ÍNDICE

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.

Topic	Nota
Network Fundamentals	20%
Network Access	20%
IP Connectivity	25%
IP Services	10%
Security Fundamentals	15%
Automation and Programmability	10%

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

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

Topic	Capítulo
Network Fundamentals	Capítulo 1
Network Access	Capítulos 2 y 6
IP Connectivity	Capítulos 3 y 4
IP Services	Capítulo 4
Security Fundamentals	Capítulo 5
Automation and Programmability	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.

1 REDES INFORMÁTICAS. CONCEPTOS BÁSICOS

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, switchs, 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 Standarization)* 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:

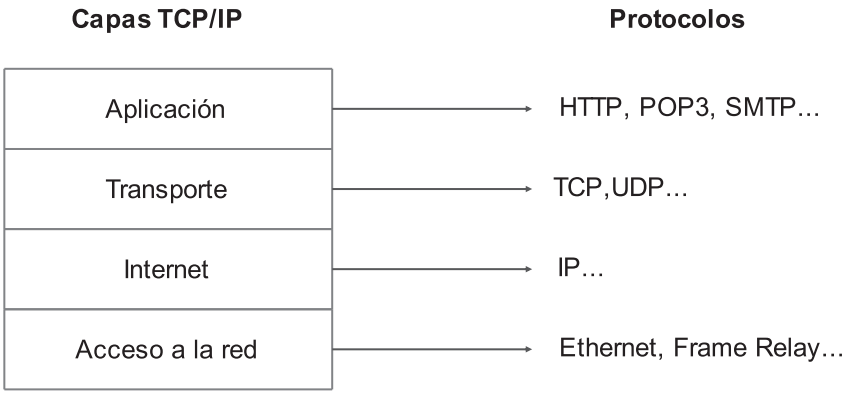

Fig. 1-1 Capas en TCP/IP y sus protocolos.

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…

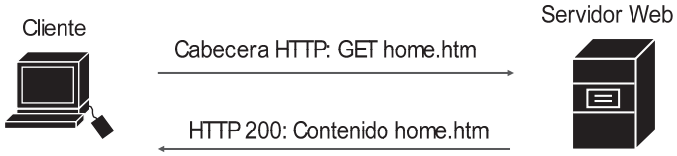

Fig. 1-2 Proceso inicial de comunicación HTTP, capa de aplicación.

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