



Redes de computadoras un enfoque práctico

Walter Marcelo Fuertes Díaz

Redes de computadoras - Un enfoque práctico

Ing. Walter Marcelo Fuertes Díaz, Ph. D.

Primera edición electrónica: junio, 2022

ISBN: 978-9942-765-72-7

Revisión científica:

Jenny Gabriela Torres Olmedo, Ph. D.

Luis Patricio Tello Oquendo, Ph. D.

Universidad de las Fuerzas Armadas-ESPE

Crnl. de C.S.M. Víctor Villavicencio A., Ph. D.

Rector

Publicación autorizada por:

Comisión Editorial de la Universidad de las Fuerzas Armadas-ESPE

Tcrn. Edison Haro- Vicerrector de Investigación

Presidente

Corrección de estilo y diseño

Lcdo. Xavier Chinga

Imagen de cubierta: <https://acortar.link/YQIayF>

Derechos reservados. Se prohíbe la reproducción de esta obra por cualquier medio impreso, reprográfico o electrónico. El contenido, uso de fotografía, gráficos, cuadros, tablas, y referencias es de exclusiva responsabilidad de los autores.

Universidad de las Fuerzas Armadas-ESPE
Av. General Rumiñahui s/n, Sangolquí, Ecuador
www.espe.edu.ec

Los derechos de esta edición electrónica son de la Universidad de las Fuerzas Armadas-ESPE, para consulta de profesores y estudiantes de la universidad e investigadores en
www.repositorio.espe.edu.ec.



Reconocimiento
- No Comercial -
Sin obras derivadas
CC BY-NC-ND 4.0



Departamento de
Ciencias de La Computación

Redes de computadoras

Un enfoque práctico

Ing. Walter Marcelo Fuertes Díaz, PhD.



A mi amada esposa Silvia, y a mis queridos hijos Walter y Mateo;

A mi madre que está en el cielo;

A mi padre y hermanos.

A mis apreciados estudiantes de grado y posgrado.

Walter Marcelo Fuertes Díaz

wmfuertes@espe.edu.ec

Profesor investigador titular principal del Departamento de Ciencias de la Computación de la Universidad de Fuerzas Armadas “ESPE” de Sangolquí-Ecuador. Actualmente cumple la función de Director de la Unidad de Gestión de Investigación y Coordinador del Grupo de Investigación en Sistemas Distribuidos, Ciberseguridad y Contenido (RACKLY) de la misma universidad.

Se graduó como Ingeniero de Sistemas e Informática en la Escuela Politécnica del Ejército (ESPE). Luego, obtuvo su maestría en Informática, mención Redes en la Escuela Politécnica Nacional de Quito-Ecuador (EPN), su maestría en Docencia Universitaria en la ESPE y su grado de Doctor (PhD) con honores, en Ingeniería Informática y de Telecomunicación en la Escuela Politécnica Superior de Informática de la Universidad Autónoma de Madrid, España.

Desde el 2006 ha participado activamente en alrededor de 15 proyectos de investigación enfocados en la aplicación de las tecnologías de Virtualización, Sistemas Distribuidos, Evaluación de Prestaciones, Seguridades en sistemas Computacionales, Ciberseguridad, Analítica de datos, Inteligencia Artificial, Seguridad cognitiva, Internet de las Cosas, Inteligencia de Negocios y Video juegos educativos. Ha sido ponente en varios congresos nacionales e internacionales y ha escrito en revistas nacionales, internacionales y conferencias. Ha publicado más de 100 artículos técnicos científicos en diferentes países del mundo.

Índice

Prólogo.....	21
Capítulo I - Fundamentos de Redes de Computadoras.....	25
Introducción.....	27
Sistema de comunicación.....	28
Terminología utilizada.....	29
Organismos de normalización de redes.....	30
Beneficios del uso de redes de datos.....	32
Recursos complementarios.....	33
Actividad de aprendizaje.....	34
Autoevaluación Capítulo 1.....	34
Capítulo II - Tipos de Redes de Computadoras.....	37
Genealogía.....	39
Características diferenciadoras.....	42
Topologías de redes.....	43
Aplicaciones de redes de área personal, local y extendida.....	47
Internet, Intranet y Extranet.....	48
Recursos complementarios.....	49
Actividad de aprendizaje.....	49
Autoevaluación Capítulo 2.....	50
Capítulo III - Dispositivos de red.....	53
Introducción.....	55

Dispositivos.....	55
Dispositivos de carga física.....	55
Dispositivos de Capa de enlace de datos.....	58
Dispositivos de Capa de red.....	59
Dispositivos de capas superiores.....	61
Recursos complementarios.....	62
Actividad de aprendizaje.....	62
Autoevaluación Capítulo 3.....	63
Capítulo IV - Medios de transmisión.....	67
Introducción.....	69
Terminología utilizada.....	70
Medios físicos o guiados.....	71
Cable UTP (Unshielded Twisted Pair).....	71
Cable STP (Shielded Twisted Pair).....	72
Código de colores del cable par trenzado.....	73
Fibra óptica.....	75
Medios inalámbricos.....	77
Microondas terrestres.....	78
Microondas vía satélite.....	79
Ondas de radio.....	79
Infrarrojos.....	80
EIA/TIA 568 de Subsistema de Cableado estructurado.....	80
Recursos complementarios.....	81

Actividad de aprendizaje.....	81
Autoevaluación Capítulo 4.....	81
Capítulo V - Modelo OSI/ISO.....	85
Caracterización del modelo OSI.....	87
Análisis y funcionamiento capa por capa.....	89
Tipos de señales capa por capa.....	90
Señal analógica y señal digital.....	91
Tipos de dispositivos capa por capa.....	92
Protocolos capa por capa.....	93
Recursos complementarios.....	94
Actividad de aprendizaje.....	94
Autoevaluación Capítulo 5.....	95
Capítulo VI - Modelo de capas TCP/IP.....	97
Introducción.....	99
Caracterización del modelo TCP/IP.....	100
Análisis y funcionamiento capa por capa.....	100
Capa de acceso a la red.....	101
Capa de Red del modelo TCP/IP.....	102
Capa de Transporte (TCP).....	103
Capa de Aplicación.....	103
Comparación con el modelo OSI/ISO.....	104
Recursos complementarios.....	105
Actividad de aprendizaje.....	106

Autoevaluación Capítulo 6.....	107
Capítulo VII - Direccionamiento IP.....	111
Dirección IP, Definición.....	113
Caracterización del Direccionamiento IP.....	113
Formato de un Paquete IP.....	114
Redes Classful.....	116
Redes Classless.....	118
Herramientas para direccionamiento IP.....	118
Ejercicios de transformación de decimal a binarios y viceversa.....	119
Recursos complementarios.....	120
Actividad de aprendizaje.....	121
Autoevaluación Capítulo 7.....	121
Capítulo VIII - Subredes de Longitud Fija y Variable.....	125
Introducción.....	127
Subredes de longitud fija/variable.....	127
Caracterización de las Subredes.....	129
Cálculo de Redes de longitud fija y variable.....	131
Recursos complementarios.....	135
Actividad de aprendizaje.....	136
Autoevaluación Capítulo 8.....	137
Capítulo IX - Tecnologías Ethernet.....	141
Introducción.....	143

Terminología utilizada.....	144
Protocolo de subcapa de MAC para la Ethernet clásica.....	145
Tecnologías Ethernet.....	147
Fast Ethernet.....	148
Gigabit Ethernet.....	150
Variantes de la Ethernet.....	150
Recursos complementarios.....	152
Actividad de aprendizaje.....	152
Autoevaluación Capítulo 9.....	153
Capítulo X - Switching capa 2 y 3.....	157
Caracterización.....	159
Switch de capa 2.....	159
Switch de capa 3.....	160
Estructura.....	162
Ejemplos y marcas de switches.....	162
Aplicaciones.....	165
Protocolos.....	166
Protocolos para switch de Capa 2.....	166
Protocolos para switch de capa 3.....	167
Diferencias.....	168
Recursos complementarios.....	169
Actividad de aprendizaje.....	169
Autoevaluación Capítulo 10.....	170

Capítulo XI - Tecnologías para PAN Wi-Fi & Bluetooth 173

Introducción..... 175

Definición de PAN..... 175

Construcción de una PAN..... 176

Wi-Fi..... 177

Ventajas y desventajas..... 180

Bluetooth..... 180

Recursos complementarios..... 182

Actividad de aprendizaje..... 182

Autoevaluación Capítulo 11..... 183

Capítulo XII - Servicios de Red..... 187

Introducción..... 189

Servidores..... 189

 Servicio DHCP (Dynamic Host Configuration Protocol)..... 189

 Servidor DNS..... 190

 Servidor Web..... 192

 Servidor E-mail..... 194

Recursos complementarios..... 196

Actividad de aprendizaje..... 196

Autoevaluación Capítulo 12..... 197

Capítulo XIII - Tecnologías WAN..... 199

Introducción..... 201

Topologías WAN..... 203

Infraestructuras WAN públicas.....	205
Infraestructura de WAN.....	207
Estándares WAN.....	208
Capa física WAN.....	208
Recursos complementarios.....	209
Actividad de aprendizaje.....	210
Autoevaluación Capítulo 13.....	210
Capítulo XIV - Enrutamiento Estático y Dinámico.....	213
El enrutador (router).....	215
Enrutamiento estático.....	217
Enrutamiento dinámico.....	218
Protocolo de información de enrutamiento (RIP).....	219
Protocolo Abierto de ruta más corta primero (OSPF).....	221
Recursos complementarios.....	223
Actividad de aprendizaje 14.....	223
Autoevaluación Capítulo 14.....	224
Capítulo XV - Capa de Transporte.....	227
Introducción.....	229
Funciones de la capa de Transporte.....	231
Protocolos de la Capa de Transporte.....	233
Protocolo TCP.....	234
Protocolo UDP.....	235
Manejo de los números de Puertos lógicos.....	237

Recursos complementarios.....	238
Actividad de aprendizaje 15.....	239
Autoevaluación Capítulo 15.....	239
Capítulo XVI - Redes de Nueva Generación.....	243
Introducción.....	245
Características fundamentales de la NGN.....	245
Capacidades de la NGN.....	246
Arquitectura general de NGN.....	248
Protocolos NGN.....	249
Equipamiento y tipo de usuarios y servicios.....	250
Recursos complementarios.....	252
Actividad de aprendizaje 16.....	253
Autoevaluación Capítulo 16.....	253
Capítulo XVII - GNS3.....	257
¿Qué es GNS3?.....	259
Características fundamentales de GNS3.....	259
Máquinas virtuales en GNS3.....	265
Recursos complementarios.....	266
Actividad de aprendizaje 17.....	266
Autoevaluación Capítulo 17.....	267
Referencias.....	270

Índice de tablas

Tabla 1 Asignaciones para los conectores de par trenzado código EI/TIA 568B.....	72
Tabla 2 Nivel de categoría de desempeño del cable de par trenzado.....	74
Tabla 3 Capas del modelo OSI.....	90
Tabla 4 Variantes del estándar IEEE-802.3 Ethernet.....	151
Tabla 5 Comparativa de las variantes de los estándares de Ethernet.....	151
Tabla 6 Diferencias entre switch capa 2 y capa 3.....	168
Tabla 7 Alcance de las distintas clases de Bluetooth en base a la potencia de transmisión.....	181
Tabla 8 Alcance de las distintas clases de Bluetooth en base a la capacidad de un canal.....	181
Tabla 9 Tabla comparativa entre RIP versión 1 y RIP versión 2.....	220
Tabla 10 División de puertos (IANA).....	238
Tabla 11 Comparación entre GNS3 y Packet Tracer.....	260
Tabla 12 Requerimientos recomendados.....	261

Índice de figuras

Figura 1 <i>Las Redes de computadoras, sus elementos, usuarios y aplicaciones.....</i>	28
Figura 2 <i>Elementos de un sistema de comunicación básico.....</i>	29
Figura 3 <i>Algunos organismos de estandarización de redes.....</i>	31
Figura 4 <i>Configuración de una Red de área personal (PAN) con Wi-Fi.....</i>	39
Figura 5 <i>Red de área local (LAN).....</i>	40
Figura 6 <i>Red inalámbrica local (WLAN).....</i>	41
Figura 7 <i>Red de área metropolitana (MAN).....</i>	41
Figura 8 <i>Red de área amplia (WAN) - Internet.....</i>	42
Figura 9 <i>Topologías de redes.....</i>	44
Figura 10 <i>Topología física en estrella extendida.....</i>	45
Figura 11 <i>Topología física en estrella extendida.....</i>	45
Figura 12 <i>Topología Física en árbol.....</i>	46
Figura 13 <i>Topología lógica.....</i>	47
Figura 14 <i>Modelo OSI y los dispositivos de red.....</i>	55
Figura 15 <i>Repetidor.....</i>	56
Figura 16 <i>Hub.....</i>	56
Figura 17 <i>Módem.....</i>	57
Figura 18 <i>Códec.....</i>	57
Figura 19 <i>Access Point.....</i>	58
Figura 20 <i>Switch.....</i>	59

Figura 21 <i>Bridge/Puente</i>	59
Figura 22 <i>Router</i>	60
Figura 23 <i>Firewall</i>	61
Figura 24 <i>Proxy</i>	61
Figura 25 <i>Medios de transmisión</i>	69
Figura 26 <i>Cable de par trenzado</i>	72
Figura 27 <i>Cable STP</i>	72
Figura 28 <i>Asignación de pines para los conectores cable directo y cruzado</i>	74
Figura 29 <i>Cable de fibra óptica</i>	75
Figura 30 <i>Tipos de fibra óptica</i>	76
Figura 31 <i>Tipos de conectores</i>	77
Figura 32 <i>Comunicaciones de microonda y satelitales</i>	79
Figura 33 <i>Filosofía del funcionamiento del modelo ISO/OSI</i>	87
Figura 34 <i>Caracterización del modelo OSI y sus principales funciones</i>	89
Figura 35 <i>Tipos de señales en la Capa Física del modelo OSI</i>	91
Figura 36 <i>Dispositivos por capa del modelo OSI</i>	92
Figura 37 <i>Protocolos de comunicaciones capa por capa del modelo OSI</i>	93
Figura 38 <i>Modelo de Capas TCP/IP</i>	99
Figura 39 <i>Protocolos, servicios y aplicaciones del modelo TCP/IP capa por capa</i>	101
Figura 40 <i>Modelo de Capas TCP/IP y su relación con el modelo OSI</i>	105

Figura 41 <i>Diagrama de una red LAN</i>	114
Figura 42 <i>Formato de paquetes IP</i>	115
Figura 43 <i>Clases de Redes Classful</i>	117
Figura 44 <i>Características de las 5 Clases</i>	117
Figura 45 <i>Calculadora de Subredes IP</i>	119
Figura 46 <i>Subredes de longitud fija</i>	128
Figura 47 <i>Topología de ejemplo de VLSM</i>	129
Figura 48 <i>Validación de los resultados</i>	133
Figura 49 <i>Matriz de validación de los resultados obtenidos</i>	135
Figura 50 <i>Ethernet Conmutada</i>	143
Figura 51 <i>Trama Ethernet e IEEE 802.3</i>	146
Figura 52 <i>Ethernet Conmutada</i>	147
Figura 53 <i>Switch CISCO Catalyst 2960</i>	148
Figura 54 <i>Diagrama LAN con switches Fast Ethernet</i>	149
Figura 55 <i>Switch capa 2</i>	160
Figura 56 <i>Switch capa 3</i>	161
Figura 57 <i>Estructura externa de un switch</i>	162
Figura 58 <i>Switch Tplink Tl-sg2452 De 48 Puertos Gigabit Admin. Capa 2, capacidad de conmutación 104Gbps, gestionable y montable en Rack</i>	163
Figura 59 <i>Switch Tplink Tl-sg2428p 24 Puertos Gigabit Poe Admin Capa2</i>	164
Figura 60 <i>Switch Cisco 3650 24 Puertos Poe, 2 SFP+ Capa 3 con capacidad de 272 Gbps de conmutación, gestionable y montable en rack</i>	164

Figura 61 <i>Switch Gigabit Linksys 28 Puertos Administrable 2 SFP Capa 3, capacidad de conmutación de 65 Gbps, montable y gestionable.....</i>	164
Figura 62 <i>Switch Enlace de Datos.....</i>	165
Figura 63 <i>Enrutamiento en Switch Capa 3.....</i>	166
Figura 64 <i>Diagrama de una red PAN.....</i>	176
Figura 65 <i>WPAN mediante Bluetooth.....</i>	177
Figura 66 <i>WPAN mediante Bluetooth.....</i>	178
Figura 67 <i>Prestaciones de las distintas bandas de frecuencias de Wi-Fi.....</i>	179
Figura 68 <i>Funcionamiento de un servidor DHCP.....</i>	190
Figura 69 <i>Estructura jerárquica de DNS.....</i>	191
Figura 70 <i>Funcionamiento del servicio DNS.....</i>	192
Figura 71 <i>Funcionamiento de un servidor WEB.....</i>	193
Figura 72 <i>Envío de correo electrónico de cliente a servidor.....</i>	195
Figura 73 <i>Estructura y conformación de una Red WAN entre dos ciudades.....</i>	101
Figura 74 <i>Elementos y terminología WAN.....</i>	203
Figura 75 <i>Topología WAN punto a punto.....</i>	203
Figura 76 <i>Topología WAN Hub y Spoke.....</i>	204
Figura 77 <i>Topología de malla.....</i>	204
Figura 78 <i>Ejemplo de Topología DSL-WAN.....</i>	206
Figura 79 <i>Ilustración de una WAN privada que utiliza una línea arrendada.....</i>	207
Figura 80 <i>Arquitectura de un enrutador genérico.....</i>	215

Figura 81 Configuración de enrutamiento estático.....	218
Figura 82 Estructura jerárquica de los protocolos de enrutamiento dinámico.....	219
Figura 83 Comandos CISCO de configuración RIP versión 2.....	221
Figura 84 Tipos de routers OSPF.....	222
Figura 85 Modelo TCP/IP, Capa de transporte y comunicaciones entre dispositivos.....	230
Figura 86 Algunos de los servicios de la capa de transporte.....	231
Figura 87 Modelo TCP/IP, protocolos.....	233
Figura 88 Segmento TCP.....	234
Figura 89 Segmento UDP.....	235
Figura 90 UDP - Aplicaciones.....	236
Figura 91 Direccionamiento del puerto.....	237
Figura 92 Ejemplo ilustrativo de la convergencia.....	248
Figura 93 Arquitectura general de las redes de nueva generación.....	249
Figura 94 Arquitectura general de las redes de nueva generación.....	251
Figura 95 Logo GNS3.....	262
Figura 96 GNS3-Tipos de plataformas de descarga.....	262
Figura 97 Panel lateral de botones de GNS3.....	263
Figura 98 Proyecto en ejecución en GNS3.....	264
Figura 99 Ejecución de la topología de red simulada.....	265
Figura 100 GNS3 VM.....	266

Prólogo

Motivación

Hoy en día, dada la cantidad de información disponible al alcance de cada estudiante a través de Internet, acciones de cómo verificar una lección u obtener más información sobre un tema determinado está a veces a sólo unos clics de distancia. Sin embargo, la organización de la información en muchos de estos sitios web no es adecuada para que los estudiantes puedan aprender de ellos. Además, hay grandes diferencias en la calidad y la profundidad de la información disponible para los distintos temas.

Estudiantes de pregrado y posgrado, investigadores y profesionales del ámbito de las redes informáticas requieren a menudo una firme comprensión conceptual de sus fundamentos teóricos. Además de ello, requieren un enfoque práctico para afianzar los conceptos teóricos adquiridos y favorecer a la comprensión de los temas tratados. Muchas veces, los textos estándar de redes de computadoras prestan poca atención a las actividades de aprendizaje y autoevaluaciones, lo que hace que sea un reto asimilar la teoría en cuestión y valorar la retención del conocimiento.

Este libro aborda estos problemas, proporcionando una única fuente para aprender sobre las redes de computadoras desde un enfoque práctico. Asumiendo que sólo se dispone un conocimiento limitado de informática, el libro proporciona una introducción intuitiva pero rigurosa a una amplia gama de temas relacionados con redes de computadoras. Los temas se tratan con suficiente detalle para que el libro pueda servir como primera y última referencia.

En esta obra se presentará la evolución de las redes a través del tiempo para así comprender cuáles son sus características actuales y tener conocimiento fundamental que permita saber cómo serán en el futuro. Cada concepto del libro se describe proporcionando un ejemplo práctico cuidadosamente elegido y ofreciendo una actividad de autoevaluación para que lo realice el lector. Esta progresión está diseñada para profundizar gradualmente en la comprensión. Se pretende que el estudiante o el profesional puedan entender la esencia de un trabajo de investigación que utilice estos fundamentos teóricos.

Se debe notar que configurar una red es un trabajo que requiere contar con conocimientos teóricos y prácticos. Desde su diseño inicial, es importante tener en cuenta una serie de factores que harán que cumpla con su cometido, sin sufrir intermitencias ni ataques que la hagan inaccesible a los usuarios o que generen pérdida de información, dinero, productividad, inclusive repu-

tación. Las tecnologías de red son cada vez más complejas. Por ello, uno de los requisitos más importantes para asegurar el correcto funcionamiento y la prestación del servicio prometido a los usuarios exigentes es asegurarse de que la red sea robusta. Esto se puede conseguir apoyándose en su diseño y configuración de un modelo de simulación previo, que permita validar el funcionamiento de la red. Por lo tanto, en este libro también dedica actividades de aprendizaje práctico utilizando los simuladores Packet Tracert de la Academia de Networking de Cisco y el Graphic Network Simulation GNS3, para instruir en esta temática.

Objetivo

El objetivo de este libro es abordar los fundamentos, modelos de interconexión, las tecnologías de las redes de computadoras, dispositivos de networking, y el diseño jerárquico de las redes de computadoras, de forma tan clara y completa como sea posible a nivel de hardware y software. Se utiliza un enfoque práctico complementario para entender la naturaleza y las características de las redes modernas y se tratan las cuestiones de diseño y las tendencias actuales en el desarrollo de modelos de simulación de redes. La obra presenta recursos complementarios útiles en cada unidad tratada, además de actividades de aprendizaje y cuestionarios de autoevaluación para afianzar los conocimientos adquiridos.

¿A quién va dirigido este libro?

El libro está dirigido a investigadores, estudiantes de pregrado y postgrado y profesionales que deseen entender en profundidad el comportamiento de los protocolos y mecanismos de comunicación en las redes de computadoras desde un enfoque práctico. El mismo puede ser usado en asignaturas de pregrado y postgrado. Así mismo, puede ser de gran ayuda para aquellos estudiantes que estén desarrollando sus trabajos de titulación, trabajos de grado de maestría o tesis doctorales en esta área.

Estructura del Libro

Con la finalidad de cumplir con el objetivo planteado, el libro se encuentra estructurado de la siguiente forma.

El Capítulo 1 presenta los conceptos de redes y sistemas de comunicación, la terminología común utilizada, los organismos de estandarización, los beneficios y sus interacciones para comprender los fundamentos de las redes

de computadoras. Luego, en el Capítulo 2 se describen los tipos de redes de computadoras. Una descripción de los dispositivos de red para que pueda coexistir y funcionar se realiza en el Capítulo 3. En el Capítulo 4 se describen los medios de transmisión mediante los cuales un emisor y receptor logran comunicarse para enviar o recibir un mensaje en la red.

El modelo de interconexión de sistemas abiertos establecido por la Organización Internacional de Normalización es introducido en el Capítulo 5; este modelo permite la interconexión de equipos de usuario final y de sistemas de telecomunicaciones para que transmitan y reciban información que pueda ser procesada utilizando reglas de comunicación compatibles y estandarizadas (protocolos). Entonces, el modelo TCP/IP, que es una suite de protocolos de comunicación de red distribuido en cuatro capas, que permiten la transferencia de datos en redes, entre equipos informáticos e Internet y que ha permitido el desarrollo exponencial de los servicios de Internet se presenta en el Capítulo 6.

En el Capítulo 7 se explica el direccionamiento IP y sus características más relevantes. Las Subredes de Longitud Fija y Variable como un método para incrementar el espacio de direcciones IPv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento de una red interna mayor se estudian en el Capítulo 8. Luego, se describe la tecnología Ethernet que conecta tanto varios equipos de usuario final como dispositivos de networking mediante commutadores o concentradores vía cable que logran vincular el software y el hardware para transmitir/recibir datos en la red en el Capítulo 9.

El Switching de capa 2 y 3 para facilitar el intercambio de recursos e información al conectar todos los dispositivos, incluidas computadoras, impresoras y servidores, en una red doméstica o empresarial se desarrolla en el Capítulo 10. El Capítulo 11 describe las tecnologías para redes de área personal Wi-Fi & Bluetooth que ha provocado que los servicios y aplicaciones que en este tipo de redes se emplean, mejoren la vida de las personas. Los servicios de red que consisten en el proceso de comunicación entre varios usuarios de dispositivos finales o sistemas informáticos que están vinculados o conectados en red para intercambiar información y compartir recursos se detallan en el Capítulo 12.

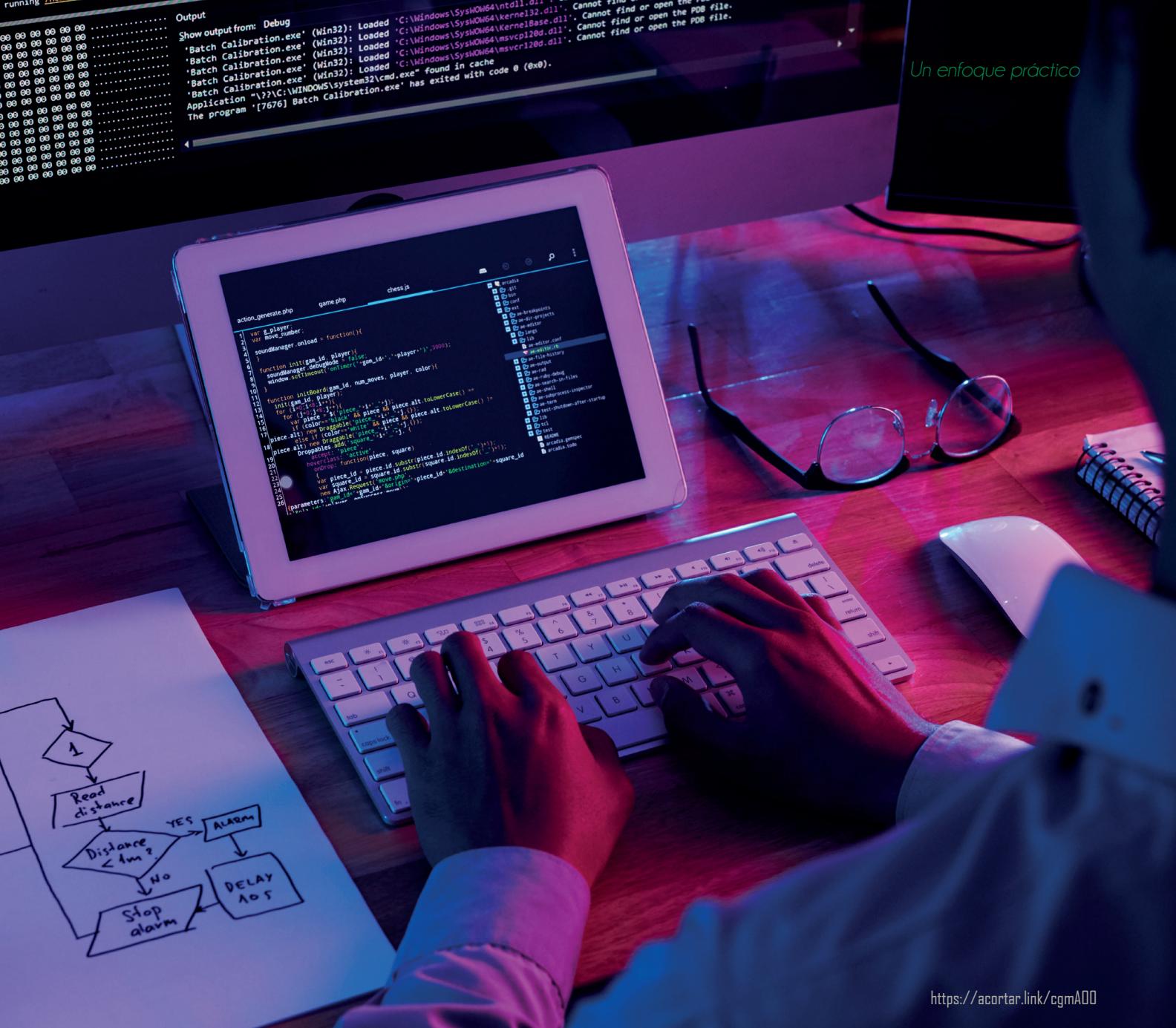
Mientras que, en el Capítulo 13, se estudia el funcionamiento, topología, tecnologías o protocolos y equipos que intervienen en la construcción de las redes de área extendida (Wide Area Network, WAN). El Capítulo 14 describe el enrutamiento estático y dinámico que son procesos para seleccionar la ruta óptima a través de una o más redes para conectarse a cualquier tipo de red de comunicaciones.

La capa de transporte, cuyo propósito es el de mantener la comunicación temporal de extremo a extremo con un nivel deseado de confiabilidad en una red de datos en las que se transmiten y reciben flujos de datos constantemente se detalla en el Capítulo 15. En el Capítulo 16 se estudian las redes de nueva generación, cuyo propósito es asegurar que todos los elementos necesarios para la interoperabilidad y las capacidades de red que soporten aplicaciones mundialmente, funcionen a través de una misma red manteniendo el concepto de separación entre transporte, servicios y aplicaciones. Finalmente, el Capítulo 17 describe GNS3 por sus siglas en inglés Graphic Network Simulation, o Simulación Gráfica de Redes que es un simulador de red gráfica multiplataforma, de código abierto muy útil para el diseño y pruebas de redes de computadoras desde la PC utilizando plataformas virtuales y software de monitoreo de redes.

Ing. Luis Tello-Oquendo, PhD.

Universidad Nacional de Chimborazo (luis.tello@unach.edu.ec)

lptelloq@ieee.org



CAPÍTULO I

Fundamentos de Redes de Computadoras

1.1 Introducción

Una red de computadoras o red de datos es un conjunto de dispositivos conectados a través de un medio de transmisión como cables de cobre, fibra óptica o a través del aire o el vacío (espectro electromagnético), e interconectados para transmitir y compartir información. Estos dispositivos pueden ser computadoras, impresoras, escáneres, cámaras de video, conmutadores, enrutadores, teléfonos celulares, entre otros.

El propósito de tener una red de datos es enviar y recibir datos almacenados en otros dispositivos a través de la red, sea de manera local o remota. Estos dispositivos a menudo se denominan nodos y pueden estar ubicados en casa, en una oficina, o en un edificio localizado en cualquier parte del mundo. No obstante, lo relevante de tener una red de datos es compartir recursos de hardware y software, lo que permiten disminuir los costos de inversión e incrementar la productividad de usuarios, empresas e industrias (Stallings, 2015).

Para que esto se logre, intervienen varios componentes, protocolos y estándares, que actúan según se encuentren organizados, distribuidos y conectados todos los dispositivos en una red, inclusive para obtener las máximas ventajas como un mejor tiempo de respuesta, seguridad y escalabilidad.

La magia de las redes de datos también se puede visualizar fácilmente en el aprovechamiento de los usuarios al utilizar los servicios y aplicaciones desde sus dispositivos móviles o equipos portátiles cuando se conectan a la red Internet. Aplicaciones y servicios como buscadores, redes sociales, mensajería instantánea (Google, WhatsApp, Facebook, Instagram, Twitter, YouTube, Gmail, Amazon Web Services, Spotify, etc.).

Internet es un conjunto descentralizado de redes de comunicaciones interconectadas universalmente, cuyo dominio es el ciber espacio, que se crea al conectar millones de usuarios alrededor de todo el mundo mediante sistemas de telecomunicaciones, redes de datos, y telefonía celular.

Entre los objetivos de aprendizaje que brinda este tema se pueden mencionar: conocer los conceptos de redes y sistemas de comunicación, la terminología común utilizada, los organismos de estandarización, los beneficios y sus interacciones para comprender los fundamentos de las redes. La Figura 1 ilustra varios elementos de las redes de datos, los usuarios, aplicaciones y su interrelación. Algunos componentes se explican a continuación:

Figura 1

Las Redes de computadoras, sus elementos, usuarios y aplicaciones.



Nota. La figura representa una abstracción del uso las redes de computadoras para el diario vivir. Obtenido de (Avantel, 2019).

1.2 Sistema de comunicación

Es el conjunto de actores, modos, medios y protocolos que interactúan entre sí para generar un sistema que hace posible la transmisión local o a distancia de todo tipo de datos. La Figura 2 ilustra el esquema más simple de un sistema de comunicación. Los elementos se explican a continuación:

El *transmisor/receptor* es un usuario que, utilizando un equipo conectado a una red, emite o recibe una señal eléctrica, código o mensaje a través de un medio de transmisión.

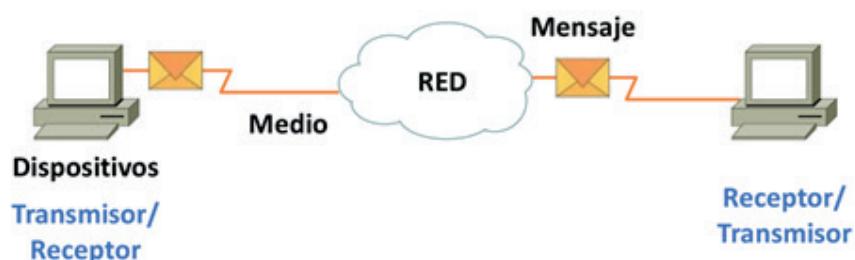
El *modo de transmisión* (o modo de comunicación) se refiere al mecanismo de transferencia de datos entre dos dispositivos conectados a través de una red. Estos modos dirigen la dirección del flujo de información. Existen tres tipos de modos de transmisión: modo simplex, semi dúplex, y dúplex completo.

Los *medios de transmisión* son un canal de comunicación que lleva la información del transmisor al receptor. Los datos se transmiten o transportan a través de señales electromagnéticas u ópticas, en forma de bits a través de una red. Algunos ejemplos: fibra óptica, cable de par trenzado, microondas, etc.

Un *protocolo de comunicaciones* es un mecanismo compuesto por reglas que permiten que dos o más dispositivos (computadoras, servidores, teléfonos celulares, conmutadores, etcétera) de un sistema de comunicación interactúen entre sí, para transmitir datos a través de cualquier medio de transmisión. Ejemplos: Ethernet, HTTP, UDP, etc.

Figura 2

Elementos de un sistema de comunicación básico



Nota. La ilustración es una representación visual de los elementos de un sistema de comunicación básico. Obtenido de: Cisco-NetAcad, "Redes de computadoras, Conceptos básicos y componentes de una Red", (Cisco, Capítulo 3, 2008)

1.3 Terminología utilizada

Para comprender de mejor manera el funcionamiento de las redes de computadoras, es primordial identificar los términos típicamente utilizados. A continuación, se los describe con una leve explicación:

- Transmisión de datos: es el proceso de transferencia de datos entre dos o más dispositivos que se encuentran conectados en la red. Los datos van ensamblados con señales de temporización generadas por un reloj interno que asegura que el transmisor y el receptor estén sincronizados.
- Topologías de red: es la forma en que los dispositivos y equipos de la red están organizados y conectados entre sí (topología física), y la forma de cómo se comunican entre sí (topología lógica).
- Dispositivos de red: consiste en varios tipos de equipos y dispositivos conectados en la red que interactúan en la transmisión de datos. Por ejemplo: computadoras, portátiles, servidores, adaptadores, dispositivos periféricos, enrutadores, puntos de acceso, etc.

- Servicios de red: se encargan de facilitar la comunicación entre dos o más usuarios de la red. Tienen el propósito de distribuir información de usuarios o empresas de manera local o remota, compartiendo recursos, ya sean hardware o software, como programas, aplicaciones, información, datos, archivos, entre otros. Ejemplos: web (HTTP, HTTPS), correo electrónico (SMTP, POP3, IMAP4), DNS, servicios de base de datos, etc.
- Sistema de cableado estructurado (SCE): es un sistema completo de cableado y hardware asociado, instalado en base a normas internacionales aceptadas por organismos de normalización, que proporciona una infraestructura de telecomunicaciones integral. Esta infraestructura sirve para la transmisión y recepción de señales de telecomunicaciones por el mismo medio de transmisión tales como: voz, datos, video, y control (sensores). El SCE es instalado para una amplia gama de usos, como el servicio telefónico digital y la transmisión de datos a través de una red informática, transmisión de video bajo demanda, comunicación local o remota, etc. El estándar EIA/TIA 568 especifica los requerimientos mínimos para el cableado de edificios comerciales tales como topologías, distancias, subsistemas, etc.
- Simulador de red: es un programa de software que permite a estudiantes y profesionales diseñar topologías y configurar equipos y servicios de red. El simulador permite reproducir las características físicas (medios de transmisión, dispositivos activos y pasivos, velocidad de transmisión, topología) y el comportamiento lógico de los equipos y dispositivos de red (servicios, direccionamiento IP, tecnologías de red, etcétera) que componen la red y que funcionarían en conjunto como si fuera una red real.

1.4 Organismos de normalización de redes

Son organismos reguladores oficiales formados por consultores independientes integrantes de los departamentos o secretarías de Estado de diferentes países y otros miembros del mundo. Estos organismos establecen estándares, normas, acuerdos y recomendaciones técnicas que regulan sistemas de transmisión de datos para que sean totalmente compatibles a nivel global utilizando la misma tecnología. Un estándar puede definir el tipo de conector, cantidad de ruido, latencia, formato de los datos, distancias, etcétera. La Figura 3, muestra algunos de ellos. Los más utilizados en redes de computadoras se describen a continuación.

Figura 3

Algunos organismos de estandarización de redes



Nota. La figura muestra algunos de los organismos de normalización que generan estándares para redes

- **ITU (International Telecommunications Union):** Su oficina principal está en Ginebra, Suiza, con 191 Estados miembros y más de 700 socios de la industria. Se centra en las tecnologías de la información y las comunicaciones, el desarrollo de redes y servicios que coordinen el uso del espectro radioeléctrico. La ITU trabaja para mejorar las infraestructuras de comunicación global, estableciendo estándares mundiales para la interconexión de sistemas de comunicación y seguridad en el ciberespacio (Comer, 2014).
- **ISO (International Organization for Standardization):** Es una organización internacional no gubernamental sin fines de lucro con sede en Ginebra (Suiza) con más de 100 países en todo el mundo. Su propósito es desarrollar una amplia gama de estándares de diferentes temas en los que destacan las arquitecturas de comunicación para la interconexión de sistemas abiertos (OSI - Open Systems Interconnection), modelo académico más utilizado en la transmisión de datos.
- **IEEE (Institute of Electrical and Electronic Engineers):** es una asociación de profesionales enfocados en la innovación tecnológica en beneficio de la humanidad. IEEE lidera una comunidad global que innova a

través de publicaciones de alto impacto, conferencias, estándares tecnológicos y actividades profesionales y educativas. Fue fundada en 1884 y desarrolla estándares y protocolos de comunicación para redes eléctricas, electrónicas y de transmisión de datos.

- **IETF (Internet Engineering Task Force):** Es una organización internacional abierta, sin fines de lucro, integrada por investigadores en el área de redes, que tiene como objetivo contribuir a la ingeniería de Internet y sus protocolos, actuando en diversas áreas, como transporte, enruteamiento y seguridad. Fue creado en los EE.UU., en 1986 y es conocido mundialmente por regular las propuestas y estándares del funcionamiento de Internet, conocidos como RFC (Request for Comments).
- **ANSI (American National Standards Institute):** Organización que define los estándares de fabricación de productos de los Estados Unidos para que otros fabricantes puedan utilizarlos de diferentes países. Es una organización sin fines de lucro encargada de supervisar el desarrollo de estándares para servicios, productos, procesos y sistemas aplicados en este país y el mundo. Es parte de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

1.5 Beneficios del uso de redes de datos

Las redes informáticas son un conjunto de equipos interconectados de forma local o remota, cuyo funcionamiento permite compartir recursos como impresoras, escáneres, archivos o aplicaciones y servicios para que sus usuarios puedan intercambiar información y facilitar la comunicación entre ellos (Meyers, 2009). Aunque sus beneficios son innumerables, a continuación, se listan los relevantes:

- Facilita la comunicación local o remota.
- Mejora la distribución de la información local o remota.
- Permite compartir recursos de hardware, discos, impresoras, archivos, dispositivos de conexión.
- Facilita compartir recursos de software, aplicaciones y servicios.
- Permite la transmisión o recepción de la información a altas velocidades, lo cual podría variar según el tipo de red, de medio de transmisión y la distancia.

- Facilita la administración y mantenimiento de puntos de red, usuarios, aplicaciones y servicios.
- Posibilidad de garantizar la seguridad de datos y aplicaciones.
- Posibilidad de ofrecer productos y servicios para la comercialización entre clientes y empresas utilizando aplicaciones y servicios Web.
- Ofrece la posibilidad de analizar el tráfico y monitorizar a los usuarios, inclusive para restringir o permitir diversas funciones inherentes.
- Posibilidad de trabajar desde cualquier ubicación geográfica mediante teletrabajo, teleeducación, o la telemedicina (Tanembaum, 2012).
- Facilita el trabajo en forma colaborativa, sea síncrona o asíncrona.
- Facilita utilizar las aplicaciones y servicios que se desarrollan en el Internet.
- Permite el ahorro de inversión e incrementa la productividad.
- Facilita el entrenamiento, así como el entretenimiento en casa por el sin número de aplicaciones en la Web (Netflix, YouTube, video juegos, etc.).

Recursos complementarios

A continuación, se pone a disposición los links para distinto material audiovisual:

- Video sobre “Micro aprendizaje: ¿Qué es una red informática?” 
- Video sobre: “Origen y evolución de las redes” 
- Video sobre “Redes Informáticas. Definición y clasificación” 
- Video sobre: “Historia de Internet (Ilustrado) Sena 2014” 
- Video sobre: “Organismos de Estandarización” 
- Presentación en PDF de Cisco NetAcad sobre: “Capítulo 3: Protocolos y comunicaciones de red” 
- Video sobre: “Sistemas de Cableado estructurado” 
- Video sobre: “Técnicas de transmisión serial y paralelo” 

Actividad de aprendizaje 1

Descripción de la actividad

Desarrolle una práctica de laboratorio en la que pruebe los siguientes comandos básicos de redes Windows desde su computador personal que debe estar conectado al Internet.

Los comandos a ejecutar son los siguientes: ipconfig, ping, tracert, route print, nslookup, dig, host, winMtr, arp, pathping, y getmac.

Se pide: Elabore un informe de laboratorio con la siguiente estructura: Tema, Objetivos de aprendizaje, Topología de prueba en la que se incluya materiales y equipos, Marco teórico, Desarrollo de la práctica, Conclusiones y Referencias bibliográficas.

Autoevaluación Capítulo 1

1. ¿Qué es un modo de transmisión?

Es un canal de comunicación que lleva información del transmisor al receptor

Es el mecanismo de transferencia de datos entre dos dispositivos

Es el mecanismo que permite que dos o más dispositivos interactúen entre sí

2. La forma en que los dispositivos y equipos de red están organizados y conectados entre sí se denomina:

Topología de red

Topología física

Topología lógica

3. Los _____ se encargan de facilitar la comunicación entre dos o más usuarios de la red.

Servicios de red

Dispositivos de red

Simuladores de red

4. El Internet está definido como:

Redes de comunicaciones conectadas localmente

Redes de comunicaciones conectadas universalmente

Redes de comunicaciones interconectadas universalmente

5. La IETF es una organización internacional abierta, ¿cuál es su objetivo?

Desarrollar estándares y protocolos de comunicación para redes eléctricas, electrónicas y de transmisión de datos

Contribuir a la ingeniería de Internet y sus protocolos

Supervisar el desarrollo de estándares para servicios, productos, procesos y sistemas aplicados en el mundo

6. Los nodos dentro de las redes de datos permiten:

Enviar y recibir datos almacenados en otros dispositivos a través de la red de forma local o remota

Enviar datos almacenados en otros dispositivos a través de la red de forma local o remota

Recibir datos almacenados en otros dispositivos a través de la red de forma local

7. ¿Cuál es el dominio de las redes de comunicaciones?

El universo

El espacio

El ciber espacio

8. ¿Cómo se denomina al mecanismo que permite que dos o más dispositivos interactúen entre sí?

Medios de transmisión

Protocolo de transmisión

Protocolo de comunicaciones

9. La organización ANSI se encarga de supervisar el desarrollo de estándares para servicios, productos, procesos y sistemas, forma parte de las organizaciones:

IEC y IEEE

IEFT e ITU

ISO y IEC

Ninguna respuesta es correcta

10. ¿Cuál de los siguientes son beneficios del uso de redes de datos?

Mejora la distribución de la información local o remota

Facilita la comunicación local o remota

Permite el ahorro de inversión en hardware y software e incrementa la productividad



<https://acortar.link/kFZOPS>

CAPÍTULO II

Tipos de Redes de Computadoras

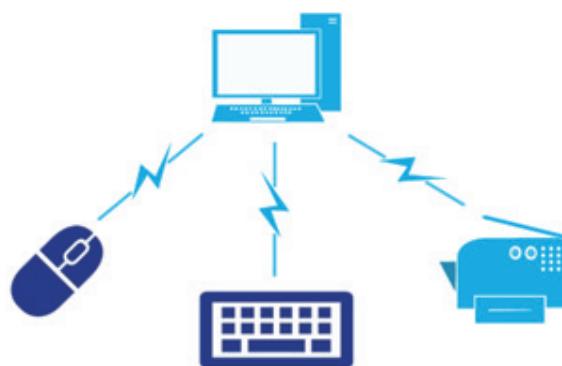
2.1 Genealogía

Como lo señala (Sathyaranayanan, 2020) una red informática conecta equipos computacionales para compartir información, chats, videoconferencias, llamadas de voz, etc. Los equipos están conectados a dispositivos de red como conmutadores (switches), enruteadores (routers) y tarjetas de interfaz de red (NIC, Network Interface Card) a través de medios de transmisión como cableados (coaxial, fibra óptica, UTP) e inalámbricos (antena, Wi-Fi). Las redes son la columna vertebral de la evolución de la tecnología de la información. En el mundo digital, desempeñan un papel importante en la conexión de todo dispositivo incluidos equipos, máquinas, dispositivos, equipos y objetos en movimiento. Las redes se pueden clasificar de acuerdo con su tamaño y propósito. El tamaño de la red incluye el rango geográfico y la cantidad de computadoras conectadas. Las redes se clasifican en:

- **PAN (Personal Area Network):** Según (Jovanov, 2001), una PAN, es una conexión directa de equipos de usuario final. Es decir, se define como una red informática que se utiliza para conectar y transmitir datos entre dispositivos ubicados en un área personal. Entre las tecnologías para PAN más conocidas están el Bluetooth (IEEE 802.15) y Wi-Fi (IEEE 802.11) para interconectar dispositivos que deben estar dentro del rango de una persona. Es decir, menor a diez metros, además, operan a velocidades entre 1 Mbps a 200 Mbps (ver Figura 4).

Figura 4

Configuración de una Red de área personal (PAN) con Wi-Fi

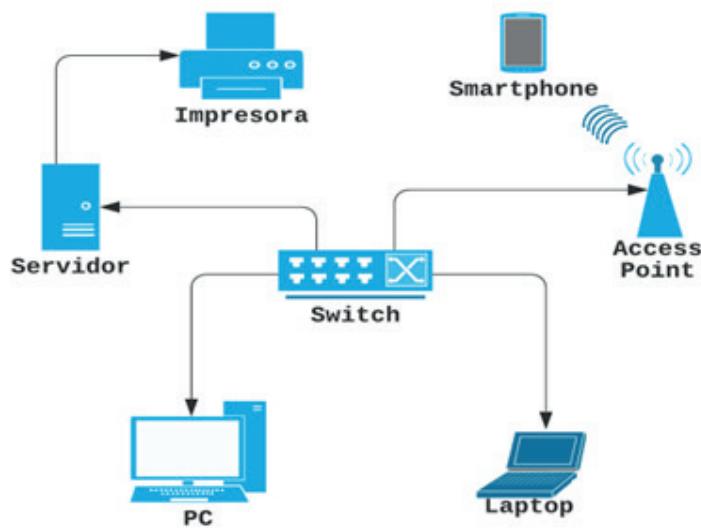


Nota. La ilustración es una representación visual de la configuración de una PAN con Wi-Fi.

- **LAN (Local Area Network):** son redes de propiedad privada que conectan dos o más computadoras en un área local con el propósito de compartir recursos e información. Operan a velocidades que van desde los 10, 100 y 1000 Mbps, 1 Gbps, 10 Gbps o más. La Figura 5 ilustra una configuración básica de una red LAN.

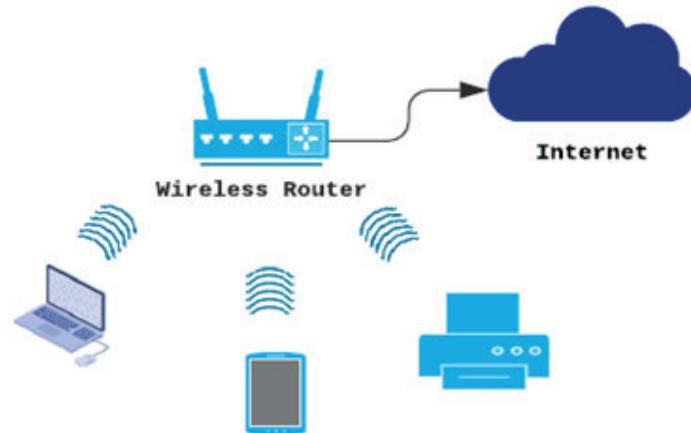
Figura 5

Red de área local (LAN)



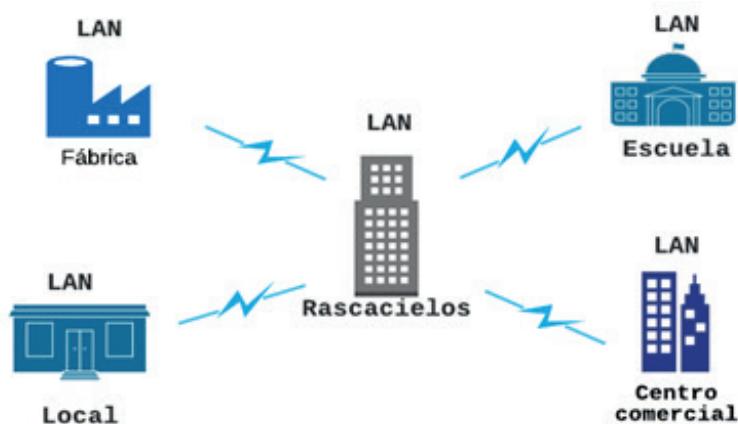
Nota. La figura es una representación visual de una LAN.

- **WLAN (Wireless Local Area Network):** Es otra LAN, en la cual no se hace uso de cables. El medio de transmisión es el aire o el de ondas electromagnéticas o radioeléctricas (i.e., aquellas ondas fijadas convencionalmente por debajo de 3000 GHz). El punto central de conexión es el punto de acceso inalámbrico (Access Point, AP) o un enrutador inalámbrico que repite las señales de radio a los dispositivos cercanos que están dentro de la cobertura local (tecnología WIFI, Wireless Fidelity). Las WLAN están diseñadas para proporcionar acceso inalámbrico en zonas de hasta 100 metros y se utiliza principalmente en el hogar, la escuela o entornos de oficina. El estándar que maneja es el IEEE 802.11x que ofrece una velocidad mínima de 11 Mbps, con posibilidades de 54, 100, 200 Mbps hasta 600 Mbps (en teoría). Sin embargo, su desempeño se ve reducida cuando hay interferencias electromagnéticas (EMI) y de radio frecuencia (RFI) e inclusive por condiciones medio ambientales. La Figura 6 ilustra un esquema de una WLAN en el hogar (Salazar, 2017).

Figura 6*Red inalámbrica local (WLAN)*

Nota. La figura representa un esquema del uso de una WLAN.

- **MAN (Metropolitan Area Network):** Una red MAN integra múltiples LAN dentro de una ciudad, en una red más grande. Las velocidades de transmisión de datos de MAN son más rápidas que las de LAN y WAN. La razón de la existencia de MAN es la necesidad de compartir y acceder a los recursos de una ciudad. Una red MAN representa un grupo de LANs interconectadas dentro del límite geográfico de un pueblo o ciudad. (Odom, 2016). La Figura 7 ilustra cómo en una ciudad por ejemplo se conectan redes de área local de una fábrica, de una escuela, de un centro comercial, e inclusive de una casa.

Figura 7*Red de área metropolitana (MAN)*

Nota. La figura representa un esquema de una MAN.

- **WAN (Wide Area Network):** Es una red informática que cubre una amplia área geográfica, por lo general un país o continente, al utilizar líneas de telecomunicaciones dedicadas tales como como líneas telefónicas, líneas arrendadas o vía satélite. En general las WAN son redes que tienen un gran alcance en su señal, es decir las WAN están compuestas por redes PAN, LAN y MAN. La Figura 8 ilustra el mejor ejemplo de una WAN (Odom, 2016).

Figura 8

Red de área amplia (WAN) - Internet



Nota. La figura representa una abstracción de una WAN. Fuente: “¿Qué son las WAN y hacia dónde se dirigen?”, (NOW, 2018)

2.2 Características diferenciadoras

Las características que ofrece cada tipo de red son distintas y semejantes. En apartados anteriores se ha explicado que existen diferentes factores como la distancia, el tipo de dato, los equipos, los servicios que influyen en su rendimiento (velocidad de transmisión y recepción) y niveles de seguridad. Algunos distintivos son las siguientes:

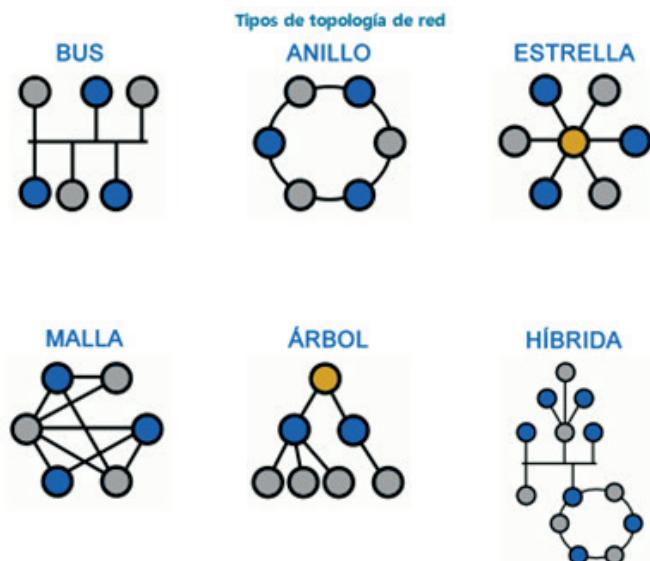
- La red PAN otorga la manipulación de la interconexión de dispositivos TI en el entorno de uno o más usuarios ubicados en lugares muy cercanos y a bajas velocidades de transmisión.
- La WAN es útil para que los proveedores de Internet puedan brindar conexión de redes y servicios de valor agregado de una zona muy amplia a sus clientes.
- La red MAN proporciona un excelente soporte para una red de gran tamaño, mayores velocidades de transmisión y un mayor acceso a las WAN.
- El desempeño de la red hace referencia a la rapidez con la que se transmiten los datos por segundo a través de la red y el tiempo de respuesta para enviar y recibir datos de un nodo a otro en una WAN (192 Kbps, 256 Kbps, 512Kbps, 1024, 2048, 4096Mbps) es siempre menor al rendimiento en una LAN que puede llegar a 10, 100,1000,10000 Mbps.
- Intercambio de datos: una de las razones por las que utilizamos una red informática es para compartir los datos entre diferentes sistemas conectados entre sí a través de un medio de transmisión.
- Una red de computadoras debe ser escalable, lo que significa que siempre debe permitirse agregar nuevas computadoras a la red ya existente.

2.3 Topologías de redes

Otra forma de categorizar las redes de computadoras es por su **topología**, o la forma en que los hosts y los nodos están organizados y conectados entre sí, y cómo se comunican entre ellos. Existen dos topologías: **física** y **lógica**.

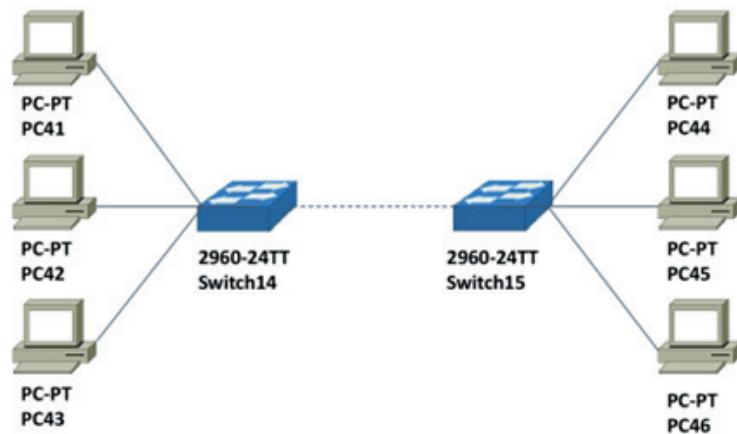
La **topología física** presenta el orden, la disposición y la ubicación de las partes físicas de una red informática, como computadoras, dispositivos periféricos, cables para la transmisión de datos y dispositivos de networking. De acuerdo con la academia de networking de Cisco, la topología física se refiere a las conexiones mediante las cuales se interconectan los dispositivos finales y de infraestructura, como los enrutadores, los conmutadores y los puntos de acceso inalámbrico. Generalmente estas topologías son punto a punto o en estrella. La Figura 9, ilustra algunas de las topologías usadas o no. A continuación, se los describe con una breve explicación:

Figura 9
Topologías de redes

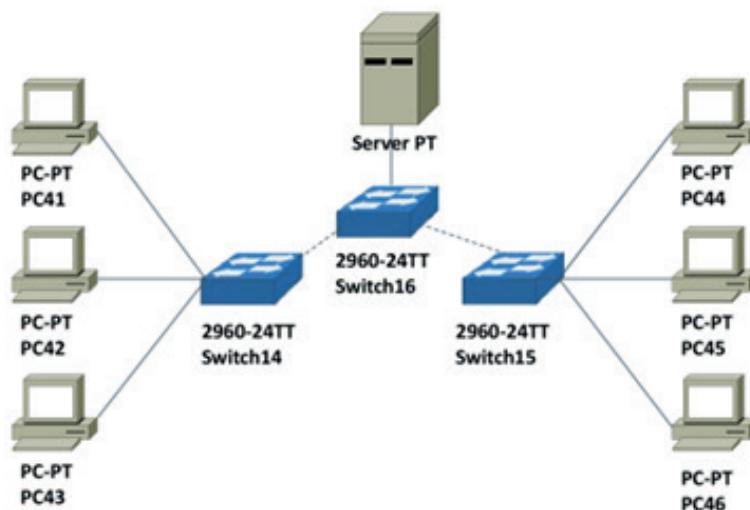


Nota. La figura muestra algunas de las topologías de red. Fuente: Redes y sus clasificaciones”, (Netink, 2020).

- **Bus:** las computadoras, periféricos y dispositivos de red se conectan a través del bus que consiste principalmente en un cable coaxial (ver Figura 9 - Bus) (Odom, 2016).
- **Anillo:** las computadoras, los periféricos y los dispositivos de red forman un ciclo cerrado que toma la forma de un anillo donde cada dispositivo está conectado entre sí (ver Figura 9- Anillo). En el pasado se usaba el cable coaxial, pero hoy en día en las redes de doble anillo se usa la fibra óptica (Odom, 2016).
- **Estrella:** las computadoras, periféricos y dispositivos de red están conectados de forma independiente con un dispositivo central (ver Figura 9- Estrella) conocido como concentrador (hub, switch, comutador). Para este tipo de topología se utiliza principalmente un cable de par trenzado o una fibra óptica (Odom, 2016).
- **Estrella extendida:** las computadoras, periféricos y dispositivos de red están conectados en dos o más redes de topología en estrella cuyos componentes centrales (es decir, los switches) se interconectan a través de un bus. En apariencia, este tipo de topología combina estrella y bus, la Figura 10 muestra una topología estrella extendida. Principalmente, se usa un par de cables trenzados para la topología en estrella, mientras que para la topología de bus se usa una fibra óptica (Odom, 2016).

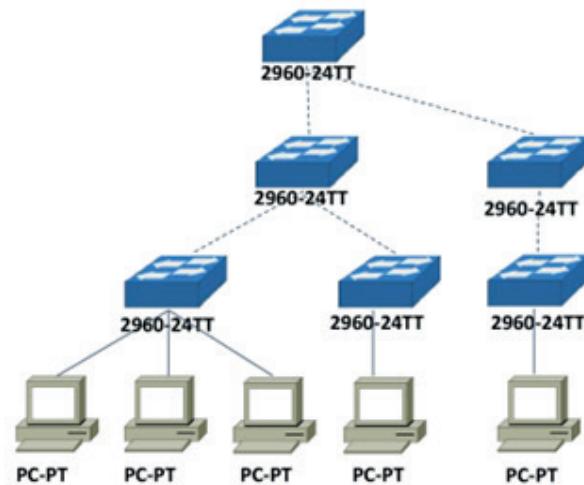
Figura 10*Topología física en estrella extendida**Nota.* La figura representa un esquema de una Topología Estrella Extendida

- **Jerárquica:** topología física que representa una mixtura de las topologías estrella y bus. Esta debe tener al menos tres niveles de jerarquía en los que las topologías en estrella deben conectar uno o más nodos a un solo nodo principal, de modo que todos estos estén conectados con el tronco principal del árbol. La Figura 11 muestra una topología jerárquica. Como en el caso de una topología en estrella extendida, esta tipología utiliza cables de par trenzado y fibra óptica (Odom, 2016).

Figura 11*Topología física en estrella extendida**Nota.* La figura representa un esquema de una Topología Física Jerárquica

- **Malla:** Cada computadora está conectada con otra para formar la red (ver Figura 9- Malla). Por lo general, una red de área extendida (WAN) utiliza este tipo de topología para interconectar LANs entre ciudades, países y continentes (Odom, 2016).
- **Árbol:** En su estructura hay muchos elementos conectados que están dispuestos como las ramas de un árbol. Solo puede haber un vínculo entre dos nodos. Las topologías de árbol forman una jerarquía de padres e hijos subyacentes. El colapso de un nodo involucra inconvenientes en las comunicaciones. La Figura 12 ilustra una topología en árbol (Hope, 2017).

Figura 12
Topología Física en árbol



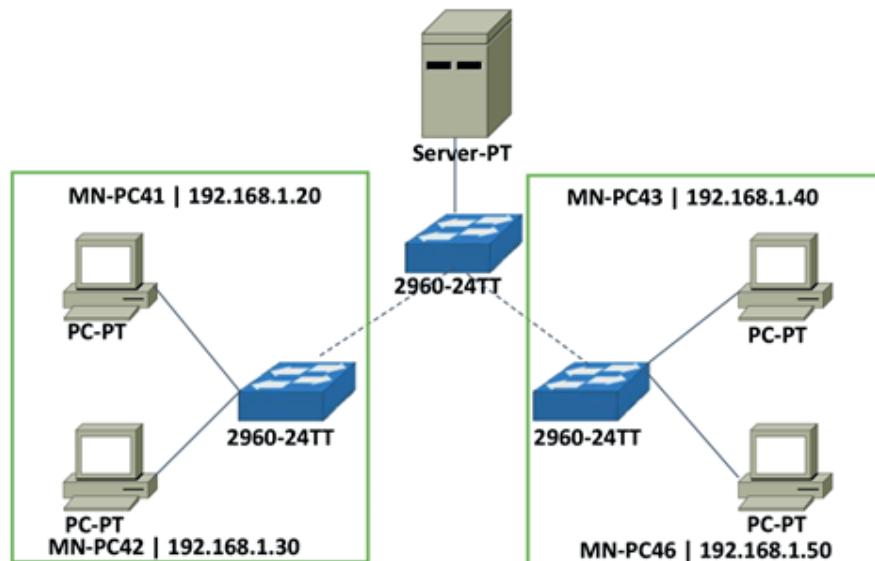
Nota. La figura representa un esquema de una Topología en árbol.

La topología lógica, a diferencia de la topología física, representa el aspecto lógico de la red informática. La Figura 13 presenta la topología lógica con sus componentes lógicos, como nombres de computadora, equipo de red, tecnología de comunicación de red, direcciones IP e inclusive servicios levantados. La Academia de Networking de Cisco señala lo siguiente:

- Se refiere a como la red transfiere tramas de un nodo al siguiente. Esta disposición consta de conexiones virtuales entre los nodos de una red.
- Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas.
- En la topología lógica, las rutas lógicas son las que se utilizan para transportar señales eléctricas o luminosas de una computadora a otra, o de un nodo de red a otro nodo.

- Esta topología representa la forma en que los datos acceden al medio de transmisión y transmiten paquetes, tramas o bits a través de él.

Figura 13
Topología lógica



Nota. La figura representa un esquema de una Topología Lógica

2.4 Aplicaciones de redes de área personal, local y extendida

Aproximadamente a partir de 1960 las aplicaciones en red se empezaron a utilizar (Jovanov, 2001). Hoy en día con el avance vertiginoso de la microelectrónica, a informática y las telecomunicaciones se siguen desarrollando aplicaciones de software para la PAN, WLAN y WAN. Desde el uso de un audífono, un mouse, un parlante, o una radio, todos inalámbricos. Los usuarios utilizan estos dispositivos para ver videos, escuchar música y diferentes formas de entretenimiento utilizando la tecnología Bluetooth.

De la misma forma, las redes inalámbricas de área local (WLAN) son cada vez más populares. Son de uso común en los hogares, los pequeños negocios, los campus universitarios o dentro de las corporaciones, y han comenzado a aparecer en las áreas públicas.

Existen varios estudios anteriores sobre redes de campus universitarios inalámbricos y redes públicas (Balazinska & Castro, 2003) complementadas con el uso de las redes de área local (LAN/WLAN) para el uso de servicios de usu-

rios y puntos de acceso en diferentes lugares en el campus como bibliotecas, bares, etc. Las tasas de transferencia de usuarios varían según la tecnología de los adaptadores inalámbricos, punto de acceso inalámbrico, distancias y cantidad de usuarios.

2.5 Internet, Intranet y Extranet

Internet es esencialmente una red universal de redes y un área global de recursos informáticos interconectados. Todos los usuarios utilizan los servicios y las aplicaciones en la red Internet. El cliente necesita estar conectado para utilizar los servicios de las empresas, así como para el teletrabajo, teleeducación y telesalud. Los empresarios, por su parte, necesitan ofrecer sus servicios y productos en el Internet. Las grandes corporaciones e instituciones de educación superior requieren acceso casi universal a Internet. Muchos usuarios han decidido rentar servicios en las nubes computacionales sean públicas, privadas e híbridas. Dependiendo de la ubicación geográfica, de los tipos de perfiles, del acceso a los diversos servicios, del tipo de equipo de usuario final se distinguen dos conceptos: la Intranet y la Extranet.

De acuerdo con (Urrutia, 2018), una Intranet la define como una red privada que permite a los empleados y al personal de una empresa compartir información al utilizar un navegador como la interfaz de usuario. De esta manera la transferencia de información se produce de manera óptima y sencilla dentro de una organización. La información, herramientas, directorios y servicios disponibles en la Intranet de una compañía no suelen estar disponibles para el público en general y deben ser restringidas solamente a los usuarios de la LAN. La intranet está diseñada para comunicaciones internas únicamente.

Por otra parte, según lo establece (Spralls III, 2011), una Extranet es una red privada que aprovecha la tecnología de Internet y el sistema público de telecomunicaciones para compartir la información o las operaciones de una empresa a través de un sistema seguro con usuarios que tienen privilegios o derechos de acceso, a proveedores registrados, a gerentes medios o altos que necesitan utilizar los servicios de manera remota. Una extranet se considera parte de la red de una empresa que se extiende a usuarios autorizados fuera de la organización. Un ejemplo es el acceso de los estudiantes a los sistemas académicos en las instituciones de educación. Otro ejemplo, cuando los clientes acceden a los servicios financieros que ofrece la banca electrónica.

Recursos complementarios

- Video sobre: "Tipos de redes. LAN y WAN" 
- Video sobre: "Topologías de Red" 
- Presentación en PDF de Cisco NetAcad sobre: "Capítulo 1: Exploración de la red" 
- Video sobre: "Cómo funcionan las redes WI-FI. No deberías usar el WI-FI gratis" 
- Video sobre: "Cómo funciona la velocidad y tu conexión a Internet" 
- Video sobre: "¿Cuáles son las Diferencias Principales Entre Internet, Intranet y Extranet?" 

Actividad de aprendizaje 2

Descripción de la actividad

Desarrolle una práctica de laboratorio en la que el estudiante pruebe algunas aplicaciones de software para gestión de redes que están disponibles en la Web tales como:

- Speed test (analizador de la velocidad de carga y descarga);
- Who is domain tool (conjunto de herramientas para sustituir al nslookup);
- Subnet online (calculadora de subredes IP en línea y colección de herramientas de red);
- Visual route (herramientas visuales red y diagnóstico);
- Cyber threat map (analizador de ataques en el ciberespacio) todos revisados en clase.

Luego instale un analizador de protocolos y de tráfico de redes denominado Wireshark. Póngalo en funcionamiento e inicie con la captura del tráfico sea de su interfaz de red inalámbrica o la que se conecta con Ethernet. Pruebe el

análisis de tráfico con ping. Luego navegue en Internet. Finalmente habrá un video de YouTube. Proceda con el análisis capa por capa, realice filtros por protocolo (ICMP, HTTP, RTP, UDP, TCP) y utilice el análisis estadístico de la propia herramienta.

Al finalizar, elabore un informe de laboratorio con la siguiente estructura: Tema, Objetivos de aprendizaje, Topología de prueba en la que se incluya materiales y equipos, Marco teórico, Desarrollo de la práctica (que incluya todas las aplicaciones revisadas a manera de resumen), Conclusiones, y Referencias bibliográficas.

El informe debe incluir ilustraciones, capturas del resultado del análisis realizado, tablas debidamente numerado, rotulado y referenciado en el texto. Suba el informe en formato PDF a la plataforma educativa.

Autoevaluación Capítulo 2

1. ¿Cuáles son los tipos de redes de computadoras?

PAN, LAN, WLAN, MAN, WAN

De Sistema, Programación y Aplicación

LAN y WAN

Ninguna de las anteriores

2. ¿Qué es la red PAN?

Es una red que cubre un área geográfica amplia.

Es aquella que se divide generalmente en segmentos lógicos más pequeños llamados grupos de trabajo.

Es una red informática que se utiliza para interconectar dispositivos que deben estar dentro del rango de una persona (menos a 10 metros).

Todas las anteriores.

3. ¿Qué es una red WAN?

Una red que se limita a un área tal como un cuarto o un solo edificio.

Es una red que cubre una gran área geográfica, utilizando líneas de telecomunicaciones dedicadas, como líneas telefónicas.

Una red que conecta las redes de dos o más localidades, pero no se extiende más allá de los límites de una ciudad.

Se define como la forma de tender el cable a estaciones de trabajo individuales.

4. ¿Qué topología física utiliza un hub o switch para la interconexión de computadoras?

Estrella

Bus

Anillo

Malla

5. ¿Qué topología física utiliza más recursos al implementarlas?

Anillo

Bus

Estrella

Malla

6. ¿La Red MAN es una red de alta velocidad que da cobertura en un área geográfica?

Extensa

Reducida

Estrecha

Mediana

7. ¿La WAN es útil para que los proveedores de Internet puedan brindar?

Mayor velocidad de carga y descarga

Mejor Conexión de Redes

Mejor infraestructura

Todas las anteriores

8. ¿La topología física de redes presenta?

El orden de dispositivos

La disposición de dispositivos

La ubicación de dispositivos

Todas las anteriores

9. ¿La Topología física en la que las computadoras, los periféricos y los dispositivos de red forman un ciclo cerrado se denomina?

Estrella

Anillo

Bus

Árbol

10. ¿La red privada interna que permite a los empleados y al personal de una empresa compartir información de forma segura?

Internet

Extranet

Intranet

Todas



<https://acortar.link/kJEv5H>

CAPÍTULO III

Dispositivos de red

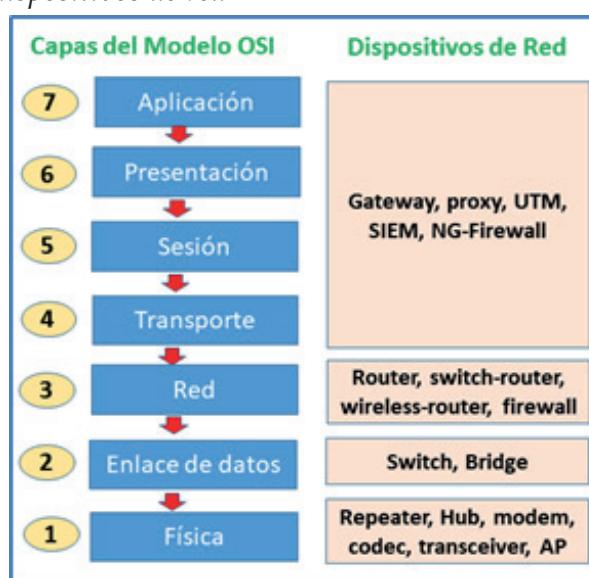
3.1 Introducción

Para que una red pueda coexistir y funcionar es necesario la interacción de varios dispositivos de red tales como enruteadores, conmutadores, módems, puntos de acceso, transceptores, etc. Estos dispositivos tienen diferentes funcionalidades que receptan, conmutan, filtran, procesan, enrutan, amplifican, y transforman las señales que se transportan a través de los medios de comunicación.

Para una mejor comprensión, la Figura 14 ilustra en dónde funcionan los dispositivos de red, capa por capa del modelo de interconexión de sistemas abiertos (Open Systems Interconnection, OSI). A continuación, se presenta la función que desempeñan algunos de los dispositivos de una red.

Figura 14

Modelo OSI y los dispositivos de red



Nota. La figura es una muestra de la relación entre el modelo OSI y los tipos de dispositivos de red capa por capa. Obtenido de (Fuertes, 2021)

3.2 Dispositivos

3.2.1 Dispositivos de carga física

- **Repetidor (repiter):** es un dispositivo cuya función principal es recoger, amplificar y regenerar la señal. A su vez, aumentar la cobertura del alcance.

ce de una red. (Fernandez, Xataca, 2021). El repetidor trabaja en la capa física del Modelo OSI (ver Figura 15).

Figura 15

Repetidor



Nota. La figura es una fotografía del repetidor RE305 de la compañía TP-Link. Obtenido de (Tp-link, 2020)

- **Hub:** su principal función es conectar varios computadores (Piquer & Mora , 2020) desde un punto central. Se trata de un dispositivo de red antiguo, que salió fuera de fabricación hace dos décadas y que fue remplazado por los conmutadores (ver Figura 16).

Figura 16

Hub



Nota. La figura es una fotografía del Hub NETGEAR EN 104. Obtenido de: (Lopez C. , 2020)

- **Modem:** este dispositivo de entrada/salida típicamente ha sido utilizado para transformar señales digitales en analógicas, o viceversa. Estas señales son provenientes de una línea telefónica que emite señales analógicas desde los proveedores de servicios de telecomunicaciones o de valor agregado y que deben ser convertidas en digitales para que puedan ser procesadas por los equipos de usuario final o por los dispositivos (Software Lab, 2021) (ver Figura 17).

Figura 17

Módem



Nota. La figura es una fotografía del modem TP-Link TD-8817. Obtenido de: (Barroyeta, 2020)

- **Códec:** la funcionalidad de este dispositivo es la de codificar o decodificar paquetes de datos entre las cuales también comprende audio y video en formatos específicos (Sathyaranarayanan, 2020). La Figura 18 ilustra un códec marca Extron.

Figura 18

Códec



Nota. La figura es una fotografía del códec 3G-SDI Extron VNC-325. Obtenido de: (Sathyaranarayanan, 2020)

- **Punto de Acceso (Access Point):** Este dispositivo puede tomar el papel de dispositivo central debido a que al ser inalámbrico tiene facilidades de accesibilidad. Este punto de conexión varía en sus tamaños dependiendo su finalidad. Por lo general para un hogar se utilizan dispositivos pequeños. En el ámbito empresarial son más robustos, con antenas altas, de mejor tecnología, con mejor alcance y mejores prestaciones. Hoy en día son de los dispositivos más utilizados en el mundo por su facilidad y utilidad. (CISCO, 2020) (Ver Figura 19).

Figura 19
Access Point



Nota. La figura es una fotografía del Access Point TP-Link TL-WA901nd N450 Mbps 3 Antenas. Obtenido de: (Más tecnologia PC, 2021)

3.2.2 Dispositivos de Capa de enlace de datos

- **Conmutador (Switch):** es un dispositivo de interconexión que realiza funciones de conmutación y concentración en el caso de los de capa 2 del modelo OSI. Así mismo, tiene ciertas funciones de enrutamiento si se trata de un switch de capa 3. Son los dispositivos más utilizados en las LAN, aunque también existen conmutadores WAN. Los switches deben ser configurables, con alta tecnología de conmutación, alta densidad de puertos a diversa de capacidad de transmisión como de 100, 1000, y 10000 Mbps (Piquer & Mora , 2020) (ver Figura 20).

Figura 20*Switch*

Nota. La figura es una fotografía del switch D-Link DGS-1100-24P. Obtenido de: (Hope, 2017)

- **Puente (Bridge):** tiene como objetivo principal el dividir una red en segmentos o dominios de colisión. Son equipos antiguos que funcionan en capa dos y que han sido reemplazados por los comutadores (Fernandez, Xataca, 2021) (ver Figura 21).

Figura 21*Bridge/Puente*

Nota. Bridge/puente Ethernet a Wireless-G. Obtenido de: (Tanenbaum A. , Redes de Computadoras, 2012)

3.2.3 Dispositivos de Capa de red

- **Enrutador (Router):** es el encargado de transmitir o recibir señales de telecomunicaciones desde una LAN hacia otra LAN a través de una WAN. El enrutador tiene varias funciones importantes en las redes tales como enrutamiento, filtrado de paquetes, traducción direcciones de red (NAT), e interco-

nexión de diversas redes (CISCO, 2021). En el mundo empresarial, se requiere de un enrutador perimetral, que es el punto de conexión más externo de la red que filtra paquetes desde las redes externas, incluida el Internet. Estos dispositivos no suelen ofrecer Wi-Fi ver Figura 22).

Figura 22

Router



Nota. La figura es una fotografía de un router Cisco 4000 integrated series. Obtenido de: (Salazar, 2017) o en la academia de networking de Cisco

En las redes domésticas, para el acceso a Internet se suele utilizar un enrutador inalámbrico, que se lo conoce también como puertas de enlace residenciales. Estos dispositivos combinan las funciones de los enrutadores perimetrales y de distribución pues incluyen el protocolo de configuración dinámico de direcciones IP (DCHP).

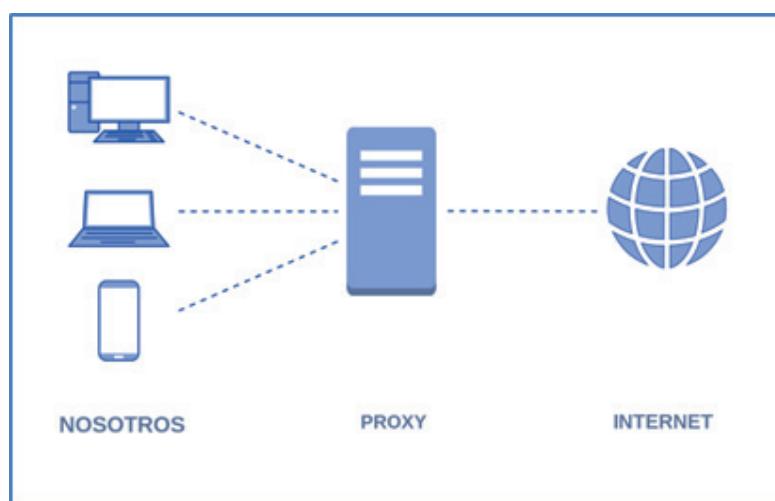
- **Cortafuegos (firewalls):** este dispositivo tiene como objetivo autorizar o filtrar la transmisión de diversos paquetes que provienen de diferentes dispositivos ubicados en diferentes lugares geográficos distintos o distantes. Normalmente forma parte de la seguridad perimetral de una red, puede segmentar lógicamente una o más dominios de broadcast para otorgarle niveles de privacidad. Los firewalls de nueva generación incluyen modernas funcionalidades para detectar malware, tráfico malicioso, software espías, entre otros (ver Figura 23).

Figura 23*Firewall*

Nota. La figura es una fotografía del Firewall Cisco-ASA-5506-X. Obtenido de: (Odom, 2016) o en la academia de networking de Cisco.

3.2.4 Dispositivos de capas superiores

- **Proxy:** este dispositivo por lo general se lo encuentra en una red como un servicio el cual responde a la función de intermediario en las peticiones de recursos entre un cliente y un servidor. Es un servicio empotrado en un programa de software o dispositivo, que hace de mediador entre las peticiones de recursos que realiza un cliente a otro servidor. Por ejemplo, el proxy recibe las peticiones para acceder a una u otra página, y se encarga de transmitírselas al servidor de la web para que esta no sepa de quien es el origen de la petición. La Figura 24, es una representación visual que abstrae el funcionamiento de un proxy.

Figura 24*Proxy*

Nota. La figura representa una ilustración del lugar que ocupa un servidor proxy en una red. Obtenido de: (Netink, 2020)

Los servidores proxys deben ser configurados. Así, por ejemplo, las conexiones entre el cliente y el servidor proxy pueden utilizar un puerto lógico TCP, que no sea el puerto 80 (HTTP), para la comunicación. Este puerto lógico suele ser el puerto TCP 3128 o 8080. De forma predeterminada, la autenticación web solo se escucha en el puerto 80. En cambio, si se configura un proxy HTTPS a través del puerto lógico 443, se crea un filtro de contenido de alto rendimiento, que examina el tráfico web para identificar contenido sospechoso en la navegación web, pero en este caso es seguro pues utiliza el protocolo TLS en la capa de transporte.

Recursos complementarios

- Video sobre la función que cumple cada dispositivo en el envío de datos “Guerreros de la red”. 
- Curso de Packet Tracer gratuito para mejorar sus habilidades. 
- Video sobre los dispositivos de una red. 
- Video sobre los componentes de una red. 
- PDF sobre la configuración e inventario de dispositivos de red y su cableado estructurado. 

Actividad de aprendizaje 3

Descripción de la actividad

Desarrolle una investigación en el Internet en grupos de hasta cuatro estudiantes sobre los diferentes dispositivos de redes (networking) que existen en el mercado, tales como: repetidores, módems, transceivers, códec, hubs, puntos de acceso inalámbricos que actúan en la capa física del modelo OSI. Conmutadores y puentes de la capa de enlace de datos. Enrutadores, firewall, enrutadores inalámbricos de la capa de red. Finalmente, los firewalls de nueva genera-

ción, UTM, SIEM y proxy de las capas superiores. Para cada uno describa sus principales características, marcas, precios, tipos de interfaces o conectores y si son configurables o no y función. Al finalizar, elabore un informe de investigación con la siguiente estructura: Tema, Objetivos de aprendizaje, Desarrollo de la investigación, Conclusiones y Referencias bibliográficas.

Autoevaluación Capítulo 3

1. El switch es un dispositivo de red cuya funcionalidad es la interconexión de equipos en la capa de enlace de datos, también es utilizado como un conmutador de paquetes. En qué otra capa del modelo OSI puede ser empleado:

Capa de aplicación
Capa Física
Capa de transporte
Capa de Red

2. ¿Cuál es la razón por qué el Proxy se ubica en 4 de las 7 capas del modelo OSI?

Porque es un intermediario entre el cliente y el servidor web en el envío de paquetes o recursos.

Porque existen varios tipos de proxy que se ubican cada uno en diferentes capas

Porque es parte del router y cambia la dirección IP a los paquetes para que lleguen más rápido a su destino.

3. ¿Cuál es la principal diferencia entre un hub y un bridge?

No existe diferencia alguna cumple la misma función y son exactamente iguales

Todos los puertos de un hub son un único dominio de colisión, mientras que un bridge divide o segmenta una red en diferentes dominios de colisión

Un hub divide una red en varios dominios de colisión (uno por cada dispositivo), mientras que un bridge tan solo conecta dispositivos sin segmentar la red.

4. ¿En qué capa del modelo OSI funciona principalmente una puerta de enlace?

Capa de transporte

Capa de red

Capa de sesión

5. ¿Los Firewalls pueden ser tanto físicos como lógicos?

Falso

Verdadero

6. ¿Cuáles son los roles de un router?

Comunicación entre redes, mejor selección de ruta, reenvío de paquetes y filtrado de paquetes.

Intermediario entre un cliente y un servidor y detecta malware.

Decodifica paquetes y a su vez comprime tramas para su posterior envío.

7. ¿Qué dispositivo inalámbrico que brinda facilidades de accesibilidad para un hogar y en el ámbito empresarial con mejores prestaciones?

Módem

Access Point

Router inalámbrico

Transceiver

8. ¿Qué orden lógico se debe cumplir en una red que cuenta con un servidor proxy?

Proxy-dispositivos-Internet

Internet-dispositivos-proxy

Dispositivos-proxy-Internet

9. ¿Cuál es la función principal del firewall (cortafuego)?

Es el encargado de transmitir o recibir señales de telecomunicaciones desde una LAN hacia otra LAN a través de una WAN.

Tiene como objetivo autorizar o filtrar la transmisión de diversos paquetes que provienen de diferentes dispositivos.

Es un dispositivo de interconexión que realiza funciones de commutación y concentración en el caso de los de capa 2 del modelo OSI.

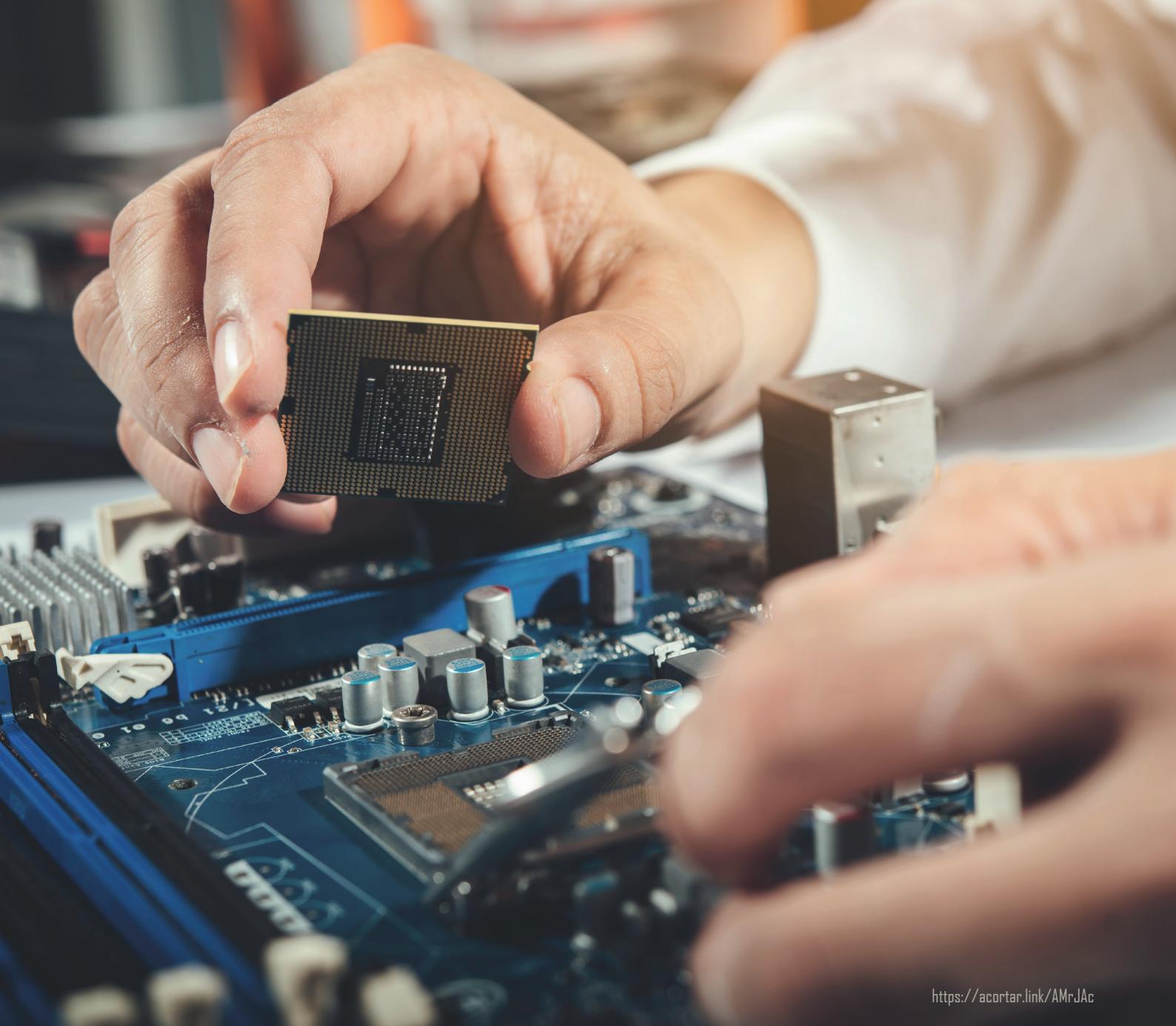
10. ¿Qué dispositivo tiene como objetivo principal el dividir una red en segmentos o dominios de broadcast?

Switch

Bridge

Cortafuegos

Router



<https://acortar.link/AMrJAc>

CAPÍTULO IV

Medios de transmisión

4.1 Introducción

Un medio de transmisión es el canal mediante el cual el emisor y receptor logran comunicarse para enviar o recibir un mensaje en la red. Para comprender la necesidad de codificación, multiplexación, conmutación, verificación de errores, etc., se debe comprender primero el comportamiento de la transmisión de señales (i.e., voz, video, datos y control) a través de los medios de transmisión.

Los medios de transmisión se pueden clasificar en guiados o inalámbricos. Los medios guiados más usados son el par trenzado, cable coaxial y fibra óptica. Por otro lado, los medios no guiados, conocidos también como inalámbricos, disponen de un medio para comunicarse con las ondas electromagnéticas sin limitar la difusión a través del aire o el vacío. Cabe recalcar que las microondas terrestres y vía satélite, la radiodifusión y los infrarrojos son algunos medios de transmisión inalámbricos.

Cuando la transmisión entre dos dispositivos en la que la señal se difunde directamente del emisor al receptor sin interferencias de otros dispositivos exceptuando amplificador o repetidor, se denomina enlace directo. En este caso, el repetidor es un elemento pasivo que sirve para regenerar y amplificar la energía de la señal. Una transmisión punto a punto existe si dispone de un enlace directo entre dos dispositivos que comparten el medio. En una configuración guiada multipunto, el mismo medio es compartido por más de dos dispositivos. La Figura 25 es una abstracción del uso de medios de transmisión.

Figura 25
Medios de transmisión



Nota. La figura representa un panel de conexión de fibra óptica. Obtenido de: (Martinez, 2019)"

4.2 Terminología utilizada

Para comprender de mejor manera los medios de transmisión físicos e inalámbricos, a continuación, se presenta la terminología utilizada:

- **Antenas:** son dispositivos que se utilizan para emitir o recibir ondas radioeléctricas. En redes de datos de dos nodos diferentes, se requiere de una antena transmisora que transforma corrientes eléctricas en ondas electromagnéticas, y una antena receptora que realiza la función inversa.
- **Antena parabólica:** se utilizan en aplicaciones de microondas terrestres y satelitales, son transmisoras, receptoras o full dúplex, debido a que pueden transmitir y recibir simultáneamente.
- **Atenuación:** es la pérdida de potencia de la señal en un canal de comunicación debido a la distancia que se expresa en decibeles (dB).
- **Diafonía:** (o crosstalk), es la perdida de la señal inducida por la interferencia electromagnética producida por cables o motores eléctricos especialmente.
- **Cable coaxial:** es un medio de transmisión que transporta señales eléctricas de alta frecuencia antiguamente utilizado en redes de datos. Hoy sigue siendo utilizado en televisión por cable, en circuitos cerrados de televisión para sistemas de video vigilancia, audio y video.
- **Cable de par trenzado:** es un medio de transmisión usado en redes de datos en el que dos conductores eléctricos aislados son trenzados para anular las interferencias electromagnéticas o de radio frecuencia.
- **Fibra óptica:** es un medio de transmisión basado en pulsos de luz dentro de un cable, que tiene como fuente de origen diodos o láser, que transmite datos, con mayor velocidad de transmisión y a largas distancias.
- **Infrarrojo:** son señales u ondas de luz infrarrojas no guiadas que son comunes para la comunicación de corto alcance, que son incapaces de traspasar objetos sólidos. Ejemplos: los controles remotos de diversos aparatos electrónicos.
- **Medio de transmisión:** soporte físico o inalámbrico capaz de transmitir datos a un emisor y un receptor.
- **Microonda:** ondas unidireccionales, en las cuales el emisor y receptor deben estar perfectamente alineados para su correcta transmisión que tienen dificultades para atravesar por muros de edificios dada la curvatura de la tierra.

- **Ondas de radio:** capaces de recorrer grandes distancias, son omnidi-reccionales. Las estaciones de radio y televisión, los teléfonos celulares generan ondas de radio.

4.3 Medios físicos o guiados

La capa física del modelo OSI/ISO es la responsable de transportar bits de un equipo computacional a un servidor u otro dispositivo de la red a través de un canal de comunicación. Los medios de transmisión físicos se agrupan en diferentes tipos de cable tales como: par trenzado (UTP), fibra óptica, o coaxial.

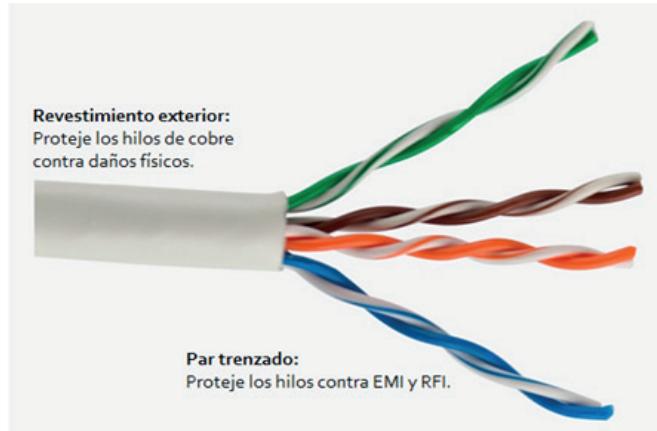
4.3.1. Cable UTP (Unshielded Twisted Pair)

El cable de par trenzado sin blindaje (UTP), es el más utilizado en el mundo para conectar redes de área local (LAN). Está fabricado por dos cables de cobre aislados de un milímetro de grosor que se encuentran trenzados entre sí. La trenza sirve para anular las interferencias de fuentes externas y diafonía de los cables adyacentes, puesto que carece de un blindaje protector contra interfe-rencias EMI y RFI.

El cable UTP consta de cuatro pares de hilos codificados por color que tie-nen un revestimiento de plástico flexible que los protege contra daños físicos menores. En sus extremos se termina con conectores RJ-45 que son el estándar típico para interconectar equipos de red, dispositivos activos (comutadores, enrutadores, etc.), y elementos pasivos (paneles de conexión, tomas de datos, etc.). La Figura 26 muestra un segmento UTP.

Figura 26

Cable de par trenzado



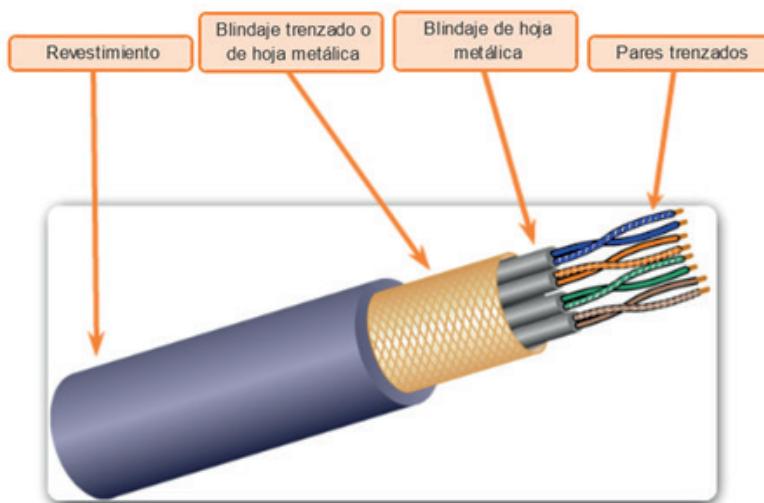
Nota. La figura representa un cable de par trenzado de Categoría 5 con cuatro pares trenzados. Obtenido de: (Tanenbaum A. , 2012)"

4.3.2 Cable STP (Shielded Twisted Pair)

El cable de par trenzado con blindaje (STP) incorpora mallas de protección para neutralizar la interferencia electromagnética (EMI) y la interferencia de radio frecuencia (RFI) a más del trenzado de hilos para neutralizar la inducción. Comparado con el cable UTP, el STP es más costoso y difícil de instalar. Al igual que el cable UTP, el STP utiliza un conector RJ-45 (ver Figura 27).

Figura 27

Cable STP



Nota. La figura representa un cable STP cubierto de una malla que tiene como función conducir. Obtenido de: (Martinez, 2019)"

4.3.3 Código de colores del cable par trenzado

Cuando se trata de realizar una conexión con cable UTP o STP, se deben aplicar el código de colores de sus pines que se establecen en la norma EI/TIA 568A o EI/TIA 568B. Mediante este código se pueden fabricar cordones de conexión directos o cruzados.

- Los cordones de conexión directos son útiles para conectar todo tipo de equipos hacia los dispositivos activos y pasivos. Ejemplo un PC y un conmutador, un conmutador y un panel de conexión.
- Los cordones de conexión cruzados sirven para conectar mediante cable equipos o dispositivos del mismo tipo (PCs con PCs, conmutadores con conmutadores, enrutadores con enrutadores, etc.).

Según el tipo que se requiere fabricar, en ambos extremos se utilizaría cualquiera de las dos normas establecidas (cable directo). Para un cable cruzado se requiere utilizar en un extremo la norma EI/TIA 568A y en el otro extremo EI/TIA 568B. La Tabla 1 muestra los colores para la norma EIA/TIA 568B:

Tabla 1

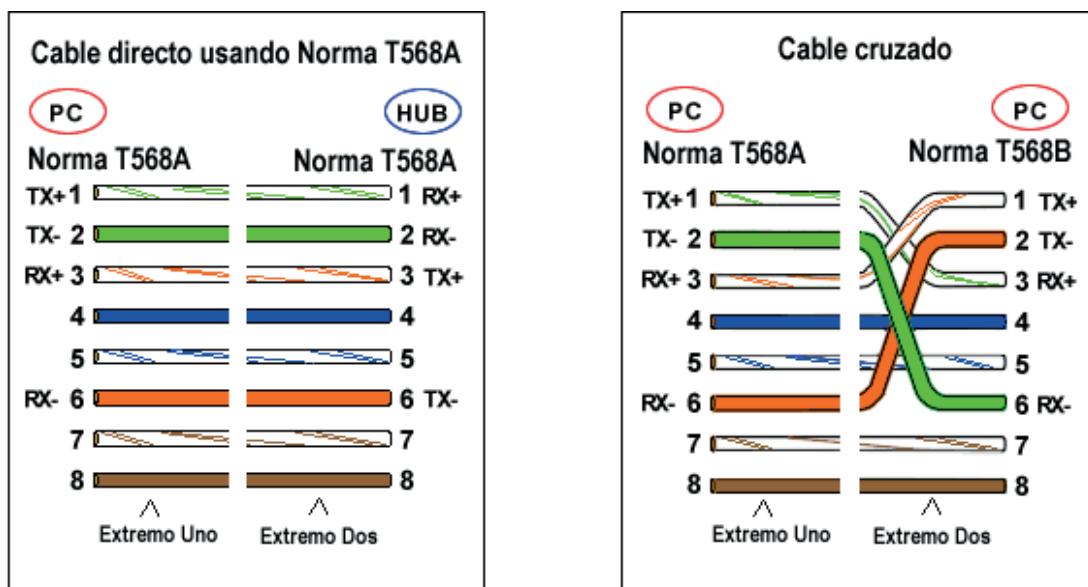
Asignaciones para los conectores de par trenzado código EI/TIA 568B

Número de pin	Color base del cable	Color de la cinta del cable	Uso del 10Base/T
1	Blanco	Naranja	Transmisión, negativo
2	Naranja		Transmisión, positivo
3	Blanco	Verde	Recepción, negativo
4	Azul		N/A
5	Blanco	Azul	N/A
6	Verde		Recepción, positivo
7	Blanco	Café	N/A
8	Café		N/A

Nota. Para obtener la norma EIA/TIA 568A, bastaría con cambiar la posición del hilo uno con el tres y la posición del dos con el seis como muestra la Figura 28.

Figura 28

Asignación de pines para los conectores cable directo y cruzado



Nota. La figura representa la asignación de colores y pines de un cable de par trenzado con cuatro pares trenzados junto al conector RJ-45. Obtenido de: (Martinez, 2019).

La Asociación de la Industria Electrónica (EIA, Electronics Industry Association), define a los cables de red de par trenzado por categorías, que evidencia su capacidad para transportar tráfico a través de la red. La Tabla 2 lista las categorías conocidas:

Tabla 2

Nivel de categoría de desempeño del cable de par trenzado

Nivel de categoría	Evaluación del desempeño
Nivel 1	Sin evaluación de desempeño
Nivel 2	1 Mbps
Categoría 3	10 Mbps
Categoría 4	16 Mbps
Categoría 5	100 Mbps a 1 Gbps
Categoría 6	>1 Gbps

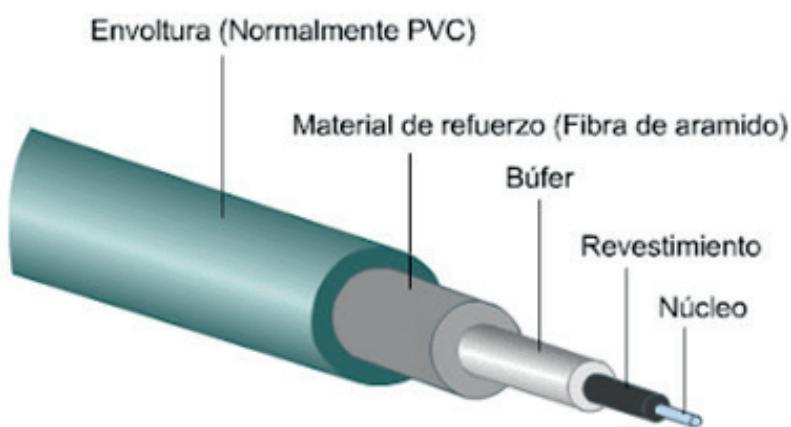
4.3.4 Fibra óptica

El cable de fibra óptica es la tecnología usada para transmitir datos en forma de pulsos de luz mediante hilos de fibra de vidrio o plástico, a largas distancias.” (Verizon, s.f.). El sistema de transmisión óptico posee tres componentes básicos: fuente de luz, medio de transmisión y detector. Se debe entender que un pulso de luz indica un bit 1, y si no hay un pulso de luz indica un bit 0. Las principales características de la fibra óptica son:

- Velocidad de transmisión sobre los miles de millones de bits por segundo (Gbps) para señales de voz, datos, vídeo, y control
- Cobertura en cortas y largas distancias
- Mínimo porcentaje de error de transmisión
- Es inmune al EMI o RFI
- Alta resistencia a corrosión
- Dimensiones y peso reducidos
- Alto costo de fabricación y mantenimiento

La fibra óptica está conformada por tres partes concéntricas. El núcleo, que contiene una o más hebras de plástico o vidrio por donde viaja la señal. El revestimiento que es una capa de material de bajo índice de refracción, que está en contacto directo con el núcleo. La capa exterior o recubrimiento, que cubre las fibras con material un poco más resistente. La Figura 29 muestra los elementos de la fibra óptica.

Figura 29
Cable de fibra óptica



Nota. La figura representa las partes de un cable de fibra óptica. Obtenido de: (Martinez, 2019)

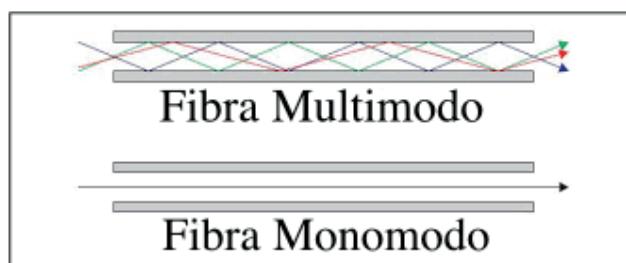
Tipos de fibra óptica

Existen dos tipos de fibra óptica: monomodo y multimodo. Esta clasificación se debe especialmente al modo de propagación de luz.

- La fibra Monomodo está enfocada en la transmisión de datos a mayores distancias. Su núcleo óptico es pequeño (9.4 micrómetros de diámetro), por lo que la luz recorre el cable en un solo rayo. Al ser sólo un haz de luz, la señal viaja más rápido, más lejos y con más potencia. La fuente de luz usada es el LÁSER.
- La fibra Multimodo tiene la capacidad de transmitir múltiples rayos de luz debido a que posee un núcleo de mayor diámetro (50 a 62.5 a 125 micrones). Este diámetro ocasiona que la luz se refleje en distintos ángulos (reflexión y refracción). La fuente de luz utilizada es el LED. Estas características producen menores velocidades de transmisión, y comunicaciones en distancias menores a 600 metros (i.e., un edificio o un campus universitario).

Figura 30

Tipos de fibra óptica



Nota. La figura representa los tipos de fibra óptica. Obtenido de: (Telpro Madrid, 2019). Nótese la única señal en monomodo versus las diferentes señales en multimodo.

Tipos de conectores de la fibra óptica

Los conectores son terminaciones que se encargan de conectar los hilos de fibra a un dispositivo activo o pasivo (transmisor o un receptor). Estas terminaciones alinean el núcleo de fibras diminutas para que los haces de luz puedan viajar a través de ellas. Los tipos de conectores disponibles son muy variados y se los explica brevemente a continuación (ver Figura 31):

- Conector ST: Conector multimodo, de cerámica o polímero para sostener la fibra, tiene una férula de 2.5 mm, se utiliza para redes de edificios y sistemas de seguridad.

- Conector SC: Conector de broche con férula de 2.5 mm, estandarizado en TIA-568A, que se utiliza en la transmisión de datos.
- Conector LC: Conector monomodo pequeño de férula de 1.25 mm, utiliza una férula de cerámica.
- Conector FC: Conector monomodo de férula de 2.5 mm, de acero inoxidable, se utiliza en la transmisión de datos y en redes de telecomunicaciones. Además, se emplea en instrumentos de alta precisión como los OTDR (Optical Time Domain Reflectometer) y es el conector utilizado en CATV (Community Antenna Television).
- Conector MTRJ: Conector dúplex, útil para distancias cortas de redes locales, e instrumentación.
- Conector MU: Conector simple y dúplex, con férula de 1.25 mm, se utiliza en sistemas de comunicación, tarjetas ópticas y redes LAN.

Figura 31

Tipos de conectores



Nota. La figura representa los diferentes tipos de conectores de fibra óptica.
Obtenido de: (FOCC, 2019)

4.4 Medios inalámbricos

Son medios que no requieren cable físico. Se los conocen también como medios no guiados, debido a que se propaga mediante una antena para su transmisión y recepción. Se considera tres intervalos de frecuencia:

- El primer intervalo conocido como frecuencias de microondas, el cual se define a partir de 1 GHz hasta 40 GHz. Son ideales debido a que logran haces altamente direccionales, de tal manera son capaces de conseguir enlaces de punto a punto. Así mismo, son utilizadas en comunicaciones satelitales a través de antenas parabólicas.
- El segundo intervalo se conoce como las ondas de radio, las cuales van desde 30 MHz hasta 1 GHz que son convenientes para las aplicaciones omnidireccionales.
- El tercer intervalo conocido como zona infrarroja del espectro, el cual es ideal para aplicaciones de cobertura local punto a punto, incluso multipunto dentro de áreas encerradas, como es el caso de habitaciones. Su rango se encuentra entre 3×10^{11} y 2×10^{14} Hz.

4.4.1 Microondas terrestres

Provee conectividad entre dos estaciones terrenas en línea de vista utilizando equipo de radio con frecuencias de portadora por encima de 1 GHz. Incluye una antena parabólica tipo plato, con un diámetro de 3 metros, la cual es empotrada a una altura elevada del nivel del suelo, con el propósito de obtener una separación mayor entre cada antena y evitar inconvenientes en la transmisión. Para alcanzar transmisiones de larga distancia, se deben conectar distintos enlaces punto a punto entre las antenas situadas en torres adyacentes.

Entre las principales aplicaciones de la microonda terrestre se pueden mencionar la telefonía básica, transmisión de datos, telegrafía, canales de televisión, audio y video e inclusive telefonía celular (entre troncales). Cabe señalar que los sistemas de microondas requieren menos repetidores en comparación con los cables de cobre, sin embargo, se demanda que las antenas estén alineadas correctamente. Además, conviene conocer que la causa de pérdida de la señal es la atenuación, la cual aumenta con las condiciones ambientales. La inferencia electromagnética es otro inconveniente, debido a que las áreas de cobertura se pueden solapar.

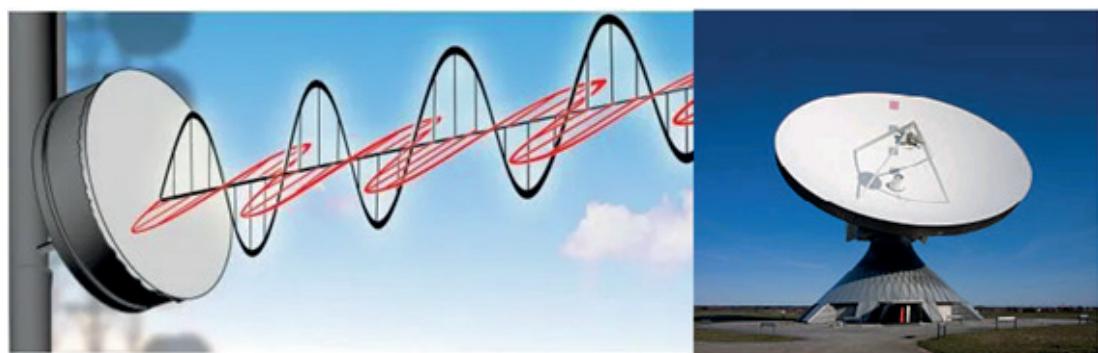
4.4.2 Microondas vía satélite

Para la transmisión de microondas vía satélite se utiliza un satélite de comunicaciones, lo que se conoce como una estación la cual enlaza dos o más receptores/transmisores terrestres, denominados estaciones base. Los canales transpondedores son llamados así, debido a que operan una serie de bandas de frecuencias. Los satélites de comunicación deben conservar la posición respecto a la tierra para un adecuado funcionamiento.

Una ventaja de la microonda vía satélite es facilitar el acceso a lugares remotos sin necesidad de grandes infraestructuras físicas y tecnológicas. En contraste, sus desventajas son el lanzamiento de satélites en órbita es costoso, existe mayor retardo de propagación en comparación con la microonda terrestre.

La transmisión vía satélite, se encuentra entre los 1 y 10 GHz del rango de frecuencias. Así mismo, se encuentra bajo de 1 GHz, el ruido por causas naturales, ruido galáctico, solar, atmosférico y aquel producido por interferencias con diferentes dispositivos electrónicos. Por otra parte, encima de los 10 GHz, la señal es afectada por la absorción atmosférica y las precipitaciones.

Figura 32
Comunicaciones de microonda y satelitales



Nota. La figura muestra la configuración de las comunicaciones satelitales. Obtenido de: (Stallings, 2015)

4.4.3 Ondas de radio

Las ondas de radio no necesitan de antenas parabólicas, debido a que son omnidireccionales. Tiene una frecuencia de entre 3 kHz y 300 GHz, lo que

se considera parte de la radio comercial AM y FM, así como de la televisión UHF y VHF. Para la difusión simultánea se tiene una frecuencia de 30 MHz y 1 GHz. Otro tipo de aplicaciones son las comunicaciones militares, teléfonos móviles, radioaficionados, redes inalámbricas, GPS (Global Positioning System) y otras cuantiosas aplicaciones de comunicaciones.

4.4.4 Infrarrojos

Las ondas infrarrojas no guiadas son comunes para la comunicación de corto alcance. Mediante transmisores/receptores logran una comunicación que modula la luz infrarroja, por lo que los transceptores deben estar alineados directamente. Dado que los infrarrojos no pueden traspasar las paredes, beneficia al tema de la seguridad anti-espionaje, no tiene dificultades de asignación de frecuencias, de igual manera no necesita permisos para operar.

4.5 EIA/TIA 568 de Subsistema de Cableado estructurado

Según (Joskowicz, 2006), el sistema de cableado estructurado se puede definir como una infraestructura basada en normas internacionalmente aceptadas útiles para instalar, mantener y administrar el cableado de un edificio o conjuntos de edificios en los que se transmiten o reciben señales de voz, video, datos y control.

El cableado estructurado, según la norma ANSI/TIA/EIA 568-B, se divide en seis subsistemas, en donde cada uno de ellos tiene una función específica, así como sus propios elementos de conexión activos, pasivos, equipos y materiales o suministros de cableado estructurado. Los subsistemas son:

1. Cuarto principal de equipos (MCD, MDF, ER)
2. Subsistema de cableado Horizontal
3. Área de Trabajo
4. Subsistema de cableado Vertical
5. Closet de Telecomunicaciones
6. Cuarto de Entrada de Servicio

Recursos complementarios

- Vídeo sobre “Medios de transmisión: ¿Qué son los medios de transmisión?” 

- Vídeo sobre: “Medios de transmisión no guiados” 

- Vídeo sobre “Cables de fibra óptica, ¿cómo funcionan?” 

- Video sobre “¿Cómo funciona su teléfono móvil?” 

- Video sobre “5G - Explicado Fácilmente” 

Actividad de aprendizaje 4

Descripción de la actividad

Desarrolle un taller grupal de hasta cuatro estudiantes sobre la fabricación de un cordón de conexión con cable de par trenzado sin blindaje UTP categoría 5E o 6. Para el taller se requiere por estudiante dos conectores RJ-45, dos protectores del conector (bootp) “recomendado”, dos metros de cable UTP. Cada grupo debe disponer de un LAN tester, una crimpadora de impacto y una pinza cortadora de cable. Investigue en YouTube un video de cómo se fabrica un cordón de conexión y proceda con el taller. Al finalizar, elabore un informe de investigación con la siguiente estructura: Tema, Objetivos de aprendizaje, Materiales y Equipos. Marco Teórico, Desarrollo de la investigación, Conclusiones y Referencias bibliográficas.

Autoevaluación Capítulo 4

1. ¿Cómo se clasifican los medios de transmisión?

[Guiados y no guiados](#)

Par trenzado y vía satélite

Inalámbrico y ondas electromagnéticas

Infrarrojo y fibra óptica

2. ¿Cómo se clasifican los medios de transmisión guiados?

Aire y ondas

Coaxial, infrarrojo, fibra de aluminio

[Par trenzado, coaxial y fibra óptica](#)

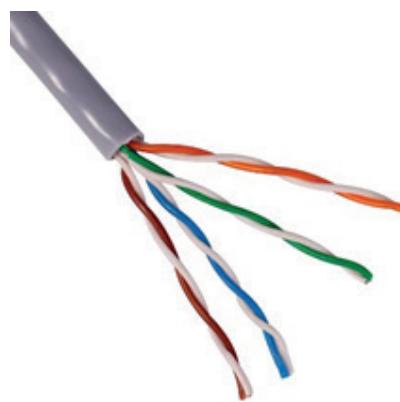
Infrarrojo

3. ¿La atenuación, distorsión y ruido reducen las señales de transmisión?

[Verdadero](#)

Falso

4. Observe la imagen y defina qué tipo de cable es:



Fibra óptica

Coaxial

RJ-45

[Par trenzado](#)

5. Complete. La comunicación inalámbrica se propaga por medio de ondas

Radiales

Satelitales

[Electromagnéticas](#)

Inalámbricas

6. ¿Cuáles son los tipos de fibra óptica?

Ondas de radio y electromagnéticas

[Monomodo y Multimodo](#)

Monomodo e Infrarrojo

Óptica y multimodo

7. ¿Cuáles son los intervalos de frecuencia de los medios inalámbricos?

Ondas de radio, infrarrojo y electromagnéticas

Microondas, fibra óptica e infrarrojos

Vía satelital, ondas electromagnéticas y radio

Microondas, ondas de radio e infrarrojos

8. ¿Cuál es la frecuencia de cobertura del espectro electromagnético?

Entre 1 y 40 GHz

Entre 1 y 30 GHz

Entre 1 y 10 Hz

Entre 1 y 20 Hz

9. ¿Las ondas de radio necesitan de antenas parabólicas?

Verdadero

Falso

10. Complete: Debido a que los medios de transmisión infrarrojos no pueden traspasar las paredes, beneficia a , dado que no tiene dificultades de asignación de frecuencias.

La transferencia de datos

La seguridad anti espionaje

La comunicación satelital.

<https://acortar.link/dKMuk0>

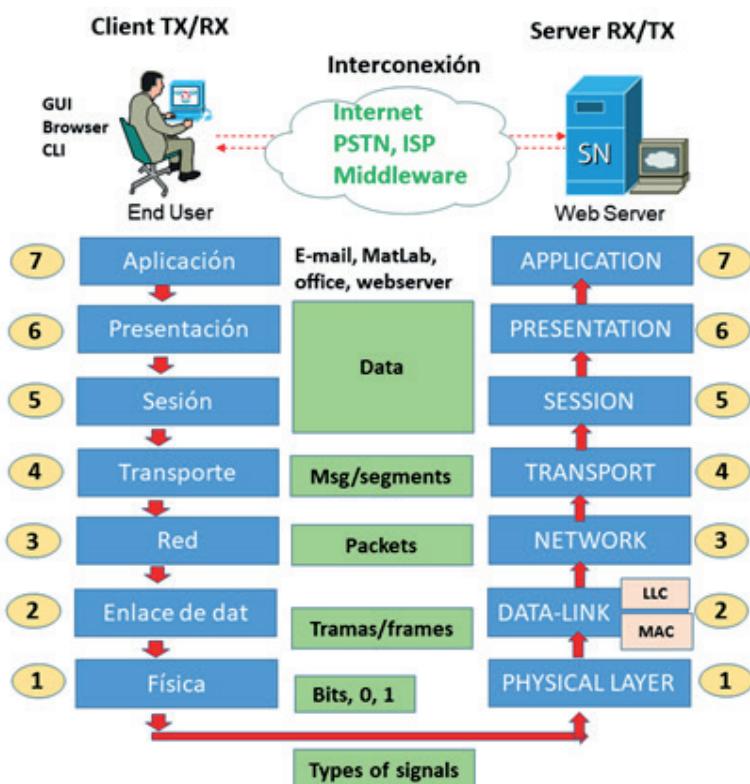
CAPÍTULO V

Modelo OSI/ISO

5.1 Caracterización del modelo OSI

El modelo de interconexión de sistemas abiertos (Open System Interconnection, OSI), por su acrónimo en inglés, es un modelo académico y conceptual, establecido por la Organización internacional de normalización (International Organization for Normalization, ISO), que permite la interconexión de equipos de usuario final y de sistemas de telecomunicaciones para que transmitan y reciban información que pueda ser procesada utilizando reglas de comunicación compatibles y estandarizadas (protocolos). El modelo OSI es un modelo de red descriptivo de sistemas abiertos, basado en siete capas o niveles de red con funcionalidades específicas, las cuales proveen servicios entre una a otra capa y trabajan en sincronía. La Figura 33 ilustra la filosofía del modelo y los tipos de señales capa por capa.

Figura 33
Filosofía del funcionamiento del modelo ISO/OSI



Nota. Esta es una representación visual de la filosofía conceptual del Modelo OSI, incluyendo los tipos de señal en cada capa

De acuerdo con (DEICY, 2011) el Modelo OSI se define como “un lineamiento funcional para tareas de comunicaciones”. Las principales funciones del modelo, capa por capa son (Programación7, 2016) (ver Figura 34):

- **Capa Física:** Es la responsable de la regulación de las características físicas, eléctricas y mecánicas de los medios de transmisión. Su función reside en la codificación en señales utilizando números binarios, mismos que conforman tramas en la capa de enlace de datos. En concreto, esta capa permite transmitir y recibir estas señales a través de los medios de transmisión para que se puedan conectar dos o más equipos en red.
- **Capa de Enlace:** Se encarga de ser la intermediaria para que pueda interactuar la capa de red y la capa física. Entre las principales funciones de esta capa se pueden citar: Direccionamiento físico o de hardware, tecnología de la red, envío y recepción de tramas, control de acceso al medio, detección de errores, control de flujo, y control de errores durante el proceso de transmisión.
- **Capa de Red:** Es la encargada de enrutar los paquetes desde punto de inicio hasta el punto final, sin necesidad de una conexión directa. Entre otras funciones se pueden citar: Direccionamiento lógico o IP, técnicas de conmutación, enrutamiento estático o dinámico, configuración de seguridades, traducción de direcciones de red, listas de control de acceso y control de la congestión.
- **Capa de Transporte:** Es la responsable de ofrecer una transmisión correcta y libre de errores. Entre sus funciones principales están: Recibir los datos de la capa de sesión, segmentarlos y re ensamblarlos para que sean enviados a la capa de red para su transmisión. Asegurar que todos los paquetes lleguen de manera correcta al nodo destino, realizar un control de flujo de extremo a extremo, el establecimiento, mantenimiento y cierre de la conexión.
- **Capa de Sesión:** Se encarga de mantener una comunicación estable o sincronizada entre las aplicaciones de usuario desde el extremo de origen al extremo final en la transferencia de datos. Esta capa además proporciona tres funciones importantes control del diálogo (full-dúplex o half-dúplex), agrupamiento y recuperación.
- **Capa de Presentación:** Es la delegada de negociar el formato (sintaxis y semántica) a los datos, comprimirlo, encriptarlos, de tal manera que puedan ser revertidos al llegar a su destino durante su transmisión.

- **Capa de Aplicación:** provee de una interfaz de usuario para que pueda interactuar con los servicios y aplicaciones que se comparten en las redes. Algunos servicios son el Web, el e-mail, servidor de base de datos, SSH, DNS, etc., además de algunas aplicaciones empresariales como la Planificación de Recursos Empresariales (ERP, Enterprise Resource Planning), la Administración de Relaciones con el Cliente (CRM, Customer Relationship Management) DSS, facturación, etc.

Figura 34*Caracterización del modelo OSI y sus principales funciones*

Nota. La figura es una representación general del Modelo OSI y sus principales funciones capa por capa. Obtenido de: (Autoayudacisco, 2010).

5.2 Análisis y funcionamiento capa por capa

Para una mejor comprensión y motivación en este tema, conviene enfatizar que el modelo OSI es muy importante pues permite asegurar mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnologías de red. Así mismo facilita comprender como los datos viajan desde los programas de

aplicación a través de un medio de trasmisión a otro usuario ubicado en otros nodos de la red. Más importante aún, el entender las funciones básicas que se producen en cada capa del modelo OSI, son la base del diseño y creación de redes de datos, la implementación de programas de software de red, la configuración de servicios y el diagnóstico de fallas en las redes.

Las siete capas representan las operaciones de transmisión de datos comunes a todos los tipos de entrega de datos entre las redes informáticas" (Oracle, 2010). La Tabla 3 describe las funciones específicas durante la transferencia:

Tabla 3

Capas del modelo OSI

N.º de capa	Nombre de capa	Descripción
7	Aplicación	Se compone de los servicios y aplicaciones de comunicación estándar que el usuario puede emplear al rededor del mundo.
6	Presentación	Se asegura de que la información se transfiera al sistema destinatario de un modo comprensible para el sistema.
5	Sesión	Sincroniza las conexiones y terminaciones entre los sistemas que cooperan.
4	Transporte	Administra la transferencia de datos de extremo a extremo. Asimismo, garantiza que los datos recibidos sean idénticos a los transmitidos.
3	Red	Administra las direcciones lógicas IP, la búsqueda de la ruta y la transferencia entre redes.
2	Enlace de datos	Administra la transferencia de datos en el medio de transmisión basada en el direccionamiento físico, así como en la tecnología de red.
1	Física	Define las características físicas, técnicas, y mecánicas de los medios de transmisión.

Nota. La tabla muestra las 7 capas del modelo OSI, así como la descripción de cada una de ellas respectivamente

5.3 Tipos de señales capa por capa

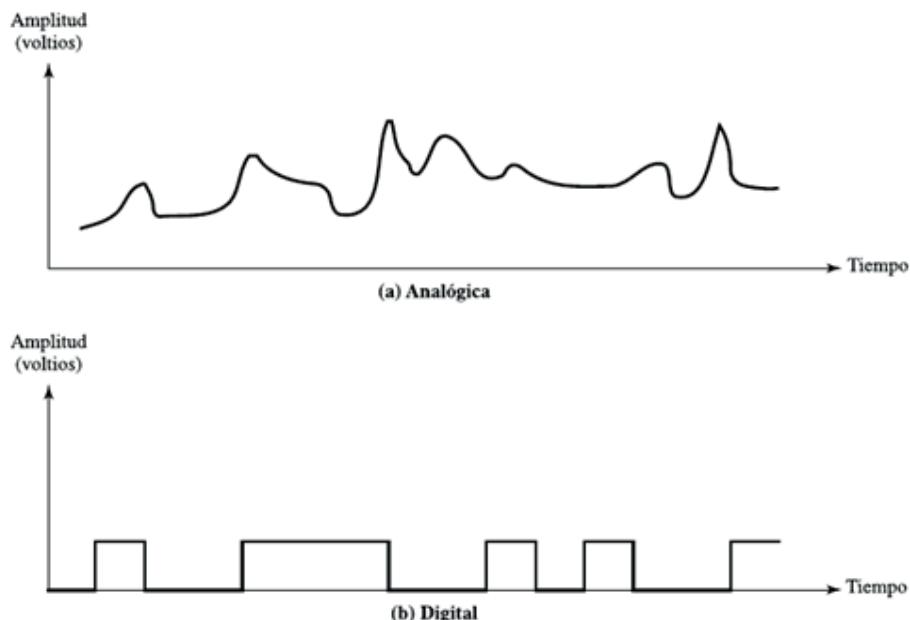
La Figura 33 del apartado 5.1 muestra las diferentes señales capa por capa. En relación a las señales de la capa física, por ejemplo, (CISCO-CCNA, 2020) señala que esta capa física dota de los medios para transportación de los bits que componen la trama de la capa de enlace de datos. El envío de tramas de la capa de enlace se la realiza a través de medios de transmisión que requiere los siguientes elementos de la capa física:

- Medios físicos o inalámbricos con conectores asociados;
- Una representación de los bits en los medios;
- Codificación de los datos y de la información de control;
- Sistema de circuitos del receptor y transmisor en los dispositivos de red.

Por otra parte, (Muñoz, 2017) plantea los tipos de señales durante la transmisión de datos sea analógica o digital. La Figura 35 muestra una representación de los tipos de señal:

Figura 35

Tipos de señales en la Capa Física del modelo OSI



Nota. La figura representa los tipos de señales, analógica y digital, en la cual se observa su forma y movimiento de acuerdo a su tipo. Obtenido de: (Muñoz, 2017)

5.3.1 Señal analógica y señal digital

- Una señal analógica es aquella en la que la intensidad de la señal varía gradualmente en el tiempo. Es decir, no presenta saltos o discontinuidades bruscas;
- Una señal digital es aquella en la que la intensidad se mantiene constante durante un determinado intervalo de tiempo, tras el cual la señal

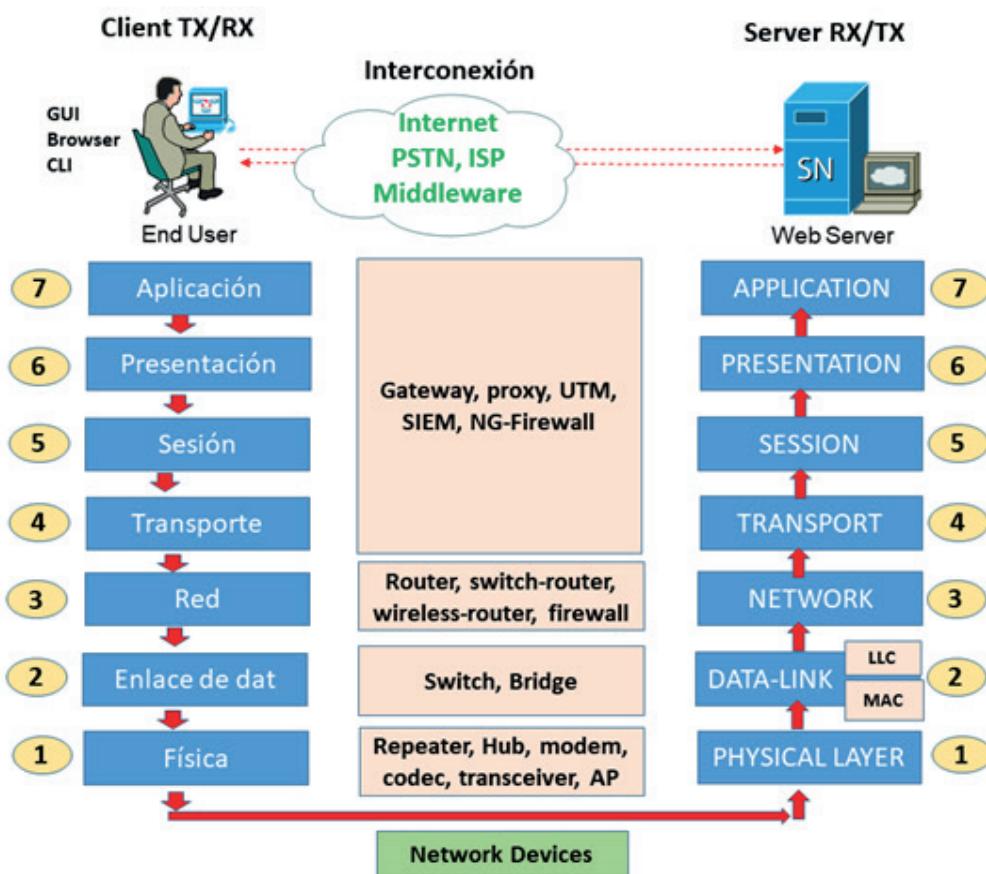
cambia a otro valor constante. La señal continua puede corresponder a voz y la señal discreta puede representar valores binarios (0 y 1).

5.4 Tipos de dispositivos capa por capa

Como se mencionó cada capa tiene un propósito específico. De esta forma cada capa posee uno o varios tipos de dispositivos diferentes que le permitan cumplir con su función de forma adecuada. La Figura 36 es una abstracción que describe en qué capa funcionan los diversos dispositivos de red, que fueron analizados en apartados anteriores.

Figura 36

Dispositivos por capa del modelo OSI



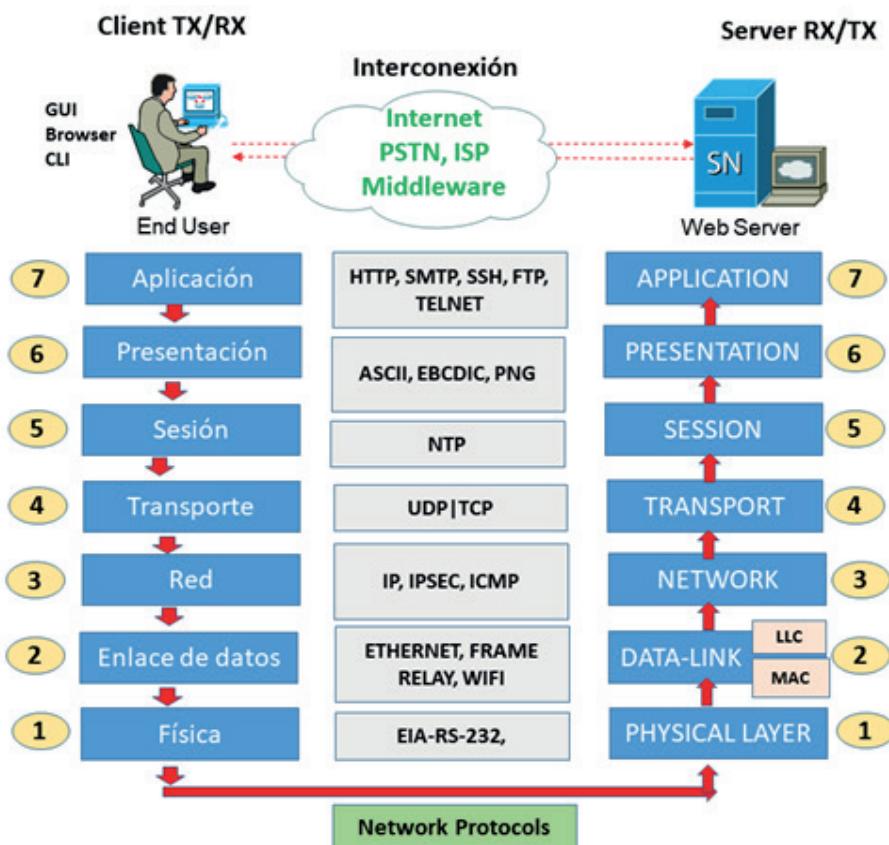
Nota. La figura representa los dispositivos de red por capas en relación al modelo OSI

5.5 Protocolos capa por capa

Cada una de las capas del Modelo OSI posee diferentes protocolos cuyo funcionamiento proporcionan reglas, normas, y estándares de calidad que favorecen el uso y una correcta transferencia de datos. La Figura 37 ilustra los más representativos:

Figura 37

Protocolos de comunicaciones capa por capa del modelo OSI



Nota. La figura representa los protocolos de comunicaciones de red capa por capas y su relación con el modelo OSI

Recursos complementarios

- Video sobre “Qué es el MODELO OSI Explicado de manera sencilla | Curso de redes y networking | Alberto López” 
- Video sobre “Modelo OSI Animación Español | Un resumen completo-Redes desde CERO hasta Avanzado” 
- Video sobre “Dispositivos de interconexión de red en el modelo OSI” 

Actividad de aprendizaje 5

Descripción de la actividad

Para poner en funcionamiento redes de computadoras la industria utiliza el típico diseño de red LAN jerárquica centralizada de campus empresarial de tres capas, el cual incluye la Capa de Acceso, la Capa de Distribución nivel 1 y nivel 2, y la Capa de Núcleo. Las ventajas de una red jerárquica favorecen la escalabilidad y la redundancia, e incrementan el rendimiento y la eficiencia de su administración.

Desarrolle una investigación bibliográfica en la que se describa el diseño de red LAN jerárquica centralizada de campus empresarial de tres capas caracterizando cada una de ellas. Luego migre ese nuevo conocimiento al simulador Packet Tracer de CISCO, póngalo en funcionamiento, y verifique la conectividad. Al finalizar, elabore un informe de laboratorio con la siguiente estructura: Tema, Objetivos de aprendizaje, Topología de prueba en la que se incluya materiales y equipos, Marco teórico, Desarrollo de la práctica, Conclusiones y Referencias bibliográficas.

Autoevaluación Capítulo 5

1. ¿El modelo OSI es un modelo de red?

Descriptivo de sistemas cerrados, basado en siete capas

Descriptivo de sistemas abiertos, basado en siete capas o niveles de red

Descriptivo de sistemas abiertos, basado en seis niveles de red

2. ¿La capa responsable de ofrecer una transmisión correcta y libre de errores es?

Capa de transporte

Capa de sesión

Capa de red

3. ¿El análisis y funcionamiento capa por capa prioritariamente permite comprender?

Como se produce el desarrollo de redes

El desarrollo de software de red

Como los datos viajan desde los programas a través de un medio

4. ¿La capa encargada de enrutar los paquetes desde punto de inicio hasta el punto final, sin necesidad de una conexión directa es?

La capa de Transporte

La capa de Enlace

La capa de Red

5. Señale cuál de las capas es la responsable de mantener una comunicación estable o sincronizada entre aplicaciones de usuario de extremo a extremo

La capa de Sesión

La capa de Presentación

La capa de Aplicación

6. Señale cuál de las siguientes capas es la que provee una interfaz de usuario para que pueda interactuar con los servicios y aplicaciones.

La capa Física

La capa de Presentación

La capa de Aplicación

7. De las siguientes opciones, indique el medio de transmisión por el cual se realiza el envío de tramas de la capa de enlace

Dispositivos de entrada y salida de datos

Medios físicos o inalámbricos con conectores asociados

Enrutador de paquetes desde punto de inicio hasta punto el final

8. Cuál de las siguientes opciones describe los protocolos de comunicaciones del modelo OSI

Repeater, Hub, Modem

UTM, SIEM, NG-Firewall

HTTP, SMTP, SSH, FTP, TELNET

9. ¿El envío de tramas de la capa de enlace se la realiza a través de qué medios?

Físicos e inalámbricos

Virtuales

Ninguna de las anteriores

10. ¿La capa de enlace está subdividida en?

MAC

LLC

MAC Y LLC



<https://acortar.link/jUKOUU>

CAPÍTULO VI

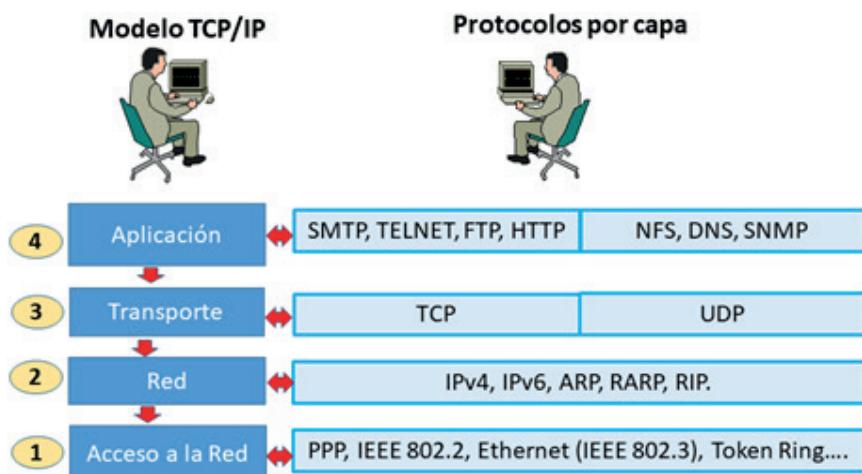
Modelo de capas TCP/IP

6.1 Introducción

Hoy en día los usuarios de computadoras se encuentran conectados a una red específica (Internet, Intranet, nube computacional, etc.) y lo hacen al emplear el modelo de capas TCP/IP. Este modelo es una suite de protocolos de comunicación de red distribuido en cuatro capas, que permiten la transferencia de datos en redes, entre equipos informáticos e Internet. TCP/IP es anterior al modelo de referencia ISO/OSI y ha permitido el desarrollo exponencial de los servicios de Internet. La Figura 38 muestra sus capas y los protocolos en cada capa.

Figura 38

Modelo de Capas TCP/IP



Nota. La figura representa una abstracción del modelo de capas y TCP/IIP

El protocolo TCP/IP se originó a partir del Proyecto del Departamento de Defensa de los Estados Unidos conocido como DARPA en 1969. En 1983 TCP/IP se estableció como estándar que finalmente se convirtió en el más usado en redes e Internet. Los protocolos que originan su nombre son:

- TCP: Es el Protocolo de Control de Transmisión que hace posible establecer una conexión y el intercambio de datos entre dos equipos de usuario final o networking, el cual brinda un transporte confiable de datos.
- IP: O protocolo de Internet, utiliza un direccionamiento universal de cuatro octetos con formato de punto decimal o binario, que transporta los datos a otros equipos de la red.

6.2 Caracterización del modelo TCP/IP

La suite o familia de protocolos TCP/IP describe un conjunto de normas generales de operación con las siguientes características:

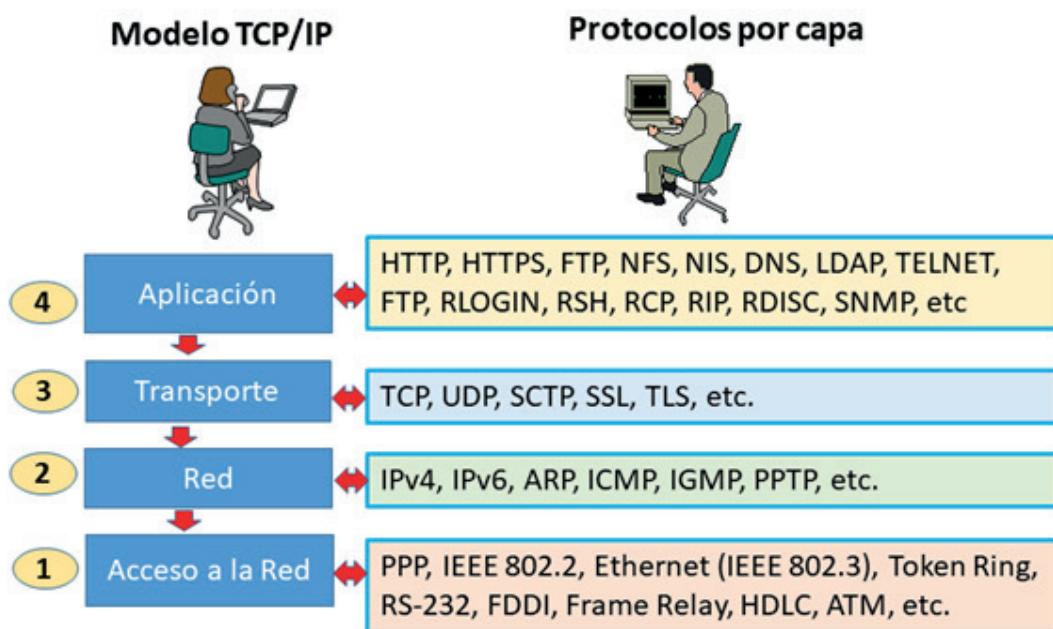
- Son estándares de protocolos abiertos sin propietario cuyo desarrollo e innovación se realiza por consenso, con un enfoque de compatibilidad.
- Es independiente del software o hardware, característica que otorga interoperabilidad de dispositivos de diferentes fabricantes, no solo a Internet sino en las LAN, WLAN, MAN, PAN y WAN.
- Provee un esquema común y universal de direccionamiento que permite a un dispositivo con TCP/IP localizar a cualquier otro en cualquier punto de la red alrededor del mundo.
- Son protocolos estandarizados de alto nivel que soportan servicios al usuario, aplicaciones diversas y sistemas multiplataforma, tanto para grandes, medianas y pequeñas redes, sean empresariales o domésticas.
- Es el protocolo estándar que se utiliza a nivel mundial para conectarse a Internet y a los servidores Web.
- El modelo de capas TCP/IP es muy útil respecto a otros protocolos de redes de datos. Una de ellas es la posibilidad de trabajar sobre una extensa gama de equipos y dispositivos de hardware y software.
- TCP/IP soporta múltiples tipos de sistemas operativos o plataformas.
- A diferencia del modelo OSI, TCP/IP apenas se conforma de cuatro capas: Aplicación, transporte, Internet y Acceso a la Red. La función de cada capa es suministrar servicios a las capas superiores e inferiores (i.e., encapsulamiento y des encapsulamiento) de tal modo que esos servicios se lleven a cabo.

6.3 Análisis y funcionamiento capa por capa

TCP/IP es un conjunto de reglas, normas y protocolos estandarizados que permiten a los usuarios de equipos y dispositivos puedan comunicarse en una red local (LAN), inalámbrica (WLAN, WIMAX), extendida (WAN) o al Internet. A continuación, se describen capa por capa los protocolos más utilizados (ver Figura 39):

Figura 39

Protocolos, servicios y aplicaciones del modelo TCP/IP capa por capa



Nota. La figura representa una abstracción del uso de la suite de protocolos TCP/IP.

6.3.1 Capa de acceso a la red

Se encuentra en la capa uno (1) que es la inferior en donde se decide cómo encapsular un paquete IP en una trama que pueda ser transmitida por la red (i.e. típicamente una trama Ethernet en la LAN). En esta capa también se especifica qué cualidades del hardware se usarán para acceder a cualquier LAN, WLAN, MAN, PAN y WAN y cómo deben transmitir los datos.

Ejemplos de protocolos que operan en esta capa son Ethernet (IEEE 802.3x), Token Ring, RS-232, FDDI, PPP, IEEE 802.2. No se debe perder de vista que esta capa correspondería a la capa física y la de enlace de datos del modelo OSI fusionadas. Finalmente, cabe señalar que el modelo de capas TCP/IP es independiente del medio de transmisión.

6.3.2 Capa de Red del modelo TCP/IP

La función de la capa de red o Internet del modelo TCP/IP o capa IP es aceptar y transferir paquetes para la red. Incluye los siguientes protocolos:

- **IP (Internet Protocol):** Es el núcleo de todo el modelo. Se encarga de especificar la dirección IP y el enrutamiento que tiene que seguir el paquete (coordenadas). Es el responsable del direccionamiento universal la versión IP-v4 e IP-v6 de nueva generación. Incluye la comunicación host a host y agrupa paquetes en unidades conocidas como datagramas.
- **ICMP (Internet Control Message Protocol):** Proporciona mensajes de diagnóstico y notificación de errores cuando falla la conectividad, es decir comprueba si una dirección destino está activa y es alcanzable o no.
- **ARP (Adress Resolution Protocol):** Se encuentra entre la capa de enlace de datos y la capa de Internet del modelo TXP/IP. Es utilizada para resolver una dirección lógica IP en función de su dirección física o MAC.
- **RARP (Reverse Address Resolution Protocol):** A contrario que el protocolo ARP, es decir, dada una dirección física MAC resuelve su dirección lógica IP.
- **NAT (Network Address Translation):** Traduce la dirección IP privada a una pública. Permite que los equipos y dispositivos de redes utilicen un rango de direcciones IP privadas y se conecten a Internet traduciendo una única dirección IP pública. Además, se utiliza para conectar redes domésticas a Internet.
- **RIP (Routing Information Protocol):** Usado por los enrutadores para intercambiar información de las distintas redes especialmente de pequeñas y medianas empresas. La versión 2 es la más reciente y utiliza el número de saltos (máximo 30) como métrica principal para enviar actualizaciones a la tabla de enrutamiento.
- **OSPF (Open Shortest Path First):** Utilizado por los empresarios para intercambiar información entre las distintas redes especialmente de las grandes compañías. Es un protocolo para enrutamiento jerárquico de pasarela interior (Interior Gateway Protocol, IGP), que usa el algoritmo Dijkstra para determinar la ruta más corta entre dos nodos y utiliza métricas de estado de enlace.

6.3.3 Capa de Transporte (TCP)

La función de la capa de transporte del modelo TCP/IP es asegurar que los paquetes lleguen sin errores y en secuencia a su destino. Esta capa se divide en dos protocolos importantes, UDP y TCP.

- **UDP (User Datagram Protocol):** Implementa una transmisión no confiable ni libre de errores. Típicamente se emplea en aplicaciones de video streaming con actualizaciones en tiempo real;
- **TCP (Transmission Control Protocol):** Implementa una transmisión confiable de datos ya que introduce una conexión entre transmisor y receptor antes de que envíen los datos. Es mucho más complejo ya que incluye detección de errores, retransmisión y otras formas de rescatar los datos perdidos.

6.3.4 Capa de Aplicación

En esta capa se definen las aplicaciones de red y los servicios de Internet estándar que puede utilizar el usuario. Estos servicios y aplicaciones emplean la capa de transporte para enviar y recibir datos. Algunas aplicaciones típicas son Twitter, Netflix, Google, YouTube, etc. Entre los protocolos más importantes de esta capa están:

- **FTP (File Transfer Protocol):** Transferencia interactiva de archivos. Protocolo que ha perdido su vigencia por no cifrar los datos que se transmiten en la red. Utiliza el puerto lógico 20 para datos y 21 para control.
- **TELNET:** Iniciación de una sesión de forma remota o a distancia en servidores ubicados en lugares geográficos distintos. Utiliza el puerto 23. Ha sido reemplazado por protocolos que encriptan los datos durante la transmisión.
- **HTTP (Hypertext Transfer Protocol):** Transferir archivos que forman las páginas web de la World Wide Web. Utiliza el puerto 80 (HTTP) y 443 (HTPPS).
- **SMTP (Simple Mail Transfer Protocol):** Transferencia de mensajes de correo electrónico entrante y archivos adjuntos. Utiliza el puerto lógico 25.
- **DNS (Domain Name System):** Resolución del nombre de dominio de un equipo terminal de usuario a la dirección IP o viceversa. Utiliza el puerto 53 tanto por UDP como por TCP.

- **SNMP (Simple Network Management Protocol)** El Protocolo simple de administración de red (SNMP) permite ver la distribución de la red y el estado de los equipos clave. SNMP también permite obtener estadísticas de red complejas del software basado en una interfaz gráfica de usuario (GUI).

6.4 Comparación con el modelo OSI/ISO

Los protocolos que componen el modelo TCP/ IP también se pueden describir en términos del modelo de referencia OSI. La Figura 40 ilustra dicha relación. A continuación, se realizará un breve análisis capa por capa.

En la capa de acceso a la red, el modelo TCP/IP no especifica qué protocolo usar al enviar la data a medios de transmisión. Las capas 1 y 2 de OSI describen los pasos necesarios para acceder a los medios de transmisión para transportar datos a través de la red.

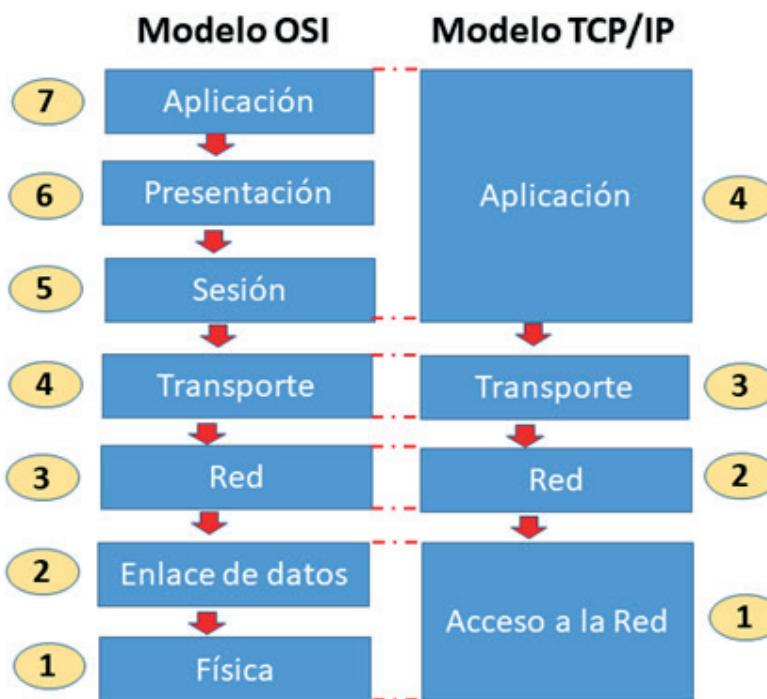
En la capa de red se encuentran las principales similitudes de ambos modelos, por ejemplo, a nivel de tráfico de red. Sin embargo, los dos modelos tienen una relación diferente entre los servicios de las capas superiores e inferiores. En la capa de Internet de TCP/IP se emplean los protocolos que abordan y enrutan paquetes a través del Internet o de una red interna.

La capa de transporte OSI, corresponde directamente a la capa de transporte TCP/IP. Esta capa describe los servicios y características comunes que brindan una entrega ordenada y confiable de datos entre los servidores de origen y destino.

La capa de aplicación de TCP/IP comprende varios protocolos que proporcionan funciones específicas para muchas aplicaciones y servicios de usuario final. Los desarrolladores de software de aplicaciones utilizan las capas 5, 6 y 7 del modelo OSI como punto de referencia para crear aplicaciones que se ejecutan en la red.

Figura 40

Modelo de Capas TCP/IP y su relación con el modelo OSI.



Nota. La figura representa una comparación y relación entre los modelos OSI y TCP/IP. Obtenido de: (Lopez C. , 2018)

Recursos complementarios

- Información más detallada de las capas del modelo TCP/IP:
- Información más detallada de los protocolos en las distintas capas:
- Información más detallada de los protocolos TCP/IP:
- Información más detallada de: “Modelo de referencia TCP/IP | | UPV”

Actividad de aprendizaje 6

Descripción de la actividad

La capa de Internet del modelo TCP / IP se alinea con la capa 3 o de red del modelo OSI. Aquí es donde funciona el direccionamiento universal IP y el enrutamiento. De hecho, cuando los datos se transmiten desde un nodo en una LAN a otro nodo en otra LAN diferente, se utiliza la capa de Internet. Cómo se ha explicado, el direccionamiento IP-v4 e IP-v6 es fundamental en el diseño y puesta en ejecución de las redes de computadoras.

Se pide:

- Realice 10 ejercicios de transformación de numeración binaria a decimal y 10 de numeración decimal a binaria. Utilice la siguiente técnica:

1	1	1	1	1	1	1	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128+	64+	32+	16+	8+	4+	2+	1
=255							

1	1	0	1	1	0	1	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64		16	8		2	1

- Realice los siguientes ejercicios:

- Transforme 11.116.155.192(10) a binario;
- Transforme 128.110.46.251(10) a binario;
- Transforme 193.169.201.249(10) a binario;
- Transforme 10.31.197.224(10) a binario;
- Transforme 128.50.146.231(10) a binario;
- Transforme 195.179.211.248(10) to binario;

- Transforme 10.216.155.191(10) a binario;
- Transforme 129.016.115.229(10) a binario;
- Transforme 172.016.222.191(10) a binario;
- Transforme 173.31.155.254(10) a binario.

3. Realice 10 ejercicios de la Operación AND

4. Realice 10 ejercicios del siguiente tipo:

Dada la dirección IP: 192.10.101.66/26 calcule la dirección de red o subred.

5. Realice 10 ejercicios del siguiente Tipo:

- Cuántas direcciones de red y cuántas direcciones de host tienen las redes clase A, B o C.
- Cuántas direcciones de red y cuántas direcciones de host tienen la dirección 192.168.100.0/24
- Cuántas direcciones de red y cuántas direcciones de host tienen la dirección 172.16.32.0/19
- Cuántas direcciones de red y cuántas direcciones de host tienen la dirección 10.16.64.0/24

Al finalizar, elabore un informe que despliegue los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de los ejercicios, Conclusiones y Referencias bibliográficas.

Autoevaluación Capítulo 6

1. ¿En qué consiste la transmisión del protocolo TCP?

Punto de partida - Transmisión completa en orden de bytes - Punto de fin

Punto de inicio - Transmisión de datos - Punto de llegada

Punto inicial - Punto medio - Punto final

2. Las siglas ARP significan:

Address Reconnection Protocol

Address Resolution Protocol

Address Router Protocol

3. ¿Cuál es la función del protocolo UDP?

Proporciona un servicio de entrega de datagramas

Verifica las conexiones entre los hosts transmisores y receptores

Acepta y envía paquetes de red

4. ¿Cuáles son protocolos de la capa física o de acceso a la red del modelo TCP/IP?

NAT - IP - Ethernet

RARP - UDP - ARP

Ethernet - CSMA/CD

5. ¿Cuál es la función de la capa de aplicación?

Brindar acceso a las aplicaciones más frecuentes que se hayan utilizado en el dispositivo

Dar servicios de red que proporcionan la interfaz con el sistema operativo para que el usuario pueda interactuar acorde con la máquina

Proporcionar acceso a las aplicaciones más recientes que se hayan ejecutado en segundo plano

6. En la capa de transporte ¿Qué implementa el UDP (User Datagram Protocol)?

Implementa una transmisión no fiable, es decir, que no está libre de errores

Implementa un datagrama de usuarios para facilitar el acceso a la información

Implementa métodos de seguridad para los datos de los usuarios

7. ¿Qué servicio de nombres proporciona nombres de host al servicio de direcciones IP?

UNIX

Archivos/etc

NIS

DNS

8. ¿De qué se encarga el protocolo de resolución de direcciones (ARP) de la capa de acceso a la red?

Este protocolo se encarga de administrar las direcciones de datos que reciba el dispositivo

Este protocolo puede direccionar los datos enviados desde el dispositivo

Este protocolo es responsable de la asociación exacta de direcciones IP con direcciones Ethernet físicas

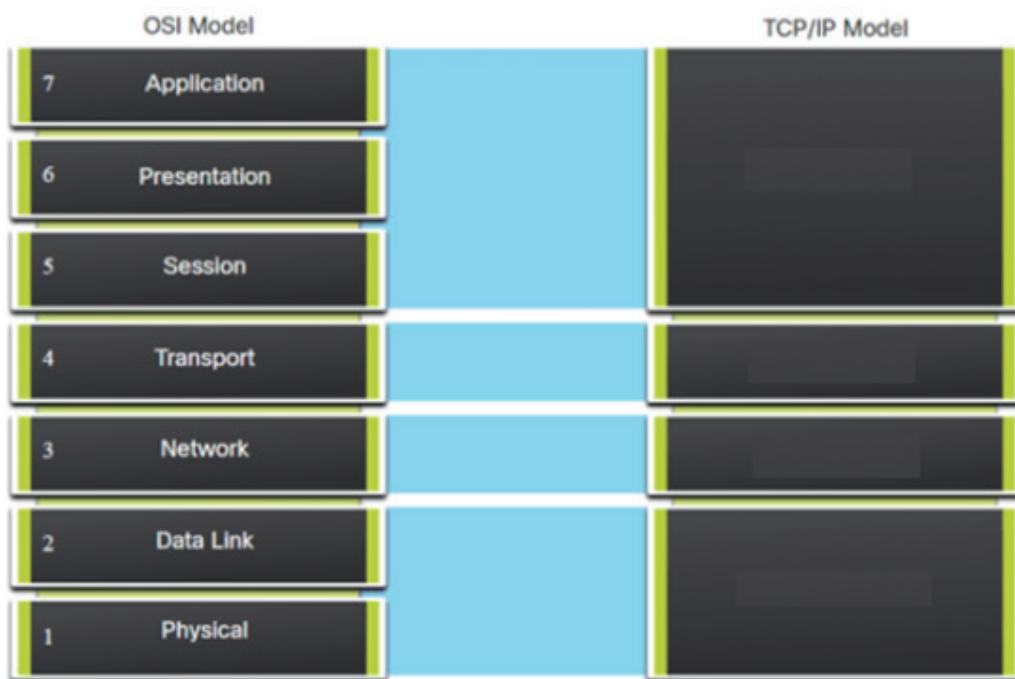
9. Cuál es la definición del protocolo de administración de red

El Protocolo completo de administración de red (SNMP) permite ver la distribución de la red y el estado de los equipos clave

El Protocolo simple de administración de red (SNMP) permite ver la distribución de la red y el estado de los equipos clave

El Protocolo simple de administración de red (SNMP) permite ver la distribución de la LAN y el estado de los equipos clave

10. Según la figura complete en forma descendente con las capas homólogas del modelo TCP/IP



Aplicación- Transporte - Internet - Acceso a Internet

Transporte -Aplicación- Internet - Acceso a Internet

Aplicación- Transporte - Acceso a Internet - Internet



<https://acortar.link/IGYDX7>

CAPÍTULO VII

Direcccionamiento IP

7.1 Dirección IP, Definición

Una dirección IP es una representación numérica única que significa la ubicación geográfica de un adaptador o interfaz de red. IP o Internet Protocol, se traduce como Protocolo de Internet e implica una serie de estándares necesarios para transmitir y recibir paquetes de datos a través de redes (Tanenbaum A. S., 2003).

De acuerdo con el estándar RFC (Request for Comments) 791, el Protocolo de Internet permite transmitir bloques de datos llamados datagramas desde un origen hacia un destino, en donde ambos son hosts identificados por direcciones de longitud fija. El Protocolo de Internet también permite, si es necesario, la fragmentación y el reensamblaje de datagramas largos para su transmisión a través de redes de “paquetes pequeños” (Information Sciences Institute, University of Southern California, 1981). Existen dos tipos de direcciones IP:

- IP versión 4 (IPv4) que tiene una longitud de 32 bits, 2^{32} direcciones únicas y se expresa en forma decimal. Por ejemplo: 192.168.100.1;
- IP versión 6 (IPv6) que tiene una longitud de 128 bits, 2^{128} direcciones únicas y se expresa en forma hexadecimal. Por ejemplo: fe80:0000:0000:0000:44e3:baf5:50f6:fe51.

7.2 Caracterización del Direccionamiento IP

Entre las características más relevantes del direccionamiento IP se tienen las siguientes:

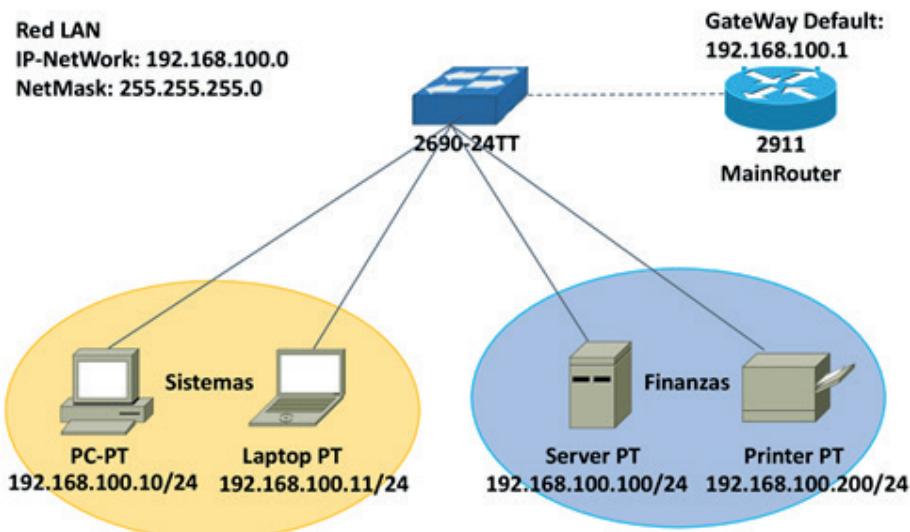
- Las direcciones IP pueden ser generadas por la CPU como direcciones lógicas, es decir aquellas que corresponden a la capa de red del modelo ISO/OSI o del modelo de capas TCP/IP.
- El direccionamiento posee un esquema jerárquico que identifica cada equipo de usuario final o dispositivo de networking de manera exclusiva, puesto que posee niveles que ayudan a transferir paquetes a través de las redes de telecomunicación.
- La dirección de red regularmente termina en cero (0) en los octetos del host para redes clase A y B, aunque no necesariamente en clase C.
- La dirección de broadcast o de difusión a todos se representa con todos los bits en uno (1) en la porción para el host de la dirección.

- La máscara de la red o subred, es una composición de bits que sirve para demarcar el espacio de una red de datos. Típicamente consiste en reemplazar los octetos de la red o subred con unos (1). Su función es revelar a los dispositivos, que parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte le corresponde al host.

La Figura 41, ilustra un ejemplo de cómo está distribuida una red LAN. Como se puede observar existen equipos de usuario final como los computadores personales, laptops, servidores e impresoras, que están conectados a los dispositivos de conectividad tales como comutadores o enruteadores a través de medios de transmisión (cables), que incluyen una dirección IP de red o host.

Figura 41

Diagrama de una red LAN



Nota. Diseño general de una red LAN mediante el software Packet Tracer, se puede apreciar distintos dispositivos conectados a un Switch mediante cable directo y este a su vez a un router. Todos incluyen direccionamiento IP.

7.3 Formato de un Paquete IP

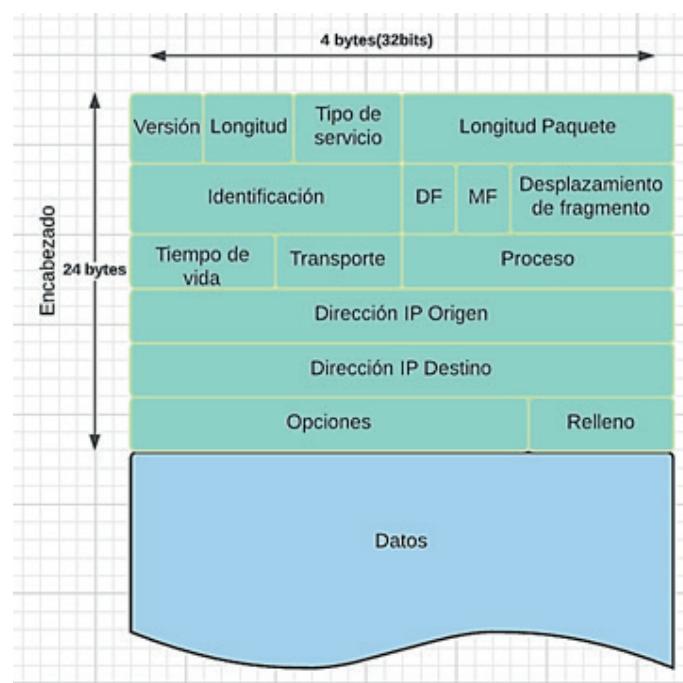
El formato de transferencia de los datos es definido por el protocolo IP que se esté utilizando. Está definido por el RFC 791 en donde se establecen las siguientes funciones (ver Figura 42):

- Especifica el formato preciso de los datos a medida que están en la Internet.

- El protocolo IP realiza la función de enrutamiento, al elegir la mejor ruta por la que se transmitirán los datos.
- IP engloba una amalgama de reglas que gobiernan la idea de una entrega de paquetes no confiable. Entre las reglas que incluye el protocolo IP se especifican:
 - Cómo los hosts y los enrutadores deben procesar los paquetes
 - Cómo y cuándo deben generarse los mensajes de error
 - Condiciones bajo las cuales los paquetes pueden descartarse

Figura 42

Formato de paquetes IP



Nota. La figura muestra que cada paquete IP contiene tanto un encabezado de 20 o 24 bytes de longitud. En él se distinguen 15 campos tales como la versión de la dirección IP, longitud, tipo de servicio, longitud de cabecera del paquete, tiempo de vida, banderas, desplazamiento del fragmento, número de protocolo, direcciones IP origen y de destino, además de otros campos que ayudan a enrutar el paquete.

7.4 Redes Classful

En el RFC 1981 publicado en el año 1996 se propuso el particionamiento de las direcciones IP. Debido al acelerado crecimiento que tuvo el Internet desde su aparición, fue necesario la creación de un método que permitiera extender la vida útil de las direcciones IPv4, para ello se planteó que los hosts de empresas que utilizan IP se dividan en tres categorías:

- Hosts que no requieren acceso a hosts en otras empresas o el Internet.
- Hosts que necesitan acceso a un conjunto limitado de servicios externos. Por ejemplo, correo electrónico, protocolo de transferencia de archivos (FTP), acceso remoto (SSH), entre otros.
- Hosts que necesitan acceso a la capa de red del modelo OSI fuera de la empresa suministrada a través de una conexión segura IP.

Los hosts de la primera y segunda categoría se consideraron privados, y los de la tercera categoría públicos (Rekhter, Cisco Systems, & Moskowitz, 1996).

El estándar RFC 1981 fue el origen de la clasificación de redes Classful que existe en la actualidad. Conceptualmente una dirección IPv4 Classful tiene tres porciones, red, subred y host definidos por la máscara y las reglas de la Clase A, B, y C. La porción de Red, que indica la dirección de la red o subred. La porción del Host, que indica la dirección del host asociado a la dirección de red correspondiente (ver Figura 42). Además, se debe considerar que las redes Classful IPv4 se categorizan en dos clases adicionales (ver Figura 43).

- Las direcciones de clase D se utilizan para Multicast
- Las direcciones de clase E están reservadas para propósitos investigativos o experimentales

Por otro lado, la Autoridad de Números Asignados de Internet ((Internet Assigned Numbers Authority, IANA) ha reservado los siguientes tres bloques de espacio de direcciones IP para Internet privado establecidos en el RFC 1918 (Direcciones Privadas):

Clase de Red	Rango inicial	Rango final
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

Figura 43
Clases de Redes Classful

RED CLASE A			
RED	HOST	HOST	HOST
0 0 0 0 0 0 0 0	0 0 0 0 1 0 1 0	0 1 1 0 0 1 0 1	0 0 1 0 0 0 0 0
0 1 1 1 1 1 1 1			
Dirección inicial: 1.0.0.0 Dirección final: 126.255.255.255			
Nº de Redes: $2^7-2=126$ Nº de host: $2^{24}-2=16777214$ Netmask by default: 255.0.0.0			
RED CLASE B			
RED	RED	HOST	HOST
1 0 0 0 0 0 0 0	0 0 0 0 1 0 1 0	0 1 1 0 0 1 0 1	0 0 1 0 0 0 0 0
1 0 1 1 1 1 1 1			
Dirección inicial: 128.0.0.0 Dirección final: 191.255.255.255			
Nº de Redes: $2^{14}-2=16384-2=16382$ Nº de host: $2^{16}=65536$ Netmask by default: 255.255.0.0			
RED CLASE C			
RED	RED	RED	HOST
1 1 0 0 0 0 0 0	0 0 0 0 1 0 1 0	0 1 1 0 0 1 0 1	0 0 0 0 0 0 0 0
1 1 0 1 1 1 1 1			
Dirección inicial: 192.0.0.0 Dirección final: 223.255.255.255			
Nº de Redes: $2^{21}-2=2097152$ Nº de host: $2^8-2=256$ Netmask por default: 255.255.255.0			

Nota. Clasificación de direcciones IP según el direccionamiento Classful. Obtenido de: IP Addressing Guide (Cisco, IP Addressing Guide, 2010)

Figura 44
Características de las 5 Clases

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Nota. La figura incluye datos de cada clase como bit identificador, bits para dirección de red, bits para dirección de host, numero de subredes, entre otros. Obtenido de: Introduction of Classful IP Addressing (GeeksforGeeks, 2019)

7.5 Redes Classless

Las redes sin clase, superredes o Classless adoptan un enfoque que es complementario al direccionamiento de subredes Classful. En lugar de utilizar un único prefijo de red IP para distintas redes físicas, permite que las direcciones asignadas a una organización abarquen varios prefijos clasificados. Conceptualmente una dirección IPv4 tiene dos porciones, el prefijo y el host definidos por la máscara, sin tener consideración del tipo de clase A, B, o C, tal como lo hace una dirección Classful.

Para comprender el funcionamiento de las superredes, como ejemplo se considera una organización de tamaño mediano que requiere conectarse a Internet la cual debería utilizar internamente una única dirección de clase B por dos razones:

- La dirección de clase C no puede disponer de más de 254 hosts.
- La dirección de clase B tiene suficientes bits para que la división en subredes sea eficiente.

Por tanto, conviene usar una dirección Classless para enfrentar el problema del agotamiento de direcciones IPv4 y especialmente para detener el crecimiento de las tablas de enrutamiento en los enrutadores de Internet.

Las direcciones Classless técnicamente son conocidas como el CIDR por su acrónimo en inglés Classless Inter-Domain Routing (enrutamiento entre dominios sin clases). El CIDR es un mecanismo para ampliar el marco de direcciones IP. Aunque en un principio se concibió como una solución temporal, ha sido utilizado más de dos décadas y parece que mantendrá su posición en los próximos años.

Un mecanismo clave del CIDR es el enmascaramiento de subredes de longitud variable (Variable Length Subnet Mask, VLSM). Este mecanismo permite que puedan implementarse subredes con máscaras de longitudes variables y no solo el enmascaramiento de subredes de longitud fija (Fixed Length Subnet Mask, FLSM), que generan desperdicio de direcciones IP.

7.6 Herramientas para direccionamiento IP

En Internet existen calculadoras de subredes IP gratuitas. En ellas se debe ingresar datos como la clase de red, la dirección IPv4 y la máscara de subred para obtener información sobre las posibles direcciones de red, los rangos de host utilizables, la clase de IP, entre otros.

Figura 45*Calculadora de Subredes IP*

IP Subnet Calculator

This calculator returns a variety of information regarding Internet Protocol version 4 (IPv4) and IPv6 subnets including possible network addresses, usable host ranges, subnet mask, and IP class, among others.

IPv4 Subnet Calculator

Network Class	<input type="radio"/> Any	<input checked="" type="radio"/> A	<input type="radio"/> B	<input type="radio"/> C
Subnet	255.255.255.254 /31			
IP Address	110.71.135.99			
<input style="background-color: #4CAF50; color: white; padding: 5px 10px; border: none; border-radius: 5px; font-weight: bold; margin-right: 10px;" type="button" value="Calculate"/> <input style="background-color: #BDBDBD; border: none; border-radius: 5px; padding: 5px 10px; font-weight: bold;" type="button" value="Clear"/>				

Nota. Calculadora de la Página Web IP Subnet Calculator. Obtenido de: <https://www.calculator.net/ip-subnet-calculator.html>

7.7 Ejercicios de transformación de decimal a binarios y vice-versa

Para fortalecer el aprendizaje de redes, como estrategia de aprendizaje, los estudiantes o profesionales deben resolver ejercicios o problemas reales. Con ello se consigue el desarrollo de habilidades, destrezas, conocimientos y las competencias esperadas mediante el ensayo, la práctica y la experiencia. A continuación, se presentan diversos tipos de ejercicios de matemática de redes para profundizar en el aprendizaje. Cabe señalar que en la Web existen un sinúmero de fuentes con ejercicios y sus respectivas respuestas que incrementarían las aptitudes de estudiantes y profesionales.

- Transformar el número 255 (base 10) a binario

1	1	1	1	1	1	1	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128+	64+	32+	16+	8+	4+	2+	1

=11111111

- Transformar el número 00001010 (base 2) a decimal

0	0	0	0	1	0	1	0
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
0	0	0	0	8+	0	2+	0
=10							

- Transformar el número 10101010 (base 2) a decimal

1	0	1	0	1	0	1	0
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128+	0+	32+	0+	8+	0	2+	0
=170							

Recursos complementarios

- Video sobre “¿Qué es la Dirección IP y para qué sirve?” 
- Video sobre “La cabecera del datagrama IPv4 | UPV” 
- Video sobre “Curso de Redes 2020 para principiantes # 6 Direccional-
miento IP” 
- Video sobre “Video 14 Direccionamiento IP modelo Classful” 

Actividad de aprendizaje 7

Descripción de la actividad

Una dirección IP es una representación numérica única que simboliza la ubicación geográfica de un adaptador o interfaz de red. IP o Internet Protocol, se traduce como Protocolo de Internet y describe una serie de estándares necesarios para crear y transmitir paquetes de datos a través de redes (Tanenbaum A. S., 2003).

De acuerdo con el estándar RFC (Request for Comments) 791, el Protocolo de Internet permite transmitir bloques de datos llamados datagramas desde un origen hacia un destino, donde ambos son hosts identificados por direcciones de longitud fija. El Protocolo de Internet también permite, si es necesario, la fragmentación y el re ensamblaje de datagramas largos para su transmisión a través de redes de “paquetes pequeños”.

Esta actividad de aprendizaje se relaciona con identificar las clases de direcciones IP con el fin de fortalecer el aprendizaje de los estudiantes.

Se pide:

Realizar la Práctica de Laboratorio No. 7.1.4.9 de la Academia de Networking de Cisco titulada “Identificación de Direcciones IP-V4”.

Autoevaluación Capítulo 7

1. Para el direccionamiento físico MAC y el lógico IP, elija la correcta de las siguientes opciones:

Trabajan solamente en redes PAN

[Trabajan en la capa 2 y en la capa 3 del modelo OSI respectivamente](#)

Existen diferentes tipos de direccionamiento de redes estas son: H, J y K

2. ¿Cómo se le conoce combinación de bits que sirve para delimitar el ámbito de una red de datos?

Dirección de versión IPv4

[Máscara de subred](#)

Encabezado

3. El Internet Protocol (IP) especifica el formato de los paquetes que viajan por Internet, los cuales contiene encabezado y datos. ¿Cuál es la longitud del encabezado anteriormente mencionado?

De 20 o 24 bytes

De 1 a 2 bytes

De 0 a 8 bits

4. ¿Qué significa Fragment Offset dentro del formato de un paquete IP?

0 significa que es el último fragmento de este paquete, 1 significa que este no es el último fragmento

Es el número único el cual es asignado por el emisor y sirve para re ensamblar un paquete fragmentado

Es utilizado por los paquetes fragmentados para ensamblarlos por completo

5. Una de las clases de direcciones de red es la clase D, ¿Para qué uso está destinada?

Enrutamiento

Multicast IP

Enlace de secuencias IP

6. ¿Qué son las redes Classful?

Son protocolos con la función de transmitir la máscara de red en sus actualizaciones

Es el resultado de la unión de direccionamientos IPv4 e IPv6

Son redes usadas para soportar el uso de varias máscaras de subred de las clases A y B

7. ¿Cuáles son los protocolos de enrutamiento que soportan las redes Classful?

TCP - UDP

WAN y WLAN

RIP 1 e IGRP

8. ¿Qué son las redes Classless?

Disponen los primeros 4 bits de la clase C

Son redes que permiten una conexión más rápida con el extranet e intranet

Son protocolos para evitar limitaciones de los protocolos Classful

9. ¿Cuáles son los dígitos identificadores de las redes Clase C?

0

10

110

Ninguna respuesta es correcta

10. ¿Cuáles son los protocolos que soportan las redes Classless?

RIP 2, OSPF EIGRP, IS-IS y BGP

HTTP, HTTPS, POP3 y SMTP

DCCP, iSCSI, UDP, SCTP, IL y SPX



<https://acortar.link/lKeqil>

CAPÍTULO VIII

Subredes de Longitud Fija y Variable

8.1 Introducción

Las subredes son un método para incrementar el espacio de direcciones IPv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento de una red interna mayor. Se le considera una subred a la división de una red general la cual contiene un conjunto de interfaces, posee máscara de red, rango de direcciones IP y asume una tecnología de interconexión como enlace punto a punto de múltiples accesos. En cualquier clase de dirección (A, B o C), las subredes proporcionan un medio de asignar parte del espacio de la dirección de host a las direcciones de red, lo cual permite tener más redes y direcciones IP. Las subredes proporcionan los siguientes beneficios para los administradores de red y usuarios:

- Evita difusiones o retransmisiones innecesarias
- Aumenta las opciones de seguridad
- Simplifica la administración
- Controla el crecimiento

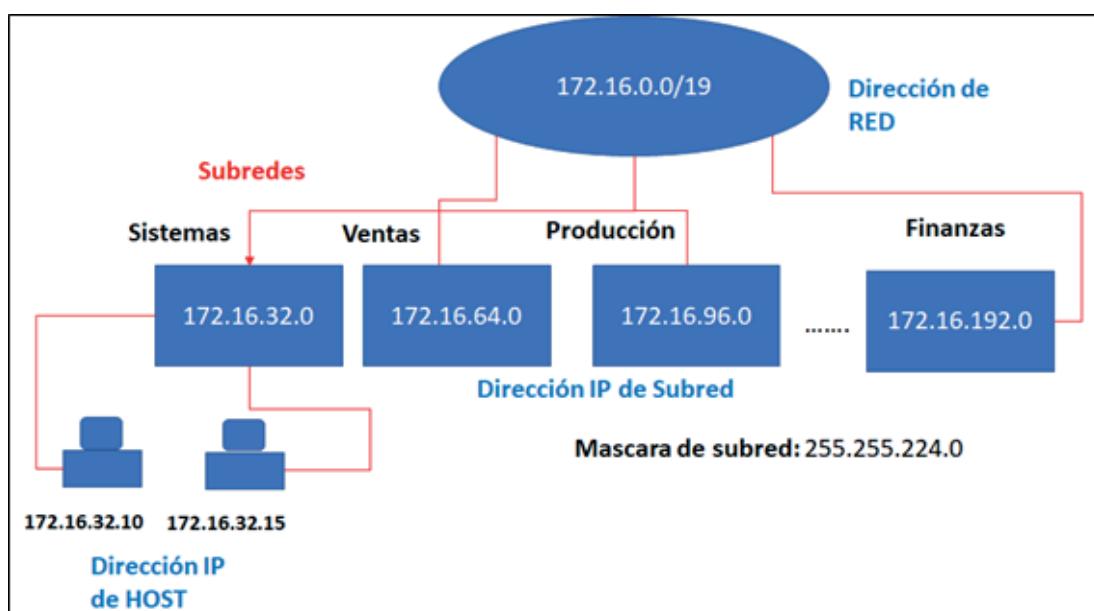
Las subredes se utilizan para redes de área local conectadas a Internet. Todos los dispositivos que están conectados a una misma subred pueden generar directamente una comunicación entre sí. Sin embargo, los dispositivos que se encuentran fuera de dicha subred deberán comunicarse a través de un router. La utilización de la subred reduce el tráfico de datos en general y sobre todo agrega una capa adicional de seguridad a todos los dispositivos y datos conectados en la misma. Esto debido a que todos los datos deben transmitirse a través del router el cual posee capacidades de firewall (dispositivo de hardware o software de seguridad de la información que monitorea y filtra los paquetes entrantes).

8.2 Subredes de longitud fija/variable

Un esquema de direccionamiento es una forma de especificar cómo se va a repartir la capacidad de numeración de hosts que tiene cierta red. Consta de una dirección de red base, una máscara de red, de subred y las direcciones IP de las subredes. Existen dos esquemas de división de una red de computadoras: Mascaras de Subredes de Longitud Fija (FLSM) y Mascara de subredes de Longitud Variable (VLSM). A continuación, se describe cada una de ellas.

Con la máscara de subred de longitud fija (Fixed Length Subnet Mask, FLSM), se asigna la misma cantidad de direcciones IP a cada subred. Si todas las subredes tuvieran los mismos requisitos en cuanto a la cantidad de hosts, estos bloques de direcciones de tamaño fijo serían suficientes. Sin embargo, esto no es lo que suele suceder. La FLSM se utiliza para el direccionamiento con clases. La FLSM también se suele denominar “división tradicional en subredes”. La Figura 46 es una representación visual de cómo una red clase B puede ser dividida en varias subredes de longitud fija.

Figura 46
Subredes de longitud fija



Nota. La figura representa el método clásico de dividir una red en subredes con máscara de longitud fija.

Las máscaras de subred de tamaño variable (Variable Length Subnet Mask, VLSM) representan otra de las tantas soluciones que se implementaron para el agotamiento de direcciones IP y otras como la división en subredes, el enruteamiento de Inter dominio sin clases (CIDR), NAT y las direcciones IP privadas. Otra de las funciones de VLSM es descentralizar las redes y de esta forma conseguir redes más seguras y jerárquicas.

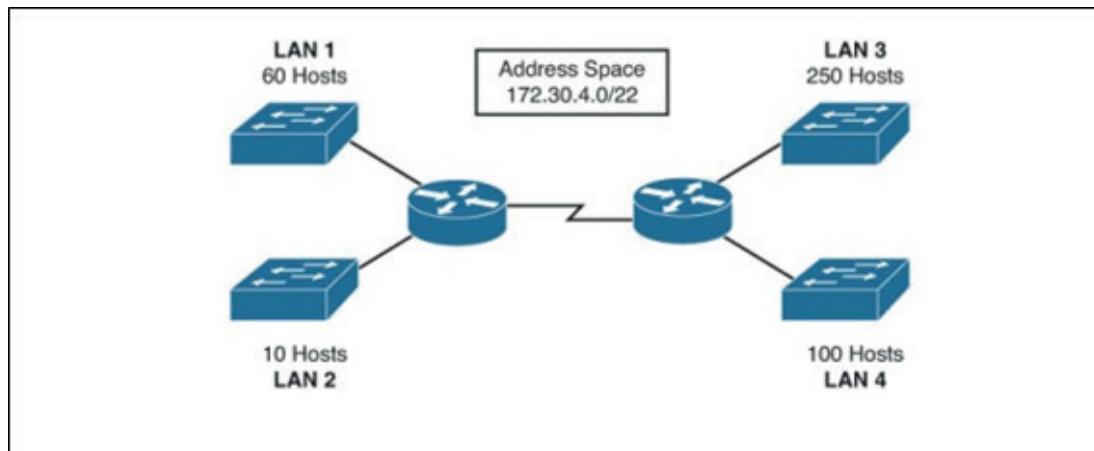
VLSM permite dividir un espacio de red en partes desiguales, es decir, la máscara de subred de una dirección IP variará según la cantidad de bits para hosts que se tomen prestados para una subred específica, se conoce también como división de subredes en subredes.

Las ventajas de VLSM:

- Evitar duplicación de direcciones
- Proporcionar y controlar el acceso
- Controlar seguridad y rendimiento

Figura 47

Topología de ejemplo de VLSM



Nota. La Figura 47 representa a las subredes, cada una de ellas para las cuatro LAN. Obtenido de: Cisco-NetAcad, “Conceptos y protocolos de enrutamiento” (Cisco, 2012).

8.3 Caracterización de las Subredes

A una subred se la puede considerar como una parte segmentada de una red, es decir, son una partición lógica de una red IP en múltiples segmentos. A continuación, se presentan las características relevantes de las subredes:

- La división en subredes mejora la eficiencia de asignación de direcciones.
- El tráfico no fluye a través de rutas innecesarias, de esta manera aumenta la velocidad de la red.
- Su tamaño dependerá de los requisitos de conectividad y la tecnología de red que se emplee.
- La subred de punto a punto permite que dos dispositivos se conecten, mientras que una subred de un centro de datos puede diseñarse para conectar mayores cantidades de dispositivos.

- Se las considera como un método para maximizar el espacio de direcciones IPv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento en una interred mayor.
- Proporcionan un medio de asignar parte del espacio de la dirección host a las direcciones de red, lo cual genera más redes.
- La parte del espacio de direcciones de host asignada a las nuevas direcciones de red se conoce como número de subred.
- Presenta ventajas como la seguridad de la información, administración simplificada y la reestructuración de redes internas sin afectar las redes externas.
- Los paquetes de datos que se envían recorren menor distancia.
- Las empresas tienen control total sobre los paquetes de datos y su tráfico.

Referente a los tipos de protocolos de enrutamiento classful y la classless se presentan las siguientes características:

Classful

- Sus direcciones tienen tres partes: host, red y subred
- El protocolo de enrutamiento no admite VLSM
- El proceso de reenvío de direcciones IP está restringido en cuanto a cómo se utiliza la ruta predeterminada
- Las subredes no aparecen en las otras subredes principales
- Si existieran fallas se las puede detectar fácilmente
- No se admite el enrutamiento entre dominios sin clase

Classless

- Admite la máscara de subred de longitud variable conocida como VLSM
- Requiere menos ancho de banda
- La dirección se divide en dos partes: subred y host
- Se utilizan actualizaciones desencadenadas
- No tiene ningún tipo de restricción sobre el uso de la ruta predeterminada

8.4 Cálculo de Redes de longitud fija y variable

Redes de longitud fija: Se recomienda el siguiente procedimiento:

- Calcular el número de subredes (calcular n)
- Determinar las Direcciones IP por cada subred
- Determinar la Máscara para todas las subredes
- Calcular el rango y la dirección de broadcast para cada subred
- Calcular el número de direcciones IP de host disponibles por cada subred
- Verificar sus resultados con el programa IP-Subnet-Calculator

Ejemplo:

La empresa Unidos somos más tiene asignada la dirección 172.30.0.0. Está dedicada a la comercialización de materiales, suministros y dispositivos de computación. Está dividida en 8 departamentos. Se requiere facilitar la administración, el mantenimiento, la ubicación de usuarios e incrementar el número de direcciones IP para que exista escalabilidad. Ha solicitado subredes de longitud fija.

1. *Calcular el # de subredes*

$$* \# \text{ de subredes} = 2^{n-2}$$

$$* 8 = 24-2$$

$$* 8 = 14$$

$$* n = 4$$

172	30	0	0
10101100	00011110	00000000	00000000

2. *Determinar las direcciones IP por cada subred*

0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0

0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
1	1	0	1
1	1	1	0
1	1	1	1

NETMASK: 255.255. 240 .0

3. Determinar la máscara para todas las subredes

1	1	1	1
---	---	---	---

1111 = 240

4. Calcular el rango y la dirección de broadcast para cada subred

#	SUBRED	IP INICIO	IP FINAL	BROADCAST
1	172.30.16.0	172.30.16.1	172.30.31.254	172.30.31.255
2	172.30.32.0	172.30.32.1	172.30.47.254	172.30.47.255
3	172.30.48.0	172.30.48.1	172.30.63.254	172.30.63.255
4	172.30.64.0	172.30.64.1	172.30.79.254	172.30.79.255
5	172.30.80.0	172.30.80.1	172.30.95.254	172.30.95.255
6	172.30.96.0	172.30.96.1	172.30.111.254	172.30.111.255
7	172.30.112.0	172.30.112.1	172.30.127.254	172.30.127.255
8	172.30.128.0	172.30.128.1	172.30.143.254	172.30.143.255

5. Calcular el número de direcciones IP de host disponibles por cada subred

$$\ast \# \text{ de host} = 2^n - 2$$

$$\ast \# \text{ de host} = 2^{12} - 2$$

$$\ast \# \text{ de host} = 4094$$

6. Comprobación de los cálculos realizados con la plataforma IP Subnet Calculator:

La Figura 48 muestra la matriz de direcciones IP de las subredes encontradas, según validación utilizando IP-Subnet Calculator.

Figura 48

Validación de los resultados

Network Address	Usable Host Range	Broadcast Address:
172.30.0.0	172.30.0.1 - 172.30.15.254	172.30.15.255
172.30.16.0	172.30.16.1 - 172.30.31.254	172.30.31.255
172.30.32.0	172.30.32.1 - 172.30.47.254	172.30.47.255
172.30.48.0	172.30.48.1 - 172.30.63.254	172.30.63.255
172.30.64.0	172.30.64.1 - 172.30.79.254	172.30.79.255
172.30.80.0	172.30.80.1 - 172.30.95.254	172.30.95.255
172.30.96.0	172.30.96.1 - 172.30.111.254	172.30.111.255
172.30.112.0	172.30.112.1 - 172.30.127.254	172.30.127.255
172.30.128.0	172.30.128.1 - 172.30.143.254	172.30.143.255

Nota. Comprobación de cálculo subredes; Obtenido de: (Subnet Calulator)

Subredes de longitud variable

Los VLSM permiten dividir un espacio de red con máscaras de subred diferentes. Es decir, la máscara de subred varía según la cantidad de bits que se toman prestados en los octetos del host para una subred específica. La red primero se divide en subredes y luego estas se vuelven a dividir en subredes. Este proceso se repite según sea necesario para crear subredes de varios tamaños.

Se recomienda el siguiente procedimiento:

- Ordenar de mayor a menor;
- Determinar la máscara actual;
- Aplicar la Formula 2^{n-2} ;
- Obtener la nueva mascara;

- Calcular el salto de red;
- Rellenar la tabla;
- Probar en el IP-Subnet Calculator;
- Simular en Packet Tracer.

Ejemplo:

Dada la dirección 192.168.1.0 / 24 se pide utilice VLSM para conseguir subredes de 60, 120.10, 24 host.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

	255	255	255	0
Máscara de red actual	11111111	11111111	11111111	00000000

Para 120 host. Fórmula: $2^{n-2} \geq \text{Nº de hosts}$: $2^7-2 = 126$; $126 \geq 120$

	255	255	255	128
Máscara de red actual	11111111	11111111	11111111	10000000

Saltos de Red: $256 - 128 = 128$

Para 60 host. Fórmula: $2^{n-2} \geq \text{Nº de hosts}$: $2^6-2 = 62$; $62 \geq 60$

	255	255	255	192
Máscara de red actual	11111111	11111111	11111111	11000000

Saltos de Red: $256 - 192 = 64$

Para 24 host. Fórmula: $2^{n-2} \geq \text{Nº de hosts}$: $2^5-2 = 32$; $32 \geq 24$

	255	255	255	224
Máscara de red actual	11111111	11111111	11111111	11100000

Saltos de Red: $256 - 224 = 32$

Para 10 host. Fórmula: $2^{n-2} \geq \text{Nº de hosts}$: $2^4-2 = 14$; $14 \geq 10$

	255	255	255	240
Máscara de red actual	11111111	11111111	11111111	11110000

Saltos de Red: $256 - 240 = 16$

#	Host sol.	Host Entrada	Prefijo Mask	Máscara decimal	IP Subred	IP INICIO	IP Final	Broadcast
1	120	126	/25	255.255.255.128	192.168.1.0	192.168.1.1	192.168.1.126	192.168.1.127
2	60	62	/26	255.255.255.192	192.168.1.128	192.168.1.129	192.168.1.190	192.168.1.191
3	24	30	/27	255.255.255.224	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
4	10	14	/28	255.255.255.240	192.168.1.224	192.168.1.225	192.168.1.234	192.168.1.239

La Figura 49 muestra la comprobación de los cálculos realizados mediante la plataforma Arcadio:

Figura 49

Matriz de validación de los resultados obtenidos

Dirección IP		Dirección de red		Máscara de red		Dirección de Broadcast	
192.168.1.0		192.168.1.0 /24		255.255.255.0		192.168.1.255	
Subred	Nº de Hosts	IP de red		Máscara	Primer Host	Último Host	Broadcast
Subred 1	126	192.168.1.0 /25		255.255.255.128	192.168.1.1	192.168.1.126	192.168.1.127
Subred 2	62	192.168.1.128 /26		255.255.255.192	192.168.1.129	192.168.1.190	192.168.1.191
Subred 3	30	192.168.1.192 /27		255.255.255.224	192.168.1.193	192.168.1.222	192.168.1.223
Subred 4	14	192.168.1.224 /28		255.255.255.240	192.168.1.225	192.168.1.238	192.168.1.239

Nota. Comprobación de cálculo subredes VLSM; Obtenido de: (Calculadora VLSM)

Recursos complementarios

- Video sobre: "VLSM (Explicado en un ejemplo)" 
- Video sobre: "Subneteo con Máscara de Longitud Fija" (Paso a paso) 

- Calculadora online sobre: "Calculadora VLSM"
- Calculadora online sobre: "IP Subnet Calculator"
- PDF sobre: "VLSM y ejercicios propuestos"
- Ejercicios sobre: "Subredes"



Actividad de aprendizaje 8

Descripción de la actividad

Las subredes son una técnica para maximizar el espacio de direcciones IPv4 y disminuir el tamaño de las tablas de enrutamiento de una dirección de red dada. La porción del espacio de direcciones de host o de los bits más significativos, se toma prestada para las nuevas direcciones de subred. Esto se conoce como cálculo de subredes. Para su cómputo, existen dos técnicas: La primera, conocida como cálculo de subredes con máscara de longitud fija (FLSM). La segunda como cálculo de subredes con máscara de longitud variable (VLSM).

Se pide:

1. Realice 10 ejercicios de cálculo de redes con máscara de longitud fija. Ejemplos:

- La red de la empresa de venta materiales y suministros de cableado estructurado, tiene la dirección IP: 172.16.0.0. Se pide dividirla en 6 subredes por disponer seis departamentos. Validar sus resultados mediante IP-SUBNET-CALCULATOR;
- La empresa Líderes dispone de la dirección 10.0.0.0. Se pide dividirla en 10 subredes por disponer diez departamentos. Validar sus resultados mediante IP-SUBNET-CALCULATOR;
- La empresa Computación dispone de la dirección 192.168.100.0. Se pide dividirla en 2 subredes por inicio de su funcionamiento. Validar sus resultados mediante IP-SUBNET-CALCULATOR;
- Determine la dirección de red y de broadcast, la cantidad de bits y la cantidad de hosts para la dirección IP: 192.168.100.25/28;
- Determine la dirección de red y de broadcast, la cantidad de bits y la cantidad de hosts para la dirección IP: 172.30.110.130/30;

- Determine la dirección de red y de broadcast, la cantidad de bits y la cantidad de hosts para la dirección IP: 10.1.113.75/19.

2. Realice 10 ejercicios de cálculo de redes con máscara de longitud variable.

Ejemplos:

- Dada la dirección de red 192.168.0.0/24, se pide determinar las direcciones de las subredes para 20, 80, 20 y 2 hosts;
- Dada la dirección de red 192.168.12.0/24, se pide determinar las direcciones de las subredes para 60, 80, 20 y 2 para los enlaces WAN.

Al finalizar, elabore un informe que despliegue los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de los ejercicios, Conclusiones y Referencias bibliográficas.

Autoevaluación Capítulo 8

1. La subred de punto a punto permite que dos dispositivos se conecten, mientras que una subred de un centro de datos puede diseñarse para conectar mayores cantidades de dispositivos.

Verdadero

Falso

2. Si se necesita tener una dirección de red de clase B dividida en exactamente 510 subredes, ¿Qué máscara de subred debe asignar?

255.255.255.252

255.255.255.128

255.255.0.0

255.255.255.192

3. ¿Qué tipo de clase de direccionamiento IP permite un máximo de 254 hosts disponibles?

Clase A

Clase B

Clase C

Clase D

4. ¿Cuál es el número decimal de la siguiente máscara de subred 11111111.

11111111.11111111.11000000?

255.255.255.128

255.255.255.192

255.255.255.224

5. ¿Cuántos hosts puedo tener en una subred que tiene la siguiente máscara de subred adaptada: 255.255.254.0?

512 hosts

255 hosts

510 sts

6. ¿Cuántas subredes tendrá si tenía una máscara por defecto de clase C y al adaptarla queda así: 255.255.255.192?

4 subredes

8 subredes

2 subredes

7. ¿Cuál es la notación de longitud de prefijo para la máscara de subred 255.255.255.224?

/27.

/28.

/26.

/25.

8. ¿Cuál es el propósito de la máscara de subred junto con una dirección IP?

Para determinar la subred a la que pertenece el host.

Para identificar de manera única un host en una red.

Para enmascarar la dirección IP a extraños.

Para identificar si la dirección es pública o privada.

9. ¿Cuántas direcciones de host están disponibles en la red 172.16.128.0 con una máscara de subred de 255.255.252.0?

1024

512

1022

2048

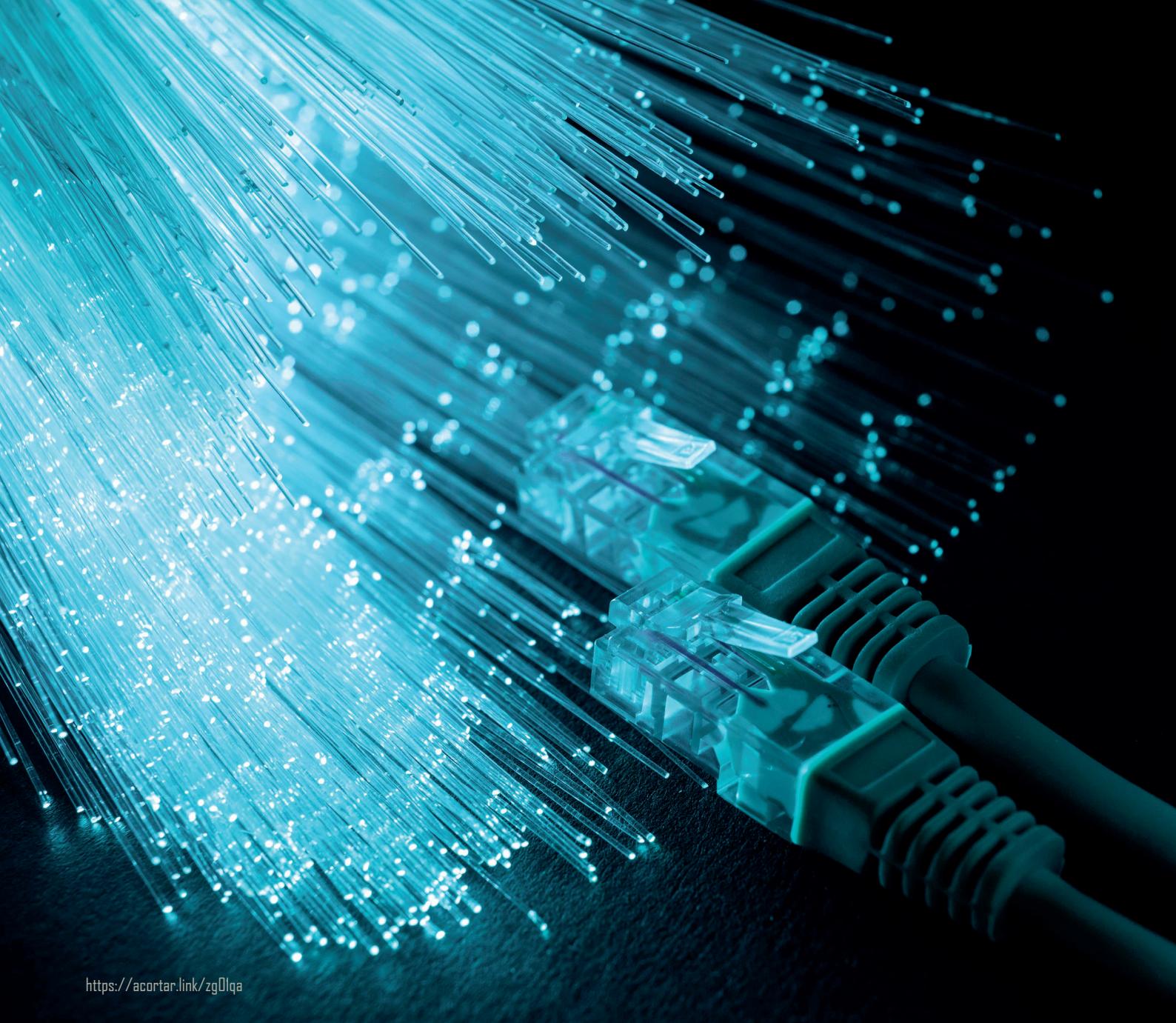
10. Se ha dicho a un administrador del sitio de una red particular que debe dar cabida a 126 hosts, ¿Qué máscara de subred se usaría que contenga el número requerido de bits de host?

255.255.255.224

255.255.255.128

255.255.255.240

255.255.255.0



<https://acortar.link/zg0lqa>

CAPÍTULO IX

Tecnologías Ethernet

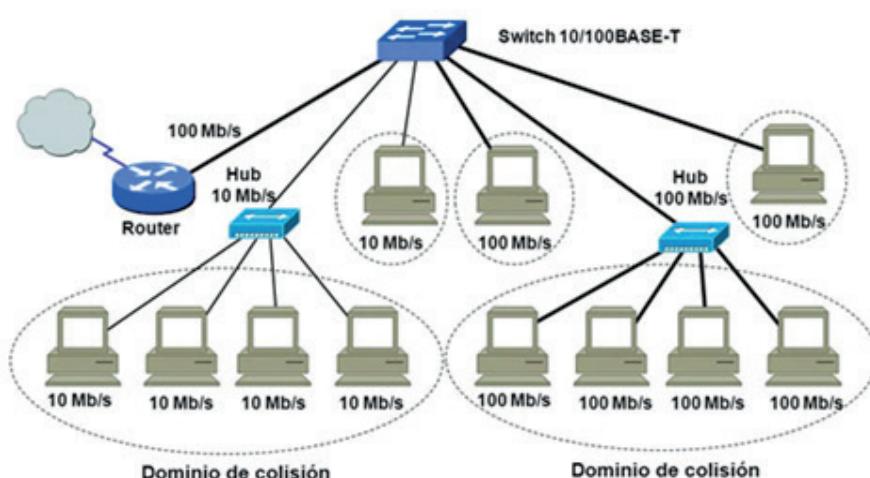
9.1 Introducción

Ethernet es una tecnología que fue desarrollada por Xerox Corporation en su Centro de Investigación de Palo Alto en California entre 1973 y 1974. Ethernet es un estándar de red dominante que conecta redes de área local (LAN) cableadas utilizada en lugares como en la oficina, casas, edificios, campos escolares, industriales, militares, etc. En 1978 Digital Equipment Corporation (DEC), Intel y Xerox, se unieron para promover Ethernet como estándar a una velocidad de 10 Mbps, también conocido como estándar DIX, referenciado comercialmente como IEEE-802.3 desde 1983.

Existen dos categorías de Ethernet, la primera se clasifica como Ethernet tradicional, la cual resuelve una necesidad de acceso múltiple, opera tasas de transmisión de 3 a 10 Mbps. La segunda se clasifica como Ethernet conmutada en la cual los dispositivos como los commutadores (switches) son utilizados para conectar diferentes equipos de usuario y dispositivos de red que transmiten a 10, 100, 1000 y 10 000 Mbps, a través de la antigua Ethernet, y sus mejores innovaciones Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet respectivamente. La Figura 50 ilustra los elementos de una red Ethernet.

Figura 50
Ethernet Conmutada

Ethernet conmutada/compartida



Nota. La figura representa un diagrama de Ethernet conmutada. Obtenido de: (Montañana, 2017).

9.2 Terminología utilizada

Para comprender de mejor manera el tema de Ethernet, a continuación, se presenta la terminología utilizada:

- LAN: Local Area Network, que es un conjunto de equipos de usuario final y de dispositivos de red conectados entre sí en redes de área local cuya cobertura geográfica es de corta distancia.
- Comutación: la Comutación es la acción de establecer un sistema de comunicación extremo a extremo entre dos puntos en la red, un emisor y un receptor a través de equipos o dispositivos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido y es un proceso que funciona en la capa de Enlace de Datos del modelo ISO/OSI. Los servicios básicos que emplean técnicas de conmutación son el teléfono, el telégrafo y las redes de datos. Existen tres técnicas de conmutación conocidas como de circuitos, de mensajes y de paquetes, cada una con sus características propias. El dispositivo central es el conmutador o switch.
- CSMA/CD: Carrier Sense Multiple Access/Collision Detection. Acceso a los medios la cual determina qué sistemas dentro de una red pueden acceder a un medio de transmisión, evitando colisiones.
- Dirección MAC: dirección física y única asignada por el fabricante y la IEEE a la tarjeta de red de un equipo o dispositivo conectado. Tiene 6 bytes o 48 bits, representada por doce números hexadecimales separados en 3 bytes respectivamente.
- IEEE: el Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronic Engineers, IEEE), es una organización profesional, que agrupa a miles de ingenieros, técnicos y científicos de más de 160 países, que se dedican al avance, innovación y desarrollo tecnológico. Una de sus especialidades es la microelectrónica y los estándares para las redes de comunicación.
- Cable coaxial: transporta señales eléctricas que poseen dos conductores concéntricos. El primero se encarga de transportar datos. El segundo que es exterior, conocido como malla, blindaje o trenza.
- Cable de par trenzado: es el medio de transmisión más utilizado en el mundo para redes de área local. Está compuesto por pares de hilos trenzados, alcanza velocidades de 10 Mbps hasta 10 Gbit/s.

- Cable de fibra óptica: transmite datos a través de señales ópticas. Para su fabricación se utiliza vidrio, cuarzo, silicio y plástico. Alcanzan velocidades de transmisión superiores a los Gbps. Son adecuadas para cubrir largas distancias.

9.3 Protocolo de subcapa de MAC para la Ethernet clásica

Para transportar los datos en redes Ethernet se utilizan tramas. Una trama de Ethernet es una unidad de datos de protocolo (Protocol Data Unit, PDU) de capa de enlace de datos del modelo OSI/ISO que utiliza los mecanismos de transportación de la capa física de Ethernet.

Una trama Ethernet tiene un formato compuesto por varios campos en los que se distinguen las direcciones MAC origen y destino de los equipos que interactúan en la red. Una trama comienza con un preámbulo y un delimitador que indica el inicio de la trama (Start Frame Delimiter, SFD), que funcionan en la capa física. El preámbulo consta de un patrón de 56 bits (siete bytes) de bits 1 y 0 alternos, lo que permite a los dispositivos de la red sincronizar los relojes del receptor a nivel de bits. El encabezado de Ethernet contiene la dirección MAC de origen y de destino con seis bytes cada una, después de lo cual está presente la carga útil de la trama.

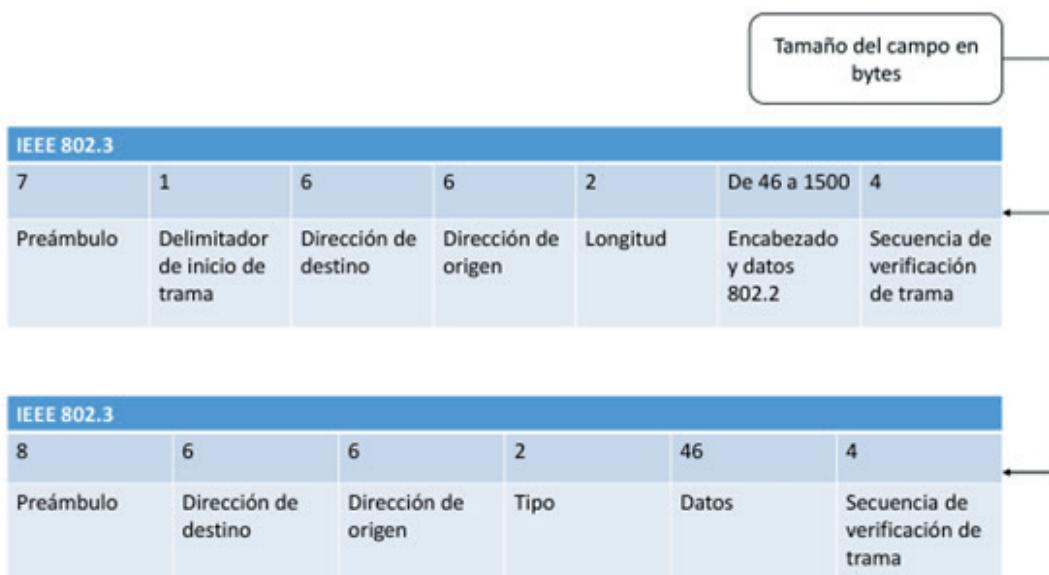
El Campo Longitud/tipo define la longitud exacta del campo de datos de la trama. Esto se utiliza posteriormente como parte del campo definido como Secuencia de verificación de trama (Frame Check Sequence, FCS) para asegurar que el mensaje se reciba apropiadamente. Si el objetivo es designar un tipo como en Ethernet II, el campo Tipo describe cuál es el protocolo que se implementa. Los campos Datos y Pad (de 46 a 1500 bytes) contienen los datos encapsulados, que son una unidad de datos de protocolo de Capa 3 o de red genérica o, con mayor frecuencia, un paquete IPv4. Todas las tramas deben tener al menos 64 bytes de longitud. Finalmente, el Campo FCS se utiliza para detectar errores en la trama mediante el campo código de redundancia cíclica (Cyclic Redundancy Check, CRC) que se utiliza para detectar si existe error durante la transmisión. El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama. El CRC es un código de detección de errores que se usa en redes de cómputo para detectar cambios accidentales en los datos a transmitir.

En conclusión, la trama Ethernet sirve para que se transmitan datos a través de Ethernet, y es la responsable de la correcta configuración de las reglas

y para la transportación de los de datos. Además, la diferencia entre la trama Ethernet con respecto a la IEEE 802.3 es el campo tipo que establece el protocolo de red de capa superior asociado al paquete, mientras que la trama IEEE 802.3, introduce el campo longitud que define la longitud exacta del campo datos de la trama. Ethernet es la tecnología de red más utilizada en el mundo. La Figura 51 muestra una comparación entre las tramas Ethernet e IEEE-802.3.

Figura 51

Trama Ethernet e IEEE 802.3



Nota. La figura representa el formato de una trama Ethernet versus la de IEEE-802.3

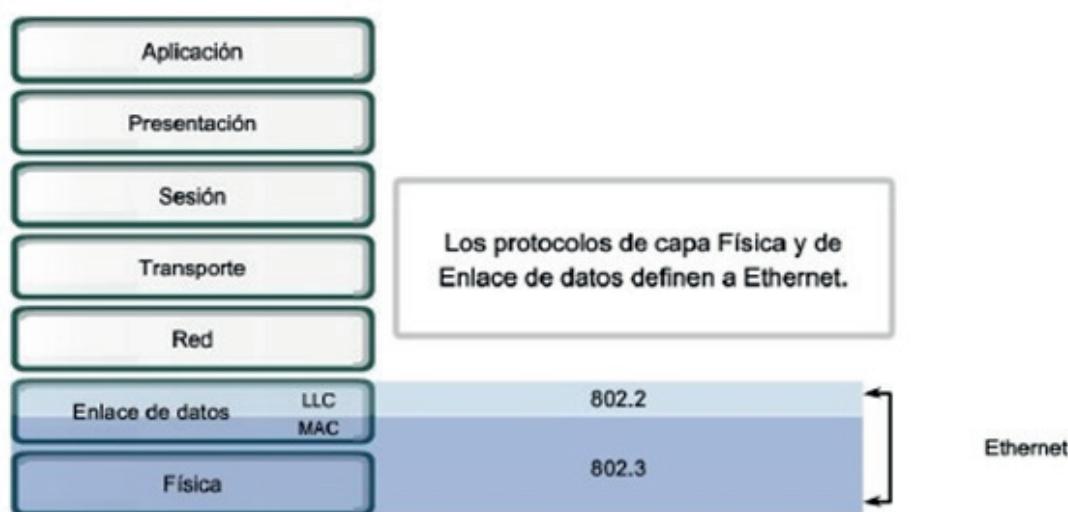
CSMA/CD

Por otra parte, Ethernet utiliza como método de control de acceso la Detección de acceso múltiple de colisión con detección de portadora (Carrier Sense Multiple Access/Collision Detection, CSMA/CD). CSMA/CD crea un procedimiento que regulariza la forma en la que debe producirse la comunicación entre nodos de una red que utilizan un medio de transmisión compartido. La mejora introducida regula además cómo actuar en caso de colisiones, es decir, cuando dos o más nodos tratan de enviar tramas de datos simultáneamente a través del medio de transmisión y estos interfieren entre sí.

Ethernet conmutada

Se la denomina así puesto que los equipos de usuario final y los dispositivos de red se conectan mediante enlaces punto a punto a través de un conmutador o switch que transmite tramas Ethernet. El switch es un dispositivo de conectividad de capa de enlace de datos o de capa de red cuyas funciones principales son la conmutación y concentración de tramas (capa 2) y de enrutamiento (capa 3). Los switches deben ser configurables y normalmente tienen alta densidad de puertos (i.e., 4, 12, 24, 48, puertos) con diferentes capacidades de transmisión (10, 100, 1000, 10000 Mbps). La Figura 52 muestra las capas en donde funciona la Ethernet conmutada, los protocolos de capa física y capa de red y su relación con el modelo ISO/OSI.

Figura 52
Ethernet Conmutada



Nota. La figura representa un diagrama del estándar para Ethernet. Obtenido de: (Montañana, 2017)

9.4 Tecnologías Ethernet

Un conmutador o switch es un dispositivo de networking que realiza las funciones de concentrador y conmutador. Contiene un plano posterior conocido como backplane de alta velocidad, el cual se encarga de conectar todos los equipos a sus puertos. Un switch es similar al viejo y desaparecido hub debido a que ambos contienen de 4 a 48 puertos junto con los conectores RJ-45 para cables de par trenzado o conectores para cables de fibra óptica.

Los switches deben ser configurables puesto que disponen de ciertas funcionalidades que son requeridas tanto en el diseño como en la gestión de redes. Por ejemplo, la posibilidad de personalizar VLANs, port trunking, STP, RMON, claves de acceso, puertos y protocolos. Algunas marcas reconocidas por la industria son CISCO, Net gear, Hewlett Packard, Dlink, Huawei, etc.

El antiguo hub se caracterizaba porque las estaciones estaban en el mismo dominio de colisión. Por su parte, en un switch cada puerto tiene su propio dominio de colisión independiente. Además, los hubs trabajaban solo en la capa física, mientras que los switches pueden funcionar en niveles 2 y 3. Dentro de un hub cualquier computadora podía ver el tráfico transmitido entre las demás computadoras. En el caso de un switch, el tráfico se reenvía sólo a los puertos a los que están destinados. La Figura 53 ilustra un switch CISCO serie 2960.

Figura 53
Switch CISCO Catalyst 2960



Nota. Switch Cisco Catalyst Ws-c2960s-48ts-l de 48 Puertos Poe + 4sfp valorado en USD 1599 para una Ethernet commutada. Obtenido de: (Mercado Libre, 1999)

9.4.1 Fast Ethernet

Un junio de 1995, fue aprobado de manera oficial por el IEEE la norma 802.3u, la cual tiene una capacidad de transmisión de hasta 100 Mbps. Fast Ethernet fue diseñado para ser compatible con las redes 10BASE-T existentes. Es decir, mantiene todos los formatos, interfaces y reglas anteriores para reducir el tiempo de transmisión 10 veces comparado con Ethernet. Además, aplica el mismo formato de trama y utiliza el método de acceso al medio CSMA/CD

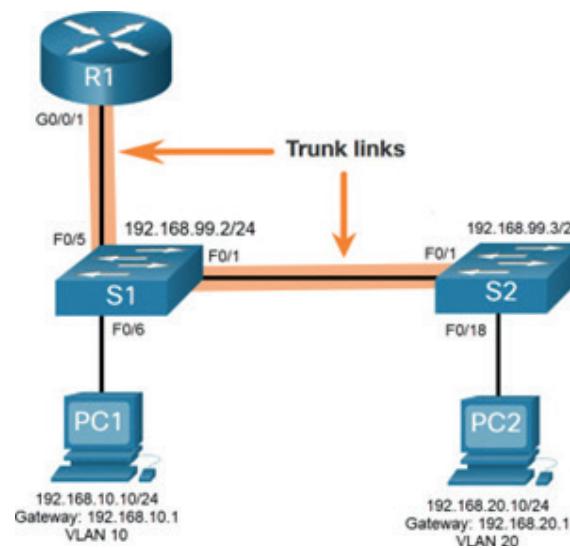
definido en el estándar IEEE-802.3. La tecnología Fast Ethernet viene embebida en switches de la LAN, y trabaja con cable de par trenzado (i.e., conectores de RJ45) norma 100BASE-T4 y cable y conectores de fibra óptica 100BASE-FX, 100BaseSX-multimodo, y 100BaseLX-monomodo.

De acuerdo con las norma y estándares de los Sistemas de Cableado Estructurado (SCE) una desventaja de utilizar cable UTP es la incapacidad de transportar 100/1000 o más Mbps a más de 100 metros. El cable de par trenzado categoría 5 puede alcanzar hasta 100 metros con facilidad, y por ello se recomienda la fibra óptica que puede recorrer distancias superiores.

Un SCE es el conjunto de estándares internacionales aprobados por la ANSI/IEC/EIA/TIA para conectar el cableado físico de las redes de área local en la que se puedan transmitir señales de voz (telefonía), datos, video y control (sensores) en oficinas, campus y edificios comerciales. La importancia de los SCE reside en que los diseñadores de red pueden elegir libremente marcas, proveedores, facilitando la escalabilidad en el caso de requerirlo. Existen diversos estándares como: la EIA/TIA-568 que es la norma para instalar SCE en edificios comerciales; ANSI/TIA/EIA-569 que permite normar rutas y espacios de telecomunicaciones para Edificios Comerciales, entre otras.

Figura 54

Diagrama LAN con switches Fast Ethernet



Nota. La figura muestra dos switches Fast Ethernet CISCO conectados mediante un enlace troncal a un router con interfaz Gigabit Ethernet. Obtenido de: (Cisco Networking Academy, 2020)

9.4.2 Gigabit Ethernet

Es una tecnología LAN definida por el estándar IEEE 802.3ab desde 1999, que ofrece velocidades de transmisión de 1000 Mbps o 1 Gbps mediante cable UPT (1000BASE-T) y fibra óptica (1000BASE-X). Gigabit Ethernet se utiliza en centros de procesamiento de datos para interconexiones de servidores o enlaces ascendentes de switches en campus, oficinas o se puede conectar directamente al escritorio. Una característica importante es que se puede reutilizar el cableado de cobre y fibra existente en conexiones de 10 o 100 Mbps. El cable de transmisión mínimo de IEEE 802.3ab es el UTP Cat5, aunque es compatible con Cat5e, Cat6, Cat6e y Cat8. La longitud máxima del segmento es de 100 metros de acuerdo con los SCE. Utiliza el conector RJ45 y puede ser utilizado con UTP, FTP y STP. Además, los puertos Gigabit pueden negociar automáticamente la transmisión y la recepción de pares trenzados en el cable (auto negociación).

En relación al uso de fibra óptica, existen el estándar IEEE 802.3z con opciones como 1000BASE-X para fibra multimodo hasta una longitud máxima de 550 m; 1000BASE-LX / LH / LX10 para fibra óptica monomodo para una longitud máxima de 10 kilómetros (km). En conclusión, Gigabit Ethernet ofrece mejoras del performance para las redes existentes, sin tener que cambiar los cables, dispositivos de red, equipos de usuario final y protocolos para las aplicaciones y servicios que ya están en producción.

Finalmente, existen los puertos SFP (la evolución de los puertos GBIC) que hacen que los switches Gigabit se conecten a varios cables de fibra óptica u otros para ampliar la funcionalidad de permutación a través de la red.

9.5 Variantes de la Ethernet

Existen diversos estándares de Ethernet dependiendo del medio de transmisión que se usa, así como su tecnología que inclusive alcanzan los 10Gbps o 40GBps. Las Tabla 4 y Tabla 5, listan algunos estándares y muestran algunos criterios de comparación para un mejor aprendizaje:

Tabla 4*Variantes del estándar IEEE-802.3 Ethernet*

Estándar	Medio	Tipo de cable	Velocidad
IEEE 802.3a	10Base2	Cable coaxial delgado	10Mbps
IEEE 802.3	10Base5	Cable coaxial grueso	10 Mbps
IEEE 802.3i	10Base-T	Cable de par trenzado UTP	10 Mbps
IEEE 802.3j	10Base-F	Fibra óptica	10 Mbps
IEEE 802.3z	100Base-FX	Fibra óptica multimodo	100 Mbps
IEEE 802.3u	100Base-TX	Cable de par trenzado	100 Mbps
IEEE 802.3ab	1000Base-TX	Cable de par trenzado	1 Gbps
IEEE 802.3z	1000Base-SX	Fibra óptica multimodo	1 Gbps
IEEE 802.3z	1000Base-LX	Fibra óptica monomodo	1 Gbps
IEEE 802.3an	10GBASE-T	Cable de par trenzado	10 Gbps
IEEE 802.3aq	10GBASE-LRM	Fibra óptica monomodo	10 Gbps

Tabla 5*Comparativa de las variantes de los estándares de Ethernet*

Estándar	Denominación	Velocidad	Tecnología de cables	Año de publicación
802.3	10Base5	10 MB/s	Cable coaxial	1983
802.3a	10Base2	10 MB/s	Cable coaxial	1988
802.3i	10Base-T	10 MB/s	Cable de par trenzado	1990
802.3j	10Base-FL	10 MB/s	Cable de fibra óptica	1992
802.3u	100Base-TX100Base-FX100Base-SX	100 MB/s	Cable de par trenzado, cable de fibra óptica	1995
802.3z	1000Base-SX100Base-FX1000Base-LX	1 GB/s	Cable de fibra óptica	1998
802.3ab	1000Base-T	1 GB/s	Cable de par trenzado	1999

	10GBase-SR, 10GBase-SW, 10GBase-LR, 10GBase-LW, 10GBase-ER, 10GBase-EW, 10GBase-LX4	10 GB/s	Cable de fibra óptica	2002
802.an	10GBase-T	10 GB/s	Cable de par trenzado	2006

Recursos complementarios

- Vídeo sobre “Tecnologías Ethernet”: ¿Qué es la tecnología Ethernet?

¿Cuál es el funcionamiento? 

- Vídeo sobre: “Ethernet”: ¿Qué es Ethernet? ¿Para qué sirve? 
- Vídeo sobre “Ethernet” 

Actividad de aprendizaje 9

Descripción de la actividad

Ethernet es una tecnología de LAN que conecta tanto varios equipos de usuario final como dispositivos de networking mediante conmutadores o concentradores vía cable que logran vincular el software y el hardware para transmitir/recibir datos en la red.

Para lograrlo se requiere configurar un conmutador o concentrador para personalizarlo en función de los requerimientos del administrador de red. Por lo tanto, los estudiantes deben aprender a configurar un conmutador con la ayuda de un simulador de redes.

Los switches de Cisco son de configuración automática y no necesitan ninguna configuración adicional para comenzar a funcionar. Sin embargo, los switches Cisco ejecutan el Cisco IOS y se pueden configurar manualmente para satisfacer mejor las necesidades de la red. Esto incluye el ajuste de los requisitos de velocidad, de ancho de banda, de seguridad de los puertos y protocolos.

El simulador de redes que se utilizará es el Packet Tracer de la Academia de Networking de CISCO, que permite desarrollar habilidades de redes y seguridades.

Esta actividad de aprendizaje se relaciona con la Configuración básica de un switch cisco utilizando el simulador Packet Tracer.

Se pide:

1. Instalar el simulador de redes Packet Tracer la última versión disponible en el sitio oficial www.cisco.com.
2. Realizar el curso de capacitación titulado Introducción a Packet Tracer disponible en el sitio oficial, hasta obtener el certificado de CISCO. Tiene 10 horas de duración y no tiene costo.
3. Realizar la práctica de laboratorio 5.4.4 titulada “Configuración básica del switch Cisco 2960, disponible en el Web desarrollado por la Academia de Networking de CISCO. Rellene todos los ejercicios que aquí se señalan.

Al finalizar, elabore un informe de la Práctica de Laboratorio que despliegue de los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de cada punto con sus resultados, Conclusiones generales y Referencias bibliográficas.

Autoevaluación Capítulo 9

1. ¿Qué es un modo de transmisión?

Es un canal de comunicación que lleva información del transmisor al receptor

Es el mecanismo de transferencia de datos entre dos dispositivos

Es el mecanismo que permite que dos o más dispositivos interactúen entre sí

2. La forma en que los dispositivos y equipos de red están organizados y conectados entre sí se denomina:

Topología de red

Topología física

Topología lógica

3. Los _____ se encargan de facilitar la comunicación entre dos o más usuarios de la red.

Servicios de red

Dispositivos de red

Simuladores de red

4. El Internet está definido como:

Redes de comunicaciones conectadas localmente

Redes de comunicaciones conectadas universalmente

Redes de comunicaciones interconectadas universalmente

5. La IETF es una organización internacional abierta, ¿cuál es su objetivo?

Desarrollar estándares y protocolos de comunicación para redes eléctricas, electrónicas y de transmisión de datos

Contribuir a la ingeniería de Internet y sus protocolos

Supervisar el desarrollo de estándares para servicios, productos, procesos y sistemas aplicados en el mundo

6. Los nodos dentro de las redes de datos permiten:

Enviar y recibir datos almacenados en otros dispositivos a través de la red de forma local o remota

Enviar datos almacenados en otros dispositivos a través de la red de forma local o remota

Recibir datos almacenados en otros dispositivos a través de la red de forma local

7. ¿Cuál es el dominio de las redes de comunicaciones?

El universo

El espacio

El ciber espacio

8. ¿Cómo se denomina al mecanismo que permite que dos o más dispositivos interactúen entre sí?

Medios de transmisión

Protocolo de transmisión

Protocolo de comunicaciones

9. La organización ANSI se encarga de supervisar el desarrollo de estándares para servicios, productos, procesos y sistemas, forma parte de las organizaciones:

IEC y IEEE

IEFT e ITU

ISO y IEC

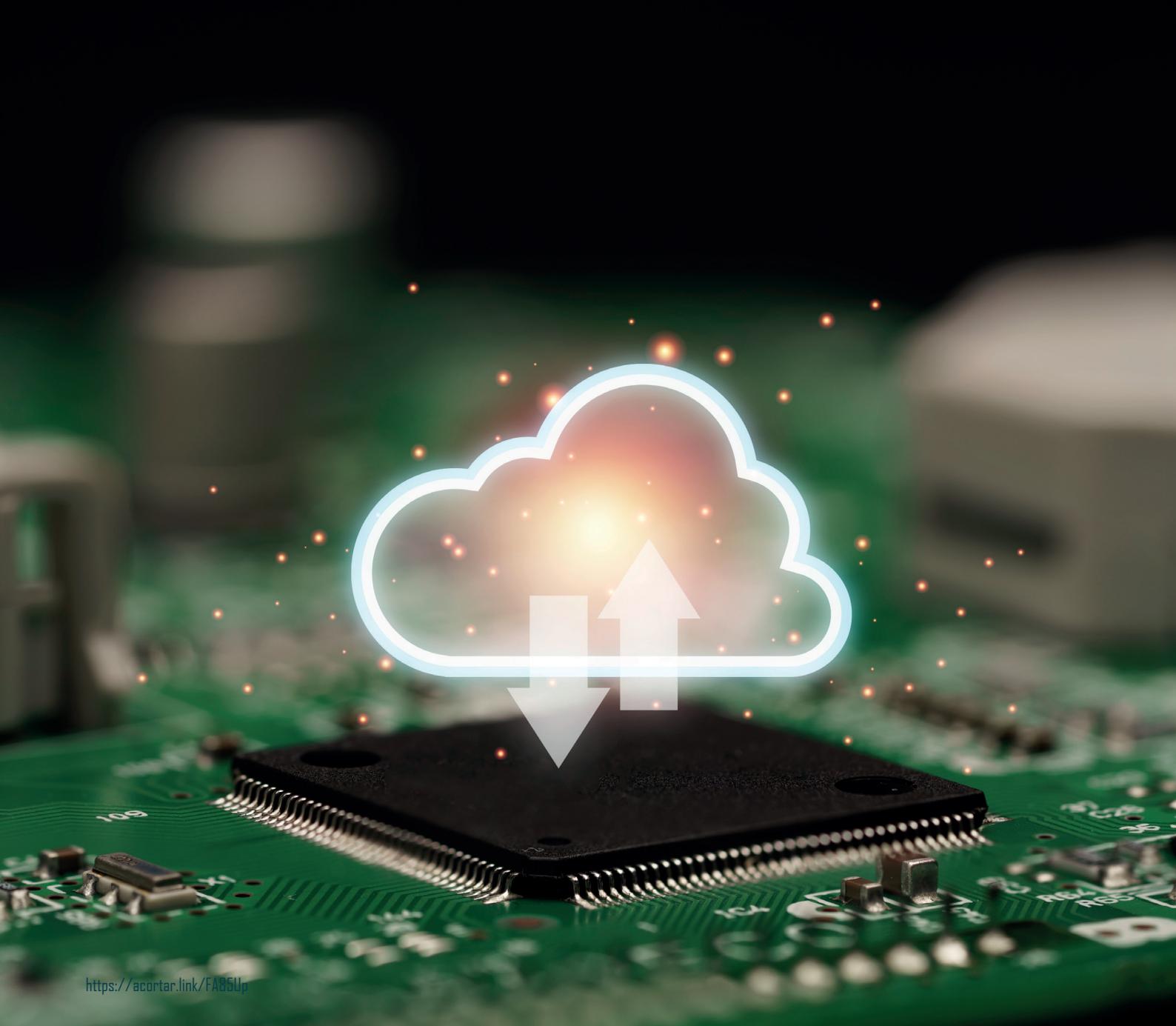
Ninguna respuesta es correcta

10. ¿Cuál no es un beneficio del uso de redes de datos?

Mejora la distribución de la interconexión local o remota

Facilita la comunicación local o remota

Permite el ahorro de inversión e incrementa la productividad



<https://acortar.link/FA85Up>

CAPÍTULO X

Switching capa 2 y 3

10.1 Caracterización

Un commutador o switch de red es un dispositivo que opera en la capa de enlace de datos o en la capa de red del modelo OSI/ISO. El commutador es el centro de una red cableada para conectarse a otros dispositivos mediante cables de par trenzado que permite conectar docenas de dispositivos. Los commutadores evitan que el tráfico entre dos dispositivos se interponga en el camino de sus otros dispositivos en la misma red.

El propósito de un switch es facilitar el intercambio de recursos al conectar todos los dispositivos, incluidas computadoras, impresoras y servidores, en una red doméstica o empresarial. Gracias al commutador, estos dispositivos conectados pueden compartir información y comunicarse entre sí, independientemente de dónde se encuentren en un edificio o en un campus.

10.1.1 Switch de capa 2

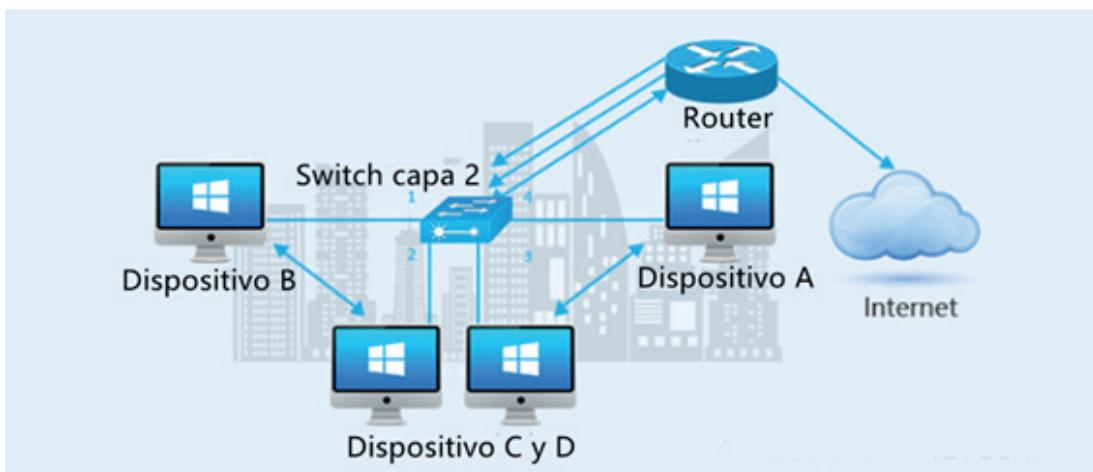
Un commutador de capa 2 funciona en la capa de enlace de datos del modelo OSI, el cual envía tramas al puerto de destino, haciendo uso de las direcciones MAC que almacenan las direcciones MAC de un dispositivo asociado a ese puerto. Entre sus principales funciones se pueden incluir

- Comunicación de capa 2, es decir, la de actuar como un puente de red, el cual conecta distintos dispositivos de red de datos en una sola plataforma.
- Se encargan de reorganizar las tramas de datos, ubicándose desde el origen hasta un extremo de destino recordando la dirección MAC del nodo de destino en la tabla de direcciones MAC.
- En la tabla de direcciones MAC se puede encontrar:
 - Direcciones MAC que el dispositivo ha aprendido cuando se realiza la conexión física al puerto de switch.
 - Puerto físico asociado donde están las direcciones vistas por última vez.
- Los switches de capa 2 son capaces de asignar VLANs a puertos específicos de los switches.

La Figura 55 muestra una ilustración del funcionamiento de un switch capa 2 y de la conexión con los equipos de usuario final u otros dispositivos.

Figura 55

Switch capa 2



Nota. La figura representa la comunicación de dispositivos en switch capa 2.

Obtenido de: (Worton, 2022)

10.1.2 Switch de capa 3

La commutación tradicional opera en la capa 2 del modelo OSI, donde las tramas se envían a un puerto de commutador específico según las direcciones MAC de destino. El enruteamiento opera en cambio en la capa 3 del modelo OSI, donde los paquetes se envían a una dirección IP específica del siguiente salto, según la dirección IP del equipo destino.

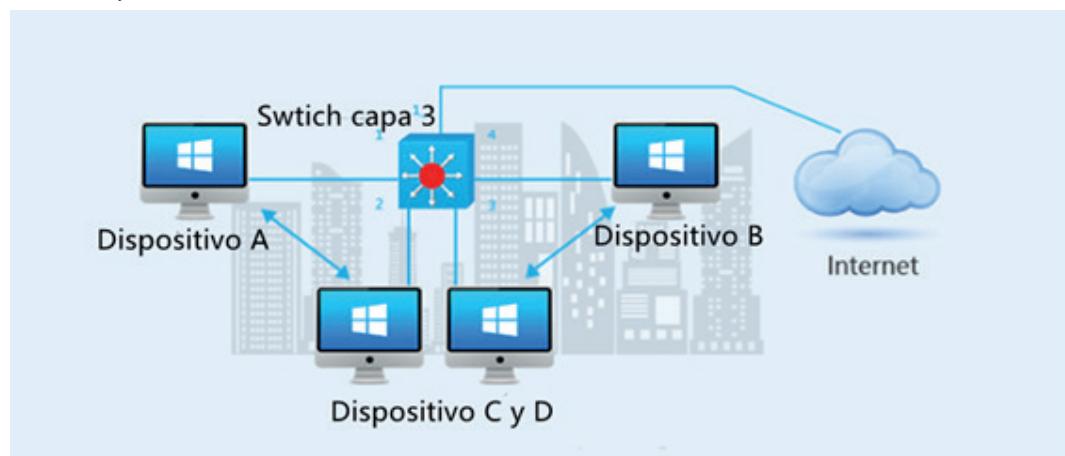
En términos generales, un commutador de capa 3 conecta equipos para formar redes de área local (LAN) y posee funciones de enruteamiento. En realidad, los switches de capa 3 tienen muchas similitudes con un router, puesto que ambos admiten los mismos protocolos de enruteamiento, inspeccionan los paquetes entrantes y toman decisiones de enruteamiento dinámico basadas en las direcciones de origen y destino internas. Sin embargo, difieren en rendimiento, flexibilidad, costo, etc. Algunas de las funciones de un switch capa 3 son las siguientes:

- Los commutadores de capa 3 son los encargados de realizar funciones de enruteamiento además de la commutación.
- Realiza el enruteamiento estático que se asigna manualmente para que se pueda realizar la transferencia de datos entre las redes LAN virtuales (VLANs).

- Realiza el enrutamiento dinámico, que es un proceso en el que un enrutador puede reenviar datos a través de una ruta diferente o un destino determinado en función de las condiciones actuales y de ciertas métricas entre los circuitos de comunicación, que permite que el conmutador realice un enrutamiento óptimo de paquetes.
- Requieren más energía para operar y ofrecen enlaces de mayor capacidad de transmisión (10 Gbps) entre los conmutadores.
- Dentro de las funciones que cumplen los conmutadores de capa 3 además se encuentran la autenticación 802.1x, la detección de bucle invertido y la Inspección ARP (Address Resolution Protocol).
- Vienen con puertos Ethernet, pero sin interfaz WAN.
- Actúa como un conmutador para conectar dispositivos dentro de la misma subred.
- El algoritmo de conmutación es simple y es el mismo para la mayoría de los protocolos de enrutamiento.

La Figura 56 ilustra una red de datos que incluye un switch capa 3. Como se puede apreciar, la presencia de un router ya estaría incluida en el switch de capa 3.

Figura 56
Switch capa 3

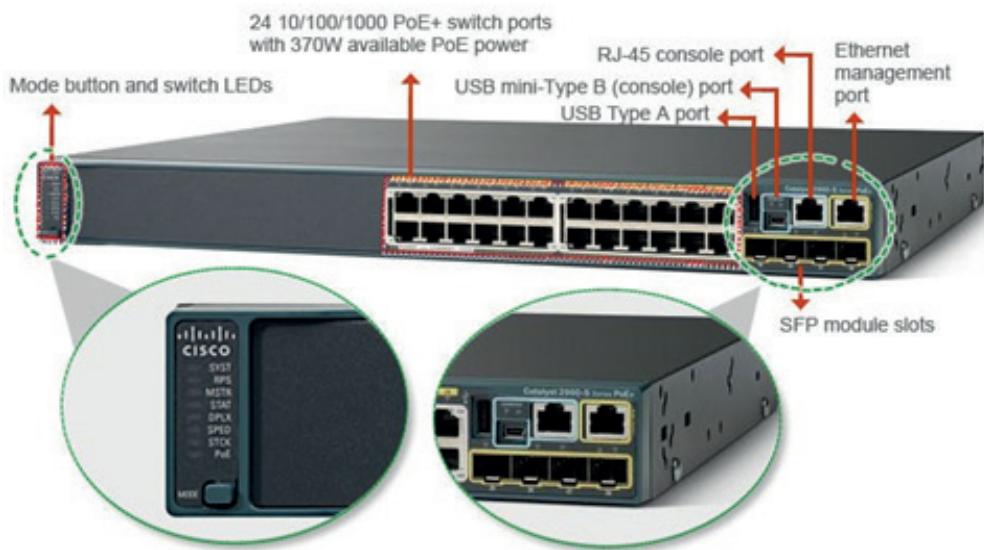


Nota. La figura representa la comunicación de dispositivos en switch capa 3.
Obtenido de: (Worton, 2022)

10.2 Estructura

Cada switch tiene una estructura o arquitectura interna y externa. La arquitectura interna está relacionada con los componentes conectados a la tarjeta principal del switch (mainboard) que incluye procesador, memorias internas (RAM, NVRAM, ROM, FLASH), ventilador y fuente de poder. En relación a la arquitectura externa incluye los puertos físicos de cable par trenzado y fibra óptica, los LEDS de servicios, el puerto de consola, puerto auxiliar, el de toma de poder. En la Figura 57 se muestra un esquema general de la estructura externa de un switch.

Figura 57
Estructura externa de un switch



Nota. Estructura general de un Switch. Obtenido de: (Galindo, 2014)

10.3 Ejemplos y marcas de switches

En la industria se pueden encontrar una variedad de tipos de switches cuyos costos dependen de las características de configuración, marcas, tecnología y funcionalidad de los mismos. Así por ejemplo dependen de las funcionalidades de configuración y personalización de los comutadores, del tipo y número de puertos físicos de par trenzado o fibra óptica, así como sus capacidades de transmisión. Entre las marcas más reconocidas según el Cuadrante Mágico

de Gartner en el 2021 están: Juniper Networks, HPE Aruba, Cisco, Huawei, Fortinet, Dlink, Tplink, Dell.

En relación a configuración de los conmutadores, es decir, la posibilidad de que los administradores y los usuarios puedan establecer personalizaciones para la gestión, el monitoreo y los controles de tráfico de la red, existen diferentes tipos de conmutadores Ethernet inteligentes, cada uno con diferentes niveles de administración disponibles. Los conmutadores modernos cuentan con administración de GUI web con funciones de conmutador como VLAN, inspección IGMP, QoS y agregación de enlaces. En conmutadores configurables de capa 2 se incluye características administradas de primer nivel, como CLI, control de PoE, listas de control de acceso, VLAN, indagación IGMP, QoS, RMON, trampa SNMP y syslog para monitoreo e integración de red flexible. En conmutadores más sofisticados de capa 3 se incluye configuración de controles de gestión de tráfico, enrutamiento IP, VLAN, QoS, controles de acceso, agregación de enlaces, resolución de problemas, supervisión SNMP, restricción MAC por puerto e inspección ARP dinámica. A continuación, se presentan algunos ejemplos de switches capa 2 y capa 3 para su análisis y mejor comprensión (ver figuras Figura 58, Figura 59, Figura 60 y Figura 61).

Figura 58

Switch Tplink Tl-sg2452 De 48 Puertos Gigabit Admin. Capa 2, capacidad de comunicación 104Gbps, gestionable y montable en Rack.



Nota. La figura muestra el switch en mención de la marca TP-Link con algunas de sus especificaciones. Obtenido de: (Mercado Libre, 1999).

Figura 59

Switch Tplink Tl-sg2428p 24 Puertos Gigabit Poe Admin Capa2



Nota. La figura muestra el switch en mención de la marca TP-Link con algunas de sus especificaciones. Obtenido de: (OCompra, 2019).

Figura 60

Switch Cisco 3650 24 Puertos Poe, 2 SFP+ Capa 3 con capacidad de 272 Gbps de commutación, gestionable y montable en rack



Nota. La figura muestra el switch en mención de la marca Cisco con algunas de sus especificaciones. Obtenido de: (Mercado Libre, 1999)

Figura 61

Switch Gigabit Linksys 28 Puertos Administrable 2 SFP Capa 3, capacidad de comunicación de 65 Gbps, montable y gestionable



Nota. La figura muestra el switch en mención de la marca Linksys con algunas de sus especificaciones. Obtenido de: (Mercado Libre, 1999)

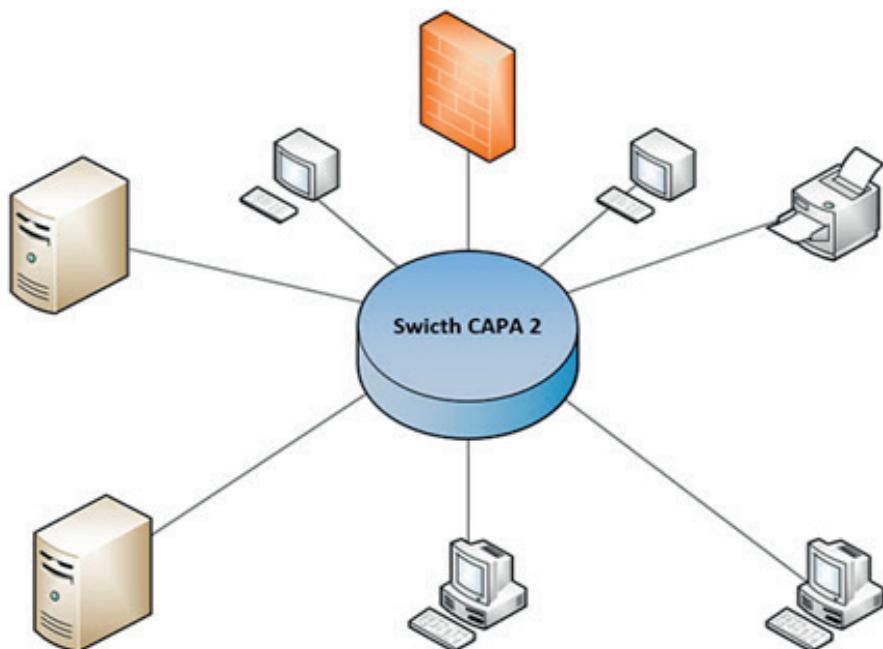
10.4 Aplicaciones

Comutadores Capa 2:

- Con los comutadores de capa 2, se puede enviar las tramas de datos desde el origen encontrado en la misma VLAN sin tener que estar conectados físicamente o ubicados en la misma localización.
- Los equipos servidores de cualquier empresa pueden ubicarse de una manera centralizada en una ubicación y los clientes dispersos en otras con la capacidad de acceder a los datos casi sin latencia.
- Dentro de las empresas se suele generar comunicaciones internas con los equipos de usuario final en la misma VLAN usando los comutadores de capa 2 y sin la necesidad de una conexión a Internet.
- Los comutadores suelen estar ubicados en la capa de core, de distribución e inclusive de acceso en los diferentes centros de datos y closet de telecomunicaciones y son aquellos que pueden otorgar escalabilidad a las redes.

La Figura 62 muestra una abstracción de la realidad cuando se tiene una red con un comutador capa 2.

Figura 62
Switch Enlace de Datos



Nota. La figura muestra cómo se realiza la conexión con comutador de capa 2. Obtenido de: (Soporte Incared, s.f.)

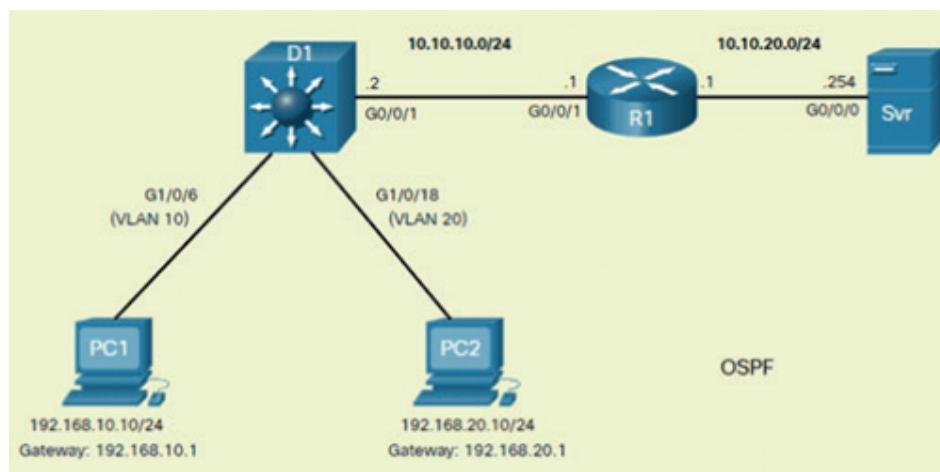
Comutadores Capa 2:

- Son muy ampliamente utilizados en centros de datos y dentro de los campus universitarios donde hay configuraciones extensas de redes de datos.
- Dada su funcionalidad con respecto al enruteamiento estático, dinámico y su velocidad, los comutadores de capa 3 son utilizados en las LAN para realizar la interconexión de inter VLANs.
- Los comutadores de capa 3 son muy inteligentes, lo que permite que tengan la capacidad de manejar y administrar el enruteamiento y el control del tráfico de los servidores hacia los dispositivos conectados de manera local con una gran capacidad de transmisión.

La Figura 63 presenta un diseño de red LAN/WAN incluyendo un comutador de capa 3 y un router.

Figura 63

Enrutamiento en Switch Capa 3



Nota. La figura muestra cómo se realiza la conexión con comutador de capa 3. Obtenido de: (CNNA, s.f.)

10.5 Protocolos

10.5.1. Protocolos para switch de Capa 2

- Ethernet: Es un protocolo de red que controla el método de comunicación entre equipos de usuario final y dispositivos de networking. La IEEE definió a Ethernet como protocolo 802.3 que protocolo de enlace

de datos del modelo ISO/OSI que suele utilizarse como parte de la pila TCP/IP.

- **Frame Relay:** es un protocolo de red WAN que define cómo se dirigen las tramas en una red de paquetes rápidos en función del campo de dirección de la trama. Frame Relay se utiliza habitualmente para conectar dos o más puentes de LAN a través de grandes distancias (IBM Docs, 2021).
- **WI-FI:** Es un estándar definido para las redes de área local inalámbricas (WLAN), basadas en la norma IEEE 802.11. Wi-Fi responde al acrónimo del término inglés “Wireless Fidelity” y se caracteriza porque la transmisión se realiza mediante el espectro electromagnético, el aire o el vacío (López F., 2020).

10.5.2 Protocolos para switch de capa 3

- **IP:** El protocolo IP es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es el responsable del crecimiento acelerado de Internet dado la funcionalidad del direccionamiento universal IP. Es uno de los protocolos de Internet más utilizados ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su entrega (Jurado, 2021).
- **IPSEC:** IPsec (Internet Protocol Security) está compuesto por varios protocolos de seguridad diferentes y está diseñado para garantizar que los paquetes de datos enviados a través de una red IP permanezcan invisibles e inaccesibles para terceros (Mocan, 2019).
- **ICMP:** (Internet Control Message Protocol) proporciona información de solicitud de conexión (echo request) y de retorno (echo replay) de los paquetes IP desde un equipo origen hacia un destino (IBM Docs, 2021)
- **IGMP:** (Internet Group Management Protocol) Protocolo de administración de grupos de Internet (IGMP) administra la membresía de equipos de usuarios finales y dispositivos de enrutamiento en grupos de multi-difusión.
- **PPTP:** (Point-to-Point Tunneling Protocol) El Protocolo de túnel punto a punto es un protocolo de red que permite la transferencia segura de datos desde un cliente remoto a un servidor empresarial privado mediante la creación de una red privada virtual (VPN) a través de redes de datos basadas en TCP/IP.

10.6 Diferencias

La Tabla 6 presenta un cuadro comparativo, en donde se pueden identificar las principales diferencias y beneficios del uso de cada tipo de switch en cada capa, con respecto a las necesidades que cada organización tiene:

Tabla 6

Diferencias entre switch capa 2 y capa 3

	Switch Capa 2	Switch Capa 3
Seguridad	No cuentan con suficientes mecanismos de seguridad. Se puede acceder a sus puertos y generar cualquier tipo de tráfico.	Cuentan con todos los niveles de control con los que un enrutador contaría. También existen métodos para prevenir el ingreso a la red de usuarios indeseados.
Tolerancia a Fallas	No cuenta con mecanismos para la tolerancia a fallas, tampoco con enlaces de redundancia y si existen, son mediante el uso de Spanning Tree que sirve gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes.	Cuenta con una variedad de mecanismos de control de fallas y también de respaldo en capa 2 o 3. Participan de los mecanismos de control de fallos en los enlaces conjuntamente con los enrutadores para que así, se pueda recuperar rápidamente la conexión entre los recursos y servicios de red.
Enrutamiento	Solo recuerdan las direcciones MAC.	Permite algunos tipos de enrutamiento estático y dinámico.
Alcance	Es utilizada en su mayoría para reducir el tráfico en una red local configurando VLANs	Tienen la capacidad de implementar Inter-VLANs. Puede comunicarse dentro o fuera de la red.
Dominio de Difusión	Conforman un solo dominio de difusión y varios dominios de colisión.	Conforma múltiples dominios de difusión.
Organizaciones	Para todo tipo de organizaciones, especialmente para pequeñas o medianas.	Las organizaciones quienes ocupan los comutadores, son grandes.
Inter-VLAN	No cuenta con una comunicación inter-VLAN.	SI cuenta con una comunicación inter-VLAN.

Recursos complementarios

- Video sobre: "Switch de capa 2 y capa 3 - Fundamentos de la Red" 
- Video sobre: "Explicación Classless Interdomain Routing" 
- Video sobre: "CAPA 2 vs CAPA 3" 
- Video sobre: "CURSO 2020 SWITCH CISCO CAPA 2 - 1 ° Parte - Curso para Gerentes o Jefes de TI configuración fácil" 
- Video sobre: "CURSO 2020 SWITCH CISCO CAPA 3 - 2 ° Parte - Curso para Gerentes o Jefes de TI configuración fácil". 

Actividad de aprendizaje 10

Descripción de la actividad

Una VLAN es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. De acuerdo con la Academia de Networking de Cisco, las VLAN:

- Segmentan lógicamente las redes conmutadas según las funciones, los equipos de proyecto o las aplicaciones de la organización, independientemente de la ubicación física o las conexiones a la red.
- Todas las estaciones de trabajo y servidores utilizados por un grupo de trabajo en particular comparten la misma VLAN, independientemente de la conexión física o la ubicación. En otras palabras, una estación de trabajo en un grupo de VLAN está restringida a comunicarse con servidores de archivos en el mismo grupo de VLAN.
- Los enrutadores en topologías de VLAN brindan filtrado de transmisión, seguridad y administración del flujo de tráfico.
- Las VLAN abordan la escalabilidad, la seguridad y la gestión de la red. Es posible que los conmutadores no puenteen el tráfico entre las VLAN, ya

que esto violaría la integridad del dominio de transmisión de la VLAN. El tráfico solo debe enrutarse entre VLAN.

- Una VLAN es un dominio de difusión creado por uno o más comutadores.
- El enrutamiento de capa 3 permite que el enrutador envíe paquetes a los tres dominios de transmisión diferentes.
- El beneficio clave de las VLAN es que permiten al administrador de la red organizar la LAN de forma lógica en lugar de físicamente.
- Las VLAN ofrecen un método para segregar una red física en una infraestructura de red lógica.
- Al implementar VLAN, se puede crear varias LAN virtuales en su infraestructura Ethernet. Las VLAN ayudan a reducir el tráfico.

El simulador **Packet Tracer** de la Academia de Networking de CISCO, permite configurar VLANs e Inter-VLANs en comutadores.

Esta actividad de aprendizaje se relaciona con la Configuración básica de una VLAN en un switch cisco utilizando el simulador Packet Tracer. Se pide:

1. Realizar la práctica de laboratorio 3.5.1 titulada “Configuración básica de una VLAN en un switch Cisco 2960, disponible en el Web desarrollado por la Academia de Networking de CISCO. Rellene todos los ejercicios que allí se señalan.

Al finalizar, elabore un informe de la Práctica de Laboratorio que despliegue de los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de cada punto con sus resultados, Conclusiones generales y Referencias bibliográficas.

Autoevaluación Capítulo 10

1. ¿Cuáles son los tipos de redes de computadoras?

PAN, LAN, MAN, WAN

De Sistema, Programación y Aplicación

LAN y WAN

Ninguna de las anteriores

2. ¿Qué es la red PAN?

Es una red que cubre un área geográfica amplia

Es aquella que se divide generalmente en segmentos lógicos más pequeños llamados grupos de trabajo

Es una red informática que se utiliza para interconectar dispositivos que deben estar dentro del rango de una persona (menos a 10 metros)

Todas las anteriores

3. ¿Qué es una red WAN?

Una red que se limita a un área tal como un cuarto o un solo edificio

Es una red que cubre una gran área geográfica, utilizando líneas de telecomunicaciones dedicadas, como líneas telefónicas

Una red que conecta las redes de dos o más localidades, pero no se extiende más allá de los límites de una ciudad

Se define como la forma de tender el cable a estaciones de trabajo individuales

4. ¿Qué topología física utiliza un hub o switch para la interconexión de computadoras?

Estrella

Bus

Anillo

Malla

5. ¿Qué topología física utiliza más recursos al implementarlas?

Anillo

Bus

Estrella

Malla

6. ¿La Red MAN es una red de alta velocidad que da cobertura en un área geográfica?

Extensa

Reducida

Estrecha

Mediana

7. ¿La WAN es útil para que los proveedores de Internet puedan brindar?

Mayor velocidad de carga y descarga

Mejor Conexión de Redes

Mejor infraestructura

Todas las anteriores

8. ¿La topología física de redes presenta?

- El orden de dispositivos
- La disposición de dispositivos
- La ubicación de dispositivos

Todas las anteriores

9. ¿La Topología física en la que las computadoras, los periféricos y los dispositivos de red forman un ciclo cerrado se denomina?

Estrella:

Anillo

Bus:

Árbol

10. ¿La red privada interna que permite a los empleados y al personal de una empresa compartir información de forma segura?

Internet

Extranet

Intranet

Todas



<https://acortar.link/JlkLS>

CAPÍTULO XI

Tecnologías para PAN
Wi-Fi & Bluetooth

11.1 Introducción

Hoy en día se pueden observar cómo los usuarios pueden disfrutar de los grandes avances tecnológicos utilizando tecnologías inalámbricas tales como WI-FI y Bluetooth, mismas que en la industria se las conoce como redes de uso personal (Personal Area Network, PAN), lo que ha provocado que los servicios y aplicaciones que en ella se emplean, mejoren la vida de las personas.

Una red de área personal conecta dispositivos electrónicos dentro del área cercana al usuario. El tamaño de una PAN varía desde unos pocos centímetros hasta unos pocos metros. Uno de los ejemplos más comunes de una PAN en el mundo real es la conexión entre un auricular Bluetooth, un teléfono inteligente o un computador portátil, tablets, impresoras, Smart Tv y otros dispositivos computarizados.

En los últimos años estas redes son las preferidas de los usuarios debido a múltiples beneficios que ofrecen, tales como movilidad, costo e infraestructura. Sin embargo, la capacidad de transmisión y aspectos relacionados con la seguridad de la información son aspectos que deben ser mejoras.

11.2 Definición de PAN

La red de área personal (PAN) es una red de datos utilizada para la comunicación entre los dispositivos electrónicos y diferentes tecnologías computacionales que son de uso personal. Algunas tecnologías conocidas infrarrojos, ZigBee, Bluetooth, Wi-Fi, etc.

PAN se enfoca en las personas ya que les permiten comunicarse con sus dispositivos personales (ejemplo, PDA, tableros electrónicos de navegación, agendas electrónicas, computadoras portátiles) para así establecer una conexión inalámbrica con el mundo externo.

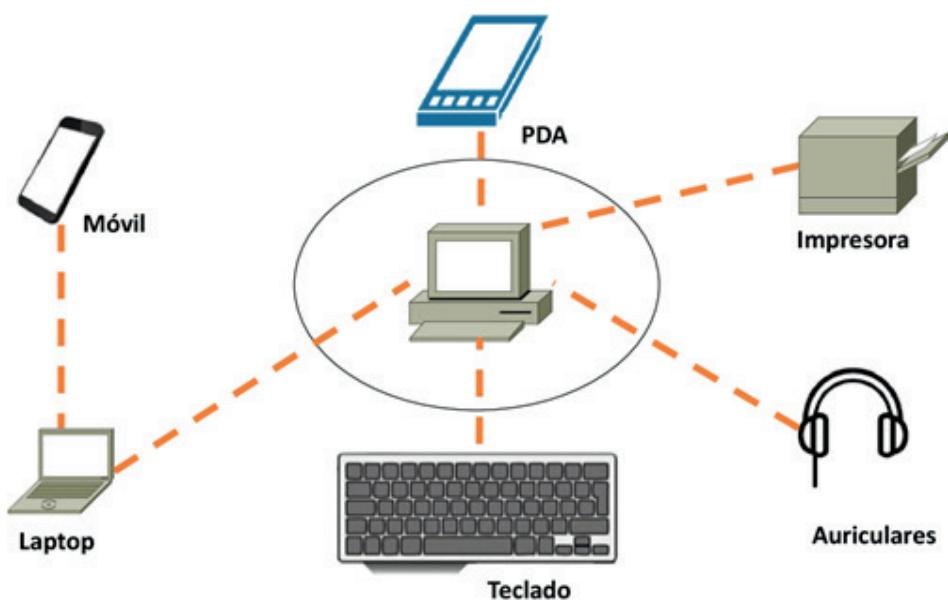
Cuando se habla de las redes PAN, estas se refieren a las redes inalámbricas que no logran tener un alcance amplio, por lo que su señal sólo puede llegar a dispositivos que se encuentren en un perímetro cercano al usuario (i.e., hogares, negocios, oficinas, etc.). De hecho, la señal es tan débil que puede semejar al alcance que tiene la tecnología Bluetooth. Sin embargo, dada esta cercanía, en el caso de los diferentes tipos de redes PAN la transferencia de los datos se hace velozmente incluyendo el acceso a Internet.

No obstante, a pesar de tener poco alcance, los usuarios pueden ampliar el espacio en donde llega su señal con el uso de repetidor o amplificador de la señal o un enrutador que permite conectar estos dispositivos al Internet.

Algunos ejemplos de dispositivos que se utilizan en un PAN son las computadoras personales, impresoras, máquinas de fax, teléfonos, PDA, escáneres y consolas de videojuegos. La Figura 64 muestra un diagrama de PAN típico (TipsMake, 2019):

Figura 64

Diagrama de una red PAN.



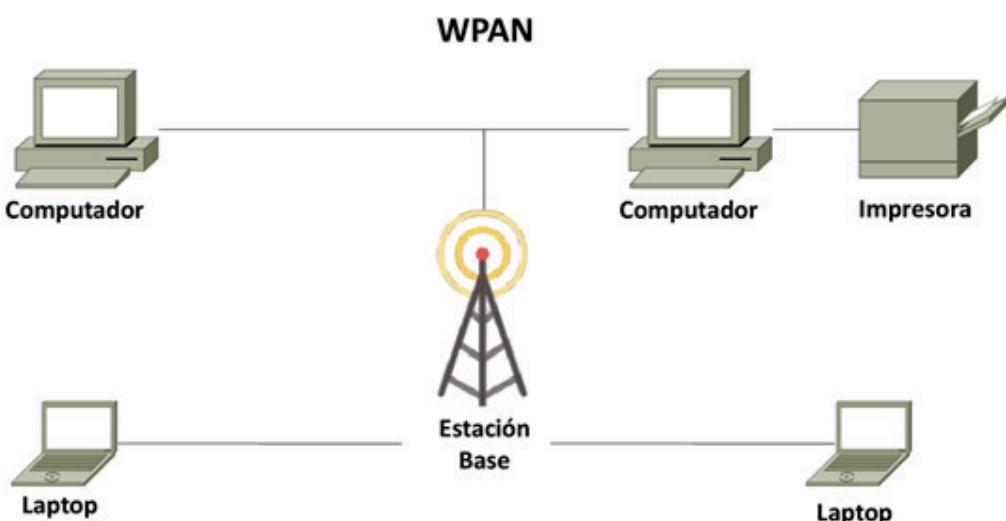
Nota. La figura representa una red PAN

11.3 Construcción de una PAN

Para la construcción de redes PAN se utilizan USB y FireWire. Tanto FireWire como USB son tecnologías que se emplean para conectar dispositivos a una computadora y transferir datos rápidamente. FireWire también se conoce como IEEE 1394 High Performance Serial Bus, y USB responde al acrónimo Universal Serial Bus. La principal diferencia entre los dos es que FireWire tiene 800 Mbps de capacidad de transmisión de datos, especialmente información de audio y visual. En cambio, un USB 2.0 tiene una tasa de transferencia de datos de 480 Mbps. Sin embargo, un USB 2.0 puede gestionar 127 dispositivos, mientras que un FireWire 800 solo puede administrar hasta 63 dispositivos.

Ambos funcionan con la tecnología plug-and-play lo que significa que puede conectar un dispositivo a su computadora mientras la computadora está encendida, y la computadora lo reconocerá y comenzará a comunicarse con él siempre y cuando el controlador ya ha sido instalado. La Figura 65 ilustra algunos de los componentes para la construcción de una PAN utilizando una estación base (TipsMake, 2019).

Figura 65
WPAN mediante Bluetooth.



Nota. La figura representa una red WPAN a través de Bluetooth. Obtenido de: (TipsMake, 2019).

Entre algunos ejemplos habituales se puede señalar: (1) Utilizar un teclado con interfaz Bluetooth que se conecta a una Tablet para controlar la interfaz que puede llegar a una bombilla inteligente cercana. Otro ejemplo, sería el de una impresora en una pequeña oficina o casa que se conecta a un escritorio, computadora portátil o teléfono cercanos. Lo mismo ocurre con los teclados y mouse u otros dispositivos que utilizan infrarrojo (IrDA, Infrared Data Association).

11.4 Wi-Fi

Wi-Fi responde al acrónimo 'Wireless Fidelity', que en español significa fiabilidad inalámbrica. Es una tecnología de transmisión de datos que utiliza el

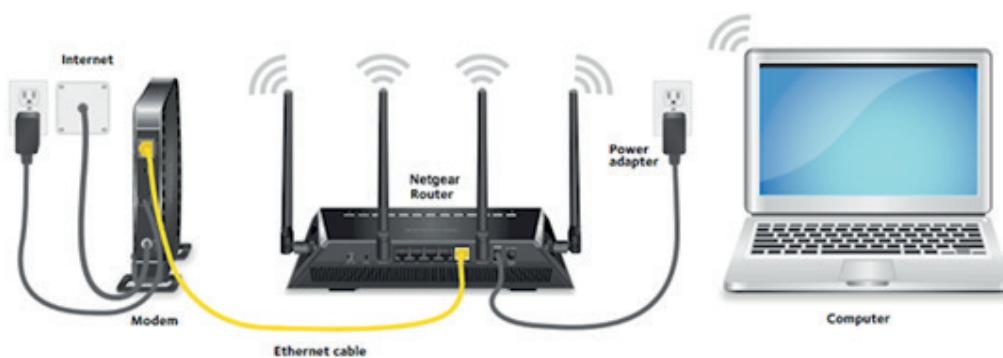
espectro electromagnético (el aire y el vacío) para una instalación que permite que las computadoras, teléfonos inteligentes u otros dispositivos se conecten a Internet o se comuniquen entre sí de forma inalámbrica dentro de un mapa de cobertura cercano.

Wi-Fi emplea señales de radio enlace que se transmite desde un enrutador inalámbrico a un equipo de usuario final cercano, que traduce la señal en datos y que se conecta al Internet conformando una red Wi-Fi. El enrutador inalámbrico está conectado físicamente a un módem del proveedor de servicios de Internet (Internet Service Provider, ISP) Internet y que actúa como un concentrador para transmitir la señal de Internet a todos sus dispositivos habilitados para Wi-Fi (véase la Figura 66).

En 1997, el IEEE lanzó el estándar 802.11, específicamente el IEEE 802.11b. Por aspectos de márquetin se decidió utilizar la abreviatura de “Wi-Fi”, que se adoptaría como el término universal para describir una red LAN inalámbrica. El estándar “b” fue el primero en aparecer y soporta una velocidad de transmisión de hasta 11 Mbps compartidos en el espectro de 2,4 Ghz. Luego apareció el estándar IEEE-802.11a en 2002, capaz de transmitir hasta 54 Mbps en el espectro de frecuencia de 5 Ghz. Actualmente, existe el estándar IEEE-802.11ac, que es capaz de transmitir hasta 1.3Gbps tanto en los 2.4Ghz como 5Ghz simultáneamente (Brown, 2019) (véase Figura 67).

Figura 66

WPAN mediante Bluetooth.



Nota. La figura representa la arquitectura de una red Wi-Fi. Obtenido de: (Brown, 2019).

En relación al rango de frecuencias 2.4 y 5 GHz, cabe señalar que ambas frecuencias difieren en el rango de cobertura y la velocidad que proporcionan las bandas. La banda de 2,4 GHz tiene cobertura en un rango más largo, sin

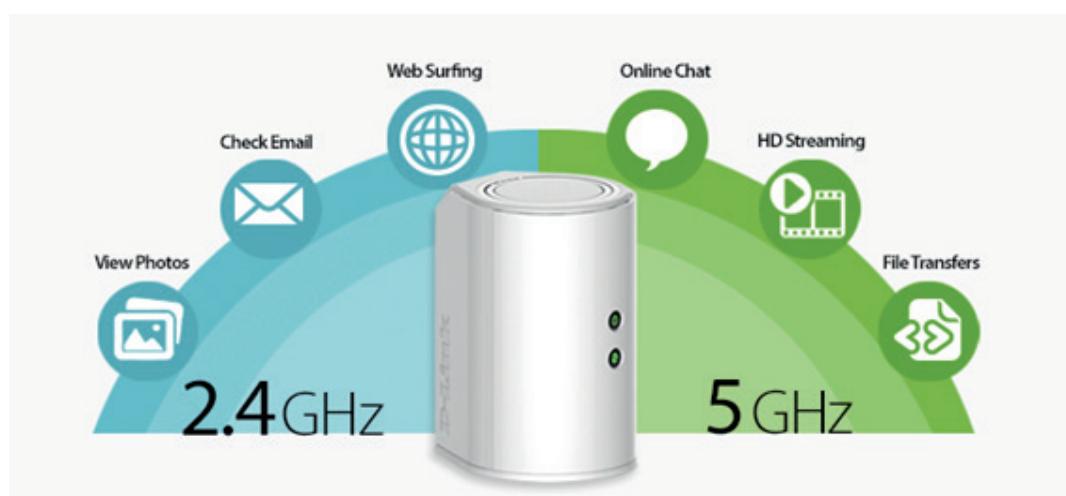
embargo, transmite datos a velocidades más lentas. La banda de 5 GHz proporciona menos cobertura, sin embargo, transmite datos a velocidades más rápidas. El rango es más bajo en la banda de 5 GHz debido a que las frecuencias más altas no pueden penetrar objetos sólidos, como paredes y pisos. Sin embargo, las frecuencias más altas permiten que los datos se transmitan más rápido que las frecuencias más bajas, por lo que la banda de 5 GHz le permite cargar y descargar archivos más eficientemente.

Es importante señalar que las conexiones Wi-Fi pueden ser afectadas debido a la interferencia de otros dispositivos (microondas y los garajes automáticos), o por aspectos relacionados con el medio ambiente como lluvias o el viento. Otro aspecto a considerar es que la banda de frecuencias de 5 GHz tiene 23 canales para que los dispositivos usen, mientras que 2.4GHz dispone solo de 11 canales.

Por tanto, si desea un mejor alcance, conviene utilizar 2,4 GHz. Si se requiere mayor velocidad, es preferible utilizar la banda de 5 GHz que es la más nueva de las dos, y que tiene el potencial de eliminar cierta la interferencia de la red para maximizar su rendimiento. Sin embargo, por diseño, 5GHz no puede llegar tan lejos como 2.4GHz que a su vez es la más compatible con varios dispositivos de red (Zona112, 2019).

Figura 67

Prestaciones de las distintas bandas de frecuencias de Wi-Fi.



Nota. La figura representa las bandas de frecuencia. Obtenido de: (Zona112, 2019).

11.5 Ventajas y desventajas

La popularidad de las LAN inalámbricas se debe principalmente a su bajo costo de instalación, operación, mantenimiento y facilidad de integración con otras redes y componentes de red. Entre las principales ventajas de Wi-Fi se puede señalar:

- Conectividad inalámbrica: No se necesita las conexiones físicas por medio de cables, uso de canaletas o suministros de cableado estructurado.
- Movilidad: Ofrece libertad para trasladar el equipo de usuario final y seguir conectado sin que esto suponga ningún problema.
- Coste: Al no invertir en cableado y dispositivos de conectividad como commutadores, hace que una red Wi-Fi tenga un coste mucho menor que las redes cableadas.
- Compatibilidad: La Wi-Fi Alliance es la organización que asegura la compatibilidad total entre dispositivos.
- Las redes Wi-Fi pueden no ser deseables por varias razones especialmente por aspectos de seguridad y rendimiento. A continuación, se listan algunas de ellas:
- Velocidad: La capacidad de transmisión es mucho menor comparado con las velocidades que se pueden lograr mediante cables.
- Latencia: Existen ciertos agentes externos que pueden afectar la conexión como muros, paredes, distancia de los equipos, entre otros.
- Interferencias: Los equipos electrónicos y electrodomésticos pueden generar ondas que interfieren con las de este tipo de redes inalámbricas. Así mismo, muros o puertas que afectan que la señal llegue a ciertos rincones de la casa.
- Seguridad: Si no existen configuraciones de seguridad de la información, son un espacio abierto para delitos informáticos.

11.6 Bluetooth

Bluetooth es un protocolo de comunicaciones que sirve para la transmisión inalámbrica de información tales como fotos, música, contactos, y voz entre diferentes dispositivos que se hallan dentro de un mapa de cobertura 1<10<100 metros. Bluetooth está asociado a los teléfonos móviles que fueron los primeros dispositivos en incorporar el protocolo. Sin embargo, esta tecnolo-

ología inalámbrica se encuentra presente, hoy en día, en smartphones, tablets, portátiles, mouses, teclados, impresoras, auriculares, televisores inteligentes, cámaras digitales, reproductores MP3 o videoconsolas. Bluetooth transmite inalámbricamente datos y voz a través de ondas de radio que operan en la banda de frecuencias de los 2,4 GHz. Bluetooth ha sido ratificado como estándar IEEE 802.15.1 en el 2002.

En Bluetooth, los equipos deben encontrarse dentro de un radio de alcance, que suele ser corto, aunque puede variar en función del dispositivo (Nat Apuntes, 2020). La Tabla 7 muestra las clases y versiones basadas en la potencia de transmisión. La Tabla 7 en cambio, muestra en función de la capacidad del canal.

Tabla 7

Alcance de las distintas clases de Bluetooth en base a la potencia de transmisión

Potencia de transmisión			
Clase	Potencia máxima permitida (mW)	Potencia máxima permitida (dBm)	Alcance (aproximado)
Clase 1	100 mW	20 dBm	~100 metros
Clase 2	2.5 mW	4 dBm	~5-10 metros
Clase 3	1 mW	0 dBm	~1 metro

Nota. La tabla representa el alcance de las clases de Bluetooth en base a la potencia de transmisión. Obtenido de: (Nat Apuntes, 2020).

Tabla 8

Alcance de las distintas clases de Bluetooth en base a la capacidad de un canal

Capacidad de canal	
Versión	Mbit/s
Versión 1.2	1
Versión 2.0 + EDR “Enhanced Data Rate” “mayor velocidad de transmisión de datos”	3
Versión 3.0 + HS	24
Versión 4.0	32

Nota. La tabla representa el alcance de las clases de Bluetooth en base al canal. Obtenido de: (Nat Apuntes, 2020).

Bluetooth tiene la necesidad de colocar la dirección de visualización. Debido a esta limitación, los controles remotos no pueden cambiar de canal si no están dirigidos al televisor o al parlante.

Recursos complementarios

- Información más detallada no solo de la red PAN sino también de las redes LAN, WAN, y WLAN. 
- Video con información más detallada de una PAN así como ejemplos más didácticos. 

Actividad de aprendizaje 11

Descripción de la actividad

WLAN son las siglas de Wireless Local Area Network (red de área local inalámbrica). Son redes de comunicación de datos que utilizan ondas electromagnéticas como medio de transmisión. Una WLAN es un sistema de comunicación de datos flexible ampliamente utilizado como alternativa o extensión de la LAN cableada. Utiliza tecnología de radiofrecuencia que permite una mayor movilidad a los usuarios al minimizar las conexiones por cable. En comparación con la red tradicional, la WLAN ofrece las siguientes ventajas:

- Movilidad: Información en tiempo real en cualquier lugar de la organización o empresa para todos los usuarios de la red.
- Facilidad de instalación: Evite trabajos para tender cables a través de paredes y techos.
- Flexibilidad: le permite ir donde el cable no puede.
- Escalabilidad: cambiar la topología de la red es fácil y trata de la misma manera a las redes grandes y pequeñas.

El simulador Packet Tracer de la Academia de Networking de CISCO, permite configurar WLANs utilizando routers inalámbricos o puntos de acceso inalámbricos (WAP).

Esta actividad de aprendizaje tiene como propósito la configuración básica de del router Linksys inalámbrico, lo que permite el acceso remoto tanto desde la PC como desde una conectividad inalámbrica con seguridad WEP utilizando el simulador Packet Tracer.

Se pide:

1. Realizar la práctica de laboratorio 7.5.1 titulada “Configuración inalámbrica básica”, disponible en la Web, desarrollado por la Academia de Networking de CISCO. Rellene todos los ejercicios que allí se señalan.

Al finalizar, elabore un informe de la Práctica de Laboratorio que despliegue de los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de cada punto con sus resultados, Conclusiones generales y Referencias bibliográficas.

Autoevaluación Capítulo 11

1. El switch es un dispositivo de red cuya funcionalidad es la interconexión de equipos en la capa de enlace de datos, también es utilizado como un conmutador de paquetes. En qué otra capa del modelo OSI puede ser empleado:

Capa de aplicación

Capa Física

Capa de transporte

Capa de Red

2. ¿Cuál es la razón por qué el Proxy se ubica en 4 de las 7 capas del modelo OSI?

Porque es un intermediario entre el cliente y el servidor web en el envío de paquetes o recursos

Porque existen varios tipos de proxy que se ubican cada uno en diferentes capas

Porque es parte del router y cambia la dirección IP a los paquetes para que lleguen más rápido a su destino

3. ¿Cuál es la principal diferencia entre un hub y un bridge?

No existe diferencia alguna cumple la misma función y son exactamente iguales

Todos los puertos de un hub son un único dominio de colisión, mientras que un bridge divide o segmenta una red en diferentes dominios de colisión

Un hub divide una red en varios dominios de colisión (uno por cada dispositivo), mientras que un bridge tan solo conecta dispositivos sin segmentar la red

4. ¿En qué capa del modelo OSI funciona principalmente una puerta de enlace?

Capa de transporte

Capa de red

Capa de sesión

5. ¿Los Firewalls pueden ser tanto físicos como lógicos?

Falso

Verdadero

6. ¿Cuáles son los roles de un router?

Comunicación entre redes, mejor selección de ruta, reenvío de paquetes y filtrado de paquetes

Intermediario entre un cliente y un servidor y detecta malware

Decodifica paquetes y a su vez comprime tramas para su posterior envío

7. ¿Qué dispositivo inalámbrico que brinda facilidades de accesibilidad para un hogar y en el ámbito empresarial con mejores prestaciones?

Módem

Access Point

Router

Transceiver

8. ¿Qué orden lógico se debe cumplir en una red que cuenta con un servidor proxy?

Proxy-dispositivos-Internet

Internet-dispositivos-proxy

Dispositivos-proxy-Internet

9. ¿Cuál es la función principal del firewall (cortafuego)?

Es el encargado de transmitir o recibir señales de telecomunicaciones desde una LAN hacia otra LAN a través de una WAN

Tiene como objetivo autorizar o filtrar la transmisión de diversos paquetes que provienen de diferentes dispositivos

Es un dispositivo de interconexión que realiza funciones de commutación y concentración en el caso de los de capa 2 del modelo OSI

10. ¿Qué dispositivo tiene como objetivo principal el dividir una red en segmentos o dominios de broadcast?

Switch

Bridge

Cortafuegos

Router



<https://acortar.link/vTSCj7>

CAPÍTULO XII

Servicios de Red

12.1 Introducción

En este apartado se abordan los servicios básicos de las redes de datos. Los servicios de redes consisten en el proceso de comunicación entre varios usuarios de dispositivos finales o sistemas informáticos que están vinculados o conectados en red para intercambiar información y compartir recursos. Son aquellos que ayudan a llevar a cabo diferentes tareas desde optimizar el uso de una impresora, hasta tareas complejas como el almacenamiento e intercambio de información de una empresa.

Un servicio de red puede ser la ejecución de una aplicación, un sistema informático, un servicio o un protocolo que se ejecuta en la capa de Aplicación del modelo OSI. El servicio puede proporcionar almacenamiento, manipulación, despliegue, comunicación u otra capacidad para trasmisir o recibir datos. Cada servicio lo proporciona un equipo computacional llamado servidor, en el cual se instala, configura y ejecuta uno o múltiples servicios a los que se accede a través de una red con usuarios registrados (clientes) que se ejecutan en otros dispositivos sean locales o remotos. Algunos ejemplos pueden ser los servicios DHCP, DNS, Web y de correo electrónico.

12.2 Servidores

12.2.1 Servicio DHCP (Dynamic Host Configuration Protocol)

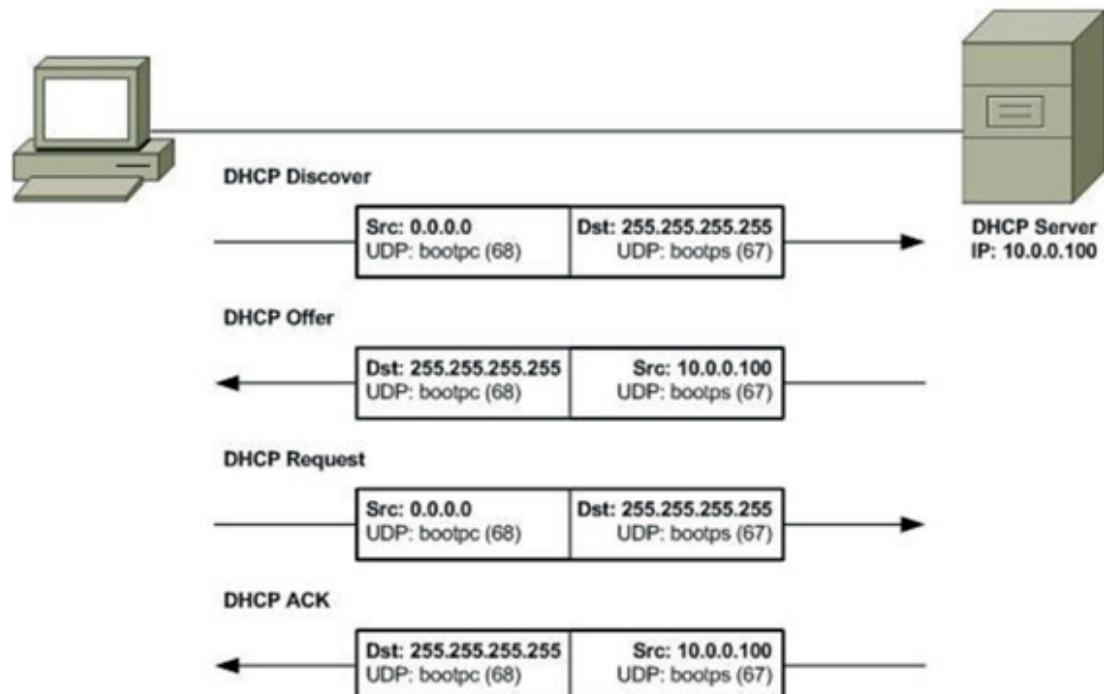
Este servidor permite la configuración dinámica o automática de direcciones IP de los equipos de usuario final o de los dispositivos de red conectados, el cual simplifica la administración y configuración IP. Se basa en el protocolo cliente-servidor estándar conocido como DHCP para responder a las consultas de difusión de los clientes. Un cliente es un dispositivo que está configurado para usar DHCP para solicitar parámetros de red desde un servidor DHCP. El servidor DHCP mantiene un grupo de direcciones IP disponibles y asigna una de ellas al host (Odom, 2016). Un servidor DHCP también puede proporcionar algunos otros parámetros, como:

- El servidor proporcionará al cliente al menos los siguientes parámetros:
 - Dirección IP
 - Máscara de subred

- Opcionalmente, el servidor DHCP podrá proporcionar otros parámetros de configuración tales como:
 - Puerta de enlace
 - Servidores DNS
 - Otros parámetros adicionales

Figura 68

Funcionamiento de un servidor DHCP



Nota. La figura representa didácticamente la petición de un cliente y la función del servidor. Obtenido de: (Aun, 2020).

La Figura 68 ilustra como el servidor DHCP asigna direcciones dentro de un rango de direcciones IP previamente establecido basándose en la dirección de un host. Sin embargo, en el caso de que existan conflictos de asignación, el cliente solicitará y comprobará otra dirección IP hasta tener una correctamente asignada (Salazar, 2017).

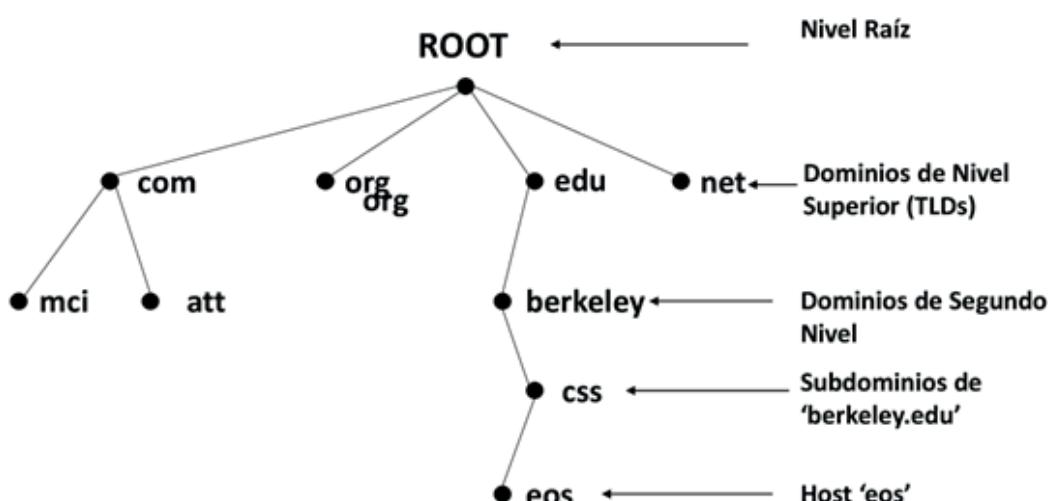
12.2.2 Servidor DNS

El sistema de nombres de dominio (Domain Name System, DNS) puede ser comparada como la guía telefónica de Internet. Cuando los usuarios escriben nombres de dominio en un navegador web tal como “www.espe.edu.

ec” o “www.google.com”, el DNS es responsable de encontrar o traducir la dirección IP correcta para esos sitios web. Inmediatamente, los navegadores usan esas direcciones para comunicarse con los servidores de origen o destino para acceder a la información del sitio web. En concreto, los servidores DNS traducen las solicitudes o consultas de nombres en direcciones IP o viceversa, controlando a qué servidor llegará un usuario final cuando escriba un nombre de dominio en su navegador web. La Figura 69 presenta la estructura del DNS.

Figura 69

Estructura jerárquica de DNS



Nota. La figura representa la jerarquía de nombres organizada en forma de árbol. Obtenido de: (InetDaemon, 2018).

La Figura 69 ilustra en la capa superior el dominio raíz. Un dominio es un grupo lógico de equipos en una red. Cada dominio de primer nivel o de niveles inferiores incluye una o más zonas de autoridad que publican la información acerca del dominio y los nombres de servicios. DNS es una base de datos distribuida jerárquica descentralizada que permite que las computadoras reconozcan correctamente un nombre de dominio completamente calificado. Un servidor de nombres contiene información de direcciones sobre otros equipos de usuario final en la red (Tanenbaum A. , Redes de Computadoras, 2012).

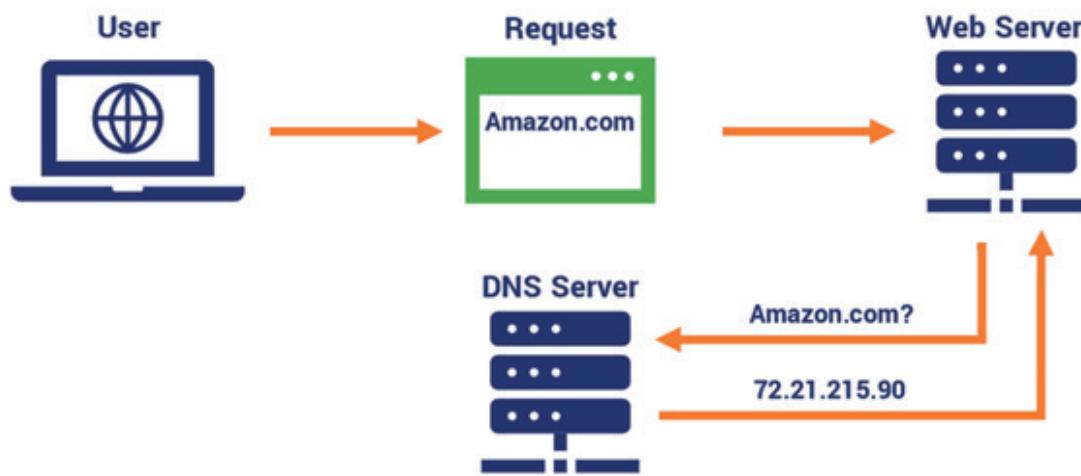
La utilidad principal de este servicio es la simplificación y la comodidad para el usuario ya que puede almacenar varios tipos de información sobre cada nombre de dominio. Además, el DNS hace que los nombres de dominio sean legibles por humanos. Por tanto, el DNS puede ser usado para diferentes propósitos. A continuación, se describen algunos de ellos:

- Búsqueda directa
- Resolución de direcciones inversa
- Resolución de servidor de correo
- Obtener claves públicas
- Localizar servidores para servicio predeterminado

De acuerdo con la Academia de Networking de Cisco, el servidor DNS funciona de la siguiente manera (Hope, 2017), (véase Figura 70):

- El cliente realiza una solicitud mediante una dirección Web, por ejemplo, www.cisco.com.
- El servidor DNS relaciona el nombre de dominio con la dirección IP, ya que los dispositivos utilizan números.
- El número se envía de regreso al cliente para utilizarlo en la realización de solicitudes del servidor.

Figura 70
Funcionamiento del servicio DNS



Nota. La figura representa como un usuario solicita el sitio web de Amazon y cómo interactúa con el DNS server. Obtenido de: (Mezquita, 2021).

12.2.3 Servidor Web

El objetivo primordial del servidor web es almacenar, procesar y entregar información entre páginas web a los usuarios. Esta intercomunicación se realiza mediante el protocolo de transferencia de hipertexto (HTTP). Los servi-

dores Web se encargan de proporcionar información que solicita un usuario determinado mediante su navegador cuando navega en el Internet (Barroyeta, 2020). Para que este servicio funcione se requiere de algunos componentes (Netink, 2020):

- **URL:** El localizador de recursos uniforme (Uniform Resource Locator, URL) que es la dirección de un recurso único dado en la Web.
- **HTTP:** El protocolo de transporte de hipertexto (Hyper Text Transfer Protocol, HTTP) que permite la transferencia de información a través de archivos en la World Wide Web.
- **WWW:** World Wide Web que es una colección de sitios o páginas web almacenadas en servidores web y conectados a computadoras locales a través de Internet.
- **HTML:** Lenguaje de marcaje de hipertexto (Hypertext Mark-up Language, HTML), que es un sistema estandarizado para etiquetar archivos de texto que poseen hipervínculos con las páginas de la World Wide Web. La Figura 71 presenta el funcionamiento de un servidor Web

Figura 71

Funcionamiento de un servidor WEB



Nota. La figura representa la función de un servidor web en una red Android. Obtenido de: (DataFlair, 2021).

Uno de los principales servidores Web más utilizados en la industria es el Apache Web server. Apache es un software de servidor web multiplataforma de código abierto y de libre distribución que funciona en casi todos los tipos de sistemas operativos tales como Windows, Linux, Mac OS, Unix, etc.

Los protocolos que procesan las solicitudes a un servidor web son HTTP que utiliza el puerto 80 y HTTPS que emplea el puerto 443. La diferencia fundamental entre los dos protocolos es que HTTPS usa TLS (Transmission Layer Security, SSL) para encriptar las solicitudes y respuestas HTTP normales. Como resultado, HTTPS es mucho más seguro que HTTP.

Hay dos tipos principales de mensajes HTTP: solicitudes y respuestas. Las solicitudes HTTP son generadas por el navegador de un usuario web. Estas solicitudes HTTP van a un servidor de origen o un servidor de caché proxy, y ese servidor generará una respuesta HTTP. Las respuestas HTTP son respuestas a las solicitudes HTTP.

Existen dos tipos de páginas web que se almacenan en un servidor web: Las páginas web estáticas que no cambian su contenido y las páginas web dinámicas que se generan cuando se solicita la página.

12.2.4 Servidor E-mail

Es un servicio que permite a los usuarios enviar y recibir correos electrónicos sobre una red de datos lo que facilita la comunicación para personas y empresas. Es un software instalado que envía y recibe correos electrónicos y que permite al administrador del sistema gestionar cuentas de correo electrónico para cualquiera de los dominios alojados en el servidor. El servidor de correo funciona mediante algunos protocolos de comunicación cuyo mensaje atraviesa por una serie de servidores para llegar a su destino final. Los servidores de correo electrónico se pueden clasificar en correos entrante y saliente. A continuación, se exponen los protocolos utilizados:

SMTP: Protocolo simple de transferencia de correo (Simple Mail Transfer Protocol, SMTP) que gestiona cualquier solicitud de correo electrónico saliente y los envía a través del Internet. Para su funcionamiento se utilizan algunos puertos lógicos. El puerto 25 establecido en 1982 que es estándar y se utiliza para la retransmisión SMTP. El puerto 587 que soporta TLS, lo que implica que los correos se envían de forma encriptada o segura. El puerto 465 que ya ha sido reemplazado por los puertos 587 y 2525. SMTP además se conecta en el puerto 110. Para correos encriptados utiliza el puerto 995 para conexiones SSL y TLS.

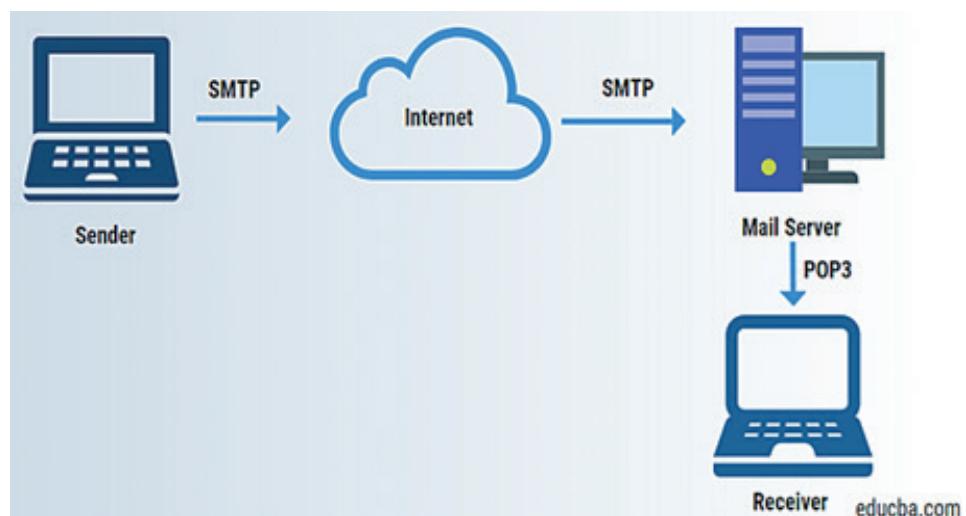
POP / IMAP: Protocolos útiles para los servidores de correo entrante. Existen dos variantes: POP3 e IMAP. Los servidores de protocolo de oficina postal

(Post Office Protocol versión 3, POP), son más conocidos por recuperar el contenido de la bandeja de entrada en el almacenamiento físico de su equipo de usuario final. Los servidores IMAP, cuya abreviatura es Protocolo de acceso a mensajes de Internet (Internet Message Access Protocol, IMAP), se utilizan para la sincronización directa de todo el buzón. Las versiones de POP son más nuevas, pues ofrecen más funciones por lo que es el protocolo preferido. POP3 se conecta al servidor de correo en el puerto 143. En el caso de un correo encriptado utiliza el puerto 993 para conexiones SSL/TLS.

En la industria existen servidores de correo, tanto comerciales como gratuitos, que utilizan SMTP, algunos ejemplos son: Amazon SES es una plataforma basada en la nube con una interfaz SMTP, Microsoft Exchange Server bajo Windows Server, Servidor de correo entrante de Gmail (pop.gmail.com.), Servidor de correo saliente de Gmail (smtp.gmail.com), Yahho.com, Send mail, Zimbra Email Server, etc. La Figura 72 presenta el funcionamiento de este servicio.

Figura 72

Envío de correo electrónico de cliente a servidor



Nota. La figura representa el proceso de envío de correo. Obtenido de: (NOW, 2018)

Recursos complementarios

- Video sobre: “DNS (Sistema de Nombres de Dominio)” 
- Video acerca del DHCP y la función que cumple dentro de un servidor 
- Video sobre los servidores web 
- Video sobre: “¿Qué es el SMTP?” 

Actividad de aprendizaje 12

Descripción de la actividad

Los servicios de red consisten en una amplia gama de aplicaciones de software y herramientas de conectividad que son administrados por un equipo central y distribuidos a las computadoras en red. Existen algunos servicios tradicionales como el DHCP y el DNS.

El simulador Packet Tracer de la Academia de Networking de CISCO permite configurar la mayoría de los servicios de Red en un entorno simulado.

Esta actividad de aprendizaje tiene como propósito la configuración básica de Servidores de DHCP y servidores DNS utilizando el simulador Packet Tracer.

Se pide:

Realizar la práctica de laboratorio 10.2.2.8 titulada “Packet Tracer: Servidores de DHCP y servidores DNS”, disponible en la Web, desarrollado por la Academia de Networking de CISCO. Rellene todos los ejercicios que allí se señalan. Al finalizar, elabore un informe de la Práctica de Laboratorio que despliegue de los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de cada punto con sus resultados, Conclusiones generales y Referencias bibliográficas.

Autoevaluación Capítulo 12

1. ¿Cómo se clasifican los medios de transmisión?

Guiados y no guiados

Par trenzado y vía satélite

Inalámbrico y ondas electromagnéticas

Infrarrojo y fibra óptica

2. ¿Cómo se clasifican los medios de transmisión guiados?

Aire y ondas

Coaxial, infrarrojo, fibra de aluminio

Par trenzado, coaxial y fibra óptica

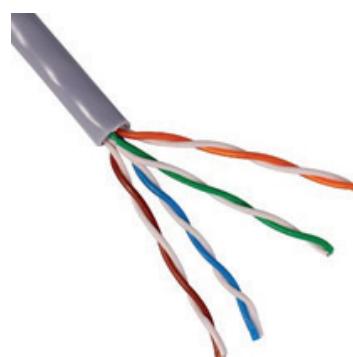
Infrarrojo

3. ¿La atenuación, distorsión y ruido reducen las señales de transmisión?

Verdadero

Falso

4. Observe la imagen y defina qué tipo de cable es:



Fibra óptica

Coaxial

RJ-45

Par trenzado

5. Complete. La comunicación inalámbrica se propaga por medio de ondas...

Radiales

Satelitales

Electromagnéticas

Inalámbricas

6. ¿Cuáles son los tipos de fibra óptica?

Ondas de radio y electromagnéticas

Monomodo y Multimodo

Monomodo e Infrarrojo

Óptica y multimodo

7. ¿Cuáles son los intervalos de frecuencia de los medios inalámbricos?

Ondas de radio, infrarrojo y electromagnéticas

Microondas, fibra óptica e infrarrojos

Vía satelital, ondas electromagnéticas y radio

Microondas, ondas de radio e infrarrojos

8. ¿Cuál es la frecuencia de cobertura del espectro electromagnético?

Entre 1 y 40 GHz

Entre 1 y 30 GHz

Entre 1 y 10 Hz

Entre 1 y 20 Hz

9. ¿Las ondas de radio necesitan de antenas parabólicas?

Verdadero

Falso

10. Complete: Debido a que los medios de transmisión infrarrojos no pueden traspasar las paredes, beneficia a , dado que no tiene dificultades de asignación de frecuencias.

La transferencia de datos

La seguridad anti espionaje

La comunicación satelital



<https://acortar.link/IoU8AE>

CAPÍTULO XIII

Tecnologías WAN

13.1 Introducción

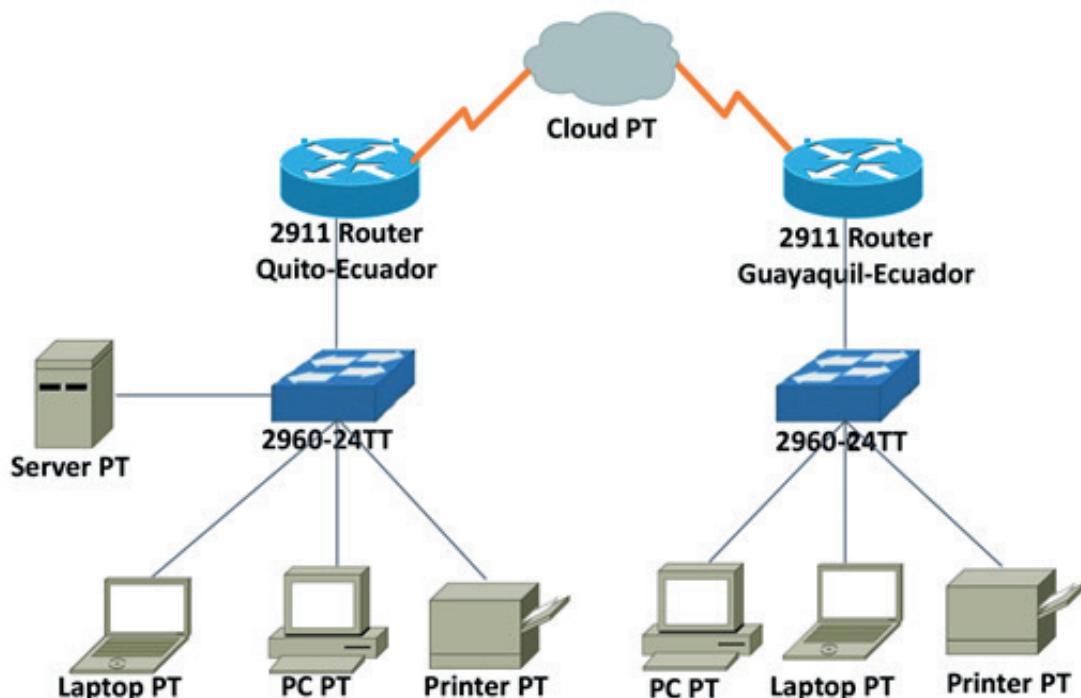
Este capítulo tiene como propósito estudiar y comprender el funcionamiento, topología, tecnologías o protocolos y equipos que intervienen en la construcción de las redes de área extendida (Wide Area Network, WAN).

Una WAN es una red de datos que cubre un área geográfica amplia utilizando líneas de telecomunicaciones dedicadas tales como líneas telefónicas, líneas arrendadas o satelitales. Las redes WAN de manera general, se basan en compartir recursos de equipos ubicados en todo el globo terráqueo y tienen como objetivo principal el estar siempre disponibles para cualquier usuario. Un ejemplo tradicional es la Internet.

Una WAN consiste además en la interconexión de varias redes de área local o metropolitana ubicadas en diferentes ciudades, países y continentes la cual requiere del uso de sistemas de telecomunicaciones para conseguir este fin. La Figura 73 ilustra la conformación y topología de una red WAN.

Figura 73

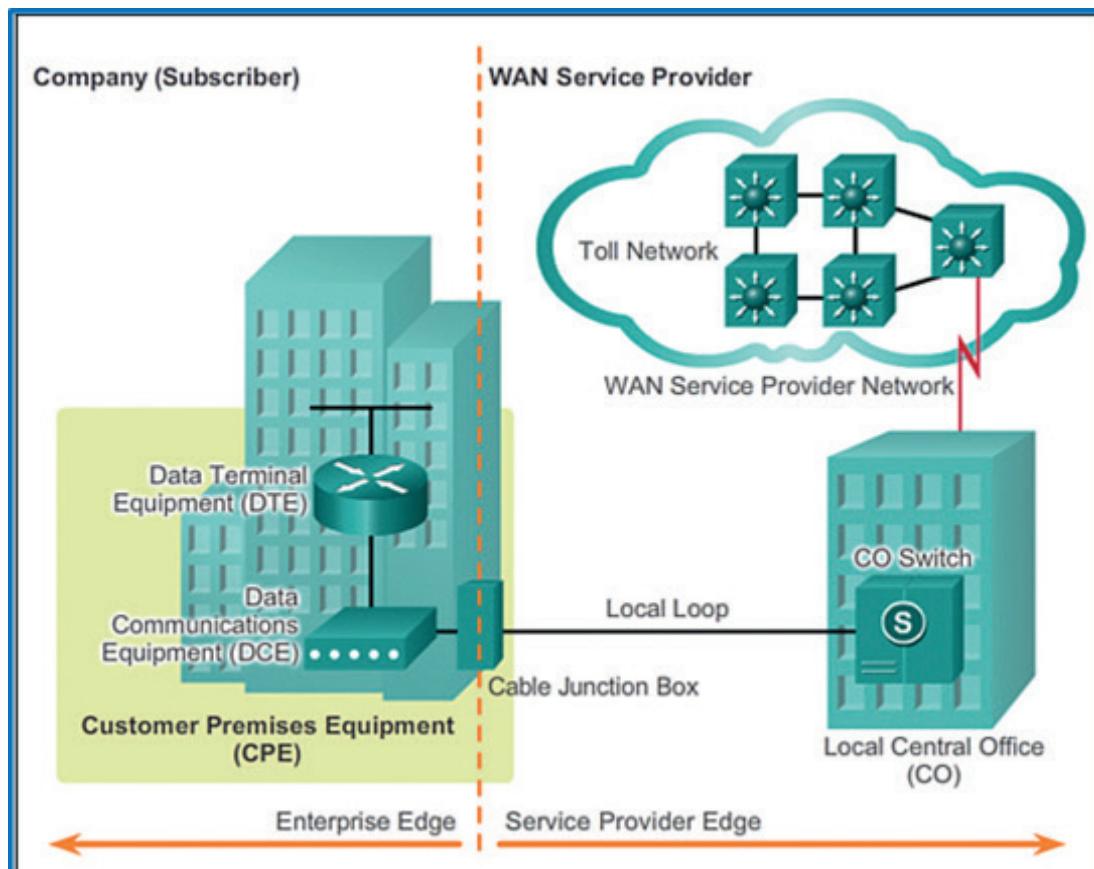
Estructura y conformación de una Red WAN entre dos ciudades



Nota. La figura representa la estructuración de una red WAN entre dos ciudades, con sus dispositivos respectivos.

En relación a los elementos de la infraestructura WAN, de acuerdo con la Academia de Networking de CISCO se distinguen (ver Figura 74):

- Equipo en las instalaciones del cliente (Customer Premises Equipment, CPE): que son los dispositivos y el cableado interno ubicados en el perímetro de la empresa que se conectan a un enlace del operador.
- Equipo de comunicaciones de datos (Data Communications Equipment, DCE): El cual provee una interfaz para conectar a los suscriptores a un enlace de comunicación en la infraestructura de la WAN.
- Equipo terminal de datos (Data terminal Equipment, DTE): El cual se conecta al bucle local a través del DCE. Es el equipo que transmite o recibe señales analógicas o digitales a través (e.g, un módem).
- Punto de demarcación (Demarcation point): es el lugar donde la responsabilidad de la conexión cambia del usuario al proveedor del servicio.
- Bucle local: el cable real de cobre o fibra que conecta el CPE al CO del proveedor de servicios (última milla)
- Oficina central (Central Office, CO): Es la instalación o el edificio del proveedor de servicios local que conecta el CPE a la red del proveedor.
- Red de peaje (Toll networks): que consta de líneas de comunicaciones de fibra óptica, commutadores, enrutadores y otros equipos digitales de larga distancia, dentro de la red del proveedor WAN.

Figura 74*Elementos y terminología WAN*

Nota. Equipos y terminología WAN. Obtenido de: (Salazar, 2017).

13.1 Topologías WAN

Punto a punto

Esta topología se basa en crear y conectar con un enlace permanente extremo a extremo o de dos nodos finales. La Figura 75 muestra de manera gráfica la topología de punto a punto.

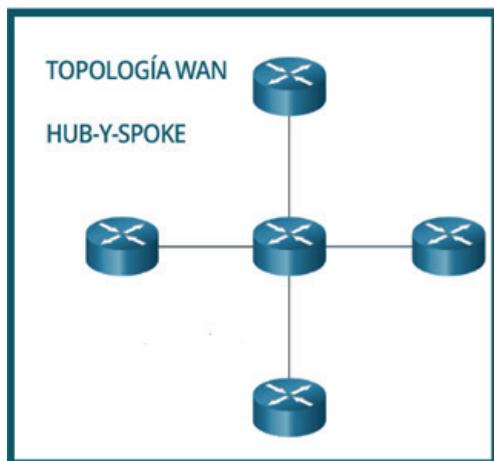
Figura 75*Topología WAN punto a punto*

HUB y SPOKE

Esta es una versión WAN con topología en estrella en la cual un nodo central interconecta nodos ubicados en lugares distintos y distantes mediante el uso de enlaces punto a punto. Estos nodos no pueden intercambiar datos con los otros nodos sin circular por el sitio central (ver Figura 76).

Figura 76

Topología WAN Hub y Spoke



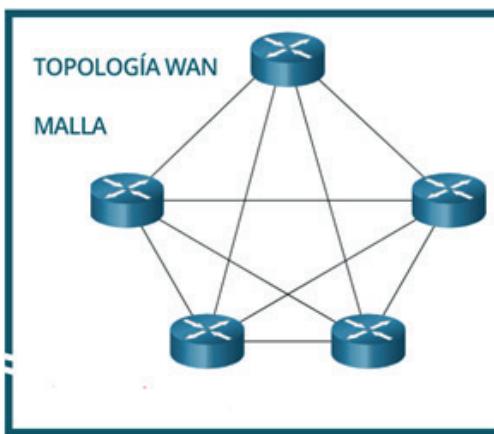
Nota. Obtenido de: (CISCO-CCNA, 2020).

Malla

Esta topología provee alta disponibilidad, sin embargo, requiere que cada nodo final esté interconectado con cualquier otro sistema. En consecuencia, los costos pueden ser representativos. Cada enlace es básicamente un enlace punto a punto al otro nodo (ver Figura 77).

Figura 77

Topología de malla



Nota. Obtenido de: (CISCO-CCNA, 2020).

13.3 Infraestructuras WAN públicas

Son redes que usan equipos portadores de telecomunicaciones en un área extensa que pertenecen por lo general a las operadoras, mismas que brindan servicios de comunicación a sus usuarios por medio de una membresía o costo de arrendamiento.

En la infraestructura de WAN pública el proveedor de servicios de telecomunicaciones puede rentar equipos portadores de telecomunicaciones y ofrecer el acceso a Internet de banda ancha mediante acceso a línea de abonado digital (Digital Subscriber Line), cable y satélite. A continuación, se explican brevemente estas tecnologías:

DSL es una tecnología de conexión siempre activa que utiliza líneas telefónicas de par trenzado existentes para transportar datos de gran ancho de banda y proporciona servicios IP a los suscriptores. Un módem DSL convierte una señal Ethernet del dispositivo del usuario en una señal DSL, que se transmite a la oficina central (ver Figura 78).

Los **módems de cable** proporcionan una conexión permanente en donde un suscriptor conecta una computadora o un enrutador LAN al módem de cable, que traduce las señales digitales en las frecuencias utilizadas para transmitir en una red de televisión por cable. La oficina local de televisión por cable, que se denomina cabecera de cable, contiene el sistema informático y las bases de datos necesarios para proporcionar acceso a Internet. Los suscriptores de módem de cable deben utilizar el ISP asociado con el proveedor de servicios.

La **tecnología inalámbrica para WAN** utiliza el espectro de radio sin licencia para enviar y recibir datos. El espectro sin licencia es accesible para cualquier persona que tenga un enrutador inalámbrico y tecnología inalámbrica en el dispositivo que esté utilizando. Algunos ejemplos son los siguientes:

- **Wi-Fi municipal:** que provee acceso a Internet de alta velocidad de forma gratuita o por un precio inferior al de otros de banda ancha.
- **WiMAX:** Liberada como el estándar IEEE 802.16. WiMAX provee un servicio de alta velocidad con acceso inalámbrico y proporciona una amplia cobertura como una red de telefonía celular. WiMAX funciona de manera similar a Wi-Fi, con velocidades superiores, en distancias mayores y para un mayor número de usuarios.
- **Internet satelital:** o VSAT, utilizado por usuarios rurales donde el cable y DSL no están disponibles. Un VSAT proporciona comunicaciones de datos bidireccionales de carga y descarga. El cable y DSL tienen velocí-

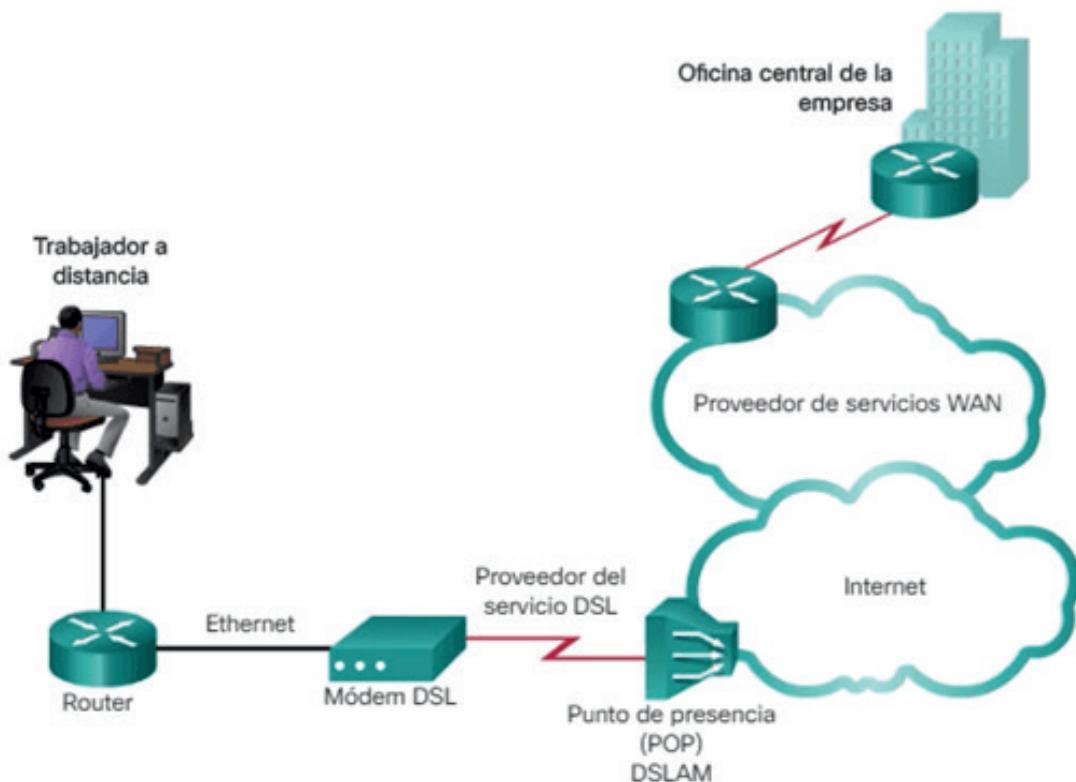
dades de descarga más altas, sin embargo, los sistemas de satélite son aproximadamente 10 veces más rápidos que un módem analógico. Para acceder a los servicios de Internet por satélite, los suscriptores necesitan una antena parabólica, dos módems con enlace ascendente y descendente y cables coaxiales entre la antena y el módem.

Telefonía Celular 3G / 4G /4G LTE, 5G, que es el servicio que utiliza a tecnología WAN inalámbrica para conectar usuarios y ubicaciones remotas. Muchos usuarios con teléfonos inteligentes y tabletas pueden usar datos móviles para enviar correos electrónicos, navegar por la Web, descargar aplicaciones y ver videos. Estos dispositivos utilizan ondas de radio para comunicarse a través de una torre de telefonía móvil cercana.

Tecnología VPN o red privada virtual (Virtual Private Network, VPN), que es una conexión encriptada entre redes privadas a través de una red pública, como Internet. Una VPN es un túnel seguro que protegen a los usuarios de la Intranet o Extranet de la interferencia y el espionaje en línea.

Figura 78

Ejemplo de Topología DSL-WAN



Nota. La figura muestra la conexión de una red pública DSL con sus respectivos dispositivos. Obtenido de: (Castillo, 2019).

13.3.1 Infraestructura de WAN privadas

Una infraestructura de WAN privada contiene recursos dedicados a un solo cliente. Los proveedores de servicios pueden ofrecer líneas arrendadas punto a punto dedicadas, enlaces de conmutación de circuitos, como PSTN o ISDN, y enlaces de conmutación de paquetes, como Ethernet WAN, ATM o Frame Relay. A continuación, se describen brevemente algunas de las tecnologías WAN privadas:

Líneas arrendadas: Cuando se requieren conexiones dedicadas permanentes, se utiliza un enlace punto a punto para proporcionar una ruta de comunicaciones WAN preestablecida desde las instalaciones del cliente hasta la red del proveedor. Las líneas arrendadas reciben diferentes nombres, como circuitos arrendados, enlace serie, línea serie, enlace punto a punto y líneas T1 / E1 o T3 / E3. En relación a la capacidad de transmisión, un enlace T1 permite 1.544 Mbps (en América del Norte), un E1 alcanza a 2.048 Mbps (Europa), un T3 43.7 Mbps y una conexión E3 admite 34.368 Mbps (Ver Figura 79).

Figura 79

Ilustración de una WAN privada que utiliza una línea arrendada



Nota. La figura muestra una topología WAN mediante línea arrendada. Obtenido de: (Castillo, 2019).

SDN o red digital de servicios integrados (Integrated Services Digital Network, ISDN) que es una tecnología de conmutación de circuitos que permite que el bucle local de una red telefónica pública conmutada (Public Switched

Telephone Network, PSTN) transmita señales digitales, con conexiones conmutadas de mayor velocidad.

Frame Relay: tecnología WAN de capa 2 del modelo ISO/OSI que crea circuitos virtuales permanentes (Permanent Virtual Circuit, PVC), que son identificador de conexión de enlace de datos (Data Link Connection Identifier, DLCI) identificados de forma única. Los PVC y DLCI garantizan la comunicación bidireccional de un dispositivo DTE a otro.

ATM o modo de transferencia asincrónica (Asynchronous Transfer Mode, ATM), para conmutación y transmisión que organiza la información en celdas capaz de transferir voz, video y datos a través de redes públicas y privadas.

WAN Ethernet que proporciona una red de conmutación de capa 2 que utiliza fibra óptica. Liberado como el estándar IEEE 1000BASE-LX que admite longitudes de 5 km. Además, el del estándar IEEE 1000BASE-ZX admite longitudes de hasta 70 km. Esta tecnología es capaz de transportar datos, voz, video y control en la WAN.

13.3.2 Estándares WAN

De acuerdo con (Payares, 2004), los estándares WAN son definidos y gestionados por un número de autoridades reconocidas incluyendo los siguientes organismos de normalización. Estos estándares WAN hacen referencia a los lineamientos técnicos tanto de la capa física como de la capa de enlace de datos del modelo OSI/ISO:

- International Telecommunication Union Telecommunication; Standardization Sector (ITU-T);
- International Organization for Standardization (ISO);
- Internet Engineering Task Force (IETF);
- Electronic Industries Association (EIA).

13.3.3 Capa física WAN

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de comunicación de datos (DCE). Tradicionalmente, el DCE es el proveedor de servicio, y el DTE es el dispositivo de conexión asociado. En este modelo, los servicios ofrecidos al DTE se hacen disponibles a través de un

módem o unidad de servicio del canal/unidad de servicios de datos ((Channel Service Unit/Data Service Unit, CSU/DSU) (Payares, 2004). El CSU/DSU es una interfaz de hardware que convierte las tramas de datos de una LAN en tramas apropiadas para una WAN y viceversa. Los estándares empleados en la capa física son:

- **EIA/TIA-232D:** norma definida como una interfaz estándar para conectar un DTE a un DCE
- **EIA/TIA-449:** norma para transmisión en serie que extienden las distancias y velocidades de transmisión más allá de la norma 232D
- **V.35:** que es una interfaz que sirve para conectar un DTE a un DCE síncrono de banda ancha.
- **X.21:** interfaz para redes de conmutación de circuitos que conecta un DTE al DCE de una WAN pública
- **G.703:** Recomendaciones del ITU-T, relativas a los aspectos generales de una interfaz
- **EIA/TIA-530:** que presenta el mismo conjunto de señales que la EIA-232D
- **HSSI:** High-Speed Serial Interface (HSSI), estándar de red para las conexiones seriales de alta velocidad (hasta 52 Mbps) sobre conexiones WAN

Recursos complementarios

- Video sobre “La Introducción a las Tecnologías WAN” 
- Video sobre “Los protocolos y estándares de redes WAN de manera más didáctica” 
- Video sobre “La capa física de las redes WAN” 

Actividad de aprendizaje 13

Descripción de la actividad

Una WAN es una red de datos que cubre un área geográfica amplia utilizando líneas de telecomunicaciones dedicadas tales como líneas telefónicas, líneas arrendadas o satelitales. Las redes WAN de manera general, se basan en compartir recursos de equipos ubicados en todo el globo terráqueo y tienen como objetivo principal el estar siempre disponibles para cualquier usuario. Un ejemplo tradicional es la Internet.

Una WAN consiste además en la interconexión de varias redes de área local o metropolitana ubicadas en diferentes ciudades, países y continentes la cual requiere del uso de sistemas de telecomunicaciones para conseguir este fin. Para este propósito se los administradores de red requieren conocer la configuración básica de routers.

El simulador Packet Tracer de la Academia de Networking de CISCO, permite configurar dispositivos de conectividad como switches y routers.

Esta actividad de aprendizaje tiene como propósito la configuración básica del router CISCO utilizando el simulador Packet Tracer.

Se pide:

Realizar la práctica de laboratorio 1.5.2 titulada “Práctica de laboratorio: Configuración básica del router”, disponible en la Web, desarrollado por la Academia de Networking de CISCO. Rellene todos los ejercicios que allí se señalan. Al finalizar, elabore un informe de la Práctica de Laboratorio que despliegue de los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de cada punto con sus resultados, Conclusiones generales y Referencias bibliográficas.

Autoevaluación Capítulo 13

1. ¿El modelo OSI es un modelo de red?

Descriptivo de sistemas cerrados, basado en siete capas

Descriptivo de sistemas abiertos, basado en siete capas o niveles de red

Descriptivo de sistemas abiertos, basado en seis niveles de red

2. ¿La capa responsable de ofrecer una transmisión correcta y libre de errores es?

Capa de transporte

Capa de sesión

Capa de red

3. ¿El análisis y funcionamiento capa por capa prioritariamente permite comprender?

Como se produce el desarrollo de redes

El desarrollo de software de red

Como los datos viajan desde los programas a través de un medio

4. ¿La capa encargada de enrutar los paquetes desde punto de inicio hasta el punto final, sin necesidad de una conexión directa es?

La capa de Transporte

La capa de Enlace

La capa de Red

5. Señale cuál de las capas es la responsable de mantener una comunicación estable o sincronizada entre aplicaciones de usuario de extremo a extremo

La capa de Sesión

La capa de Presentación

La capa de Aplicación

6. Señale cuál de las siguientes capas es la que provee una interfaz de usuario para que pueda interactuar con los servicios y aplicaciones.

La capa Física

La capa de Presentación

La capa de Aplicación

7. De las siguientes opciones, indique el medio de transmisión por el cual se realiza el envío de tramas de la capa de enlace

Dispositivos de entrada y salida de datos

Medios físicos o inalámbricos con conectores asociados

Enrutador de paquetes desde punto de inicio hasta punto final

8. Cuál de las siguientes opciones muestra los protocolos de comunicaciones del modelo OSI

Repeater, Hub, Modem

UTM, SIEM, NG-Firewall

HTTP, SMTP, SSH, FTP, TELNET

9. ¿El envío de tramas de la capa de enlace se la realiza a través de qué medios?

Físicos e inalámbricos

Virtuales

Ninguna de las anteriores

10. ¿La capa de enlace está subdividida en?

MAC

LLC

MAC Y LLC



<https://acortar.link/om0Hmy>

CAPÍTULO XIV

Enrutamiento Estático y Dinámico

14.1 El enrutador (router)

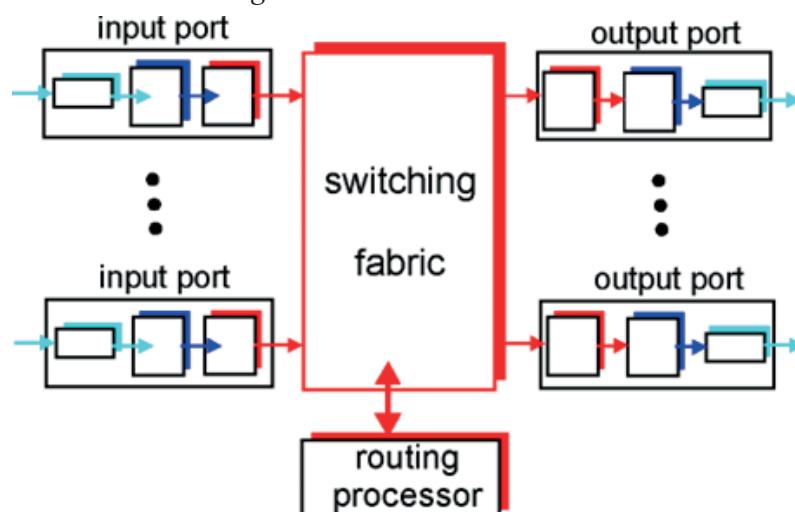
Un router es un dispositivo de networking que opera en la capa de red del modelo OSI. En realidad, se trata de un sistema computacional que tiene un funcionamiento específico el cual es interconectar segmentos de red o redes enteras en un área global. Se dice un sistema computacional pues dispone de una tarjeta madre, procesador, RAM, ventilador, fuente de alimentación, etc.

El router es el dispositivo responsable del enrutamiento que es el proceso de seleccionar la ruta óptima a través para conectarse a cualquier tipo de red de comunicaciones. En las redes de conmutación de paquetes, como Internet, por ejemplo, el enrutamiento selecciona las rutas para que los paquetes IP viajen desde su origen hasta su destino atravesando por los enrutadores que encuentra en su trayectoria.

A continuación, se describirá brevemente la estructura interna y externa de un enrutador. En la Figura 80 se muestra una abstracción de alto nivel de una arquitectura de enrutador genérico.

Figura 80

Arquitectura de un enrutador genérico



Nota. La figura representa los componentes internos y externos de un enrutador genérico. En la práctica se agrupan varios puertos con diferentes funcionalidades a la misma tarjeta. Obtenido de: (Web, 21)

Arquitectura interna del enrutador

- **Switching Fabric:** es la estructura de conmutación que conecta los puertos de entrada del enrutador a sus puertos de salida. Es una combinación

de hardware, software y firmware que controla el tráfico hacia y desde un nodo de red con el uso de varios conmutadores. Los datos entran por un puerto y lógicamente salen por otro.

- CPU: es el procesador necesario para ejecutar las instrucciones que recibe. Actúa para arrancar el sistema operativo, inicializar las configuraciones previas y proveer conexión a los diferentes dispositivos que estén conectados.
- RAM: componente en donde se almacena la información que está siendo procesada aleatoriamente, mientras esté encendido. Aquí reside volátilmente un archivo especial de configuración denominado running-config.
- FLASH: es una memoria no volátil que contiene una imagen del sistema operativo del enrutador (e.g. el IOS de Cisco) y todos los archivos de configuración del sistema (e.g. `rsp-jsv-mz.120-8.0.2.T`).
- NVRAM: es la memoria de acceso aleatorio no volátil (Non-Volatile Random Access Memory, NVRAM) capaz de almacenar información y no perderla al perder la alimentación eléctrica del componente. Aquí se almacena el archivo de configuración denominado startup-config.
- ROM: es la memoria de sólo lectura que almacena códigos de diagnóstico de forma permanente.
- Fuente de alimentación: que otorga la energía eléctrica para mantenerlo en funcionamiento, pues se trata de un dispositivo electrónico.

Arquitectura externa del enrutador

- **Conector de corriente:** que permite unir la fuente de alimentación con la corriente eléctrica.
- **Interruptor de alimentación:** es el botón de encendido y apagado. El enrutador siempre debe estar encendido.
- **Puertos seriales:** o interfaces seriales que sirven para interconectar los enrutadores entre sí y para conectarlo a la WAN. Las interfaces seriales necesitan señales de sincronización que controle las comunicaciones.
- **Puerto WAN:** o interfaz WAN es el puerto que obtiene los servicios del proveedor de servicios de Internet.
- **Conector LAN:** que son puertos RJ-45 que permiten conectar cable de par trenzado al conmutador o a equipos de usuario final para proveer los servicios LAN a través de cuatro puertos Fast Ethernet o Gigabit Ethernet.

- **Conector SC/APC:** Son puertos del enrutador a donde llega la conexión de fibra óptica de parte del proveedor de servicios de Internet.
- **LEDs:** diodos emisores de luz, que actúan como indicadores del estado y funcionamiento de cada interfaz.
- **Antena:** En los últimos años, la mayoría de la industria produce enruteadores inalámbricos que incluyen antenas Wi-Fi incorporadas.

Un enrutador puede direccionar o descubrir redes remotas de dos modos: (1) Manualmente, cuyas IP de redes remotas se introducen de forma manual en la tabla de enrutamiento al configurarlas como rutas estáticas. (2) Dinámicamente, en este caso, las rutas remotas se descubren de forma automática mediante un protocolo de enrutamiento dinámico y diferentes métricas. En los siguientes apartados se explicarán estas dos opciones:

14.2 Enrutamiento estático

El enrutamiento estático es el proceso de una configuración manual de las direcciones IP a las interfaces del router y la selección de una ruta de red, generalmente gestionadas por el administrador de la red. Se implementa en escenarios donde se espera que los parámetros de red y el entorno permanezcan constantes. Entre los parámetros de configuración de enrutamiento estático, es primario conocer la dirección IP y máscara de red de los nodos.

El enrutamiento estático es óptimo (i.e., **ventajas**) puesto que no se anuncian a través de la red, lo cual acrecienta la seguridad. Además, consumen menos ancho de banda en comparación de los protocolos de enrutamiento dinámico.

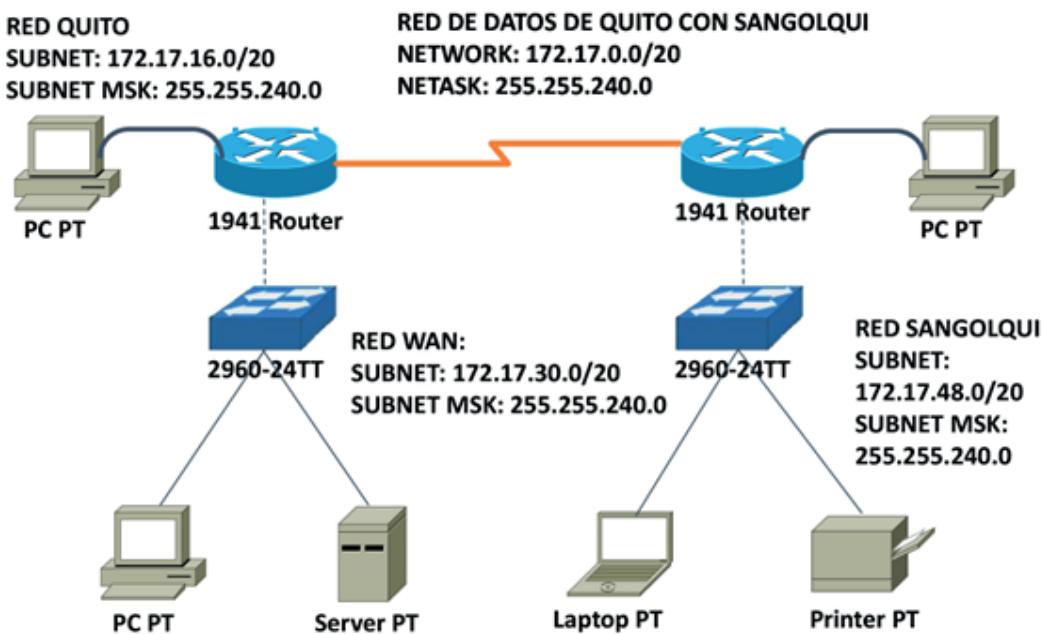
El enrutamiento estático no es óptimo (i.e., **desventajas**) en algunas situaciones por ejemplo cuando las rutas configuradas no están disponibles, los cuales podría causar degradación, latencia y congestión de la red. Además, la configuración es propensa a errores, especialmente en redes extensas.

Existen cuatro tipos de rutas estáticas: La primera es la **estándar**, la cual indica al router el cómo alcanzar a una red. El segundo tipo es la ruta **predeterminada** cuya función es identificar la dirección IP del Gateway al cual el router envía todos los paquetes. El tercer tipo es la **ruta resumida**, es decir las redes de destino son contiguas y se pueden resumir en una dirección unifica de red, dando como resultado una sola ruta en la tabla de enrutamiento. Como último tipo está la ruta **flotante**, que es aquella que sirve como respaldo para otra ruta

estática o dinámica principal en el caso de existir una falla (GeeksforGeeks, 2019). La Figura 81 es un ejemplo de configuración de enruteamiento estático.

Figura 81

Configuración de enruteamiento estático



Nota. La figura muestra la configuración de enruteamiento estático mediante Packet Tracer a través del simulador Packet Tracer de dos ciudades: Quito y Sangolquí

14.3 Enrutamiento dinámico

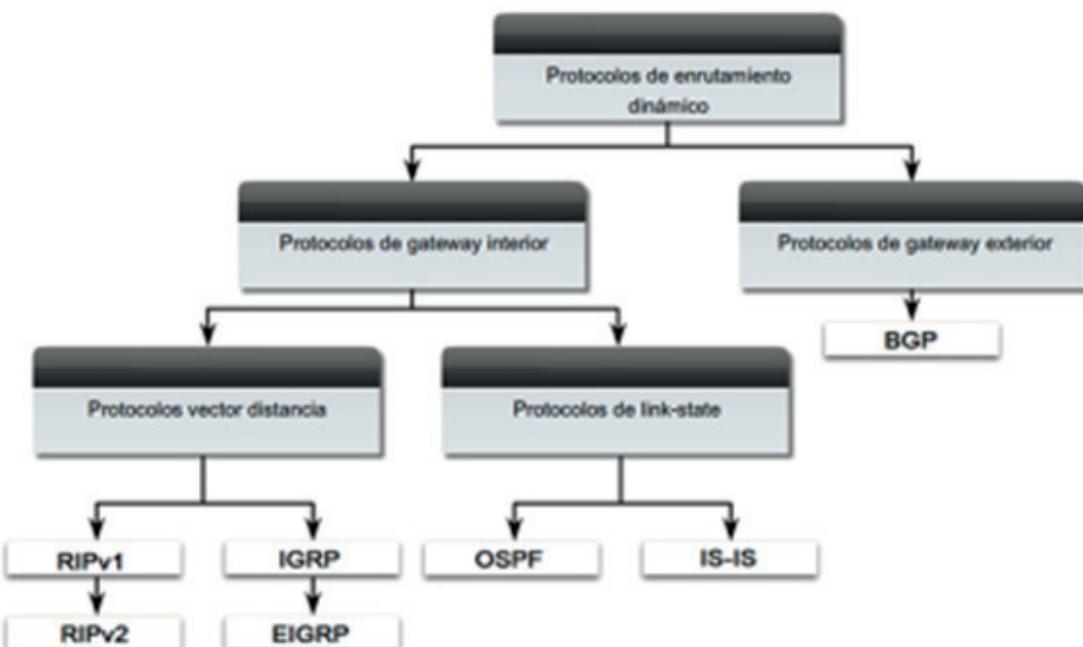
El enruteamiento dinámico permite a los enruteadores seleccionar rutas de acuerdo con las actualizaciones en el diseño de la red en tiempo real. En el enruteamiento dinámico, el protocolo de enruteamiento configurado en el enruteador es responsable de la creación, mantenimiento y actualización de la tabla de enruteamiento. Los protocolos de enruteamiento dinámico realizan algunas actividades tales como la detección de redes y el mantenimiento de las tablas de enruteamiento.

El enruteamiento dinámico permite reconocer automáticamente las mejores rutas entre diferentes enruteadores sobre la base de diferentes métricas. Las métricas son las variables de red que se utilizan para decidir dinámicamente qué ruta se prefiere. Entre las más conocidas se distinguen: número de saltos,

ancho de banda, retardo, confiabilidad, carga y costo. En la Figura 82 se ilustra un mapa jerárquico donde se puede observar los tipos y subtipos de enruteamiento dinámico.

Figura 82

Estructura jerárquica de los protocolos de enrutamiento dinámico



Nota. La figura muestra la clasificación de los protocolos de enrutamiento Dinámico. Obtenido de: (Cisco Networking Academy, 2020).

A continuación, en los siguientes apartados se presentan dos de los protocolos más utilizados en el enruteamiento dinámico, los cuales son: el protocolo de información de enruteamiento (Routing Information Protocol, RIP) y el protocolo abierto de ruta más corta primero (Open Shortest Path First, OSPF).

14.4 Protocolo de información de enruteamiento (RIP)

Routing Information Protocol (RIP) es un protocolo de enruteamiento dinámico que utiliza el número de saltos como métrica de enruteamiento para descubrir la mejor ruta entre la red de origen y la de destino. Es un protocolo de enruteamiento por vector de distancia que tiene un valor de distancia administrativa (Administrative Distance, AD) = 120 y funciona en la capa de aplicación del modelo OSI. RIP utiliza el puerto lógico 520 (Netink, 2020).

El número de saltos representa el número de enrutadores que se encuentran entre la red de origen y la de destino. La ruta con el menor número de saltos se reconoce como la mejor ruta para llegar a una red destino. El número máximo de saltos permitido para RIP Versión 1 es 15, por tanto, cuando llega a 16 saltos se considera red inalcanzable. El número máximo de saltos permitido para RIP versión 2 es 30 (GeeksforGeeks, 2019). La Tabla 9 describe una comparación entre las dos versiones de RIP.

Tabla 9

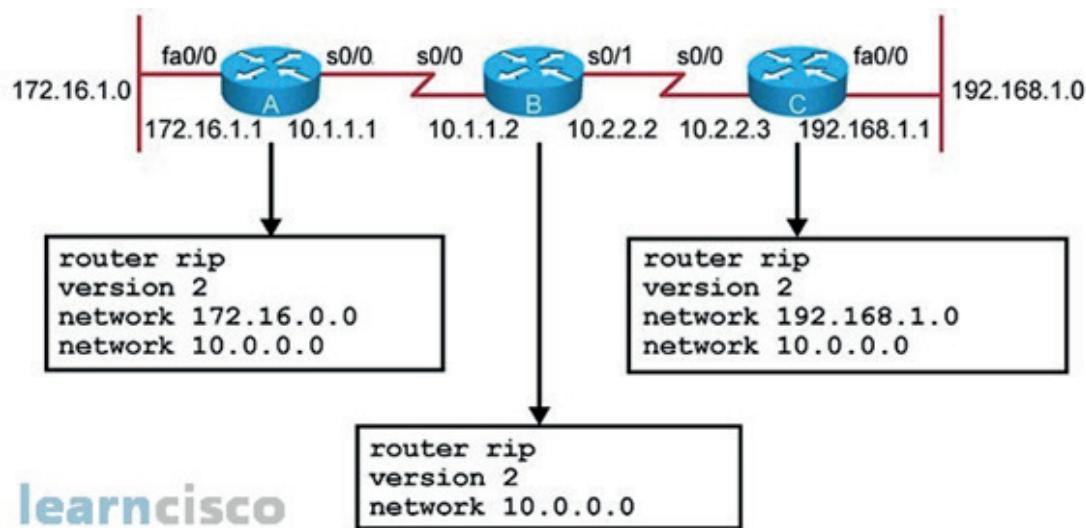
Tabla comparativa entre RIP versión 1 y RIP versión 2

RIP versión 1	RIP versión 2
Protocolo de enrutamiento Classful	Protocolo de enrutamiento Classless
Utiliza broadcast para enviar actualizaciones periódicas	Utiliza Multicast para enviar actualizaciones periódicas
No soporta autenticación	Soporta autenticación
No soporta VLSM/CIDR	Soporta VLSM/CIDR

Entre las ventajas de RIP se pueden señalar que es más fácil de configurar comparado con otros protocolos. Su algoritmo de encaminamiento para el cálculo de la mejor ruta requiere de menores recursos computacionales. Es libre y por lo tanto también es soportado por la mayoría de los fabricantes.

Entre sus desventajas conviene destacar que: determina la mejor métrica únicamente considerando el número de saltos, descartando otros factores como ancho de banda, tráfico, carga, retardo, confiabilidad, etc. Además, el límite máximo de saltos es menor que el de otros protocolos, por lo que solo se puede utilizar en redes medianas o pequeñas. El RFC 1720 describe algunas limitaciones técnicas de RIP.

Finalmente, y de acuerdo con (GeeksforGeeks, 2019), entre las principales características de RIP se pueden citar: (1) Las actualizaciones de la red se intercambian periódicamente; (2) Las actualizaciones de las tablas de enrutamiento siempre se transmiten; (3) Las tablas de enrutamiento completas se envían en actualizaciones; (4) Los enrutadores siempre confían en la información de enrutamiento recibida de los enrutadores vecinos. La Figura 83 muestra una topología con RIP 2 y los comandos de configuración en enrutadores Cisco.

Figura 83*Comandos CISCO de configuración RIP versión 2*

Nota. La figura ilustra los comandos necesarios para configurar RIP versión 2 en cada enrutador de la topología de ejemplo. Obtenido de: (LearnCisco, 21)

14.5 Protocolo Abierto de ruta más corta primero (OSPF)

Open Shortest Path First es un protocolo de puerta de enlace interior (Interior Gateway Protocol, IGP) que se utiliza para distribuir información de enrutamiento dentro de un único sistema autónomo (Autonomous System, AS). Está basado en tecnología de estado de enlace, que ha incorporado nuevos conceptos como la autenticación de actualizaciones de enrutamiento, máscaras de subred de longitud variable (VLSM), resumen de rutas, sistemas y áreas autónomas. OSPF está documentado en el RFC 2328. La Figura 84 muestra un escenario típico de OSPF y los tipos de routers que se necesitan.

Entre las principales características de OSPF se pueden citar: No hay limitación en el número de saltos. El uso de VLSM es muy útil en la asignación de direcciones IP. Utiliza multidifusión IP para enviar actualizaciones de estado de enlace. Asegura un mejor uso del ancho de banda. Permite una definición lógica de red cuando los enrutadores se pueden dividir en áreas. Permite la autenticación de enrutamiento mediante el uso de diferentes métodos de autenticación de contraseña. Permite la transferencia y etiquetado de rutas externas inyectadas en un sistema autónomo (MetaSwitch, 21).

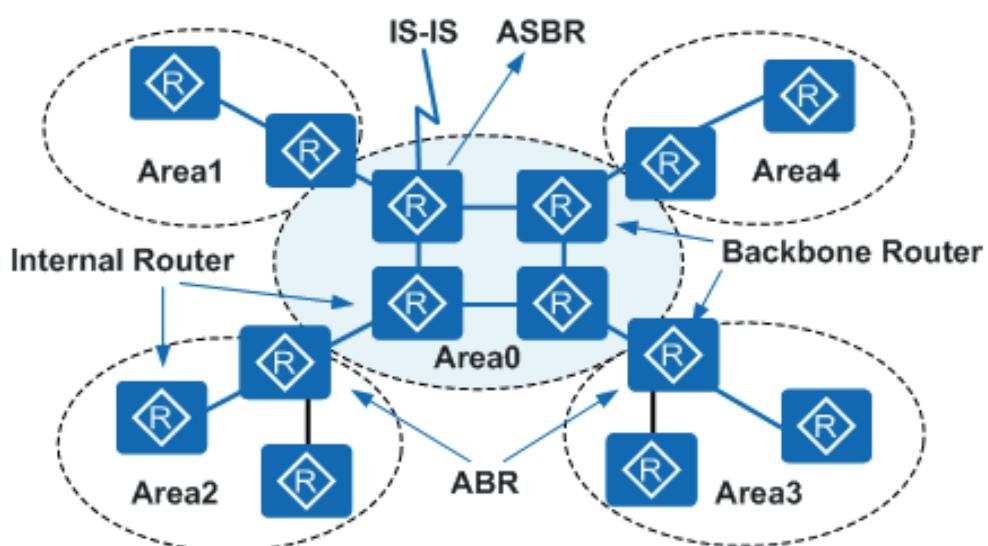
La principal ventaja OSPF es que el conocimiento total de la topología permite a los enrutadores calcular rutas que cumplen criterios particulares. Esto

puede ser útil para fines de ingeniería de tráfico, donde las rutas se pueden delimitar para cumplir con requisitos particulares de calidad de servicio (MetaSwitch, 21).

La principal desventaja de OSPF es que no escala bien a medida que se añaden más enrutadores al dominio de enrutamiento. Aumentar el número de enrutadores aumenta el tamaño y la frecuencia de las actualizaciones de topología, y también el tiempo que lleva calcular las rutas de un extremo a otro. Esta falta de escalabilidad significa que un protocolo de enrutamiento de estado de enlace no es adecuado para el enrutamiento a través de Internet en general, razón por la cual los IGP solo enrutan el tráfico dentro de un único sistema autónomo (MetaSwitch, 21).

Figura 84

Tipos de routers OSPF



Nota. Los routers OSPF se categorizan de acuerdo la función que desempeñan en el dominio de routing. Obtenido de: (Huawei, 2021).

Recursos complementarios

- Video sobre un ejemplo de enrutamiento dinámico por RIP.
- Video sobre un ejemplo de enrutamiento dinámico por OSPF



Actividad de aprendizaje 14

Descripción de la actividad

Un router es un dispositivo de networking que opera en la capa de red del modelo OSI. En realidad, se trata de un sistema computacional que tiene un funcionamiento específico el cual es interconectar segmentos de red o redes enteras en un área global. Se dice un sistema computacional pues dispone de una tarjeta madre, procesador, RAM, ventilador, fuente de alimentación, etc. El router es el dispositivo responsable del enrutamiento que es el proceso de seleccionar la ruta óptima a través para conectarse a cualquier tipo de red de comunicaciones. En las redes de conmutación de paquetes, como Internet, por ejemplo, el enrutamiento selecciona las rutas para que los paquetes IP viajen desde su origen hasta su destino atravesando por los enrutadores que encuentra en su trayectoria.

El simulador Packet Tracer de la Academia de Networking de CISCO, permite configurar dispositivos de conectividad como switches y routers.

Esta actividad de aprendizaje tiene como propósito la configuración de enruteamiento estático y dinámico utilizando el simulador Packet Tracer.

Se pide:

Realizar las siguientes prácticas de laboratorio: 2.8.1: “Configuración básica de la ruta estática”, y 7.2.2 “Configuración de RIP”, ambas disponibles en la Web, desarrollado por la Academia de Networking de CISCO. Rellene todos los ejercicios que allí se señalan en cada una de ellas.

Al finalizar, elabore un solo informe de la Práctica de Laboratorio que despliegue de los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de cada punto con sus resultados, Conclusiones generales y Referencias bibliográficas.

Autoevaluación Capítulo 14

1. ¿En qué consiste la transmisión del protocolo TCP?

Punto de partida - Transmisión completa en orden de bytes - Punto de fin

Punto de inicio - Transmisión de datos - Punto de llegada

Punto inicial - Punto medio - Punto final

2. Las siglas ARP significan:

Address Reconnection Protocol

Address Resolution Protocol

Address Router Protocol

3. ¿Cuál es la función del protocolo UDP?

Proporciona un servicio de entrega de datagramas

Verifica las conexiones entre los hosts transmisores y receptores

Acepta y envía paquetes de red

4. ¿Cuáles son protocolos de la capa física o de acceso a la red del modelo TCP/IP?

NAT - IP - Ethernet

RARP - UDP - ARP

Ethernet - CSMA/CD

5. ¿Cuál es la función de la capa de aplicación?

Brindar acceso a las aplicaciones más frecuentes que se hayan utilizado en el dispositivo

Dar servicios de red que proporcionan la interfaz con el sistema operativo para que el usuario pueda interactuar acorde con la máquina

Proporcionar acceso a las aplicaciones más recientes que se hayan ejecutado en segundo plano

6. En la capa de transporte ¿Qué implementa el UDP (User Datagram Protocol)?

Implementa una transmisión no fiable, es decir, que no está libre de errores

Implementa un datagrama de usuarios para facilitar el acceso a la información

Implementa métodos de seguridad para los datos de los usuarios

7. ¿Qué servicio de nombres proporciona nombres de host al servicio de direcciones IP?

UNIX

Archivos/etc

NIS

DNS

8. ¿De qué se encarga el protocolo de resolución de direcciones (ARP) de la capa de acceso a la red?

Este protocolo se encarga de administrar las direcciones de datos que reciba el dispositivo

Este protocolo puede direccionar los datos enviados desde el dispositivo

Este protocolo es responsable de la asociación exacta de direcciones IP con direcciones Ethernet físicas.

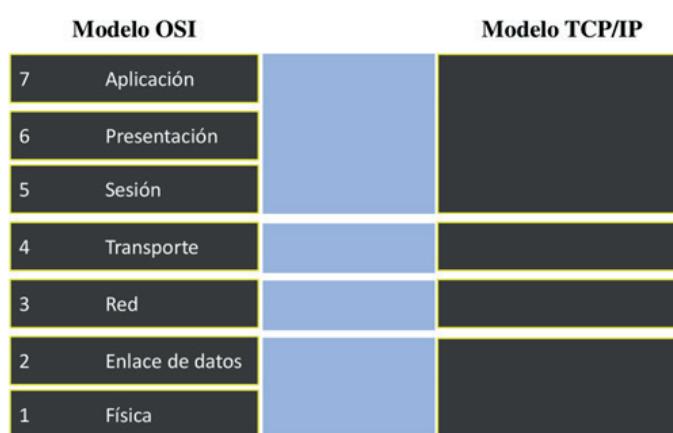
9. ¿Cuál es la definición del protocolo de administración de red?

El Protocolo completo de administración de red (SNMP) permite ver la distribución de la red y el estado de los equipos clave

El Protocolo simple de administración de red (SNMP) permite ver la distribución de la red y el estado de los equipos clave

El Protocolo simple de administración de red (SNMP) permite ver la distribución de la LAN y el estado de los equipos clave

10. Según la figura complete en forma descendente con las capas homólogas del modelo TCP/IP



Aplicación- Transporte - Internet - Acceso a Internet

Transporte -Aplicación- Internet - Acceso a Internet

Aplicación- Transporte - Acceso a Internet - Internet



<https://acortar.link/I2SP02>

CAPÍTULO XV

Capa de Transporte

15.1 Introducción

De acuerdo con (Alani, 2014), la capa de transporte es la responsable de las comunicaciones sean locales o remotas entre un host origen y destino (extremo a extremo), lo que permite que se mantenga una comunicación temporal de extremo a extremo, y por tanto, la transmisión de datos con un nivel deseado de confiabilidad.

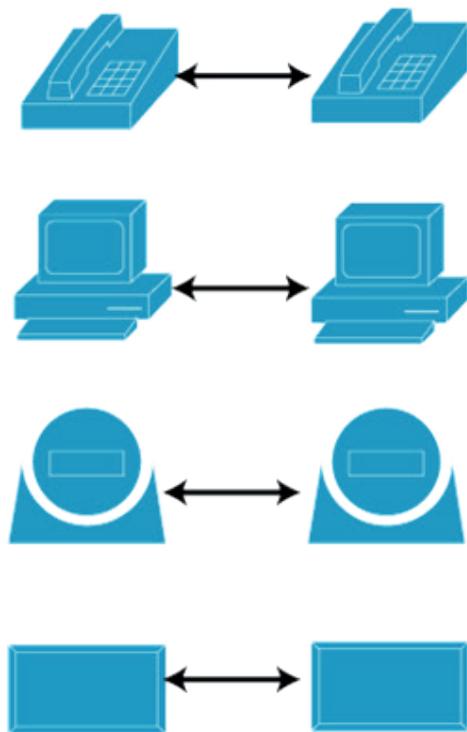
El propósito de la capa de transporte es la de mantener una red de datos en las que se transmiten y reciben flujos de datos constantemente. Estas comunicaciones deben ser lo más seguras posibles entre los dispositivos de red conectados, ya sea de manera local o remota. Es decir, la capa de transporte TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores. Para que esto se logre, intervienen varios componentes y protocolos o reglas que actúan según se encuentren organizados, distribuidos y conectados los dispositivos en una red.

La capa de transporte funciona en la capa 4 del modelo ISO/OSI o en la capa 3 del modelo de capas TCP/IP. La capa de transporte proporciona una transferencia transparente de datos entre usuarios finales, suministrando servicios de transferencia de datos confiables a las capas superiores. Además, controla la confiabilidad de un enlace dado a través del control de flujo, segmentación, de-segmentación y control de errores. La capa de transporte también proporciona el acuse de recibo de la transmisión de datos correcta y envía los datos siguientes si no se produjeron errores.

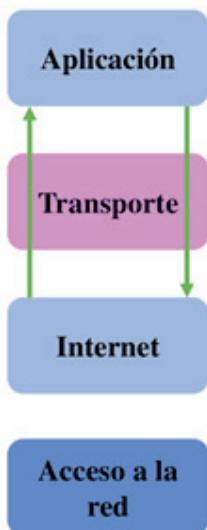
En el modelo TCP/IP, hay dos protocolos definidos que operan en esta capa: el protocolo de control de transmisión (Transmission Control Protocol, TCP) y el protocolo de datagramas de usuario (User Datagram Protocol, UDP). Estos dos protocolos proporcionan comunicaciones orientadas a la conexión y sin conexión respectivamente (Alano, 2014). La capa de transporte recibe los datos que vienen de la capa de aplicación. En esta capa se le añade los puertos lógicos de origen y destino (Felipe, 2013). Esta capa además provee servicios a la capa de red (capa 3 del modelo OSI o 2 de TCP/IP) en la cual se añaden la dirección IP origen y destino. En la Figura 85 se ilustra una abstracción de la capa de transporte. Algunas funciones se explican a continuación:

Figura 85

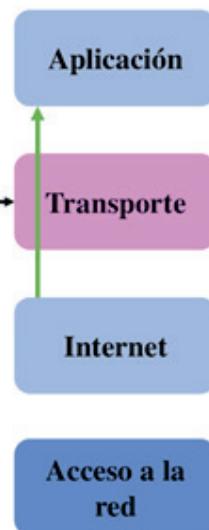
Modelo TCP/IP, Capa de transporte y comunicaciones entre dispositivos



Modelo TCP/IP



Modelo TCP/IP



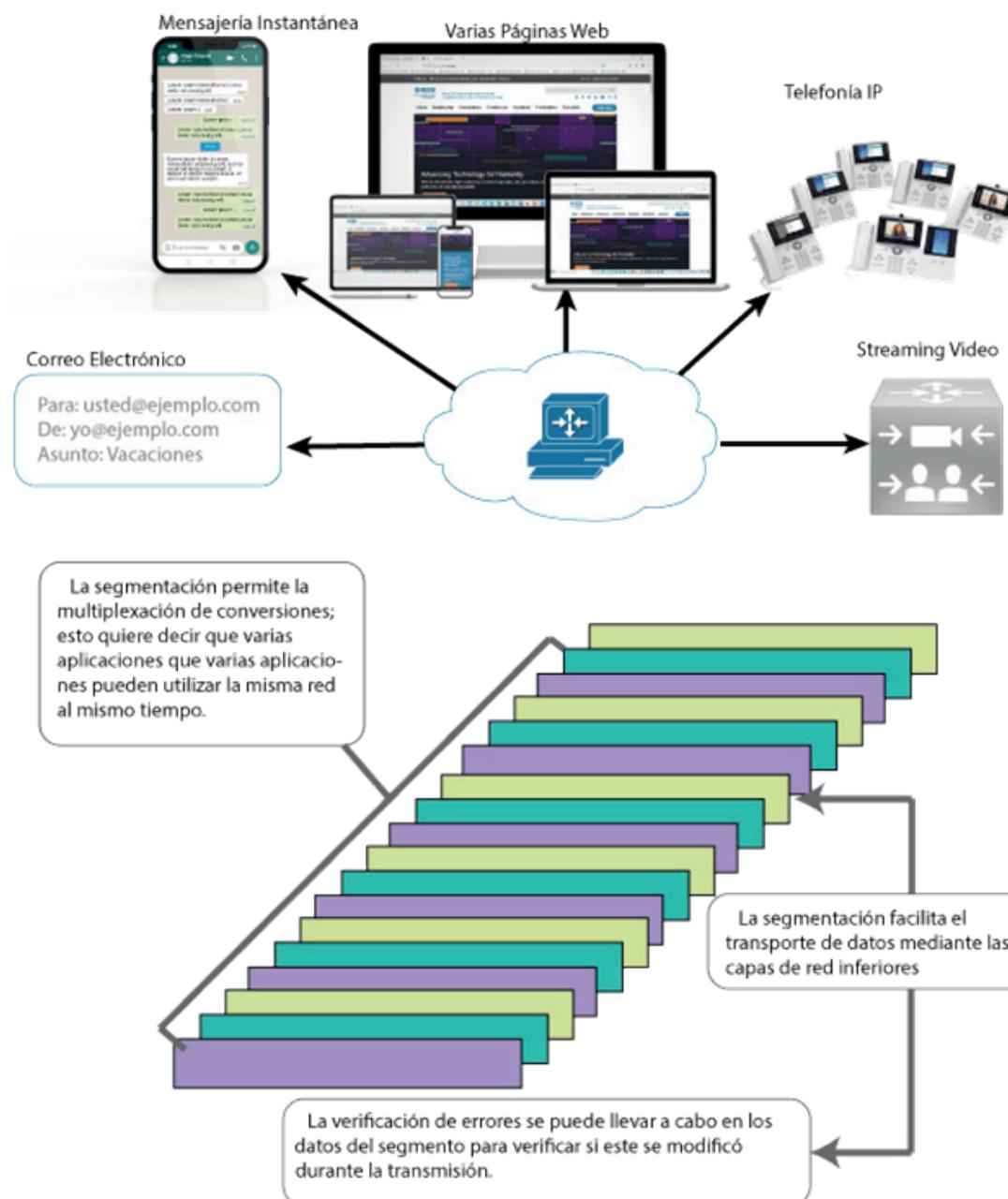
Nota. La figura representa una abstracción de la capa de transporte. Adaptado de: (Cisco, Capítulo 3, 2008).

15.2 Funciones de la capa de Transporte

De acuerdo con Mónica Jha en (Jha, 2019) a más de las características señaladas en el apartado anterior, la capa de transporte tiene varias funciones específicas. La Figura 86 ilustra algunas de ellas:

Figura 86

Algunos de los servicios de la capa de transporte



Nota. La figura muestra algunos de los servicios de la capa de transporte. Obtenido de: Cisco-NetAcad, “Capítulo 7: Capa de Transporte”, (Cisco, Capítulo 3, 2008)

- Direccionamiento de puntos de servicio: Las computadoras pueden ejecutar programas simultáneamente. Debido a ello, la entrega de origen a destino significa la entrega de un trabajo específico en una computadora a un trabajo específico en otra. Por esta razón, la capa de transporte agregó un tipo específico de dirección a su encabezado, que se denomina dirección de punto de servicio o dirección de puerto.
- Segmentación y reensamblaje: Significa que un mensaje se divide en segmentos transmisibles en el cual cada segmento contiene un número de secuencia. Este número permite que esta capa vuelva a ensamblar el mensaje. Al llegar a su sistema de destino, el mensaje se vuelve a ensamblar correctamente, identifica y reemplaza los paquetes que se perdieron en la transmisión.
- Control de conexión: Puede ser de dos tipos: (1) Capa de transporte sin conexión, en el cual el receptor no envía un acuse de recibo al remitente sobre la recepción de un paquete. Esta es una técnica de comunicación más rápida; (2) Capa de transporte orientada a la conexión, que crea una conexión con la máquina de destino antes de transmitir los paquetes. Para crear una conexión, se pueden seguir tres pasos: establecimiento de conexión, transferencia de datos y terminación de la conexión
- Multiplexación y demultiplexación: (1) Multiplexación, que consiste en recopilar datos de múltiples procesos de aplicación del remitente, envolver esos datos con un encabezado y enviarlos como un todo al receptor previsto. Estos paquetes se diferencian por sus números de puerto y los pasan a la capa de red después de agregar los encabezados adecuados; (2) Demultiplexación que es la entrega de segmentos recibidos en el lado del receptor a los procesos de capa de aplicación correctos (Yáñez & Janine, 2002).
- Control de flujo: La capa de transporte es la responsable del mecanismo de control de flujo entre las capas adyacentes del modelo TCP/IP.
- Control de errores: La corrección de errores se logra mediante la retransmisión del paquete.
- Seguimiento de conversaciones individuales: Cada conjunto de datos que circula entre una aplicación de origen y otra de destino se le conoce como una conversación y se rastrea por separado. La capa de transporte tiene la responsabilidad de mantener y rastrear estas conversaciones múltiples. Naturalmente, un host puede tener múltiples aplicaciones que se comunican a través de la red al mismo tiempo. (CCNA, 2008).

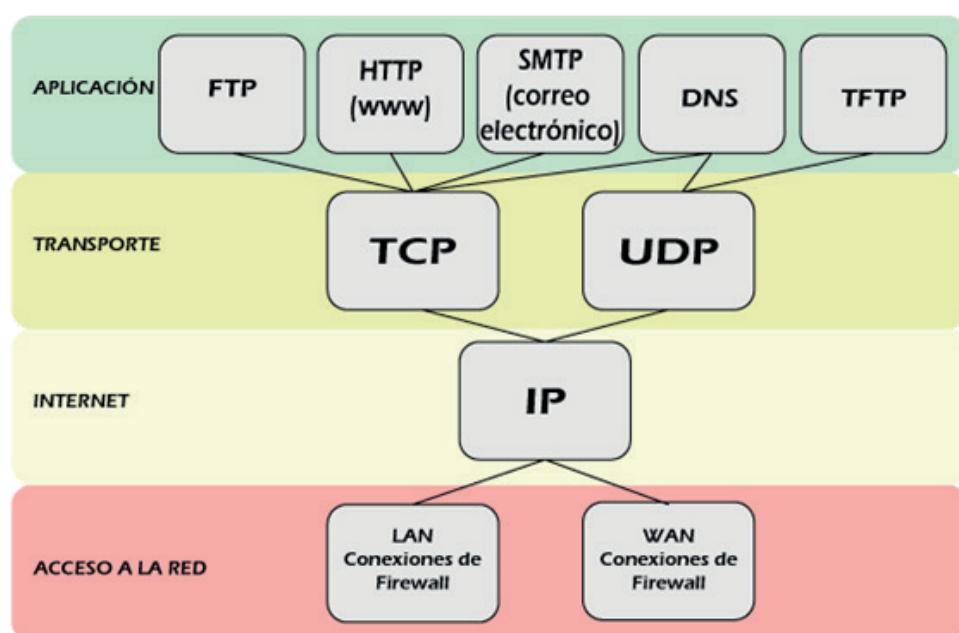
- Agregar información de encabezado: El encabezado está formado por datos binarios que están organizados en varios campos y en cada bloque de datos. Estos valores escritos en cada uno de los campos permiten que varios protocolos de la capa de transporte realicen diferentes acciones en la gestión de la comunicación de datos. (CCNA, 2008).

15.3 Protocolos de la Capa de Transporte

Tal como se explicó en los apartados anteriores, la capa de transporte TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al confirmar la recepción de los datos y retransmitir los paquetes perdidos. A este tipo de comunicación se le conoce como transmisión punto a punto. Los protocolos que están presentes en la capa de transporte son el TCP y el UDP. El protocolo TCP proporciona un servicio de transmisión de datos completo y confiable. Por el contrario, UDP proporciona un servicio de entrega de los datagramas no tan confiable. Las diferentes aplicaciones tienen distintos requisitos de confiabilidad de transporte. La Figura 87 ilustra los protocolos utilizados por las otras capas de modelo TCP/IP, y cómo se relacionan (Smith, 2001).

Figura 87

Modelo TCP/IP, protocolos



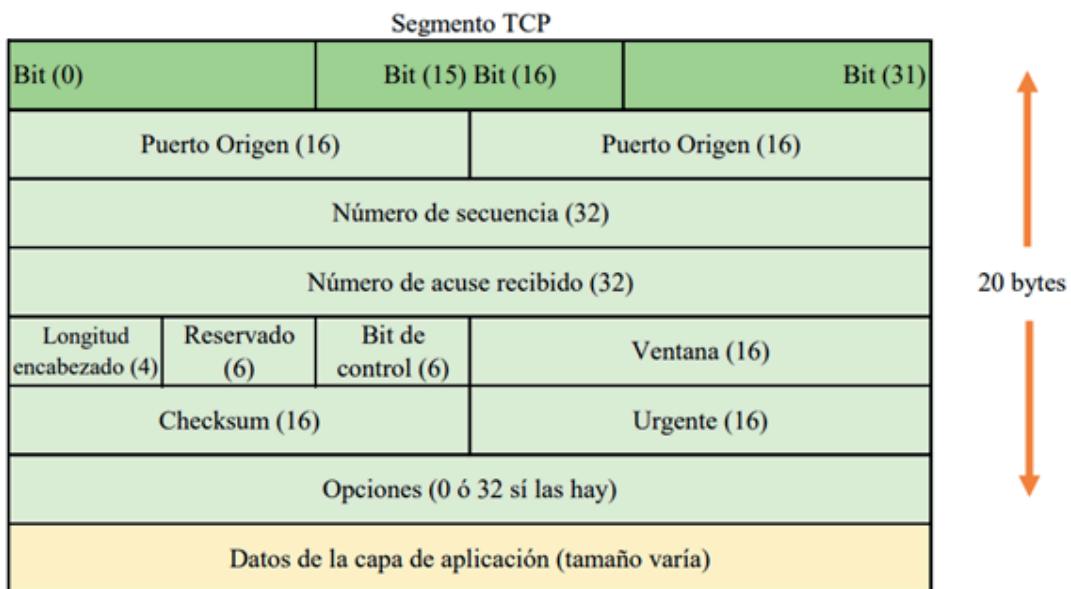
Nota. La figura muestra los protocolos del Modelo TCP/IP. Adaptado de: (Cisco, Capítulo 3, 2008).

15.4 Protocolo TCP

TCP es un protocolo de la capa de transporte confiable que garantiza que todos los datos lleguen al destino, incluyendo campos que aseguran la entrega de los datos de la capa de aplicación. TCP divide los datos en segmentos. La segmentación de paquetes es el proceso de dividir un paquete de datos en unidades más pequeñas para su transmisión a través de la red. Estos campos requieren un procesamiento adicional por parte de los hosts que trasmiten y reciben, por lo cual el procesamiento de los segmentos se demora un poco más. (CCNA, 2008). Una vez que los datos están segmentados, se encapsulan dentro de TCP. El segmento TCP y el encabezado TCP luego se pasan al Protocolo de Internet (IP), que rellena el segmento TCP y el encabezado en la carga útil del paquete IP.

En la Figura 88 se ilustra un segmento TCP y sus atributos, el cual está compuesto por los datos enviados desde la capa de aplicación y la cabecera añadida por el protocolo de transporte (CCNA, 2008). El número de secuencia es el número de bytes del primer byte de datos en el segmento TCP enviado. El número de acuse de recibo es el número de secuencia del siguiente byte que el receptor espera recibir. Algunas de las características que tiene este protocolo se describen con una breve explicación.

Figura 88
Segmento TCP



Nota. La figura muestra cómo está conformado un segmento TCP de la capa de transporte. Adaptado de (Cisco, Capítulo 3, 2008)

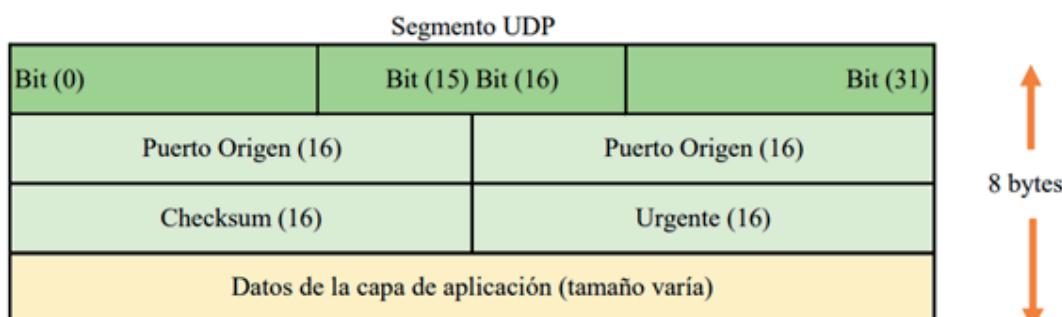
- El RFC de TCP es el 793.
- TCP crea una sesión entre el origen y destino por lo cual se conoce como un protocolo orientado a la conexión.
- TCP realiza una entrega confiable ya que retransmite los datos perdidos o dañados.
- TCP reconstruye los datos de forma ordenada, utilizando numeración y secuenciación de segmentos.
- TCP tiene control del flujo, puesto que regula la cantidad de datos que se transmiten.
- TCP es un protocolo con estado ya que siempre está al pendiente de los datos por lo cual realiza un seguimiento de la sesión.

15.5 Protocolo UDP

UDP es un protocolo de capa de transporte más simple que TCP ya que no provee confiabilidad, además de que no dispone de control del flujo, lo que significa que requiere menos campos en el encabezado. UDP divide los datos en datagramas que también se conocen como segmentos. Los datagramas UDP pueden procesarse más rápido que los segmentos TCP ya que no tiene que gestionar la confiabilidad, ni tampoco el control del flujo (CCNA, 2008).

En la Figura 89 se ilustra un datagrama UDP, en el cual se puede observar que tiene menos atributos que el segmento TCP. Lo que sí tienen en común son los puertos lógicos origen y destino (CCNA, 2008). Algunas de las características que tiene este protocolo se los describe con una leve explicación.

Figura 89
Segmento UDP

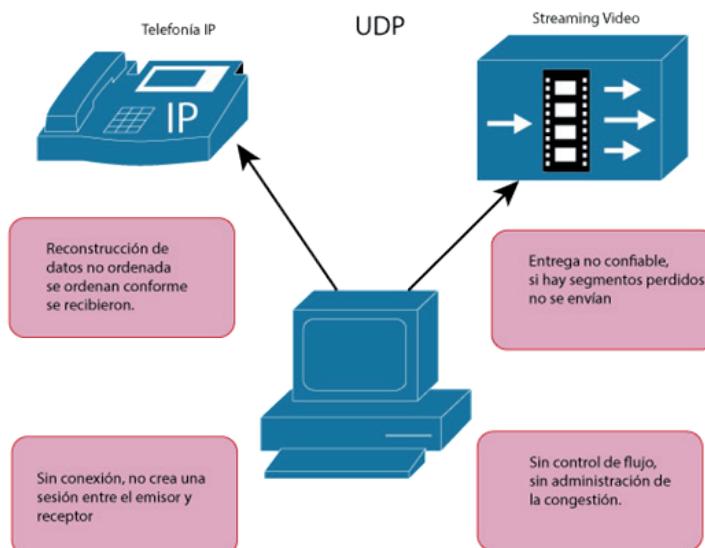


Nota. La figura muestra cómo está conformado un segmento UDP de la capa de transporte. Adaptado de: (Cisco, Capítulo 3, 2008).

- El RFC de UDP es el 768.
- UDP es un protocolo sin conexión.
- La entrega de los datos es poco confiable.
- Reconstruye los datos de forma aleatoria.
- Como no rastrea la información enviada o recibida entre el cliente y el servidor, se conoce como un protocolo sin estado.
- UDP se utiliza cuando el reconocimiento de datos no tiene importancia.
- UDP es un protocolo que permite que los datos fluyan en una dirección.
- UDP es simple y adecuado para comunicaciones basadas en consultas.
- UDP no proporciona un mecanismo de control de congestión.

UDP se utiliza para una comunicación simple de solicitud-respuesta cuando el tamaño de los datos es menor y, por lo tanto, existe una menor preocupación por el control del flujo y los errores. Es muy adecuado para la multidifusión, ya que UDP admite la commutación de paquetes. Se utiliza para aplicaciones en tiempo real que no pueden tolerar retrasos entre secciones de un mensaje recibido. UDP se utiliza para algunos protocolos de actualización de enruttamiento como RIP. Algunas aplicaciones que utilizan UDP son las Sistema de nombres de dominio (Domain Name Service, DNS), streaming video, Voz sobre IP (VOIP), Protocolo de tiempo de red (Network Time Protocol, NTP), TFTP, RTSP, etc. En la Figura 90, se ilustran algunas aplicaciones de UDP.

Figura 90
UDP - Aplicaciones



Nota. La figura ilustra las características de UDP, además de las aplicaciones que hacen uso de esta. Adaptado de: (Cisco, Capítulo 3, 2008).

15.6 Manejo de los números de Puertos lógicos

Cuando se envía un mensaje utilizando TCP o UDP, los protocolos y servicios solicitados se identifican con un número de puerto lógico para diferenciarse entre aplicaciones. Un puerto es un identificador numérico que tiene cada segmento y se utiliza para realizar un seguimiento a transmisiones específicas y de servicios de destino solicitados. Cada mensaje que envía un host contiene un puerto de origen y uno de destino (Velasco, 2016).

El número de puerto de la aplicación o servicio que realiza la solicitud se utiliza como número de puerto de destino en la respuesta que vuelve del servidor. La Agencia de asignación de números por Internet (Internet Assigned Numbers Authority, IANA) asigna números de puerto (Cisco, Capítulo 3, 2008). La IANA es una unidad operativa de la Corporación de Números y Nombres Asignados de Internet (Internet Corporation for Assigned Names and Numbers, ICANN) que mantiene las bases de datos de números de protocolo, direcciones IP y dominios de nivel superior. En la Figura 91, se muestra de manera abstracta el proceso de direccionamiento del puerto.

Figura 91

Direccionamiento del puerto



Nota. La figura ilustra de manera abstracta el direccionamiento del puerto. Obtenido de: Cisco-NetAcad, “Capítulo 7: Capa de Transporte”, (Cisco, Capítulo 3, 2008).

IANA es un organismo normativo responsable de asegurar diferentes estándares de direccionamiento, incluidos los números de puerto de 16 bits. Los 16 bits son utilizados para identificar los números de puerto de origen y destino, estos proporcionan un rango de puertos de 0 a 65535 (CCNA, 2008). La IANA ha dividido el rango de números en los siguientes tres grupos de puertos lógicos. La Tabla 10, enumera la división de puertos.

Tabla 10

División de puertos (IANA)

Rango de Números de puerto	Grupos de puertos
Entre 0 y 1023	Puertos conocidos
Entre 1024 y 49151	Puertos registrados
Entre 49152 y 65535	Puertos privados y/o dinámicos.

Nota. La tabla ilustra la división de puertos (IANA). Adaptado de: (Cisco, Capítulo 3, 2008).

- Puertos conocidos (números del 0 al 1023): rango determinado para aplicaciones como HTTP (80), HTTPS (puerto 143), FTP (puertos 20 y 21), SNMP (25), SSH (22), y se requiere de privilegios de administrador para activar una aplicación en uno de estos puertos o servicios, e.g., puerto 80 (HTTP) (Toad, 2005).
- Puertos registrados (números del 1024 al 49151): estos números de puerto se asignan a procesos o aplicaciones específicas que el usuario elige instalar, e.g., el puerto 3306 (MySQL). (Toad, 2005).
- Puertos dinámicos o privados (números 49152 a 65535): también conocidos como puertos efímeros, que se asignan de forma dinámica a las aplicaciones cliente cuando se inicia una conexión a un servicio. (Toad, 2005).

Recursos complementarios

- Video sobre: “El Modelo TCP/IP: Capa de Transporte” 
- Video sobre: “Capas de transporte: TCP Y UDP” 
- Presentación en PDF de Cisco NetAcad sobre: “Capítulo 7: Capa de Transporte” 

Actividad de aprendizaje 15

Descripción de la actividad

De acuerdo con Computer Weekly.es, el enrutamiento dinámico o adaptativo, es un proceso para determinar la ruta óptima que debe seguir un paquete de datos a través de una red para llegar a un destino específico.

El enrutamiento adaptativo utiliza algoritmos y protocolos de enrutamiento que leen y responden a cambios en la topología de la red de manera automática. Además de Open Shortest Path First (OSPF), otros protocolos de enruteamiento que facilitan el enrutamiento adaptativo incluyen el protocolo de Sistema Intermedio a Sistema Intermedio (IS-IS) para redes grandes como Internet y el protocolo de información de enrutamiento (RIP) para transporte de corta distancia.

El simulador Packet Tracer de la Academia de Networking de CISCO, permite configurar dispositivos de conectividad como switches y routers.

Esta actividad de aprendizaje tiene como propósito la configuración de enruteamiento dinámico OSPF utilizando el simulador Packet Tracer.

Se pide:

Realizar las siguientes prácticas de laboratorio: 11.6.1: “Práctica de laboratorio: Práctica de laboratorio de configuración básica de OSPF”, disponible en la Web, desarrollado por la Academia de Networking de CISCO. Rellene todos los ejercicios que allí se señalan en ella.

Al finalizar, elabore un solo informe de la Práctica de Laboratorio que despliegue los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de cada punto con sus resultados, Conclusiones generales y Referencias bibliográficas.

Autoevaluación Capítulo 15

1. Para el direccionamiento físico MAC y el lógico IP, elija la correcta de las siguientes opciones.

Trabajan solamente en redes PAN.

Trabajan en la capa 2 y en la capa 3 del modelo OSI respectivamente.

Existen diferentes tipos de direccionamiento de redes estas son: H, J y K.

2. ¿Cómo se le conoce combinación de bits que sirve para delimitar el ámbito de una red de datos?

Dirección de versión IPv4

Máscara de subred

Encabezado

3. El Internet Protocol (IP) especifica el formato de los paquetes que viajan por Internet, los cuales contiene encabezado y datos. ¿Cuál es la longitud del encabezado anteriormente mencionado?

De 20 o 24 bytes

De 1 a 2 bytes

De 0 a 8 bits

4. Qué significa Fragment Offset dentro del formato de un paquete IP?

0 significa que es el último fragmento de este paquete, 1 significa que este no es el último fragmento

Es el número único el cual es asignado por el emisor y sirve para re ensamblar un paquete fragmentado

Es utilizado por los paquetes fragmentados para ensamblarlos por completo

5. Una de las clases de direcciones de red es la clase D, ¿Para qué uso está destinada?

Enrutamiento

Multicast IP

Enlace de secuencias IP

6. ¿Qué son las redes Classful?

Son protocolos con la función de transmitir la máscara de red en sus actualizaciones

Es el resultado de la unión de direccionamientos IPv4 e IPv6

Son redes usadas para soportar el uso de varias máscaras de subred de las clases A y B

7. ¿Cuáles son los protocolos de enrutamiento que soportan las redes Classful?

TCP - UDP

WAN y WLAN

RIP 1 e IGRP

8. ¿Qué son las redes Classless?

Disponen los primeros 4 bits de la clase C

Son redes que permiten una conexión más rápida con el extranet e intranet

Son protocolos para evitar limitaciones de los protocolos Classful

9. ¿Cuáles son los dígitos identificadores de las redes Clase C?

0

10

110

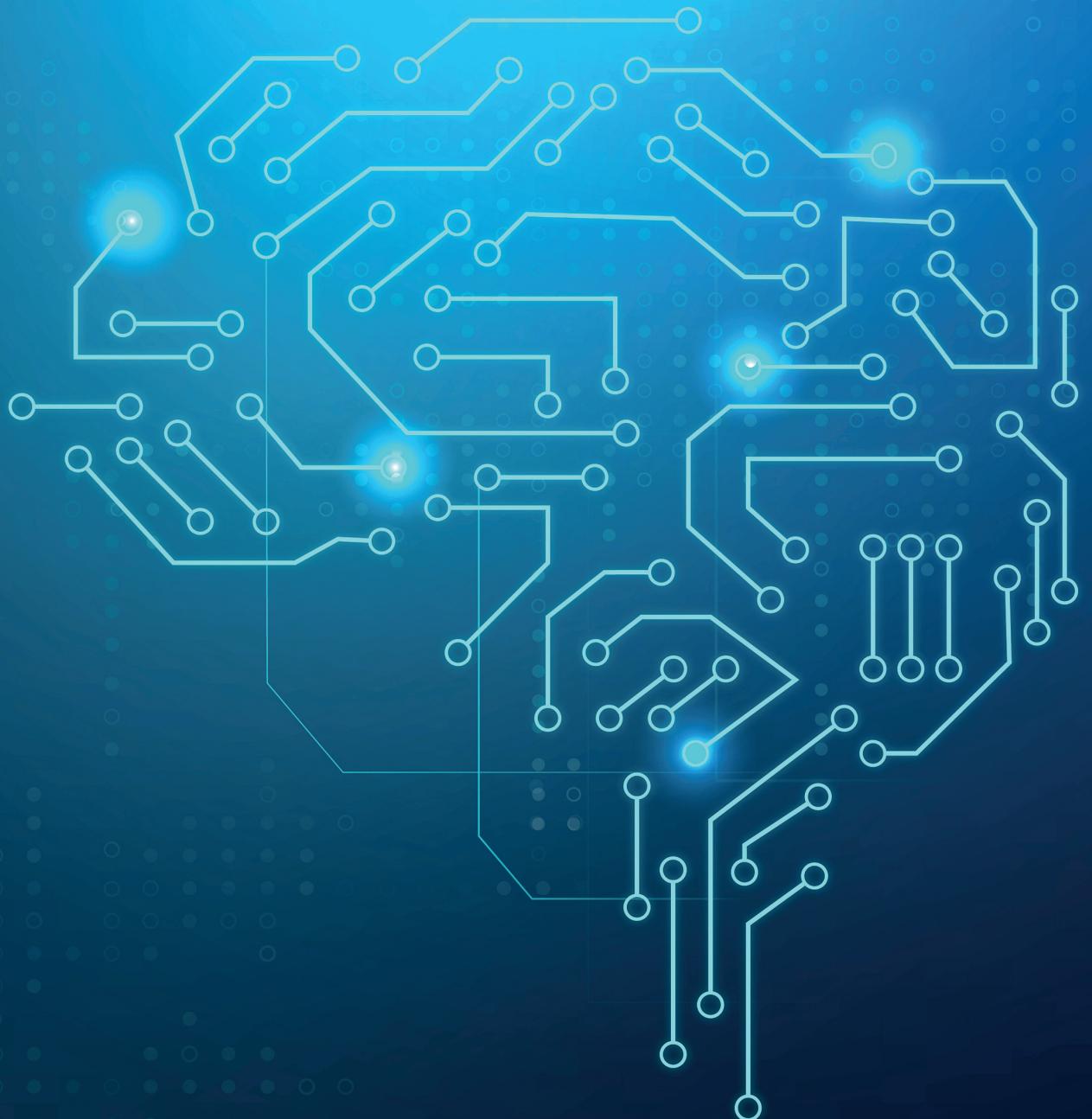
Ninguna respuesta es correcta

10. ¿Cuáles son los protocolos que soportan las redes Classless?

RIP 2, OSPF EIGRP, IS-IS y BGP

HTTP, HTTPS, POP3 y SMTP

DCCP, iSCSI, UDP, SCTP, IL y SPX



● <https://acortar.link/NwW5XA>

CAPÍTULO XVI

Redes de Nueva Generación

16.1 Introducción

De acuerdo con la Recomendación de la Unión Internacional de Telecomunicaciones (International Communications Unit, UIT) Rec. UIT-T Y.2001 (12/2004) (ITU, 2004) el objetivo primordial las redes de nueva generación (New Generation Networks, NGN) es facilitar la convergencia de redes y la convergencia de servicios. Desde ese entonces, el propósito de las NGN ha sido asegurar que todos los elementos necesarios para la interoperabilidad y las capacidades de red que soporten aplicaciones mundialmente, a través una misma red de manteniendo y el concepto de separación entre transporte, servicios y aplicaciones.

Según esta recomendación (ITU, 2004), la red de próxima generación se define como una red basada en la conmutación de paquetes, la cual permite la prestación de servicios de telecomunicaciones además del uso de tecnologías múltiples que se relacionan al transporte de banda ancha.

Entre los objetivos que persigue la NGN están el promover una competencia justa, se busca estimular la inversión privada y definir un marco tanto para la arquitectura como para las capacidades que permitan cumplir requisitos reglamentarios y ofrecer un acceso abierto hacia las redes, los requerimientos dentro de estos objetivos son asegurar la prestación y el acceso universal, favorecer a la igualdad de oportunidades para los ciudadanos, promover la diversidad de contenido, incluir la diversidad lingüística y cultural, reconocer la necesidad de la cooperación mundial y atender a los países menos adelantados.

16.2 Características fundamentales de la NGN

La implementación de NGN tiene un gran impacto en los sistemas de telecomunicaciones empleados en la actualidad, pues involucra calidad y garantía del servicio de extremo a extremo (Matango F. , 2016). De conformidad con la recomendación (ITU, 2004), la NGN debe cumplir con las siguientes características fundamentales:

- Transferencia basada en paquetes
- Separación de las funciones de control en capacidades de portador, llamada/sesión, y aplicación/servicio
- Separación entre la prestación del servicio y el transporte, y la provisión de interfaces abiertas

- Red multiservicio capaz de manejar voz, datos y vídeo
- Interoperabilidad con redes tradicionales a través de interfaces abiertas;
- Movilidad generalizada
- Acceso sin restricciones de los usuarios a diferentes proveedores de servicios
- Variedad de esquemas de identificación
- Percepción por el usuario de características unificadas para el mismo servicio
- Convergencia de servicios entre fijo y móvil
- Independencia de las funciones relativas al servicios con respecto a las tecnologías de transporte subyacentes
- Soporte de múltiples tecnologías de la última milla;
- Red con el plano de control (señalización, control) separado del plano de transporte y conmutación/encaminamiento
- Posee interfaces abiertas para el inter-funcionamiento entre los niveles de transporte, control y las aplicaciones
- Garantiza QoS para distintos tipos de tráfico y de Acuerdo de Nivel de Servicio (SLA) extremo a extremo
- Transferencia basada en datagramas IP para el transporte de todo tipo de información
- Compatibilidad con una amplia gama de servicios, aplicaciones y mecanismos basados en módulos de servicios
- Acceso sin restricciones por los usuarios a diferentes proveedores de servicios
- Características del servicio unificado para el mismo servicio que percibe el usuario
- Conformidad con todos los requisitos reglamentarios, por ejemplo, en cuanto a comunicaciones de emergencia, seguridad, privacidad, interceptación legal, etc.

16.3 Capacidades de la NGN

Desde el 2004, la Recomendación Rec. UIT-T Y.2001 (12/2004) (ITU, 2004) proyectó las siguientes capacidades:

La implementación de la infraestructura y protocolos con el objetivo de permitir la creación, introducción y gestión de los tipos de servicios existentes

(incluidos aquellos que utilizan diferentes tipos de medios), junto a los tipos de esquemas de codificación y servicios de datos de mensajería y la transferencia simple de datos en tiempo real y no real, también los que sean sensibles al retardo y tolerantes al mismo.

Separar los servicios y transporte que permite que se ofrezca por separado dando paso a la evolución independiente. Permite, además, el aprovisionamiento de servicios nuevos y existentes dentro de la red y el tipo de acceso que se utilice.

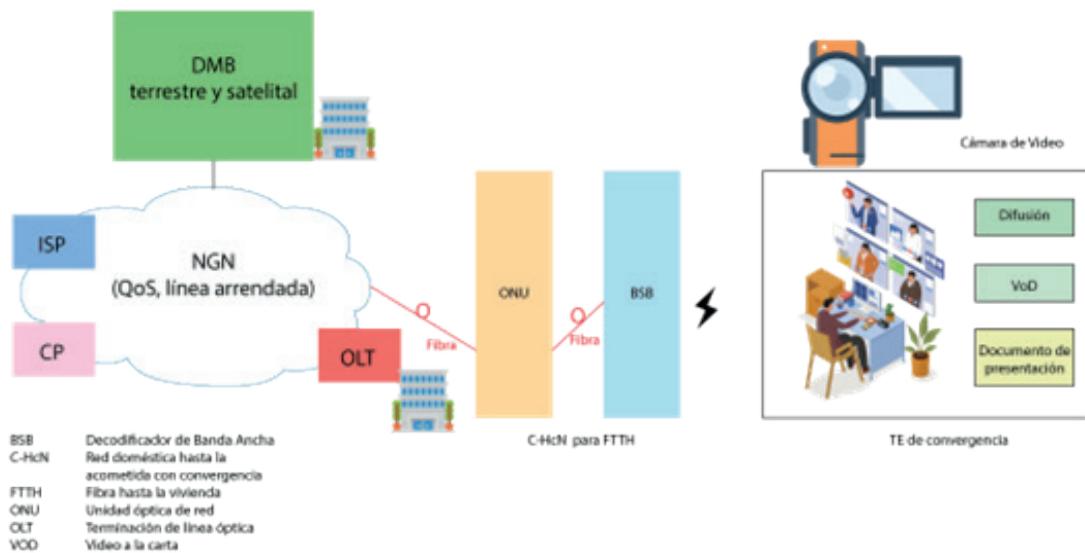
Permite que las entidades funcionales que se encuentran dentro de la NGN, controladoras de la política, medios, prestación de servicios, seguridad y sesiones, puedan distribuirse a lo largo de la infraestructura. Cuando se encuentran físicamente distribuidas, su forma de comunicación se da a través de interfaces abiertas.

Soporta dispositivos terminales extremos que existen y los que perciben la NGN. Los terminales son aquellos que se conectan a la NGN que incluyen dispositivos terminales como teléfonos o aparatos RDSI.

Proporciona mecanismos de seguridad que permitan proteger el intercambio de información sensible a través de la infraestructura con el fin de proteger contra ataques externos y contra el uso fraudulento de los servicios que proporcionan los proveedores.

Ofrece la convergencia de servicios en base a lo que establece la recomendación Rec. UIT-T Y.2011 (10/2004) (ITU-IT, 2004) que contiene capacidades de banda para ofrecer nuevos modelos de servicio como es la difusión hacia participantes múltiples a través de comunicaciones interactivas incluyendo los servicios inalámbricos. La Figura 92 muestra un ejemplo ilustrativo de la convergencia.

Figura 92
Ejemplo ilustrativo de la convergencia



Nota. La figura representa una red que permite la transmisión de varias señales de telecomunicaciones por el mismo canal de transmisión (ITU-IT, 2004).

16.4 Arquitectura general de NGN

Según (Matango F. , 2016), la arquitectura básica de NGN está basada en una topología jerárquica distribuida en cuatro capas, con conectividad al nivel superior y dentro del mismo nivel (Ver Figura 93). A continuación, se describen brevemente cada una de las capas:

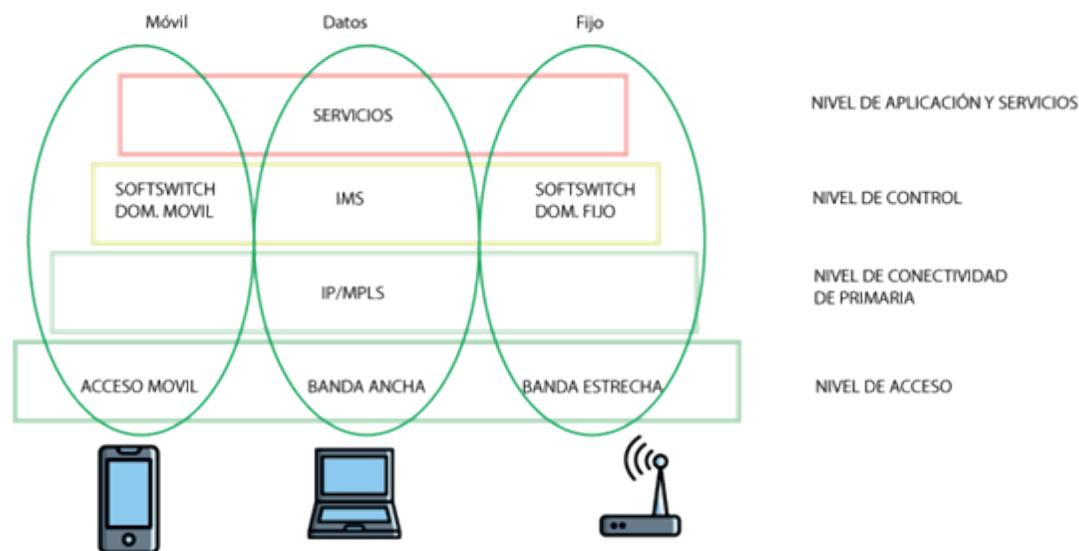
- Capa de Acceso: de acuerdo con (Matango F. , 2016) esta capa incluye las tecnologías para conectarse con los clientes finales tales como DSL, líneas de cobre, sistemas de cable, sistemas inalámbricos, anillos Metro Ethernet, fibra óptica, etc.
- Nivel de Conectividad Primaria (Núcleo): como lo señala (Matango F. , 2016) esta capa que se encarga de las tareas de conmutación, enruteamiento de los segmentos o datagramas IP de extremo a extremo, además del transporte y control de la señalización. Este nivel se basa en IP utilizando ATM, MPLS y Ethernet.
- Capa de Control: esta capa coordina todos los elementos en las otras capas y es la encargada de asegurar la interoperabilidad de la Red de

transporte con los servicios y aplicaciones mediante la interpretación, generación, distribución y traducción de la señalización correspondiente con los protocolos.

- Capa de Servicio: los tipos de servicios deben abarcar los ya existentes y además una gama de servicios de datos y de multimedia en cualquier combinación posible (voz, datos, video, TV, Web mail, etc.). Estos deben ser independientes de la tecnología a utilizar y son colocados generalmente de forma centralizada a fin de lograr mayor eficiencia y además distribuirlos a la Red. Este nivel incluye el equipamiento necesario para proporcionar los servicios y aplicaciones a la Red.

Figura 93

Arquitectura general de las redes de nueva generación



Nota. La figura representa una arquitectura que ilustra las cuatro capas de una NGN, así como los protocolos, equipos y servicios. Obtenido de: (Meyers, 2009)

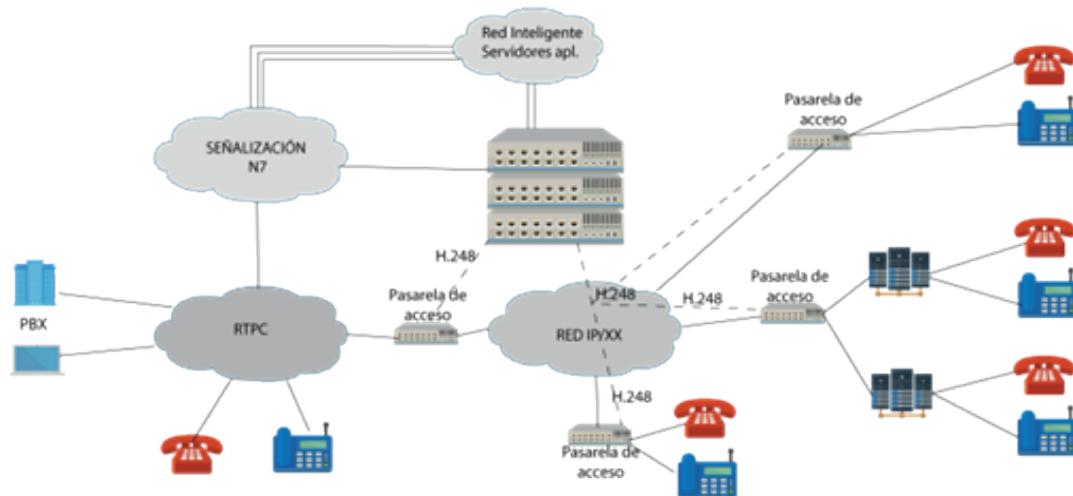
16.5 Protocolos NGN

En las redes de próxima generación se utilizan un conjunto de protocolos, estándares y sistemas que dependen del tipo de aplicación requerida, de la tecnología a utilizar y de los fabricantes. En NGN existe un uso marcado del SIP, debido a la facilidad de implementación y desarrollo de ciertos servicios y aplicaciones. A continuación, se explican brevemente los más utilizados:

- **H.323:** estándar liberado en 1996 por la ITU que fue desarrollado para redes de conmutación de paquetes, para proveer servicios para la transmisión de datos, vídeo y voz en tiempo real. Hoy en día, H.323 está siendo utilizado para la telefonía sobre IP y posibilita que los productos y aplicaciones puedan operar conjuntamente entre ellas.
- **Protocolo H.248:** definido por la UIT-T conocido como MEGACO empleado para para la gestión de sesiones y señalización.
- **SIP:** Protocolo de Iniciación de Sesiones (Session Initiation Protocol, SIP) para manejar la señalización de las comunicaciones, como por ejemplo para activar el servicio de Voz sobre IP (VoIP).
- **ENUM:** o (Electronic Numbering) que permite establecer una correspondencia entre la numeración telefónica tradicional y las direcciones de acceso relacionadas con las redes de conmutación de paquetes.
- **MPLS:** (Multiprotocol Label Switch, MPLS) es una tecnología que enruta el tráfico utilizando la ruta más corta basada en marcadores que los asigna a los paquetes de información. Además, establece un túnel para el envío extremo a extremo.
- **IMS:** Subsistema multimedia estándar (IP Multimedia Subsystem, IMS) que define una arquitectura genérica para proveer servicios multimedia con aplicaciones comunes a muchas tecnologías como: GSM, WCDMA, CDMA, WiMAX, etc.

16.6 Equipamiento y tipo de usuarios y servicios

La industria de telecomunicaciones desarrolla aplicaciones y soluciones para hacer frente a las redes de nueva generación y tener una participación importante en el sector. Según la ITU (González-Soto, 2006), una abstracción de la topología de una NGN, puede ser la que se muestra en la Figura 94. Entre los principales componentes de esta topología están los siguientes:

Figura 94*Arquitectura general de las redes de nueva generación*

Nota. La figura representa una topología NGN con su equipamiento, servicios y usuarios. Obtenido de: (González-Soto, 2006).

- Pasarela de enlace: que permiten a las redes telefónicas clásicas de multiplexación por división de tiempo (Time Division Multiplexing, TDM) y a las redes de nueva generación trabajar en forma conjunta.
- Pasarela de acceso: que permite a los usuarios de telefonía tradicional o simple servicio telefónico antiguo (Plain Old Telephone Service, POTS) acceder a las redes y a los servicios ofrecidos por las redes de nueva generación.
- Pasarela de señalización (Signalling Gateway, SG): que son componentes de la red responsables del cambio de señalización entre cualquier red y una red de nueva generación.
- Softswitch: que es uno de los dispositivos más importantes en la NGN que es un dispositivo programable que controla los servicios ofrecidos sobre una red IP, el control de llamada, las llamadas de voz sobre IP. Además, el Softswitch permite la correcta integración de los diferentes protocolos dentro de la NGN.
- Redes de Paquetes: la conmutación de paquetes es un método de agrupar los datos transmitidos a través de una red digital en unidades de tamaño variable. La inclinación de NGN es usar redes IP sobre varias posibilidades de transporte (ATM, SDH, WDM, MPLS, etc.).

- Servidor de Aplicaciones (AS): que provee la ejecución de los servicios para controlar los servidores de llamadas, servidores de medios y servidores de mensajes.
- Sistema telefónico Central (Private Branch Exchange, PBX): que generalmente se instala en empresas donde se debe permitir a los usuarios realizar llamadas dentro de ella y administrar las llamadas entrantes y/o salientes de la red telefónica.
- IP PBX: de funcionamiento similar al de un PBX compatible con el protocolo IP que transforma la voz en paquetes.
- Equipos de usuario final: cualquier tipo de teléfonos fijos o móviles, computadores de escritorio, portátiles, televisores inteligentes, tabletas, etc.
- VoIP (Telefonía sobre IP): que a diferencia de la VoIP permite realizar llamadas utilizando las redes IP como medio de transporte. Además, de prestar los mismos servicios que un PBX, la telefonía IP traen nuevos servicios como los son transferencia de archivos, mensajería, integración con otros servicios IP, etc.
- IPTV: televisión por protocolo de Internet (Internet Protocol televisión, IPTV) es un servicio de un ISP que provee programación de televisión y contenido de video por demanda utilizando TCP/IP), en contraposición a las señales de televisión por transmisión, televisión por cable o satélite.
- Centrex IP: que es un servicio de voz en la nube de Telefónica, que le permite realizar todas las funciones de una centralita, con lo cual se evita la inversión de un PBX. El equipo pertenece y es operado por un proveedor de servicios.

Recursos complementarios

- Video sobre la arquitectura de una red de nueva generación NGN 
- Video sobre “Elementos de una red de nueva generación NGN” 
- Oportunidades y tendencias futuras de las redes de nueva generación en idioma inglés. 

Actividad de aprendizaje 16

Descripción de la actividad

Frame Relay es una tecnología de protocolo de red de conmutación de paquetes digital de capa de enlace de datos diseñada para conectar redes de área local.

El simulador Packet Tracer de la Academia de Networking de CISCO, permite configurar nubes Frame Relay.

Esta actividad de aprendizaje tiene como propósito la configuración de una red WAN Frame Relay utilizando el simulador Packet Tracer.

Se pide:

Realizar la siguiente práctica de laboratorio: 3.5.1 “Configuración de Frame Relay básico”, disponible en la Web, desarrollado por la Academia de Networking de CISCO. Rellene todos los ejercicios que se señalan en ella.

Al finalizar, elabore un solo informe de la Práctica de Laboratorio que despliegue los resultados obtenidos, con la siguiente estructura: Tema, Objetivos de aprendizaje, Marco teórico, Desarrollo de cada punto con sus resultados, Conclusiones generales y Referencias bibliográficas.

Autoevaluación Capítulo 16

1. La subred de punto a punto permite que dos dispositivos se conecten, mientras que una subred de un centro de datos puede diseñarse para conectar mayores cantidades de dispositivos.

Verdadero

Falso

2. Si se necesita tener una dirección de red de clase B dividida en exactamente 510 subredes, ¿Qué máscara de subred debe asignar?

255.255.255.252

255.255.255.128

255.255.0.0

255.255.255.192

3. ¿Qué tipo de clase de direccionamiento IP permite un máximo de 254 hosts disponibles?

Clase A

Clase B

Clase C

Clase D

4. ¿Cuál es el número decimal de la siguiente máscara de subred 11111111.11111111.11000000?

255.255.255.128

255.255.255.192

255.255.255.224

5. ¿Cuántos hosts puedo tener en una subred que tiene la siguiente máscara de subred adaptada: 255.255.254.0?

512 hosts

255 hosts

510 hosts

6. ¿Cuántas subredes tendrá si tenía una máscara por defecto de clase C y al adaptarla queda así: 255.255.255.192?

4 subredes

8 subredes

2 subredes

7. ¿Cuál es la notación de longitud de prefijo para la máscara de subred 255.255.255.224?

/27.

/28.

/26.

/25.

8. ¿Cuál es el propósito de la máscara de subred junto con una dirección IP?

Para determinar la subred a la que pertenece el host

Para identificar de manera única un host en una red

Para enmascarar la dirección IP a extraños

Para identificar si la dirección es pública o privada

9. ¿Cuántas direcciones de host están disponibles en la red 172.16.128.0 con una máscara de subred de 255.255.252.0?

1024

512

1022

2048

10. Se ha dicho a un administrador del sitio de una red particular que debe dar cabida a 126 hosts, ¿Qué máscara de subred se usaría que contenga el número requerido de bits de host?

255.255.255.224

255.255.255.128

255.255.255.240

255.255.255.0

0 1



<https://acortar.link/sWhZS2>

CAPÍTULO XVII

GNS3

17.1 ¿Qué es GNS3?

En el diseño y construcción de redes es indispensable el uso de simuladores, emuladores, y software especializado que beneficie el aprendizaje y pruebas de concepto de redes de computadoras. De esta manera, el estudiante o el profesional diseñador de redes puedan diseñar topologías de red simples o complejas, realizar configuraciones de dispositivos de red, levantamiento de servicios y poner en marcha simulaciones sobre ellos. Uno de los simuladores-emuladores más utilizados en la academia e industria en el mundo es el GNS3.

GNS3 por sus siglas en inglés Graphic Network Simulation, o Simulación Gráfica de Redes, es el resultado del trabajo colaborativo entre Christopher Filot, Jeremy Grossmann y Julien Duponchelle. GNS3 es un simulador de red gráfica multiplataforma, de código abierto, que funciona sobre Windows, OS X, y Linux. GNS3 existe desde hace más de 10 años y según su sitio web, tiene una comunidad creciente de más de 800 000 miembros. GNS3 es muy útil para el diseño y pruebas de redes de computadoras desde la PC. Puede trabajar con imágenes de Cisco IOS, Juniper, MikroTik, Arista y redes Vyatta. GNS3 viene siendo mejorado permanentemente por su grupo de trabajo con lo cual se incluyen modificaciones y mejoras acorde al avance tecnológico. Sin embargo, GNS3, requiere de recursos computacionales robustos como memoria, procesador, y dispositivos de entrada y salida, en razón de que trabaja con máquinas virtuales y software adicional como el analizador de tráfico y protocolos Wireshark.

GNS3 es un simulador que facilita la preparación para aprobar los exámenes de certificación como Cisco CCNA o CCNP. Adi lo ayuda a probar y verificar las implementaciones del mundo real.

17.2 Características fundamentales de GNS3

GNS3 es una herramienta interesante y completa que reúne muchas bondades técnicas. Entre sus características se encuentran:

- Creación de simulaciones en tiempo real.
- Permiten conectar un entorno simulado a una red de computadores real.
- Estrechamente vinculado con otras herramientas como: Dnamips, VirtualBox, Wireshark.

- Permite la ejecución directa de la imagen (ISO) del sistema operativo, no la emula como lo hace Packet Tracer.
- Facilita la personalización de una red de acuerdo a una necesidad.
- Permite integrar una cantidad ilimitada de objetos de diferente tecnología, incluyendo a Cisco, Juniper, etc.

Emulador y Simulador

GNS3 admite dispositivos emulados y simulados. La emulación significa que GNS3 imita o emula el hardware de un dispositivo y ejecuta imágenes reales en el dispositivo virtual tal como que fuera en el mundo real. La simulación, por su parte significa que GNS3 simula las características y la funcionalidad de un dispositivo como un interruptor. No está ejecutando sistemas operativos reales (como Cisco IOS), sino un dispositivo simulado desarrollado por GNS3, como el conmutador de capa 2 integrado.

Con GNS3 se puede crear redes virtuales utilizando una variedad de enrutadores, conmutadores y PCs. Algunos de las IOS más utilizados se encuentran en la página oficial de Cisco (Teletrónica, 2019). Un ejemplo interesante es creación de máquinas virtuales utilizando la plataforma de virtualización Virtual Box e integradas en un simulador de red como GNS3.

Existen diferencias entre GNS3 y otras aplicaciones dedicadas a la simulación de redes como Packet Tracert. GNS3, se ejecuta sobre un hipervisor que no solo permite la emulación del hardware, sino que también la ejecución de una imagen IOS real en la PC. Esto permite que cualquier función que sea compatible con la versión de la IOS, esté disponible para usar en el diseño de la red. En la tabla 11 se listan las diferencias entre los dos simuladores principales:

Tabla 11

Comparación entre GNS3 y Packet Tracer

CARACTERÍSTICA	GNS3	PACKET TRACER
Cisco IOS imágenes	También puede responder a Cisco IOS. Sin embargo, debe introducir sus propias imágenes de IOS	Aplica las imágenes reales de Cisco IOS y responde como lo haría un enrutador Cisco en tiempo real.
Open Source	Es un simulador de software de red de código abierto y de libre distribución.	No es una herramienta de simulación visual multiplataforma de código abierto.

IOS	GNS3 permite trabajar con imágenes reales de IOS que pueden ejecutarse con éxito en un entorno virtual.	Ofrece IOS simulado con funcionalidad sobre la base de características parciales.
Consumo de RAM	consume la memoria RAM real del dispositivo. El consumo por cada router se estima en unos 512 MB de RAM.	No consume la memoria RAM real del dispositivo.
Rango de conectividad	Permite a los usuarios tener una interfaz de línea de comandos de enrutadores. Sin embargo, no permite tomar la interfaz de línea de comandos de un commutador o cualquier otro tipo de dispositivo de usuario final.	Brinda la posibilidad de tener commutadores, enrutadores y CLI (interfaz de línea de comandos) del servidor, así como la opción de agregar dispositivos finales como teléfono de voz, computadora portátil, PC, etc.

EGNS3 es una plataforma que le permite simular topologías de red utilizando imágenes de proveedores como Cisco y Juniper. El logo representativo de GNS3 se muestra en la figura 93. La tabla 12 lista los requisitos recomendados para un entorno Windows:

Tabla 12

Requerimientos recomendados

Ítem	Requerimientos Recomendados
Sistema Operativo	Windows 7 (64 bit) o superior.
Procesador	4 o más núcleos lógicos – AMD-V / RVI Series or Intel VT-X / EPT
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	16 GB RAM
Espacio en disco	<ul style="list-style-type: none"> • Disco de Estado Sólido (SDD) • 35 GB de espacio disponible.
Notas adicionales	La virtualización tiene una penalización conocida como overhead, lo que significa que se necesita que los equipos tengan buenos recursos de memoria y procesador especialmente.

Figura 95

Logo GNS3

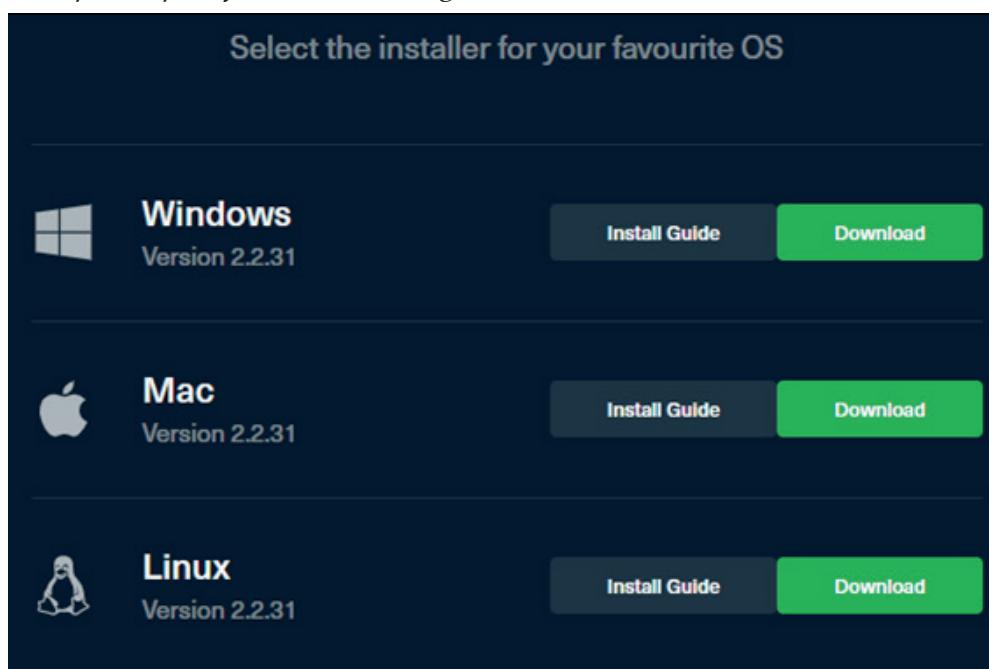


Nota. Para la instalación de GNS3 se puede acceder al artículo publicado por (XarCom, 2019).

Para que pueda acceder a GNS3, es conveniente revisar los requerimientos mininos. Luego se debe acceder al sitio web: <https://gns3.com>. En el sitio se muestra los tipos de plataformas o sistemas operativos que se pueden descargar, luego de un corto proceso de registro individual de los usuarios, están habilitados para la descarga. La figura 96 muestra esta interfaz a la fecha:

Figura 96

GNS3-Tipos de plataformas de descarga



GNS3 dispone algunas opciones para la parte del servidor del software: servidor GNS3 local, máquina virtual GNS3 local y máquina virtual GNS3 remo-

ta. Cuando se crea topologías en GNS3 utilizando el cliente GUI de software todo en uno, los dispositivos creados deben ser alojados y ejecutados por un proceso de servidor. Es decir, se ejecuta localmente en la misma PC donde se instaló el software, (más conocido todo en uno GNS3). Este es el esquema tradicional que es muy utilizado por los estudiantes en el mundo.

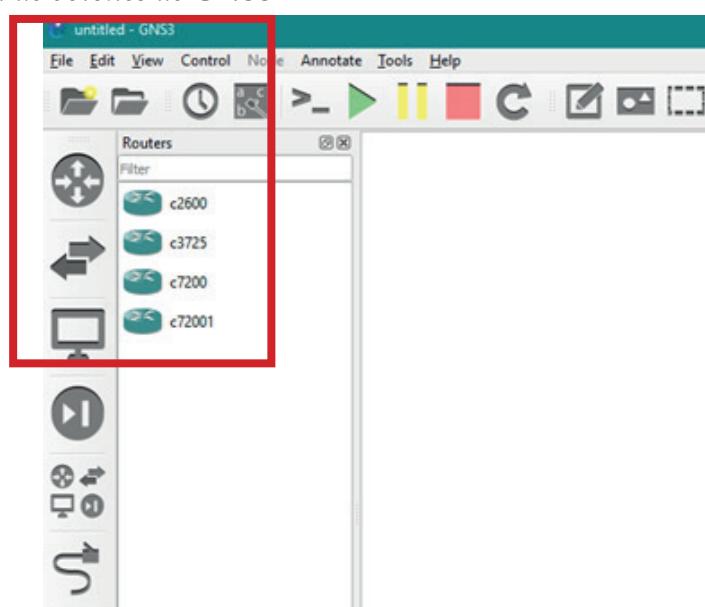
Si se decide utilizar la VM GNS3 que es el más recomendado, se puede ejecutar la VM GNS3 localmente en su computador personal usando las plataformas de virtualización VMware Workstation, Virtualbox o Hyper-V. Además, se puede ejecutar la VM GNS3 de forma remota en un servidor usando VMware ESXi o inclusive en la nube computacional.

Luego del proceso de instalación, es importante revisar la forma del funcionamiento de GNS3. En principio, la interfaz de GNS3 le exige la creación de un nuevo proyecto, que consiste en el conjunto de imágenes de los IOS de los dispositivos de conectividad, así como los medios de transmisión utilizados, las configuraciones de equipos de usuario final, medios de transmisión, servicios de red, etc de una sola topología de trabajo. Esta información se almacena en la carpeta de usuario de su propio PC.

Una vez creado el proyecto, la consola de GNS3 muestra la interfaz de configuración inicial. Como toda interface, se compone de una barra de menús, con varios íconos que operativizan su funcionamiento. Adicionalmente, en la barra lateral se encuentran disponibles los dispositivos de red como conmutadores, routers, PCS, terminales y otros. La Figura 97 muestra el panel.

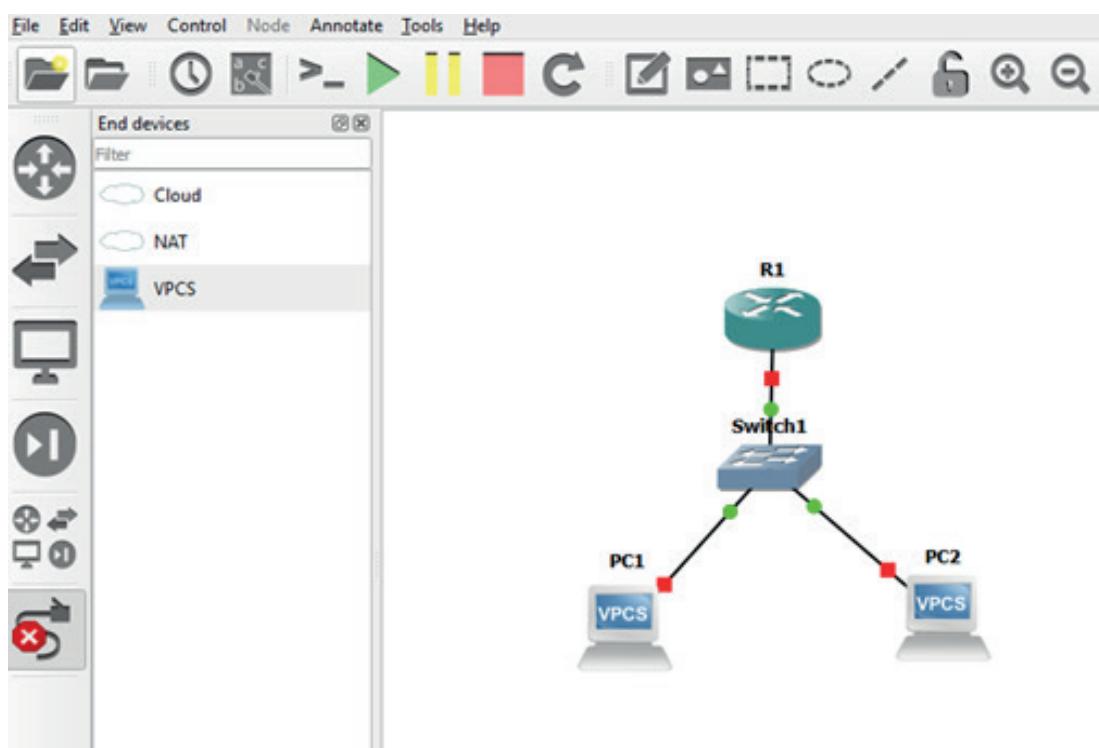
Figura 97

Panel lateral de botones de GNS3



Para agregarlos a la topología de red, basta con desplegarlos al área de trabajo. Así mismo, se puede conectarlos con los medios de transmisión disponibles (ver Figura 96). En la interface se incluyen algunas imágenes de enruteadores o conmutadores. No obstante, es necesario descargar otras imágenes GNS3 de Cisco IOS para GNS3. En este punto, recomendaría leer en la Web White papers que ilustran cómo descargar imágenes de Cisco IOS que se ejecutan en GNS3. En el siguiente enlace se pueden descargar algunos de ellos: <http://tfr.org/cisco-ios/26xx/>.

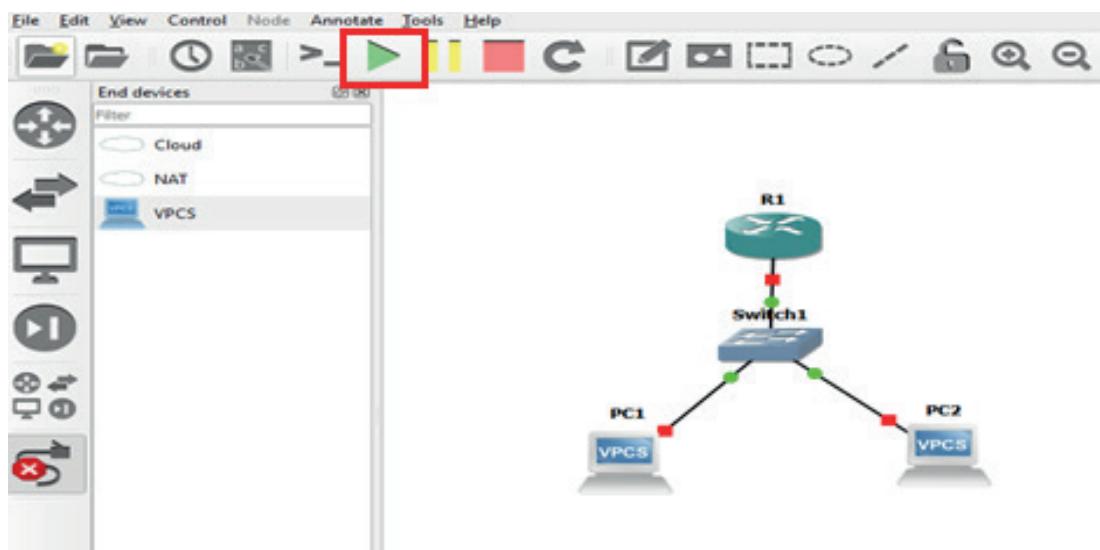
Figura 98
Proyecto en ejecución en GNS3



Después de configurar la topología e iniciar la simulación, presione el botón de encendido en la barra superior. En GNS3, cada elemento funciona de forma independiente, por lo que el efecto de este botón es activar cada dispositivo. No es necesario activar todos los dispositivos a la vez, e incluso es posible agregar o eliminar dispositivos mientras otros se están ejecutando (Ver figura 99).

Figura 99

Ejecución de la topología de red simulada



En resumen, GNS3 permite el diseño gráfico de topologías de red a simular. Puede utilizar una gran variedad de IOS Cisco, Juniper, IPS y firewalls Cisco de tipo ASA y PIX. Permite simular redes Ethernet, ATM, OSPF, Frame Relay, MPLS y todo tipo de enrutamiento. Además, simula una conexión de red en el entorno real, con una integración de captura de paquetes con Wireshark y la combinación de máquinas virtuales (Qemu, VirtualBox y VMware).

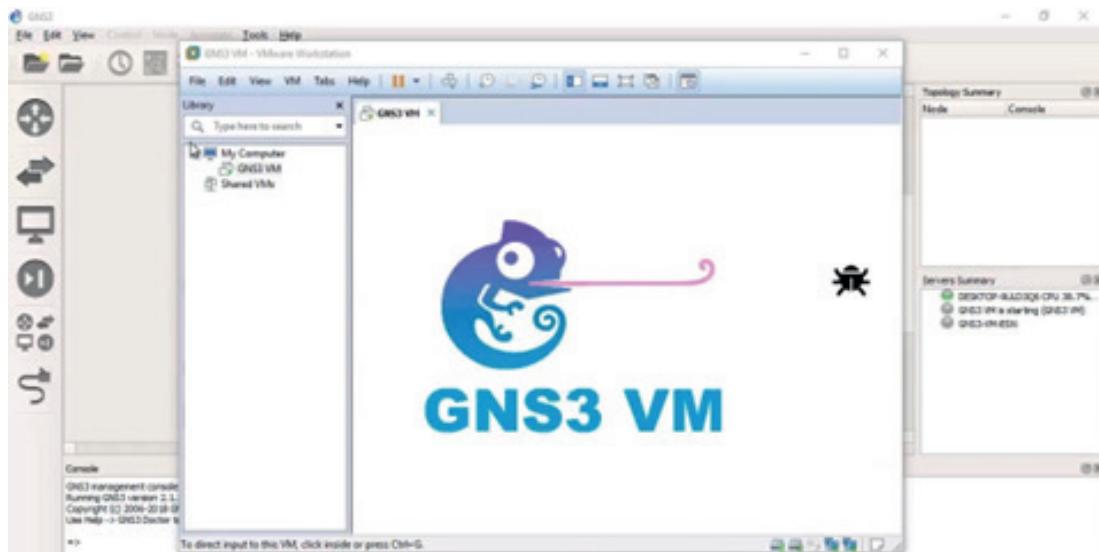
17.3 Máquinas virtuales en GNS3

GNS3 es completamente gratuito para los sistemas operativos Windows, Linux y MacOS. Así mismo, proporciona máquinas virtuales configuradas para ejecutar servidores GNS3 con un rendimiento favorable en cualquier plataforma.

GNS3 cuenta con una nueva máquina virtual (GNS3 VM) con sistema operativo de base Ubuntu 18.04 LTS, mismo que es compatible con VMware, Virtual Box. Una de las nuevas características es que también será compatible con Hyper - Microsoft - V, recomendada para usar esta VM GNS3. La figura 100 muestra esta interfaz.

Figura 100

GNS3 VM



Recursos complementarios

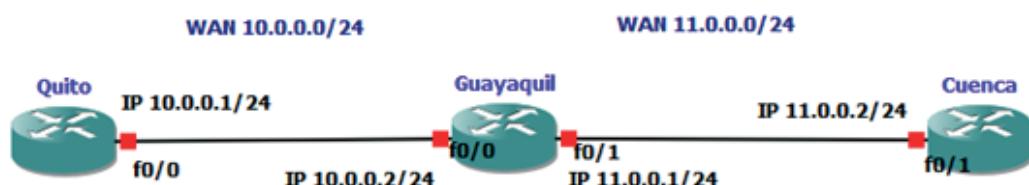
- Video sobre la instalación y configuración de GNS3+VMware 
- Video sobre GNS3 VM, laboratorio virtual en 2021 (Nueva Versión) 

Actividad de aprendizaje 17

Descripción de la actividad

Práctica de laboratorio 1: Enrutamiento dinámico configuración de OSPF y MPLS.

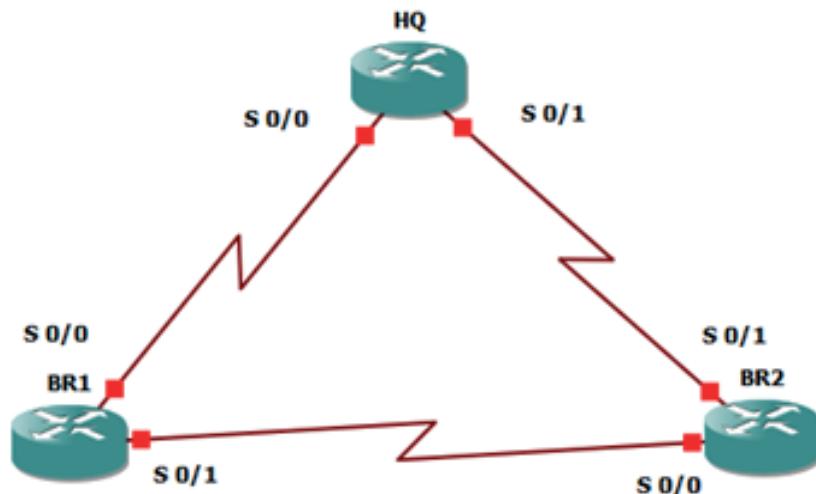
ENRUTAMIENTO DINAMICO CONFIGURACION DE OSPF Y MPLS



```
router ospf 10
network 0.0.0.0 255.255.255.255 area 0
```

Práctica de laboratorio 2: Diseño e implementación de direccionamiento IPv4 con VLSM.

Diseño y e implementación de direccionamiento IPV4 con VLSM



Autoevaluación Capítulo 17

1. ¿Cuántas direcciones host se encuentran disponibles en una red /17?

31958

32766

30675

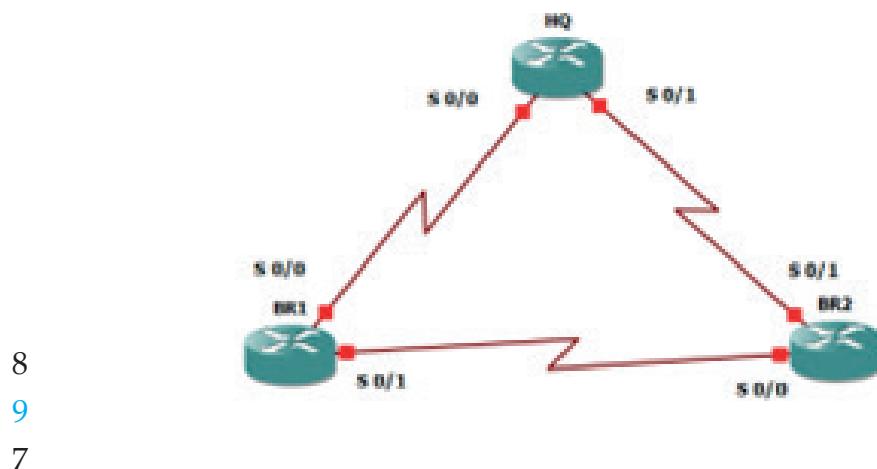
2. ¿Cuál es la cantidad total de direcciones host que se necesitan en el diagrama de la topología?

30865

31506

32543

3. ¿Cuántas subredes se necesitan en la topología de la red?



4. ¿Cuántas direcciones host se necesitan para cada enlace de subred serial?

- 4
- 2
- 6

5. ¿Cuál es la subred más pequeña que admite esa cantidad de direcciones host?

- /24 o 255.255.255.255
- /18 o 255.255.192.0**
- /30 o 255.255.255.252

6. ¿Qué significa GNS3?

- Graphic Nothing Similar
- Graphic Network Simulation**
- Simulation Graphic Nice

7. Configure la interfaz conectada al S2 como enlace troncal

show elan brief
switchport mode trunk
switch mode

8. Comando para configurar las VLAN y los nombres que se indican.

switched brief
show vlan brief
show brief

9. Comando para habilitar una interfaz en específico.

no shutdown

no save

Are you safe?

10. ¿Cómo se llama el software que permite integrar una máquina virtual en GNS3?

VirtualBox

GNS3VM

Hyper V. Microsoft

Referencias

- Alani. (2014). Springer Link. TCP/IP Model: https://sci-hub.se/https://doi.org/10.1007/978-3-319-05152-9_3
- Arcadio. (2019). Calculadora VLSM. <https://arcadio.gq/calculadora-sobre-des-vlsm.html>
- Aun, A. (18 de May de 2020). Getting Dynamic IP with DHCP. <https://avocado89.medium.com/getting-dynamic-ip-with-dhcp-ee1ee1e722b0>
- Autoayudacisco. (2 de diciembre de 2010). Autoayudacisco.over-blog.es (Modelo OSI). <http://autoayudacisco.over-blog.es/article-modelo-osi-62175120.html>
- Avantel. (24 de Julio de 2019). Redes informáticas: ¿por qué son importantes? <https://www.avantel.co/blog/tecnologia/redes-informaticas-por-que-son-importantes/>
- Balazinska & Castro. (2003). Characterizing mobility and network usage in a corporate wireless local-area network. In *Proceedings of the 1st international conference on Mobile systems, applications and services*. 303-316.
- Barroyeta, C. (25 de 12 de 2020). Qué es un módem | Tipos, historia y características. Recuperado el 22 de 8 de 2021, de 24/7 tecnó: <https://247tecno.com/modem/>
- Brown, F. (18 de December de 2019). How Does a Netgear WiFi Router Work? An Easy Explanation. <https://ko-fi.com/post/How-Does-a-Netgear-WiFi-Router-Work-An-Easy-Expla-Z8Z01AJFI>
- Castillo, J. (17 de January de 2019). Red Pública y Privada. Recuperado el 8 de September de 2021, de *Profesional Review*: <https://www.profesionalreview.com/2019/01/17/red-publica-y-privada/>
- CCNA. (2008). Módulo 14. Capa de Transporte: <https://ccnadesdecero.es/capa-transporte-definicion-y-funciones/>
- Cisco. (2008). Capítulo 3. Protocolos y Communicaciones de Red: http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter3_Protocolos%20y%C2%A0comunicaciones%20de%20red.pdf
- Cisco. (2010). IP Addressing Guide: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sba_ipAddr_dg.pdf
- Cisco. (2012). Conceptos y protocolos de enrutamiento.
- Cisco. (2019). Cisco. http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter3_Protocolos%20y%C2%A0comunicaciones%20de%20red.pdf

- CISCO. (12 de 3 de 2020). CISCO. <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-access-point.html>
- CISCO. (10 de 4 de 2021). CISCO. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html
- Cisco Networking Academy. (29 de July de 2020). Inter-VLAN Routing. Cisco Press: <https://www.ciscopress.com/articles/article.asp?p=3089357&seqNum=5>
- CISCO-CCNA. (2020). CISCO-CCNA. Capítulo 8. Capa física del modelo OSI. <https://blog.utp.edu.co/ee973/files/2012/04/capitulo08-Capa-Fisica.pdf>
- CNNA. (s.f.). Enrutamiento entre VLAN con Switches Capa 3. <https://ccna-desdecero.es/enrutamiento-entre-vlan-switches-capa-3/>
- Comer, D. (2014). Internetworking with TCP/IP. USA: Pearson Education.
- DataFlair. (2021). Android Web Services – Architecture, Features and Types. Data Flair: <https://data-flair.training/blogs/android-web-services/>
- DEICY. (8 de noviembre de 2011). DEICY-Características del modelo OSI. <http://deicy10.blogspot.com/2011/11/caracteristicas-modelo-osi.html>
- Fernandez, Y. (26 de 3 de 2021). Xataca. <https://www.xataka.com/basics/repetidor-wifi-que-como-funciona>
- Fernandez, Y. (19 de 4 de 2021). Xataca. <https://www.xataka.com/basics/modo-bridge-que-sirve-como-configurarlo-tu-router>
- FOCC. (21 de June de 2019). Conector de Fibra óptica. Fibresplitter: esplitter.com/info/fiber-optic-connector-tutorial-37155571.html
- Freepng. (2020). Freepng. Ícono de enrutador. <https://www.freepng.es/png-7olzr9/download.html>
- Fuertes, W. (20 de 5 de 2021). Capas del Modelo OSI. Quito, Pichincha, Ecuador: Grupo3.
- Galaxy Techonologies LLC. (2021). GNS3 documentation. <https://docs.gns3.com>
- Galindo, D. (21 de August de 2014). CLASSFUL y CLASSLESS.
- GeeksforGeeks. (09 de Septiembre de 2019). Introduction of Classful IP Addressing: <https://www.geeksforgeeks.org/introduction-of-classful-ip-addressing/>
- González-Soto, O. (2006). Seminario regional sobre Costes y Tarifas para los países miembros del Grupo TAL, BDT UIT. Sao Paulo.

- Hope, C. (30 de 10 de 2017). Tree topology. Recuperado el 30 de 07 de 2021, de Computerhope: <https://www.computerhope.com/jargon/t/treetopo.htm#:~:text=A%20tree%20topology%20is%20a,the%20information%20in%20a%20database>.
- Huawei. (2021). *Tipos de Routers de OSPF para Routers AR Huawei*.
- IBM Docs. (14 de April de 2021). IBM i 7.2. <https://www.ibm.com/docs/es/i/7.2?topic=standards-frame-relay-network>
- InetDaemon. (19 de May de 2018). DNS Hierarchy. InetDaemon.com: <https://www.inetdaemon.com/tutorials/internet/dns/operation/hierarchy.shtml>
- Information Sciences Institute, University of Southern California. (Septiembre de 1981). RFC 791, Internet Protocol. Obtenido de IETF: <https://data-tracker.ietf.org/doc/html/rfc791>
- ITU, U. I. (2004). Recomendación UIT-T Y.2001 (12/2004).
- ITU-IT. (2004). Redes de la próxima generación- - Marcos y modelos arquitecturales funcionales. Rec. UIT-T Y.2011: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-Y.2011-200410-I!!PDF-S&type=items
- Jha, M. (2019). Functions of Transport Layer in the OSI Model.
- Joskowicz, J. (2006). Cableado Estructurado.
- Jovanov, E. R. (2001). Patient Monitoring Using Personal Area Networks of Wireless Intelligent Sensors. 37.
- Jurado. (12 de February de 2021). ¿Qué es el protocolo IP y para qué sirve? CCM. <https://es.ccm.net/contents/274-el-protocolo-ip>
- Know, H. (2016). Qué es un proxy. IONOS: <https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-proxy/>
- LearnCisco. (21). Configuring RIP.
- Lopez, C. (30 de Diciembre de 2018). Aprende de redes. Modelo TCP/IP Capa a Capa – ¿Qué es?, Ejemplos de Uso: <https://aprendederedes.com/redes/introduccion/modelo-tcp-ip/>
- Lopez, C. (2 de 9 de 2020). ¿Qué es un concentrador o hub? Recuperado el 22 de 8 de 2021, de CCM: <https://es.ccm.net/faq/10391-que-es-un-concentrador-o-un-hub>
- López, C. (2 de febrero de 2021). CCMBenchmark. ¿Qué es un puente de red y para qué sirve? <https://es.ccm.net/contents/296-equipos-de-red-puentes>
- López, F. (2020). El estándar IEEE 802.11 Wireless LAN. <https://www.dit.upm.es/~david/tar/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf>

- Martinez, J. (2019). Medios de Transmisión: Guiados y no guiados.
- Mas tecnologia PC. (2 de 4 de 2021). Access Point Tp-Link Tl-Wa901nd N450 Mbps 3 Antenas. Recuperado el 22 de 8 de 2021, de *Mas tecnologia PC computadoras*: <http://www.mastecnologiapc.com/shop/access-point-tp-link-tl-wa901nd-n450mbps-3-antenas/>
- Mas tecnologia PC. (2 de 4 de 2021). Access Point Tp-Link Tl-Wa901nd N450 Mbps 3 Antenas. Recuperado el 22 de 8 de 2021, de *Mas tecnologia PC computadoras*: <http://www.mastecnologiapc.com/shop/access-point-tp-link-tl-wa901nd-n450mbps-3-antenas/>
- Mas tecnologia PC. (2 de 4 de 2021). Access Point Tp-Link Tl-Wa901nd N450 Mbps 3 Antenas. Recuperado el 22 de 8 de 2021, de *Mas tecnologia PC computadoras*: <http://www.mastecnologiapc.com/shop/access-point-tp-link-tl-wa901nd-n450mbps-3-antenas/>
- Mas tecnologia PC. (2 de 4 de 2021). Access Point Tp-Link Tl-Wa901nd N450 Mbps 3 Antenas. Recuperado el 22 de 8 de 2021, de *Mas tecnologia PC computadoras*: <http://www.mastecnologiapc.com/shop/access-point-tp-link-tl-wa901nd-n450mbps-3-antenas/>
- Mas tecnologia PC. (2 de 4 de 2021). Access Point Tp-Link Tl-Wa901nd N450 Mbps 3 Antenas. Recuperado el 22 de 8 de 2021, de *Mas tecnologia PC computadoras*: <http://www.mastecnologiapc.com/shop/access-point-tp-link-tl-wa901nd-n450mbps-3-antenas/>
- Mas tecnologia PC. (2 de 4 de 2021). Access Point Tp-Link Tl-Wa901nd N450 Mbps 3 Antenas. Recuperado el 22 de 8 de 2021, de *Mas tecnologia PC computadoras*: <http://www.mastecnologiapc.com/shop/access-point-tp-link-tl-wa901nd-n450mbps-3-antenas/>
- Mas tecnologia PC. (2 de 4 de 2021). Access Point Tp-Link Tl-Wa901nd N450 Mbps 3 Antenas. Recuperado el 22 de 8 de 2021, de *Mas tecnologia PC computadoras*: <http://www.mastecnologiapc.com/shop/access-point-tp-link-tl-wa901nd-n450mbps-3-antenas/>
- Matango, F. (2016). Componentes de voz sobre IP. Server VoIP: <http://www.servervoip.com/blog/tag/osi/>.
- Matango, F. (2016). Redes de nueva generación.
- MetaSwitch. (21). What is Open Shortest Path First (OSPF)?

- Meyers, M. (2009). Administración y Mantenimiento de Redes de computadoras. España: Anaya.
- Mezquita, T. (6 de January de 2021). Domain Name System (DNS). Cyber-Hoot: <https://cyberhoot.com/cybrary/domain-name-system-dns/>
- Mocan, T. (30 de August de 2019). ¿Qué Es IPSec y Cómo Funciona? Cactus-VPN. . Obtenido de <https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/que-es-ipsec/>
- Montañana, R. (2017). Arquitectura de LAN conmutada.
- Muñoz, J. (2017). Planificación y Administración de redes. Concepto de capa física. Tipos de señales. <https://planificacionadministracionredes.readthedocs.io/es/latest/Tema03/Teoria.html>
- Nat Apuntes. (25 de March de 2020). IEEE 802.15 – Body & Personal Area Networks. <https://www.natapuntes.es/ieee-802-15/>
- Netink. (2020). REDES IT Y SUS CLASIFICACIONES. Recuperado el 2021, de Netink St: <https://www.netinkst.com/notas/redesit.html>
- NOW, I. (31 de 07 de 2018). ¿Qué son las WAN y hacia dónde se dirigen? Recuperado el 31 de 07 de 2021, de RevistaITnow: <https://revistaITnow.com/que-son-las-wan-y-hacia-donde-se-dirigen/>
- OCompra. (2019). Compra. <https://www.ocompra.com>
- Odom, W. (2016). CCENT/CCNA. Recuperado el 30 de 07 de 2021, de Packtpub: https://subscription.packtpub.com/book/networking_and_servers/9781788621434/1/ch01lvl1sec04/types-of-computer-networks
- Oracle. (2010). Oracle-Guía y administración del sistema (Modelo de referencia OSI). <https://docs.oracle.com/cd/E19957-01/820-2981/ipv-8/index.html>
- Passos, S., Kazah, H., & Galperin, M. (2 de August de 1999). Mercado Libre. Obtenido de <https://www.mercadolibre.com.ec>
- Passos, S., Kazah, H., & Galperin, M. (2 de August de 1999). Mercado Libre. <https://www.mercadolibre.com.ec>
- Payares, B. (2004). Conmutación, enrutamiento y tecnologías WAN. Repositorio UTB, <http://repositorio.utb.edu.co/handle/20.500.12585/1743>. Obtenido de Repositorio UTB.
- Pérez, S. (enero de 2017). ResearchGate. Dispositivos y Protocolos en redes LAN y WAN. https://www.researchgate.net/figure/Dispositivos-de-red-en-relacion-al-modelo-OSI_fig69_312029712
- Piquer, S., & Mora , A. (14 de 1 de 2020). PCWorld. <https://www.pcworld.es/articulos/otros-dispositivos/hub-multipuerto-recomendaciones-3674729/>

- PNGWINGLE. (2020). PNGWINGLE. Hub-concentrador. <https://www.pn-gwing.com/es>
- Programación7. (6 de junio de 2016). Programación7-Universidad Latina Sede Azuero (Características principales del modelo OSI). <https://programacion7ulatlebs3096.wordpress.com/2016/06/06/caracteristicas-principales-del-modelo-osi/>
- Rekhter, Y., Cisco Systems, & Moskowitz, B. (Febrero de 1996). IETF. RFT 1981, Address Allocation for Private Internets: <https://datatracker.ietf.org/doc/html/rfc1918>
- Salazar, J. (2017). REDES INALÁMBRICAS. Recuperado el 2021, de Upcommons: https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf
- Sathyaranayanan, A. (2020). Types of Network. Educba: <https://www.educba.com/types-of-network/>
- Smith. (2001). What TCP/IP Protocol Headers Can Tell U About the Web. <https://sci-hub.se/https://doi.org/10.1145/378420.378789>
- Software Lab. (30 de 7 de 2021). Software Lab.org. <https://softwarelab.org/es/que-es-un-router-y-un-modem-en-que-se-diferencian/>
- SoporteIncared. (s.f.). SwitchCapa2. *Incared*:<https://incared.net/2015/08/13/definicion-de-switch-capa-2/>
- Spralls III, S. A. (2011). Extranet Use and Building Relationship Capital in Interfirm Distribution Networks: The Role of Extranet Capability. Science-Direct, 59 - 74.
- Stallings, W. (2015). Comunicaciones y Redes de Computadores. España: Prentice Hall.
- Subnet Calulator. (s.f.). IP Subnet Calculator. <https://www.calculator.net/ip-subnet-calculator.html>
- Tanenbaum, A. (2012). Redes de Computadores. Ambato: Pearson Education.
- Tanenbaum, A. (2012). Redes de Computadoras. Recuperado el 2021, de Bibliotecavirtualapure: https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_computadoras-freelibros-org.pdf
- Tanenbaum, A. (2012). Redes de Computadoras. Pearson, 328.
- Tanenbaum, A. S. (2003). Computer Networks. Amsterdam: Pearson Educación.
- Telectrónica. (2019). Cisco IOS, Imágenes para GNS3 Dynamips. Telectrónica: <https://www.teletronika.com/descargas/cisco-imagenes-ios-para-gns3-dynamips-y-vm/>

- Telpro Madrid. (5 de April de 2019). Fibra óptica monomodo y multimodo
- Que es y en que se diferencian. TELPRO: <https://telpromadrid.eu/que-es-la-fibra-optica-monomodo-y-multimodo/>
- TipsMake. (2019). Learn about Personal Area Network. <https://tipsmake.com/learn-about-personal-area-network-pan>
- Toad. (2005). Introducción a TCP/IP. Características de TCP: https://www.um.es/docencia/barzana/DIVULGACION/INFORMATICA/Introduccion_a_TCPIP.pdf
- Tp-link. (15 de 3 de 2020). RE305. Recuperado el 22 de 8 de 2021, de Tp-link: <https://www.tp-link.com/ec/home-networking/range-extender/re305/>
- Urrutia, A. A. (2018). Convergencia Revista de Ciencias Sociales. <https://convergencia.uaemex.mx/article/view/9562>
- Velasco, L. (2016). Introducción a TCP y UDP. <http://capasdesaia.blogspot.com/2016/06/introduccion-tcp-y-udp.html>
- Verizon. (s.f.). What is Fiber Optics - Definition, Meaning & Explanation. <https://verizon.com/info/definitions/fiber-optics/>
- Web. (21). What's inside a router?
- Worton. (14 de February de 2022). ¿Cuál es la diferencia entre el Switch de Capa 2 y el Switch de Capa 3? e FS | community: <https://community.fs.com/es/blog/layer-2-switch-vs-layer-3-switch-what-is-the-difference.html>
- XarCom. (17 de March de 2019). Instalación y configuración de GNS3 con GNS3 VM . Xarcom.net: <https://www.xarcom.net/blog/installacion-y-configuracion-de-gns3-con-gns3-vm/>
- Yáñez, A., & Janine, D. (2002). BIBDIGITAL. Generador y Colector de paquetes UDP: <https://bibdigital.epn.edu.ec/bitstream/15000/5387/1/T1920.pdf>
- Zona112. (11 de May de 2019). WI-FI 2.4GHZ VS WI-FI 5GHZ. DIFERENCIAS. <https://www.zona112.com/noticia/wi-fi-24ghz-vs-wi-fi-5ghz-diferencias>
- ZONAXIAOMI. (13 de julio de 2021). ADSLZONE. Diferencias entre router y modem-¿Para qué sirve cada uno? <https://www.adslzone.net/reportajes/internet/modem-vs-router/>

Redes de computadoras

Las redes de computadoras, en esencia, forman parte del diario vivir de las personas y las empresas. Los clientes requieren estar conectados local o remotamente para realizar sus actividades estudiantiles, profesionales o laborales. Las organizaciones, por su parte, necesitan ofrecer sus productos y servicios utilizando interfaces Web que le provee la red Internet para mejorar su productividad y reducir sus costos de operación. Las personas utilizan día a día los servicios y aplicaciones que les brindan las redes celulares y los dispositivos móviles que hacen uso de la interconectividad y las tecnologías de las redes de telecomunicaciones. El mundo está conectado en el ciberespacio.

Esta obra está orientada al estudio y aprendizaje de las redes de computadoras para estudiantes, docentes, investigadores y profesionales, desde sus fundamentos hasta su diseño, con un enfoque teórico-práctico utilizando varios recursos didácticos en los que se incluye software especializado, así como herramientas de simulación de redes de código abierto y libre distribución.

El libro que usted, estimado lector, tiene en sus manos está fundamentado en muchos años de actividad docente, investigativa y de ejercicio profesional del autor. En suma, se presenta una estupenda obra que coadyuvará en formar profesionales o en especialistas en redes de computadoras.

Finalmente, es preciso agradecer a todos quienes ayudaron en la revisión, corrección idiomática, diagramación y publicación de este libro, a los estudiantes y profesionales que inspiraron y colaboraron en la materialización del mismo.

El autor

ISBN: 978-9942-765-72-7



9 789942 765727

