

# ÍNDICE

<b>Prefacio</b> .....	<b>XV</b>
<b>Capítulo 1. Redes informáticas. Conceptos básicos</b> .....	<b>1</b>
Introducción a las redes informáticas .....	1
Estándares de comunicación: TCP/IP y OSI .....	2
Modelo TCP/IP.....	3
Capa de aplicación.....	4
Capa de transporte.....	5
Capa de Internet.....	7
Capa de acceso a la red .....	7
Proceso de encapsulación y envío de datos .....	8
Modelo OSI.....	10
Capa 7 - Aplicación .....	12
Capa 6 - Presentación .....	12
Capa 5 - Sesión .....	12
Capa 4 - Transporte .....	12
Capa 3 - Red.....	14
Capa 2 - Enlace de datos.....	14
Capa 1 - Física .....	16

Comparación entre el modelo OSI y TCP/IP .....	17
Redes LAN Ethernet.....	18
Evolución de las redes LAN.....	20
LAN Ethernet 10BASE-T .....	23
Mejoras de rendimiento gracias al switch .....	24
Elementos en el diseño de una LAN Ethernet .....	27
Dominios de colisión.....	27
Dominios de broadcast.....	28
Importancia de los dominios de colisión y broadcast.....	29
VLAN (Virtual Lan).....	30
Redundancia.....	31
Diseños y arquitecturas de red.....	33
Cableado y conectores de red .....	36
Protocolos de enlace de datos.....	42
Ethernet framing .....	42
Direccionamiento .....	43
Detección de errores .....	44
Enrutamiento y direccionamiento IP.....	45
Enrutamiento.....	46
Lógica de enrutamiento.....	47
Paquetes y cabecera IP.....	48
Protocolos de enrutamiento.....	49
Direccionamiento IP .....	51
Protocolos TCP y UDP.....	52
TCP ( <i>Transmission Control Protocol</i> ).....	52
Utilización de puertos.....	53
Multiplexación.....	54
Establecimiento y finalización de la conexión .....	55
Recuperación de errores .....	56
Control de Flujo - Ventana deslizante.....	58

Reensamblaje de datos en el destino .....	59
UDP ( <i>User Datagram Protocol</i> ).....	59
Diferencias entre TCP y UDP.....	60
Redes WAN.....	60
Redes WAN privadas: líneas arrendadas .....	61
Protocolo HDLC ( <i>High-Level Data Link Control</i> ).....	62
Redes WAN privadas: Ethernet WAN .....	63
Fundamentos básicos de virtualización.....	64
Software as a Service ( <i>SaaS</i> ).....	70
Infraestructure as a Service ( <i>IaaS</i> ).....	70
Platform as a Service ( <i>PaaS</i> ) .....	71
<b>Capítulo 2. Comunicación en capa 2. Modo de operar y configuración de switches Cisco .....</b>	<b>73</b>
Evolución en dispositivos de interconexión.....	73
Switchs – Características y modo de operar.....	74
Tabla de MAC .....	76
Reenvío de tramas.....	77
Procesamiento interno en switchs Cisco .....	78
Evitar bucles de capa 2 mediante STP .....	79
Acceso y configuración de interfaces .....	79
Acceso a la configuración a través de consola.....	80
Modos de operar .....	81
Modos de configuración .....	82
Modificar el nombre del dispositivo .....	83
Comandos show y debug.....	83
Ficheros de configuración en IOS .....	83
Configuración de interfaces.....	87
Configuración básica de Interfaces.....	87
Verificar la tabla de MAC.....	91
Configuración de IP para acceso remoto.....	93

Protocolos de autodescubrimiento en capa 2 .....	93
CDP ( <i>Cisco Discovery Protocol</i> ) .....	94
LLDP ( <i>Link Layer Discovery Protocol</i> ) .....	95
VLANs (Virtual LANs) .....	95
Configuración y verificación de VLANs .....	97
Enlaces troncales .....	98
Configuración y verificación de enlaces troncales .....	101
Lista de VLANs permitidas en enlaces troncales .....	102
Enrutamiento entre VLANs .....	103
Modo de operar de las interfaces .....	106
VTP ( <i>VLAN Trunking Protocol</i> ) .....	107
Configuración y verificación de VTP .....	108
Spanning Tree Protocol (STP) .....	110
Modo de operar de STP .....	113
Roles del switch .....	114
Roles y estado de interfaz .....	118
RSTP (Rapid-STP) .....	122
Roles y estado de interfaz en RSTP .....	123
Protocolos propietarios de Cisco: PVST+ y RPVST+ .....	125
Configuración de RPVST+ .....	126
Etherchannels .....	128
Configuración manual de un etherchannel .....	129
Configuración de un etherchannel mediante autonegociación .....	130
Balanceo de carga en etherchannels .....	132
<b>Capítulo 3. Conectividad IP. Protocolos IPv4 e IPv6 .....</b>	<b>135</b>
Protocolo IPv4 .....	135
Formato de direcciones en IPv4 .....	136
Direcciones IP unicast reservadas en IPv4 .....	139
Subnetting en IPv4 .....	140
Número de subredes necesarias .....	141

Selección del rango de direcciones.....	142
Implementación de subredes en la topología real .....	148
Ejercicios prácticos de subnetting .....	149
Protocolo IPv6 .....	156
Formato de direcciones en IPv6 .....	156
Longitud y prefijo de red .....	158
Enrutamiento .....	159
Direccionamiento y subnetting en IPv6.....	160
Global unicast.....	161
Unique local.....	167
Tipos de direcciones IPv6 .....	170
Configuración automática de IPv6 en hosts .....	172
NDP - Neighbor Discovery Protocol.....	172
DHCPv6: Modo de operar.....	175
Verificar conectividad IP .....	179
<b>Capítulo 4. Comunicación en capa 3. Configuración de routers Cisco .....</b>	<b>181</b>
Instalación y configuración inicial.....	181
Configuración IP de interfaces Ethernet.....	183
Estudio de la tabla de rutas .....	185
Rutas directamente conectadas .....	186
Enrutamiento Inter-VLAN .....	187
Rutas estáticas.....	190
Rutas estáticas por defecto .....	192
Protocolos de enrutamiento .....	194
Protocolos de enrutamiento IGP .....	195
OPSFv2: Algoritmo y modo de operación.....	199
Algoritmo aplicado en OSPF .....	200
Intercambio de rutas en enlaces punto a punto.....	200
Intercambio de rutas en entornos multiacceso.....	202
Cálculo de rutas .....	204

Modo de operación .....	205
Descubrimiento de vecinos .....	205
Distribución en áreas .....	206
Tipos de LSA.....	208
Configuración de OSPFv2 en routers Cisco.....	208
Protocolos y servicios IP .....	212
DHCP en redes IPv4 .....	213
NAT ( <i>Network Address Translation</i> ) .....	216
NAT estático .....	218
NAT dinámico .....	219
NAT con sobrecarga o PAT.....	221
NTP ( <i>Network Time Protocol</i> ).....	225
SNMP .....	226
QoS ( <i>Quality of Service</i> ).....	227
Clasificación e identificación de tráfico .....	229
Gestión de envío.....	232
Protocolos FTP y TFTP.....	234
FHRP ( <i>First-Hop Redundancy Protocols</i> ) .....	235
<b>Capítulo 5. Fundamentos de seguridad.....</b>	<b>237</b>
Conceptos básicos .....	237
Amenazas de seguridad: Tipos de ataque .....	238
Fase inicial: Reconocimiento .....	238
Ataque de denegación de servicio.....	239
Ataques man-in-the-middle.....	240
Ataques de desbordamiento de buffer.....	241
Malware.....	241
Ataques a contraseñas .....	242
Ingeniería social .....	243
Dispositivos y protocolos de seguridad .....	245
Firewalls.....	245

IPS.....	248
Protocolos de monitorización: Syslog.....	249
Protocolos AAA.....	250
Seguridad en el acceso a dispositivos Cisco.....	251
Autenticación mediante contraseña .....	251
Autenticación mediante usuario y contraseña .....	254
Acceso remoto mediante SSH .....	255
Seguridad en capa 2 .....	256
DHCP Snooping.....	256
Configuración de DHCP Snooping.....	259
Dynamic ARP Inspection.....	261
Configuración de DAI en switchs Cisco .....	262
Port security .....	264
Seguridad en capa 3 .....	267
Listas de control de acceso.....	267
ACL estándar numerada .....	268
Lógica aplicada en una ACL estándar.....	268
Crear una ACL estándar .....	269
Configuración de ACL estándar numerada .....	271
ACL extendida numerada .....	273
Filtrado basado en protocolo y direcciones de origen y destino .....	273
Filtrado basado en números de puerto TCP y UDP.....	274
Configuración de ACL extendida numerada .....	276
ACLs nombradas .....	278
Redes WAN: Seguridad en el acceso remoto .....	280
Protocolos de seguridad: IPSec y SSL.....	283
IPSec .....	283
SSL .....	285
<b>Capítulo 6. Redes inalámbricas .....</b>	<b>287</b>
Conceptos básicos .....	287

Transmisión RF .....	287
Dispositivos.....	290
Puntos de acceso .....	290
Repetidores .....	291
Controladora .....	291
Workgroup Bridge .....	292
Outdoor Bridge.....	292
Topologías inalámbricas .....	292
Independent basic service set .....	293
Basic Service Set (BSS) .....	293
Distribution system.....	294
Extended Service Set .....	296
MESH .....	297
Arquitecturas inalámbricas Cisco .....	297
Arquitectura basada en APs autónomos .....	297
Arquitectura basada en la nube .....	298
Arquitectura basada en controladoras.....	300
Seguridad en redes inalámbricas.....	301
Protocolos de autenticación .....	302
802.1x/EAP .....	303
Protocolos de privacidad e integridad .....	304
TKIP.....	305
CCMP .....	306
GCMP.....	306
WPA, WPA2 y WPA3.....	306
<b>Capítulo 7. Arquitecturas basadas en software y automatización .....</b>	<b>309</b>
Arquitecturas de red: Modelo tradicional .....	309
Arquitecturas de red: Modelo SDN .....	311
Interfaz SBI ( <i>Southbound Interface</i> ).....	313
Interfaz NBI ( <i>Northbound Interface</i> ).....	313



---

Comunicación entre APIs: REST y JSON .....	314
REST-Based APIs .....	315
Estandarización de datos: JSON.....	318
Cisco SDA (Software-Defined Access).....	321
DNA Center: Comunicación a través de la SBI .....	322
SDA Underlay.....	322
SDA Overlay .....	324
SDA Fabric.....	326
DNA CENTER: Comunicación a través de la NBI.....	327
Gestión de configuraciones: Ansible, Puppet y Chef .....	328
Ansible .....	329
Puppet .....	330
Chef .....	331
Comparativa entre Ansible, Puppet y Chef.....	331
<b>Índice analítico .....</b>	<b>333</b>

# PREFACIO

En el ámbito informático, las certificaciones constituyen uno de los títulos más importantes y reconocidos a nivel mundial. Gracias a ellas, empresas líderes en el sector acreditan que sus poseedores disponen de los conocimientos y habilidades necesarios para ejercer laboralmente las funciones de una determinada rama profesional. Microsoft, Cisco, HP, VMWare, Juniper, Fortinet, Oracle, IBM, CheckPoint o Citrix son solo algunos ejemplos de compañías que basan su formación en torno a certificaciones.

En cuanto a redes y seguridad se refiere, el CCNA adquiere un valor especial, primero, porque abarca desde los conceptos más básicos de *routing* y *switching* hasta protocolos realmente avanzados, y segundo, porque su título es acreditado por Cisco, compañía líder en el sector de redes y comunicaciones.

El objetivo principal de este libro consiste en dotar a sus lectores de los conocimientos necesarios para afrontar con éxito el examen de certificación 200-301 de Cisco, así como capacitarlos para implementar, asegurar y administrar una red corporativa de tamaño medio, aplicando sobre la misma los protocolos y configuraciones más adecuados. Su contenido, dividido en 7 capítulos, incluye la totalidad del temario oficial requerido para el CCNA, ofreciendo al lector explicaciones detalladas sobre cada uno de los conceptos necesarios.

En cuanto al examen de certificación, denominado como *Cisco Certified Network Associate v1.0 (CCNA 200-301)*, de 120 minutos de duración y tipo test, Cisco incluye los siguientes *topics*, asignando a cada uno de ellos un porcentaje sobre la nota total.

<b>Topic</b>	<b>Nota</b>
<i>Network Fundamentals</i>	20%
<i>Network Access</i>	20%
<i>IP Connectivity</i>	25%
<i>IP Services</i>	10%
<i>Security Fundamentals</i>	15%
<i>Automation and Programmability</i>	10%

\*Fuente oficial: <https://learningnetwork.cisco.com/s/ccna-exam-topics>

Que, a su vez, están incluidos en los siguientes capítulos del presente libro:

<b>Topic</b>	<b>Capítulo</b>
<i>Network Fundamentals</i>	Capítulo 1
<i>Network Access</i>	Capítulos 2 y 6
<i>IP Connectivity</i>	Capítulos 3 y 4
<i>IP Services</i>	Capítulo 4
<i>Security Fundamentals</i>	Capítulo 5
<i>Automation and Programmability</i>	Capítulo 7

Con ello, su estudio cubre la totalidad de fundamentos necesarios para obtener la certificación e iniciar una carrera en el ámbito de redes y comunicaciones.

## El autor

Daniel Pérez Torres nació en Santa Cruz de Tenerife en 1983. Estudió en la administración de sistemas informáticos, especializándose a posteriori en la rama de redes y seguridad, en cuyo campo posee las certificaciones Cisco CCNP, CCNA, CCNA Security, Juniper JNCIA y CompTIA Security+, entre otros títulos. Así mismo, instruye en dichas certificaciones y colabora en diferentes blogs y portales tecnológicos.

Su trayectoria profesional ha estado vinculada al servicio de la administración pública, donde actualmente pertenece al área de redes y comunicaciones, trabajando a diario con las tecnologías más avanzadas del sector como Cisco, Palo Alto, Extreme Networks, FortiNet, ForcePoint o F5.

# REDES INFORMÁTICAS. CONCEPTOS BÁSICOS

# 1

## **INTRODUCCIÓN A LAS REDES INFORMÁTICAS**

---

El objetivo principal del CCNA consiste en dotar a sus aspirantes de los conocimientos necesarios para diseñar y administrar una red de tamaño medio de manera segura y eficiente. Para lograrlo, Cisco basa su estudio en análisis detallados de cada uno de los elementos que la conforman, abarcando desde las nociones más básicas hasta los protocolos más avanzados, comenzando por un concepto esencial. ¿Qué es una red?

Una red puede ser definida como la comunicación entre un conjunto de miembros que hacen uso del mismo medio compartido con el fin de intercambiar información y recursos entre sí. Este concepto, aplicado al ámbito informático, se lleva a cabo mediante la interconexión de dispositivos, donde cada uno de ellos tomará un rol y la totalidad de los mismos definirá el tamaño y propósito final. Dicha comunicación resulta viable gracias a la aplicación de diferentes medios, tanto físicos como lógicos. Los primeros hacen referencia a elementos de hardware, como cableado y tarjetas de red, mientras que los segundos, al software y protocolos necesarios para poder llevar a cabo la comunicación.

En cuanto al tamaño, la red más básica se compone de dos equipos, físicamente en el mismo lugar y conectados entre sí mediante un único cable. Mientras, la más compleja puede albergar millones de hosts ubicados a lo largo del planeta, logrando comunicarse gracias a multitud de dispositivos intermediarios como routers, switches, o firewalls, entre muchos otros. Un ejemplo bastante claro de ello es Internet.

Evidentemente, este nivel de complejidad nace como fruto de la evolución llevada a cabo a lo largo del tiempo. En este sentido, una de las primeras redes de computadoras creadas y que sin duda establece el origen de las actuales fue ARPANET, desarrollada en 1968 por el departamento de defensa de EE.UU. y utilizada para la comunicación privada entre diferentes instituciones del país. A raíz de ella, el estudio y avance de esta tecnología ha sufrido un crecimiento exponencial hasta la actualidad, donde cualquier dispositivo puede acceder a información ubicada en cualquier parte del planeta.

Por último, una red puede ser apreciada de diferentes maneras. Para un usuario simplemente significa obtener acceso a determinados recursos o servicios, como aplicaciones corporativas o Internet. Sin embargo, desde el punto de vista de un administrador resulta más complejo, incluyendo aquellos dispositivos encargados de la comunicación, configuraciones, seguridad, diseño, protocolos, servidores, etc.

No cabe duda que el rol de un aspirante a CCNA debe ser el de administrador, por tanto, y para comenzar, resulta imprescindible realizar un estudio de los modelos de comunicación TCP/IP y OSI, los cuales definen el modo de operar y las características necesarias para que la transmisión de datos pueda llevarse a cabo de manera eficaz y fiable.

## **ESTÁNDARES DE COMUNICACIÓN: TCP/IP Y OSI**

---

La finalidad de una red informática consiste en habilitar la comunicación entre todos los dispositivos que la componen, pero ¿cómo es posible llevarla a cabo? Para lograrlo resulta necesario establecer una serie de “normas” que se deberán ejecutar de la misma manera en todos los sistemas. Gracias a ello, los datos generados por cualquier host pueden ser recibidos e interpretados por el receptor de los mismos. Con dicho objetivo nacen los modelos de comunicación TCP/IP y OSI, desarrollados para definir los estándares, procedimientos y protocolos a aplicar para que la creación, transporte y entrega de datos se lleve a cabo de igual manera en cada dispositivo, sin importar ni el fabricante ni los elementos de hardware presentes en el mismo. OSI fue desarrollado por la agencia ISO (*International Organization for Standardization*) mientras que TCP/IP por voluntarios de varias universidades, siendo ambos modelos abiertos, es decir, sin coste económico ni limitaciones sobre su implementación.

Hoy día resulta prácticamente imposible encontrar dispositivos que no los soporten. Todos los sistemas operativos, incluyendo aquellos presentes en *smartphones* o *tablets*, lo implementan. Entonces, ¿cuál utilizar? Normalmente dependerá de la aplicación o sistema, pero, de ambos, el más común resulta TCP/IP, primero, porque se estandarizó con mayor rapidez, y segundo, porque la productividad de los datos está considerada más eficiente que en OSI.

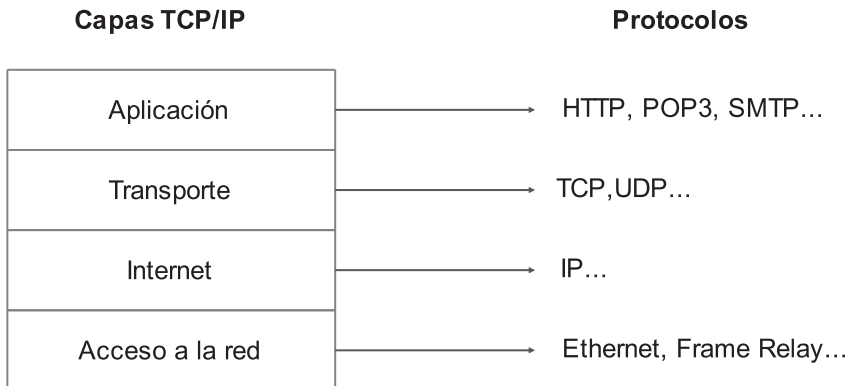
A lo largo de la historia se han desarrollado diversos estándares con el mismo propósito, como SNA (*System Network Architecture*), creado por IBM. Sin embargo, no han tenido éxito ni continuidad por tratarse de modelos propietarios de dichas compañías, debido a lo cual su utilización supone un coste económico, y lo que es peor, las modificaciones y actualizaciones del mismo solo pueden ser llevadas a cabo por la compañía en cuestión.

## Modelo TCP/IP

TCP/IP es considerado el estándar por excelencia para llevar a cabo la comunicación en redes informáticas. Su función consiste en definir el procedimiento necesario para que los datos generados en el origen sean entregados e interpretados en el destino. Para lograrlo hace uso de diferentes protocolos, cada uno de ellos con una función específica, las cuales serán analizadas a lo largo del capítulo.

Una manera para comprenderlo mejor es comparándolo con la telefonía. Si en nuestro hogar disponemos de un teléfono antiguo y lo sustituimos por otro de última generación, al conectarlo a la línea telefónica permitirá realizar y recibir llamadas de la misma manera que el anterior, no serían necesarias ni configuraciones especiales ni la sustitución del cableado. Ello es posible gracias a que ambos hacen uso de los mismos protocolos de comunicación, los cuales han sido definidos y aprobados para su aplicación a nivel mundial. Lo mismo ocurre con TCP/IP, cualquier dispositivo que haga uso de él podrá comunicarse con otros que también lo hagan sin importar el fabricante, el modelo o el lugar donde se encuentren.

Como otros estándares de red, TCP/IP basa su modo de operar en capas, cada una de ellas con una función específica donde se incluyen los protocolos necesarios para poder llevar a cabo diferentes tipos de comunicación. Estas son:



*Fig. 1-1 Capas en TCP/IP y sus protocolos.*

Los datos son generados en la capa de aplicación y enviados sucesivamente hacia las capas inferiores, aplicando cada una de ellas el protocolo correspondiente. Una vez finalizado el proceso, dichos datos son enviados al medio y recibidos por el destinatario.

Una de las grandes ventajas de TCP/IP es que es un estándar abierto, de tal manera que, si fuera necesaria la inclusión de algún nuevo protocolo, podría llevarse a cabo sin problema. Un claro ejemplo de ello fue la aparición de Word Wide Web (www), hecho que conllevó agregar HTTP en la capa de aplicación, cuyo propósito consiste en enviar solicitudes a servidores web para que estos respondan con el contenido requerido.

El proceso y las funciones llevadas a cabo en cada una de las capas son los siguientes.

## **CAPA DE APLICACIÓN**

Es la encargada de proporcionar los protocolos necesarios a servicios o aplicaciones para que estos puedan iniciar el proceso de comunicación en red. Para facilitar la comprensión tomaremos como ejemplo el intercambio de mensajes entre un cliente y un servidor web, con el fin de analizar cómo son manipulados los datos en cada una de las capas para luego ser enviados al medio.

En este caso el proceso lo inicia el cliente a través de un navegador, por ejemplo, Firefox, haciendo uso del protocolo HTTP en la capa de aplicación. ¿Qué sucede cuando un dispositivo desea enviar una solicitud a un servidor web? Realmente lo que se generan son una serie de mensajes definidos por el propio protocolo, con el fin de que ambos sistemas se “entiendan”, logrando con ello que la comunicación

concluya con éxito. En el lado del cliente se generan mensajes GET, mientras que el servidor responde a estos mediante algún código (como el 200, con significado OK), además entra en juego otro protocolo, HTML, que define el formato del documento que es enviado.

La comunicación a nivel de capa de aplicación sería la siguiente...

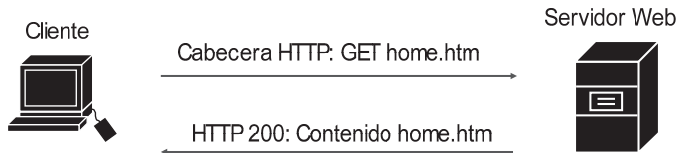


Fig. 1-2 Proceso inicial de comunicación HTTP, capa de aplicación.

En este caso, el navegador ha solicitado el documento “*home.htm*” y ha obtenido como respuesta el código 200. Ello significa que, efectivamente, dicho documento se encuentra almacenado en el servidor, que será enviado posteriormente. Cualquier otra circunstancia daría como resultado la generación de otro código, siendo el más común el 404, utilizado para indicar que el contenido solicitado no se encuentra disponible (*Page not Found*).

En HTTP, el cliente genera una cabecera, que incluye información y datos propios de la capa de aplicación. Esta será recibida, analizada y respondida por su homóloga en el destino. Este modo de operar también se aplica al resto de capas, es decir, los datos agregados por cada una de ellas solo serán analizados y comprendidos por la misma en ambos sistemas (cliente y servidor).

La capa de aplicación no identifica al software en sí, sino a los protocolos que se ejecutan en él.

## CAPA DE TRANSPORTE

Una vez que la capa de aplicación ha generado sus datos los envía a la capa de transporte, la cual se encarga de diferentes funciones, entre las que se encuentra identificar la aplicación a la que va dirigida la comunicación. Para ello hace uso de dos protocolos, TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*), ambos analizados en profundidad en este mismo capítulo.

Continuando con el ejemplo anterior, ¿qué ocurriría si la solicitud enviada por el cliente no es recibida por el servidor, o viceversa? ¿Cómo determina un dispositivo que sus datos han sido recibidos por el destinatario? TCP/IP requiere un mecanismo