topología de una red es la organización de su cableado, ya que define la configuración básica de la interconexión de estaciones y, en algunos casos, el camino de una transmisión de datos sobre el cable.

Redes de Área Local Olga Minguet 11

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

- **Método de acceso a la red:** todas las redes que poseen un medio compartido para transmitir la información necesitan ponerse de acuerdo a la hora de enviar información, ya que no pueden hacerlo a la vez. En este caso, si dos estaciones transmiten a la vez en la misma frecuencia, la señal recogida en los receptores será una mezcla de las dos. Para las redes que no posean un medio compartido, el método de acceso al cable es trivial y no es necesario llevar a cabo ningún control para transmitir.
- **Protocolos de comunicaciones:** Son las normas y procedimientos utilizados en una red para realizar la comunicación. Esas normas tienen en cuenta el método utilizado para corregir errores, establecer una comunicación, velocidad de transmisión, tipo de información, formato de los mensajes, etc.

Redes de Área Local Olga Minguet 12

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

Topologías física vs lógica

Redes de Área Local Olga Minguet 13

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

Redes de Área Local Olga Minguet 14

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

Un **protocolo de red** define unas **normas** a seguir a la hora de **transmitir la información**.

Estas normas que pueden ser:

- velocidad de transmisión,
- tipo de información,
- formato de los mensajes, etc.

El estudio de las tecnologías de redes se simplifica estructurando las distintas tecnologías involucradas en las comunicaciones en **familias de protocolos de comunicación** en las que se definen perfectamente las relaciones de unos con otros.



Redes de Área Local Olga Minguet 15

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

Por ejemplo, podemos hacer la **analogía con el sistema telefónico**. En este caso, los servicios proporcionados pueden ser *transmisión de voz, transmisión de datos, llamada en espera, llamada a tres, etc.* Así mismo, el protocolo para establecer una comunicación (transmisión de voz) debe seguir estrictamente los siguientes pasos:

1. Descolgar el teléfono.
2. Comprobar si hay línea.
3. Si no hay, colgar y volver al paso 1.
4. Marcar número del otro usuario.
5. Esperar tono.
6. Si el tono es comunicando, colgar y volver al paso 1.
7. Si da mas de 6 tonos y no contesta, ir al paso 8.
8. Hablar cuando el otro usuario conteste.
9. Colgar.

Redes de Área Local Olga Minguet 16

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

Es habitual que los **protocolos** se expongan públicamente como normativas o recomendaciones de las asociaciones de estándares.

Los fabricantes que se ajustan a estas normativas tienen la seguridad de ser **compatibles entre sí** en aquellos aspectos regulados por el protocolo.

- El **protocolo abierto** a aquel que se acoge a los estándares internacionales y que es implementado por muchos fabricantes. No suele requerir licencias o pago por su uso.
- El **protocolo cerrado o propietario** es diseñado por compañías concretas y exigen licencias de uso a fabricantes que quieran incorporarlos a sus sistemas de comunicación.

Redes de Área Local Olga Minguet 17

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

Familias de protocolos usuales:

A) **Familia NetWare**, utiliza un protocolo propietario desarrollado por **Novell**, denominado **IPX/SPX** (intercambio de paquetes entre redes/intercambio secuencial de paquetes).



B) **Familia NetBEUI**, de **Microsoft**. NetBeui es una familia de protocolos que controla tanto los datos como los mensajes entre aplicaciones. Hoy en día, aunque todos los sistemas de Microsoft "hablan" NetBeui, paralelamente están incorporando como nativo a TCP/IP.



Redes de Área Local Olga Minguet 18

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

C. Familia AppleTalk, diseñada por **Apple** para sus Macintosh. El diseño original se pensó para compartir ficheros e impresoras entre usuarios. Actualmente el sistema operativo de Apple, además de incorporar de forma nativa AppleTalk, también incorpora TCP/IP.



D. Familia TCP/IP. Utilizado por **UNIX** para comunicación en red, extendido mundialmente, de protocolo abierto. Esta tecnología TCP/IP (*Transmission Control Protocol/Internet Protocol*), está definida en un conjunto de documentos denominados **RFC** (Petición de comentarios), accesibles a cualquier usuario con objeto de mejorar cada protocolo.

La importancia de TCP/IP es tan grande que **la mayor parte de las redes hablan TCP/IP**, sin perjuicio de que además puedan incorporar otras familias nativas.

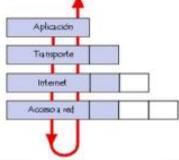


Redes de Área Local Olga Minguet 19

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

- ✓ Con el fin de simplificar la complejidad de cualquier red, los diseñadores de redes han convenido estructurar las diferentes funciones que realizan en una serie de **niveles o capas**. Las **capas están jerarquizadas**. Cada capa se construye sobre su predecesora.
- ✓ El número de capas y, en cada una de ellas, sus servicios y funciones **varían con cada tipo de red**.
- ✓ La misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo.
- ✓ De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente **inferior**, a quien solicita servicios, y del nivel inmediatamente **superior**, a quien devuelve resultados.
- ✓ Por ejemplo, la siguiente imagen muestra las capas para la familia de protocolos TCP/IP.



Redes de Área Local Olga Minguet 20

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

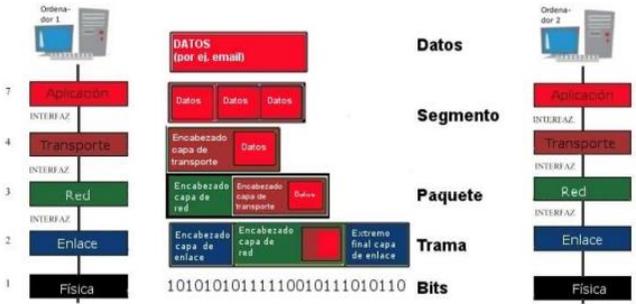
Datos: Unidad de datos en la capa de aplicación.
Segmento: Unidad de datos en la capa de transporte.
Paquete: Unidad de datos en la capa de red.
Trama: Unidad de datos en la capa de enlace.
Bits: Unidad de datos en la capa física, que es cuando se transmiten físicamente datos a través de un medio.



Redes de Área Local Olga Minguet 21

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES



Redes de Área Local Olga Minguet 22

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

Una aplicación (proceso 1) en el ordenador 1 desea enviar cierto mensaje (por ejemplo un email) a otra aplicación (proceso 2) del ordenador 2.

El **proceso de comunicación** incluye los siguientes **pasos**:

1. El proceso 1 crea los datos a nivel de la capa de aplicación y realiza una llamada al servicio al servicio correspondiente en la capa de transporte y le entrega el mensaje.
2. La capa de transporte de red y transporte añaden una cabecera o encabezado (encapsulación) generando lo que se llama un paquete y lo entrega a la capa de enlace a través de la correspondiente solicitud de servicio. Puede ocurrir que debido al tamaño de los datos generados, la capa de transporte y de red se vean obligados a partir el mensaje (segmentación).

Redes de Área Local Olga Minguet 23

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

3. En la capa de enlace se repite el mismo proceso hasta llegar a la capa física.
4. Transporte de los datos a través de la red hasta el ordenador 2.
5. Cuando los datos llegan al nivel físico de la máquina destino (ordenador 2), se produce justamente el proceso contrario al anterior: cada capa recibe los datos, le quita y analiza su cabecera (desencapsulación) correspondiente y si todo es correcto los pasa al nivel superior. En el caso de que los datos se hayan segmentado, deberán ser rearmados por la capa de red o transporte del ordenador 2.
6. Entrega de los datos al proceso 2 (ordenador 2).

Redes de Área Local Olga Minguet 24

UD1. Caracterización de Redes Locales

5. ARQUITECTURA DE REDES

Para entender en qué consiste el proceso de encapsulación, se puede asemejar a las muñecas rusas o matrioska.

Redes de Área Local Olga Minguet 25

UD1. Caracterización de Redes Locales

Realiza las siguientes ACTIVIDADES DE TEORIA:

- Actividad 16
- Actividad 17
- Actividad 18
- Actividad 19

Redes de Área Local Olga Minguet 26

UD1. Caracterización de Redes Locales 

6. EL MODELO DE REFERENCIA OSI

Las primeras redes informáticas que se construyeron, tanto comerciales como militares, **utilizaban sus propios protocolos**. Esta situación llevó a que las empresas mantuvieran redes de diferentes fabricantes.

Cuando necesitaron comunicar esas redes, surgieron los problemas: los sistemas de transmisión **no eran compatibles** y, o bien había que deshacerse de todo lo instalado y montar redes nuevas, o bien había que desarrollar equipos adaptadores de redes, una alternativa de coste muy elevado. A partir de entonces, se comprobó que era necesario definir un **conjunto común de normas**.

OSI es el nombre del **modelo de referencia** de una arquitectura de capas para redes de ordenadores y sistemas distribuidos, propuesta por la ISO (International Standards Organization u Organización Internacional de Normalización) como estándar de interconexión de sistemas abiertos.

Redes de Área Local Olga Minguet 27

UD1. Caracterización de Redes Locales 

6. EL MODELO DE REFERENCIA OSI

Los **principios teóricos** en los que se basaron para la realización de OSI fueron fundamentalmente:

- Cada capa de la arquitectura está pensada para realizar una función bien definida.
- El número de niveles debe ser suficiente para que no se agrupen funciones distintas, pero no tan grande que haga la arquitectura inmanejable.
- Debe crearse una nueva capa siempre que se necesite realizar una función bien diferenciada del resto.

Redes de Área Local Olga Minguet 28

UD1. Caracterización de Redes Locales 

6. EL MODELO DE REFERENCIA OSI

- Las divisiones en las capas deben establecerse de forma que se minimice el flujo de información entre ellas, es decir, que la interfaz sea más sencilla.
- Permitir que las modificaciones de funciones o protocolos que se realicen en una capa no afecten a los niveles contiguos.
- Utilizar la experiencia de protocolos anteriores. Las fronteras entre niveles deben situarse donde la experiencia ha demostrado que son convenientes.
- Cada nivel debe interactuar únicamente con los niveles contiguos a él (es decir, el superior y el inferior).
- La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.

Redes de Área Local Olga Minguet 29

UD1. Caracterización de Redes Locales 

6. EL MODELO DE REFERENCIA OSI

OSI realmente no es una arquitectura de red sino un modelo de referencia, es decir, un punto de mira desde el que calibrar cómo deben relacionarse unas redes con otras por contraste con un modelo teórico, que es OSI.

El modelo propuesto por OSI estructura los servicios de red en siete **capas o niveles**.

La **primera capa** es la más cercana al **medio físico** de transmisión mientras que la **séptima capa** es la más cercana a las **aplicaciones** de usuario.

Cuando un usuario necesita transmitir datos a un destino, el sistema de red va añadiendo información de control (**cabeceras**) para cada uno de los servicios que utilizará la red para ejecutar la orden de transmisión.

Modelo OSI

7. Aplicación

6. Presentación

5. Sesión

4. Transporte

3. Red

2. Enlace de datos

1. Física

Redes de Área Local Olga Minguet 30

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

Los siete niveles de OSI reciben los siguientes nombres de menor a mayor: **físico, enlace, red, transporte, sesión, presentación y aplicación.**

Redes de Área Local Olga Minguet 31

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

Redes de Área Local Olga Minguet 32

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

Ejemplo de porqué es necesario usar OSI:

Supongamos que deseamos enviar un mensaje en papel, pero es tan grande que es necesario segmentarlo en diversas porciones → *el papel sería como la información a enviar por la red y cada porción sería una trama*

Cada trozo deberá ir acompañado de una etiqueta identificativa con el fin de poder reconstruir en el destino el mensaje original → *la información de numeración de estas etiquetas podría ser la cabecera de cada porción.*

Redes de Área Local Olga Minguet 33

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

Cada nivel tiene su propia **unidad de datos de protocolo (PDU):**

UNIDAD DATOS	NOMBRE	CAPA	NOMBRE CAPA
APDU	<i>Application Protocol Data Unit</i>	7	Aplicación
PPDU	<i>Presentation Protocol Data Unit</i>	6	Presentación
SPDU	<i>Service Protocol Data Unit</i>	5	Sesión
TPDU	<i>Presentation Protocol Data Unit</i>	4	Transporte
PAQUETE	<i>Packet</i>	3	Red
TRAMA	<i>Frame</i>	2	Enlace
BITS		1	Física

Redes de Área Local Olga Minguet 34

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

Modelo OSI

- 7. Aplicación
- 6. Presentación
- 5. Sesión
- 4. Transporte
- 3. Red
- 2. Enlace de datos
- 1. Física

Niveles OSI orientados a la red

- Nivel FÍSICO o nivel 1
- Nivel de ENLACE DE DATOS o nivel 2
- Nivel de RED o nivel 3

La Capa o Nivel de TRANSPORTE o nivel 4

Niveles OSI orientados a la aplicación

- Nivel de SESIÓN o nivel 5
- Nivel de PRESENTACIÓN o nivel 6
- Nivel de APLICACIÓN o nivel 7

Redes de Área Local Olga Minguet 35

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

6.1. Niveles OSI orientados a la red

Se dice que las **capas física, de enlace y de red** están orientadas a la red. Al subconjunto de estas tres capas inferiores se le llama bloque.

A) LA CAPA FÍSICA O NIVEL 1

- ✓ La capa física se ocupa de definir las **características mecánicas, eléctricas**, funcionales y de procedimiento para poder establecer y liberar conexiones entre dos equipos de la red.
- ✓ Debe garantizar la compatibilidad de los conectores, cuántos pines tiene cada conector y la función de cada uno de ellos, el tipo de sistema de cableado que utilizará, la duración de los pulsos eléctricos, la modulación si la hubiera, el número de voltios de cada señal, el modo de explotación del circuito, etc.
- ✓ Es la capa de **más bajo nivel**, por tanto, se ocupa de las transmisiones de los **bits expresados como señales físicas**.

Redes de Área Local Olga Minguet 36

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

6.1. Niveles OSI orientados a la red

A) LA CAPA FÍSICA O NIVEL 1

La Capa Física prepara el mensaje para la transmisión según el medio. Por ejemplo, si vamos a transmitir a través de un cable de par trenzado, es en este nivel donde el mensaje se "convierte" a pulsos eléctricos.

Redes de Área Local Olga Minguet 37

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

6.1. Niveles OSI orientados a la red

B) LA CAPA DE ENLACE DE DATOS O NIVEL 2

- ✓ La misión de la capa de enlace es establecer una línea de **comunicación libre de errores** que pueda ser utilizada por la capa inmediatamente superior: la capa de red.
- ✓ La capa de enlace fracciona el mensaje en bloques de datos denominados **tramas (frames)**.
- ✓ Estas tramas serán **enviadas en secuencia** por la línea de transmisión a través de la capa física, y **quedará a la escucha** de las tramas de confirmación que genere la capa de enlace del receptor.
- ✓ Este nivel se suele subdividir en 2 subniveles: **Subnivel de Control de Acceso al Medio (MAC)** y **Subnivel de Control Lógico de Enlace (LLC)**.

Redes de Área Local Olga Minguet 38

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.1. Niveles OSI orientados a la red
B) LA CAPA DE ENLACE DE DATOS O NIVEL 2

Los protocolos de la capa de enlace de datos regulan cómo se da formato a una trama para utilizarla en diferentes medios.

Es posible que distintos protocolos se encuentren en uso para diferentes medios.

En cada salto a lo largo de la ruta, un dispositivo intermedio acepta tramas de un medio, la desencapsula y luego envía los paquetes en una nueva trama. Los encabezados de cada trama se formatean para el medio específico que cruzará.

Redes de Área Local Olga Minguet 39

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.1. Niveles OSI orientados a la red
C) LA CAPA DE RED O NIVEL 3

- ✓ La principal función de este nivel es la del **encaminamiento o enrutamiento**, es decir, el tratamiento de cómo **elegir la ruta más adecuada** para que el bloque de datos del nivel de red (paquete) llegue a su destino.
- ✓ Otra función importante de esta capa es el **tratamiento de la congestión**. Cuando hay muchos paquetes en la red, unos obstruyen a los otros generando cuellos de botella en los puntos más sensibles.

Redes de Área Local Olga Minguet 40

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.1. Niveles OSI orientados a la red
C) LA CAPA DE RED O NIVEL 3

Determinación de la ruta: La Capa de red opera para encontrar la mejor ruta a través de la Internetwork

Redes de Área Local Olga Minguet 41

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.2. La capa de transporte o Nivel 4

- ✓ La capa de transporte es una **capa de transición** entre los niveles orientados a la red (subred) y los niveles orientados a las aplicaciones.
- ✓ Es la encargada de:
 - Permitir que un programa emisor puede **conversar** con otro receptor.
 - La **transferencia libre de errores** de los datos entre el emisor y el receptor, aunque no estén directamente conectados.
 - Proporcionar un **transporte de datos transparente** entre la máquina de origen a la de destino, independientemente de las redes físicas que existan en el emisor y receptor.

Redes de Área Local Olga Minguet 42

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

6.2. La capa de transporte o Nivel 4

Capa de Transporte

Verifica que los datos se transmitan correctamente

¿Son estos datos buenos?

Error de comprobación de mensaje

Este paquete no es bueno. Reenviar.

Conexión extremo a extremo (host a host)

Paquetes de datos

Las PDU de esta capa se llaman segmentos o mensajes

Redes de Área Local Olga Minguet 43

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

6.3. Niveles OSI orientados a la aplicación

Las capas situadas por encima del nivel transporte están **orientadas a las aplicaciones** y, por tanto, la terminología utilizada se centra más bien en las funciones de aplicación

A) LA CAPA DE SESIÓN O NIVEL 5

- ✓ Permite el diálogo entre emisor y receptor estableciendo una conexión entre ambos, denominada **sesión**.
- ✓ Facilita el **diálogo entre las aplicaciones** del emisor y del receptor.
- ✓ Se encarga de la **resincronización** de la transferencia cuando haya cortes en la transmisión, de modo que en la siguiente conexión se transmitieran datos a partir del bloque transmitido sin error.

Redes de Área Local Olga Minguet 44

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

6.3. Niveles OSI orientados a la aplicación

A) LA CAPA DE SESIÓN O NIVEL 5

Sincroniza el intercambio de datos entre capas inferiores y superiores

Me gustaría enviarte algo

Buena idea!

Gracias

De nada!

Cerrar Conexión

Establecer Conexión

Redes de Área Local Olga Minguet 45

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI

6.3. Niveles OSI orientados a la aplicación

B) LA CAPA DE PRESENTACIÓN O NIVEL 6

- ✓ Se ocupa de la sintaxis y de la semántica de la información que se pretende transmitir, es decir, investiga en el contenido informativo de los datos.
- ✓ **Comprimir los datos** para que las comunicaciones sean menos costosas.
- ✓ **Encriptación de la información**, que garantiza la privacidad de la misma.

Por ejemplo, si el ordenador emisor utiliza el código ASCII para la representación de información alfanumérica y el ordenador receptor utiliza código EBCDIC, no habrá forma de entenderse salvo que la red provea algún servicio de conversión y de interpretación de datos.

Redes de Área Local Olga Minguet 46

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.3. Niveles OSI orientados a la aplicación

B) LA CAPA DE PRESENTACIÓN O NIVEL 6

Convierte los datos de la red al formato requerido por la aplicación

Redes de Área Local Olga Minguet 47

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.3. Niveles OSI orientados a la aplicación

C) LA CAPA DE APLICACIÓN O NIVEL 7

- ✓ Es la **capa superior** de la jerarquía OSI.
- ✓ En ella se definen los protocolos que utilizarán las **aplicaciones** (modos de comunicarse) y **procesos** de los usuarios.
- ✓ Se aplica a procesos que residen en **ordenadores distintos**.
- ✓ Cuando dos procesos que desean comunicarse residen en el **mismo ordenador** utilizan para ello las funciones que le brinda **el sistema operativo**.

Redes de Área Local Olga Minguet 48

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.3. Niveles OSI orientados a la aplicación

C) LA CAPA DE APLICACIÓN O NIVEL 7

Por ejemplo, si un usuario de red quiere comunicarse con otro, podría comunicarse mediante el correo electrónico con:

- un sistema de mensajería electrónica instantánea;
- mediante una aplicación de transmisión de voz;
- si tuviera que transmitir información gráfica podrían compartir una pizarra digital, etc

Pero existen muchas más aplicaciones que requieren comunicación, como por ejemplo, la carga/ descarga de ficheros, la consulta de una página web, la impresión de documentos en red, etc.

Cada una de estas aplicaciones da origen a uno o varios protocolos del nivel 7.

Redes de Área Local Olga Minguet 49

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.3. Niveles OSI orientados a la aplicación

C) LA CAPA DE APLICACIÓN O NIVEL 7

Por ejemplo:

- ✓ Los protocolos SMTP, POP e IMAP constituyen una familia de protocolos de nivel de aplicación para la gestión del correo electrónico (servidores de correo),
- ✓ HTTP es un protocolo de nivel 7 para uso de la web (servidor web),
- ✓ FTP es el protocolo de aplicación específico para la carga y descarga de ficheros (servidor FTP), etc.

El número de protocolos de nivel 7 es muy elevado y no deja de crecer: cada aplicación nueva requiere los protocolos indispensables para su funcionamiento.

Redes de Área Local Olga Minguet 50

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI
6.3. Niveles OSI orientados a la aplicación

C) LA CAPA DE APLICACIÓN O NIVEL 7

¿Que debo enviar?

- Es la interfaz que ve el usuario final
- Muestra la información recibida
- En ella residen las aplicaciones
- Envía los datos de usuario a la aplicación de destino usando los servicios de las capas inferiores

Redes de Área Local Olga Minguet 51

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI vs TCP/IP

Modelo del protocolo	Modelo de referencia
Modelo TCP/IP	Modelo de interconexión de sistemas abiertos (OSI)
<p>Modelo TCP/IP</p>	<p>Modelo OSI</p>

Redes de Área Local Olga Minguet 52

UD1. Caracterización de Redes Locales

6. EL MODELO DE REFERENCIA OSI vs TCP/IP

Modelo OSI	Modelo TCP/IP
7. Aplicación	Aplicación
6. Presentación	
5. Sesión	Transporte
4. Transporte	
3. Red	Internet
2. Enlace de datos	Acceso a la red
1. Física	

Ambos modelos son de uso general, por lo tanto, se recomienda estar muy familiarizado con ellos.

Redes de Área Local Olga Minguet 53

UD1. Caracterización de Redes Locales

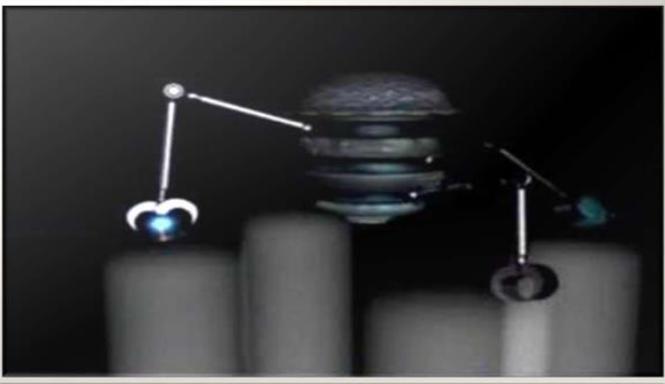
Realiza las siguientes ACTIVIDADES DE TEORIA:

- Actividad 20
- Actividad 21
- Actividad 22

Redes de Área Local Olga Minguet 54

UD1. Caracterización de Redes Locales

WARRIORS OF THE NET - 1ª PARTE



Redes de Área Local Olga Minguet 55

UD1. Caracterización de Redes Locales

WARRIORS OF THE NET - 2ª PARTE



Redes de Área Local Olga Minguet 56

8.1.2 Cuaderno de actividades

Cuaderno de Actividades

- UNIDAD 1- Caracterización de redes locales

Objetivos

- Consolidar los contenidos vistos en la Unidad Didáctica 1 del curso de Redes de Área Local.
- Aprender las diferentes topologías de redes, en un nivel teórico.
- Identificar los diferentes elementos que componen una red de ordenadores
- Conocer los niveles o capas del modelo OSI

CUADERNO DE ACTIVIDADES

Actividades

1. Comenta qué problemas se pueden generar en una red de cada topología estudiada cuando se rompe uno de los segmentos de red, por ejemplo, la conexión entre dos estaciones contiguas en un anillo, el bus de una red en árbol, etc.

Solución:

TOPOLOGÍA	PROBLEMA
Estrella	
Anillo	
Bus	
Árbol	
Malla	

2. El Instituto de Ingenieros Electrónicos y Eléctricos (IEEE) establece una numeración que *estandariza* cada una de las tecnologías utilizadas en redes. Realiza una pequeña búsqueda en Internet y averigua: ¿Cómo se llaman los estándares de la red Ethernet? ¿Y el de la red Token Ring?

Solución:

red Ethernet	
red Token Ring	

3. Elabora una lista con las ventajas e inconvenientes de cada una de las topologías de red vistas: estrella, anillo, bus, malla, árbol, irregular. Extrae al menos 1 ventaja y 1 inconveniente de las diapositivas vistas en clase.

Solución:

	Ventaja	Inconveniente
Bus		
Anillo		
Estrella		
Malla		
Árbol		

CUADERNO DE ACTIVIDADES

4. Averigua si son verdaderas o falsas las siguientes afirmaciones. Justifica la respuesta:

Solución:

Afirmación	V/F	Justificación
Una red en estrella es más rápida que una red en bus		
La rotura del anillo de una red impide totalmente la comunicación en toda la red		
La rotura de un segmento de red en una red en árbol impide la comunicación en toda la red		
Una red en bus es muy sensible a la congestión provocada por exceso de tráfico		
Una red en bus se adapta mejor a la estructura de cableado de un edificio		
Una red en anillo se adapta mejor a la estructura de un campus		
Todas las redes metropolitanas son anillos		

5. Elige qué tipo de topología de red de área local sería más adecuada para instalar en un centro docente según las situaciones siguientes. En algunos casos, sería adecuado utilizar 2 topologías diferentes. Así pues, es necesario para que sea correcta, que justifiques la respuesta.

Solución:

TIPO RED	JUSTIFICACIÓN
	Queremos conectar todos los ordenadores de un aula en una red.

CUADERNO DE ACTIVIDADES

El centro tiene tres plantas. En cada planta tenemos varias aulas y despachos. Queremos conectar en red las diferentes redes de cada una de dichas plantas

El centro está dentro de un campus y está conectado a otros edificios, en concreto a la biblioteca, al polideportivo y a secretaría

6. Busca en internet e indica dos ventajas y dos desventajas de los cuatro tipos de conmutación. En este caso puedes hacer uso de Wikipedia, pero es conveniente que tengas en tu biblioteca sitios web de contenido técnico fiable.

Solución:

	VENTAJAS	INCONVENIENTES
Conmutación de mensajes		
Conmutación de circuitos		
Conmutación de paquetes		
Multipunto		

7. ¿Cuántos tipos de nubes hay en relación con el propietario de los servicios? Define cada una de ellas tomando la teoría vista en las diapositivas.

Solución:

CUADERNO DE ACTIVIDADES

8. ¿Dónde residen los datos cuando se utiliza *Cloud computing*? ¿Y las aplicaciones?

Solución:

9. Ordena las siguientes redes de menor a mayor alcance: MAN, PAN, WAN, LAN. Indica para cada una de ellas un ejemplo de uso habitual (por ejemplo: doméstico, para comunicar una oficina, un hogar, edificios, ...)

Solución:

Mayor Alcance	Red	Ejemplo de uso
		
	Menor Alcance	

10. Enlaza los siguientes elementos característicos de distintos tipos de redes:

a) LAN	1) Entorno mundial	ij) Entorno público
b) WAN	2) Red doméstica	ii) Difusión de TV
c) MAN	3) Entorno de una ciudad	iii) Entorno privado
d) PAN	4) Entorno de un edificio u oficina	iv) Bluetooth

Solución:

CUADERNO DE ACTIVIDADES

a) LAN		
b) WAN		
c) MAN		
d) PAN		

11. Una interconexión de ordenadores en que cada uno se puede comunicar con cualquier otro sin intermediarios, ¿es propio de una red de área local o de una red de área extensa? Justifica la respuesta

Red de área local o de una red de área extensa:

Justificación:

12. Clasifica las redes que intervienen en las circunstancias que se citan a continuación según sean PAN, WAN, LAN, MAN, WLAN o WAN-Cloud computing. Razona la respuesta.

Solución:

Circunstancia	Red	Justificación
Una conexión por módem a Internet		
Un televisor recibe una transmisión televisiva por cable		
Un receptor de radio recibe por su antena la radiodifusión de un programa musical		
Un ordenador se conecta a una red para imprimir por una impresora de red		

CUADERNO DE ACTIVIDADES

Una agenda electrónica sincroniza el correo electrónico utilizando Bluetooth		
Varios usuarios comparten una conexión a Internet sin necesidad de cables		
Dos campus universitarios en la misma ciudad, pero distantes, se conectan mediante fibra óptica		
Una aplicación accede a sus datos en Internet desde cualquier lugar		

13. Una instalación de red quiere añadir dos impresoras a la red. Cada impresora se conecta a través de su interfaz de red. Sobre la primera impresora se desea que puedan imprimir todos los usuarios de la red, pero sobre la segunda impresora se quieren mantener unas ciertas restricciones. ¿Qué modelo de red —cliente/servidor o *peer to peer*— sería el más apropiado para cada una de las impresoras? Razona la respuesta.

Solución:

Primera impresora

Segunda impresora

14. Define la estructura Cliente/servidor siguiendo las indicaciones de la teoría explicada en clase.

Después cita 3 ventajas y 3 inconvenientes de esta estructura. Puedes utilizar la información contenida en tus páginas web de referencia tecnológica.

Solución:

Definición estructura cliente/servidor:

CUADERNO DE ACTIVIDADES

VENTAJAS	INCONVENIENTES

15. De los elementos que se enumeran a continuación, di cuáles son dispositivos activos de interconexión de red y cuáles no. Recuerda que un dispositivo ACTIVO significa que "hace algo" con lo que recibe antes de transmitirlo, esto es, ejerce algún tipo de *control*.

Razona la respuesta.

Solución:

Elemento	Activo / Pasivo	Justificación
Encaminador		
Punto de acceso inalámbrico		
Cable coaxial		
Conmutador		
Armario de comunicaciones		
Disco duro		
Sistema operativo de red		
Módem		
Conexión ADSL		
Router ADSL		

CUADERNO DE ACTIVIDADES

16. ¿Cuál es la familia de protocolos de red más utilizada en la actualidad?

Solución:

Busca por Internet 5 protocolos que pertenezcan a ésta familia y di para qué se utilizan:

NOMBRE	PARA QUÉ SE USA
Protocolo 1	
Protocolo 2	
Protocolo 3	
Protocolo 4	
Protocolo 5	
Protocolo 6	

17. Enlaza los siguientes elementos característicos sobre familias de protocolos:

1. NetWare	a. Internet	i. NWLink
2. NetBeui	b. NetBIOS	ii. IBM y Microsoft
3. TCP/IP	c. IPX/SPX	iii. RFC

Solución:

1) NetWare		
2) NetBeui		
3) TCP/IP		

18. ¿Qué es y para qué sirve un documento RFC?

Solución:

CUADERNO DE ACTIVIDADES

19. ¿Cuál es el protocolo de red nativo para las primitivas redes de ordenadores de Microsoft?

¿Puede convivir este protocolo con otros de otras familias?

20. Vamos a consolidar la nomenclatura de cada una de las capas OSI rellenando en la siguiente tabla conceptual los nombres de las capas y las funciones fundamentales de cada una de ellas. Es importante que entresagues toda la información posible de la TEORIA que hemos visto en clase.

Solución:

Niveles OSI	Se llama	Sus funciones son
Nivel 1		
Nivel 2		
Nivel 3		
Nivel 4		
Nivel 5		
Nivel 6		
Nivel 7		

21. ¿Qué es una trama de red?

¿Y un paquete de red?

CUADERNO DE ACTIVIDADES

¿Y una TPDU?

¿Y una SPDU?

22. ¿Qué función de red podrías asociar con cada nivel OSI?

Solución:

Función	Nivel OSI asociado
Agrupación de bits en tramas	
Mandar un correo electrónico	
Establecer la ruta de destino de un paquete	
Consolidar un cable en un conector	
Codificar una página web	

8.1.3 Cuaderno de prácticas

UNIDAD 1. CARACTERIZACIÓN DE REDES LOCALES

MI RED LOCAL

Objetivos

- Registrar todos los diferentes dispositivos conectados a la red en el aula.
- Investigar cómo se conecta cada dispositivo a la red para enviar y recibir información.
- Crear un diagrama que represente la topología de la red.
- Marcar cada dispositivo con su función dentro de la red.

Aspectos básicos

El trayecto que toma un mensaje desde el origen al destino puede ser tan simple como un solo cable que conecta una computadora con otra o tan complejo como una red que, literalmente, abarca todo el planeta. La infraestructura de red contiene tres categorías de componentes de hardware:

- Terminales
- Dispositivos de red intermedios
- Medios de red

Observa atentamente la red que tienes en clase.

Por ejemplo:

No es necesario que tú realices una tabla así, solamente que observes cada una de estas características en los dispositivos que existen en tu red.

Fabricante	Dispositivo	Conexión	Medios
Apple	iPhone	Inalámbrica	Wifi y celular
Samsung	Galaxy Smart Phone	Inalámbrica	Wifi y celular
Cisco	Cable módem	Cableada	Cable coaxial de TV por cable y cable de Ethernet
Linksys	Router inalámbrico	Cableada	Cable de Ethernet
HP	Impresora o escáner	Inalámbrica	Wifi
Apple	MacBook Air	Inalámbrica	Wifi
Beats by Dre	Auriculares	Inalámbrica	Bluetooth
Microsoft	Xbox	Cableada	Cable de Ethernet

UNIDAD 1 – PRACTICA 1

Ejercicio 1. Dibuja un diagrama de la red local. Marca cada dispositivo con nombre y ubicación.

UNIDAD 1 – PRACTICA 1

Ejercicio 2. ¿Hay otros dispositivos electrónicos que no están conectados a la red local para compartir información y recursos con nuestra red? ¿Cuál sería el beneficio de tener estos dispositivos en línea?

Ejercicio 3. ¿Qué tipo de conectividad se usa con más frecuencia en esta red local, cableada o inalámbrica? ¿Y generalmente, qué tipo de conectividad se usa con más frecuencia?

UNIDAD 1 – PRACTICA 2

UNIDAD 1. CARACTERIZACIÓN DE REDES LOCALES

MI DÍA EN LÍNEA

Objetivos

- Registrar todas sus interacciones en línea durante un solo día.
- Categorizar las razones que respaldan sus actividades en línea.
- Describir cómo podría realizar las mismas tareas sin estar en línea.

Aspectos básicos

Todo a lo que accede en línea se encuentra en algún lugar en la Internet global. Los sitios de medios sociales, juegos multijugador, centros de mensajería que proporcionan correo electrónico... todos los destinos de Internet se conectan a redes locales que envían y reciben información a través de Internet.

Piense en todas las interacciones que realiza durante el día que requieren estar en línea. Use esta hoja de trabajo para hacer una lista y compartirla con sus compañeros. Agregue todos los renglones o páginas que sean necesarios.

Muestra:

Hora	Dispositivo	Actividad	Motivo	Alternativa
8:00	Teléfono	Revisar correo	Responder mensajes importantes	Ninguna
8:15	Teléfono	Revisar los mensajes de texto que llegaron durante la noche	Saber qué novedades hay	¿Llamar a todos?
8:30	Computadora de escritorio	Iniciar sesión en la biblioteca de la escuela para revisar las tareas	Prepararme para clase	Imprimir el calendario, los horarios de los cursos y el programa
8:35	Teléfono	Revisar Facebook e Instagram	Actualizar	Imprimir y compartir fotos Copiar vídeos en un pen drive y mostrárselos a alguien en persona
9:00	Teléfono	Jugar a "Angry Birds"	Entretenimiento	Aburrimiento
Mediodía	Teléfono	Usar Google Maps para pedir una pizza	Hambre	Llamar a asistencia de directorio

1

UNIDAD 1 – PRACTICA 2

Realiza tu propia lista con las actividades que realizaste ayer, por ejemplo, o las que sueles realizar normalmente:

Hora	Dispositivo	Actividad	Motivo	Alternativa

Ejercicio 1. ¿Cuántas de tus actividades diarias en línea no serían posibles sin conectarse a Internet o a la red local?

Ejercicio 2. ¿Cuántos dispositivos diferentes has utilizado para realizar tus actividades en línea?

2

UNIDAD 1 – PRACTICA 2

Ejercicio 3. ¿Qué cantidad promedio de tiempo estás habitualmente "conectado"?

Ejercicio 4. ¿Con cuántos dispositivos puedes estar conectado a la vez?

Ejercicio 5. ¿Crees que la edad es un motivo para estar más o menos "conectado"?

Ejercicio 6. ¿Crees que el género es un motivo para estar más o menos "conectado"?

Ejercicio 7. ¿Cómo crees que influyen todos estos datos a la forma de desarrollarse y funcionar de las empresas?

UNIDAD 1 – PRACTICA 3

UNIDAD 1. CARACTERIZACIÓN DE REDES LOCALES

CONCEPTO ACTUAL DE INTERNET

Objetivos

- Demostrar que las redes constan de varios componentes diferentes.

Aspectos básicos

Dibuja y rotula un mapa de Internet tal como la interpretas en el presente. Incluye la ubicación de tu hogar o lugar de estudios y el cableado, los equipos y los dispositivos correspondientes, entre otros elementos. Es posible que te ayude incluir algunos de los siguientes elementos:

- o Dispositivos o equipos
- o Medios (cableado)
- o Direcciones o nombres de enlace
- o Orígenes y destinos
- o Proveedores de servicios de Internet

Aquí tienes el ejemplo de un alumno que te puede ayudar a comenzar:



No es necesario que tú realices una tabla así, solamente que observes cada una de estas características en los dispositivos que existen en tu red.

También puedes visitar <http://www.kk.org/internet-mapping> donde encontrarás otros dibujos similares de otros alumnos.

UNIDAD 1 – PRACTICA 3

Ejercicio 1. Dibuja tu concepto actual de Internet, con las indicaciones realizadas en el enunciado de la Práctica.



UNIDAD 1 – PRACTICA 3

Ejercicio 2. Tras haber visto los dibujos de otros compañeros de clase, ¿crees que había dispositivos informáticos que podrías haber incluido en tu diagrama? ¿Cuáles?

Ejercicio 3. ¿Qué similitudes y diferencias encuentras en los diseños de algunos modelos? ¿Realizarías alguna modificación importante a tu dibujo después de ver los otros?

Ejercicio 4. ¿Crees que tu dibujo y los iconos que has realizado pueden ayudar, a ti y a tus compañeros, a organizar el proceso mental y facilitar el aprendizaje del concepto de Internet?

UNIDAD 1 – PRACTICA 4

UNIDAD 1. CARACTERIZACIÓN DE REDES LOCALES

CREACIÓN DE UNA RED SIMPLE

Topología



Tabla de direccionamiento

Dispositivo	Interface	Dirección IP	Máscara de subred
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Objetivos

Parte 1: Configuración de la topología de la red (Ethernet únicamente)

- Identificar los cables y puertos para usar en la red.
- Realizar el cableado de una topología física de laboratorio.

Parte 2: Configuración de hosts en las PC

- Introducir la información de dirección IP estática en la interfaz LAN de los hosts.
- Verificar que las PC puedan comunicarse por medio de la utilidad ping.

Aspectos básicos

Las redes están formadas por tres componentes principales: hosts, switches y routers. En este laboratorio, armará una red simple con dos hosts y un switch. En esta práctica de laboratorio, aplicará la asignación de direcciones IP a las PC para habilitar la comunicación entre estos dos dispositivos. Use la utilidad ping para verificar la conectividad.

Nota: Los switches que se usan son Cisco Catalyst 2960 con Cisco IOS Release 15.0(2) (imagen lanbasek9). Se pueden utilizar otros switches y otras versiones de Cisco IOS.

UNIDAD 1 – PRACTICA 4

Recursos necesarios

- 1 switch (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o similar)
- 2 PC (Windows 10)
- 2 cables Ethernet como se muestra en la topología.

UNIDAD 1 – PRACTICA 4

Part 1: Configuración de la topología de la red (Ethernet únicamente)

En la parte 1, realizará el cableado para conectar los dispositivos según la topología de la red.

Paso 1: Encienda los dispositivos.

Encienda todos los dispositivos de la topología. Los switches no tienen un interruptor de corriente; se encienden en cuanto enchufa el cable de alimentación.

Paso 2: Conecte las PC al switch.

- Conecte un extremo de un cable Ethernet al puerto de NIC en PC-A. Conecte el otro extremo del cable a F0/6 en S1. Después de conectar la PC al switch, la luz de F0/6 debería tomarse ámbar y luego verde, lo que indica que la PC-A se conectó correctamente.
- Conecte un extremo de un cable Ethernet al puerto de NIC en PC-B. Conecte el otro extremo del cable a F0/1 en S1. Después de conectar la PC al switch, la luz de F0/1 debería tomarse ámbar y luego verde, lo que indica que la PC-B se conectó correctamente.

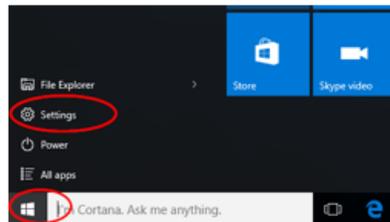
Paso 3: Inspeccione visualmente las conexiones de red.

Después de realizar el cableado de los dispositivos de red, tómese un momento para verificar cuidadosamente las conexiones con el fin de minimizar el tiempo necesario para solucionar problemas de conectividad de red más adelante.

Part 2: Configuración de hosts en las PC

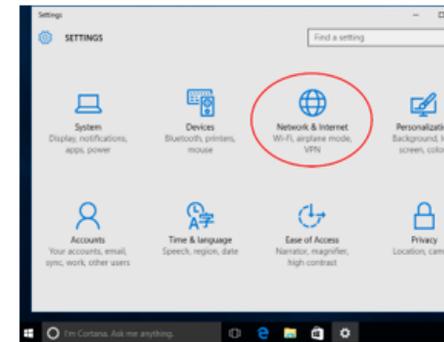
Paso 1: Configure la información de dirección IP estática en las PC.

- Para configurar los ajustes de red en PC-A, haga clic en Inicio, luego en Configuración.

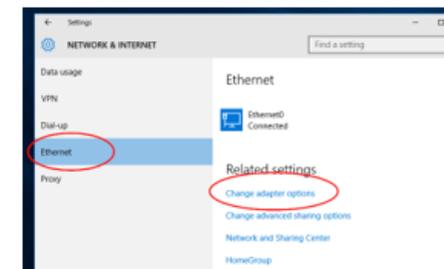


UNIDAD 1 – PRACTICA 4

- En la ventana Configuración, haga clic en **Redes e Internet**.

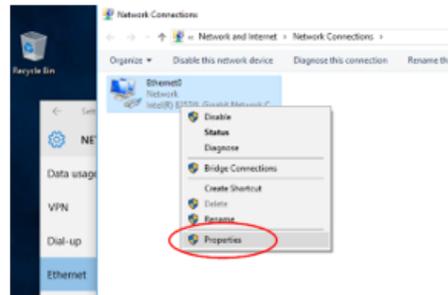


- En el panel izquierdo, seleccione **Ethernet**, luego haga clic en **Cambiar configuración del adaptador**.

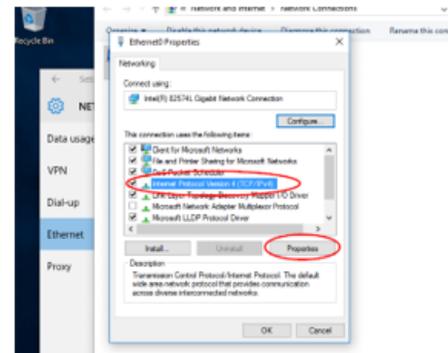


UNIDAD 1 – PRACTICA 4

- d. La ventana Conexiones de red muestra las interfaces de red disponibles en la PC. Haga clic con el botón secundario del mouse en la interfaz **Ethernet0** y seleccione **Propiedades**.



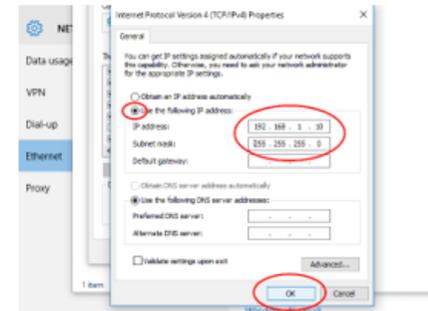
- e. Seleccione la opción **Protocolo de Internet versión 4 (TCP/IPv4)** y, a continuación, haga clic en **Propiedades**.



Nota: También puede hacer doble clic en **Protocolo de Internet versión 4 (TCP/IPv4)** para que se muestre la ventana Propiedades.

UNIDAD 1 – PRACTICA 4

- f. Haga clic en el botón de opción **Usar la siguiente dirección IP** para introducir manualmente una dirección IP, la máscara de subred y el Gateway predeterminado. Escriba la dirección IP 192.168.1.10 y la máscara de subred 255.255.255.0.



Nota: En el ejemplo anterior, se ingresó la dirección IP y la máscara de subred para la PC-A. No se ingresó el Gateway predeterminado porque no había ningún router conectado a la red. Consulte la tabla de direccionamiento de la página 1 para obtener información de dirección IP para la PC- B.

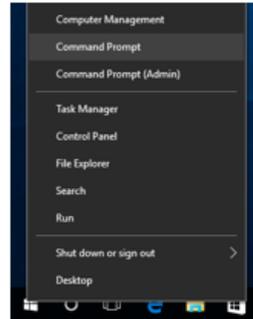
- g. Después de introducir toda la información IP, haga clic en **Aceptar**. Haga clic en **Aceptar** en la ventana de propiedades de Ethernet0 para asignar la dirección IP al adaptador LAN.
h. Repita estos pasos para introducir la información de la dirección IP en PC-B.

UNIDAD 1 – PRACTICA 4

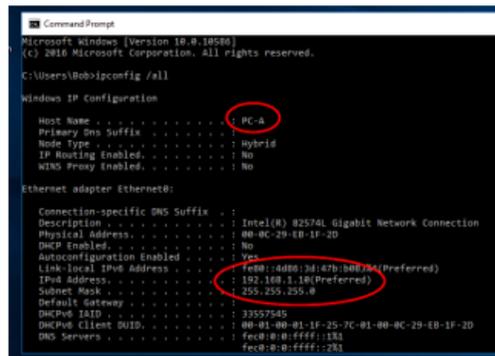
Paso 2: Verifique la configuración y la conectividad de la PC.

Use la línea de comandos para verificar la configuración de la PC y la conectividad.

- a. Desde PC-A, haga clic con el botón secundario del mouse en Inicio, seleccione Línea de comandos.

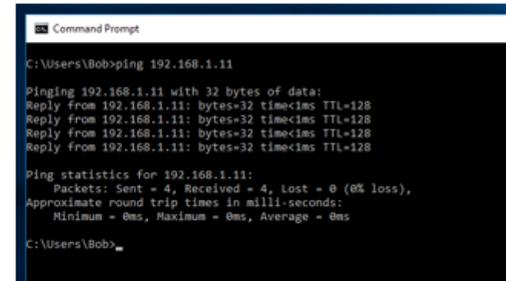


- b. En la ventana cmd.exe, puede introducir comandos directamente en la PC y ver los resultados de esos comandos. Verifique la configuración de la PC mediante el comando ipconfig /all. Este comando muestra información sobre el nombre del host de la PC y la dirección IPv4.



UNIDAD 1 – PRACTICA 4

- c. Escriba ping 192.168.1.11 y presione Intro.



¿Fueron correctos los resultados del ping?

Si no, es muy probable que el Firewall de Windows esté bloqueando las solicitudes de eco ICMP (ping). Haga clic en Inicio > Configuración > Redes e Internet > Ethernet > Firewall de Windows para apagarlo.

Nota: Si no obtuvo una respuesta de PC-B, intente hacer ping a PC-B nuevamente. Si sigue sin obtener respuesta de PC-B, intente enviar un comando ping a PC-A desde PC-B. Si no puede obtener respuesta desde la PC remota, pida al instructor que lo ayude a solucionar el problema.

8.1.4 Trabajo de investigación

UNIDAD 1 – TRABAJO DE INVESTIGACIÓN 1

UNIDAD 1. CARACTERIZACIÓN DE REDES LOCALES

INVESTIGACIÓN REDES PAN, LAN, MAN Y WAN, Y MEDIOS DE TRANSMISIÓN

Objetivos

- Conocer las principales características de los diferentes tipos de redes en función de su alcance.
- Extraer una opinión objetiva sobre las ventajas e inconvenientes de los distintos tipos de redes.

Aspectos básicos

Esta es una práctica de investigación sobre topologías de red. Tendremos que responder de forma extensa, a modo de trabajo, a las siguientes actividades que se indican. El tamaño de la letra se debe respetar, aunque podemos incluir títulos y subtítulos según nuestra creatividad.

El total de esta práctica/trabajo no sobrepasará las 6 páginas, ni estará por debajo de las 4.

UNIDAD 1 – TRABAJO DE INVESTIGACIÓN 1

Ejercicio 1. Buscar información en Internet sobre los diferentes tipos de redes visto en clase según su alcance: PAN, LAN, MAN y WAN

Realizaremos un apartado para tipo de red en el que se indicará, para cada uno de ellos:

- > Una breve descripción de la red en cuestión.
- > Radio de cobertura máximo.
- > Velocidades que se pueden obtener.
- > Medios de transmisión más habituales.
- > Ventajas que tiene este tipo de red.
- > Inconvenientes que tiene este tipo de red.
- > 2 ejemplos de redes de este tipo que podemos encontrar.

Ejercicio 2. Buscar información en Internet sobre los siguientes tipos de tecnologías de transmisión de información entre dispositivos: Bluetooth, infrarrojos, Wifi, cable de par de cobre y fibra óptica.

Realizaremos un apartado para cada tipo de tecnología en el que se indicará, para cada uno de ellos:

- > Una breve descripción del tipo de tecnología en cuestión.
- > Alcance (distancia) máxima que se suele conseguir.
- > Velocidades que se pueden obtener.
- > Ventajas que tiene este tipo de tecnología.
- > Inconvenientes que tiene este tipo de tecnología.
- > 2 ejemplos de aplicación de esta tecnología.

UNIDAD 1 – TRABAJO DE INVESTIGACIÓN 2

UNIDAD 1. CARACTERIZACIÓN DE REDES LOCALES

**INVESTIGACIÓN SOBRE LOS NIVELES DEL
MODELO OSI (Grupos de 2 personas)**

Objetivos

- Conocer los niveles del modelo OSI y las principales funcionalidades de cada uno.

Aspectos básicos

Esta es una práctica de investigación sobre el MODELO OSI.

Vamos a realizar una PRESENTACIÓN en PowerPoint de 9 diapositivas donde tendremos que seguir las siguientes especificaciones:

- Introducción: qué es OSI y breve historia: quién o quienes lo inventaron y cuándo, uso actual, ... (1 diapositiva).
- Realizar un Cuadro sinóptico/Esquema en el que se identifiquen los 7 niveles de OSI (1 diapositiva) y para cada uno se incluya un hipervínculo a su diapositiva de explicación.
- Pulsando en cada nivel, la presentación mostrará la diapositiva de detalle que describe dicho nivel (1 diapositiva por cada nivel, en total hay 7 niveles). De cada nivel se indicará información sobre sus funciones más importantes, para qué se utiliza y aplicación práctica.

El trabajo NO contendrá videos ni enlaces a videos.

8.2 Unidad didáctica 2

Esta segunda unidad se ocupa del nivel físico de la red, es decir, de las funciones y especificaciones de la primera capa del modelo de referencia OSI. Sin embargo, la instalación de red no solo implica cables y conectores. La red debe extenderse, lo que hace que el despliegue del sistema de cableado sea más complejo que la simple confección de los cables por donde viajará la señal de red.

Otro aspecto importante será la topología de la red local. De cada topología se comprueba que existen distintas tecnologías que se distinguen según del medio de transmisión a utilizar, la velocidad de transmisión, la longitud máxima de la red, etc., en vistas a una calidad de transmisión. El medio debe ser adecuado para la transmisión de la señal física con objeto de producir la conexión y la comunicación entre dos dispositivos.

Se trabaja que, antes de proceder a la instalación física de la red, es necesario realizar un estudio previo que recoja todas las necesidades, factores de costo y opciones de implementación de la red. De cara a planificar y diseñar la misma. Y, una vez realizado el diseño, se procede a la instalación física de la red.

La creación del diseño físico de una red de área local y la elaboración de un listado de materiales, diseñando el cableado y situando los elementos funcionales comunicados entre sí, es el objetivo que se pretende conseguir con ésta unidad didáctica.

8.2.1 Presentación teórica

CURSO

Redes de Área Local

UNIDAD 2

Identificación de elementos y espacios físicos de una red local. Medios de transmisión.

Redes de Área Local
Olga Minguet
1

UD2. Identificación de elementos y espacios físicos

ÍNDICE

1. [Transmisión de señales. Conceptos básicos](#)
2. [Los medios de transmisión](#)
3. [Dispositivos de conexión de cables](#)
4. [El cableado de la red. Cableado estructurado y certificado. Instalación del CPD.](#)

Redes de Área Local
Olga Minguet
2

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

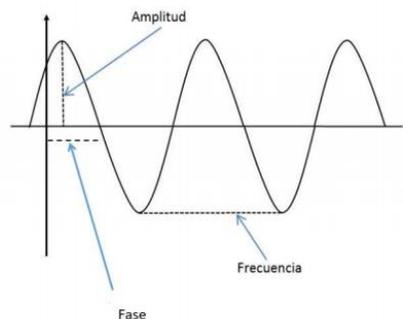
Una señal viene definida por tres características:

- ✓ **Amplitud**, que es el valor máximo de la señal en un intervalo.
- ✓ **Frecuencia**, que determina el número de veces que la señal se repite por segundo (medido en Hertzios o Hz)
- ✓ **Fase**, que indica el intervalo de tiempo que va desde el instante inicial al primer punto donde la señal toma el valor 0.

Redes de Área Local
Olga Minguet
3

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos



Redes de Área Local
Olga Minguet
4

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

Múltiplos del Sistema Internacional para hercio (Hz)

Submúltiplos			Múltiplos		
Valor	Símbolo	Nombre	Valor	Símbolo	Nombre
10 ⁻¹ Hz	dHz	decihercio	10 ¹ Hz	daHz	decahercio
10 ⁻² Hz	cHz	centihercio	10 ² Hz	hHz	hectohercio
10 ⁻³ Hz	mHz	milihercio	10 ³ Hz	kHz	kilohercio
10 ⁻⁶ Hz	μHz	microhercio	10 ⁶ Hz	MHz	megaheercio
10 ⁻⁹ Hz	nHz	nanohercio	10 ⁹ Hz	GHz	gigaheercio
10 ⁻¹² Hz	pHz	picohercio	10 ¹² Hz	THz	teraheercio
10 ⁻¹⁵ Hz	fHz	femtohercio	10 ¹⁵ Hz	PHz	petaheercio
10 ⁻¹⁸ Hz	aHz	attohercio	10 ¹⁸ Hz	EHz	exaheercio
10 ⁻²¹ Hz	zHz	zeptohercio	10 ²¹ Hz	ZHz	zettaheercio
10 ⁻²⁴ Hz	yHz	yoctohercio	10 ²⁴ Hz	YHz	yottaheercio

Los prefijos más comunes están en negrita.

Redes de Área Local Olga Minguet 5

UD2. Identificación de elementos y espacios físicos

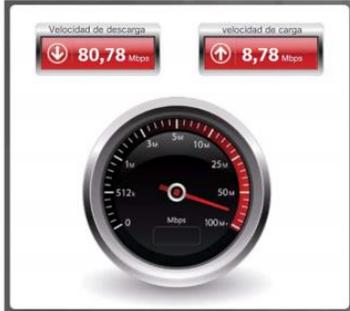
1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental de ancho de banda
Kilobits por segundo	kbps	1 kbps = 1000 bps = 10 ³ bps
Megabits por segundo	Mb/s	1 Mb/s = 1 000 000 bps = 10 ⁶ bps
Gigabits por segundo	Gb/s	1 Gb/s = 1 000 000 000 bps = 10 ⁹ bps
Terabits por segundo	Tb/s	1 Tb/s = 1 000 000 000 000 bps = 10 ¹² bps

Redes de Área Local Olga Minguet 6

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos



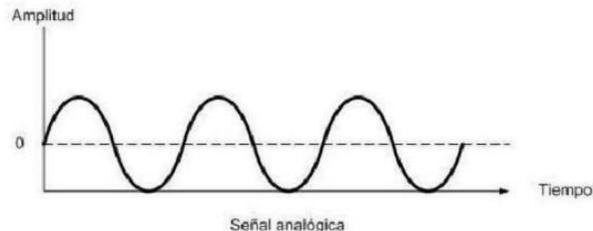
<https://www.speedtest.net/speedtest>

Redes de Área Local Olga Minguet 7

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

Las **señales analógicas** se caracterizan por representar funciones **continuas en el tiempo** y pueden tomar **cualquier valor** de voltaje dentro de un rango que permita el medio de transmisión.

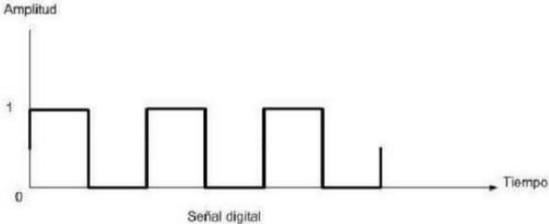


Redes de Área Local Olga Minguet 8

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

Las **señales digitales** se caracterizan por representar funciones **discretas en el tiempo** y únicamente pueden tomar **algunos valores** dentro de un rango (la más común es la binaria, que sólo puede tomar dos valores, 0 y 1).



Amplitud

1

0

Tiempo

Señal digital

Redes de Área Local Olga Minguet 9

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

Para transmitir la información por un determinado medio (el aire, cables, etc.), es necesario **convertir de alguna forma los BITS (0 y 1) de la señal digital** para que puedan viajar hasta el receptor y éste pueda interpretarlos correctamente.

En el interior de un ordenador, los dígitos binarios se transmiten de unos dispositivos a otros como señales eléctricas convenientemente codificadas.

A cada dígito binario se le puede asociar un nivel de tensión o voltaje diferente. **Éste es el principio fundamental de la electrónica digital.**

Redes de Área Local Olga Minguet 10

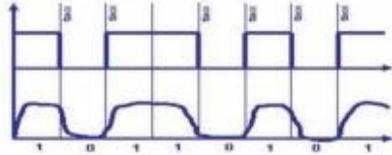
UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

Por ejemplo: un valor de +5 voltios para representar un "1" y 0 voltios para representar un "0".

Esto es equivalente a decir que los circuitos de un ordenador interpretan:

- un "1" cuando por la conexión correspondiente reciben corriente eléctrica (la tensión se aproxima a +5 voltios)
- un "0" cuando no hay corriente.



Redes de Área Local Olga Minguet 11

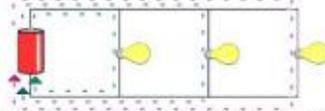
UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

El funcionamiento de los circuitos digitales es análogo al de una bombilla corriente:

- ✓ cuando se **enciende**, podemos considerarlo un "1" y
- ✓ cuando está **apagada**, como un "0".

Solamente se encenderá la bombilla cuando circule corriente eléctrica a través de ella (y su voltaje sea adecuado).



Es necesario que exista un cable que haga de masa (tierra) para que el circuito se cierre y pueda circular corriente por él; además, se toma como voltaje de referencia (0 voltios).

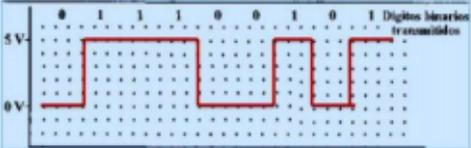
Redes de Área Local Olga Minguet 12

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Conceptos básicos

Ejemplo

Supongamos que deseamos transmitir el número 334 (101001110 en binario) por un único cable de cobre de dos hilos.



Otra característica que determina a una señal digital es la duración de cada pulso (de cada dígito binario), para poder saber cuántos llegan en caso de que recibamos el mismo dígito repetido de forma consecutiva.

Redes de Área Local Olga Minguet 13

UD2. Identificación de elementos y espacios físicos

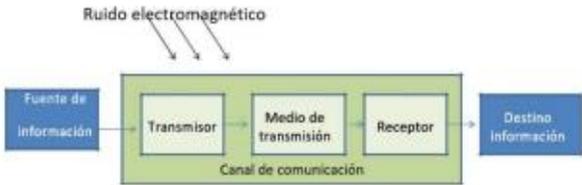
Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 1
- Actividad 2

Redes de Área Local Olga Minguet 14

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Perturbaciones en la transmisión

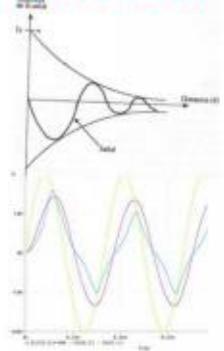


Redes de Área Local Olga Minguet 15

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Perturbaciones en la transmisión

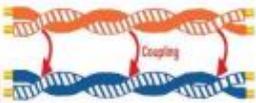
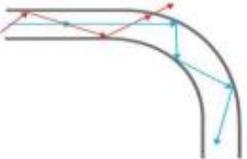
- ✓ **Atenuación**
 - Disminución de la amplitud de la señal.
 - Depende de la distancia recorrida.
 - Afecta a todos los tipos de señales.
- ✓ **Interferencia electromagnética**
 - El medio de transmisión se verá afectado por ondas electromagnéticas emitidas por equipos eléctricos o por comunicaciones inalámbricas.
 - Las señales eléctricas se ven afectadas por esta perturbaciones.
 - No afectan a las comunicaciones ópticas.



Redes de Área Local Olga Minguet 16

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Perturbaciones en la transmisión

- ✓ **Diafonía**
 - Interferencia entre señales producidas cuando los cables están muy juntos.
 - Afecta a las transmisiones eléctricas.
- ✓ **Dispersión**
 - El haz de luz rebota en las paredes de la fibra hasta llegar a su destino, provocando pérdida de señal.
 - Sólo se da en medios de transmisión ópticos.

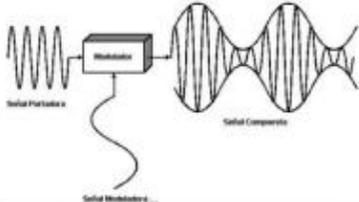
Redes de Área Local Olga Minguet 17

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Modulación

Una **señal portadora** (con la información) está **modulada** por otra **señal moduladora** que modifica algún parámetro (**amplitud, frecuencia o fase**) de la primera.

Al dispositivo que realiza esta conversión se le llama **módem (MODuladorDEModulador)**.



Redes de Área Local Olga Minguet 18

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Modulación

AM: Modulación de Amplitud (*Amplitude Modulation*)
FM: Modulación de Frecuencia (*Frequency Modulation*)
PM: Modulación de Fase (*Phase Modulation*)

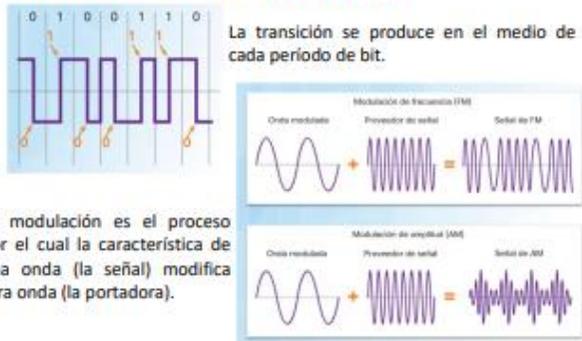
Señal digital	0	1	0	1	1	0	1	1
AM								
FM								
PM								

Redes de Área Local Olga Minguet 19

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Modulación

La transición se produce en el medio de cada período de bit.



La modulación es el proceso por el cual la característica de una onda (la señal) modifica otra onda (la portadora).

Redes de Área Local Olga Minguet 20

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Canal de comunicación

Banda base

- ✓ La información **se transmite tal cual** por el medio de transmisión, normalmente en **forma digital**.
- ✓ Esto hace que **no sea idónea para comunicaciones remotas**, ya que la señal se degrada con la distancia y tampoco se adecúa a entornos expuestos a ruidos electromagnéticos e interferencias.
- ✓ En este caso no haría falta módems por lo que es adecuada para **cortas distancias**.
- ✓ Sólo se puede enviar **una única señal por el mismo medio**.

Ejemplo de transmisión en banda base son la **conexión entre un ordenador y una impresora**.

Redes de Área Local Olga Minguet 21

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Canal de comunicación

Banda ancha

- ✓ La información se transmite por el medio de transmisión, normalmente en forma **analógica**.
- ✓ La señal que transporta la información está **modulada**, por lo que sufre una serie de variaciones que pueden afectar al valor de su amplitud, frecuencia o fase.
- ✓ En un mismo medio se pueden transmitir diversas portadoras (**diversas señales**).

Ejemplo de característico de la transmisión en banda ancha lo constituye las **señales de radio o de televisión**.

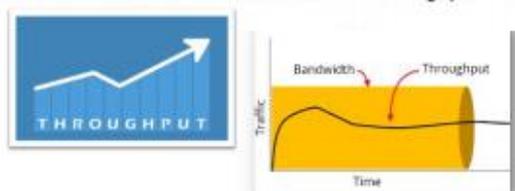
Redes de Área Local Olga Minguet 22

UD2. Identificación de elementos y espacios físicos

1. TRANSMISIÓN DE SEÑALES. Canal de comunicación

THROUGHPUT

Se llama *throughput* (rendimiento de la transmisión) al volumen de trabajo o de **información neto** que fluye a través de un sistema, como puede ser una red de computadoras. Al **modular** las señales, se **aumenta** el *throughput* del sistema.



Redes de Área Local Olga Minguet 23

UD2. Identificación de elementos y espacios físicos

Realiza las siguientes **ACTIVIDADES** del Cuaderno de Actividades:

- **Actividad 3**
- **Actividad 4**
- **Actividad 5**

Redes de Área Local Olga Minguet 24

UD2. Identificación de elementos y espacios físicos 

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

Los cables de pares están formados por pares de filamentos **metálicos** y constituyen el modo más **simple y económico** de todos los medios de transmisión.

Sin embargo, presentan algunos inconvenientes: cuando se sobrepasan ciertas longitudes, hay que acudir al **uso de repetidores** para restablecer el nivel eléctrico de la señal.

Tanto la transmisión como la recepción utilizan un par de conductores que, **si no están apantallados, son muy sensibles a interferencias y diafonías** producidas por la inducción electromagnética de unos conductores en otros.

Redes de Área Local Olga Minguet 25

UD2. Identificación de elementos y espacios físicos 

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

Un modo de subsanar estas interferencias consiste en **trenzar los pares** de modo que las intensidades de transmisión y recepción anulen las perturbaciones electromagnéticas sobre otros conductores próximos.

Esta es la razón por la que este tipo de cables se llaman **cables de pares trenzados**.

Existen fundamentalmente **dos tipos** de cables de pares trenzados:

- ✓ UTP son las siglas de Unshielded Twisted Pair
- ✓ STP son las siglas de Shielded Twisted Pair

Redes de Área Local Olga Minguet 26

UD2. Identificación de elementos y espacios físicos 

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

Cable UTP

Par de cable no apantallado (Unshielded Twisted Pair)

- ✓ Es un cable de pares trenzado y sin recubrimiento metálico externo, de modo que es sensible a las interferencias.
- ✓ Es un cable barato, flexible y sencillo de instalar.



Redes de Área Local Olga Minguet 27

UD2. Identificación de elementos y espacios físicos 

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

Cable FTP

Par de cable con pantalla global (Folied Twisted Pair)

- ✓ Este cable es semejante al UTP, ya que los pares trenzados no están recubiertos pero se le añade un **recubrimiento metálico global**.
- ✓ Este recubrimiento debe ser conectado a la tierra de la instalación.
- ✓ Es un cable **más protegido y menos flexible que el UTP**.
- ✓ El sistema de trenzado es idéntico al del cable UTP.



Redes de Área Local Olga Minguet 28

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

Cable STP

Par de cable apantallado (Shielded Twisted Pair)

- ✓ Este cable es semejante al UTP pero se le añade un **recubrimiento metálico** para evitar las interferencias externas.
- ✓ Este recubrimiento debe ser conectado a la tierra de la instalación.
- ✓ Es un cable **más protegido**, pero **menos flexible** que el UTP y FTP.



Redes de Área Local Olga Minguet 29

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

El cable STP es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.

Para situaciones de **protección extrema** podemos encontrar el cable **SFTP**, que es una combinación de cables STP y FTP, ya que posee cubierta metálica global y en cada par trenzado



Redes de Área Local Olga Minguet 30

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

Comparación entre UTP y STP

- ✓ **Eléctricamente**, el cable STP tiene más ventajas eléctricas que el cable UTP (menos interferencias).
- ✓ **En cuanto a la instalación**, debido a que STP está apantallado, es mucho menos flexible, lo que a veces dificulta el tendido del cable debido a su rigidez.
Esto hace que solo se utilice donde realmente hace falta: en entornos eléctricamente hostiles (con muchas interferencias electromagnéticas).
- ✓ Además, las mallas protectoras de los cables STP deben estar conectados a tierra, lo que multiplica el trabajo de instalación.

Redes de Área Local Olga Minguet 31

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

Comparación entre UTP y STP.

- ✓ **En cuanto al throughput**: ambos tipos de cables pueden transmitir desde 10 Mbps hasta 10 Gbps.
- ✓ **En cuanto al coste del cable**: STP es más caro que UTP.
- ✓ **En cuanto al coste de instalación**: STP es más caro puesto que requiere la conexión de su malla externa metálica a tierra, algo que no es requerido en UTP.
- ✓ **En cuanto a los conectores**: ambos pueden utilizar conectores RJ45.
- ✓ **En cuanto al ruido y la inmunidad a señales no deseadas**: STP es mucho más inmune al ruido que UTP, ya que está más protegido.

Redes de Área Local Olga Minguet 32

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

Clasificación cables de pares. 1ª clasificación: las categorías.
 Típicamente se puede construir una red Ethernet con topología en **estrella** con cable UTP de **categoría 5e o 6** utilizando **segmentos de 100m** como máximo.

Clasificación cables de pares. 2ª clasificación: las clases.
 Cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de estas características.

Redes de Área Local Olga Minguet 33

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

CLASES	Clase A	Clase B	Clase C	Clase D	Clase E	Clase F
Ancho de banda	100 KHz	1 MHz	20 MHz	100 MHz	250 MHz	600 MHz
Cat. 3	2 km	500 m	100 m	No hay	No hay	No hay
Cat. 4	3 km	600 m	150 m	No hay	No hay	No hay
Cat. 5	3 km	700 m	160 m	100 m	No hay	No hay
Cat. 6	Sin uso	Sin uso	Sin uso	Sin uso	1 Gbps	No hay
Cat. 7	Sin uso	10 Gbps				

Características de longitudes posibles y anchos de banda para las clases y categorías de pares trenzados.

Redes de Área Local Olga Minguet 34

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos



Cable de Categoría 3 (UTP)



Cable de Categoría 5 o 5e (UTP)



Cable de Categoría 6 (UTP)

- El cableado UTP cumple con los estándares establecidos por la TIA/EIA.
 - TIA/EIA-568 establece los estándares de cableado para las instalaciones de LAN.
- Cable de categoría 3
 - Se utiliza para la comunicación de voz.
 - Se utiliza con mayor frecuencia para líneas telefónicas.
- Cable de categoría 5 y 5e
 - Utilizado para la transmisión de datos.
 - Los cables de categoría 5 admiten velocidades de 100 Mbps y pueden admitir velocidades de 1000 Mbps, pero esto no se recomienda.
 - Los cables Cat6 admiten velocidades de 1000 Mbps.
- Cable de categoría 6
 - Utilizado para la transmisión de datos.
 - Cuenta con un separador agregado entre cada par de cables para permitir que funcione a velocidades más elevadas.
 - Admite velocidades desde 1000 Mbps hasta 10 Gbps, aunque esta última no se recomienda.

Redes de Área Local Olga Minguet 35

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Los cables de pares y metálicos

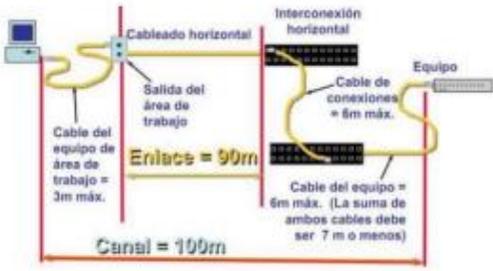


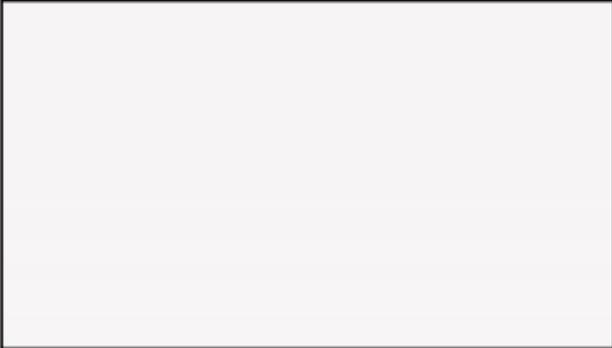
Diagram illustrating network cabling layout constraints:

- Canal = 100m
- Enlace = 90m
- Cableado horizontal
- Interconexión horizontal
- Equipo
- Cable del equipo de área de trabajo = 3m máx.
- Salida del área de trabajo
- Cable de conexiones = 5m máx.
- Cable del equipo = 5m máx. (La suma de ambos cables debe ser 7 m o menos)

Redes de Área Local Olga Minguet 36

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. UTP vs F.O.



Redes de Área Local Olga Minguet 37

UD2. Identificación de elementos y espacios físicos

 Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 6
- Actividad 7

Redes de Área Local Olga Minguet 38

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Cable coaxial

El cable coaxial es otro medio típico de transmisión. Este cable tiene mejor blindaje que el par trenzado, por lo que puede:

- ✓ alcanzar velocidades de transmisión mayores
- ✓ los tramos entre repetidores pueden ser más largos.

La velocidad de transmisión de este cable depende de su longitud: en cables de **1 km** es posible entre **1 y 2 Gbps**.

El cable coaxial consta de:

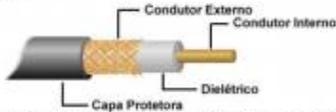
- un alambre de cobre duro en su parte central (vivo) por donde circula la señal,
- un material aislante que rodea a este alambre.
- el aislante está rodeado por un conductor cilíndrico presentado como una malla de cobre trenzado que hace de masa.
- una capa externa de plástico protector.

Redes de Área Local Olga Minguet 39

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Cable coaxial

Esta construcción le confiere un **elevado ancho de banda** y excelente **inmunidad al ruido**.



Está siendo sustituido por la fibra óptica. Sin embargo, el cable coaxial todavía se utiliza para la **televisión por cable** y para acceso a **redes de área extensa (WAN)**.

Se trabajan en dos modalidades:

- ✓ **Coaxial de banda base** (transmisión digital).
- ✓ **Coaxial de banda ancha** (transmisión analógica), comúnmente para TV por cable.

Redes de Área Local Olga Minguet 40

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Cable coaxial

Tipos de cable coaxial en banda base

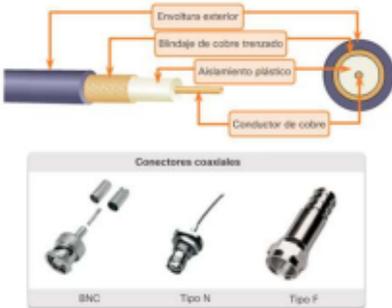
- ✓ **Coaxial grueso:** comenzó a utilizarse en redes locales y hoy en día sólo se emplea para realizar la estructura troncal (principal) de distribución de la red.
- ✓ **Coaxial fino:** dada su flexibilidad es más fácil de instalar, aunque es más caro y posee menor inmunidad frente a interferencias.




Redes de Área Local Olga Minguet 41

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Cable coaxial



Redes de Área Local Olga Minguet 42

UD2. Identificación de elementos y espacios físicos



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- **Actividad 8**

Redes de Área Local Olga Minguet 43

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

La fibra óptica permite la transmisión de **señales luminosas**.

La fibra, que suele ser de **vidrio** u otros **materiales plásticos**. Al no tener metal, es **insensible a interferencias electromagnéticas** externas.

La luz ambiental es una mezcla de señales de muchas frecuencias distintas, por lo que no es una buena fuente de señal portadora luminosa para la transmisión de datos. Son necesarias fuentes especializadas: **fuentes láser y diodos LED**.



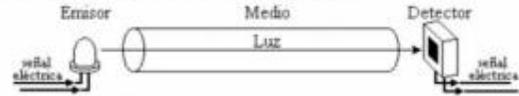
Redes de Área Local Olga Minguet 44

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

Un sistema de transmisión óptico tiene tres componentes:

- ✓ **La fuente de luz:** es un diodo LED o un láser y convierte una señal digital eléctrica (0 y 1) en una señal óptica. Típicamente se utiliza un pulso de luz para representar un "1" y la ausencia de luz para un "0", o se modifica su longitud de onda.
- ✓ **El medio de transmisión:** es una fibra de vidrio ultradelgada que transporta la luz.
- ✓ **El detector:** se encarga de generar un pulso eléctrico en el momento en el que la luz incide sobre él.

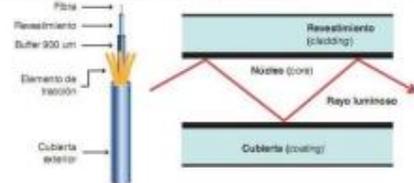


Redes de Área Local Olga Minguet 45

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

El cable de fibra óptica consta básicamente de un núcleo, un revestimiento y una cubierta externa protectora.



El **núcleo** es el conductor de la señal luminosa. La señal es conducida por el interior de este núcleo fibroso, sin poder escapar de él debido a las reflexiones internas y totales que se producen con el **revestimiento**, impidiendo tanto el escape de energía hacia el exterior como la adición de nuevas señales externas indeseadas.

Redes de Área Local Olga Minguet 46

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

Actualmente se utilizan dos tipos de fibras ópticas para la transmisión de datos: fibras monomodo y fibras multimodo.

Fibra monomodo (Single Mode Fiber, SMF)

- ✓ Utiliza un **núcleo estrecho** (menor de 10 micras de diámetro)
- ✓ El núcleo es atravesado por un láser en un único camino, **sin apenas reflexiones** de la luz en las paredes.



Fibra monomodo

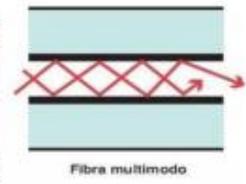
Redes de Área Local Olga Minguet 47

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

Fibra multimodo (Multimode Fiber; MMF)

- ✓ Tiene un **diámetro más grande** (entre las 50 y 115 micras, aunque la más común es la de 62,5 micras), que conduce la luz procedente de **múltiples diodos láser** cada uno con un **ángulo distinto** en la entrada de la fibra.
- ✓ En este caso la luz viaja haciendo **múltiples reflexiones** en las paredes internas de la fibra.



Fibra multimodo

Redes de Área Local Olga Minguet 48

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

Normalmente la fibra óptica se encuentra **instalada en grupos, en forma de mangueras**, con un núcleo metálico que les sirve de **protección y soporte** frente a las tensiones producidas en el cable ya que la fibra, por sí misma, es extraordinariamente frágil.



Redes de Área Local Olga Minguet 49

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

Ventajas e inconvenientes de la fibra

- ↑ Su **throughput**, puede llegar a **100 Gbps** o más. Es posible efectuar transmisiones de decenas de miles de llamadas telefónicas o través de una sola fibra dado su gran ancho de banda.
- ↑ Gran **fiabilidad**, su tasa de error es mínima.
- ↑ Su **peso y diámetro reducido** la hacen ideal frente a los cables de pares o coaxiales.
- ↑ El **ruido** y las emisiones radioeléctricas **NO** le afectan.
- ↑ Se pueden crear segmentos de red de **40 km** o más.
- ↓ Su **instalación** es más **cara** que el cable de cobre.
- ↓ Las **interfaces** de red también son algo más **caras** que sus equivalentes para par trenzado.
- ↓ Gran **dificultad** para realizar una buena conexión de distintas fibras.

Redes de Área Local Olga Minguet 50

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica



Conectores ST

Conectores SC

Conector WSA

Conectores LC multimodo duplex

Redes de Área Local Olga Minguet 51

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

Cables de conexión de fibra comunes



Cable de conexión multimodo SC-SC

Cable de conexión monomodo LC-LC

Cable de conexión multimodo ST-LC

Cable de conexión monomodo SC-ST

Redes de Área Local Olga Minguet 52

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica

Cuestiones de implementación	Cableado UTP	Cableado de fibra óptica
Admitido por ancho de banda	10 Mbps a 10 Gbps	10 Mbps a 100 Gbps
Distancia	Relativamente corta (de 1 a 100 m)	Relativamente alta (1 - 100 000 m)
Inmunidad a EMI y RFI	Baja	Alta (Totalmente inmune)
Inmunidad a peligros eléctricos	Baja	Alta (Totalmente inmune)
Costos de medios y de conectores	Mínimas	Máximas
Se necesitan habilidades de instalación	Mínimas	Máximas
Precauciones de seguridad	Mínimas	Máximas

Redes de Área Local Olga Minguet 53

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica



Redes de Área Local Olga Minguet 54

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas de fibra óptica



Redes de Área Local Olga Minguet 55

UD2. Identificación de elementos y espacios físicos

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- > Actividad 9
- > Actividad 10
- > Actividad 11

Redes de Área Local Olga Minguet 56

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

Las **comunicaciones inalámbricas** consisten en el envío y recepción de **ondas electromagnéticas** que se propagan a la velocidad de la luz.

- ✓ Se utilizan en las **redes de área local** porque es más barato, no son necesarios complejos sistemas de cableado, los puestos de la red se pueden desplazar fácilmente, etc.
- ✓ Para llevar a cabo la transmisión se utiliza un sistema de **antenas** emisoras y receptoras.
- ✓ La propagación por el medio atmosférico produce en ocasiones **problemas de transmisión** debido a los agentes meteorológicos.
- ✓ Su **ancho de banda no es muy alto**.
- ✓ Los **obstáculos** (paredes, suelos, techos, mobiliario, lluvia,...) también **alteran** las comunicaciones inalámbricas, haciendo que las ondas se reflejen, se desvíen de su camino o se dispersen al incidir sobre ellos.

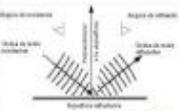
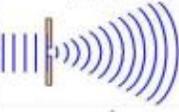


Redes de Área Local Olga Minguet 57

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

Los efectos físicos que pueden alterar las comunicaciones inalámbricas son los siguientes:

Reflexión	Se produce cuando la onda electromagnética se encuentra con un obstáculo reflectante que hace que la señal se refleje en él y produzca interferencia consigo misma.	
Difracción	En este caso la señal divide su camino, lo que hace que se bordeen los obstáculos que se encuentra y haciendo que el destino reciba la misma señal por varios caminos, pero desfasados uno de otro.	
Dispersión	Es la difusión o reflexión de la señal en múltiples y diferentes direcciones sin un control direccional definido.	

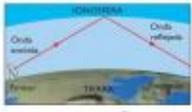
Redes de Área Local Olga Minguet 58

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

La **frecuencia determina** la forma en la que se propaga la onda electromagnética.

- ✓ Si es **inferior a 2 MHz**, la onda viaja por la **superficie**.
- ✓ Si está **entre 2 y 30 MHz**, la onda se transmite hacia arriba, rebotando en la **ionosfera** con lo que se consigue **mayor alcance**.
- ✓ Por encima de los **30 MHz**, la transmisión se realiza por **visión directa** entre emisor y receptor (**satélite**).

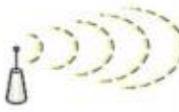

Redes de Área Local Olga Minguet 59

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

Existen dos configuraciones para la emisión y recepción de la energía.

- ✓ **Transmisión direccional**
 Toda la energía se concentra en un haz que es emitido en una **cierta dirección**. Se usa para **altas frecuencias** (microondas o láser).
- ✓ **Transmisión omnidireccional**
 La energía es dispersada en **todas las direcciones**. Se usa para **bajas frecuencias** (ondas de radio y TV)




Redes de Área Local Olga Minguet 60

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

Redes de Área Local Olga Minguet 61

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

ONDAS DE RADIO

- ✓ Son fáciles de generar, pueden recorrer largas distancias, penetran en los edificios sin problemas y viajan en todas direcciones desde la fuente emisora.
- ✓ Funcionan en el espectro entre los 10 kHz y 1 GHz (bajas y medias frecuencias).
- ✓ Las tecnologías que utilizan ondas de radio suelen utilizar antenas omnidireccionales. Este es el caso de la telefonía celular.
- ✓ Cuando estas redes cubren largas distancias, es necesario realizar un control estricto por parte de los gobiernos para que las diferentes transmisiones no se interfieran entre sí. Sin embargo, en señales de radio que cubren distancias más cortas, no es necesario solicitar permisos especiales y varias redes cercanas pueden utilizar frecuencias diferentes.

Redes de Área Local Olga Minguet 62

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

ONDAS DE RADIO

Redes de Área Local Olga Minguet 63

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

MICROONDAS

- ✓ Además de su aplicación en hornos, las microondas permiten transmisiones tanto terrestres como con satélites.
- ✓ Las comunicaciones que utilizan microondas utilizan antenas direccionales, como es el caso de los enlaces punto a punto entre distintas zonas geográficas. Por tanto emisor y receptor deben alinearse de forma muy precisa.
- ✓ Funcionan en la banda de frecuencias de 1GHz a 300 GHz (altas frecuencias). Posibilitan velocidades de transmisión aceptables, del orden de 10 Mbps.
- ✓ A diferencia de las ondas de radio, las microondas NO atraviesan bien los obstáculos. Por tanto, es necesario situar antenas repetidoras para realizar comunicaciones a largas distancias.

Redes de Área Local Olga Minguet 64

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

MICROONDAS

Redes de Área Local Olga Minguet 65

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

ONDAS INFRARROJAS

- ✓ Las ondas infrarrojas y milimétricas se utilizan mucho para la comunicación de corto alcance, en **controles remotos** de televisores, grabadoras de vídeo, estéreos, etc.
- ✓ También era frecuente encontrar un puerto de **comunicación infrarroja** en los ordenadores portátiles.
- ✓ Tienen un inconveniente importante: **no atraviesan los objetos sólidos**.
- ✓ **No puede usarse en exteriores** porque el Sol también emite gran cantidad de radiaciones infrarrojas que perturban la señal enviada.
- ✓ Se encuentran en la banda comprendida entre los 200 GHz y los 400 THz (**muy altas frecuencias**).

Redes de Área Local Olga Minguet 66

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

ONDAS INFRARROJAS

Redes de Área Local Olga Minguet 67

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

ONDAS DE LUZ

- ✓ Las ondas de luz permiten la comunicación de diferentes zonas, siempre que exista una visión directa entre ellas, ya que se transmiten en **línea recta y no atraviesan los objetos**.
- ✓ Una de las señales más utilizadas es el **láser**, ya que el haz de luz se mantiene enfocado en un punto muy estrecho a lo largo de su trayecto.
- ✓ La señalización óptica mediante láser es **unidireccional**, de modo que cada edificio necesita un emisor láser y un receptor.
- ✓ Tiene un **coste muy bajo**, es **fácil de instalar** y posee una **elevada velocidad de transmisión**.
- ✓ El rayo láser es **fácilmente interferido por los agentes climáticos**.

Redes de Área Local Olga Minguet 68

UD2. Identificación de elementos y espacios físicos

2. LOS MEDIOS DE TRANSMISIÓN. Sistemas inalámbricos

ONDAS DE LUZ

Redes de Área Local Olga Minguet 69

UD2. Identificación de elementos y espacios físicos

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 12
- Actividad 13
- Actividad 14

Redes de Área Local Olga Minguet 70

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES

Los cables que forman parte de una red de transmisión de datos no pueden utilizarse si la señal eléctrica no entra en ellos debidamente.

De esta función se ocupan los **conectores**, que no son más que **interfaces** que adecúan la señal del cable a la interfaz del receptor.

Frecuentemente, los conectores de una misma familia se duplican en forma de «macho» o «hembra», que deben acoplarse mecánicamente en la instalación.

En una LAN, los conectores **conectan los cables a las tarjetas de red**.

En el caso de **redes inalámbricas no podemos hablar de conectores** sino de antenas de radiación. En cada extremo de la comunicación debe haber una antena o varias, dependiendo de la tecnología utilizada. Convierten la señal eléctrica de los circuitos electrónicos en ondas de radio.

Redes de Área Local Olga Minguet 71

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Conectores para redes

Algunos de estos conectores se describen a continuación:

- ✓ **RJ11, RJ12, RJ45.** Estos conectores se suelen utilizar con cables UTP, STP y otros **cables de pares**. Al adquirir los conectores se debe especificar la categoría del cable que se pretende utilizar con ellos.
- ✓ **AUI, DB15.** Utilizados en la formación de topologías en estrella con cables de pares, o para la conexión de transeceptores a las estaciones.
- ✓ **BNC.** Se utiliza con cable **coaxial fino**, típico de Ethernet. Mantiene la estructura coaxial del cable en cada conexión.
- ✓ **T coaxial.** Es el modo natural de conectar una estación en un bus de cable coaxial.
- ✓ **DB25 y DB9.** Son conectores utilizados para **transmisiones serie**.

Redes de Área Local Olga Minguet 72

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Conectores para redes

 Cable coaxial	 Cable UTP	 Fibra óptica y su protección
 RJ45	 D825	 D89
 Piezas que componen un conector BNC para cable coaxial y un terminador de 50 W	 Conectores RJ45	 Conectores y latiguillos para fibra óptica

Redes de Área Local Olga Minguet 73

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Conectores para F.O.

ST	se usa en redes de área local de edificios y en sistemas de seguridad
SC	se utiliza para la transmisión de datos en redes de área local
FC	se usa en la transmisión de datos y en las telecomunicaciones
FDDI	se usa para redes WAN de fibra óptica
LC y MT	son utilizados en transmisiones de alta densidad de datos

Los conectores **más comunes** utilizados en instalaciones de fibra óptica para redes de área local (LAN) son los conectores **ST y SC**.

En redes FDDI (WAN) de fibra óptica) suele utilizarse el conector de tipo **FDDI**.

 Conector ST	 Conector SC	 Conector FC
 Conector FDDI	 Conector LC	 Conector MTRJ

Redes de Área Local Olga Minguet 74

UD2. Identificación de elementos y espacios físicos

 Realiza las siguientes **ACTIVIDADES** del Cuaderno de Actividades:

- **Actividad 15**
- **Actividad 16**

Redes de Área Local Olga Minguet 75

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Herramientas

Cuanta **mayor sea la velocidad** de transmisión de las señales de la red tanto mayor será la necesidad de **calidad** en los conectores y las conexiones que conforman.

Antes de su utilización, cada cable construido debe ser **probado** para asegurarse de que cumple con las especificaciones de calidad requeridas en la instalación.

Si no se tiene seguridad en la construcción del cable con sus conectores incluidos, el cable debe rechazarse.

Redes de Área Local Olga Minguet 76

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Herramientas

Las herramientas utilizadas en la construcción de las conexiones del cableado dependerán del tipo de cable y de conector. Toman formas especializadas como alicates, cuchillas y **crimpadoras**. Se pueden adquirir en los comercios especializados por separado o formando parte de kits para cada tipo de cable.



Redes de Área Local Olga Minguet 77

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Componentes

Baluns y transceptores	Son capaces de adaptar la señal pasándola de coaxial a UTP o, en general, a cables de pares, sean o no trenzados. La utilización de este tipo de elementos produce pérdidas de señal ya que deben adaptar la impedancia de un tipo de cable al otro.	 
Rack	Es un armario que recoge de modo ordenado las conexiones de toda o una parte de la red.	

Redes de Área Local Olga Minguet 78

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Componentes

Canaleta	Es una estructura metálica o de plástico, adosada al suelo o a la pared, que alberga en su interior todo el cableado de red, de modo que el acceso a cualquier punto esté más organizado y se eviten deterioros indeseados en los cables.	
Placas de conectores y rosetas	Son conectores que se insertan en las canaletas, o se adosan a la pared y que sirven de interfaz entre el latiguillo que lleva la señal al nodo y el cable de red.	

Redes de Área Local Olga Minguet 79

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Componentes

Macarrón termorretráctil	Se trata de cables huecos contruidos con un material plástico termorretráctil, es decir, que se comprimen por aplicación de calor . Suele instalarse en la unión del cable con el conector para que una vez apretado por efecto del calor, el conector quede más sólidamente sujeto al cable.	
Bridas	Son elementos plásticos que abrochan los cables entre sí o a los armarios y canaletas por donde se instalan de modo que se fije su trayectoria y se impida su movilidad.	

Redes de Área Local Olga Minguet 80

UD2. Identificación de elementos y espacios físicos

3. DISPOSITIVOS DE CONEXIÓN DE CABLES. Componentes

Etiquetas identificativas	Constituyen un sistema de información que se adjunta a cada cable para tenerlo identificado en todo momento.	
Otro tipo de herramientas	Como destornilladores, pelacables, tijeras, punzones, cuchillas, pinzas, resinas, cinta aislante, etc.	

Redes de Área Local Olga Minguet 81

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. El proyecto de instalación

La instalación consiste en la **ejecución ordenada**, según las directrices del proyecto de instalación de un conjunto de tareas que revierten en proporcionar el servicio que necesitaba el cliente que solicitó la instalación. Algunas de estas tareas son:

- ✓ **Instalación de las tomas de corriente.** Esta tarea suele realizarla un electricista. Debemos asegurarnos de que hay suficientes tomas de corriente para alimentar todos los equipos de comunicaciones.
- ✓ **Instalación de rosetas y jacks.** Es la instalación de los puntos de red finales desde los que se conectarán los equipos de comunicaciones sirviéndose de latiguillos. La mayor parte de estas conexiones residirán en canaletas o en armarios de cableado.
- ✓ **Tendido de los cables.** Se trata de medir la distancia que debe recorrer cada cable y añadirle una longitud prudente que nos permita trabajar cómodamente con él antes de cortarlo. Debemos asegurarnos de que el cable tenga la certificación necesaria.

Redes de Área Local Olga Minguet 82

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. El proyecto de instalación

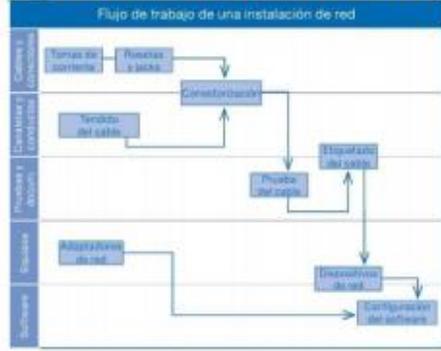
- ✓ **Conectorización de los cables** en los patch panels y en las rosetas utilizando las herramientas de crimpado apropiadas. A esto se le denomina cross-connect.
- ✓ **Probado de los cables instalados.** Cada cable construido y conectorizado debe ser inmediatamente probado para asegurarse de que cumplirá correctamente su función.
- ✓ **Etiquetado y documentación del cable y conectores.** Todo cable debe ser etiquetado en ambos extremos, así como los conectores de patch-panels y rosetas, quedando identificados unívocamente.
- ✓ **Instalación de los adaptadores de red.** Los equipos informáticos no siempre vienen ya con la tarjeta de red instalada.
- ✓ **Instalación de los dispositivos de red.** Se trata de instalar y configurar los concentradores, conmutadores, puentes y encaminadores.
- ✓ **Configuración del software** de red en clientes y servidores

Redes de Área Local Olga Minguet 83

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. El proyecto de instalación

Flujo de trabajo de una instalación de red



Redes de Área Local Olga Minguet 84

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de la instalación

A. Armarios

En instalaciones de tamaño mediano o grande, los equipos de comunicaciones se instalan en **armarios especiales** que tienen unas **dimensiones estandarizadas** y en los que es fácil su manipulación y la fijación de los cables que a ellos se conectan.

Dentro de estos armarios o racks se instalan bandejas de soporte o patch panels para la conexión de jacks o de otro tipo de conectores.

Redes de Área Local Olga Minguet 85

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de la instalación

A. Armarios

- ✓ La **anchura** de los racks está normalizada a **19 pulgadas**
- ✓ La **altura** de los armarios suele medirse en «U».
- ✓ Una «U»: es la medida estandarizada de las bandejas de un rack o armario. Es la abreviatura de **Rack Unit**.
- ✓ Una «U» equivale a una altura de 1,75 pulgadas (44,45 mm).
- ✓ Por ejemplo, el armario de la imagen anterior medía 42 «U».
- ✓ Los fabricantes de dispositivos suelen ajustar sus equipos para que se puedan ensamblar en estos armarios ocupando 1,2 o más «U».
- ✓ La mayoría de los racks que hay los centros de procesos de datos tienen una altura de **42 U** (aproximadamente **1,8 metros**).
- ✓ En cada «U» se incluyen en las paredes del rack tres tornillos de fijación.

Redes de Área Local Olga Minguet 86

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de la instalación

A. Armarios

Redes de Área Local Olga Minguet 87

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de la instalación

B. Canaletas

- ✓ Las canaletas son los conductos a través de los cuales se tienden los cables para que queden recogidos y protegidos convenientemente.
- ✓ Hay canaletas decorativas, de aspecto más acabado cuya misión es ocultar los cables, y canaletas acanaladas que suelen instalarse en los falsos techos o falsos suelos y que son suficientemente grandes como para llevar muchos cables.
- ✓ Las canalizaciones de datos y de fuerza suelen estar separadas para evitar interferencias.

Redes de Área Local Olga Minguet 88

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de la instalación

C. Suelos y techos técnicos

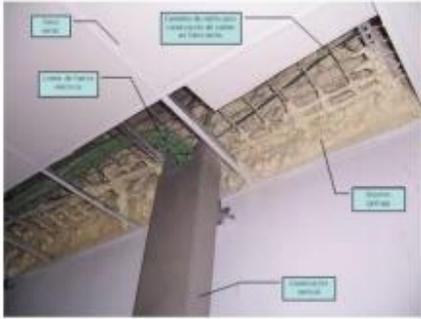
- ✓ Las canalizaciones tendidas por **falsos suelos y techos técnicos** mejoran la limpieza de la instalación haciéndola además mucho más estética.
- ✓ En el diseño hay que cuidar que no estorben al paso y que queden protegidas para evitar su deterioro.
- ✓ Los cables llegan a los armarios a través de los falsos suelos justo **por debajo de ellos**, lo que ayuda a la limpieza de la instalación.
- ✓ Los distintos cables avanzan normalmente embridados hasta ser conectados en algún dispositivo o en algún **patch panel**.



Redes de Área Local Olga Minguet 89

UD2. Identificación de elementos y espacios físicos

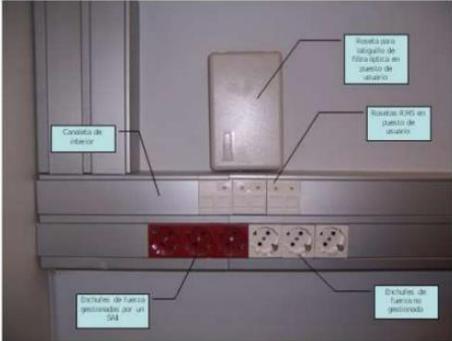
4. EL CABLEADO DE LA RED. Elementos de la instalación



Redes de Área Local Olga Minguet 90

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de la instalación



Redes de Área Local Olga Minguet 91

UD2. Identificación de elementos y espacios físicos

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

➤ Actividad 17

Redes de Área Local Olga Minguet 92

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. La instalación eléctrica y de a.a.

Es muy importante que la instalación eléctrica esté muy bien hecha para evitar **riesgos importantes, incluso de electrocución**. Los problemas eléctricos suelen ser muy difíciles de diagnosticar y provocan deterioros importantes en los dispositivos de red.

Todos los dispositivos de red deben estar conectados a **enchufes con tierra**.

Las carcasas de estos dispositivos, los armarios, las canaletas mecánicas, etc., también deben ser conectados a tierra.

Toda la instalación de la red debe estar a su vez conectada a la tierra del edificio.



Redes de Área Local Olga Minguet 93

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. La instalación eléctrica y de a.a.

Otra necesidad muy importante en una instalación informática es el **control de la temperatura y la humedad** del ambiente en que se sitúan los ordenadores y otros dispositivos de red. La regulación de estos parámetros se realiza mediante la instalación de **aire acondicionado**.

Esto reviste una **especial importancia en los Centros de Procesos de Datos (CPD)**.



Redes de Área Local Olga Minguet 94

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. La instalación eléctrica y de a.a.

Otro problema importante que hay que resolver viene originado por los **cortes de corriente o las subidas y bajadas de tensión**. Para ello podemos utilizar Sistemas de Alimentación Ininterrumpida (**SAI**), que actúan de estabilizadores, garantizan el fluido frente a cortes de corriente, proporcionan el flujo eléctrico adecuado, etc.

El SAI contiene en su interior unos acumuladores que se cargan en el régimen normal de funcionamiento. En caso de corte de corriente, los acumuladores producen la energía eléctrica que que tuvieran abiertos las aplicaciones de los **permite guardar los datos** usuarios y **cerrar ordenadamente los sistemas operativos**.

Los servidores pueden comunicarse con un SAI a través de alguno de sus **puertos de comunicaciones**, de modo que el SAI informa al servidor de las incidencias que observa en la corriente eléctrica.



Redes de Área Local Olga Minguet 95

UD2. Identificación de elementos y espacios físicos

 Realiza las siguientes **ACTIVIDADES** del Cuaderno de Actividades:

➤ **Actividad 18**

Redes de Área Local Olga Minguet 96

UD2. Identificación de elementos y espacios físicos

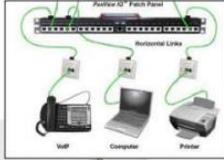
4. EL CABLEADO DE LA RED. Elementos de conectividad

A. Patch panels y latiguillos

Un patch panel es un **dispositivo de interconexión** a través del cual los cables instalados se pueden conectar a otros dispositivos de red o a otros patch panels.

Sobre un armario se instalan patch panels que se conectan al cableado de la instalación por todo el edificio y otros patch panels que se conectan a los conectores de los dispositivos de red.

El cable largo instalado conectará las rosetas con los patch panels.



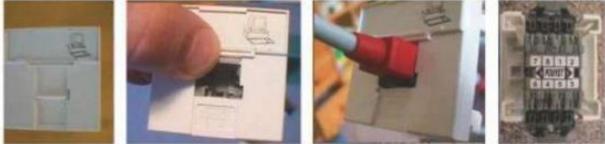

Redes de Área Local Olga Minguet 97

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de conectividad

B. Conexiones a rosetas RJ45

La roseta presenta un conector por un lado y una estructura de fijación de los cables de pares por su reverso, a la que serán crimpados.



En redes de área local sobre cables UTP deben utilizarse **conectores y rosetas RJ45**. De los cuatro pares del cable UTP, la red solo utilizará dos de ellos. Los otros dos pueden utilizarse para telefonía o alguna otra aplicación de telecomunicaciones.

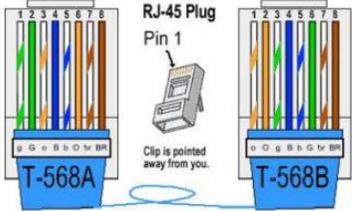
Redes de Área Local Olga Minguet 98

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de conectividad

C. Confección de latiguillos RJ45

Quando se quieren **conectar dos ordenadores directamente** por sus tarjetas de red sin ningún dispositivo intermedio se tiene que utilizar un **cable cruzado**, que altera el orden de los pares para que lo que es recepción en un extremo sea emisión en el otro y viceversa.



Redes de Área Local Olga Minguet 101

UD2. Identificación de elementos y espacios físicos

4. EL CABLEADO DE LA RED. Elementos de conectividad

D. Etiquetado de los cables

La norma EIA/TIA-606 especifica que cada terminación de hardware debe tener alguna etiqueta que lo identifique de manera exclusiva. Un **cable** tiene dos terminadores, por tanto **cada uno de estos extremos recibirá un nombre**.

Para los **dispositivos** es recomendable **nomenclaturas neutras independientemente de su ubicación**: por ejemplo, si se etiqueta un PC como «PC», y luego el lugar del edificio en donde se ubica, si cambiamos el ordenador de sitio, tendríamos que cambiar también el etiquetado. Por ello se debe intentar que el etiquetado sea fijo.

Para los **cables** se recomienda la utilización de etiquetas que incluyan **un identificador de sala y un identificador de conector**, así sabremos todo sobre el cable: dónde empieza y dónde acaba.

Redes de Área Local Olga Minguet 102

UD2. Identificación de elementos y espacios físicos

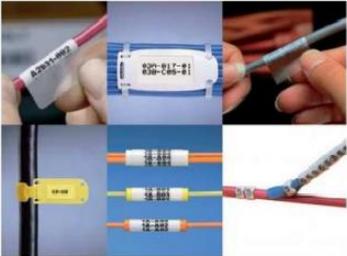
4. EL CABLEADO DE LA RED. Elementos de conectividad

D. Etiquetado de los cables

Como vemos en la imagen, podríamos **etiquetar un cable** con el siguiente identificador: **03RS02-05RS24**.

Este cable indicaría que está tendido desde la roseta (RS) número 02 de la sala 03 hasta la roseta 24 de la sala 05.

Las rosetas en las salas 03 y 05 irían etiquetadas con 03RS02 y 05RS24 respectivamente.



Redes de Área Local Olga Minguet 103

UD2. Identificación de elementos y espacios físicos

Realiza las siguientes **ACTIVIDADES** del Cuaderno de Actividades:

➤ **Actividad 19**

Redes de Área Local Olga Minguet 104

UD2. Identificación de elementos y espacios físicos

4. CABLEADO ESTRUCTURADO Y CERTIFICADO. Estructuración del cable

Un sistema de cableado bien diseñado debe tener al menos estas dos cualidades: **seguridad y flexibilidad**.

- Seguridad significa que debe ser fiable y no provocar fallos.
- Flexibilidad significa que debe ser capaz de adaptarse fácilmente a los cambios que se hagan en la red.

La estructuración del cable se consigue construyendo **módulos independientes que segmenten la red completa en subsistemas de red**, independientes pero integrados, de forma que un subsistema queda limitado por el siguiente subsistema.

Estos subsistemas siguen una **organización jerarquizada por niveles** desde el sistema principal hasta el último de los subsistemas.

Redes de Área Local Olga Minguet 105

UD2. Identificación de elementos y espacios físicos

4. CABLEADO ESTRUCTURADO Y CERTIFICADO. Estructuración del cable

Localización de cada puesto de trabajo	A cada puesto deben poder llegar todos los posibles medios de transmisión de la señal que requiera cada equipamiento: Wireless, UTP, fibra óptica, baluns, etc
Subsistema horizontal o de planta	Es recomendable la instalación de una canaleta o un subsuelo por el que llevar los sistemas de cableado a cada puesto.
Subsistema distribuidor o administrador	Incluye los racks, los distribuidores de red con sus latiguillos, etc
Subsistema vertical o backbone	Encargado de comunicar todos los subsistemas horizontales, por lo que requiere de medios de transmisión de señal con un ancho de banda elevado y de elevada protección
Subsistema de campus	Extiende la red de área local al entorno de varios edificios
Cuartos de entrada de servicios	Son los lugares apropiados para recoger las entradas de los servicios externos a la organización, la instalación de la maquinaria de comunicaciones y para los equipamientos informáticos centralizados

Redes de Área Local Olga Minguet 106

UD2. Identificación de elementos y espacios físicos

4. CABLEADO ESTRUCTURADO Y CERTIFICADO. Estructuración del cable

1 Equipo de usuario
2 Roseta
3 Cableado horizontal de planta
4 Cuarto de comunicaciones o distribuidor de planta
5 Cableado vertical

Planta n + 1
Planta n
BACCIONES VERTICALES
Subsistemas horizontales

Redes de Área Local Olga Minguet 107

UD2. Identificación de elementos y espacios físicos

4. CABLEADO ESTRUCTURADO Y CERTIFICADO. Certificación de la instalación

El correcto funcionamiento del sistema de cableado es tan importante que en muchas instalaciones se exige la certificación de cada cable.

La **certificación** de una instalación significa que todos los cables que la componen **cumplen con esos patrones de referencia** y, por tanto, se tiene la garantía de que cumplirán con las exigencias para las que fueron diseñados.

La organización internacional TIA/EIA contempla un conjunto de estándares para el cableado estructurado.

Estándar	Descripción
EIA-568-B.1	Estándar con requisitos generales para el cableado de telecomunicaciones en edificios comerciales.
EIA-568-B.2	Componentes de cableado de par trenzado.
EIA-568-B.3	Componentes de cableado de fibra óptica.
EIA-568-B	Estándares de cableado.
EIA-569-A	Estándares sobre recorridos y espacios de telecomunicaciones para edificios comerciales.
EIA-570-A	Estándar para el cableado de comunicaciones en zonas residenciales y pequeño comercio.
EIA-606	Estándar de administración de la infraestructura de telecomunicaciones en edificios comerciales.
EIA-607	Especificación de requisitos de conexión a tierra.

Redes de Área Local Olga Minguet 108

UD2. Identificación de elementos y espacios físicos

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 20
- Actividad 21

Redes de Área Local Olga Minguet 109

UD2. Identificación de elementos y espacios físicos

4. INSTALACIÓN DEL CPD.

Un **CPD** es un edificio o sala de gran tamaño usada para mantener en él una **gran cantidad de equipamiento electrónico**. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Por ejemplo, un banco puede tener un centro de procesamiento de datos con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el **garantizar la continuidad del servicio** a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como **servidores** de bases de datos que puedan contener información crítica.

Redes de Área Local Olga Minguet 110

UD2. Identificación de elementos y espacios físicos

4. INSTALACIÓN DEL CPD.

En el Centro de Proceso de Datos (CPD) es muy importante cuidar la **accesibilidad a los equipos** de modo que se pueda actuar rápidamente en caso de cualquier avería.

Los lugares en los que se instalan servidores o que contienen puntos neurálgicos de las comunicaciones deben ser lugares **cerrados bajo llave**: frecuentemente el acceso a estos lugares es restringido y se realiza bajo la supervisión de algún sistema de control de presencia con tarjetas de bandas magnéticas, reconocimiento biométrico u otros sistemas de identificación seguros.



Redes de Área Local Olga Minguet 111

UD2. Identificación de elementos y espacios físicos

4. INSTALACIÓN DEL CPD.

Entre los factores que hay que tener en cuenta para este diseño están los siguientes:

- ✓ **Aire acondicionado redundante.**
- ✓ **Doble acometida eléctrica:** si fuera posible, de varias compañías suministradoras distintas.
- ✓ **Redundancia en las comunicaciones con el exterior:** cables de red, fibras ópticas, telefonía, etc. Si es posible, también de diferentes compañías.
- ✓ **Montacargas, altura y anchura de puertas suficiente** para introducir las máquinas que alojará el CPD.
- ✓ **Seguridad de acceso controlada por puntos de presencia.** Vigilancia. Alarmas. Seguridad contra incendios.
- ✓ **Control de parámetros medioambientales:** temperatura y humedad.
- ✓ **Cuadros de distribución eléctrica independientes y seguros.**
- ✓ **Falsos suelos y techos.**
- ✓ **SAI y generadores de corriente.**

Redes de Área Local Olga Minguet 112

UD2. Identificación de elementos y espacios físicos

4. INSTALACIÓN DEL CPD.

- ✓ En la página <http://platea.pntic.mec.es/~lmar2/cableado.htm> para ampliar conocimientos sobre las condiciones de instalación de los cuartos de comunicaciones.
- ✓ En la dirección http://www.ngsoft.es/cable_estruc.htm tienes un buen resumen de las tecnologías implicadas en la estructuración del cable.
- ✓ En la web http://guimi.net/monograficos/G-Cableado_estructurado/G-Cableado_estructurado.pdf tienes información sobre cableado estructurado: cableado horizontal, backbone vertical y cableado de campus.

Redes de Área Local Olga Minguet 113

UD2. Identificación de elementos y espacios físicos



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- **Actividad 22**

Redes de Área Local Olga Minguet 114

8.2.2 Cuaderno de actividades

Cuaderno de Actividades

- UNIDAD 2-

Identificación de elementos y espacios físicos de una red local. Medios de transmisión.

CUADERNO DE ACTIVIDADES

Objetivos

- Consolidar los contenidos vistos en la Unidad 2 del curso de Redes de Área Local.
- Aprender los diferentes medios de transmisión de señales, en un nivel teórico.
- Identificar los diferentes elementos que componen una instalación de red.
- Conocer el sistema de cableado estructurado.

Actividades

1. Indica el valor numérico de las siguientes magnitudes.

Magnitud	Valor numérico
20,6 KHz	
0,42 GHz	
400,3 MHz	
0,057 TByte	
7050 Mbyte	
0,001 KHz	

- Indica la magnitud más adecuada para los siguientes valores numéricos

CUADERNO DE ACTIVIDADES

Valor numérico	Magnitud
234.440.000 Hz	
0,0001 GHz	
0,0543 MHz	
654.000 Mbyte	
0,0045 GHz	
44.003.000 Hz	

2. Asocia a cada situación la característica adecuada de una señal (amplitud, frecuencia y fase).

	Característica
La señal ha llegado con un retardo de 0,01 segundos	
El conector admite una señal máxima de 5 voltios	
Es capaz de procesar 4000 bits en un segundo	

3. Busca por internet las definiciones de banda base y banda ancha y dos ejemplos de uso de cada una de ellas.

Banda base. Definición

UD02 – Identificación de elementos y espacios físicos de una red local 3-15

CUADERNO DE ACTIVIDADES

Banda base. Dos ejemplos de uso

Banda ancha. Definición

Banda ancha. Dos ejemplos de uso

Incluye los links donde has encontrado la información.

4. Haz una tabla donde en las filas estén los medios de transmisión siguientes: (Onda aérea, cable cobre y fibra óptica) y en las columnas cada una de las 4 perturbaciones que hemos visto. Identifica cada medio de transmisión porque perturbación se ven afectados.

UD02 – Identificación de elementos y espacios físicos de una red local 4-15

CUADERNO DE ACTIVIDADES

	Cable de cobre	Fibra óptica	Onda aérea
Atenuación			
Interferencia electromagnética			
Diafonía			
Dispersión			

5. Busca por internet la definición de ancho de banda.

Busca también información de tres proveedores de servicios de internet que oferten fibra óptica, ADSL y Datos Móviles. Indica qué velocidades máximas ofrecen y a qué precio

Proveedor 1			
	ADSL	Fibra Óptica	Datos Móviles
Velocidades máximas			
Precios			

Proveedor 2			
	ADSL	Fibra Óptica	Datos Móviles
Velocidades máximas			
Precios			

CUADERNO DE ACTIVIDADES

Proveedor 3			
	ADSL	Fibra Óptica	Datos Móviles
Velocidades máximas			
Precios			

6. ¿Cuándo utilizarías cables de pares UTP y cuándo STP?

Cables de pares UTP

Cables de pares STP

7. Elabora una tabla comparativa sobre los cables UTP y STP en la que se indiquen en una columna tres ventajas y en otra columna tres inconvenientes de cada uno de usar STP respecto a UTP.

	VENTAJAS	INCONVENIENTES
STP respecto a UTP		

CUADERNO DE ACTIVIDADES

8. ¿Cuáles son las dos modalidades en las que se trabaja con cable coaxial? Para cada una indica:

- Transmisión señal original o modulación.
- Único canal o multicanal
- Ancho de banda y longitud máxima segmentos

Modalidad 1:

Original o modulación	Monocanal /multicanal	Ancho de banda	Longitud máxima segmentos

Modalidad 2:

Original o modulación	Monocanal /multicanal	Ancho de banda	Longitud máxima segmentos

9. Di tres ventajas y tres inconvenientes que tendría sustituir el cable STP por fibra óptica

CUADERNO DE ACTIVIDADES

VENTAJAS	INCONVENIENTES

10. ¿Qué modos de propagación se utilizan para conducir la señal luminosa en el núcleo de una fibra óptica? Explica en qué consiste cada uno de ellos

Modos de propagación

Modo 1

Modo 2

11. Elabora una tabla con los medios de transmisión guiados que hemos visto: pares de cable, coaxial, fibra óptica. Para cada uno indica tres ventajas e inconvenientes

CUADERNO DE ACTIVIDADES

	VENTAJAS	INCONVENIENTES
Par de cobre		
Coaxial		
Fibra óptica		

12. Enumera dos elementos positivos y dos negativos de utilizar sistemas inalámbricos para las comunicaciones en redes de ordenadores.

POSITIVOS	NEGATIVOS

13. Describe los tres factores (reflexión, difracción y dispersión) que generan problemas en la radiación de las señales inalámbricas.

Reflexión

CUADERNO DE ACTIVIDADES

Difracción

Dispersión

14. Elabora una tabla con los medios inalámbricos que hemos visto: ondas de radio, microondas, infrarrojos y luz. Para cada una de ellas indica:

- Rangos de frecuencia en el que operan
- Velocidades de transmisión
- Si es omnidireccional o direccional
- 2 Ventajas
- 2 Inconvenientes

	Rango	Velocidades	O/D	2 Ventajas	2 Inconvenientes
Onda de radio				• •	• •
Microondas				• •	• •
Infrarrojo				• •	• •
Laser				• •	• •

15. ¿Cuáles son los dos conectores más utilizados en las instalaciones de red con fibra óptica? ¿Qué características mecánicas tiene cada uno de ellos? Indica las webs donde has encontrado la información.

Los dos conectores más usados

CUADERNO DE ACTIVIDADES

Conector 1

Conector 2

Direcciones web

16. ¿Qué conector corresponde a qué tipo de cable?

Conector	Tipo de cable
RJ45	
RJ11	
ST	
BNC	

17. ¿Qué es una «U» en un armario de comunicaciones?

CUADERNO DE ACTIVIDADES

18. ¿Indica 5 precauciones básicas que debe tomar el instalador de redes para evitar accidentes laborales?

Protección 1	
Protección 2	
Protección 3	
Protección 4	
Protección 5	

19. ¿Cuál es el código de colores para la conectorización de un conector RJ45 según la norma T568B?

Para un cable no cruzado:

Contacto	Color (T568B)
1	
2	
3	
4	
5	
6	
7	
8	

Para un cable cruzado:

Contacto	Color (T568B)
1	
2	
3	
4	
5	
6	
7	

CUADERNO DE ACTIVIDADES

8

20. Declara como verdaderas o falsas las afirmaciones siguientes. Razona la respuesta.

a. El cableado vertical o de *backbone* siempre se tiende desde las plantas superiores a las inferiores o viceversa.

Verdadero/Falso	Justificación

b. El subsistema de campus siempre se corresponde con una red MAN.

Verdadero/Falso	Justificación

c. Los latiguillos de red pertenecen al cableado estructurado.

Verdadero/Falso	Justificación

d. Los armarios de comunicaciones no pertenecen al cableado estructurado.

Verdadero/Falso	Justificación

e. Un cable UTP no puede superar los 100 metros de extremos a extremo.

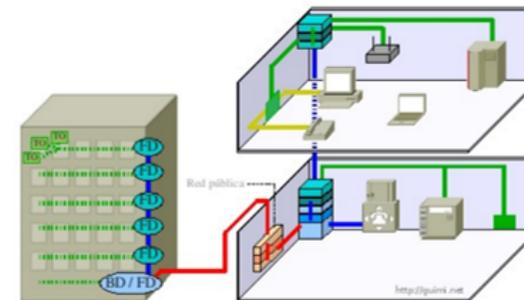
Verdadero/Falso	Justificación

f. La máxima distancia permitida para un cable UTP es de 90 m sin contar los latiguillos de conexión en los extremos.

CUADERNO DE ACTIVIDADES

Verdadero/Falso	Justificación

21. Dada la configuración de red la imagen



Responde a las siguientes cuestiones:

• ¿Qué elementos conectarías con cableado horizontal?

• ¿Qué elementos conectarías con el cableado vertical de edificio (backbone vertical)?

• ¿Qué elementos conectarías con el cableado vertical de campus (backbone de campus)?

CUADERNO DE ACTIVIDADES

--

22. Declara como verdaderas o falsas las afirmaciones siguientes:

a. El acceso al CPD debe ser siempre restringido.

Verdadero/Falso	Justificación

b. Deben certificarse todos los cables tendidos, pero no los latiguillos de red.

Verdadero/Falso	Justificación

c. El aire acondicionado de un CPD debe ser redundante.

Verdadero/Falso	Justificación

d. Es importante que el CPD se mantenga a una temperatura baja, pero no importa la humedad.

Verdadero/Falso	Justificación

e. Los cables deben llegar al CPD por falso suelo o por falso techo.

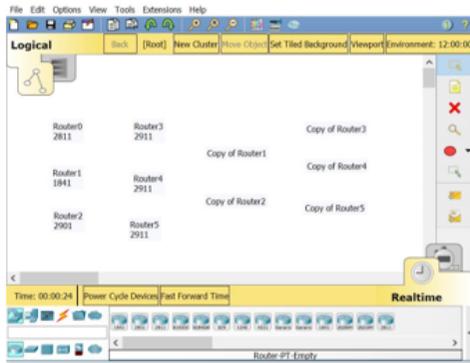
Verdadero/Falso	Justificación

f. Los equipos del CPD deben estar protegidos contra subidas de tensión.

Verdadero/Falso	Justificación

8.2.3 Cuaderno de prácticas

UD02 Medios de transmisión	PRÁCTICAS
Cuaderno de PRÁCTICAS 1: Iniciación a Packet Tracer	
Nombre y apellidos	<input style="width: 80%;" type="text"/>
Breve descripción	En este Cuaderno de prácticas vamos a introducirnos en el mundo de la simulación de redes de la mano del conocido programa de simulación de CISCO.
Material necesario	<ul style="list-style-type: none"> Cuaderno de trabajo Bolígrafo y/o lápiz 1 PC con Packet Tracer
Fuentes de información	<ul style="list-style-type: none"> Diapositivas de la Unidad 2 Explicaciones de clase
Desarrollo	
<ul style="list-style-type: none"> ✓ PRÁCTICA 1: Introducción a PKT. ✓ PRÁCTICA 2: Creando y cableando dispositivos en PKT. ✓ PRÁCTICA 3: Configurando dispositivos. ✓ PRÁCTICA 4: Creación de una red sencilla. 	
Página 1	

UD02 Medios de transmisión	PRÁCTICAS
Práctica 1	
<i>Introducción a Packet Tracer</i>	
<p>Paso 1: Abra el archivo Deploying DevicesPacket Tracer.</p> <p>Haga doble clic en el Deploying Devices.pkt archivo para abrirlo. Debería aparecer una pantalla similar a la que se muestra en la figura. Si el archivo no se abre, asegúrese de haber instalado correctamente el programa de aplicación Packet Tracer.</p>	
	
<p>Paso 2: Aprenda a implementar dispositivos en Packet Tracer.</p> <p>Una lista de etiquetas de dispositivos está visible en el espacio de trabajo, utilizaremos varios métodos para implementar los dispositivos enumerados.</p> <p>A) Primero ubique el enrutador 2811 en el Cuadro de selección específico del dispositivo que se muestra a continuación.</p>	
	
Página 2	

- B) Con el mouse, haga clic en el enrutador 2811 y mientras mantiene presionado el botón del mouse, arrastre el enrutador sobre el Enrutador 0, luego suelte.
- C) Ahora haga clic en el enrutador 1841 en el cuadro de selección específico del dispositivo y luego haga clic en la etiqueta Enrutador1 en el espacio de trabajo.
- D) Utilice cualquiera de los métodos de los puntos A o B para colocar un enrutador 2901 en el espacio de trabajo sobre el Enrutador2 etiqueta.

Consejo n.º 1

Si desea colocar varios dispositivos del mismo tipo en el espacio de trabajo, hacer clic y arrastrar puede resultar muy tedioso. Para evitar esto, mantenga presionada la tecla <CTRL> mientras hace clic en el dispositivo en el Cuadro de selección específico del dispositivo.

- E) Mantenga presionada la tecla <CTRL> y haga clic en el enrutador 2911 en el cuadro de selección específico del dispositivo. Ahora haga clic en las etiquetas Enrutador3, Enrutador4 y Enrutador5. Para cancelar la operación, haga clic en el símbolo  Cancelar donde

estaba el enrutador 2911 en el Cuadro de selección específico del dispositivo.

Consejo n.º 2

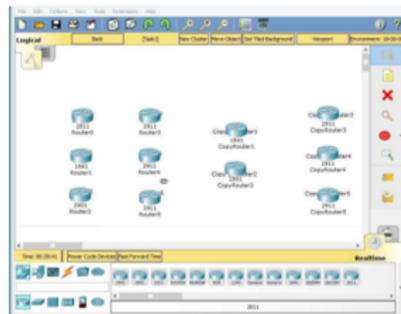
El usuario también puede copiar dispositivos en el espacio de trabajo de dos formas.

- F) Método n.º 1: arrastre el cursor sobre los dispositivos que desea copiar. Arrastra un cuadro sobre Enrutador3, 4 y 5, deberían aparecer descoloridos. Mantenga presionada la tecla <CTRL> y arrastre Enrutador3 sobre la etiqueta Copia de Router3.

- G) Método # 2: Mantenga presionada la tecla <MAYUS> y haga clic en los dispositivos que se copiarán. Seleccione Enrutador1 y Enrutador2 (haga clic en Enrutador1 y Enrutador2 mientras mantiene presionada la tecla <SHIFT>), volverán a tener un aspecto desvaído.

Apuntar a Enrutador1, mantenga presionada la tecla <CTRL> y arrastre los dispositivos sobre la etiqueta Copia de Router1 y suelte.

Su pantalla debe verse como la imagen a continuación si ha implementado los dispositivos correctamente. Si el archivo no parece correcto, vuelva a cargarlo y comience de nuevo.



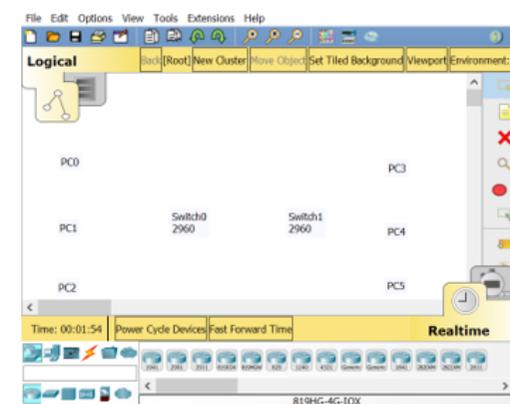
Si la imagen es correcta, entonces guárdelo y entréguelo.

Práctica 2

Creando y cableando dispositivos en PKT

Paso 1: Abra el archivo de implementación y cableado de dispositivos de Packet Tracer.

Haga doble clic en el archivo Deploying and Cabling Devices.pkt para abrirlo. Debe aparecer una pantalla similar a la que se muestra en la figura. Si el archivo no se abre, asegúrese de haber instalado correctamente el programa Packet Tracer.



Paso 2: Aprenda a implementar dispositivos y realizar el cableado en Packet Tracer.

1. La primera tarea en esta actividad es realizar ejercicios de uso del cuadro de selección de tipo de dispositivo.



UDO2 Medios de transmisión

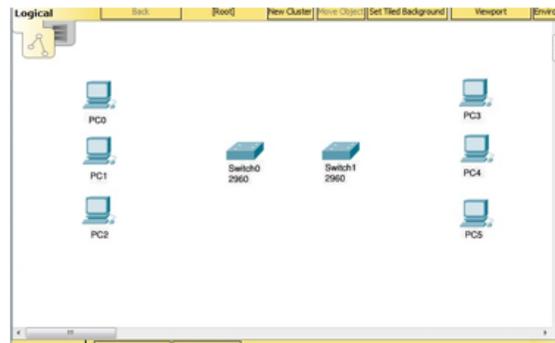
PRÁCTICAS

La fila superior de iconos representa las categorías de dispositivos y la fila inferior representa las subcategorías. Coloque el cursor sobre la fila superior de iconos lentamente y mire el cuadro de etiqueta entre las filas; aparecen los nombres de las categorías. Ahora coloque el cursor sobre la fila inferior de iconos y verá sus nombres.

En esta actividad, debe implementar switches y PC. Coloque el cursor sobre los iconos de la fila inferior hasta que vea una etiquetada con la palabra Switches. Haga clic en ese icono, y verá que los dispositivos que figuran en el cuadro de selección de dispositivos específicos cambian.



Ahora se muestran los switches disponibles en Packet Tracer. Implemente dos switches 2960 (si no recuerda cómo hacerlo, revise la actividad anterior) en las etiquetas Switch0 y Switch1 en el espacio de trabajo. Ahora, haga clic en la categoría End Device (Dispositivo Final) en el cuadro de selección de tipo de dispositivo, e implemente seis PCs. Si no está seguro de qué dispositivo es el punto específico de la PC en el dispositivo que figura en el cuadro de selección de dispositivos específicos, observe el área de etiqueta debajo de los dispositivos: debe decir PC-PI (recuerde que no tiene que seleccionar el icono de PC seis veces para implementarlas; hay un acceso directo). El espacio de trabajo debe parecerse a este.



Ahora vamos a conectar las PC a los switches.

UDO2 Medios de transmisión

PRÁCTICAS

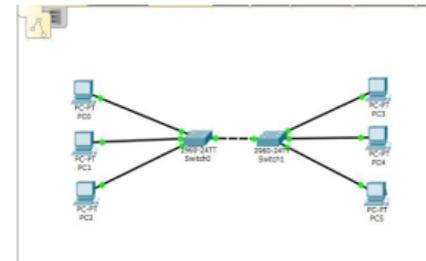
Haga clic en la categoría que tiene un aspecto similar a un rayo, etiquetada con el término Connections (Conexiones). En el cuadro de selección de dispositivos específicos, se muestra una serie de tipos de cable; seleccione el tipo Copper Straight-Through cable (Cable de cobre de conexión directa). Ahora, coloque el cursor en el centro de PC0 y haga clic en esta opción. Aparece un menú emergente que muestra los tipos de conexión de cables. Coloque el cursor sobre el menú, y haga clic en la selección FastEthernet0. Ahora se muestra un cable conectado a la PC. Coloque el cursor sobre Switch0, y haga clic en esta opción. Aparece otro menú emergente con un conjunto de selecciones mucho más grande; coloque el cursor sobre el menú, y haga clic en la selección FastEthernet0/1. Ahora el cable se ve conectado y aparecen dos luces de enlace parpadeantes: una verde y una ámbar. Después de un tiempo, la luz ámbar cambia a color verde por motivos que comprenderá a medida que aprenda sobre redes. Ahora realicemos el cableado de las seis PC con los switches.

Puede seleccionar el cable cada vez, o bien utilice la tecla <CTRL> al igual que en la primera actividad. Este es el conjunto de conexiones que se deben realizar.

- PC1 FastEthernet0 al Switch0 FastEthernet0/2
 - PC2 FastEthernet0 al Switch0 FastEthernet0/3
 - PC3 FastEthernet0 al Switch1 FastEthernet0/1
 - PC4 FastEthernet0 al Switch1 FastEthernet0/2
 - PC5 FastEthernet0 al Switch1 FastEthernet0/3
- Si utilizó la tecla <CTRL> para hacer varias copias, cancele el uso haciendo clic en el indicador de cancelar .

Ahora bien, necesitamos otro tipo de cable para conectar los dos switches.

Seleccione Copper Cross-Over cable (Cable de cobre de conexión cruzada). Haga clic en esta opción, y luego coloque el cursor y haga clic en Switch0. En el menú emergente, seleccione la interfaz Gigabit0/1 que está casi al final de la lista. Luego, coloque el cursor y haga clic en Switch1, y seleccione la misma interfaz de esta lista. Aparece el cable, y ambas luces de enlace son de color ámbar, pero, en alrededor de un minuto, cambiarán a color verde. La actividad completa debe parecerse a lo siguiente.



Si el espacio de trabajo se parece a la imagen anterior, guarda el archivo y entrégalo.

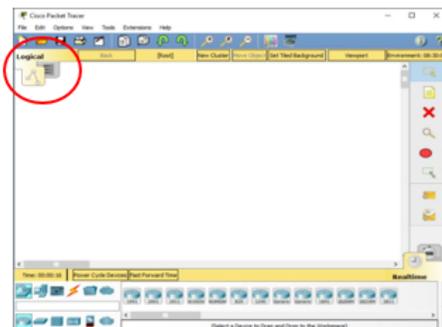
Práctica 3

Configurando dispositivos

Paso 1: Abrir la vista física de Packet Tracer

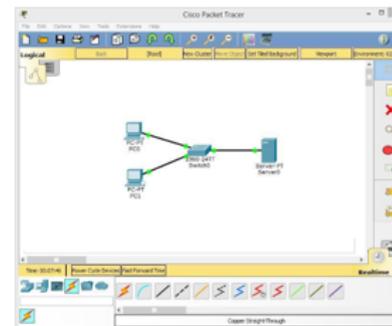
a) Inicia Packet Tracer.

Cuando se abre Packet Tracer, la vista predeterminada es la vista lógica.



Paso 2: construir la topología

1. Cree la red que se muestra a continuación (si necesita ayuda, consulte las actividades anteriores).
 - a) Utilice el puerto FastEthernet0 / 1 en el conmutador para PC0
 - b) Utilice el puerto FastEthernet0 / 2 en el conmutador para PC1
 - c) Utilice el puerto FastEthernet0 / 3 en el conmutador para Servero0



2. Una vez que las luces de enlace se pongan verdes, haga clic en Servidor0. Luego configúrelo de la siguiente manera: una. Haga clic en la pestaña Escritorio.

- a) Haga clic en el icono de configuración de IP.
- b) Haga clic en el cuadro de diálogo Dirección IP.
- c) Escribir 192.168.1.1 como la dirección y presione Enter.
- d) Debería aparecer un valor predeterminado de 255.255.255.0 en la máscara de subred.
- e) No es necesario configurar nada más en este cuadro de diálogo, así que haga clic en la "X" en la esquina superior derecha para cerrar la ventana Configuración de IP.
- f) clic en la "X" roja en la esquina superior derecha para cerrar la ventana Servero0.

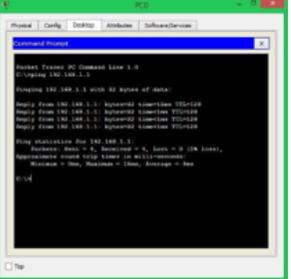
3. Haga clic en PC0. Luego configúrelo de la siguiente manera: una. Haga clic en la pestaña Escritorio.

- a) Haga clic en el icono de configuración de IP.
- b) Haga clic en el cuadro de diálogo Dirección IP.
- c) Escribir 192.168.1.2 como la dirección y presione Enter.
- d) Debería aparecer un valor predeterminado de 255.255.255.0 en el campo Máscara de subred.
- e) No es necesario configurar nada más en este cuadro de diálogo, así que haga clic en la "X" en la esquina superior derecha para cerrar la ventana Configuración de IP
- f) Clic en el icono etiquetado CommandPrompt y debería aparecer el siguiente mensaje

UD02 Medios de transmisión PRÁCTICAS



g) Escriba el siguiente comando en el indicador: ping 192.168.1.1 y presione Enter.
 h) Si ha hecho todo correctamente, debería ver el siguiente resultado. Su salida podría variar un poco, pero las declaraciones de respuesta deberían estar ahí. Si las respuestas no están ahí, intente rehacer la configuración del dispositivo hasta este punto.



i) j. Haga clic en la "X" junto a la barra de título de CommandPrompt.
 j) k. Haga clic en la "X" roja en la esquina superior derecha para cerrar la ventana PC0.

- Repita los mismos pasos de configuración y ping desde # 3 PC1, excepto que use 192.168.1.3 como dirección IP. Los resultados deberían ser los mismos.
- Por último, vuelva a hacer clic en PC0.
 - Haga clic en la pestaña Escritorio, si aún no está abierta.
 - Haga clic en el icono del navegador web.
 - Tipo 192.168.1.1 en el cuadro URL y haga clic en el botón [IR].
 - Debe observar lo siguiente. Si no lo hace, repita los pasos anteriores para confirmar la configuración. Esto sucede porque la función del servidor web está activada de forma predeterminada en el servidor y PC0 acaba de conectarse a la página predeterminada.

Página 9

UD02 Medios de transmisión PRÁCTICAS



- Haga clic en un enlace y luego use las flechas frontal y posterior a la izquierda del cuadro de URL para avanzar y retroceder por las páginas.
- Cuando termine, haga clic en la "X" junto a la barra de título del navegador web.
- Haga clic en la "X" roja en la esquina superior derecha para cerrar la ventana PC0.

La siguiente sección involucra alguna configuración básica de dispositivos de red, en este caso un conmutador. Los enrutadores tienen las mismas pestañas que los conmutadores, por lo que su interfaz funciona de la misma manera.

- Haga clic en Switch0, luego haga clic en la pestaña Config.

Nota: Anteriormente, se dio una advertencia sobre no usar la pestaña Configuración ya que no está disponible en equipos de red reales, pero estamos explicando esta pestaña por dos razones.

 - Algunos dispositivos simples solo tienen pestañas de configuración.
 - La pestaña de configuración puede ser útil para el aprendizaje básico de comandos, especialmente para principiantes.

a) Al hacer clic en la pestaña Configuración, se muestra una lista de componentes que se pueden configurar en este dispositivo. No vamos a cubrir cuáles son estos componentes, ya que se aprende en un curso de redes, pero mostraremos cómo navegar y usar la interfaz.

Página 10



b) La pestaña Configuración global permite al usuario cambiar el nombre de un dispositivo que se muestra en el espacio de trabajo. También permite cambiar el nombre interno que se muestra en la línea de comandos, así como los botones para guardar, cargar, exportar y borrar archivos de configuración.

c) Haga doble clic en el cuadro de diálogo Nombre de host resaltando la palabra Cambiar, escriba Central y presione "Enter". Packet Tracer mostrará los comandos de IOS necesarios para realizar el cambio de nombre en el cuadro Comandos de IOS equivalentes. Los comandos mostrados deben ser:

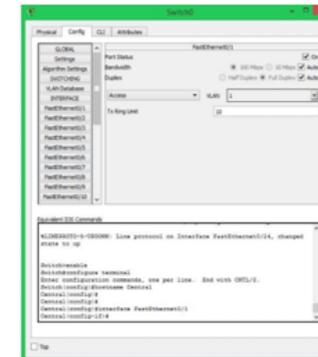
```
Switch> enable
Switch # configure terminal
Ingrese los comandos de configuración, uno por línea. Termine con CNTL / Z.
Switch (config) #hostname Central
Central (config) #
```

Estos serían los comandos que se ingresarían para hacer lo mismo desde la interfaz de línea de comandos o CLI. Si no sabía cómo hacer esto desde la CLI, la pestaña de configuración mostraría los comandos para ilustrar cómo se debe hacer.

UD02 Medios de transmisión PRÁCTICAS

d) Al hacer clic en la etiqueta FastEthernet0 / 1, aparecerá una interfaz Ethernet para configurar.

e) Observe el cuadro Comandos IOS equivalentes a continuación, muestra un comando de "interfaz FastEthernet0/1" que habría sido el comando utilizado para seleccionar la interfaz de la CLI.



f) Seleccione la pestaña CLI para cambiar a la interfaz CLI. Observe que los mismos comandos que estaban en el cuadro Comandos IOS equivalentes se enumeran en la ventana CLI.

g) Clic a la derecha junto al símbolo del sistema en la parte inferior de la lista que se ve así: "Central (config-if) #"

h) Luego escribe cerrar, y presione Enter dos veces.

```
Central (config-if) #shutdown
Central (config-if) #
% LINK-5-CHANGED: Interfaz FastEthernet0 / 1, estado cambiado a administrativamente inactivo
% LINEPROTO-5-UPDOWN: Protocolo de línea en la interfaz FastEthernet0 / 1, estado cambiado a inactivo
Central (config-if) #
```

Este comando simplemente cierra la interfaz desde la línea de comando.

UD02 Medios de transmisión

PRÁCTICAS

- i) Haga clic en la "X" roja en la esquina superior derecha para cerrar la ventana CLI del servidor. Observe cómo los luces de enlace para la conexión entre PC0 y Switch0 son rojas. Dado que la interfaz del conmutador se cerró, la conexión ya no está activa y se muestra en rojo.

Esto cubre algunas configuraciones básicas y operación de dispositivos finales en Packet Tracer. Guarda y entrega la actividad.

Página 13

UD02 Medios de transmisión

PRÁCTICAS

Práctica 4

Creación de una red sencilla

Topología

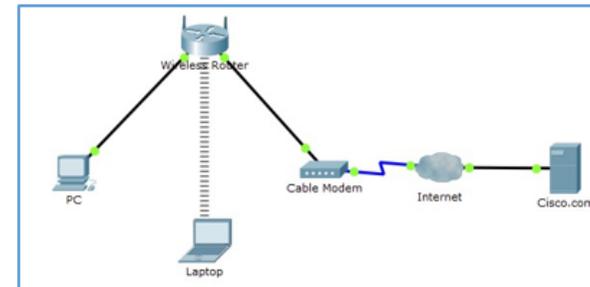


Tabla de direcciones

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC	Ethernet0	DHCP		192.168.0.1
Wireless Router	LAN	192.168.0.1	255.255.255.0	
	Internet	DHCP		
Cisco.com Server	Ethernet0	208.67.220.220	255.255.255.0	
Laptop	Wireless0	DHCP		

Parte 1: Construir una red simple en el espacio de trabajo de topología lógica

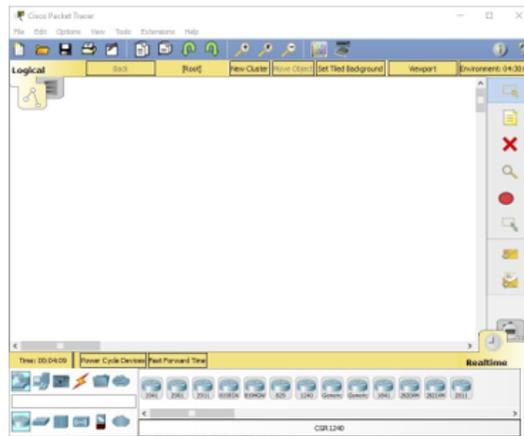
Paso 1: Inicie Packet Tracer.

Página 14

UD02 Medios de transmisión PRÁCTICAS

a. Inicie Packet Tracer en su PC o computadora portátil

Haga doble clic en el icono de Packet Tracer en su escritorio o navegue hasta el directorio que contiene el archivo ejecutable de Packet Tracer e inicie Packet Tracer. Packet Tracer debe abrirse con un espacio de trabajo de topología lógica predeterminado en blanco, como se muestra en la figura.



Paso 2: construir la topología

a) Agregue dispositivos de red al espacio de trabajo.

Usando el cuadro de selección de dispositivos, agregue los dispositivos de red al espacio de trabajo como se muestra en el diagrama de topología.

Para colocar un dispositivo en el espacio de trabajo, primero elija un tipo de dispositivo del Selección del tipo de dispositivo caja. Luego, haga clic en el modelo de dispositivo deseado de la Selección específica del dispositivo caja. Finalmente, haga clic en una ubicación en el espacio de trabajo para colocar su dispositivo en esa ubicación. Si desea cancelar su selección, haga clic en el icono Cancelar para cancelar el dispositivo. Alternativamente, puede hacer clic y arrastrar un dispositivo desde el Selección específica del dispositivo caja en el espacio de trabajo.

b) Agregue dispositivos de red al espacio de trabajo.

UD02 Medios de transmisión PRÁCTICAS

Usando el cuadro de selección de dispositivos, agregue los dispositivos de red al espacio de trabajo como se muestra en el diagrama de topología.

Para colocar un dispositivo en el espacio de trabajo, primero elija un tipo de dispositivo del Selección del tipo de dispositivo caja. Luego, haga clic en el modelo de dispositivo deseado de la Selección específica del dispositivo caja. Finalmente, haga clic en una ubicación en el espacio de trabajo para colocar su dispositivo en esa ubicación. Si desea cancelar su selección, haga clic en el icono Cancelar para eliminar ese dispositivo. Alternativamente, puede hacer clic y arrastrar un dispositivo desde el Selección específica del dispositivo caja en el espacio de trabajo.

c) Cambiar los nombres de visualización de los dispositivos de Network.

Para cambiar los nombres de visualización de los dispositivos de red, haga clic en el icono del dispositivo en el espacio de trabajo de Packet Tracer Logical, luego haga clic en el Config pestaña en la ventana de configuración del dispositivo. En la pestaña Configuración, escriba el nuevo nombre del dispositivo en el Nombre para mostrar cuadro como se muestra en la figura.

d) Agregue el cableado físico entre dispositivos en el espacio de trabajo

Usando el cuadro de selección de dispositivos, agregue el cableado físico entre los dispositivos en el espacio de trabajo como se muestra en el diagrama de topología.

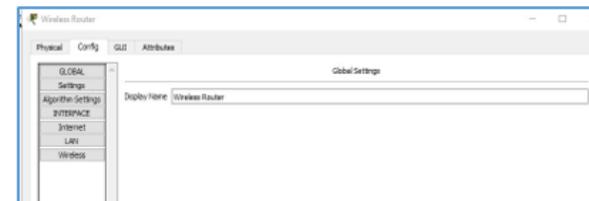
La PC necesitará un cable de cobre directo para conectarse al enrutador inalámbrico. Seleccione el cobre cable directo en el cuadro de selección de dispositivo y conéctelo a la interfaz FastEthernet0 de la PC y a la interfaz Ethernet 1 del enrutador inalámbrico.

El enrutador inalámbrico necesitará un cable de cobre directo para conectarse al módem por cable. Seleccione el cable de cobre de conexión directa en el cuadro de selección de dispositivo y conéctelo a la interfaz de Internet del enrutador inalámbrico y la interfaz del puerto 1 del módem por cable.

El módem por cable necesitará un cable coaxial para conectarse a la nube de Internet. Seleccione el cable coaxial en el cuadro de selección de dispositivo y adjuntarlo a la interfaz del puerto 0 del módem por cable y la interfaz coaxial de la nube de Internet.

La nube de Internet necesitará un cable de cobre directo para conectarse al servidor de Cisco.com. Seleccione el cable de cobre de conexión directa en el cuadro de selección de dispositivo y conéctelo a la interfaz Ethernet de la nube de Internet y la interfaz FastEthernet0 del servidor Cisco.com.

Parte 2: configurar los dispositivos de red



Paso 1: configurar el enrutador inalámbrico

a) Cree la red inalámbrica en el enrutador inalámbrico

Haga clic en el icono del Enrutador inalámbrico en el espacio de trabajo de Packet Tracer Logical para abrir la ventana de configuración del dispositivo.

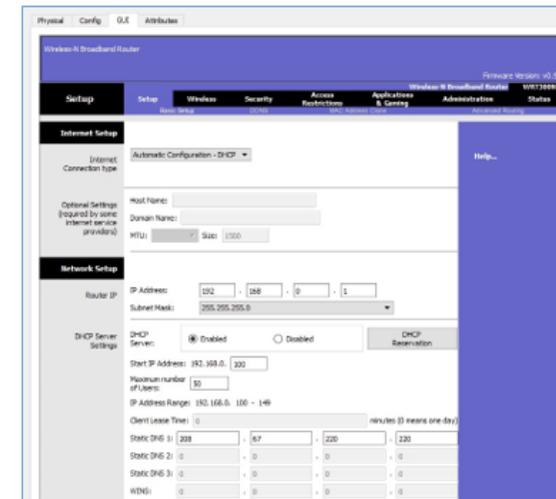
En la ventana de configuración del enrutador inalámbrico, haga clic en la pestaña GUI para ver las opciones de configuración del enrutador inalámbrico.

A continuación, haga clic en el Inalámbrico pestaña en la GUI para ver la configuración inalámbrica. La única configuración que debe cambiarse de los valores predeterminados es el Nombre de red (SSID). Aquí, escriba el nombre "HomeNetwork" como se muestra en la figura.

b) Configure la conexión a Internet en el enrutador inalámbrico Haga clic en Preparar en la pestaña GUI del enrutador inalámbrico.

En la configuración del servidor DHCP, verifique que el Habilitado está seleccionado y configure la dirección IP estática del servidor DNS como 208.87.220.220 como se muestra en la figura.

d) Haz click en el Guardar ajustes lengüeta.



Paso 2: configurar la computadora portátil

a) Configure la computadora portátil para acceder a la red inalámbrica

Haga clic en el icono de Laptop en el espacio de trabajo de Packet Tracer Logical y en las ventanas de configuración de Laptop seleccione la pestaña Física.

En la pestaña Física, deberá quitar el módulo de cobre Ethernet y reemplazarlo con el módulo WPC300N inalámbrico.

Para hacer esto, primero apague la computadora portátil haciendo clic en el botón de encendido en el costado de la computadora portátil. Luego retire el módulo de cobre Ethernet instalado actualmente haciendo clic en el módulo en el costado de la computadora portátil y arrastrándolo a la Módulos panel a la izquierda de la ventana Laptop. Luego instale el módulo Wireless WPC300N haciendo clic en él en el Módulos panel y arrastrándolo al puerto del módulo vacío en el costado de la computadora portátil. Vuelva a encender la computadora portátil haciendo clic en el botón de encendido de la computadora portátil nuevamente.

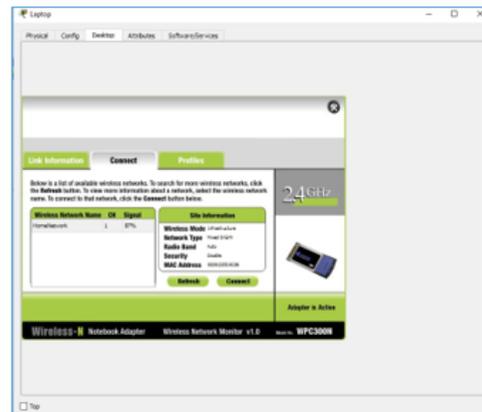
Con el módulo inalámbrico instalado, la siguiente tarea es conectar la computadora portátil a la red inalámbrica.

Haz click en el Escritorio en la parte superior de la ventana de configuración del portátil y seleccione la PC inalámbrico icono.

UD02 Medios de transmisión PRÁCTICAS

Una vez que la configuración del Adaptador de portátil inalámbrico N esté visible, seleccione Conectar lengüeta. La red inalámbrica "HomeNetwork" debe estar visible en la lista de redes inalámbricas como se muestra en la figura.

Seleccione la red y haga clic en el Conectar pestaña que se encuentra debajo de la Información del sitio.

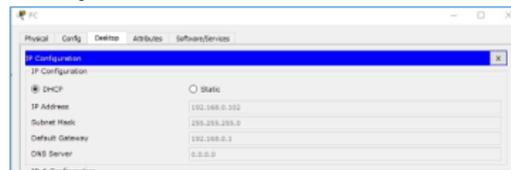


Paso 3: configurar la PC

a) Configure la PC para la red cableada

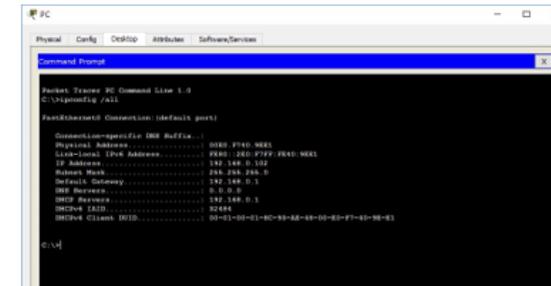
Haga clic en el icono de PC en el espacio de trabajo de Packet Tracer Logical y seleccione Escritorio pestaña y luego la Configuración IP icono.

En la ventana Configuración de IP, seleccione el DHCP botón de radio como se muestra en la figura para que la PC use DHCP para recibir una dirección IPv4 del enrutador inalámbrico. Cierre la ventana Configuración de IP.



UD02 Medios de transmisión PRÁCTICAS

Haga clic en el icono del símbolo del sistema. Verifique que la PC haya recibido una dirección IPv4 emitiendo el comando ipconfig /all desde el comando como se muestra en la figura. La PC debe recibir una dirección IPv4 en el Rango 192.168.0.x.

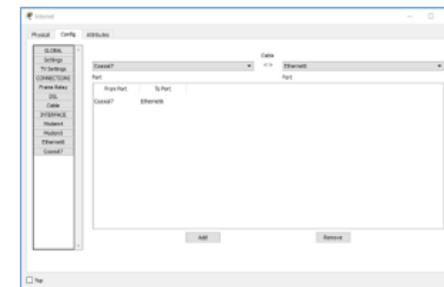


Paso 4: configurar la nube de Internet

a) Instale módulos de red si es necesario

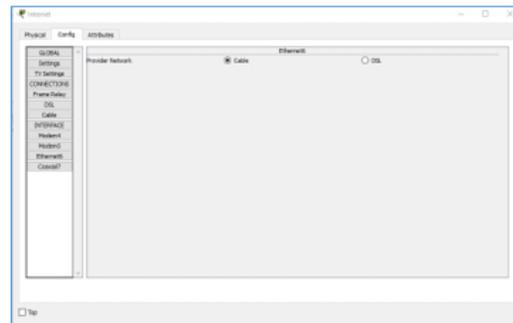
Haga clic en el icono de Internet Cloud en el espacio de trabajo de Packet Tracer Logical y luego haga clic en la pestaña Física. El dispositivo en la nube necesitará dos módulos si aún no están instalados. El PT-CLOUD-NM-1CX que es para la conexión del servicio de cable módem y el PT-CLOUD-NM-1CFE que es para una conexión de cable Ethernet de cobre. Si faltan estos módulos, apague los dispositivos físicos en la nube haciendo clic en el botón de encendido y arrastre cada módulo a un puerto de módulo vacío en el dispositivo y luego vuelva a encender el dispositivo.

b) Identificar los puertos de origen y destino. Haz clic en el Config pestaña en la ventana del dispositivo en la nube. En el panel izquierdo, haga clic en Cable debajo CONEXIONES. En el primer cuadro desplegable, elija Coaxial y en el segundo cuadro desplegable elija Ethernet y luego haga clic en Añadir para agregarlos como From Port y To Port como se muestra en la figura.



c) Identificar el tipo de proveedor

Mientras todavía en el Config pestaña haga clic en Ethernet debajo INTERFAZ en el panel izquierdo. En la ventana de configuración de Ethernet, seleccione Cable como la red de proveedores como se muestra en la figura.



Paso 5: configurar el servidor Cisco.com

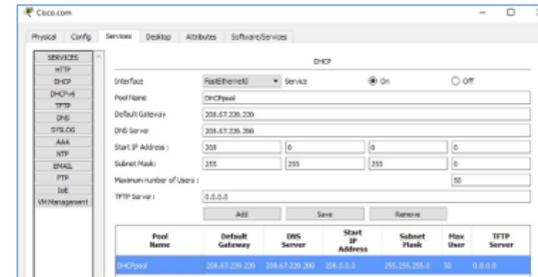
a) Configure el servidor de Cisco.com como servidor DHCP

Haga clic en el icono del servidor Cisco.com en el espacio de trabajo de Packet Tracer Logical y seleccione Servicios lengüeta. Seleccione DHCP desde el SERVICIOS lista en el panel izquierdo.

En la ventana de configuración de DHCP, configure un DHCP como se muestra en la figura con la siguiente configuración.

- Hacer clic En para activar el servicio DHCP Nombre del grupo: DHCPpool
- Puerta de enlace predeterminada: 208.67.220.220
- Servidor DNS: 208.67.220.220
- Dirección IP inicial: 208.67.220.1 Máscara de subred 255.255.255.0
- Número máximo de usuarios: 50

Hacer clic Añadir para agregar la piscina

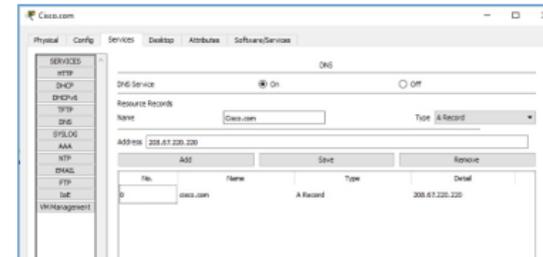


b) Configure el servidor Cisco.com como un servidor DNS para proporcionar el nombre de dominio a la resolución de direcciones IPv4. Todavía en el Servicios pestaña, seleccione DNS desde el SERVICIOS enumerados en el panel izquierdo.

Configure el servicio DNS utilizando los siguientes ajustes como se muestra en la figura.

- Hacer clic En para activar el servicio DNS en Nombre:
- Cisco.com
- Tipo: un registro
- Dirección: 208.67.220.220

Hacer clic Añadir para agregar la configuración del servicio DNS



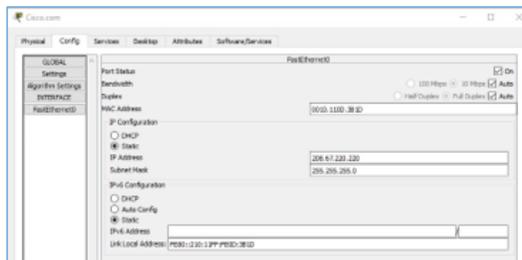
c) Configure las configuraciones globales del servidor de Cisco.com.
 Seleccione el Config lengüeta. Haga clic en Configuraciones en el panel izquierdo.
 Configure los ajustes globales del servidor de la siguiente manera:

- **Seleccione Estático**
- **Puerta de enlace: 208.67.220.1**
- **Servidor DNS: 208.67.220.220**



d) Configure los ajustes de la interfaz FastEthernet0 del servidor Cisco.com.
 Haga clic en FastEthernet en el panel izquierdo del Config lengüeta
 Configure los ajustes de la interfaz FastEthernet del servidor de la siguiente manera:

- **Seleccione Estático en Configuración IP Dirección**
- **IP: 208.67.220.220**
- **Máscara de subred: 255.255.255.0**



Parte 3: verificar la conectividad

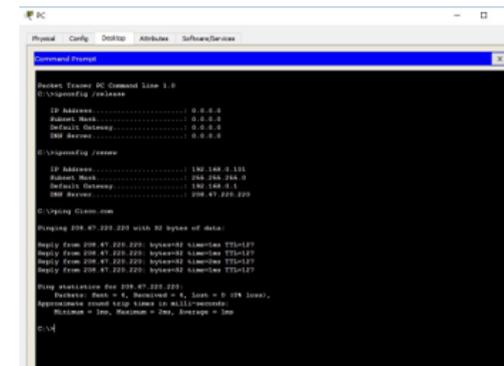
Paso 1: actualice la configuración de IPv4 en la PC

a) Verifique que la PC esté recibiendo información de configuración de IPv4 de DHCP.

Haz click en el ordenador personal en el espacio de trabajo de Packet Tracer Logical y luego selecciona la pestaña Escritorio de la ventana de configuración de la PC.

Haz click en el icono Símbolo del sistema

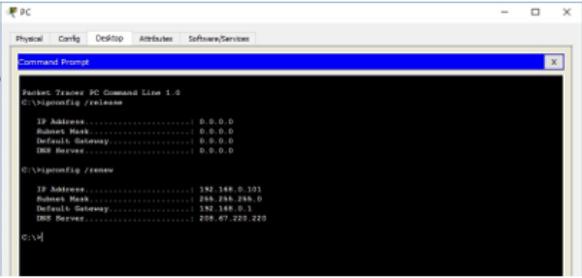
En el símbolo del sistema, actualice la configuración de IP emitiendo los comandos `ipconfig /release` y entonces `ipconfig /renew`. El resultado debe mostrar que la PC tiene una dirección IP en el rango 192.168.0.x, una máscara de subred, una puerta de enlace predeterminada y una dirección de servidor DNS como se muestra en la figura.



b) Pruebe la conectividad al servidor de Cisco.com desde la PC

Desde el símbolo del sistema que emite el comando `ping Cisco.com`. Pueden pasar unos segundos hasta que vuelva el ping. Se deben recibir cuatro respuestas como se muestra en la figura.

UD02 Medios de transmisión PRÁCTICAS



```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /release

IP Address . . . . . 0.0.0.0
Subnet Mask . . . . . 0.0.0.0
Default Gateway . . . . . 0.0.0.0
DNS Servers . . . . . 0.0.0.0

C:\>ipconfig /renew

IP Address . . . . . 192.168.0.101
Subnet Mask . . . . . 255.255.255.0
Default Gateway . . . . . 192.168.0.1
DNS Servers . . . . . 208.87.229.229

C:\>
```

Parte 4: Guarde el archivo y cierre Packet Tracer

Paso 1: Guarde el archivo como un archivo de actividad de Packet Tracer (*.pkt)

Para guardar la red completa, haga clic en Archivo en la barra de menú de Packet Tracer y luego seleccione **Guardar como...** en el menú desplegable. En la ventana Guardar archivo, elija un directorio para guardar el archivo y asígnele un nombre de archivo apropiado. Guardar como tipo tiene como valor predeterminado el Archivo de actividad de Packet Tracer (*.pkt).

Página 25

Cuaderno de PRÁCTICAS: Medios de transmisión

Nombre y apellidos	
--------------------	--

Breve descripción	Entrenarnos en seleccionar el cable adecuado y en cómo conectar correctamente los dispositivos será el objetivo principal de estas prácticas. Además exploraremos las redes en Packet Tracer.
Material necesario	<ul style="list-style-type: none"> • Cuaderno de trabajo • Bolígrafo y/o lápiz • 1 PC con Packet Tracer • Herramientas de redes de taller (crimpadoras, comprobador-testers, destornilladores, ...) • Materiales específicos de redes (cable UTP, terminales RJ45, rosetas, switch,
Fuentes de información	<ul style="list-style-type: none"> • Diapositivas de la Unidad 2 • Explicaciones de clase

Desarrollo
<ul style="list-style-type: none"> ✓ PRÁCTICA 1: Conexión de una LAN por cable y una LAN inalámbrica. ✓ PRÁCTICA 2: Explorando la red mediante PDUs. ✓ PRÁCTICA 3: Vista física de Packet Tracer. ✓ PRÁCTICA 4: Crimpado.

Práctica 1

Conexión de una LAN por cable y una LAN inalámbrica

Topología

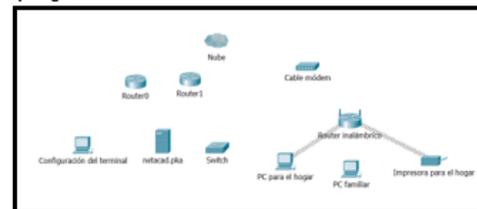


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Conectar a
Nube	Eth6	N/D	F0/0
	Coax7	N/D	Puerto 0
Cable módem	Puerto 0	N/D	Coax7
	Puerto1	N/D	Internet
Router0	Consola	N/D	RS232
	F0/0	192.168.2.1/24	Eth6
	F0/1	10.0.0.1/24	F0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	F1/0	172.18.0.1/24	F0/1
Router inalámbrico	Internet	192.168.2.2/24	Puerto 1
	Eth1	192.168.1.1	F0
PC familiar	F0	192.168.1.102	Eth1
Switch	F0/1	172.18.0.2	F1/0
Netacad.pka	F0	10.0.0.254	F0/1
Configuración del terminal	RS232	N/D	Consola

Parte 1: Conectarse a la nube

Paso 1: Conectar la nube al Router0

- En la esquina inferior izquierda, haga clic en el ícono de rayo anaranjado para abrir las conexiones disponibles.
- Elija el cable adecuado para conectar la interfaz Fa0/0 del Router0 a la interfaz Eth6 de la nube. La nube es un tipo de switch, de modo que debe usar una conexión por cable de cobre de conexión directa. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 2: Conectar la nube al cable módem

Elija el cable adecuado para conectar la interfaz Coax7 de la nube al Puerto0 del módem. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Parte 2: Conectar el Router0

Paso 1: Conectar el Router0 al Router1

Elija el cable adecuado para conectar la interfaz Ser0/0/0 del Router0 a la interfaz Ser0/0 del Router1. Use uno de los cables seriales disponibles. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 2: Conectar el Router0 a netacad.pka

Elija el cable adecuado para conectar la interfaz F0/1 del Router0 a la interfaz F0 de netacad.pka. Los routers y las PC tradicionalmente utilizan los mismos cables para transmitir (1 y 2) y recibir (3 y 6). El cable adecuado que se debe elegir consta de cables cruzados. Si bien muchas NIC ahora pueden detectar automáticamente qué par se utiliza para transmitir y recibir, el Router0 y netacad.pka no tienen NIC con detección automática.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 3: Conectar el Router0 al terminal de configuración

Elija el cable adecuado para conectar la consola del Router0 al terminal de configuración RS232. Este cable no proporciona acceso a la red al terminal de configuración, pero le permite configurar el Router0 a través de su terminal.

Si conectó el cable correcto, las luces de enlace del cable cambian a color negro.

Parte 3: Conectar los dispositivos restantes

Paso 1: Conectar el Router1 al switch

Elija el cable adecuado para conectar la interfaz F1/0 del Router1 a la interfaz F0/1 del switch. Si conectó el cable correcto, las luces de enlace del cable cambian a color verde. Deje que transcurran unos segundos para que la luz cambie de color ámbar a verde.

Paso 2: Conectar el cable módem al router inalámbrico

Elija el cable adecuado para conectar el Puerto1 del módem al puerto de Internet del router inalámbrico.

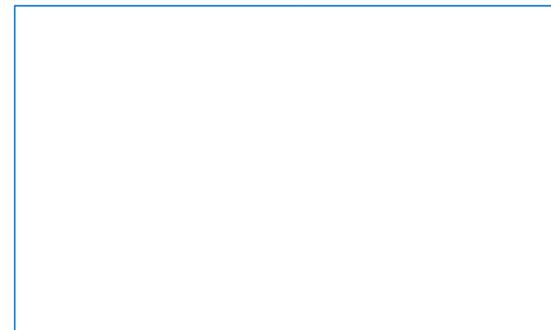
Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Paso 3: Conectar el router inalámbrico a la PC familiar

Elija el cable adecuado para conectar la interfaz Ethernet 1 del router inalámbrico a la PC familiar.

Si conectó el cable correcto, las luces de enlace del cable cambian a color verde.

Inserta a continuación un Recorte del montaje completo con el cableado que has introducido, incluyendo las etiquetas de los puertos donde has conectado cada cable en cada dispositivo (Options>Preference>Always Show Port Labels).

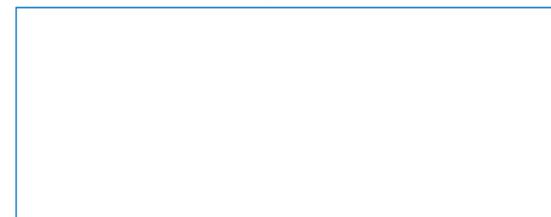


Parte 4: Verificar las conexiones

Paso 1: Probar la conexión de la PC familiar a netacad.pka

- Abra el símbolo del sistema de la PC familiar y haga ping a netacad.pka.

Inserta captura del resultado del ping:



- Abra el explorador web e introduzca dirección web <http://netacad.pka>.

Inserta captura del resultado mostrado en el navegador:

UD02 Medios de transmisión PRÁCTICAS

Paso 2: Hacer ping al switch desde la PC doméstica

Abra el símbolo del sistema de la PC doméstica y haga ping a la dirección IP del switch para verificar la conexión.

Inserta captura del resultado del ping:

Paso 3: Abrir el Router0 desde el terminal de configuración

- Abra el CLI del Router0.
- Presione **Intro** para ver el símbolo del sistema Router0>.
- Escriba **show ip interface brief** para ver el estado de las interfaces.

Inserta una captura del resultado de introducir este comando en el CLI:

Página 5

UD02 Medios de transmisión PRÁCTICAS

Parte 5: Examinar la topología física

Paso 1: Examinar la nube

- Haga clic en la pestaña **Espacio de trabajo físico** (arriba a la izquierda del escritorio de trabajo) o presione **Shift + P** y **Shift + L** para alternar entre los espacios de trabajo lógicos y físicos.
- Haga clic en el ícono **Ciudad de residencia**.
- Haga clic en el ícono **Nube**. ¿Cuántos cables están conectados al switch en el rack azul?

- Haga clic en **Regresar** para volver a la pantalla de **Ciudad de residencia**.

Paso 2: Examinar la red principal

- Haga clic en el ícono **Red principal**. Presione el puntero del mouse en los distintos cables. ¿Qué se encuentra sobre la mesa a la derecha del rack azul?

- Haga clic en **Regresar** para volver a la pantalla de **Ciudad de residencia**.

Paso 3: Examinar la red secundaria

- Haga clic en el ícono **Red secundaria**. Presione el puntero del mouse en los distintos cables. ¿Por qué hay dos cables anaranjados conectados a cada dispositivo?

- Haga clic en **Regresar** para volver a la pantalla de **Ciudad de residencia**.

Paso 4: Examinar la red doméstica

- ¿Por qué crees que hay una malla ovalada que cubre la red doméstica? ¿Tiene que ver con que es una conexión inalámbrica? ¿Qué representa ésta malla?

Página 6

- UD02 Medios de transmisión PRÁCTICAS
- b. Haga clic en el ícono Red doméstica. ¿Por qué no hay ningún rack para contener el equipo?
- c. Haga clic en la ficha Espacio de trabajo lógico para volver a la topología lógica.

Práctica 2

Explorando la red mediante PDUs

Topología

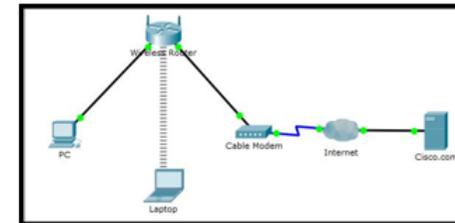


Tabla de direcciones

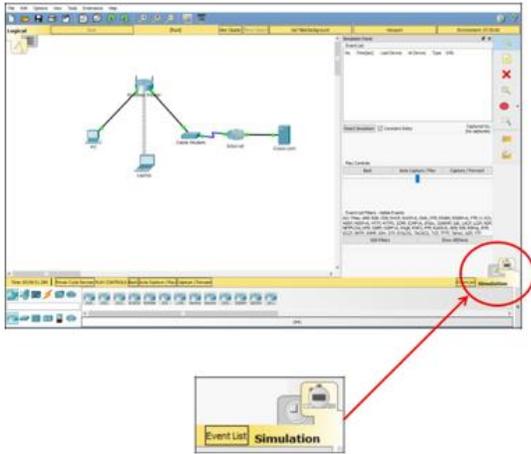
Device	Interface	IP Address	Subnet Mask	Default Gateway
PC	Ethernet0	DHCP		192.168.0.1
Wireless Router	LAN	192.168.0.1	255.255.255.0	
	Internet	DHCP		
Cisco.com Server	Ethernet0	208.67.220.220	255.255.255.0	
Laptop	Wireless0	DHCP		

Parte 1: Crear una PDU Simple en modo de simulación

Paso 1: Abra el fichero *.pkt, que está adjunto en la Tarea de TEAMS correspondiente. Cambia el nombre del Wireless Router y nómbralo con tu NombreApellido.

- a) Entra en el modo Simulación, para ello haz click en la esquina inferior derecha de la ventana de Packet Tracer para abrir el panel *Simulation*.

UD02 Medios de transmisión PRÁCTICAS



Paso 2: Crea una PDU simple, para ello debes seguir los siguientes pasos:

a) Vamos a crear una PDU simple que envíe un ping desde la PC a la computadora portátil.

Haz clic en el icono "Agregar PDU simple" (parece un sobre cerrado) en el panel derecho de la ventana de Packet Tracer.

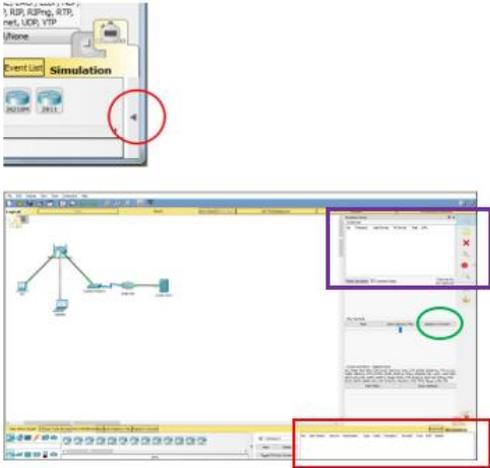


El cursor del ratón ahora cambiará a un sobre con un signo más.

Con este cursor, primero haz clic en la PC para que se convierta en la fuente (emisor) del ping y luego haz clic en la computadora portátil para que se convierta en el destino (receptor).

Página 9

Ahora debemos ampliar el panel de *Simulación de eventos* haciendo clic en la flecha gris en la parte inferior derecha de la ventana de Packet Tracer.



b) Observa el tráfico que se mueve a través de la red, para ello:

Haz clic en el botón "Capturar / Reenviar" (*Capture/Forward*) y observa el tráfico que se mueve a través de la red cada vez que se hace clic en el botón. Es un paso a paso de todo el proceso de comunicación que se está realizando con el PING.

Observa también que cada vez que haces clic en el botón "Capturar / Reenviar" los paquetes enviados se muestran en la ventana "Lista de eventos" (*Event List*), situada en la parte de arriba.

Continúe haciendo clic en Capturar / Reenviar hasta que el paquete ICMP de retorno regrese a la PC. De modo que realicemos el proceso completo del ping.

Inserta a continuación un recorte de tu "Event List" tras la realización del proceso completo, de modo similar al que tienes en la imagen:

Ws.	Time(sec)	Last Device	All Device	Type	Info
	0.000	--	PC	ICMP	
	0.000	--	PC	ARP	
	0.001	PC	Wireless ...	ARP	
	0.006	--	Wireless ...	ARP	
	0.007	Wireless Ro...	Laptop	ARP	
	0.012	--	Laptop	ARP	
	0.013	Laptop	Wireless ...	ARP	
	0.014	Wireless Ro...	PC	ARP	
	0.014	--	PC	ICMP	

[Inserta la captura aquí]

Recuerda que debes haber cambiado el nombre del Router original por tu NombreApellido

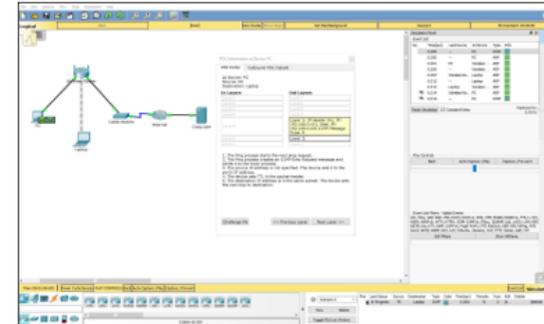
Parte 2: Analizar el contenido de las PDUs.

Paso 1: Usar la lista de eventos para ver la información de la PDU.

a) Vamos a analizar la información del primer "paquete ICMP" de la PDU desde la PC, para ello:

En la ventana "Event List" haz clic en el cuadrado verde de la columna "Información" en la primera línea de ICMP que aparece en la lista. Esto abrirá una ventana de Información de la PDU en el PC. (Porque el primer paso del PING es la salida desde el PC emisor).

Aparecerá una ventana como la siguiente:



Realiza una captura completa de tu ventana de PACKET TRACER con esta ventana de Información e insértala a continuación:

[Inserta la captura aquí]

UD02 Medios de transmisión PRÁCTICAS

Observa la información que aparece en la pestaña "Modelo OSI".

Observa que se trata de una PDU de capa 3 ("Layer 3", NIVEL DE RED donde se insertan las cabeceras de IP) saliente y que se muestran las direcciones IPv4 de origen y destino, de manera similar a como se muestra en la figura siguiente:



Escribe a continuación cuál es la IP de Emisor (Source IP "Src IP") que se indica y cuál es la IP de receptor (Destino IP "Dest IP"):

[Responde aquí]

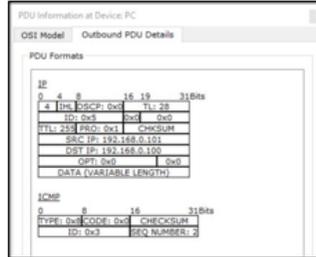
¿Con qué dispositivos se corresponde cada una de estas IP's?

[Responde aquí]

Página 13

UD02 Medios de transmisión PRÁCTICAS

A continuación, haz clic en la pestaña "Detalles de PDU salientes" (Outbound PDU Details). Observa como esta pestaña muestra detalles de los encabezados del protocolo. Y también que sólo tenemos detalles de salida. ¿Por qué crees que es esto?



[Responde aquí]

b) Explora el contenido de otras PDU enumeradas en el Panel de Simulación (Event List) y revisa la información disponible en cada una. ¿Aparece alguna Información de línea en que nos indique información de PDU de entrada y salida ("Inbound PDU Details" y "Outbound PDU Details")?. Haz una captura de esta ventana de Información e insértala a continuación:

[Inserta la captura aquí]

Página 14

UDO2 Medios de transmisión PRÁCTICAS

Paso 2: Elimina la PDU simple.

c) Vamos a **eliminar la simulación del PDU simplex** desde el panel de Simulación (abajo derecha), para ello:

Haz clic en Eliminar en la parte inferior de la ventana de Packet Tracer.

Debemos eliminar las simulaciones que realizamos para no arrastrar residuos en las siguientes simulaciones, puesto que podría producirnos resultados erróneos.

Parte 3: Crear una PDU compleja en modo de simulación.

Paso 1: Crear una PDU compleja.

a) Agrega una PDU compleja para enviar pings desde la PC a la computadora portátil.
Haz clic en la imagen de **Agregar PDU compleja**, la que parece un **sobre abierto**, en el panel derecho de la ventana de Packet Tracer.



Ahora el cursor cambiará a un sobre con un signo más.

Haz clic primero en el PC, para que sea el dispositivo de origen de los pings, y luego haz clic en la computadora portátil para que sea el destino.

Aparecerá la ventana "Crear PDU compleja".

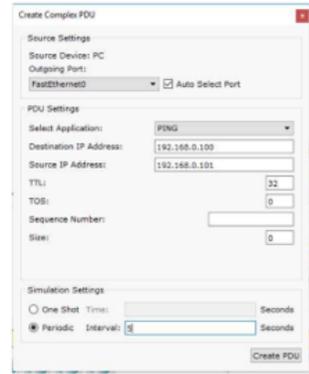
b) Ahora debemos configurar la PDU para enviar los pings cada 5 segundos.
En la ventana "Crear PDU compleja", hay muchas configuraciones que se pueden personalizar. Para enviar un ping cada 5 segundos desde la PC a la computadora portátil:

- El campo **Dirección IP de destino** debe tener la dirección IPv4 de la computadora portátil (192.168.0.100).
- El campo **Dirección IP de origen** debe ser la dirección IP de la PC (192.168.0.101).
- En la parte inferior de la Configuración de simulación, en la sección **Periódico** debemos configurar el intervalo a 5 segundos.

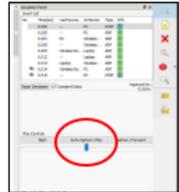
La configuración debe quedar como se observa en la imagen a continuación:

Página 15

UDO2 Medios de transmisión PRÁCTICAS



c) **Observa el tráfico que se mueve a través de la red.**
Haz clic ahora en el botón "Captura / reproducción automática" (**Auto Capture/Play**) y observa cómo se mueve el tráfico a través de la red y las PDU que completan la lista de eventos (**Event List**) del panel de Simulación.



Debido a que configuramos la PDU compleja en un intervalo de 5 segundos, se creará una nueva PDU cada 5 segundos. Haz clic en el botón "Captura/Reproducción automática" de nuevo para detener la simulación.

Página 16

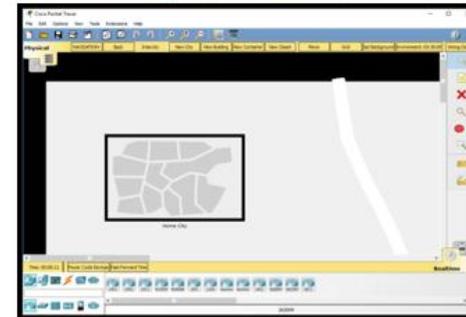
Realiza una captura de la Lista de Eventos e insértala a continuación:

[Inserta la captura aquí]

Para eliminar la PDU compleja, de nuevo haz clic en el Eliminar botón en Simulación de eventos en la parte inferior de la ventana de Packet Tracer.

Práctica 3

Vista física de Packet Tracer



Paso 1: Abrir la vista física de Packet Tracer

a) Inicia Packet Tracer.

Cuando se abre Packet Tracer, la vista predeterminada es la vista lógica.



UD02 Medios de transmisión PRÁCTICAS

b) Cambiar a la vista física.

Haz clic en el botón Vista física para cambiar a la vista física (Physical). El botón Vista física está detrás del botón Vista lógica en la parte superior izquierda del espacio de trabajo.



La vista física predeterminada en Packet Tracer es Intercity.



Paso 2: Aplicar una imagen de fondo de vista física

Vamos a utilizar una imagen del mundo que tendrás en los archivos de la Tarea de TEAMS. Descárgala en tu local.

Página 19

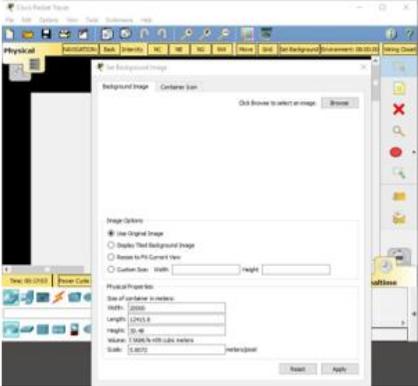
UD02 Medios de transmisión PRÁCTICAS

a) Carga la imagen en Packet Tracer.
Asegúrate de que en la Vista Física Interurbano (Intercity) está seleccionado en la barra de herramientas.



Haz clic en la ventana Definir fondo (Set Background) en la parte superior de la ventana de Packet Tracer. Se abrirá una ventana para poder establecer una imagen de fondo, para ello haz clic en Browse para navegar a la imagen guardada en tu local. Selecciona la imagen y luego haz clic en Aplicar (Apply).

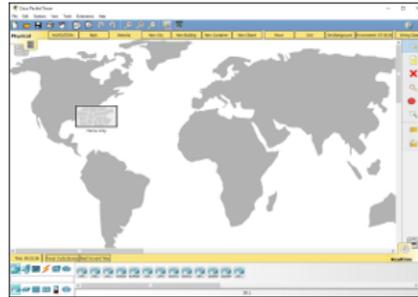
Cierre la ventana para establecer la imagen de fondo del mundo.



Página 20

UD02 Medios de transmisión PRÁCTICAS

Después de hacer clic en Aplicar, la imagen se guarda como fondo de la vista física.



Paso 3: Editar y mover entre contenedores.

a) Reubica la ciudad local.

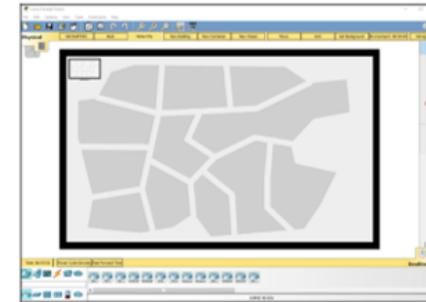
Observa como en la vista Intercity hay un **contenedor** de ciudad local (**Home City**). El contenedor de la ciudad local se puede mover a cualquier ubicación en la vista física.

Haz clic y arrastra el contenedor Ciudad local a cualquier lugar del fondo del mapa mundial.

b) Aplica una imagen de fondo a la ciudad local.

Haz clic en el contenedor Ciudad local. Observa que la vista cambia y lo que está en el espacio de trabajo ahora es el fondo predeterminado de la ciudad local. Puedes reducir la imagen haciendo clic en la lupa con el signo menos para que todo el fondo sea visible.

UD02 Medios de transmisión PRÁCTICAS



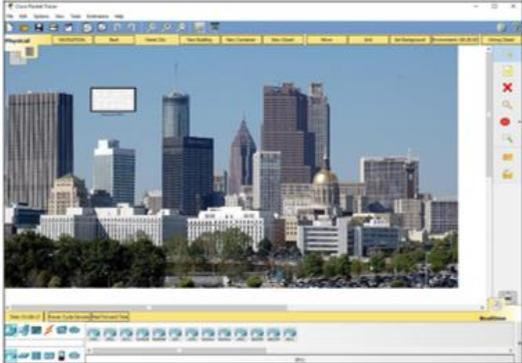
c) Repite el paso 2 para descargar una imagen de una ciudad desde la Tarea de TEAMS y aplicarlo a la ciudad local.

Haz clic en **Set Background** en la parte superior de la ventana de Packet Tracer y en la ventana "Establecer imagen de fondo", haz clic en **Browse** para navegar a la imagen guardada. Selecciona la imagen y luego haz clic en **Apply**.

Cierra la ventana "Establecer imagen de fondo".

Es posible que debas acercar y volver a centrar el fondo para que sea completamente visible en el espacio de trabajo.

UD02 Medios de transmisión PRÁCTICAS



Si haces clic en el botón "Atrás" (Back) del menú en la barra de herramientas de la Vista física, puedes ver que el fondo de la ciudad que aplicaste ahora también se usa en el contenedor "Ciudad local" en la vista Interurbano.

Back

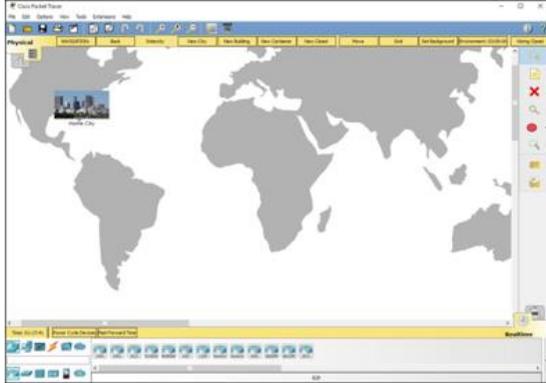
Haz clic en el nombre de la Ciudad y cambia el nombre de la misma por tu NombreApellido. En este ejemplo, el nombre se cambia a Atlanta.



Página 23

UD02 Medios de transmisión PRÁCTICAS

Inserta a continuación una captura de la vista física del mundo con la imagen de la ciudad que también has insertado con tu NombreApellido:



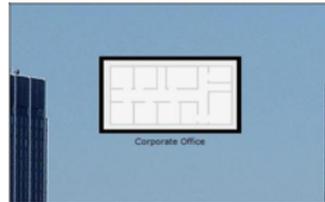
Después haz clic en el contenedor de la Ciudad para entrar a la vista física de la ciudad local que has insertado con tu NombreApellido.

Página 24

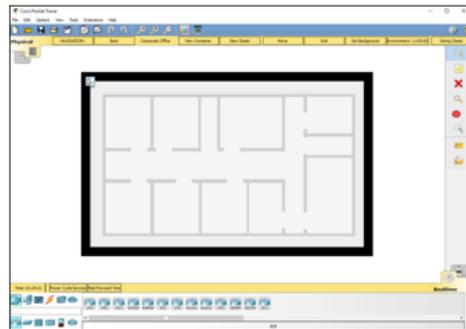
Paso 4: Agregar dispositivos a un Wiring Closet

a. Ingresar a la vista Oficina corporativa.

Hay un contenedor de Oficina corporativa (**Corporate Office**) en el fondo de la ciudad local, que también puedes desplazar y situar donde quieras.

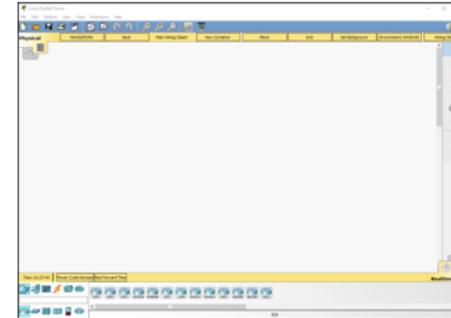


Haz clic en el contenedor Oficina corporativa y reduce el zoom para que el fondo predeterminado de la oficina corporativa sea visible.



El fondo de la oficina corporativa incluye otro contenedor llamado **Main Wiring Closet**. Haga clic en el Armario de cableado principal en vase.

El contenedor Main Wiring Closet tiene un espacio de trabajo en blanco.

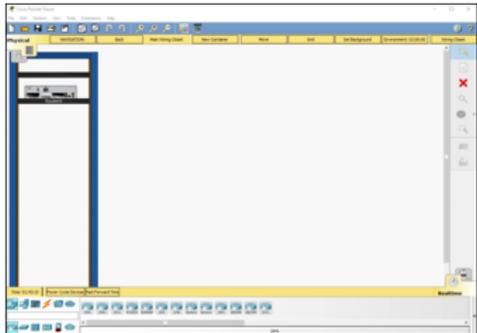


b) Agrega dispositivos al armario de cableado principal.

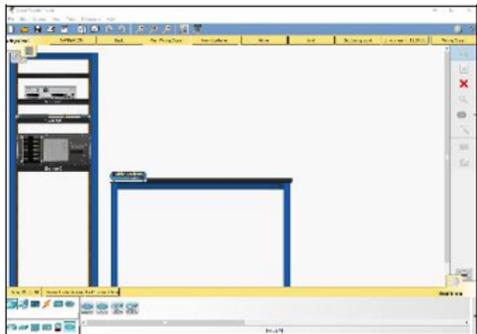
Agrega un Rack pulsando en **New Rack**. En la vista del Rack, agrega un enrutador (**Router**) al espacio de trabajo tal como lo harías en la vista Lógica haciendo clic en un enrutador en la ventana del dispositivo y luego en el espacio de trabajo.

UD02 Medios de transmisión PRÁCTICAS

Debido a que estamos en la vista física, Packet Tracer muestra un bastidor con el enrutador instalado en el bastidor.



c) Agrega más dispositivos al armario de cableado.
Agregue un conmutador de red (Switch), un servidor genérico y un Cable-Módem al Rack.



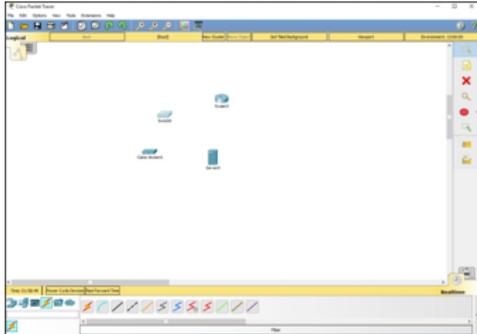
Página 27

UD02 Medios de transmisión PRÁCTICAS

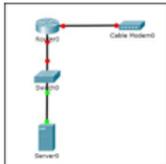
d) Agrega ahora el cableado a los dispositivos del Rack.

Para agregar cableado a los dispositivos, vuelva a la **vista lógica** en Packet Tracer. Es posible que debas acercar y volver a centrar el espacio de trabajo para ver los dispositivos.

Los dispositivos se colocan aleatoriamente en el espacio de trabajo de la vista lógica.



Organiza y conecta los dispositivos juntos utilizando los tipos de cable adecuados en la vista lógica.



Página 28

UD02 Medios de transmisión

PRÁCTICAS

Vuelve a la vista física. Es posible que debas acercar la imagen. Ahora hay cables físicos conectados a las interfaces de los dispositivos. Inserta a continuación una captura con el conexionado de cables en la Vista Física:

[Inserta aquí la captura]

Pasa el puntero del mouse sobre los extremos del cable para ver información sobre cada cable e interfaz.

Paso 5: Experimenta

Ahora que sabes cómo navegar por la vista física y agregar contenedores y dispositivos de red, experimenta agregando contenedores adicionales a tu ciudad local y a tu oficina corporativa. Intente construir armarios de cableado de red más complejos agregando tipos adicionales de dispositivos

Práctica 4

Crimpado

Tarea 1: crimpado de cables

1.1- Busca por internet qué se entiende por crimpado o engastado de terminales.

1.2- Además de cable UTP, se pueden construir conectores con otro cable llamado STP. Busca por internet qué es un cable STP y en qué se diferencia del UTP, que es el que vamos a utilizar.

1.3- Un cable para redes Ethernet tiene 8 hilos con diferentes colores. Indica los colores que tiene dicho cable.

1.4- Los cables de 8 hilos para redes se fabrican trenzados por parejas. ¿Por qué se fabrican así?

1.5- Busca por internet cuál es el orden adecuado en el que hay que colocar los cables anteriores para un conector RJ45 según el estándar TIA/EIA-568-B.

1.6- Los terminales RJ45 se fijan a los cables con una herramienta llamada crimpadora. Busca por internet una imagen de una crimpadora para este tipo de terminales.

Tarea 2: crimpado terminales RJ45 (CABLE CRUZADO)

2.1- Busca por internet para qué se utiliza un cable cruzado con terminales RJ45.

2.2- Busca por internet en qué orden se han de conectar los cables en cada extremo del cable para montar un cable cruzado con terminales RJ45. Inserta una imagen donde se vea el orden de los colores en cada extremo.

2.3- Una vez montado un cable Ethernet, se ha de verificar su correcto montaje con un comprobador. Busca por internet una imagen de un comprobador de cable de red Ethernet RJ45.

Tarea 3: crimpado terminales RJ45 (CABLE DIRECTO)

3.1- Busca por internet para qué se utiliza un cable directo con terminales RJ45.

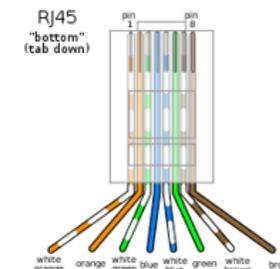
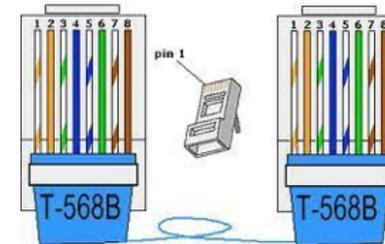
3.2- Busca por internet en qué orden se han de conectar los cables en cada extremo del cable para montar un cable directo con terminales RJ45. Inserta una imagen donde se vea el orden de los colores en cada extremo.

Tarea 4

Objetivo	Aprender a montar un conector RJ45 y comprobar que funciona
Precauciones	<ul style="list-style-type: none"> Una vez acabada la práctica, recoger y tirar a la basura todos los restos de cables y dejar la mesa de trabajo limpia.
Material	<ul style="list-style-type: none"> 2 Segmentos de cable UTP de 20 a 30 cm de longitud. Cuatro terminales RJ45 Crimpadora RJ45 Comprobador de cables de red RJ45
Desarrollo proceso crimpado RJ45 (CABLE DIRECTO)	<ul style="list-style-type: none"> Coger un segmento de cable UTP de 20 a 30 cm de longitud Cortar con la crimpadora la punta donde se va a colocar el terminal. Retirar 1,5 cm de funda de plástico del extremo donde se quiere colocar el terminal. Colocar los cables en el orden adecuado según el estándar TIA/EIA-568-B. Estirar bien los cables hasta que queden bien rectos. Insertar el terminal RJ45 en el extremo pelado, hasta asegurar que el cable llega hasta el extremo final del conector. Poner el terminal en la boca adecuada de la crimpadora. Cerrar fuertemente la tenaza hasta que el conector quede fuertemente crimpado en el cobre del cable. Tirar del terminal para asegurarse de que ha quedado fuertemente sujeto. Repetir la operación en el otro extremo del cable con el mismo orden de colores.
Desarrollo proceso crimpado RJ45 (CABLE CRUZADO)	<ul style="list-style-type: none"> Coger un segmento de cable UTP de 20 a 30 cm de longitud Cortar con la crimpadora la punta donde se va a colocar el terminal. Retirar 1,5 cm de funda de plástico del extremo donde se quiere colocar el terminal. Colocar los cables en el orden adecuado según el estándar TIA/EIA-568-B. Estirar bien los cables hasta que queden bien rectos. Insertar el terminal RJ45 en el extremo pelado, hasta asegurar que el cable llega hasta el extremo final del conector. Poner el terminal en la boca adecuada de la crimpadora. Cerrar fuertemente la tenaza hasta que el conector quede fuertemente crimpado en el cobre del cable. Tirar del terminal para asegurarse de que ha quedado fuertemente sujeto. Repetir la operación en el otro extremo del cable con el orden de colores que indica el estándar TIA/EIA-568-A.

Comprobación cable de red	<ul style="list-style-type: none"> Coger el comprobador de cable de red. Conectar los terminales del cable construido a los conectores del comprobador. Poner el comprobador de cable en ON. Comprobar que se recibe señal eléctrica por cada uno de los 8 cables. Si no hay señal en alguno de los cables, habrá que repetir la práctica, recortando el tubo UTP para retirar los terminales colocados y volviendo a colocar dos nuevos terminales.
----------------------------------	---

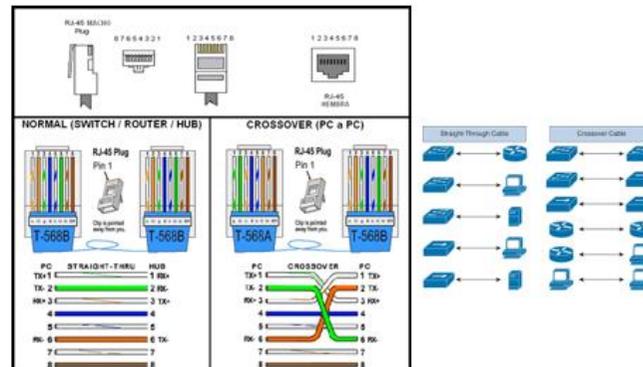
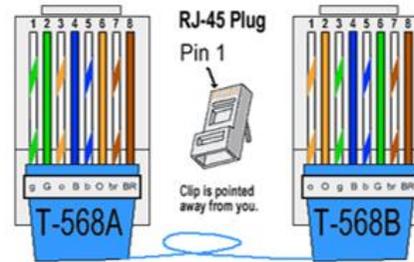
Se utiliza **cable directo** cuando se **conecta el ordenador a un dispositivo de la red local**.
En este caso los dos conectores del cable se hacen idénticos.



UD02 Medios de transmisión

PRÁCTICAS

Cuando se quieren **conectar dos ordenadores directamente** por sus tarjetas de red sin ningún dispositivo intermedio se tiene que utilizar un **cable cruzado**, que altera el orden de los pares para que lo que es recepción en un extremo sea emisión en el otro y viceversa.



8.2.4 Trabajo de investigación

UNIDAD 2 – TRABAJO DE INVESTIGACIÓN

UNIDAD 2. IDENTIFICACIÓN DE ELEMENTOS Y ESPACIOS FÍSICOS DE UNA RED LOCAL

DISEÑO DE UN CENTRO DE PROCESADO DE DATOS

Objetivos

- Conocer las principales características de un Centro de Proceso de Datos.
- Diseñar los elementos básicos que componen un Centro de Proceso de Datos.

Descripción

1. El nombre del documento será: Proyecto Diseño CPD_NombreApellidos
2. El trabajo se realizará en formato WORD. (Justificar el texto y evitar faltas de ortografía, tamaño de fuente máximo 13, mínimo 10, a excepción de títulos)
3. Debe contener una portada con un título y el nombre y apellidos del autor y un índice.
4. La extensión máxima del mismo, sin contar la portada ni el índice, no sobrepasará las 15 páginas ni estará por debajo de los 5.
5. El trabajo se entregará en la carpeta personal compartida de RL en OneDrive.

Criterios de calificación

Se valorará:

- ✓ Presentación y pulcritud.
- ✓ Corrección gramatical y ortográfica.
- ✓ Uso de un lenguaje técnico adecuado.
- ✓ En caso de usar imágenes, que éstas aporten información de utilidad.

Página 1

UNIDAD 2 – TRABAJO DE INVESTIGACIÓN

Desarrollo

El trabajo consiste en investigar qué es un Centro de Proceso de Datos (CPD), describiendo qué contiene y su función y hacer un diseño de un CPD.

En nuestro armario-rack del CPD vamos a tener:

- Un servidor Web
- Un servidor de correo, archivos y base de datos
- Un proxy
- Un firewall

La actividad consta de dos partes:

- Una primera parte de investigación y recopilación de información de qué es un CPD, los componentes más habituales y sus normas de instalación.
- Una segunda parte en la que se realizará un pequeño proyecto de instalación de un CPD.

Parte 1

Esta parte del trabajo consistirá en describir a grandes rasgos en qué consiste un CPD. Contendrá los siguientes apartados:

- **Introducción**
Describir qué es un CPD, su función y lista de los elementos más habituales que podemos encontrar en él.
- **Ejemplos de CPD**
Investiga algún ejemplo de CPDs por Internet, indicando sus características más relevantes y los enlaces. Puedes encontrar CPDs de universidades, gobiernos, empresas, ...
- **Descripción de los elementos más habituales que se pueden encontrar en un CPD**
Describir los siguientes elementos que hemos de tener en cuenta en la obra civil.
 - Dónde se suelen ubicar los CPD en los edificios.
 - Falsos suelos y techos.
 - Altura y anchura de puertas suficiente para introducir los racks y las máquinas que alojará el CPD.
 - Sistemas de Aire acondicionado y control de parámetros medioambientales: temperatura y humedad.

Describir los siguientes sistemas que podemos encontrar en un CPD. Indicar para qué sirven y sus principales características.

- Servidor Web, proxy y firewall: busca información de para qué sirve cada uno de estos sistemas.
- Rack. Tamaños más habituales.
- SAI y generadores de corriente.
- Redundancia en las comunicaciones con el exterior: cables de red, fibras ópticas, etc.

Página 2

UNIDAD 2 – TRABAJO DE INVESTIGACIÓN

- Seguridad de acceso. Vigilancia. Alarmas.
- Seguridad contra incendios.
- Cuadros de distribución eléctrica independientes y seguros.

Parte 2

Esta parte del trabajo se indicará cual es la solución escogida, fabricante y características de los diferentes sistemas analizados e investigados en el apartado anterior. Se pueden incluir planos genéricos sobre la ubicación del CPD y cómo estaría organizado.

- Dónde se ubicará el CPD.
- Por dónde se realizará la instalación de los cables (paredes, suelos, techos, ...) y cómo se hará.
- Sistema de Aire acondicionado y control de parámetros medioambientales: temperatura y humedad que habrá en el CPD.
- Tamaño Rack.
- Modelo de SAI.
- Sistema de Seguridad de acceso. Vigilancia. Alarmas.
- Sistema de Seguridad contra incendios.

8.3 Unidad didáctica 3

El diseño, la implementación y la administración de un plan de asignación de direcciones IP eficaz asegura que las redes puedan operar de una manera eficaz y eficiente. Esto es así especialmente a medida que aumenta la cantidad de conexiones de dispositivos a una red. Comprender la estructura jerárquica de la dirección IP y cómo modificar esa jerarquía a fin de satisfacer con mayor eficiencia los requisitos de diseño constituye una parte importante de la planificación de un esquema de asignación de direcciones IP, y es el objetivo principal de ésta unidad didáctica.

Se muestran también cuáles son los estándares más utilizados para este tipo de redes, desde el punto de vista más teórico, sin olvidar que ésta información es fundamental a la hora de tomar decisiones en la práctica para configurar de la manera más adecuada una red de área local.

Añadido a esto, a medida que las redes crecen y muchas organizaciones agregan cientos e incluso miles de dispositivos a su red, es necesario implementar jerarquías de más de dos niveles. Por ello aparece la subdivisión de redes, creando subgrupos adicionales dentro de una red IP, lo que facilita una entrega más rápida de los paquetes y proporciona más características de filtrado, minimizando el tráfico local.

Se analizan las técnicas más utilizadas para la creación de subredes dentro de una red local, delimitando así dominios de difusión, mejorando el rendimiento y aumentando la seguridad de la misma. Gran parte del desarrollo de ésta unidad se centra en realizar actividades escritas, simuladas y de montaje sobre el diseño y la configuración lógica de la red de área local.

8.3.1 Presentación teórica

CURSO

Redes de Área Local

UNIDAD 3

Instalación y configuración de los equipos de red

Redes de Área Local
Olga Minguet
1

UD3. Instalación y configuración de los equipos de red

ÍNDICE

1. Los protocolos básicos en TCP/IP
2. Conversión (binario-decimal)
3. El direccionamiento de red en TCP/IP
4. Cálculo de direcciones IP
5. Subnetting
6. Subnetting con VLSM
7. Protocolos TCP/IP de nivel superior
8. Utilidades propias de redes TCP/IP

Redes de Área Local
Olga Minguet
2

UD3. Instalación y configuración de los equipos de red

ÍNDICE

1. Los protocolos básicos en TCP/IP

- A) Protocolo IP
 - B) Protocolo ICMP
 - C) Protocolo TCP
 - D) Protocolo UDP
 - E) Protocolo ARP
 - F) Protocolo RARP
2. Conversión (binario-decimal)
3. El direccionamiento de red en TCP/IP
4. Cálculo de direcciones IP
5. Subnetting
6. Subnetting con VLSM
7. Protocolos TCP/IP de nivel superior
8. Utilidades propias de redes TCP/IP

Redes de Área Local
Olga Minguet
3

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

LA FAMILIA DE PROTOCOLOS TCP/IP

- Es una familia de protocolos en la que destaca especialmente:
 - el **protocolo IP**, en la capa de red
 - y el **protocolo TCP**, en la capa de transporte.
- Hay muchos más protocolos, pero la importancia de estos dos ha hecho que a toda la arquitectura de protocolos se le llame “familia de protocolos TCP/IP”.
- Aunque TCP/IP no sigue la arquitectura OSI exactamente, se pueden establecer paralelismos:

Modelo OSI	
Aplicación	Presentación
Sección	Sección
Transporte	Transporte
Red	Red
Enlace	Enlace
Física	Física

Modelo TCP/IP	
Aplicación	Aplicación
Transporte	Transporte
Internet	Internet
Interfaz de red	Interfaz de red

Protocolos TCP/IP					
NetBIOS	FTP	SMTP	...	SNMP	RPC
TCP, UDP					
IP					
ARP					
ICMP					
Interfaz de red					

Sistema de direccionamiento	
Direcciones Específicas: URL (http://google.es)	
Fuente (http: TCP-30)	
Direcciones IP (192.168.15.12)	
Direcciones MAC (08-00-2B-12-4E-F2)	

Redes de Área Local
Olga Minguet
4

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

A) Protocolo IP

- **IP (Internet Protocol)** es el protocolo de nivel de red en ARPANET, el sistema de comunicaciones que tradicionalmente han utilizado los sistemas UNIX.
- Proporciona un sistema de direcciones para que cada nodo de la red quede identificado por una dirección de **cuatro números enteros** separados por puntos (o 32 bits) denominada **dirección IP o de nivel 3**.

Ejemplo: 192.168.15.159

Se distingue de la dirección MAC (física) o de nivel 2 que se compone de 12 dígitos hexadecimales.

- Cada bloque de datos, que en este nivel se denominan **segmentos**, debe ser transferido a través de la red en forma de datagramas.

Redes de Área Local Olga Minguet 5

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

A) Protocolo IP

- Para llevar a cabo este transporte, normalmente la **capa de red debe fraccionar los datagramas** en un conjunto de paquetes IP, que deben ser ensamblados en el destino para que el mensaje sea al final reconstruido con fidelidad.
- IP es un **protocolo no orientado a la conexión**, es decir, se transmite los datos, sin tener que asegurarse de que el receptor esté disponible y listo para recibirlos. Además cada paquete puede seguir una ruta distinta, el protocolo de capa superior TCP se encarga de la gestión a la hora de reconstruir la información.



Redes de Área Local Olga Minguet 6

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

B) Protocolo ICMP

- **ICMP (Internet Control Message Protocol)** es el protocolo de mensajes de control entre redes. Es un protocolo que expresa en un único paquete algún evento que se produce en la red. Por tanto, se trata de un protocolo de *supervisión*.
- Cualquier TCP/IP debe utilizar el protocolo ICMP.
- En ICMP son posibles, entre otros, mensajes como los siguientes:
 - Destino inalcanzable.
 - Tiempo excedido.
 - Enfriar fuente.
 - Redirecciones.

Redes de Área Local Olga Minguet 7

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

C) Protocolo TCP

- **TCP (Transmission Control Protocol)** es el protocolo de mensajes de control de transmisión.
- Fue especialmente diseñado para realizar conexiones en redes con poca fiabilidad en las transmisiones. Es un protocolo de capa de transporte adecuado para **proporcionar fiabilidad a IP**.
- La fiabilidad en TCP tiene un precio, ya que supone:
 - grandes cabeceras de mensajes
 - y necesidad de confirmaciones de mensajes para asegurar las comunicaciones.
 Estas confirmaciones generan un tráfico sobreañadido en la red que ralentiza las transmisiones, pero aportan fiabilidad.

Redes de Área Local Olga Minguet 8

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

D) Protocolo UDP

- **UDP (User Datagram Protocol)** o protocolo de datagrama de usuario. Es un protocolo de **transporte sin conexión**, es decir, permite la transmisión de mensajes sin necesidad de establecer ninguna conexión y, por tanto, sin garantías de entrega.
- Actúa simplemente como una interfaz entre los procesos de los usuarios de la red y el protocolo IP. Se utiliza en transmisiones rápidas que no necesitan seguridad en la transmisión.
- UDP no impone el uso de confirmaciones, puesto que su objetivo no es la seguridad, y esto hace de él un protocolo de transporte de mucho mayor rendimiento que TCP, aunque más inseguro.

Redes de Área Local Olga Minguet 9

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

D) Protocolo UDP

TCP	UDP
Es un protocolo confiable	No es confiable
Orientado a la conexión	No establece una conexión inicial
Lleva gestión de las retransmisiones y control de flujo	No gestiona retransmisiones
Secuencia numéricamente los segmentos (paquetes de datos enviados o recibidos)	No gestiona un secuenciamiento de segmentos
Admite segmentos de acuse de recibo	No incorpora acuse de recibo

Redes de Área Local Olga Minguet 10

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

E) Protocolo ARP

- **ARP (Address Resolution Protocol)** o protocolo de resolución de direcciones. Es un protocolo de la capa de enlace de datos que es el responsable de encontrar la **dirección física (dirección MAC)** que corresponde a una determinada **dirección lógica (dirección IP)**.
- ARP funciona del siguiente modo:

Redes de Área Local Olga Minguet 11

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

E) Protocolo ARP

- 1) Cuando un host quiere transmitir un paquete IP necesita averiguar la dirección MAC del host destinatario cuya dirección es la dirección de destino del campo "dirección de destino del paquete IP".
- 2) Para ello genera un paquete de petición ARP que difunde por toda la red. Todos los nodos de la red detectan este paquete y solo aquel host que tiene la dirección IP encapsulada en el paquete ARP contesta con otro paquete ARP de respuesta con su dirección MAC.
- 3) De este modo el host emisor relaciona dirección IP y dirección MAC, guardando estos datos en una tabla residente en memoria para su uso en transmisiones posteriores.

Redes de Área Local Olga Minguet 12

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP

F) Protocolo RARP

- **RARP (Reverse ARP)** . Es el protocolo inverso del ARP, es decir, localiza la dirección lógica (*dirección IP*) de un nodo a partir de la dirección física (*MAC*) del mismo.
- Fundamentalmente es utilizado en estaciones de trabajo sin disco, que han conseguido su sistema operativo a través de la red.

Redes de Área Local Olga Minguet 13

UD3. Instalación y configuración de los equipos de red

1. Los protocolos básicos en TCP/IP



Redes de Área Local Olga Minguet 14

UD3. Instalación y configuración de los equipos de red



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

➤ Actividad 1

Redes de Área Local Olga Minguet 15

UD3. Instalación y configuración de los equipos de red

ÍNDICE

1. Los protocolos básicos en TCP/IP
2. Conversión (binario-decimal)
3. El direccionamiento de red en TCP/IP
4. Cálculo de direcciones IP
5. Subnetting
6. Subnetting con VLSM
7. Protocolos TCP/IP de nivel superior
8. Utilidades propias de redes TCP/IP

Redes de Área Local Olga Minguet 16

UD3. Instalación y configuración de los equipos de red

2. Conversión -Binario a decimal-

- En el Sistema Decimal podemos escribir números como 451, 672, 30, etc. Es decir, podemos formar cualquier combinación de los dígitos del 0 al 9 (cifras).
- En el Sistema Binario podemos escribir números como 01100111, 110, 011, 1, etc. Es decir, podemos formar cualquier combinación de los dígitos 0 y 1 (bits).
- Cada número en Sistema Decimal tiene su equivalente en Sistema Binario, y viceversa. Pero, ¿Cómo se convierten los números de Sistema Binario a Sistema Decimal?
- Vamos a convertir el número **11001011** a Sistema decimal:

7	6	5	4	3	2	1	0	exponentes
1	1	0	0	1	0	1	1	

$$1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 128 + 64 + 8 + 2 + 1 = 203$$

Redes de Área Local Olga Minguet 17

UD3. Instalación y configuración de los equipos de red

2. Conversión -Binario a decimal-

128	64	32	16	8	4	2	1	Answers	Scratch Area
1	0	0	1	0	0	1	0	146	128 64
0	1	1	1	0	1	1	1	119	16 32
1	1	1	1	1	1	1	1	255	16 4
1	1	0	0	0	1	0	1	197	2
1	1	1	1	0	1	1	0	246	119
0	0	0	1	0	0	1	1	19	
1	0	0	0	0	0	0	1	129	
0	0	1	1	0	0	0	1	49	
0	1	1	1	1	0	0	0	120	
1	1	1	1	0	0	0	0	240	
0	0	1	1	1	0	1	1	59	
0	0	0	0	0	1	1	1	7	

Redes de Área Local Olga Minguet 18

UD3. Instalación y configuración de los equipos de red

2. Conversión -Decimal a binario-

- En el Sistema Decimal podemos escribir números como 451, 672, 30, etc. Es decir, podemos formar cualquier combinación de los dígitos del 0 al 9 (cifras).
- En el Sistema Binario podemos escribir números como 01100111, 110, 011, 1, etc. Es decir, podemos formar cualquier combinación de los dígitos 0 y 1 (bits).
- Cada número en Sistema Decimal tiene su equivalente en Sistema Binario, y viceversa. Pero, ¿Cómo se convierten los números de Sistema Binario a Sistema Decimal?
- Vamos a convertir el número **77** a Sistema Binario:

Redes de Área Local Olga Minguet 19

UD3. Instalación y configuración de los equipos de red

2. Conversión -Decimal a binario-

128	64	32	16	8	4	2	1	= 255	Scratch Area
1	1	1	0	1	1	1	0	238	238 34
0	0	1	0	0	0	1	0	34	-128 -32
0	1	1	1	1	0	1	1	123	110 2
0	0	1	1	0	0	1	0	50	-64 -2
1	1	1	1	1	1	1	1	255	46 -2
1	1	0	0	1	0	0	0	200	-32 14
0	0	0	0	1	0	1	0	10	-8
1	0	0	0	1	0	1	0	138	6
									-4
									2
									-2
									0

Redes de Área Local Olga Minguet 20

UD3. Instalación y configuración de los equipos de red



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 2

Redes de Área Local Olga Minguet 21

UD3. Instalación y configuración de los equipos de red

ÍNDICE

1. Los protocolos básicos en TCP/IP
2. Conversión (binario-decimal)
3. El direccionamiento de red en TCP/IP
 - A) Clases de redes
 - B) Máscaras de subred
4. Cálculo de direcciones IP
5. Subnetting
6. Subnetting con VLSM
7. Protocolos TCP/IP de nivel superior
8. Utilidades propias de redes TCP/IP

Redes de Área Local Olga Minguet 22

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

- El sistema de direccionamiento IP está ampliamente aceptado por la comunidad mundial.
- Cada dirección IP consta de **32 bits** agrupados en **grupos de 8 bits**.
- Una dirección IP se expresa con **cuatro números decimales** separados por puntos.
- Cada uno de estos números varía entre **0 y 255**, aunque hay algunas restricciones.
- Un ejemplo de dirección IP sería 128.100.3.67

Redes de Área Local Olga Minguet 23

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

- Cada dirección IP indica una red y un host dentro de esa red.
- Con los primeros bits de cada dirección se averigua el tipo de subred (Clase) de que se trata y su dirección concreta. La Clase definirá qué nos va a decir cada byte (8 bits) de la dirección IP.
- Los bits restantes codifican el host de que se trata dentro de esa subred.

Redes de Área Local Olga Minguet 24

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

0	8	16	24	32	
0	Red ID (bits 2 al 8)	ID de host (24 bits)			Dirección clase A
1 0	Red ID (bits 3 al 16)	ID de host (16 bits)			Dirección clase B
1 1 0	Red ID (bits 4 al 24)	ID de host (8 bits)			Dirección clase C
1 1 1 0	Grupo de direcciones de multidifusión (28 bits)				Dirección clase D
1 1 1 1	ID de direcciones experimentales (bits 5 al 32)				Dirección clase E

Redes de Área Local Olga Minguet 25

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

CLASE A } LAN & WAN

CLASE B } LAN & WAN

CLASE C } Multicasting

CLASE D } Multicasting

CLASE E } Investigación y desarrollo

CLASE A 0 127.255.255.255

CLASE B 10 128.0.0.0 hasta 191.255.255.255

CLASE C 110 192.0.0.0 hasta 223.255.255.255

CLASE D 1110 224.0.0.0 hasta 239.255.255.255

Bit para red (orange square)
Bit para host (green square)
Dirección de multidifusión (blue square)

Redes de Área Local Olga Minguet 26

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

Redes de Área Local Olga Minguet 27

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

Redes de Clase A

0	8	16	24	32
0	Red ID (bits 2 al 8)	ID de host (24 bits)		

- El primer bit siempre es **0**
- Los **7 bits** siguientes codifican la **subred**.
Los valores posibles para la subred varían entre 1 y 128, que coincide con el valor del primer byte de la dirección, es decir, **hay 128 subredes** posibles del tipo A.
Direcciones desde **0.x.x.x (00000000.x.x.x)** hasta **127.x.x.x (01111111.x.x.x)**
- Los **24 bits** restantes codifican la identificación del **host** dentro de esa subred. Cada una de ellas puede contener **16.777.214 hosts** distintos.
- Este sistema de direccionamiento se utiliza, por tanto, para **subredes muy grandes**.

Redes de Área Local Olga Minguet 28

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

Redes de Clase B



- Los dos primeros bits de la dirección son **10**
- Los **14 bits** siguientes codifican la **subred**.

Los valores posibles para la subred varían entre 128 y 191 para el primer byte de la dirección, por tanto son posibles **16.384 subredes** posibles del tipo B.

Direcciones desde **128.x.x.x** (10000000.x.x.x) hasta **191.x.x.x** (10111111.x.x.x)

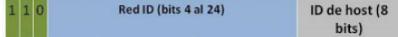
- Los **16 bits** restantes codifican la identificación del **host** dentro de esa subred. Cada una de ellas puede contener **65.534 hosts** distintos.

Redes de Área Local Olga Minguet 29

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

Redes de Clase C



- Tienen sus tres primeros bits con el valor **110**
- Los **21 bits** siguientes codifican la **subred**.

Es posible codificar **2.097.152 subredes** posibles del tipo C.

Direcciones desde **192.x.x.x** (11000000.x.x.x) hasta **223.x.x.x** (11011111.x.x.x)

- Los **8 bits** restantes codifican la identificación del **host** dentro de esa subred. Cada una de ellas puede contener **254 hosts** distintos.

Redes de Área Local Olga Minguet 30

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP



Redes de Clase D

- Cuando el campo de dirección **comienza** por la secuencia **1110**, se entiende que los 28 bits restantes codifican una dirección de **multidifusión**, es decir, una dirección especial en donde **el destinatario no es único**.

Direcciones desde **224.x.x.x** (11100000.x.x.x) hasta **239.x.x.x** (11101111.x.x.x)

Redes de Clase E

- Las direcciones **comienzan** por **1111** se reservan para protocolos especiales como los de administración de grupos de Internet, multitransmisión y otras futuras implementaciones o uso experimental.

Direcciones desde **240.x.x.x** (11110000.x.x.x) hasta **255.x.x.x** (11111111.x.x.x)

Redes de Área Local Olga Minguet 31

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

Usos específicos

- El valor **127** para el **primer byte** de una dirección IP está reservado para pruebas de bucle cerrado (retroalimentación), es decir, para las comunicaciones entre procesos dentro de la misma máquina.
- La Autoridad de Asignación de Números de Internet (IANA) reserva tres bloques del espacio de direcciones del protocolo de Internet (IP) para intrarredes **privadas**. La tabla siguiente muestra qué bloques de la dirección reserva la IANA:

Clase de red	Inicio del bloque de dirección	Fin del bloque de dirección
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Direcciones reservadas para uso privado de Internet (intranet)

Redes de Área Local Olga Minguet 32

UD3. Instalación y configuración de los equipos de red



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 3
- Actividad 4

Redes de Área Local Olga Minguet 33

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

ANEXO: IPv4 vs IPv6

- Al actual protocolo se le suele llamar **IPv4** para distinguirlo de otra especificación que se está implantando, el protocolo **IPv6**.
- Con **IPv4** se utilizan direcciones de red de **32 bits**, lo que es claramente insuficiente cuando todas las redes se integran entre sí, como en el caso de Internet. IPv4: 192.168.0.1
- Aunque tiene muchas más ventajas añadidas en las que aquí no entraremos, **IPv6** viene a resolver este asunto, pues su sistema de direccionamiento es de **128 bits**. Gran parte de los sistemas operativos modernos así como los dispositivos de red ya vienen preparados para la migración de IPv4 a IPv6. IPv6: 2607:f0d0:4545:3:200:f8ff:fe21:67cf

- Total de espacio IPv4: 4,294,967,296 direcciones.
- Total de espacio IPv6: 340,282,366,920,938,463,463,374,607,431,768,211,456 direcciones.

Redes de Área Local Olga Minguet 34

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

B) Máscaras de subred

- Una máscara de subred es una secuencia de **32 bits** (4 bytes) que sirve para distinguir con facilidad qué parte de una dirección codifica la subred (una subdivisión o grupo de la red total) y qué parte el host.
- Una máscara se construye poniendo:
 - a 1 los bits que pertenecen a la subred
 - y a 0 los bits que pertenecen a la identificación del host.
- Este modo de asignación permite multiplicar extraordinariamente los distintos tipos de subredes.
- Son posibles combinaciones cualesquiera de los bits para generar subredes y host dentro de las subredes siempre que tanto los 1's como los 0's aparezcan consecutivos.

Redes de Área Local Olga Minguet 35

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

B) Máscaras de subred

- subred de clase A
máscara 11111111 00000000 00000000 00000000 (255.0.0.0)
- subred de clase B
máscara 11111111 11111111 00000000 00000000 (255.255.0.0)
- subred de clase C
máscara 11111111 11111111 11111111 00000000 (255.255.255.0)

Redes de Área Local Olga Minguet 36

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

B) Máscaras de subred: Notación CIDR

- CIDR (Classless Inter-Domain Routing), Encaminamiento Inter-Dominios sin Clases
- Frecuentemente, para facilitar la notación, suele expresarse la dirección IP en formato CIDR, que consiste en escribir la dirección IP en su forma habitual seguida de otro entero cuyo valor es el de la máscara, separados por el símbolo /
- Ejemplo: **128.100.3.67/24**
 Significaría que el interfaz de red posee:
 -la dirección IP 128.100.3.67
 -tiene una máscara 255.255.255.0 (24 "unos" seguidos de 8 "ceros")
 Por tanto, pertenece a la red 128.100.3.0

Redes de Área Local Olga Minguet 37

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

B) Máscaras de subred: Notación CIDR

- Los posibles valores que puede tomar una máscara por defecto son:

Clase	Bits	IP Subred	IP Broadcast	Máscara en decimal	CIDR
A	0000	0.0.0.0	127.255.255.255	255.0.0.0	/8
B	1000	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	1100	192.0.0.0	223.255.255.255	255.255.255.0	/24
D	1110	224.0.0.0	238.255.255.255	255.255.255.255	/32
E	1111	240.0.0.0	255.255.255.254	255.255.255.255	/64

Redes de Área Local Olga Minguet 38

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP



Redes de Área Local Olga Minguet 39

UD3. Instalación y configuración de los equipos de red

3. El direccionamiento de red en TCP/IP

En resumen:

- **Dirección IP:** conjunto de 4 números de 8 bits (32 bits en total) que identifican unívocamente la dirección de un ordenador en una red TCP/IP.
- **Máscara IP:** es una secuencia de unos y ceros, ambos contiguos, que sirve para denotar en las redes TCP/IP qué identifica la red (secuencia inicial de unos) y qué la subred o conjunto de nodos (secuencia final de ceros).
- **CIDR:** es una mejora del sistema de direccionamiento IP.

Redes de Área Local Olga Minguet 40

UD3. Instalación y configuración de los equipos de red



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 5

Redes de Área Local Olga Minguet 41

UD3. Instalación y configuración de los equipos de red

ÍNDICE

1. Los protocolos básicos en TCP/IP
2. Conversión (binario-decimal)
3. El direccionamiento de red en TCP/IP
4. Cálculo de direcciones IP
5. Subnetting
6. Subnetting con VLSM
7. Protocolos TCP/IP de nivel superior
8. Utilidades propias de redes TCP/IP

Redes de Área Local Olga Minguet 42

UD3. Instalación y configuración de los equipos de red

4. Cálculo de direcciones IP

Para realizar todos los cálculos referentes a direcciones IP y redes vamos a trabajar sobre un Caso práctico. Generalmente nos darán la dirección IP del equipo y, o la máscara de red, o la clase a la cual pertenece. Con estos datos ya podemos obtener (según nos soliciten):

- Máscara de red o la Clase, según la que nos hayan dado en el enunciado
- Dirección de red
- Dirección de broadcast
- Dirección del *primer dispositivo* de dicha red, o primer host disponible.
- Dirección del *último dispositivo* de la red, o último host disponible.

NOTA: Dirección broadcast o dirección de difusión, se utiliza cuando un nodo quiere enviar datos a todos los nodos de su red lógica.

Redes de Área Local Olga Minguet 43

UD3. Instalación y configuración de los equipos de red

4. Cálculo de direcciones IP

Caso práctico 1

Supongamos un caso práctico en el que se dispone de un nodo con:

- dirección IP **192.168.15.12**
- máscara de red **192.168.15.12/24** en notación CIDR

Obtener las 4 direcciones IP que definen completamente una red.

Redes de Área Local Olga Minguet 44

UD3. Instalación y configuración de los equipos de red

4. Cálculo de direcciones IP

Caso práctico 1

Con los datos obtenidos podemos especificar:

Dirección IP: 192.168.15.12
 Máscara por defecto de red: (/24) 255.255.255.0 } Enunciado

Clase de red: Clase C

Dirección de red: 192.168.15.0
 Dirección de broadcast: 192.168.15.255
 Dirección del primer dispositivo: 192.168.15.1
 Dirección del último dispositivo: 192.168.15.254

Redes de Área Local Olga Minguet 45

UD3. Instalación y configuración de los equipos de red

4. Cálculo de direcciones IP

Caso práctico 1

192.168.15.12/24

IP red	IP primer host	IP último host	IP broadcast
192.168.15.0	192.168.15.1	192.168.15.254	192.168.15.255

Redes de Área Local Olga Minguet 46

UD3. Instalación y configuración de los equipos de red

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 6
- Actividad 7
- Actividad 8

Redes de Área Local Olga Minguet 47

UD3. Instalación y configuración de los equipos de red

5. Subnetting

Concepto de Subnetting

- A veces interesa que la división que produce una máscara de red entre la parte de nodo y la parte de red no sea tan generosa como la que proporcionan las redes de clase A, B y C.
- Por ejemplo, podría darse el caso (habitual) de una empresa que ha contratado una red de direcciones IP públicas de clase C para repartir entre todos los departamentos de que consta. Donde cada departamento tiene, a su vez, muchos host.
- Esta empresa tiene que hacer una subdivisión del direccionamiento IP contratado, confeccionando un conjunto de **redes más pequeñas** para cada departamento.

Redes de Área Local Olga Minguet 48

UD3. Instalación y configuración de los equipos de red

5. Subnetting

Concepto de Subnetting

- A veces interesa que la división que produce una máscara de red entre la parte de nodo y la parte de red no sea tan generosa como la que proporcionan las redes de clase A, B y C.
- Por ejemplo, podría darse el caso (habitual) de una empresa que ha contratado una red de direcciones IP públicas de clase C para repartir entre todos los departamentos de que consta. Donde cada departamento tiene, a su vez, muchos host.
- Esta empresa tiene que hacer una subdivisión del direccionamiento IP contratado, confeccionando un conjunto de **redes más pequeñas** para cada departamento.

A esta operación de **fraccionamiento del sistema de direccionamiento se le llama Subnetting.**

Redes de Área Local Olga Minguet 49

UD3. Instalación y configuración de los equipos de red

5. Subnetting

Concepto de Subnetting

- La técnica de Subnetting consiste en crear máscaras de **mayor número de bits puestos a uno** que las que proporcionan las máscaras por defecto de Clase.
- Esta división genera un conjunto de **subredes**, y cada una de estas subredes tiene:
 - su propio sistema de direccionamiento,
 - su nueva máscara,
 - su dirección de red
 - y su dirección de difusión.
- Vamos a verlo con un caso práctico:

Redes de Área Local Olga Minguet 50

UD3. Instalación y configuración de los equipos de red

5. Subnetting

Caso práctico 2

Supongamos que tenemos la siguiente IP de la red de Clase C: **192.168.15.0** y que tendremos que repartir en **tres subrangos** de red porque hay tres departamentos. A cada departamento le asignaremos una de estas subredes.

Para resolverlo debemos seguir los siguientes pasos:

1º) Debemos calcular cuántos **bits de la máscara** tendremos que *modificar* para poder direccionar las 3 subredes que nos piden. Para ello,

$$2^n \geq n^{\circ} \text{ subredes que nos piden}$$

Siendo "n" el nº de 1's que debemos añadir en la máscara por defecto. Por tanto, la **nueva máscara** de subred o máscara adaptada será:

$$255.255.255.1100\ 0000 = 255.255.255.192$$

Redes de Área Local Olga Minguet 51

UD3. Instalación y configuración de los equipos de red

5. Subnetting

Caso práctico 2

2º) Con esto, podemos calcular en **número de hosts** que pueden direccionarse en cada subred. Para ello, se toman los ceros que nos han quedado (restantes) en la nueva máscara y se aplica la ecuación anterior, pero ahora:

$$2^m - 2 = n^{\circ} \text{ de hosts direccionables en cada subred}$$

En la ecuación restamos 2 porque la primera ni la última dirección obtenidas son **útiles** para host.

Por tanto, para nuestro caso práctico, el número de hosts válidos en cada subred será:

$$2^6 - 2 = 32 - 2 = 30 \text{ hosts/subred}$$

Redes de Área Local Olga Minguet 52

UD3. Instalación y configuración de los equipos de red

5. Subnetting

Caso práctico 2

3º) Con los datos obtenidos (nº de subredes a obtener, máscara de subred y nº de direcciones útiles para host en cada subred) ya podemos calcular las 4 direcciones IP que definen totalmente cada subred:

- IP subred (la dirección IP que identifica la red)
- IP de Primer host direccionable
- IP de Último host direccionable
- IP de Broadcast o difusión

Redes de Área Local Olga Minguet 53

UD3. Instalación y configuración de los equipos de red

5. Subnetting

Caso práctico 2

3º) Con los datos obtenidos (nº de subredes a obtener, máscara de subred y nº de direcciones útiles para host en cada subred) ya podemos calcular : **las 4 direcciones IP que definen totalmente cada subred:**

Subred	IP red	IP primer host	IP último host	IP broadcast
1	192.168.15 .0000 0000	192.168.15 .0000 0001	192.168.15 .0011 1110	192.168.15 .0011 1111
2	192.168.15 .0100 0000	192.168.15 .0100 0001	192.168.15 .0111 1110	192.168.15 .0111 1111
3	192.168.15 .1000 0000	192.168.15 .1000 0001	192.168.15 .1011 1110	192.168.15 .1011 1111

Redes de Área Local Olga Minguet 54

UD3. Instalación y configuración de los equipos de red

5. Subnetting

Caso práctico 2

3º) Con los datos obtenidos (nº de subredes a obtener, máscara de subred y nº de direcciones útiles para host en cada subred) ya podemos calcular : **las 4 direcciones IP que definen totalmente cada subred:**

Subred	IP red	IP primer host	IP último host	IP broadcast
1	192.168.15.0	192.168.15.1	192.168.15.30	192.168.15.31
2	192.168.15.32	192.168.15.33	192.168.15.62	192.168.15.63
3	192.168.15.64	192.168.15.65	192.168.15.94	192.168.15.95
4	<i>Subred sobrante, reservada para futuras ampliaciones</i>			

Redes de Área Local Olga Minguet 55

UD3. Instalación y configuración de los equipos de red



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- **Actividad 9**
- **Actividad 10**
- **Actividad 11**

Redes de Área Local Olga Minguet 56

UD3. Instalación y configuración de los equipos de red

6. Subnetting con VLSM

- El subnetting con **VLSM** (Variable Length Subnet Mask) o máscara de subred de longitud variable, es uno de los métodos que se implementó para **evitar el agotamiento de direcciones IPv4** permitiendo un mejor aprovechamiento y optimización del uso de direcciones. Es el resultado del proceso por el cual se divide una red o subred en subredes más pequeñas cuyas máscaras son diferentes según a las necesidades de hosts por subred.
- A diferencia del subnetting, que genera una máscara común y cantidad de hosts iguales a todas las subredes, el proceso de VLSM toma una dirección de red o subred y divide en subredes más pequeñas, adaptando las máscaras según las necesidades de hosts de cada subred. Generando una máscara diferente para las distintas subredes de una red.

Esto permite no desaprovechar un gran número de direcciones.

Redes de Área Local

Olga Minguet

57

UD3. Instalación y configuración de los equipos de red

6. Subnetting con VLSM

Caso práctico 3

Dada la red 192.168.0.0/24, desarrolla un esquema de direccionamiento, usando la técnica VLSM, que cumpla con los siguientes requerimientos:

- Una subred de 20 hosts para ser asignada a la VLAN de Profesores.
- Una subred de 80 hosts para ser asignada a la VLAN de Estudiantes.
- Una subred de 20 hosts para ser asignada a la VLAN de Invitados.
- Tres subredes de 2 hosts para ser asignada a los enlaces entre enrutadores.

Pasos a seguir:

- 1) La máscara de red es /24, esto es **255.255.255.0**
- 2) Ordenamos las subredes en **orden decreciente**:
Subred de 80 > subredes de 20 > subredes de 2

Redes de Área Local

Olga Minguet

58

UD3. Instalación y configuración de los equipos de red

- 3) Primera Subred: Para **80 hosts** necesito **7 bits**

Cálculo	Nº de hosts
$2^6 - 2$	62
$2^7 - 2$	126
$2^8 - 2$	254

Recuerda que se restan 2 (dirección de red y broadcast)

Por lo tanto de los últimos 8 bits dedicados al host, con 7 bits me bastarían para codificarlos, con lo que el primer bit lo uso para la nueva máscara y los 7 restantes para el host

La nueva máscara será: /24+1 = /25

Máscara: 255.255.255.10000000 = 255.255.255.128

La primera subred será: 192.168.0.00000000 = 192.168.0.0/25

El primer host será: 192.168.0.00000001 = 192.168.0.1

El último host será: 192.168.0.01111110 = 192.168.0.126

Dirección broadcast: 192.168.0.01111111 = 192.168.0.127

Redes de Área Local

Olga Minguet

59

UD3. Instalación y configuración de los equipos de red

- 4) Segunda Subred: Para **20 hosts** necesito **5 bits**

Cálculo	Nº de hosts
$2^4 - 2$	14
$2^5 - 2$	30
$2^6 - 2$	62

Recuerda que se restan 2 (dirección de red y broadcast)

Por lo tanto de los últimos 8 bits dedicados al host, con 5 bits me bastarían para codificarlos, con lo que los tres primeros bits los uso para la nueva máscara y los 5 restantes para el host

La nueva máscara será: /24+3 = /27

Máscara: 255.255.255.11100000 = 255.255.255.224

La segunda subred será: 192.168.0.10000000 = 192.168.0.128/27

El primer host será: 192.168.0.10000001 = 192.168.0.129

El último host será: 192.168.0.10011110 = 192.168.0.158

Dirección broadcast: 192.168.0.10011111 = 192.168.0.159

Redes de Área Local

Olga Minguet

60

UD3. Instalación y configuración de los equipos de red

6. Subnetting con VLSM

Caso práctico 3

5) Tercera Subred: Igual que antes: 5 bits y 30 hosts

Máscara: 255.255.255.11100000 = 255.255.255.224
 La tercera subred será: 192.168.0.10100000 = 192.168.0.160/27
 El primer host será: 192.168.0.10100001 = 192.168.0.161
 El último host será: 192.168.0.10111110 = 192.168.0.190
 Dirección broadcast: 192.168.0.10111111 = 192.168.0.191

Redes de Área Local Olga Minguet 61

UD3. Instalación y configuración de los equipos de red

6) Enlace 1: Para **2 hosts** necesito **2 bits**

Cálculo	Nº de hosts
$2^1 - 2$	0
$2^2 - 2$	2
$2^3 - 2$	6

Recuerda que se restan 2 (dirección de red y broadcast)

Por lo tanto de los últimos 8 bits dedicados al host, con 2 bits me bastarían para codificarlos, con lo que los 6 primeros bits los uso para la nueva máscara y los 2 restantes para el host

La nueva máscara será: /24+6 = /30
 Máscara: 255.255.255.11111100 = 255.255.255.252
 La cuarta subred será: 192.168.0.11000000 = 192.168.0.192/30
 El primer host será: 192.168.0.11000001 = 192.168.0.193
 El último host será: 192.168.0.11000010 = 192.168.0.194
 Dirección broadcast: 192.168.0.11000011 = 192.168.0.195

Redes de Área Local Olga Minguet 62

UD3. Instalación y configuración de los equipos de red

7) Enlace 2: Igual que antes: **2 hosts y 2 bits**

Máscara: 255.255.255.11111100 = 255.255.255.252
 La quinta subred será: 192.168.0.11000100 = 192.168.0.196/30
 El primer host será: 192.168.0.11000101 = 192.168.0.197
 El último host será: 192.168.0.11000110 = 192.168.0.198
 Dirección broadcast: 192.168.0.11000111 = 192.168.0.199

8) Enlace 3: Igual que antes: **2 hosts y 2 bits**

Máscara: 255.255.255.11111100 = 255.255.255.252
 La sexta subred será: 192.168.0.11001000 = 192.168.0.200/30
 El primer host será: 192.168.0.11001001 = 192.168.0.201
 El último host será: 192.168.0.11001010 = 192.168.0.202
 Dirección broadcast: 192.168.0.11001011 = 192.168.0.203

Redes de Área Local Olga Minguet 63

UD3. Instalación y configuración de los equipos de red

Red	Dir	Broadcast	Rango	Máscara
Estudiantes(80)	192.168.0.0/25	192.168.0.127	.1-.126	255.255.255.128
Profesores(20)	192.168.0.128/27	192.168.0.159	.129-158	255.255.255.224
Invitados(20)	192.168.0.160/27	192.168.0.191	.161-190	255.255.255.224
Enlace 1(2)	192.168.0.192/30	192.168.0.195	.193-194	255.255.255.252
Enlace 2(2)	192.168.0.196/30	192.168.0.199	.197-198	255.255.255.252
Enlace 3(2)	192.168.0.200/30	192.168.0.203	.201-202	255.255.255.252

Se puede observar que los rangos de direcciones asignados son continuos y que queda disponible para crecimiento futuro un rango de direcciones desde 204 en adelante.

Redes de Área Local Olga Minguet 64

UD3. Instalación y configuración de los equipos de red

ÍNDICE

1. Los protocolos básicos en TCP/IP
2. Conversión (binario-decimal)
3. El direccionamiento de red en TCP/IP
4. Cálculo de direcciones IP
5. Subnetting
6. Subnetting con VLSM
7. Protocolos TCP/IP de nivel superior

FTP, HTTP, SNMP, RPC, SMTP, POP, IMAP

8. Utilidades propias de redes TCP/IP

Redes de Área Local Olga Minguet 65

UD3. Instalación y configuración de los equipos de red

7. Protocolos TCP/IP de nivel superior

- En el nivel superior de la arquitectura TCP/IP hay una infinidad de protocolos. Aquí nos vamos a referir a los más comunes, pero existen casi tantos protocolos distintos como tipos de aplicaciones o servicios de nivel de aplicación.
- La mayor parte de los protocolos de nivel superior tienen asociado uno o más números de puerto en sus sockets de comunicación, por ejemplo, FTP-21, HTTP-80, SMTP-25, POP-110, etc., aunque esta asociación puede ser alterada por las aplicaciones o por el administrador de la red.

Redes de Área Local Olga Minguet 66

UD3. Instalación y configuración de los equipos de red

7. Protocolos TCP/IP de nivel superior

FTP	Es utilizado para la descarga o carga de ficheros en Internet. Define dos canales de comunicación, uno para el control de ésta y otro para la transferencia de datos.
HTTP	Es el protocolo utilizado por los navegadores para el acceso a las páginas web.
SNMP	Utilizado para la gestión de la red.
RPC	Se encarga de establecer diálogos entre las aplicaciones clientes y sus servicios. Se trata de un protocolo básico para la arquitectura de las aplicaciones cliente-servidor.
SMTP	Es el protocolo básico para el intercambio de mensajes de correo electrónico entre servidores de correo o el que usa la aplicación cliente de correo para enviar mensajes al servidor al que se conecta.
POP	Es el protocolo de comunicaciones de alto nivel que se encarga de descargar mensajes de correo electrónico desde el servidor de correo en donde se encuentra el buzón a la bandeja de entrada del cliente de correo. La versión actual es POP3
IMAP	Semejante a POP, pero más recomendable en situaciones de congestión.

Redes de Área Local Olga Minguet 67

UD3. Instalación y configuración de los equipos de red

ÍNDICE

1. Los protocolos básicos en TCP/IP
2. Conversión (binario-decimal)
3. El direccionamiento de red en TCP/IP
4. Cálculo de direcciones IP
5. Subnetting
6. Subnetting con VLSM
7. Protocolos TCP/IP de nivel superior
8. Utilidades propias de redes TCP/IP

- A) nslookup
- B) ping
- C) arp
- D) ipconfig
- E) netstat
- F) tracert
- G) route
- H) ftp y tftp
- I) telnet y ssh

Redes de Área Local Olga Minguet 68

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

A) Utilidad nslookup

- (Name System Lookup) es una herramienta que permite consultar un servidor de nombres y obtener información relacionada con el dominio o nombre del host y así diagnosticar los eventuales problemas de configuración que pudieran haber surgido en el DNS (servicio de asignación de nombres a direcciones IP).
- Es un programa utilizado para saber si el DNS está resolviendo correctamente los nombres y las IP's.

Redes de Área Local Olga Minguet 69

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

A) Utilidad nslookup

Sintaxis. La forma común de utilizarlo es bajo la siguiente sintaxis:
>nslookup<dominio.com>

Al ejecutarlo, el resultado devuelve los siguientes componentes:

- ✓ Servidor: aquí nos indica el nombre del servidor DNS que utilizará la herramienta para hacer las consultas.
- ✓ Address: nos indica la dirección IP del servidor DNS que estamos usando.
- ✓ Respuesta no autoritativa: nos indica un servidor DNS que no es dueño del dominio que estamos buscando pero al que se puede consultar para obtener más información.
- ✓ Nombre: es el nombre del dominio que estamos buscando.
- ✓ Addresses: nos indica las direcciones IP que responden a este dominio que estamos buscando.

Redes de Área Local Olga Minguet 70

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

B) Utilidad ping

- Ping (Pocket Internet Groper, tanteo de paquetes de Internet) es una utilidad que sirve para enviar mensajes a una dirección de red concreta que se especifica como argumento con el fin de realizar un test a la red utilizando el protocolo ICMP.
- El nodo destinatario nos reenviará el paquete recibido para confirmarnos que se realiza correctamente el transporte entre los dos nodos. Además, proporciona información añadida sobre la red.
- Sintaxis. La forma común de utilizarlo es bajo la siguiente sintaxis:
>ping<dominio.com> ping <IP>

Redes de Área Local Olga Minguet 71

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

B) Utilidad ping

Cuando se ejecuta, ping proporciona una respuesta de este tipo:

```
Haciendo ping a dirección ip con 32 bytes de datos:
Respuesta desde 127.0.0.1: bytes=32 tiempo= <10 ms TTL=128
```

- ✓ TTL es el tiempo de vida del paquete enviado y su valor óptimo es 128.
- ✓ En la respuesta obtenida de ping pueden aparecer algunos de los siguientes errores:
 - "Red de destino inaccesible" significa que no existe ninguna ruta al destino.
 - "Ha terminado el tiempo de espera para esta solicitud" indica errores en la conexión.

Redes de Área Local Olga Minguet 72

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

B) Utilidad ping

- Ping puede configurar varios parámetros cuando se ejecuta desde la línea de comandos, por ejemplo, es posible indicarle, entre otros:
 - n: cuántos paquetes queremos enviar,
 - w: el tiempo de espera,
 - l: el tamaño de cada paquete enviado,
 - 6: usar IPv6. Si no se especifica lo contrario, siempre se supone que es la versión de la red es la 4 (IPv4).

Tendremos que recurrir a la ayuda del comando ping en cada sistema para asegurarnos de la sintaxis exacta de la orden. En Windows se obtiene escribiendo ping /help.

Redes de Área Local Olga Minguet 73

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

C) Utilidad arp

- ARP (Address Resolution Protocol), Protocolo de resolución de direcciones. Es una utilidad que sirve para asignar automáticamente direcciones IP a direcciones físicas (MAC).
- Muestra y modifica las tablas de traducción de direcciones IP a direcciones físicas.
- Con el comando arp -a se interroga al sistema mediante ARP cuáles son las direcciones IP que tiene resueltas, es decir, de las que conoce su dirección física, y cuál fue el tipo de asignación, dinámica o estática.
- Además, arp incorpora más opciones, entre las cuales destacamos: -d: borra el host especificado de la lista; -s: agrega el host y relaciona la dirección Internet a la Física.

Interfaz	192.168.1.107	---	0af		
Dirección de Internet				Dirección física	Tipo
192.168.1.1			5c-35-3b-0e-2a-00		dinámico
192.168.1.172			54-00-0e-45-0f-70		dinámico
192.168.1.211			3c-1b-0d-00-70-00		dinámico
192.168.1.255			ff-ff-ff-ff-ff-ff		estático
224.0.0.252			01-00-5e-00-00-5e		estático

Redes de Área Local Olga Minguet 74

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

D) Utilidad ipconfig (Windows) e ifconfig/iwconfig (Linux)

- Configura la dirección del host o bien proporciona información sobre la configuración actual.
- La utilidad equivalente en Linux es ifconfig para las redes cableadas e iwconfig para las redes inalámbricas, aunque la mayor parte de las distribuciones ya permiten configurar muchos de los parámetros que admiten a través de la interfaz gráfica.
- La ejecución del comando "ipconfig help" en Windows e "ifconfig -h" y "iwconfig -h" en Linux nos proporcionarán la ayuda necesaria para la utilización de la orden, ejemplos incluidos.
- En general, cualquiera de estas órdenes tiene su propia ayuda con el calificador HELP para Windows y -h o -help para Linux.

Redes de Área Local Olga Minguet 75

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

D) Utilidad ipconfig (Windows) e ifconfig/iwconfig (Linux)

Opciones de ipconfig más habituales:

- **/all**: Muestra toda la configuración de la red, incluyendo los servidores DNS, WINS, DHCP, etc.
- **/renew** [tarjeta]: renueva la dirección IP de todas las tarjetas (si ninguna tarjeta es especificada), o de sólo una tarjeta específica si utiliza el parámetro tarjeta.
- **/release** [tarjeta]: libera la dirección IP de todas las tarjetas (si ninguna tarjeta es especificada), o de sólo una tarjeta específica si utiliza el parámetro tarjeta.

Redes de Área Local Olga Minguet 76

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

E) Utilidad netstat

- Netstat (Network status), proporciona información sobre el **estado de la red**.
- Funciona solo mediante la línea de comandos.
- Puede usarse para conocer información sobre las conexiones establecidas por el equipo, como:
 - los puertos abiertos,
 - conexiones en segundo plano,
 - conexiones establecidas por programas espía, etc.
- Cuando se utiliza netstat sin parámetro, se muestran las conexiones activas existentes, mostrando los protocolos utilizados.

Redes de Área Local Olga Minguet 77

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

E) Utilidad netstat



Redes de Área Local Olga Minguet 78

UD3. Instalación y configuración de los equipos de red

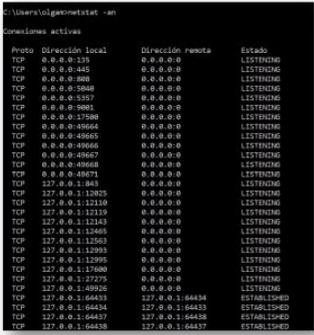
8. Utilidades propias de redes TCP/IP

E) Utilidad netstat

También podemos utilizar netstat con diversos parámetros. Podemos conocer los parámetros utilizando la opción `-h` o `/help`.

A continuación vamos a ver los más habituales.

- **an**: muestra todas las conexiones, además de los puertos abiertos. Esta opción es utilizada para conocer los puertos abiertos en un equipo.



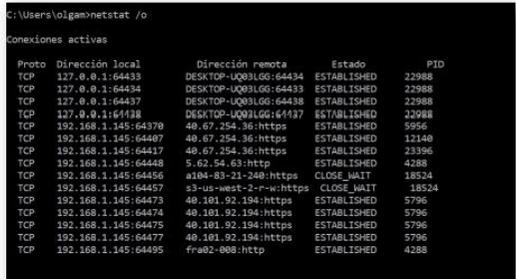
Redes de Área Local Olga Minguet 79

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

E) Utilidad netstat

- **o**: muestra además la identidad del proceso de cada conexión.



Redes de Área Local Olga Minguet 80

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

F) Utilidad tracert

Se utiliza para **controlar los saltos de red** que deben seguir los paquetes hasta alcanzar su destino.

Cuando el número de saltos es 1, esto quiere decir que la red es plana, es decir, se trata de una red de área local.

```
C:\Users\olgam>tracert www.google.es
Traza a la dirección www.google.es [216.58.201.163]
sobre un máximo de 30 saltos:

  1  8 ms  3 ms  3 ms  HOME [192.168.1.1]
  2  12 ms  8 ms  67 ms  100.84.0.1
  3  9 ms  10 ms  12 ms  10.14.7.69
  4  11 ms  9 ms  10 ms  10.0.12.33
  5  9 ms  9 ms  10 ms  10.14.3.14
  6  18 ms  18 ms  18 ms  209.85.168.54
  7  18 ms  18 ms  18 ms  172.253.50.37
  8  2088 ms  17 ms  19 ms  72.14.233.125
  9  23 ms  50 ms  17 ms  mdd0806c-in-f3.1e100.net [216.58.201.163]

Traza completa.
```

Redes de Área Local

Olga Minguet

81

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

F) Utilidad tracert

- También podemos controlar algunos parámetros de ejecución del comando. Con la opción `-h` o `/help` podemos verlos todos.

- Algunos muy habituales son:

- h**: para limitar el número máximo de saltos.

- w**: tiempo de espera en milisegundos para esperar cada respuesta.

```
C:\Users\olgam>tracert -h 4 www.google.es
Traza a la dirección www.google.es [216.58.201.131]
sobre un máximo de 4 saltos:

  1  19 ms  48 ms  88 ms  192.168.1.1
  2  9 ms  4 ms  4 ms  100.84.0.1
  3  21 ms  69 ms  10 ms  10.14.7.69
  4  9 ms  10 ms  10 ms  10.0.12.33

Traza completa.
```

Redes de Área Local

Olga Minguet

82

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

G) Utilidad route

- Sirve para determinar las rutas que deben seguir los paquetes de red. Una ruta indica el camino apropiado por el que un paquete pueda alcanzar su destino o, al menos, aproximarse a él.

- Para manejar las tablas de rutas, en sistemas Windows suele utilizarse la orden *route*, mientras que en sistemas Linux hay una gran diversidad de órdenes y utilidades, aunque la más usual es *ip route*, que admite una multitud de parámetros que deberemos consultar en cada versión para utilizarlo con propiedad.

Por ejemplo, con *route print* obtenemos las rutas disponibles para un nodo.

Redes de Área Local

Olga Minguet

83

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

H) Utilidad ftp y tftp

- La utilidad ftp sirve **para intercambiar ficheros** entre dos nodos de la red utilizando el protocolo FTP.

- FTP tiene su parte de cliente y su parte de servidor.

- Cuando se ejecuta el **cliente ftp**, aparece el identificador de utilidad FTP sobre la que se ejecutan los comandos ftp: listar, traer (bajar) o dejar (subir) ficheros, etc.

- Previamente a la utilización del FTP para realizar transferencias, es necesario preparar una conexión segura a través del protocolo TCP. Esto se realiza con el **comando open** seguido de la dirección IP o el nombre DNS del host remoto.

Redes de Área Local

Olga Minguet

84

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

H) Utilidad ftp y tftp

- La utilización de un **servidor ftp** exige tener acceso al servidor a través de un nombre de usuario y una contraseña que nos asignará el administrador del sistema remoto. Muchos servidores en Internet tienen información pública a la que se accede sin necesidad de tener cuenta en el equipo, permitiendo conexiones de usuarios anónimos.
- El comando **tftp** es similar al ftp, más fácil de configurar, pero con menos prestaciones.

Redes de Área Local Olga Minguet 85

UD3. Instalación y configuración de los equipos de red

8. Utilidades propias de redes TCP/IP

I) Utilidades telnet y ssh

- Sirve para realizar conexiones remotas interactivas en forma terminal virtual a través del protocolo de alto nivel TELNET. El comando va acompañado de la dirección IP del nodo remoto o de su dirección DNS.
- Los servidores Windows implementan un servidor TELNET, que sirve sesiones en forma de ventanas emuladoras DOS a los clientes TELNET que se conectan o ellos desde su red, lo que es muy interesante para ejecutar scripts en máquinas remotas.
- En el mundo Linux, la utilidad equivalente más moderna es ssh. Esta es una de las utilidades más versátiles que tiene su parte de cliente y de servidor.
- Puede ejecutar aplicaciones remotas, copiar ficheros, crear sesiones remotas gráficas, crear túneles de comunicación, etc. Funcionalmente, ssh puede sustituir las conexiones remotas de TELNET, pero la gran ventaja de ssh es que cifra las conexiones, por lo que es mucho más seguro que TELNET.

Redes de Área Local Olga Minguet 86

UD3. Instalación y configuración de los equipos de red

 Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 12
- Actividad 13
- Actividad 14
- Actividad 15
- Actividad 16
- Actividad 17
- Actividad 18

Redes de Área Local Olga Minguet 87

8.3.2 Cuaderno de actividades

Cuaderno de Actividades

-UNIDAD 3-
Instalación y configuración de los equipos de red

CUADERNO DE ACTIVIDADES

Objetivos

- Consolidar los contenidos vistos en la Unidad 3 del curso.
- Identifica los protocolos y servicios de red proporcionados por los sistemas operativos.
- Utiliza las herramientas básicas para la gestión de protocolos de red.
- Configura el sistema de direccionamiento de los equipos de la red.

Actividades

1. Realiza los apartados siguientes:

a) **Elabora una tabla en la que se asocie cada nivel OSI con los niveles de la familia de protocolos TCP/IP y con los protocolos básicos que se utilizan en cada nivel TCP/IP. Para ello puedes apoyarte en la imagen de la diapositiva correspondiente de la teoría.**

	Nivel OSI	Nivel TCP/IP	Protocolos
1			
2			
3			
4			
5			
6			
7			

UD03_Instalación y configuración de los equipos de red 2-16

CUADERNO DE ACTIVIDADES

b) Indica las características o usos más relevantes de cada uno de los siguientes protocolos de la familia TCP/IP. *Esta es una actividad muy importante, desarróllala con atención utilizando las diapositivas de clase.*

Protocolo	Características
IP	
ICMP	
TCP	
UDP	
ARP	
RARP	

2. Realiza las siguientes conversiones:

a) De binario a decimal

10011110	
00010001	
00100110	
1110	
111011101110	
10110110	
0	
10	
1	

b) De decimal a binario

32	
147	
43	
80	
7512	
145	
1	
0	

CUADERNO DE ACTIVIDADES

CLASES DE REDES

3. Reconocer los rangos de IP que corresponden con cada Clase de Red es muy importante. Observa la tabla que se detalla a continuación, como extensión a la vista en la teoría, e identifica la clase de red de cada dirección IP expuesta en las tablas posteriores.

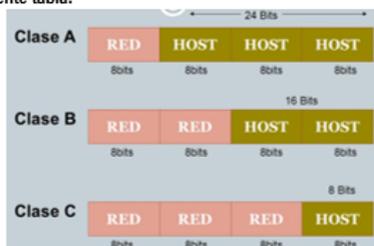
Clase	Primer octeto de la dirección IP	Valor más bajo del primer octeto (binario)	Valor más alto del primer octeto (binario)	Rango de valores del primer octeto (decimal)	Octetos en ID de red / host	Rango teórico de direcciones IP
A	0xxx xxxx	0000 0001	0111 1110	De 1 a 126	1 / 3	De 1.0.0.0 a 126.255.255.255
B	10xx xxxx	1000 0000	1011 1111	De 128 a 191	2 / 2	De 128.0.0.0 a 191.255.255.255
C	110x xxxx	1100 0000	1101 1111	De 192 a 223	3 / 1	De 192.0.0.0 a 223.255.255.255
D	1110 xxxx	1110 0000	1110 1111	De 224 a 239	-	De 224.0.0.0 a 239.255.255.255
E	1111 xxxx	1111 0000	1111 1111	De 240 a 255	-	De 240.0.0.0 a 255.255.255.255

Dirección	Clase
10.250.1.1	
150.10.15.0	
192.14.2.0	
148.17.9.1	
193.42.1.1	
126.8.156.0	
220.200.23.1	
230.230.45.58	
177.100.18.4	

Dirección	Clase
119.18.45.0	
249.240.80.78	
199.155.77.56	
117.89.56.45	
215.45.45.0	
199.200.15.0	
95.0.21.90	
33.0.0.0	
158.98.80.0	

CUADERNO DE ACTIVIDADES

4. Conociendo los bytes que se corresponden en cada dirección IP con Red y con Host. Completa, conociendo la Clase que identifica el número de bytes con la tabla anterior y apoyándote en el esquema adjunto, la siguiente tabla:



Dirección	Clase	Red	Host
177.100.18.4			
119.18.45.0			
209.240.80.78			
199.155.77.56			
117.89.56.45			
215.45.45.0			
192.200.15.0			
95.0.21.90			
33.0.0.0			
158.98.80.0			
217.21.56.0			
10.250.1.1			
150.10.15.0			
192.14.2.0			
148.17.9.1			
193.42.1.1			
126.8.156.0			
220.200.23.1			

CUADERNO DE ACTIVIDADES

MASCARAS DE RED

5. Realiza los apartados sobre Máscaras de Red que se enuncian a continuación:

a) Realiza esta actividad de visualización a la par con tu profesora. Tecllea un `ipconfig/all` en el cmd, y observa, entre los datos que te aparecen, la máscara de red. Realiza una captura de pantalla e insértala a continuación. Podrás observar, en la puesta en común, que todos tienen la misma máscara de red, el mismo sistema de direccionamiento, esto es, pertenecen a la misma red.

b) Conociendo la Clase de red a la que pertenece cada dirección IP (con la tabla de la actividad 5), escribe la máscara de subred y la notación CIDR correspondiente a cada una de estas direcciones

Dirección	Máscara	CIDR
77.251.200.51		
189.210.50.1		
88.45.65.35		
1.1.10.50		
220.90.130.45		
177.100.18.4		
119.18.45.0		
191.249.234.191		
223.23.223.109		
126.123.23.1		
223.69.230.250		
192.12.35.105		

CUADERNO DE ACTIVIDADES

6. A partir del siguiente par: dirección IP, máscara de red (193.168.14.3, 255.255.255.0) obtén:

a) La clase de red.

b) La dirección de red en decimal y en binario

c) La dirección IP en notación CIDR.

d) La primera y última dirección posible para un dispositivo concreto en esa red.

e) La dirección de multidifusión

CUADERNO DE ACTIVIDADES

7. A partir del siguiente par: dirección IP, máscara de red (150.14.32.128, 255.255.0.0) obtén:

a) La clase de red.

b) La dirección de red en decimal y en binario

c) La dirección IP en notación CIDR.

d) La primera y última dirección posible para un dispositivo concreto en esa red.

e) La dirección de multidifusión

CUADERNO DE ACTIVIDADES

8. A partir del siguiente par: dirección IP, máscara de red (8.45.127.12, 255.0.0.0) obtén:

a) La clase de red.

b) La dirección de red en decimal y binario

c) La dirección IP en notación CIDR.

d) La primera y última dirección posible para un dispositivo concreto en esa red.

e) La dirección de multidifusión

CUADERNO DE ACTIVIDADES

SUBNETTING

9. Una empresa quiere fraccionar su sistema de direccionamiento de red en 5 subredes aplicando la técnica de *Subnetting*. La dirección de red de la que se parte es 192.168.5.0.

a) Indica la siguiente información de la red

Clase de red	
Máscara por defecto	
Dirección CIDR	

b) Calcula el número de subredes máximo que podemos obtener.

c) Indica cual es la nueva máscara de subred en notación decimal. Puedes expresarla también en binario para ayudarte a hacer los cálculos.

d) Indica en la nueva máscara de subred cuantos bits de la máscara servirán para identificar a la red y cuantos bits a los hosts.

CUADERNO DE ACTIVIDADES

10. Una empresa quiere fraccionar su sistema de direccionamiento de red en **55 subredes** aplicando la técnica de *Subnetting*. La dirección de red de la que se parte es **172.10.0.0**.

a) Indica la siguiente información de la red

Clase de red	
Máscara por defecto	
Dirección CIDR	

b) Calcula el número de subredes máximo que podemos obtener.

c) Indica cual es la nueva máscara de subred en notación decimal. Puedes expresarla también en binario para ayudarte a hacer los cálculos.

d) Indica en la nueva máscara de subred cuantos bits de la máscara servirán para identificar a la red y cuantos bits a los hosts.

CUADERNO DE ACTIVIDADES

11. Una empresa quiere fraccionar su sistema de direccionamiento de red en **1000 subredes** aplicando la técnica de *Subnetting*. La dirección de red de la que se parte es **20.0.0.0**.

a) Indica la siguiente información de la red

Clase de red	
Máscara por defecto	
Dirección CIDR	

b) Calcula el número de subredes máximo que podemos obtener. Has de indicar la fórmula que has usado para calcularlo.

c) Indica cual es la nueva máscara de subred en notación decimal. Puedes expresarla también en binario para ayudarte a hacer los cálculos.

d) Indica en la nueva máscara de subred cuantos bits de la máscara servirán para identificar a la red y cuantos bits a los hosts.

CUADERNO DE ACTIVIDADES

UTILIDADES DE REDES TCP/IP

12. Comando nslookup

- a) Haciendo uso de la orden nslookup averiguar la dirección IP del servidor de google.es así como sus alias. Escribe el comando que has ejecutado

- b) Captura la pantalla con el comando "Imprimir pantalla" o la aplicación Recortes de Windows y adjúntala en tu documento de actividades como solución a esta actividad.

13. Comando ping

- a) Haciendo uso del comando ping, haced un ping a la dirección IP del servidor de google.es de forma que haga dos solicitudes de eco en vez de las tres habituales. Escribe el comando que has ejecutado

- b) Captura la pantalla.

- c) ¿Cuántos bytes envía un ping de forma estándar?

- d) Después haced una solicitud de eco que envíe 256 bytes. Captura la pantalla.

CUADERNO DE ACTIVIDADES

- 14. Comando arp. (En <http://es.ccm.net/faq/430-comandos-tcp-ip-para-windows> puedes encontrar ayuda para hacer este ejercicio).

- a) Haz uso del comando arp para averiguar cuál es vuestra tabla arp. Escribe el comando que has ejecutado

- b) Captura la pantalla.

- c) ¿Cómo añadirías un nodo nuevo o entrada nueva a la tabla arp?

- d) ¿Cómo la eliminarías?

15. Comando ipconfig

- a) Haciendo uso del comando ipconfig, averiguar cual es vuestra puerta de enlace predeterminada, vuestra ip, vuestra máscara de red, vuestro servidor de DNS, vuestro servidor DHCP y vuestra MAC. Escribe el comando que has ejecutado

- b) Captura la pantalla

- c) Ahora liberad vuestra dirección ip y volved a conseguir una dirección IP. Indica los comandos que has ejecutado para hacerlo.

CUADERNO DE ACTIVIDADES

16. Haciendo uso del comando netstat averigüad qué conexiones TCP tenéis activas y el número de puerto de la dirección remota con el que os estáis conectando.

a) Escribe el comando que has utilizado

b) Captura la pantalla.

17. Ejecuta comando tracert para el destino que tú quieras (dirección web) y anota el número de saltos y el nombre y dirección IP de los routers que atraviesa en una tabla. Incluye la dirección IP de la máquina destino, así como la clase a la que pertenece cada una de las IP's.

a) Escribe el comando que has utilizado

b) Captura la pantalla.

18. Haciendo uso del comando route, imprime la tabla de rutas que tienes en el ordenador.

a) Escribe el comando que has utilizado

b) Captura la pantalla.

CUADERNO DE ACTIVIDADES

c) ¿Qué destino de red piensas que elegirá vuestro ordenador para "salir" a internet?

8.3.3 Cuaderno de prácticas

<p style="font-size: small; margin: 0;">UD03 Instalación y configuración de los equipos de red PRÁCTICAS</p>								
<p style="font-weight: bold; margin: 10px 0;">Cuaderno de PRÁCTICAS: Subnetting y VLSM</p>								
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 5px;">Nombre y apellidos</td> <td style="width: 80%;"></td> </tr> <tr> <td style="padding: 5px;">Breve descripción</td> <td style="padding: 5px;">Aprender a diseñar una subred utilizando las técnicas de Subnetting y VLSM y a comparar los diferentes diseños de red obtenidos utilizando una u otra.</td> </tr> <tr> <td style="padding: 5px;">Material necesario</td> <td style="padding: 5px;"> <ul style="list-style-type: none"> Cuaderno de trabajo Bolígrafo y/o lápiz 1 PC con Packet Tracer </td> </tr> <tr> <td style="padding: 5px;">Fuentes de información</td> <td style="padding: 5px;"> <ul style="list-style-type: none"> Diapositivas de la Unidad 3 Explicaciones de clase </td> </tr> </table>	Nombre y apellidos		Breve descripción	Aprender a diseñar una subred utilizando las técnicas de Subnetting y VLSM y a comparar los diferentes diseños de red obtenidos utilizando una u otra.	Material necesario	<ul style="list-style-type: none"> Cuaderno de trabajo Bolígrafo y/o lápiz 1 PC con Packet Tracer 	Fuentes de información	<ul style="list-style-type: none"> Diapositivas de la Unidad 3 Explicaciones de clase
Nombre y apellidos								
Breve descripción	Aprender a diseñar una subred utilizando las técnicas de Subnetting y VLSM y a comparar los diferentes diseños de red obtenidos utilizando una u otra.							
Material necesario	<ul style="list-style-type: none"> Cuaderno de trabajo Bolígrafo y/o lápiz 1 PC con Packet Tracer 							
Fuentes de información	<ul style="list-style-type: none"> Diapositivas de la Unidad 3 Explicaciones de clase 							
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Desarrollo</td> </tr> <tr> <td style="padding: 5px;"> <ul style="list-style-type: none"> ✓ PRÁCTICA 1: Diseño de una red de Clase C con 3 subredes aplicando Subnetting. ✓ PRÁCTICA 2: Diseño de una red de Clase C con 8 subredes aplicando Subnetting. ✓ PRÁCTICA 3: Diseño de una red de Clase B con 4 subredes aplicando Subnetting. ✓ PRÁCTICA 4: Simulación y Verificación del diseño de una red Clase C con Packet Tracer. ✓ PRÁCTICA 5: Diseño de una red Clase C aplicando la técnica de VLSM </td> </tr> </table>	Desarrollo	<ul style="list-style-type: none"> ✓ PRÁCTICA 1: Diseño de una red de Clase C con 3 subredes aplicando Subnetting. ✓ PRÁCTICA 2: Diseño de una red de Clase C con 8 subredes aplicando Subnetting. ✓ PRÁCTICA 3: Diseño de una red de Clase B con 4 subredes aplicando Subnetting. ✓ PRÁCTICA 4: Simulación y Verificación del diseño de una red Clase C con Packet Tracer. ✓ PRÁCTICA 5: Diseño de una red Clase C aplicando la técnica de VLSM 						
Desarrollo								
<ul style="list-style-type: none"> ✓ PRÁCTICA 1: Diseño de una red de Clase C con 3 subredes aplicando Subnetting. ✓ PRÁCTICA 2: Diseño de una red de Clase C con 8 subredes aplicando Subnetting. ✓ PRÁCTICA 3: Diseño de una red de Clase B con 4 subredes aplicando Subnetting. ✓ PRÁCTICA 4: Simulación y Verificación del diseño de una red Clase C con Packet Tracer. ✓ PRÁCTICA 5: Diseño de una red Clase C aplicando la técnica de VLSM 								
<p style="font-size: x-small; margin: 0;">Página 1</p>								

<p style="font-size: small; margin: 0;">UD03 Instalación y configuración de los equipos de red PRÁCTICAS</p>
<p style="font-weight: bold; margin: 10px 0; background-color: #cccccc; padding: 5px;">Práctica 1</p>
<p style="font-weight: bold; color: #0070c0; margin: 10px 0;">Diseño de una red Clase C aplicando Subnetting</p> <p style="font-size: x-small; margin: 5px 0;">Una empresa dedicada a la venta de material informático dispone de 8 departamentos (<i>Compras, Ventas, Administración, Recursos Humanos, Almacén, Taller, Marketing y Dirección</i>) y nos ha pedido que diseñemos su red de área local. Las especificaciones que nos dan son las siguientes:</p> <ul style="list-style-type: none"> > Su dirección de red es 192.168.12.0/24 > Se nos pide que desarrollemos un esquema de direccionamiento usando Subnetting. > Creación de 3 subredes, una por cada tres departamentos de la empresa (<i>si sobran direcciones IP para direccionar otra subred quedarían para una posterior ampliación</i>).
<p>1.1- Cuál es la CLASE de red y la MÁSCARA que le corresponde por defecto.</p> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>
<p>1.2- NÚMERO DE SUBREDES que podemos obtener (<i>recuerda que siempre ha de ser un número igual o superior a las subredes que solicitan</i>).</p> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>
<p>1.3- NUEVA MÁSCARA DE RED para obtener las subredes necesarias.</p> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>
<p>1.4- NÚMERO DE HOST MÁXIMO que pueden direccionarse en cada subred.</p> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>
<p>1.5- SALTO DE RED, en decimal.</p> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>
<p style="font-size: x-small; margin: 0;">Página 2</p>

 UD03 Instalación y configuración de los equipos de red **PRÁCTICAS**

1.6- Completa la TABLA siguiente obteniendo las 4 direcciones IP's con las que definimos completamente cada subred. En BINARIO la porción que varía.

	IP Red	IP Primer host disponible...	...IP Ultimo host disponible	IP Broadcast o Difusión
Subred 1				
Subred 2				
Subred 3				
Subred 4				

1.7- Completa la TABLA RESULTADO en decimal completamente.

	IP Red	IP Primer host disponible...	...IP Ultimo host disponible	IP Broadcast o Difusión
Subred 1				
Subred 2				
Subred 3				
Subred 4				

UD03 Instalación y configuración de los equipos de red PRÁCTICAS

Práctica 2

Diseño de una red Clase C aplicando Subnetting

Una empresa dedicada a la venta de material informático dispone de 8 departamentos (*Compras, Ventas, Administración, Recursos Humanos, Almacén, Taller, Marketing y Dirección*) y nos ha pedido que diseñemos su red de área local. Las especificaciones que nos dan son las siguientes:

- Su dirección de red es 221.123.10.12/24
- Se nos pide que desarrollemos un esquema de direccionamiento usando Subnetting.
- Creación de 8 subredes, una por cada departamento de la empresa.

2.1- Cuál es la CLASE de red y la MÁSCARA que le corresponde por defecto.

2.2- NÚMERO DE SUBREDES que podemos obtener (*recuerda que siempre ha de ser un número igual o superior a las subredes que solicitan*).

2.3- NUEVA MÁSCARA DE RED para obtener las subredes necesarias.

2.4- NÚMERO DE HOST MÁXIMO que pueden direccionarse en cada subred.

2.5- SALTO DE RED, en decimal.

Página 4

UD03 Instalación y configuración de los equipos de red PRÁCTICAS

2.6- Cálculo de las direcciones de red para cada una de las 8 subredes de la empresa, EN BINARIO.

	IP Red	IP Primer host disponible...	...IP Ultimo host disponible	IP Broadcast o Difusión
Subred 1				
Subred 2				
Subred 3				
Subred 4				
Subred 5				
Subred 6				
Subred 7				
Subred 8				

2.7- **Compras:** dirección de la subred, direcciones del primer y último host y direcciones de broadcast.

Dirección de la subred:
Dirección del Primer y del Último host:
Dirección broadcast:

2.8- **Ventas:** dirección de la subred, direcciones del primer y último host y direcciones de broadcast.

Dirección de la subred:
Dirección del Primer y del Último host:
Dirección broadcast:

Página 5

UD03 Instalación y configuración de los equipos de red PRÁCTICAS

2.9- Administración: dirección de la subred, direcciones del primer y último host y direcciones de broadcast.

Dirección de la subred:
Dirección del Primer y del Último host:
Dirección broadcast:

2.10- Recursos Humanos: dirección de la subred, direcciones del primer y último host y direcciones de broadcast.

Dirección de la subred:
Dirección del Primer y del Último host:
Dirección broadcast:

2.11- Almacén: dirección de la subred, direcciones del primer y último host y direcciones de broadcast.

Dirección de la subred:
Dirección del Primer y del Último host:
Dirección broadcast:

2.12- Taller: dirección de la subred, direcciones del primer y último host y direcciones de broadcast.

Dirección de la subred:
Dirección del Primer y del Último host:
Dirección broadcast:

2.13- Marketing: dirección de la subred, direcciones del primer y último host y direcciones de broadcast.

Dirección de la subred:
Dirección del Primer y del Último host:
Dirección broadcast:

2.14- Dirección: dirección de la subred, direcciones del primer y último host y direcciones de broadcast.

Dirección de la subred:
Dirección del Primer y del Último host:
Dirección broadcast:

UD03 Instalación y configuración de los equipos de red PRÁCTICAS

2.15- ¿Cuántas direcciones habría disponibles para host si no aplicamos Subnetting? Calcula

¿Cuántas direcciones hay disponibles al aplicar Subnetting? Calcula

UD03 Instalación y configuración de los equipos de red PRÁCTICAS

Práctica 3

Diseño de una red Clase B aplicando Subnetting

En Burjassot se precisa configurar una Red de área metropolitana con 4 subredes y un número elevado de host para cada una de las subredes. Las especificaciones que nos dan son las siguientes:

- > Su dirección de red es 138.115.0.0/24
- > Se nos pide que desarrollemos un esquema de direccionamiento usando Subnetting.
- > Creación de 4 subredes (recuerda siempre que si sobran direcciones IP para direccionar otra subred quedarían para una posterior ampliación).

3.1- Cuál es la CLASE de red y la MÁSCARA que le corresponde por defecto.

3.2- NÚMERO DE SUBREDES que podemos obtener (recuerda que siempre ha de ser un número igual o superior a las subredes que solicitan).

3.3- NUEVA MÁSCARA DE RED para obtener las subredes necesarias.

3.4- NÚMERO DE HOST MÁXIMO que pueden direccionarse en cada subred.

3.5- SALTO DE RED, en decimal.

 UD03 Instalación y configuración de los equipos de red **PRÁCTICAS**

3.6- Completa la TABLA siguiente obteniendo las 4 direcciones IP's con las que definimos completamente cada subred. En BINARIO las porciones que varían.

Subred	IP Red	IP Primer host disponible...	...IP Ultimo host disponible	IP Broadcast o Difusión

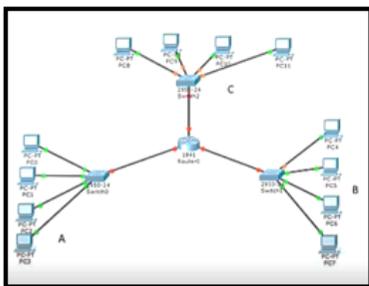
3.7- Completa la TABLA RESULTADO en decimal completamente.

Subred	IP Red	IP Primer host disponible...	...IP Ultimo host disponible	IP Broadcast o Difusión

Práctica 4

Simulación y Verificación del diseño de una red Clase C con Packet Tracer

Tomando los resultados obtenidos en la PRÁCTICA 1, vamos a implementar y verificar la configuración de nuestro diseño de subredes para una RED DE ÁREA LOCAL.



4.1- Construye la VISTA FÍSICA de la red completa que vas a implementar. El nombre de tu Router va a ser tu "NombreApellido". Inserta en un documento en Word en blanco, con el nombre PRÁCTICA 4, una captura del montaje que has realizado indicando Solución 4.1 junto a la captura.

IMPORTANTE: Es posible que el Router genérico que has elegido no tenga suficientes puertos Ethernet para la conexión de cada Switch. Será necesario que, desde la pestaña Física del Router, insertes los módulos necesarios para poder disponer de los 4 puertos Ethernet.

4.2- Configura cada SUBRED. Para ello deberás configurar cada uno de los PC's utilizando una de las direcciones IP útiles dentro de cada rango.

IMPORTANTE: Recuerda que la primera dirección útil de cada Subred generalmente se deja reservada para la Gateway o Puerta de enlace predeterminada (esto es, la dirección IP de la interfaz del Router que está conectada a esa subred).

Inserta un cuadro de texto junto a cada grupo de PC's para indicar de qué Subred se trata en cada grupo. Después realiza una captura de nuevo con el montaje completo insertándola en el documento de Word indicando Solución 4.2 junto a la captura.

- 4.3- Realiza un PING dentro de cada Subred, entre dos ordenadores distintos de la misma, utilizando para ello el Command Prompt de uno de los PC's. Inserta en el documento de Word una captura con cada uno de los PINGS realizados en cada subred indicando Solución 4.3, verificando así que la Configuración de cada una de las Subredes es correcta.
- 4.4- Configura el Router. El Router debe poseer una interfaz (Tarjeta de red) para cada una de las conexiones Ethernet realizadas, lo que significa que debemos configurar en cada una de ellas una dirección IP propia de la subred. Generalmente se reserva la primera dirección útil (o la última) para este fin: Gateway o Puerta de enlace predeterminada. La profesora os explicará en clase como realizar la configuración de cada interfaz del Router desde la pestaña CLI:

```
NombreApellido>enable
NombreApellido# configure terminal
NombreApellido (config)# interface f0/0
NombreApellido (config-if)# ip address 192.168.12.1 255.255.255.224
NombreApellido (config-if)# no shutdown
NombreApellido (config-if)# exit

(estas líneas de configuración para cada interfaz)
NombreApellido (config)# interface f0/1 .....
```

Deberás realizar una captura de la configuración que has realizado en el Router, siguiendo las instrucciones de la profesora, indicando junto a la captura Solución 4.4.

- 4.5- Realiza un PING ahora entre Subredes, esto es, desde el PC de una de las subredes hacia otro PC de otra de las subredes. Realiza al menos 4 PINGS, uno desde cada una de las subredes, para verificar que todas las conexiones intermedias están correctas. Deberás insertar una captura de cada uno de los PINGS realizados indicando junto a las capturas Solución 4.5.

Práctica 5

Diseño de una red Clase C aplicando la técnica de VLSM

La misma empresa de la PRÁCTICA 1 nos pide que diseñemos su red, pero usando un esquema de direccionamiento basado en VLSM y que cumpla los siguientes requerimientos:

- Su dirección de red es 192.168.12.0/24
- Se nos pide que desarrollemos un esquema de direccionamiento usando la técnica de VLSM (Longitud variable de máscara de subred).
- Creación de 7 subredes:
 - Una subred de 60 hosts para VLAN de Compras y Ventas
 - Una subred de 80 hosts para la VLAN de Taller y Almacén
 - Una subred de 20 hosts para la VLAN de Dirección, Administrativos y Marketing
 - Cuatro subredes de 2 hosts para los enlaces entre enrutadores

5.1- Ordena adecuadamente las subredes para aplicar la técnica de VLSM.

5.2- Calcula la primera subred: máscara de subred, dirección de la subred, direcciones del primer y último host y dirección de broadcast

MÁSCARA DE SUBRED:

5.3- Calcula la segunda subred: máscara de subred, dirección de la subred, direcciones del primer y último host y dirección de broadcast

MÁSCARA DE SUBRED:

5.4- Calcula la tercera subred: máscara de subred, dirección de la subred, direcciones del primer y último host y dirección de broadcast

MÁSCARA DE SUBRED:

5.5- Calcula el enlace 1: máscara de subred, dirección de la subred, direcciones del primer y último host y dirección de broadcast

MÁSCARA DE SUBRED:

5.6- Calcula el enlace 2: máscara de subred, dirección de la subred, direcciones del primer y último host y dirección de broadcast

MÁSCARA DE SUBRED:

5.7- Calcula el enlace 3: máscara de subred, dirección de la subred, direcciones del primer y último host y dirección de broadcast

MÁSCARA DE SUBRED:

5.8- Calcula el enlace 4: máscara de subred, dirección de la subred, direcciones del primer y último host y dirección de broadcast

MÁSCARA DE SUBRED:

UD03 Instalación y configuración de los equipos de red **PRÁCTICAS**



Subred	IP Red	IP Primer host disponible...	...IP Ultimo host disponible	IP Broadcast o Difusión



8.3.4 Trabajo de investigación

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

UNIDAD 3. INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS DE RED

Utilidades propias de TCP/IP

Objetivos

- Entrenarnos en las herramientas aprendidas en la Unidad 3 para observación y comprobación de aspectos fundamentales en redes.

Desarrollo

El trabajo consiste en el desarrollo de 4 actividades, tanto de cmd como de simulación, respondiendo a las cuestiones que se nos indican en el recorrido de las mismas.

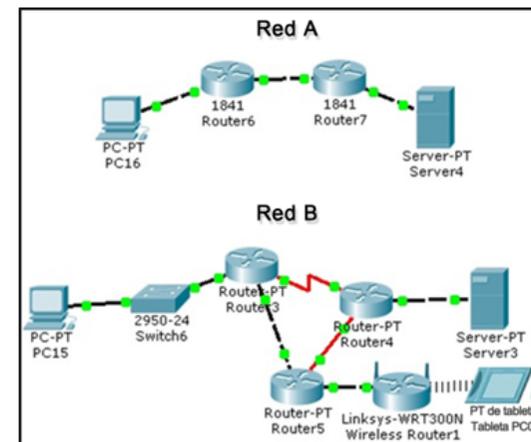
- ✓ ACTIVIDAD 1: Observación de topologías de red.
- ✓ ACTIVIDAD 2: Comprobación de la conectividad con `tracert`.
- ✓ ACTIVIDAD 3: Observación de la resolución DNS con `nslookup`.
- ✓ ACTIVIDAD 4: Administración de redes usando los comandos `show`

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

Actividad 1

Observación de topologías de red

Explicar cómo se crea, configura y verifica una red pequeña de segmentos directamente conectados.



Observa las dos redes en el diagrama de la topología. Responde las siguientes preguntas y anota la respuesta:

- Compara visualmente la red A y la red B. ¿En qué sentido son iguales? Justifica tu respuesta (Ejemplos: ¿Son útiles para la conexión del mismo tipo de dispositivos? ¿Crees que se configuran para la misma área geográfica?)

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

- Anota los dispositivos que se usan en cada diseño de red. Dado que los dispositivos están etiquetados, ya sabes de qué tipos de terminales y dispositivos intermediarios se trata. Con estos datos, responde a lo contrario: ¿En qué sentido las dos redes son diferentes? ¿La cantidad de dispositivos en cada una es la única diferencia? Justifica tu respuesta.

- ¿Qué red elegirías si fueras propietario de una empresa pequeña o mediana? Justifica tu elección de la red en función del coste, la velocidad, los puertos, la capacidad de expansión y la facilidad de administración.

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

Actividad 2

Comprobación de la conectividad con traceroute

En esta práctica vamos a aprender a resolver problemas de conectividad con la utilidad **TRACERT** (en el lado del PC, en Windows), y **TRACEROUTE** (en el lado del router, en IOS), rastreando una ruta de origen a destino para determinar la causa del problema de red que se plantea.

Una vez corregido el problema que aparecerá, utilizaremos de nuevo los comandos para verificar la finalización.

Sigue los pasos que se detallan a continuación, utilizando el archivo PKT adjunto en la Tarea de TEAMS que acompaña este trabajo.

Parte 1: Probar la conectividad de extremo a extremo con el comando tracert

Paso 1: Enviar un ping de un extremo de la red al otro.

Haz clic en **PC1** y abre el **símbolo del sistema**. Haz ping a **PC3** en **10.1.0.2**. ¿Qué mensaje aparece como resultado del ping? ¿Ha funcionado el ping?

Paso 2: Rastrear la ruta desde PC1 para determinar en qué parte del recorrido falla la conectividad.

- Desde el **símbolo del sistema** de **PC1**, introduce el comando **tracert 10.1.0.2**.
- Cuando recibas el mensaje **Request timed out** (Tiempo de espera agotado), presiona **Ctrl+C**. ¿Cuál fue la primera dirección IP indicada en el resultado del comando **tracert**?

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

- c. Observa los resultados del comando **tracert**. ¿Cuál es la última dirección que se alcanzó con el comando **tracert**?

Paso 3: Corregir el problema de red que existe

- a. Compara la última dirección que se alcanzó con el comando **tracert** con las direcciones de red indicadas en la topología. El dispositivo más alejado del host 10.0.0.2 con una dirección en el rango de la red que se encontró es el punto de fallo. ¿Qué dispositivos tienen direcciones configuradas para la red donde ocurrió el fallo?

- b. Haz clic en **RouterC** y luego en la ficha **CLI**. ¿Cuál es el estado de las interfaces?

- c. Compara las direcciones IP en las interfaces con las direcciones de red en la topología. ¿Hay algo que parezca fuera de lo normal?

- d. Ahora debes hacer los cambios necesarios para restaurar la conectividad, pero no modifiques las subredes. ¿Cuál es la solución que crees que debes aplicar para que funcione la comunicación?

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

Paso 4: Verificar que la conectividad de extremo a extremo esté establecida.

- a. Desde el símbolo del sistema de PC1, introduce el comando **tracert 10.1.0.2**.
b. Observa el resultado del comando **tracert**. ¿El comando funcionó correctamente?

Parte 2: Comparar con el comando traceroute en un router

- a. Haz clic en **RouterA** y luego en la ficha **CLI**.
b. Introduce el comando **traceroute 10.1.0.2**. ¿El comando se completó correctamente?

- c. Compara el resultado del comando **traceroute** del router con el comando **tracert** de la PC. ¿Cuál es la diferencia más notable de la lista de direcciones que se devolvió?

Parte 3: Uso de Traceroute extendido

Además de **traceroute**, Cisco IOS incluye un comando **traceroute** extendido. Este comando permite que el administrador ajuste parámetros menores en la operación de **traceroute** con algunas preguntas sencillas.

Como parte del proceso de verificación, puedes utilizar el comando **traceroute** extendido en **RouterA** para aumentar la cantidad de paquetes ICMP que **traceroute** envía a cada salto.

Nota: El comando **tracert** de Windows también permite que el usuario ajuste algunos aspectos a través de la línea de comandos.

- a. Haz clic en **RouterA** y luego en la ficha **CLI**.
b. Introduce **traceroute** y presiona **ENTER**. Ten en cuenta que solo debe introducirse el comando **traceroute**.
c. Responde las preguntas que realiza el comando **traceroute** extendido de la siguiente manera: (El comando **traceroute** extendido se ejecutará inmediatamente después de responder la última pregunta)

Protocolo [ip]: ip

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

Target IP address: 10.1.0.2
 Source address: 10.100.100.1
 Numeric display [n]: n
 Timeout in seconds [3]: 3
 Probe count [3]: 5
 Minimum Time to Live [1]: 1
 Maximum Time to Live [30]: 30

Nota: El valor que aparece entre corchetes es el predeterminado, y es el que será utilizado por **tracert** si no se ingresa otro. Para usar el valor predeterminado, solo debes presionar **ENTER**.

¿Cuántas preguntas se respondieron con valores diferentes a los predeterminados? ¿Cuál era el valor nuevo?

¿Cuántos paquetes ICMP envió RouterA?

Nota: El recuento de sondas especifica la cantidad de paquetes ICMP que **tracert** envía a cada salto. Una mayor cantidad de sondas permite un tiempo de ida y vuelta más preciso para los paquetes.

d. En RouterA, ejecuta nuevamente el comando **tracert** extendido, pero esta vez cambia el valor de tiempo de espera a 7 segundos.

¿Qué ocurrió? ¿Cómo afecta a **tracert** el valor de tiempo de espera diferente?

¿Se te ocurre otro uso que podemos darle en administración de redes al parámetro de tiempo de espera?

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

Actividad 3

Observación de la resolución DNS con **nslookup**

Cuando se escribe una dirección del localizador uniforme de recursos (URL), como <http://www.cisco.com>, en un navegador web, se invoca el sistema de nombres de dominio (DNS). La primera parte del URL describe el protocolo que se utiliza. Los protocolos comunes son el protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de hipertexto sobre la capa de sockets seguros (HTTPS) y el protocolo de transferencia de archivos (FTP).

El DNS utiliza la segunda parte de la dirección URL, que en este ejemplo es www.cisco.com. El DNS traduce el nombre de dominio (www.cisco.com) por una dirección IP para permitirle al host de origen llegar al host de destino.

En esta actividad vamos a observar DNS en acción, para ello utilizaremos el comando **nslookup** (búsqueda de servidor de nombres) para obtener información adicional de DNS. Sigue los pasos que se indican a continuación:

Parte 1: Observar la conversión de una URL en una dirección IP mediante DNS

- a. Entra en tu **cmd** de Windows. Aparecerá la ventana del símbolo del sistema.
- b. Haz ping a la URL de Internet Corporation for Assigned Names and Numbers (ICANN), www.icann.org.

ICANN coordina las funciones de DNS, de las direcciones IP, de la administración del sistema de nombres de dominio superior y de la administración del sistema de servidores raíz.

El equipo debe traducir www.icann.org a una dirección IP para saber adónde enviar los paquetes del protocolo de mensajes de control de Internet (ICMP).

La primera línea del resultado muestra el nombre de dominio www.icann.org convertido en una dirección IP por el DNS. Deberías poder ver el efecto del DNS, aun cuando haya un firewall instalado en nuestro Centro que impida enviar pings o aun cuando el servidor de destino haya impedido hacer ping al servidor web.

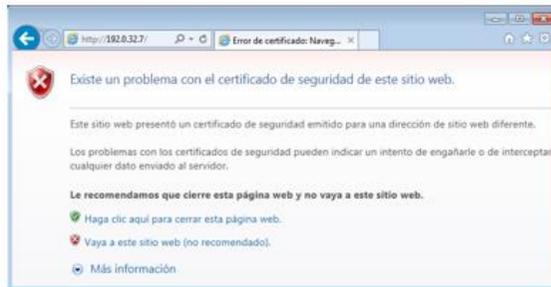
Nota: Si el nombre de dominio se resuelve en una dirección IPv6, usa el comando **ping -4 www.icann.org** para traducirlo a una dirección IPv4, si no lo deseas en IPv6.

```
C:\>ping www.icann.org
Pinging www.vip.icann.org [192.0.32.7] with 32 bytes of data:
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=24ms TTL=246
Reply from 192.0.32.7: bytes=32 time=28ms TTL=246
Ping statistics for 192.0.32.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 28ms, Average = 24ms
```

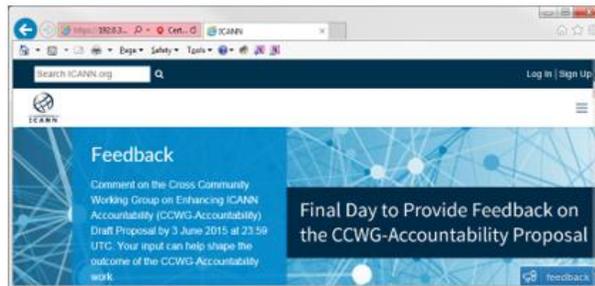
UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

Escribe a continuación la dirección IP de www.icann.org que te aparece en el ping.

c. Escribe la dirección IP del paso b en tu navegador web, en lugar de la URL. Haz clic en **Ir a este sitio web (no recomendado)** para continuar.



d. Observa que se muestra la página web de inicio de ICANN.



A la mayoría de los seres humanos nos resulta más fácil recordar palabras que números. Si le indicas a alguien que acceda a www.icann.org, probablemente lo recordará, pero si le indicas que acceda a 192.0.32.7, le resultará difícil recordar una dirección IP.

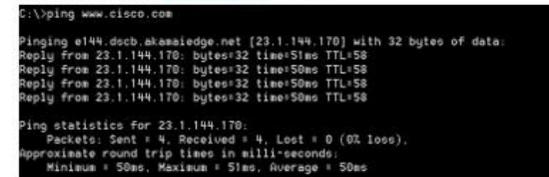
Los equipos informáticos procesan números (sistema binario).

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

El DNS es el proceso por el cual las palabras se traducen por números. Luego, se realiza una segunda traducción.

Los seres humanos pensamos en números con base 10 (sistema decimal). En informática, se procesan números con base 2 (sistema binario). La dirección IP 192.0.32.7 con base 10 es equivalente a 11000000.00000000.00100000.00000111 con base 2. ¿Qué sucede si cortas estos números con base 2 y los pegas en un navegador? ¿Por qué crees que sucede esto?

e. Ahora escribe ping www.cisco.com en el cmd.



Cuando haces ping a www.cisco.com ¿obtienes la misma dirección IP que la del ejemplo? ¿Por qué?

Escribe la dirección IP que obtuviste cuando hiciste ping a www.cisco.com en tu navegador web. ¿Aparece el sitio web? ¿Por qué crees que pasa esto?

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

Parte 2: Vamos a observar la búsqueda DNS mediante el comando nslookup en un sitio web

a. En el cmd, escribe el comando nslookup.

```
C:\>nslookup
Default Server: dslrouter.westell.com
Address: 192.168.1.1
>
```

¿Cuál es la dirección IP del servidor DNS predeterminado que estás utilizando?

Observa que el símbolo del sistema cambió por el símbolo "mayor que" (>). Este es el símbolo de nslookup. Desde aquí, puedes introducir comandos relacionados con el DNS.

Ahora escribe ? para ver una lista de todos los comandos disponibles que puede utilizar en el modo nslookup.

Después escribe www.cisco.com.

```
> www.cisco.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
Name:   e144.dscb.akamaiedge.net
Address: 2600:1408:7:1:9300::90
        2600:1408:7:1:8000::90
        2600:1408:7:1:9000::90
        23.1.144.170
Aliases: www.cisco.com
         www.cisco.com.akadns.net
         wwwds.cisco.com.edgekey.net
         wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

¿Cuál es la dirección IP traducida?

Nota: Es posible que la dirección IP de tu ubicación sea distinta, porque Cisco utiliza servidores reflejados en diversas ubicaciones en todo el mundo.

¿Es la misma dirección IP que aparece con el comando ping?

Debajo de las direcciones, además de la dirección IP 23.1.144.170, aparecen los siguientes números: 2600:1408:7:1:9300::90, 2600:1408:7:1:8000::90, 2600:1408:7:1:9000::90. ¿De qué crees que se trata?

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

b. En el símbolo del sistema, escribe la dirección IP del servidor Web de Cisco que acabas de encontrar. Si no conoces la URL, puede usar el comando nslookup para obtener el nombre de dominio de una dirección IP.

```
> 23.1.144.170
Server: dslrouter.westell.com
Address: 192.168.1.1

Name:   a23-1-144-170.deploy.akamai.com
Address: 23.1.144.170
```

Puedes utilizar la herramienta nslookup para traducir nombres de dominio a direcciones IP. También puedes utilizarla para traducir direcciones IP a nombres de dominio.

Mediante la herramienta nslookup, registra ahora las direcciones IP asociadas con www.google.com.

Parte 3: Observar la búsqueda DNS mediante el comando nslookup en servidores de correo

a. En el cmd escribe set type=mx a fin de usar nslookup para identificar los servidores de correo.

```
> set type=mx
```

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

b. Escribe cisco.com.

```
> cisco.com
Server: dolrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
cisco.com      MX preference = 10, mail exchanger = rcdn-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = alln-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = ans-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = rtp-mx-01.cisco.com

ans-mx-01.cisco.com internet address = 64.103.36.169
rcdn-mx-01.cisco.com internet address = 72.163.7.166
```

Un principio fundamental del diseño de red es la redundancia (la configuración de más de un servidor de correo). De esta manera, si no es posible acceder a uno de los servidores de correo, el equipo que realiza la consulta intenta con el segundo servidor.

Los administradores de correo electrónico determinan a qué servidor se contacta primero mediante **MX preference** (preferencia MX; consulta la imagen de arriba). Primero se contacta al servidor de correo con el valor de **MX preference** más bajo. Según el resultado de la imagen de arriba, ¿qué servidor de correo se contactará primero cuando se envíe correo electrónico a cisco.com?

- c. En el símbolo de nslookup, escribe **exit** para volver al cmd normal del equipo.
- d. En el cmd escribe **ipconfig /all**.
- e. Escribe las direcciones IP de todos los servidores DNS que utiliza nuestro Centro, o tu hogar.

¿Cuál es el propósito fundamental del DNS? Explicáte con tus propias palabras.

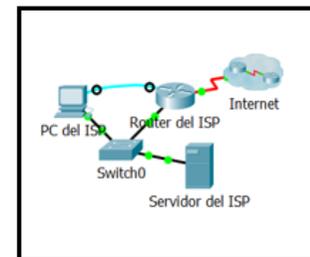
UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

Actividad 4

Administración de redes usando los comandos **show**

En esta actividad vamos a examinar el resultado de varios comandos **show** para conocer su uso.

No se trata de una actividad de configuración, sino de visualización, para ello utilizaremos un PKT ya creado adjunto en la Tarea de TEAMS correspondiente.



Conéctate con ISPRouter.

1. Haz clic en **ISP PC** y luego en la ficha **Desktop** (Escritorio) y en **Terminal**.
2. Ingresa al modo EXEC privilegiado.
3. Usa los siguientes comandos **show** para responder las preguntas de reflexión que hay a continuación:
 - show arp
 - show flash:
 - show ip route
 - show interfaces
 - show ip interface brief
 - show protocols
 - show users
 - show version
4. ¿Qué comandos brindan la dirección IP, el prefijo de red y la interfaz?

UNIDAD 3 – TRABAJO DE INVESTIGACIÓN

5. ¿Qué comandos brindan la dirección IP y la asignación de interfaz, pero no el prefijo de red?

6. ¿Qué comandos muestran el estado de las interfaces?

7. ¿Qué comandos brindan información sobre el IOS cargado en el router?

8. ¿Qué comandos brindan información sobre las direcciones de las interfaces del router?

9. ¿Qué comandos brindan información sobre la cantidad de memoria flash disponible?

10. ¿Qué comandos brindan información sobre las líneas que se están usando para configuración o control de dispositivo?

11. ¿Qué comandos brindan estadísticas sobre el tráfico de las interfaces del router?

12. ¿Qué comandos brindan información sobre las rutas disponibles para el tráfico de red?

13. ¿Qué interfaces están actualmente activas en el router?

8.4 Unidad didáctica 4

Esta unidad didáctica expone los protocolos de la capa 2 o capa de enlace de datos del modelo OSI. Sin la capa de enlace de datos, un protocolo como IP, tendría que tomar medidas para conectarse con todos los tipos de medios que pudieran existir a lo largo de la ruta de envío. Más aún, debería adaptarse cada vez que se desarrolle una nueva tecnología de red o medio, dificultando la innovación y desarrollo de protocolos y medios de red.

A medida que los datos en la comunicación se transfieren de origen a destino, generalmente deben atravesar diferentes redes físicas. Estas redes físicas, tal y como hemos enumerado en la Unidad Didáctica 3, pueden constar de diferentes tipos de medios físicos, como cables de cobre, fibra óptica y tecnología inalámbrica compuesta por señales electromagnéticas, frecuencias de radio y microondas, y enlaces satelitales.

En ésta unidad didáctica, junto a la Unidad Didáctica 5, se presentan los dispositivos necesarios para interconectar toda la serie de dispositivos de una red de área local. Dispositivos de interconexión como concentradores o hubs, puntos de acceso, conmutadores o switch, puentes, y routers. Iniciándose también en la configuración básica de los mismos.

Se pretende hacer una distinción sustancial entre aquellos dispositivos que se utilizan dentro de la propia red local (dispositivos específicos de la red local), y los dispositivos que se utilizan para interconectar la red local con otras redes existentes (interconexión de redes).

También se estudian los conceptos de red de área local virtual, o, dicho de otro modo, VLAN, que nos ofrecen la posibilidad de segmentar la red a nivel de switch, con las ventajas que supone el reducir el dominio de difusión de una red.

8.4.1 Presentación teórica

CURSO

Redes de Área Local

UNIDAD 4

Interconexión de equipos en redes locales (I) -Dispositivos específicos de la red local-

Redes de Área Local
Olga Minguet
1

UD4. Interconexión de equipos en redes locales (I)



ÍNDICE

1. EL ACCESO REMOTO A LA RED
 - A. Tecnología ADSL
 - B. Módems de cable
 - C. Módems de fibra
2. REPETIDORES Y CONCENTRADORES
3. PUENTES
4. CONMUTADORES
5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES
 - 5.1. Redes de área local virtuales o VLAN
 - 5.2. Enlaces entre conmutadores

Redes de Área Local
Olga Minguet
2

UD4. Interconexión de equipos en redes locales (I)



ÍNDICE

1. EL ACCESO REMOTO A LA RED

- A. Tecnología ADSL
 - B. Módems de cable
 - C. Módems de fibra
2. REPETIDORES Y CONCENTRADORES
3. PUENTES
4. CONMUTADORES
5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES
 - 5.1. Redes de área local virtuales o VLAN
 - 5.2. Enlaces entre conmutadores

Redes de Área Local
Olga Minguet
3

UD4. Interconexión de equipos en redes locales (I)



1. EL ACCESO REMOTO A LA RED

El acceso a los servicios proporcionados por la red de área local se realiza normalmente desde las estaciones conectadas a la misma LAN. Sin embargo, en ocasiones esto no es posible debido a la distancia geográfica que separa al cliente del servidor.

***Módem:** es un conversor analógico-digital que se utiliza para transmitir información digital por las líneas telefónicas apropiadas para la transmisión de señales analógicas. También suele aplicarse este término para el caso de los módems ADSL o los módems de cable.*

Los módems de cable, junto a los de la tecnología DSL, son los dos tipos principales de acceso a la Internet de banda ancha.

Redes de Área Local
Olga Minguet
4

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

TIPOS DE CONEXIONES A INTERNET

Redes de Área Local Olga Minguet 5

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

- DSL son las siglas de Digital Subscriber Line. Delante de estas siglas suele ponerse otra letra que identifica la familia específica dentro de DSL, por ello nos referiremos, en general, a tecnologías xDSL.
- Con ADSL se trata de aprovechar el mismo cableado del teléfono analógico (el par de cobre) para la transmisión de datos a Internet a alta velocidad estableciendo tres canales de comunicación sobre la misma línea física.

Redes de Área Local Olga Minguet 6

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

- Transmisión digital a través de la línea telefónica (mediante router).
- Conexión permanente (dedicada), no de conmutación.
- Utiliza frecuencias que no utiliza el teléfono por lo que es posible conectar Internet y hablar por teléfono a la vez.

Redes de Área Local Olga Minguet 7

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

Configuración de ADSL con splitter

Redes de Área Local Olga Minguet 8

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

- En una línea ADSL se establecen tres canales de comunicación:
 - canal de envío de datos,
 - canal de recepción de datos, y
 - canal de servicio telefónico normal.
- En ADSL hay que distinguir el ancho de banda de subida del de bajada, es decir, la velocidad a la que se pueden poner datos en la red y a la que se pueden descargar es diferente.

Esta conexión ha mejorado de ADSL a ADSL2 y, posteriormente ADSL2+, con rangos de subida de [0,5-3,3 Mbps] y rangos de bajada de [1,5-24 Mbps]. Aunque aún queda lejos de la Fibra óptica (de 300 Mbps)

Redes de Área Local Olga Minguet 9

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

Redes de Área Local Olga Minguet 10

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

- Esta tecnología se denomina **asimétrica** porque las capacidades de descarga (desde la red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden.
- La tecnología ADSL está diseñada para que la **capacidad de bajada o descarga sea mayor que la de subida**, lo que se corresponde con el uso de Internet por parte de la mayoría de usuarios finales, que reciben más información de la que envían (o descargan más de lo que suben).
- Esto se ha de tener en cuenta si tenemos una red con mucho tráfico de salida hacia Internet ya que la velocidad de subida es mucho menor que la de bajada.

Redes de Área Local Olga Minguet 11

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

- Las empresas de telefonía implantaron junto a las versiones mejoradas (ADSL2 y ADSL2+) mejoras para evitar interferencias o ruido, y disminuir los efectos de la atenuación, alcanzando distancias de hasta 9 km.
- ADSL es una tecnología que utiliza el par de cobre y tiene menos ancho de banda que otras tecnologías como **cable-módem**, pero presenta ventajas importantes como la posibilidad de dividir el ancho de banda en distintos canales, lo cual mejora considerablemente la calidad del servicio (**QoS**).

Redes de Área Local Olga Minguet 12

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

- En las instalaciones domésticas en las que se comparten varios supletorios telefónicos sobre la misma línea compartida con el servicio ADSL debe instalarse en cada teléfono un **microfiltro**.
- El microfiltro filtra la señal de envío y recepción de datos y **deja sólo la de voz para el teléfono**, ya que si no el teléfono la interpretaría como ruido.
- Este microfiltro no será necesario cuando el servicio de telefonía se realiza a través de Voz IP.



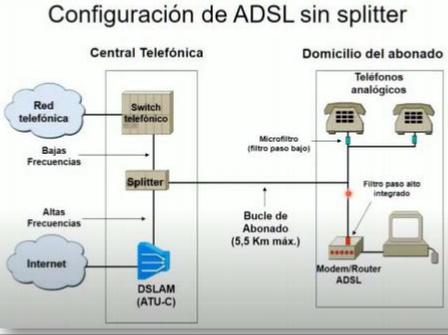
Redes de Área Local Olga Minguet 13

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

Configuración de ADSL sin splitter



Redes de Área Local Olga Minguet 14

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

- La tecnología **SDSL** es una variante de la DSL y se trata de una línea **simétrica** permanente con velocidades de hasta 3 Mbps, muy reducidas para los requerimientos actuales de una conexión a Internet.
- SDSL proporciona igual ancho de banda para subida y bajada de datos.** Generalmente es más costosa y menos disponible que ADSL.

DSL - Digital Subscriber Line.

HDSL - High-bit-rate Digital Subscriber Line.

S-HDSL - Single-Pair High-bit-rate Digital Subscriber Line.

SDSL - Symmetric Digital Subscriber Line.

ADSL - Asymmetric Digital Subscriber Line.

RADSL - Rate Adaptive Digital Subscriber Line.

VDSL - Very High-bit-rate Digital Subscriber Line.

Tipo	ADSL+	CDSL	HDSL/HDSL2	ISL	SDSL	VDSL/VDSL2
Frecuencia	2,2 MHz	1,1 MHz	196 kHz	196 kHz	196 kHz	12 MHz /30 MHz
Vel. Máx. Subida (upstream)	1,2 Mbps	Hasta 1 Mbps	1,544 Mbps /2,048 Mbps	Interfaz bidireccional (BRI) RDSI	2,048 Mbps	15 Mbps /100 Mbps
Vel. Máx. Bajada (downstream)	24 Mbps	16-128 Kbps	Lo mismo	Lo mismo	Lo mismo	55 Mbps /100 Mbps
Distancia máx. bucle local	2,5 km	4,5 km	4,5 km/4,5 km	5,5 km	3 km	300-1300 m

Redes de Área Local Olga Minguet 15

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

A) Tecnología ADSL

	ADSL	ADSL2	ADSL2+
Frecuencia	0,5 MHz	1,1 MHz	2,2 MHz
Velocidad Max. Subida	1 Mbps	1 Mbps	1,2 Mbps
Velocidad Max. Bajada	8 Mbps	12 Mbps	24 Mbps
Distancia	2 Km	2,5 Km	2,5 KM
Tiempo Sincronización	10-30 s	3 s	3 s
Corrección de Errores	No	Sí	Sí

Redes de Área Local Olga Minguet 16

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

B) Módems de cable

VIDEO

- Un módem de cable o cable-módem es un dispositivo que nos permite acceder a Internet a **alta velocidad** utilizando la infraestructura de las redes de televisión por cable (**CTV**).
- De esta forma los usuarios pueden estar recibiendo sus canales de televisión y simultáneamente estar transmitiendo y recibiendo datos de Internet.
- La señal se transmite a grandes velocidades por redes de **fibra óptica**, utilizándose segmentos de **cable coaxial** en los tramos de llegada a las viviendas.
- Las velocidades de transmisión son muy variables, puesto que se trata de **redes mixtas**, aunque la tecnología permite transmisiones mayores de los 100 Mbps. Actualmente se ofrecen conexiones a 500 Mbps.

Redes de Área Local Olga Minguet 17

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

B) Módems de cable

Redes de Área Local Olga Minguet 18

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

B) Módems de cable

Los abonados de un mismo vecindario comparten el ancho de banda proporcionado por una única línea de cable coaxial. Los cablemódems se utilizan principalmente para distribuir el acceso a Internet de banda ancha, aprovechando el ancho de banda que no se utiliza en la red de televisión por cable.

Redes de Área Local Olga Minguet 19

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

C) Módems de fibra

En la última década el ADSL ha sido lo más utilizado. Suponía menor coste comparado con las nuevas inversiones de crear nuevas infraestructuras en fibra. Sin embargo, las actuales necesidades de conexión exigen un ancho de banda muy superior que, de momento, sólo es capaz de ofrecer el FTTH.

Redes de Área Local Olga Minguet 20

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

C) Módems de fibra

- La tecnología de telecomunicaciones **FTTH** (Fiber To The Home), también conocida como fibra hasta el hogar, se basa en la utilización de **cables de fibra óptica** para la distribución de servicios avanzados hasta el domicilio del abonado.

Puede ofrecer anchos de banda de 1 Gbps o más.

- Con técnicas como WDM (Wavelength Division Multiplexing), conseguimos multiplexar varias señales sobre una sola fibra óptica, utilizando portadoras de diferente longitud de onda. De esta forma se incrementa la velocidad y la flexibilidad, pudiendo transmitir punto a punto y punto-multipunto.

Redes de Área Local Olga Minguet 21

UD4. Interconexión de equipos en redes locales (I)

1. EL ACCESO REMOTO A LA RED

C) Módems de fibra

15 de Febrero de 2019

El total de líneas de fibra óptica hasta el hogar (FTTH) sufre un crecimiento mensual de 129.132 líneas. El 46% del total de líneas FTTH corresponde a Movistar, con un parque de 3,9 millones de líneas.

A nivel anual, respecto a diciembre de 2017 destaca el aumento de 2 millones de líneas FTTH, frente a la pérdida de 1,3 millones de líneas con tecnología DSL, informa Servimedia.

El 89,2% del total de líneas se concentra en los tres principales operadores, **Movistar, Orange (incluido Jazztel) y Vodafone (incluido Ono)**. En un año, esta cuota conjunta se ha reducido en tres puntos.

Redes de Área Local Olga Minguet 22

UD4. Interconexión de equipos en redes locales (I)

Realiza las siguientes **ACTIVIDADES** del Cuaderno de Actividades:

- Actividad 1
- Actividad 2
- Actividad 3

Redes de Área Local Olga Minguet 23

UD4. Interconexión de equipos en redes locales (I)

ÍNDICE

1. EL ACCESO REMOTO A LA RED
 - A. Tecnología ADSL
 - B. Módems de cable
 - C. Módems de fibra
2. REPETIDORES Y CONCENTRADORES
3. PUENTES
4. CONMUTADORES
5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES
 - 5.1. Redes de área local virtuales o VLAN
 - 5.2. Enlaces entre conmutadores

Redes de Área Local Olga Minguet 24

UD4. Interconexión de equipos en redes locales (I)



Repetidores

Redes de Área Local Olga Minguet 25

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

- Las señales eléctricas se degradan al transmitirse. Cuando la longitud del cable de red es grande, la señal puede llegar al otro extremo casi imperceptible, lo que origina problemas graves en las transmisiones.
- El modo más básico de solucionar estos problemas consiste en la utilización de **repetidores** o concentradores (**hubs**).

Redes de Área Local Olga Minguet 26

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

Repetidores

- Los repetidores son dispositivos que se encargan de **regenerar la información**.
- Reciben una señal eléctrica que está perdiendo su intensidad y la concentran de modo tal que se mantenga siempre constante la calidad de la señal emitida.
- Un repetidor es capaz de limpiar la distorsión de la señal, de entrada, aplanándola y eliminando el ruido y la distorsión. Además la amplifica dándole más energía.
- Cabe recordar que los repetidores **NO procesan la señal**, simplemente la regeneran.

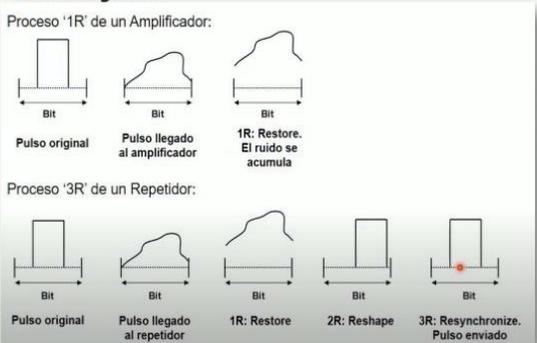


Redes de Área Local Olga Minguet 27

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

Repetidores: re-genera



Proceso '1R' de un Amplificador:

Bit Bit Bit

Pulso original Pulso llegado al amplificador 1R: Restore. El ruido se acumula

Proceso '3R' de un Repetidor:

Bit Bit Bit Bit Bit

Pulso original Pulso llegado al repetidor 1R: Restore 2R: Reshape 3R: Resynchronize. Pulso enviado

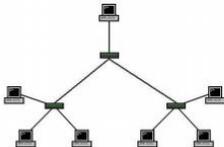
Redes de Área Local Olga Minguet 28

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

Repetidores

- Se dice que varios elementos están **instalados en cascada** o de modo jerárquico cuando están conectados entre ellos de modo que la **salida de uno está conectada a la entrada de otro**.
- Teóricamente es posible instalar tantos repetidores en una red como sean necesarios, sin embargo, en la práctica no se recomienda su instalación en cascada en gran número.



Redes de Área Local Olga Minguet 29

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

Repetidores

- Los repetidores operan en el **nivel físico**, puesto que trabajan con señales. Esto hace que sean **rápidos**, ya que **no procesan los datos** que circulan por ellos.
- En ocasiones, los repetidores se pueden utilizar para convertir la señal de un sistema de cableado en otro.

		
Repetidor coaxial-Ethernet	Repetidor fibra-Ethernet	Repetidor Wireless-Ethernet

Redes de Área Local Olga Minguet 30

UD4. Interconexión de equipos en redes locales (I)

Concentrador o Hub



Redes de Área Local Olga Minguet 31

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

Concentradores (hub)

- La **ventaja principal** de un hub reside en la facilidad de operación: **se limita a copiar bits** de un segmento de red en otros.
- **No requiere de ningún tipo de configuración especial**. Simplemente **repite la señal** de la red a **gran velocidad**.



Redes de Área Local Olga Minguet 32

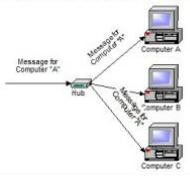
UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

Concentradores (hub)

- La **mayor limitación** del hub consiste en que **difunde por todos sus otros puertos** cualquier trama que le llega por uno de ellos.
- No aísla de los problemas del tráfico generado en la red en cada uno de los segmentos. Al contrario, al difundir **cualquier trama que llega a sus puertos**, generan una gran cantidad de difusión, aumentando de forma considerable el tráfico de red.

Conforme le llega la trama, el HUB la repite al resto de ordenadores



Redes de Área Local Olga Minguet 33

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

El punto de acceso o Access Point (AP)

- Conocido por las siglas WAP (**Wireless Access Point**), o AP (**Access Point**) es un dispositivo de red **similar a un hub** y es **inalámbrico**.
- WAP se suele instalar en **redes pequeñas** (domésticas u oficinas). Actualmente mejorado con **WEP/WEP2**.



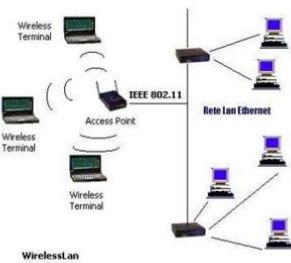
Redes de Área Local Olga Minguet 34

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

El punto de acceso o Access Point (AP)

El AP (Punto de acceso) hace de **intermediario** entre los equipos Wi-fi y una red Ethernet cableada.



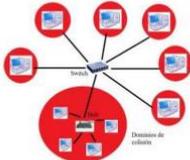
Redes de Área Local Olga Minguet 35

UD4. Interconexión de equipos en redes locales (I)

2. REPETIDORES Y CONCENTRADORES

- Tanto repetidores como hubs **no pueden aislar el tráfico de broadcast o multidifusión**. Esto puede llevar a **congestiones** serias en la red.
- Por lo tanto, un repetidor o un concentrador **nunca dividen un dominio de colisión** y no serán capaces de para las tormentas de tramas de multidifusión.

***Dominio de colisión:** dos nodos de la red pertenecen al mismo dominio de colisión si sus tramas pueden interferir entre sí.*



- El repetidor y el hub operan con señales eléctricas, por eso es un dispositivo que **sólo contempla la capa física** para unir los nodos origen y destino.

Redes de Área Local Olga Minguet 36

UD4. Interconexión de equipos en redes locales (I)





Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 4
- Actividad 5

Redes de Área Local Olga Minguet 37

UD4. Interconexión de equipos en redes locales (I)



ÍNDICE

1. EL ACCESO REMOTO A LA RED
 - A. Tecnología ADSL
 - B. Módems de cable
 - C. Módems de fibra
2. REPETIDORES Y CONCENTRADORES
3. PUENTES
4. CONMUTADORES
5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES
 - 5.1. Redes de área local virtuales o VLAN
 - 5.2. Enlaces entre conmutadores

Redes de Área Local Olga Minguet 38

UD4. Interconexión de equipos en redes locales (I)




Redes de Área Local Olga Minguet 39

UD4. Interconexión de equipos en redes locales (I)



3. PUENTES

- El puente o bridge es un elemento de **cierta capacidad de control**. Puede aceptar y reexpedir (reenviar) las **tramas** que le llegan **en función del contenido** de las mismas.
- Los puentes operan en el nivel 2 de OSI. De modo que solo pueden operar con direcciones MAC. **Separan redes a nivel MAC.**



Redes de Área Local Olga Minguet 40

UD4. Interconexión de equipos en redes locales (I)

3. PUENTES

¿Para qué se usan los puentes?

- Para conectar dos o más LANs **del mismo tipo**.
- **Mejorar el rendimiento**, ya que sirven para separar el tráfico local.
- **Seguridad**, ya que generan subredes reduciendo el tráfico de broadcast.
- **Fiabilidad**, ya que un problema en una subred no afecta a toda la red. Actúan como puertas cortafuegos.
- Recomendados para conectar redes con **poco tráfico**.

Redes de Área Local Olga Minguet 41

UD4. Interconexión de equipos en redes locales (I)

3. PUENTES

Cuando un puente debe pasar una trama de un segmento a otro de la red ejecuta una serie de **fases**:

- 1) **Almacena** en su memoria la trama recibida por cualquier puerto para su análisis posterior.
- 2) **Comprueba** el campo de control de errores de la trama con el fin de asegurarse de la integridad de la misma.
 - Si encontrara un **error**, eliminaría la trama de la red, con lo que las tramas erróneas o incompletas no traspasarán este tramo de la red.
 - Algunos puentes son capaces de **retocar** de modo sencillo el formato de la trama con el fin de adecuarla al formato del segmento destinatario del mismo.
- 3) El puente **reexpide** (reenvía) la trama si determina que el destinatario se encuentra en un segmento de red accesible por alguno de sus puertos.

Redes de Área Local Olga Minguet 42

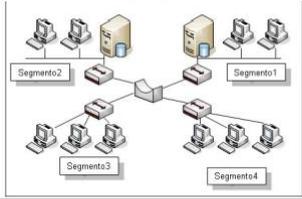
UD4. Interconexión de equipos en redes locales (I)

3. PUENTES

- A este aislamiento de tráfico que se opera en los puentes o en dispositivos de red de nivel superior se le suele denominar **“separación de los dominios de colisión”**.
- Las tramas de dos estaciones situadas en diferentes segmentos **no pueden colisionar**, ya que no pueden atravesar la frontera de los segmentos de red, salvo que el puente decida que pueden atravesarlas.

El dibujo muestra un puente separando 4 segmentos de red.

Se han creado 4 dominios de colisión.

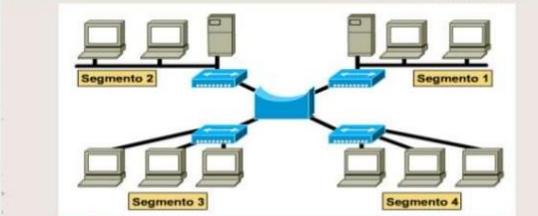


Redes de Área Local Olga Minguet 43

UD4. Interconexión de equipos en redes locales (I)

3. PUENTES

Segmentación con puentes



- La segmentación permite reducir la cantidad de usuarios por segmento
- Los puentes guardan y luego envían todas las tramas basándose en las direcciones de capa 2

Redes de Área Local Olga Minguet 44

UD4. Interconexión de equipos en redes locales (I)

3. PUENTES

Redes de Área Local Olga Minguet 45

UD4. Interconexión de equipos en redes locales (I)

3. PUENTES

Tradicionalmente los puentes se clasifican en:

Transparentes	Es un puente que no requiere ninguna configuración para su funcionamiento. Determina la reexpedición de las tramas en función de los sucesos que observa en cada uno de sus puertos.
No transparentes	Es un puente que necesita que la trama lleve información sobre el nodo en que debe ser reexpedida (reenviada).

Redes de Área Local Olga Minguet 46

UD4. Interconexión de equipos en redes locales (I)

Funcionamiento de un puente transparente

Dirección	Interfaz
A	α
B	β
C	α

- A genera una trama con destino B que el puente recibe por α .
- El puente busca a B en su tabla de direcciones; como no la encuentra reenvía la trama por β .
- El puente incluye la dirección de A en su tabla de direcciones asociada a la interfaz α .
- Cuando B envía una trama de respuesta el puente incluirá la dirección de B en la tabla, asociada a la interfaz β .
- Más tarde C envía una trama hacia A. El puente la recibe por α pero no la reenvía por β pues ya sabe que A está en α .
- Al ver la dirección de origen de esta trama el puente asocia C con α .

Redes de Área Local Olga Minguet 47

UD4. Interconexión de equipos en redes locales (I)

3. PUENTES

Otra clasificación de los puentes es:

Locales	Un puente local aglutina en sí dos o más segmentos de la misma red LAN
Remotos	Un puente remoto está dividido en dos partes. Cada una de las partes conecta un segmento de red. Las dos partes están conectadas a través de la línea de una red WAN.

Redes de Área Local Olga Minguet 48

UD4. Interconexión de equipos en redes locales (I)

3. PUENTES

Puentes locales y remotos

(a)

(b)

Redes de Área Local Olga Minguet 49

UD4. Interconexión de equipos en redes locales (I)

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 6
- Actividad 7

Redes de Área Local Olga Minguet 50

UD4. Interconexión de equipos en redes locales (I)

ÍNDICE

1. EL ACCESO REMOTO A LA RED
 - A. Tecnología ADSL
 - B. Módems de cable
 - C. Módems de fibra
2. REPETIDORES Y CONCENTRADORES
3. PUENTES
4. CONMUTADORES
5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES
 - 5.1. Redes de área local virtuales o VLAN
 - 5.2. Enlaces entre conmutadores

Redes de Área Local Olga Minguet 51

UD4. Interconexión de equipos en redes locales (I)

Conmutadores

Switches

Redes de Área Local Olga Minguet 52

UD4. Interconexión de equipos en redes locales (I)

4. CONMUTADORES

- El **switch** o conmutador es un dispositivo que tiene funciones del **nivel 2 de OSI** y que, por tanto, se parece a un puente (*bridge*) en cuanto a su funcionamiento. Trabaja en la capa de enlace.
- En la actualidad se comercializan también conmutadores de **nivel 3**, que incorporan también funciones de **encaminamiento** y con la velocidad de la conmutación.
- Su **función** es **interconectar** dos o más segmentos de red **pasando datos** de un segmento a otro de acuerdo con la **dirección MAC** de destino de las tramas en la red.
- Los **conmutadores** son en la actualidad los dispositivos **más utilizados** para realizar el despliegue de la red.
- Los **repetidores y concentradores** sólo se utilizan en casos muy específicos y siempre **minoritarios**.



Redes de Área Local Olga Minguet 53

UD4. Interconexión de equipos en redes locales (I)

4. CONMUTADORES

Tienen algunas **características** que lo distinguen:

- El *switch* es siempre **local**. No se utiliza para conexiones remotas.
- Son dispositivos **multipuerto**. Las tramas se **envían sólo a los puertos de destino**.
- La **velocidad** de operación del *switch* es **mayor** que la del puente remoto.
- En un conmutador se puede **repartir el ancho de banda** de la red de una manera apropiada en cada segmento de red o en cada nodo.

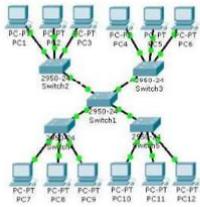
Redes de Área Local Olga Minguet 54

UD4. Interconexión de equipos en redes locales (I)

4. CONMUTADORES

A diferencia de los concentradores, los conmutadores **no se suelen instalar en cascada**. La razón es que en cascada se incrementan los retardos de la red.

Lo habitual es instalarlos **en estrella**.



Redes de Área Local Olga Minguet 55

UD4. Interconexión de equipos en redes locales (I)

4. CONMUTADORES

Funcionamiento de un conmutador:

- El conmutador construye una **tabla por cada puerto** con las direcciones físicas (MAC) de los dispositivos que ve.
- Cuando le llega una trama **investiga en sus tablas** para averiguar por qué puerto de todos los disponibles alcanza su destino.
- Transmite la trama por ese puerto de destino, **y sólo por ese**.

Redes de Área Local Olga Minguet 56

UD4. Interconexión de equipos en redes locales (I)

4. CONMUTADORES

Por ejemplo, si al *switch* del siguiente dibujo le llega una trama cuya dirección física de destino es MAC4,

- 1) el conmutador buscará esa dirección entre sus tablas de direcciones,
- 2) la hallará disponible en el puerto 2 y conmutará la trama para que salga por ese puerto.
- 3) la trama llegará al hub conectado al puerto 2
- 4) el hub la transmitirá por todos sus puertos llegando a las estaciones PC4 y PC5.
- 5) Sólo la estación PC4 la cogerá, ya que es el destino.

Redes de Área Local Olga Minguet 57

UD4. Interconexión de equipos en redes locales (I)

4. CONMUTADORES

Al igual que los puentes, los conmutadores **permiten limitar las tormentas de difusión.**

Redes de Área Local Olga Minguet 58

UD4. Interconexión de equipos en redes locales (I)

Realiza las siguientes **ACTIVIDADES** del Cuaderno de Actividades:

- **Actividad 8**
- **Actividad 9**
- **Actividad 10**

Redes de Área Local Olga Minguet 59

UD4. Interconexión de equipos en redes locales (I)

ÍNDICE

1. EL ACCESO REMOTO A LA RED
 - A. Tecnología ADSL
 - B. Módems de cable
 - C. Módems de fibra
2. REPETIDORES Y CONCENTRADORES
3. PUENTES
4. CONMUTADORES
5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES
 - 5.1. Redes de área local virtuales o VLAN
 - 5.2. Enlaces entre conmutadores

Redes de Área Local Olga Minguet 60

UD4. Interconexión de equipos en redes locales (I)

VLAN ASIMÉTRICAS

Redes de Área Local Olga Minguet 61

UD4. Interconexión de equipos en redes locales (I)

VLANS 802.1q

Redes de Área Local Olga Minguet 62

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

- Las redes de área local son muy dependientes del cableado.
- El cambio de posición geográfica de un usuario de una red supone modificar la **configuración del cableado de red**, lo que casi siempre es imposible.
- La tecnología **VLAN** (Virtual LAN) permite que los nodos de la red se conecten a **redes lógicas** en vez de a redes físicas.

Redes de Área Local Olga Minguet 63

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.1. Redes de área local virtuales o VLAN

Cada VLAN está formada por un **grupo lógico** de estaciones físicamente unidas a los puertos de uno o más conmutadores que son gestionadas en grupo **como si estuvieran en la misma red de área local física**.

Redes de Área Local Olga Minguet 64

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.1. Redes de área local virtuales o VLAN

- En lo que concierne a la **seguridad**, hay que tener en cuenta que los dispositivos pertenecientes a una VLAN **no tienen acceso** a los que se encuentren en otras y viceversa.
- Resulta útil cuando queremos **segmentar los equipos y limitar el acceso** entre ellos por temas de seguridad.
- Otro beneficio en una VLAN es que con un switch podemos tener varias redes sin necesidad de comprar varios equipos.

Redes de Área Local Olga Minguet 65

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.1. Redes de área local virtuales o VLAN

- La pertenencia a una VLAN puede estar asignada:
 - manualmente (**VLAN estáticas**).
 - dinámicamente (**VLAN dinámicas**), mediante un registro automático a través del **protocolo GVRP** (Generic VLAN Registration Protocol).
- El estándar más frecuente de creación de VLAN es el **IEEE802.1Q** o **VLAN Tagging**. Gracias a él se pueden definir VLAN a través de la red con independencia del fabricante de los conmutadores.

Redes de Área Local Olga Minguet 66

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.1. Redes de área local virtuales o VLAN

Principales **ventajas** que proporciona una VLAN:

- Mejoras en la velocidad** de la red por una mejora en la gestión de los puertos de comunicaciones.
- Incremento del ancho de banda** o mejora de la asignación del mismo en función de las necesidades.
- Incremento de la seguridad de la red** por segregación de usuarios con necesidades especiales o por aislamiento de conexiones que generen excesivo tráfico y que puedan dañar el rendimiento global de la red.
- Generación de grupos de dispositivos** con protocolos obsoletos e incompatibles con el tráfico habitual de la red y que se canalizarán a través de una VLAN específica.

Redes de Área Local Olga Minguet 67

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.1. Redes de área local virtuales o VLAN

Las VLAN permiten que los nodos de la red se agrupen según unos criterios lógicos denominados **polícies** o **políticas de conexión** que los independizan de su ubicación haciendo que dos nodos que pertenecen a segmentos distintos de la red pertenezcan de hecho a la misma VLAN.

Redes de Área Local Olga Minguet 68

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.1. Redes de área local virtuales o VLAN

Tipos de redes VLAN según las políticas de conexión (policies):

VLAN con asignaciones de direcciones MAC	Los conmutadores de la red crean grupos lógicos con direcciones MAC de los nodos a los que tienen acceso.
VLAN con asignaciones de puertos	Es una VLAN semejante a la anterior, con la peculiaridad de que las asociaciones se realizan agrupando puertos del conmutador en vez de direcciones MAC de los nodos. Es la más usada.
VLAN por tipo de protocolo	La VLAN queda determinada por el tipo de protocolo . Por ejemplo, se asociaría VLAN1 al protocolo IPv4, VLAN2 al protocolo IPv6, VLAN3 a AppleTalk, VLAN4 a IPX
VLAN de niveles superiores	Se crea una VLAN para cada aplicación : FTP, flujos multimedia, correo electrónico....

Redes de Área Local Olga Minguet 69

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.1. Redes de área local virtuales o VLAN

Los switches tienen dos tipos de puertos: **access** y **trunk**.

Puertos access:

- ✓ La principal utilidad que se les da a este tipo de puertos es **para conectar equipos finales**.
- ✓ Sólo transportan tráfico de **una sola VLAN**.
- ✓ **No** es recomendable usarlos **para conectar switches entre sí**, ya que una implementación de este tipo **no es escalable**.

El switch es quien le pone al paquete el identificador de la vlan a la que pertenece.

Redes de Área Local Olga Minguet 70

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.1. Redes de área local virtuales o VLAN

Los switches tienen dos tipos de puertos: **access** y **trunk**.

Puertos trunk:

- ✓ La principal utilidad que se les da a este tipo de puertos es **para realizar la conexión entre switches**.
- ✓ Un puerto trunk puede **transportar tráfico de múltiples VLANs**.
- ✓ Podemos tener **múltiples VLANs** en los switches y solo un enlace para transportar todo el tráfico.

Redes de Área Local Olga Minguet 71

UD4. Interconexión de equipos en redes locales (I)

ENLACES TRUNKS VLANS

Redes de Área Local Olga Minguet 72

UD4. Interconexión de equipos en redes locales (I)

5. TECNOLOGÍAS ESPECÍFICAS DE LOS CONMUTADORES

5.2. Enlaces entre conmutadores

- En las instalaciones reales es habitual tener que utilizar **más de un conmutador** para dar servicio a todos los usuarios, bien porque el número de usuarios sea muy elevado y supera el número de puertos del *switch* o bien porque la red se extiende geográficamente por zonas a las que un único conmutador no podría llegar.
- Los conmutadores **se enlazan entre sí** a través de unos segmentos de red que los unen y que transportan el tráfico entre ellos.
- Técnicamente, a un segmento que une dos conmutadores se le denomina **uplink** y los conmutadores suelen tener un puerto específico para ello. Los puertos uplink se suelen conectar con cable cruzado.



Uplink Ports

Redes de Área Local Olga Minguet 73

UD4. Interconexión de equipos en redes locales (I)



Realiza las siguientes **ACTIVIDADES** del Cuaderno de Actividades:

- **Actividad 11**
- **Actividad 12**

Redes de Área Local Olga Minguet 74

8.4.2 Cuaderno de actividades

Cuaderno de Actividades

-UNIDAD 4-
Interconexión de equipos en redes locales (I)

CUADERNO DE ACTIVIDADES

Objetivos

- Consolidar los contenidos vistos en la Unidad 4 del curso de Redes de Área Local.
- Se han descrito los principios de funcionamiento de las redes locales.
- Se han reconocido los principios funcionales de las redes locales.
- Se han identificado los distintos tipos de redes y los protocolos.
- Se han configurado los parámetros básicos.
- Se han aplicado mecanismos básicos de seguridad.

Actividades

1. Busca los errores técnicos en el siguiente razonamiento:

“Mi portátil tiene integrado un modem analógico. He contratado un acceso ADSL con mi compañía telefónica y me han comunicado que me lo servirán por mi línea actual de teléfono analógica. Para evitar tener que comprar un modem ADSL, utilizaré mi modem que, al ser analógico, es compatible con el servicio ADSL que me enviarán por mi línea de teléfono analógica.”

2. Haz una búsqueda e indica en la siguiente tabla comparativa ventajas e inconvenientes del ADSL y del cable-modem.

	Ventajas	Inconvenientes
ADSL		
CABLE-MODEM		

CUADERNO DE ACTIVIDADES

3. Realiza una tabla también con las principales diferencias entre ADSL y Fibra óptica.

	Ventajas	Inconvenientes
ADSL		
FIBRA OPTICA		

4. Una red local está compuesta por varios segmentos de red. Los segmentos están unidos por medio de un segmento de interconexión. Una estación de la red está infectada con un virus de tipo gusano y está generando mucho tráfico Ethernet en el segmento de red en que está la estación.

Razona ambas respuestas:

a) ¿Pasa el tráfico de red de un segmento a otro si el dispositivo de interconexión es un repetidor?

b) ¿Y si es un concentrador?

5. Seguimos trabajando sobre la configuración de red del ejercicio precedente. Ahora vamos a suponer que el cableado de red es coaxial y lo que ocurre es que se rompe uno de los segmentos de red. Como la red

CUADERNO DE ACTIVIDADES

queda abierta, el segmento de red en que se ha producido la rotura deja de funcionar.

a) ¿Funcionarán el resto de los segmentos de red si el dispositivo de interconexión es un repetidor?

b) ¿Y si la red fuera de cable de pares en vez de coaxial y el dispositivo de interconexión fuera un concentrador?

6. Descubre los errores técnicos en el siguiente argumento:

“En mi oficina hay dos departamentos claramente diferenciados. En cada uno de ellos se genera mucho tráfico, pero apenas tienen relación entre sí.

Se ha pensado en instalar un puente entre las dos redes departamentales, pero no hemos podido puesto que las dos redes están en el mismo edificio y los puentes solo pueden operar remotamente”.

7. Una compañía tiene sede en dos ciudades, pero sólo poseen una red local compartida entre las dos sedes y conectadas por un puente de red a través de redes públicas.

El segmento de red de una de las ciudades es minoritario, pero en la otra sede residen los servidores y en su segmento de red se produce mucho tráfico local.

CUADERNO DE ACTIVIDADES

a) ¿Pasará ese tráfico al segmento de red minoritario?

--

b) Un usuario de la sede minoritaria quiere enviar un fichero al servidor que reside en la sede mayoritaria a través del puente. A pesar de que el puente aísla del tráfico local, ¿podrá hacerlo?

--

8. Di si son verdaderas o falsas las siguientes afirmaciones y justifica porqué:

Los conmutadores son más rápidos que los puentes	
Cierto/falso	
Justificación	

Un conmutador es siempre local	
Cierto/falso	
Justificación	

El conmutador, como el puente, no puede gestionar el ancho de banda	
Cierto/falso	
Justificación	

Todos los conmutadores se pueden escalar	
--	--

CUADERNO DE ACTIVIDADES

Cierto/falso	
Justificación	

9. Indica en la siguiente tabla de resumen las características más importantes de los dispositivos que hemos visto.

	Repetidor	Concentrador	Puente	Conmutador
Nivel OSI				
Tiene lógica de control (Si/No)				
Se puede conectar en cascada (Si/No)				
Segmenta la red (Si/No)				
Restringe multidifusión (Si/No)				

CUADERNO DE ACTIVIDADES

Opera con MAC (Si/No)				
Se usa en LAN (Si/No)				
Puede conectar redes en remoto (Si/No)				
Velocidad (Alta/Media/Baja)				

10. Vamos a hacer una tabla en la que indiquemos las principales ventajas y desventajas de los dispositivos que hemos visto:

	Ventajas	Inconvenientes
repetidores		
concentradores (hub)		
puentes (bridges)		
conmutadores (switches)		

11. ¿Es posible crear VLAN utilizando conmutadores? Justifica la respuesta.

UD04 – Interconexión de equipos en redes locales (I)

7-9

CUADERNO DE ACTIVIDADES

¿Y utilizando concentradores? Justifica la respuesta.

12. Busca en las sedes web de 3 fabricantes de dispositivos de red información técnica y comercial sobre conmutadores.

Compara los distintos modelos de varios fabricantes para familiarizarte con las características básicas de este tipo de dispositivos. Consigue además los precios para compararlos.

Ayuda: las comparativas de precios no se hacen por conmutador, sino por puertos, es decir, se divide el precio total del conmutador por el número de puertos que posee.

Se propone hacer una comparativa para:

- a) Un concentrador de 8 puertos de cada fabricante

- b) Para uno de estos fabricantes, un hub de 8 puertos frente a un switch de 8 puertos.

UD04 – Interconexión de equipos en redes locales (I)

8-9

CUADERNO DE ACTIVIDADES

- c) Para uno de estos fabricantes, un switch de 24 puertos frente a otro de la misma marca y de 48 puertos

8.4.3 Cuaderno de prácticas

Guía del Cuaderno de PRÁCTICAS - UNIDAD 4 - Packet Tracer

Interconexión de equipos en redes locales (I)

Nombre y apellidos

Desarrollo
<ul style="list-style-type: none"> ✓ 1ª PARTE: Configurar una red local básica con punto de acceso y hub. ✓ 2ª PARTE: Enlace de redes híbridas. ✓ 3ª PARTE: Configuración de VLAN's en Packet Tracer.

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

Introducción

Este conjunto de actividades pretende que el alumno conozca las funcionalidades básicas generales y avanzadas, acerca del funcionamiento de la herramienta que provee CISCO llamada PACKET TRACER. Esta herramienta sirve para poner en marcha la construcción de redes de ordenadores, sin la necesidad de tener dispositivos de hardware o software adicionales a la maquina en la que está instalado esta herramienta.

Permite crear redes, permitiendo su configuración real, en el IOS que provee CISCO en sus routers. Esto agrega un gran valor, pues esta herramienta dispone de interfaces de hardware genéricas y específicas de dicha empresa. No necesitando tener ordenadoras, routers, interfaces, cables, etc., para saber el comportamiento físico y real de una red. Ahorrando así, tiempo en construcción de redes. Muchos paquetes de configuración de routers utilizando una versión parecida a la que provee IOS. Por lo que solamente se necesita saber las variantes que existen, si las hubiera.

Objetivos

- Consolidar los contenidos vistos en esta unidad didáctica 4 del curso de Redes de Área Local.
- Aprender a configurar redes de ordenadores, en un nivel básico.
- Utilizar la herramienta Cisco Packet Tracer.
 - Utilizar comandos de consola de IOS
 - Utilizar interfaces gráficas para la configuración.
 - Uso de protocolos de enrutamiento dinámico.
- Disposiciones de configuraciones reales de ordenadores a pequeña y gran escala.

Consideraciones



Esta imagen indica que el resultado de la tarea a realizar ha de ser indicado en el Cuaderno de la Actividad. Las capturas de pantalla se han de hacer con la herramienta **Recortes** de Windows

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

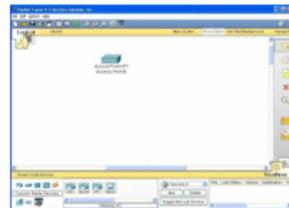
1ª PARTE: CONFIGURAR UNA RED LOCAL BÁSICA CON PUNTO DE ACCESO Y HUB

IMPORTANTE: La red que vamos a crear se debe guardar con el nombre **PRÁCTICA 4.1.pkt** y después subirlo a la tarea correspondiente de TEAMS.

A continuación, se hará un montaje bastante básico de una red inalámbrica mediante un Punto de Acceso (Access Point).

Paso 1.1:

Se desea implementar una red LAN en forma inalámbrica, constituida por dos equipos mediante el uso de un Access Point. Para ello, lo primero es dibujar el un *Access Point* Genérico, el cual se encuentra en el menú Dispositivos Inalámbricos.



Paso 1.2:

Posteriormente se dibujan los dos PCs con **tarjeta inalámbrica**, los cuales se encuentran ya configurados en la opción Custom Made Devices, el cual al dibujarlo comienza a negociar



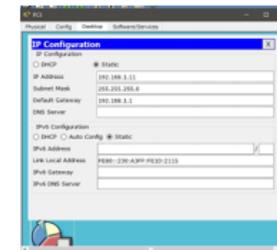
UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

con el Access Point hasta establecer una conexión inalámbrica con él, tal como se muestra en la siguiente figura.

Paso 1.3:

Definir en cada uno de los PCs una dirección IP, la cual por el momento se hará de manera **estática**. A los PCs se les configurará con las direcciones IP **192.168.1.11** y **192.168.1.12**, utilizando máscara por defecto y dirección de Gateway **192.168.1.1** tal como se ilustra en la figura siguiente.



- Realiza la actividad Paso 1.3 del Cuaderno de Actividades

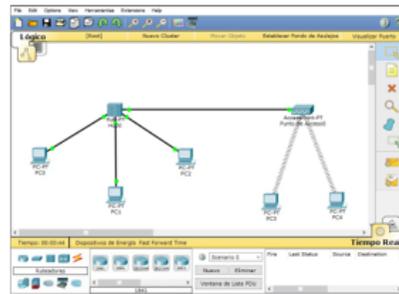
Paso 1.4:

Hasta aquí simplemente se ha implementado una red inalámbrica básica, sin embargo, muchas veces es necesario interconectar redes alámbricas cableadas con redes inalámbricas.

A continuación, vamos a integrar la red que has diseñado junto con una red de interconexión de host en forma cableada y utilizando direcciones IP estáticas que pertenezcan a la misma red pero que no se repitan. También deben tener la misma máscara de red y puerta de enlace. Sin embargo, para que exista comunicación entre los equipos de la red cableada y los equipos de la red inalámbrica, debe existir una conexión física entre los equipos concentradores, es decir, entre el hub y el Acces point. Por tal razón, es necesario conectar a éstos dos dispositivos mediante un cable de conexión directa, tal y como se ilustra en la siguiente figura.

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS



-Realiza la actividad Paso 1.4 del Cuaderno de Actividades

**2ª PARTE:
ENLACE DE REDES HIBRIDAS**

En el diseño anterior, has comprobado que al usar hubs, que son dispositivos que sólo trabajan en el nivel 1 de OSI, las tramas se propagan a todos los dispositivos de la red, generando un gran tráfico de red innecesario.

En este apartado vamos a modificar el diseño anterior para conectar las dos redes mediante diferentes dispositivos vistos en esta unidad.

Paso 2.1:

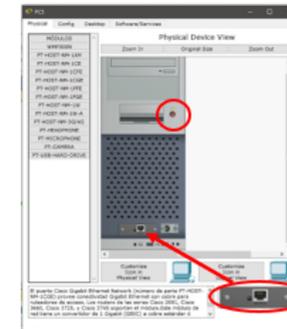
Primero vamos a eliminar el Punto de Acceso y lo vamos a sustituir por un hub. Quedará un diseño de red como el siguiente. Ten en cuenta que los ordenadores conectados al punto de acceso tienen interfaz inalámbrica. Para poder conectarlos al hub has de configurar en ellos una interfaz Ethernet.

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

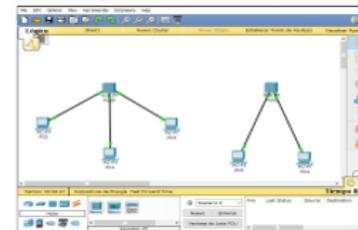
Para ello has de seguir los siguientes pasos:

- Doble clic en el pc a configurar
- Pulsar el botón de off para poder cambiar su hardware
- Arrastrar la interfaz inalámbrica que tiene instalada al apartado de módulos. Comprobaras que el hueco que ocupaba queda libre.
- Seleccionar en módulos uno que tenga conector rj-45 y arrastrarlo al hueco que ha quedado libre.
- Pulsar el botón de On para encender el pc.
- Comprobar que la dirección IP y puerta de enlace que tiene es correcta.



Repetimos los pasos con el otro ordenador inalámbrico.

Quedará una red como la siguiente:

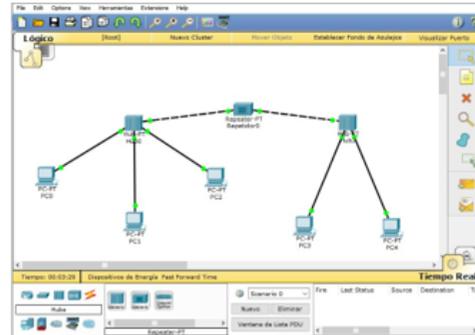


UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

Paso 2.2:

En este paso vamos a unir las dos redes mediante un **repetidor**. Para ello deberás diseñar una red como la siguiente:



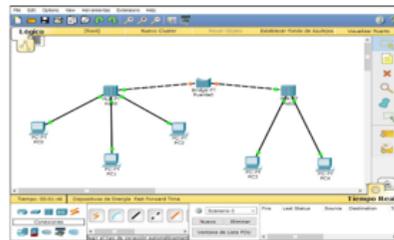
IMPORTANTE: La red que has creado hasta aquí se debe guardar con el nombre **PRÁCTICA 4.2.pkt** y después subirlo a la tarea correspondiente de TEAMS.



-Realiza la actividad Paso 2.2 del Cuaderno de Actividades

Paso 2.3:

En este paso vamos a unir las dos redes mediante un **punto**. Para ello deberás diseñar una red como la siguiente:



UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

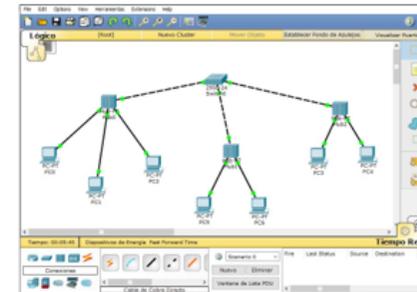
IMPORTANTE: La red que has creado hasta aquí se debe guardar con el nombre **PRÁCTICA 4.3.pkt** y después subirlo a la tarea correspondiente de TEAMS.



-Realiza la actividad Paso 2.3 del Cuaderno de Actividades

Paso 2.4:

En este paso vamos a unir las dos redes mediante un **Switch 2950-24**. Además, vamos a añadir una tercera red con dos ordenadores más. Recuerda que para que la red sea operativa debes asignar IPs válidas a los ordenadores. Para ello deberás diseñar una red como la siguiente:



IMPORTANTE: La red que has creado hasta aquí se debe guardar con el nombre **PRÁCTICA 4.4.pkt** y después subirlo a la tarea correspondiente de TEAMS.



-Realiza la actividad Paso 2.4 del Cuaderno de Actividades

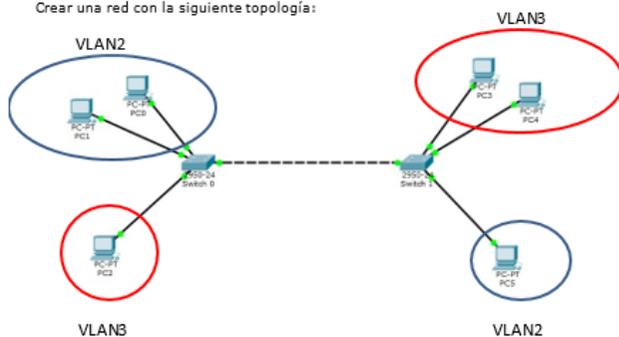
3ª PARTE: CONFIGURACIÓN DE VLAN'S EN PACKET TRACER

IMPORTANTE: La red que has creado hasta aquí se debe guardar con el nombre **PRÁCTICA 4.5.pkt** y después subirlo a la tarea correspondiente de TEAMS.

A continuación, se hará un montaje básico de una red VLAN en Packet Tracer.

Paso 3.1:

Crear una red con la siguiente topología:



El funcionamiento de la red ha de ser el siguiente:

- PC0, PC1 y PC5 pertenecen a la misma VLAN (VLAN2), por lo que se pueden comunicar mutuamente.
- PC2, PC3 y PC4 pertenecen a la misma VLAN (VLAN3), por lo que se pueden comunicar mutuamente.
- En cambio, un pc de VLAN2 no podrá comunicarse con un pc de VLAN3 y viceversa.

NOTAS:

- Cada PC debe tener una IP distinta, perteneciente al rango de IP de su vLAN correspondiente.
- Dentro de un rango de IP como 192.168.1.0, la primera IP (192.168.1.1) está restringida para el default gateway.

La configuración de los PC's debería quedar así:

VLAN2 (192.168.1.0)	
PC0	IP: 192.168.1.2 Máscara: 255.255.255.0 Default gateway: 192.168.1.1
PC1	IP: 192.168.1.3 Máscara: 255.255.255.0 Default gateway: 192.168.1.1
PC5	IP: 192.168.1.4 Máscara: 255.255.255.0 Default gateway: 192.168.1.1

VLAN3 (192.168.2.0)	
PC2	IP: 192.168.2.2 Máscara: 255.255.255.0 Default gateway: 192.168.2.1
PC3	IP: 192.168.2.3 Máscara: 255.255.255.0 Default gateway: 192.168.2.1
PC4	IP: 192.168.2.4 Máscara: 255.255.255.0 Default gateway: 192.168.2.1

Paso 3.2: Configuración del switch0.

En este paso vamos a crear la VLAN2 y la VLAN3 en la base de datos de VLANs del switch0. Para ello vamos a sus propiedades > pestaña Config > Base de Datos de la VLAN.

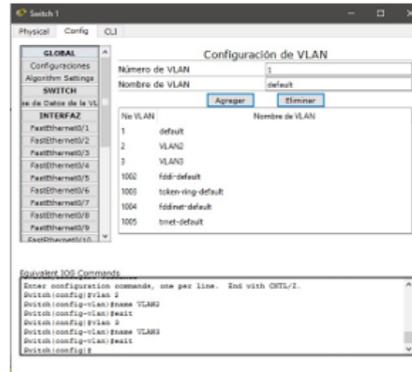
Indicamos:

- Número de VLAN: 2
- Nombre de VLAN: VLAN2

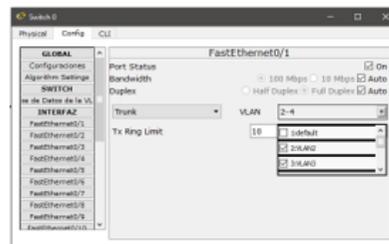
Fijate que en la consola inferior aparecen los comandos equivalentes que se ejecutan. Sería lo mismo ejecutar estos comandos desde la pestaña CLI.

Repetimos el proceso y creamos 3:VLAN3 también.

UD04 Interconexión de equipos en redes locales (1) PRÁCTICAS

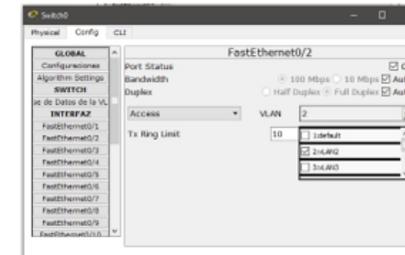


Identifica qué interfaz del switch0 se conecta al otro switch. Para ella tendrás que ir a sus propiedades y asignar el puerto TRUNK. Comprueba que SÓLO las VLAN2 y VLAN3 están activadas para permitir el tráfico entre ellas a través del switch0.



Identifica qué interfaces del switch son las que están conectadas a PC0, PC1 y a PC6. Para las TRES tendrás que ir a sus propiedades y asignar el puerto ACCESS a la VLAN2 que acabas de crear (2:VLAN2)

UD04 Interconexión de equipos en redes locales (1) PRÁCTICAS



Paso 3.3: Configuración del switch1.

En este paso vamos a crear las VLAN2 y VLAN3 en el switch1 siguiendo los mismos pasos que hemos hecho antes. Vamos a configurarla para comunicarse con el switch0 por puerto TRUNK y con PC3, PC4 y PC5 por puerto ACCESS.

Paso 3.4: Comprobar el funcionamiento correcto de la red.



-Realiza la actividad Paso 3.4 del Cuaderno de Actividades

Cuaderno de PRÁCTICAS - UNIDAD 4 - Packet Tracer

Interconexión de equipos en redes locales (I)

Nombre y apellidos

Desarrollo

- ✓ 1ª PARTE: Configurar una red local básica con punto de acceso y hub.
- ✓ 2ª PARTE: Enlace de redes híbridas.
- ✓ 3ª PARTE: Configuración de VLAN's en Packet Tracer.

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

1ª PARTE:

CONFIGURAR UNA RED LOCAL BÁSICA CON PUNTO DE ACCESO Y HUB

Paso 1.3

- Busca información por Internet sobre qué es un *Hub o Concentrador* y para qué se utiliza. SÉ BREVE Y PON UNA EXPLICACIÓN QUE SEA COMPRESIBLE PARA TI

Indica el enlace del que has obtenido la información.

- Busca información por Internet sobre qué es un *Punto de Acceso o Access Point* y para qué se utiliza. SÉ BREVE Y PON UNA EXPLICACIÓN QUE SEA COMPRESIBLE PARA TI

Indica el enlace del que has obtenido la información.

- Resultado de ejecutar *IPCONFIG* para el ordenador PC0

- Inserta la captura de la pantalla

UD04 Interconexión de equipos en redes locales (I) PRÁCTICAS

- Indica en la tabla la información obtenida al ejecutar el comando

dirección IP	
máscara de Subred	
dirección de Gateway	

• Resultado de ejecutar PING desde PC0 a PC1

- Inserta la captura de la pantalla

- Indica en la tabla la información obtenida al ejecutar el comando

Nº de Bytes de datos	
Nº de intentos	
Tiempo de respuesta de cada uno de los intentos	
Nº de paquetes enviados	
Nº de paquetes recibidos	
Nº de paquetes perdidos	

Paso 1.4 - Enlace de redes mediante concentradores

En este ejercicio vas a comprobar el funcionamiento de un hub.

Primero has de borrar todas las pruebas previas que hayas hecho en la red (comando Eliminar de la barra inferior de pruebas).

Para ello vas a ir a la pestaña Simulación que está en la esquina inferior derecha de la pantalla (detrás de la pestaña Tiempo Real).

Una vez aquí, vas a enviar una PDU simple (por defecto ejecuta el comando PING) entre PC0 y PC1.

UD04 Interconexión de equipos en redes locales (I) PRÁCTICAS

Pulsa la opción "Auto Captura / Reproducir" del menú derecho.

Comprobarás que se muestra la comunicación que se establece entre los dispositivos.

Analiza qué sucede en la red y responde a las siguientes preguntas.

- Inserta una captura de pantalla de la red que has montado.

- El paquete que PC0 envía a PC1, ¿a qué ordenadores y dispositivos de la red llega también? Indica a continuación la lista de nodos de la red que reciben el paquete.

- En el panel de simulación se muestra la comunicación entre cada dispositivo de la red. Inserta una captura de pantalla con el resultado.

- Borra la información de la prueba que has hecho. Ahora envía una PDU Simple entre PC0 y PC4, ¿a qué ordenadores y dispositivos de la red llega también el paquete? Indica a continuación la lista de nodos de la red que reciben el paquete.

- En el panel de simulación se muestra la comunicación entre cada dispositivo de la red. Inserta una captura de pantalla con el resultado.

UD04 Interconexión de equipos en redes locales (I) PRÁCTICAS

- Viendo lo que sucede en la red, ¿cuál crees que es el principal inconveniente de utilizar *hubs* en una red?

- Inserta una captura de pantalla con la vista física (*Physical view*) del hub

- ¿Cuántos puertos como máximo podemos tener en el modelo de hub que has utilizado?

UD04 Interconexión de equipos en redes locales (I) PRÁCTICAS

2ª PARTE.

ENLACE DE REDES HÍBRIDAS

Paso 2.2 – Enlace de redes mediante repetidores

- Busca información por Internet sobre qué es un *Repetidor* y para qué se utiliza. SÉ BREVE Y PON UNA EXPLICACIÓN QUE SEA COMPRENSIBLE PARA TI

Indica el enlace del que has obtenido la información.

- Inserta una captura de pantalla de la red que has montado.

- El paquete que PC0 envía a PC1, ¿a qué ordenadores y dispositivos de la red llega también? Indica a continuación la lista de nodos de la red que reciben el paquete.

- En el panel de simulación se muestra la comunicación entre cada dispositivo de la red. Inserta una captura de pantalla con el resultado.

UD04 Interconexión de equipos en redes locales (I) PRÁCTICAS

- Borra la información de la prueba que has hecho. Ahora envía una PDU Simple entre PC0 y PC4, ¿a qué ordenadores y dispositivos de la red llega también el paquete? Indica a continuación la lista de nodos de la red que reciben el paquete.

- En el panel de simulación se muestra la comunicación entre cada dispositivo de la red. Inserta una captura de pantalla con el resultado.

- Viendo lo que sucede en la red, ¿cuál crees que es el principal inconveniente de utilizar *repetidores* en una red?

- Inserta una captura de pantalla con la vista física (Physical view) del repetidor

- ¿Cuántos puertos como máximo podemos tener habitualmente en un repetidor?

UD04 Interconexión de equipos en redes locales (I) PRÁCTICAS

Paso 2.3 – Enlace de redes mediante puentes

- Busca información por Internet sobre qué es un *Puente* y para qué se utiliza. SÉ BREVE Y PON UNA EXPLICACIÓN QUE SEA COMPRESIBLE PARA TI

Indica el enlace del que has obtenido la información.

- Inserta una captura de pantalla de la red que has montado.

- El paquete que PC0 envía a PC1, ¿a qué ordenadores y dispositivos de la red llega también? Indica a continuación la lista de nodos de la red que reciben el paquete.

- En el panel de simulación se muestra la comunicación entre cada dispositivo de la red. Inserta una captura de pantalla con el resultado.

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

- Borra la información de la prueba que has hecho. Ahora envía una PDU Simple entre PC0 y PC4, ¿a qué ordenadores y dispositivos de la red llega también el paquete? Indica a continuación la lista de nodos de la red que reciben el paquete.

- En el panel de simulación se muestra la comunicación entre cada dispositivo de la red. Inserta una captura de pantalla con el resultado.

- Viendo lo que sucede en la red, ¿cuál crees que es la principal diferencia entre la red anterior con un *repetidor* y la red que has montado ahora con un *puentes*?

- Inserta una captura de pantalla con la vista física (Physical view) del puente

- ¿Cuántos puertos como máximo podemos tener habitualmente en un puente?

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

Paso 2.4 – Enlace de redes mediante conmutadores

- Busca información por Internet sobre qué es un *Switch* o *conmutador* y para qué se utiliza. **SÉ BREVE Y PON UNA EXPLICACIÓN QUE SEA COMPENSIBLE PARA TI**

Indica el enlace del que has obtenido la información.

- Inserta una captura de pantalla de la red que has montado.

- El *switch* es un dispositivo de una cierta inteligencia. En el modelo que has elegido podemos entrar en modo terminal para ver/modificar su configuración. Entra en las propiedades del *switch* de la red, pestaña CLI y ejecuta *show* ? Verás que aparece la lista de opciones que tiene el comando que permite visualizar la configuración del *switch*.

Inserta una captura de pantalla con el resultado mostrado por el router.

- Ejecuta *show mac-address-table* para visualizar el contenido de la tabla de macs del router. ¿Aparece algún contenido? ¿Por qué crees que para esto?

UD04 Interconexión de equipos en redes locales (I) PRÁCTICAS

- Inserta una captura de pantalla con el resultado mostrado por el comando.

- Envía ahora una PDU Simple entre PC0 y PC4, de forma que el paquete pase por el *Switch*. Ejecuta *show mac-address-table* de nuevo ¿Qué información aparece ahora?

- ¿Por qué crees que ahora aparece información nueva que antes no aparecía?

- Inserta una captura de pantalla con el resultado mostrado por el comando.

- Envía ahora varias PDU Simple entre diferentes PCs de la red. Ejecuta *show mac-address-table* de nuevo. Inserta una captura de pantalla con el resultado mostrado por el comando.

- En el contenido de la tabla de direcciones del *switch* aparece type DYNAMIC ¿Qué significa esta información? Búscalo en los apuntes de la unidad.

UD04 Interconexión de equipos en redes locales (I) PRÁCTICAS

- Borra las pruebas anteriores. Entra en la pestaña Simulación y envía un paquete entre PC0 y PC5. El *switch* “aprende” las macs de los nodos. Vuelve a enviar otra vez una PDU Simple entre los mismos ordenadores. Pulsa “Auto Captura / Reproducir”, ¿a qué ordenadores y dispositivos de la red llega el paquete? Indica a continuación la lista de nodos de la red que reciben el paquete.

- Viendo lo que sucede en la red, ¿cuál crees que es la principal ventaja que aporta el uso de un *switch* en una red?

- Inserta una captura de pantalla con la vista física (Physical view) del *Switch*

- ¿Cuántos puertos como máximo podemos tener en el modelo de *Switch* elegido?

3ª PARTE.

CONFIGURACIÓN DE VLAN'S EN PACKET TRACER

Paso 3.4

- Inserta una captura de la red final que has montado con las dos VLANs
- Inserta una captura de la pestaña Config > Base de datos de la VLAN del Switch0
- Inserta una captura de la pestaña Config > Base de datos de la VLAN del Switch1
- La comunicación entre los switches se ha configurado usando los puertos TRUNK. Indica para qué se utiliza este puerto. Busca la información en los apuntes de clase.
- Inserta una captura de la pestaña Config > Interfaz del Switch0 al que has asociado el puerto TRUNK

- La comunicación entre cada switch y los ordenadores se ha configurado usando los puertos ACCESS. Indica para qué se utiliza este puerto. Busca la información en los apuntes de clase.

- Inserta una captura de la pestaña Config > Interfaz del Switch0 al que has asociado el PC0

- Inserta una captura de la pestaña Config > Interfaz del Switch0 al que has asociado el PC2

Vamos a probar que la red funciona correctamente. Para ello vas a ir a la pestaña "Simulación".

- Crea una PDU Simple entre PC0 y PC1 y pulsa "Auto Captura / Reproducir". ¿Hay comunicación entre los ordenadores? ¿Por qué?

- Inserta una captura con el resultado del panel de simulación

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

- Borra la prueba anterior. Crea una PDU Simple entre PC0 y PC2 y pulsa "Auto Captura / Reproducir". ¿Hay comunicación entre los ordenadores? ¿Por qué?

- Inserta una captura con el resultado del panel de simulación

- Borra la prueba anterior. Crea una PDU Simple entre PC0 y PC3 y pulsa "Auto Captura / Reproducir". ¿Hay comunicación entre los ordenadores? ¿Por qué?

- Inserta una captura con el resultado del panel de simulación

- Borra la prueba anterior. Crea una PDU Simple entre PC0 y PC5 y pulsa "Auto Captura / Reproducir". ¿Hay comunicación entre los ordenadores? ¿Por qué?

- Inserta una captura con el resultado del panel de simulación

UD04 Interconexión de equipos en redes locales (I)

PRÁCTICAS

UD04 Interconexión de equipos en redes locales

PRÁCTICAS

Cuaderno de PRÁCTICAS 2: -TALLER-

Nombre y apellidos	
Breve descripción	Aprender a realizar las configuraciones básicas del switch, implementando después conectividad básica mediante la configuración de direcciones IP en switches y PC's. Utilizaremos comandos básicos de Administración de Sistemas, como show y ping , para verificar las configuraciones y la conectividad.
Material necesario	<ul style="list-style-type: none"> • Cuaderno de trabajo • Bolígrafo y/o lápiz • 1 PC con Packet Tracer
Fuentes de información	<ul style="list-style-type: none"> • Diapositivas de la Unidad 4 • Explicaciones de clase

Desarrollo	
✓ PARTE 1: Verificar la configuración predeterminada del switch	
✓ PARTE 2: Establecer una configuración básica del switch	
✓ PARTE 3: Configurar un aviso de MOTD	
✓ PARTE 4: Guardar los archivos de configuración en la NVRAM	
✓ PARTE 5: Configurar el S2	
✓ PARTE 6: Configurar las PC's	
✓ PARTE 7: Configurar la interfaz de administración de switches.	

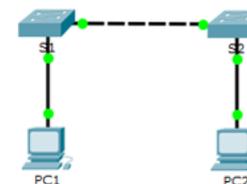
Página 1 de 8

UD04 Interconexión de equipos en redes locales

PRÁCTICAS

PRÁCTICA DE TALLER

Topología



Parte 1: Verificar la configuración predeterminada del switch

Paso 1: Ingrese al modo EXEC privilegiado.

Puede acceder a todos los comandos del switch en el modo EXEC privilegiado. Sin embargo, debido a que muchos de los comandos privilegiados configuran parámetros operativos, el acceso privilegiado se debe proteger con una contraseña para evitar el uso no autorizado.

El conjunto de comandos EXEC privilegiados incluye aquellos comandos del modo EXEC del usuario, así como también el comando **configure** a través del cual se obtiene acceso a los modos de comando restantes.

- Haga clic en S1 y luego en la ficha CLI. Pulse Intro.
- Ingrese al modo EXEC privilegiado introduciendo el comando **enable**:

```
Switch> enable
Switch#
```

Observe que el indicador cambia en la configuración para reflejar el modo EXEC privilegiado.

Paso 2: Examine la configuración actual del switch.

- Ingrese el comando **show running-config**.

```
Switch# show running-config
```
- Responda las siguientes preguntas:
 - ¿Cuántas interfaces FastEthernet tiene el switch? _____
 - ¿Cuántas interfaces Gigabit Ethernet tiene el switch? _____
 - ¿Cuál es el rango de valores que se muestra para las líneas vty? _____
 - ¿Qué comando muestra el contenido actual de la memoria de acceso aleatorio no volátil (NVRAM)?

Página 2 de 8

UD04 Interconexión de equipos en redes locales PRÁCTICAS

5) ¿Por qué el switch responde con `startup-config is not present`?

Parte 2: Crear una configuración básica del switch

Paso 1: Asigne un nombre a un switch.

Para configurar los parámetros de un switch, quizá deba pasar por diversos modos de configuración. Observe cómo cambia la petición de entrada mientras navega por el switch.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#
```

Paso 2: Proporcione acceso seguro a la línea de consola.

Para proporcionar un acceso seguro a la línea de la consola, acceda al modo config-line y establezca la contraseña de consola en `letmein`.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

¿Por qué se requiere el comando `login`?

Paso 3: Verifique que el acceso a la consola sea seguro.

Salga del modo privilegiado para verificar que la contraseña del puerto de consola esté vigente.

```
S1# exit
Switch con0 is now available
Press RETURN to get started.
```

```
User Access Verification
Password:
S1>
```

Nota: Si el switch no le pidió una contraseña, entonces no se configuró el parámetro `login` en el paso 2.

Paso 4: Proporcione un acceso seguro al modo privilegiado.

Establezca la contraseña de `enable` en `c1$c0`. Esta contraseña protege el acceso al modo privilegiado.

UD04 Interconexión de equipos en redes locales PRÁCTICAS

Nota: El 0 en `c1$c0` es el número 0, no la letra O en mayúscula. Esta contraseña no se calificará como correcta hasta después de haberla cifrado en el paso 8.

```
S1> enable
S1# configure terminal
S1(config)# enable password c1$c0
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Paso 5: Verifique que el acceso al modo privilegiado sea seguro.

- Introduzca el comando `exit` nuevamente para cerrar la sesión del switch.
- Presione <Intro>; a continuación, se le pedirá que introduzca una contraseña:
User Access Verification
Password:
- La primera contraseña es la contraseña de consola que configuró para line con 0. Introduzca esta contraseña para volver al modo EXEC del usuario.
- Introduzca el comando para acceder al modo privilegiado.
- Introduzca la segunda contraseña que configuró para proteger el modo EXEC privilegiado.
- Para verificar la configuración, examine el contenido del archivo de configuración en ejecución:
S1# show running-config
Observe que las contraseñas de consola y de enable son de texto no cifrado. Esto podría presentar un riesgo para la seguridad si alguien está viendo lo que hace.

Paso 6: Configure una contraseña encriptada para proporcionar un acceso seguro al modo privilegiado.

La contraseña de `enable` se debe reemplazar por una nueva contraseña secreta encriptada mediante el comando `enable secret`. Configure la contraseña de `enable secret` como `itsasecret`.

```
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#
```

Nota: La contraseña de `enable secret` sobrescribe la contraseña de `enable`. Si ambas están configuradas en el switch, debe introducir la contraseña de `enable secret` para ingresar al modo EXEC privilegiado.

Paso 7: Verifique si la contraseña de `enable secret` se agregó al archivo de configuración.

- Introduzca el comando `show running-config` nuevamente para verificar si la nueva contraseña de `enable secret` está configurada.
Nota: Puede abreviar el comando `show running-config` como
S1# show run
- ¿Qué se muestra como contraseña de `enable secret`?
- ¿Por qué la contraseña de `enable secret` se ve diferente de lo que se configuró?

UD04 Interconexión de equipos en redes locales

PRÁCTICAS

Paso 8: Encripte las contraseñas de consola y de enable.

Como pudo observar en el paso 7, la contraseña de `enable secret` estaba cifrada, pero las contraseñas de `enable` y de consola aún estaban en texto no cifrado. Ahora encriptaremos estas contraseñas de texto no cifrado con el comando `service password-encryption`.

```
S1# config t
S1(config)# service password-encryption
S1(config)# exit
```

Si configura más contraseñas en el switch, ¿se mostrarán como texto no cifrado o en forma cifrada en el archivo de configuración? Explique.

Parte 3: Configurar un aviso de MOTD

Paso 1: Configure un aviso de mensaje del día (MOTD).

El conjunto de comandos de Cisco IOS incluye una característica que permite configurar los mensajes que cualquier persona puede ver cuando inicia sesión en el switch. Estos mensajes se denominan "mensajes del día" o "avisos de MOTD". Coloque el texto del mensaje en citas o utilizando un delimitador diferente a cualquier carácter que aparece en la cadena de MOTD.

```
S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only!"
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

- 1) ¿Cuándo se muestra este aviso? _____
- 2) ¿Por qué todos los switches deben tener un aviso de MOTD? _____

Parte 4: Guardar los archivos de configuración en la NVRAM

Paso 1: Verifique que la configuración sea precisa mediante el comando show run.

Paso 2: Guarde el archivo de configuración.

Usted ha completado la configuración básica del switch. Ahora haga una copia de seguridad del archivo de configuración en ejecución a NVRAM para garantizar que los cambios que se han realizado no se pierdan si el sistema se reinicia o se apaga.

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
```

¿Cuál es la versión abreviada más corta del comando `copy running-config startup-config`?

UD04 Interconexión de equipos en redes locales

PRÁCTICAS

Paso 3: Examine el archivo de configuración de inicio.

- ¿Qué comando muestra el contenido de la NVRAM? _____
- ¿Todos los cambios realizados están grabados en el archivo? _____

Parte 5: Configurar S2

Completó la configuración del S1. Ahora configurará el S2. Si no recuerda los comandos, consulte las partes 1 a 4 para obtener ayuda.

Configure el S2 con los siguientes parámetros:

- a. Nombre del dispositivo: S2
- b. Proteja el acceso a la consola con la contraseña `letmein`.
- c. Configure `ct5c0` como la contraseña de `enable` y `itsasecret` como la contraseña de `enable secret`.
- d. Configure el siguiente mensaje para aquellas personas que inician sesión en el switch:
`Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.`
- e. Cifre todas las contraseñas de texto no cifrado.
- f. Asegúrese de que la configuración sea correcta.
- g. Guarde el archivo de configuración para evitar perderlo si el switch se apaga.

```
Switch> enable
Switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname S2
S2(config)# line console 0
S2(config-line)# password letmein
S2(config-line)# login
S2(config-line)# enable password ct5c0
S2(config)# enable secret itsasecret
S2(config)# banner motd $any text here$
S2(config)# service password-encryption
S2(config)# copy running-config startup-config
```

Parte 6: Configurar las PC

Configure la PC1 y la PC2 con direcciones IP.

Step 1: Configure ambas PC con direcciones IP.

- a. Haga clic en PC1 y luego en la ficha Escritorio.
- b. Haga clic en Configuración de IP. En la tabla de direccionamiento anterior, puede ver que la dirección IP para la PC1 es 192.168.1.1 y la máscara de subred es 255.255.255.0. Introduzca esta información para la PC1 en la ventana Configuración de IP.

UD04 Interconexión de equipos en redes locales

PRÁCTICAS

- c. Repita los pasos 1a y 1b para la PC2.

Paso 2: Pruebe la conectividad a los switches.

- a. Haga clic en PC1. Cierre la ventana Configuración de IP si todavía está abierta. En la ficha Escritorio, haga clic en Símbolo del sistema.

- b. Escriba el comando ping y la dirección IP para el S1 y presione Intro.

Packet Tracer PC Command Line 1.0

```
PC> ping 192.168.1.253
```

¿Tuvo éxito? Explique.

Parte 7: Configurar la interfaz de administración de switches

Configure el S1 y el S2 con una dirección IP.

Step 1: Configure el S1 con una dirección IP.

Los switches pueden usarse como dispositivos plug-and-play. Esto significa que no necesitan configurarse para que funcionen. Los switches reenvían información desde un puerto hacia otro sobre la base de direcciones de control de acceso al medio (MAC). Si este es el caso, ¿por qué lo configuraríamos con una dirección IP?

Use los siguientes comandos para configurar el S1 con una dirección IP.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.253 255.255.255.0
S1(config-if)# no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# exit
S1#
```

¿Por qué debe introducir el comando no shutdown?

Paso 1: Configure el S2 con una dirección IP.

Use la información de la tabla de direccionamiento para configurar el S2 con una dirección IP.

Paso 2: Verifique la configuración de direcciones IP en el S1 y el S2.

Use el comando show ip interface brief para ver la dirección IP y el estado de todos los puertos y las interfaces del switch. También puede utilizar el comando show running-config.

UD04 Interconexión de equipos en redes locales

PRÁCTICAS

Paso 3: Guarde la configuración para el S1 y el S2 en la NVRAM.

¿Qué comando se utiliza para guardar en la NVRAM el archivo de configuración que se encuentra en la RAM?

Paso 4: Verifique la conectividad de la red.

Puede verificarse la conectividad de la red mediante el comando ping. Es muy importante que haya conectividad en toda la red. Se deben tomar medidas correctivas si se produce una falla. Desde la PC1 y la PC2, haga ping al S1 y S2.

- a. Haga clic en PC1 y luego en la ficha Escritorio.

- b. Haga clic en Símbolo del sistema.

- c. Haga ping a la dirección IP de la PC2.

- d. Haga ping a la dirección IP del S1.

- e. Haga ping a la dirección IP del S2.

Nota: También puede usar el comando ping en la CLI del switch y en la PC2.

Todos los pings deben tener éxito. Si el resultado del primer ping es 80 %, inténtelo otra vez. Ahora debería ser 100 %. Más adelante, aprenderá por qué es posible que un ping falle la primera vez. Si no puede hacer ping a ninguno de los dispositivos, vuelva a revisar la configuración para detectar errores.

8.5 Unidad didáctica 5

Las aplicaciones y servicios de red de un terminal se pueden comunicar con las aplicaciones y servicios que se ejecutan en otro terminal gracias a los protocolos de la capa de red o nivel 3 del modelo OSI. Los protocolos de éste nivel especifican el direccionamiento y los procesos que permiten que se transfieran los paquetes de datos de un origen a un destino dentro de una red, o a otra red.

Los protocolos de la capa de red especifican la estructura de paquete y los procesos que se utilizan para transportar la información de un dispositivo a otro, sin tener en cuenta los datos que contiene cada paquete.

Existen varios protocolos de capa de red, sin embargo, en ésta unidad didáctica se analiza el Protocolo de Internet versión 4 (IPv4). Más adelante, en la Unidad Didáctica 7 se caracteriza el Protocolo de Internet versión 6 (IPv6), que ofrece mayor espacio de direcciones y mejor manejo de paquetes de datos. Siendo los dos protocolos de capa de red que suelen implementarse.

En la mayoría de las situaciones se pretende que nuestros dispositivos se conecten más allá del segmento de red local, esto es, que se envíe un paquete a un dispositivo de destino remoto. Para ello se necesita la ayuda de los routers. Con esta unidad didáctica se pretende completar el estudio de los dispositivos de interconexión en redes con el estudio del router, dispositivo que trabaja en el nivel 3 del modelo OSI. Se presenta la caracterización del router y se plantean actividades prácticas de configuración básica del mismo, y de resolución de incidencias en la comunicación.

8.5.1 Presentación teórica

CURSO
Redes de Área Local

UNIDAD 5
Interconexión de equipos en redes locales (II)
-Interconexión de redes-

Redes de Área Local Olga Minguet 1

UD5. Interconexión de equipos en redes locales (II) 

ÍNDICE

- 1. El encaminador o Router
- 2. El acceso a las redes WAN

Redes de Área Local Olga Minguet 2

UD5. Interconexión de equipos en redes locales (II) 

ÍNDICE

- 1. **EL ENCAMINADOR O ROUTER**
 - 1.1. Características generales de los routers
 - 1.2. Tipos de encaminadores
 - Según su ubicación en la red
 - Según el tipo de algoritmo de encaminamiento
 - 1.3. Protocolos de encaminamiento
 - 1.4. Configuración del enrutamiento
 - 1.5. Rutas de protocolo IP
 - 1.6. Configuración de la tabla de rutas
- 2. **EL ACCESO A LAS REDES WAN**

Redes de Área Local Olga Minguet 3

UD5. Interconexión de equipos en redes locales (II) 

1. EL ENCAMINADOR O ROUTER



Redes de Área Local Olga Minguet 4

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

- Los encaminadores, **enrutadores** o **routers** son dispositivos **software** o **hardware** que se pueden configurar para **encaminar paquetes** entre sus distintos puertos de red utilizando la dirección lógica (**dirección IP**).
- El encaminamiento se realiza de acuerdo con reglas del **nivel 3 de OSI**.
- Solo serán enrutables aquellos protocolos que utilicen este nivel.

Redes de Área Local Olga Minguet 5

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

Router de banda ancha inalámbrica Cisco WRP500

Redes de Área Local Olga Minguet 6

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.1. Características generales de los routers

- El encaminador interconecta redes de área local operando en el nivel 3 de OSI.
- El **rendimiento** de los **enrutadores** es **menor** que el de los **conmutadores (switches)** ya que deben gastar tiempo del proceso en analizar los paquetes del nivel de red que le llegan.
- Permiten una organización muy flexible de la interconexión de las redes.
- **Interpretan** las **direcciones lógicas** de capa 3, en vez de las direcciones MAC de capa de enlace.
- Son capaces de **cambiar el formato de la trama** (lo adaptan al medio de transmisión).

Redes de Área Local Olga Minguet 7

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.1. Características generales de los routers

- Poseen un **elevado nivel de inteligencia** y pueden manejar distintos protocolos previamente establecidos.
- Cada enrutador encamina **uno o más protocolos**. La condición que debe imponerse al protocolo es que sea enrutable (nivel 3 de OSI), porque no todo protocolo se puede encaminar.
- Los routers comerciales suelen tener capacidad para encaminar los protocolos de red más utilizados, todos ellos de nivel 3: **IP, IPX, AppleTalk, DECnet, XNS**, etc.
- **Proporcionan seguridad** a la red puesto que se pueden configurar para restringir los accesos a esta mediante filtrado.

Redes de Área Local Olga Minguet 8

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.1. Características generales de los routers

- **Reducen la congestión** de la red aislando el tráfico y los dominios de colisión en las distintas subredes que interconectan.

Redes de Área Local Olga Minguet 9

UD5. Interconexión de equipos en redes locales (II)

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- **Actividad 3**
- **Actividad 4**

Redes de Área Local Olga Minguet 10

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.2. Tipos de encaminadores

- Según su ubicación en la red

Es frecuente que los routers se clasifiquen de acuerdo con el **ámbito de la red** a la que proporcionan servicio.

- Según el tipo de algoritmo de encaminamiento

Los routers confeccionan una **tabla de encaminamiento** en donde registran qué **nodos y redes son alcanzables** por cada uno de sus puertos. De aquí nace una segunda clasificación de los algoritmos utilizados por los encaminadores para realizar su función.

Redes de Área Local Olga Minguet 11

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.2. Tipos de encaminadores

- Tipos de routers según su ubicación en la red

Router de interior (Interior router)	Encaminador para ser instalado en una LAN para dar servicio de encaminamiento dentro de la propia red de área local proporcionando a los paquetes de red la posibilidad de saltar de unos segmentos de la red a otros.
Router de exterior (Exterior router)	El encaminador comunica nodos y redes en el exterior de la LAN. Estos routers operan típicamente en el núcleo de Internet y son utilizados por los operadores de Internet para comunicarse entre ellos.
Router de borde, frontera o perímetro (Gateway)	Es un encaminador que se encarga de conectar routers interiores con routers exteriores.

Redes de Área Local Olga Minguet 12

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.2. Tipos de encaminadores



Puerta de Enlace predeterminada

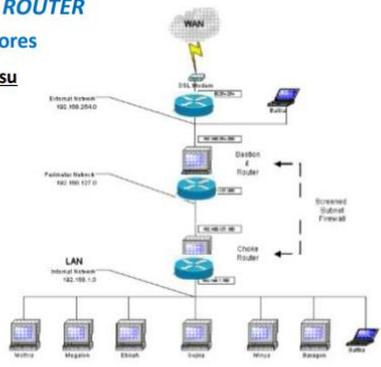
Redes de Área Local Olga Minguet 13

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.2. Tipos de encaminadores

- Tipos de routers según su ubicación en la red



Redes de Área Local Olga Minguet 14

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.2. Tipos de encaminadores

- Tipos de routers según el tipo de algoritmo de encaminamiento

Algoritmo de encaminamiento estático (static routing)	La tabla de encaminamiento es programada por el administrados de red. Carecen de capacidad para aprender la topología de la red por sí mismos, cualquier adaptación a cambios topológicos de la red requiere una intervención manual del administrador del router.
Algoritmos de encaminamiento adaptativo o dinámico (Dynamic routing)	Son capaces de aprender por sí mismos la topología de la red. Su rendimiento es menor ya que tienen que consumir recursos en el intercambio de información con otros enrutadores para, dinámicamente, confeccionar las tablas de encaminamiento que contienen la información con la que tomará las decisiones de enrutamiento de paquetes.

Redes de Área Local Olga Minguet 15

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.2. Tipos de encaminadores



El router Enrutamiento estático

Redes de Área Local Olga Minguet 16

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.3. Protocolos de encaminamiento

- Un protocolo de encaminamiento es aquel que utiliza un router para calcular el **mejor camino** (best path, en la terminología profesional) que le separa de un destino determinado.
- El mejor camino calculado representa la **ruta más eficiente** que debe seguir un paquete desde que sale de un nodo origen hasta que llega a su destino pasando por el router.
- El **coste de una ruta** (route cost) es un valor numérico que representa cuán bueno es el camino que la representa: a menor coste, mejor camino.

Redes de Área Local Olga Minguet 17

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.3. Protocolos de encaminamiento

- El mejor camino dependerá de muchos factores:
 - ✓ la actividad de la red,
 - ✓ de si hay enlaces fuera de servicio,
 - ✓ de la velocidad de transmisión de los enlaces,
 - ✓ de la topología de la red,
- **Tiempo de convergencia** es el tiempo que tarda un router en encontrar el **mejor camino** cuando se produce una alteración topológica en la red que exige que se recalculen las rutas para adaptarse a la nueva situación.
- Hay que diseñar los protocolos de enrutamiento para que tengan el **menor tiempo de convergencia posible**.

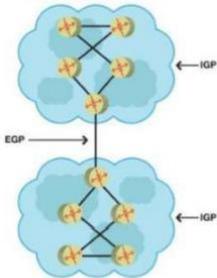
Redes de Área Local Olga Minguet 18

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.3. Protocolos de encaminamiento

- Protocolos **IGP** (Interior Gateway Protocol) son los utilizados con routers de **Interior**.
- Protocolos **EGP** (Exterior Gateway Protocol) son los utilizados con routers de **Exterior**.



Redes de Área Local Olga Minguet 19

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.3. Protocolos de encaminamiento (basados en el vector-distancia)

- Un protocolo de encaminamiento basado en un vector-distancia es aquel que determina cuál es el mejor camino calculando la **distancia al destino**.
- El router debe **intercambiar** periódicamente su **información** de enrutamiento **con otros routers vecinos** para recalcular las nuevas distancias entre ellos.
- Los protocolos de enrutamiento basados en vector-distancia más utilizados son **RIP, RIPv2 y BGP**.

Redes de Área Local Olga Minguet 20

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.3. Protocolos de encaminamiento (basados en el vector-distancia)

- La distancia es un número calculado que puede contemplar otros parámetros como:
 - » la longitud
 - » el número de saltos que dará para llegar al destino,
 - » la latencia (tiempo de espera)

Redes de Área Local Olga Minguet 21

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.3. Protocolos de encaminamiento (basados en el vector-distancia)

RIP o RIPv1 (Routing Information Protocol)	-Sólo se utiliza en routers interiores y de borde . -Si la red es grande, RIP genera excesivo tráfico de red. -Es poco escalable . No excede de 15 saltos. -Es un protocolo muy estable.
RIPv2	-Se utiliza en routers interiores y de borde . -Genera menos tráfico de broadcast , admite subnetting. -Mejora la seguridad pues en el intercambio de información de enrutamiento se emplean contraseñas . -Es poco escalable . No excede de 15 saltos.
BGP (Border Gateway Protocol)	-Protocolo de frontera exterior . -Típicamente propiedad de los proveedores de Internet .

Redes de Área Local Olga Minguet 22

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.3. Protocolos de encaminamiento (basados en el estado del enlace)

- Un protocolo de encaminamiento basado en el estado del enlace (link-state) es aquel que le permite a un router **crearse un mapa de la red** para que él mismo pueda determinar el mejor camino a un destino por sí mismo examinando el mapa que se ha construido.
- En función de la información de los enlaces que mantiene **con sus routers vecino** y la información que estos le proporcionen sobre los segmentos de la red que ellos ven, construirán **árboles de caminos** que representen el mapa de la red.

Los protocolos de enrutamiento basados en el estado del enlace más utilizados actualmente son **OSPF** e **IS-IS**.

Redes de Área Local Olga Minguet 23

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.3. Protocolos de encaminamiento (basados en el estado del enlace)

EIGRP Communications

OSPF Communications

Redes de Área Local Olga Minguet 24

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER
1.3. Protocolos de encaminamiento (basados en el estado del enlace)

OSPF (Open Shortest Path First)	-El envío del paquete siempre se realiza por la ruta más corta de todas las disponibles, que siempre es la que requiere un número menor de saltos . -Alta escalabilidad. -Es muy común en las LAN y se utiliza en routers interiores y de borde .
IS-IS (Intermediate System to Intermediate System)	-Soporta encaminamiento en grandes dominios y en combinaciones de muchos tipos de subredes. -Solo se utiliza en routers interiores .

Redes de Área Local Olga Minguet 25

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER
1.3. Protocolos de enrutamiento

Redes de Área Local Olga Minguet 26

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER
1.3. Protocolos de enrutamiento

Parámetro	RIPv1	RIPv2	IGRP	OSPF	EIGRP
Tipo	Vector-distancia	Vector-distancia	Vector-distancia	Estado enlace	Híbrido
Coste	120	120	100	110	90 (ruta interna) o 170 (ruta externa)
Tipo de red enrutada	De clase	Subnetting	De clase	Subnetting	Subnetting
Métrica	Número de saltos	Número de saltos	Ancho de banda y latencia	Coste y ancho de banda	Ancho de banda y latencia
Mensajes a otros enrutadores	Broadcast (255.255.255.255)	Multicast (224.0.0.0)	Broadcast (255.255.255.255)	Multicast (224.0.0.5 y 224.0.0.6)	Multicast (224.0.0.10)
Tiempo convergencia	Lento	Lento	Lento	Rápido	Rápido
Escalabilidad	Pobre	Baja	Alta	Alta	Alta

Redes de Área Local Olga Minguet 27

UD5. Interconexión de equipos en redes locales (II)

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

➤ **Actividad 5**

Redes de Área Local Olga Minguet 28

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.4. Configuración del enrutamiento

- Cada nodo de una red IP debe tener configurados sus parámetros de red.
- Desde el punto de vista del enrutamiento, el parámetro más significativo es la **puerta por defecto**.
- Cuando el emisor y el receptor de un paquete IP están en la **misma red lógica** no hay problemas de comunicación porque el emisor sabe que el receptor está en su misma red mediante ARP y, por tanto, todo lo que él escriba en la red será leído por el receptor.

Redes de Área Local Olga Minguet 29

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.5. Rutas de protocolo IP

- Cuando emisor y receptor están en **distintas redes**, es muy posible que el emisor no sepa qué tiene que hacer para que el paquete llegue a su destino.
- Una **ruta** es la **dirección IP de un nodo (router)** que tiene suficiente inteligencia para saber qué hacer con un paquete IP que ha recibido de un nodo de la red con objeto de que llegue a su destino, o al menos saber a quién puede enviárselo para que lo resuelva en su nombre.
- **Ruta por defecto o default Gateway** es la ruta a la que se envía un paquete cuando ninguna otra ruta es apropiada, con la confianza de que dicho router sepa cómo distribuir el paquete.

Redes de Área Local Olga Minguet 30

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.6. Configuración de la tabla de rutas

No todas las tablas de rutas son iguales, dependen del sistema operativo; sin embargo, la mayoría de las tablas de rutas tienen los siguientes atributos:

- Destino de red.** Es el nombre de la red que se pretende alcanzar.
- Máscara de red.** Define la máscara de red de destino. La máscara de red junto con el destino de red definen el conjunto de nodos de red a los que se dirige la ruta.
- Puerta de acceso o puerta de enlace.** Dirección IP del router (Gateway o puerta de acceso), que debe ser capaz de resolver los paquetes que se dirijan a ese destino de red.
- Interfaz.** Es la dirección IP o, en ciertos casos, el nombre de la interfaz de red que la posee por el que se deben enviar los paquetes de datos para alcanzar la puerta de enlace.
- Métrica.** Es un parámetro que define una medida del coste telemático que supone enviar el paquete a la red destinataria a través de la puerta de acceso.

Redes de Área Local Olga Minguet 31

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.6. Configuración de la tabla de rutas

The diagram shows a network topology with three routing tables:

Destino	Gateway	Metrica	Face
172.16.0.0	0.0.0.0	255,255,255.0	eth0
0.0.0.0	172.16.0.1	0.0.0.0	eth0

Destino	Gateway	Metrica	Face
192.168.0.0	0.0.0.0	255,255,255.0	eth0
172.16.0.0	0.0.0.0	255,255,255.0	eth1
0.0.0.0	192.168.0.20	0.0.0.0	eth0

Destino	Gateway	Metrica	Face
192.168.0.0	0.0.0.0	255,255,255.0	eth1
172.16.0.0	192.168.0.1	255,255,255.0	eth1
0.0.0.0	10.0.2.2	0.0.0.0	eth0

Redes de Área Local Olga Minguet 32

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.6. Configuración de la tabla de rutas

```

C
L
192.168.10.0/24 is directly connected, GigabitEthernet0/0
192.168.11.0/24 is directly connected, GigabitEthernet0/0
  
```

Redes de Área Local Olga Minguet 33

UD5. Interconexión de equipos en redes locales (II)

1. EL ENCAMINADOR O ROUTER

1.6. Configuración de la tabla de rutas

En Windows:

- ROUTE ADD: orden para añadir rutas a la tabla de rutas. Se puede acompañar de un calificador (-P) que hace que la ruta añadida sea permanente.
- ROUTE DELETE orden para borrarlas.
- ROUTE CHANGE para cambiar una ruta existente.

Además habrá que especificar la dirección de la red de destino junto con su **máscara y la puerta de enlace**

Ejemplo:
route -p add 192.168.100.0 mask 255.255.255.0 192.168.1.254

En Linux:

- Se utiliza la orden **iptables** o **ip route**, que también admite muchos calificadores (**show** para ver el contenido, **add** para añadir,...).

Redes de Área Local Olga Minguet 34

UD5. Interconexión de equipos en redes locales (II)

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 6
- Actividad 7

Redes de Área Local Olga Minguet 35

UD5. Interconexión de equipos en redes locales (II)

ÍNDICE

1. EL ENCAMINADOR O ROUTER
2. EL ACCESO A LAS REDES WAN
 - 2.1. Protocolos de acceso remoto
 - A. Protocolo PPP
 - B. El protocolo de tunelización PPTP
 - 2.2. Servicios de acceso remoto
 - Escenario de conexión RAS

Redes de Área Local Olga Minguet 36

UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

- Los ordenadores no son entidades aisladas, y las redes tampoco. De igual modo que los ordenadores se relacionan entre sí utilizando redes de área local, estas pueden interconectarse mediante otras redes de ámbito mayor: las **redes de área extensa (WAN)**.
- Las redes **WAN** no suelen conectar directamente nodos, sino que **interconectan redes**.
- Lo específico de las redes WAN es que las líneas que suelen utilizar son **públicas** y los protocolos de comunicación que requieren deben tener en cuenta la **seguridad** de un modo especial.

Redes de Área Local Olga Minguet 37

UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

2.1. Protocolos de acceso remoto

- La importancia que tenía el adaptador de red y los protocolos de nivel uno y dos para las redes de área local la tienen ahora los **protocolos de acceso remoto** para las redes **WAN**.

A. Protocolo PPP
B. El protocolo de tunelización PPTP

Redes de Área Local Olga Minguet 38

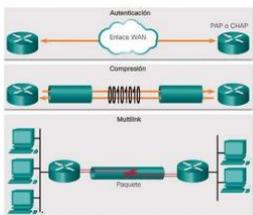
UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

2.1. Protocolos de acceso remoto

A. Protocolo PPP

- Bajo la denominación PPP (Point to Point Protocol) se designa a un conjunto de protocolos que permiten el acceso remoto para el **intercambio de tramas y autenticaciones** en un entorno de red de **múltiples fabricantes**.
- Un **cliente PPP** puede efectuar llamadas y, por tanto, establecer conexiones a **cualquier servidor** que cumpla las especificaciones PPP.



Redes de Área Local Olga Minguet 39

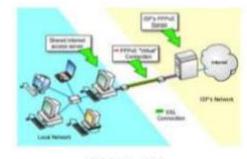
UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

2.1. Protocolos de acceso remoto

A. Protocolo PPP

- La arquitectura PPP permite que los clientes puedan ejecutar cualquier combinación de los protocolos **NetBeui, IPX y TCP/IP**.
- Existe una versión en la que se encapsula PPP sobre una capa **Ethernet** denominada **PPPoE** (PPP over Ethernet).
- Es muy utilizada para proveer conexiones de **banda ancha** añadiendo a Ethernet las ventajas que PPP ofrece como **autenticación, cifrado y compresión de datos**.



Redes de Área Local Olga Minguet 40

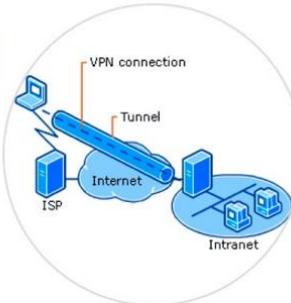
UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

2.1. Protocolos de acceso remoto

B. Protocolo de tunelización PPTP

- **PPTP** (Point to Point Tunneling Protocol, protocolo de tunelización punto a punto) es un protocolo de comunicaciones desarrollado por **Microsoft**.
- Sus comunicaciones son **cifradas** y es bastante popular en **redes privadas virtuales**, ya que Microsoft incorporó un servidor y un cliente PPTP a partir de Windows NT.



Redes de Área Local Olga Minguet 41

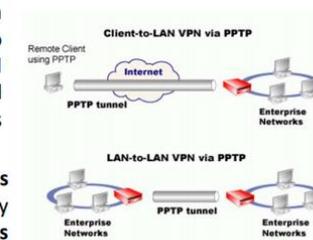
UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

2.1. Protocolos de acceso remoto

B. Protocolo de tunelización PPTP

- **PPTP** permite la transferencia **segura** de datos desde un **equipo remoto a un servidor privado** al crear una conexión de red **privada virtual** a través de redes de datos basadas en IP.
- PPTP acepta **redes privadas virtuales** bajo demanda y multiprotocolo a través de **redes públicas, como Internet**.



Redes de Área Local Olga Minguet 42

UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

2.1. Protocolos de acceso remoto

B. Protocolo de tunelización PPTP

- El servicio de acceso remoto (**RAS, Remote Access Service**) **conecta equipos remotos**, posiblemente móviles, con redes corporativas habilitando **los mismos servicios** para estos usuarios remotos que los que poseen los usuarios presentados localmente.
- Por tanto, **RAS** es un encaminador software:
 - › **multiprotocolo**
 - › con capacidad de **autenticación**
 - › **encriptación** de los datos transmitidos



Redes de Área Local Olga Minguet 43

UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

2.2. Servicios de acceso remoto

Escenario de conexión RAS

- El servicio de acceso remoto tiene **una parte de cliente y otra parte de servidor**.
- RAS es capaz de encaminar tres protocolos de LAN: **IPX, TCP/IP y NetBeui**, ya que frecuentemente utiliza PPP como transporte y este puede encapsular los tres protocolos de LAN.
- Es posible configurar el servicio RAS para que el cliente tenga acceso a toda la red o exclusivamente al servidor RAS.
- Si un cliente RAS se conecta vía **TCP/IP**, necesitará una **dirección IP compatible con la red** a la que intenta conectarse. Lo normal es que el servidor RAS le asigne **dinámicamente** una dirección IP mediante **DHCP**.
- Para el cliente RAS todo el procedimiento de red es transparente.

Redes de Área Local Olga Minguet 44

UD5. Interconexión de equipos en redes locales (II)

2. EL ACCESO A LAS REDES WAN

2.2. Servicios de acceso remoto

Escenario de conexión RAS

Ejemplo de conexión mediante servicio RAS en una red con Windows Server

Redes de Área Local Olga Minguet 45

UD5. Interconexión de equipos en redes locales (II)

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 1
- Actividad 2

Redes de Área Local Olga Minguet 46

8.5.2 Cuaderno de actividades

Cuaderno de Actividades

- UNIDAD 5 -
Interconexión de equipos en redes locales (II)

CUADERNO DE ACTIVIDADES

Objetivos

- Consolidar los contenidos vistos en la Unidad 5 del curso de Redes de Área Local.
- Se han descrito los principios de funcionamiento de las redes locales.
- Se han reconocido los principios funcionales de las redes locales.
- Se han identificado los distintos tipos de redes y los protocolos.
- Se han configurado los parámetros básicos.
- Se han aplicado mecanismos básicos de seguridad.

Actividades

1. Confirma la veracidad de las siguientes afirmaciones:

El protocolo PPP puede gestionar intercambio de paquetes de cualquier protocolo de red

Cierto/falso	
--------------	--

Justificación	
---------------	--

PPTP es un protocolo que crea túneles sobre los que se encapsula TCP/IP, NetBeui o SPX/IPX

Cierto/falso	
--------------	--

Justificación	
---------------	--

Un protocolo de gestión de autenticación es el que se encarga de pedir el nombre de usuario y la contraseña

Cierto/falso	
--------------	--

Justificación	
---------------	--

Basta con incorporar a la comunicación cualquier protocolo de autenticación para que la comunicación sea totalmente segura

CUADERNO DE ACTIVIDADES

Cierto/falso	
Justificación	

2. Descubre el error en el siguiente razonamiento:

“El administrador de red de una instalación ha preparado un sistema Linux en un portátil de un comercial que se va de viaje. Desde el portátil el comercial hará conexiones remotas hacia el servidor RAS Windows localizado en la sede central de las oficinas. El servidor sólo tiene configurado el protocolo NetBeui. Cuando el portátil se conecta al servidor RAS usa el protocolo TCP/IP.

Como RAS es compatible con TCP/IP y NetBeui, no importa que cliente y servidor 'hablen' con protocolos distintos, ya que el servicio hace transparente la comunicación al usuario.”

3. Confirma la veracidad de las siguientes afirmaciones:

El encaminador opera siempre en el nivel 3 de OSI	
Cierto/falso	
Justificación	

Algunos encaminadores toman funciones de niveles superiores al 3	
Cierto/falso	
Justificación	

UD05 – Interconexión de equipos en redes locales (II) 3-10

CUADERNO DE ACTIVIDADES

Un router sólo puede encaminar paquetes IP	
Cierto/falso	
Justificación	

Todos los protocolos de red son encaminables con el router adecuado	
Cierto/falso	
Justificación	

Los routers no pueden encadenarse en cascada	
Cierto/falso	
Justificación	

4. Escribe en la columna de la derecha la dirección de la red del nodo que aparece en la de la izquierda.

Nodo	Red
10.0.1.88/24	
192.168.1.1/16	
192.168.1.1/8	
192.168.1.1/32	

5. Confirma la veracidad de las siguientes afirmaciones:

Los encaminadores pueden ser abiertos, cerrados o de frontera	
Cierto/falso	
Justificación	

Los algoritmos de encaminamiento estático son aquellos que impiden que se cambien las tablas de rutas del encaminador en el que se ejecutan	
---	--

UD05 – Interconexión de equipos en redes locales (II) 4-10

CUADERNO DE ACTIVIDADES

Cierto/falso	
Justificación	

Un algoritmo de encaminamiento adaptativo habilita al router para aprender por sí mismo la topología de la red

Cierto/falso	
Justificación	

El coste de una ruta es el precio económico que se ha de pagar por transmitir un paquete

Cierto/falso	
Justificación	

El tiempo de convergencia es el tiempo que tarda un router en arrancar desde que se enciende hasta que queda operativo

Cierto/falso	
Justificación	

La distancia telemática al destino se mide con un parámetro que se denomina coste de la ruta

Cierto/falso	
Justificación	

RIPv1 está limitado a 15 saltos, sin embargo, la versión RIPv2 supera esta limitación

Cierto/falso	
Justificación	

CUADERNO DE ACTIVIDADES

OSPF siempre envía el paquete por la ruta más corta según el número de saltos

Cierto/falso	
Justificación	

6. En esta actividad vamos a gestionar la tabla de rutas de nuestro ordenador con Windows. Para cada apartado INDICA EL COMANDO que has ejecutado y captura la pantalla si estás realizando ésta actividad online.

a) Crea una ruta para alcanzar la red 192.168.30 por el enrutador 192.168.30.254.

Comando

Captura

b) Crea una ruta que alcance la red 192.168 por el enrutador 192.168.101.254.

Comando

Captura

CUADERNO DE ACTIVIDADES

c) Visualiza las rutas para comprobar que están creadas correctamente.

Comando

Captura

d) Modifica la segunda ruta para que el enrutador sea 192.168.71.254

Comando

Captura

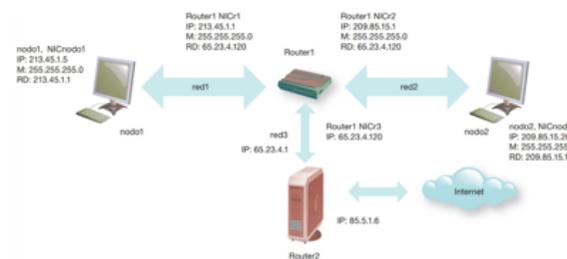
e) Borra las dos rutas.

Comando

Captura

7. En la imagen anterior se muestran varias redes interconectadas entre sí

CUADERNO DE ACTIVIDADES



Donde "RD" indica la puerta de enlace

A continuación, se proponen tres situaciones:

- A. El ordenador con IP 213.45.1.5 se quiere comunicar con un ordenador con IP 213.45.1.8
- B. El ordenador con IP 213.45.1.5 se quiere comunicar con el ordenador con IP 209.85.15.20
- C. El ordenador con IP 213.45.1.5 quiere abrir una página web en Internet en la dirección 20.14.15.6

Rellena la información de la siguiente tabla:

	Situación A	Situación B	Situación C
dirección de la red del ordenador origen en notación CIDR			
dirección de la red del ordenador destino en notación CIDR			
puerta de enlace mediante la que el ordenador origen podrá comunicarse con el destino			
interfaz de red usada para dicha			

CUADERNO DE ACTIVIDADES

conexión			
las redes por las que pasarán los paquetes de información			

8. Busca los errores técnicos en el siguiente comentario.

«Para proteger una red de área local de los accesos indebidos desde la red externa se ha instalado un cortafuegos al que se conectan la red local, Internet y una red perimetral.

Para que un paquete de red procedente de Internet llegue a la red desmilitarizada, previamente debe pasar por la red local protegida.

Sin embargo, los paquetes con destino en Internet que proceden de la red local no es necesario que pasen por el cortafuegos ya que los riesgos siempre están en la red externa.»

9. Imaginemos un nodo de la red local que no necesita conectarse a Internet más que para navegar por la web.

a) Si no puede acceder a un servidor proxy, ¿debe tener configurada al menos la puerta por defecto para poder navegar por la Web?

CUADERNO DE ACTIVIDADES

b) ¿Y si tiene acceso a un servidor proxy que está en la red de área local?

c) ¿Y si tiene acceso a un servidor proxy que está en otra red?

8.5.3 Cuaderno de prácticas

Guía del Cuaderno de PRÁCTICAS

- UNIDAD 5 - Packet Tracer

Interconexión de equipos en redes locales (II)
Interconexión de redes

Nombre y apellidos	
--------------------	--

Desarrollo
✓ PRÁCTICA 1: Red híbrida controlada por un router inalámbrico.
✓ PRÁCTICA 2: Red WAN entre 3 ciudades.
✓ PRÁCTICA 3: Configuración de un Firewall.

Introducción

Este conjunto de actividades pretende que el alumno conozca las funcionalidades básicas generales y avanzadas, acerca del funcionamiento de la herramienta que provee CISCO llamada PACKET TRACER. Esta herramienta sirve para poner en marcha la construcción de redes de ordenadores, sin la necesidad de tener dispositivos de hardware o software adicionales a la maquina en la que está instalado esta herramienta.

Permite crear redes, permitiendo su configuración real, en el IOS que provee CISCO en sus routers. Esto agrega un gran valor, pues esta herramienta dispone de interfaces de hardware genéricas y específicas de dicha empresa. No necesitando tener ordenadoras, routers, interfaces, cables, etc., para saber el comportamiento físico y real de una red. Ahorrando así, tiempo en construcción de redes. Muchos paquetes de configuración de routers utilizando una versión parecida a la que provee IOS. Por lo que solamente se necesita saber las variantes que existen, si las hubiera.

Objetivos

- Consolidar los contenidos vistos en el curso de Redes de Área Local.
- Aprender a configurar redes de ordenadoras, en un nivel teórico.
- Utilizar la herramienta Cisco Packet Tracer.
- Utilizar comandos de consola de IOS
- Utilizar interfaces gráficas para la configuración.
- Uso del protocolo de enrutamiento dinámico.
- Disposiciones de configuraciones reales de ordenadores a pequeña y gran escala.

Consideraciones



Esta imagen indica que el resultado de la tarea a realizar ha de ser indicado en el Cuaderno de la Actividad. Las capturas de pantalla se han de hacer con la herramienta Recortes de Windows

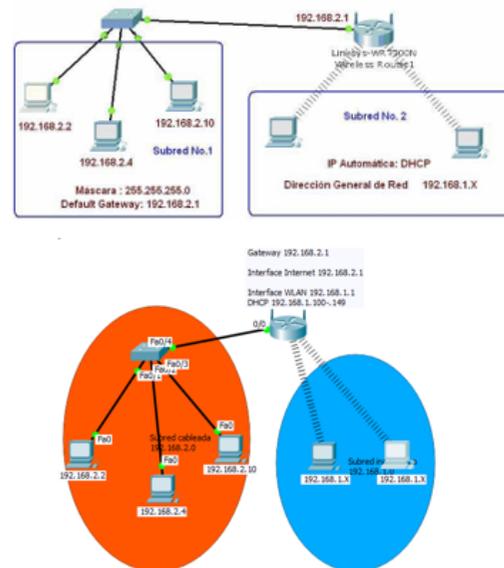
Práctica de simulación 1

RED HÍBRIDA CONTROLADA POR UN ROUTER INALÁMBRICO

El resultado de esa actividad se guardará en un archivo con el nombre: **Solución Práctica 1.pkt**

En esta configuración de red, vamos a tener una subred cableada y una subred inalámbrica. Los equipos que hacen parte de la red cableada pertenecen a una dirección de subred diferente a los equipos que pertenecen a la red inalámbrica. Adicionalmente, se aprovechará la oportunidad para configurar los equipos de tal forma que los hosts pertenecientes a la LAN cableada utilicen direccionamiento IP estático y los hosts de la WLAN (Wireless LAN) utilicen direccionamiento IP dinámico bajo el uso del protocolo DHCP.

El esquema topológico que vamos a diseñar es el siguiente:



En la figura se indica claramente las direcciones IP requeridas para la subred cableada, las cuales pertenecen a la dirección de subred: **192.168.2.0**; la subred inalámbrica trabajará bajo el uso del protocolo DHCP distribuyendo las direcciones IP al host propio de la dirección de subred: **192.168.1.0**

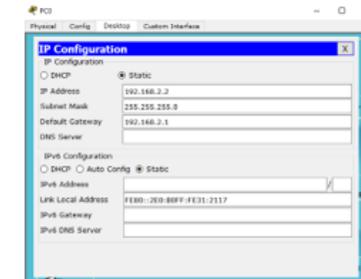
Paso 1.1:

En vista de lo anterior, lo primero que se debe hacer es montar una red con los elementos indicados en la figura anterior:

- 1 switch 2950-24
- 3 PCs genéricos
- 1 router inalámbrico WRT300N
- 2 PCs Wireless

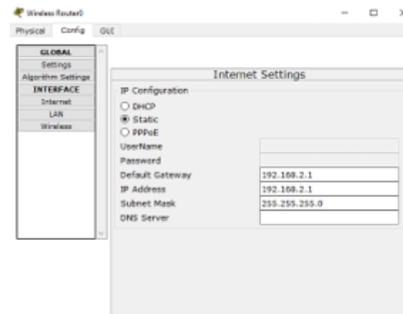
Conectar los dispositivos alámbricos con el cableado adecuado.

Posteriormente se han de configurar las direcciones IP, máscara de Subred y Default Gateway en cada uno de los equipos que hacen parte de la red cableada, según los criterios de diseño del esquema topológico anterior, tal como se ilustra en la figura siguiente.



Como se hace uso de un Router Inalámbrico, hay necesidad de configurar la dirección de Gateway, la cual es la aquella dirección que utilizarán los host para acceder a otras subredes, en éste caso, para acceder a la subred 192.168.1.0. Para ello se ha de configurar el router en Config/Internet tal y como se indica en la figura siguiente.

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS



Paso 1.2:

Cuando se realiza la conexión física entre el Switch y el Router Inalámbrico, se hace a través de la interfaz de INTERNET; sobre la cual se debe configurar la dirección de Gateway tal como se ilustra en la figura siguiente.

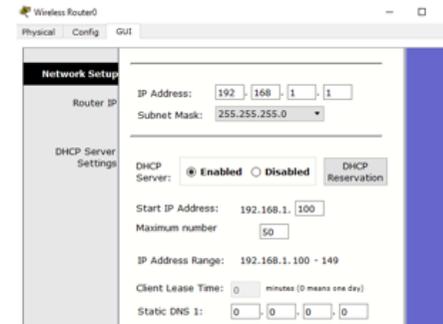
Se selecciona el Router inalámbrico, se escoge la opción GUI sobre la cual se definen los siguientes parámetros:

Los parámetros que se configuran son:

- IP Address: 192.168.1.1 (Interfaz gateway subred inalámbrica)
- Subnet Mask (Máscara de subred): 255.255.255.0
- DHCP Enabled : Indicando que se utilizará el protocolo DHCP
- Start IP Address: 192.168.1.100 (Dirección inicial para la adjudicación de direcciones IP en forma automática)
- Número máximo de usuarios: 50
- Rango de direcciones IP para distribución: 192.168.1.100 - 192.168.1.149

Recuerda hacer clic en "Save Settings" para guardar la configuración.

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS



Paso 1.3:

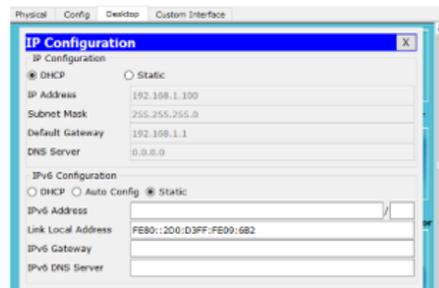
Recuerda que cada host posee un módulo de conexión Ethernet que debe ser cambiado por uno de conexión inalámbrica. Además, cada host que hacen parte de la red inalámbrica se deben configurar utilizando el protocolo DHCP, el cual se encargará de adjudicar según sus criterios las direcciones IP a cada uno de los Host.



Es importante comprender en qué lugar se deben definir aquellos parámetros que rigen la distribución de direcciones IP, propias de la red inalámbrica.

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS



- Realiza la actividad Paso 1.3 del Cuaderno de Actividades

Paso 1.4:

Todas las redes inalámbricas deben tener implementado algún tipo de sistema de seguridad. En este paso se va a hacer uso del Protocolo WEP en redes.

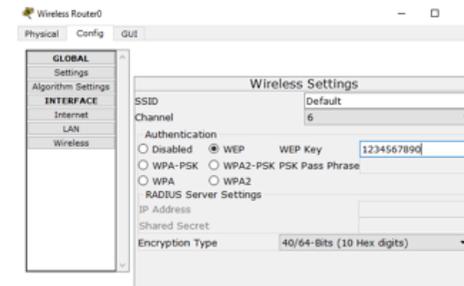
Utilizando el mismo esquema de red anterior, tal como se ilustra en la siguiente figura, seleccionamos el router inalámbrico y nos ubicamos en la sección Config. Allí se establece el modo de Seguridad a utilizar, el cual por defecto se encuentra deshabilitado.

En éste caso en particular, seleccionamos WEP y establecemos la contraseña o Key, la cual será utilizada por el router inalámbrico y los PCs para encriptar su información bajo el uso de éste protocolo. Vale la pena mencionar que ésta contraseña deberá ser de al menos 10 caracteres.

UD05 Interconexión de equipos en redes locales (II)

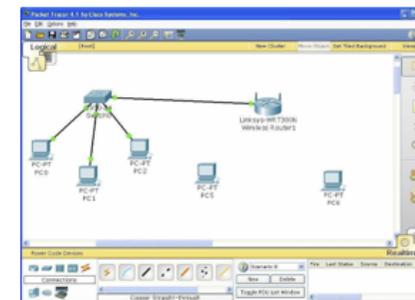
PRÁCTICAS

Existen herramientas software especializadas en generar éste tipo de contraseñas teniendo en cuenta criterios de seguridad mayores a los que usualmente poseen las contraseñas convencionales.



Obsérvese, que, si activamos el protocolo WEP en el router, los equipos o host no establecerán comunicación con él hasta que en cada uno de ellos no se defina que se utilizará éste protocolo y se defina la misma contraseña de encriptación configurada en el router.

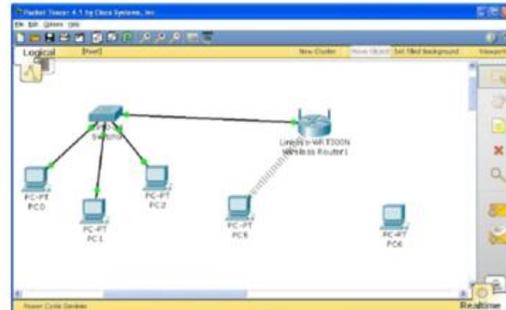
En la siguiente figura se ilustra claramente ésta situación. En la primera figura se evidencia que ninguno de los host inalámbricos presenta comunicación con el Router.



UD05 Interconexión de equipos en redes locales (II)

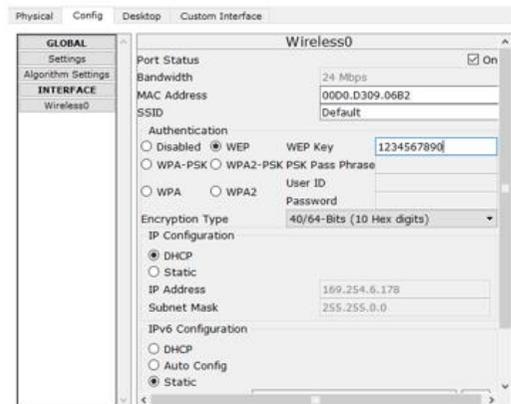
PRÁCTICAS

Y tan pronto ésta configuración se realiza en uno de los PCs, automáticamente inicia el proceso de comunicación. Pero, para ello, será necesario realizar el Paso 1.5



Paso 1.5:

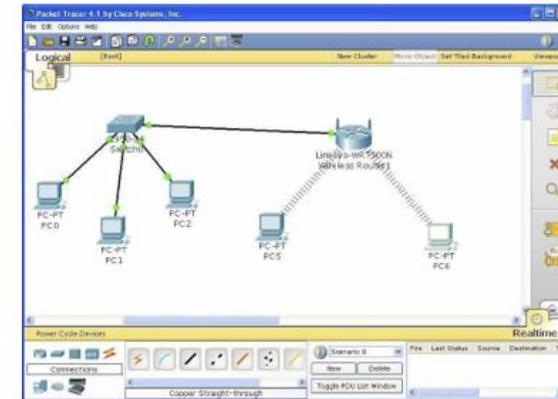
En la siguiente figura se ilustra la configuración en uno de los PCs. Se ha de aplicar esta configuración a los dos PCs inalámbricos.



UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Finalmente queda configurada la red de la siguiente forma:



Paso 1.6:



- Realiza la actividad Paso 1.6 del Cuaderno de Actividades

Práctica de simulación 2

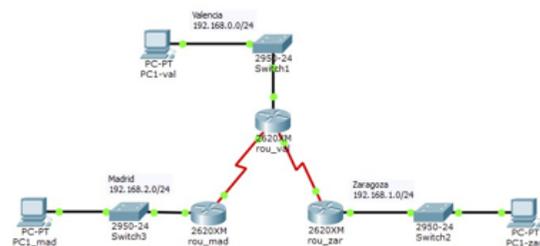
RED WAN ENTRE TRES CIUDADES

El resultado de esa actividad se guardará en un archivo con el nombre: **Solución Práctica 2.pkt**

En esta actividad se va a diseñar una red WAN que va a comunicar las redes de tres ciudades mediante tres routers.

Paso 2.1:

El esquema topológico que vamos a diseñar es el siguiente:



Dispositivos que vamos a utilizar:

- Tres Routers 2620XM
- Tres switches 2950-24
- Cuatro Módulos seriales WIC - 1T

Con base en la topología de la red arrastra tres router Cisco 2620XM, para lo cual selecciona router en la parte inferior izquierda (Reset Networks) y en la ventana siguiente donde aparecen los router selecciona el router 2620XM y páselo al área de trabajo.

Realiza de forma similar para pasar los Tres Switches 2950-24

De igual forma selecciona en dispositivos finales (End Devices) el ordenador y arrastre tres ordenadores genéricos

Paso 2.2:

Se debe adicionar a los router los módulos seriales para la interconexión WAN de las redes.

En el router de Valencia se le deben añadir dos módulos seriales WIC - 1T (Uno para interconectar cada ciudad) y en los otros dos routers un solo serial. Para realizarlos realiza los siguientes pasos.

1. Selección del router (doble clic)
2. Apaga el router, dando clic en el interruptor del router
3. Añade el módulo WIC - 1T seleccione Physical/Modules/ WIC - 1T y arrastre el módulo a los slots pequeños, en el Router de Valencia añade dos módulos y debe quedar como aparece en la figura siguiente.
4. Acciona el router, dando clic en el interruptor del router
5. En los routers de Madrid y Zaragoza añade un módulo serial WIC - 1T de forma similar



UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS

Paso 2.3:

En este paso vas a interconectar los dispositivos LAN y WAN.

Usando los Switches interconecta en cada ciudad el ordenador y el router para lo cual realiza los siguientes pasos:

1. Con base en la topología de la red indicada al principio de la actividad 3, seleccione **Connections** (Conexiones) parte inferior izquierda (ResetNetworks) y en la ventana siguiente seleccione **Cooper Straight-Through** (cable de cobre directo) y realice una línea entre el Ordenador y Switch, seleccionando el puerto Ethernet del ordenador y cualquier puerto libre del switch. De igual forma entre el Router y el Switch
2. Realiza este paso de igual forma en las otras dos ciudades.

Usando los puertos seriales de los router interconecta las ciudades para lo cual realiza el siguiente paso:

1. Selecciona **Connections** (Conexiones) parte inferior izquierda (**Reset Networks**) y en la ventana siguiente seleccione **Serial DTE** (cable Serial del equipo de Control de Datos) y realice una línea entre el Router de Valencia y Router de Madrid.
2. Realiza este paso de igual forma entre los router de Valencia y Zaragoza.

Paso 2.4:

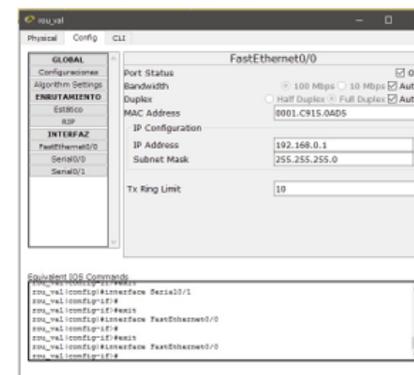
En este paso vamos a realizar la configuración del direccionamiento IP de los dispositivos LAN y WAN.

Para la configuración del direccionamiento IP de las interfaces LAN (**FastEthernet - Fa0/0**) y de las interfaces WAN (**Serial 0/0 - S0/0**) realiza el siguiente proceso:

1. Selección el router de la red de Valencia (doble clic).
2. Para configurar el nombre del router en el Menú selecciona

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS

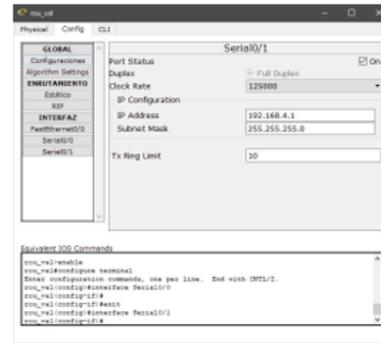
3. Config/Global/Settings y en los campos **Display Name** y **Hostname** escribe el nombre del router en el caso de Valencia rou-val Para configurar la dirección IP del router en la **Interface LAN**, en el Menú selecciona **Interfaces/FastEthernet0/0**, activa la interface seleccionado el campo **Port Status** y en los campos **Ip Address** y **Subnet Mask** escribe la dirección IP y la máscara de subred, para el router de Valencia la dirección IP sería **192.168.0.1** y la máscara **255.255.255.0** y debe quedar como aparece en la figura siguiente.



4. Para configurar la dirección IP del router en la **Interface WAN** entre **Valencia** y **Madrid**, en el Menú selecciona **Config/Interfaces/Serial0/1**, activa la interface seleccionado el campo **Port Status**, como el router de Valencia es el DTE (Equipo Control de Datos - MODEM) configura la velocidad de transmisión a 125000 bits por segundo en el campo **Clock Rate** y en los campos **Ip Address** y **Subnet Mask** escribe la dirección IP y la máscara de subred, para el router de Valencia la dirección IP sería **192.168.4.1** y la máscara **255.255.255.0** y debe quedar como aparece en la figura siguiente:

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS



5. Configura la dirección IP del router en la Interface WAN entre Valencia y Zaragoza (Serial 0/0) igual que el punto anterior con los siguientes datos.

Campo	Valor
Interface	Serial 0/0
Port Status	Activo
Clock Rate	125000 bps
Ip Address	192.168.3.1
Subnet Mask	255.255.255.0

Tabla 1. Datos Interface WAN Router de Valencia a Zaragoza

6. Configura la interface LAN del router de Zaragoza con los datos de la tabla siguiente igual hiciste en el router de Valencia (puntos 1,2 y 3).

Campo	Valor
Display Name	Rou_zar
Hostname	Rou_zar
Interface	FastEthernet 0/0
Ip Address	192.168.1.1
Subnet Mask	255.255.255.0

Tabla 2. Datos Interface LAN Router de Zaragoza

7. Configura la dirección IP del router en la Interface WAN entre Zaragoza y Valencia (Serial 0/0) igual que en el punto 4 con los siguientes datos.

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Campo	Valor
Interface	Serial 0/0
Port Status	Activo
Clock Rate	Not Set
Ip Address	192.168.3.2
Subnet Mask	255.255.255.0

Tabla 3. Datos Interface WAN Router de Zaragoza a Valencia

8. Configura la interface LAN del router de Madrid con los datos de la tabla 4 igual que se hizo en el router de la red de Valencia (puntos 1,2 y 3).

Campo	Valor
Display Name	Rou_mad
Hostname	Rou_mad
Interface	FastEthernet 0/0
Ip Address	192.168.2.1
Subnet Mask	255.255.255.0

Tabla 4. Datos Interface LAN Router de Madrid

9. Configura la dirección IP del router en la Interface WAN entre Madrid y Valencia (Serial 0/0) igual que el punto 4 con los siguientes datos.

Campo	Valor
Interface	Serial 0/0
Port Status	Activo
Clock Rate	Not Set
Ip Address	192.168.4.2
Subnet Mask	255.255.255.0

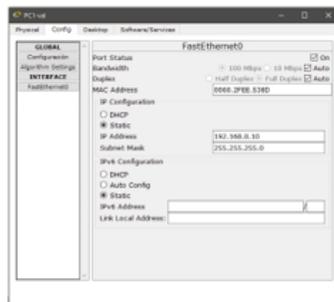
Tabla 5. Datos Interface WAN Router de Madrid a Valencia

10. Para configurar la dirección IP de los ordenadores selecciona el ordenador de la red de Valencia (doble clic). Para configurar el nombre del ordenador y la puerta de enlace en el Menú selecciona Config/Global/Settings y en los campos Display Name y Gateway escribe el nombre del ordenador en el caso de Valencia pc1-val y como puerta de enlace 192.168.0.1
11. Para configurar la dirección IP del ordenador en la Interface LAN, en el Menú seleccione Interfaces/FastEthernet0/0, active la interface seleccionado el campo Port Status y en los campos Ip Address y Subnet Mask escribe la dirección IP y la máscara de subred, para el ordenador de Valencia la dirección IP sería 192.168.0.10 y la máscara 255.255.255.0 y debe quedar como aparece en la

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

figura siguiente.



12. Configura la interface LAN del ordenador de Zaragoza con los datos de la tabla siguiente de igual forma que lo hizo en el ordenador de la red de Valencia (puntos 11 y 12).

Campo	Valor
Display Name	Pc1_zar
Gateway	192.168.1.1
Interface	FastEthernet 0/0
Ip Address	192.168.1.10
Subnet Mask	255.255.255.0

Tabla 6. Datos Interface LAN Ordenador de Zaragoza

13. Configura la interface LAN del ordenador de Madrid con los datos de la siguiente de igual forma que se hizo en el ordenador de la red de Valencia (puntos 11 y 12).

Campo	Valor
Display Name	Pc1_mad
Gateway	192.168.2.1
Interface	FastEthernet 0/0
Ip Address	192.168.2.10
Subnet Mask	255.255.255.0

Tabla 7. Datos Interface LAN Ordenador de Madrid

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Paso 2.5:

Configurar el enrutamiento dinámico (RIP). Para configurar el enrutamiento dinámico en cada router se debe informar qué direcciones de red tiene conectada directamente a cada router (adyacentes) y el protocolo de enrutamiento se encarga de averiguar y actualizar las tablas de enrutamiento.

En el router de Valencia tiene tres redes adyacentes:

Red	Dirección de Red
LAN Valencia	192.168.0.0
WAN entre Valencia y Zaragoza	192.168.3.0
WAN entre Valencia y Madrid	192.168.4.0

Tabla 8. Redes adyacentes al router de Valencia

En el router de Zaragoza tiene dos redes adyacentes:

Red	Dirección de Red
LAN Zaragoza	192.168.1.0
WAN entre Zaragoza y Valencia	192.168.3.0

Tabla 9. Redes adyacentes al router de Zaragoza

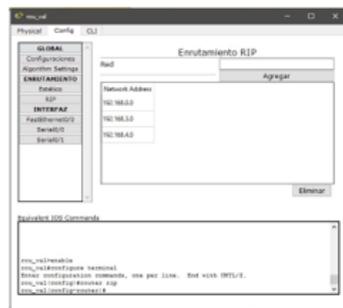
En el router de Madrid dos redes adyacentes:

Red	Dirección de Red
LAN Madrid	192.168.2.0
WAN entre Madrid y Valencia	192.168.4.0

Tabla 10. Redes adyacentes al router de Madrid

Para configurar el enrutamiento dinámico en el router sigue los siguientes pasos

1. Selección el router de la red de Valencia (doble clic).
2. Para configurar el enrutamiento RIP en el router de Valencia en el Menú selecciona Config/Routing/RIP y añade las tres direcciones de red adyacentes en el campo Network, que están en la tabla 8 y queda como aparece en la figura siguiente:



3. Realiza el mismo proceso en los router de Zaragoza y Madrid añadiendo las redes que están conectadas directamente a cada router (adyacentes), como aparece en las tablas 9 y 10.

Paso 2.6:



- Realiza la actividad Paso 2.6 del Cuaderno de Actividades

Paso 2.7:



- Realiza la actividad Paso 2.7 del Cuaderno de Actividades

Práctica de simulación 3

CONFIGURACIÓN DE UN FIREWALL

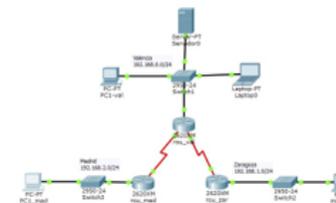
El resultado de esa actividad se guardará en un archivo con el nombre: **Solución Práctica 3.pkt**

En esta actividad vamos a partir del diseño de red que hicimos en la Actividad 2 para configurar un firewall que añade seguridad a nuestra red.

Para ello, vamos a configurar un servidor para que sólo acepte peticiones externas mediante protocolo IP y TCP, lo que nos permitirá abrir páginas web o comunicar via FTP.

En cambio, vamos a configurar que cualquier petición a través del protocolo ICMP que venga del exterior será rechazada, ya que habitualmente es el protocolo que se suele utilizar cuando se pretende acceder a una red de forma no autorizada desde el exterior. Por ejemplo, de esta forma no se puede realizar PING a máquinas de la red.

Partimos del esquema topológico básico de la actividad 2, añadiendo un servidor:



Por lo tanto, vamos a definir los siguientes servicios en el servidor para poder hacer las pruebas:

- El servicio **DNS** para poder abrir páginas web desde cualquier ordenador de la red.
- El servicio **FTP** para poder transferir archivos entre el servidor y los ordenadores de la red.

El cortafuego debe permitir que estos servicios funcionen correctamente en todos los equipos de la red.

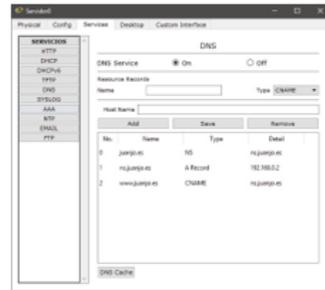
Paso 3.1: CONFIGURACIÓN DEL SERVICIO DNS

Acceder a través del navegador indicando direcciones IP es poco práctico. Vamos a configurar el servicio de DNS que nos permita traducir nombres de dominios a direcciones IP.

Vamos a configurar el servicio DNS en el servidor. Para ello ve en el servidor a las opciones Services/DNS y añade los registros:

- CNAME (Nombre canónico)
- NS (nameserver)
- A Record (Apuntador a registro)

Configúralos con tu nombre (por ejemplo juanjo.es, pero cambia juanjo por tu nombre. Si es de más de una palabra usa el carácter "_" para separarlas). En la figura siguiente se indica la configuración:



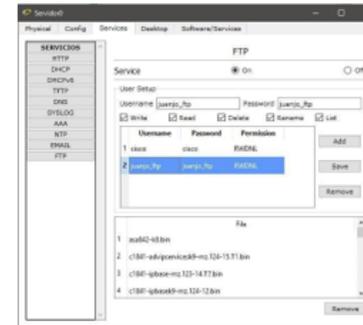
Ahora que tenemos un servidor DNS activo y funcionando, habrá que indicar en los PCs de la red que, en su configuración, el servidor DNS primario indique la dirección IP de nuestro servidor DNS.

Realiza esta configuración en los todos los ordenadores de la red.

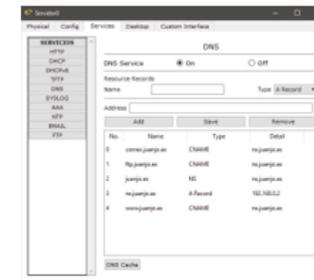
Desde un pc cualquiera carga alguna página del servidor con el URL de su dominio (según la configuración de la imagen sería <http://www.olga.es>). Ahora ya no es necesario usar la dirección IP para acceder a las páginas.

Paso 3.2: CONFIGURACIÓN DEL SERVICIO FTP

En la ventana de configuración del servicio FTP del servidor, crea un usuario con tu nombre tal y como se indica en la figura y que tenga permisos para escribir, leer, modificar, borrar y listar los archivos del servidor ftp.



Y a continuación se ha de configurar este servicio en el servidor DNS tal y como se muestra en la figura. Has de indicar en tu caso la IP de tu servidor.



Y ahora prueba el servicio desde uno de los ordenadores que hay comunicación mediante protocolo FTP. Para ello crea una PDU compleja (ADD complex PDU) de tipo FTP en la opción de la barra derecha de la pantalla.

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

En el ejemplo de la imagen siguiente se prueba el servicio FTP conectando el ordenador con la IP 192.168.0.10 con la IP del servidor (en este ejemplo es 192.168.0.2). Los puertos habituales con los que trabaja el protocolo FTP son el 20 y el 21, que son los utilizados en la prueba.



En tu caso, has de indicar las direcciones IP que hayas configurado en los equipos.

Paso 3.3: CONFIGURACIÓN DEL CORTAFUEGOS

Abrimos la pantalla de configuración del servidor y vamos a Desktop/Firewall. Configuramos los siguientes parámetros:

Campo	Valor
Action	Deny
Protocol	ICMP
Remote IP	0.0.0.0
Remote Wildcard Mask	255.255.255.255
Remote Port	
Local Port	

Tabla 11. Denegación acceso Protocolo ICMP

Campo	Valor
Action	Allow
Protocol	IP
Remote IP	0.0.0.0
Remote Wildcard Mask	255.255.255.255
Remote Port	
Local Port	

Tabla 12. Permiso acceso Protocolo IP

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

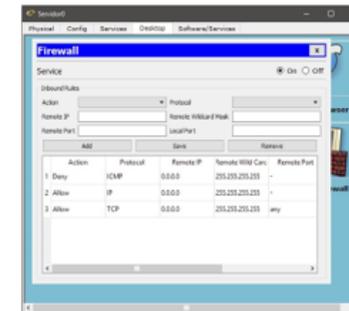
Campo	Valor
Action	Allow
Protocol	TCP
Remote IP	0.0.0.0
Remote Wildcard Mask	255.255.255.255
Remote Port	any
Local Port	any

Tabla 13. Permiso acceso Protocolo TCP

La dirección 0.0.0.0 indica que se aplica la regla a cualquier dirección IP que acceda al servidor. La máscara 255.255.255.255 indica que se aplica la regla a cualquier valor de máscara.

Pulsamos 'On' para activar el firewall en el servidor.

En la siguiente imagen se muestra la configuración resultante.



Paso 3.4:

A continuación, vamos a comprobar que el cortafuego funciona correctamente cuando ejecutamos los diferentes servicios configurados en el servidor. Para ello vamos a probar la comunicación entre diferentes hosts de la red para confirmar que se comporta tal y como deseamos.

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Antes de empezar las pruebas, borra todas las pruebas antiguas que tengas en la ventana de la esquina inferior derecha.



- Realiza la actividad Paso 3.2 del Cuaderno de Actividades

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Cuaderno de PRÁCTICAS

- UNIDAD 5 -

PACKET TRACER

Interconexión de equipos en redes locales (II)

Interconexión de redes

Nombre y apellidos	
--------------------	--

Desarrollo
<ul style="list-style-type: none"> ✓ PRÁCTICA 1: Red híbrida controlada por un router inalámbrico. ✓ PRÁCTICA 2: Red WAN entre 3 ciudades. ✓ PRÁCTICA 3: Configuración de un Firewall.

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Práctica de simulación 1

RED HÍBRIDA CONTROLADA POR UN ROUTER INALÁMBRICO

Paso 1.3



A continuación, se verifica la comunicación entre un equipo de la red cableada y un host inalámbrico, específicamente, desde la dirección 192.168.2.2 (LAN Cableada) a la dirección 192.168.1.102 (LAN Inalámbrica)

Inserta la captura de la pantalla

Paso 1.6:



A continuación, vamos a verificar que hay comunicación entre los diferentes ordenadores de la red. Para ello, en la barra de opciones derecha vamos a seleccionar "Add Simple PDU" y vamos a probar la comunicación entre:

- PC0 y PC6. Inserta la captura de la pantalla

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

- PC6 y PC1. Inserta la captura de la pantalla

- PC6 y PC5. Inserta la captura de la pantalla

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Práctica de simulación 2

RED WAN ENTRE TRES CIUDADES

Paso 2.6:



A continuación, vamos a probar la conectividad LAN. Desde el ordenador de cada red vamos a realizar un ping a la puerta de enlace para probar conectividad en cada LAN. Seguiremos los siguientes pasos

- Selección del ordenador de la red de Valencia (doble clic), para realizar un ping a la puerta de enlace de Valencia (192.168.0.1)
Inserta la captura de la pantalla

Realizar la misma prueba en los ordenadores de cada ciudad. En caso de problemas revisar todo el proceso

- Entre un ordenador de Valencia y uno de Madrid
Inserta la captura de la pantalla

- Entre un ordenador de Valencia y uno de Zaragoza
Inserta la captura de la pantalla

- Entre un ordenador de Zaragoza y uno de Madrid

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS

Inserta la captura de la pantalla

Paso 2.7:



En este paso vamos a comprobar la **conectividad WAN**. Desde el ordenador de cada red realizar un **ping** y un **tracert** a los ordenadores de las otras redes, para probar conectividad en cada LAN.

Por ejemplo, seleccionando el ordenador de la red de Valencia (doble clic), para realizar un ping al ordenador de la red de Zaragoza, selecciona **Desktop/Command Prompt**, y escribe el comando **ping 192.168.1.10** y **tracert 192.168.1.10**.

Inserta la captura de la pantalla del resultado del ping

Inserta la captura de la pantalla del resultado del tracert

Repite la operación entre un ordenador de Valencia y uno de Madrid.

Inserta la captura de la pantalla del resultado del ping

Inserta la captura de la pantalla del resultado del tracert

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS

Repite la operación entre un ordenador de Madrid y uno de Zaragoza.

Inserta la captura de la pantalla del resultado del ping

Inserta la captura de la pantalla del resultado del tracert

Práctica de simulación 3. CONFIGURACIÓN DE UN FIREWALL

Paso 3.2:



Prueba si el ordenador PC1-val se puede comunicar haciendo **ping** con el servidor.

Prueba si el servidor se puede comunicar haciendo **ping** con el ordenador PC1-val. Inserta captura de pantalla.

Prueba si el ordenador PC1-mad se puede comunicar haciendo **ping** con el servidor. Inserta captura de pantalla.

Prueba si el servidor se puede comunicar haciendo **ping** con el ordenador PC1-mad. Inserta captura de pantalla.



Prueba si desde PC1-val se puede abrir la página web del servidor. Inserta captura de pantalla.



Prueba si desde PC1-mad se puede abrir la página web del servidor. Inserta captura de pantalla.



Prueba si desde PC1-val se puede hacer FTP al servidor. Inserta captura de pantalla.



Prueba si desde PC1-mad se puede hacer FTP al servidor. Inserta captura de pantalla.

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

PRÁCTICAS DE TALLER

Nombre y apellidos	
--------------------	--

Breve descripción	Visualizar tablas de enrutamiento y aprender a realizar las configuraciones básicas del router , implementando después conectividad básica mediante la configuración de direcciones IP en dispositivos intermedios y PC's. Utilizaremos comandos básicos de Administración de Sistemas, como show y ping , para verificar las configuraciones y la conectividad.
Material necesario	<ul style="list-style-type: none"> • Cuaderno de trabajo • Bolígrafo y/o lápiz • 1 PC con Packet Tracer
Fuentes de información	<ul style="list-style-type: none"> • Diapositivas de la Unidad 5 • Explicaciones de clase

Desarrollo	<ul style="list-style-type: none"> ✓ PRÁCTICA 1: Visualización de las tablas de enrutamiento de host. ✓ PRÁCTICA 2: Construcción de una red con switch y router.
-------------------	--

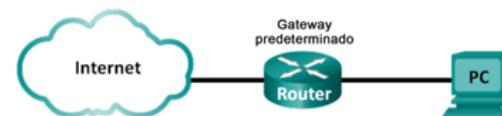
UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

PRÁCTICA 1

Visualización de las tablas de enrutamiento de un host

Topología



Desarrollo

Para acceder a un recurso en una red, el host determina la ruta hacia el host de destino mediante la tabla de routing o enrutamiento.

La tabla de enrutamiento del host es similar a la de un router, pero es específica del host local y mucho menos compleja. Para que un paquete llegue a un destino local, se requiere la tabla de routing del host local. Para llegar a un destino remoto, se requieren la tabla de enrutamiento del host local y la tabla de enrutamiento del router.

Los comandos **netstat -r** y **route print** proporcionan detalles sobre la forma en que el host local enruta los paquetes al destino.

En esta práctica de taller, mostrarás y examinarás la información en la tabla de routing de host de la PC utilizando los comandos **netstat -r** y **route print**. Asimismo, determinarás la forma en que la PC enrutará paquetes según la dirección de destino.

Por supuesto, es necesario que tengamos conexión a Internet.

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS

Parte 1: [Acceder a la tabla de enrutamiento del host](#)

Paso 1: Registrar la información del PC.

En el PC, abre una ventana de símbolo del sistema y escribe el comando `ipconfig /all` para visualizar la siguiente información y registrarla:

Dirección IPv4	
Dirección MAC	
Gateway predeterminado	

Paso 2: Mostrar las tablas de enrutamiento.

En una ventana de símbolo del sistema, escribe el comando `netstat -r` para visualizar la tabla de enrutamiento de host.

¿Cuáles son las tres secciones que se muestran en el resultado?

Paso 3: Examinar la lista de interfaces.

En la primera sección, Interface List, se muestran las direcciones de control de acceso al medio (MAC) y el número de interfaz asignado de cada interfaz con capacidad de red en el host.

```
Interface List
13...90 4c e5 be 15 63 .....Atheros AR9285 802.11b/g/n WiFi Adapter
1 .....Software Loopback Interface 1
25...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
12...00 00 00 00 00 00 e0 Microsoft Gt04 Adapter
26...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
14...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
```

La primera columna corresponde al número de interfaz. La segunda columna corresponde a la lista de direcciones MAC asociadas a las interfaces con capacidad de red en los hosts. Estas interfaces pueden incluir adaptadores Ethernet, Wi-Fi y Bluetooth. La tercera columna muestra el fabricante y una descripción de la interfaz.

En este ejemplo, la primera línea muestra la interfaz inalámbrica que está conectada a la red local.

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS

Nota: Si el PC tiene una interfaz Ethernet y un adaptador inalámbrico habilitados, se incluirán las dos interfaces en la lista de interfaces.

¿Cuál es la dirección MAC de la interfaz conectada a la red local? ¿Cómo se compara la dirección MAC con la dirección MAC registrada en el paso 1?

La segunda línea corresponde a la interfaz de bucle invertido. Cuando el protocolo de control de transmisión/protocolo de Internet (TCP/IP) se ejecuta en un host, a la interfaz de bucle invertido se le asigna automáticamente una dirección IP 127.0.0.1.

Las cuatro últimas líneas representan la tecnología de transición que permite la comunicación en un entorno mixto e incluye IPv4 e IPv6.

Parte 2: [Examinar las entradas de la tabla de routing de host IPv4](#)

Vamos a examinar la tabla de enrutamiento de host IPv4. Esta tabla se encuentra en la segunda sección como resultado del comando `netstat -r`. Enumera todas las rutas IPv4 conocidas, incluidas las conexiones directas, la red local y las rutas predeterminadas locales.

```
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1     192.168.1.11     25
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        306
127.255.255.255           255.255.255.255 On-link         127.0.0.1        306
192.168.1.0                255.255.255.0   On-link         192.168.1.11     281
192.168.1.11              255.255.255.255 On-link         192.168.1.11     281
192.168.1.255             255.255.255.255 On-link         192.168.1.11     281
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         192.168.1.11     281
255.255.255.255           255.255.255.255 On-link         127.0.0.1        306
255.255.255.255           255.255.255.255 On-link         192.168.1.11     281
=====
Persistent Routes:
None
```

El resultado se divide en cinco columnas: *Network Destination* (Destino de red), *Netmask* (Máscara de red), *Gateway*, *Interface* (Interfaz) y *Metric* (Métrica).

- En la columna Network Destination, se indica la red con la que hay posibilidad de conexión. El destino de red se utiliza con la máscara de red para coincidir con la dirección IP de destino.
- En la columna Netmask, se indica la máscara de subred que el host utiliza para determinar las porciones de red y host de la dirección IP.

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

- En la columna Gateway, se indica la dirección que el host utiliza para enviar los paquetes a un destino de red remoto. Si un destino está conectado directamente, el gateway aparece como On-link (En enlace) en el resultado.
- En la columna Interface, se indica la dirección IP que está configurada en el adaptador de red local. Se utiliza para reenviar un paquete en la red.
- En la columna Metric, se indica el costo de usar una ruta. Se utiliza para calcular la mejor ruta a un destino. Una ruta preferida tiene un número de métrica menor que otras rutas de la lista.

El resultado que ves en el ejemplo muestra cinco tipos diferentes de **rutas activas**:

- La ruta predeterminada local 0.0.0.0 se utiliza cuando el paquete no coincide con otras instrucciones especificadas en la tabla de routing. El paquete se envía hacia el gateway desde la PC para un procesamiento adicional. En este ejemplo, el paquete se envía hacia 192.168.1.1 desde 192.168.1.11.
- Las direcciones de bucle invertido, 127.0.0.0 – 127.255.255.255, están relacionadas con la conexión directa y prestan servicios al host local.
- Todas las direcciones para la subred, 192.168.1.0 – 192.168.1.255, están relacionadas con el host y la red local. Si el destino final del paquete está en la red local, el paquete sale de la interfaz 192.168.1.11.
 - La dirección de la ruta local 192.168.1.0 representa todos los dispositivos en la red 192.168.1.0/24.
 - La dirección del host local es 192.168.1.11.
 - La dirección de difusión de la red 192.168.1.255 se utiliza para enviar mensajes a todos los hosts en la red local.
- Las direcciones de multidifusión de clase D especiales 224.0.0.0 están reservadas para ser utilizadas a través de la interfaz de bucle invertido (127.0.0.1) o del host (192.168.1.11).
- La dirección de difusión local 255.255.255.255 se puede utilizar a través de la interfaz de bucle invertido (127.0.0.1) o del host (192.168.1.11).

Según el contenido de la tabla de routing IPv4, si la PC deseara enviar un paquete a 192.168.1.15, ¿qué haría y adónde enviaría el paquete?

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS

Si la PC deseara enviar un paquete a un host remoto ubicado en 172.16.20.23, ¿qué haría y adónde enviaría el paquete?

¿Cómo es el número de bits para la red que se indica para IPv4? ¿Y cómo es para IPv6?

¿Por qué hay información tanto de IPv4 como de IPv6 en las tablas de routing de host?

UD05 Interconexión de equipos en redes locales (II) PRÁCTICAS

PRÁCTICA 2

Montaje de una red con switch y router

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.0.1	255.255.255.0	N/D
	G0/1	192.168.1.1	255.255.255.0	N/D
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Desarrollo

Esta es una práctica de laboratorio exhaustiva para repasar los comandos del IOS que se abarcaron anteriormente. En esta práctica de laboratorio, conectará el equipo tal como se muestra en el diagrama de topología. Luego, configurará los dispositivos según la tabla de direccionamiento. Cuando se haya guardado la configuración, la verificará probando la conectividad de red.

Una vez que los dispositivos estén configurados y que se haya verificado la conectividad de red, utilizará los comandos del IOS para recuperar la información de los dispositivos y responder preguntas sobre los equipos de red.

En esta práctica de laboratorio, se proporciona la ayuda mínima relacionada con los comandos que, efectivamente, se necesitan para configurar el router. Sin embargo, los comandos necesarios se encuentran en el apéndice A. Ponga a prueba su conocimiento e intente configurar los dispositivos sin consultar el apéndice.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco de la serie 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte ¡Error! No se encuentra el origen de la referencia. al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Recursos necesarios

- 1 router Cisco
- 1 switch Cisco
- 2 PC's con Windows y un programa de emulación de terminal, como Tera Term
- Cables de consola para configurar los dispositivos con Cisco IOS
- Cables Ethernet, como se muestra en la topología

Nota: las interfaces Gigabit Ethernet en los routers Cisco actuales tienen detección automática M-DIX, y se puede utilizar indistintamente cable directo o cable cruzado de Ethernet entre el router y la PC-B. Si utilizamos un modelo de router Cisco antiguo, puede ser necesario obligatoriamente usar un cable Ethernet cruzado, porque no dispone de esta tecnología.

Página 8 de 16

UD05 Interconexión de equipos en redes locales (II)

PRÁCTICAS

Parte 1: Establecer la topología e inicializar los dispositivos

Paso 1: Realizar el cableado de red tal como se muestra en la topología.

- a. Conecta los dispositivos que se muestran en el diagrama de topología y tiende el cableado, según sea necesario.
- b. Enciende todos los dispositivos de la topología.

Hay que tener en cuenta que si los archivos de configuración se guardaron previamente en el router y el switch (se hizo un *copy run start*) será necesario inicializar y volver a cargar estos dispositivos con los parámetros básicos. Habla para ello con tu profesora.

Parte 2: Configurar los dispositivos y verificar la conectividad

Vamos a configurar la topología de la red y los parámetros básicos, como direcciones IP de la interfaz, el acceso de los dispositivos y contraseñas. Consulta la Topología y la Tabla de direccionamiento que aparecen al principio de la práctica para obtener información sobre nombres de dispositivos y direcciones.

Paso 1: Asignar información de IP estática a las interfaces de la PC.

- a. Configura la dirección IP, la máscara de subred y los parámetros del gateway predeterminado en la PC-A.
- b. Configura la dirección IP, la máscara de subred y los parámetros del gateway predeterminado en la PC-B.
- c. Haz ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.
¿Por qué crees que los pings no fueron correctos?

Paso 2: Configurar el router.

- a. Accede al router mediante el puerto de consola y habilita el modo EXEC privilegiado.
- b. Entra al modo de configuración (*configure terminal*).
- c. Asigna un nombre de dispositivo al router.
- d. Deshabilita la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.
- e. Asigna **class** como la contraseña cifrada del modo EXEC privilegiado.

Página 10 de 16

UD05 Interconexión de equipos en redes locales (II) **PRÁCTICAS**

- f. Asigna `cisco` como la contraseña de consola y permita el inicio de sesión.
- g. Asigna `cisco` como la contraseña de VTY y permita el inicio de sesión.
- h. Cifra las contraseñas de texto no cifrado.
- i. Crea un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
- j. Configura y active las dos interfaces en el router.
- k. Ahora deberíamos guardar la configuración en ejecución en el archivo de configuración de inicio, pero nosotros NO lo vamos a realizar para trabajar otros grupos.
- l. Configura el reloj en el router.
Nota: utilice el signo de interrogación (?) para poder determinar la secuencia correcta de parámetros necesarios para ejecutar este comando.
- m. Haz ping a la PC-B en una ventana con el símbolo del sistema en la PC-A.
¿Ahora fueron correctos los pings? ¿Por qué?

Parte 3: Mostrar información del dispositivo

Ahora vamos a utilizar los comandos `show` para recuperar información del router y del switch.

Paso 1: Recuperar información del hardware y del software de los dispositivos de red.

- a. Utiliza el comando `show version` para responder las siguientes preguntas sobre el router.

¿Cuál es el nombre de la imagen de IOS que el router está ejecutando?

¿Cuánta memoria DRAM tiene el router?

UD05 Interconexión de equipos en redes locales (II) **PRÁCTICAS**

¿Cuánta memoria NVRAM tiene el router?

¿Cuánta memoria flash tiene el router?

- b. Utiliza el comando `show version` y responde las siguientes preguntas sobre el switch.
¿Cuál es el nombre de la imagen del IOS que el switch está ejecutando?

UD05 Interconexión de equipos en redes locales (II) **PRÁCTICAS**

¿Cuánta memoria de acceso aleatorio dinámica (DRAM) tiene el switch?

¿Cuánta memoria de acceso aleatorio no volátil (NVRAM) tiene el switch?

¿Cuál es el número de modelo del switch?

Paso 2: Mostrar la tabla de routing en el router.

Utiliza el comando **show ip route** en el router y responde las preguntas siguientes:

¿Qué código se utiliza en la tabla de routing para indicar una red conectada directamente? _____

¿Cuántas entradas de ruta están codificadas con un código C en la tabla de routing?

¿Qué tipos de interfaces están asociadas a las rutas con código C?

UD05 Interconexión de equipos en redes locales (II) **PRÁCTICAS**

Paso 3: Mostrar la información de la interfaz en el router.

Utiliza el comando **show interface g0/1** (o la interfaz que tengas conectada en tu caso en su lugar) y responde las preguntas siguientes:

¿Cuál es el estado operativo de la interfaz G0/1?

¿Cuál es la dirección de control de acceso a los medios (MAC) de la interfaz G0/1?

¿Cómo se muestra la dirección de Internet en este comando?

Paso 4: Mostrar una lista de resumen de las interfaces del router y del switch.

Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. Uno de los más útiles es el comando **show ip interface brief**. El resultado del comando muestra una lista resumida de las interfaces en el dispositivo e informa de inmediato el estado de cada interfaz.

a. Introduce el comando **show ip interface brief** en el router.

Después,

b. Introduce el comando **show ip interface brief** en el switch.

Y responde,

Si la interfaz G0/1 (o la que tú tengas conectada en su lugar) se mostrara administrativamente inactiva, ¿qué comando de configuración de interfaz utilizarías para activar la interfaz?

¿Qué ocurriría si hubiéramos configurado incorrectamente la interfaz G0/1 en el router con una dirección IP 192.168.1.2?

8.6 Unidad didáctica 6

Las averías más frecuentes son fáciles de diagnosticar, porque tienen efectos que solo pueden ser producidos por causas bien determinadas, de modo que, conociendo el efecto negativo producido, somos capaces de determinar su causa y actuar sobre ella. Sin embargo, ocasionalmente hay averías que son muy difíciles de diagnosticar, donde no se sabe si la causa de la avería viene de un mal funcionamiento del hardware, del software o de la red. Esto ocurre especialmente si el defecto producido por la avería puede ser debido a causas muy distintas.

En ésta unidad didáctica se pretende dar las herramientas necesarias para resolver incidencias en una red de área local, siguiendo los cinco pasos de todo proceso de resolución: 1) documentar la red, para lo cual es importantísimo de cara a facilitar la resolución de problemas mantener un mapa actualizado de la red donde se indique las topologías y direcciones de los equipos; 2) recopilar toda la información disponible y analizar los síntomas de la avería. ¿Dónde se ha producido la avería? Esto implicará conocer en qué ordenador o en qué cable se encuentra, la ubicación física en el edificio, etc.; 3) localizar y aislar la avería, esto es, conocer cuál es la causa de la avería, qué produjo la avería. Para ello se deberán emplear herramientas de monitorización (comprobadores de red o de cables, analizadores de red y monitores de red) y de diagnóstico, en especial las herramientas de red; 4) solución de la avería y verificar que está resuelta; 5) documentar los resultados. Para terminar, debemos documentar el problema y la reparación.

8.6.1 Presentación teórica

CURSO

Redes de Área Local

UNIDAD 6

***Resolución de incidencias de una red de área local.
Protección, vigilancia y soporte de redes***

Redes de Área Local
Olga Minguet
1

UD6. Resolución de incidencias de una red de área local

ÍNDICE

1. CONDICIONES FÍSICAS Y AMBIENTALES DE LA INSTALACIÓN
2. ESTRATEGIAS: PARÁMETROS DE RENDIMIENTO
3. INCIDENCIAS FÍSICAS E INCIDENCIAS LÓGICAS EN REDES LOCALES
4. MONITORIZACIÓN DE REDES CABLEADAS E INALÁMBRICAS
5. HERRAMIENTAS DE DIAGNÓSTICO
6. VIGILANCIA Y MANTENIMIENTO DE LA RED

Redes de Área Local
Olga Minguet
2

UD6. Resolución de incidencias de una red de área local

ÍNDICE

1. **CONDICIONES FÍSICAS Y AMBIENTALES DE LA INSTALACIÓN**
 - 1.1. Condiciones físicas
 - Ubicación de los armarios de cableado
 - Tamaño de los armarios de cableado
 - 1.2. Condiciones ambientales
 - Temperatura y humedad
 - Ruidos e interferencias electromagnéticas
 - Inundaciones
 - Iluminación
 - Incendios
 - Otros

Redes de Área Local
Olga Minguet
3

UD6. Resolución de incidencias de una red de área local

1. CONDICIONES FÍSICAS Y AMBIENTALES DE LA INSTALACIÓN

Debemos tener en cuenta las condiciones físicas y ambientales para una correcta instalación de la red de área local.




Redes de Área Local
Olga Minguet
4

UD6. Resolución de incidencias de una red de área local

1. CONDICIONES FÍSICAS Y AMBIENTALES DE LA INSTALACIÓN

1.1. Condiciones físicas

Ubicación de los armarios de cableado
 En los armarios de cableado se encuentran muchos de los cables y dispositivos de la red, por eso su ubicación es un factor importante.



Para la elección de la ubicación hay que tener en cuenta las necesidades de suministro de corriente, conexión a tierra y climatización (calefacción, ventilación o aire acondicionado).
 Existen normas que rigen todos los aspectos relacionados con los armarios de cableado: ubicación, materiales para paredes, suelos y techos, temperatura, humedad, iluminación, toma de corriente, acceso a la sala y al equipo, y soporte y acceso a los cables.

Redes de Área Local Olga Minguet 5

UD6. Resolución de incidencias de una red de área local

1. CONDICIONES FÍSICAS Y AMBIENTALES DE LA INSTALACIÓN

1.1. Condiciones físicas

Tamaño de los armarios de cableado

El armario de cableado debe ser lo suficiente grande como para albergar los dispositivos de interconexión y el cableado, contemplando las futuras ampliaciones.



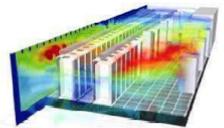
Redes de Área Local Olga Minguet 6

UD6. Resolución de incidencias de una red de área local

1. CONDICIONES FÍSICAS Y AMBIENTALES DE LA INSTALACIÓN

1.2. Condiciones ambientales

Las condiciones ambientales de la instalación son también muy importantes, pues de ellas depende el buen funcionamiento de la red.



Ejemplos:

- Temperatura y humedad**
 La temperatura del armario de cableado debe mantenerse entre 18 y 24°C
 La humedad relativa debe mantenerse entre 30% y 55%
- Ruidos e interferencias electromagnéticas**
 Causados por lámparas fluorescentes, líneas de alta tensión, motores, microondas, teléfonos y copiadoras... estas perturbaciones electromagnéticas causan errores en la transmisión, por eso es importante elegir un lugar para nuestra red donde sean mínimos.

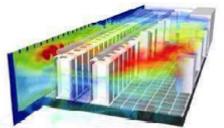
Redes de Área Local Olga Minguet 7

UD6. Resolución de incidencias de una red de área local

1. CONDICIONES FÍSICAS Y AMBIENTALES DE LA INSTALACIÓN

1.2. Condiciones ambientales

Las condiciones ambientales de la instalación son también muy importantes, pues de ellas depende el buen funcionamiento de la red.



Ejemplos:

- Inundaciones**
 Hay que proteger los armarios de cableado de cualquier amenaza de inundación.
- Iluminación**
 Los armarios deben estar bien iluminados, con la luz situada preferiblemente en el techo.
- Incendios**
 Los armarios deben estar protegidos ante el riesgo de incendios.

Redes de Área Local Olga Minguet 8

UD6. Resolución de incidencias de una red de área local

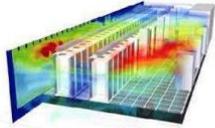
1. CONDICIONES FÍSICAS Y AMBIENTALES DE LA INSTALACIÓN

1.2. Condiciones ambientales

Las condiciones ambientales de la instalación son también muy importantes, pues de ellas depende el buen funcionamiento de la red.

Ejemplos:

- Además existen **otros factores ambientales** comunes a todos los lugares de trabajo determinados:
 - .Vibraciones
 - .Materiales y sustancias peligrosos en el entorno.
 - .Calidad del aire.
 - .Contaminación acústica
 - .Radiaciones.



Redes de Área Local Olga Minguet 9

UD6. Resolución de incidencias de una red de área local

2. ESTRATEGIAS: PARÁMETROS DE RENDIMIENTO

Medidas de rendimiento:

- El rendimiento de una red: Se puede medir con la velocidad de transferencia y nos informa si la red funciona de forma óptima.
- Número de paquetes de datos: Es el camino por el cual pasan los paquetes de datos de un nodo de la red al otro. También confirma a través del porcentaje de paquetes que llegan al destino si es una red con buen rendimiento o no.
- En algunos casos pueden alterarse los paquetes en el camino.
- Tiempo de respuesta: Es lo que determina si el rendimiento de una red es rápido o es lento.
- Otros Factores: El rendimiento de una red depende de unos factores como el diseño de red, la topología, los protocolos, los adaptadores de red, etc...



Redes de Área Local Olga Minguet 10

UD6. Resolución de incidencias de una red de área local

3. INCIDENCIAS FÍSICAS E INCIDENCIAS LÓGICAS EN REDES LOCALES

Incidencias físicas

Una de las incidencias más típicas suelen ser fallos en tarjetas de red, para conexión cableada o para conexión inalámbrica. Podemos observar que no funciona si no parpadea el led.

El *procedimiento* sería el siguiente:

- Comprobar si está bien conectado el cable, en ambos lados de la conexión.
- Ver si está conectado a la toma de corriente
- Verificar que tiene instalados sus drivers



Redes de Área Local Olga Minguet 11

UD6. Resolución de incidencias de una red de área local

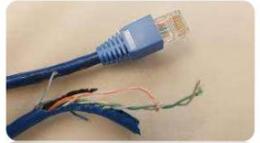
3. INCIDENCIAS FÍSICAS E INCIDENCIAS LÓGICAS EN REDES LOCALES

Incidencias físicas

Otra de las incidencias más frecuentes son fallos en los cables de red.

El *procedimiento* sería el siguiente:

- Revisar el estado de los conectores
- Comprobar la conexión
- Comprobar que no superen la longitud máxima para su categoría
- Revisar el estado del cable



Redes de Área Local Olga Minguet 12

UD6. Resolución de incidencias de una red de área local

3. INCIDENCIAS FÍSICAS E INCIDENCIAS LÓGICAS EN REDES LOCALES

Incidencias físicas

Fallos de los dispositivos de interconexión.

El *procedimiento* sería el siguiente:

- Revisar que está conectado a la corriente
- Comprobar que no esté recalentado
- Si un nodo tiene un fallo con un puerto este se probará en otro



Redes de Área Local Olga Minguet 13

UD6. Resolución de incidencias de una red de área local

3. INCIDENCIAS FÍSICAS E INCIDENCIAS LÓGICAS EN REDES LOCALES

Incidencias lógicas

Las mas comunes suelen darse en las impresoras y los ataques de seguridad.

Problemas con impresoras

- Reinstalar los driver
- Ver que esté encendida
- Comprobar que esté bien compartida en la red



Redes de Área Local Olga Minguet 14

UD6. Resolución de incidencias de una red de área local

3. INCIDENCIAS FÍSICAS E INCIDENCIAS LÓGICAS EN REDES LOCALES

Incidencias lógicas

Incidencias provocadas por ataques a la seguridad

Los efectos de estos:

- Destrucción de información del disco duro, inutilización del sistema operativo
- Borrado de la bios
- Spyware
- Saturar la red
- Spam
- Colapsar servidores



Redes de Área Local Olga Minguet 15

UD6. Resolución de incidencias de una red de área local

3. INCIDENCIAS FÍSICAS E INCIDENCIAS LÓGICAS EN REDES LOCALES

Incidencias lógicas

Incidencias provocadas por ataques a la seguridad

Medidas preventivas:

- Uso de antivirus actualizado
- Cortafuegos
- Buenas contraseñas
- Cifrar los datos
- Uso de protocolos de seguridad



Redes de Área Local Olga Minguet 16

UD6. Resolución de incidencias de una red de área local

 Realiza las siguientes **ACTIVIDADES** del Cuaderno de Actividades:

- **Actividad 1**
- **Actividad 2**
- **Actividad 3**

Redes de Área Local Olga Minguet 17

UD6. Resolución de incidencias de una red de área local

4. MONITORIZACIÓN DE REDES CABLEADAS E INALÁMBRICAS

El objetivo de la monitorización es asegurarse de que la red funciona correctamente.
Al monitorizar una red es importante establecer una línea base que determina los valores normales de rendimiento de la red. Estos valores son actualizados cuando se realizan cambios en la red.

Algunas herramientas para llevar a cabo la monitorización de redes:

- ✓ **Monitores de rendimiento**
- ✓ **Monitores de red**
- ✓ **Programas agentes (SNMP)**
- ✓ **Analizadores de red**
- ✓ **Logs del sistema**



Redes de Área Local Olga Minguet 18

UD6. Resolución de incidencias de una red de área local

4. MONITORIZACIÓN DE REDES CABLEADAS E INALÁMBRICAS

✓ **Monitores de rendimiento**

La mayoría de los sistemas operativos de red actuales incluyen esta herramienta que permite:

- Obtener y almacenar datos de rendimiento.
- Enviar alertas al administrador de la red.
- Iniciar otro programa que devuelva al sistema a unos rangos aceptables.

Un ejemplo sería el software IPHost Network Monitor para Windows disponible en shareware.



Redes de Área Local Olga Minguet 19

UD6. Resolución de incidencias de una red de área local

4. MONITORIZACIÓN DE REDES CABLEADAS E INALÁMBRICAS

✓ **Monitores de red**

Algunos servidores incluyen software para la monitorización de la red. Esta herramienta captura y analiza secuencias de datos de la red desde y hasta el servidor, que se utilizan para diagnosticar problemas potenciales de la red.

Algunos ejemplos son:

- PCAP: Es una librería de programación para la captura de paquetes.
- NetGong de Tsarfin Computing Ltd para Windows
- Nagios: no es solo un monitor de red, sino que permite monitorizar también servidores, conmutadores, aplicaciones y servicios.

Redes de Área Local Olga Minguet 20

UD6. Resolución de incidencias de una red de área local

4. MONITORIZACIÓN DE REDES CABLEADAS E INALÁMBRICAS

✓ **Protocolo básico de gestión de red (SNMP)**

En un entorno SNMP, hay unos programas denominados agentes que se ejecutan en cada dispositivo de la red. Estos monitorizan el tráfico de la red para recopilar datos estadísticos que guardan en sus bases de información de gestión.

Además de los agentes hay un gestor que procesa esta información y puede actuar en consecuencia activando alarmas, provocando la ejecución de programas, etc.

Ejemplo: HP Automated Network Management, de Hewlett-Packard Co.

Redes de Área Local Olga Minguet 21

UD6. Resolución de incidencias de una red de área local

4. MONITORIZACIÓN DE REDES CABLEADAS E INALÁMBRICAS

✓ **Analizadores de red**



Los analizadores de red pueden ser hardware, software o mixtos. Su finalidad es supervisar el tráfico de una red de comunicaciones, es decir, capturar la información que circula por la red para realizar su monitorización, y pueden incluir funciones de gestión de alarmas e informes. Ejemplos:

- PRTG Network Monitor de la compañía Paessler AG para Windows.
- Network Packet Analyzer de la compañía AirGrab para MAC.

Redes de Área Local Olga Minguet 22

UD6. Resolución de incidencias de una red de área local

4. MONITORIZACIÓN DE REDES CABLEADAS E INALÁMBRICAS

✓ **Logs del sistema**

Un log del sistema es un fichero en el que se registra lo que sucede en un determinado sistema durante un intervalo de tiempo específico.

Puede almacenar tráfico de paquetes, colisiones, fallos, etc. Estos datos pueden ser analizados por el administrador de la red para asegurar que funcione de manera correcta sin errores.



Redes de Área Local Olga Minguet 23

UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Proceso para solucionar un problema en la red:

1º:Identificar el problema. Se trata de obtener una descripción lo más exacta posible del problema e intentar determinar cual fue la secuencia exacta de los sucesos	2º:Aislar el problema Para saber exactamente cual es el problema hay que saber como se produce y cuáles son los resultados.	3º:Planificar reparación Primero buscaremos soluciones sencillas (cables conectados, equipos encendidos...) y descartarlas para seguir con las más complejas.
4º:Confirmar resultados Hay que confirmar que el problema se ha resuelto, para ello debemos contar con los usuarios que al testearlo no den otros problemas	5º:Documentar los resultados Nos servirá para futuros problemas similares.	

Redes de Área Local Olga Minguet 24

UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Gracias a diferentes herramientas podemos averiguar las causas de los problemas

Herramientas para el hardware:

- **Voltímetro**
Nos permite comprobar:
 - Si el cable es continuo
 - Si transmite señal
 - Si una parte expuesta del cable está tocando otro conductor, como una superficie metálica
 - Si dos partes del mismo cable están tocándose.



Redes de Área Local Olga Minguet 25

UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Gracias a diferentes herramientas podemos averiguar las causas de los problemas

Herramientas para el hardware:

- **Reflectómetros de dominio temporal (TDR)**
El TDR envían pulsos a través de los cables para localizar cortes, cortocircuitos o imperfecciones. Si el TDR encuentra un problema lo analiza, y presenta el resultado.



Redes de Área Local Olga Minguet 26

UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Gracias a diferentes herramientas podemos averiguar las causas de los problemas

Herramientas para el hardware:

- **Analizadores de LAN**
Los analizadores de LAN permiten comprobar el estado de las redes LAN en todos los niveles.



Redes de Área Local Olga Minguet 27

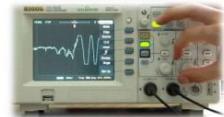
UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Gracias a diferentes herramientas podemos averiguar las causas de los problemas

Herramientas para el hardware:

- Otras herramientas:
 - Generador y localizador de tonos**
Mide la continuidad y la polaridad de una línea
 - Osciloscopio**
Mide y representa señales gráficamente

Redes de Área Local Olga Minguet 28

UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Herramientas software:

Son necesarias para monitorizar tendencias e identificar problemas en el rendimiento de la red. La principal es el analizador de protocolos.

Los analizadores de protocolos capturan todas las tramas que viajan por la red, decodificándolas y analizando su contenido.

Redes de Área Local Olga Minguet 29

UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Herramientas software:

1. Detectan fuentes de problemas (como errores de conexión o cuellos de botella)
2. Generan estadísticas tanto de la red como en los usuarios (tamaño de tramas, tráfico recibido y enviado,...)
3. Gestionan alarmas ante determinadas circunstancias, como superación del tamaño máximo de tramas.
4. Gestionan datos de uso de la red e informes de gestión
5. Identifican muchos aspectos de la red
6. Equipos más activos
7. Rendimiento de la red
8. Pueden detectar y filtrar paquetes en función del tipo, protocolo destinatario, etc.

Redes de Área Local Olga Minguet 30

UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Herramientas software:

Ejemplo: *Filtrado de contenidos web*

Podemos filtrar los contenidos de Internet acudiendo a dos técnicas:

- 1) Reconociendo en la información transmitida las palabras para compararlas con una **lista de palabras prohibidas**. Cuando coincide alguna de las palabras, se deniega el acceso a la página. Es un método poco eficaz.
- 2) El segundo método se basa en la utilización de **listados de sitios prohibidos** que han sido previamente clasificados por la empresa que nos suministra el filtro. El problema de este método reside en que las páginas de Internet cambian con frecuencia y no hay una manera razonable de tener las listas actualizadas.

Redes de Área Local Olga Minguet 31

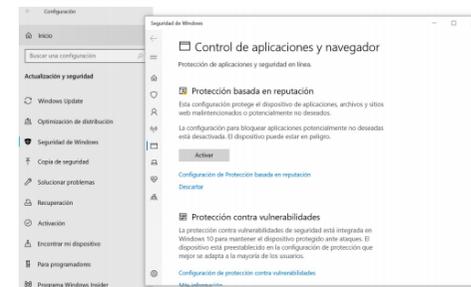
UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Herramientas software:

Ejemplo: *Filtrado de contenidos web*

Windows 10 dispone de herramientas para definir sitios web de confianza o sitios web restringidos a los que no se permitirá el acceso. Desde *Configuración*.



Redes de Área Local Olga Minguet 32

UD6. Resolución de incidencias de una red de área local

5. HERRAMIENTAS DE DIAGNÓSTICO

Herramientas software:

Analizadores de protocolos

- ✓ Wireshark
- ✓ Sniffer Products
- ✓ Capsa

Wireshark es uno de los analizadores de tráfico de red más difundidos. Con esta herramienta se pueden visualizar los protocolos que se están utilizando con fines educativos, pero, además, puede ser mal-utilizada para obtener aquellas páginas que se están utilizando sin ningún tipo de cifrado y capturar desde ahí una cuenta de usuario y contraseña, lo que nos tiene que hacer reflexionar sobre la importancia de mantener las redes seguras.

Redes de Área Local Olga Minguet 33

UD6. Resolución de incidencias de una red de área local

Wireshark

Analizador de protocolos

Redes de Área Local Olga Minguet 34

UD6. Resolución de incidencias de una red de área local

6. VIGILANCIA Y MANTENIMIENTO DE LA RED (a nivel usuario)

A) Del tráfico de red

Windows 10 dispone de una herramienta para monitorizar el tráfico de red local para cada uno de los adaptadores o interfaces de red instalados.

Redes de Área Local Olga Minguet 35

UD6. Resolución de incidencias de una red de área local

6. VIGILANCIA Y MANTENIMIENTO DE LA RED (a nivel usuario)

B) Del rendimiento

Redes de Área Local Olga Minguet 36

UD6. Resolución de incidencias de una red de área local

6. VIGILANCIA Y MANTENIMIENTO DE LA RED (a nivel usuario)

C) Visor de eventos

La auditoría es una de las funciones más importantes de los administradores de redes. Se diseña un sistema de recogida de datos para detectar averías o intrusos.

Windows dispone de un **Visor de Eventos** que realiza un registro del sistema de forma automática. Desde **Herramientas administrativas de Windows**:



Redes de Área Local **Olga Minguet** **37**

UD6. Resolución de incidencias de una red de área local

6. VIGILANCIA Y MANTENIMIENTO DE LA RED (a nivel usuario)

D) Consolas de gestión remota

Un gestor de consolas, de sesiones remotas o simplemente gestor de control remoto, es una aplicación que es capaz de visualizar sobre una consola local lo que está ocurriendo en una consola remota, incluso ejecutar acciones en el sistema remoto comandados desde el sistema local.

Destacan Escritorio Remoto (Windows), TeamViewer o VNC por ser software libre, de amplio uso y además están soportados por muchos sistemas operativos.



Redes de Área Local **Olga Minguet** **38**

UD6. Resolución de incidencias de una red de área local

6. VIGILANCIA Y MANTENIMIENTO DE LA RED (a nivel usuario)

E) Firewall (Cortafuegos)

Seguridad de Windows

El servicio Seguridad de Windows es el lugar de inicio para ver y administrar la seguridad y el estado de tu dispositivo.

Abre Seguridad de Windows

Actualización y seguridad
Windows Update, recuperación, copia de seguridad

Áreas de protección

- Protección contra virus y amenazas: No se requieren acciones.
- Protección de cuentas: No se requieren acciones.
- Firewall y protección de red: No se requieren acciones.
- Control de aplicaciones y exploradores: Acciones recomendadas.
- Seguridad del dispositivo: No se requieren acciones.

Seguridad de Windows

Firewall y protección de red
¿Quién y qué puede tener acceso a las redes.

- Red de dominio: El firewall está activado.
- Red privada: El firewall está activado.
- Red pública (activa): El firewall está activado.

Permitir una aplicación a través de firewall
Solicitudes de problemas de red e Internet
Configuración de notificaciones del firewall
Configuración avanzada
Restaurar Firewall a los valores predeterminados

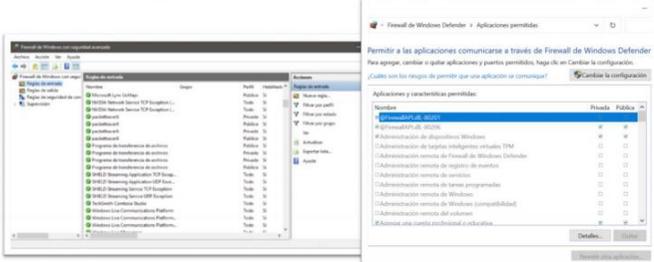
Redes de Área Local **Olga Minguet** **39**

UD6. Resolución de incidencias de una red de área local

6. VIGILANCIA Y MANTENIMIENTO DE LA RED (a nivel usuario)

E) Firewall (Cortafuegos)

Desde configuración avanzada podemos ver las reglas tanto de entrada como de salida que están configuradas en el cortafuegos.



Redes de Área Local **Olga Minguet** **40**

UD6. Resolución de incidencias de una red de área local



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 4
- Actividad 5
- Actividad 6
- Actividad 7
- Actividad 8

8.6.2 Cuaderno de actividades

Cuaderno de Actividades

- UNIDAD 6 -

Resolución de incidencias de una red de área local.
Protección, vigilancia y soporte de redes

CUADERNO DE ACTIVIDADES

Objetivos

- Consolidar los contenidos vistos en la Unidad 6 del curso de Redes de Área Local.
- Se han descrito los principios de funcionamiento de las redes locales.
- Se han reconocido los principios funcionales de las redes locales.
- Se han identificado los distintos tipos de redes y los protocolos.
- Se han configurado los parámetros básicos.
- Se han aplicado mecanismos básicos de seguridad.

Actividades

1. Lee el contenido de la página web de Wikipedia <https://es.wikipedia.org/wiki/Subcontrataci%C3%B3n> sobre la externalización (*outsourcing*) de servicios, para contestar a las siguientes preguntas:
 - a) ¿Qué es la subcontratación u *outsourcing*?
 - b) ¿Cuál es el principal objetivo del *outsourcing*?
 - c) ¿Qué es la deslocalización?
2. Lee el contenido de la página web https://es.wikipedia.org/wiki/Mesa_de_ayuda sobre los servicios *Help Desk*, para contestar a las siguientes cuestiones:
 - a) ¿Qué es un *Help Desk*?
 - b) ¿Qué recursos técnicos componen la base de un *Help Desk*?
 - c) ¿Qué conocimientos deben tener los técnicos de un *Help Desk* para sistemas TI?
3. Lee la página de Wikipedia https://es.wikipedia.org/wiki/Free_Software_Foundation sobre la *Free Software Foundation*, organización que promueve el software libre, para contestar posteriormente a estas cuestiones:
 - a) ¿Qué es el proyecto GNU?
 - b) ¿Qué es el *Free Software Directory*?
 - c) ¿Quién es el presidente de la FSF y del proyecto GNU?

CUADERNO DE ACTIVIDADES

Actividades TIC

- Incrementa tus conocimientos de seguridad visualizando el vídeo <https://www.youtube.com/watch?v=gFuTGQUPfdE> (2m 38s) que proporciona información sobre los principales problemas de seguridad en el uso de redes sociales y cómo evitarlos. Posteriormente construye un mapa conceptual sencillo sobre el contenido del vídeo (un resumen/esquema).
- En el vídeo <http://www.youtube.com/watch?v=86cr-EfBz1o> (6m, 04s) tienes un documental sobre seguridad en Internet. Visualiza el vídeo y con la información que registra confecciona una pequeña guía de navegación segura para los usuarios.
- La importancia de tener actualizado un antivirus es fundamental. En el vídeo <http://www.youtube.com/watch?v=natrpUAZmKY> (4m, 42s) tienes una comparativa de algunos antivirus en sus versiones gratuitas. Visualiza el vídeo, descarga algunos de los antivirus que aparecen en el vídeo y realiza una instalación en el entorno de laboratorio.

UD06 – Resolución de incidencias de una red de área local

3-4

CUADERNO DE ACTIVIDADES

Ampliación de Actividades TIC

- Wireshark es uno de los analizadores de tráfico de red más difundidos. Conéctate a Youtube y en el vídeo <http://www.youtube.com/watch?v=O1JMQfbHFal> (8m, 41s) dispones de un videotutorial sobre esta magnífica herramienta. Posteriormente, en tu entorno doméstico podrás instalar Wireshark en tu equipo y probar a realizar algunas capturas de tráfico en la red siguiendo las indicaciones del vídeo visualizado.
Con esta herramienta no solamente se pueden visualizar los protocolos que se están utilizando con fines educativos, sino que, además, puede ser mal-utilizada para obtener aquellas páginas que se están utilizando sin ningún tipo de cifrado y capturar desde ahí una cuenta de usuario y contraseña, lo que nos tiene que hacer reflexionar sobre la importancia de mantener las redes seguras.

Wireshark es un programa analizador de protocolos de red o sniffer, que le permite capturar y navegar de forma interactiva por los contenidos de los paquetes capturados en la red. El objetivo del proyecto fue crear un analizador de calidad comercial para Unix. Funciona muy bien en Linux y Windows (con una interfaz gráfica de usuario), fácil de utilizar y puede reconstruir flujos TCP/IP y VoIP!

[Clic aquí para descargar la versión de Linux](#)

[Clic aquí para descargar la versión de Windows](#)

- Sobre la plataforma Youtube podrás encontrar el vídeo <http://www.youtube.com/watch?v=XyKGI29Xh0> (4m, 47s) que contiene un videotutorial sobre la tecnología Wake on LAN que describe cómo se pueden arrancar los ordenadores remotamente a través de la red. El vídeo continúa con este otro: <http://www.youtube.com/watch?v=Ymuw3GdPdVo> (9m, 07s). Si dispones del hardware suficiente en tu ordenador personal, puedes intentar crear una configuración en la que despiertes a un sistema desde otro.

UD06 – Resolución de incidencias de una red de área local

4-4

8.6.3 Cuaderno de prácticas

<p>UD06: Resolución de incidencias en una red de área local</p> <p style="text-align: right;">PRÁCTICAS</p> <hr/> <div style="text-align: center; background-color: #cccccc; padding: 5px; font-weight: bold; font-size: 1.2em;">PRÁCTICA 1</div> <div style="text-align: center; font-weight: bold; color: #0070c0; font-size: 1.1em;">Uso de Wireshark</div> <p>TOPOLOGÍA</p> <p>Destacaremos una captura de TCP de una sesión FTP. Esta topología consta de un PC con acceso a Internet.</p> <div style="display: flex; align-items: center; justify-content: center;"> </div> <p>OBJETIVO</p> <p>Identificar campos de encabezado y operación TCP mediante una captura de sesión FTP de Wireshark.</p> <p>EXPLICACIÓN TEÓRICA</p> <p>Dos de los protocolos de la capa de transporte de TCP/IP son TCP (definido en RFC 761) y UDP (definido en RFC 768). Los dos protocolos admiten la comunicación de protocolos de capa superior. Por ejemplo, TCP se utiliza para proporcionar soporte de capa de transporte para el protocolo de transferencia de hipertexto (HTTP) y FTP, entre otros. UDP proporciona soporte de capa de transporte para el sistema de nombres de dominio (DNS) y TFTP, entre otros.</p> <p>Nota: <i>Comprender las partes de los encabezados y de la operación de TCP y UDP es una habilidad fundamental para los ingenieros de red.</i></p> <p>En esta práctica de laboratorio, vamos a utilizar la herramienta de código abierto Wireshark para capturar y analizar campos de encabezado del protocolo TCP para las transferencias de archivos FTP entre el equipo host y un servidor FTP anónimo.</p> <p>Para conectarnos a un servidor FTP anónimo y descargar un archivo, se emplea la utilidad de línea de comandos de Windows.</p> <p>Se puede descargar Wireshark desde el siguiente enlace: http://www.wireshark.org/download.html</p> <p>RECURSOS NECESARIOS</p> <p>1 PC, acceso a Internet y Wireshark instalado</p> <p style="text-align: right; font-size: 0.8em;">Página 1 de 9</p>	<p>UD06: Resolución de incidencias en una red de área local</p> <p style="text-align: right;">PRÁCTICAS</p> <hr/> <div style="text-align: center; font-weight: bold; color: #0070c0; font-size: 1.1em;">Identificar campos de encabezado y operación TCP mediante una captura de sesión FTP de Wireshark</div> <p>Vamos a utilizar Wireshark para capturar una sesión FTP e inspeccionar los campos de encabezado de TCP.</p> <p>Paso 1: Inicia una captura de Wireshark, siguiendo estos pasos:</p> <ol style="list-style-type: none"> Cierra todo el tráfico de red innecesario, como el navegador web, para limitar la cantidad de tráfico durante la captura de Wireshark. Inicia la captura de Wireshark. <div style="text-align: center;"> </div> <p>Paso 2: Descargar el archivo Léame:</p> <ol style="list-style-type: none"> En el símbolo del sistema, introduce <code>ftp ftp.cdc.gov</code>. Conéctate al sitio FTP de los <i>Centros para el Control y la Prevención de Enfermedades (CDC)</i> con el usuario <code>anonymous</code> y sin contraseña. <pre style="background-color: black; color: white; padding: 5px; font-family: monospace; font-size: 0.9em;"> C:\Users\user1>ftp ftp.cdc.gov Connected to ftp.cdc.gov. 220 Microsoft FTP Service User (ftp.cdc.gov:(none)): anonymous 331 Anonymous access allowed, send identity (e-mail name) as password. Password: 230 Anonymous user logged in. </pre> <ol style="list-style-type: none"> Localiza y descarga el archivo Léame usando el comando <code>ls</code> para mostrar los archivos. <pre style="background-color: black; color: white; padding: 5px; font-family: monospace; font-size: 0.9em;"> [ftp] ls 200 PORT command successful. 150 Opening ASCII mode data connection for file list. lsnet_client pub Readme SiteInfo up.htm w3c web.config welcome.nsg 226 Transfer complete. ftp: 76 bytes received in 0.00Seconds 19.00Kbytes/sec. </pre> <ol style="list-style-type: none"> Introduce el comando <code>get Readme</code> para descargar el archivo. Cuando finalices la descarga, introduce el comando <code>quit</code> para salir. <pre style="background-color: black; color: white; padding: 5px; font-family: monospace; font-size: 0.9em;"> [ftp] get Readme 200 PORT command successful. 150 Opening ASCII mode data connection for Readme(1428 bytes). 226 Transfer complete. ftp: 1428 bytes received in 0.01Seconds 204.00Kbytes/sec. [ftp] quit 221 </pre> <p style="text-align: right; font-size: 0.8em;">Página 2 de 9</p>
---	--

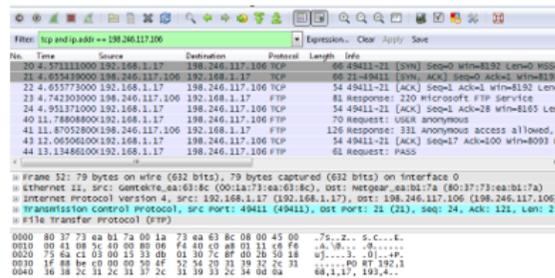
UD06: Resolución de incidencias en una red de área local

PRÁCTICAS

Paso 3: Para la captura Wireshark (pulsando el cuadrado rojo de la barra de herramientas rápida).

Paso 4: Vamos a visualizar ahora la ventana principal de Wireshark.

Wireshark capturó muchos paquetes durante la sesión FTP para ftp.cdc.gov. Para limitar la cantidad de datos para el análisis, escribe tcp and ip.addr == 198.246.117.106 en el área de entrada Filter: (Filtrar) y haz clic en Apply (Aplicar). La dirección IP, 198.246.117.106 es la dirección para ftp.cdc.gov en este momento.



Paso 5: Vamos a analizar los campos TCP.

Una vez aplicado el filtro TCP, las primeras tres tramas en el panel de la lista de paquetes (sección superior) muestran el protocolo de la capa de transporte TCP que crea una sesión confiable. La secuencia de [SYN], [SYN, ACK] y [ACK] ilustra el protocolo de enlace de tres vías.

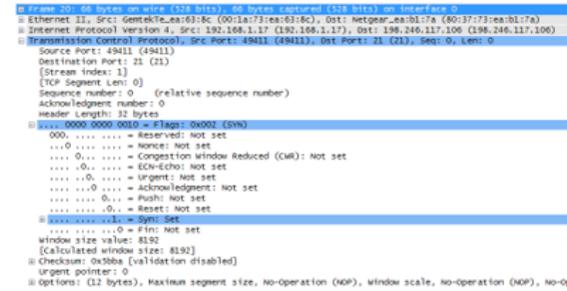


TCP se utiliza en forma continua durante una sesión para controlar la entrega de datagramas, verificar la llegada de datagramas y administrar el tamaño de la ventana. Para cada intercambio de datos entre el cliente FTP y el servidor FTP, se inicia una nueva sesión TCP. Al término de la transferencia de datos, se cierra la sesión TCP. Cuando finaliza la sesión FTP, TCP realiza un cierre y un apagado ordenados.

En Wireshark, se encuentra disponible información detallada sobre TCP en el panel de detalles del paquete (sección media). Resalta el primer datagrama TCP del equipo host clicando sobre esa línea y expande el datagrama TCP. El datagrama TCP expandido se muestra de manera similar al panel de detalles de paquetes que se muestra a continuación.

UD06: Resolución de incidencias en una red de área local

PRÁCTICAS



La imagen anterior es un diagrama del datagrama TCP. Se proporciona una explicación de cada campo para referencia:

- El número de puerto de origen TCP pertenece al host de la sesión TCP que abrió una conexión. Generalmente el valor es un valor aleatorio superior a 1.023.
- El número de puerto de destino TCP se utiliza para identificar el protocolo o la aplicación de capa superior en el sitio remoto. Los valores en el intervalo de 0 a 1023 representan los "puertos bien conocidos" y están asociados a servicios y aplicaciones populares (como se describe en la RFC 1700), por ejemplo, Telnet, FTP y HTTP. La combinación de la dirección IP de origen, el puerto de origen, la dirección IP de destino y el puerto de destino identifica de manera exclusiva la sesión para el remitente y para el destinatario.

Nota: En la siguiente captura de Wireshark, el puerto de destino es 21, que es FTP. Los servidores FTP escuchan las conexiones de cliente FTP en el puerto 21.

- Sequence number (Número de secuencia) especifica el número del último octeto en un segmento.

UD06: Resolución de incidencias en una red de área local **PRÁCTICAS**

- **Acknowledgment number** (Número de reconocimiento) especifica el siguiente octeto que espera el destinatario.
- **Code bits** (bits de código) tiene un significado especial en la administración de sesiones y en el tratamiento de los segmentos. Entre los valores interesantes se encuentran:
 - ACK: reconocimiento de la recepción de un segmento.
 - SYN: sincronizar, solo se configura cuando se negocia una nueva sesión TCP durante el protocolo de enlace de tres vías TCP.
 - FIN: finalizar, la solicitud para cerrar la sesión TCP.
- **Window size** (Tamaño de la ventana) es el valor de la ventana deslizante. Determina cuántos octetos pueden enviarse antes de esperar un reconocimiento.
- **Urgent pointer** (Puntero urgente) solo se utiliza con un marcador urgente (URG) cuando el remitente necesita enviar datos urgentes al destinatario.
- En **Options** (Opciones), hay una sola opción actualmente, y se define como el tamaño máximo del segmento TCP (valor opcional).

Utiliza la captura Wireshark del inicio de la primera sesión TCP (bit SYN fijado en 1) para **completar la información acerca del encabezado TCP**.

De la PC al servidor CDC (solo el bit de SYN está configurado en 1):

Dirección IP de origen	
Dirección IP de destino	
Número de puerto de origen	
Número de puerto de destino	
Número de secuencia	
Número de reconocimiento	
Longitud del encabezado	
Tamaño de la ventana	

En la segunda captura filtrada de Wireshark, el servidor FTP de CDC reconoce la solicitud de la PC. Observe los valores de los bits de SYN y ACK.

Página 6 de 8

UD06: Resolución de incidencias en una red de área local **PRÁCTICAS**

```

# Frame 21: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
# Ethernet II, Src: Netgear_ea:0b:7a:80:37:73,ea:0b:7a, Dst: Gsmakta_ea:63:8c:00:1a:73,ea:63:8c
# Internet Protocol Version 4, Src: 198.246.117.106 (198.246.117.106), Dst: 192.168.1.17 (192.168.1.17)
# Transmission Control Protocol, Src Port: 21 (21), Dst Port: 49411 (49411), Seq: 0, Ack: 1, Len: 0
  Source Port: 21 (21)
  Destination Port: 49411 (49411)
  [Stream Index: 1]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  Header length: 32 bytes
  00000000:00000010 = Flags: SYN, ACK
  00000000:00000000 = Reserved: not set
  ...0 .... = Nonce: not set
  ....0 .... = Congestion window reduced (cwr): not set
  ....0 .... = ECN-echo: not set
  ....0 .... = Urgent: not set
  00000000:00000000 = Window: not set
  ....0 .... = Push: not set
  ....0 .... = Reset: not set
  00000000:00000000 = SYN: set
  ....0 .... = FIN: not set
  window size value: 65535
  [calculated window size: 65535]
  checksum: 0x0000 (validation disabled)
  urgent pointer: 0
  options: (12 bytes), Maximum segment size, No-operation (nop), window scale, No-operation (nop), no
  [Seq/Ack analysis]
    
```

Completa la siguiente información sobre el mensaje de SYN-ACK.

Dirección IP de origen	
Dirección IP de destino	
Número de puerto de origen	
Número de puerto de destino	
Número de secuencia	
Número de reconocimiento	
Longitud del encabezado	
Tamaño de la ventana	

En la etapa final de la negociación para establecer las comunicaciones, la PC envía un mensaje de reconocimiento al servidor. Observa que solo el bit ACK está establecido en 1, y el número de secuencia se incrementó a 1.

Página 8 de 8

UD06: Resolución de incidencias en una red de área local

PRÁCTICAS

```

Frame 22: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: GensetkTe_ea:63:8c:00:1a:73:ea:63:8c, Dst: Netgear_ea:b1:7a:80:37:73:ea:b1:7a
Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 198.246.117.106 (198.246.117.106)
Transmission Control Protocol, Src Port: 49411 (49411), Dst Port: 21 (21), Seq: 1, Ack: 1, Len: 0
Source Port: 49411 (49411)
Destination Port: 21 (21)
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
header length: 20 bytes
0000 0000 0001 0000 = Flags: 0x010 (ACK)
000. .... = Reserved: NOT set
...0 .... = Nonce: NOT set
.... 0.... = Congestion window Reduced (CWR): not set
.... .0.. = ECN-Echo: NOT set
.... ..0. = Urgent: NOT set
..... 0... = Push: NOT set
.... .... = Reset: NOT set
.... .... = SYN: NOT set
..... ..0. = FIN: NOT set
window size value: 8192
[calculated window size: 8192]
[window size scaling factor: 1]
Checksum: 0x6ffa [validation disabled]
urgent pointer: 0
[Seq/Ack analysis]
    
```

Complete la siguiente información sobre el mensaje de ACK.

Dirección IP de origen	
Dirección IP de destino	
Número de puerto de origen	
Número de puerto de destino	
Número de secuencia	
Número de reconocimiento	
Longitud del encabezado	
Tamaño de la ventana	

Una vez establecida una sesión TCP, puede haber tráfico FTP entre la PC y el servidor FTP. El cliente y el servidor FTP se comunican entre ellos, sin saber que TCP controla y administra la sesión. Cuando el servidor FTP envía el mensaje **Response: 220** (Respuesta:220) al cliente FTP, la sesión TCP en el cliente FTP envía un reconocimiento a la sesión TCP en el servidor. Esta secuencia es visible en la siguiente captura de Wireshark.

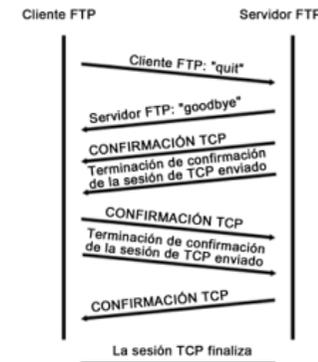
```

21 4.742101000 198.246.117.106 192.168.1.17 FTP 81 Response: 220 Microsoft FTP Service
24 4.931371000 192.168.1.17 198.246.117.106 TCP 54 49411->21 [ACK] Seq=1 ACK=28 Win=8165 Len=0
40 11.78808000 192.168.1.17 198.246.117.106 FTP 70 Request: USER anonymous
41 11.87952800 198.246.117.106 192.168.1.17 FTP 126 Response: 331 Anonymous access allowed, send
41 11.87952800 198.246.117.106 192.168.1.17 FTP 126 Response: 331 Anonymous access allowed, send
    
```

UD06: Resolución de incidencias en una red de área local

PRÁCTICAS

Cuando termina la sesión FTP, el cliente FTP envía un comando para "salir". El servidor FTP reconoce la terminación de FTP con un mensaje **Response: 221 Goodbye** (Adiós). En este momento, la sesión TCP del servidor FTP envía un datagrama TCP al cliente FTP que anuncia la terminación de la sesión TCP. La sesión TCP del cliente FTP reconoce la recepción del datagrama de terminación y luego envía su propia terminación de sesión TCP. Cuando quien originó la terminación TCP (servidor FTP) recibe una terminación duplicada, se envía un datagrama ACK para reconocer la terminación y se cierra la sesión TCP. Esta secuencia es visible en la captura y el diagrama siguientes.



Si se aplica un filtro **ftp**, puede examinarse la secuencia completa del tráfico FTP en Wireshark. Observe la secuencia de los eventos durante esta sesión FTP. Para recuperar el archivo **Léame**, se utilizó el nombre de usuario **anonymous** (anónimo). Una vez que se completó la transferencia de archivos, el usuario finalizó la sesión FTP.

```

Filter: ftp
No. Time Source Destination Protocol Length Info
182 4.742101000 198.246.117.106 192.168.1.17 FTP 81 Response: 220 Microsoft FTP Service
40 11.78808000 192.168.1.17 198.246.117.106 FTP 70 Request: USER anonymous
41 11.87952800 198.246.117.106 192.168.1.17 FTP 126 Response: 331 Anonymous access allowed, send
51 16.33224000 192.168.1.17 198.246.117.106 FTP 79 Request: PORT 192.168.1.17,191.4
52 16.41008000 198.246.117.106 192.168.1.17 FTP 5 [RETRANSMISSION] response: 200 PORT OK
53 17.36344200 192.168.1.17 198.246.117.106 FTP 60 Request: NLST
56 17.44303200 198.246.117.106 192.168.1.17 FTP 93 Response: 150 opening ASCII mode data conn
62 19.89744100 198.246.117.106 192.168.1.17 FTP 78 Response: 226 Transfer complete.
73 24.29718100 192.168.1.17 198.246.117.106 FTP 79 Request: PORT 192.168.1.17,191.5
74 24.30849000 198.246.117.106 192.168.1.17 FTP 5 [RETRANSMISSION] response: 200 PORT OK
82 25.14328000 198.246.117.106 192.168.1.17 FTP 84 [RETRANSMISSION] response: 200 PORT OK
83 25.14328000 192.168.1.17 198.246.117.106 FTP 61 Request: RETR README
101 25.27518100 198.246.117.106 192.168.1.17 FTP 93 Response: 150 opening ASCII mode data conn
127 27.78452300 198.246.117.106 192.168.1.17 FTP 78 Response: 226 Transfer complete.
147 30.48390300 192.168.1.17 198.246.117.106 FTP 60 Request: QUIT
148 30.5611700 198.246.117.106 192.168.1.17 FTP 68 Response: 221 Goodbye.
    
```

UD06: Resolución de incidencias en una red de área local

PRÁCTICAS

Vuelve a aplicar el filtro TCP en Wireshark para examinar la terminación de la sesión TCP. Se transmiten cuatro paquetes para la terminación de la sesión TCP. Dado que la conexión TCP es de dúplex completo, cada dirección debe terminar independientemente. Examina las direcciones de origen y destino.

En este ejemplo, el servidor FTP no tiene más datos para enviar en la secuencia. Envía un segmento con el marcador FIN configurado en la trama 149. La PC envía un mensaje ACK para reconocer la recepción del mensaje FIN para terminar la sesión del servidor al cliente en la trama 150.

En la trama 151, la PC envía un mensaje FIN al servidor FTP para terminar la sesión TCP. El servidor FTP responde con un mensaje ACK para reconocer el mensaje FIN de la PC en la trama 152. Ahora, la sesión TCP terminó entre el servidor FTP y la PC.

```

147 30.48299200192.168.1.17 198.246.117.106 FTP 60 Request: QUIT
148 30.56511700198.246.117.106 192.168.1.17 FTP 68 Response: 221 Goodbye.
149 30.56677000192.168.1.17 198.246.117.106 TCP 54 49411->21 [ACK] Seq=89 Ack=326 win=7668 L
150 30.56879900192.168.1.17 198.246.117.106 TCP 54 49411->21 [FIN, ACK] Seq=89 Ack=326 win=0
151 30.66777000198.246.117.106 192.168.1.17 TCP 54 21->49411 [ACK] Seq=326 Ack=100 win=132099
152 30.66777000198.246.117.106 192.168.1.17 TCP 54 21->49411 [ACK] Seq=326 Ack=100 win=132099

```

* Frame 149: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 * Ethernet II, Src: Netgear_ea:bb:17:a (80:37:73:ea:bb:17:a), Dst: Gasteke_ea:63:8c (00:1a:73:ea:63:8c)
 * Internet Protocol Version 4, Src: 198.246.117.106 (198.246.117.106), Dst: 192.168.1.17 (192.168.1.17)
 * Transmission Control Protocol, Src Port: 21 (21), Dst Port: 49411 (49411), Seq: 326, Ack: 100, Len: 54

Conclusión

Dado que ni FTP ni TFTP son protocolos seguros, todos los datos transferidos se envían en texto no cifrado. Esto incluye cualquier ID de usuario, contraseña o contenido de archivos de texto no cifrado. Si analizas la sesión FTP de capa superior identificarás rápidamente el ID de usuario, la contraseña y las contraseñas de archivo de configuración.

PRÁCTICA 2

Configuración de contraseñas seguras y SSH

Topología

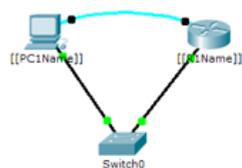


Tabla de direccionamiento

El administrador	Interfaces	IP Address (Dirección IP)	Subnet Mask (Máscara de subred)	Gateway predeterminado
[[R1Name]]	G0/0	[[R1Add]]	255.255.255.0	N/A
[[PC1Name]]	NIC	[[PC1Add]]	255.255.255.0	[[R1Add]]

Situación

El administrador de red le solicitó que prepare [[R1Name]] para la implementación. Antes de que pueda conectarse a la red, se deben habilitar las medidas de seguridad.

Requisitos

- Configure el direccionamiento IP en [[R1Name]] según la tabla de direccionamiento.
- Acceda al [[R1Name]] mediante el puerto de consola desde el terminal en PC-A.
- Configure el direccionamiento IP en [[R1Name]] y habilite la interfaz.
- Configure el nombre del host como [[R1Name]].
- Cifre todas las contraseñas de texto.
- [[R1Name]](config)# service password-encryption
- Establezca la contraseña secreta segura que desee.
- Establezca el nombre de dominio en [[R1Name]] (distinguir mayúsculas de minúsculas para la puntuación de PT).
- [[R1Name]](config)# ip domain-name [[R1Name]].com
- Cree un usuario de su elección con una contraseña segura.
- [[R1Name]](config)# username any_user password any_password
- Genere claves RSA de 1024 bits.

Nota: en Packet Tracer, introduzca el comando `crypto key generate rsa` y presione la tecla Intro para continuar.

```
[[R1Name]](config)# crypto key generate rsa
```

```
The name for the keys will be: [[R1Name]].[[R1Name]].com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

- Bloquee durante tres minutos a cualquier persona que no pueda iniciar sesión después de cuatro intentos en un periodo de dos minutos.
- [[R1Name]](config)# login block-for 180 attempts 4 within 120
- Configure las líneas VTY para el acceso por SSH y solicite los perfiles de usuarios locales para la autenticación.
- [[R1Name]](config)# line vty 0 4
- [[R1Name]](config-line)# transport input ssh
- [[R1Name]](config-line)# login local
- Guarda la configuración en la NVRAM.
- Esté preparado para demostrar al instructor que estableció el acceso por SSH de [[PC1Name]] a [[R1Name]].

```
ID de Isomorph: [[indexNames]][[indexAdd]]
```

PRÁCTICA 3

Herramientas de administración de redes

Topología



Tabla de direccionamiento

El administrador	Interfaces	IP Address (Dirección IP)	Subnet Mask (Máscara de subred)	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/D
	Lo0	209.165.200.225	255.255.255.224	N/D
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

- Parte 1: Establecer la topología e inicializar los dispositivos
- Parte 2: configurar los dispositivos y verificar la conectividad
- Parte 3: Recopilar información sobre los dispositivos de red

Aspectos básicos/situación

La documentación de una red en funcionamiento es una de las tareas más importantes que puede realizar un profesional de red. Tener la documentación correspondiente de las direcciones IP, los números de modelo, las versiones del IOS y los puertos utilizados, así como probar la seguridad, puede resultar muy útil para resolver los problemas de una red.

En esta práctica de laboratorio, armará una red pequeña, configurará los dispositivos, implementará seguridad básica y documentará las configuraciones mediante la emisión de diversos comandos en el router, el switch y la PC para recopilar la información.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 1 routers (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 1 PC (Windows 7 u 8 con un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1: establecer la topología e inicializar los dispositivos

En la parte 1, establecerá la topología de la red, borrará cualquier configuración, de ser necesario, y configurará los parámetros básicos del router y el switch.

Paso 1: Realice el cableado de red tal como se muestra en la topología.

- a. Conecte los dispositivos tal como se muestra en la topología y realice el cableado según sea necesario.
- b. Encienda todos los dispositivos de la topología.

Paso 2: inicializar y volver a cargar el router y el switch.

Parte 2: Configurar dispositivos y verificar la conectividad

En la parte 2, establecerá la topología de la red y configurará los parámetros básicos del router y el switch. Consulte la topología y la tabla de direccionamiento que se encuentran al principio de esta práctica de laboratorio para obtener información sobre nombres de dispositivos y direcciones.

Paso 1: Configurar la dirección IPv4 para la PC

Configure la dirección IPv4, la máscara de subred y la dirección de gateway predeterminado para la PC-A según la tabla de direccionamiento.

Paso 2: Configurar el router.

- a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.
- b. Configure la hora correcta en el router.
- c. Ingrese al modo de configuración global.
 - 1) Asigne un nombre de dispositivo al router según la topología y la tabla de direccionamiento.
 - 2) Desactive la búsqueda del DNS.
 - 3) Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
 - 4) Asigne class como la contraseña cifrada del modo EXEC privilegiado.
 - 5) Asigne cisco como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.

UD06: Resolución de incidencias de una red de área local **PRÁCTICAS**

- 6) Cifre las contraseñas de texto no cifrado.
- 7) Cree un nombre de dominio `cisco.com` para el acceso por SSH.
- 8) Cree un usuario denominado `admin` con la contraseña secreta `cisco` para el acceso por SSH.
- 9) Genere una clave de módulo RSA. Use `1024` para la cantidad de bits.
- d. Configure el acceso a las líneas VTY.
 - 1) Use la base de datos local para la autenticación de SSH.
 - 2) Habilite SSH solo para el acceso de inicio de sesión.
- e. Vuelva al modo de configuración global.
 - 1) Cree la interfaz Loopback 0 y asigne la dirección IP según la tabla de direccionamiento.
 - 2) Configure y habilite la interfaz G0/1 en el router.
 - 3) Configure las descripciones de interfaz para G0/1 y L0.
 - 4) Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.

Paso 3: Configure el switch.

- a. Acceda al switch mediante el puerto de consola e ingrese al modo EXEC privilegiado.
- b. Configure la hora correcta en el switch.
- c. Ingrese al modo de configuración global.
 - 1) Asigne un nombre de dispositivo al switch según la topología y la tabla de direccionamiento.
 - 2) Desactive la búsqueda del DNS.
 - 3) Cree un mensaje MOTD que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
 - 4) Asigne `class` como la contraseña cifrada del modo EXEC privilegiado.
 - 5) Cifre las contraseñas de texto no cifrado.
 - 6) Cree un nombre de dominio `cisco.com` para el acceso por SSH.
 - 7) Cree un usuario denominado `admin` con la contraseña secreta `cisco` para el acceso por SSH.
 - 8) Genere una clave RSA. Use `1024` para la cantidad de bits.
 - 9) Cree y active una dirección IP en el switch según la topología y la tabla de direccionamiento.
 - 10) Configure el gateway predeterminado en el switch.
 - 11) Asigne `cisco` como la contraseña de consola y habilite el acceso de inicio de sesión a la consola.
- d. Configure el acceso a las líneas VTY.
 - 1) Use la base de datos local para la autenticación de SSH.
 - 2) Habilite SSH solo para el acceso de inicio de sesión.
 - 3) Guarde el archivo de configuración en ejecución en el archivo de configuración de inicio.
- e. Ingrese al modo correspondiente para configurar las descripciones de interfaz de F0/5 y F0/6.

Paso 4: Verificar la conectividad de la red

- a. Desde el símbolo del sistema en la PC-A, haga ping a la dirección IP de la VLAN 1 del S1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.
- b. En el símbolo del sistema de la PC-A, haga ping a la dirección IP del gateway predeterminado en el R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.

UD06: Resolución de incidencias de una red de área local **PRÁCTICAS**

- c. En el símbolo del sistema de la PC-A, haga ping a la interfaz loopback en R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.
- d. Vuelva a acceder al switch mediante la consola y haga ping a la dirección IP de G0/1 en el R1. Si los pings no se realizaron correctamente, resuelva los problemas de configuración física y lógica.

Parte 3: Recopilar información sobre los dispositivos de red

En la parte 3, utilizará una variedad de comandos para recopilar información sobre los dispositivos en la red, así como algunas características de rendimiento. La documentación de la red es un componente muy importante de la administración de una red. La documentación de la topología física y lógica es importante, al igual que la verificación de los modelos de plataforma y las versiones del IOS de los dispositivos de red. Tener conocimientos de los comandos adecuados para recopilar esta información es fundamental para los profesionales de red.

Paso 1: Recopilar información sobre el R1 mediante los comandos del IOS.

Uno de los pasos más básicos consiste en recopilar información sobre el dispositivo físico, así como la información del sistema operativo.

- a. Emita el comando adecuado para obtener la siguiente información:

Modelo de router: _____

Versión del IOS: _____

RAM total: _____

NVRAM total: _____

Memoria flash total: _____

Archivo de imagen de IOS: _____

Registro de configuración: _____

Paquete de tecnología: _____

UD06: Resolución de incidencias de una red de área local

PRÁCTICAS

- ¿Está cifrada la contraseña de consola? _____
 ¿Está cifrada la contraseña de SSH? _____

Paso 2: Recopilar información sobre el S1 mediante los comandos del IOS.

Muchos de los comandos que usó en R1 se pueden utilizar con el switch. Sin embargo, existen algunas diferencias con algunos de los comandos.

- a. Emita el comando **show versión** para obtener la siguiente información:

Modelo de switch: _____

Versión del IOS: _____

NVRAM total: _____

Archivo de imagen de IOS: _____

¿Qué comando emitió para recopilar la información?

- b. Emita el comando **show ip interface brief** para mostrar un resumen de la información de estado sobre las interfaces del switch. Registre sus resultados a continuación.

Nota: registre solo las interfaces activas.

- c. Emita el comando **show mac address-table** para mostrar la tabla de direcciones MAC del switch. Registre solo las direcciones MAC dinámicas en el siguiente espacio.

- d. Verifique que el acceso a VTY por Telnet esté deshabilitado en el S1. Con un cliente Telnet, como Tera Term o PuTTY, intente acceder al S1 mediante Telnet con la dirección 192.168.1.11. Registre sus resultados a continuación.

- e. En la PC-A, realice pruebas para asegurar que SSH funcione correctamente. Con un cliente SSH, como Tera Term o PuTTY, acceda al S1 mediante SSH desde la PC-A. Si aparece un mensaje de

UD06: Resolución de incidencias de una red de área local

PRÁCTICAS

advertencia en relación con una clave diferente, haga clic en **Continue** (Continuar). Inicie sesión con un nombre de usuario y una contraseña adecuados. ¿Tuvo éxito?

- f. Complete la siguiente tabla con información sobre el router R1 utilizando los comandos adecuados en el S1.

Id. del dispositivo	Interfaz local	Capacidad	N.º de modelo	ID del puerto remoto	IP Address (Dirección IP)	Versión del IOS
---------------------	----------------	-----------	---------------	----------------------	---------------------------	-----------------

- g. Verifique que todas las contraseñas en el archivo de configuración estén cifradas, con **show running-config (show run)**. Escriba el comando y registre sus resultados a continuación.

¿Está cifrada la contraseña de consola? _____

Paso 3: Recopilar información sobre la PC-A.

Mediante diversos comandos de utilidades de Windows, recopilará información sobre la PC-A.

- a. En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all** y registre sus respuestas a continuación.

¿Cuál es la dirección IP de la PC-A?

¿Cuál es la máscara de subred de la PC-A?

¿Cuál es la dirección de gateway predeterminado de la PC-A?

¿Cuál es la dirección MAC de la PC-A?

- b. Emita el comando **ping** para probar el stack de protocolos TCP/IP con la NIC. ¿Qué comando utilizó?

UD06: Resolución de incidencias de una red de área local

PRÁCTICAS

c. Haga ping a la interfaz loopback del R1 desde el símbolo del sistema de la PC-A. ¿El ping se realizó correctamente?

d. Emita el comando `tracert` en la PC-A para rastrear la lista de saltos de router para los paquetes provenientes de la PC-A a la interfaz loopback en R1. Registre el comando y el resultado a continuación.

e. Emita el comando `arp -a` en la PC-A para buscar las asignaciones de direcciones de capa 2 y capa 3 que se realizaron en la NIC. Registre sus respuestas a continuación. Registre solo las respuestas para la red 192.168.1.0/24.

Reflexión

¿Por qué es importante registrar los dispositivos de red?

8.6.4 Trabajo de investigación

<p>UNIDAD 6 – TRABAJO DE INVESTIGACIÓN</p> <hr/> <p><i>UNIDAD 6. RESOLUCIÓN DE INCIDENCIAS DE UNA RED DE ÁREA LOCAL</i></p> <p>Investigación de amenazas de seguridad de red</p> <p>Objetivos</p> <p>Parte 1: Explorar el sitio web de SANS Parte 2: Identificar amenazas de seguridad de la red recientes Parte 3: Describir con detalle una amenaza específica de seguridad de la red</p> <p>Descripción</p> <p>Para defender una red contra ataques, el administrador debe identificar las amenazas externas que representan un peligro para la red. Pueden usarse sitios web de seguridad para identificar amenazas emergentes y para proporcionar opciones de mitigación para defender una red.</p> <p>Uno de los sitios más populares y confiables para la defensa contra amenazas de seguridad informática y de redes es el de SysAdministration, Audit, Networking and Security (SANS). El sitio de SANS proporciona varios recursos, como una lista de los 20 principales controles de seguridad fundamentales para una defensa cibernética eficaz y el boletín informativo semanal " @Risk: The Consensus Security Alert". Este boletín detalla nuevos ataques y vulnerabilidades de red.</p> <p>En esta práctica de laboratorio, navegará hasta el sitio de SANS, lo explorará y lo utilizará para identificar amenazas de seguridad de red recientes, investigará otros sitios web que identifican amenazas, e investigará y presentará detalles acerca de un ataque de red específico.</p> <p>Recursos necesarios</p> <ul style="list-style-type: none"> • Dispositivo con acceso a Internet • PC para la presentación con PowerPoint u otro software de presentación instalado <p>Criterios de calificación</p> <p>Se valorará:</p> <ul style="list-style-type: none"> ○ Presentación y pulcritud. ○ Corrección gramatical y ortográfica. ○ Uso de un lenguaje técnico adecuado. ○ En caso de usar imágenes, que éstas aporten información de utilidad. <p>Página 1 de 4</p>	<p>UNIDAD 6 – TRABAJO DE INVESTIGACIÓN</p> <hr/> <p>Desarrollo</p> <p>Parte 1: Explorar el sitio web de SANS</p> <p>En la parte 1, navegue hasta el sitio web de SANS y explore los recursos disponibles.</p> <p>Paso 1: Localizar los recursos de SANS.</p> <p>Vaya a www.SANS.org. En la página de inicio, resalte el menú Recursos (Recursos). Indique tres recursos disponibles.</p> <hr/> <hr/> <p>Página 2 de 4</p>
---	---

UNIDAD 6 – TRABAJO DE INVESTIGACIÓN

Paso 2: Localizar el recurso Top 20 Critical Controls.

El documento *Twenty Critical Security Controls for Effective Cyber Defense* (Los 20 controles de seguridad críticos para una defensa cibernética eficaz) que aparece en el sitio web de SANS es el resultado de una asociación de carácter público-privado entre el Departamento de Defensa de los EE. UU. (DoD, Department of Defense), la National Security Association, el Center for Internet Security (CIS) y el instituto SANS. La lista se desarrolló para establecer el orden de prioridades de los controles de ciberseguridad y los gastos para el DoD y se convirtió en la pieza central de programas de seguridad eficaces para el gobierno de los Estados Unidos. En el menú **Recursos**, seleccione **Top 20 Critical Controls** (Los principales 20 controles críticos).

Seleccione uno de los 20 controles críticos e indique tres de las sugerencias de implementación para ese control.

Paso 3: Localizar el menú Newsletter.

Resalte el menú **Resources** y seleccione **Newsletters** (Boletines informativos). Describa brevemente cada uno de los tres boletines disponibles.

Parte 2: Identificar amenazas de seguridad de red recientes

En la parte 2, investigará las amenazas de seguridad de red recientes mediante el sitio de SANS e identificará otros sitios que contienen información de amenazas de seguridad.

Paso 1: Localizar el archivo del boletín @Risk: Consensus Security Alert.

En la página **Newsletters**, seleccione **Archive** (Archivo) para acceder a **@RISK: The Consensus Security Alert**. Desplácese hacia abajo hasta **Archives Volumes** (Volumenes de archivo) y seleccione un boletín informativo semanal reciente. Revise las secciones **Notable Recent Security Issues and Most Popular Malware Files** (Problemas de seguridad recientes destacados y Archivos de malware más populares).

Enumere algunos de los ataques recientes. Explore varios boletines informativos recientes, si fuera necesario.

UNIDAD 6 – TRABAJO DE INVESTIGACIÓN

Paso 2: Identificar sitios que proporcionen información sobre amenazas de seguridad recientes.

Además del sitio de SANS, identifique otros sitios web que proporcionen información sobre amenazas de seguridad recientes.

Enumere algunas de las amenazas de seguridad recientes que se mencionan en estos sitios web.

Parte 3: Describir con detalle un ataque específico de seguridad de la red

En la parte 3, investigará un ataque de red específico que haya ocurrido y creará una presentación basada en sus conclusiones. Complete el formulario que se encuentra a continuación con sus conclusiones.

Paso 1: Complete el formulario a continuación según el ataque de red seleccionado.

Nombre del ataque:	
Tipo de ataque:	
Fecha de los ataques:	
Equipos/organizaciones afectadas:	
Cómo funciona y qué daños causó:	
Opciones de mitigación:	
Referencias y enlaces de información:	

8.7 Unidad didáctica 7

Esta unidad didáctica es la última del curso y en ella se pretende ahondar en la actualidad de las redes, centrandose siempre los contenidos desde el punto de vista de las redes de área local.

Se presentan las redes inalámbricas, de creciente aplicación en el mundo de las redes, especialmente en ámbitos locales, domésticos y empresariales. Con los conocimientos ya vistos en el recorrido del curso, ésta inmersión específicamente en inalámbricas debe resultar sencilla, puesto que ya se han ido realizando actividades prácticas donde se ha trabajado con esquemas mixtos, cableados e inalámbricos.

Se añade también, en esta última unidad didáctica, una exposición de las tecnologías más recientes relacionadas con las redes: Big data y Cloud computing, Internet de las cosas (IoT), inteligencia artificial añadida a las redes basadas en la intención, y una presentación del funcionamiento y configuración de las redes IP versión 6, que actualmente conviven con la versión 4. En cada uno de los puntos mencionados se plantea una actividad de resolución práctica.

8.7.1 Presentación teórica

CURSO
Redes de Área Local

UNIDAD 7
Redes mixtas integradas

Redes de Área Local
Olga Minguet
1

UD7. Redes mixtas integradas

ÍNDICE

-  INTRODUCCIÓN
-  REDES INALÁMBRICAS
-  BIG DATA & CLOUD COMPUTING
-  INTELIGENCIA ARTIFICIAL
-  REDES IPv6

Redes de Área Local
Olga Minguet
2

UD7. Redes mixtas integradas

1. INTRODUCCIÓN
La evolución de la transformación digital

En la actualidad hay más dispositivos inteligentes que personas.

Muchas personas están conectadas a Internet durante las 24 horas del día. Para 2025, cada consumidor poseerá 6,58 dispositivos inteligentes.

Las redes digitales modernas hacen que todo esto sea posible.



La transformación digital es la aplicación de la tecnología digital para proporcionar el entorno adecuado para la innovación de las empresas y la industria.

Redes de Área Local
Olga Minguet
3

UD7. Redes mixtas integradas

1. INTRODUCCIÓN
¿Cuál es tu generación digital?



Redes de Área Local
Olga Minguet
4

UD7. Redes mixtas integradas

1. INTRODUCCIÓN

¿Cuál es tu generación digital?

¿Qué cantidad promedio de tiempo estás habitualmente "conectado"?

¿Con cuántos dispositivos puedes estar conectados?

¿Crees que la edad es un motivo para estar más o menos "conectado"?

¿Crees que el género es un motivo para estar más o menos "conectado"?

¿Cómo crees que afecta esto a la forma de funcionar de las empresas?

Redes de Área Local Olga Minguet 5

UD7. Redes mixtas integradas

1. INTRODUCCIÓN

La digitalización transforma los negocios

La tecnología digital ha permitido que las empresas innoven su enfoque para interactuar con la sociedad. Personas de todas las generaciones se sienten más cómodas con la tecnología digital y utilizan dispositivos inteligentes para su beneficio en los días atareados.



Redes de Área Local Olga Minguet 6

UD7. Redes mixtas integradas

1. INTRODUCCIÓN

¿Los dispositivos inteligentes pueden pensar?

Si se programan de manera correcta, los dispositivos inteligentes pueden **evaluar** los datos que reciben, y modificar los procesos o la configuración "en el acto".



Si se les proporcionan los datos suficientes, pueden **"aprender"** y modificar sus propios códigos según los nuevos parámetros.

Las **llaves inteligentes** usan sensores para controlar muchos de sus sistemas de infraestructura, tales como el flujo de tráfico, el estacionamiento, la utilización del agua y el suministro hidrológico.

Los **automóviles** con piloto automático están equipados con muchos sensores de ultrasonido, cámaras, GPS de precisión y ordenadores.

Redes de Área Local Olga Minguet 7

UD7. Redes mixtas integradas

1. INTRODUCCIÓN

Las redes son la base de la conexión global

- 50 000 millones de objetos proporcionan billones de gigabytes de datos.
- Las redes proporcionan la base para Internet y el mundo digitalizado.
- Las redes pueden ir desde redes simples, compuestas por dos PC, hasta redes que conectan millones de dispositivos.
- Las redes pueden proporcionar productos y servicios a los clientes a través de su conexión a Internet.
- Internet es la red más grande que existe, y proporciona "la capa electrónica" que rodea al planeta de manera eficaz.



Redes de Área Local Olga Minguet 8

UD7. Redes mixtas integradas 

1. INTRODUCCIÓN

Tipos de redes

- **Red de área personal (PAN):** conectar tu smartphone a tu coche vía Bluetooth es un ejemplo de una PAN.
- **Red de área local (LAN):** redes que se encuentran en un área geográfica pequeña, tales como una vivienda a una empresa pequeña.
- **Red de área amplia (WAN):** un conjunto de LAN que brinda conexión entre LAN y con Internet.
- **Internet:** un sistema de redes globales multicapa que conecta a cientos de millones de computadoras.
- **Redes inalámbricas:** utilizan ondas electromagnéticas para transportar señales a través de la red.
- **La nube:** centros de datos o grupos de servidores conectados utilizados para almacenar y analizar datos, brindar acceso a aplicaciones en línea y ofrecer servicios de respaldo.



Redes de Área Local Olga Minguet 9

UD7. Redes mixtas integradas 

1. INTRODUCCIÓN

El futuro de las redes



- ✓ **La Inteligencia artificial (AI):** los dispositivos tienen la capacidad de "pensar" por su cuenta.
- ✓ **Redes basadas en la intención (IBN):** proporcionar software con reglas, pautas o intenciones, de modo que los datos pudieran modificar la red, las funciones de la infraestructura o las funciones de seguridad dentro de una red.

Ejemplo: una empresa define que un empleado contratado recibe acceso a solo un conjunto específico de datos y aplicaciones. Esta es la intención. En un sistema de IBN todos los dispositivos de red se configurarán automáticamente para cumplir con este requisito en toda la red, sin importar dónde esté conectado el empleado.

Redes de Área Local Olga Minguet 10

UD7. Redes mixtas integradas 

2. REDES INALÁMBRICAS

Redes de área local inalámbricas (WLAN) son redes locales que transmiten mediante ondas de radio y ofrece dos ventajas:

- No es necesario usar cableado.
- Admite la movilidad de los ordenadores de la red.

Por el contrario tiene inconvenientes, como que el ancho de banda es significativamente menor, y la seguridad, que si no se cuida puede verse seriamente comprometida.

Aunque las redes inalámbricas más extendidas actualmente siguen el estándar Wi-Fi, existen más redes inalámbricas, como, por ejemplo, las redes de infrarrojos y las de Bluetooth.

Redes de Área Local Olga Minguet 11

UD7. Redes mixtas integradas 

2. REDES INALÁMBRICAS

Wi-Fi: estándar IEEE 802.11

- Utiliza acceso múltiple con detección de portador/prevención de colisiones (CSMA/CA).
- La tarjeta NIC inalámbrica debe esperar hasta que el canal esté libre.

Bluetooth: estándar IEEE 802.15

- Red de área personal inalámbrica (WPAN).
- Utiliza un proceso de emparejamiento de dispositivos para distancias de 1 a 100 m.

WiMAX: estándar IEEE 802.16

- Interoperabilidad mundial para acceso por microondas.
- Acceso por banda ancha inalámbrico.



Redes de Área Local Olga Minguet 12

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

BLUETOOTH



- ✓ **Bluetooth** es un protocolo de comunicación inalámbrica entre dispositivos. Con él podemos conectar diferentes dispositivos con una radiofrecuencia segura en la banda ISM de los 2.4GHz, y a través de esta conexión se pueden transmitir voz y datos entre ellos sin necesidad de conexión cableada.
- ✓ Este protocolo permite conectar periféricos (como teclados y ratones), compartir archivos entre dispositivos (música, fotografías, vídeos, documentos, ...), permite sincronizar altavoces o auriculares, etc.
- ✓ Hoy en día podemos encontrar Bluetooth en todo tipo de dispositivos, desde ordenadores hasta smartphones, tabletas y portátiles. También ratones, teclados, impresoras, cámaras digitales, auriculares, televisores y todo tipo de receptores. Integrado en los propios dispositivos.

Bluetooth utiliza la banda de frecuencia de espectro ISM de 2.4 GHz (2400 a 2483.5 MHz). Además, la banda de 2.4 GHz está disponible en todo el mundo, por lo que es un estándar para la conectividad inalámbrica de baja potencia.

www.bluetooth.com

Redes de Área Local Olga Minguet 13

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

BLUETOOTH




- ✓ Uno de los grandes logros que consiguió el Bluetooth desde sus inicios es **no interferir en otros sistemas inalámbricos** que operan por radiofrecuencia. Para ello, esta tecnología envía señales débiles de menos de 1mW, limitando el rango de acción de los equipos a un máximo de determinados metros de distancia (según la versión o clase).
- ✓ De esta manera, los datos viajan de manera eficaz y sin ser interferidos por otras señales. Además, al contrario que las conexiones por infrarrojos **el Bluetooth no necesita estar en la línea de visión** de los equipos para realizar la comunicación. Eso quiere decir que los dispositivos que conectan no tienen que estar en la misma habitación, ya que la señal Bluetooth consigue atravesar paredes.

Redes de Área Local Olga Minguet 14

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

BLUETOOTH



El desarrollo de la tecnología de radio "short-link", que luego pasó a llamarse Bluetooth, fue iniciado en 1989 por Ericsson Mobile. Desde entonces, este protocolo ha ido evolucionando con diferentes versiones, cada una aportando diferentes novedades que mejoran la tecnología añadiendo más funcionalidades y posibilidades.

- **Clase 1:** Alcance hasta de 100m, lo que implica una potencia de 100mW, con un Ancho de Banda de hasta 1Mbps
- **Clase 2:** Alcance hasta de 20 m, lo que implica una potencia de 2.5mW, y un Ancho de Banda de hasta 3Mbps.
- **Clase 3:** Alcance hasta 1m, con una potencia de 1mW, y Ancho de Banda de hasta 24Mbps.
- **Clase 4:** Alcance hasta 0'5m, con una potencia de 0'5mW, y Ancho de Banda hasta 32Mbps.
- **Clase 5:** Alcance hasta 10m (sin repetidores) y Ancho de Banda hasta 50Mbps.

Redes de Área Local Olga Minguet 15

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

BLUETOOTH



Bluetooth 1.0. La primera versión utilizada para la transmisión que a día de hoy ya no se implementa. Al tratarse de la primera versión tuvo serios problemas para conectar dispositivos. Tuvo dos actualizaciones (1.1 y 1.2) que finalmente consiguieron colocar la Bluetooth como un estándar de comunicación IEEE. La tasa de transmisión era de 721 kbps aprox.

Bluetooth 2.0. Le sucedieron la versión 2.1 + EDR, la cual supuso un antes y un después en el campo de la conectividad inalámbrica debido a su versatilidad y potencia nunca vistas hasta su aparición. Permitted entre otras cosas que un terminal pudiera agregar a otro con Bluetooth y conectarse automáticamente. Con la versión 2.1 + EDR se alcanzan transferencias de hasta de 2 Mbps.

Bluetooth 3.0. Pese a que se mejoró mucho la velocidad respecto a la versión anterior esta es un "imposse" entre la última versión de 2.0 y la 4.0. Se incorporó el término *HS -High Speed-*, que permite transferir paquetes de información más largos como archivos de vídeo o formatos de audio de mayor calidad. Su tasa de transmisión alcanza los 24 Mbps.

Bluetooth 4.0. Posteriormente actualizada a 4.1 y 4.2. Aquí apareció la tecnología *Bluetooth Smart* y el *Bluetooth Low Energy (BLE)* destinado para dispositivos que funcionen con internet de las cosas (IoT). Y sobre todo mejoró en su consumo energético bastante más bajo que las versiones anteriores. En general Bluetooth 4.0 permite transferencias desde 25 Mbps hasta 32 Mbps.

Redes de Área Local Olga Minguet 16

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

BLUETOOTH



- ✓ El **Bluetooth 5.0** fue presentado en diciembre del 2016. A principios del 2019 se presentó la versión 5.1, seguida de la 5.2 a finales de año. Como es habitual en otros desarrollos, al no realizarse un cambio de unidad en la versión, nos indica que se trata más de una evolución de la versión anterior que de una versión más completa. Evoluciones en aspectos como la ubicación de otros dispositivos a los que estén conectados.
- ✓ Esta versión de Bluetooth admite potencias de transmisión del orden de 0.01mW, con rangos aproximados de alcance de 10m sin necesidad de repetidores (con repetidores hasta 100m), y Ancho de Banda de hasta 50Mbps.
- ✓ Esta última versión está enfocada especialmente a IoT, mejorando su versión anterior Bluetooth 4.

Redes de Área Local Olga Minguet 17

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

BLUETOOTH



En cuanto a la **topología**, Bluetooth crea un modelo de redes denominadas **piconets**, que deben cumplir las siguientes características:

1. **Todo enlace Bluetooth debe pertenecer a una piconet** que le une con un destino por medio de un canal físico compartido y sincronizado mediante un reloj común y una secuencia de saltos de frecuencia única para ese canal. Uno de los extremos de la comunicación hace de maestro y el otro de esclavo.
2. Es posible la **coexistencia de varios canales**, cada uno de los cuales tiene su propio maestro, reloj y secuencia de saltos.
3. Un **dispositivo maestro** solo puede serlo de una piconet, aunque un esclavo puede serlo de varias piconets simultáneamente.
4. Un dispositivo puede ser **maestro de una única piconet** a lo sumo, pero simultáneamente puede ser **esclavo de otra** u otras piconets distintas de las que él es maestro.

Redes de Área Local Olga Minguet 18

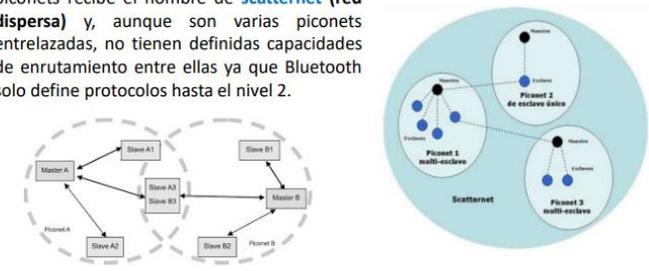
UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

BLUETOOTH



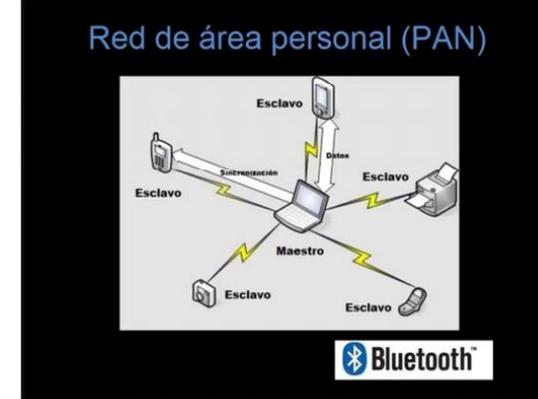
Este solapamiento de maestros y esclavos en piconets recibe el nombre de **scatternet (red dispersa)** y, aunque son varias piconets entrelazadas, no tienen definidas capacidades de enrutamiento entre ellas ya que Bluetooth solo define protocolos hasta el nivel 2.



Redes de Área Local Olga Minguet 19

UD7. Redes mixtas integradas

Red de área personal (PAN)



Redes de Área Local Olga Minguet 20

UD7. Redes mixtas integradas

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

➤ Actividad 1

Redes de Área Local Olga Minguet 21

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES Wi-Fi

La operativa de funcionamiento de una Wi-Fi consiste en que:

1. El punto de acceso transmite una trama de administración que contiene un identificador único **SSID** (Service Set Identifier) o **BSSID** (Basic SSID). El valor de SSID se establece en tiempo de configuración del punto de acceso.
2. La estación inalámbrica cliente escuchará esta trama de administración e identificará al punto de acceso.
3. El cliente elegirá un punto de acceso y establecerá una asociación con él si la negociación de autenticación tiene éxito.
4. El cliente inalámbrico comunicará con otras estaciones a través del punto de acceso, que hará de puente entre los distintos segmentos de red y el resto de estaciones inalámbricas asociadas con él.

Redes de Área Local Olga Minguet 22

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES Wi-Fi

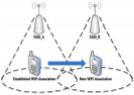
Punto de acceso o AP (Access Point)
Es el dispositivo que centraliza las comunicaciones inalámbricas. Suele hacer de integrador entre la red cableada y la red inalámbrica.

Canal de transmisión de una LAN
Es un parámetro que especifica la frecuencia a la que se transmitirán las señales entre emisor y receptor.

SSID
Service Set Identifier es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

MIMO
(Multiple Input Multiple Output) permite una cobertura mayor en zonas de difícil acceso eliminando en lo posible la pérdida de paquetes de datos.

Roaming
Es la función de los sistemas inalámbricos formados por varias celdas por las que un cliente que se desplaza cambiando de celda a celda, buscando la mejor cobertura y sin perder la conexión a la troncal de la red a la que se conectan todas las celdas.



Redes de Área Local Olga Minguet 23

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES Wi-Fi

IEEE 802.11 es el estándar para redes locales inalámbricas. En él se define un modo de seguridad básico:

1) **WEP** (Wired Equivalent Privacy), llamado así porque proporcionaba una seguridad equivalente a la obtenida en redes cableadas sin encriptación. WEP es un protocolo que presenta un método de cifrado que se aplica a todos los mensajes que circulan por la red. La clave de encriptación debe ser conocida por todas las estaciones y por el punto de acceso. Sólo quien posee la clave correcta es capaz de descifrar mensajes. Sin embargo, **WEP es una protección muy débil** que fácilmente se puede romper, ya que es estática. Cuanto más larga sea la clave, mayor será la protección. Puede llegar a tener claves de encriptación de hasta **128 bits**.



Redes de Área Local Olga Minguet 24

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES Wi-Fi



IEEE 802.11 es el estándar para redes locales inalámbricas. En él se define un modo de seguridad básico:

- 2) **WPA** (Wi-Fi Protected Access) emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica por lo que es el método recomendado si el dispositivo es compatible con este tipo de cifrado. Las claves se insertan con dígitos alfanuméricos, sin restricción de longitud.
- 3) **WPA2** es la segunda generación de WPA. Necesita el **Estándar avanzado de cifrado (AES)** para el cifrado de los datos, que aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias gubernamentales.

Redes de Área Local Olga Minguet 25

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES Wi-Fi



IEEE 802.11 establece dos métodos de autenticación o de autorización: **sistema abierto y clave compartida**.

1. **Sistema abierto.** Cualquier estación puede asociarse al punto de acceso emitiendo una solicitud que siempre será aceptada.
2. **Clave compartida.** La autenticación será correcta si el cliente sabe la clave secreta que deben compartir punto de acceso y cliente.



ESTÁNDAR: 802.11g
ENCRIPCIÓN: 1. SISTEMA ABIERTO
2. WEP
3. WPA
4. WPA2

Redes de Área Local Olga Minguet 26

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES Wi-Fi



Existen varios estándares de **IEEE 802.11 Wi-Fi**: www.wi-fi.org

1. **IEEE 802.11b.** (1999) Utiliza la banda de frecuencia de 2,4GHz.
2. **IEEE 802.11g.** (2003) Aumenta la velocidad a 54 Mbps.
3. **IEEE 802.11a.** Utiliza la banda de frecuencia de 5GHz. Frecuencia mayor, distancia menor, pero permite mayor número de canales de comunicación simultáneos.
4. **IEEE 802.11n.** (2007) Utiliza por primera vez el estándar MIMO, 2,4GHz y 5GHz, con velocidades de hasta 600Mbps. **MIMO permite una cobertura mayor en zonas de difícil acceso eliminando en lo posible la pérdida de paquetes y proporciona mayor velocidad inalámbrica por usar varias antenas de forma simultánea.**

Redes de Área Local Olga Minguet 27

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES Wi-Fi



5. **IEEE 802.11ac.** También conocido como Wi-Fi 5G o Wi-Fi Gigabit. Los enrutadores inalámbricos domésticos actuales son compatibles con este estándar y funcionan en el espacio de frecuencia 5GHz. Con entrada múltiple, salida múltiple (MIMO). Consigue teóricamente tasas de 3.4Gbps.
6. **IEEE 802.11ad.** (2012) Aumenta la velocidad, aunque esto implica reducción de distancia: solo 3'3 metros del punto de acceso.
7. **IEEE 802.11ah.** (2017) Utiliza bandas de frecuencia por debajo de 1GHz, saliendo de los rangos de 2.4 y 5GHz. Con velocidades de hasta 347Mbps. Compite así con Bluetooth. Su objetivo: reducir el gasto de energía. De esta forma se podría utilizar para los dispositivos de Internet (IoT).
8. **Está prevista la aprobación de la siguiente versión del estándar IEEE 802.11 serie b,** mejorando el "ah" y siguientes hasta el "ax", y enfocado a menores consumos para los dispositivos al tiempo que rendimientos óptimos"

Redes de Área Local Olga Minguet 28

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES WI-FI



Redes de Área Local Olga Minguet 29

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

REDES WI-FI

Standard	Freq Band	Bandwidth	Modulation	Max Data Rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mbs
802.11b	2.4 GHz	20 MHz	DSSS	11 Mbs
802.11a	5.0 GHz	20 MHz	OFDM	55 Mbs
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	55 Mbs
802.11n	2.4 GHz, 5.0 GHz	20 MHz, 40 MHz	OFDM	600 Mbs
802.11ac	5.0 GHz	20 MHz, 40 MHz, 80 MHz, 160 MHz	OFDM	6.93 Gbs
802.11ax	2.4 GHz, 5.0 GHz	20MHz, 40MHz, 80MHz, 160MHz	OFDM	9.60 Gbs

Redes de Área Local Olga Minguet 30

UD7. Redes mixtas integradas

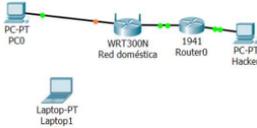
2. REDES INALÁMBRICAS

Integración de Wi-Fi con red cableada

Cuando se diseña la instalación de una red no suele empezarse por las conexiones inalámbricas. Normalmente se diseña primero la **estructura de cable** y los **servicios** que proveerán los servicios.

En una segunda fase se **estudian los clientes** y su modo de acceso. Si los clientes necesitan movilidad, entonces habrá que diseñar una red inalámbrica que se integre con la parte de red cableada **formando una red mixta**.

Tendremos clientes inalámbricos que se conectan a la red cableada a través de un punto de acceso. Podrá existir un servidor que encamine los paquetes entre la LAN cableada y otro router que proporcione acceso a Internet.



Redes de Área Local Olga Minguet 31

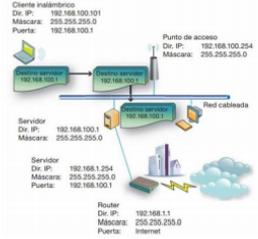
UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

Integración de Wi-Fi con red cableada

¿Qué debe ocurrir para que el cliente inalámbrico envíe un paquete al servidor y, en concreto, a la dirección de su interfaz interna (192.168.100.1)?

1. El cliente se pondrá en contacto con su punto de acceso y le enviará las tramas.
2. El punto de acceso observa que el destino del paquete está también en su misma red y lo pondrá en la red cableada sabiendo que el servidor lo leerá.



Redes de Área Local Olga Minguet 32

UD7. Redes mixtas integradas

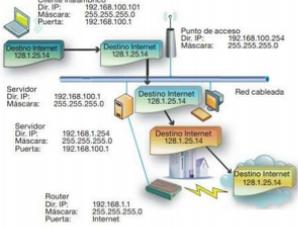
2. REDES INALÁMBRICAS

Integración de Wi-Fi con red cableada



¿Qué debe ocurrir para que el cliente inalámbrico envíe un paquete hacia una dirección en Internet, por ejemplo, la 128.1.25.14?

1. El cliente se pondrá en contacto con su punto de acceso.
2. El punto de acceso se da cuenta de que el destino del paquete no está en ninguna de las redes conectadas a sus interfaces y enviará el paquete a la puerta de enlace por defecto (192.168.1.1).
3. Sacará el paquete por la interfaz que le permitirá alcanzar el router. El router lo enviará a Internet.



Cliente inalámbrico
 Dir. IP: 192.168.100.101
 Máscara: 255.255.255.0
 Puerta: 192.168.100.1

Punto de acceso
 Dir. IP: 192.168.100.254
 Máscara: 255.255.255.0

Red cableada
Router
 Dir. IP: 192.168.1.1
 Máscara: 255.255.255.0
 Puerta: Internet

Destino Internet
 128.1.25.14

Redes de Área Local Olga Minguet 33

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

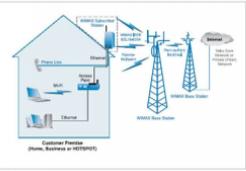
El estándar WiMAX



WiMAX es el nombre por el que se conoce a las redes inalámbricas que siguen el estándar IEEE 802.16, y que define una especificación para **redes metropolitanas** inalámbricas de banda ancha que pueden llegar hasta los **66GHz**.

WiMax, siglas de Worldwide Interoperability for Microwave Access (**Interoperabilidad mundial para acceso por microondas**).

Se compone de dispositivos electrónicos y la torre o **estación base WiMax**. Esta torre funciona exactamente igual que las torres de teléfonos de red situadas en un punto elevado para emitir señales de radio, pero la antena WiMax emite señales de microondas.



Redes de Área Local Olga Minguet 34

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

El estándar WiMAX



Las **dudas sobre la seguridad** han sido el principal freno tanto para los operadores comerciales como para los usuarios empresariales a la hora de realizar mayores inversiones y acometer proyectos Wi-Fi o de gran envergadura. Esto ha llevado a que el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y el conjunto de empresas que conforman el **WiMax Fórum** trabajen en conjunto para la definición de un entorno de seguridad robusto y consolidado que ofrezca plena confianza a los usuarios.



Redes de Área Local Olga Minguet 35

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

Wi-Fi vs WiMAX



No es necesario configurar un punto de acceso, tal como en Wi-Fi o en cualquier otro dispositivo de acceso. Todo lo que necesitamos es que el dispositivo este habilitado para WiMAX y una suscripción de pago, según el uso, o bien, se puede conectar a una red mantenida por un proveedor de servicios que ofrezca servicio de WiMAX dentro de tu área. También necesitaremos un software de recepción de red, normalmente proporcionado por la compañía suministradora.

	
Tasa de transferencia 15-54 Mbit/s	Tasa de transferencia 124 Mbit/s
Cobertura 300 metros	Cobertura 40-70 Kilómetros

Redes de Área Local Olga Minguet 36

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

Tecnología Li-Fi




Redes de Área Local Olga Minguet 37

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

WWAN: 5G



Redes de Área Local Olga Minguet 38

UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

CABLEADO vs INALÁMBRICO



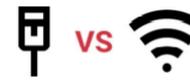
<p>Redes cableadas</p> <ul style="list-style-type: none"> • IEEE 802.3 • Es un medio 'acotado' • Sólo dos dispositivos conectados • Sin movilidad 	<p>Redes inalámbricas</p> <ul style="list-style-type: none"> • IEEE 802.11 • Espacio libre • Más de dos dispositivos conectados • Movilidad
--	--

Redes de Área Local Olga Minguet 39

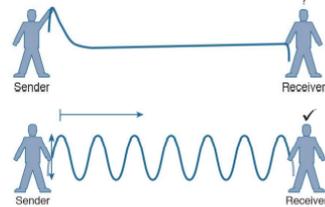
UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

CABLEADO vs INALÁMBRICO



¿Cómo pasan los datos a través de la conexión inalámbrica?



Redes de Área Local Olga Minguet 40

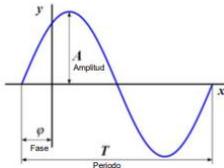
UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

CABLEADO vs INALÁMBRICO



¿Cómo pasan los datos a través de la conexión inalámbrica?



Frequency (Hz)	Frequency notation	Radio Frequencies (RF)
10 ²¹	10 ²¹ Hz	Subsonic
10 ²⁰	10 ²⁰ Hz	Subsonic
10 ¹⁹	10 ¹⁹ Hz	Subsonic
10 ¹⁸	10 ¹⁸ Hz	Subsonic
10 ¹⁷	10 ¹⁷ Hz	Subsonic
10 ¹⁶	10 ¹⁶ Hz	Subsonic
10 ¹⁵	10 ¹⁵ Hz	Subsonic
10 ¹⁴	10 ¹⁴ Hz	Subsonic
10 ¹³	10 ¹³ Hz	Subsonic
10 ¹²	100 GHz	Subsonic
10 ¹¹	10 GHz	Subsonic
10 ¹⁰	1 GHz	Subsonic
10 ⁹	100 MHz	Subsonic
10 ⁸	10 MHz	Subsonic
10 ⁷	1 MHz	Subsonic
10 ⁶	100 kHz	Subsonic
10 ⁵	10 kHz	Subsonic
10 ⁴	1 kHz	Subsonic
10 ³	100 Hz	Subsonic
10 ²	10 Hz	Subsonic
10 ¹	1 Hz	Subsonic
10 ⁰	0 Hz	Subsonic

Cosmic Rays
 Gamma Rays
 X-Rays
 Ultraviolet Light
 Visible Light
 Infrared Light
 Microwave and Radar
 Television and FM Radio
 Shortwave Radio
 AM Radio
 Low Frequency Radio
 Sound
 Subsonic

5 GHz Wireless
 2.4 GHz Wireless
 Radio Frequencies (RF)

Redes de Área Local Olga Minguet 41

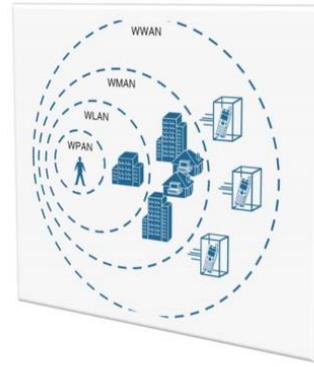
UD7. Redes mixtas integradas

2. REDES INALÁMBRICAS

RESUMEN

Tipos de redes inalámbricas:

- WPAN – Red inalámbrica de área personal
- WLAN – Red inalámbrica de área local
- WMAN – Red inalámbrica de área metropolitana
- WWAN – Red inalámbrica de área amplia



Redes de Área Local Olga Minguet 42

UD7. Redes mixtas integradas



Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 2
- Actividad 3
- Actividad 4
- Actividad 5

Redes de Área Local Olga Minguet 43

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

¿Qué son los datos masivos o Big Data?

Los **datos** son la información que proviene de una variedad de fuentes, como personas, imágenes, texto, sensores, sitios web y dispositivos de tecnología.



Hay **tres características** que indican que una organización puede estar haciendo frente a datos masivos:

- 1) Una gran cantidad de datos que requiere cada vez más espacio de almacenamiento (**volumen**).
- 2) Una cantidad de datos que crece exponencialmente rápido (**velocidad**).
- 3) Datos que se generan en diferentes formatos (**variedad**).

Redes de Área Local Olga Minguet 44

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

¿Qué son los datos masivos o Big Data?

Los **datos** son la información que proviene de una variedad de fuentes, como personas, imágenes, texto, sensores, sitios web y dispositivos de tecnología.

Ejemplos de volúmenes de datos recopilados por los sensores:

- Un *automóvil* autónomo puede generar 4000 gigabits (Gb) de datos por día.
- Un *hogar inteligente* conectado puede producir 1 gigabyte (GB) de información de la semana.



Redes de Área Local Olga Minguet 45

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

Grandes conjuntos de datos

- Las empresas **no necesariamente** tienen que generar sus propios datos masivos.
- Hay fuentes de conjuntos de datos **gratuitos** disponibles y listas para usar y analizar.



Redes de Área Local Olga Minguet 46

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

¿Cuáles son los desafíos de los datos masivos?

Los cálculos de datos masivos de **IBM** concluyen que “cada día creamos 2,5 trillones de bytes de datos”.

Hay cinco problemas de magnitud en cuanto al almacenamiento con los datos masivos:

- Administración
- Seguridad
- Redundancia
- Análisis
- Acceso



Redes de Área Local Olga Minguet 47

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

¿Dónde podemos almacenar los datos masivos?

“Muchas veces en la industria nos hemos encontrado con nombres que han sonado bien para el marketing pero que tecnológicamente no representaban absolutamente nada diferente o novedoso... poco a poco el término Fog Computing (quizás implementado primero por Cisco System quien a su vez junto a otras empresas como Dell, Intel Microsoft, la Universidad de Princeton y ARM Holdings fundaron en el 2015 OpenFog Consortium o Edge Computing e incluso Cloudlet Computing se empiezan a hacer más conocidos y a sonar más en la cabeza de todos... ¿estaremos nuevamente ante ingeniosos nombres de marketing o realmente será algo diferencial en el mundo del IoT? Tampoco podremos dejar de analizar estos nuevos conceptos desde la óptica de seguridad para entender sus implicaciones tanto técnicas como legales. (Chema Alonso, 2017)



Redes de Área Local Olga Minguet 48

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

¿Dónde podemos almacenar los datos masivos?

Por lo general, **los datos masivos se almacenan en varios servidores** en centros de datos.

La **computación en la niebla** utiliza dispositivos "perimetrales" o de clientes de usuarios finales para ejecutar gran parte del procesamiento previo y almacenamiento.



Los datos adquiridos a partir de ese análisis de procesamiento previo pueden introducirse en los sistemas de las empresas para modificar los procesos, de ser necesario.
 Las comunicaciones hacia y desde los servidores y dispositivos es más rápida y requiere menos ancho de banda que lo que supondría constantemente recurrir a la nube.

Redes de Área Local Olga Minguet 49

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

La nube y la computación en la nube



La nube es una **colección de centros de datos** o grupos de servidores conectados.

Los **servicios** en la nube para las personas incluyen lo siguiente:

- *Almacenamiento de datos*, tales como imágenes, música, películas y correos electrónicos.
- *Acceso a muchas aplicaciones* en lugar de descargar en el dispositivo local.
- *Acceso a datos y aplicaciones en cualquier lugar*, en cualquier momento y en cualquier dispositivo.

Redes de Área Local Olga Minguet 50

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

La nube y la computación en la nube



Los servicios en la nube **para las empresas** incluyen lo siguiente:

- ✓ Acceso a los datos de la organización en cualquier momento y en cualquier lugar.
- ✓ Optimiza las operaciones de TI de una organización.
- ✓ Elimina o reduce la necesidad de equipos, mantenimiento, y administración de TI en el sitio.
- ✓ Reduce el costo de necesidades de equipos, energía, requisitos físicos de la planta y la capacitación del personal.

Redes de Área Local Olga Minguet 51

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

¿Por qué las empresas analizan datos?

El **análisis de datos** permite que las empresas comprendan mejor el impacto de sus productos y servicios, ajusten sus métodos y objetivos, y proporcionen a sus clientes mejores productos más rápido.

Los **valores** provienen de los dos tipos de datos procesados principales: *transaccionales* y *analíticos*.

La información *transaccional* se captura y se procesa a medida que se producen eventos.

-Se utiliza para analizar informes de ventas y planes de fabricación diarios a fin de determinar cuánto inventario transportar.

La información *analítica* permite que se realicen tareas de análisis a nivel gerencial, como determinar si la organización debe instalar una nueva planta de fabricación.



Redes de Área Local Olga Minguet 52

UD7. Redes mixtas integradas

3. BIG DATA & CLOUD COMPUTING

Visualización de los datos

Tener una estrategia permite que una empresa determine el tipo de análisis de datos requerido y la mejor herramienta para realizar el análisis.

Las **herramientas y aplicaciones** varían desde el uso de una hoja de cálculo de Excel o Google Analytics para muestras de datos de pequeñas a medianas, hasta las aplicaciones dedicadas a la manipulación y al análisis de conjuntos de datos realmente masivos.

Entre los ejemplos se incluyen a **Knime, OpenRefine, Orange y RapidMiner.**




Redes de Área Local Olga Minguet 53

UD7. Redes mixtas integradas

4. INTELIGENCIA ARTIFICIAL

Cuando las cosas comienzan a pensar

- ❑ Muchos dispositivos ahora incorporan la tecnología inteligente para modificar su comportamiento en determinadas circunstancias.
- ❑ Esto puede ser tan simple como cuando un dispositivo inteligente reduce su consumo de energía durante períodos de demanda pico o tan complejo como conducir un auto de manera autónoma.
- ❑ Cada vez que se toma una decisión o un curso de acción mediante un dispositivo en función de información externa, dicho dispositivo luego se reconoce como dispositivo inteligente.

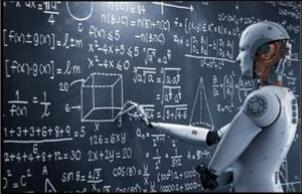


Redes de Área Local Olga Minguet 54

UD7. Redes mixtas integradas

4. INTELIGENCIA ARTIFICIAL

¿Qué es la inteligencia artificial y el aprendizaje automático?



La **Inteligencia artificial (AI)** es la inteligencia que demuestran las máquinas.

- La AI utiliza agentes inteligentes que pueden percibir el entorno y tomar decisiones.
- La AI hace referencia a los sistemas que imitan las funciones cognitivas normalmente asociadas a la mente humana, como el aprendizaje y la resolución de problemas.

El **aprendizaje automático (ML)** es un subconjunto de AI que utiliza técnicas estadísticas para otorgar a las computadoras la capacidad para "aprender" de su entorno. Esto permite que las computadoras mejoren su funcionamiento en una tarea puntual sin que se programe específicamente para esa tarea.

Redes de Área Local Olga Minguet 55

UD7. Redes mixtas integradas

4. INTELIGENCIA ARTIFICIAL

Aprendizaje automático (ML) e IoT

- ✓ Entre los usos de tecnología de ML se incluyen:
 - ✓ **Reconocimiento de voz:** se usa en asistentes digitales.
 - ✓ **Recomendación del producto:** los sistemas crean un perfil del cliente, y recomiendan productos o servicios en función de los patrones anteriores.
 - ✓ **Reconocimiento de la forma:** hay programas que permiten que diagramas y notas elaborados a mano de forma rudimentaria se conviertan en diagramas y texto más formales.
 - ✓ **Detección de fraudes de tarjetas de crédito:** se crea un perfil sobre los patrones de compra de un cliente.
 - ✓ **Reconocimiento facial**



VIDEO

Redes de Área Local Olga Minguet 56

UD7. Redes mixtas integradas

4. INTELIGENCIA ARTIFICIAL

¿Qué son las redes basadas en la intención (IBN)?



La industria de TI crea un enfoque sistemático para vincular la administración de infraestructuras con la intención empresarial (IBN).

- La red empresarial debe integrarse de manera segura y sin inconvenientes dispositivos de IoT, servicios basados en la nube y oficinas remotas.
- La red debe proteger estas nuevas iniciativas digitales del panorama de amenazas en constante cambio.
- La red debe ser lo suficientemente dinámica para adaptarse rápidamente a los cambios de las políticas y los procedimientos de seguridad, los servicios para empresas y las aplicaciones, y las políticas operativas.

Redes de Área Local Olga Minguet 57

UD7. Redes mixtas integradas

4. INTELIGENCIA ARTIFICIAL

¿Cómo se vinculan el ML, la AI y las IBN?

Las redes basadas en la intención aprovechan el poder de la **automatización** la AI y el ML para controlar la función de una red a fin de lograr un propósito o una intención específica.

La red es capaz de **traducir la intención en las políticas** y, a continuación, usar la **automatización** para implementar las configuraciones adecuadas necesarias.



Redes de Área Local Olga Minguet 58

UD7. Redes mixtas integradas

Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 6
- Actividad 7

Redes de Área Local Olga Minguet 59

UD7. Redes mixtas integradas

5. Redes IPv6

Necesidad de utilizar IPv6



- **IPv6 comparado con IPv4:**
 - Cuenta con un espacio de direcciones mayor de 128 bits.
 - 340 sextillones de direcciones.
 - Resuelve las limitaciones de IPv4.
 - Añade mejoras como la configuración automática de direcciones.
- **Por qué es necesario IPv6:**
 - La población que accede a Internet aumenta rápidamente.
 - Agotamiento de IPv4.
 - Problemas con NAT.
 - Internet de las cosas.

Redes de Área Local Olga Minguet 60

UD7. Redes mixtas integradas

5. Redes IPv6

Técnicas de migración de IPv4 a IPv6

Dual stack (Doble pila): los dispositivos ejecutan pilas de protocolos IPv4 e IPv6 de manera simultánea.

Tunelización: el paquete IPv6 se encapsula dentro de un paquete IPv4.

- IPv6 tenga que ser transportada sobre IPv4.
- IPv4 e IPv6 tengan que convivir en la red.
- Un protocolo tenga que ser traducido a otro.

Traducción: la traducción de direcciones de red 64 (NAT64) permite que los dispositivos habilitados para IPv6 se comuniquen con los habilitados para IPv4.

Redes de Área Local
Olga Minguet
61

UD7. Redes mixtas integradas

5. Redes IPv6

Técnicas de migración de IPv4 a IPv6

Tunelización: el paquete IPv6 se encapsula dentro de un paquete IPv4.

Redes de Área Local
Olga Minguet
62

UD7. Redes mixtas integradas

5. Redes IPv6

Técnicas de migración de IPv4 a IPv6

Traducción: la traducción de direcciones de red 64 (NAT64) permite que los dispositivos habilitados para IPv6 se comuniquen con los habilitados para IPv4.

Doble traducción Stateful de direcciones y puertos IPv4

Doble traducción
CLAT Stateless NAT64 (SNT)
PLAT Stateful NAT64

Ejem:
la dirección 192.168.150.23 se traducirá como 0:0:0:0:FFFF:C0A8:9617

Redes de Área Local
Olga Minguet
63

UD7. Redes mixtas integradas

5. Redes IPv6

Direccionamiento IPv6: Representación

El encaminamiento de IPv6 es mucho **más sencillo** que el de IPv4, ya que en la definición original del protocolo se han tenido en cuenta las dificultades que presentaba IPv4 para ser enrutado.

Direcciones IPv6:

- tiene 128 bits de longitud
- Cada 4 bits se representan por un dígito **hexadecimal**
- **Hexteto:** término no oficial que se refiere a un segmento de 16 bits o de **cuatro valores hexadecimales**

4 dígitos hexadecimales = 16 dígitos binarios

Redes de Área Local
Olga Minguet
64

UD7. Redes mixtas integradas

5. Redes IPv6

Direccionamiento IPv6: Representación

Formato preferido para la representación de IPv6

2001	:	0DB8	:	0000	:	1111	:	0000	:	0000	:	0000	:	0200
2001	:	0DB8	:	0000	:	00A3	:	ABCD	:	0000	:	0000	:	1234
2001	:	0DB8	:	00GA	:	0001	:	0000	:	0000	:	0000	:	0100
2001	:	0DB8	:	AAAA	:	0001	:	0000	:	0000	:	0000	:	0200
FE80	:	0000	:	0000	:	0000	:	0123	:	4567	:	89AB	:	CDEF
FE80	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
FF02	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
FF02	:	0000	:	0000	:	0000	:	0000	:	0001	:	FF00	:	0200
0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000

Redes de Área Local Olga Minguet 65

UD7. Redes mixtas integradas

5. Redes IPv6

Direccionamiento IPv6: Representación

➤ Regla 1: Omitir los ceros iniciales

Con el fin de reducir o comprimir IPv6, la primera regla es omitir los ceros iniciales en cualquier hexteto.

Recomendado	2001:0DB8:0000:1111:0000:0000:0000:0200
Sin ceros iniciales	2001:DB8:0:1111:0:0:0:200

Recomendado	2001:0DB8:000A:1000:0000:0000:0000:0100
Sin ceros iniciales	2001:DB8:A:1000:0:0:0:100

Recomendado	0000:0000:0000:0000:0000:0000:0000:0000
Sin ceros iniciales	0:0:0:0:0:0:0:0

Redes de Área Local Olga Minguet 66

UD7. Redes mixtas integradas

5. Redes IPv6

Direccionamiento IPv6: Representación

➤ Regla 2: Omitir segmentos de 0

Los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hextetos) que estén compuestas solo por ceros.

Recomendado	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Sin ceros iniciales	2001:DB8:0:0:ABCD:0:0:100
Comprimido	2001:DB8::ABCD:0:0:100
0	
Comprimido	2001:DB8:0:0:ABCD::100

Redes de Área Local Olga Minguet 67

UD7. Redes mixtas integradas

5. Redes IPv6

Direccionamiento IPv6: Representación

➤ Regla 2: Omitir segmentos de 0 (continuación)

Los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hextetos) que estén compuestas solo por ceros.

Recomendado	FF02:0000:0000:0000:0000:0000:0000:0001
Sin ceros iniciales	FF02:0:0:0:0:0:0:1
Comprimido	FF02::1

Recomendado	0000:0000:0000:0000:0000:0000:0000:0000
Sin ceros iniciales	0:0:0:0:0:0:0:0
Comprimido	::

Redes de Área Local Olga Minguet 68

UD7. Redes mixtas integradas

5. Redes IPv6

Direccionamiento IPv6: Representación

➤ **Regla 3: Notación mixta IPv4-IPv6**

Cuando nos encontramos en entornos en donde **IPv6 debe convivir con IPv4** suele ser conveniente una notación mixta en donde **los últimos 32 bits** de la dirección IPv6 se escriben como si fueran una dirección IPv4.

Ejemplo: la notación mixta de 192.168.150.23 será:

::FFFF:192.168.150.23

Redes de Área Local Olga Minguet 69

UD7. Redes mixtas integradas

5. Redes IPv6

Direccionamiento IPv6: Representación

La **longitud del prefijo IPv6** se usa para indicar la porción de red de la dirección IPv6:

- La longitud de prefijo puede ir de 0 a 128.
- La longitud de prefijo IPv6 típica en la mayor parte de las redes LAN es /64.

64 bits	64 bits
Prefijo	ID de interfaz
Por ejemplo: 2001:DB8:A::/64	
2001:0DB8:000A:0000	0000:0000:0000:0000

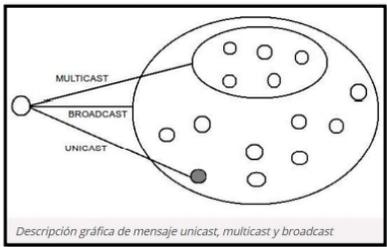
Redes de Área Local Olga Minguet 70

UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6:



Descripción gráfica de mensaje unicast, multicast y broadcast

Redes de Área Local Olga Minguet 71

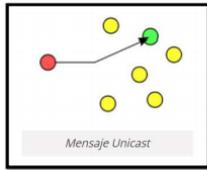
UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6:

1) UNICAST o Unidifusión: Cuando la comunicación se produce de un único emisor a un único receptor IPv6.



Mensaje Unicast



Redes de Área Local Olga Minguet 72

UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6: Unicast

Cuando un paquete es enviado a una dirección unicast, éste se entrega a la única interfaz de red que posee esa dirección.

Existen tres tipos:

- Direcciones unicast globales (2000::)
- Direcciones link-local (FE80::)
- Direcciones local addresses (FC00::)

Redes de Área Local Olga Minguet 73

UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6: Unicast

Direcciones unicast globales

Son las direcciones IPv6 que se pueden enrutar públicamente (del mismo modo que IPv4).
El ISP proporciona un ID de red mínimo /48, que a su vez proporciona 16 bits para crear una dirección de interfaz de enrutador única de 64 bits. Los últimos 64 bits son el ID de host único.
Estas direcciones tienen la siguiente estructura IPv6:
2000::<ID de interfaz>/3

Redes de Área Local Olga Minguet 74

UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6: Unicast

Direcciones link-local

Es para comunicaciones dentro de una subred local.
Son utilizadas cuando se comunica con un nodo adyacente o vecino.
Los routers no enrutan paquetes con este tipo de comunicación de enlace local.
Estas direcciones tienen la siguiente estructura IPv6:
FE80::<ID de interfaz>/10

Ejemplo:
Supongamos un dispositivo con MAC=08-00-02-12-34-56
La dirección IPv6 local de enlace sería: FE80::800:0212:3456

Redes de Área Local Olga Minguet 75

UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6: Unicast

Direcciones local addresses

Estas direcciones también están destinadas al ámbito local, aunque globalmente son únicas. Fueron diseñadas para ser las equivalentes a las IPv4 exclusivamente privadas.
Estas direcciones tienen la siguiente estructura IPv6:
FC00::<ID de interfaz>:<ID de interfaz>/7

Ejemplo:
Supongamos un dispositivo con MAC=00-00-0C-12-34-56
La dirección IPv6 local de sitio sería: FEC0::11:0:C12:3456

Redes de Área Local Olga Minguet 76

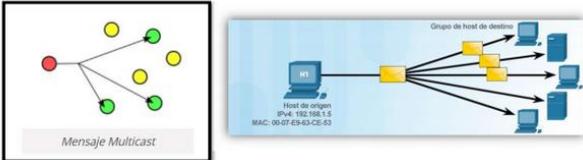
UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6:

2) **MULTICAST o Multidifusión:** Cuando la comunicación se produce de un único emisor a un grupo de destinos IPv6.



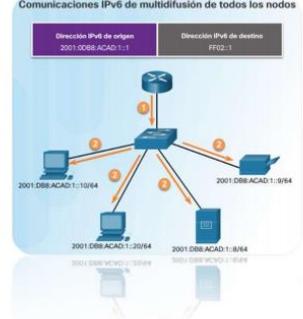
Redes de Área Local Olga Minguet 77

UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6: Multicast

Es una dirección que identifica a un conjunto de interfaces y cuando un paquete es enviado a una dirección multicast, el paquete será entregado en todas y cada una de las interfaces que posean esa dirección multicast y que estén operativas.



Las direcciones que comienzan por <1111 1111> en binario, o **FF** en hexadecimal, corresponden a multicast.

FFx::dirección

Redes de Área Local Olga Minguet 78

UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6:

3) **ANYCAST o Broadcast por proximidad:** Cuando la comunicación se produce de un único emisor a todos los destinos posibles dentro de la red del emisor.



Redes de Área Local Olga Minguet 79

UD7. Redes mixtas integradas

5. Redes IPv6

Tipos de direcciones IPv6: Anycast

Al igual que las direcciones de multicast, una dirección anycast identifica múltiples interfaces en varios dispositivos. Pero hay una gran diferencia: el paquete anycast es recogido por un solo dispositivo, en realidad, el más cercano que se encuentra situado en términos de distancia de enrutamiento.

Las direcciones anycast normalmente sólo se configuran en routers, nunca hosts, y una dirección de origen nunca podrá ser una dirección anycast.

Redes de Área Local Olga Minguet 80

UD7. Redes mixtas integradas

5. Redes IPv6

Direcciones especiales
 Puesto que con IPv6 tenemos una 'galaxia' de direcciones, podemos reservar algunos rangos para usos específicos sin preocuparnos por la limitación de direcciones. Los más importantes que convendrá recordar son:

0:0:0:0:0:0:0:0	Igual que en IPv4, es típicamente la dirección de fuente antes de recibir una dirección IP
0:0:0:0:0:0:0:1	Es el equivalente a 127.0.0.1 en IPv4
0:0:0:0:0:0:192.168.100.1	Es así como se escribirá una dirección IPv4 en un entorno mixto IPv6/IPv4
2000::/3	El rango global de direcciones de unicast
FC00::/7	El único rango local unicast
FE80::/10	El rango de link-local unicast
FF00::/8	El rango de Multicast
3FFF:FFFF::/32	Reservado para ejemplos y documentación
2001:0DB8::/32	También reservado para ejemplos y documentación
2002::/16	Se utiliza con túneles de 6 a 4, que es un sistema de transición IPv4 a IPv6.

Redes de Área Local Olga Minguet 81

UD7. Redes mixtas integradas

 Realiza las siguientes ACTIVIDADES del Cuaderno de Actividades:

- Actividad 8
- Actividad 9
- Actividad 10
- Actividad 11
- Actividad 12

Redes de Área Local Olga Minguet 82

8.7.2 Cuaderno de actividades

<h3 style="margin: 0;">Cuaderno de Actividades</h3> <p style="margin: 10px 0 0 0;">- UNIDAD 7 -</p> <p style="margin: 0 0 0 0;">Redes mixtas integradas</p>	<p>CUADERNO DE ACTIVIDADES</p> <p style="text-align: center;">Objetivos</p> <ul style="list-style-type: none"> • Consolidar los contenidos vistos en la Unidad 7 del curso de Redes de Área Local. • Se han descrito los principios de funcionamiento de las redes locales. • Se han reconocido los principios funcionales de las redes locales. • Se han identificado los distintos tipos de redes y los protocolos. • Se han configurado los parámetros básicos. • Se han aplicado mecanismos básicos de seguridad. <p style="text-align: center;">Actividades</p> <p>1. Confirma la veracidad de las siguientes afirmaciones relacionadas con las redes Bluetooth:</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 10px;"> <tr> <td colspan="2" style="padding: 2px;">Un dispositivo puede ser simultáneamente maestro y esclavo de la misma piconet</td> </tr> <tr> <td style="width: 20%; padding: 2px;">Cierto/falso</td> <td style="padding: 2px;"></td> </tr> <tr> <td style="padding: 2px;">Justificación</td> <td style="padding: 2px;"></td> </tr> </table> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 10px;"> <tr> <td colspan="2" style="padding: 2px;">Un dispositivo maestro en una piconet también lo puede ser simultáneamente de otra piconet</td> </tr> <tr> <td style="width: 20%; padding: 2px;">Cierto/falso</td> <td style="padding: 2px;"></td> </tr> <tr> <td style="padding: 2px;">Justificación</td> <td style="padding: 2px;"></td> </tr> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2" style="padding: 2px;">Un dispositivo puede ser esclavo simultáneamente de varias piconets</td> </tr> <tr> <td style="width: 20%; padding: 2px;">Cierto/falso</td> <td style="padding: 2px;"></td> </tr> <tr> <td style="padding: 2px;">Justificación</td> <td style="padding: 2px;"></td> </tr> </table> <p style="font-size: small; margin-top: 20px;">UD07 – Redes mixtas integradas 2-8</p>	Un dispositivo puede ser simultáneamente maestro y esclavo de la misma piconet		Cierto/falso		Justificación		Un dispositivo maestro en una piconet también lo puede ser simultáneamente de otra piconet		Cierto/falso		Justificación		Un dispositivo puede ser esclavo simultáneamente de varias piconets		Cierto/falso		Justificación	
Un dispositivo puede ser simultáneamente maestro y esclavo de la misma piconet																			
Cierto/falso																			
Justificación																			
Un dispositivo maestro en una piconet también lo puede ser simultáneamente de otra piconet																			
Cierto/falso																			
Justificación																			
Un dispositivo puede ser esclavo simultáneamente de varias piconets																			
Cierto/falso																			
Justificación																			

CUADERNO DE ACTIVIDADES

Una piconet puede tener uno o más dispositivos maestros simultáneamente

Cierto/falso	
Justificación	

Las piconets de una misma scatternet deben funcionar sincronizadas a la misma frecuencia de reloj

Cierto/falso	
Justificación	

2. Relaciona los elementos de la columna de la izquierda (Estándar) con los de la derecha (Característica).

Estándar	Característica
IEEE 802.11b	WiMAX
IEEE 802.11g ó a	Hasta 54 Mbps
IEEE 802.11n	Hasta 11 Mbps
Bluetooth	PAN
IEEE 802.16	MIMO y hasta 600 Mbps

Indica la relación correcta en la siguiente tabla:

Estándar	Característica
IEEE 802.11b	
IEEE 802.11g ó a	
IEEE 802.11n	
Bluetooth	
IEEE 802.16	

CUADERNO DE ACTIVIDADES

3. Descubre los errores en el siguiente razonamiento:

«He configurado un punto de acceso inalámbrico para que los clientes utilicen MIMO como mecanismo de encriptación en sus comunicaciones. Para aumentar la seguridad de la red inalámbrica se ha deshabilitado la publicación del SSID de la red.

Cada cliente accederá con su propia clave WEP (distinta para cada cliente) que el administrador de red suministrará a cada portátil inalámbrico».

4. Descubre cuál es el problema del usuario que se describe a continuación:

«El usuario de un equipo de sobremesa dispone de un dispositivo USB en cuya superficie el fabricante ha serigrafiado una etiqueta con el texto "USB WiMAX connector".

Después de conectar en el puerto USB el adaptador, el usuario ha querido iniciar la conexión a una red IEEE 802.11g que tiene desplegada en su empresa, pero el equipo no encuentra la red y no se puede conectar a ella.»

CUADERNO DE ACTIVIDADES

5. Decide en función de las circunstancias concretas que se describen a continuación si conectarías un cliente a la red local a través de una red inalámbrica o a través de una red cableada e indica porqué.

- a) Un cliente envía datos esporádicamente a un servidor local.

- b) Hay un cliente en la red que genera un flujo de datos muy intenso durante algunas horas al día

- c) Un cliente de red envía algunos datos en tiempo real, pero la densidad de portátiles inalámbricos es muy alta

- d) Un cliente detecta una docena de células Wi-Fi en su radio de acción

6. Si utilizas servicios en línea para almacenar datos o comunicarte con tus amigos o familiares, probablemente hiciste un acuerdo con el proveedor.

Los Términos de servicio, también conocidos como Términos de uso o Términos y condiciones, son un contrato de vinculación legal que rige las reglas de la relación entre tú, tu proveedor, y otras personas que utilizan el servicio.

Dirígete al sitio web de un servicio en línea que utilices y busca el acuerdo de los Términos de servicio. A continuación, se muestra una lista donde se encuentran los términos de servicio de muchas redes sociales y servicios de almacenamiento en línea conocidos:

UD07 – Redes mixtas integradas

5-8

CUADERNO DE ACTIVIDADES

Redes sociales

Facebook: <https://www.facebook.com/policies>

Instagram: <http://instagram.com/legal/terms/>

Twitter: <https://twitter.com/tos>

Pinterest: <https://about.pinterest.com/en/terms-service>

Almacenamiento en línea

iCloud: <https://www.apple.com/legal/internet-services/icloud/en/terms.html>

Dropbox: <https://www.dropbox.com/terms2014>

OneDrive: <http://windows.microsoft.com/en-us/windows/microsoft-services-agreement>

Revisa los términos, accediendo desde el enlace correspondiente, y responde las siguientes preguntas:

- a) ¿Tienes una cuenta con algún proveedor de redes sociales y/o almacenamiento en línea? Si es así, ¿has leído el acuerdo de los términos de servicio? Contesta a continuación.
 - b) ¿Cuál es la política de uso de datos del proveedor que has elegido? Puedes realizar una captura donde lo indica.
 - c) ¿Cuáles son tus derechos en relación con sus datos? ¿Puedes solicitar una copia de tus datos? Contesta a continuación con tus propias palabras.
 - d) ¿Qué puede hacer el proveedor con los datos que tú cargas
7. ¿Has visualizado alguna vez cuál es tu *huella digital*? Entra en tu navegador predeterminado, a ser posible en su última versión, y escribe tu nombre entre comillas. Por ejemplo "Antonio Pérez".
- a) ¿En cuántos ítems de búsqueda aparece información de ti mismo? Haz una captura e insértala a continuación.
 - b) ¿Te ha sorprendido? Imagino que aparecerán páginas de terceros que están "ofreciendo" tus datos recogidas de otros enlaces. ¿Es así en tu caso? Responde a continuación.
 - c) ¿Conoces que puedes solicitar la cancelación de estas publicaciones? Entra en ellas y bloquea aquello que creas necesario.....

UD07 – Redes mixtas integradas

6-8

CUADERNO DE ACTIVIDADES

8. Escribe en la forma IPv6 más abreviada posible las siguientes direcciones IPv6 e IPv4:

Dirección IPv6 o IPv4	Forma abreviada IPv6
FF01:0000:0000:0000:0000:0000:0144:0001	
FF01:0000:0000:0000:12DF:0000:0144:0001	
0000::1	
192.168.20.20	
0000::FFFF:192.168.10.20	
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A	
0E80:0000:0000:0000:02AA:00FF:FE9A:4CA2	
192.168.12.122	
FF02:0003:0000:0000:0000:0000:0000:0005	

9. En las siguientes IPv6 indica su tipo (anycast, multicast, unicast o IPv4)

Dirección IPv6 o IPv4	Tipo
FF03:0000:0000:A35F:0000:DF25:0144:0001	
FE80::0000:A35F:0000:DF25:0144:0001	
::FFFF:192.168.150.20	
FFC0::0000:A35F:0000:DF25:0144:0001	
023F::0000:A35F:0000:DF25:0144:0001	

10. Asocia las características tecnológicas (primera columna) con el tipo de paquete IP correspondiente (unicast, multicast o anycast).

Característica	Topología inalámbrica
A. La dirección de destino implica a varios nodos	
B. La dirección de destino es única	
C. La dirección de destino implica a varios nodos, pero sólo a uno de ellos	

CUADERNO DE ACTIVIDADES

11. En la primera columna de la siguiente tabla se exponen una serie de tecnologías. Rellena con SI o NO en las dos columnas siguientes según la tecnología especificada en la primera columna sea o no aplicable a las redes inalámbricas y a las cableadas.

Tecnologías	WLAN	Red cableada
Dirección IP		
Máscara de red		
Dirección MAC		
SSID		
Punto de acceso		
Antenas		
WEP		
Conectores de red		
WPA2		
Ethernet		
Wi-Fi		
IEEE 802.11		

12. Busca los errores en el siguiente argumento técnico:

«Los hackers saben muy bien cómo crackear una clave WEP. El procedimiento es casi inmediato si la clave WEP es de 64 bits, pero es más difícil si la clave tiene una longitud de 128 bits.

Para mejorar la seguridad de las comunicaciones inalámbricas, se ha mejorado WEP con el protocolo WPA, que también funciona con redes cableadas.

Todas las comunicaciones que establecen los clientes inalámbricos con el punto de acceso mediante WPA viajan encriptadas según indica el protocolo de cifrado SSL.»

8.7.3 Cuaderno de prácticas

UD07: Redes mixtas Integradas

PRÁCTICA 1

Crea un diagrama de flujo de un proceso

EXPLICACIÓN TEÓRICA

El software de rastreo de rutas se utiliza para enumerar las redes que los datos deben atravesar desde el dispositivo final del usuario que los origina hasta una red de destino remota.

Esta herramienta de red, generalmente, se ejecuta en la línea de comandos de esta manera:

```
tracert <nombre de red de destino o dirección de dispositivo final>
(Sistemas Microsoft Windows)
```

o

```
traceroute <nombre de red de destino o dirección de dispositivo final>
(Unix y sistemas similares)
```

Las utilidades de rastreo de rutas permiten a un usuario determinar la trayectoria o las rutas, como así también la demora en una red IP.

La herramienta **traceroute** (o **tracert**) se utiliza, generalmente, para resolver problemas de redes. Al mostrar una lista de los routers que se atraviesan, permite al usuario identificar la ruta tomada para llegar a un destino determinado en la red o en redes interconectadas. Cada router representa un punto en el que una red se conecta a otra y a través del cual se reenvió el paquete de datos.

La cantidad de routers se conoce como la cantidad de "saltos" por los que viajaron los datos desde el origen hasta el destino.

La lista que se muestra puede ayudar a identificar problemas de flujo de datos cuando se intenta acceder a un servicio, como un sitio web. También se puede utilizar para realizar tareas como descarga de datos. Si hay varios sitios web (sitios reflejados) disponibles para el mismo archivo de datos, se puede rastrear cada uno de estos para tener una idea clara de cuál sería el más rápido para utilizar.

Dos rastreos de rutas entre el mismo origen y destino realizados en diferentes momentos pueden producir distintos resultados. Esto se debe a la naturaleza de "malla" de las redes interconectadas que conforman Internet y a la capacidad de los protocolos de Internet para seleccionar diferentes rutas por las que se deben enviar paquetes.

Por lo general, el sistema operativo del dispositivo final tiene integradas herramientas de rastreo de rutas basadas en la línea de comandos (ejemplo, el `cmd`).

Otras herramientas, como VisualRoute™, son programas exclusivos que proporcionan información adicional. VisualRoute utiliza la información disponible en línea para mostrar la ruta gráficamente.

Página 1 de 10

UD07: Redes mixtas Integradas

Esta práctica de laboratorio supone la **instalación de VisualRoute**. Si la computadora que utiliza no tiene VisualRoute instalado, puede descargar el programa en el siguiente enlace: <http://www.visualroute.com/download.htm> Debemos descargar la edición Lite.

En el General de RL en Teams también tendrás un ejecutable para realizar directamente la instalación de la última versión de VisualRoute. Son 4Mb

¿QUÉ VAMOS A HACER EN ESTA PRÁCTICA?

Con una conexión a Internet, utilizaremos 3 utilidades de rastreo de rutas para examinar la ruta de Internet hacia las redes de destino.

- 1) En primer lugar, utilizaremos la utilidad **ping** integrada de Windows para verificar la conectividad.
- 2) En segundo lugar, utilizaremos la utilidad **tracert** integrada de Windows.
- 3) En tercer lugar, utilizaremos una herramienta **traceroute basada en Web**, clicando en el siguiente enlace (<http://www.subnetonline.com/pages/network-tools/online-traceroute.php>).
- 4) Por último, utilizaremos el programa trazador (**traceroute**) de **VisualRoute**, la aplicación que hemos indicado en el apartado anterior.

¿QUÉ NECESITAMOS PARA HACER LA PRÁCTICA?

1 PC con acceso a Internet

!! NO ES UNA PRÁCTICA DE PACKET TRACER !!

Página 2 de 10

UD07: Redes mixtas Integradas

Parte 1: Probar la conectividad de red mediante el comando ping

Paso 1: Determinar si hay posibilidad de conexión al servidor remoto.

Para rastrear la ruta hacia la red remota, el ordenador que se utilice debe tener una conexión a Internet que funcione.

- a. La primera herramienta que utilizaremos es **ping**.

Ping es una herramienta que se utiliza para probar si hay posibilidad de conexión a un host. Se envían paquetes de información al host remoto con instrucciones para responder. La computadora local mide si se recibe una respuesta a cada paquete y el tiempo que dichos paquetes demoran en cruzar la red. El nombre "ping" proviene de la tecnología de sonar activo en la que un impulso sonoro se envía por debajo del agua, y rebota en tierra o en otras embarcaciones.

- b. En el ordenador, busque "cmd".



- c. En la petición de línea de comandos, escriba **ping www.cisco.com**.

INSERTA LA CAPTURA AQUÍ

- d. Fíjate, **en la primera línea de resultados aparece el nombre de dominio totalmente calificado (FQDN) 9144.dscc.akamaiedge.net**. A continuación, aparece la dirección IP 23.1.43.170. Cisco aloja el mismo contenido web en diferentes servidores en todo el mundo (conocidos como "servidores reflejados"). Por lo tanto, según dónde se encuentre geográficamente, el FQDN y la dirección IP serán diferentes.

- e. De esta porción del resultado, se desprende lo siguiente:

```
Ping statistics for 23.1.43.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Se enviaron cuatro pings y se recibió una respuesta de cada ping. Como se respondió cada ping, hubo una pérdida de paquetes del 0%. En promedio, **los paquetes tardaron 54 ms (milisegundos)** en atravesar la red. Un milisegundo es una milésima de segundo.

La transmisión de video y los juegos en línea son dos aplicaciones que se ven afectadas cuando hay pérdida de paquetes o una conexión de red lenta. Es posible determinar la velocidad de una

```
C:\>ping -n 100 www.cisco.com
```

conexión a Internet de manera más precisa al enviar 100 pings, en lugar de los 4 predeterminados. Para ello, se debe hacer lo siguiente:

UD07: Redes mixtas Integradas

Siendo el resultado:

INSERTA LA CAPTURA AQUÍ

¿Qué promedio (Average) de tiempo nos da con el envío de 100 paquetes?

Este promedio que hemos obtenido es mucho más fiable que con el envío de sólo 4 paquetes.

Ahora, haga ping a los **sitios web del registro regional de Internet (RIR)** en distintas partes del mundo:

Para África:
C:\> ping www.afnic.net

INSERTA LA CAPTURA AQUÍ

Para Australia:
C:\> ping www.apnic.net

INSERTA LA CAPTURA AQUÍ

Para Europa:
C:\> ping www.ripe.net

INSERTA LA CAPTURA AQUÍ

UD07: Redes mixtas Integradas

Para América del Sur:
C:\> ping www.lacnic.net

INSERTA LA CAPTURA AQUÍ

Todos estos pings realmente se ejecutaron en un ordenador ubicado en EE. UU. ¿Qué sucede con el tiempo promedio de ping en milisegundos cuando los datos viajan dentro del mismo continente (América del Norte) en comparación con los datos que viajan desde América del Norte hacia distintos continentes?

¿Qué se puede destacar de los pings que se enviaron al sitio web europeo? ¿Es posible que en el momento en que se enviaron estos pings el sitio estaba inaccesible (Request timed out)?

UD07: Redes mixtas Integradas

Parte 2: Rastrear una ruta a un servidor remoto mediante tracert

Paso 1: Determinar qué ruta a través del tráfico de Internet llega al servidor remoto.

Ahora que hemos verificado la posibilidad de conexión básica utilizando la herramienta ping, es útil observar más detenidamente cada segmento de red que se atraviesa. Para ello, se utilizará la herramienta **tracert**.

- a. En la petición de entrada de la línea de comandos, escriba **tracert www.cisco.com**.

INSERTA LA CAPTURA AQUÍ

Para que esté correcta, debe aparecer en la última línea "Trace complete"

- b. Guarde el resultado del comando tracert en un archivo de texto de la siguiente manera:
- 1) Haga clic con el botón secundario en la barra de título de la ventana del símbolo del sistema y seleccione **Editar > Seleccionar todo**.
 - 2) Vuelva a hacer clic con el botón secundario en la barra de título del símbolo del sistema y seleccione **Editar > Copiar**.
 - 3) Busque y abra el **Bloc de notas**.
 - 4) Para pegar el resultado en el Bloc de notas, seleccione **Edición > Pegar**.
 - 5) Seleccione **Archivo > Guardar como** y guarde el archivo del Bloc de notas en el escritorio con el nombre **tracert1.txt**.

Esto solo lo vamos a realizar para la conexión con www.cisco.com para realizar una **Reflexión Final**.

- c. Ejecute **tracert** para cada sitio web de destino restante.

C:\> tracert www.afknic.net

INSERTA LA CAPTURA AQUÍ

C:\> tracert www.lacnic.net

INSERTA LA CAPTURA AQUÍ

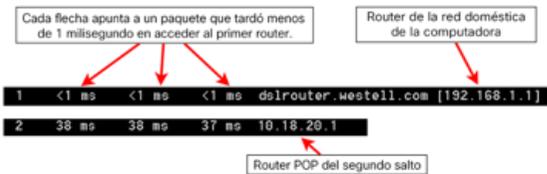
UD07: Redes mixtas integradas

d. Interprete los resultados de **tracert**.

Las rutas rastreadas pueden atravesar muchos saltos y distintos proveedores de servicios de Internet (ISP), según el tamaño del ISP y la ubicación de los hosts de origen y destino. Cada "salto" representa un router.

Dado que las computadoras se comunican mediante números, en lugar de palabras, los routers se identifican de manera exclusiva mediante direcciones IP (números con el formato x.x.x.x para direcciones IPv4). La herramienta **tracert** permite ver qué ruta toma un paquete de información en la red para llegar a su destino final. La herramienta **tracert** también le da una idea de la velocidad con la que avanza el tráfico en cada segmento de la red. Se envían tres paquetes a cada router en el trayecto y el tiempo de retorno se mide en milisegundos. Ahora, utilice esta información para analizar los resultados de **tracert** para www.cisco.com.

Mostrando el desglose del resultado que habrá obtenido, similar a esto:



En el resultado de ejemplo que se muestra arriba, los paquetes de **tracert** viajan desde la computadora de origen hasta el **gateway predeterminado del router local (salto 1: 192.168.1.1)** y, desde allí, hasta el **router de punto de presencia (POP) de ISP (salto 2: 10.18.20.1)**. Cada ISP tiene numerosos routers POP. Estos routers POP se encuentran en el perímetro de la red del ISP y son los medios por los cuales los clientes se conectan a Internet.

Los paquetes viajan por la red de **Verizon** a través de dos saltos y, luego, saltan a un router que pertenece a **alter.net**. Esto podría significar que los paquetes viajaron a otro ISP. Esto es importante porque, a veces, se produce una pérdida de paquetes en la transición entre ISP o, a veces, un ISP es más lento que otro.

Existe una **herramienta de Internet** que se conoce como **"Whois"**, que ya hemos trabajado en clase. La herramienta Whois nos permite determinar a quién pertenece un nombre de dominio. La herramienta web Whois se encuentra en <http://whois.domaintools.com/>. Según la herramienta web Whois, este dominio también pertenece a Verizon, observa:

```
Registrant:
Verizon Business Global LLC
Verizon Business Global LLC
One Verizon Way
Basking Ridge NJ 07920
US
domainregcontact@verizon.com +1.7033513164 Fax: +1.7033513469
Domain Name: alter.net
```

En resumen, el tráfico de Internet comienza en una computadora doméstica y atraviesa el router doméstico (salto 1). Luego, se conecta al ISP y atraviesa la red (saltos 2 a 7) hasta que llega al servidor remoto (salto 8). Este es un ejemplo relativamente inusual en el que solo participa un ISP desde el

UD07: Redes mixtas integradas

inicio hasta el final. Es común que participen dos o más ISP, como se muestra en los ejemplos siguientes.

Parte 3: Rastree una ruta a un servidor remoto mediante herramientas de web y herramientas software (VisualRoute Lite Edition)

Paso 1: Utilizar una herramienta traceroute basada en Web.

a. Utilice <http://www.subnetonline.com/pages/network-tools/online-tracepath.php> para rastrear la ruta a los siguientes sitios web:

- www.cisco.com
- www.aftrinic.net

Para ello es importante que en la web, situemos la herramienta que queremos utilizar:

Captura ambos resultados y guarda el resultado obtenido de www.cisco.com en el Bloc de notas solamente. El otro no nos será necesario.

www.cisco.com

INSERTA LA CAPTURA AQUÍ DEL RESULTADO DE LA HERRAMIENTA WEB

www.aftrinic.com

INSERTA LA CAPTURA AQUI DEL RESULTADO DE LA HERRAMIENTA WEB

¿En qué se diferencia el comando traceroute cuando se accede a www.cisco.com desde el símbolo del sistema (consulte la parte 2) en lugar de hacerlo desde el sitio web en línea? (Los resultados pueden variar según dónde se encuentre geográficamente y según el ISP que proporcione conectividad). ¿Es posible que la conexión a distintos servidores sea debido a que el sitio web está en los Países Bajos?

UD07: Redes mixtas Integradas

Compare el comando `tracert` de la parte 1 que va a África con el comando `tracert` que va a África desde la interfaz web. ¿Qué diferencia advierte? ¿Pasa por otro ISP?

Algunos de los `tracert`s tienen la abreviatura `asymm`. ¿Tiene alguna idea de a qué se refiere? ¿Qué significa? Puedes realizar una pequeña búsqueda por Internet.

Paso 2: Use "VisualRoute Lite Edition".

VisualRoute es un programa `tracert` exclusivo que puede mostrar gráficamente los resultados de la ruta de rastreo.

a. Si VisualRoute Lite Edition no está instalado, descárguelo del enlace siguiente:
<http://www.visualroute.com/download.html>

b. Rastree las rutas a **www.cisco.com** utilizando VisualRoute.

INSERTA LA CAPTURA AQUÍ DE LA VENTANA GRÁFICA COMPLETA

c. Registra las direcciones IP del trayecto, para ello escríbelas en el Bloc de notas.

INSERTA LA CAPTURA AQUÍ DEL BLOCK DE NOTAS

Página 8 de 10

UD07: Redes mixtas Integradas

Parte 4: Comparar los resultados de traceroute

Compara los resultados de `tracert` para **www.cisco.com** de las partes 2 y 3, que has escrito en el Bloc de Notas.

Paso 1: Indicar la ruta a **www.cisco.com** que se obtiene al utilizar el comando `tracert`. Escríbelo así (Ejem) `192.168.1.1>10.18.20.1>130.81.196.190>.....` indicando solamente las IPs de los saltos realizados.

Paso 2: Indicar la ruta a **www.cisco.com** que se obtiene al utilizar la herramienta basada en Web que se encuentra en **subnetonline.com**.

Paso 3: Indicar la ruta a **www.cisco.com** que se obtiene al utilizar **VisualRoute Lite Edition**.

¿Todas las utilidades de `tracert` usaron las mismas rutas para llegar a **www.cisco.com**? Explicite.

REFLEXIÓN FINAL

Ahora que se analizaste `tracert` mediante tres herramientas diferentes (`tracert`, interfaz web y **VisualRoute**), ¿**VisualRoute** proporciona algún detalle que las otras dos herramientas no ofrezcan?

Página 10 de 10

UD07: Redes mixtas integradas

PRÁCTICA 2

Configurar la seguridad inalámbrica en una red doméstica

¿Qué vamos a hacer en esta práctica?

- Crear una red doméstica con un router inalámbrico seguro

Introducción: Orden que seguiremos en el desarrollo

En esta actividad, configurarás un router inalámbrico para lo siguiente:

- Modificar la contraseña predeterminada.
- Modificar el SSID predeterminado y no difundirla.
- Utilizar el modo WPA2 personal como método de seguridad.
- Deshabilitar la administración remota.

Paso 1: Carga el archivo .pkt y cambia el módulo Ethernet por inalámbrico en el portátil

- Descarga el archivo Packet Tracer – Configure Wireless Security.pkt de la Tarea de Teams.
- Presiona el botón de **encendido/apagado** en la Laptop1 (Computadora portátil 1) para apagarla.
- Arrastra el puerto **Ethernet** a la lista **Modules** (Módulos) para eliminarlo.
- Arrastra el módulo **WPC300N** a la ranura vacía en **Laptop1** (Computadora portátil 1) y presiona el botón **power** (encendido) para arrancar la **Laptop1** (Computadora portátil 1).
- Ahora ya conecta (por ondas) con el Router inalámbrico.

Paso 2: Modifica la contraseña predeterminada.

- Haz clic en el router inalámbrico y selecciónale la **GUI** para la configuración.
- Haz clic en **Administration > Management** (Administración > Gestión).

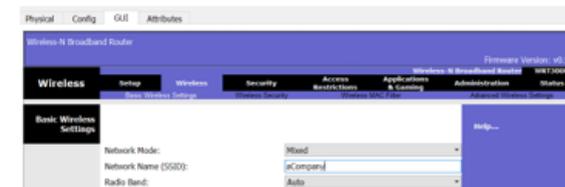


UD07: Redes mixtas integradas

- Modifica la contraseña del router a una más fuerte. Cambie la contraseña a **aCompAny3**. Ten en cuenta que la nueva contraseña tiene 8 caracteres con letras mayúsculas y minúsculas, dígitos, y algunas de las vocales se cambiaron por números.
- Después selecciona **Save Settings** (Guardar configuración) en la parte inferior de esa pantalla. (Te recomiendo que vuelvas a abrir la misma ventana y confirmes que se han quedado grabados los cambios).

Paso 3: Modifica el nombre del SSID predeterminado y deshabilita la característica de difusión.

- De nuevo, dentro de la configuración del router inalámbrico haz clic en **Wireless** (Inalámbrico) y cambia el nombre del SSID **Network Name** (que ahora está en "Default") por **aCompany**.



- En la misma ventana, selecciona **SSID Broadcast** (Difusión de SSID) y haz clic en **Disabled** (Deshabilitado). De nuevo, haz clic en **Save Settings** (Guardar configuración) en la parte inferior de esa pantalla. Y comprueba que se ha quedado guardado.
- Responde: ¿La Laptop0 (Computadora portátil 0) perdió la conectividad con el router inalámbrico? Si esto es correcto, ¿por qué?

Paso 4: Configurar la seguridad WPA2 en el router inalámbrico

- Vuelve a la pestaña de GUI del router inalámbrico. Haz clic en **Wireless > Wireless Security** (Inalámbrica > Seguridad inalámbrica). Cambie el modo de seguridad a **WPA2 Personal**. Actualmente, **AES** es el protocolo de cifrado más sólido disponible. Déjalo seleccionado.
- Configura **aCompWIFI** como la contraseña en Passphrase. Desplázate hacia la parte inferior de la ventana y haz clic en **Save Settings** (Guardar configuración).

UD07: Redes mixtas integradas



Paso 5: Configurar Laptop0 (Ordenador portátil 0) como el cliente inalámbrico

- a. Configura la Laptop0 (Ordenador portátil 0) en la red inalámbrica mediante la configuración de seguridad que estableciste en el router inalámbrico.

- 1) Selecciona **Laptop0 > Desktop > PC Wireless** (Computadora portátil 0 > Escritorio > PC inalámbrica).



- 2) Selecciona **Profiles > New** (Perfiles > Nuevo) y agrega cualquier nombre para el perfil.

UD07: Redes mixtas integradas



- 3) Después seleccione **Advanced Setup** (Configuración avanzada) en la esquina inferior derecha de la nueva ventana que te aparece.



- 4) En **Wireless Network Name** (Nombre de la red inalámbrica) ingresa el nuevo nombre de SSID: **aCompany**.



- 5) Acepta la configuración de red predeterminada seleccionando **Next** (Siguiente) dos veces.
- 6) Cambie la seguridad con el cuadro desplegable por **WPA2-Personal** y seleccione **Next** (Siguiente).

UD07: Redes mixtas Integradas



7) Introducez en esta nueva ventana la clave precompartida: **8CompWIFI** y seleccione **Next** (Siguiente).



8) Repasa los datos y Guarda el perfil que has configurado (**Save**).



9) En la ventana de felicitación que aparece, selecciona **Connect to Network** (Conectarse a la red).

Página 6 de 8

UD07: Redes mixtas Integradas



Aparecerá esta ventana de simulación de la conexión:



10) Si el ordenador portátil no se conecta correctamente, vuelve al perfil y modifícalo. Revisa el nombre del SSID que escribiste y la clave precompartida. Algo no has escrito bien en alguna de las ventanas de configuración.

b. Cierra la ventana **PC Wireless** (Computadora inalámbrica) y haz clic en **Command Prompt** (Símbolo del sistema).

c. Escribe **ipconfig /all** y toma nota de la dirección IP y la dirección MAC. Si lo prefieres inserta una captura del resultado en el cmd.

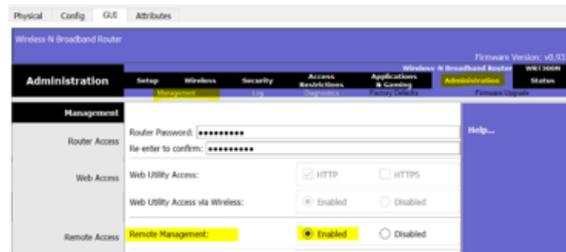
Podrás comprobar que ahora si hay señal inalámbrica entre el router y el portátil.
Con esta dirección MAC podríamos configurar el Router para establecer restricciones de conexión. Esto es, desde el Router podemos configurar un **Filtro de MAC** estableciendo así qué dispositivos se podrán conectar y qué otros no.

Página 8 de 8

UD07: Redes mixtas integradas

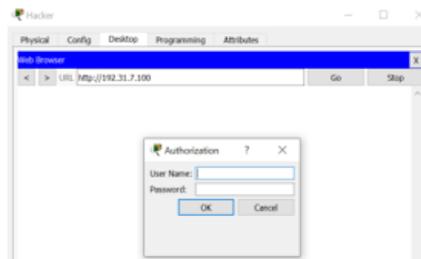
Paso 6: Deshabilita la administración remota en el router inalámbrico.

- a. Revisa el estado actual de la administración remota en el router inalámbrico. Selecciona **Administration > Management > Remote Management**. Si está deshabilitado, habilítalo seleccionando ENABLE. Recuerda "Save Settings"



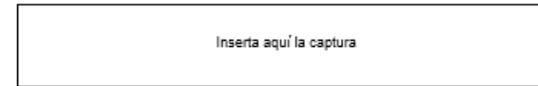
Cierra la ventana.

- b. Selecciona ahora **PC-PT Hacker** (PC de hacker) y clic en **Desktop > Web Browser** (Escritorio > Web Browser (Navegador web)). Introduce la dirección **192.31.7.100** y toque **Go** (Ir). Debe aparecer la solicitud de ID de usuario y contraseña. Observamos que ahora podríamos acceder a la GUI del router inalámbrico. Sin introducir ningún dato, sal del Escritorio.



- c. Regresa ahora a la página de configuración del router inalámbrico.
- d. Vuelve a **Administration > Management > Remote Management** (Administración remota). Vamos ahora a deshabilitar la conexión remota para ofrecer más seguridad, para ello selecciona **Disabled** (Deshabilitado) y haz clic en **Save Settings** (Guardar configuración) en la parte inferior de la pantalla.
- e. Vuelve ahora al **PC-PT Hacker** (PC de Hacker) y selecciona **Desktop > Web Browser** (Escritorio > Web Browser (Navegador web)) exactamente igual que antes. Introduce la dirección **192.31.7.100**. ¿Qué resultado te aparece? Inserta la captura.

UD07: Redes mixtas integradas



Conclusión: con la deshabilitación de esta opción, ya no podrás conectarte mediante el navegador web, lo que **aporta seguridad a nuestra red**.

UD07: Redes mixtas integradas

PRÁCTICA 3

Fuentes de datos abiertas

¿QUE VAMOS A HACER EN ESTA PRACTICA?

Estudiar los diferentes sitios web que proporcionan datos disponibles sin restricciones.

Parte 1: Open Government Partnership

Parte 2: Sitios web de datos sin restricciones

Parte 3: Visualización de los datos

INTRODUCCIÓN

A la fecha, se han generado y almacenado cantidades incommensurables de datos. Los datos son útiles solamente si se los puede emplear para generar más conocimientos. Cuando los datos se ponen a libre disposición de otras personas, *sin restricciones relacionadas con la propiedad intelectual*, se los considera **datos sin restricciones** (o abiertos). Es posible que los datos sin restricciones requieran que se mencione la fuente original. Los productos derivados del trabajo original también se pueden designar como datos sin restricciones.

En esta práctica de laboratorio estudiará varias fuentes de datos sin restricciones. También estudiará la capacidad de visualización de datos disponible en estos **sitios web para generar conclusiones basadas en hechos** (datos).

¿QUÉ NECESITAMOS PARA HACER LA PRÁCTICA?

- 1 Ordenador o dispositivo móvil con acceso a Internet

!! NO ES UNA PRÁCTICA DE PACKET TRACER !!

Página 1 de 14

UD07: Redes mixtas integradas

Parte 1: "Open Government Partnership"

Open Government Partnership (OGP) se fundó en 2011. La meta de la sociedad es crear una plataforma internacional con el fin de que los gobiernos se muestren más abiertos, sean más responsables y respondan mejor a sus ciudadanos.

- Dirígete a www.opengovpartnership.org/ donde existe información sobre OGP.
- Haz clic en **Miembros** (Nacionales), en la parte superior central de la pantalla.



Al final de la página aparece una lista de los diversos países que integran OGP. Escribe a continuación algunos de los que se indican (al menos 10).

Responde aquí

- Selecciona un país en la lista de la parte inferior de la página para ver información sobre la participación de dicho país en los datos sin restricciones. Con Albania como ejemplo, vemos que aparece una página con la descripción general de los pasos que siguió para unirse a OGP. También vemos gran cantidad de enlaces a información relacionada con la transición de ese país hacia un gobierno más abierto.

Página 2 de 14

UD07: Redes mixtas Integradas

Inserta una captura del Frontend de la página del país que has elegido:

Responde aquí

¿Desde qué año es miembro del OGP?

Responde aquí

En la página de cada país aparece información y enlaces a recursos relacionados con su compromiso por LOGRAR UN GOBIERNO ABIERTO. Haz clic en **Plan de Acción Actual** para conocer más sobre qué está realizando el país que has elegido. ¿En qué plan de acción se encuentra (número del plan) y qué periodo de años implica?

Responde aquí

¿En cuántos compromisos se ha implicado con este Plan de Acción? Enuméralos (puedes visualizarlos en el listado de Compromisos).

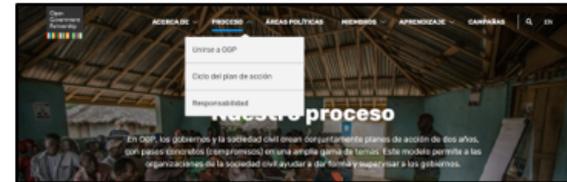
Responde aquí

Al final de la página que estás visualizando aparecen las Dimensiones seleccionadas para trabajar en convertirse en un Gobierno Abierto. Enuméralas a continuación.

Responde aquí

d. Vuelve a la página principal. En la parte superior de la pantalla aparece el menú principal. Desde aquí se indica las herramientas para poder desarrollar nuestro plan de acción, aprender de otros países, seguir el progreso en OGP y transmitir los efectos que se derivan de este progreso.

UD07: Redes mixtas Integradas



e. Por ejemplo: en la categoría **Unirse a OGP** aparecen las premisas necesarias para unirse a OGP y poder convertirte en un Gobierno abierto.

- Cumplir con los criterios básicos de elegibilidad y pasar la verificación de valores.
- Identificar un ministerio o agencia líder.
- Enviar una carta de intenciones.
- Involucrar a la sociedad civil en el proceso.

Lee estas premisas rápidamente. En tu carácter de ciudadano, ¿qué beneficios crees que puedes obtener si tu gobierno es más abierto? ¿Crees que es importante/que aporta algún beneficio? Explicáte.

Responde aquí

UD07: Redes mixtas Integradas

Parte 2: Sitios web de datos sin restricciones

Muchas organizaciones (gobiernos, universidades, empresas y organizaciones sin fines de lucro) publican sus datos sin restricciones. ¿Te interesan los datos sobre el clima, sobre viviendas o sobre el delito?

a. Dirígete a <http://www.data.gov>. Este sitio web es la página central de los datos sin restricciones del Gobierno de EE. UU. Aquí podrás encontrar datos y recursos sobre investigaciones, desarrollo de software y otros proyectos relacionados con los datos. Desde este sitio web también podrás dirigirte a los sitios web originales que proporcionaron la información publicada.

b. En la parte superior de la pantalla, haz clic en Datos.

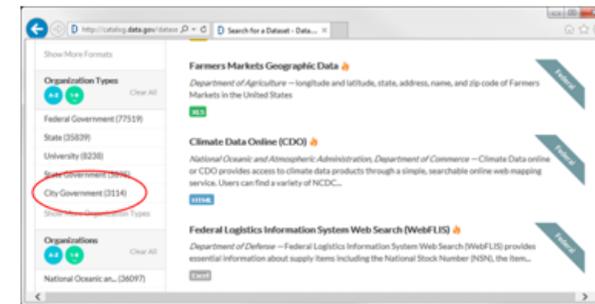


c. ¿Cuántos conjuntos de datos hay disponibles?

Responde aquí

UD07: Redes mixtas Integradas

d. Estudia un conjunto de datos interesante u otra categoría temática. Por ejemplo: puedes filtrar por diferentes categorías desde el Panel de la izquierda. Si solo estás interesado en los datos provistos por el gobierno de una ciudad. Filtra los datos eligiendo Gobierno Local. Desplázate hacia abajo por la lista hasta encontrar Tipos de organización. Y allí haz click en Gobierno de la ciudad.



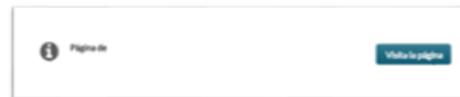
e. Haz click en el conjunto de datos de arrestos de la policía de Nueva York (datos de arrestos desde el 2008). En este conjunto de datos se ofrece el histórico de arrestos correspondientes a la ciudad de Nueva York. Observa que una vez dentro, te ofrece la posibilidad de descargarlo en diferentes formatos de archivo:

UD07: Redes mixtas integradas

¿Cuáles son los formatos de archivo para descargar disponibles? Enuméralos.

Responde aquí

Haz clic en el enlace de la página de bienvenida **Archivos de valores separados por comas**. En esta sección de descargas aparece una URL para descargar el excel de datos externo correspondiente. Al abrirlo es posible visualizar un listado de detenciones realizadas. Si clickas en alguna de las filas podrás visualizar los datos de dicha detención, fecha, motivo, posición geográfica, etc. En lugar de descargar ningún archivo, vamos a realizar una visualización desde la web. Para ello, haz clic en **Visita la página** donde nos conectará con un enlace externo.



UD07: Redes mixtas integradas

¿Cuándo fue la última actualización de datos?

Responde aquí

Al final de la página web aparece una tabla con un resumen de todos los arrestos realizados de forma ordenada. Si sitúas el ratón encima de cualquier celda podrás leer los datos referentes a cada arresto. Puedes hurgar un poco en estos datos. Haz una captura de esta tabla.

Responde aquí

f. Si estás interesado en otros datos de organización, puedes regresar a <http://www.data.gov> y buscar otros temas. Si buscas en Internet, podrás encontrar sitios web similares correspondientes a otros países. Por ejemplo:

Australia: <http://data.gov.au/>

Reino Unido: <http://data.gov.uk>

Canadá: <http://data.gc.ca>

→ Para ESPAÑA tenemos la misma iniciativa: <http://datos.gob.es>

g. ¿Qué conclusión sacas? Realiza una pequeña reflexión personal. ¿Crees que es importante o interesante tener acceso a este tipo de metadatos? Justifica tu reflexión.

Responde aquí

h. ¿Qué es un metadato?

Responde aquí

UD07: Redes mixtas Integradas

Parte 3: Visualización de datos

La visualización de datos puede ayudarte a interpretar listas de cifras y a exponerlas de un modo significativo. La visualización puede ayudarte a "ver" tendencias que podrían pasar desapercibidas de otro modo.

Diversos sitios web te proporcionan visualización de datos. Vamos a estudiar la visualización de datos con los gráficos que se proporcionan en estos dos sitios web: www.knoema.com y www.gapminder.org.

Paso 1: Navegar en knoema

En www.knoema.com puedes encontrar muchas formas de representar datos estadísticos gráficamente.

- a. Desplázate hacia abajo en la página de inicio. Verá una lista de distintos temas, como This Just In (Lo más reciente) y Viz of the day (Visualización del día). Desplácese hacia abajo por la página para ver muchos otros temas que puede consultar.



- b. ¿Cuál es el tema que aparece como de MAS ACTUALIDAD en el Banner negro superior? Explóralo.

UD07: Redes mixtas Integradas

Responde aquí

- c. ¿Cuáles son los temas de Visualización del día? (Aparecen como opciones en el buscador central)

Responde aquí

- d. Haz click en uno de los títulos y estudie los temas y los diferentes gráficos que se le presentan. Inserta uno de los gráficos que has podido visualizar.

Responde aquí

- e. En la parte superior de la página, haz click en Datos. Se abrirá una ventana desplegable. Haz click en Atlas Mundial de Datos. Desde aquí (o desde cualquier categoría), puedes estudiar la amplia variedad de datos disponibles.

UD07: Redes mixtas integradas



Paso 2: Navegar en Gapminder

La misión de la Fundación Gapminder es combatir el desconocimiento por medio de datos estadísticos recopilados de diversas fuentes. Como se generan visualizaciones de datos de excelente calidad y presentaciones animadas de datos, las estadísticas pasan a ser muy interesantes.

Vamos a visualizar los materiales gratuitos que se ofrecen en www.gapminder.org.

- Dirígete a www.gapminder.org.

Página 11 de 14

UD07: Redes mixtas integradas



- Haz clic en **Videos** (dentro del menú principal) para ver presentaciones en las que se corporizan datos estadísticos y se realiza su relevancia. Elige un vídeo que te interese. Haz una captura del vídeo que has elegido.

Inserta la captura aquí
- Para interactuar con los gráficos de burbuja que se presentan en algunos vídeos, haz clic en **Herramientas** (Herramienta Gapminder). Visualizarás un diagrama de burbujas como el siguiente. Vamos a centrarnos en España. Para ello debes Seleccionar en la ventana de la derecha únicamente a España (Spain). Aparecerá como un círculo amarillo, actualizado a 2019.

Página 12 de 14

UD07: Redes mixtas Integradas



- d. Ahora haz click en **Play** (Reproducir). Observa los cambios del gráfico de dispersión correspondientes a la tendencia entre **Life expectancy (years)** (Expectativa de vida [años]) e **Income per person** (Ingreso por persona). Cada una de estas burbujas representa el progreso de España en cada año. Es decir, como evoluciona España en la relación de años de vida frente a ingresos. Inserta una captura con el resultado final de la gráfica Gpmminder para España.

Inserta la captura aquí

¿Qué conclusión sacas de la evolución de España viendo esta representación de datos?

Responde aquí

Como puedes observar podemos visualizar en los ejes de la gráfica otros parámetros indicadores que nos interesen, y ver así qué evolución ha sucedido históricamente, por ejemplo. Además de visualizar estos mismos datos en otros países.

UD07: Redes mixtas Integradas

Reflexión

Acabamos de ver brevemente la visualización de datos ofrecida por diferentes sitios web. Elige el sitio web de visualización de datos que más te haya gustado y ejecuta el proceso. ¿Cuál de ellos?

Responde aquí

¿Has realizado alguna otra prueba de visualización además de la indicada en el enunciado de la práctica? ¿Cuál?

Responde aquí

UD07: Redes mixtas Integradas

PRÁCTICA 4

Examinar NAT y Resolver problemas de conexión

EXPLICACIÓN TEÓRICA

CURSO DE REDES DE ÁREA LOCAL
- UNIDAD 7 -
VIDEO INTRODUCTORIO A LA PRÁCTICA 4

¿QUÉ VAMOS A HACER EN ESTA PRÁCTICA?

- Examinar la configuración NAT en un router inalámbrico
- Configurar 4 PC para que se conecten a un router inalámbrico mediante DHCP
- Examinar el tráfico que atraviesa la red mediante NAT
- Por último, identificar y corregir un dispositivo inalámbrico configurado incorrectamente.

¿QUÉ NECESITAMOS PARA HACER LA PRÁCTICA?

1 PC con **PACKET TRACER** en la versión 7

¿QUÉ TENEMOS QUE ENTREGAR DE LA PRÁCTICA?

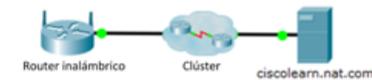
Este archivo Word completamente relleno, y el archivo *.pkt de configuración realizada.

Página 1 de 8

UD07: Redes mixtas Integradas

Part 1: Examinar NAT en un router inalámbrico.

Topología



Descarga en tu PC el archivo pkt con el nombre PRACTICA 4 PARTE 1

Paso 1: Vamos a examinar la configuración para acceder a la red externa.

- Haz clic en **Wireless Router** (Router inalámbrico). Haz clic en la ficha **GUI**.
- Haz clic en la opción de menú **Status** (Estado) en la esquina superior derecha, es la última opción. Cuando se selecciona, muestra la página de submenús (del router).
- Desplázate hacia abajo por la página del router hasta la opción de conexión a Internet. La dirección IP asignada aquí es la dirección asignada por el ISP (Proveedor de Servicios de Internet).

(Si no hay una dirección IP aparece 0.0.0.0, entonces debes cerrar la ventana, esperar unos segundos e inténtalo nuevamente. Así el router inalámbrico de nuevo realizará el proceso de obtener una dirección IP del servidor DHCP del ISP).

La dirección que se ve aquí es la dirección asignada al puerto de Internet en el router inalámbrico. Después de escuchar la teoría correspondiente a esta práctica ¿La dirección asignada es una dirección privada o una pública? Justifica tu respuesta indicando de qué Clase es y cuál es el rango en el que se encuentra. Recuerda que dentro de cada Clase de Red había unos rangos de direcciones que eran solamente de uso público o privado.

[Responde aquí]

Paso 2: Examina la configuración para acceder a la red interna como se indica paso a paso.

- Haz clic en **Local Network** (Red local) dentro de la barra de submenús Status (Estado). Es la siguiente opción de submenú a la trabajada en el paso 1.
- Desplázate hacia abajo para analizar la información de la red local. Esta es la dirección asignada a la red interna. Inserta a continuación una captura de esta ventana de configuración.

[Insértala aquí]

Página 2 de 8

UD07: Redes mixtas integradas

- c. Desplázate aún más abajo para examinar la información del servidor DHCP y el rango de direcciones IP que se pueden asignar a los hosts conectados.

¿Son direcciones privadas o públicas? Responde justificadamente igual que has hecho con la pregunta anterior.

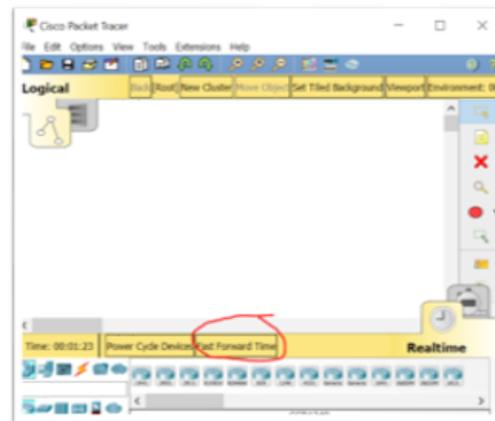
[Responde aquí]

- d. Cierra la ventana de configuración del router inalámbrico.

Paso 3: Ahora vamos a conectar 4 ordenadores al router inalámbrico.

- a. Agrega 4 PCs (el primero que aparece en la barra de dispositivos por defecto) y conéctalos al router inalámbrico con cables directos.

Espera a que todas las luces de enlace se vuelvan verdes antes de continuar con el siguiente paso o, si quieres acelerar que se pongan en verde, puedes hacer clic en **Fast Forward** (Adelantar).



Entra en la ventana de configuración de cada PC que has añadido, y haz clic en la pestaña **Desktop** (Escritorio).

Selecciona **IP Configuration**. Y aquí haz clic en **DHCP** a fin de habilitar cada dispositivo para que reciba una dirección IP mediante DHCP en el router inalámbrico.

UD07: Redes mixtas integradas

Cierra **IP Configuration** (Configuración IP) cuando termines.

- b. Ahora vamos a confirmar que la configuración de cada ordenador se ha realizado correctamente. Para ello entra de nuevo en la ventana de configuración de cada uno y haz clic en **Command Prompt** (Línea de comandos, cmd) para verificar la configuración IP de cada dispositivo utilizando el comando **ipconfig /all**. Inserta una captura del resultado de este comando para cada PC, esto es, 4 capturas.

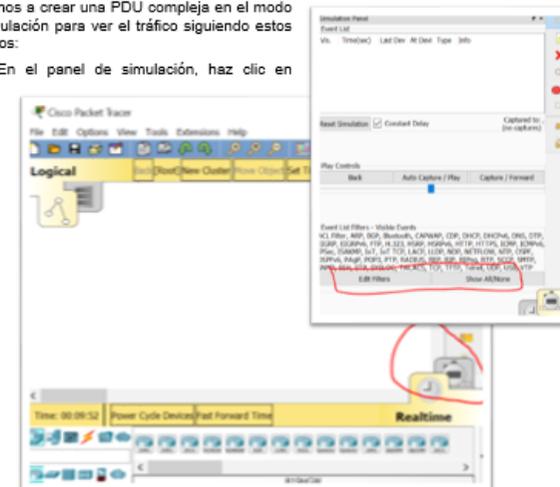
Atento: Estos dispositivos deben haber recibido una dirección privada. Es importante que recuerdes que las direcciones privadas no pueden atravesar Internet; por lo tanto, se debe realizar una traducción de NAT (protocolo de traducción de dirección privada a pública, en el router-gateway).

[Inserta las 4 capturas aquí]

Paso 4: Vamos a ver ahora la traducción NAT en el router inalámbrico.

- a. Entra al modo de simulación haciendo clic en la ficha **Simulation** (Simulación) en la esquina inferior derecha. La ficha Simulation se encuentra detrás de la ficha **Realtime** (Tiempo real) y tiene el símbolo de un cronómetro.

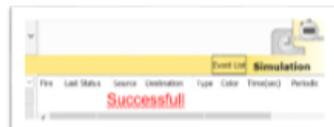
- b. Vamos a crear una PDU compleja en el modo Simulación para ver el tráfico siguiendo estos pasos:
 - 1) En el panel de simulación, haz clic en



UD07: Redes mixtas integradas

Show All/None (Mostrar todos/ninguno) para no ver ningún evento. Ahora haga clic en **Edit Filters** (Editar filtros) y en la ficha **Misc**, marque las casillas de TCP y HTTP.

- 2) Agrega una PDU complex (compleja) haciendo clic en el sobre abierto que se encuentra en la barra de herramientas de la derecha del Escritorio.
- 3) Después haz clic en una de las PC para especificarla como origen. Aparecerá entonces una ventana de selección de la PDU complex.
- c. Especifica la configuración de la PDU compleja cambiando lo siguiente en la ventana de la PDU compleja:
 - 1) En **PDU Settings** (Configuración de PDU) > **Select Application** (Seleccionar aplicación) debe ser: **HTTP**.
 - 2) Sin cerrar esta ventana, haz clic en el servidor **ciscolearn.nat.com** para que la ventana lo recoja como dispositivo de destino. Observarás que aparecerá ahora la dirección IP del servidor escrita.
 - 3) En **Starting Port** (Puerto de origen), introduce **1000**.
 - 4) Abajo, en **Simulation Settings** (Configuración de simulación), selecciona **Periodic** (Periódica). Introduce **120** segundos en **Interval** (Intervalo).
 - 5) Una vez todo especificado, haz clic en **Create PDU** (Crear PDU) en la ventana.
- d. Observa el flujo de tráfico haciendo clic en el botón **Auto Capture/Play** (Captura automática/reproducir) en el panel de simulación. Podemos acelerar la animación deslizando el control hacia la derecha.
- e. Una vez que aparezca en la ventana de resultados de Simulaciones (abajo a la derecha del escritorio de Packet Tracer) "Successful", podemos detener la simulación y pasar a analizar el resultado.



Paso 5: Vamos a analizar el resultado, viendo la información del encabezado de los paquetes que se han enviado con la simulación.

- a. Vamos a examinar los encabezados de los paquetes enviados entre una PC y el servidor web.
 - 1) En el panel de simulación, haz doble clic en la **tercera línea** hacia abajo en la lista de eventos, donde aparece cada uno de los protocolos utilizados en la comunicación. Aparecerá ahora la imagen de un sobre sobre algunos de los dispositivos de la red en el área de trabajo. Este sobre representa el segmento concreto de la comunicación en esa línea.

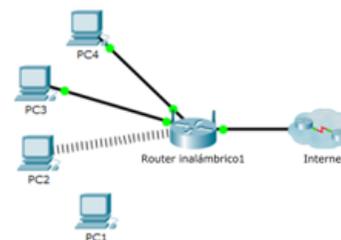
UD07: Redes mixtas integradas

- 2) Aparecerá también una ventana en el área de trabajo donde podemos ver la información del encabezado y el paquete.
 - b. Haz clic en una de las pestañas de detalles:
 - **Inbound PDU** (PDU entrante). Examina la información del paquete en busca de la dirección IP de origen (SRC) y la dirección IP de destino.
 - **Outbound PDU** (PDU saliente). Examina la información del paquete en busca de la dirección IP de origen (SRC) y la dirección IP de destino.
 Observa el cambio en la dirección IP SRC (dirección IP desde donde parte el mensaje). Haz captura de cada pestaña que aparezca en esta ventana de comunicación:

[Inserta las capturas aquí]

Part 2: Resolver problemas de una conexión inalámbrica.

Topología



Descarga en tu PC el archivo pkt con el nombre PRACTICA 4 PARTE 2

El propietario de una pequeña empresa se entera de que un usuario que se conecta de manera inalámbrica no puede tener acceso a la red. Todas las PC están configuradas con un direccionamiento IP estático. Identifique y corrija el problema.

UD07: Redes mixtas Integradas

Paso 1: Vamos a verificar la conectividad de cada ordenador.

Clicando en cada ordenador, abrimos la ventana de configuración. Entra en **Desktop > Web Browser** (Escritorio > Navegador web) en cada PC inalámbrica y escribe **www.cisco.pka** en la URL. Con ello identificamos cuales de las PC que no se pueden conectar con el servidor Web, porque aparece un mensaje de error.

Recuerda: Que todos los dispositivos requieren un tiempo para realizar el proceso de arranque. Deja pasar un tiempo para recibir una respuesta de la Web, es normal.

Tras realizar la prueba de conexión web, ¿Qué PC tiene problemas para conectarse al servidor Web?

[Responde aquí]

Este PC va a ser el objeto de nuestro estudio práctico, para ello vamos a ir revisando como técnicos que somos la configuración, tanto del PC como del router.

Paso 2: Primero vamos a examinar la configuración IP del ordenador.

a. En la PC que no se puede conectar, accede a **Command Prompt** (Línea de comandos) desde la pestaña **Desktop** (Escritorio) en la ventana de configuración.

b. Escribe el comando **ipconfig /all** e inserta una captura del resultado del mismo.

[Inserta la captura aquí]

c. ¿Observas algún dato extraño?

[Responde aquí]

Paso 3: En segundo lugar, vamos a examinar la configuración inalámbrica en el cliente inalámbrico.

a. En la ficha **Desktop** (Escritorio) del PC que no se puede conectar. Haz clic en **PC Wireless** (PC inalámbrica) para acceder a la configuración inalámbrica.

Haz clic en la ficha **Connect** (Conectar) y anota el SSID asociado. Escríbelo a continuación, recuerda que es muy importante distinguir mayúsculas y minúsculas.

[Responde aquí]

Cierra la ventana.

Paso 4: Por último, vamos a examinar la configuración inalámbrica en el router inalámbrico. Recuerda que estamos localizando dónde está el error por el que no conecta.

a. Accede al router inalámbrico introduciendo su IP desde el navegador web (Web Browser) de una **PC cableada**.

Utiliza el nombre de usuario **admin** y la contraseña **admin** para acceder al router inalámbrico.

¿Qué dirección IP has insertado en la URL? (Pista: debe ser la del gateway predeterminado).

UD07: Redes mixtas Integradas

[Responde aquí]

b. Ya dentro de la configuración del router, desde el navegador de este PC, en la página **Basic Setup** (Configuración básica), examina la configuración **DHCP Server Setting** (Configuración del servidor DHCP) y responde.

¿DHCP está habilitado?

[Responde aquí]

c. Haz clic ahora en la ficha **Wireless** (Inalámbrica).

d. Y examina la información de configuración en la ficha **Wireless**.

¿Cuál es el SSID? ¿Coincide con el SSID configurado en el cliente?

[Responde aquí]

e. Ahora haz clic en el submenú **Wireless Security** (Seguridad inalámbrica).

f. Y examina las configuraciones de seguridad.

¿Cuál es el modo de seguridad inalámbrica?

[Responde aquí]

¿Cuál es la frase de contraseña?

[Responde aquí]

Solo nos queda ahora realizar en el cliente los cambios necesarios. Paso 5.

UD07: Redes mixtas integradas

Paso 5: Haz los cambios de configuración necesarios en el cliente inalámbrico.

- a. En la ficha **Desktop** (Escritorio) del PC que no se puede conectar. Haz clic en **PC Wireless** (PC inalámbrica) para corregir las configuraciones inalámbricas.
- b. Haz clic en la ficha **Connect** (Conectar). Selecciona la red inalámbrica **Academy** y haz clic en **Connect** (Conectar).
- c. Introduce la frase de contraseña (clave compartida) registrada del router inalámbrico. Haz clic en **Connect** (Conectar). Inserta una captura de la Conexión ok.

[Inserta la captura aquí]

- d. Mediante **Web Browser** (Navegador web) dentro de la ficha **Desktop** (Escritorio), conéctate con **www.cisco.pka** para verificar que los cambios de configuración hayan resuelto el problema.

Inserta a continuación la ventana del Web Browser del PC donde se observa la ventana de configuración del router. Configuración remota.

[Inserta la captura aquí]

Recuerda compartir además de este Word completo, el archivo que has realizado en Packet Tracer (*.pkt)

UD07: Redes mixtas integradas

PRÁCTICA 5

IPv6

¿QUÉ VAMOS A HACER EN ESTA PRÁCTICA?

En esta actividad, vamos a practicar la configuración de direcciones IPv6 en un router, en servidores y en clientes. También verificaremos que lo que hemos configurado funciona.

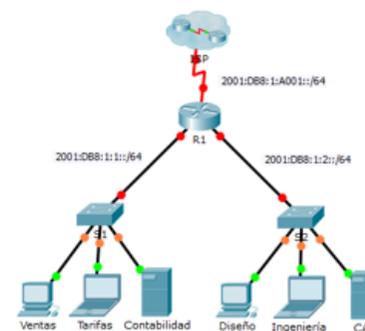
- Parte 1: Configurar el direccionamiento IPv6 en el **router** (mediante línea de comandos).
- Parte 2: Configurar el direccionamiento IPv6 en los **servidores** (utilizando ventana gráfica).
- Parte 3: Configurar el direccionamiento IPv6 en los **clientes** (utilizando ventana gráfica).
- Parte 4: Probar y verificar la conectividad de red

TABLA DE DIRECCIONAMIENTO IPv6

Dispositivo	Interfaz	Dirección/Prefijo IPv6	Gateway predeterminado
Router R1	G0/0	2001:DB8:1:1::1/64	N/D
	G0/1	2001:DB8:1:2::1/64	N/D
	S0/0/0	2001:DB8:1:A001::2/64	N/D
	Link-local	FE80::1	N/D
Ventas	NIC	2001:DB8:1:1::2/64	FE80::1
Tarifas	NIC	2001:DB8:1:1::3/64	FE80::1
Contabilidad	NIC	2001:DB8:1:1::4/64	FE80::1
Diseño	NIC	2001:DB8:1:2::2/64	FE80::1
Ingeniería	NIC	2001:DB8:1:2::3/64	FE80::1
CAD	NIC	2001:DB8:1:2::4/64	FE80::1

UD07: Redes mixtas integradas

TOPOLOGÍA



UD07: Redes mixtas integradas

Parte 1: Configurar el direccionamiento IPv6 en el router

Paso 1: Primero tendremos que habilitar el router para que pueda reenviar paquetes IPv6:

- Haz clic en el router **R1** y, a continuación, en la ficha CLI. Presione **Entrar**.
- Introduce el comando de configuración global ipv6 unicast-routing, tal y como lo tienes escrito a continuación. Este comando es el que **va a habilitar el router para que reenvie paquetes IPv6**. Este curso únicamente vamos a visualizar como funciona, pero el curso siguiente lo analizaremos con más detalle.

```
R1> enable para pasar del modo invitado al modo privilegiado
R1# configure terminal para entrar en modo configuración
R1 (config)# ipv6 unicast-routing habilitamos IPv6
R1 (config)# exit
R1# exit
R1>
```

Cierra la ventana. **ATENCIÓN:** Estos comandos utilizados para entrar y salir de los diferentes modos-niveles en un router son muy importantes y será necesario que los aprendas de memoria. Ten en cuenta que discrimina entre mayúsculas y minúsculas, y no debes confundirte al escribir cada comando.

Paso 2: Ahora vamos a configurar el direccionamiento IPv6 en la interfaz GigabitEthernet 0/0:

- De nuevo haz clic en el router **R1** y, a continuación, en la ficha CLI. Presione **Entrar**.
- Entra de nuevo en el modo EXEC privilegiado tal y como lo has hecho en el Paso 1:

```
R1> enable para pasar del modo invitado al modo privilegiado
R1#
```

- Vamos a introducir ahora los comandos necesarios para entrar al modo de configuración de la interfaz GigabitEthernet 0/0, para ello:

```
R1# configure terminal para entrar en modo configuración
R1 (config)# interface gigabitethernet 0/0 entramos así en la configuración de la interfaz
R1 (config-if)#
```

- Estando ya dentro de la configuración de la interfaz, vamos a configurar la dirección IPv6 de esta interfaz, con el siguiente comando:

```
R1 (config-if)# ipv6 address 2001:DB8:1:1::1/64 Introducimos la dirección de la interfaz
```

- Ahora configuramos la dirección IPv6 link-local con el siguiente comando:

UD07: Redes mixtas integradas

```
R1 (config-if)# ipv6 address FE80::1 link-local Introducimos la dirección de la link-local
```

- Una vez configurada completamente la interfaz, es necesario ACTIVARLA. Para ello, desde el punto donde estamos introducimos:

```
R1 (config-if)# no shutdown habilitamos la interfaz (ON)
R1 (config-if)# exit
R1 (config)# exit
R1#
```

Ahora ya tenemos esta interfaz del router completamente configurada y activada. Vamos a hacerlo ahora con la segunda interfaz (observa que el router del esquema tiene 3 conexiones, lo que significa que debe tener 3 interfaces distintas).

Puedes observar como el punto de esta interfaz del router ahora está en **verde**.

Paso 3: Vamos a configurar el direccionamiento IPv6 en la segunda interfaz del router: GigabitEthernet 0/1.

- Ahora ya de memoria, introduce los comandos necesarios para la entrar al modo de configuración de la interfaz **GigabitEthernet 0/1**. Recuerda que los comandos están en los pasos anteriores. Inserta aquí la captura con los comandos que has introducido.

```
R1> enable
R1# configure terminal
R1 (config)# interface gigabitethernet 0/1
R1 (config-if)#
```

- Una vez dentro de la configuración de la interface gigabitethernet 0/1, mira en la **tabla de direccionamiento** que aparece arriba en el enunciado para obtener la dirección IPv6 que debes configurar en esta interfaz. Escribe a continuación la dirección IPv6 de esta interfaz.

[Responde aquí]

- Con esta dirección IPv6, debemos configure la dirección IPv6 y la dirección link-local, y por último activar la interfaz. Para ello debes introducir las 3 líneas de comandos igual que has realizado con la interfaz del Paso 2, pero teniendo en cuenta que ahora tenemos otra IP para la interfaz (no para link-local, que es la misma para todos). Inserta a continuación la captura con los comandos que has introducido.

```
R1 (config-if)# ipv6 address 2001:DB8:1:2::1/64
R1 (config-if)# ipv6 address FE80::1 link-local
R1 (config-if)# no shutdown
R1 (config-if)# exit
R1 (config)# exit
R1#
```

UD07: Redes mixtas integradas

Paso 4: Nos falta todavía por configurar la IPv6 en la tercera interfaz Serial 0/0/0.

- Para ello, consultando la **tabla de direccionamiento** del enunciado, obtén la IPv6 para esta interfaz y sigue todos los pasos que hemos realizado tanto en la primera interfaz g0/0, como en la segunda interfaz g0/1.

Recuerda: entra en modo configuración, después en configuración de la interfaz, configura la dirección IPv6 de la interfaz y del link-local, y, por último, ACTIVA la interfaz.

Inserta a continuación una captura con todos los comandos que has introducido para la Configuración de esta interfaz. Ahora todos en una única captura.

[inserta aquí la captura]

Parte 2: Configurar el direccionamiento IPv6 en los servidores

Después de haber configurado el router, ahora vamos a proceder a configurar los servidores. Los servidores se pueden configurar directamente desde la ventana gráfica, esto es, desde Escritorio>Configuración de IP, y seleccionaremos la parte que corresponde a IPv6, algo que hasta ahora en clase no hemos utilizado.

Paso 1: Configurar el direccionamiento IPv6 en el Servidor de Contabilidad.

- Haz clic en el servidor llamado **Contabilidad** y, a continuación, en la pestaña **Desktop** (Escritorio) > **IP Configuration** (Configuración de IP).
- Vamos a escribir directamente la dirección **2001:DB8:1:1::4** con el prefijo **/64** en la sección de **dirección IPv6** (en la parte de debajo de la ventana).
- Recuerda que debes establecer la dirección **FE80::1** como la dirección del **gateway** para **IPv6**.

Inserta a continuación una captura de esta ventana de Configuración IP con todos los datos que has introducido.

[inserta aquí la captura]

Cierra la ventana. Te recomiendo que antes de continuar con la práctica revises que la Configuración que has realizado se ha quedado guardada.

Paso 2: Configurar el direccionamiento IPv6 en el Servidor CAD.

Repite todos los pasos que hemos realizado con el Servidor de Contabilidad para el Servidor llamado **CAD**. Será necesario que consultes la **tabla de direccionamiento** del enunciado para obtener la dirección IPv6 que corresponde a este Servidor.

Inserta a continuación una captura de esta ventana de Configuración IP con todos los datos que has introducido.

[inserta aquí la captura]

Cierra la ventana. Te recomiendo que antes de continuar con la práctica revises que la Configuración que has realizado se ha quedado guardada.

UD07: Redes mixtas integradas

Parte 3: Configurar el direccionamiento IPv6 en los clientes

Por último solo nos queda configurar los **CLIENTES**. Se configuran exactamente del mismo modo que hemos configurado los Servidores.

Paso 1: Configurar el direccionamiento IPv6 en los Clientes de Ventas y Tarifas.

- Haz clic en el Cliente llamado **Tarifas** y, a continuación, selecciona la ficha **Desktop** (Escritorio) > **IP Configuration** (Configuración de IP).
- Establece **2001:DB8:1:1::3** con el prefijo **/64** como la **dirección IPv6**.
- Establece la dirección **FE80::1** como el **gateway IPv6**. Inserta una captura de la ventana de Configuración que acabas de completar.

[inserta aquí la captura]

- Repite los pasos anteriores para configurar el Cliente **Ventas**. Recuerda que debes consultar la **tabla de direccionamiento** del enunciado para obtener la dirección IPv6. Inserta una captura de la ventana de Configuración que acabas de completar.

[inserta aquí la captura]

Paso 2: Solamente nos falta configurar el direccionamiento IPv6 en los Clientes de Ingeniería y Diseño.

- Haz clic en el Cliente llamado **Ingeniería** y, a continuación, selecciona la ficha **Desktop** (Escritorio) > **IP Configuration** (Configuración de IP).
- Establece **2001:DB8:1:2::3** con el prefijo **/64** como la **dirección IPv6**.
- Establece la dirección **FE80::1** como el **gateway IPv6**. Inserta una captura de la ventana de Configuración que acabas de completar.

[inserta aquí la captura]

- Repite los pasos anteriores para configurar el Cliente **Diseño**. Recuerda que debes consultar la **tabla de direccionamiento** del enunciado para obtener la dirección IPv6. Inserta una captura de la ventana de Configuración que acabas de completar.

[inserta aquí la captura]

UD07: Redes mixtas Integradas

Parte 4: Probar y verificar la conectividad de red

Paso 1: ¿Cómo podremos verificar que sí hay conectividad en la red? Vamos a tratar de acceder desde el navegador de uno de los clientes al servidor, siguiendo estos pasos:

- Haz clic en el **Ciente Ventas** y, a continuación, en la pestaña **Desktop** (Escritorio).
- Dentro de Desktop haz clic en **Web Browser** (Navegador web) y escribe la dirección IPv6 **2001:DB8:1:1::4** del Servidor Contabilidad en el cuadro de dirección URL. Luego haz clic en **Go** (Ir).
Debería aparecer el sitio web del Servidor **Contabilidad**. Haz una captura.
[Inserta aquí la captura]
- Estando en la misma ventana de Web Browser, ahora cambia la URL y escribe la dirección **2001:DB8:1:2::4** del Servidor CAD. Luego haz clic en **Go** (Ir).
Debería aparecer el sitio web del Servidor **CAD**. Haz una captura.
[Inserta aquí la captura]

UD07: Redes mixtas Integradas

Paso 2: Por último, vamos a hacer ping al ISP (Proveedor de Servicios de Internet).

- Abre una ventana de configuración de cualquier equipo Cliente haciendo clic sobre él.
- Haz clic en la ficha **Desktop** (Escritorio) > **Command Prompt** (Símbolo del sistema).
- Prueba la conectividad al **ISP** con el siguiente comando:

```
PC> ping 2001:DB8:1:A001::1
```

- Inserta una captura del resultado del ping, demostrando el ok de la Conectividad.
[Inserta aquí la captura]

8.7.4 Proyecto final de redes

PROYECTO DE REDES		Trabajo final
PROYECTO FINAL DE UNA RED DE ÁREA LOCAL		
Nombre y apellidos		
Breve descripción	Se realizará el diseño completo (físico y lógico) de una red de área local, siguiendo las especificaciones que se enuncian en el trabajo.	
Material necesario	Cuaderno de trabajo Bolígrafo y/o lápiz 1 PC con Packet Tracer	
Fuentes de información	Diapositivas de todo el curso de redes Explicaciones de clase	

PROYECTO DE REDES		Trabajo final
Objetivos		
<ul style="list-style-type: none"> ✓ Consolidar los contenidos vistos en el curso de Redes de Área Local. ✓ Aprender a configurar redes de ordenadores. ✓ Utilizar la herramienta Cisco Packet Tracer. ✓ Utilizar comandos de consola de IOS. ✓ Utilizar interfaces gráficas para la configuración. ✓ Disposiciones de configuraciones reales de ordenadores a pequeña y gran escala. 		
Introducción		
<p>Un Centro de estudios va a renovar o cambiar de ubicación los componentes de la instalación de red existente (routers, switches, puntos de acceso, servidores, patch panels, cables, ...) porque va a haber un rediseño del espacio de cara al próximo curso.</p> <p>Se precisa contratar una empresa especializada en la instalación de redes que permita que en un breve periodo de tiempo tener operativo todo el servicio de red. Para ello se convoca un concurso, en el cual las empresas tienen un periodo de tiempo para presentar el presupuesto-proyecto de cada empresa, que consistirá en lo siguiente: apoyándose en el plano que se facilita de las instalaciones se debe realizar un <u>mapa físico</u> y un <u>mapa lógico</u> de la red propuesta.</p>		

PROYECTO DE REDES Trabajo final

Preámbulo

En Packet Tracer se dibujará el mapa físico y lógico de la red sobre un plano:

- El **mapa físico** consiste en cómo se van a instalar físicamente todos los ordenadores, los equipos de interconexión de redes y todo el cableado.
- En el **mapa lógico** se debe reflejar el direccionamiento de la red (direcciones IP, puertas de enlace, ...).

El mapa físico se podrá dibujar sobre un plano buscado por el estudiante, sobre la imagen subida adjunta o sobre la imagen por defecto que tiene Packet- Tracer.

En caso de usar la imagen por defecto de Packet-Tracer, ésta será la propuesta de distribución de los elementos de la red:



PROYECTO DE REDES Trabajo final

Especificaciones

- La red está compuesta por tres subredes:
 - 192.168.0.0: recepción, dirección y CPD
 - 192.168.1.0: taller
 - 192.168.2.0: aula 1 y aula2.
- Las tres subredes están interconectadas a través de un **router 2620-XM** ubicado en el CPD.
- Los ordenadores de recepción y dirección serán inalámbricos y se conectarán a la red mediante un punto de acceso **AccessPoint-PT-A**
- Especificaciones **mapa físico** de la red:

Subred 192.168.1.0	<ul style="list-style-type: none"> ➤ 1 Switch 2950-24 ➤ 8 Laptop Ethernet (portátiles) en el taller
Subred 192.168.2.0	<ul style="list-style-type: none"> ➤ 1 Switch 2950-24 ➤ 4 Ordenadores Ethernet en Aula 1 ➤ 4 Ordenadores Ethernet en Aula 2
Subred 192.168.0.0	<ul style="list-style-type: none"> ➤ Recepción: 2 ordenadores con módulo Wireless PT-HOST-NM-1W-A ➤ Dirección: 2 ordenadores con módulo Wireless PT-HOST-NM-1W-A ➤ 1 AccessPoint-PT-A para los ordenadores de recepción y dirección. ➤ CPD: <ul style="list-style-type: none"> ○ 1 Servidor ○ 1 Switch 2950-24 ○ 1 Router 2620-XM que incluye módulo NM-4E para

PROYECTO DE REDES

Trabajo final

	<p>conectar a los 3 switches.</p> <ul style="list-style-type: none"> ➤ Los tres switches 2950-24 se conectan al router del CPD. ➤ El AccessPoint se conecta al switch del CPD.
--	--

- Especificaciones mapa lógico de la red:

Subred 192.168.1.0	<ul style="list-style-type: none"> ➤ IP estáticas a partir de 192.168.1.10
Subred 192.168.2.0	<ul style="list-style-type: none"> ➤ IP estáticas a partir de 192.168.2.10
Subred 192.168.0.0	<ul style="list-style-type: none"> ➤ Todas las estaciones con IP dinámica ➤ Servidor <ul style="list-style-type: none"> ○ IP estática 192.168.0.2 ○ Puerta enlace: 192.168.0.1 ○ Servicios habilitados y configurados: <ul style="list-style-type: none"> ▪ DHCP (primera IP asignada 192.168.0.100, máximo 50 usuarios) ▪ HTTP, DNS, FTP ➤ Router 2620-XM con puertas de enlace configuradas: <ul style="list-style-type: none"> ○ IP 192.168.0.1 hacia la red 192.168.0.0 ○ IP 192.168.1.1 hacia la red 192.168.1.0 ○ IP 192.168.2.1 hacia la red 192.168.2.0 ➤ AccessPoint-PT-A con: <ul style="list-style-type: none"> ○ protección WEP2 activada ○ SSID: CampusWifi

9 Bibliografía

Abad, A. (2012). *Redes Locales*. Madrid: McGraw-Hill Interamericana.

Cisco Packet Tracer. (2020). *Software simulador de redes*.
<https://www.netacad.com/courses/packet-tracer>

Cisco Learning Network. (13 de febrero de 2020). *Games Arcade*.
<https://learningnetwork.cisco.com/s/article/games-arcade>

Cisco Network Academy. (28 de julio de 2019). *CCNA R&S: Introduction to Networks v6*. Curso para instructores. <https://www.netacad.com/portal/learning>

Cisco Network Academy. (8 de septiembre de 2017). *Big Data & Analytics v2.01*. Curso para instructores. <https://www.netacad.com/portal/learning>

Cisco Network Academy. (22 de marzo de 2018). *Introduction to Cybersecurity v2.1*. Curso para instructores. <https://www.netacad.com/portal/learning>

Cisco Network Academy. (1 de septiembre de 2017). *Introduction to Packet Tracer v1.0*. Curso para instructores. <https://www.netacad.com/portal/learning>

Cisco Network Academy. (19 de diciembre de 2017). *IoT Fundamentals: Connecting Things v2.0*. Curso para instructores. <https://www.netacad.com/portal/learning>

Cisco Network Academy. (28 de marzo de 2017). *Networking Essentials v1*. Curso para instructores. <https://www.netacad.com/portal/learning>

Comer, D. E. (2009). *Computer networks and internets*. Upper Sandle River: Prentice Hall.

Coronel, M., y Curotto, M. (2008). La resolución de problemas como estrategia de enseñanza y aprendizaje. *Revista Electrónica de Enseñanza de las Ciencias*, 7(2), 464.

Gómez-Martín, M. A., Gómez-Martín, P. P., y González-Calero, P. A. (2004). Aprendizaje basado en juegos. *ICONO 14*, 2(4), 6.

Johnson, D., Johnson, R., y Holubec, E. (1994). El aprendizaje cooperativo en el aula. (G. Vitale, Trad.) Editorial Paidós.

Kahoot!. (2013). *Aplicación móvil educativa*. <https://create.kahoot.it>

- Kurose, J. F., y Ross, K. W. (2006). *Redes de computadores: un enfoque descendente basado en Internet*. Madrid: Pearson Educación.
- Molina, F. J. (2009). *Redes Locales*. Madrid: RA-MA.
- Serrano, E., M, R., y Russo, C. (1 de marzo de 2021). *Pildoras educativas como instrumento de enseñanza universitaria*. http://educacaoaberta.org/wpcontent/uploads/2017/07/IVWREA_serrano.pdf
- Stallings, W. (2004). *Comunicaciones y redes de computadores*. Madrid: Pearson Prentice Hall.
- Stallings, W. (2000). *Local and metropolitan area networks*. Upper Saddle River: Prentice Hall International.
- Tera Term. (2020). *Software emulador de terminal*. <https://g.co/kgs/PWmq9L>
- Valcárcel Pérez, M. V. (2009). Plan FIPRUMU VII. *La clase magistral*, 15. (U. d. Murcia, Ed.). https://www.um.es/c/document_library/get_file?uuid=6a9e9620-b306-42c8-91e5-cef7198d39e4&groupId=316845
- Valdivia, C. (2019). *Sistemas informáticos y redes locales*. Madrid: Paraninfo.
- Wireshark. (2020). *Software analizador de protocolos*. www.wireshark.org

10 Anexo: Presupuesto

En el presente apartado se encuentra el presupuesto del trabajo que se ha mostrado a lo largo del documento. Para ello, se mostrará un desglose del número de horas dedicadas a la creación de cada Unidad Didáctica, y se realizará una suma de dichos costes obteniendo el coste total que ha supuesto la creación de todos los contenidos técnicos expuestos.

Imputando un coste de 20€/hora, se muestra un desglose asociado a la creación de cada Unidad Didáctica en la Tabla 17, Tabla 18 y Tabla 19, respectivamente.

Tabla 17. Relación costes bloque de contenidos 1

Bloque de contenidos 1: Introducción a las redes locales.		
Unidades Didácticas	Coste temporal (h)	Coste (€)
UD01. Caracterización de redes locales	52	1040
UD02. Identificación de elementos y espacios físicos de una red local. Medios de transmisión	51	1020
Total bloque de contenidos 1	103	2060

Tabla 18. Relación costes bloque de contenidos 2

Bloque de contenidos 2: Instalación y configuración de las redes locales.		
Unidades Didácticas	Coste temporal (h)	Coste (€)
UD03. Instalación y configuración de los equipos de red	51	1020
UD04. Interconexión de equipos en redes locales (I). Dispositivos específicos de la red local	26	520
UD05. Interconexión de equipos en redes locales (II). Interconexión de redes	17	340
Total bloque de contenidos 2	94	1880

Tabla 19. Relación costes bloque de contenidos 3

Bloque de contenidos 3: Resolución de incidencias en redes locales.		
Unidades Didácticas	Coste temporal (h)	Coste (€)
UD06. Resolución de incidencias de una red de área local. Protección, vigilancia y soporte de redes	43	860
UD07. Redes mixtas integradas. Proyecto.	60	1200
Total bloque de contenidos 3	103	2060

Finalmente se resumen los costes totales para la realización de los contenidos técnicos en la Tabla 20.

Tabla 20. Relación costes totales

Desglose de costes totales		
Bloques de contenido	Coste temporal (h)	Coste (€)
Total bloque de contenidos 1	103	2060
Total bloque de contenidos 2	94	1880
Total bloque de contenidos 3	103	2060
Total costes	300	6000

Total costes	6.000 €
IVA (21%)	1.260 €
TOTAL PRESUPUESTO	7.260 €

Por tanto, la realización del trabajo supone un coste total de 7.260€