Telemática I

Autor: Juan Carlos Ramirez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Telemática I / Juan Carlos Ramirez Zapata, / Bogotá D.C.,
Fundación Universitaria del Área Andina. 2017

978-958-5455-68-9

Catalogación en la fuente Fundación Universitaria del Área Andina (Bogotá).

Edición:
Fondo editorial Areandino
Fundación Universitaria del Área Andina
Calle 71 11-14, Bogotá D.C., Colombia
Tel.: (57-1) 7 42 19 64 ext. 1228
E-mail: publicaciones@areandina.edu.co
http://www.areandina.edu.co

Primera edición: noviembre de 2017

Corrección de estilo, diagramación y edición: Dirección Nacional de Operaciones virtuales
Diseño y compilación electrónica: Dirección Nacional de Investigación

Hecho en Colombia
Made in Colombia

Telemática I

Autor: Juan Carlos Ramirez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

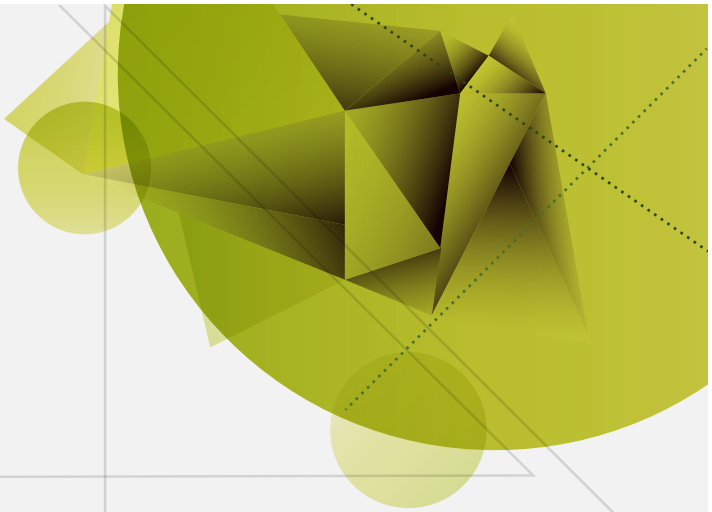
Índice

Índice

1

Unidad 1

Introducción a las redes de computadores



Telemática I

Autor: Juan Carlos Ramirez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

La primera unidad de Telemática se enmarca en una revisión teórica permanente de los principios de las redes de computadores a través del análisis de los componentes físicos, los requisitos de diseño de acuerdo a su cobertura, los protocolos y modelos de referencia a las que pueden estar sujetas.

La lectura y análisis permanente de este material permite una contextualización a nivel mundial conociendo la teoría general y la aplicación práctica en contextos específicos.

U1 Metodología

Este módulo provee a los estudiantes referentes teóricos sobre cada uno de los temas propuestos, los cuales deben leerse, analizarse y ampliarse con los recursos que se sugieren para profundización; también, encuentran ejercicios que deben desarrollarse para la comprensión y aplicación activa de conceptos abordados.

U1

Desarrollo temático

Introducción a las redes de computadores

Estándares de red

En el contexto de las modernas tecnologías, las relacionadas con las comunicaciones no escapan al cumplimiento de reglas propias de cada entorno; de la misma manera que sucede en las diferentes variantes de la comunicación humana, donde se requiere el cumplimiento de acuerdos previamente establecidos, el éxito de la comunicación soportada por plataformas tecnológicas, demanda el acatamiento de un conjunto de reglas o protocolos. Una vía de inicio para la comprensión del funcionamiento de redes de comunicaciones es tener presente la analogía con la comunicación humana; vemos por ejemplo que en una comunicación persona a persona existe emisor, receptor, método o modalidad de comunicación, lenguaje, rapidez de la comunicación, posible necesidad de confirmación, entre otros; elementos que, como veremos con mayor detalle, también están presentes en la comunicación a través de las redes de telecomunicación.

Entre las diferentes redes de telecomunicación están las redes de datos, creadas a través de la interconexión de un conjunto de computadores y otros equipos con el fin de compartir información y recursos, estas redes varían en un amplio rango de tamaño y capacidad, pero todas deben cumplir con un conjunto de estándares, los cuales posibilitan la interoperabilidad de hardware y software creados por diferentes fabricantes.

Componentes físicos de redes de computadores

Los elementos físicos que componen las redes se clasifican en dispositivos finales, dispositivos intermedios y los medios a través de los cuales viaja la información.

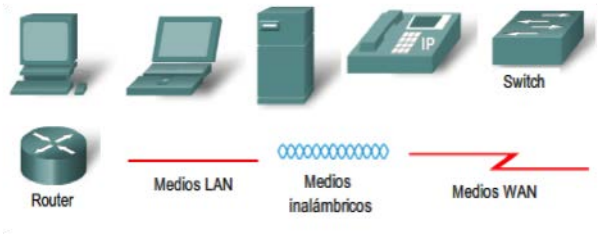


Imagen 1
Fuente: Propia, adaptada de currículo CCNA Exploration

Dispositivos finales

Los dispositivos finales en general son los computadores y dispositivos origen o destino de mensajes transmitidos a través de la red, pueden actuar como servidor, como cliente o ambos según el software que ejecuten. Un servidor brinda servicios a los clientes, por ejemplo, un servidor de correo electrónico permite el acceso a buzones de correo desde un equipo cliente.

Dispositivos intermedios

Son equipos que proporcionan conectividad a los equipos finales y a otros equipos intermedios. Generalmente los usuarios de las redes hacen uso de dispositivos finales, sin embargo éstos requieren conectarse a dispositivos como routers, switches, puntos de accesos y otros dispositivos, que son contribuyen con la conectividad.

Medios de red

La conexión entre dispositivos de la red, sea dispositivos finales o intermedios, se da a través de los medios de red. Los medios pueden inicialmente clasificarse en medios guiados y no guiados, entre los primeros encontramos los basados en cable de cobre, que transportan información en forma de señales eléctricas; los medios de fibra óptica, que transportan información en forma de señales de luz. Por su parte, los medios no guiados utilizan el aire como elemento de propagación, la información transmitida a través de medios no guiados viaja en forma de ondas electromagnéticas.

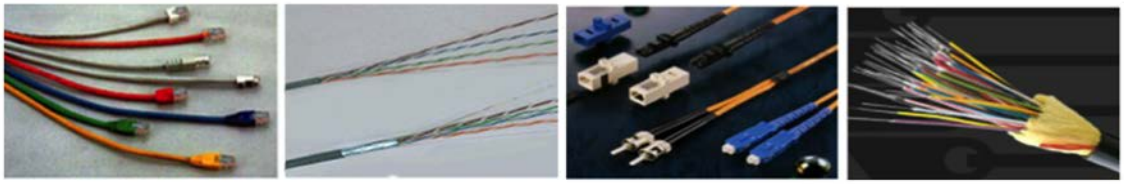


Imagen 2
Fuente: Propia, adaptada de currículo CCNA Exploration

La estructura física basada en estos elementos debe cumplir con el objetivo soportar los diferentes servicios utilizados por los usuarios, ello demanda que antes de la implementación de la red se considere factores de diseño que conlleven al éxito de la implementación.

Requisitos de diseños de las redes

Las modernas redes de computadores soportan múltiples aplicaciones y servicios al tiempo que tienen la capacidad de funcionar con diferentes infraestructuras físicas, para el logro de esto el diseño debe cumplir un conjunto de requisitos, entre los cuales se tiene los siguientes.

Tolerancia a fallas

La tolerancia a fallas de una red se refiere a la capacidad de limitar el perjuicio producto de una anomalía, al tiempo que pueda recuperarse rápidamente de las mismas. La tolerancia a fallas se soporta en redundancia de recursos, por ejemplo enlaces o rutas duplicadas y equipos de respaldo disponibles. El diseño debe ser tal que si un recurso falla, los procesos implementados están en capacidad de posibilitar la transmisión de información.

Escalabilidad

Un diseño escalable de una red permite su ampliación con relativa facilidad, de tal forma que puede soportar nuevos usuarios y aplicaciones sin deterioro del rendimiento. Un diseño jerárquico, en el que los equipos se organizan en grupos que a su vez forman parte de una estructura más compleja, y el uso de dispositivos modulares facilita la escalabilidad de la red.

Calidad de servicio (QoS)

El soporte de calidad de servicio en una red se relaciona con su capacidad de satisfacer diferentes niveles de exigencias de los servicios que presta, por ejemplo, la transmisión de voz y video en vivo presenta mayor demanda de recursos de forma ininterrumpida, lo que no sucede con transmisión de texto. El diseño de la red debe posibilitar que la estructura de la misma se adapte a exigencias variables satisfacción todas las necesidades.

Seguridad

Toda red debe contar con privacidad y seguridad en el intercambio de información. La rápida evolución de las redes, y las posibilidades que ofrece, da lugar al mismo tiempo a la necesidad de fortalecer medidas que protejan la seguridad frente a posibles amenazas, algunas de estas medidas se relacionan con implementación de políticas de acceso, encriptación o cifrado de información, necesidad de autenticación de usuarios, entre otras.

Clasificación de las redes según el área de cobertura

Una red puede ser tan simple como aquellas compuestas por dos computadores o tan grande y compleja que abarque uno o varios edificios, una ciudad, país o todo el planeta. Básicamente las redes se clasifican en Redes de Área Local (LAN) y Redes de Área Amplia (WAN).

Red de Área Local (LAN)

Una LAN (Local Área Network) es una red que abarca áreas geográficas limitadas a uno o varios edificios cercanos, administrada por una sola organización. Redes al interior de las empresas, y los hogares constituyen ejemplos de redes de área local.

Red de Área Amplia (WAN)

Dos o más redes LAN, separadas geográficamente, se pueden conectar a través de organizaciones Proveedoras de Servicios de Telecomunicaciones (TSP), con lo cual se configura una red WAN (Wide Area Network). Los TPS deben disponer de equipos especializados que permitan la interconexión de las diferentes redes locales. Cada empresa dueña de las diferentes LAN controla el funcionamiento de ellas internamente, pero el TPS es el responsable de la administración de la interconexión de las diferentes LAN de las empresas a las que les presta servicio.

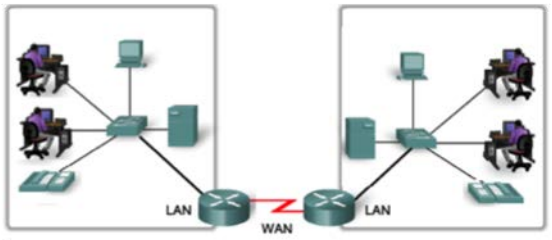


Imagen 3
Fuente: Propia, adaptada de currículo CCNA Exploration

Un interesante concepto asociado a las redes LAN y WAN es el de una Intranet, la cual es una conexión privada o interna de LAN y WAN con acceso permitido sólo al personal de la empresa. La figura siguiente muestra representa la conexión de dos redes LAN formando una WAN.

La Internet es la mayor red WAN existente, es un conjunto de redes de acceso público interconectadas a nivel mundial que satisface actuales necesidades de comunicación. La Internet existe gracias a la interconexión de redes pertenecientes a Proveedores de Servicios de Internet (ISP). Los ISP al interconectarse entre ellos proporcionan los diferentes servicios de los que gozamos a través de la red mundial.

Protocolos de redes

En una conversación entre personas se da un conjunto de reglas que contribuyen al éxito de la comunicación, de la misma manera, las comunicaciones a través de redes de computadores demandan el cumplimiento de un gran conjunto de reglas, implementadas en el

hardware y software requerido, a este conjunto de reglas se le conoce como protocolos de red. Según las diferentes funciones asociadas a las comunicaciones a través de redes se implementan diferentes protocolos.

Los protocolos de red rigen aspectos como el formato del mensaje, método para compartir información sobre rutas entre dispositivos, la administración de sesiones, los tipos de mensajes de control que se transmiten, por ejemplo solicitudes de servicios, acuses de recibo, mensajes de estado o notificación de error.

El proceso de comunicación entre computadores corresponde a un conjunto de complejas etapas, cada una regida por protocolos de red específicos, cada servicio de nivel superior depende de la funcionalidad de los protocolos de nivel inferior. Esta forma de ver la comunicación en un conjunto de etapas se le llama modelo en capas, y al conjunto de protocolos se le llama suite o stack de protocolos.

Las actuales redes de computadores obedecen protocolos avalados por la industria y ratificados por entidades de estandarización como IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), el IETF (Grupo de trabajo de ingeniería de Internet). El acatamiento de estándares asegura la compatibilidad entre diferentes fabricantes.

Los protocolos son independientes de la tecnología

Los protocolos de red definen las funciones dadas en la comunicación a través de las redes, pero generalmente no describen cómo debe darse la respectiva función. Es posible que protocolos diferentes utilicen tecnologías diferentes para realizar la misma tarea, pero dado que cumplen con la necesidad definida por el estándar, se afirma entonces que los protocolos son independientes de la tecnología. Por ejemplo, el software a través del cual interactúan los usuarios con la red, debe seguir estándares de software, sin embargo el estándar no específico del lenguaje de programación a utilizar.

Modelos de referencia y de protocolos

En el contexto de las redes de computadores básicamente hay dos clases de modelos de red: Modelos de Referencia y Modelo de Protocolo. Los modelos de referencia, como lo indica su nombre son precisamente una referencia conceptual respecto a las funciones que se dan en la comunicación. Un modelo de referencia no corresponde precisamente a la definición de las implementaciones reales, su finalidad es describir y ayudar a comprender las funciones involucradas en el proceso de comunicación. Por su parte, un modelo de protocolo generalmente coincide con la estructura de un conjunto particular de protocolos. Los modelos de red de aceptación generalizada son Modelo de referencia OSI y modelo de protocolos TCP/IP, brevemente descritos en las dos secciones siguientes.

Modelo TCP/IP

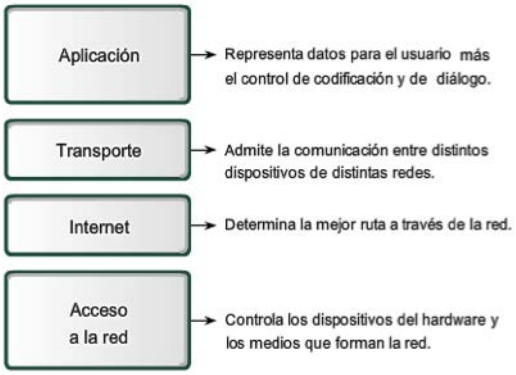


Imagen 4
Fuente: Propia, adaptada de currículo CCNA Exploration

El modelo TCP/IP *(Transmision Control Protocol/Internet Protocol o Protocolo de Control de Transmisión/Protocolo Internet)*. Es el modelo creado por el

Departamento de Defensa de los Estados Unidos en la década de 1970, es el conjunto de protocolos con base en el cual funciona la Internet, conocido también como modelo de Internet. El modelo TCP/IP describe la comunicación en un conjunto cuatro fases o capas. El modelo TCP/IP es un estándar abierto. Las capas del modelo son: Aplicación, Transporte, Internet y Acceso a Red.

Los protocolos de la pila TCP/IP se implementan en el software de los dispositivos emisor y receptor e interactúan para la exitosa comunicación a través de la red. Algunos de estos protocolos también se implementan en dispositivos intermedios.

Etapas básicas de la comunicación sobre TCP/IP

El proceso de comunicación de mensajes en redes TCP/IP básicamente comprende los siguientes pasos:

- Creación de datos de usuario mediante el software de aplicación del origen.
- Segmentación y encapsulación de datos según los protocolos de las diferentes capas en el origen.

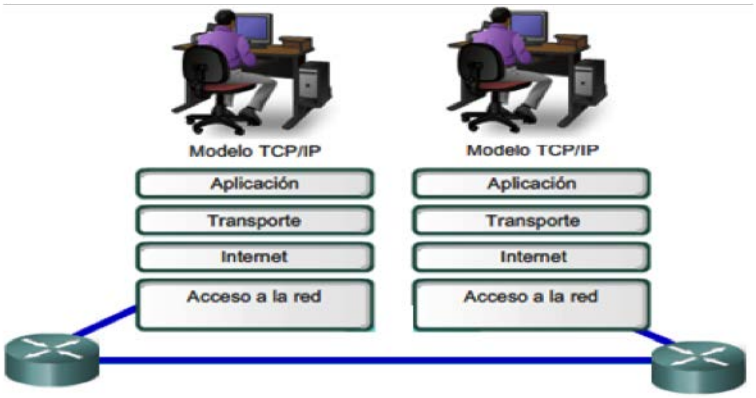


Imagen 5
Fuente: Propia, adaptada de currículo CCNA Exploration

- Entrega de datos a los medios, función dada en la capa de acceso a la red.
- Transferencia de datos a través de la red, valiéndose de la interconexión de dispositivos intermedios.
- Recibo de datos en la capa de acceso a la red del dispositivo destino.
- Desencapsulación y reensamble de datos por los protocolos de las diferentes capas en el destino.
- Transmisión de datos a la aplicación del destino.

Multiplexación de mensajes

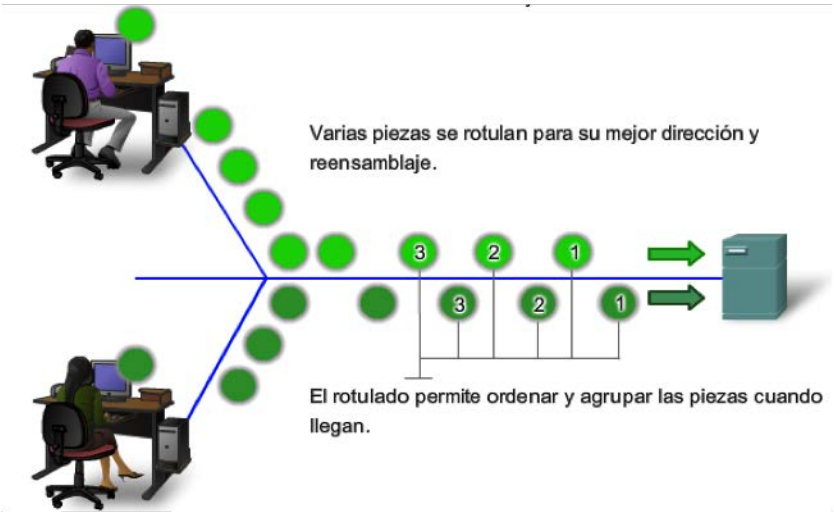


Imagen 6
Fuente: Propia, adaptada de: currículo CCNA Exploration

En una red normalmente hay muchos equipos compitiendo por el uso de los canales de transmisión. El intercambio de mensajes se da de tal forma que el recurso se asigna a equipos individuales de forma alternada durante breves lapsos de tiempo, esta forma de aprovechamiento del recurso recibe el nombre de Multiplexación.

La Multiplexación hace necesario el fraccionamiento de la información, lo que agrega cierta complejidad, pero el beneficio obtenido es que ante una falla en la transmisión sólo habría pérdida parcial del mensaje, y por tanto no se requeriría la retransmisión de la totalidad del mismo. Además de lo anterior, frente a la saturación de alguna ruta, diferentes segmentos pueden seguir distintos caminos, mejorando la confiabilidad de la red. Con el avance en las tecnologías de hardware sobre ellas, estas alternancias y segmentaciones son prácticamente imperceptibles para el usuario.

Unidades de Datos de Protocolos

En las etapas del proceso de envío, los diferentes protocolos agregan información adicional a la información recibida de protocolos de capa superior, lo que genera una nueva **Unidad de Dato de Protocolo** o **PDU**, cada PDU tiene su respectivo formato. Esta tarea agregar información y formar una PDU en un formato diferente se conoce como encapsulación. Dependiendo la etapa del proceso, las PDU toman nombres distintos. Las PDU en el modelo TCP/IP son:

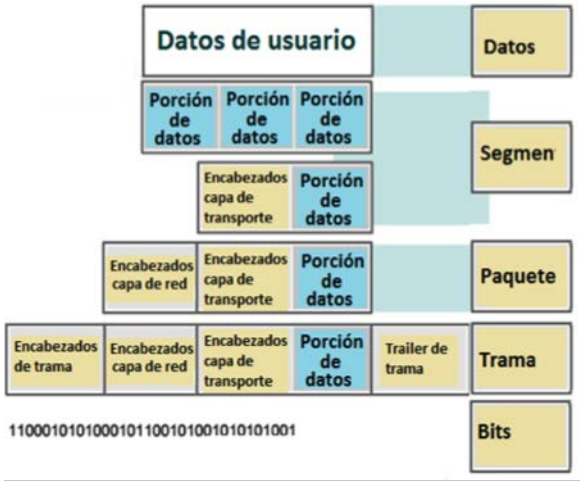


Imagen 7

Fuente: Propia, adaptada de currículo CCNA Exploration

- ***Dato*:** producidos en capa de aplicación.
- ***Segmento*:** producidos en capa de transporte.
- ***Paquete*:** PDU de capa Internet.

- ***Trama*:** en la capa de acceso de red.
- ***Bits*:** transmitidos físicamente en forma de señales.

El proceso en el destino se inicia con la recepción y decodificación de los bits y luego se da la desencapsulamiento de cada PDU, pasándose la información resultante a la respectiva capa superior.

Modelo de referencia OSI

El modelo *OSI (Open System Interconexión o Interconexión de Sistemas Abiertos)* es el modelo de referencia más conocido. Usado en el diseño y especificaciones de redes y como enfoque de solución de problemas. Fue planteado por la Organización Internacional para la Estandarización *(ISO, International Organization for Standarization)* con el fin de ofrecer un esquema sobre el cual crear conjuntos de protocolos. El modelo OSI especifica un conjunto de funciones que deben darse en cada etapa, estas funciones se distribuyen en siete capas numeradas a continuación:

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

Paralelo entre los modelos OSI y TCP/IP

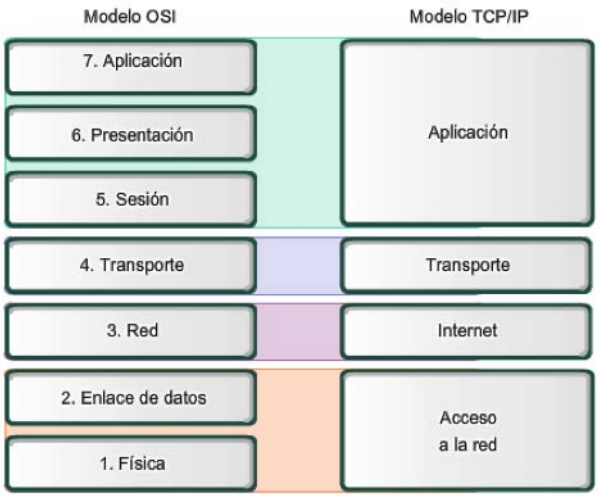


Imagen 7
Fuente: Propia, adaptada de currículo CCNA Exploration

Dada las diferencias en cuanto a la estructura de cada modelo, resulta pertinente indicar de qué manera se corresponden las diferentes funciones en el proceso de comunicación según cada modelo. La imagen adjunta ilustra un paralelo entre los dos modelos.

Direcciones en el contexto de redes

Ante el gran número de porciones de mensajes que viajan a través de una red, es necesario que cada una contenga información suficiente que facilite la llegada al respectivo destino, con este fin existen diferentes tipos de identificadores o direcciones, los cuales sucintamente se describen a continuación:

Dirección física

Desde el punto de vista del modelo OSI, esta dirección se agrega como parte del encabezado en el proceso de encapsulamiento a nivel de la Capa 2 para obtener una trama. La Capa 2 está relacionada con la entrega de los mensajes en una red local única. La dirección física o de Capa 2 es exclusiva. En una red local Ethernet, la dirección física se denomina dirección de Control de Acceso al Medio o dirección MAC, esta dirección es definida por el fabricante e implementada físicamente en la tarjeta de red a través de la cual se conecta el equipo a la red. Las tramas que viajan en una red Ethernet local contienen las direcciones MAC de los equipos origen y destino. Cuando el destino recibe la trama, la desencapsula, elimina las direcciones MAC y entrega a la Capa 3 la información resultante.

Dirección lógica

Una gran red puede estar dividida en varios segmentos de red local, en este caso la dirección física no resulta suficiente para el intercambio de información entre dos segmentos diferentes, por lo tanto se requiere de protocolos que posibiliten la interconexión de redes locales. Desde la perspectiva del modelo OSI, a nivel de capa 3 se define el direccionamiento lógico de redes. Las direcciones de capa 3, también conocidas como direcciones lógicas, deben proporcionar la manera identificar la red en la que se encuentra un host específico. Desde la óptica del modelo TCP/IP, esta dirección es la dirección IP, la cual contiene información sobre la red en la que está ubicado el host.

Imagen 8
Fuente: Propia, adaptada de currículo CCNA Exploration

La interconexión de redes se vale de dispositivos enrutadores que usan la dirección IP para hacer la entrega de información al destino correcto.

Entre las funciones que ejecutan los enrutadores se tiene las siguientes:

- Desencapsular las tramas entrantes.
- Leer los encabezados de capa 3 de los paquetes.
- Leer el identificador de la red a partir de la dirección IP de destino del paquete.
- Seleccionar la interfaz de salida para el reenvío de paquetes nuevamente entramado de tal manera que pueda llegar a su destino.

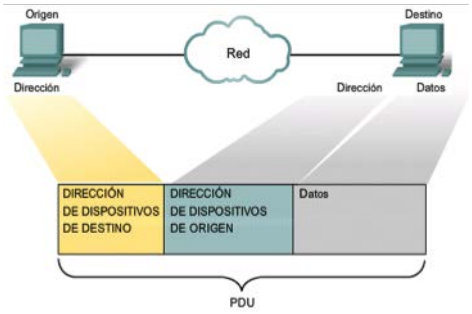


Imagen 9
Fuente: Propia, adaptada de currículo CCNA Exploration

Números de puertos o direcciones de capa 4

La dirección MAC identifica un equipo en una red local, mientras que la dirección lógica permite identificar la red a la que pertenece. Cuando la información llega al dispositivo destino, antes de ser visualizada por el usuario es separada según la aplicación correspondiente. Es posible que en un usuario de un computador esté utilizando varios servicios de red, por ejemplo, correo electrónico, navegación web, mensajería instantánea u otro. La separación de los diferentes flujos se realiza en función de un identificador conocido como número de puerto, el cual es parte de la información contenida en el encabezado de los segmentos (PDU de capa 4). Un intercambio único entre dispositivos se identifica mediante números de puerto de origen y de destino.

La capa de transporte utiliza el esquema de direccionamiento basado en números de puertos que identifican las aplicaciones. Algunos de los servicios de capa de aplicación y los respectivos números de puertos son:

- Sistema de nombres de dominios (DNS) - TCP/UDP puerto 53.
- Protocolo de transferencia de hipertexto (HTTP) - TCP puerto 80.
- Protocolo simple de transferencia de correo (SMTP) - TCP puerto 25.
- Protocolo de oficina de correos (POP) - TCP puerto 110.

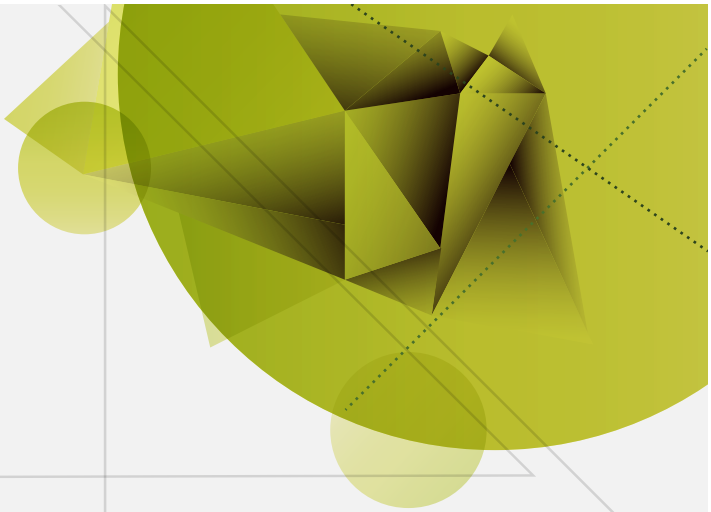
- Protocolo de configuración dinámica de host - UDP puertos 67 y 68.
- Protocolo Telnet TCP puerto 23.

En los siguientes capítulos tendremos la oportunidad de tratar algunos detalles de los protocolos de las diferentes capas, particularmente en la unidad dos analizaremos aspectos de los protocolos de la capa de aplicación más comúnmente utilizados.

1

Unidad 1

Protocolos de capa de aplicación



Telemática I

Autor: Juan Carlos Ramirez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

La segunda semana contiene bases teóricas sobre las capas de aplicación de diferentes modelos a través de los cuales los usuarios interactúan con la red. En este espacio el reconocer nombres, funcionalidades y modelos permitirá una relación eficiente con las redes presentes en su quehacer.

U1 Metodología

Los estudiantes como centro activo de aprendizaje deben hacer la lectura y análisis permanente de este material, que les permite realizar una contextualización a nivel mundial del tema, conociendo la teoría general y su aplicación práctica en contextos específicos.

U1

Desarrollo temático

Protocolos de capa de aplicación

Introducción sobre capas de aplicación

La capa de aplicación constituye la interfaz a través de la cual los usuarios interactúan con la red, las utilidades empleadas por el usuario son programas, más comúnmente conocidas como software o aplicaciones de red desarrolladas por diferentes fabricantes según sus objetivos. Claros ejemplos de aplicaciones de red son los navegadores utilizados para acceso a la red, las aplicaciones mediante las cuales se puede tener acceso a bases de datos remotas, o aquellas propias de los servicios de correo; existen otras aplicaciones de uso no evidente para usuarios finales, pero sin las cuales no es posible la comunicación, algunas de ellas y sus respectivos protocolos son descritas en este capítulo. En el presente capitulo se aborda detalles de un conjunto de aplicaciones y protocolos de aplicación que están presentes en la transmisión de información a través de redes.

Tareas de capas superiores del modelo OSI

La comparación entre los modelos OSI y TCP/IP muestra que las funciones de protocolos de Aplicación TCP/IP se asimilan a las capas de Aplicación, Presentación y Sesión del modelo OSI, en la práctica las funciones correspondientes a estas capas se incorporan a nivel de software, por ejemplo, en los navegadores Web, herramientas de correo electrónico y aplicaciones diseñadas con fines particulares.

Capa de Aplicación del Modelo OSI

En el ámbito de las redes de computadores las aplicaciones se refieren a servicios que proporcionan la interfaz para que el usuario aproveche la red con fines de recepción y envío de información, la capa de Aplicación del modelo de referencia OSI define las funcionalidades que deben cumplirse en cuanto a la interfaz de la red con el usuario. Las diferentes aplicaciones utilizan para sus propósitos un conjunto de protocolos apropiados. La aparición de nuevas aplicaciones requiere de la implementación de nuevos protocolos.

Capa de presentación del Modelo OSI

El modelo OSI define, en la capa de Presentación, las funciones relacionadas con codificación y conversión de datos, Compresión/Descompresión y Encriptación/Desencriptación. Situaciones en las que se involucra los diferentes formatos de archivos, tales como .docx, .pdf, .jpg, entre otros, atañen a la capa de Presentación.

Capa de Sesión del Modelo OSI

En esta capa se definen las funciones que crean y mantienen diálogos entre las aplicaciones de origen y destino, administra el intercambio de información para iniciar los diálogos, mantenerlos, reiniciar sesiones interrumpidas.

Capa de aplicación del modelo TCP/IP

Con el fin de una mayor comprensión de las tareas referenciadas en las tres capas superiores del modelo OSI, desde la perspectiva de su implementación práctica, conviene analizar la Capa de Aplicación TCP/IP. Como usuarios de la Internet, frecuentemente hacemos uso de servicios soportados por los protocolos de la capa de aplicación de TCP/IP, los cuales especifican información de control y formato. Algunos de los protocolos de aplicación TCP/IP son **DNS** o Protocolo de Servicio de Nombres de Dominio (DNS, *Domain Name Service*), **HTTP** o Protocolo de Transferencia de Hipertexto (HTTP, *Hypertext Transfer Protocol),* **SMTP** o Protocolo Simple de Transferencia de Correo, **Telnet** o Protocolo de Emulación de Terminal, **FTP** o Protocolo de Transferencia de Archivos. Posteriormente en este documento se describe con mayor detalle estos protocolos. La comunicación exitosa requiere que diferentes protocolos de capa de aplicación sean implementados en los equipos origen y destino que participan en la comunicación.

Las funcionalidades de la capa de aplicación se fundamentan en dos tipos de software denominados aplicaciones y servicios. Las aplicaciones, como se ha comentado antes, corresponden al software empleado por el usuario para interactuar con la red, ejemplos de ello son los clientes de correo electrónico y los exploradores. Los servicios son procesos que ayudan a las aplicaciones empleadas por el usuario, estos servicios son los programas que se comunican con la red y se ejecutan sin el control del usuario, se da incluso que una misma aplicación utilice diferentes servicios de la capa de aplicación, por ejemplo, un cliente puede necesitar de diversos procesos individuales para formular sólo una solicitud a un servidor. Además, los servidores generalmente tienen múltiples clientes que solicitan información al mismo tiempo, estas solicitudes individuales del cliente pueden manejarse en forma simultánea y separada. Los servicios y procesos de la capa de aplicación dependen del soporte de las funciones de la capa inferior para administrar en forma exitosa las múltiples comunicaciones.

Modelo cliente/servidor

Como usuario de redes de computadores, se tiene frecuentemente la necesidad de utilizar un dispositivo final para acceder a información almacenada en otro dispositivo, ello requiere la utilización de un conjunto de aplicaciones estructuradas con tal finalidad. Un ejemplo

de tal contexto lo constituye el modelo Cliente/Servidor, el cual se refiere al hecho en que un dispositivo final (cliente) solicita información a un equipo servidor, el servidor responde al cliente según los parámetros de la solicitud. Muy posiblemente se requiera procesos de autenticación de usuario, lo que el servidor manejar con base en la configuración de un conjunto de cuentas de usuario asociadas a sus respectivas contraseñas.

Ejemplos de redes cliente/servidor son los entornos empresariales en que los empleados usan servidores de correo, servidores de descarga de música y video, redes de cajeros electrónicos bancarios, acceso a bases de datos remotas, acceso a servidores de páginas Web, para ello es necesario el uso del navegador instalado en el equipo cliente, el navegador es una aplicación cliente utilizada en la conexión a la World Wide Web. Posteriormente describiremos aquí algunos servicios de capa de aplicación que funciona bajo el esquema cliente servidor.

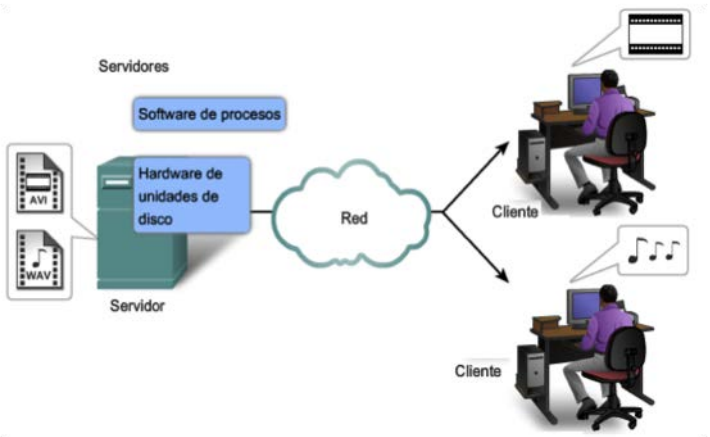


Imagen 1
Fuente: Propia, adaptada de currículo CCNA Exploration

Redes y aplicaciones punto a punto

Al referirnos al entorno punto a punto es necesario distinguir entre dos conceptos, las redes punto a punto en sí mismas y las aplicaciones punto a punto.

Redes punto a punto

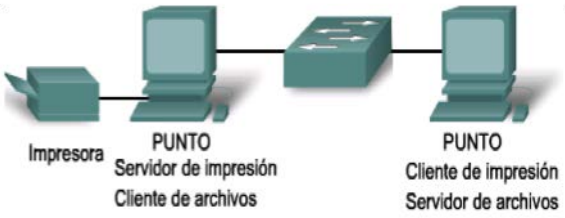


Imagen 2
Fuente: Propia, adaptada de currículo CCNA Exploration

Son entornos en los cuales dos o más equipos se conectan sin el uso de un servidor que controle el flujo de información. Los equipos de la red pueden actuar como un servidor de una sesión al tiempo que son clientes de otra. Ejemplo de red punto a punto es una red casera en la que se comparte una impresora.

El responsable de cada computador lo configurar para compartir recursos a través de la red. En las redes punto a punto la administración y recursos no se centralizan. Generalmente en redes punto a punto no se maneja cuentas de usuarios centralizadas, lo que dificulta la implementar sólidas medidas de seguridad.

Aplicaciones punto a punto

No debe confundirse una aplicación punto a punto con una red punto a punto. En una aplicación punto a punto cada dispositivo puede funcionar como cliente o como servidor dentro de la misma comunicación, pero es necesario que cada uno proporcione una interfaz de usuario y ejecute un servicio en segundo plano. Las aplicaciones punto a punto pueden utilizarse en las redes punto a punto, en redes cliente-servidor y en Internet.

Imagen 3
Fuente: Propia, adaptada de currículo CCNA Exploration

Siguiendo con diferentes servicios que dan soporte a las comunicaciones de usuario a través de redes de computadores, veremos a continuación algunos protocolos de capa de aplicación TCP/IP.

Sistema de nombres de dominios DNS

El envío y recepción de información entre redes de datos es posible gracias a la inclusión de direcciones IP origen y destino en los paquetes, pero a la mayoría de usuarios se les facilita más el uso de nombres de dominio, por ejemplo, www.areandina.edu.co en lugar que el de una dirección numérica. Los nombres de dominios, fáciles de recordar, se asocian a direcciones IP.

Podemos suponer, por ejemplo, que desde un equipo cliente web con acceso a la Internet deseamos conectarnos al portal virtual de la Fundación Universitaria del Área Andina y que la correspondiente dirección IP es 200.69.61.105; sin el uso del Sistema de Nombres de Dominios (DNS), deberíamos escribir esta identificación numérica en la barra de direcciones del navegador para que cada paquete enviado la contenga.

Usando DNS podemos escribir la información relativa al nombre de dominio www.areandina.edu.co, con lo cual inicialmente se establece una solicitud a un servidor DNS en la red para que proporcione al cliente la correspondiente dirección IP, con la cual efectivamente se puede establecer la comunicación. DNS utiliza un conjunto distribuido de servidores para resolver los nombres asociados con estas direcciones numéricas. En general, cuando la aplicación de usuario solicita conexión mediante el uso de nombre, el cliente consulta uno de estos servidores para resolver el nombre a una dirección numérica.

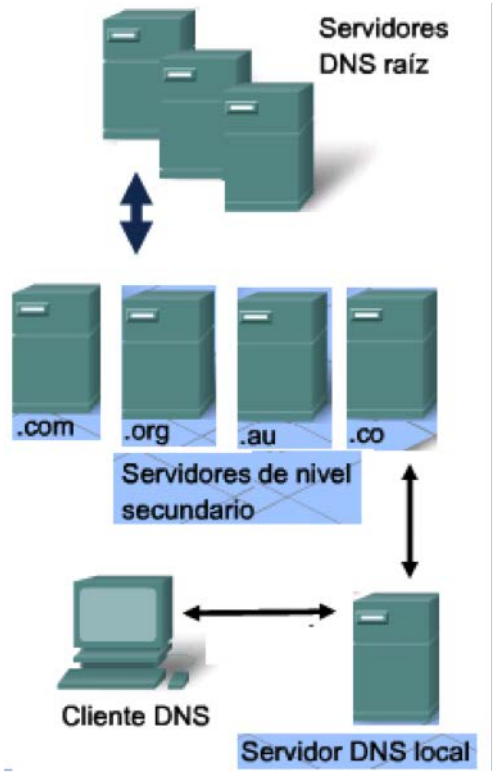


Imagen 4
Fuente: Propia, adaptada de currículo CCNA Exploration

Es necesario que los equipos clientes y otros equipos de red, estén configurados con direcciones de uno o más servidores DNS que pueden ser utilizadas. Generalmente el Proveedor de Servicios de Internet (ISP) proporciona estas direcciones de servidores DNS.

Cuando un cliente realiza una consulta con fines de resolución de nombres de dominio, el proceso del servidor busca inicialmente en sus registros para ver si puede realizar la resolución, en caso de no poder hacerlo, contacta a otros servidores. Una solicitud puede requerir la consulta a una secuencia de servidores, encontrada la asociación, esta se devuelve al servidor solicitante inicial, el cual la almacena temporalmente en memoria caché, este almacenamiento en cache puede reducir el tráfico de solicitudes.

DNS usa un sistema jerárquico para crear una base de datos de resoluciones de nombres. En la parte alta de la jerarquía, se encuentran los servidores raíz que almacenan información para alcanzar los servidores de dominio de nivel superior, los que a su vez tienen registros que apuntan a los dominios de nivel secundario. Los dominios de primer nivel representan el tipo de organización o país.

World wide web (www) y protocolo de transferencia de hipertexto (HTTP)

Al pretender acceder a una página de Internet escribimos la correspondiente dirección web en la barra con ello el navegador establece la conexión al servicio Web del servidor, este servicio Web usa el protocolo HTTP o Protocolo de Transferencia de Hipertexto.

Los términos reales que corresponden a direcciones Web son URL (Localizador Uniforme de Recursos) y URI (Identificador Uniforme de Recursos). Un URL como http://www.areandina,edu.co/index.html se referiría a una página Web (recurso) identificada como index.html y almacenada en el servidor areandina.edu.co.

Una vista general del proceso se compone de tres pasos: a) Solicitud del cliente al servidor HTTP b) Respuesta del servidor enviando el código html correspondiente a la página solicitada c) Interpretación del código html, por parte del navegador del cliente para que la página sea visualizada por el usuario. La imagen adjunta esquematiza el proceso.

HTTP es uno de los protocolos de TCP/IP, desarrollado para la transferencia de datos, es de los protocolos de capa de aplicación de mayor uso. HTTP es muy flexible pero no es muy seguro dado que la información transferida puede ser fácilmente interceptada e interpretada. Para transferencia de información que demanda mayor seguridad se usa el protocolo HTTP seguro (HTTPS), el cual puede utilizar autenticación de usuarios y encriptación de información.

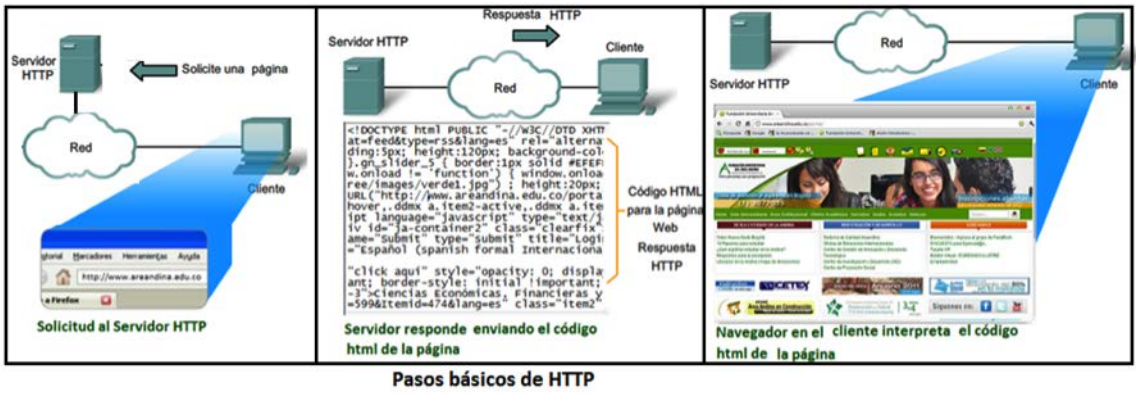


Imagen 5
Fuente: Propia, adaptada de currículo CCNA Exploration

Servicios de correo electrónico

El correo electrónico es un servicio que opera bajo el esquema Cliente/Servidor, dos protocolos de aplicación para el manejo de correo electrónico son el Protocolo de Oficina de Correos (POP) y el Protocolo Simple de Transferencia de Correo (SMTP).

Proceso del cliente para el manejo de correo

Los procesos de manejo de correo en el equipo del usuario comúnmente usan una aplicación conocida como MUA o Agente de Usuario de Correo, el MUA

El cliente puede usar POP para el recibo de correos desde un servidor, mientras que para el envío a un servidor usa SMTP.

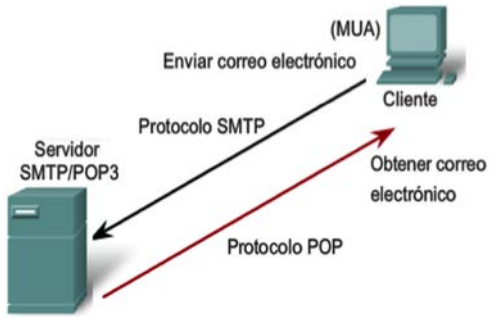


Imagen 6
Fuente: Propia, adaptada de currículo CCNA Exploration

Procesos del servidor de correo electrónico

La comunicación vía correo electrónico entre diferentes usuarios puede involucrar diferentes servidores, por ejemplo Yahoo y Hotmail, por ello los servidores de correo electrónico utilizan dos procesos: MTA o Agente de Transferencia de correo y MDA o Agente de Envío de correo. MTA al recibir mensajes de un MUA o de otro MTA determina como renviarlo, si el mensaje está destinado a un usuario con buzón en el mismo servidor local, se entrega al MDA; si en cambio el destino no está en el servidor local, el agente MTA envía el mensaje al MTA en el servidor asociado al destino.

Protocolo de transferencia archivos FTP

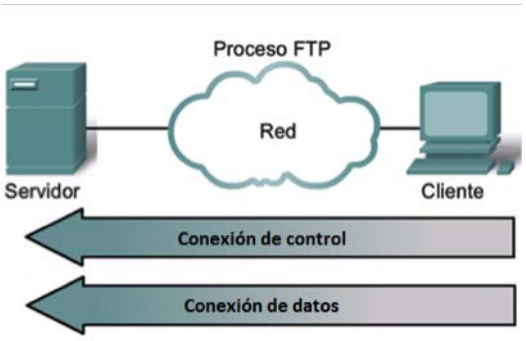


Imagen 7
Fuente: Propia, adaptada de currículo CCNA Exploration

FTP o protocolo de transferencia de archivos fue desarrollado para realizar transferencias de archivos entre cliente y servidor. Se considera como cliente FTP a aquella aplicación ejecutable en un computador, diseñada para la carga y descarga de archivos hacia o desde un servidor que ejecuta el servicio FTP. El funcionamiento de FTP requiere dos conexiones entre cliente y servidor, una de ellas es para el intercambio de comandos de solicitudes y respuesta, conocida como conexión de control, establecida por el cliente a través del puerto 21. La otra conexión se utiliza para la transferencia de los archivos en sí, se realiza a través del puerto 20.

Protocolo de configuración dinámica de host (DHCP)

En toda red que funcione bajo el esquema TCP/IP cada computador requiere una configuración IP, la cual incluye una dirección IP y otros parámetros que analizaremos posteriormente, esta configuración podría darse de forma manual o automática.

Mediante el uso de DHCP cada quipo que se conecta a la red obtiene la configuración IP de forma automática o dinámica, para ello inicialmente se lleva a cabo una conexión a un servidor DHCP, previamente configurado, mediante tal conexión el equipo solicita una con-

figuración, El servidor DHCP ofrece una de las configuraciones disponibles para ser aceptada por el solicitante. La configuración asignada no es permanente, hay periodos de asignación, si un equipo cliente se apaga o se desconecta de la red, la configuración IP que tenía queda libre y el servidor puede asignarla a otro equipo, de ahí que se habla de configuración dinámica. El servidor de DHCP asegura que las configuraciones IP de cada equipo dentro de una red sean únicas.

Diferentes equipos en la red pueden actuar como servidores DHCP si ejecutan el correspondiente software. En redes de gran tamaño el servidor de DHCP es un equipo local exclusivamente para realizar este servicio. En redes pequeñas, como nuestras redes caseras y de conexión a la Internet, el servidor DHCP se encuentra en las instalaciones del Proveedor de Servicios, un equipo de la red recibe la configuración directamente del proveedor.

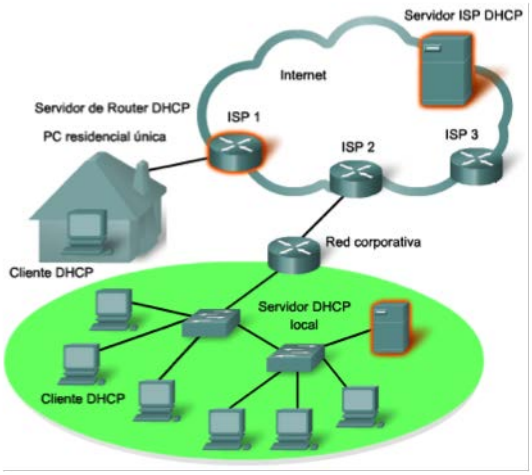


Imagen 8
Fuente: Propia, adaptada de currículo CCNA Exploration

Se debe tener sumo cuidado con los riesgos de seguridad asociados al uso de DHCP, cualquier equipo que se conecte a la red puede recibir una configuración, una medida importante puede ser la seguridad física y otras restricciones. En redes grandes se recomienda el uso de DHCP para la configuración de hosts de propósitos generales, mientras que para equipos particulares como routers, servidores, impresoras se recomienda el uso de direcciones fijas configuradas manualmente.

El proceso de configuración se lleva a cabo en un conjunto de etapas. Cuando un dispositivo configurado para DHCP se inicia, su software cliente envía una solicitud de DESCUBRIMIENTO de DHCP con el fin de identificar servidores disponibles. Un servidor responde con una OFERTA de DHCP, la cual contiene la configuración ofrecida.

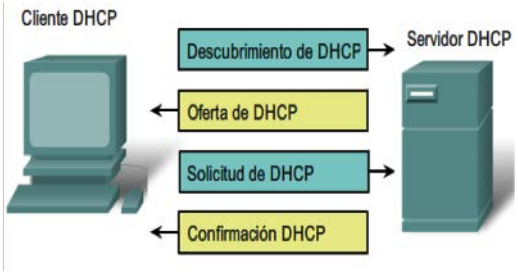


Imagen 9
Fuente: Propia, adaptada de currículo CCNA Exploration

Ante la existencia de varios servidores, el cliente podría recibir múltiples OFERTAS DE DHCP, por tanto debe elegir y enviar una SOLICITUD DE DHCP con la identificación de un servidor particular y la oferta aceptada. Finalmente el servidor confirma la asignación. Cuando al cliente se le ha asignado una configuración, puede renovarla mediante otro mensaje de SOLICITUD DE DHCP, antes de vencer el tiempo de asignación.

TELNET

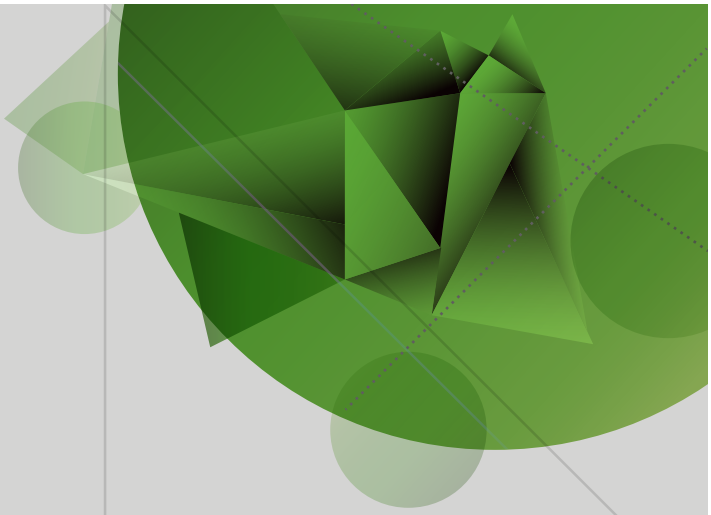
El servicio Telnet brinda un procedimiento estándar, basado en texto, de emulación de terminal desde un equipo remoto. Una conexión Telnet se llama sesión de terminal virtual (VTY). Telnet utiliza software para crear un dispositivo virtual con iguales características de una sesión de terminal con acceso. La mayoría de sistemas operativos incluye un cliente de Telnet, por ejemplo, Telnet puede ejecutarse desde el indicador de símbolo del sistema en un computador con sistema operativo Windows.

Establecida una sesión Telnet e posible realizar cambios autorizados en el servidor tal como si se estuviera frente a él. Telnet permite autenticación de usuario, pero no admite encriptación de datos, por tanto la información transferida puede ser interceptada y fácilmente interpretada. Un método alternativo con las mismas finalidades de Telnet y que brinda mayor seguridad es el Protocolo shell seguro (SSH), el cual brinda otros servicios de red seguros.

2

Unidad 2

Capa de transporte y capa de red



Telemática I

Autor: Juan Carlos Ramirez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En la tercera semana analizaremos la transmisión de información a través de redes que involucran protocolos de capa de transporte, los cuales deben ser interpretados y revertidos por los respectivos protocolos.

La capa de red es de suma importancia por su participación en tareas de preparación y función de algunos dispositivos intermedios que deben redirigir la información a lo largo de la red hasta el destino. El direccionamiento y enrutamiento son los ejes de las bases teóricas a tratar.

U2

Metodología

Los estudiantes como centro activo de aprendizaje deben hacer la lectura y análisis permanente de este material, que les permite realizar una contextualización del tema, conociendo la teoría general y su aplicación práctica en contextos específicos.

U2

Desarrollo temático

Capa de transporte y capa de red I

Introducción

La transmisión de información a través de redes de computadores involucra complejas fases implementadas en la práctica a través de protocolos. Los protocolos de capa de Transporte en el origen se encargan de algunas de las tareas iniciales de preparación para la transferencia de información, las que a su vez son interpretadas y revertidas por los respectivos protocolos en el destino, luego de la contribución de las diferentes capas inferiores. La capa de Red participa en las tareas de preparación en el origen, pero también está presente en la función de algunos dispositivos intermedios que deben redirigir la información a lo largo de la red hasta el destino. Es enorme el volumen de contenidos relacionados con las funciones de las capas de trasporte y la capa de red, pero, a través del presente capítulo, se pretende brindar al estudiante un conjunto de elementos básicos que permitan comprender las funcionalidades de estas capas. En la unidad cuatro se abordará el tema de direccionamiento y se presentará una introducción al enrutamiento, tópicos que atañen a la capa de red.

La capa de transporte

En la unidad anterior describimos algunas funcionalidades y protocolos de la capa de aplicación, anotando que ella genera los datos mediante las utilidades de usuario. Los flujos de información de usuario producidos por la capa de aplicación requieren de varios procesos de preparación para poder ser transmitidos, en este sentido se dice que la información de usuario "es entregada a la capa de transporte" de tal manera que las funcionalidades de esta capa inicien la adecuación para la transferencia.

Funciones básicas de la capa de transporte

La capa de Transporte se encarga de la transferencia de datos de extremo a extremo, desde la perspectiva del Modelo TCP/IP, la capa de transporte es el vínculo entre la capa de Aplicación y la capa Internet.

Las principales tareas, de la transmisión de datos en una red, llevadas a cabo por la capa de transporte son descritas a continuación:

Segmentación de datos de aplicación

Los flujos de datos de usuario producidos a nivel de capa de aplicación deben ser procesados según los protocolos de la capa de transporte; los datos son inicialmente fragmentados y los diferentes fragmentos junto con información adicional agregada, o encabezados de capa de transporte, son encapsulados en segmentos.

Los encabezados incluyen información que, por ejemplo, permite identificar la aplicación a la cual corresponde el fragmento y en algunos casos un número de secuencia para facilitar el rearmado en el punto de recepción. La segmentación de la información permite la multiplexación, en la cual diferentes comunicaciones comparten un mismo canal de transmisión.

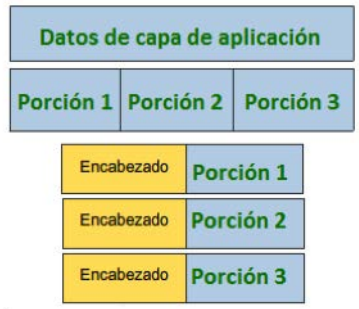


Imagen 1
Fuente: Propia, adaptada de currículo CCNA Exploration

Seguimiento de comunicaciones individuales

Como usuarios de la Internet es muy usual que en ciertos momentos hagamos uso simultáneo de varias comunicaciones a través de la red, por ejemplo, mientras esperamos que finalice la descarga de un archivo de gran tamaño, aprovechamos para mantener una sesión de chat, al tiempo que hacemos uso del servicio de correo electrónico o consultamos una página Web. Es claro que a cada una de estas sesiones de comunicación o conversaciones corresponde una ventana de su respectiva aplicación, no vemos, por ejemplo, que la información de la sesión de chat aparezca en la ventana del navegador para la consulta de la página Web, o que los datos del archivo en descarga se mezclen con la información de correo. Cada conversación entre nuestro equipo y aquellos con los que se comunica, se mantienen separada de las otras, esto es posible gracias a que los protocolos de capa de transporte proporcionan mecanismos para ello.

Imagen 2
Fuente: Propia, adaptada de currículo CCNA Exploration

Reensamble de la información

Dado que los diferentes flujos de información se fragmentan para su envío, se hace necesario que en el equipo destino se realice el proceso de reensamble.

Identificación de aplicaciones

Los protocolos de capa de transporte tienen entre sus funciones la separación de cada conversación individual entre diferentes aplicaciones, para ello se requiere que exista forma de identificar la respectiva aplicación. La capa de trasporte del modelo TCP/IP utiliza identificadores conocidos como números de puerto para distinguir entre las diferentes conversaciones, estos números de puerto son parte de la información de encabezado que contienen los segmentos. A cada proceso que accede a la red desde un computador se le asigna un número de puerto único en ese computador.

Direccionamiento de puerto

Entre las tareas fundamentales de la capa de transporte está la identificación de los diferentes flujos de información, el direccionamiento de puerto es el esquema de identificación a nivel de capa de transporte, los números de puerto identifican las diferentes conversaciones en las que está involucrado un equipo. En la transmisión de información sobre redes TCP/IP, los números de puerto origen y destino se incluyen como campos en los encabezados de los segmentos.

Los números de puertos se asignan dependiendo si el mensaje es de solicitud o respuesta. A los procesos de servidores usualmente se asigna números de puerto fijo contenidos en el rango de 1 a 1023, los equipos clientes seleccionan dinámicamente números de puertos únicos, en el rango de 1024 a 49151, para cada conversación.

En ambientes Cliente/Servidor, el software del cliente debe contar con la configuración del número de puerto correspondiente al proceso del servidor asociado. Algunas aplicaciones de uso común cuentan con asignación predeterminada de números de puerto, por ejemplo,

un navegador Web usa el puerto 80, a menos que se indique otro número, como puerto de destino en la solicitud a un servidor Web. El número de puerto del solicitante se usa como número destino en la respuesta del servidor.

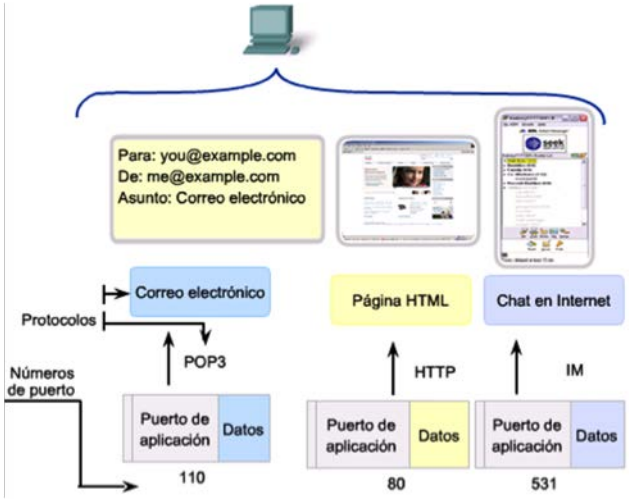


Imagen 3
Fuente: Propia, adaptada de currículo CCNA Exploration

Tipos de números de puerto

Los números de puerto se clasifican en diferentes rangos, según se indica a continuación.

- **Puertos bien conocidos:** les corresponden números del 0 al 1023, se reservan para servicios y aplicaciones de servidores tales como servidores Web, servidor de correo electrónico, entre otros; esto facilita que las aplicaciones cliente se puedan programar para solicitar conexiones.
- **Puertos registrados:** van del número 1024 al 49151, son los números de puertos para procesos o aplicaciones del usuario.
- **Puertos dinámicos o privados** (números 49152 a 65535): también conocidos como puertos efímeros, están usualmente asignados de forma dinámica a las aplicaciones cliente cuando se inicia una conexión. No es muy común que un cliente se conecte a un servicio utilizando un puerto dinámico o privado (aunque algunos programas que comparten archivos punto a punto lo hacen).

Funciones especiales de la capa de transporte

Adicional a las funciones básicas antes señaladas, un protocolo particular de capa de transporte tiene la capacidad de brindar funciones especializadas como: comunicación orientada a conexión, comunicación confiable, entrega de segmentos en el orden correcto y control del flujo, estas funciones se describen brevemente a continuación.

Comunicación orientada a conexión

La comunicación orientada a conexión se refiere al establecimiento de sesión previo a la transmisión de datos de aplicación. Los protocolos de capa de trasporte orientados a conexión crean una sesión de comunicación entre las aplicaciones de tal manera que las prepara para la transmisión de información de usuario.

Entrega confiable de segmentos

Es posible, por diversas razones, que un intento de comunicación entre aplicaciones presente fallas que podrían dar lugar a pérdida o daño de una parte de la información. En el ámbito de las redes de comunicación, se entiende por confiabilidad de la comunicación a la capacidad de garantizar que cada segmento sea entregado al correspondiente destino.

A nivel de capa de transporte, la confiabilidad se implementa fundamentalmente mediante los siguientes elementos:

- **Seguimiento de segmentos transmitidos:** con base en un número de secuencia asignado a cada segmento en el origen, los procesos de la capa de transporte en los dispositivos finales registran los segmentos transmitidos y recibidos. El número de secuencia es un campo incluido en los segmentos de un protocolo específico de transporte, el protocolo TCP descrito posteriormente.
- **Acuse de recibo (ACK):** el ACK o confirmación de información recibida, es un mensaje que el destinatario envía al origen notificando la recepción exitosa de segmentos. El ACK es un campo numérico en los segmentos del protocolo TCP, su valor está estrechamente relacionado con los números de secuencia.
- **Retransmisión de segmentos perdidos:** si el dispositivo origen no recibe un ACK del destinatario, dentro de un lapso de tiempo predeterminado, considera la posible pérdida de los segmentos, entonces, para garantizar que la información sea recibida, retransmite los respectivos segmentos.

El uso de confiabilidad da lugar a recarga sobre los recursos, generada por la necesidad de seguimiento, acuse de recibo y posibles retransmisiones. No todos los servicios de red se implementan para funcionar sobre comunicaciones confiables, ejemplos de servicios que sí lo requieren son el correo electrónico y la consulta de páginas Web, en los cuales un breve retraso se toma como aceptable con tal de que se reciba la información completa. Por su parte, ejemplos de aplicaciones que podrían tolerar pequeñas pérdidas, que muchas veces no resultan notorias, son la transmisión de video y voz, pero que a su vez son altamente susceptibles a retrasos.

Entrega en el orden correcto

En su viaje hacia el destino, los diferentes fragmentos de información pueden tomar rutas distintas, lo cual posiblemente dé lugar a que lleguen al destino en orden diferente al que fueron producidos por la aplicación origen. Si se utiliza protocolos de capa de transporte

que numeren los segmentos, se puede garantizar que en el equipo receptor se puedan reensamblarlos de tal manera que sean entregados en orden correcto a la aplicación destino.

Control del flujo

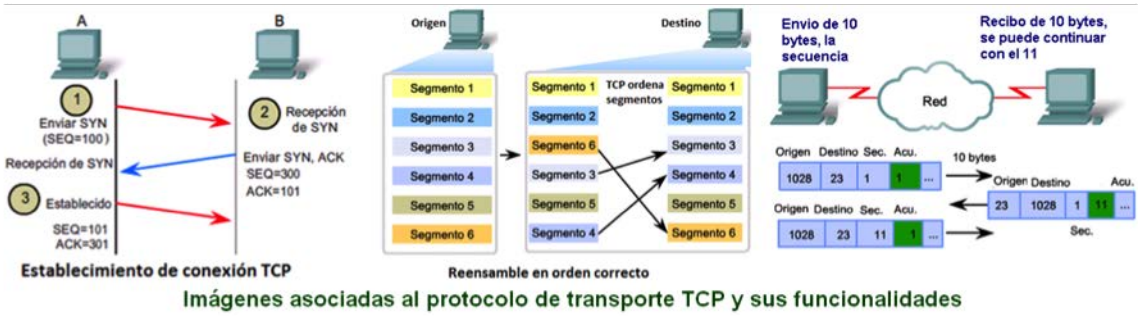
Si los recursos de un equipo receptor resultan insuficientes en una conversación, puede darse la pérdida de segmentos que se le envíen, dando lugar a posibles retransmisiones o degradación de la comunicación, algunos protocolos de capa de transporte pueden forzar la disminución de velocidad del flujo de datos de la aplicación origen. El adecuado control de flujo ayuda a evitar pérdida de segmentos y la necesitad de retransmisión.

Protocolos TCP Y UDP

TCP (Protocolo de Control de Transmisión) y UDP (Protocolo de Datagramas de Usuario) son los protocolos de capa de transporte usados dentro del stack de protocolos TCP/IP. Los dos protocolos administran la comunicación de múltiples aplicaciones, pero presentan importantes diferencias en sus funcionalidades.

Protocolo de Control de Transmisión (TCP)

Es el protocolo más robusto de la capa de transporte, es un protocolo orientado a la conexión. A través de TCP se aplican las funcionalidades de entrega en el orden correcto, confiabilidad y control de flujo.



Imágenes asociadas al protocolo de transporte TCP y sus funcionalidades

Imagen 4
Fuente: Propia, adaptada de currículo CCNA Exploration

Entre las aplicaciones más conocidas que utilizan TCP están: los exploradores Web, correo electrónico y transferencias de archivos.

Cada segmento TCP, además de los datos que trasporta, agrega 20 bytes de sobrecarga de encabezados.

Imagen 5
Fuente: Propia, adaptada de currículo CCNA Exploration

Protocolo de Datagramas de Usuario (UDP)

Es un protocolo sencillo, no orientado a conexión, sin garantía de entrega en el orden correcto y no confiable; no confiable significa que no hay acuse de recibo y por tanto no hay retransmisión de segmentos no recibidos por el destino l. Las aplicaciones que usan UDP toleran pequeñas pérdidas a cambio de mayor rapidez de transmisión, ejemplo de ellas son: DNS, video y voz sobre IP y juegos en línea. Los segmentos UDP tiene una recarga de 8 bytes de encabezado.

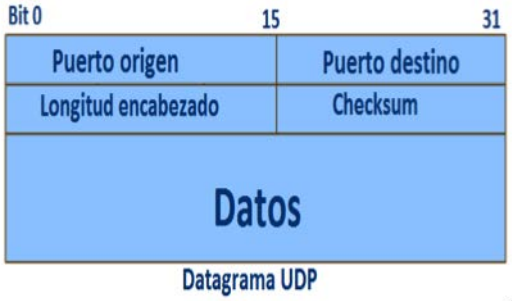


Imagen 6
Fuente: Propia, adaptada de currículo CCNA Exploration

La capa de red

La capa de red, o simplemente capa 3, del modelo de referencia OSI define el direccionamiento lógico o identificación de equipos en función de la red a la que pertenecen, también define los procedimientos facilitadores del encapsulamiento y envío de los segmentos de capa de transporte. La capa de Red considera la división de grandes redes en redes más pequeñas para ayudar a su administración y a la comunicación entre esas pequeñas entidades. En la práctica las tareas de la capa 3 del Modelo OSI se asimilan a la Capa Internet del Modelo TCP/IP.

Funciones de la capa de red

La participación de la capa de red en la comunicación a través de red, se centran básicamente en las funciones de direccionamiento, encapsulación, enrutamiento y desencapsulación. Una introducción a esta tarea se describe brevemente a continuación.

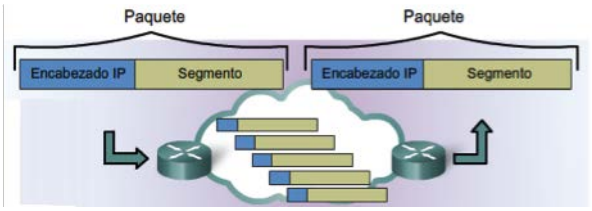


Imagen 7
Fuente: Propia, adaptada de currículo CCNA Exploration

Direccionamiento

A través del direccionamiento, la capa de red establece el direccionamiento o identificación de dispositivos de red. Cada dispositivo en una red debe tener una dirección de red única. La implementación práctica del direccionamiento en redes TCP/IP asigna a cada dispositivo de red, o host como también se conoce, una configuración específica que incluye la dirección IP.

Encapsulación

Los segmentos de capa de transporte se consideran como datos a encapsular a nivel de capa de red, a estos segmentos se les agrega encabezados que contienen, entre otra información, las direcciones de red los dispositivos origen y destino de los datos. Con los segmentos y los encabezados agregados se crea la PDU de capa de red, en el ámbito de redes TCP/IP la PDU correspondiente recibe el nombre de paquete IP.

Enrutamiento

El enrutamiento es la funcionalidad implementada en equipos enrutadores o separadores de diferentes redes, mediante la cual los paquetes son guiados a su destino a través de rutas disponibles, seleccionadas en función de la dirección IP y según diferentes criterios relacionados con la estructura de la red. En su viaje, los paquetes pueden tener la necesidad de pasar por varios enrutadores, el paso de la información de un enrutador a otro se conoce como salto.

Desencapsulación

Es la tarea realizada por la capa de Red en el destino al encontrarse que es efectivamente el destino final del paquete. Los encabezados de capa 3 se eliminan y los segmentos se pasan a la capa de Transporte.

El protocolo IP

El Protocolo IP, o Internet Protocol, corresponde a la implementación TCP/IP del direccionamiento de capa de red. IP versión 4 (IPv4), es el protocolo de red original de TCP/IP y la de mayor uso actual, es el protocolo estudiado en este curso. Una versión que avanza en su implementación es IPv6, la que puede operar junto a IPv4 y está llamado sustituirlo en el futuro. IP se considera un protocolo de bajo costo en el sentido que se limita a bridar las funciones necesarias para el envío de paquetes entre origen y destino a través de una red, por ejemplo no cumple funciones de seguimiento ni control de flujo. Las características fundamentales de IPv4 se describen brevemente a continuación:

IP como protocolo no orientado a conexión

A través del uso del protocolo IP no se establece conexión o comunicación entre origen y destino previo al envío de paquetes. Ante el envío de un paquete, el origen no sabe si el destinatario está activo en la red o si lo recibió, el destinatario tampoco sabe sobre el instante de la llegada del paquete. Una analogía de sistemas no orientados a conexión es el envío de información a través de cartas. El origen de la comunicación la envía sin notificación previa de ello.

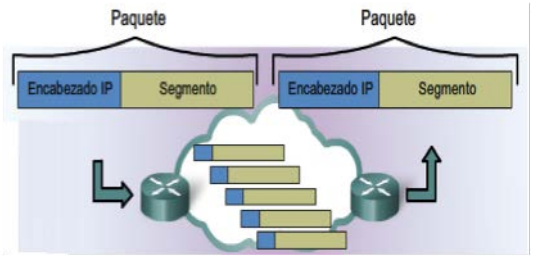


Imagen 8
Fuente: Propia, adaptada de currículo CCNA Exploration

IP como protocolo basado en el mejor esfuerzo

IP es un protocolo no confiable, ello no quiere decir que sea inconveniente usarlo ni que las comunicaciones basadas en él sean de mala calidad, es no confiable en el sentido que no contempla mecanismos de garantía de entrega. Si se incluyera en el paquete IP confirmación de recibo por parte del destinatario y otros elementos para el manejo de confiabilidad, se generaría mayor sobrecarga en detrimento de la eficiencia. La pérdida y retransmisión de información es gestionada por la capa de transporte. Parte de la información contenida en los encabezados habilita a los enrutadores intermedios a entregar los paquetes al siguiente dispositivo en la ruta y que este a su vez continúe con sus funciones de renvío, esto es lo que se conoce como mecanismo de entrega con base en el mejor esfuerzo.

IP protocolo independencia de los medios físicos de transmisión

Los paquetes IP se crean en la capa de red y son procesados por capas inferiores de tal manera que no interesa el medio físico a través de cual viaja la información, evidencia de esta afirmación la encontramos en las configuraciones IP de nuestras redes caseras, podemos conectar un computador portátil a la red bien sea a través de cable o de forma inalámbrica dentro del mismo esquema de direccionamiento.

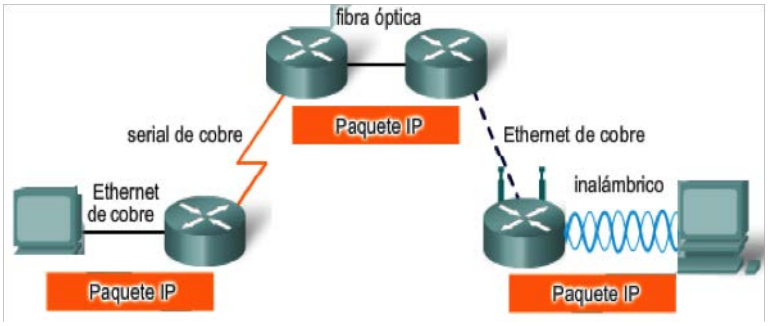


Imagen 9
Fuente: Propia, adaptada de currículo CCNA Exploration

Encabezados del paquete IP

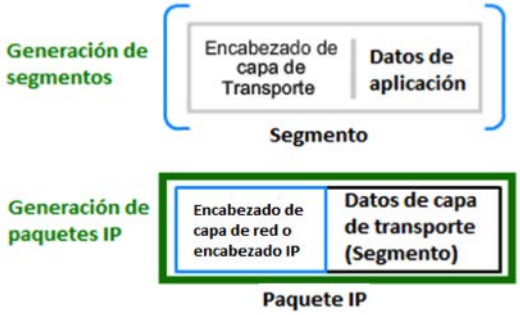


Imagen 10
Fuente: Propia, adaptada de currículo CCNA Exploration

La encapsulación de segmentos de capa de transporte junto con el encabezado IP corresponde a los paquetes o PDU de capa de Red. El encabezado IP es un conjunto de información adicional definida en varios campos de diferente tamaño, los cuales resultan útiles en la transmisión de paquetes a medida que se renvían a través de la red.

Algunos de los campos del encabezado IP son:

- **Dirección IP origen:** dirección IP del equipo en que origina el paquete.
- **Dirección IP de destino:** dirección IP de destino del paquete.
- **Tiempo de vida (TTL):** realmente no es una medida de tiempo, sino una cantidad que disminuye en uno por cada salto del paquete entre uno enrutador y otro. Si el TTL llega a cero el router que lo recibe lo elimina de tal manera que no siga haciendo parte del flujo de datos, evitando así posibles ciclos indefinidos de tales paquetes.
- **Tipo de Servicio (ToS):** es un valor usado para establecer prioridades en la transmisión de datos, por ejemplo, un router se puede configurar de tal manera que envíe con mayor prioridad los paquetes que transportan mensajes de voz.
- **Protocolo:** indica el tipo de contenido del paquete, permite pasar los datos al apropiado protocolo de capa de transporte. Ejemplos: 06 para TCP, 17 para UDP.

Paquetes IP transportan datos entre extremos

En el proceso de preparación de los datos en el origen, las PDU de capa de transporte se encapsulan en paquetes IP. Si el equipo destino se encuentra en la misma red que el origen, el paquete se envía sin necesidad del uso de un router.

En caso que los hosts extremos estén en redes distintas, el paquete necesitará cruzar uno o más routers. En cada enlace entre los diferentes routers, las decisiones de envío se basan en la información del encabezado del paquete IP. Inicialmente el host origen debe enviar el paquete hacia su Gateway, el cual corresponde a la dirección de la interfaz del router a la que se conecta la red local en que está el host. A cada host, dentro de su configuración TCP/IP, se le asigna o indica la dirección de Gateway por defecto.

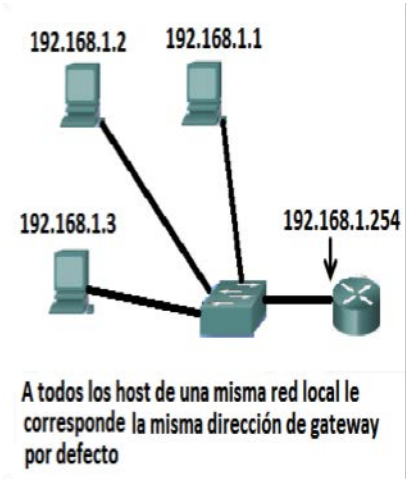
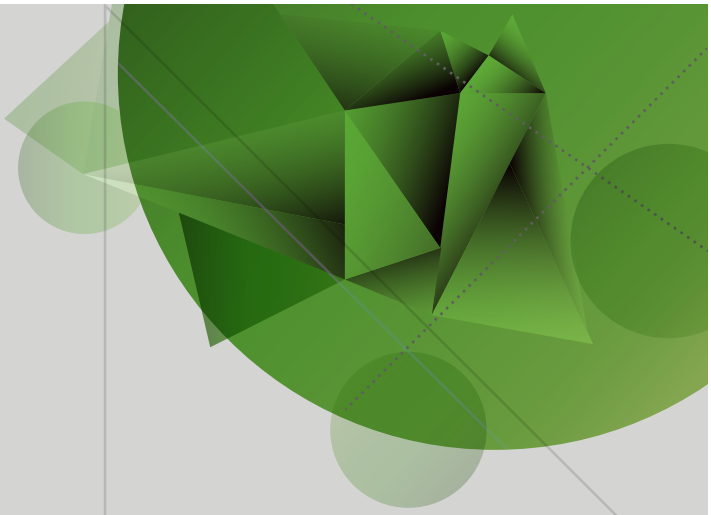


Imagen 11
Fuente: Propia, adaptada de currículo CCNA Exploration

2

Unidad 2

Direccionamiento IP e introducción al enrutamiento



Telemática I

Autor: Juan Carlos Ramirez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En la cuarta semana analizaremos el esquema de identificación de dispositivos y su agrupación según las redes y/o subredes a la que pertenezcan. Aquí se destacará la importancia de conocer y aprender sobre las funciones de enrutamiento.

U2

Metodología

Los estudiantes como centro activo de aprendizaje deben hacer la lectura y análisis permanente de este material, que les permite realizar una contextualización del tema, conociendo la teoría general y su aplicación práctica en contextos específicos.

U2

Desarrollo temático

Direccionamiento IP e introducción al enrutamiento

Introducción

Siguiendo el estudio de las funcionalidades involucradas en la comunicación a través de redes a la luz del Modelo OSI, en este capítulo se presentan detalles de la implementación práctica de las tareas de la capa de Red, una de estas tareas es el direccionamiento, el cual contempla tópicos como el esquema de identificación de dispositivos en función de la red a la que pertenecen, la agrupación de los diferentes equipos en subredes. IP es el esquema de direccionamiento implementado como parte de la pila de protocolos TCP/IP, estudiaremos específicamente el direccionamiento IP Versión 4 (IPv4), la estructura de direcciones IP, la división de redes en subredes, considerando en ello la división mediante el uso de máscaras de subred de longitud fija y de longitud variable, estos aspectos relacionados con IPv4 demandan habilidades de conversión entre números de los sistemas decimal y binario.

Otra tarea importante de la capa de red es el enrutamiento, encargado de decisiones de envío según la dirección del destino y apoyado en información para alcanzar el destino. Este capítulo tratará una breve introducción de las funciones de enrutamiento.

Direccionamiento jerárquico

Un sistema de direccionamiento jerárquico contempla diferentes niveles dentro de un esquema. Por ejemplo, si la Fundación Universitaria del Área Andina, sede Bogotá, envía un certificado a uno de sus estudiantes, utiliza una dirección que indica información de ubicación de varios niveles dentro de una jerarquía. En este caso el nivel más alto es el de ciudad o municipio, incluyendo posiblemente el departamento, por ejemplo: Barranquilla (Atlántico), un siguiente nivel contemplaría la ubicación de un edificio en una cuadra, por ejemplo, carrera 14 No 64 – 33 y finalmente un número de apartamento, por ejemplo 301, el cual hace referencia a que el mismo corresponde al primer apartamento del tercer piso. La empresa de envío utiliza esta información para hacer llegar la correspondencia, de tal manera que en el nivel más alto sólo se preocupa por hacerla llegar a la ciudad de Barranquilla, sin ocuparse de detalles específicos. Al llegar a la oficina de correo de la ciudad destino, se dispone de un funcionario que atienda la zona o el barrio destino, el funcionario ubica la dirección y la entrega en portería, desde donde se hace llegar al apartamento 301.

En la comunicación a través de redes IP, el direccionamiento lógico de equipos se realiza dentro del marco del esquema IPv4, un sistema jerárquico que en principio contempla dos niveles, el nivel de red y el de host. Los dispositivos enrutadores se ocupan del envío de paquetes a la red destino valiéndose de información de direccionamiento y enrutamiento a nivel de red. Cuando el paquete llega a la red, dispositivos intermedios al interior de la misma gestionan la entrega al equipo destino con base en la información a nivel de host. En redes de gran tamaño frecuentemente se realiza la división en redes más pequeñas o subredes, con lo cual se crea niveles intermedios de direccionamiento.

Direccionamiento IP

El direccionamiento IPv4 es un esquema jerárquico compuesto básicamente por los niveles de red y de host. A todo host participante en una red IP se debe asignar una configuración IP, que permite identificar en un primer nivel la red a la que pertenece el host. El eficaz funcionamiento de grandes redes está muy ligado al adecuado diseño y buena planificación del direccionamiento. La dirección IP de un host es asignada a la interfaz de red del host. Algunos equipos como routers y servidores pueden tener varias interfaces, a cada una de las interfaces se ha de asignar una configuración IP.

Formato de las direcciones IP

Los paquetes IP que transportan datos contienen campos para las direcciones IP origen y destino. Con el fin de conocer más detalles del direccionamiento IP conviene tratar la estructura de las direcciones IP. Básicamente, y como es tratado a nivel de máquina, una dirección IP corresponde a una secuencia de 32 bits, sin embargo, para facilitar su lectura por parte de las persona, los 32 dígitos binarios se agrupan en cuatro bytes u octetos, y los valores binarios correspondientes se presentan en formato decimal separado por un punto, esta notación decimal punteada es usada al asignar una configuración IP.

- Ejemplo de dirección IP

  Secuencia binaria de la dirección IP en 4 octetos:

  10101100.00010000.00000100.00010100

  Dirección IP en notación decimal punteada: 172.16.4.20

Partes de una dirección IP

Básicamente una dirección IP está compuesta por dos partes: la porción o identificador de red que corresponde al nivel más alto de la jerarquía, y la porción de host, la cual identifica a un host específico en la red, todos los hosts de una misma red deben coincidir en la porción de red.

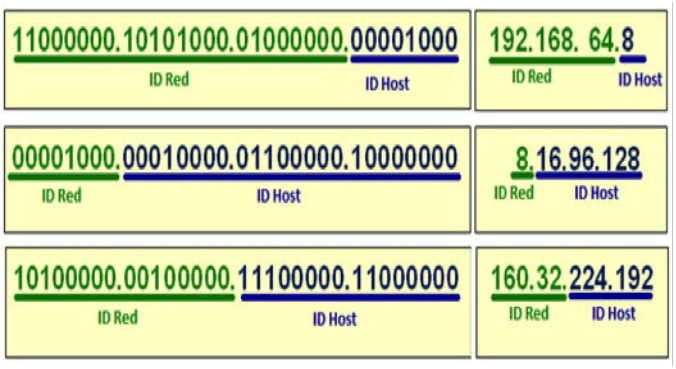


Imagen 1
Fuente: Propia, adaptada de currículo CCNA Exploration

La cantidad de bits que se toma para identificar las porciones de red y de host es variable, se toma siempre los bits de mayor orden como parte de red y los restantes como parte de host. La figura muestra algunas posibles distribuciones de los bits de direcciones IP.

Dirección de red y de broadcast

Son múltiples las posibilidades de direcciones IP correspondientes a una red, de todas ellas hay dos direcciones especiales, la dirección de red y la de broadcast, las cuales no se pueden asignar hosts individuales, cualquier otra dirección diferente a las de red y de broadcast son direcciones asignables a los diferentes equipos de la red.

Dirección de la red

La dirección de la red es la de menor valor de todo el rango de direcciones, escrita en binario, es aquella en la cual todos los bits de la porción de host son cero (0). Es la dirección utilizada para identificar a la red como un todo.

Imagen 2
Fuente: Propia, adaptada de currículo CCNA Exploration

Dirección de broadcast

La dirección de broadcast es la de más alto valor dentro del rango, lo que significa que, escrita en binario, los bits de la porción de host de la dirección son todos uno (1). Es una dirección especial utilizada para envío de mensajes a todos los hosts de la red.

Imagen 3
Fuente: Propia, adaptada de currículo CCNA Exploration

Longitud de prefijos de red y máscara de subred

Una pregunta interesante es ¿Cómo saber cuántos bits de una dirección IP dada corresponden al identificador de red y cuantos al identificador de host?, la respuesta a este interrogante está asociada a los dos ítems descritos a continuación.

Longitud de prefijo

Un término importante asociado a temas de direccionamiento es el de longitud de prefijo, el cual hace referencia a la cantidad de bits que conforman la porción de red, con tal propósito, al escribir direcciones IP en formato decimal, es usual acompañarla de la longitud de prefijo, separada de una barra inclinada. Por ejemplo, al escribir la dirección IP 172.16.41.10 /24, con /24 se indica que los primeros 24 bits corresponden a la porción de red, con lo cual los 8 bits restantes se emplean como porción de host.

La máscara de subred

Cuando se configura un host en una red IP, esta configuración además de la dirección IP incluye la máscara de subred. La máscara de subred es también una secuencia de 32 bits e indica qué parte de toda la dirección identifica la red y qué parte identifica al host. Escrita en binario, la totalidad de bits de orden superior colocados en "1s" indican la porción de red y los bits restantes se colocan en "0s" para representar la porción de host.

Cuando un host necesita enviar paquetes, determina las redes en la que se encuentra ubicado él mismo y el host destino, esto lo realiza con base en la operación AND. La red origen corresponde al resultado de la operación AND entre la dirección del origen y la máscara de subred, de forma similar se halla la red de destino pero usando la dirección IP del destino. Si los resultados coinciden significa que los dispositivos se encuentran en la misma red, por tanto el paquete se puede enviar localmente, en caso contrario el emisor lo envía al Gateway

por defecto para que sea enviado a otra red. El Gateway por defecto de los hosts en una red la dirección IP de la interfaz del router a la que se conecta la red, el Gateway hace parte de la configuración IP del host. A manera de ejemplo de uso de la máscara de red se analiza el escenario mostrado en la figura adjunta.

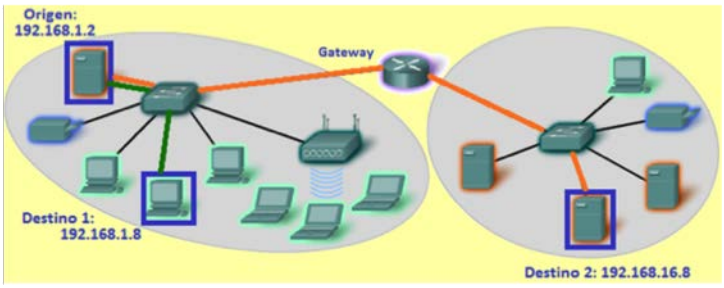


Imagen 4
Fuente: Propia, adaptada de currículo CCNA Exploration

La figura muestra que origen y destino 1 se encuentran en la misma red, mientras que origen y destino 2 se encuentran en redes diferentes.

Los cálculos asociados indican efectivamente que origen y destino 1 están en la misma red, (192.168.1.2) mientras que destino 2 se encuentra en una red diferente (192168.16.0), en este caso la responsabilidad de envío se deja al router que conecta redes distintas.

Los routers usualmente cuentan con varias interfaces de red, a las que se conectan redes locales u otros routers, cada interfaz se configura con una dirección IP y mascara de red. Dado que los routers toman decisiones de renvío de paquetes, deben primero determinar la red de destino para decidir la interfaz de salida, con este propósito también utilizan la operación AND como antes se describió.

Direcciones de hosts		
Dir. IP Origen:	11000000.10101000.00000001.00000010	192.168.1.2
Dir. IP Destino 1:	11000000.10101000.00000001.00001000	192.168.1.8
Dir. IP Destino 2:	11000000.10101000.00010000.00001000	192.168.16.8
Mascara de Red:	11111111.11111111.11111111.00000000	255.255.255.0
Determinación de la red de origen		
Dir. IP Origen:	11000000.10101000.00000001.00000010	192.168.1.2
AND		
Mascara de Red:	11111111.11111111.11111111.00000000	255.255.255.0
Red del origen:	11000000.10101000.00000001.00000000	192.168.1.0
Determinación de la red de destino 1		
Dir. IP Destino 1:	11000000.10101000.00000001.00001000	192.168.1.8
AND		
Mascara de Red:	11111111.11111111.11111111.00000000	255.255.255.0
Red del destino 1:	11000000.10101000.00000001.00000000	192.168.1.0
Determinación de la red de destino 2		
Dir. IP Destino 2:	11000000.10101000.00010000.00001000	192.168.16.8
AND		
Mascara de Red:	11111111.11111111.11111111.00000000	255.255.255.0
Red del destino 2:	11000000.10101000.00000001.00000010	192.168.15.0

Imagen 5
Fuente: Propia, adaptada de currículo CCNA Exploration

Cantidad de host en una red

El tamaño de una red, en términos de la cantidad máxima de host que podría contener, depende de la longitud del prefijo o cantidad de bits de la porción de red. Teniendo en cuenta que la dirección IP está compuesta de 32 bits, si la longitud de la máscara es de m bits, quedan n = 32 – m bits para representar la porción de hosts.

n = 2	n = 3	
00	000	100
01	001	101
10	010	110
11	011	111

Imagen 6
Fuente: Propia, adaptada de currículo CCNA Exploration

Por ejemplo, si n=2 bits para porción de host, en formato binario se tiene cuatro posibles identificadores de host, si n=3, el número de posibilidades sería 8. En ambos casos las diferentes posibilidades se muestran en la figura adjunta.

En general la cantidad total de valores diferentes, en función del número n de bits de la porción de host, corresponde a 2^n. Teniendo en cuenta que la dirección más baja y la más alta de todas las posibles no se pueden asignar a hosts, por ser las direcciones de la red y de broadcast, respectivamente, encontramos que para una red cuya porción de host tiene tamaño n, el número máximo de direcciones de host que puede haber en la red está dado por:

$$N = 2^n - 2.$$

Cálculo de direcciones de host y dirección de broadcast

El rango útil de direcciones de host se refiere al intervalo de direcciones que pueden asignarse a hosts dentro de una red. En aras de calcular de manera ágil el rango útil de direcciones de host y la dirección de broadcast, a partir de la dirección de la red y la longitud del prefijo, presentamos los siguientes ejemplos:

Ejemplo 1: cálculo de la dirección de broadcast y el rango de direcciones útiles para la Red 160.80.40.0/25.

Longitud de prefijo = 25. (25 bits para red)

Tamaño de la porción de host: n = 32 – 25 = 7

Cantidad total de valores de host: N' = $2^7 = 128$ (valor que incluye las direcciones de red y broadcast), este rango de 128 valores comienza en 0 y termina en 127, por tanto:

Dirección de broadcast: 160.80.40.127/25.

Rango de direcciones útiles: va desde la dirección siguiente a la de red, o segunda dirección del rango, hasta la inmediatamente anterior a la de broadcast, penúltima dirección, por tanto el rango de direcciones para asignar a hosts individuales es:

160.80.40.1/25 hasta 160.80.40.126/25.

Ejemplo 2: cálculo de la dirección de broadcast y el rango de direcciones útiles para la Red 160.80.48.0/22.

Longitud de prefijo = 22.

Tamaño de la porción de host: n = 32 – 22 = 10

Cantidad total de valores de host: N' = $2^{10} = 1024.$ En este ejemplo la cantidad de bits de la porción de host toma todo el cuarto octeto y los dos bits menos significativos del tercero. Podemos hallar los valores pedidos escribiendo en binario los dos últimos números de la dirección de red, resaltando en ello la porción de host.

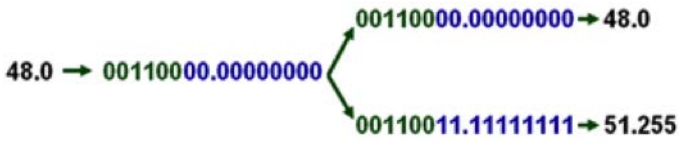


Imagen 7
Fuente: Propia, adaptada de currículo CCNA Exploration

Tenemos entonces que la dirección de broadcast es: **160.80.51.255** y el rango de direcciones asignables a hosts es:

160.80.48.1 hasta 160.80.51.254.

El número total de direcciones IP es 1024, el cuarto octeto sólo da 256 valores posibles, de 0 a 255; dado que 1024 es exactamente cuatro veces 256, por las 256 posibilidades del último octeto se requiere cuatro valores del tercero, el primero de ellos es el valor del tercer octeto de la dirección de la red. La cantidad de valores que se requiere tomar del tercer octeto (rango de octeto) corresponde a 2 elevado al número de bits de ese octeto que hacen parte del identificador de host.

Ejemplo 3: cálculo de la dirección de broadcast y el rango de direcciones útiles para la Red 170.80.64.0/20.

Longitud de prefijo = 20.

Tamaño de la porción de host: n = 32 – 20 = 12.

Cantidad total de valores de host: N' = $2^{12} = 4096$. La cantidad de bits de la porción de host toma los ocho bits del cuarto octeto y cuatro del tercero.

Rango de tercer octeto: $2^{4} = 16$ (comenzando en 64), por tanto el rango total de direcciones toma 16 valores consecutivos en el tercer octeto comenzando 64, el rango correspondiente va de **170.80.64.0 hasta 170.80.79.255.**

La dirección de broadcast es 170.80.79.255 y el rango de direcciones útiles es:

De 170.80.64.1 hasta 170.80.79.254.

Patrones de tráfico

En este aparte nos referimos a los diferentes patrones de tráfico, en función de la cantidad de destinatarios de un mensaje, los patrones de tráfico son los siguientes:

Tráfico unicast

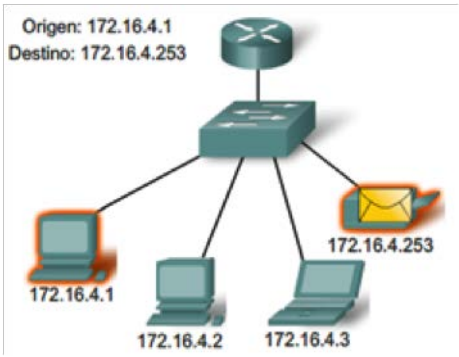


Imagen 8
Fuente: Propia, adaptada de currículo CCNA Exploration

Este patrón de tráfico tiene como destinatario un host individual, por tanto la dirección IP de destino debe estar dentro del rango de direcciones válidas para hosts. La comunicación unicast es utilizada en la comunicación entre hosts. El tráfico unicast, de ser necesario podría ser transferido a otras redes por parte de los enrutadores.

Tráfico de broadcast

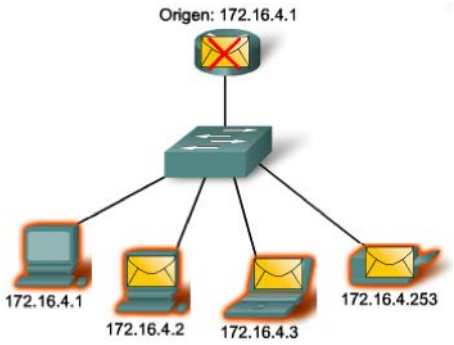


Imagen 9
Fuente: Propia, adaptada de currículo CCNA Exploration

Patrón de tráfico que tiene como destinatario todos los host de la red, por tanto los paquetes tendrían en el campo de destino la correspondiente dirección de broadcast de la red. Este tipo de comunicación es empleado para localizar equipos o servicios específicos de los que no se conoce la dirección. Un ejemplo en el que se usa tráfico de broadcast corresponde a las solicitudes DHCP.

El tráfico de broadcast podría degradar notablemente el rendimiento de la red y por tanto es altamente recomendable limitarlo para reducir sus efectos negativos. Al dividir redes en subredes se reduce el tamaño de los dominios de broadcast.

Tráfico multicast

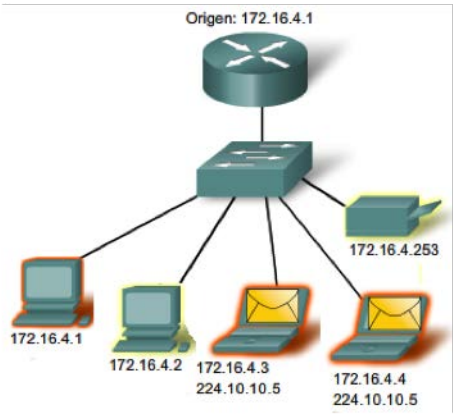


Imagen 10
Fuente: Propia, adaptada de currículo CCNA Exploration

Tiene como destino un grupo específico de hosts. Un ejemplo en el que se usa transmisión de multicast es la transmisión de audio y video de conferencias en línea e intercambio de información de enrutamiento por medio de protocolos de enrutamiento. Las direcciones de destino en el tráfico multicast pertenecen a rangos de direcciones por fuera de las direcciones asignables a host individuales.

Direccionamiento con clase

Antiguamente, el espacio total de direcciones IP se agrupaban en 5 clases: por una parte las clases A, B y C conocidas como direcciones comerciales, utilizadas para el direccionamiento de las diferentes redes, y por otra parte la clase D reservada para multicast, y la E, para uso experimental y posible uso futuro. En la actualidad se mantiene la imposibilidad de usar las direcciones clase D y E como direcciones de red.

Cada clase comercial tiene una máscara de subred por defecto. El criterio de agrupamiento se basa en el valor binario del primer octeto. La siguiente tabla resume detalles de las direcciones según su clase.

Clase	Rango binario primer octeto	Rango decimal del primer octeto	Distrib de octetos	Longitud prefijo
A	00000000 - 01111111	1 - 127 (*)	R.H.H.H	8
B	10000000 - 10111111	128 - 191	R.R.H.H	16
C	11000000 - 11011111	192 - 223	R.R.R.H	24
D	11100000 - 11101111	224 - 239		
E	11110000 - 11111111	240 - 255		

(*): los valores 0 y 127 en primer octeto no son utilizados para direcciones de host.

Tabla 1

Fuente: Propia, adaptada de currículo CCNA Exploration

El cuadro anterior nos indica la clase de dirección a partir del valor del primer octeto, esta información resultaría importante ya que según la clase de dirección se sabe cuál es la máscara de subred, lo que significa que se tiene información de la cantidad de bits que conforman la porción de red.

Direcciones IP públicas y privadas

Una dirección IP pública es aquella que se utilizada para acceso a la Internet, los paquetes IP con este tipo de direcciones en los campos origen y destino son renviados por los enrutadores de acceso a la red mundial con esas mismas direcciones. Para conectarse a Internet un host requiere una dirección pública, sin embargo es de anotar que la cantidad de equipos

a nivel mundial que hacen parte de alguna red, y que en cualquier momento podrían conectarse a Internet, es superior al número de direcciones válidas existentes. Del espacio de direccionamiento total, la mayoría son direcciones públicas y una parte de ellas se reservan como direcciones IP privadas.

Las direcciones privadas son de uso libre en redes locales no conectadas a la Internet, un paquete IP que contenga direcciones privadas no es enrutado hacia la Internet por los dispositivos de acceso a Internet.

Los rangos reservados para direcciones privadas son:

- **Desde 10.0.0.0 a 10.255.255.255 (la red 10.0.0.0 /8)**
- **Desde 172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)**
- **Desde 192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)**

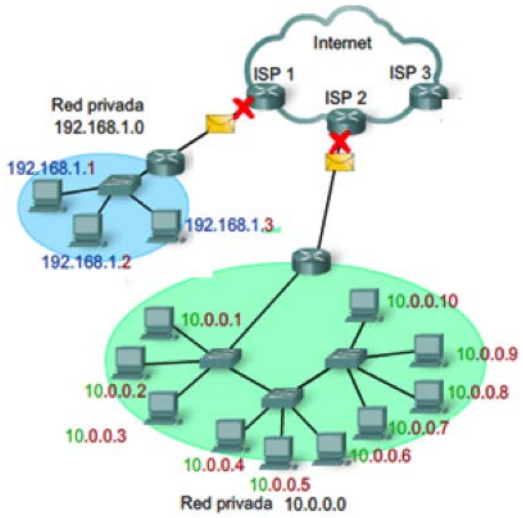


Imagen 11
Fuente: Propia, adaptada de currículo CCNA Exploration

Muchos hosts en distintas redes pueden utilizar las mismas direcciones privadas, esto no da lugar a conflictos de direccionamiento debido a que las redes privadas permanecen aisladas. En este punto surge un interrogante clave ¿Qué sucede si un equipo con dirección IP privada ha de conectarse a la internet? Como respuesta se tiene que debe existir un dispositivo en las fronteras de la red local que temporalmente asigne o "preste" una dirección pública al host, este proceso de conversión de dirección recibe el nombre de **Traducción de Direcciones de Red (NAT o Network Address Translator).** NAT es un servicio que debe configurarse en los enrutadores que conectarían la red privada a la Internet.

Planificación del direccionamiento

La asignación de direcciones de red, y en general la administración del espacio de almacenamiento debe ser planificada y documentada, la adecuada planificación ayuda a evitar el uso duplicado de direcciones y a establecer medidas para controlar el rendimiento, el acceso, la seguridad y administración de la red. Con una planificación y documentación correctas del direccionamiento de red, es posible identificar el dispositivo de la red con problemas de dirección. La planificación debe considerar las situaciones en las cuales usar direcciones privadas y el uso de NAT.

Asignación de direcciones IP

Todo equipo que participa en una red TCP/IP comúnmente cuenta con una configuración IP que incluye la dirección IP, la máscara de subred y el Gateway por defecto. Existen dos mecanismos de asignación de configuración IP, asignación estática y asignación dinámica.

Asignación estática de configuración IP

Es realizada manualmente en los equipos por un administrador de red, esta configuración es permanente a menos que el administrador la cambie manualmente, se requiere que se guarde registro de las configuraciones asignadas con el fin de evitar duplicidad de direcciones. La configuración estática demanda una carga de trabajo para el administrador y se corre riesgo de cometer errores al digitar la configuración, pero por razones de seguridad y control de acceso es muy recomendable aplicarla en algunos equipos especializados de la red, aquellos que son punto de concentración para el tráfico de red, como servidores que brindan servicios de red, y aquellos accesibles desde Internet.

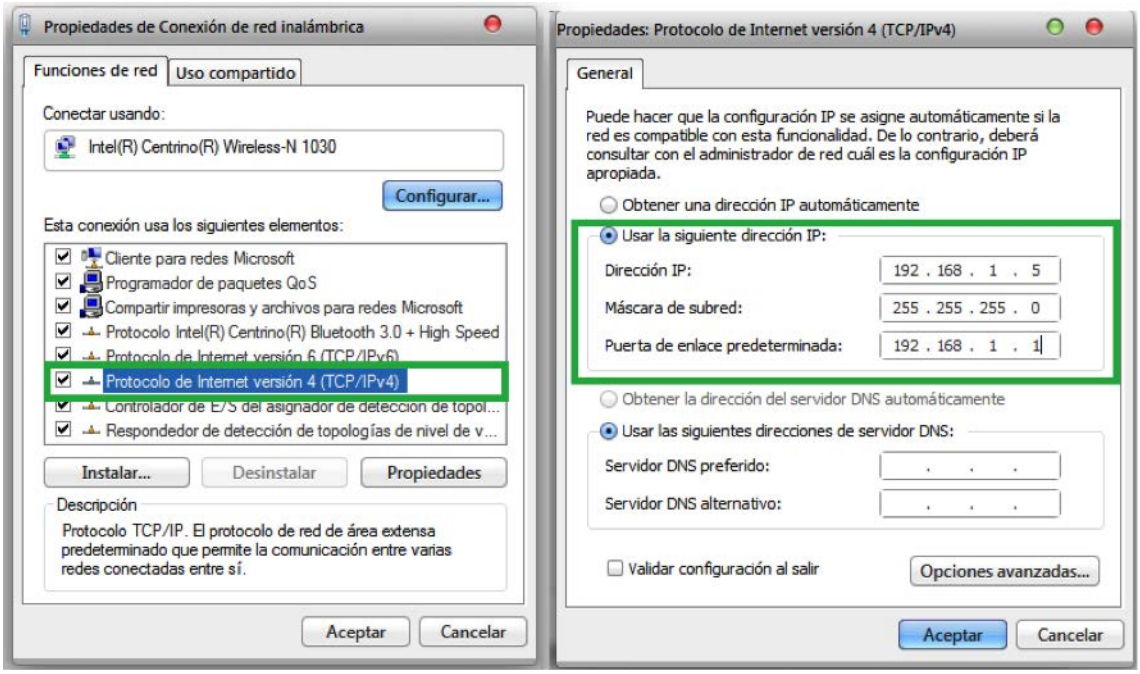


Imagen 12. Ventanas para la configuración IP
Fuente: Propia.

Asignación Dinámica de configuración IP

Se lleva a cabo mediante el uso del servicio **DHCP**, o **Protocolo de Configuración Dinámica de Host**, descrito en la unidad 2. DHCP asigna configuración IP de forma automática o dinámica. El servidor DHCP debe ser previamente configurado con un grupo o pool de direcciones IP para ser asignado como parte de la configuración IP de los equipos de la red que lo soliciten. La planificación debe considerar cuales direcciones se usarán para direccionamiento estático y excluirlas del pool DHCP. En redes con gran cantidad de equipos por lo general se usa DHCP como método de configuración IP, ya que reduce la carga de trabajo administrativo errores de direccionamiento.

La IANA o Autoridad de Números Asignados de Internet administraba directamente todo el espacio de direcciones IPv4 hasta mediados de la década de los años noventa, desde ese entonces, se delegó la administración del espacio restante a otras entidades regionales llamadas Registros Regionales de Internet (RIR). Los principales registros son:

- **AfriNIC:** African Network Information Centre, región África.
- **APNIC** Asia Pacific Network Information Centre, región Asia y Pacífico.
- **ARIN:** American Registry for Internet Numbers, región América del Norte.
- **LACNIC:** Regional Latin-American and Caribbean IP Address Registry, América Latina y el Caribe.
- **RIPE NCC:** Reseaux IP Europeans, Europa, Medio Oriente y Asia Central.

División de redes

Por diversas razones es aconsejable la división de redes grandes en grupos de redes más pequeñas o subredes. La división en subredes debe atender criterios robustos de diseño y planificación. La división de una red mediante la creación de diferentes grupos a partir de los equipos que la conforman podría llegar a contemplar la ubicación física de los equipos, sus propósitos o finalidad, sus propietarios o administradores.

Beneficios de la división en subredes

A mayor cantidad de host que se encuentren en una red puede haber mayores motivaciones para dividir la red en redes más pequeñas y aprovechar así sus beneficios. Entre los beneficios que se pueden obtener de la división de redes se cuentan los señalados en los siguientes apartes.

La división de redes favorece el rendimiento

En una redes de grandes empresas normalmente hay grupos de equipos de usuario que requieren comunicarse frecuentemente entre ellos, agrupar estos equipos para que formen una subred disminuye el tráfico innecesario a través de toda la infraestructura.

Un factor que puede reducir seriamente el rendimiento de una red es el tráfico de broadcast.

Lo ideal es procurar que los broadcast se contengan en segmentos locales o dominios de broadcast, la reducción del tamaño de los dominios de broadcast se logra con mediante la división de redes en subredes.

La división de redes favorece la seguridad

Es enorme la cantidad de redes en el mundo que se conectan a la Internet, sin embargo, el hecho que tales redes se conecten a red global no significa que todos sus recursos deban estar disponibles al público general. La división en pequeñas redes ayuda a restringir el acceso a los recursos de la red, permitiendo el acceso público solo a determinadas porciones, con lo que se contribuye a la seguridad de la red. Las restricciones de acceso a las redes se implementan equipos especializados con funciones de firewall en las fronteras de la red.

La división de redes favorece la administración de direcciones

Son millones los host que se encuentran conectados a la internet, dado que las redes normalmente se dividen en subredes, cada equipo intermedio requiere tener conocimiento de ruta para alcanzar el equipo fronterizo al cual se conecta la red y no necesita conocer las direcciones de todos los host que pertenecen a la red.

Cálculos asociados a la división en subredes

Mediante la división en subredes se puede crear varias redes más pequeñas a partir de un solo rango de direcciones IP. Cada una de las subredes creadas se conecta a una interfaz de un router, esta interfaz debe tener una dirección IP perteneciente al rango valido de la red conectada.

La división en subredes se fundamenta en la reasignación o "préstamo" de algunos bits de host de mayor orden para que sean parte del identificador de red, este préstamo de bits da lugar a una mayor longitud de prefijo.

Imagen 13
Fuente: Propia, adaptada de currículo CCNA Exploration

Tomando un bit de la porción de host, se tendría dos posibilidades binarias de identificadores de subred, al tomar dos bits se tendría 4 posibilidades. En general, si de la cantidad "n" de bits de la porción de host se toman "k" bits como identificador de subred y "j = n – k", como identificador de host, se obtiene 2^k subredes y cada una con un espacio total de direcciones de 2^j. La cantidad total de direcciones de cada subred corresponde a la cantidad de direcciones de la red original dividido por 2^k.

A manera de ejemplo consideremos la red 192.168.1.0/24 en la cual hay 8 bits para la porción de host, lo que corresponde a un espacio total de $2^8 = 256$ direcciones.

Al tomar 3 bits para porción de subred, se obtiene $2^3 = 8$ subredes, quedando 5 bits para host, cada subred abarca un espacio de $2^5 = 32$ direcciones, el cual corresponde a 256 dividido por 8. La nueva máscara tiene una longitud de prefijo de 27 (24 + 3) y su escritura en notación decimal punteada es 255.255.255.224.

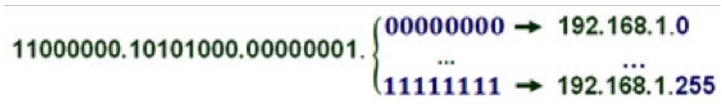


Imagen 14
Fuente: Propia, adaptada de currículo CCNA Exploration

El cuadro adjunto resume la división de la red. Se muestra las porciones de red, subred, así como los primeros y últimos números de host de cada subred en formato binario, también se muestra la representación decimal de primera y última dirección de cada subred, es decir las direcciones de red y de broadcast respectivamente.

	Porción o Identificador de: Red	Subred	Host	Rango de direcciones
0	11000000.10101000.00000001	000	00000 ... 11111	192.168.1.0 ... 192.168.1.31
1	11000000.10101000.00000001	001	00000 ... 11111	192.168.1.32 ... 192.168.1.63
2	11000000.10101000.00000001	010	00000 ... 11111	192.168.1.64 ... 192.168.1.95
3	11000000.10101000.00000001	011	00000 ... 11111	192.168.1.96 ... 192.168.1.127
4	11000000.10101000.00000001	100	00000 ... 11111	192.168.1.128 ... 192.168.1.159
5	11000000.10101000.00000001	101	00000 ... 11111	192.168.1.160 ... 192.168.1.191
6	11000000.10101000.00000001	110	00000 ... 11111	192.168.1.192 ... 192.168.1.223
7	11000000.10101000.00000001	111	00000 ... 11111	192.168.1.224 ... 192.168.1.255

Imagen 14
Fuente: Propia, adaptada de currículo CCNA Exploration

- La dirección de la primera subred corresponde a la dirección de la red original, pero con un prefijo o máscara diferente.
- La dirección de cada subred, a partir de la segunda, se obtiene sumando a la anterior la cantidad total de direcciones por subred.
- La dirección de broadcast de cada subred, a partir de la segunda, se obtiene sumando a la anterior a la dirección de broadcast de la anterior subred la cantidad total de direcciones por subred.

El desglose del rango de direcciones se muestra a continuación.

Subred	Dirección de red	Rango útil para host	Dirección de broadcast
0	192.168.1.0/27	192.168.1.1 – 192.168.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 – 192.168.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 – 192.168.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97. – 192.168.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 – 192.168.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 – 192.168.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 – 192.168.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 – 192.168.254	192.168.1.255

Tabla 2
Fuente: Propia, adaptada de currículo CCNA Exploration

Como ejemplo adicional considérese una empresa que dispone del espacio de direcciones 160.40.8.0/19 y requiere la creación de seis subredes para sus sucursales. Según estas necesidades tenemos el siguiente análisis que nos conduce al esquema de direccionamiento.

Dirección de la red: 160.40.64.0/19.

Mascara de red original: 255.255.224.0.

Cantidad total de direcciones: al haber 13 bits para la porción de host, la cantidad total de direcciones IP es $2^{13} = 8192$.

Dirección de broadcast: La cantidad de bits de la porción de host toma los ocho bits del cuarto octeto y cinco del tercero, lo que indica que la amplitud de valores del tercer octeto para esta red es $2^5 = 32$, con valor inicial 64, por tanto el conjunto de valores del tercer octeto para la red va de 64 a 95, la dirección de broadcast es la última de todas las posibilidades, es decir, 160.40.95.255.

Cantidad de bits requeridos para porción de subred: dado que se debe crear seis subredes, la cantidad de bits a tomar para la porción de subred es 3, (al tomar dos sólo se obtendría 4 subredes).

Máscara requerida para la división: al incrementar la longitud del prefijo de 19 a 22, la nueva máscara de subred es 255.255.252.0 (o /22).

Cantidad de subredes resultante: aunque la necesidad de la empresa es de 6 subredes, al tomar 3 bits como porción de subred se obtiene un total de $2^3 = 8$ subredes.

Cantidad total de direcciones por subred: al quedar 10 bits para la porción de host, la cantidad total de direcciones por cada subred es de $2^{10} = 1024\ (= 4x256)$. Los 2 últimos bits del tercer octeto son de la porción de host, con lo que la amplitud del tercer octeto para cada subred es de $2^2 = 4$, valor que marca la variación que permite obtener las subsiguientes direcciones de cada subred.

Dirección de las subredes: la dirección de la primera subred es la misma dirección de la red original pero con el nuevo prefijo, es decir 160.40.64.0/22, para obtener las subsiguientes direcciones de subred se suma a la anterior amplitud del tercer octeto para subred.

Dirección de broadcast de cada subred: la dirección de broadcast de cada subred es la última de su rango, el rango total de la subred incluye variación de 4 en el tercer octeto, en el caso de la primera subred el rango inicia en 64 y termina en 67, por tanto la dirección de broadcast es 160.40.67.255, las direcciones de broadcast de las subsiguientes subredes se obtiene sumando a la anterior la amplitud del tercer octeto.

El siguiente cuadro resume el cálculo correspondiente:

Subred	Dirección de red	Rango útil para host	Dirección de broadcast
0	160.40.64.0/22	160.40.64.1 a 160.40.67.254	192.168.67.255
1	160.40.68.0/22	160.40.68.1 a 160.40.71.254	192.168.71.255
2	160.40.72.0/22	160.40.72.1 a 160.40.75.254	192.168.75.255
3	160.40.76.0/22	160.40.76.1 a 160.40.79.254	192.168.79.255
4	160.40.80.0/22	160.40.80.1 a 160.40.83.254	192.168.83.255
5	160.40.84.0/22	160.40.84.1 a 160.40.87.254	192.168.87.255
6	160.40.88.0/22	160.40.88.1 a 160.40.91.254	192.168.91.255
7	160.40.92.0/22	160.40.92.1 a 160.40.95.254	192.168.95.255

Tabla 3
Fuente: Propia, adaptada de currículo CCNA Exploration

VLSM (Mascaras de Subred de Longitud Variable)

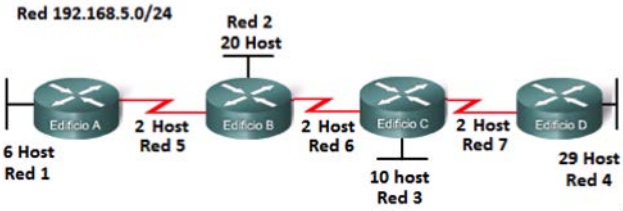


Imagen 15
Fuente: Propia, adaptada de currículo CCNA Exploration

Los ejemplos tratados anteriormente son una muestra de división en los cuales todas las subredes obtenidas tienen la misma cantidad de direcciones, esto en razón al uso de una misma máscara o máscara de longitud fija, sin embargo, las redes de las empresas presentan necesidades de división con diferentes cantidades de host por subred. Por ejemplo, los enlaces WAN entre 2 routers solamente requieren 2 direcciones, mientras que las redes de usuarios pueden requerir decenas o cientos de direcciones. Los administradores o responsable deben tomar en consideración este aspecto y el posible crecimiento al planificar el esquema de direccionamiento de la red.

La división de subredes mediante el uso de máscaras de longitud fija generalmente da lugar a la pérdida grandes cantidades de direcciones de host. Por ejemplo, la figura muestra una estructura que requiere de un total de 7 subredes separadas, lo cual demanda la toma de 3 bits para subred, dado que el prefijo de la dirección disponible es 24, la nueva máscara ha de tener 27 bits y cada una de las 8 subredes resultantes contarían con un total de 32 direcciones, pero vemos por ejemplo que los enlaces entre routers necesitan únicamente 2 direcciones en cada subred, al tomar dos direcciones válidas de una subred las demás direcciones del bloque no pueden ser usadas en otra red conectada a otra interfaz, dándose un gran desperdicio. En los segmentos LAN también se presenta notable desperdicio de direcciones de red, las que podrían usarse para crecimiento futuro de la red de usarse un esquema eficiente.

La necesidad de subredes de diferentes tamaños y la escases de direcciones IPv4 dio lugar al diseño de un esquema basado en Mascara de Subred de Longitud Variable o VLSM (*Variable Length Subnet Mask*), concepto que se asocia a la subdivisión de una subred. VLSM permite maximizar el aprovechamiento de direcciones al utilizar máscara de longitud más corta para subredes que demandan mayor cantidad de direcciones y máscaras más largas para aquellas subredes con menor demanda de direcciones. La definición del esquema de direccionamiento debe considerar primero las necesidades de subredes con mayor número de host.

Requisito	Mínimo posible	Bits de host	Prefijo
Red 4 29 host	32 host	5	/27
Red 2 20 host	32 host	5	/27
Red 3 10 host	16 host	4	/28
Red 1 6 host	8 host	3	/28
Red 5 2 host	4 host	2	/30
Red 6 2 host	4 host	2	/30
Red 7 2 host	4 host	2	/30

Tabla 4
Fuente: Propia, adaptada de currículo CCNA Exploration

Basados en la figura anterior presentamos un ejemplo de uso de VLSM, omitiendo los detalles binarios de los cálculos. La tabla adjunta muestra, de mayor a menor, las necesidades de direcciones y el tamaño mínimo que la satisface. Se debe contar las direcciones requeridas, las direcciones de red y de broadcast de cada subred.

La tabla siguiente muestra el resumen de un esquema adecuado de división.

Red a dividir 192.168.5.0/24			
Número total de Dir	Dirección de subred	Rango útil para hosts	Dirección de broadcast
32 host	192.168.5.0/27	192.168.5.1 - 192.168.5.30	192.168.5.31
32 host	192.168.5.32/27	192.168.5.33 192.168.5.62	192.168.5.63
16 host	192.168.5.64/28	192.168.5.65 192.168.5.78	192.168.5.79
8 host	192.168.5.80/29	192.168.5.81 192.168.5.86	192.168.5.87
4 host	192.168.5.88/30	192.168.5.89 192.168.5.90	192.168.5.91
4 host	192.168.5.92/30	192.168.5.93 192.168.5.94	192.168.5.95
4 host	192.168.5.96	192.168.5.97 192.168.5.98	192.168.5.99

Tabla 5
Fuente: Propia, adaptada de currículo CCNA Exploration

Otra posibilidad de realizar la división se presenta en la siguiente tabla, en la cual se omite la dirección de broadcast y el rango útil de direcciones de host de cada subred. Inicialmente la red original se divide en cuatro subredes y luego se aplica subdivisiones sucesivas según las necesidades.

Red a dividir 192.168.5.0/24				
Dirección de Subred				Uso
192.168.5.0/26	192.168.5.0/27			Red 1
	192.168.5.32/27			Red 2
192.168.5.64/26	192.168.5.64/27	192.168.5.64/28		Red 3
		192.168.5.80/28	192.168.5.80/29	Red 4
			192.168.5.80/29	Disponible
	192.168.5.96/27	192.168.5.96/28	192.168.5.96/30	Red 5
			192.168.5.100/30	Red 6
			192.168.5.104/30	Red 7
			192.168.5.108/30	Disponible
		192.168.5.112/28		Disponible
192.168.5.128/26				Disponible
192.168.5.192/26				Disponible

Tabla 6
Fuente: Propia, adaptada de currículo CCNA Exploration

Algunas pruebas de la capa de red

En la detección de fallas de una red existen diferentes mecanismos y utilidades que permiten identificar el origen de la anomalía y así poder proceder a su corrección, entre los diferentes tipos se cuentan las pruebas de capa de red.

Ping

Es una utilidad cuya finalidad es verificar la conectividad IP entre dos hosts, consiste en el envío de solicitudes de eco o solicitudes de respuestas a un destino específico. Ping usa el protocolo ICMP (*Internet Control Message Protocol*) o Protocolo de Mensajes de Control de Internet,). Si el destino recibe la solicitud de eco, responde con un datagrama de respuesta

de eco ICMP. La utilidad ping mide el tiempo requerido hasta la recepción de la respuesta, lo cual permite establecer parámetros de retardo en la red. Si la respuesta no llega dentro de un límite de espera, la utilidad considera que el destino es inalcanzable y emite un mensaje de respuesta no recibida.

Ping al Gateway

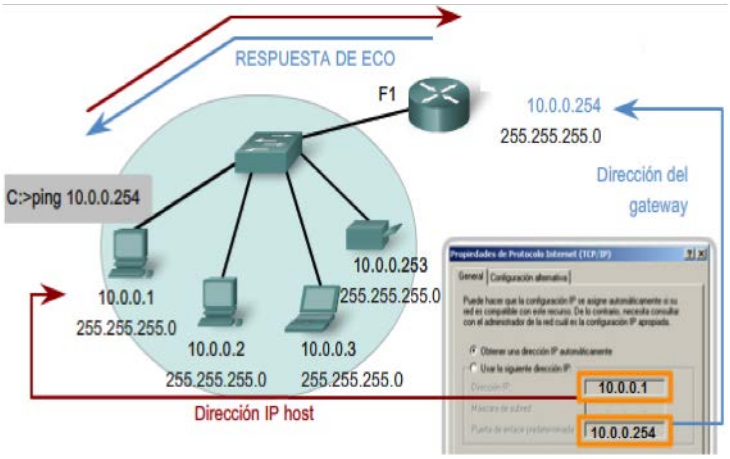


Imagen 16
Fuente: Propia, adaptada de currículo CCNA Exploration

El Gateway por defecto es la interfaz del router a la cual se conecta la red. Para probar conectividad del host con otra red, se puede hacer un ping al Gateway, si no se obtiene respuesta, se puede intentar Ping a un host en la red local, si en este caso se obtiene respuesta, la no conectividad al Gateway podría ser por un problema con la respectiva interfaz, por ejemplo, una configuración IP equivocada.

Prueba de Loopback

Permite probar la configuración ITCP/P de un equipo, es un caso particular de la utilidad Ping, en la que se usa como destino la dirección reservada 127.0.0.1. Una respuesta de esta dirección indica que el TCP/IP está bien instalado en el host, pero no significa que las direcciones, máscaras y gateways estén correctamente configurados.

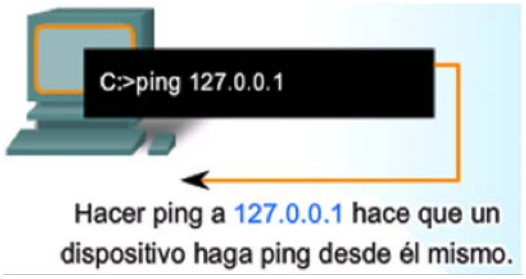


Imagen 17
Fuente: Propia, adaptada de currículo CCNA Exploration

Traceroute

A diferencia de Ping, la utilidad Traceroute permite identificar la ruta entre dos host, generándose el listado de los saltos exitosamente alcanzados, con lo cual se puede aislar el punto del problema.

Introducción al enrutamiento

Cuando un host requiere enviar información a un dispositivo en otra red, el host origen debe estar configurado para enviar los paquetes a la interfaz del router a la cual se conecta la red, este es el Gateway por defecto.

A nivel de capa 3 los routers son la columna vertebral de grandes redes, a cada router se puede conectar varias redes LAN, en la cual se encuentran múltiples host que pueden ser dispositivos destino. Con base en la dirección de la red destino los routers tienen la tarea de reenviar el tráfico recibido de redes locales o de otros routers. Teniendo en cuenta que a cada una de las diferentes redes destino le corresponde un camino o ruta, para realizar el reenvío, los routers deben contar con información sobre tales rutas, de tal manera que puedan decidir por cuál de sus interfaces debe reenviar el tráfico que reciban, ésta puede la interfaz de una red directamente conectada o la salida hacia el siguiente salto, donde la tarea de reenvío pasa a ser responsabilidad del respectivo router. A la función de enrutamiento se asocia diferentes elementos como tabla de enrutamiento, rutas predeterminadas y protocolos de enrutamiento descritos en los siguientes apartes.

Tabla de enrutamiento

La información de rutas requerida recibe el nombre de información de enrutamiento, y la estructura lógica que almacena esta información de recibe el nombre de Tablas de enrutamiento. Si la tabla de enrutamiento de un router no registra información de rutas hacia un destino, los paquetes no pueden ser reenviados y se descartan, a menos que se configure una ruta por defecto.

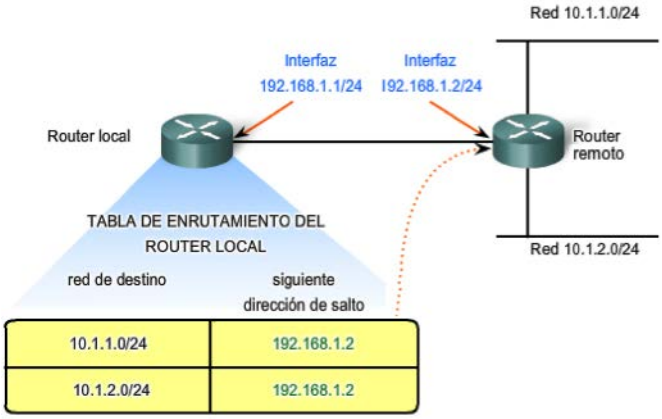


Imagen 18
Fuente: Propia, adaptada de currículo CCNA Exploration

Ruta predeterminada

Un router puede configurarse con una ruta predeterminada, la cual es usada como ruta de paquetes destinados a redes para las cuales no hay información de enrutamiento, generalmente se dirigen a la internet.

Métodos de configuración de enrutamiento

Un router obtiene su información de enrutamiento mediante la configuración manual o estática, realizada por un administrador de red, y/o de forma automática o dinámica mediante la previa definición de un protocolo de enrutamiento.

Respecto a la configuración estática de rutas hay que anotar que si la estructura de la red cambia, bien sea por la caída de un enlace o la aparición de nuevos saltos, puede ser necesaria la actualización manual de la información de enrutamiento, de no realizarse oportunamente la actualización se puede generar importantes fallas de comunicación en la red. En redes de gran tamaño no resulta conveniente que toda la configuración de enrutamiento sea de forma manual, conviene en gran medida el uso de protocolos de enrutamiento dinámico, diseñados para actualizar de forma periódica y automática la información de enrutamiento.

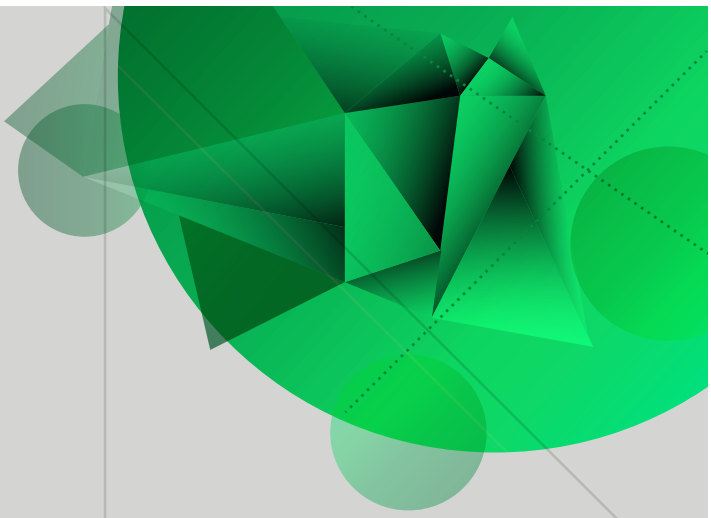
Los protocolos de enrutamiento

Son reglas mediante las cuales los routers comparten información de rutas. Frente a cambios de la estructura de las redes conectadas a un router informa de los cambios de tal manera que aquellos que la reciben actualizan sus tablas de enrutamiento y comparten a su vez sus actualizaciones. Entre los protocolos de enrutamiento más utilizados se cuentan RIP, EIGRP y OSPF. El estudio detallado de protocolos de enrutamiento supera los alcances de este curso.

3

Unidad 3

Capas de enlace de datos y capa física



Telemática I

Autor: Juan Carlos Ramírez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En la presente semana se brinda al estudiante una introducción a los aspectos básicos del entramado de paquetes, los protocolos de enlace de datos, los diferentes métodos de control para acceder a los medios físicos, las topologías de red, su relación con el acceso al medio y los más importantes estándares de capa física.

U3

Metodología

Los estudiantes como centro activo de aprendizaje deben hacer la lectura y análisis permanente de este material, que les permite realizar una contextualización del tema, conociendo la teoría general y su aplicación práctica en contextos específicos.

U3

Desarrollo temático

Capas de enlace de datos y capa física

Introducción

Las unidades anteriores se han centrado sobre las funcionalidades de las capas superiores del modelo OSI, describiéndose la capa de aplicación como aquella que proporciona la interfaz del usuario con la red; la preparación dada a nivel de capa de trasporte en función de las aplicaciones involucradas y el direccionamiento lógico, a nivel de capa de red, que facilitan el viaje de la información a través de la infraestructura física en función de la red de destino. Dado que los paquetes no cuentan con información que les permitan manejar el acceso directo a los diferentes medios físicos a través de los cuales pueden viajar, la capa de enlace de datos del modelo de referencia OSI define las funcionalidades mediante las cuales los paquetes se entraman o preparan para ser transmitidos, también define los procedimientos de control de acceso a los medios. Por su parte la capa física trata los detalles asociados a los medios físicos de transmisión, así como la codificación y señalización física.

Capa de enlace de datos como soporte de capas superiores

Los paquetes de datos, que a su vez contienen los segmentos pertenecientes a las diferentes conversaciones de capa de aplicación son encapsulados mediante funciones de la capa de enlace de datos. La capa de Enlace de datos tiene entre sus tareas el control de acceso de datos a los medios. La Unidad de Dato de Protocolo o PDU correspondiente a la capa de enlace de datos recibe el nombre de trama, con lo que puede decirse que la capa de enlace de datos maneja el intercambio de tramas entre los diferentes nodos de una red.

Entramado de paquetes: preparación para su acceso a los medios

Frente a la posible necesidad de saltos de la información a través de la red, los routers reciben tramas por una de sus interfaces, realizan la operación de desencapsulación para leer los encabezados del paquete, luego entrama nuevamente el paquete para enviarla por otra interfaz, que posiblemente esté conectada a un medio diferente al de la interfaz de entrada. Esta posibilidad de intercambio de paquetes a través de diferentes tipos de tramas da lugar al requerimiento de variados protocolos de capa de enlace de datos.

Direccionamiento físico frente a direccionamiento lógico

Es importante resaltar que la dirección MAC sólo tiene significado a nivel local, no da información sobre la red o segmento de red en que se ubica un computador. Ante la necesidad de intercomunicación de dos equipos en redes locales diferentes, el sólo uso de la dirección MAC no es suficiente, puesto que esta dirección no da indicación de la red en la que se ubica el host. Además de lo anterior, es posible que los respectivos paquetes deban pasar por múltiples interfaces intermedias pertenecientes a diferentes tecnologías LAN o WAN, por lo que es lógico suponer que un equipo emisor no cuente con el conocimiento de las diferentes tecnologías involucradas a lo largo de la ruta hacia el destino y por tanto tampoco sobre el direccionamiento físico y las estructuras de trama.

En el orden de ideas de lo antes expuesto resulta de vital importancia el uso de un esquema de direccionamiento lógico, tal como IP, el cual permite la identificación de equipos en función de la red lógica en que se encuentran. Se requiere que los paquetes entramados lleven siempre la misma dirección lógica de destino, pero en lo que se refiere a la dirección física, cada trama lleva como dirección MAC de destino la de la interfaz por la cual ingresa a cada dispositivo intermedio, éste desentrama el paquete con el fin de leer la información de direccionamiento lógico y decidir así la interfaz por donde debe ser renviada, y por consiguiente la siguiente interfaz en la ruta, con lo cual entrama nuevamente el paquete con información de direccionamiento físico relativo al entorno local que involucra las interfaces.

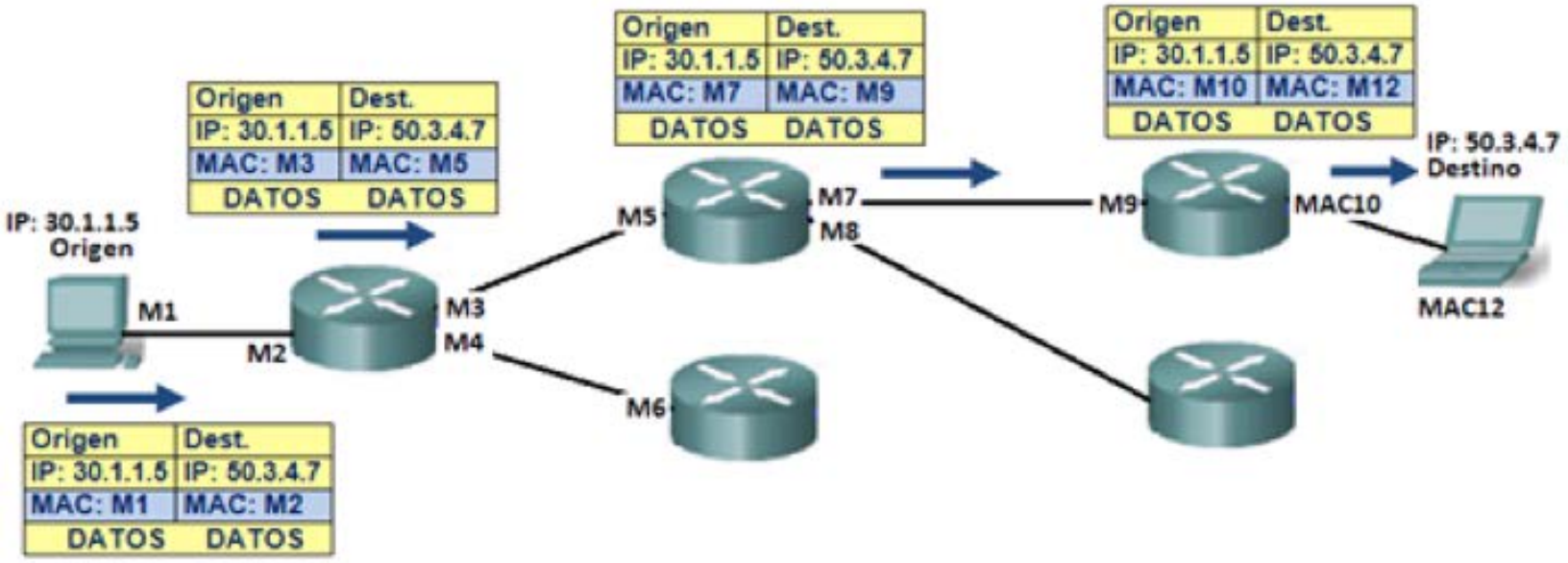


Imagen 1
Fuente: Propia, adaptada de currículo CCNA Exploration

La capa de enlace de datos, o capa 2, evita que los protocolos de la capa de red deban manejar información relativa al tipo de medio de conexión. Los servicios de la capa de Enlace de Datos deben considerar los tipos de medios y su método de acceso. A través de sus protocolos, la capa de enlace de datos define el entramado de paquetes y los métodos usados para colocar la información en los medios de red y recibirlos de ellos, estos métodos se conocen genéricamente como Control de Acceso al Medio (MAC). La transferencia a través de diferentes medios, conectados a diferentes tipos de interfaces, requiere de diferentes métodos de control de acceso. Por ejemplo un computador para conectarse a una red puede usar una tarjeta de interfaz de red, la cual tiene implementados los protocolos de capa de Enlace de datos, encargados de administrar la trama y el control de acceso a los medios. Los dispositivos intermedios, al tener diversos tipos de interfaces usan protocolos diferentes para el cumplimiento de esta tarea.

Composición básica de una trama

Las tramas pueden entenderse como la unión de paquetes e información de control usada por los protocolos de enlace de datos. La información de control hace referencia a identificación de los nodos que se comunican, al inicio y fin de la comunicación, entre otros. La capa de enlace de datos prepara los paquetes para su transporte a través de los medios locales.

Imagen 2
Fuente: Propia, adaptada de currículo CCNA Exploration

Una trama genérica de la capa de enlace de datos, además de los paquetes de capa 3 y los campos encabezados de capa 2, incluye campos de información de control adicional contenida en un componente conocido como Tráiler. El encabezado contiene información sobre direcciones físicas de los nodos origen y destino y otro tipo de información al inicio de la trama, mientras que el tráiler incluye información de control finalizando la trama.

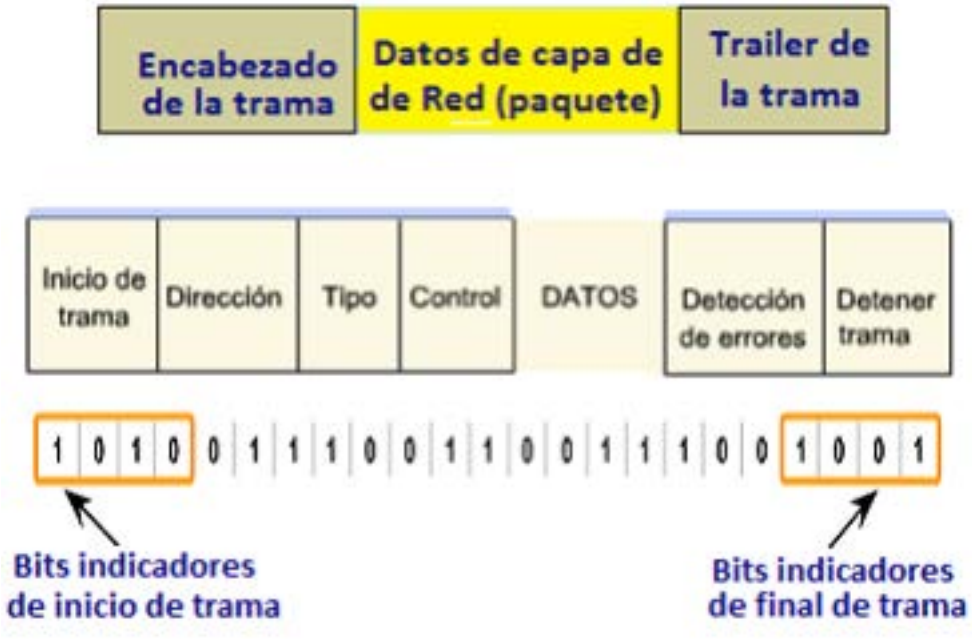


Imagen 3
Fuente: Propia, adaptada de currículo CCNA Exploration

Los campos de la trama obedecen una secuencia específica que permite al receptor interpretar la secuencia binaria según su ubicación. Entre los campos que se incluyen en una trama se tiene: indicadores de inicio y terminación de trama, direcciones físicas origen y destino, campos de tipo, campo de datos (En TCP/IP son los paquetes de capa de red). Los diferentes protocolos de enlace de datos definen sus propios formatos de trama.

En términos prácticos se puede afirmar que las especificaciones de la capa de enlace de datos se implementan en las tarjetas de interfaz de red de los equipos, a este componente físico se asocia el componente de software que define su funcionamiento. En computadores de redes locales de pequeñas empresas y hogares, Ethernet es la tecnología dominante a nivel de capa 2, el componente físico es la tarjeta Ethernet.

Imagen 4
Fuente: Propia, adaptada de currículo CCNA Exploration

División de la capa de enlace de datos

Imagen 5
Fuente: Propia, adaptada de currículo CCNA Exploration

La capa de Enlace de Datos opera como intermediaria entre la capa de Red y la capa Física, teniendo en cuenta que esta última involucra diferentes tipos de medios, la capa de enlace se divide en dos subcapas: Control de Enlace Lógico (LLC) y Control de Acceso al Medio (MAC), descritas brevemente a continuación.

Subcapa LLC

maneja los procesos de software requeridos para poder prestar los respectivos servicios a la capa de red, LLC es independiente de la tecnología de los diversos medios de transmisión, y las diferentes posibilidades se asocian a los diferentes protocolos de capa de red, esto significa que si el direccionamiento lógico de una red corresponde al esquema IP, se tiene coincidencia en las subcapas LLC de computadores de escritorio, con tarjeta de red Ethernet para conexión por cable, y la de computadores portátiles, con tarjeta de Red inalámbrica.

Subcapa MAC

Maneja los procesos de control de acceso a los medios existentes, varía según la tecnología del medio físico de transmisión (coaxial, par trenzado, fibra óptica, inalámbrico) se tiene diferentes requisitos de señalización física y mecanismos de control de acceso.

Entidades de estandarización

La comparación entre el modelo de referencia OSI y el modelo TCP/IP deja ver que la capa de Acceso a la Red de TCP/IP puede asimilarse a la combinación de las capas de enlace de datos y capa Física del modelo OSI. Entidades como el IEEE Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), Instituto Nacional Estadounidense de Estándares (ANSI), Unión Internacional de Telecomunicaciones (ITU) y la propia ISO, definen protocolos y las debidas funcionalidades asociadas a la capa de Acceso a Red, estas especificaciones se implementan mediante diferentes estándares que deben considerar los tipos de medios y tecnologías. La implementación de los procesos asociados a la capa de enlace de datos involucra tanto hardware como software, el componente de hardware en este caso es la tarjeta de interfaz de red, a la cual se asocia una configuración de software.

Funciones de control de acceso al medio

A nivel de capa de enlace de datos el control de acceso define de qué manera se emplean o comparten los medios entre los diferentes nodos en una red, la idea de control de acceso puede asimilarse a reglas de tráfico de datos necesarias para acceder a los medios de red, esto es análogo a las reglas de tráfico de vehículos sobre una red vial. Ejemplos de métodos de control de acceso en el caso del tráfico vehicular, lo constituyen la regulación implementada a través de los semáforos (espera de un turno) o en su defecto el conductor juzga si tiene o no la posibilidad de circular. En redes de computadores, en las que generalmente un medio es compartido por varios nodos, el método de control de acceso depende de la estructura de la red, desde el punto de vista físico esto corresponde a la disposición de los enlaces.

En una red de medios compartidos puede darse que varios nodos quieran participar en la transmisión de información en cualquier instante, esta situación genera la necesidad de mecanismos para controlar que los diferentes nodos puedan compartir el medio. Existen dos métodos genéricos de control de acceso los cuales se describen brevemente en los siguientes dos numerales.

Acceso controlado por asignación de turnos

Cada nodo participante dispone de un lapso de tiempo para utilizar los medios, es un método programado de tal manera que si un equipo con derecho a usar el medio no requiere hacerlo, la posibilidad de usarlo durante ese tiempo se otorga al siguiente equipo en la secuencia de turnos. Este método controlado por turnos presenta la ventaja de brindar un rendimiento predecible, pero como desventaja muestra cierta ineficiencia y sobrecarga debido a la necesidad de espera de turno debido a la necesidad de espera de turno.

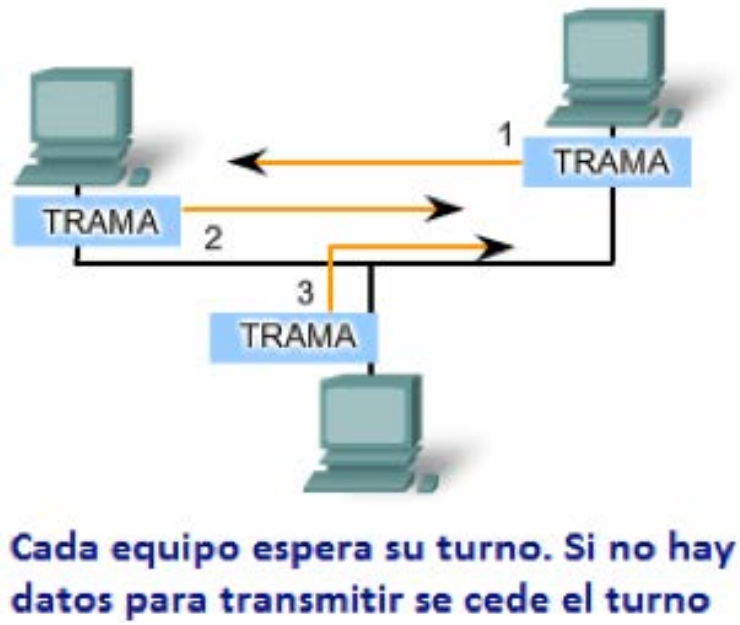


Imagen 6
Fuente: Propia, adaptada de currículo CCNA Exploration

Acceso con base en contención

En redes en que se implementa un método de acceso de este tipo, los equipos compiten por utilizar el medio de transmisión y cualquier nodo puede intentar usarlo, se requiere la existencia de algún mecanismo orientado a evitar el intento de uso simultáneo por parte de dos o más nodos. Uno de estos mecanismos se conoce como Acceso Múltiple por Detección de Portadora (CSMA), con base en el cual, antes de intentar transmitir, un nodo primero detecta si el medio está en uso por parte de otro participante, en cuyo caso espera hasta que el medio esté libre. El equipo transmite información si no detecta una señal viajando a través del medio.

Existe la posibilidad que dos equipos que intentan transmitir detectan al mismo instante que el medio está libre, al transmitir en estas condiciones se presenta lo que en redes de computadores se conoce como colisión de datos.

Los métodos de acceso por contención no tienen la recarga propia de la asignación de turnos, lo que en cierta forma los podrían hacer más eficientes, sin embargo la probabilidad de colisiones aumenta con el número de nodos que comparten el medio. Las redes se deben diseñar de tal manera que un mismo medio sea compartido por un número no muy grande de nodos. Cada segmento o porción de la red en que los equipos comparten los medios se conoce como un dominio de colisión.

Imagen 7
Fuente: Propia, adaptada de: currículo CCNA Exploration

Dos casos importantes en los que se utiliza acceso por contención son las tecnologías Ethernet y las redes LAN inalámbricas, cada una de estas tecnologías implementa, al lado de CSMA, un mecanismo para resolver los problemas asociados a las colisiones, estos son Detección de colisiones y prevención de colisiones.

Detección de Colisión (CD)

Implementado en la tecnología Ethernet, constituyendo, al lado de CSMA, el mecanismo CSMA/CD, la detección de colisiones consiste en que si los diferentes equipos de la red detectan señales producto de colisiones, cada equipo posterga sus intentos de envío durante tiempos definidos aleatoriamente.

Prevención de Colisiones (CA)

Es la variante que complementa CSMA y es implementada en las redes locales inalámbricas, en CSMA/CA la prevención consiste en que si un equipo que quiere transmitir detecta que el medio está libre, envía una señal manifestando su intensión de transmitir, con el fin que cualquier otro equipo no intente hacerlo, luego de ella envía los datos.

Topología lógica y topología física

El término topología, en el contexto de las redes de computadores, corresponde a la estructura de la red, su configuración o relación de los diferentes equipos que la conforman y los enlaces entre ellos. La topología de una red puede verse desde las perspectivas física y lógica. La topología física hace referencia a las interconexiones entre los diferentes nodos a través de los medios de red, por su parte la topología lógica se refiere a la forma en que se transmiten las tramas entre nodos, independiente de la topología física o ubicación de los equipos. Las topologías lógica y física generalmente utilizadas en redes se describen brevemente a continuación:

Topología Punto a Punto

Imagen 8
Fuente: Propia, adaptada de currículo CCNA Exploration

Una red punto a punto, desde la perspectiva física, conecta dos nodos entre sí, el control de acceso toma en cuenta la simplicidad de la ruta entre nodos y de esta forma se implementa a través de protocolos con muy poca sobrecarga.

Desde la perspectiva lógica, en las redes punto a punto los equipos se pueden conectar a través de una diversidad de posibilidades de interconexiones físicas intermedias, sin que ello afecte el flujo lógico de información.

Imagen 9
Fuente: Propia, adaptada de currículo CCNA Exploration

Topología lógica de acceso múltiple

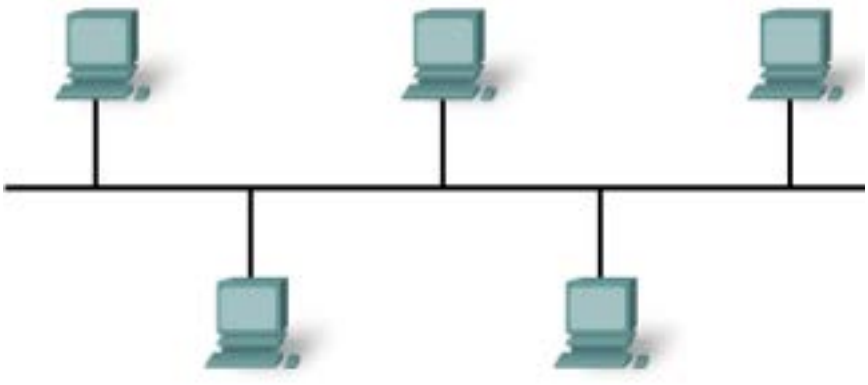


Imagen 10
Fuente: Propia, adaptada de currículo CCNA Exploration

Es una configuración en la cual varios nodos pueden comunicarse a través de medios compartidos. La información procedente de un origen llega a los demás nodos del entorno, pero sólo el legítimo destino la procesa. Los métodos de control CSMA/CD o CSMA/CA, brevemente descritos antes, usan las topologías lógicas de acceso múltiple.

Topología de anillo

Imagen 11
Fuente: Propia, adaptada de currículo CCNA Exploration

Una topología lógica de anillo se caracteriza por el hecho que cada nodo que recibe una trama la reenvía al siguiente en caso que no sea el propio destino. Esto facilita que un anillo use una técnica de control de acceso llamado paso de tokens. En una topología lógica de anillo la topología física puede ser diferente a una topología física de anillo.

Protocolos de capa de enlace de datos

Ante la existencia de diferentes medios de red se tiene diversos protocolos de capa de enlace de datos, cada protocolo encapsula la PDU de Capa de Red en una trama cuya estructura varía según el protocolo.

El encabezado registra información de control requerida para la efectiva transmisión, los encabezados de una trama genérica podrían incluir campos para indicar: Inicio de trama, direcciones físicas de origen y de destino, definiciones de prioridad y/o calidad de servicio, entre otros. Según los protocolos de capa de enlace de datos de la tecnología implementada se puede tener tramas con estructuras algo diferentes. Debido a que los fines y funciones de los protocolos de capa de enlace de datos se relacionan con las topologías específicas y los medios, es recomendable examinar cada protocolo para tener una comprensión más detallada de su estructura de trama.

Entre los elementos más importantes del encabezado se encuentran los campos relativos al direccionamiento físico, el cual permite la transmisión de tramas en redes locales de medios compartidos. El direccionamiento físico se considera un esquema de direccionamiento plano en el sentido que una dirección física en particular no da indicación de la red en la cual se encuentra el host, la dirección física de un dispositivo no cambia con el traslado del dispositivo a otra red, la dirección física sólo tiene significado a nivel de redes locales.

Si paquetes entramados deben viajar hacia una red externa, el router que separa la red local de las otras redes desencapsula la trama, elimina la información de direccionamiento físico original y crea una nueva trama con información de direccionamiento relativa a él mismo y a la del siguiente salto.

El tráiler generalmente contiene información útil en la detección de errores en tramas entrantes. Las señales que viajan a través de los medios son susceptibles a interferencia y otro tipo de problemas que podrían generar alteraciones en los valores de los bits de la señal. La detección se hace con base en el contenido del campo secuencia de verificación de trama el cual corresponde a un cálculo realizado sobre los bits del contenido de la trama.

En una red se implementa protocolos de capa 2 según la topología lógica y la implementación de la capa física, asociada a la diversidad de medios. Son varios los protocolos de capa de enlace de datos que existen, entre ellos tenemos: Ethernet, Protocolo punto a punto (PPP), Control de enlace de datos de alto nivel (HDLC), Frame Relay y Modo de Transferencia Asíncrona (ATM).

En diferentes dispositivos de red se puede implementar uno o más de estos protocolos de capa de enlace de datos según las interfaces de red de que dispongan. Aspectos como el alcance geográfico de la red, la topología, la tecnología, tamaño de la red, servicios que presta un dispositivo, determinan el protocolo de capa de enlace de datos a utilizar.

Ethernet, Protocolo de amplia utilización para Redes de Área Local

El IEEE, a través de sus diferentes comités, define un conjunto de estándares de capa de enlace de datos y de capa física para redes LAN. A través de 802.2 define las funcionalidades correspondientes a la subcapa LLC, común a las diferentes tecnologías LAN. Las particularidades de la familia de tecnologías Ethernet son definidas en los comités 802.3. Ethernet es la tecnología de Red de Área Local más ampliamente utilizada, con ella se puede crear redes locales de alta velocidad ya que presenta variantes que soportan anchos de banda 10, 100, 1000, o 10000 Mbps, las variantes se diferencian en los métodos de detección de y colocación de tramas en el medio físico.

Ethernet proporciona servicio no orientado a conexión y no confiable, en el sentido de no manejar acuse de recibido, en el método de control de acceso al medio, CSMA/CD. El encabezado de la trama Ethernet incluye las direcciones físicas origen y destino, conocidas como direcciones MAC. Una dirección MAC Ethernet corresponde a una secuencia de 48 bits, que generalmente se expresan en forma hexadecimal. Posteriormente en este curso se ampliará detalles respecto a la tecnología Ethernet.

Protocolo para redes inalámbricas locales: 802.11 o Wifi

IEEE, a través de 802.11 define las particularidades de las redes WLAN o Redes de Área Local Inalámbricas. El estándar IEEE 802.11, conocido también como tecnología Wifi, es un sistema basado en contención que se vale del método de control de acceso CSMA/CA o Acceso Múltiple con Detección de Portadora y Prevención de Colisiones. Dado que el medio físico de transmisión es el aire o espacio abierto, se requiere consideraciones especiales en la transferencia de tramas a través de redes inalámbricas,

entre ellas se cuenta el uso de acuse de recibo a nivel de capa 2, servicios de autenticación y encriptación de la información, entre otros.

Protocolo Punto a Punto (PPP), un protocolo de capa 2 para redes WAN

PPP es un protocolo de enlace de datos empleado en transferencia de tramas entre dispositivos de interconexión WAN, el protocolo puede valerse de diferentes medios físicos como cable de par trenzado y fibra óptica.

La capa física

El nivel físico de una red, a la luz del Modelo OSI, hace referencia a los aspectos relacionados con los medios físicos a través de los cuales viajan las señales que transportan información. Se puede decir que la capa física en el origen o en nodos intermedios, toma los bits que corresponden a las tramas y los codifica como una secuencia de señales caracterizadas por patrones físicos que han de viajar a través del medio; un equipo intermedio receptor o un destino final toma la secuencia de señales físicas que llegan a la interfaz y las decodifica para obtener la representación binaria de la trama.

Los medios se agrupan básicamente en cables de cobre, fibra óptica e inalámbrica, la forma de representación de los bits depende del medio en uso. En los medios basados en cobre la señal portadora son pulsos eléctricos, en fibra óptica son patrones de luz y en los medios inalámbricos corresponden a ondas de radio. En cualquier caso, la capa física también cuenta con funcionalidades que permite distinguir el inicio y final de tramas, análogas a las de la capa de enlace de datos, de tal manera que los dispositivos puedan reconocer el recibo exitoso de la misma.

Estandarización de capa física

Los estándares de capa física, asociados al hardware de redes de computadores, son definidos por organizaciones consideradas autoridades en el campo de la ingeniería eléctrica y en comunicaciones. Entre estas organizaciones se tiene la ISO, IEEE, el Instituto Nacional Estadounidense de Estándares (ANSI), la Unión Internacional de Telecomunicaciones (ITU), La Asociación de Industrias Electrónicas y la Asociación de las Industrias de las Telecomunicaciones (EIA/TIA), entre otras. Los estándares atienden aspectos relacionados con: Propiedades físicas y eléctricas de los medios, Propiedades mecánicas propias de los materiales y medidas de los cables y conectores, codificación de los bits según la forma de representación de acuerdo al medio de transmisión, definición de las señales de la información de control.

Funcionalidades básicas de la capa física

La capa física se encarga de funciones fundamentales relacionadas con componentes físicos, codificación de bits y señalización. A nivel de capa física, la codificación es el proceso mediante el cual una cadena especifica de bits, correspondientes al contenido de las tramas, se convierten según un código de patrones predefinidos. La señalización atañe a la representación de los bits, aquí se define qué tipo de señal representa un "1" y un "0", esto puede corresponder, por ejemplo, a un cambio de nivel en una señal eléctrica, o un impulso óptico.

Señalización

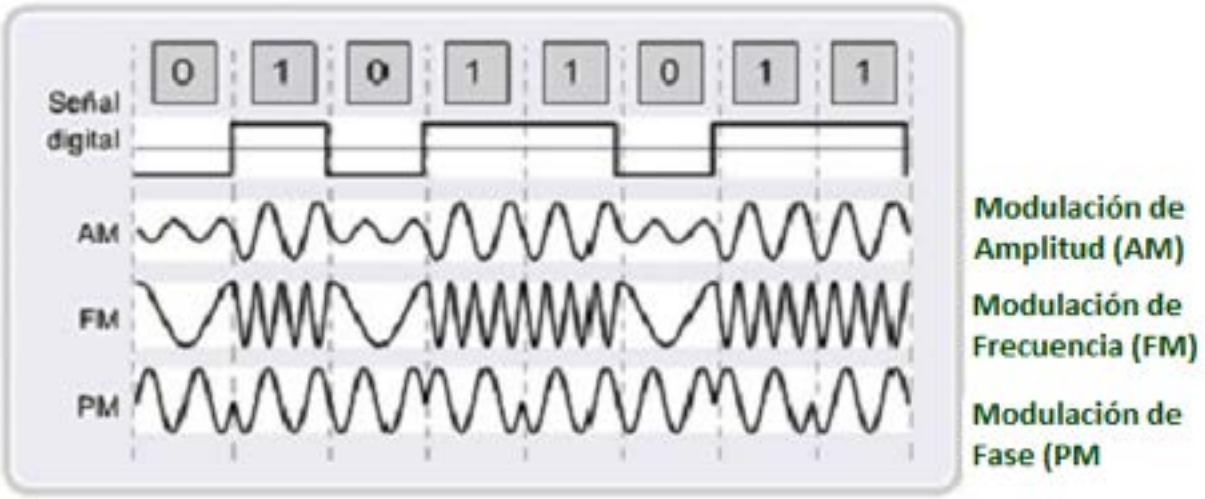


Imagen 12
Fuente: Propia, adaptada de currículo CCNA Exploration

La capa física representa cada bit como una señal, la cual cuenta con un tiempo de duración, llamado tiempo de bit. En el receptor se revierte el proceso tomando las señales para asociarlas bits.

Se emplea diferentes métodos de señalización implementados mediante la modificación de características de la señal portadora, entre las cuales están la amplitud, la frecuencia y fase.

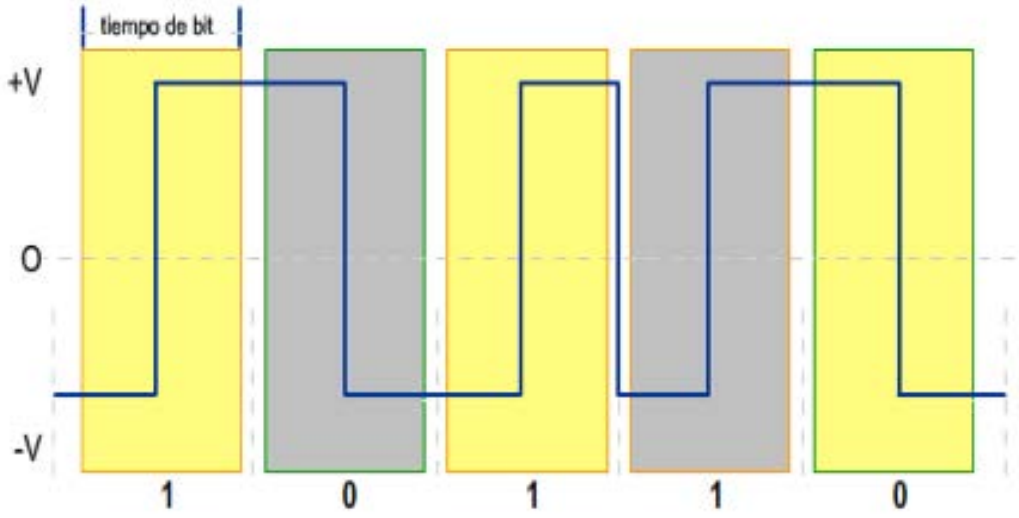


Imagen 13
Fuente: Propia, adaptada de currículo CCNA Exploration

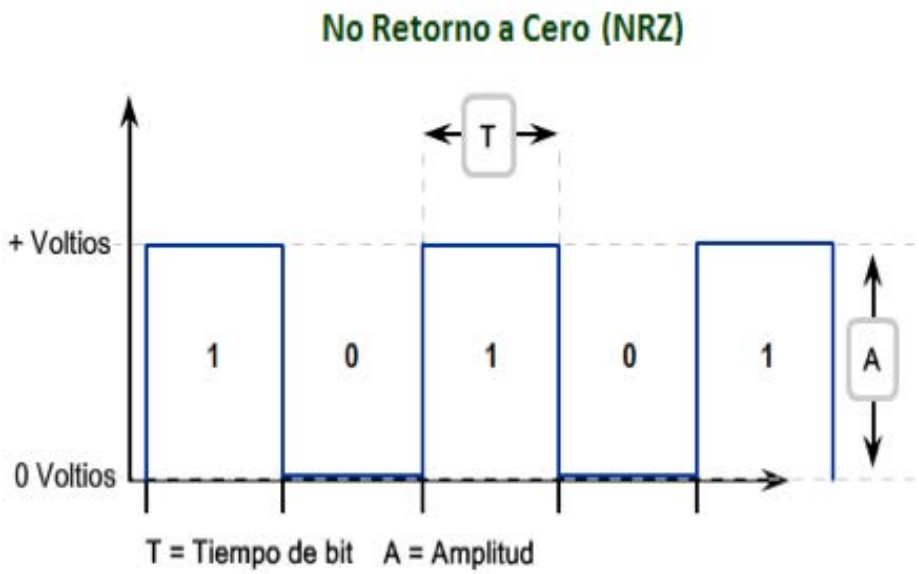


Imagen 14
Fuente: Propia, adaptada de currículo CCNA Exploration

En el método de señalización conocido como No Retorno a Cero (NRZ), el 0 binario se puede representar mediante un nivel específico de voltaje durante un tiempo de bit y un 1, con otro nivel. NRZ se adapta a sistemas de enlaces de baja velocidad, y se ve seriamente afectado por interferencias electromagnéticas, los límites entre bits pueden perderse en la transmisión de largas cadenas de bits del mismo valor (muchos unos o muchos ceros consecutivos) debido a que no se detectan transiciones de voltaje durante muchos tiempos de bits dificultando así la sincronización en el receptor.

Otros métodos se basan en transiciones de voltajes o ausencia de ellas para representar los dos posibles valores binarios durante un tiempo de bit. Los estándares dan lugar a la necesidad de acuerdos respecto a la señalización entre transmisor y receptor.

En la codificación Manchester los valores se dan mediante un salto de voltaje en la mitad del tiempo de bit, por ejemplo al cero le puede corresponder una transición de un valor alto a un valor bajo, mientras que el uno se representa a través de un salto ascendente. El método de codificación Manchester es el método usado por las primeras implementaciones de Ethernet.

Codificación

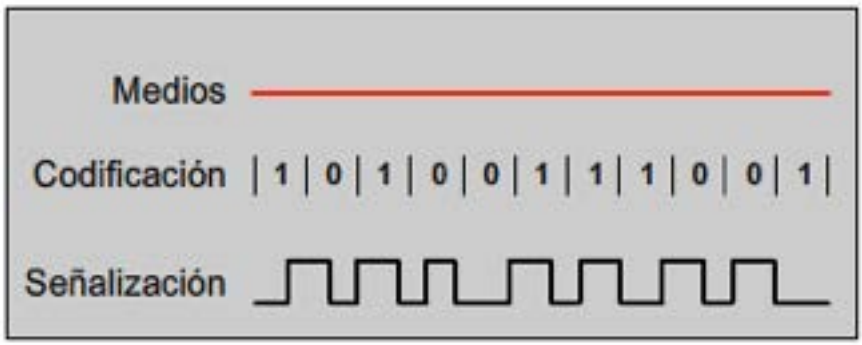


Imagen 15
Fuente: Propia, adaptada de currículo CCNA Exploration

La codificación se utiliza para representar grupos de bits antes de su colocación en los medios. La posibilidad de transmitir a mayores velocidades incrementa el riesgo de daño de los datos, la codificación por agrupación permite mayores facilidades de detección de errores. Existen patrones predefinidos válidos, el receptor detecta señales y debe poder identificar señales válidas y aquellas que contienen errores. De igual forma existen patrones de señales de control empleadas para indicar el inicio y final de trama, las tramas no delimitadas por estos patrones se ignoran por parte del receptor.

Los patrones de bits en la codificación reciben el nombre de símbolos. En la capa física se usa conjuntos de símbolos codificados, o grupos de códigos mediante los cuales se representa la información. Por ejemplo, los cinco bits de código 10101 podrían representar los cuatro bits de datos 0011.

El uso de grupos de códigos genera sobrecarga al agregar bits adicionales en la transmisión, pero como contraprestación se mejora la solidez de la transmisión, principalmente las realizadas a través de enlaces de alta velocidad. Esta característica se aplica especialmente a la transmisión de datos de mayor velocidad.

Un ejemplo típico de codificación por grupos de códigos es 4B/5B, método mediante el cual cada byte a transmitir se divide en 2 grupos de cuatro bits y se codifica en símbolos de cinco bits.

Codificación de datos 4B/5B			
Datos	Símbolos	Datos	Símbolos
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

Imagen 16
Fuente: Propia, adaptada de currículo CCNA Exploration

Estos símbolos se utilizan para representar datos y códigos de control para la transmisión. 4B/5B garantiza la aplicación de al menos un cambio de nivel por código para proporcionar sincronización.

Factores que determinan la capacidad de transmisión

Según el medio empleado, la transmisión de bits puede darse a diferentes velocidades. Generalmente la capacidad del medio para la transferencia de datos se asocia a tres factores que son: Ancho de banda, Rendimiento y Capacidad de transferencia útil.

Ancho de banda

Hace referencia a la capacidad del medio en el trasporte de datos. El ancho de banda digital mide la cantidad de información por unidad de tiempo que puede fluir entre puntos conectados por el medio. La unidad básica de medida es el bit por segundo (bps), pero en la práctica se emplea múltiplos de esta cantidad, tales como Kilobits por segundo (Kbps), Megabits por segundo (Mbps) o Gigabits por segundo (Gbps). El ancho de banda en una red está determinado, entre otros aspectos, por la tecnología, los medios físicos, métodos de señalización y detección de señales de red.

Rendimiento

Se refiere a la medida de transferencia de bits durante un tiempo específico, se esperaría que el rendimiento coincidiera con ancho de banda, pero en la práctica resulta ser menor que el ancho de banda que especifica cada tecnología. Entre los elementos que determinan el rendimiento están el número de dispositivos conectados a la red, el volumen y tipo de tráfico. En redes Ethernet, en las cuales se emplea el método de acceso AMCS/CD, el rendimiento se ve notablemente afectado por el número de nodos que comparten el medio.

Capacidad de transferencia útil

Este elemento mide la rapidez de transferencia efectiva de datos de usuario a nivel de capa de aplicación. Es de tener en cuenta que cada capa genera sobrecarga sobre los datos de aplicación al agregar encabezados que posibilitan el éxito de la transmisión.

Tipos de medios

Los principales medios de transmisión en redes de computadores se clasifican en guiados y no guiados, entre los medios guiados están los cables basados en cobre y los cables de fibra óptica, mientras que los medios no guiados se refieren a los medios inalámbricos.

Medios basados en cobre

Existen diferentes especificaciones de cables de cobre empleados en las comunicaciones de red, los más conocidos son los cables de par trenzado y cable coaxial. El tipo elegido depende del estándar de la capa física a utilizar como soporte de la capa de enlace de datos. Medios de cobre diferentes pueden usarse en la conexión de computadores y dispositivos de interconexión en una red de área local, al igual que en la conexión de enlaces WAN. Cada tipo de medio emplea accesorios de acoplamiento específicos según sus características.

Es importante considerar que la transmisión de datos, en forma de señales eléctricas a través de medios de cobre, se ve afectada por la interferencia debido a señales externas que pueden alterar la señal de datos, estas interferencias no deseadas, o señales de

ruido, se originan por la presencia de ondas de radio y elementos como luces fluorescentes y motores eléctricos.

Los efectos del ruido y otros problemas de cableado pueden limitarse mediante el acatamiento de estándares y el seguimiento de técnicas de cableado asociadas al tipo de cable. Por ejemplo, los estándares correspondientes a medios de cobre consideran el tipo de cable, el ancho de banda de la tecnología, el tipo de conectores, diagrama de pines, código de colores, longitudes y grosores de los cables, características eléctricas del cable, entre otros. Los principales cables de cobre son:

Cable de par trenzado no blindado

En redes de comunicación, un tipo de cableado de amplio uso es el compuesto por pares de hilos trenzados y distinguibles por sus colores, la identificación por colores resulta útil en la terminación de los cables, mientras que el trenzado produce un benéfico efecto electromagnético que reduce o cancela la interferencia de señales de ruido. La circulación de una corriente eléctrica a lo largo de un conductor produce un campo magnético alrededor del conductor, cuando dos conductores están cercanos entre sí los campos electromagnéticos asociados a cada uno puede interferir la circulación de la corriente a través del otro. La interferencia en los hilos del mismo par trenzado, son procesadas en el receptor de manera opuesta cancelando la interferencia electromagnética.

La cancelación producto del trenzado también ayuda a prevenir el crosstalk, o interferencia electromagnética debida a pares del mismo cable. Si corrientes de igual intensidad fluyen en sentido opuesto por pares cercanos, los respectivos campos magnéticos, se anulan mutuamente. El cable de par trenzado debe cumplir con los estándares TIA/EIA, definidos por la Asociación de Industrias de las Telecomunicaciones (TIA) y la Asociación de Industrias Electrónicas (EIA). El cable de par trenzado de mayor uso es el UTP, o cable de par trenzado no blindado, es el medio empleado en las redes de las actuales tecnologías Ethernet.

Imagen 17
Fuente: http://alisverissepeti.com/image/cache/data/urunler/POLYGOLD-PG-1053-2-2-METRE-CAT5-_7737_1-500x500.jpg

El cable UTP consiste en cuatro pares cubiertos por un revestimiento plástico que les brinda protección. Para UTP se definen los estándares TIA/EIA -568A y 568 B empleados en la iinterconexión de equipos como computadores, switches y routers, la terminación de cables según estas normas usa conectores RJ-45. Además de lo anterior, el IEEE califica el cableado UTP en categorías según su capacidad y rendimiento en el transporte de datos. Las categorías de cable de mayor uso actual son Categoría 5 (Cat5), Categoría 5 mejorado (Cat5e) y Categoría 6 (Cat6), las categorías superiores se usan en entornos de mayor exigencia.

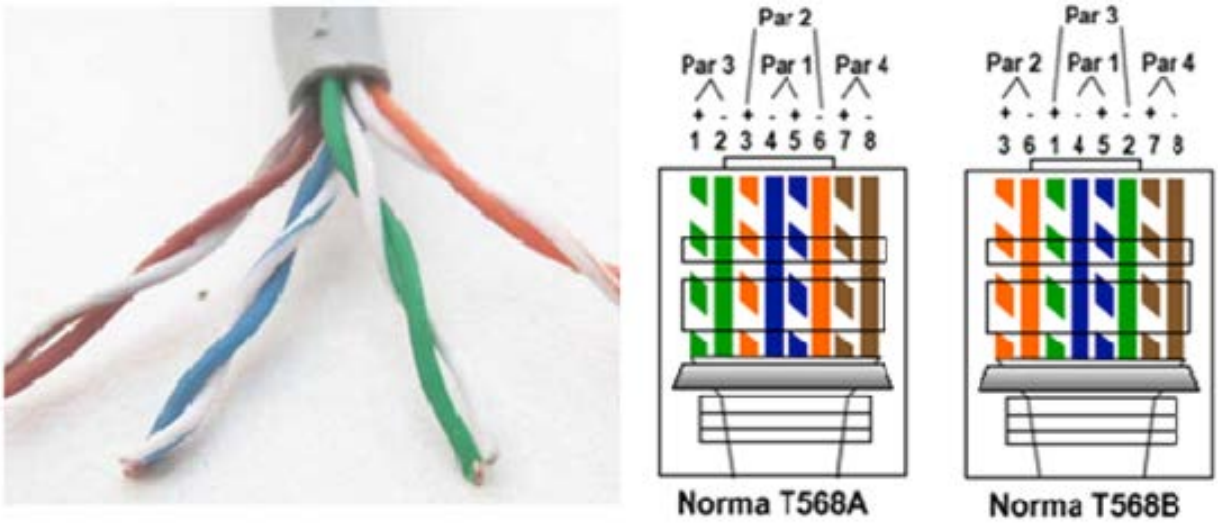


Imagen 18
Fuente: Propia, adaptada de currículo CCNA Exploration

Dependiendo el par de equipos a conectar, puede requerirse armado de cable diferente, es decir, diferentes configuraciones de conexión de hilos a los pines del conector RJ-45, según la configuración de conexión el cable toma su nombre, las posibilidades existentes son: cable de interconexión directa, cable de interconexión cruzada y cable traspuesto. En las actividades de laboratorios propias de este curso se tendrá la oportunidad de profundizar sobre el uso y elaboración de cables UTP.

Al intentar conectar dos equipos de la red mediante un cable equivocado no habrá comunicación entre ellos. En actividades de diagnóstico de problemas de red la revisión del cableado en uso es de las primeras tareas que debe llevar a cabo un técnico de redes de computador.

Cable Coaxial

Imagen 19
Fuente: https://donaldocepeda.files.wordpress.com/2011/03/imagescai2rhgs1.jpg

Consiste en un hilo conductor de cobre recubierto por una capa aislante y flexible que lo aísla de un blindaje metálico en malla de cobre o en hoja metálica que a su vez opera como segundo conductor, un recubrimiento final envuelve el blindaje más externo. Existen diferentes especificaciones de cable coaxial las cuales varían en grosor del cable y los respectivos conectores. El cable coaxial era el medio utilizado en las antiguas versiones de la tecnología Ethernet y actualmente se usa como medio de transmisión de señales por proveedores que brindan servicios de televisión, Internet y teléfono a hogares y pequeñas empresas.

Cable de fibra óptica

En este tipo de medidas las señales portadoras son pulsos de luz que viajan a través de una fibra de plástico o de vidrio. Los pulsos de luz son generados por diodos emisores de luz (LED) o por rayos laser. Entre las más importantes ventajas que otorga el uso de cables de fibra óptica se tiene:

- ***Elevadas velocidades de transmisión de datos:*** permite tendidos de mayores longitudes que las de cables de cobre, esto debido a la muy baja pérdida de potencia de la señal. Se permite tendido de varios kilómetros sin necesidad de repotenciar la señal.
- ***Inmunidad frente a interferencia electromagnética,*** gracias a que no conduce corriente eléctrica.

Al lado de las ventajas también se tiene algunas desventajas, la principal se asocia a elevado costo y necesidad de mayor cuidado en la realización de empalmes. El cable de fibra óptica es apropiado para cableado de backbone para grandes volúmenes de tráfico.

Un cable de fibra óptica está compuesto por un recubrimiento exterior y materiales adicionales de refuerzo interno alrededor de la fibra misma.

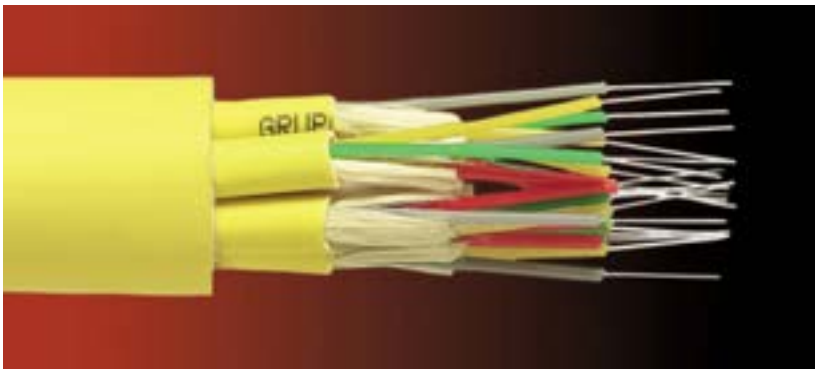


Imagen 20
Fuente: http://letranueva.blogia.com/upload/20130222133706-cables-de-fibra-optica.jpg

El revestimiento inmediato a la fibra tiene como función limitar la pérdida de señal. Debido a que la luz sólo viaja en una dirección, es necesario el uso de dos fibras en una comunicación full dúplex. La terminación del cable incluye conectores de fibra especificados en estándares respectivos.

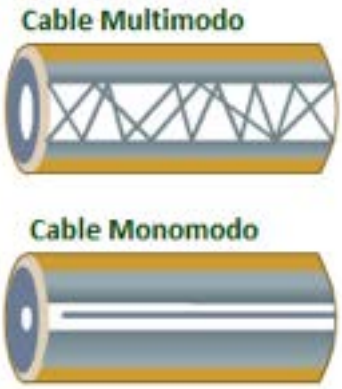


Imagen 21
Fuente: Propia, adaptada de currículo CCNA Exploration

Los cables de fibra óptica vienen en los tipos monomodo y multimodo. Por la fibra monomodo, como su nombre lo indica, viaja un solo rayo de luz generalmente producto de la emisión de un rayo láser. El cable monomodo es apropiado para transmitir impulsos agrandes distancias; por su parte el cable de fibra multimodo utiliza LED como fuente de emisión de luz, la cual puede ingresar al núcleo de la fibra en diferentes ángulos generando así varias trayectorias posibles, debido a la multiplicidad de trayectorias se requiere que existan diferentes períodos para el viaje de cada señal, también se produce un fenómeno llamado dispersión modal, el cual limita la longitud de los tramos de cable multimodo.

Medios inalámbricos

Las redes inalámbricas transmiten datos valiéndose de las ondas electromagnéticas que viajan a través del aire, las ondas se caracterizan por diferentes frecuencias dentro de un amplio rango de valores, conocido como espectro electromagnético. Los rangos de valores de frecuencias empleados por las tecnologías de redes inalámbricas pertenecen al rango de las microondas y las frecuencias de radio.

Existen diversos tipos de redes inalámbricas que obedecen diferentes estándares. En el caso de redes inalámbricas de área local se cuenta con la familia de estándares IEEE 802.11, también conocidos como Wifi. Otras tecnologías de comunicación inalámbrica son:

- ***Bluetooth:*** sujeta al estándar 802.15, utilizada para comunicación de dispositivos a corta distancia.
- ***GSM o Sistema global para comunicaciones móviles:*** habilitan la implementación del protocolo Servicio general de radio por paquetes (GPRS) que brinda transferencia de datos a través de redes de teléfonos celulares.

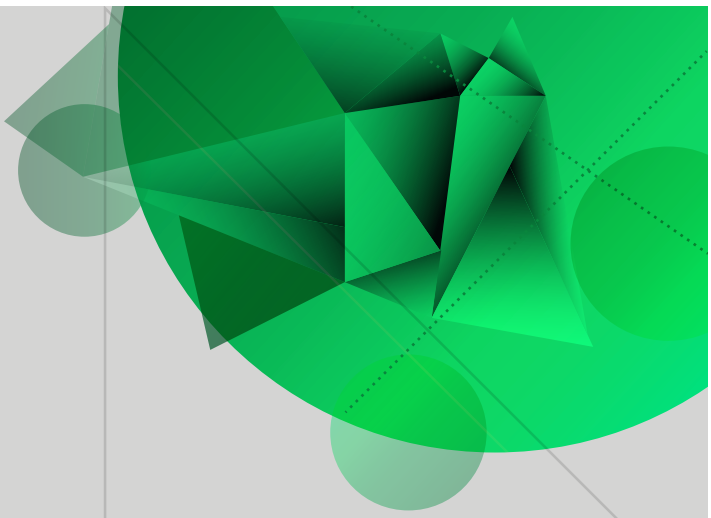
- ***Comunicaciones satelitales:*** brindan conectividad a ubicaciones en los que no se dispone de otros medios, permiten comunicación entre estaciones terrestres y enlaces satelitales.

Las especificaciones de capa física de los diferentes tipos de redes inalámbricas contemplan codificación y señalización, rangos de frecuencia, potencia de la señal, entre otros. El uso de tecnologías de comunicación inalámbrica da lugar a la necesidad de dispositivos compatibles con la transmisión de señales electromagnéticas, tales como tarjetas de interfaz inalámbricas, puntos de acceso inalámbricos, antenas entre otros. En el capítulo siguiente se ampliará aspectos relacionados a las tecnologías inalámbricas, principalmente los correspondientes a la tecnología WI-FI, considerando en ello el medio de transmisión.

3

Unidad 3

Introducción a las tecnologías ethernet y wifi



Telemática I

Autor: Juan Carlos Ramírez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En la presente semana reconoceremos las diferentes tecnologías de las redes locales a través de una línea del tiempo que muestra los avances a través del tiempo.

U3 Metodología

Los estudiantes como centro activo de aprendizaje deben hacer la lectura y análisis permanente de este material, que les permite realizar una contextualización del tema, conociendo la teoría general y su aplicación práctica en contextos específicos.

Introducción a las tecnologías ethernet y wifi

Introducción

Nos hemos dedicado en los primeros capítulos a una descripción de las diferentes funciones presentes en la comunicación a través de redes de datos desde el punto de vista del modelo de referencia OSI y del modelo de protocolos TCP/IP. Cada computador en una red hace parte de un segmento local, es decir, pertenece a una LAN o Red de Área Local, de las cuales existen diferentes tecnologías. En el campo de las LAN cableadas, Ethernet es la tecnología dominante, mientras que en el campo de las redes locales inalámbricas, la de mayor popularidad corresponde a la tecnología Wifi. En la presente unidad se esboza características básicas de estas tecnologías.

Ethernet 802.3

La primera especificación de Ethernet fue publicada como estándar abierto por el consorcio DIX (Digital – Intel – Xerox), pero los primeros desarrollos se dieron en la década de 1980. Actualmente los estándares Ethernet están regidos por la norma IEEE 802.3.

Imagen 1
Fuente: Propia, adaptada de currículo CCNA Exploration

Ethernet abarca fundamentalmente la subcapa MAC, o subcapa inferior de la capa de enlace de datos y la capa física del modelo OSI. Las funciones de la subcapa LLC están definidas en el estándar IEEE 802.2, esta subcapa representa la interfaz de comunicación entre los componentes de hardware de la capa de red.

Como se indicó en la unidad anterior, la subcapa LLC o Control de Enlace Lógico, es independiente de la tecnología de medios físicos, su funcionamiento corresponde a la implementación de software de la capa de enlace de datos, mientras que la subcapa MAC, o Control de Acceso al Medio corresponde a la implementación de hardware, las tareas de entramado, o encapsulación a nivel de capa de enlace de datos, y control de acceso al medio son funcionalidades de esta subcapa.

Desde el punto de vista lógico, la topología de la tecnología Ethernet corresponde a bus multiacceso, en la cual todos los nodos de segmento local comparten los medios, el hecho de compartir los medios da lugar a que las tramas lleguen a la NIC de cada equipo de la red local, con lo cual se hace necesario que cada uno determine, con base en la dirección física de destino, si la trama entrante debe ser procesada o descartada. El método de control de acceso al medio utilizado por Ethertnet es CSMA/CD o Acceso Múltiple con Detección de Portadora y Detección de Colisiones.

Desde sus inicios Ethernet ha evolucionado notablemente, los primeros productos utilizaban cable coaxial, luego se incorporó el cable UTP, y las implementaciones actuales van desde el uso de cable de par trenzado hasta medios de fibra óptica, estas últimas ofrecen velocidades de 10 Gigabits por segundo, con lo cual se redefine el alcance geográfico de la tecnología Ethernet, esto gracias al mayor cubrimiento que permite la fibra óptica.

Imagen 2
Fuente: Propia, adaptada de currículo CCNA Exploration

Dado su asocio con la capa física, Ethernet contempla la implementación de codificación y decodificación del contenido de tramas, otro aspecto importante de esta tecnología es que, pese a la diversidad de tipos de medios utilizados, todas las implementaciones tienen la misma estructura de trama, motivo por el cual versiones anteriores cumplen con los requisitos actuales.

El manejo de colisiones en Ethernet

Las antiguas redes locales Ethernet se valían generalmente de dispositivos intermediarios como hubs, dispositivo que al recibir una corriente de bits por una de sus interfaces, las reenvía por las demás, lo que resultaba en un entorno de medios compartidos, en el que sólo uno de los nodos podía transmitir a la vez (modo half-duplex); si al dispositivo concentrador se conectaban más nodos, se aumentaba la probabilidad de colisiones dando lugar a la degradación del desempeño de la red.

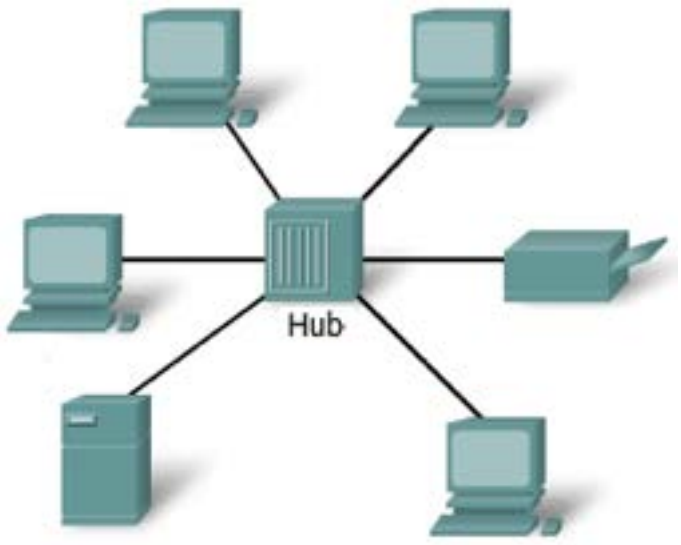


Imagen 3
Fuente: Propia, adaptada de currículo CCNA Exploration

Las redes Ethernet actuales emplean switches o conmutadores en lugar de hubs. Un switch es un dispositivo con la capacidad de reenviar información recibida a la interfaz correspondiente con base en la dirección física en caso que se conozca. La utilización de switch reduce la probabilidad de colisiones al limitar el número de equipos que reciben las tramas reenviadas, lo que sumado a la posibilidad de transmitir y enviar información al mismo tiempo (comunicación full-duplex), ha facilitado la evolución que permite contar hoy con Ethernet del orden de los Gbps.

Tamaño de la trama Ethernet

Recordemos que una trama genérica se compone de encabezados de trama, datos de capa de red y tráiler. El tamaño mínimo de una trama Ethernet IEEE 802.3 es de 64 bytes en tanto que el tamaño máximo es de 1518 bytes. Un estándar nuevo, IEEE 802.3ac, que está fuera del alcance de este curso, cuenta con un tamaño máximo de 1522 bytes.

Los campos en los que se distribuye el tamaño total de la trama se muestran en la siguiente figura y algunos de ellos e describen brevemente a continuación.

IEEE 802.3						
7 bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 a 1500 Bytes	4 Bytes
Preámbulo	Límite Inicio trama	MAC Destino	MAC Origen	Long	Encabezad y datos 802.2	FCS

Imagen 4
Fuente: Propia, adaptada de currículo CCNA Exploration

- Preámbulo y Delimitador de inicio de trama: son campos importantes en la sincronización de la comunicación entre nodos finales, podría decirse que su utilidad es prevenir a los equipos receptores sobre la llegada de una nueva trama.
- Dirección MAC de destino: corresponde a la dirección física del equipo al que se ha de enviar un flujo de información. Mediante el valor contenido en este campo, un equipo puede determinar si es el destinatario de una trama. Cada equipo al que llega una trama compara el contenido del campo de la dirección MAC destino con el identificador de su propia tarjeta de interfaz de red, si hay coincidencia entre estos valores el dispositivo procesa la trama.
- Dirección MAC de origen: es la dirección o identificador de la tarjeta de red del equipo que envía la información.
- Longitud: los estándares IEEE 802.3 anteriores a 1997, usaban el campo Longitud para indicar la longitud exacta del campo de datos. Una versión de Ethernet, no descrita aquí usa en su lugar un campo Tipo para indicar el protocolo que se implementa.
- Datos y Pad: contienen los datos de capa de red, generalmente es un paquete IP, si se entrama un paquete con poco contenido, el Pad se utiliza para ajustar el tamaño de la trama hasta alcanzar el tamaño mínimo requerido.
- Secuencia de verificación de trama: es empleado en la detección de errores en el contenido de la trama. Su valor se fundamenta en un cálculo de CRC realizado por el emisor con base en el contenido de la trama al momento del envío, por su parte el receptor calcula nuevamente el CRC, la no coincidencia de los valores de CRC es indicación de errores en la transmisión.

Direcciones MAC Ethernet

Es la dirección física o dirección de Control de Acceso al Medio. Como se indicó en la unidad anterior, la dirección MAC corresponde a una cadena de 48 bits que se expresa mediante 12 dígitos hexadecimales. (Recuérdese que hay una única correspondencia entre los

16 dígitos hexadecimales y los posibles valores de cadenas de 4 bits). De los 48 bits o 12 dígitos hexadecimales, la mitad de orden superior identifica al fabricante de la tarjeta de interfaz de red y se conoce como Identificador Único Organizacional (OUI); la otra mitad identifica una tarjeta específica de determinado fabricante. Estas son normas implementadas por el IEEE para garantizar la exclusividad del identificador de cada tarjeta, el propio IEEE asigna el OUI a cada fabricante y este último graba la dirección completa en la Memoria de Sólo Lectura (ROM) de la NIC.

Patrones de tráfico Ethernet

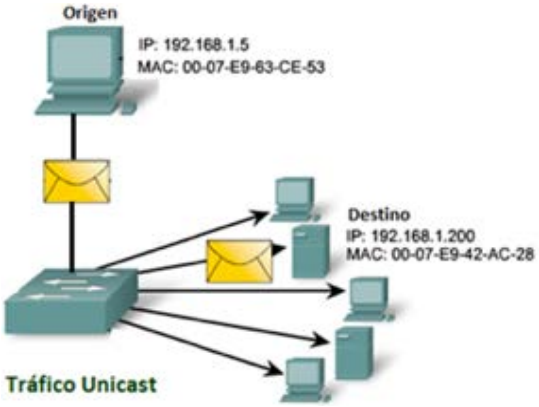


Imagen 5
Fuente: Propia, adaptada de currículo CCNA Exploration

En la unidad cuatro se describió los patrones de tráfico a nivel de capa de red, estos son Unicast, Multicast y Broadcast, cada patrón de tráfico se define según el tipo de dirección IP de destino. A nivel de capa de enlace de datos los patrones son caracterizados por el valor de la dirección física del destino. La imagen adjunta ilustra los patrones de tráfico, en ella se señala las direcciones físicas y lógicas.

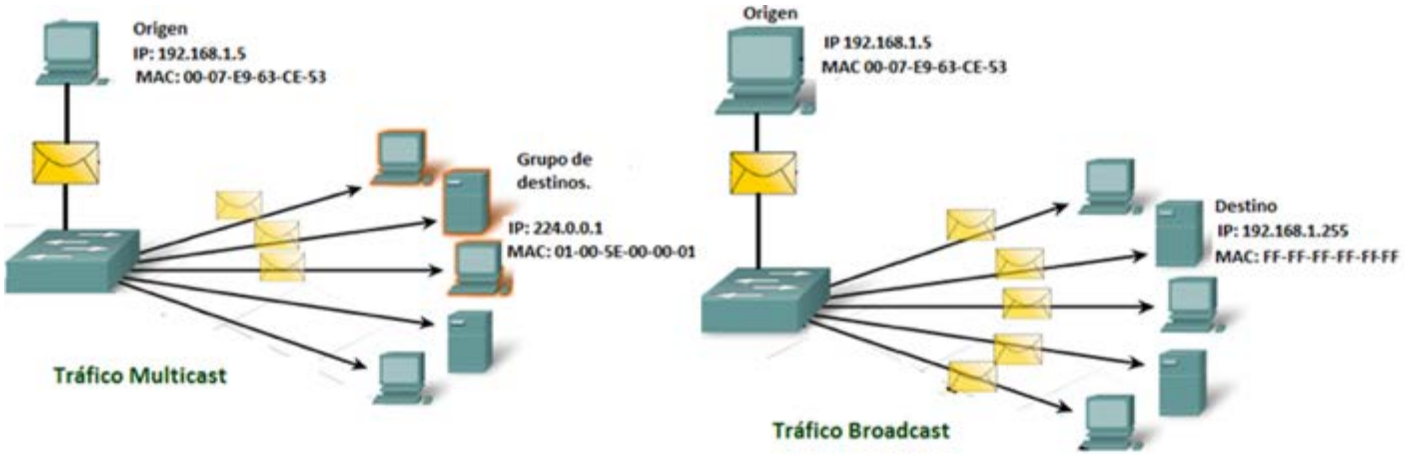


Imagen 6
Fuente: Propia, adaptada de currículo CCNA Exploration

El control de Acceso al medio Ethernet

Ethernet emplea el método de control CSMA/CD o Acceso Múltiple con Detección de Portadora y detección de Colisiones, mediante el cual los dispositivos que requieren transmitir datos deben detectar previamente si el medio está libre para poder transmitir, en caso que detecte que el medio está siendo ocupado por otro dispositivo, posterga su intento de transmisión. Es posible que la transmisión iniciada por un dispositivo no haya sido detectada por otro equipo en la red, esto en razón a la latencia asociada a la distancia que debe recorrer la señal, si esto sucede y otro equipo inicia su transmisión, se produce una colisión en la cual las dos señales se combinan en una señal sin sentido, con parámetros, anormales que es detectada por los demás nodos como una colisión. La detección de una colisión da lugar a que todos los nodos que requieran transmitir desistan de hacerlo hasta que desaparezca la señal producto de la colisión. Los nodos involucrados en la colisión aplazan sus intentos de retransmisión a instantes posteriores definidos aleatoriamente tras la ejecución un algoritmo de postergación, lo que garantiza que no haya coincidencia en los instantes de nuevos intentos de transmisión.

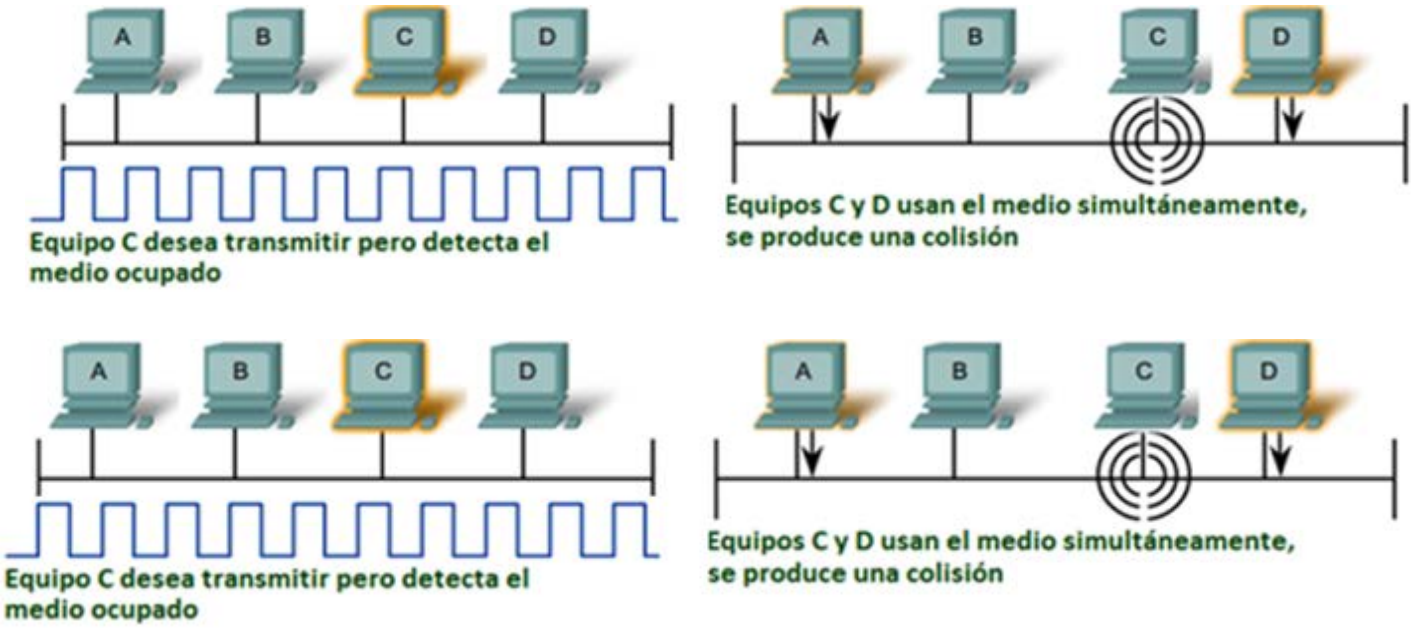


Imagen 7
Fuente: Propia, adaptada de currículo CCNA Exploration

Generalidades del componente físico de Ethernet

El componente físico de la tecnología Ethernet, denominado PHY, determina las diferencias entre las diferentes especificaciones.

Las diferencias que existen entre Ethernet estándar, Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet tienen lugar en la capa física, generalmente denominada Ethernet PHY. Los medios de transmisión empleados por Ethernet son el cable UTP y la fibra óptica, los cuales, claro está, soportan velocidades diferentes. IEEE define cuatro variantes comerciales con diferentes velocidades de transmisión de datos, estas son:

- 10Base-T Ethernet (velocidad de 10 Mbps).
- Fast Ethernet (100 Mbps).
- Gigabit Ethernet (1000 Mbps).
- 10 Gigabit Ethernet (10 Gbps).

Redes inalámbricas

Las Redes de Área Local Inalámbricas o WLAN (Wireless Local Area Network), a diferencia de las LAN cableadas no se encuentran sujetas a las restricciones de cableado. Las tecnologías WLAN dan lugar a la reformulación de redes locales, teniéndose por ejemplo redes de cubrimiento del orden de los kilómetros y una infraestructura móvil no confinada a los muros de las construcciones. La información es transportada en forma de ondas electromagnéticas que viajan por el aire.

Las redes inalámbricas no necesariamente constituyen un sustituto de las redes cableadas, sino que resultan ser un complemento a las mismas, dispositivos de la tecnología inalámbrica se pueden incorporar a la infraestructura de una red cableada en funcionamiento. En la actualidad se cuenta con la tecnología Wifi que permite la creación de redes de computadores, los equipos deben disponer de una tarjeta de interfaz de red inalámbrica.

Razones del uso de las WLAN

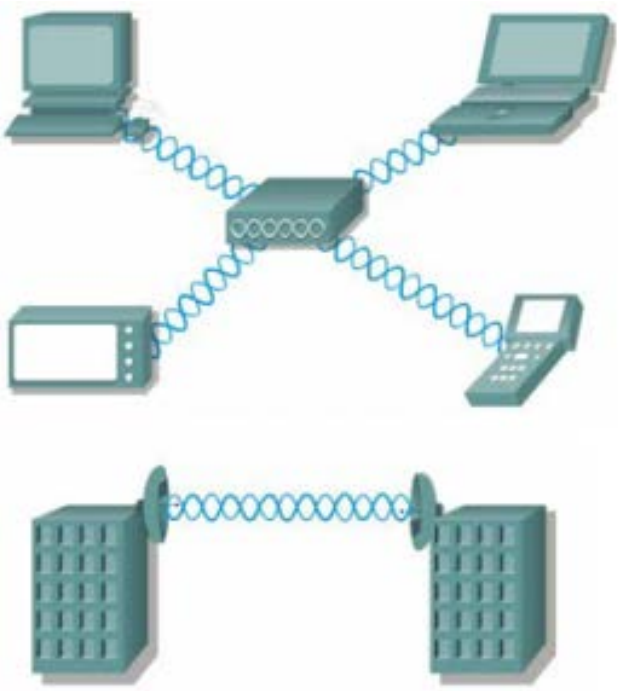


Imagen 8
Fuente: Propia, adaptada de currículo CCNA Exploration

Las redes cableadas basadas en la tecnología Ethernet funcionan a velocidades de hasta 10 Gbps, la mayoría de WLAN funcionan a 11 Mbps y algunas a 54 Mbps, sin embargo, pese a estas desventajas en cuanto a la velocidad, de las redes WLAN frente a las LAN Ethernet, las WLAN resultan suficientes para muchos entornos de pequeñas empresas, obteniéndose el beneficio de la movilidad de usuarios dentro de un área definida. Por otro lado existen dispositivos LAN que brindan conectividad entre sitios separados

hasta 40 kms, evitando así la necesidad de contratar líneas de comunicación para enlazar sitios separados tales distancias.

Comparación entre una WLAN y una LAN

Las LAN Ethernet se enmarcan en los estándares IEEE 802.3 y LAN inalámbrica corresponden al estándar 802.11. Las WLAN utilizan una parte de la banda de frecuencia de radio (RF). Las señales que se propagan a través de ondas de radio no están confinadas a la trayectoria definida por un cable, esto hace que las tramas de datos estén disponibles para cualquiera que pueda recibir la señal, además de lo anterior la señal no se encuentra protegida y es más susceptible de ser afectada por otras señales de frecuencias similares en la misma área.

Los diferentes computadores o equipos clientes en una WLAN, provistos de tarjetas de interfaz de red inalámbricas, se conectan generalmente a través de un router inalámbrico o un dispositivo conocido como punto de acceso inalámbrico o Access Point (AP). Una de las debilidades de las tecnologías WLAN se relaciona con la seguridad, ya que las señales son fácilmente intersectadas.

Estándares de LAN inalámbricas

Las LAN inalámbrica 802.11 se enmarcan en un conjunto de estándar IEEE que definen la utilización de la radiofrecuencia (RF) en las bandas libres. Estos estándares han evolucionado desde su creación y en la actualidad los más populares son IEEE 802.11a, IEEE 802.11b, IEEE 802.11g y 802.11n.

802.11a y g funcionan a velocidades de hasta 54 Mb/s, 802.11b maneja un máximo de 11 Mbps. Las diferencias en las velocidades se relacionan con las técnicas de modulación utilizada. Las referidas a los estándares aquí referenciados son Espectro de Dispersión de Secuencia Directa (DSSS) y Multiplexación por División de Frecuencias ortogonales (OFDM), temáticas que se escapan del alcance de esta asignatura, basta saber que OFDM proporciona velocidades mayores, pero que la implementación de DSSS es más simple y económica que OFDM.

Estándar IEEE 802.11A

Usa modulación OFDM y utiliza la banda de 5 GHz. Los dispositivos de esta tecnología son menos propensos a interferencias que los que operan en la banda de 2.4 GHz debido a que en un entorno dado hay menos dispositivos comerciales que utilizan la banda de 5 GHz. Entre las desventajas de trabajar en la banda de 5 GHz se tiene que a frecuencia más alta, mayor es la absorción por parte de obstáculos.

Estándares IEEE 802.11b y 802.11g

El estándar 802.11b especificó las velocidades de 1; 2; 5.5 y 11 Mbps en la banda de 2.4 GHz utilizando modulación DSSS; 802.11b especifica velocidades mayores en la misma banda usando modulación OFDM. IEEE 802.11g también especifica la utilización de DSSS para la compatibilidad con los sistemas IEEE 802.11b. El DSSS admite tasas de datos de 1; 2; 5.5 y 11 Mbps, como también las tasas de datos OFDM de 6; 9; 12; 18; 24; 48 y 54 Mbps.

Aunque los dispositivos que operan en la banda de 2.4 GHz tienen mayor alcance que los de la banda de 5 GHz, presentan como desventaja que muchos dispositivos de clientes también utilizan la misma banda, dando lugar a posibles interferencias.

Estándar IEEE 802.11n

Planteado para mejorar las velocidades

y alcance. Utiliza múltiples radios y antenas en puntos finales, cada uno transmitiendo en la misma frecuencia (tecnología de entrada múltiple/salida múltiple o MIMO), en teoría la tasa máxima de transferencia de datos podría llegar a 600 Mbps.

Certificación Wifi

Las tres organizaciones con influencia sobre los estándares de las LAN Inalámbricas son: **ITU-R, IEEE y Wifi Alliance.**

- El ITU-R: regula la asignación del espectro RF y órbitas satelitales.
- El IEEE: desarrolla y mantiene los estándares para redes de área local y metropolitana con la familia de estándares IEEE 802.11.
- La Wifi Alliance: es una asociación de proveedores encargada de la promoción y crecimiento y aceptación de las WLAN y expide la certificación Wifi. Su objetivo es promover y mejorar la interoperabilidad de productos basados en el estándar 802.11, y certifica proveedores en conformidad con las normas.

Imagen 9
Fuente: https://image.freepik.com/free-icon/wifi--ios-7-interface-symbol_318-34377.png

Componentes de la tecnología inalámbrica

Imagen 10
Fuente: Propia, adaptada de currículo CCNA Exploration

En esta parte se describe algunos elementos componentes de las tecnologías inalámbricas, entre los cuales destacamos las NIC inalámbricas y los puntos de acceso o AP.Tarjeta de interfaz de red inalámbrica.

La tarjeta de interfaz inalámbrica o NIC inalámbrica es el componente del dispositivo cliente que permite recepción y envío de las señales de radio de las WLAN. Los dispositivos portátiles vienen generalmente provistos de una NIC inalámbrica. A los computadores de escritorio podemos instalarles tarjetas inalámbricas mediante una de las ranuras de expansión o mediante un puerto USB.

Puntos de Acceso inalámbrico

Si los dispositivos clientes no se comunican directamente entre ellos, lo hacen a través de un AP (Access Point) o punto de acceso, este dispositivo también facilita la conexión de los clientes inalámbricos a la red cableada. Un AP es un dispositivo de Capa 2. Los dispositivos WLAN están diseñados para evitar las colisiones mediante el uso de un método de acceso conocido como CSMA/CA.

Routers inalámbricos

Imagen 11
Fuente: Propia, adaptada de currículo CCNA Exploration

Son dispositivos que integran funciones de punto de acceso, switch Ethernet y router. Son apropiados para redes de uso casero y de pequeñas empresas.

Control de acceso 802.11

En las LAN Ethernet el control de acceso CSMA se complementa con la detección de presencia de colisiones (CD). Con el fin de evitar las colisiones, en las WLAN 802.11, CSMA se complementa con mecanismos orientados a evitar las colisiones (CA). Los puntos de acceso ejecutan una Función de Coordinación Distribuida (DCF), también llamada Acceso Múltiple por Detección de Portadora con Prevención de Colisiones (CSMA/CA). Los dispositivos de la WLAN detectan el nivel de energía que indica si el medio está ocupado, y si este no es el caso espera a que se libere antes de enviar. Dado que se requiere que todos los dispositivos lo realicen, se distribuye la función de coordinar el acceso al medio.

Si un punto de acceso recibe información desde la estación de un cliente, le envía un acuse de recibo para confirmar que se recibió la información. Este acuse de recibo evita que el cliente suponga que se produjo una colisión e impide la retransmisión de información por parte del cliente.

Operación inalámbrica

Para que un equipo cliente pueda participar en una red inalámbrica a través de un punto de acceso, se requiere la configuración de un conjunto de parámetros tanto en el AP como en el cliente. Entre los parámetros configurables se tiene: modo de red inalámbrica, SSID y canal.

- ***Modo de red inalámbrica:*** hace referencia a los estándares 802.11a, b, g, o n. La compatibilidad de 802.11g con 802.11b, los puntos de acceso admiten ambos estándares. Por ejemplo, cuando un punto de acceso Linksys se configura para permitir clientes de 802.11b y 802.11g, opera en modo mixto. Para que un AP admita 802.11a b y g, requiere contar con la capacidad de operar en las bandas diferentes de RF.
- ***SSID:*** el SSID o Identificador de Conjunto de Servicios es el identificador usado por los clientes para distinguir las diferentes WLAN detectadas. La figura adjunta muestra un ejemplo de SSID correspondientes a redes detectadas por un cliente. Los SSID son cadenas alfanuméricas con longitud de 2 a 32 caracteres distinguiendo entre mayúsculas y minúsculas.
- ***Canal:*** al hablar de la banda de 2.4 Ghz en el contexto de IEEE 802.11, se considera un espectro dividido en 11 o 13 canales, cada canal con un ancho de banda de 22 Mhz y superpuestos de tal forma que las frecuencias centrales de canales sucesivos están separadas 5 Mhz.

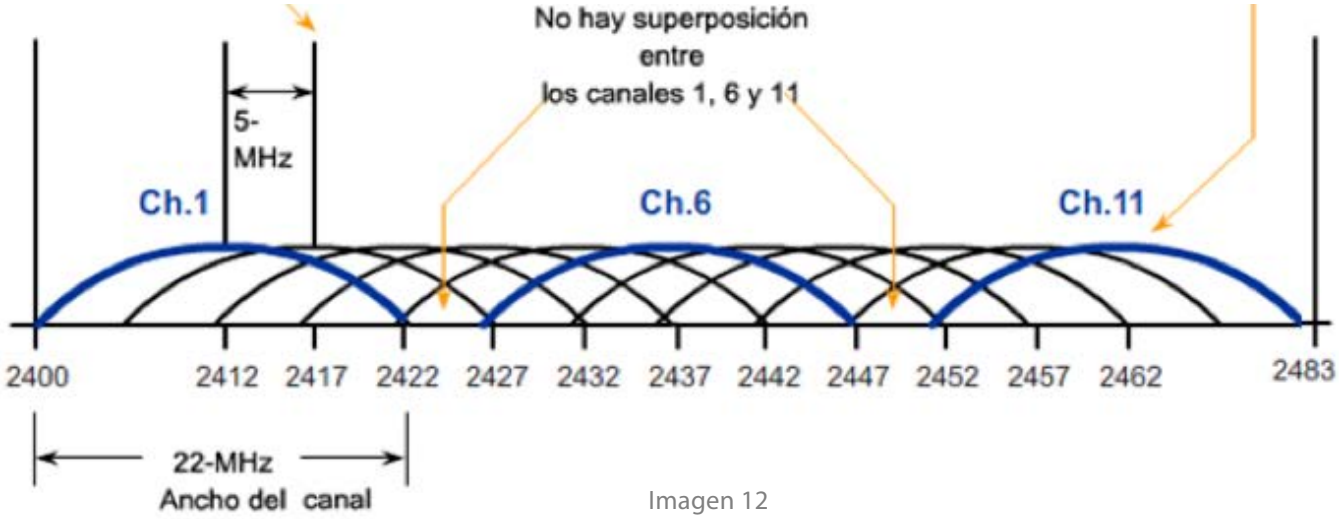


Imagen 12
Fuente: Propia, adaptada de currículo CCNA Exploration

Si se requiere el uso de varios puntos de acceso, se deben configurar de tal manera que usen canales no superpuestos, por ejemplo tres AP adyacentes podrían utilizar los canales 1, 6 y 11. Muchos AP tienen la capacidad de seleccionar automáticamente un canal. Algunos productos realizan monitoreo continuo para ajustar la configuración de canal.

Topologías 802.11

La configuración de una WLAN puede ser de diferentes topologías de red, la unidad fundamental de la tecnología 802.11 es el Conjunto de Servicios Básicos o BSS. Las diferentes topologías inalámbricas son:

Redes Ad hoc

Una red Ad-Hoc es aquella que opera sin el uso de AP. Los clientes conectados se configuran de tal manera que operen en este modo. IEEE 802.11 considera a una red Ad hoc como un BSS (IBSS) independiente.

Redes de infraestructura

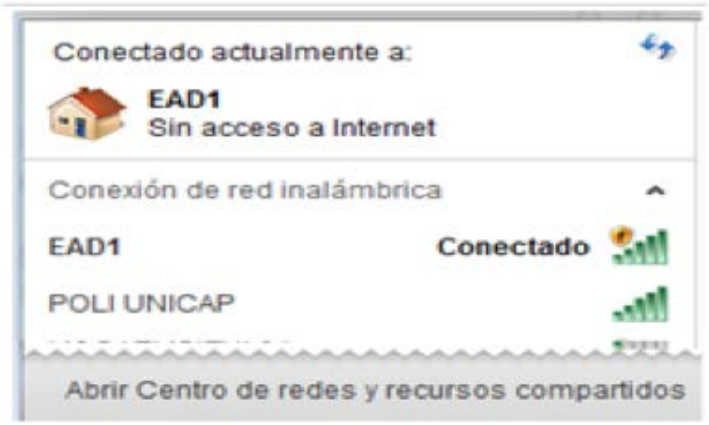


Imagen 13
Fuente: Propia, adaptada de currículo CCNA Exploration

Un único punto de acceso se encarga de la administración de los parámetros inalámbricos, la topología correspondiente recibe el nombre de BSS. El área que cubre se llama área de servicios básicos (BSA).

Conjuntos de servicios extendidos

Para lograr una mayor cobertura, una red puede requerir de la instalación de varios AP obteniéndose una topología denominada **Conjunto de Servicios extendidos (ESS).** En esta topología, los diferentes BSS se diferencian por los Identificadores BSS (BSSID), cada identificador corresponde a la dirección MAC del respectivo AP. El área de cobertura se llama área de servicio extendida (ESA).

Sistema de distribución común

Con el fin de que un **ESS** parezca ser un **BSS**, se tiene la posibilidad de un sistema de distribución común. Un **ESS** incluye generalmente un **SSID** común para permitir al usuario moverse de un punto de acceso a otro.

Las celdas corresponden al área de cobertura de un único canal. Un ESS debe contar con 10 a 15 por ciento de superposición entre celdas, un SSID común y canales no superpuestos para poder contar con la capacidad de roaming.

Asociación del cliente y el AP

Para que un cliente pueda conectarse a una WLAN debe previamente asociarse a ella. Los pasos y componentes que intervienen en este proceso son:

- Tramas beacons: utilizadas por la red para anunciarse con el fin que los clientes puedan detectar redes disponibles y que puedan así elegir una red o un AP a utilizar.
- Sondas: tramas utilizadas por los clientes para detectar la presencia de redes.
- Autenticación: proceso que permite o niega la conexión de un cliente a la red, puede basarse en el uso de contraseña.
- Asociación: establecimiento de conexión entre el AP y un cliente.

Los puntos de acceso transmiten tramas beacons periódicamente, mientras que el sondeo, autenticación y asociación se usa únicamente en la asociación propiamente dicha.

Proceso conjunto 802.11 (Asociación)

- Sondeo de 802.11: los clientes buscan una red mediante sondeo a múltiples canales, especificando SSID y tasas de bit. Si el cliente sólo deseas saber las WLAN disponibles, el sondeo se realiza sin SSID, y los AP configurados para responder estos sondeos responderán. Los AP con la característica de broadcast SSID deshabilitada no responden al sondeo.
- Autenticación 802.11: el estándar 802.11 se desarrolló inicialmente con dos mecanismos de autenticación, uno llamado autenticación abierta, en la cual el cliente pide ser autenticado y el AP lo autentica sin el uso de contraseñas. El otro mecanismo de autenticación, llamado autenticación de clave compartida, se fundamenta en el uso de contraseñas.
- Asociación 802.11: con la etapa de asociación se completan elementos relacionados con la seguridad y se establece la conexión entre cliente y punto de acceso.

En las actividades de laboratorios correspondientes a este capítulo se ha de realizar la configuración de un router inalámbrico.

Configuración de punto de acceso inalámbrico

La configuración de un AP en una red inalámbrica abarca tareas como definición del SSID, activación de seguridad, configuración de canal entre otras. Es útil realizar una copia de respaldo con fines de restauración de la configuración.

Un enfoque muy útil en la implementación de la red inalámbrica, puede ser realizar configuraciones y pruebas progresivas, por ejemplo iniciar con un AP y un cliente, verificando conectividad y que el cliente haya sido configurado dinámicamente mediante DHCP y que se superen las pruebas básicas de red. Luego de las pruebas, si son exitosas, se procede a la configuración de la seguridad.

La mayoría de los AP vienen con una configuración predeterminada que los hace funcionales, sin embargo es recomendable cambiarla por razones de seguridad y para lograr mayor funcionalidad. En muchos casos la configuración se puede realizar a través de una interfaz gráfica.

La configuración del punto de acceso se inicia conectándolo a un PC mediante un cable al puerto Ethernet del computador y abriendo el navegador web disponible. Se puede acceder a la aplicación de configuración mediante la dirección IP predeterminada del WRT310N, ésta es 192.168.1.1. Hecho lo anterior se puede ver una ventana solicitando usuario y contraseña. El nombre de usuario lo podemos dejar en blanco e ingresar la contraseña predeterminada admin. En caso de haber configurado previamente el router, es posible que usuario y contraseña se hayan cambiado.

Algunos de los elementos que se pueden configurar se describen brevemente a continuación:

- Network Mode: se refiere al estándar particular, 802.11a, 802.11b 802.11g, 802.11n. si a través del AP se debe conectar equipos de más de uno de estos estándares se debe seleccionar el modo Mixed, pero se disminuye el rendimiento.
- Network Name (SSID): es el nombre de la red, debe ser idéntico para todos los dispositivos. Se debe tener en cuenta que se distingue entre mayúsculas y minúsculas la longitud máxima es de 32 caracteres, es recomendable cambiar el SSID predeterminado (linksys).
- SSID Broadcast: de forma predeterminada los AP de la marca Linksys transmiten el SSID en broadcast, de tal manera que los clientes inalámbricos detectan el broadcast del SSID mediante el punto de acceso. Esta opción se puede deshabilitar para evitar la difusión del SSID.
- Radio Band: un mejor rendimiento en redes que usan dispositivos de las variantes n, g y b, es elegir la opción **Auto** como la predeterminada. Si sólo se usa dispositivos de la tecnología 802.11n se debe seleccionar la opción **Wide - 40MHz Channel**. Para tecnologías 802.11 g o b, únicamente, la mejor opción es Standard - 20MHz Channel.
- Wide Channel: opción disponible para canal Wireless-N principal si se ha seleccionado **Wide - 40MHz Channel** del parámetro Radio Band. Se puede seleccionar cualquier canal del menú desplegable.

Standard Channel: es el canal secundario si se ha seleccionado, el Wide - 40MHz Channel para la configuración de Radio Band.

- Security Mode: permite especificar el modo de seguridad inalámbrica. Los modos existentes, por ejemplo, para un router WRT310N son:

WEP.

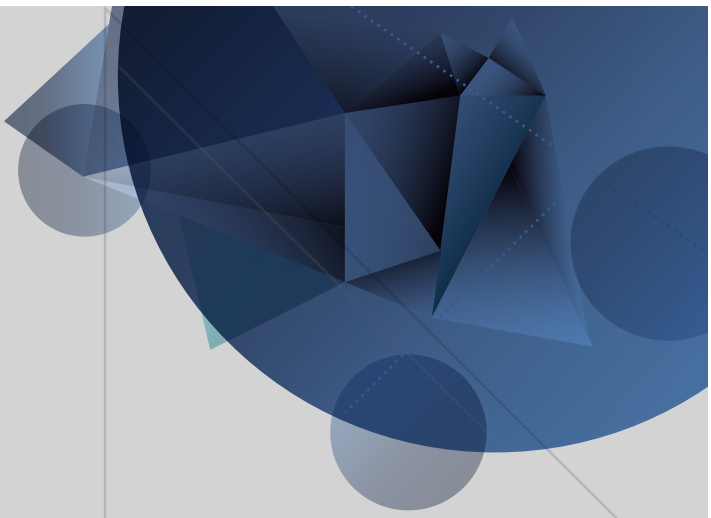
- PSK-Personal o WPA-Personal en v0.93.9 firmware o posterior.
- PSK2-Personal o WPA2-Personal en v0.93.9 firmware o posterior.
- PSK-Enterprise o WPA-Enterprise en v0.93.9 firmware o posterior.
- PSK2-Enterprise o WPA2-Enterprise en v0.93.9 firmware o posterior.
- RADIUS.
- Disabled.

En actividades de laboratorios relacionadas con configuración de redes inalámbricas se tendrá la oportunidad de profundizar en la conceptualización de estos modos.

4

Unidad 4

Configuración básica de equipos de red



Telemática I

Autor: Juan Carlos Ramírez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Esta parte trata la configuración de routers centrándose en equipos marca Cisco, para lo cual se hace uso de los comandos del sistema operativo Cisco IOS. El capítulo brinda conocimientos sobre routers y prácticas relacionados con el IOS de Cisco, el archivo de configuración, modos de operación del IOS, uso de comandos del IOS, entre otros.

U4 Metodología

Los estudiantes como centro activo de aprendizaje deben hacer la lectura y análisis permanente de este material, que les permite realizar una contextualización del tema, conociendo la teoría general y su aplicación práctica en contextos específicos.

Configuración básica de equipos de red

Routers

Un router es un dispositivo responsable de la entrega de paquetes entre diferentes redes y conecta múltiples redes a través de sus diferentes interfaces, cada una de las interfaces pertenece a una red diferente. La efectividad de las comunicaciones de red depende, en gran medida, de la capacidad de los routers para reenviar paquetes de la manera más eficiente posible. Los routers pueden usar rutas alternativas con el fin de garantizar la posibilidad de conexión de la red, en caso de que la ruta principal falle. Al igual que los computadores, los routers tienen componentes de hardware como: CPU, memoria RAM y ROM, también cuentan con elementos de software como Sistema operativo y archivos de configuración.

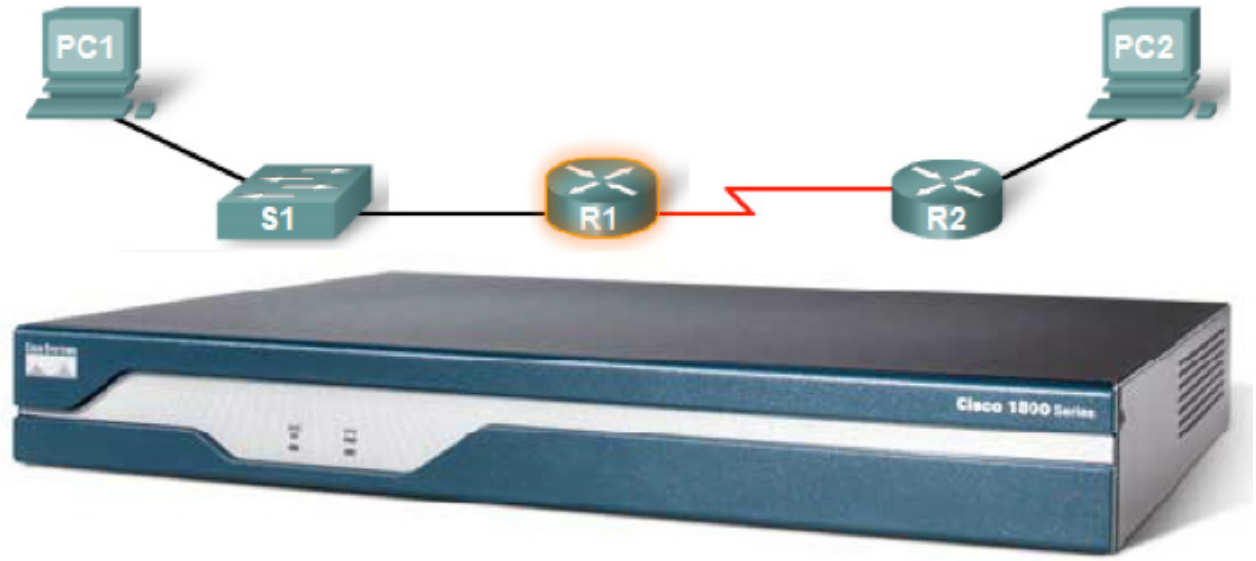


Imagen 1
Fuente: Propia, adaptada de currículo CCNA Exploration

Cuando un router recibe un paquete IP en una interfaz, determina la interfaz a través de la cual reenviar el paquete hacia su destino, por ejemplo, una interfaz LAN Ethernet para un destino en una red directamente conectada al router, o una conexión WAN que conecta un router a otro router.

El proceso de reenvío de paquete realizado por un router, básicamente consiste en examinar la dirección IP de destino del paquete a reenviar y consultar la tabla de enrutamiento para decidir por cuál de sus interfaces hacer el envío.

Dado que un router puede tener diferentes tipos de interfaces, asociadas a diferentes tipos de tecnologías de enlace de datos, el entramado, o encapsulación de enlace de datos, de un paquete depende del tipo de interfaz por donde entra o sale un paquete y del tipo de medio al que se conecta la interfaz, la tecnología de enlace de datos de la interfaz de salida puede ser diferente de la de entrada. Entre las diferentes tecnologías de enlace de datos se cuenta LAN Ethernet y conexiones seriales WAN como T1, Frame Relay y ATM.

Routers y capa de red

Un router es principalmente un dispositivo de capa 3, ya que toma decisiones de reenvío en función de información del paquete IP que debe reenviar, pero también opera en la capa 2, al encapsular el paquete de Capa 3 como parte de una trama de enlace de datos según el tipo de interfaz de salida; y también opera en la Capa 1 puesto que la trama de Capa 2 se codifica en señales físicas que representan bits.

Cada router en la ruta de un paquete realiza el proceso de desentramado del paquete, busca en la tabla de enrutamiento para tomar la decisión de reenvío y realizar el respectivo entramado.

Componentes de hardware del router

Los diferentes tipos y modelos de routers cuentan con un conjunto de componentes de hardware, consistente en procesador, memorias, interfaces, entre otros.

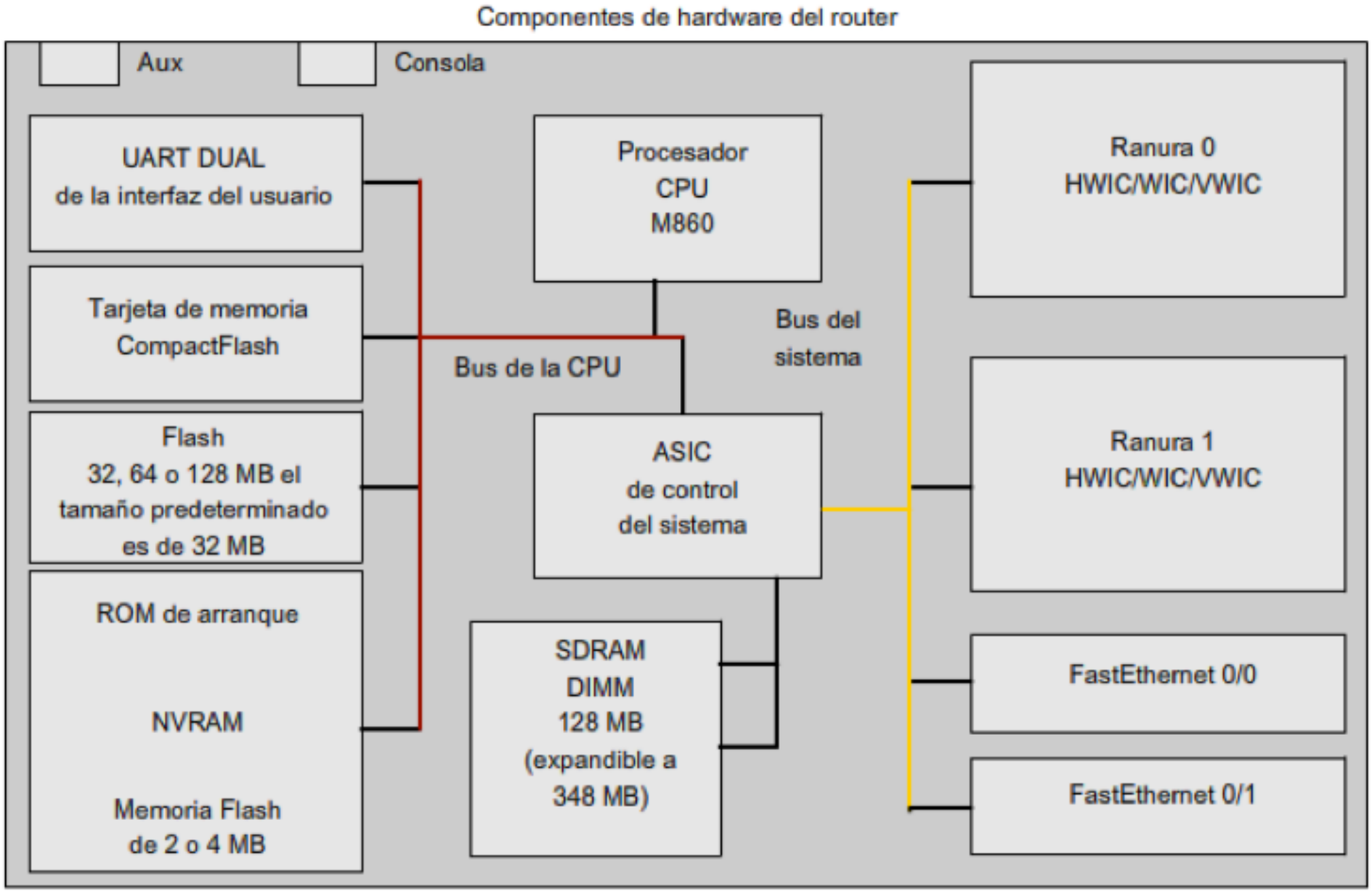


Imagen 2
Fuente: Propia, adaptada de currículo CCNA Exploration

Memorias y procesador

El procesador o CPU: es responsable de las tareas de procesamiento de información relacionada con el funcionamiento del router, ejecuta las instrucciones del sistema operativo y las definidas en la configuración.

Memoria RAM: almacena las instrucciones y datos que procesa la CPU, específicamente almacena componentes como: Sistema operativo, archivo de configuración en ejecución, tabla de enrutamiento IP, la cual contiene información útil para alcanzar redes destino, caché ARP, el cual asocia direcciones IP y direcciones MAC y búfer de paquetes. La memoria RAM pierde el contenido cuando se apaga o reinicia el router.

Memoria ROM: es una forma de almacenamiento permanente. Los dispositivos Cisco usan la memoria ROM para almacenar elementos de software relacionados con el arranque del router.

Memoria Flash: memoria no volátil que se puede almacenar y borrar de manera eléctrica, se usa como almacenamiento permanente para el sistema operativo. La memoria flash consiste en tarjetas SIMM o PCMCIA actualizables.

Memoria RAM No Volatil (NVRAM): no pierde su contenido cuando se desconecta la alimentación eléctrica, se usa como almacenamiento permanente para el elemento de software conocido como archivo de configuración de inicio.

Puertos e interfaces

Puertos de administración: son conectores físicos usados con fines de administración del router, no son usados para reenvío de paquetes. El puerto de administración más común es el puerto de consola, al cual se conecta una terminal para configurar el router sin necesidad de acceso a la red para ese router. El puerto auxiliar es otro puerto de administración con el que cuentan algunos routers y puede usarse para conectar un modem.

Imagen 3
Fuente: Propia, adaptada de currículo CCNA Exploration

Interfaces físicas del router: se usan para el recibo y envío de paquetes, los routers pueden tener muchas interfaces para conectarse a múltiples redes. Normalmente las interfaces se conectan a distintos tipos de redes, lo que significa que se necesitan distintos tipos de medios y conectores. Generalmente un router tiene interfaces FastEthernet para conectarse a redes LAN y distintos tipos de interfaces WAN para conectar una variedad de enlaces seriales, (T1, DSL e ISDN).

Los routers Cisco usan indicadores LED para proveer información de estado. Un LED de interfaz indica la actividad de la interfaz correspondiente. Si un LED está apagado cuando la interfaz está activa y bien conectada, puede ser señal de un problema en la interfaz. Si la interfaz está en gran actividad, el LED estará continuamente encendido.

Cada interfaz en un router hace parte de diferentes redes y se debe configurar con dirección IP y máscara de subred de redes diferentes. El IOS no permitirá que dos interfaces activas en el mismo router pertenezcan a la misma red.

Interfaces LAN: se usan para conectar el router a la LAN, también tiene una dirección MAC de Capa 2 y es parte de la LAN Ethernet como cualquier otro PC en esa LAN.

Interfaces WAN: se usan para conectar un router a redes externas, cada interfaz WAN tiene su propia dirección IP y máscara de subred, que la identifica como miembro de una red específica, usan sus propias direcciones de Capa 2 según la tecnología.

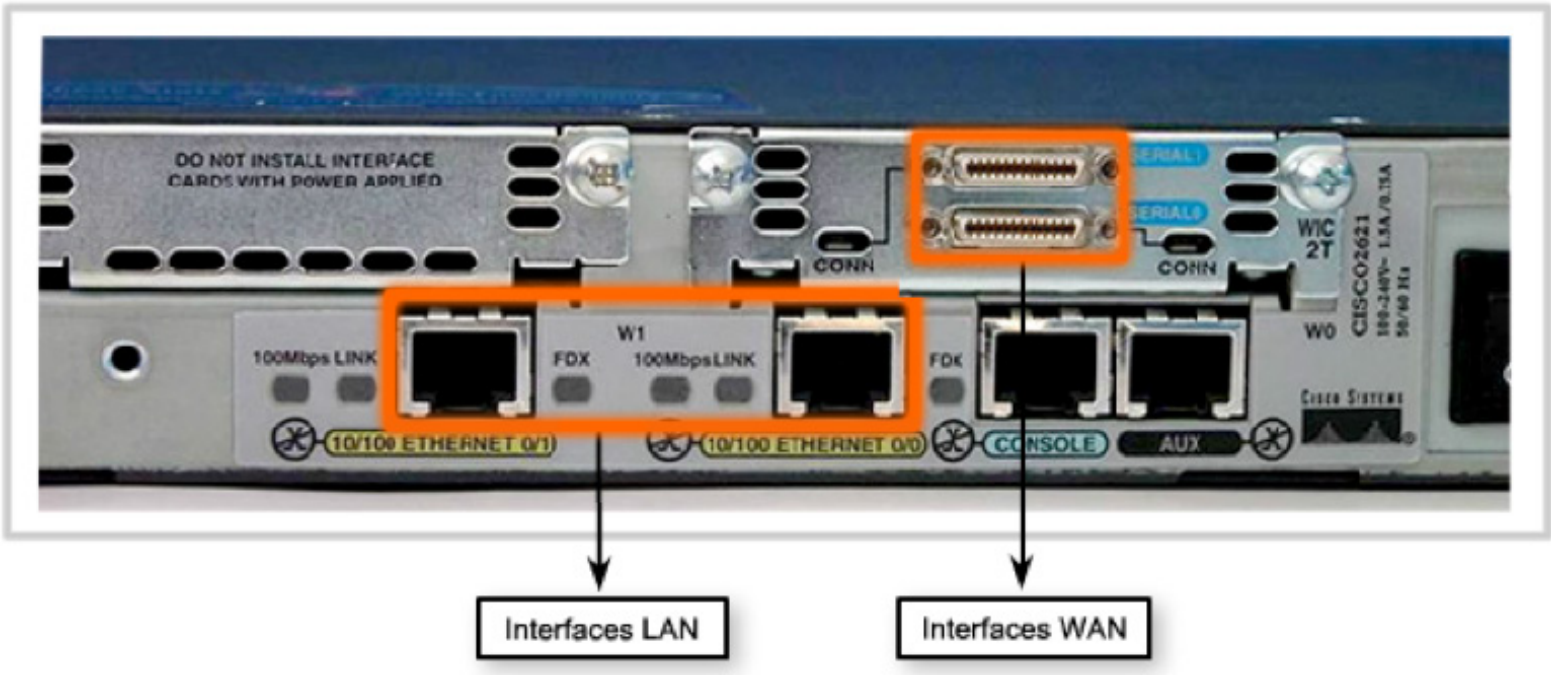


Imagen 4
Fuente: Propia, adaptada de currículo CCNA Exploration

Componentes de software de un router

Los componentes de software fundamentales en un router son el sistema operativo y el archivo de configuración.

Sistema Operativo IOS: es el software que administra el hardware y otros componentes de software de un router Cisco. Existen diferentes imágenes según las capacidades del router. Algunos routers proveen una interfaz gráfica de usuario (GUI), pero muchas veces es preferible el uso de la interfaz de línea de comandos (CLI). El sistema operativo de los routers Cisco se conoce como IOS (*Internetwork Operating System)* de Cisco. A través de IOS se puede definir configuraciones orientadas a funciones de enrutamiento, conmutación, seguridad de acceso, escalabilidad de la red.

Archivo de configuración: define el funcionamiento del equipo, corresponde a un script de comandos del IOS. Todo router contiene dos archivos de configuración, archivo de configuración en ejecución y archivo de configuración de inicio.

Proceso de arranque

Proceso de arranque: el arranque de un router consiste fundamentalmente en las cuatro etapas descritas a continuación:

1. Ejecución del POST (Prueba de Autodiagnóstico al encender POST): se utiliza para probar el hardware del router, es ejecutado por el software en la ROM. Finalizado el POST se ejecuta el bootstrap.
2. Ejecución del bootstrap: la tarea principal de este programa bootstrap es ubicar al IOS para cargarlo en la RAM. El bootstrap se copia de la ROM a la RAM y es ejecutado por la CPU.
3. Ubicación y carga del Cisco IOS: generalmente el IOS se almacena en la memoria flash, pero también puede almacenarse en un servidor TFTP, el cual se usa como servidor de respaldo para el IOS o como punto central de almacenamiento y fuente de carga. Si no se localiza una imagen completa del IOS, se copia una versión más básica desde la ROM con el fin de ayudar a diagnosticar problemas o para cargar una versión completa del IOS. (Algunos routers antiguos ejecutan el IOS desde la memoria flash).
4. Ubicación y carga del archivo de configuración: luego de la carga del IOS, el bootstrap busca el archivo de configuración de inicio en la NVRAM. El archivo de configuración contiene los parámetros y comandos de configuración que definen el funcionamiento particular del router. Si el archivo de configuración de inicio se encuentra en la NVRAM, se copia a la RAM como archivo de configuración en ejecución. Si el archivo de configuración de inicio no existe en la NVRAM, el router puede buscar un servidor TFTP.

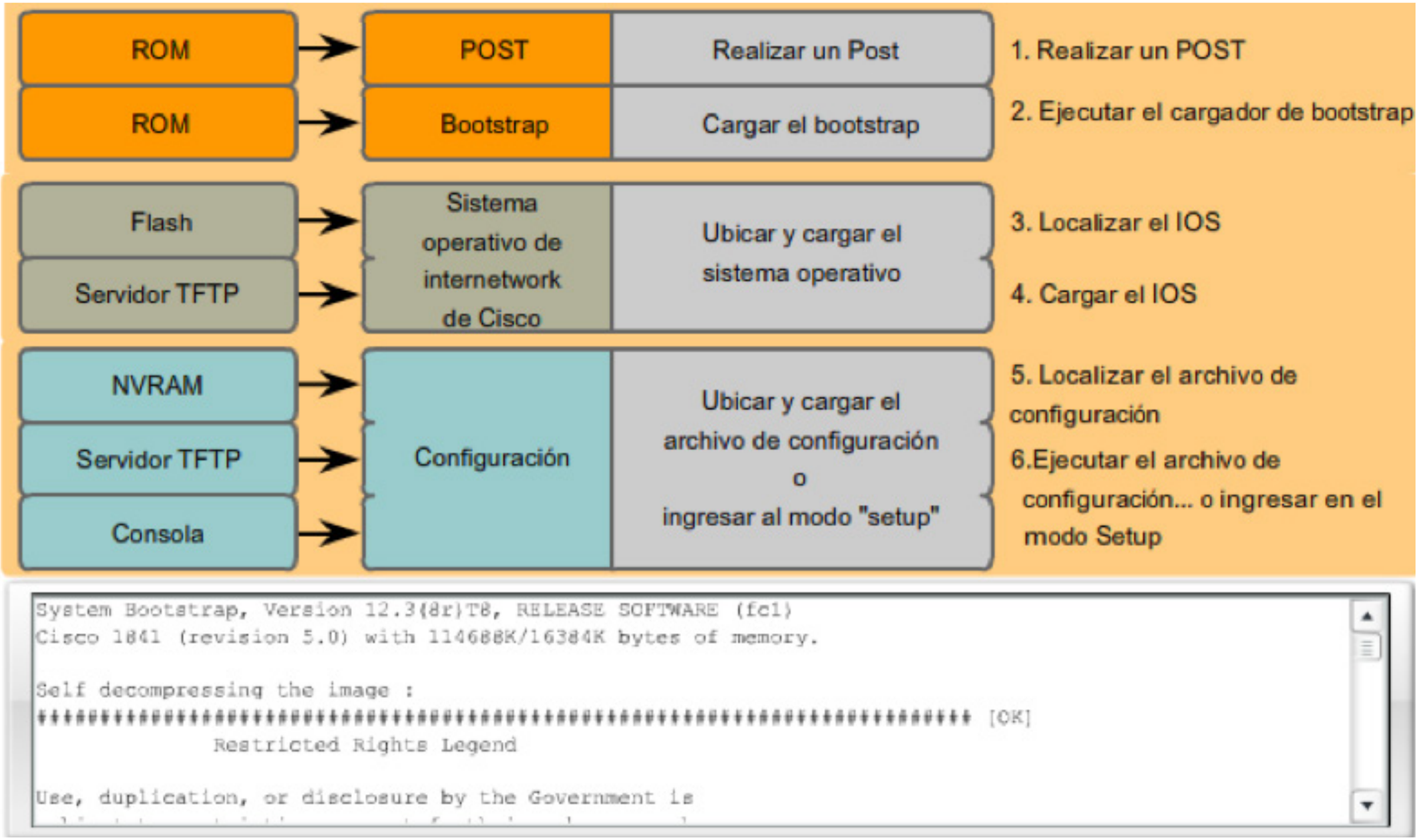


Imagen 5
Fuente: Propia, adaptada de currículo CCNA Exploration

Ingreso al modo Setup (opcional): si no se puede localizar el archivo de configuración de inicio, el router indica al usuario que ingrese en el modo Setup, el cual consiste en una serie de preguntas que piden información de configuración básica, normalmente no se usa para configuraciones complejas.

Al arrancar un router sin archivo de configuración de inicio, el IOS pregunta si se desea ingresar al diálogo de configuración inicial. Dado que en este curso la configuración se hará a través de la escritura de comandos, se debe contestar negativamente. Si ya hay archivo de configuración de inicio, se mostrará la petición de entrada de la interfaz de línea de comandos, a partir de la cual se puede ingresar comandos que modifiquen la configuración del router.

Métodos de acceso

Métodos de acceso a un router con fines de configuración: entre las formas de acceso a un router se tiene:

Acceso por consola: el puerto de consola es un puerto de administración que no requiere conectividad de red, es empleado cuando el equipo se inicia por primera vez, o se han presentado fallas en los servicios de red o se debe realizar procedimientos de recuperación de contraseñas. A través de este se puede acceder a la CLI del IOS mediante una conexión entre el puerto de consola del router y una conexión serial de PC que ejecute un software de emulación de terminal, el software de emulación de terminal se usa como interfaz de configuración.

Se deben configurar los equipos de tal forma que se disponga de contraseñas que eviten el acceso no autorizado por consola, también es deseable limitar el acceso físico al equipo.

Acceso por Telnet y SSH: es un método de acceso remoto que es posible usarlo si hay funcionalidades de red. Los equipos con software Cisco IOS cuentan con procesos de servidor y cliente Telnet. Cualquier equipo con cliente Telnet podría ejecutar una sesión Telnet o vty que se ejecute en el dispositivo Cisco. Para ayudar a evitar accesos no autorizados, el IOS exige que a toda sesión Telnet se le configure contraseña. Un protocolo denominado SSH (Secure Shell), ofrece mayor seguridad en contextos de acceso remoto, al usar procedimientos de autenticación de mayor poder además de usar procedimientos de encriptación. Las nuevas versiones del IOS contienen un servidor SSH. En algunos dispositivos, este servicio se activa en forma predeterminada.

Acceso a través del puerto auxiliar: requiere el uso de una conexión telefónica y un módem con conexión al puerto auxiliar de un router; no se necesita funcionalidades de red habilitadas en el router, también puede usarse el puerto auxiliar como puerto local de consola, con una conexión directa a una computadora que ejecute un programa de emulación de terminal. Generalmente, el único caso en que se usa el puerto auxiliar en forma local en lugar del de consola es cuando hay problemas con este último.

Se sabe ya que el archivo de configuración define el funcionamiento del router, todo router contiene dos archivos de configuración, el archivo de configuración en ejecución y el archivo de configuración de inicio, descritos brevemente a continuación: el que se encuentra en ejecución (running-configuration), es usado por el router mientras está funcionando. Es frecuente guardar un archivo de respaldo en un servidor remoto.

Archivo de configuración de inicio (startup-config): usado como configuración de respaldo o de inicio del sistema, permanece almacenado en la memoria RAM No Volátil, o NVRAM, y se carga una copia a la memoria RAM al inicio del router, la copia en RAM pasa a ser el archivo de configuración en ejecución.

Archivo de configuración en ejecución (running-configuration): es la configuración que usa el equipo mientras está funcionando, se carga en la RAM a partir de una copia de la configuración de inicio guardado en la NVRAM. El archivo running-configuration se modifica a medida que se introducen comandos, afectando la operación del equipo inmediatamente. Luego de realizar los cambios que sean necesarios, se puede guardar el running-configuration en la memoria NVRAM, actualizando el archivo startup-config.

Modos de operación del IOS

Los modos de operación hacen referencia a diferentes ámbitos o dominios de operación. La Interfaz de Línea de comandos (CLI) contempla una estructura jerárquica para los modos de operación. Los modos de operación son: Modo Usuario, Modo Exec privilegiado, Modo de configuración global y modos de configuración específicos. Desde cada modo se introduce un conjunto definido de comandos para tareas específicas. La jerarquía es tal que desde el modo usuario se puede ingresar al Exec privilegiado, desde este último, al modo de configuración global y desde el modo global se accede a otros modos de configuración específicos. Cada modo se distingue por una petición de entrada o indicadores del sistema, la cual empieza con el nombre del equipo, por ejemplo: Router (config) # es el indicador del modo de configuración global.

El modo EXEC del usuario: permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo de visualización solamente. El modo usuario no permite la ejecución de ningún comando que cambie la configuración del router, la petición de entrada o indicador corresponde al nombre del router seguido del signo >, por ejemplo Router>. Es aconsejable definir una contraseña para acceso a este modo.

Modo EXEC privilegiado: se emplea para la introducción de comandos que afectan el funcionamiento del dispositivo, es aconsejable definir una contraseña para acceso al modo privilegiado. La petición de entrada corresponde al nombre del router seguido del símbolo #, ejemplo, Router#. Se ingresa al modo privilegiado, desde el modo usuario, mediante el uso del comando enable, ejemplo,

Router>enable.

Luego de confirmar, con la tecla enter, la petición de entrada de comandos cambia a:

Router# (el router está ahora en modo privilegiado).

Si se ha configurado contraseña para acceso al modo privilegiado, luego de la confirmación del comando enable se pide la contraseña.

Router>enable

Contraseña:

Router#

Se puede regresar al modo usuario mediante el comando disable, por ejemplo, Router#disable.

Estructura básica de comandos

Los comandos obedecen una sintaxis que incluye palabras clave y los argumentos correspondientes, que indican donde y como ejecutar el comando según se requiera. Terminada la escritura completa del comando y sus palabras clave se debe confirmar con la tecla enter.

Por ejemplo, en:

Switch#show running-config

La palabra clave running-config especifica que se muestre la configuración actual o en ejecución.

Ayuda de la CLI

Se puede hacer uso de las diferentes formas de ayuda disponibles en el IOS, estas son: Ayuda contextual, verificación de la sintaxis, teclas de acceso rápido, métodos abreviados

Ayuda contextual: indica una lista de comandos y sus argumentos asociados dentro del contexto del modo actual. Para tener acceso a la ayuda contextual se puede introducir un signo de interrogación (?) ante cualquier petición de entrada, se obtiene ayuda sin necesidad de usar la tecla <Intro>. Es útil si se quiere saber la lista de comandos disponibles en un modo determinado o cuando se tiene dudas sobre la escritura de un comando.

Ejemplo de una secuencia de comandos usando la ayuda contextual de CLI

```
Cisco#cl?
clear  clock
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
Cisco#clock set 19:50:00
% Incomplete command.
```

Explicaciones de comandos

Mensajes de comandos incompletos

Mensajes de entradas no válidas

Formatos variables

```
Cisco#clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
Cisco#clock set 19:50:00 25 6
                            ^
Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 25 June
% Incomplete command.
Cisco#clock set 19:50:00 25 June ?
  <1993-2035>  Year
Cisco#clock set 19:50:00 25 June 2007
Cisco#
```

Imagen 6
Fuente: Propia, adaptada de currículo CCNA Exploration

Otra utilidad es ver una lista de comandos o palabras clave que empiezan con uno o varios caracteres específicos. Luego de escribir uno o más caracteres e inmediatamente se escribe un signo de interrogación, sin espacio, se muestra la lista de comandos o palabras clave para este contexto que comienzan con los caracteres ingresados.

Si se ingresa un comando, y luego palabras clave y luego un espacio y finalmente?, se obtiene la lista de opciones que siguen al comando y palabras clave.

- **Verificación de la sintaxis del comando:** al confirmar la introducción de un comando, el intérprete de comandos lo verifica de izquierda a derecha, tan pronto detecta un error mostrará un comentario que lo describe. Los diferentes de mensajes de error son:

Comando ambiguo: ambiguous command.

Comando incompleto: incomplete command.

Comando incorrecto: incorrect command.

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

```
Switch#c
% Ambiguous command:'c'
```

El IOS devuelve un "^" para indicar dónde el intérprete de comandos no puede descifrar el comando:

```
Switch#clock set 19:50:00 25 6
                          ^
% Invalid input detected at '^' marker.
```

Imagen 7
Fuente: Propia, adaptada de currículo CCNA Exploration

- **Teclas de acceso rápido y métodos abreviados:** facilitan el manejo de comandos. Algunas de ellas son:

Tab: completa la parte restante del comando o palabra clave.

Ctrl-R: vuelve a mostrar una línea.

Ctrl-Z: sale del modo de configuración y vuelve al EXEC.

Flecha hacia abajo: permite al usuario desplazarse hacia adelante a través de los comandos anteriores.

Flecha hacia arriba: permite al usuario desplazarse hacia atrás a través de los comandos anteriores.

Ctrl-Shift-6: permite al usuario interrumpir un proceso IOS tal como ping o traceroute.

Ctrl-C: cancela el comando actual y sale del modo configuración.

- **Comandos o palabras clave abreviadas:** la escritura de comandos se puede abreviar a una cantidad mínima de caracteres que los identifican, por ejemplo, el comando running-config se puede abreviar mediante run, ya que running-config es el único comando que empieza con run. También se puede aplicar esto a palabras claves, por ejemplo, se puede escribir int s0 en lugar de interface serial 0.

Comandos show

Se utilizan para revisar y resolver problemas. El comando show tiene diferentes opciones o variantes. Si se escribe: show? se puede ver una lista de los comandos disponibles en un modo o contexto determinado.

Comando show versión: muestra información sobre el hardware y la versión de software en el dispositivo.

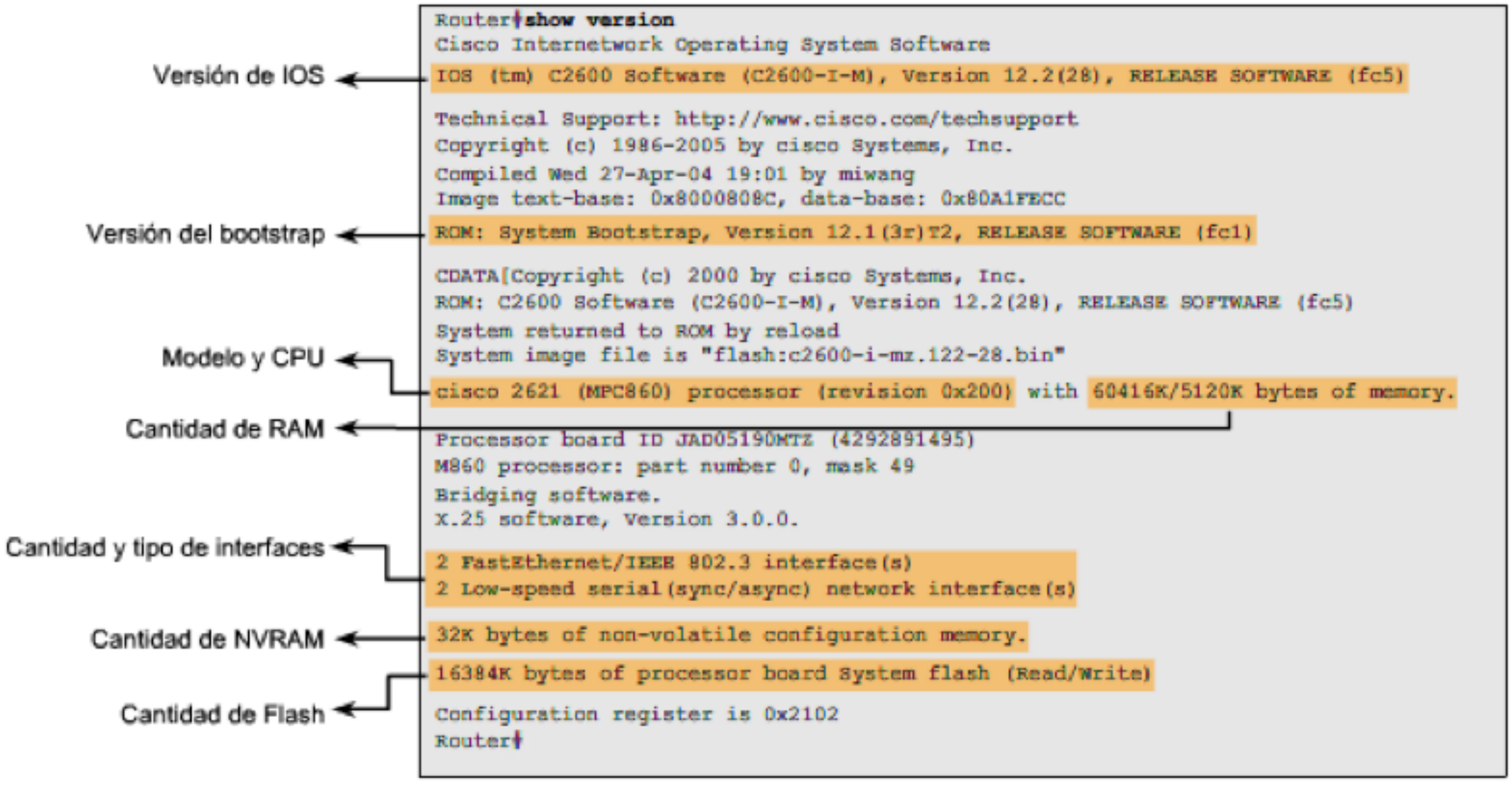


Imagen 8
Fuente: Propia, adaptada de currículo CCNA Exploration

El resultado del comando show versión incluye:

Versión de IOS: es la versión del Cisco IOS que está usando el router.

Cisco Internetwork Operating System Software

IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Programa bootstrap almacenado en la memoria ROM

ROM: System Bootstrap, Version 12.1(3r) T2, RELEASE SOFTWARE (fc1).

Ubicación del IOS: muestra ubicación del bootstrap y donde está cargado en el Cisco IOS, además del nombre de la imagen del IOS.

System image file is "flash:c2600-i-mz.122-28.bin"

CPU y cantidad de RAM: la primera parte muestra el tipo de CPU en el router. La última parte, la cantidad de DRAM.

cisco 2621 (MPC860) processor (revisión 0x200) with 60416K/5120K bytes of memory.

Algunas series de routers, como el 2600, usan una parte de la DRAM como memoria de paquete. La memoria de paquetes se usa para paquetes de almacenamiento intermedio.

Para determinar la cantidad total de DRAM en el router, se deben sumar ambos números. En este ejemplo, el router Cisco 2621 tiene 60 416 kb (kilobytes) de DRAM libre utilizada para almacenar temporalmente el Cisco IOS y otros procesos del sistema. Los otros 5 120 KB se reservan para la memoria de paquete. La suma de estos números es 65 536 k o 64 megabytes (MB) de DRAM total.

Interfaces: muestra las interfaces físicas en el router. En el ejemplo, el router Cisco 2621 tiene dos interfaces FastEthernet y dos seriales de baja velocidad.

2 FastEthernet/IEEE 802.3 interface(s).

2 Low-speed serial(sync/async) network interface(s).

Cantidad de NVRAM

32K bytes of non-volatile configuration memory.

Cantidad de memoria flash

16384K bytes of processor board System flash (Read/Write).

Registro de configuración: es la última línea del resultado de show versión muestra el valor del registro de configuración en hexadecimales. Si hay un segundo valor entre paréntesis, implica el valor del registro de configuración que se debe utilizar durante la siguiente recarga.

```
Configuration register is 0x2102
```

El registro de configuración tiene varios usos, incluida la recuperación de la contraseña. La configuración predeterminada de fábrica para el registro de configuración es 0x2102. Este valor indica que el router intentará cargar una imagen del software Cisco IOS desde la memoria flash y cargar el archivo de configuración de inicio desde la NVRAM.

Otros comandos show

Otros comandos show muy utilizados son:

- show interfaces: muestra información sobre las interfaces del dispositivo. Si se quiere información sobre una interfaz específica se usa el comando show interfaces seguido de la interfaz específica, por ejemplo:

```
Router#show interfaces serial 0/1
```

- show arp: muestra la tabla ARP del dispositivo.
- show mac-address-table: (sólo switch) muestra la tabla MAC de un switch.
- show startup-config: muestra la configuración guardada que se ubica en la NVRAM.
- show running-config: muestra el contenido del archivo de configuración actualmente en ejecución o la configuración para una interfaz específica, o información de clase de mapa.
- show ip interfaces: muestra las estadísticas IPv4 para todas las interfaces de un router. Para ver las estadísticas de una interfaz específica, ejecute el comando show ip interfaces seguido del número de puerto/ranura de la interfaz específica.
- show ip interface brief: útil para obtener un resumen de las interfaces y su estado operativo.
- show ip route: muestra la tabla de enrutamiento que está usando el IOS.
- show interfaces: muestra todos los parámetros y estadísticas de configuración de la interfaz.

La petición de entrada More: cuando un comando muestra información que ocupa más de un pantallazo, aparece al final la petición --More—indicando que hay más información, presionando la barra espaciadora se puede visualizar otro pantallazo, si se presiona enter se ve la siguiente línea, presionando cualquier otra tecla, se cancela el resultado.

Modos de configuración global

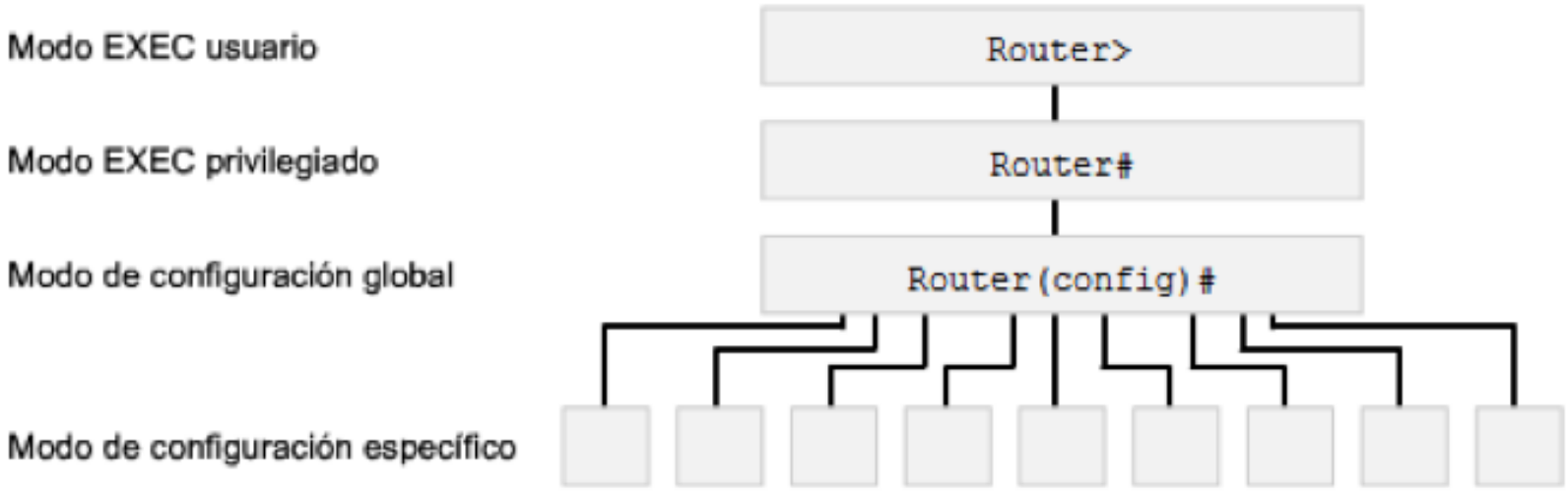
Es el modo desde el que se realizan cambios en la configuración aplicables a todo el Router, también se usa como entrada a los modos de configuración específicos. Se ingresa al modo global desde el modo privilegiado mediante el comando configure terminal (conf t). Ejemplo.

Router#configure terminal

Al confirmar el comando la petición de entrada de comandos cambia a: Router(config)#

Modos de configuración específicos

Permiten realizar tareas específicas en el dispositivo. Con el comando exit se sale de un modo de configuración específico y se vuelve al modo global, con Ctrl-Z se pasa directamente al modo privilegiado.



Modo de configuración	Indicador
Interfaz	Router(config-if)#
Línea	Router(config-line)#
Routers	Router(config-router)#

Imagen 9
Fuente: Propia, adaptada de currículo CCNA Exploration

Configuración de nombre de dispositivos

De forma predeterminada, el nombre de un router es "Router". Lo lógico es cambiar este nombre por otro apropiado. Los nombres deben comenzar con una letra, no incluir espacios, terminar con una letra o un número, se puede incluir guiones y tener máximo 63 caracteres. El nombre se configura desde el modo global mediante el uso del comando hostname seguido del nombre que se asigne al router. Al ejecutar el comando, la petición de entrada de comandos refleja el nuevo nombre. La secuencia completa de comandos para cambiar el nombre a Bogotá es:

Router>

Router>enable

Router#

Router#configure terminal

Router(config)#hostname Bogotá

BogotaRouter(config)#

Para anular los efectos de un comando, se escribe la palabra "no" antes del comando que se quiere anular, por ejemplo, para eliminar el nombre de un dispositivo se usa no hostname en modo global.

Configuración de contraseña y mensajes de seguridad

Se debe seguir adecuadas políticas de contraseñas, algunas de las contraseñas usadas y su procedimiento de configuración son:

Configuración de contraseña de consola: se configura para restringir las posibilidades de acceso no autorizado por consola, se pedirá la contraseña siempre que se intente acceso por consola, para configurarla, en un equipo llamado Bogotá, se usa la siguiente secuencia de comandos (desde el modo global):

Bogota (config)#line console 0

Bogota (config-line)#password Contraseña especifica la contraseña a asignar

Bogota (config-line)#login obliga la petición de la contraseña

Contraseña de enable y contraseña secreta de enable: restringen los intentos de acceso al modo privilegiado. Es preferible usar el comando enable secret debido a que brinda mayor seguridad al encriptar la contraseña, lo que no hace enable password, el comando enable password se usa sólo si enable secret no se ha configurado, pero hay que tener en cuenta

que en algunas versiones antiguas del IOS no está disponible enable secret. Para configurar estas contraseñas se usa los siguientes comandos:

Bogota(config)#enable password contraseña configure la contraseña enable

Bogota(config)#enable secret contraseña configure la contraseña secret

Contraseña de VTY: se usan para restringir el acceso a través de telnet. De forma predeterminada, muchos equipos Cisco admiten cinco líneas VTY con numeración del 0 al 4, a las cuales se les debe configurar contraseña. Para configurar la misma contraseña a las cinco líneas en el equipo Bogotá se usa la siguiente secuencia de comandos desde el modo global.

Bogota(config)#line vty 0 4

Bogota (config-line)#password contraseña

Bogota(config-line)#login

Nota: Si no se configura contraseña enable password ni enable secret, el IOS impide el acceso al modo privilegiado. Por defecto, el IOS incluye el comando login en las líneas VTY. Si no se ha establecido una enable password, una sesión Telnet aparecería como:

Bogota>enable

% No password set

Bogota>

Configuración de encriptación de contraseñas: para que las contraseñas aparezcan cifradas en el script del archivo de configuración, se usa el comando service password-encryption, con lo que se aplica una encriptación débil. La cancelación del servicio de encriptación no revierte la encriptación.

Configuración de mensajes de aviso: es importante disponer de un mensaje que advierta la prohibición de acceso a personas no autorizadas. Un aviso común es el mensaje del día (MOTD). Con frecuencia se usa para notificaciones legales ya que se visualiza en todos los terminales conectados. Para configurar el MOTD se usa el comando banner motd del modo global, y se usa delimitadores antes y después del texto del mensaje.

Bogota(config)#banner motd # texto del mensaje que se quiere mostrar #

Configuración de las interfaces Ethernet: las interfaces Ethernet se usan como gateway para los dispositivos finales en las LAN conectadas directamente al router. Cada interfaz Ethernet debe tener una dirección IP y una máscara de subred. La configuración de una interfaz Ethernet requiere el ingreso, desde el modo global, al modo específico de configuración de la interfaz y especificar la dirección IP y máscara de subred y habilitar.

A continuación se muestra un ejemplo:

Bogota(config)#interface FastEthernet 0/0

Bogota (config-if)#ip address 192.168.1.1 255.255.255.0

Bogota (config-if)#no shutdown

Configuración de las interfaces seriales del router: las interfaces seriales se usan para conectar WAN a routers en un sitio remoto, se configuran de forma similar a las Ethernet. Además de máscara de subred, dirección IP y habilitar la interfaz, se debe configurar la velocidad de reloj si el cable es DCE.

Bogota (config)#interface Serial 0/0/0

Bogota (config-if)#ip address 190.10.10.1 255.255.255.252

Bogota (config-if)#clock rate 56000

Bogota (config-if)#no shutdown

Configuración de descripción de interfaz: útil para dar información sobre el propósito de la interfaz, esta descripción se puede ver en los resultados de los comandos show startup-config, show running-config y show interfaces. Para configurar una descripción de interfaz se usa el comando description como se muestra en el siguiente ejemplo para una interfaz FastEthernet:

Bogota#configure terminal

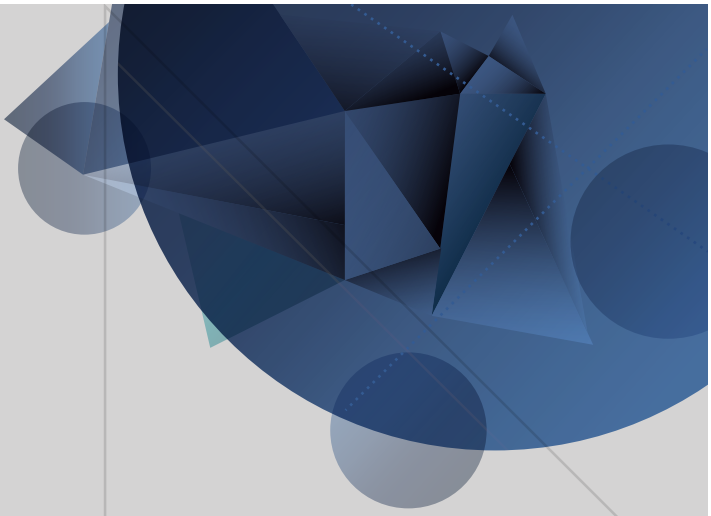
Bogota(config)#interface fa0/1

Bogota(config-if)#description Conectarse al router principal de la sede 3

4

Unidad 4

Administración de equipos de red



Telemática I

Autor: Juan Carlos Ramírez Zapata

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Esta parte trata la administración de routers centrándose en equipos marca Cisco, para lo cual se hace uso de los comandos del sistema operativo Cisco IOS. El capítulo brinda conocimientos sobre routers y prácticas relacionados con el IOS de Cisco, el archivo de configuración, modos de operación del IOS, uso de comandos del IOS, entre otros.

U4

Metodología

Los estudiantes como centro activo de aprendizaje deben hacer la lectura y análisis permanente de este material, que les permite realizar una contextualización del tema, conociendo la teoría general y su aplicación práctica en contextos específicos.

Administración de equipos de red

Prueba del stack

Uso de ping en una secuencia de prueba:

El comando ping del IOS puede usarse en secuencia para aislar problemas de red, se inicia aplicándolo a dispositivos dentro de la LAN y luego a redes remotas. Ping proporciona un método de verificación de la pila de protocolos y la configuración de IP en un host.

Prueba de loopback: se realiza con el comando ping a una dirección de loopback (127.0.0.1), con esto se verifica la operación de la pila de protocolos TCP/IP en el propio dispositivo.

Verificación de las interfaces del router

Comando show ip interface brief: brinda un resultado abreviado sobre una interfaz ip.

El up en la columna de estado muestra que esta interfaz está en funcionamiento en la Capa 1. El up en la columna de protocolo señala que el protocolo de Capa 2 está funcionando.

La indicación correspondiente a administratively down dice que la interfaz no ha sido habilitada.

Prueba de conectividad del router:

Como con un dispositivo final, es posible verificar la conectividad de la Capa 3 con los comandos ping y traceroute. En la figura del Router 1 se puede ver un ejemplo de los resultados de un ping a un host en la LAN local y un trace a un host remoto a través de la WAN.

Ping extendido

Se ingresa escribiendo ping en modo privilegiado sin una dirección IP de destino, aparece entonces una serie de peticiones de entrada, presionando la tecla Enter se aceptan los valores por defecto, pero se puede ingresar valores específicos

Router#ping

Protocol [ip]:

Target IP address:10.0.0.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:5

Extended commands [n]: n

Al ingresar un período de tiempo de espera

más prolongado que el predeterminado, se podrán detectar posibles problemas de latencia. Si la prueba de ping es exitosa con un valor superior, existe una conexión entre los hosts, pero es posible que haya un problema de latencia en la red.

Verificación de la configuración de router

Se puede revisar la configuración en ejecución con el comando siguiente:

Bogota#show running-config.

Si se está seguro de guardar esta configuración, para que esté disponible como archivo de inicio en un siguiente arranque del router, se usa el comando señalado a continuación.

R1#copy running-config startup-config.

Para verificar el archivo startup-config se usa el siguiente comando.

R1#show startup-config.

Administración de archivos de configuración

Volver a la configuración original del dispositivo: Si los cambios de configuración en ejecución no tienen el efecto deseado, puede ser necesario volver a la configuración de inicio guardada en la NVRAM si no se ha modificado. La manera de hacerlo es mediante la ejecución del comando reload desde modo privilegiado, con ello se reinicia el dispositivo a partir de la configuración de respaldo.

En el reinicio se indica que se detectó cambios no guardados y se pregunta si se quieren guardar, en este caso se descarta ingresando no. Luego aparece otra petición de confirmación de la recarga se confirma con la tecla enter, cualquier otra tecla cancelará el proceso.

Copia de respaldo en un servidor TFTP: es recomendable tener una copia de la configuración en un servidor TFTP, para ello se usa el comando copy running-config tftp o copy startup-config tftp y los siguientes pasos:

1. Ingrese el comando copy running-config tftp.
2. Ingrese la dirección IP del host en el cual se almacenará el archivo de configuración.
3. Ingrese el nombre que se asignará al archivo de configuración.
4. Presione Intro para confirmar cada elección.

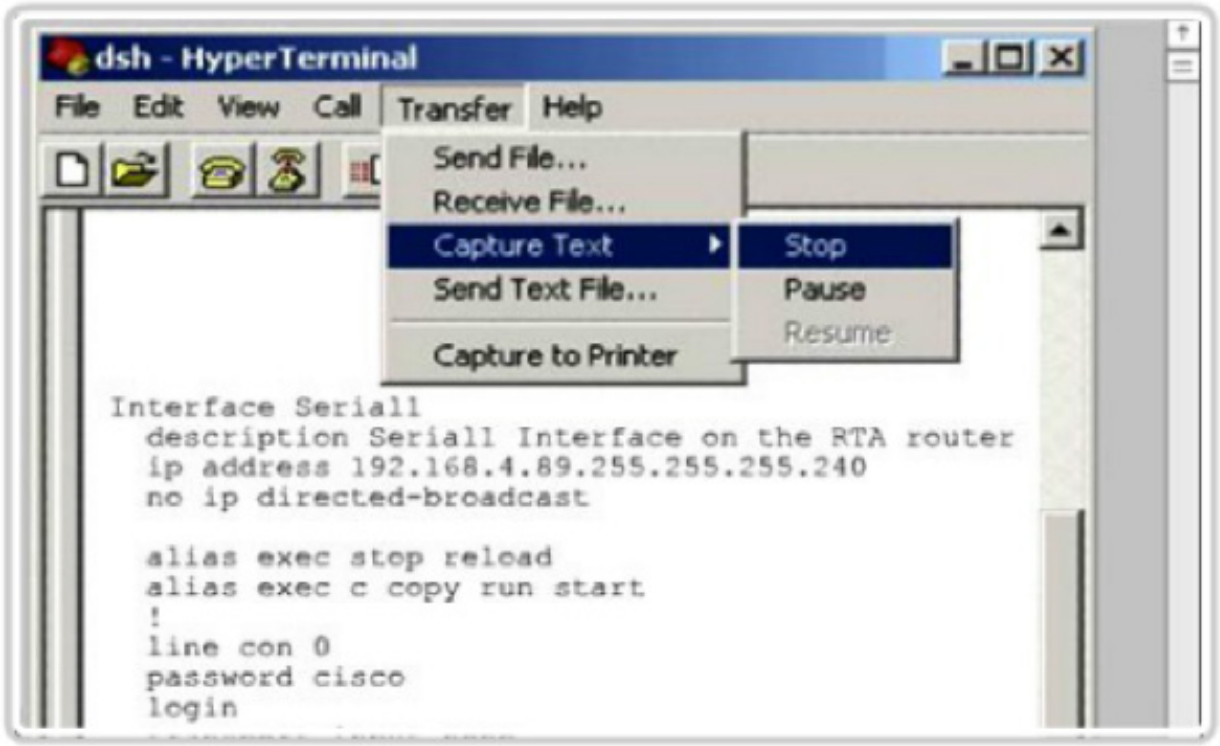
Eliminación de todas las configuraciones

Si se ha guardado cambios no deseados, es posible que se deba borrar la configuración de inicio y reiniciar el dispositivo, esto se hace mediante los comandos erase startup-config y reload, el comando de borrado solicita la confirmación, luego se debe ejecutar el comando reload.

Eliminada la configuración de inicio de la NVRAM, se debe reiniciar el dispositivo para eliminar la configuración en ejecución. El dispositivo cargará entonces la configuración de inicio predeterminada que se envió originalmente con el dispositivo en la configuración en ejecución.

Configuraciones de respaldo con captura de texto (HyperTerminal): útil para guardar configuración en documento de texto para su uso posterior, los pasos con el uso de HyperTerminal son los siguientes:

1. Hacer clic en la opción Capture Text del menú Transfer.
2. Elegir la ubicación.
3. Iniciar la captura con Start.
4. Iniciada la captura, se debe ejecutar el comando show running-config o show startup-config desde la línea de entrada del modo privilegiado. El texto de la ventana se copiará en el archivo de texto.
5. Cuando se ha visualizado toda la configuración se detiene la captura con Stop.
6. Verificar el resultado.



En la sesión de terminal:

1. Inicie el proceso de captura de texto
2. Emita un comando **`show running-config`**
3. Detenga el proceso de captura
4. Guarde el archivo de texto

Imagen 1
Fuente: Propia, adaptada de currículo CCNA Exploration

Restauración de las configuraciones de texto: los archivos de texto deben editarse para eliminar texto que no hagan parte de la configuración, también el dispositivo debe estar en el modo global para recibir los comandos del archivo de texto, desde HyperTerminal, los pasos son:

1. Ubicar y abrir el archivo de texto con la configuración.
2. Copiar el texto completo.
3. En el menú Edit, haga clic en paste to host.

El texto en el archivo estará aplicado como comandos en la CLI y pasará a ser la configuración en ejecución en el dispositivo. Éste es un método conveniente para configurar manualmente un router.

La tabla de enrutamiento

La tabla de enrutamiento se carga en la RAM y se usa para almacenar la información de rutas sobre redes remotas o conectadas directamente, contiene asociaciones entre la red y el siguiente salto para indicar al router como alcanzar un destino en particular. La asociación del siguiente salto también puede ser la interfaz de salida hacia el destino final.

Una red conectada directamente está conectada a una de las interfaces del router. Cuando se configura una interfaz de router, la interfaz pasa a ser un host en esa red conectada. La dirección de red y la máscara de subred de la interfaz, junto con el número y el tipo de interfaz, se ingresan en la tabla de enrutamiento como una red conectada directamente. Una red remota es aquella a la que sólo se puede llegar pasando por otros routers. El contenido de la tabla de enrutamiento se puede ver usando el comando show ip route:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

Imagen 2
Fuente: Propia, adaptada de currículo CCNA Exploration

La figura muestra un ejemplo de tabla de enrutamiento, se ve un conjunto de convenciones al inicio, por ejemplo una C significa que la información es sobre una red directamente conectada. También se observa direcciones IP, las cuales corresponden a redes destino, las interfaces a través de las cuales se puede llegar a ellas.

Incorporación de una red conectada a la tabla de enrutamiento

Luego de configurar y activar la interfaz del router, ésta debe recibir una señal portadora desde otro dispositivo, por ejemplo un switch conectado a la interfaz, al que a su vez se conectan computadores, para que el estado de la interfaz se considere "activo". Cuando la interfaz está "activa", la red conectada a la interfaz se incorpora a la tabla de enrutamiento como red directamente conectada.

Incorporación de redes remotas a la tabla de enrutamiento

Puede hacerse de forma manual o automática. La configuración manual recibe el nombre de enrutamiento estático, mientras que la forma automática se llama enrutamiento dinámico, este último se realiza mediante la configuración de un protocolo de enrutamiento. A cada red remota está asociada una interfaz de salida para alcanzarla, la ruta se agrega a la tabla de enrutamiento si la respectiva interfaz esté habilitada.

Una ruta estática incluye la dirección de red y la máscara de subred de la red remota, junto con la dirección IP del router del siguiente salto o la interfaz de salida. Las rutas estáticas se indican con el código S en la tabla de enrutamiento.

Las rutas estáticas se usan en casos como los siguientes:

Cuando una red se compone de pocos routers: con el fin de evitar la carga administrativa de los protocolos de enrutamiento.

Para conectar una red al ISP

No se necesita configuración automática por ser siempre el único punto de salida hacia Internet.

Una red grande con topología hub-and-spoke: Una topología hub-and-spoke comprende una ubicación central (el hub) y múltiples ubicaciones de sucursales (spokes), donde cada spoke tiene solamente una conexión al hub. El uso del enrutamiento dinámico sería innecesario porque cada sucursal tiene un único camino hacia un destino determinado, a través de la ubicación central.

En la mayoría de routers se configuran con rutas estáticas y rutas dinámicas, pero primero se debe configurar las rutas a redes conectadas directamente, ya que se usan para acceder a redes remotas.

Enrutamiento dinámico

Generalmente los routers usan protocolos de enrutamiento dinámico para compartir información que posibilita la conexión a redes remotas. La ejecución de enrutamiento dinámico en los routers consiste en tareas como descubrimiento de red y actualización y mantenimiento de las tablas de enrutamiento.

Descubrimiento automático de las redes

Es la capacidad de compartir información sobre redes conocidas con otros routers, permitiendo a los routers obtener información automáticamente sobre tales redes.

Mantenimiento de las tablas de enrutamiento

Luego del descubrimiento inicial de redes, los protocolos de enrutamiento dinámico actualizan y mantienen la tabla de enrutamiento del router. Además de determinar la mejor ruta, los protocolos de enrutamiento dinámico, también determinan la mejor nueva ruta si la inicial falla o si cambia la topología.

Protocolos de enrutamiento IP

Para el caso de enrutamiento dinámico IP hay varios protocolos. Entre ellos están: RIP (RIP, Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), IS-IS (Intermediate-System-to-Intermediate-System), BGP (Border Gateway Protocol).

Principios de tablas de enrutamiento

1. Cada router toma decisiones en forma independiente, según la información de su tabla de enrutamiento.
2. La información de enrutamiento de un router, respecto a una red destino, no necesariamente coincide con las de los otros.
3. La información de enrutamiento acerca de una ruta de una red a otra no da información respecto a la ruta de retorno.

Enrutamiento asimétrico

Hace referencia a que los paquetes pueden recorrer la red en un sentido, utilizando un camino, y que la comunicación en sentido inverso sea por otra ruta.

Campos de trama y paquete

La mejor ruta

Decidir cuál es la mejor ruta implica la evaluación de múltiples rutas hacia la misma red de destino y la selección de la mejor de ellas, la mejor ruta se elige según el valor o de la variable usada para tomar la decisión, esta variable recibe el nombre de métrica. Ejemplos de métricas usadas por algunos protocolos son: el número de saltos o cantidad de routers que se debe cruzar para llegar al destino, el ancho de banda de los enlaces, la confiabilidad, el retardo.

Balanceo de carga

Si una tabla de enrutamiento tiene dos o más rutas con la misma métrica a un destino, el router puede realizar un balanceo de carga de igual costo. La tabla de enrutamiento mostrará múltiples interfaces de salida. El router enviará paquetes usando múltiples interfaces de salida. Si está bien configurado, el balanceo de carga puede aumentar el rendimiento de la red. Un router también se puede configurar un router para enviar paquetes a través de rutas de métricas de diferente costo.

Determinación de ruta

Un router revisa su tabla de enrutamiento para determinar el destino de paquete. Si el destino es una red directamente conectada, el paquete se encapsula para ser enviado directamente al destino. Si el destino es una red remota, el paquete se encapsula para ser reenviado a otro router. Si la dirección de red de destino del paquete no figura en la tabla de enrutamiento, y si el router no tiene una ruta predeterminada, el paquete se descarta y el router envía al origen un mensaje ICMP de destino inalcanzable.

Función de conmutación

Es el proceso usado por el router para recibir un paquete por una interfaz y reenviarlo por otra. En la función de conmutación

se encapsula paquetes según el tipo de trama de enlace de datos de la interfaz de salida.

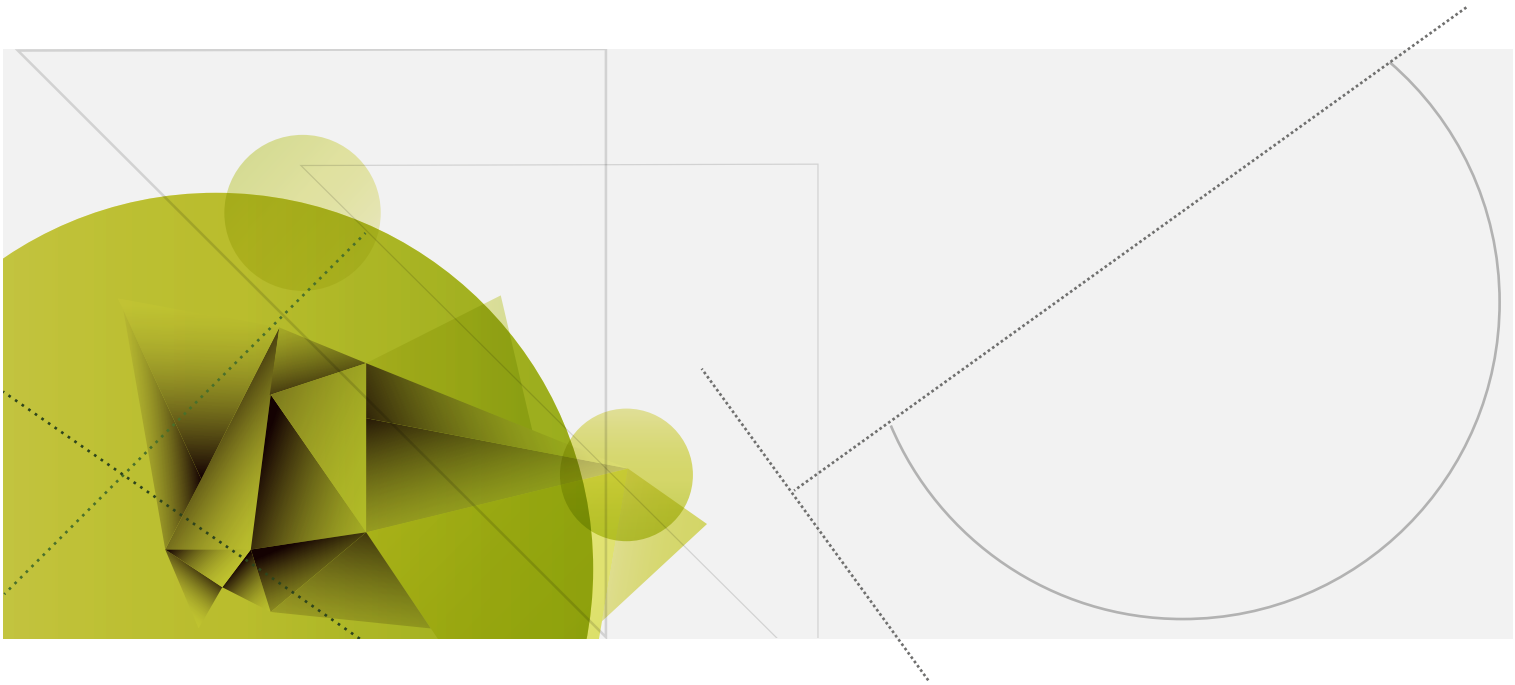
Es de resaltar que si un router recibe un paquete destinado a otra red, desentrama el paquete eliminando el encabezado y el tráiler de la trama de Capa 2; examina la dirección IP de destino para determinar la interfaz de salida; entrama nuevamente el paquete según el tipo de interfaz de salida.

En el reenvío de paquete de un router al siguiente, el entramado del paquete es tal que las direcciones origen y destino a nivel de capa de enlace de datos son las de la interfaz de salida y la de entrada al siguiente salto respectivamente. El paquete en sí no cambia, salvo el campo Tiempo de vida (TTL), el cual disminuye en uno, si el valor TTL resultante es cero, el router descarta el paquete para para evitar que los paquetes IP viajen indefinidamente a través de las redes.

Bibliografia

- Barbancho, J., Benjumea, J., Rivera, O., Ropero, J., Sánchez, G., & Sivianes, F. (2014). Redes locales. Madrid: Ediciones Paraninfo, SA.
- Graziani, R., & Allan, J. (2008). Routing protocols and concepts, CCNA Exploration Companion Guide. Indianapolis: Cisco Press.
- Huidobro, J., Blanco, A., & J. Jordan, C. (2008). Redes de área local: administración de sistemas informáticos. Madrid: Ediciones Paraninfo, SA.
- Wayne Lewis, P. (2008). LAN Switching and Wireless CCNA Exploration Guide. Indianapolis: Cisco Press.

Esta obra se terminó de editar en el mes de noviembre
Tipografá Myriad Pro 12 puntos
Bogotá D.C,-Colombia.



AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO