TEMA 5 Nivel de Red

1. Capa de Red

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

Direccionamiento
Encapsulamiento
Enrutamiento
Desencapsulamiento.

1.1 Direccionamiento

La Capa de red debe proveer un mecanismo para **direccionar** los paquetes a los dispositivos finales. Estos dispositivos deben tener una dirección única cada uno. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se le denomina host.

1.2 Encapsulamiento

La capa de Red debe proveer **encapsulación**. Las PDU (unidad de datos de protocolo) de la capa de Red, deben, contener estas direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3.

Cuando nos referimos a la capa de Red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino.

El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la llama dirección de origen.

1.3 Enrutamiento

Los hosts de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final.
Los dispositivos intermediarios que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. **A este proceso se lo conoce como enrutamiento.** Durante el enrutamiento a través de una internetwork, el paquete puede recorrer muchos dispositivos intermediarios. A cada ruta que toma un paquete para llegar al próximo dispositivo se la llama salto. A medida que el paquete es enviado, su contenido (la PDU de la Capa de transporte) permanece intacto hasta que llega al host destino.

1.4 Desencapsulamiento

Finalmente, el paquete llega al host destino y es procesado en la Capa 3. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

2. Protocolos a nivel de Red

Un protocolo a nivel de red puede compararse con el sistema postal: Se utiliza un **direccionamiento** que permite al cartero conocer la localización exacta del destinatario y, con ello, la ruta a seguir para alcanzarlo.

De forma similar al sistema postal, trabaja el protocolo más importante del nivel de red, el **protocolo IP (Internet Protocol) definido en RFC 791** que establece el direccionamiento y define el formato de los paquetes que se transmiten.

3. El protocolo IP

Las características básicas de IPv4 son:
Sin conexión: No establece conexión antes de enviar los paquetes de datos.
Máximo esfuerzo (no confiable): No se usan encabezados para garantizar la entrega de paquetes.
Medios independientes: Operan independientemente del medio que lleva los datos.

IP trabaja sin conexión y no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que los paquetes sean enviados, ni requiere campos adicionales en el encabezado de la PDU para mantener esta conexión. Este proceso reduce en gran medida la sobrecarga del IP.

El protocolo IP no sobrecarga el servicio IP suministrando confiabilidad. Comparado con un protocolo confiable, el encabezado del IP es más pequeño. Transportar estos encabezados más pequeños genera una menor sobrecarga: significa menos demora en la entrega. Al IP a menudo se lo considera un protocolo no confiable. **No confiable significa simplemente que IP no tiene la capacidad de administrar ni recuperar paquetes no entregados o corruptos.**

Cualquier paquete IP individual puede ser comunicado eléctricamente por cable, como señales ópticas por fibra, o sin cables como las señales de radio. **Es responsabilidad de la capa de Enlace de datos de OSI tomar un paquete IP y prepararlo para transmitirlo por el medio de comunicación.**

3.1 Dirección IP

Cada dispositivo de una red debe ser definido en forma exclusiva. En la capa de red es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales.
Con IPv4, esto significa que cada paquete posee una dirección de origen de 32 bits y una dirección de destino de 32 bits (4 octetos) en el encabezado de Capa 3. Para hacer llegar los paquetes a su destino, el protocolo IP utiliza las direcciones IP.

Estas direcciones se pueden especificar en binario, aunque resulta más cómodo utilizar la notación decimal con puntos. Para pasar una dirección de binario a decimal, sólo hay que convertir los números tomando de ocho en ocho dígitos. Posteriormente se separa cada número en decimal con puntos para construir la dirección completa.

3.2 Partes de una dirección IP

En cada dirección IPv4, alguna porción de los bits de orden superior representa la dirección de red. En la Capa 3, se define una red como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red de sus direcciones. Además, existe una cantidad variable de bits que conforman la porción de host de la dirección. El número de bits usado en esta porción del host determina el número de hosts que podemos tener dentro de la red.

Por lo tanto, **una dirección IP tiene dos partes: un identificador de red y un identificador de host.** El identificador de red se utiliza para numerar cada una de las redes que componen Internet de forma única. El identificador de estación se usa para numerar cada uno de los equipos que forman parte de una red.

Con 8 bits se puede lograr un total de 256 patrones de bits diferentes. Esto significa que los bits para los tres octetos superiores representarían la porción de red. En función de cómo se divida el número de 32 bits en dos partes se da lugar a tres clases.

3.3 Clases de redes

Redes de Clase A: usan 8 bits para el identificador de red y 24 para el identificador de host, lo que no permite tener 28 (256)redes diferentes y 224 (16 millones) equipos por red. Se utiliza para redes extremadamente grandes.
Redes de Clase B: usan 16 bits para el identificador de red y 16 bits para el identificador de host, lo que nos permite 65536 redes distintas y 65536 equipos por red. Se usan para redes de tamañomoderado a grande.

Redes de Clase C: usan 24 bits para el identificador de red y 8 bits para el identificador de host, lo que nos permite tener un máximo de 16 millones de redes distintas y 256 equipos por red. Se usan para redes pequeñas.

Cada clase se caracteriza por un campo clase. Este campo se sitúa al principio de la dirección. Clase IP Valor del campo
A 0
B 10
C 110

Además de las clases A, B y C, en IPv4 se definieron las clases D (campo clase 1110) y E (campo clase 11110).

La clase D no se usa para asignar direcciones a equipos sino para crear grupos de equipos de multidifusión o broadcast (permite enviar el mismo mensaje a un grupo de equipos a la vez).

La clase E se reservó para investigación y desarrollo y no se usa.

3.3.1 Rangos de direcciones para las clases de IP

Clase IP Rango

A 1.0.0.0-127.255.255.255
B 128.0.0.0-191.255.255.255
C 192.0.0.0-223.255.255.255
D 224.0.0.0-239.255.255.255
E 240.0.0.0-247.255.255.255

3.4 Tipos de direcciones en una red IPv4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:
Dirección de red: la dirección en la que se hace referencia a la red.
Dirección de broadcast: una dirección especial utilizada para enviar datos a todos los hosts de la red.
Direcciones host: las direcciones asignadas a los dispositivos finales de la red.

3.4.1 Direcciones de red

La dirección de red es una manera estándar de hacer referencia a una red. Dentro del rango de dirección IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección.

3.4.2 Direcciones de broadcast

La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red. La dirección de broadcast utiliza la dirección más alta en el rango de la red.

3.4.3 Direcciones de host

Cada dispositivo final requiere una dirección única para enviar un paquete a dicho host. En las direcciones IPv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en dicha red.

3.5 Prefijos de red

Hoy en día, las clases han dejado de ser utilizadas y ya es posible tener una ip de clase A con 24 bits para la red. Al expresar una dirección de red IPv4, se agrega una longitud de prefijo a la dirección de red. La longitud de **prefijo es la cantidad de bits en la dirección que conforma la porción de red.**

El prefijo asignado puede variar de acuerdo con la cantidad de hosts de la red. Tener un número de prefijo diferente cambia el rango de host y la dirección de broadcast para cada red.

3.6 Máscara de red

Otra entidad que se utiliza para especificar la porción de red de una dirección IPv4 en los dispositivos de red es la máscara de subred. La máscara de subred consta de 32 bits, al igual que la dirección, y utiliza unos para indicar qué bits de la dirección son bits de red y ceros para indicar qué bits son bits de host.

La máscara de subred sirve a los routers para averiguar si los dos host que quieren comunicarse están o no en la misma red. Cada Clase tiene una máscara de red por defecto, la Clase A 255.0.0.0, la Clase B 255.255.0.0 y la Clase C 255.255.255.0.
3.6 Máscara de red Supongamos la red 10.0.0.0 con máscara 255.255.255.0 ó prefijo /24 (es lo mismo).

3.7 Cálculo de direcciones host, red y broadcast

Supongamos la red 172.16.20.0 /25. Con un prefijo de 25 bits, los últimos 7 bits son bits de host. Para representar la dirección de red, todos estos bits de host son “0". De esta forma, la dirección de red es 172.16.20.0 /25.

Calculamos ahora la dirección de broadcast de la red. Por lo tanto, los siete bits de host utilizados en esta red son todos "1". A partir del cálculo, se obtiene 127 en el último octeto. Esto produce una dirección de broadcast de 172.16.20.127.

Calculamos ahora la dirección host más baja. Ésta es siempre un número mayor que la dirección de red. En este caso, el último de los siete bits de host se convierte en "1". Con el bit más bajo en la dirección host establecido en 1, la dirección host más baja es 172.16.20.1.

Calculamos ahora la dirección host más alta. La dirección host más alta de una red es siempre un númeromenor que la dirección de broadcast. Esto significa que el bitmás bajo del host es un '0' y todos los otros bits '1'. Como se observa, esto hace que la dirección host más alta de la red sea 172.16.20.126.

4. Lógica AND

Cuando se crea o envía un paquete IPv4, la dirección de red de destino debe obtenerse de la dirección de destino. Esto se hace pormedio de una lógica llamada AND. Se aplica la lógica AND a la dirección host IPv4 y a su máscara de subred para determinar la dirección de red a la cual se asocia el host. Cuando se aplica esta lógica AND a la dirección y a la máscara de subred, el resultado que se produce es la dirección de red. AND es una de las tres operaciones binarias básicas utilizadas en la lógica digital. La lógica AND es la comparación de dos bits que produce los siguientes resultados:
1 AND 1 = 1
1 AND 0 = 0
0 AND 1 = 0
0 AND 0 = 0

Los routers usan AND para determinar una ruta aceptable para un paquete entrante. El router verifica la dirección de destino e intenta asociarla con un salto siguiente. Cuando

llega un paquete a un router, éste realiza el procedimiento de aplicación de AND en la dirección IP de destino en el paquete entrante y con la máscara de subred de las rutas posibles. De esta forma, se obtiene una dirección de red que se compara con la ruta de la tabla de enrutamiento de la cual se usó la máscara de subred.

5. Unicast, broadcast y multicast

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:
Unicast: el proceso por el cual se envía un paquete de un host a un host individual.
Broadcast: el proceso por el cual se envía un paquete de un host a todos los hosts de la red.
Multicast: el proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts.

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como dirección de origen.

5.1 Tráfico Unicast

La comunicación unicast **se usa para una comunicación normal de host a host,** tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino.
Sin embargo, los paquetes broadcast y multicast usan direcciones especiales como dirección de destino.

5.2 Tráfico Broadcast

Dado que el tráfico de broadcast se usa para enviar paquetes a todos los hosts de la red, un paquete usa una dirección de broadcast especial. Cuando un host recibe un paquete con la dirección de broadcast como destino, éste procesa el paquete como lo haría con un paquete con dirección unicast. La transmisión de broadcast se usa para ubicar servicios/ dispositivos especiales para los cuales no se conoce la dirección o cuando un host debe brindar información a todos los hosts de la red.
Cuando un host necesita información envía una solicitud, llamada consulta, a la dirección de broadcast. Todos los hosts de la red reciben y procesan esta consulta. Uno o más hosts que poseen la información solicitada responderán, típicamente mediante unicast. De forma similar, cuando un host necesita enviar información a los hosts de una red, éste crea y envía un paquete de broadcast con la información.

A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente están restringidos a la red local. Esta restricción depende de la configuración del router y del tipo de broadcast. Existen dos tipos de broadcasts:

Broadcast dirigido: Se envía un broadcast dirigido a todos los hosts en una red específica. Este tipo de broadcast es útil para enviar un broadcast a todos los hosts de una red local. Por ejemplo: para que un host fuera de la red se comunique con los hosts dentro de la red 172.16.4.0 /24, la dirección de destino del paquete sería 172.16.4.255.

Broadcast limitado: El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes usan una dirección IPv4 de destino **255.255.255.255**. Los routers no envían estos broadcasts.

Los paquetes dirigidos a la dirección de broadcast limitada sólo aparecerán en la red local. A modo de ejemplo, un host dentro de la red 172.16.4.0 /24 transmitiría a todos los hosts en su red utilizando un paquete con una dirección de destino 255.255.255.255.

5.3 Tráfico Multicast

Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino. Los hosts que desean recibir datos multicast específicos se denominan clientes multicast. Los clientes se suscriben a un grupo multicast. Cada grupo multicast está representado por una sola dirección IPv4 de destino multicast.

Cuando un host IPv4 se suscribe a un grupo multicast, el host procesa paquetes dirigidos a esta dirección multicast y paquetes dirigidos a su dirección unicast exclusivamente asignada. **IPv4 ha apartado un bloque especial de direcciones desde 224.0.0.0 a 239.255.255.255 para direccionamiento de grupos multicast.**

6. Direcciones IPv4 reservadas

El rango de direcciones IPv4 es de 0.0.0.0 a 255.255.255.255. No todas estas direcciones pueden usarse como direcciones host para la comunicación unicast.

Se distinguen:

Direcciones experimentales: Un importante bloque de direcciones reservado con objetivos específicos es el rango de direcciones IPv4 experimentales de 240.0.0.0 a 255.255.255.254. Actualmente, estas direcciones se mencionan como reservadas para uso futuro (RFC 3330). Esto sugiere que podrían convertirse en direcciones utilizables. En la actualidad, no es posible utilizarlas en redes IPv4. Sin embargo, estas direcciones podrían utilizarse con fines de investigación o experimentación.

Direcciones multicast: otro bloque importante de direcciones reservado con objetivos específicos es el rango de direcciones IPv4 multicast de 224.0.0.0 a 239.255.255.255.

Direcciones host: si quitamos los rangos reservados para las direcciones experimentales y las direcciones multicast, queda el rango de direcciones de 0.0.0.0 a 223.255.255.255 que podría usarse con hosts IPv4. Sin embargo, dentro de este rango existen muchas direcciones que ya están reservadas con objetivos específicos.

7. Direcciones públicas y privadas

Aunque la mayoría de las direcciones IPv4 de host son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que

se utilizan en redes que requieren o no acceso limitado a Internet. A estas direcciones se las denomina direcciones privadas.

Los bloques de direcciones privadas son:

10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)
172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

Los bloques de direcciones de espacio privadas se separan para utilizar en redes privadas. Muchos hosts en diferentes redes pueden utilizar las mismas direcciones de espacio privado. Los paquetes que utilizan estas direcciones como la dirección de origen o de destino no deberían aparecer en la Internet pública. El router de estas redes privadas deben bloquear o convertir estas direcciones.

7.1 NAT (Traducción de direcciones de red)

Con servicios para traducir las direcciones privadas a direcciones públicas, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Estos servicios, llamados Traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada. NAT permite a los hosts de la red "pedir prestada" una dirección pública para comunicarse con redes externas.

7.2 Actividad

Actividad 6.2.5: Indica si las siguientes direcciones IP son públicas o privadas.

7.3 Direcciones IPv4 especiales

La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aun dentro de estos bloques de direcciones, existen muchas direcciones designadas para otros fines específicos, como por ejemplo:

Direcciones de red y broadcast: no es posible asignar la primera ni la última dirección a hosts dentro de cada red.

Ruta predeterminada: se representa la ruta predeterminada IPv4 como 0.0.0.0. La ruta predeterminada se usa como ruta “**comodín**" cuando no se dispone de una ruta más específica. El uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8).

Loopback: Una de estas direcciones reservadas es la dirección IPv4 de loopback **127.0.0.1**. La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. A pesar de que sólo se usa la dirección única 127.0.0.1, se reservan las direcciones 127.0.0.0 a 127.255.255.255. Cualquier dirección dentro de este bloque producirá un loop back dentro del host local.

Direcciones de enlace local: Las direcciones IPv4 del bloque de direcciones de **169.254.0.0 a 169.254.255.255** son designadas como direcciones de enlace local. El sistema operativo puede asignar automáticamente estas direcciones al host local en

entornos donde no se dispone de una configuración IP. Éstas pueden usarse en una pequeña red punto a punto o con un host que no podría obtener automáticamente una dirección de un servidor de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host, DHCP).

Direcciones TEST-NET: Se establece el bloque de direcciones de 1**92.0.2.0 a 192.0.2.255 (192.0.2.0 /24) para fines de enseñanza y aprendizaje.** A diferencia de las direcciones experimentales, los dispositivos de red aceptarán estas direcciones en su configuración.

8. Limitaciones del sistema basado en clases

La asignación con clase de espacio de direcciones a menudo desperdiciaba muchas direcciones, lo cual agotaba la disponibilidad de direcciones IPv4.

8. Direccionamiento sin clase

El sistema que utilizamos actualmente se denomina direccionamiento sin clase. Con el sistema **classless**, se asignan los bloques de direcciones adecuados para la cantidad de hosts a las compañías u organizaciones sin tener en cuenta la clase.

9. Asignación de direcciones dentro de una red

Los hosts se asocian con una red IPv4 por medio de una porción de red en común de la dirección. Dentro de una red, existen diferentes tipos de hosts:
Dispositivos finales para usuarios.
Servidores y periféricos.
Dispositivos intermediarios.

Cada uno de los diferentes tipos de dispositivos **debe ser asignado en un bloque lógico** de direcciones dentro del rango de direcciones de la red.

Ver animación 6.3.1

Una parte importante de la planificación de un esquema de direccionamiento IPv4 es decidir cuándo utilizar direcciones privadas y dónde se deben aplicar. Se debe tener en cuenta si los dispositivos a los que se pueden asignar direcciones privadas requieren acceso a Internet, y si está la red capacitada para proveer el servicio de Traducción de dirección de red (NAT).

Si hay más dispositivos que direcciones públicas disponibles, sólo esos dispositivos que accederán directamente a Internet, como los servidores Web, requieren una dirección pública. Un servicio NAT permitiría a esos dispositivos con direcciones privadas compartir de manera eficiente las direcciones públicas restantes.

9.1 Direcciones para dispositivos de usuario

En la mayoría de las redes de datos, la mayor población de hosts incluye dispositivos finales como PC, teléfonos y asistentes digitales personales (PDA). Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a estos hosts.

Las direcciones IP pueden asignarse de manera estática o dinámica.

9.1.1 Asignación estática

Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host. Como mínimo, esto implica ingresar la dirección IP del host, la máscara de subred y el gateway por defecto. Las direcciones estáticas tienen algunas ventajas en comparación con las direcciones dinámicas. Por ejemplo, resultan útiles para impresoras, servidores y otros dispositivos de red que deben ser accesibles a los clientes de la red.

Si los hosts normalmente acceden a un servidor en una dirección IP en particular, esto provocaría problemas si se cambiara esa dirección. Sin embargo, puede llevar mucho tiempo ingresar la información en cada host.

Al utilizar direccionamiento IP estático, es necesario mantener una lista precisa de las direcciones IP asignadas a cada dispositivo. Éstas son direcciones permanentes y normalmente no vuelven a utilizarse.

9.1.2 Asignación dinámica

Los dispositivos de usuarios finales a menudo poseen direcciones dinámicamente asignadas, utilizando el Protocolo de configuración dinámica de host (DHCP).

El DHCP permite la asignación automática de información de direccionamiento como la dirección IP, la máscara de subred, el gateway por defecto y otra información de configuración. DHCP es generalmente el método preferido para asignar direcciones IP a los hosts de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada.

Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la "alquila" durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta función es muy útil para los usuarios móviles que entran y salen de la red.

9.2 Direcciones para servidores y periféricos

Cualquier recurso de red como un servidor o una impresora debe tener una dirección IPv4 estática. Los hosts clientes acceden a estos recursos utilizando las direcciones IPv4de estos dispositivos. Por lo tanto, son necesarias direcciones predecibles para cada uno de estos servidores y periféricos.

Los servidores y periféricos son un punto de concentración para el tráfico de red. Se envían muchos paquetes desde las direcciones IPv4 de estos dispositivos y hacia éstas. Al monitorear el tráfico de red con una herramienta como Wireshark, un administrador de red debe poder identificar rápidamente estos dispositivos.

9.3 Direcciones para dispositivos intermedios

Los dispositivos intermediarios también son un punto de concentración para el tráfico de red. Casi todo el tráfico dentro de las redes o entre ellas pasa por alguna forma de dispositivo intermediario. Debido a que es necesario saber cómo comunicarse con dispositivos intermedios, éstos deben tener direcciones predecibles. Por lo tanto, típicamente, las direcciones se asignan manualmente.

Además, las direcciones de estos dispositivos deben estar en un rango diferente dentro del bloque de red que las direcciones de dispositivos de usuario. Normalmente, la interfaz del router utiliza la dirección más baja o más alta de la red. Esta asignación debe ser uniforme en todas las redes de la empresa, de manera que el personal de red siempre conozca la gateway dela red, independientemente de cuál sea la red en la que están trabajando.

10. Proveedores de servicios de Internet (ISP)

La mayoría de las compañías u organizaciones obtiene sus bloques de direcciones IPv4 de un ISP. Un ISP (Internet Server Provider) generalmente suministrará una pequeña cantidad de direcciones IPv4 utilizables (6 ó 14) a sus clientes como parte de los servicios. Se pueden obtener bloques mayores de direcciones de acuerdo con la justificación de las necesidades y con un costo adicional por el servicio.

En cierto sentido, el ISP presta o alquila estas direcciones a la organización. Si se elige cambiar la conectividad de Internet a otro ISP, el nuevo ISP suministrará direcciones de los bloques de direcciones que ellos poseen, y el ISP anterior devuelve los bloques prestados a su asignación para prestarlos nuevamente a otro cliente.

11. División en subredes

La división en subredes permite crear múltiples redes lógicas de un solo bloque de direcciones. Creamos las subredes utilizando uno o más de los bits del host como bits de la red. Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuanto más bits de host se usen, mayor será la cantidad de subredes que puedan definirse.

Para cada bit que se tomó prestado, se duplica la cantidad de subredes disponibles.

Por ejemplo: si se toma prestado 1 bit, es posible definir 2 subredes. Si se toman prestados 2 bits, es posible tener 4 subredes. Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones host por subred.

El router A posee dos interfaces para interconectar dos redes. Dado un bloque de direcciones 192.168.1.0 /24, se crearán dos subredes. Se toma prestado un bit de la porción de host utilizando una máscara de subred 255.255.255.128, en lugar de la máscara original 255.255.255.0. El bit más significativo del último octeto se usa para diferenciar dos subredes. Para una de las subredes, este bit es "0" y para la otra subred, este bit es “1".

11.1 Fórmula para calcular subredes y hosts

Use esta fórmula para calcular la cantidad de subredes: 2^n donde n = la cantidad de bits que se tomaron prestados
En el ejemplo, el cálculo es así: 2^1 = 2 subredes
Para calcular la cantidad de hosts por red, se usa la fórmula 2^n - 2 donde n = la cantidad de bits para hosts.
La aplicación de esta fórmula, (2^7 - 2 = 126) muestra que cada una de estas subredes puede tener 126 hosts.

En cada subred, el valor del último octeto es:
Subred 1: 00000000 = 0
Subred 2: 10000000 = 128

11.2 Ejemplo con 3 subredes

A continuación, piensa en una internetwork que requiere tres subredes.

Nuevamente, se comienza con el mismo bloque de direcciones 192.168.1.0 /24. Tomar prestado un solo bit proporcionará únicamente dos subredes. Para proveer más redes, se cambia la máscara de subred a 255.255.255.192 y se toman prestados dos bits. Esto proveerá cuatro subredes.

Calcule la subred con esta fórmula: 2^2 = 4 subredes

Para calcular la cantidad de hosts, comience por examinar el último octeto. Observe estas subredes.
Subred 0: 0 = 00000000
Subred 1: 64 = 01000000
Subred 2: 128 = 10000000
Subred 3: 192 = 11000000

Aplique la fórmula de cálculo de host. 2^6 - 2 = 62 hosts por subred

11.3 Ejemplo con 6 subredes

Considere un ejemplo con cinco LAN y una WAN para un total de 6 redes. Para incluir 6 redes, coloque la subred 192.168.1.0 /24 en bloques de direcciones mediante la fórmula: 2^3 = 8
Para obtener al menos 6 subredes, pida prestados tres bits de host. Una máscara de subred 255.255.255.224 proporciona los tres bits de red adicionales.
Para calcular la cantidad de hosts, comience por examinar el último octeto.
0 = 00000000
32 = 00100000
64 = 01000000
96 = 01100000
128 = 10000000
160 = 10100000
192 = 11000000
224 = 11100000
Aplique la fórmula de cálculo de host: 2^5 - 2 = 30 hosts por subred.

11.4 División en redes del tamaño adecuado

Cada red dentro de la internetwork de una empresa u organización está diseñada para incluir una cantidad limitada de hosts. Es necesario que los administradores de red diseñen el esquema de direccionamiento de la internetwork para incluir la cantidad máxima de hosts para cada red. La cantidad de hosts en cada división debe permitir el crecimiento de la cantidad de hosts.

11.4.1 Determine la cantidad total de host

Primero, considere la cantidad total de hosts necesarios por toda la internetwork corporativa. Se debe usar un bloque de direcciones lo suficientemente amplio como para incluir todos los dispositivos en todas las redes corporativas.

Esto incluye dispositivos de usuarios finales, servidores, dispositivos intermediarios e interfaces de routers. Considere el ejemplo de una internetwork corporativa que necesita incluir 800 hosts en sus cuatro ubicaciones.

11.4.2 Determine la cantidad y el tamaño de las redes

A continuación, considere la cantidad de redes y el tamaño de cada una requeridas de acuerdo con los grupos comunes de hosts. Se dividen las subredes de la red para superar problemas de ubicación, tamaño y control. Al diseñar el direccionamiento, se tienen en cuenta los factores para agrupar los hosts antes tratados:

Agrupar basándonos en una ubicación geográfica común
Agrupar hosts usados para propósitos específicos
Agrupar basándonos en la propiedad

11.4.3 Asignación de direcciones

Ahora que se conoce la cantidad de redes y la cantidad de hosts para cada red, es necesario comenzar a asignar direcciones a partir del bloque general de direcciones. Este proceso comienza al asignar direcciones de red para ubicaciones de redes especiales. Se comienza por las ubicaciones que requieren la mayoría de los hosts y se continúa hasta los enlaces punto a punto. Son 200

11.5 Máscara de red de longitud variable (VLSM)

El uso de una Máscara de subred de longitud variable (VLSM) fue diseñada para maximizar la eficiencia del direccionamiento. Al identificar la cantidad total de hosts que utiliza la división tradicional en subredes, se asigna la misma cantidad de direcciones para cada subred. Si todas las subredes tuvieran los mismos requisitos en cuanto a la cantidad de hosts, estos bloques de direcciones de tamaño fijo serían eficientes. Sin embargo, esto no es lo que suele suceder.

Por ejemplo, la topología en la red anterior muestra los requisitos de subred de siete subredes, una para cada una de las cuatro LAN y una para cada una de las tres WAN.

Con la dirección 192.168.20.0, es necesario pedir prestados 3 bits de los bits del host en el último octeto para satisfacer los requisitos de subred de siete subredes.

Estos bits son bits que se toman prestados al cambiar la máscara de subred correspondiente por números "1" para indicar que estos bits ahora se usan como bits de red. Entonces, el último octeto de la máscara se representa en binario con 11100000, que es 224. La nueva máscara 255.255.255.224 se representa mediante la notación /27 para representar un total de 27 bits para la máscara.
Al tomar prestados tres de los bits de host para usar como bits de red, quedan cinco bits de host. Estos cinco bits permitirán más de 30 hosts por subred.
A pesar de que se ha cumplido la tarea de dividir la red en una cantidad adecuada de redes, esto se hizo mediante la pérdida significativa de direcciones no utilizadas.
Por ejemplo: sólo se necesitan dos direcciones en cada subred para los enlaces WAN. Hay 28 direcciones no utilizadas en cada una de las tres subredesWAN que han sido bloqueadas en estos bloques de direcciones.

Seguir ejemplo de VLSM en el material de CISCO (apartado 6.5.3)

Actividades

Actividad 6.5.4 Actividad 6.5.5 Actividad 6.5.6
Actividad 6.5.7 obligatoria
Actividad 6.5.8 obligatoria

12. Encabezado del paquete IPv4

Un protocolo IPv4 define muchos campos diferentes en el encabezado del paquete.
Versión: Contiene el número IP de la versión (4).
Longitud del encabezado (IHL). Especifica el tamaño del encabezado del paquete.
Longitud del Paquete: Este campo muestra el tamaño completo del paquete, incluyendo el encabezado y los datos, en bytes.

Identificación: Este campo es principalmente utilizado para identificar únicamente fragmentos de un paquete IP original.

Checksum del encabezado: El campo de checksum se utiliza para controlar errores del encabezado del paquete.

Opciones: Existen medidas para campos adicionales en el encabezado IPv4 para proveer otros servicios pero éstos son rara vez utilizados.

Dirección IP destino: El campo de Dirección IP destino contiene un valor binario de 32 bits que representa la dirección de host de capa de red de destino del paquete.

Dirección IP origen: El campo de Dirección IP origen contiene un valor binario de 32 bits que representa la dirección de host de capa de red de origen del paquete.

Tiempo de vida (TTL): es un valor binario de 8 bits que indica el tiempo remanente de "vida" del paquete. El valor TTL disminuye al menos en uno cada vez que el paquete es procesado por un router (es decir, en cada salto). Cuando el valor se vuelve cero, el router

descarta o elimina el paquete y es eliminado del flujo de datos de la red. Este mecanismo evita que los paquetes que no pueden llegar a destino sean enviados indefinidamente entre los routers en un routing loop. Si se permitiera que los loops de enrutamiento continúen, la red se congestionaría con paquetes de datos que nunca llegarían a destino.

Disminuyendo el valor TTL en cada salto se asegura que eventualmente se vuelva cero y que se descartará el paquete con el campo TTL vencido.

Protocolo: Este valor binario de 8 bits permite a la Capa de red pasar los datos al protocolo apropiado de la capa superior. Los valores de ejemplo son:
06 TCP, y
17 UDP.

Tipo de servicio: contiene un valor binario de 8 bits que se usa para determinar la prioridad de cada paquete. Este valor permite aplicar un mecanismo de Calidad del Servicio (QoS) a paquetes de alta prioridad, como aquellos que llevan datos de voz en telefonía. El router que procesa los paquetes puede ser configurado para decidir qué paquete es enviado primero basado en el valor del Tipo de servicio.

Desplazamiento de fragmentos: un router puede tener que fragmentar un paquete cuando lo envía desde un medio a otro medio que tiene una MTU más pequeña. Cuando se produce una fragmentación, el paquete IPv4 utiliza el campo Desplazamiento de fragmento y el señalizador MF en el encabezado IP para reconstruir el paquete cuando llega al host destino. El campo de desplazamiento del fragmento identifica el orden en el cual ubicar el fragmento del paquete en la reconstrucción.

Señalizador de Más fragmentos (MF): es un único bit en el campo del señalizador usado con el Desplazamiento de fragmentos para la fragmentación y reconstrucción de paquetes. Cuando está configurado el señalizador Más fragmentos, significa que no es el último fragmento de un paquete. Cuando un host receptor ve un paquete que llega con MF = 1, analiza el Desplazamiento de fragmentos para ver dónde ha de colocar este fragmento en el paquete reconstruido. Cuando un host receptor recibe un paquete con el MF = 0 y un valor diferente a cero en el desplazamiento de fragmentos, coloca ese fragmento como la última parte del paquete reconstruido. Un paquete no fragmentado tiene toda la información de fragmentación cero (MF = 0, desplazamiento de fragmentos = 0).

Señalizador de No Fragmentar (DF): es un solo bit en el campo del señalizador que indica que no se permite la fragmentación del paquete. Si se establece el bit del señalizador No Fragmentar, entonces la fragmentación de este paquete NO está permitida. Si un router necesita fragmentar un paquete para permitir el paso hacia abajo hasta la capa de Enlace de datos pero el bit DF se establece en 1, entonces el router descartará este paquete.

12.1 Ejemplo paquete IPv4

Ver = 4; versión IP.
IHL = 5; tamaño del encabezado en palabras de 32 bits (4 bytes). Este encabezado tiene 5*4 = 20 bytes, el tamaño mínimo válido. Longitud total = 472; tamaño del paquete

(encabezado y datos). Identificación = 111; identificador original del paquete (requerido si se fragmenta posteriormente).
Señalizador = 0; significa que el paquete puede ser fragmentado si se requiere.
Desplazamiento de fragmentos = 0; significa que este paquete no está actualmente fragmentado (no existe desplazamiento).
Período de vida = 123; es el tiempo de procesamiento en segundos de la Capa 3 antes de descartar el paquete.
Protocolo = 6; significa que los datos llevados por este paquete son un segmento TCP.

13. Prueba de la capa de red - PING

Ping es una utilidad para probar la conectividad IP entre hosts. Ping envía solicitudes de respuestas desde una dirección host específica.Ping usa un protocolo de capa 3 que forma parte del conjunto de aplicaciones TCP/IP llamado Control Message Protocol (Protocolo de mensajes de control de Internet, ICMP). Ping usa un datagrama de solicitud de eco ICMP. Si el host en la dirección especificada recibe la solicitud de eco, éste responde con un datagrama de respuesta de eco ICMP. En cada paquete enviado, el ping mide el tiempo requerido para la respuesta.

A medida que se recibe cada respuesta, el ping muestra el tiempo entre el envío del ping y la recepción de la respuesta. Ésta es una medida del rendimiento de la red. **Ping posee un valor de límite de tiempo de espera para la respuesta**. Si no se recibe una respuesta dentro de ese intervalo de tiempo, el ping abandona la comunicación y proporciona un mensaje que indica que no se recibió una respuesta.

Después de enviar todas las peticiones, la utilidad de ping provee un resumen de las respuestas. Este resumen incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

13.1 PING del loopback local

Existen casos especiales de prueba y verificación para los cuales se puede usar el ping. Un caso es la prueba de la configuración interna del IP en el host local. Para hacer esta prueba, se realiza el ping de la dirección reservada especial del loopback local (127.0.0.1)

Una respuesta de 127.0.0.1 indica que el IP está correctamente instalado en el host.

Sin embargo, esta respuesta no indica que las direcciones, máscaras o los gateways estén correctamente configurados. Sencillamente, prueba la IP en la capa de red del protocolo IP. Si se obtiene un mensaje de error, esto indica que el TCP/IP no funciona en el host.

13.2 PING de gateway

También es posible utilizar el ping para probar la capacidad de comunicación del host en la red local. Generalmente, esto se hace haciendo ping a la dirección IP del gateway del host. Un ping en el gateway indica que la interfaz del host y del router que funcionan como gateway funcionan en la red local. Para esta prueba, se usa la dirección de gateway con mayor frecuencia, debido a que el router normalmente está en funcionamiento. Si la

dirección de gateway no responde, se puede intentar con la dirección IP de otro host que sepa que funciona en la red local.

Si el gateway u otro host responden, entonces los hosts locales pueden comunicarse con éxito en la red local.

Si el gateway no responde pero otro host sí lo hace, esto podría indicar un problema con la interfaz del router que funciona como gateway. Una posibilidad es que se tiene la dirección equivocada para el gateway.

Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde a peticiones de ping.

También puede suceder que otros hosts tengan la misma restricción de seguridad aplicada.

13.3 PING de host remoto

También se puede utilizar el ping para probar la capacidad de comunicación del host IP local con una LAN remota.
El host local puede hacer ping a un host que funciona en una red remota. Si el ping se realiza con éxito significa que se ha verificado la comunicación del host en la red local, el funcionamiento del router que se usa como gateway y los demás routers que puedan encontrarse en la ruta entre la red y la red del host remoto.
Recuerde: muchos administradores de red limitan o prohíben la entrada de datagramas ICMP en la red corporativa. Por lo tanto, la ausencia de una respuesta de ping podría deberse a restricciones de seguridad y no a elementos que no funcionan en las redes.

Ver animación 6.6.3

14. Traceroute (Prueba de la ruta)

El ping se usa para indicar la conectividad entre dos hosts. **Traceroute (tracert)** es una utilidad que permite observar la ruta entre estos hosts. El rastreo genera una lista de saltos alcanzados con éxito a lo largo de la ruta.

Esta lista puede suministrar información importante para la verificación y el diagnóstico de fallas. Si los datos llegan a destino, entonces el rastreador menciona la interfaz en cada router que aparece en el camino.
Si los datos fallan en un salto durante el camino, se tiene la dirección del último router que respondió al rastreo.
Esto indica el lugar donde se encuentra el problema o las restricciones de seguridad.

14.1 Tiempo de ida y vuelta

El uso de traceroute proporciona el tiempo de ida y vuelta (RTT) para cada salto a lo largo del camino e indica si se produce una falla en la respuesta del salto. El tiempo de ida y vuelta (RTT) es el tiempo que le lleva a un paquete llegar al host remoto y a la respuesta regresar del host. Se usa un asterisco (*) para indicar la pérdida de un paquete.

14.2 Tiempo de vida (TTL)

El campo TTL se usa para limitar la cantidad de saltos que un paquete puede cruzar. Cuando un paquete ingresa a un router, el campo TTL disminuye en 1. Cuando el TTL llega a cero, el router no envía el paquete y éste es descartado. Además de descartar el paquete, el router normalmente envía un mensaje de tiempo superado de ICMP dirigido al host de origen.

Ver animación 6.6.4

http://support.microsoft.com/kb/162326/es

15. ICMP v4

ICMP es el protocolo de mensajería para el conjunto de aplicaciones TCP/IP. ICMP proporciona mensajes de control y error y se usa mediante las utilidades ping y traceroute.

Los mensajes ICMP más comunes son:
Confirmación de host: Se puede utilizar un mensaje de eco del ICMP para determinar si un host está en funcionamiento. El host local envía una petición de eco de ICMP a un host. El host que recibe el mensaje de eco responde mediante la respuesta de eco de ICMP. Este uso de los mensajes de eco de ICMP es la base de la utilidad ping.

Destino o servicio inalcanzable: Se puede usar el destino inalcanzable de ICMP para notificar a un host que el destino o servicio es inalcanzable. Cuando un host o gateway recibe un paquete que no puede enviar, puede enviar un paquete de destino inalcanzable de ICMP al host que origina el paquete. El paquete de destino inalcanzable tendrá códigos que indican el motivo por el cual el paquete no pudo ser enviado.

Entre los códigos de destino inalcanzable se encuentran:
0 = red inalcanzable
1 = host inalcanzable
2 = protocolo inalcanzable
3 = puerto inalcanzable

Los códigos para las respuestas red inalcanzable y host inalcanzable son respuestas de un router que no puede enviar un paquete. Si un router recibe un paquete para el cual no posee una ruta, puede responder con un código de destino inalcanzable de ICMP = 0, que indica que la red es inalcanzable.
Si un router recibe un paquete para el cual posee una ruta conectada pero no puede enviar el paquete al host en la red conectada, el router puede responder con un código de destino inalcanzable de ICMP = 1, que indica que se conoce la red pero que el host es inalcanzable.
Los códigos 2 y 3 (protocolo inalcanzable y puerto inalcanzable) son utilizados por un host final para indicar que el segmento TCP o el datagrama UDP en un paquete no pudo ser enviado al servicio de capa superior.

Tiempo superado: Un router utiliza un mensaje de tiempo superado de ICMP para indicar que no se puede enviar un paquete debido a que el campo TTL del paquete ha expirado. Si un router recibe un paquete y dismimuye el campo TTL del paquete a cero, éste descarta el paquete. El router también puede enviar un mensaje de tiempo superado de ICMP al host de origen para informar al host el motivo por el que se descartó el paquete.

Redireccionamiento de ruta: Un router puede usar un mensaje de redireccionamiento de ICMP para notificar a los hosts de una red acerca de una mejor ruta disponible para un destino en particular. Es posible que este mensaje sólo pueda usarse cuando el host de origen esté en la misma red física que ambos gateways.

Disminución de velocidad en origen: El mensaje de disminución de velocidad en origen de ICMP puede usarse para informar al origen que deje de enviar paquetes por un tiempo. Si un router no posee suficiente espacio en búfer para recibir paquetes entrantes, un router descartará los paquetes. También puede enviar un mensaje de disminución de velocidad en origen de ICMP a los hosts de origen por cada mensaje que descarta. Un host de destino también puede enviar un mensaje de disminución de velocidad en origen si los datagramas llegan demasiado rápido para ser procesados. Cuando un host recibe un mensaje de disminución de velocidad en origen de ICMP, lo informa a la capa de transporte.

Actividades

Actividad 6.7.1

Actividad 6.7.2

Actividad 6.7.5 entregar

Actividad 6.8.1 entregar

16. Descripción de IPv6

A principios de los años noventa, el Grupo de trabajo de ingeniería de Internet (IETF) centró su interés en el agotamiento de direcciones de red IPv4 y comenzó a buscar un reemplazo para este protocolo.

Esta actividad produjo el desarrollo de lo que hoy se conoce como IPv6. Crear mayores capacidades de direccionamiento fue la motivación inicial para el desarrollo de este nuevo protocolo.También se consideraron otros temas durante el desarrollo de IPv6,
como:

Manejo mejorado de paquetes

Escalabilidad y longevidad mejoradas

Mecanismos QoS (Calidad del Servicio)

Seguridad integrada

Para proveer estas características, IPv6 ofrece: Direccionamiento jerárquico de 128 bits: para expandir las capacidades de direccionamiento

Simplificación del formato de encabezado: para mejorar el manejo de paquetes

Capacidad de rotulado de flujo: como mecanismos QoS

Capacidades de autenticación y privacidad: para integrar la seguridad

16.1 Transición a IPv6

IPv6 se está implementando lentamente y en redes selectas. Debido a las mejores herramientas, tecnologías y administración de direcciones en los últimos años, IPv4 todavía se utiliza ampliamente y probablemente permanezca durante algún tiempo en el futuro.

Sin embargo, IPv6 podrá eventualmente reemplazar a IPv4 como protocolo de Internet dominante.

17. Enrutamiento

Dentro de una red o subred, los hosts se comunican entre sí sin necesidad de un dispositivo intermediario de capa de red. Cuando un host necesita comunicarse con otra red, un dispositivo intermediario o router actúa como un gateway hacia la otra red.

Como parte de su configuración, un host tiene una dirección de gateway por defecto definida.Esta dirección de gateway es la dirección de una interfaz de router que está conectada a la misma red que el host. El router también necesita una ruta que defina dónde enviar luego el paquete. A esto se lo denomina dirección del siguiente salto.

El router examina la porción de la red de la dirección de destino del paquete y envía el paquete a la interfaz adecuada. Si la red de destino está conectado directamente a este router, el paquete es enviado directamente a ese host.

Si la red de destino no está conectada directamente, el paquete es enviado a un segundo router, que es el router del siguiente salto.

Ver animación 5.3.2

17.1 Gateway

El gateway, también conocido como gateway por defecto, es necesario para enviar un paquete fuera de la red local. Si la porción de red de la dirección de destino del paquete es diferente de la red del host de origen, el paquete tiene que hallar la salida fuera de la red original. Para esto, el paquete es enviado al gateway. Este gateway es una interfaz del router conectada a la red local.

La interfaz del gateway tiene una dirección de capa de Red que concuerda con la dirección de red de los hosts.

17.2 Tabla de Enrutamiento

Un router toma una decisión de reenvío para cada paquete que llega a la interfaz del gateway. Este proceso de reenvío es denominado enrutamiento. Para reenviar un paquete a una red de destino, el router requiere una ruta hacia esa red. Si una ruta a una red de destino no existe, el paquete no puede reenviarse. Los routers agregan rutas para las redes conectadas a su tabla de enrutamiento.

Cuando se configura una interfaz de router con una dirección IP y una máscara de subred, la interfaz se vuelve parte de esa red. La tabla de enrutamiento ahora incluye esa

red como red directamente conectada. Todas las otras rutas, sin embargo, deben ser configuradas o adquiridas por medio del protocolo de enrutamiento. Para reenviar un paquete, el router debe saber dónde enviarlo. Esta información está disponible como rutas en una tabla de enrutamiento.

La tabla de enrutamiento almacena la información sobre las redes conectadas y remotas.
Las redes conectadas están directamente adjuntas a una de las interfaces del router. Estas interfaces son los gateways para los hosts en las diferentes redes locales. Las redes remotas son redes que no están conectadas directamente al router. Las rutas a esas redes se pueden configurar manualmente en el router por el administrador de red o aprendidas automáticamente utilizando protocolos de enrutamiento dinámico.

Revisar
Tema 5 de CISCO
Apartado 10.2.3 del Tema 10 de CISCOApartado 10.5.1 del Tema 10 de CISCO Apartado 10.5.2 del Tema 10 de CISCO

Actividades
Actividad 5.5.1 obligatoria
Actividad 5.6.1 obligatoria (ver trazas)
Actividad 10.2.3 obligatoria
Actividad 10.6.1 obligatoria
Actividad 10.7.1 obligatoria
Examen CISCO Tema 5
Examen CISCO Tema 6
Examen CISCO Tema 10

TEMA 6 Nivel de Transporte

1. Introducción

Las aplicaciones como clientes de correo electrónico, exploradoresWeb y clientes de mensajería instantánea permiten que las personas utilicen las computadoras y las redes para enviar mensajes y buscar información.
Los datos de cada una de estas aplicaciones se empaquetan, transportan y entregan al servidor o aplicación adecuados en el dispositivo de destino.
Los procesos descritos en la capa de Transporte del modelo OSI aceptan los datos de la capa de Aplicación y los preparan para el direccionamiento en la capa de Red. La capa de Transporte es responsable de la transferencia de extremo a extremo general de los datos de aplicación.

2. Funciones de la capa de transporte

Las responsabilidades principales que debe cumplir son:

Seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino.

Segmentación de datos y gestión de cada porción.

Reensamble de segmentos en flujos de datos de aplicación

Identificación de las diferentes aplicaciones.

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación.

2.1 Seguimiento de Conversaciones Individuales

Cualquier host puede tener múltiples aplicaciones que se están comunicando a través de la red. Cada una de estas aplicaciones se comunicará con una o más aplicaciones en hosts remotos. Es responsabilidad de la capa de Transporte mantener los diversos streams de comunicación entre estas aplicaciones.

2.2 Segmentación de datos

Debido a que cada aplicación genera un stream de datos para enviar a una aplicación remota, estos datos deben prepararse para ser enviados por los medios en partes manejables.

Los protocolos de la capa de Transporte describen los servicios que segmentan estos datos de la capa de Aplicación. Esto incluye la encapsulación necesaria en cada sección de datos. Cada sección de datos de aplicación requiere que se agreguen encabezados en la capa de Transporte para indicar la comunicación a la cual está asociada.

2.3 Reensamble de segmentos

En el host de recepción, cada sección de datos puede ser direccionada a la aplicación adecuada. Además, estas secciones de datos individuales también deben reconstruirse para generar un stream completo de datos que sea útil para la capa de Aplicación.

Los protocolos de la capa de Transporte describen cómo se utiliza la información de encabezado de dicha capa para reensamblar las secciones de datos en streams y enviarlas a la capa de Aplicación.

2.4 Identificación de las aplicaciones

Para poder transferir los streams de datos a las aplicaciones adecuadas, la capa de Transporte debe identificar la aplicación de destino. Para lograr esto, la capa de Transporte asigna un identificador a la aplicación.

Los protocolos TCP/IP denominan a este identificador número de puerto.

Este número de puerto se utiliza en el encabezado de la capa de Transporte para indicar con qué aplicación está asociada esa sección de datos. La capa de Transporte es el enlace entre la capa de Aplicación y las capas inferiores, que son responsables de la transmisión en la red. Esta capa acepta datos de distintas conversaciones y los transfiere

a las capas inferiores como secciones manejables. Las aplicaciones no necesitan conocer los detalles de operación de la red en uso.
Las aplicaciones generan datos que se envían desde una aplicación a otra sin tener en cuenta el tipo de host destino, el tipo de medios sobre los que los datos deben viajar, la congestión en un enlace o el tamaño de la red. Además, las capas inferiores no tienen conocimiento de que existen varias aplicaciones que envían datos en la red. Su responsabilidad es entregar los datos al dispositivo adecuado.

Luego la capa de Transporte ordena esta secciones antes de entregarlas a la aplicación adecuada.

3. Control de las conversaciones

Las funciones principales especificadas por todos los protocolos de la capa de Transporte incluyen:
Segmentación y reensamblaje: La mayoría de las redes poseen una limitación en cuanto a la cantidad de datos que pueden incluirse en una única PDU (Unidad de datos del protocolo). La capa de Transporte divide los datos de aplicación en bloques de datos de un tamaño adecuado. En el destino, la capa de Transporte reensambla los datos antes de enviarlos a la aplicación o servicio de destino.

Multiplexación de conversaciones: Pueden existir varias aplicaciones o servicios ejecutándose en cada host de la red. A cada una de estas aplicaciones o servicios se les asigna una dirección conocida como puerto para que la capa de Transporte pueda determinar con qué aplicación o servicio se identifican los datos.

Además de utilizar la información contenida en los encabezados para las funciones básicas de segmentación y reensamblaje de datos, algunos protocolos de la capa de Transporte proveen:

Conversaciones orientadas a la conexión: la capa de Transporte puede brindar esta orientación a la conexión creando una sesión entre las aplicaciones. Estas conexiones preparan las aplicaciones para que se comuniquen entre sí antes de que se transmitan los datos.

Entrega confiable: es posible que una sección de datos se corrompa o se pierda por completo a medida que se transmite a través de la red. La capa de Transporte puede asegurar que todas las secciones lleguen a destino al contar con el dispositivo de origen para volver a transmitir los datos que se hayan perdido.

Reconstrucción ordenada de datos: Ya que las redes proveen rutas múltiples que pueden poseer distintos tiempos de transmisión, los datos pueden llegar en el orden incorrecto. Al numerar y secuenciar los segmentos, la capa de Transporte puede asegurar que los mismos se reensamblen en el orden adecuado.
Control del flujo: Los hosts de la red cuentan con recursos limitados, como memoria o ancho de banda. Cuando la capa de Transporte advierte que estos recursos están sobrecargados, algunos protocolos pueden solicitar que la aplicación que envía reduzca la velocidad del flujo de datos. Esto se lleva a cabo en la capa de Transporte regulando la cantidad de datos que el origen transmite como grupo. El control del flujo puede prevenir la pérdida de segmentos en la red y evitar la necesidad de retransmisión.

4. Determinación de la necesidad de confiabilidad

Confiabilidad significa asegurar que cada sección de datos que envía el origen llegue al destino. Las aplicaciones, como bases de datos, las páginas Web y los e-mails, requieren que todos los datos enviados lleguen al destino en su condición original, de manera que los mismos sean útiles.
Todos los datos perdidos pueden corromper una comunicación y dejarla incompleta o ilegible. Por lo tanto, estas aplicaciones se diseñan para utilizar un protocolo de capa de Transporte que implemente la confiabilidad.

Otras aplicaciones son más tolerantes en lo que se refiere a la pérdida de pequeñas cantidades de datos. Por ejemplo, si uno o dos segmentos de un stream de vídeo no llegan al destino, sólo generará una interrupción momentánea en el stream. Esto puede representar distorsión en la imagen pero quizás ni sea advertido por el usuario.

La imagen en un streaming vídeo se degradaría en gran medida si el dispositivo de destino tuvo que dar cuenta de los datos perdidos y demorar el stream mientras espera que lleguen.
Es conveniente proporcionar la mejor imagen posible al momento en que llegan los segmentos y renunciar a la confiabilidad.

5. Protocolos de la capa de transporte

Los dos protocolos más comunes de la capa de Transporte del conjunto de protocolos TCP/IP son:

El protocolo de datagramas de usuario (UDP).
El protocolo de control de transmisión (TCP)

5.1 UDP

UDP (Protocolo de datagramas de usuario) es un protocolo simple, sin conexión, descrito en la RFC 768. Cuenta con la ventaja de proveer la entrega de datos sin utilizar muchos recursos. **Las porciones de comunicación en UDP se llaman datagramas.**

Entre las aplicaciones que utilizan UDP se incluyen:
Sistema de nombres de dominios (DNS)
Streaming de vídeo
Voz sobre IP (VoIP)

5.2 TCP

TCP (Protocolo de control de transmisión) es un protocolo orientado a la conexión, descrito en la RFC 793. TCP proporciona funciones adicionales como son garantizar el orden de entrega, entrega confiable y control de flujo. Las porciones de comunicación en TCP se llaman segmentos.
Las aplicaciones que utilizan TCP son:
ExploradoresWeb
E-mail
Transferencia de archivos

Cada segmento de TCP posee 20 bytes de carga en el encabezado, que encapsulan los datos de la capa de Aplicación, mientras que cada segmento UDP sólo posee 8 bytes de carga.

5.3 Encabezados TCP y UDP

6. Direccionamiento del puerto

Considere un ejemplo de una computadora que recibe y envía e-mails, mensajes instantáneos, páginas Web y llamadas telefónicas VoIP de manera simultánea. Para diferenciar los segmentos y datagramas para cada aplicación, tanto TCP como UDP cuentan con campos de encabezado que pueden identificar de manera exclusiva estas aplicaciones.

Estos identificadores únicos son los números de los puertos. En el encabezado de cada segmento o datagrama hay un puerto de origen y destino. El número de puerto de origen es el número para esta comunicación asociado con la aplicación que origina la comunicación en el host local. El número de puerto de destino es el número para esta comunicación asociado con la aplicación de destino en el host remoto.

Los números de puerto se asignan de varias maneras, en función de si el mensaje es una solicitud o una respuesta. Mientras que los procesos en el servidor poseen números de puertos estáticos asignados a ellos, los clientes eligen un número de puerto de forma dinámica para cada conversación. Cuando una aplicación de cliente envía una solicitud a una aplicación de servidor, el puerto de destino contenido en el encabezado es el número de puerto que se asigna al servicio que se ejecuta en el host remoto. El software del cliente debe conocer el número de puerto asociado con el proceso del servidor en el host remoto. Este número de puerto de destino se puede configurar, ya sea de forma predeterminada o manual.

Por ejemplo, cuando una aplicación de explorador Web realiza una solicitud a un servidor Web, el explorador utiliza TCP y el número de puerto 80 a menos que se especifique otro valor. El puerto de origen del encabezado de un segmento o datagrama de un cliente se genera de manera aleatoria.
Siempre y cuando no entre en conflicto con otros puertos en uso en el sistema, el cliente puede elegir cualquier número de puerto. El número de puerto actúa como dirección de retorno para la aplicaciónque realiza la solicitud. La capa de Transporte mantiene un seguimientode este puerto y de la aplicación que generó la solicitud, de manera que cuando se devuelva una respuesta, pueda ser enviada a la aplicación correcta.

La combinación del número de puerto de la capa de Transporte y de la dirección IP de la capa de Red asignada al host identifica de manera exclusiva un proceso en particular que se ejecuta en un dispositivo host específico. Esta combinación se denomina socket.

Por ejemplo, una solicitud de página Web HTTP que se envía a un servidor Web (puerto 80) y que se ejecuta en un host con una dirección IPv4 de Capa 3 192.168.1.20 será destinada al socket 192.168.1.20:80.

Si el explorador Web que solicita la página Web se ejecuta en el host 192.168.100.48 y el número de puerto dinámico asignado al explorador Web es 49.150, el socket para la páginaWeb será 192.168.100.48:49150.

La Autoridad de números asignados de Internet (IANA) asigna números de puerto. IANA es un organismo de estándares responsable de la asignación de varias normas de direccionamiento.

Existen distintos tipos de números de puerto:
Puertos bien conocidos (Números del 0 al 1 023): estos números se reservan para servicios y aplicaciones. Por lo general, se utilizan para aplicaciones como HTTP (servidorWeb), POP3/SMTP (servidor de email) y Telnet.

Puertos Registrados (Números 1024 al 49151): estos números de puertos están asignados a procesos o aplicaciones del usuario. Estos procesos son principalmente aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un puerto bien conocido.

6.1 Utilización de los dos protocolos TCP y UDP

Algunas aplicaciones pueden utilizar los dos protocolos: TCP y UDP.

Por ejemplo, el bajo gasto de UDP permite que DNS atienda rápidamente varias solicitudes de clientes. Sin embargo, a veces el envío de la información solicitada puede requerir la confiabilidad de TCP. En este caso, el número 53 de puerto conocido es utilizado por ambos protocolos con este servicio.

6.2 Puertos

http://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_puerto
http://www.iana.org/assignments/port-numbers.

7. Netstat

A veces es necesario conocer las conexiones activas que están abiertas y en ejecución en el host de red. Netstat es una utilidad de red importante que puede usarse para verificar esas conexiones. Netstat indica el protocolo en uso, la dirección y el número de puerto locales, la dirección y el número de puerto ajenos y el estado de la conexión.

Ver animación máquina

4.1.5

8. Segmentación y reensamblaje

Algunas aplicaciones transmiten grandes cantidades de datos; en algunos casos, varios gigabytes. Resultaría poco práctico enviar todos estos datos en una sola gran sección ya que no puede transmitirse ningún otro tráfico de red mientras se envían estos datos.

Una gran sección de datos puede tardar minutos y hasta horas en enviarse. Además, si hubiera algún error, el archivo de datos completo se perdería o tendría que ser reenviado. Los dispositivos de red no cuentan con buffers de memoria lo suficientemente grandes como para almacenar esa cantidad de datos durante la transmisión o recepción. Dividir

los datos de aplicación en secciones garantiza que los datos se transmitan dentro de los límites del medio y que los datos de distintas aplicaciones puedan sermultiplexados en el medio.

TCP y UDP gestionan la segmentación de forma distinta. Con TCP, cada encabezado de segmento contiene un número de secuencia. Este número de secuencia permite que las funciones de la capa de Transporte del host de destino reensamblen los segmentos en el mismo orden en el que fueron transmitidos. Esto asegura que la aplicación de destino cuente con los datos en la forma exacta en la que se enviaron.

UDP no tiene en cuenta el orden en el que se transmitió la información ni el mantenimiento de la conexión. No existe número de secuencia en el encabezado UDP. UDP es un diseño simple y genera menos carga que TCP, lo que produce una transferencia de datos más rápida.

La información puede llegar en un orden distinto al que fue transmitida, ya que los paquetes pueden tomar diversas rutas a través de la red. Una aplicación que utiliza UDP debe tolerar el hecho de que los datos no lleguen en el orden en el que fueron enviados.

Hacer Actividad 4.1.6

9. Protocolo TCP

La diferencia clave entre TCP y UDP es la confiabilidad. La confiabilidad de la comunicación TCP se lleva a cabo utilizando sesiones orientadas a la conexión. Antes de que un host que utiliza TCP envíe datos a otro host, la capa deTransporte inicia un proceso para crear una conexión con el destino. Este proceso asegura que cada host tenga conocimiento de la comunicación y se prepare.
Luego de establecida la sesión, el destino envía acuses de recibo al origen por los segmentos que recibe. Estos acuses de recibo forman la base de la confiabilidad dentro de la sesión TCP.

Cuando el origen recibe un acuse de recibo, reconoce que los datos se han entregado con éxito y puede dejar de rastrearlos.Si el origen no recibe el acuse de recibo dentro de un tiempo predeterminado, retransmite esos datos al destino. Esta confiabilidad se logra contando con campos en el segmento TCP, cada uno con una función específica.

9.1 Establecimiento y finalización de la conexión TCP

Cuando dos hosts se comunican utilizando TCP, se establece una conexión antes de que puedan intercambiarse los datos. Luego de que se completa la comunicación, se cierran las sesiones y la conexión finaliza.
Ver explicación CISCO- Apartado 4.2.3, 4.2.4 y 4.2.5
Opcional: Actividad 4.2.5ver trazas

9.2 Reensamblaje de segmentos TCP

Cuando los servicios envían datos utilizando TCP, los segmentos pueden llegar a destinos desordenados. Para que el receptor comprenda el mensaje original, los datos en estos segmentos se reensamblan en el orden original. Para lograr esto, se asignan números de

secuencia en el encabezado de cada paquete.Durante la configuración de la sesión, se establece un número de secuencia inicial (ISN). Este número de secuencia inicial representa el valor de inicio para los bytes de esta sesión que se transmitirán a la aplicación receptora.

A medida que se transmiten los datos durante la sesión, el número de secuencia se incrementa en el número de bytes que se han transmitido. Este rastreo de bytes de datos permite que cada segmento se identifique y se envíe acuse de recibo de manera exclusiva.

El proceso TCP receptor coloca los datos del segmento en un búfer de recepción. Los segmentos se colocan en el orden de número de secuencia adecuado y se pasa a la capa de Aplicación cuando son reensamblados. Todos los segmentos que llegan con números de secuencia no contiguos se mantienen para su procesamiento posterior.

9.3 Confirmación de recepción de segmentos

Una de las funciones de TCP es asegurar que cada segmento llegue a su destino. Los servicios TCP en el host de destino envían a la aplicación de origen una cuse de recibo de los datos recibidos. El número de secuencia y el número de acuse de recibo del encabezado del segmento se utilizan para confirmar la recepción de los bytes de datos contenidos en los segmentos.

TCP utiliza el número de reconocimiento en segmentos que se vuelven a enviar al origen para indicar el próximo byte de esta sesión que espera el receptor. Esto se llama acuse de recibo de expectativa.

Se le informa al origen que el destino ha recibido todos los bytes de este stream de datos, pero sin incluir, el byte especificado por el número de acuse de recibo. Se espera que el host emisor envíe un segmento que utiliza un número de secuencia igual al número de acuse de recibo. Los números de secuencia y de acuse de recibo se intercambian en ambas direcciones.

9.3.1 Ejemplo

El host en la izquierda envía datos al host de la derecha. Envía un segmento que contiene 10 bytes de datos para esta sesión y un número de secuencia igual a 1 en el encabezado. El host receptor de la derecha recibe el segmento en la Capa 4 y determina que el número de secuencia es 1 y que posee 10 bytes de datos. Luego el host envía un segmento de vuelta al host de la izquierda para acusar recibo de estos datos. En este segmento, el host establece el número de acuse de recibo en 11 para indicar que el próximo byte de datos que espera recibir en esta sesión es el byte número 11.

Cuando el host emisor de la izquierda recibe este acuse de recibo, puede enviar el próximo segmento que contiene datos para esta sesión a partir del byte 11.

9.3.2 Tamaño de la ventana

Observando este ejemplo, si el host emisor tuviera que esperar el acuse de recibo por la recepción de cada uno de los 10 bytes, la red estaría demasiado sobrecargada. Para reducir la sobrecarga de estos acuses de recibo, los segmentos de datos múltiples

pueden enviarse previamente y ser reconocidos con un mensaje TCP simple en la dirección opuesta. Este reconocimiento contiene un número de acuse de recibo en base al número total de bytes recibidos en la sesión.
Por ejemplo, si se comienza con un número de secuencia 2000, si se reciben 10 segmentos de 1000 bytes cada uno, se devolverá al origen un número de reconocimiento igual a 12001.

La cantidad de datos que un origen puede transmitir antes de que un acuse de recibo deba ser recibido se denomina tamaño de la ventana. El tamaño de la ventana es un campo en el encabezado TCP que permite la administración de datos perdidos y el control del flujo.

9.4 Manejo de la pérdida de segmentos

Por óptimo que sea el diseño de una red, siempre se producirán pérdidas ocasionales de datos. Por lo tanto, TCP cuenta con métodos para gestionar dichas pérdidas de segmentos. Entre los mismos existe un mecanismo para retransmitir segmentos con datos no reconocidos. Un servicio de host de destino que utiliza TCP, por lo general sólo reconoce datos para secuencias de bytes contiguas. Si uno o más segmentos se pierden, sólo se acusa recibo de los datos de los segmentos que completan el stream.

Por ejemplo, si se reciben los segmentos con números de secuencia de 1500 a 3000 y de 3400 a 3500, el número de acuse de recibo será 3001. Esto sucede porque existen segmentos con números de secuencia de 3001 a 3399 que no se recibieron.

Cuando TCP en el host de origen no recibe un acuse de recibo pasado un tiempo predeterminado, volverá al último número de acuse de recibo que recibió y retransmitirá los datos a partir de éste.

El proceso de retransmisión no es especificado por RFC, sino que depende de la implementación de TCP en particular. Para una implementación de TCP típica, un host puede transmitir un segmento, colocar una copia del segmento en una cola de retransmisión e iniciar un temporizador. Cuando se recibe el acuse de recibo de los datos, se elimina el segmento de la cola. Si no se recibe el acuse de recibo antes de que el temporizador venza, el segmento es retransmitido.
Los hosts actuales también suelen emplear una función opcional llamada Acuses de recibo selectivos. Si ambos hosts admiten el Acuse de recibo selectivo, es posible que el destino reconozca los bytes de segmentos discontinuos y el host sólo necesitará retransmitir los datos perdidos.

Ver animación apartado 4.3.3.

9.5 Control de flujo

TCP también provee mecanismos para el control del flujo. El control del flujo contribuye con la confiabilidad de la transmisión TCP ajustando la tasa efectiva de flujo de datos entre los dos servicios de la sesión. El campo Tamaño de la ventana en el encabezado TCP especifica la cantidad de datos que puede transmitirse antes de que se reciba el acuse de recibo. El tamaño de la ventana inicial se determina durante el comienzo de la sesión a través del enlace de tres vías. El mecanismo de retroalimentación de TCP ajusta

la tasa de transmisión de datos efectiva al flujo máximo que la red y el dispositivo de destino pueden soportar sin sufrir pérdidas.

9.5.1 Ejemplo

El tamaño de la ventana inicial para una sesión TCP representada se establece en 3000 bytes. Cuando el emisor transmite 3000 bytes, espera por un acuse de recibo de los mismos antes de transmitir más segmentos para esta sesión. Una vez que el emisor ha recibido este acuse de recibo del receptor, ya puede transmitir 3000 bytes adicionales.

9.5.2 Reducción del tamaño de la ventana

Otra forma de controlar el flujo de datos es utilizar tamaños dinámicos de ventana. Cuando los recursos de la red son limitados, TCP puede reducir el tamaño de la ventana para lograr que los segmentos recibidos sean reconocidos con mayor frecuencia. Esto disminuye de manera efectiva la tasa de transmisión, ya que el origen espera que los datos sean recibidos con más frecuencia.

El host receptor TCP envía el valor del tamaño de la ventana al TCP emisor para indicar el número de bytes que está preparado para recibir como parte de la sesión. Si el destino necesita disminuir la tasa de comunicación debido a limitaciones de memoria del búfer, puede enviar un valor de tamaño de la ventanamenor al origen como parte de un acuse de recibo.

9.5.2.1. Ejemplo

Si un host de recepción sufre una congestión, puede responder al host emisor con un segmento con el tamaño de la ventana reducido. En este gráfico, se produjo la pérdida de uno de los segmentos.
El receptor cambió el campo ventana en el encabezado de los mensajes devueltos en esta conversación de 3000 a 1500. Esto hizo que el emisor redujera el tamaño de la ventana a 1500.

Después de períodos de transmisión sin pérdidas de datos o recursos limitados, el receptor comenzará a aumentar el tamaño de la ventana. Esto reduce la sobrecarga de la red, ya que se requiere enviar menos acuses de recibo.
El tamaño de la ventana continuará aumentando hasta que haya pérdida de datos, lo que producirá una disminución del tamaño de la ventana. Estas disminuciones y aumentos dinámicos del tamaño de la ventana representan un proceso continuo en TCP, que determina el tamaño de la ventana óptimo para cada sesión TCP.
En redes altamente eficientes, los tamaños de la ventana pueden ser muy grandes porque no se pierden datos. En redes donde se está estresando la infraestructura subyacente, el tamaño de la ventana probablemente permanecerá pequeño.

10. Protocolo UDP

UDP es un protocolo simple que provee las funciones básicas de la capa de Transporte.
Genera mucho menos sobrecarga que TCP, ya que no es orientado a la conexión y no cuenta con los sofisticados mecanismos de retransmisión, secuenciación y control del flujo. Pese a que es relativamente baja la cantidad total de tráfico UDP que puede

encontrarse en una red típica, entre los protocolos principales de la capa de Aplicación que utilizan UDP se incluyen:

sistema de denominación de dominio (DNS),
protocolo simple de administración de red (SNMP),
protocolo de configuración dinámica de host (DHCP),
protocolo de información de enrutamiento (RIP),
protocolo trivial de transferencia de archivos (TFTP), y
juegos en línea.

Algunas aplicaciones como los juegos en línea o VoIP pueden tolerar algunas pérdida de datos. Si estas aplicaciones utilizaran TCP, experimentarían largas demoras, ya que TCP detecta la pérdida de datos y los retransmite. Estas demoras serían más perjudiciales para la aplicación que las pequeñas pérdidas de datos.
La baja sobrecarga de UDP lo hacen deseable para dichas aplicaciones.

10.1 Reensamblaje de datagramas UDP

Ya que UDP opera sin conexión, las sesiones no se establecen antes de que se lleve a cabo la comunicación, como sucede con TCP. Se dice que UDP es basado en transacciones. En otras palabras, cuando una aplicación posee datos para enviar, simplemente los envía.

Muchas aplicaciones que utilizan UDP envían pequeñas cantidades de datos que pueden ocupar un segmento. Sin embargo, algunas aplicaciones enviarán cantidades mayores de datosque deben dividirse en varios segmentos.
La PDU de UDP se conoce como datagrama, pese a que los términos segmento y datagrama a veces se utilizan de manera indistinta para describir una PDU de la capa de Transporte.

Cuando se envían múltiples datagramas a un destino, los mismos pueden tomar rutas distintas y llegar en el orden incorrecto. UDP no mantiene un seguimiento de los números de secuencia de la manera en que lo hace TCP. UDP no puede reordenar los datagramas en el orden de la transmisión. Por lo tanto, UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación.

10.2 Procesos y solicitudes del servidor UDP

Al igual que las aplicaciones basadas en TCP, a las aplicaciones de servidor basadas en UDP se les asigna números de puerto bien conocidos o registrados. Cuando UDP recibe un datagrama destinado a uno de esos puertos, envíalos datos de aplicación a la aplicación adecuada en base a su número de puerto.

10.3 Procesos del cliente UDP

Como en TCP, la comunicación cliente/servidor se inicia por una aplicación cliente que solicita datos de un proceso del servidor. El proceso de cliente UDP selecciona al azar un número de puerto del rango dinámico de números de puerto y lo utiliza como puerto de origen para la conversación. El puerto de destino por lo general será el número de puerto bien conocido o registrado asignado al proceso del servidor.

Ya que no se crean sesiones con UDP, tan pronto como los datos están listos para ser enviados y los puertos estén identificados, UDP puede formar el datagrama y enviarlo a la capa de Red para direccionamiento y envío a la red. Cabe recordar que una vez que el cliente ha elegido los puertos de origen y destino, estos mismos puertos se utilizarán en el encabezado de todos los datagramas que se utilicen en la transacción.
Para la devolución de datos del servidor al cliente, se invierten los números de puerto de origen y destino en el encabezado del datagrama.

Ver animación 4.4.4 y actividad 4.4.4ver trazas
Actividades
Actividad 4.5.3 ver trazas
Actividad 4.6.1
Examen Tema 4 CISCO

TEMA 7 Nivel de Aplicación

1. Introducción

La capa de Aplicación, Capa siete, es la capa superior de los modelos OSI y TCP/IP. Proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino.

Ver animación 3.1.1

2. Software de la capa de Aplicación

Cuando abrimos un explorador Web o una ventana de mensajería instantánea, se inicia una aplicación, y el programa se coloca en la memoria del dispositivo donde se ejecuta. Cada programa ejecutable cargado a un dispositivo se denomina proceso. Dentro de la capa de Aplicación, existen dos formas de procesos o programas de software que proporcionan acceso a la red: aplicaciones y servicios.

2.1 Aplicaciones reconocidas por la red

Aplicaciones son los programas de software que utiliza la gente para comunicarse a través de la red. Algunas aplicaciones de usuario final son compatibles con la red, lo cual significa que implementan los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores del stack de protocolos. Los clientes de correo electrónico y los exploradoresWeb son ejemplos de este tipo de aplicaciones.

2.2 Servicios de la capa de aplicación

Otros programas pueden necesitar la ayuda de los servicios de la capa de Aplicación para utilizar los recursos de la red, como la cola de impresión en red. Aunque son transparentes para el usuario, estos servicios son los programas que se comunican con la

red y preparan los datos para la transferencia. Diferentes tipos de datos, ya sea texto, gráfico o vídeo, requieren de diversos servicios de red para asegurarse de que estén bien preparados para procesar las funciones de las capas inferiores del modelo OSI. Cada servicio de red o aplicación utiliza protocolos que definen los estándares y formatos de datos a utilizarse. Sin protocolos, la red de datos no tendría una manera común de formatear y direccionar los datos.

3. Aplicaciones, servicios y protocolos

La capa de Aplicación utiliza los protocolos implementados dentro de las aplicaciones y servicios. Mientras que las aplicaciones proporcionan a las personas una forma de crear mensajes y los servicios de la capa de aplicación establecen una interfaz con la red, los protocolos proporcionan las reglas y los formatos que regulan el tratamiento de los datos. Un único programa ejecutable puede utilizar los tres componentes e inclusive el mismo nombre.

Por ejemplo: cuando analizamos "Telnet" nos podemos referir a la aplicación, el servicio o el protocolo.
Ver animación 3.1.3

4. Funciones de los protocolos

Los protocolos de la capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación. Para que las comunicaciones sean exitosas, deben coincidir los protocolos de capa de aplicación implementados en el host de origen y destino. Los protocolos establecen reglas consistentes para intercambiar datos entre las aplicaciones y los servicios cargados en los dispositivos participantes.
Los protocolos especifican cómo se estructuran los datos dentro de los mensajes y los tipos de mensajes que se envían entre origen y destino. Estos mensajes pueden ser solicitudes de servicios, acuses de recibo, mensajes de datos, mensajes de estado o mensajes de error.

5. El modelo cliente-servidor

Cuando la gente intenta acceder a información en sus dispositivos conectados a la red, los datos pueden no estar físicamente almacenados en sus dispositivos.

Si así fuere, se debe solicitar al dispositivo que contiene los datos, permiso para acceder a esa información. En el modelo cliente-servidor, el dispositivo que solicita información se denomina cliente y el dispositivo que responde a la solicitud se denomina servidor. El cliente comienza el intercambio solicitando los datos al servidor, que responde enviando uno o más streams de datos al cliente.

Los protocolos de capa de Aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores. Un ejemplo de una red cliente/servidor es un entorno corporativo donde los empleados utilizan un servidor de e-mail de la empresa para enviar,

recibir y almacenar e-mails. El cliente de correo electrónico en la computadora de un empleado emite una solicitud al servidor de e-mail para un mensaje no leído. El servidor responde enviando el e-mail solicitado al cliente.
Aunque los datos generalmente se describen como un flujo del servidor al cliente, algunos datos siempre fluyen del cliente al servidor.

Por ejemplo, un cliente puede transferir un archivo al servidor con fines de almacenamiento.

La transferencia de datos de un cliente a un servidor se conoce como subida y la de los datos de un servidor a un cliente, descarga.

5.1 Servidor

En un contexto general de redes, cualquier dispositivo que responde a una solicitud de aplicaciones de cliente funciona como un servidor. Un servidor generalmente es una computadora que contiene información para ser compartida con muchos sistemas de cliente. Por ejemplo, páginas Web, documentos, bases de datos, imágenes, archivos de audio y vídeo pueden almacenarse en un servidor y enviarse a los clientes que lo solicitan.

En otros casos, como una impresora de red, el servidor de impresión envía las solicitudes de impresión del cliente a la impresora específica. Algunos servidores pueden requerir de autenticación de la información de cuenta del usuario para verificar si el usuario tiene permiso para acceder a los datos solicitados o para utilizar una operación en particular.

Dichos servidores deben contar con una lista central de cuentas de usuarios y autorizaciones, o permisos (para operaciones y acceso a datos) otorgados a cada usuario.

Cuando se utiliza un cliente FTP, por ejemplo, si usted solicita subir datos al servidor FTP, se le puede dar permiso para escribir su carpeta personal pero no para leer otros archivos del sitio. En una red cliente-servidor, el servidor ejecuta un servicio o proceso, a veces denominado daemon de servidor.
Al igual que la mayoría de los servicios, los daemons generalmente se ejecutan en segundo plano y no se encuentran bajo control directo del usuario.

Los daemons se describen como servidores que "escuchan" una solicitud del cliente, porque están programados para responder cada vez que el servidor recibe una solicitud para el servicio proporcionado por el daemon.

Cuando un daemon "escucha" una solicitud de un cliente, intercambia los mensajes adecuados con el cliente, según lo requerido por su protocolo, y procede a enviar los datos solicitados al cliente en el formato correspondiente.

Actividad 3.2.3 ver trazas

6. Redes P2P: modelo punto a punto

Además del modelo cliente/servidor para redes, existe también un modelo punto a punto.

Las redes punto a punto tienen dos formas distintivas:
Diseño de redes punto a punto
Aplicaciones punto a punto (P2P).

6.1 Redes entre pares

En una red entre pares, dos o más computadoras están conectadas a través de una red y pueden compartir recursos (por ejemplo, impresora y archivos) sin tener un servidor dedicado. Cada dispositivo final conectado (conocido como punto) puede funcionar como un servidor o como un cliente.

Una computadora puede asumir el rol de servidor para una transacción mientras funciona en forma simultánea como cliente para otra transacción.

Un ejemplo de una red entre pares es una simple red doméstica con dos computadoras conectadas que comparten una impresora. Cada persona puede configurar su computadora para compartir archivos, habilitar juegos en red o compartir una conexión de Internet.

A diferencia del modelo cliente/servidor, que utiliza servidores dedicados, las redes punto a punto descentralizan los recursos en una red. En lugar de ubicar información para compartir en los servidores dedicados, la información puede colocarse en cualquier parte de un dispositivo conectado.

6.2 Aplicaciones punto a punto

Una aplicación punto a punto (P2P), a diferencia de una red punto a punto, permite a un dispositivo actuar como cliente o como servidor dentro de la misma comunicación. En este modelo, cada cliente es un servidor y cada servidor es un cliente.Ambos pueden iniciar una comunicación y se consideran iguales en el proceso de comunicación.

Sin embargo, las aplicaciones punto a punto requieren que cada dispositivo final proporcione una interfaz de usuario y ejecute un servicio en segundo plano.

Cuando inicia una aplicación punto a punto específica, ésta invoca la interfaz de usuario requerida y los servicios en segundo plano. Luego, los dispositivos pueden comunicarse directamente.

Las aplicaciones punto a punto pueden utilizarse en las redes punto a punto, en redes cliente/servidor y en Internet.

7. Protocolos

Entre los protocolosmás conocidos de la capa de aplicación destacan:

1. **Sistema de nombres de dominio (DNS): puerto TCP/UDP 53.**
2. **Protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol): puerto TCP 80.**

3. **Protocolo simple de transferencia de correo (SMTP, Simple Mail Transfer Protocol): puerto TCP 25.**
4. **Protocolo de oficina de correos (POP): puerto UDP 110.**
5. **Telnet: puerto TCP 23.**
6. **Protocolo de configuración dinámica de host (DHCP): puerto UDP 67.**
7. **Protocolo de transferencia de archivos (FTP, File Transfer Protocol): puertos TCP 20 y 21.**

7.1 DHCP

El servicio Protocolo de configuración dinámica de host (DHCP) permite a los dispositivos de una red obtener direcciones IP y demás información de un servidor DHCP.

Este servicio automatiza la asignación de direcciones IP, máscaras de subred, gateways y otros parámetros de redes IP. DHCP permite a un host obtener una dirección IP en forma dinámica cuando se conecta a la red. Se realiza el contacto con el servidor de DHCP y se solicita una dirección.

El servidor DHCP elije una dirección de un rango configurado de direcciones denominado "pool" y se la asigna ("alquila") al host por un período establecido. Las direcciones de DHCP distribuidas no se asignan a los hosts en forma permanente, sólo se alquilan durante un período de tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse.

Cuando un dispositivo configurado por DHCP se inicia o conecta a la red, el cliente envía un paquete DESCUBRIMIENTO de DHCP para identificar cualquier servidor de DHCP disponible en la red.

Un servidor DHCP contesta con una OFERTA de DHCP, que es un mensaje de oferta de alquiler con información asignada de dirección IP, máscara de subred, servidor DNS y gateway por defecto, como también la duración del alquiler.

El cliente puede recibir varios paquetes de oferta de DHCP si hay más de un servidor DHCP en la red local, por lo tanto debe escoger entre ellos y enviar un broadcast de paquete con una solicitud de DHCP que identifique el servidor y la oferta de alquiler específicos que el cliente está aceptando.

Teniendo en cuenta que la dirección IP solicitada por el cliente u ofrecida por el servidor, aún es válida, el servidor devolverá un mensaje ACK DHCP que le informa al cliente que se aceptó el alquiler.

Si la oferta ya no es válida, quizás debido al tiempo o que a otro cliente se le asignó el alquiler, el servidor seleccionado responderá con un mensaje NACK DHCP (acuse de recibo negativo).

Si se envía un mensaje NACK DHCP, el proceso de selección debe comenzar nuevamente con la transmisión de un nuevo mensaje DHCP DISCOVER.

Una vez que el cliente tenga el alquiler, debe renovarse antes de la expiración del alquiler por medio de otro mensaje DHCP REQUEST.

Tema 8 Configuración de dispositivos de interconexión

1. Introducción

Al igual que una computadora personal, un router o switch no puede funcionar sin un sistema operativo. Sin un sistema operativo, el hardware no puede realizar ninguna función. **El sistema operativo Internetwork (IOS) de Cisco es el software del sistema en la mayoría de los mdispositivos Cisco,** independientemente del tamaño o tipo de dispositivo. Se usa en routers, switches LAN, pequeños puntos de acceso inalámbricos, grandes routers con decenas de interfaces y muchos otros dispositivos.

Se tiene acceso a los servicios que proporciona el IOS de Cisco **mediante una Interfaz de línea de comandos (CLI)**. El archivo IOS en sí tiene un tamaño de varios megabytes y se encuentra en un área de memoria semipermanente llamada flash.

La memoria flash provee almacenamiento no volátil. Esto significa que los contenidos de la memoria no se pierden cuando el dispositivo se apaga. El IOS se copia en la RAM cuando se enciende el dispositivo y el IOS se ejecuta desde la RAM cuando el dispositivo está funcionando. Esta función mejora el rendimiento del dispositivo.

2. Métodos de acceso

Existen varias formas de acceder al entorno de la CLI.
Los métodos más comunes son:
Consola
Telnet o SSH
Puerto auxiliar

2.1 Consola

Se puede tener acceso a la CLI a través de una sesión de consola, también denominada línea CTY. La consola usa una conexión serial de baja velocidad para conectar directamente un equipo o un terminal al puerto de consola en el router o switch. El puerto de consola es un puerto de administración que provee acceso al router.

El puerto de consola se suele utilizar para tener acceso a un dispositivo cuando no se han iniciado o han fallado los servicios de networking. Ejemplos del uso de la consola son:

La configuración de inicio del dispositivo de red.

Procedimientos de recuperación de desastres y resolución de problemas donde no es posible el acceso remoto.

Procedimientos de recuperación de contraseña.

2.2 Telnet y SSH

Un método que sirve para acceder en forma remota a la sesión CLI es hacer telnet al router. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de networking activos en el dispositivo. El dispositivo de red debe tener configurada por lo menos una interfaz activa con una dirección de Capa 3, como por ejemplo una dirección IPv4.
Un host con un cliente Telnet puede acceder a las sesiones vty que se ejecutan en el dispositivo Cisco. Por razones de seguridad, el IOS requiere que la sesión Telnet use una contraseña, comométodomínimo de autenticación.
El Secure Shell protocol (SSH) es un método que ofrece más seguridad en el acceso al dispositivo remoto. Este protocolo provee la estructura para una conexión remota similar a Telnet, salvo que utiliza servicios de red más seguros.

2.3 Auxiliar

Otra manera de establecer una sesión CLI en forma remota es a través de una conexión de marcado telefónico mediante un módem conectado al puerto auxiliar del router.

De manera similar a la conexión de consola, este método no requiere ningún servicio de networking para configurarlo o activarlo en el dispositivo. Generalmente, en la única oportunidad que el puerto auxiliar se usa en forma local en lugar del puerto de consola es cuando surgen problemas en el uso del puerto de consola.

2.4 Formas de acceso

3. Archivos de configuración

Los dispositivos de red dependen de dos tipos de software para su funcionamiento: el sistema operativo y la configuración. Los archivos de configuración contienen los comandos del software IOSde Cisco utilizados para personalizar la funcionalidad de un dispositivo Cisco.
Los comandos son analizados (traducidos y ejecutados) por el software IOS de Cisco cuando inicia el sistema (desde el archivo startup-config) o cuando se ingresan los comandos en la CLI mientras está en modo configuración.

El administrador de red crea una configuración que define la funcionalidad deseada del dispositivo Cisco.

3.1 Tipos de archivos de configuración

Un dispositivo de red Cisco contiene dos archivos de configuración: El archivo de configuración de inicio, utilizado como la configuración de respaldo, se carga al iniciar el dispositivo El archivo de configuración en ejecución, utilizado durante la operación actual del dispositivo

3.1.1 Archivo de configuración de inicio

El archivo de configuración de inicio (startup-config) se usa durante el inicio del sistema para configurar el dispositivo. El archivo de configuración de inicio o el archivo startup-config se almacena en la RAM no volátil (NVRAM).

Como la NVRAM es no volátil, el archivo permanece intacto cuando el dispositivo Cisco se apaga. Los archivos startup-config se cargan en la RAM cada vez que se inicia o se vuelve a cargar el router. Una vez que se ha cargado el archivo de configuración en la RAM, se considera la configuración en ejecución o running-config.

3.1.2 Configuración en ejecución

Una vez en la RAM, esta configuración se utiliza para operar el dispositivo de red. La configuración en ejecución se modifica cuando el administrador de red realiza la configuración del dispositivo. Los cambios en la configuración en ejecución afectarán la operación del dispositivo Cisco en forma inmediata.
Luego de realizar los cambios necesarios, el administrador tiene la opción de guardar tales cambios en el archivo startup-config, de manera que se utilicen la próxima vez que se reinicie el dispositivo. Como el archivo de configuración en ejecución se encuentra en la RAM, se pierde si se apaga la energía que alimenta al dispositivo o si se reinicia el dispositivo.

También se perderán los cambios realizados en el archivo running-config si no se guardan en el archivo startup-config antes de apagar el dispositivo.

3.1.3 Esquema archivos de configuración

4. Modelo CISCO IOS

El Cisco IOS está diseñado como un sistema operativomodal. El término modal describe un sistema en el que hay distintos modos de operación, cada uno con su propio dominio de operación.

En orden descendente, los principales modos son:

1. **Modo de ejecución usuario**
2. **Modo de ejecución privilegiado**
3. **Modo de configuración global**
4. **Otros modos de configuración específicos**

Cada modo se utiliza para cumplir determinadas tareas y tiene un conjunto específico de comandos que se encuentran disponibles cuando el modo está habilitado.

Por ejemplo, para configurar una interfaz del router, el usuario debe ingresar al modo de configuración de interfaces.

4. Modelo CISCO IOS

5. Peticiones de entrada de comando

Cuando se usa la CLI, el modo se identifica mediante la petición de entrada de línea de comandos que es exclusiva de ese modo. La petición de entrada está compuesta por las palabras y los símbolos en la línea a la izquierda del área de entrada. Se usa la frase petición de entrada porque el sistema le solicita que ejecute una entrada.

De manera predeterminada, cada petición de entrada empieza con el nombre del dispositivo. Después del nombre, el resto de la petición de entrada indica el modo.

Por ejemplo: la petición de entrada por defecto para el modo de configuración global en un router sería: Router(config)#

Como se utilizan comandos y cambian los modos, la petición de entrada cambia para reflejar el contexto actual.

6. Modos principales

Los dos modos de operación principales son:

- **EXEC del usuario**
- **EXEC privilegiado**

Cada modo tiene comandos similares. Sin embargo, el modo EXEC privilegiado tiene un nivel de autoridad superior en cuanto a lo que permite que se ejecute.

6.1 Modo de ejecución usuario

El modo de ejecución usuario o, para abreviar, EXEC del usuario, tiene capacidades limitadas pero resulta útil en el caso de algunas operaciones básicas. Este modo es la primera entrada en la CLI de un router IOS. El modo EXEC usuario permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo de visualización solamente.

El nivel EXEC usuario no permite la ejecución de ningún comando que podría cambiar la configuración del dispositivo. El modo EXEC usuario se puede reconocer por la petición de entrada de la CLI que termina con el símbolo >.
Este es un ejemplo que muestra el símbolo > en la petición de entrada:
Switch>

6.2 Modo EXEC privilegiado

La ejecución de comandos de configuración y administración requiere que el administrador de red use el modo EXEC privilegiado.

El modo EXEC privilegiado se puede reconocer por la petición de entrada que termina con el símbolo #.

Switch#

6.3 Intercambio entre los modos EXEC usuario y EXEC privilegiado

Los comandos enable y disable se usan para cambiar la CLI entre el modo EXEC usuario y el modo EXEC privilegiado, respectivamente. Para acceder al modo EXEC privilegiado, use el comando enable. La sintaxis para ingresar el comando enable es:

Router>enable

Cuando se presiona <Intro>, la petición de entrada del router cambia a: Router#
El símbolo # al final de la petición indica que el router está ahora en modo EXEC privilegiado. Si se ha configurado la autenticación de la contraseña para el modo EXEC privilegiado, el IOS pide la contraseña.

El comando disable se usa para volver del modo EXEC privilegiado al modo EXEC del usuario. Por ejemplo:
Router#disable
Router>

7. Estructura básica de comandos de IOS

Cada comando de IOS tiene un formato o sintaxis específicos y se ejecuta con la petición de entrada correspondiente. La sintaxis general para un comando es el comando seguido de las palabras clave y los argumentos correspondientes.

El comando es la palabra o las palabras iniciales ingresadas en la línea de comandos. Los comandos no distinguen mayúsculas de minúsculas. A continuación del comando siguen una o más palabras clave y argumentos. Las palabras clave describen parámetros específicos al intérprete de comandos. Por ejemplo, el comando show se usa para mostrar información sobre el dispositivo.

7. Estructura básica de comandos de IOS

Este comando tiene varias palabras clave que pueden usarse para definir el resultado particular que se mostrará. Por ejemplo:
Switch#show running-config

El comando show va seguido de la palabra clave running-config. La palabra clave especifica que, como resultado, se mostrará la configuración en ejecución. Un comando puede requerir uno o más argumentos. A diferencia de unapalabra clave, generalmente un argumento no es una palabra predefinida.

Un argumento es un valor o una variable definida por el usuario.

Como ejemplo, cuando se solicita una descripción a una interfaz con el comando description, se debe ingresar una línea de estas características:

Switch(config-if)#description MainHQ Office Switch
El comando es: description.
El argumento es: MainHQ Office Switch.
El usuario define el argumento. Para este comando, el argumento puede ser cualquier cadena de texto con un máximo de 80 caracteres.

Después de ingresar cada comando completo, incluso cualquier palabra clave y argumento, presione la tecla <Intro> para enviar el comando al intérprete de comandos.

8. Uso de la ayuda de la CLI

El IOS ofrece varias formas de ayuda: Ayuda sensible al contexto: proporciona una lista de comandos y los argumentos asociados con esos comandos dentro del contexto del modo actual. Para acceder a la ayuda contextual, ingrese un signo de interrogación (?) ante cualquier petición de entrada. Habrá una respuesta inmediata sin necesidad de usar la tecla <Intro>.

Otro de los usos de la ayuda contextual es para visualizar una lista de los comandos o palabras clave que empiezan con uno o varios caracteres específicos. Después de ingresar una secuencia de caracteres, si inmediatamente se ingresa un signo de interrogación, sin espacio, el IOS mostrará una lista de comandos o palabras clave para este contexto que comienzan con los caracteres ingresados.

Por ejemplo, ingrese sh? para obtener una lista de los comandos que empiezan con la secuencia de caracteres sh.

Un último tipo de ayuda contextual se utiliza para determinar qué opciones,palabras clave o argumentos concuerdan con un comando específico. Cuando ingresa un comando, escriba un espacio seguido de ? para determinar qué puede o debe ingresarse a continuación.

Verificación de la sintaxis del comando: Cuando se envía un comando al presionar la tecla <Intro>, el intérprete de la línea de comandos analiza al comando de izquierda a derecha para determinar qué acción se está solicitando. El IOS generalmente provee sólo comentarios negativos. Si el intérprete comprende el comando, la acción requerida se ejecuta y la CLI vuelve a la petición de entrada correspondiente. Sin embargo, si el intérprete no puede comprender el comando que se ingresa, mostrará un comentario que describe el error del comando.

Existen tres tipos diferentes de mensajes de error:
Comando ambiguo
Comando incompleto
Comando incorrecto

Teclas de acceso rápido y accesos directos: La interfaz de línea de comandos IOS provee teclas de acceso rápido y métodos abreviados que facilitan la configuración, el monitoreo y la resolución de problemas:

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 abajo: Permite al usuario desplazarse hacia adelante a través los comandos anteriores

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

Ctrl-Shift-6: Permite al usuario interrumpir un proceso IOS, como ping o traceroute

Ctrl-C: Cancela el comando actual y sale del modo de configuración

9. Comandos de análisis de IOS

Para verificar y resolver problemas en la operación de la red, debemos examinar la operación de los dispositivos. El comando básico de examen es el comando show. La figura muestra cómo el típico comando show puede proveer información sobre la configuración, la operación y el estado de partes de un router Cisco.
Algunos de los comandos usados con más frecuencia son:

show interfaces Muestra estadísticas de todas las interfaces del dispositivo. Para ver las estadísticas de una interfaz específica, ejecute el comando show interfaces seguido del número de puerto/ranura de la interfaz específica. Por ejemplo:
Router#show interfaces serial 0/0/1

showversion Muestra información sobre la versión de software actualmente cargada, además de información de hardware y del dispositivo.

showarp: 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 enejecución o la configuración para una interfaz específica o información de clase de mapa.

show ip interfaces: Muestra las estadísticas IPv4 para todas lasinterfaces de un router. Para ver las estadísticas de una interfazespecífica, ejecute el comando show ip interfaces seguido delnúmero de puerto/ranura de la interfaz específica. Otro formatoimportante de este comando es show ip interface brief. Es útil para obtener un resumen rápido de las interfaces y su estado operativo.

10. La petición de entrada *more*

Cuando un comando devuelve más resultados de los que pueden mostrarse en una única pantalla, aparece la petición de entrada —Más-- en la parte inferior de la pantalla. Cuando aparece la petición de entrada --More--, presione la barra espaciadora para visualizar el tramo siguiente del resultado.

Para visualizar sólo la siguiente línea, presione la tecla Intro. Si se presiona cualquier otra tecla, se cancela el resultado y se vuelve a la petición de entrada.

11. Modos de configuración de IOS

El modo de configuración principal recibe el nombre de configuración global o global config. Desde configuración global, se realizan cambios en la configuración de la CLI que afectan la operación del dispositivo en su totalidad.

El siguiente comando de la CLI se usa para cambiar el dispositivo del modo EXEC privilegiado al modo de configuración global y para permitir la entrada de comandos de configuración desde una terminal:

Router#configure terminal

Una vez que se ejecuta el comando, la petición de entrada cambia para mostrar que el router está en modo de configuración global. Router(config)#
Desde el modo de configuración global, pueden ingresarse a muchos modos de configuración diferentes. Cada uno de estos modos permite la configuración de una parte o función específica del dispositivo IOS.
La lista que se presenta a continuación muestra algunos de ellos:

Modo de interfaz: para configurar una de las interfaces de red (Fa0/0, S0/0/0, etc.)
Modo de línea: para configurar una de las líneas (física o virtual) (consola,,auxiliar, VTY, etc.).
Modo de router: para configurar los parámetros de uno de los protocolos de enrutamiento

Para salir de un modo de configuración específico y volver al modo de configuración global, ingrese exit ante la petición de entrada. Para salir completamente del modo de configuración y volver al modo EXEC privilegiado, ingrese end o use la secuencia de teclas Ctrl-Z.

Cuando se ha realizado un cambio desde el modo global, conviene guardarlo en el archivo de configuración de inicio almacenado en la NVRAM. Así se evita que los cambios se pierdan por cortes de energía o un reinicio intencional.
El comando para guardar la configuración en ejecución en el archivo de configuración de inicio es:

Router#copy running-config startup-config

12. Los dispositivos necesitan nombres

El nombre de host se usa en las peticiones de entrada de la CLI. Si el nombre de host no está explícitamente configurado, el router usa el nombre de host predeterminado, asignado de fábrica, "Router".

El switch tiene el nombre de host predeterminado, asignado de fábrica, “Switch". Imagine que una internetwork tiene varios routers y todos recibieron el nombre predeterminado "Router". Se crearía una importante confusión durante la configuración y el mantenimiento

de la red. Cuando se accede a un dispositivo remoto con Telnet o SSH, es importante tener la confirmación de que se ha hecho una conexión al dispositivo adecuado.

Si todos los dispositivos quedaran con sus nombres predeterminados, no se podría identificar que el dispositivo correcto esté conectado.

Al elegir y documentar nombres atinadamente, resulta más fácil recordar, analizar e identificar dispositivos de red. Para nombrar los dispositivos de manera uniforme y provechosa, es necesario el establecimiento de una convención de denominación que se extienda por toda la empresa. Siempre conviene crear la convención de denominación al mismo tiempo que el esquema de direccionamiento para permitir la continuidad dentro de la organización.

Según ciertas pautas de convenciones de denominación, los nombres deberían:
Comenzar con una letra.
No debe incluirse ningún espacio.
Finalizar con una letra o dígito.
Sólo deben incluirse caracteres que sean letras, dígitos y guiones.
Tener 63 caracteres o menos.

12.1 Configuración del nombre de host de IOS

Desde el modo EXEC privilegiado, acceda al modo de configuración global ingresando el comando configure terminal (configurar terminal):

Router#configure terminal

Después de que se ejecuta el comando, la petición de entrada cambiará a: Router(config)#

En el modo global, ingrese el nombre de host:
Router(config)#hostname AtlantaHQ

Después de ejecutar ese comando, la petición de entrada cambiará a: AtlantaHQ(config)#
Observe que el nombre de host aparece en la petición de entrada.

Para anular los efectos de un comando, establezca el prefacio del comando con la palabra clave no. Por ejemplo: para eliminar el nombre de un dispositivo, utilice:
AtlantaHQ(config)# no hostname
Router(config)#

Nótese que el comando no hostname provoca que el router vuelva a usar el nombre de host por defecto, “Router."

12.2 Actividad
Actividad 11.1.6
Actividad 11.1.7
Actividad 11.2.1

13. Configuración, contraseñas y uso de mensajes

La limitación física del acceso a los dispositivos de red con armarios o bastidores con llave resulta una buena práctica; sin embargo, las contraseñas son la principal defensa contra el acceso no autorizado a los dispositivos de red. Cada dispositivo debe tener contraseñas configuradas a nivel local para limitar el acceso.

Como se comentó anteriormente, el IOS usa modos jerárquicos para colaborar con la seguridad del dispositivo. Como parte de este cumplimiento de seguridad, el IOS puede aceptar diversas contraseñas para permitir diferentes privilegios de acceso al dispositivo.

Las contraseñas ingresadas son:

Contraseña de consola: limita el acceso de los dispositivos mediante la conexión de consola

Contraseña de enable: limita el acceso al modo EXEC privilegiado

Contraseña enable secret: encriptada, limita el acceso del modo EXEC privilegiado

Contraseña de VTY: limita el acceso de los dispositivos que utilizan Telnet

Siempre conviene utilizar contraseñas de autenticación diferentes para cada uno de estos niveles de acceso. Si bien no es práctico iniciar sesión con varias contraseñas diferentes, es una precaución necesaria para proteger adecuadamente la infraestructura de la red ante accesos no autorizados. Además, utilice contraseñas seguras que no se descubran fácilmente. El uso de contraseñas simples o fáciles de adivinar continúa siendo un problema de seguridad en muchas facetas del mundo empresarial.

Considere estos puntos clave cuando elija contraseñas:

Use contraseñas que tengan más de 8 caracteres.
Use en las contraseñas una combinación de secuencias de letras mayúsculas y minúsculas o numéricas.

Evite el uso de la misma contraseña para todos los dispositivos.

Evite el uso de palabras comunes como contraseña o administrador, porque se descubren fácilmente.

13.1 Contraseña de consola

El puerto de consola de un dispositivo Cisco IOS tiene privilegios especiales. El puerto de consola de dispositivos de red debe estar asegurado, comomínimo, mediante el pedido de una contraseña segura al usuario. Así se reducen las posibilidades de que personal no autorizado conecte físicamente un cable al dispositivo y obtenga acceso a éste.

Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola:

```
Switch(config)#line console 0
Switch(config-line)#password password
Switch(config-line)#login
```

Desde el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea para la consola.
El cero se utiliza para representar la primera (y, en la mayoría de los casos, la única) interfaz de consola para un router. El segundo comando, password password especifica una contraseña en una línea. El comando login configura al router para que pida la autenticación al iniciar sesión.

Cuando el login está habilitado y se ha configurado una contraseña, habrá una petición de entrada de una contraseña.

Una vez que se han ejecutado estos tres comandos, aparecerá una petición de entrada de contraseña cada vez que un usuario intente obtener acceso al puerto de consola.

13.2 Contraseña enable y enable secret

Para proporcionar una mayor seguridad, utilice el comando enable password o el comando enable secret.
Puede usarse cualquiera de estos comandos para establecer la autenticación antes de acceder al modo EXEC privilegiado (enable). Si es posible, use siempre el comando enable secret, no el comando anterior enable password. El comando enable secret provee mayor seguridad porque la contraseña está encriptada.

El comando enable password se ejecutaría si el dispositivo usa una versión anterior del software IOS de Cisco que no reconoce el comando enable secret.

Los siguientes comandos se utilizan para configurar las contraseñas:

```
Router(config)#enable password contraseña

Router(config)#enable secret contraseña
```

13.3 Contraseña VTY

Las líneas vty permiten el acceso a un router a través de Telnet. En forma predeterminada, muchos dispositivos Cisco admiten cinco líneas VTY con numeración del 0 al 4. Es necesario configurar una contraseña para todas las líneas voy disponibles. Puede configurarse la misma contraseña para todas las conexiones. Sin embargo, con frecuencia conviene configurar una única contraseña para una línea a fin de proveer un recurso secundario para el ingreso administrativo al dispositivo si las demás conexiones están en uso.

Los siguientes comandos se usan para configurar una contraseña en líneas vty:

```
Router(config)#line vty 0 4
Router(config-line)#password contraseña
Router(config-line)#login
```

Por defecto, el IOS incluye el comando login en las líneas VTY. Esto impide el acceso Telnet al dispositivo sin la previa solicitud de autenticación. Si por error, se configura el comando no login, que elimina el requisito de autenticación, personas no autorizadas podrían conectarse a la línea a través de Telnet. Esto representaría un gran riesgo de seguridad

13.4 Visualización de contraseñas de encriptación

Existe otro comando de utilidad que impide que las contraseñas aparezcan como texto sin cifrar cuando se visualizan los archivos de configuración.

Ese comando es el service password-encryption.

Este comando provee la encriptación de la contraseña cuando ésta se configura. El comando service password encryption aplica una encriptación débil a todas las contraseñas no encriptadas. El propósito de este comando es evitar que individuos no autorizados vean las contraseñas en el archivo de configuración.

Si se ejecuta el comando show running-config o show startup-config antes de ejecutar el comando service password-encryption, las contraseñas no encriptadas estarán visibles en el resultado de configuración.

El comando service password-encryption puede entonces ejecutarse y se aplicará la encriptación a las contraseñas. Una vez que se ha aplicado la encriptación, la cancelación del servicio de encriptación no revierte la encriptación.

13.5 Mensajes de aviso

Aunque el pedido de contraseñas es un modo de impedir el acceso a la red de personas no autorizadas, resulta vital proveer un método para informar que sólo el personal autorizado debe intentar obtener acceso al dispositivo.

El contenido o las palabras exactas de un aviso dependen de las leyes locales y de las políticas de la empresa. A continuación se muestran algunos ejemplos de información que se debe incluir en un aviso:
"El uso del dispositivo es exclusivo del personal autorizado".
"Es posible que se esté controlando la actividad".
"Se aplicarán medidas legales en caso de uso no autorizado."

El IOS provee varios tipos de avisos. 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. El comando banner motd requiere el uso de delimitadores para identificar el contenido del mensaje del aviso.

El comando banner motd va seguido de un espacio y un carácter delimitador. Luego, se ingresan una o más líneas de texto para representar el mensaje del aviso. Una segunda ocurrencia del carácter delimitador denota el final del mensaje. El carácter delimitador

puede ser cualquier carácter siempre que no aparezca en el mensaje. Por este motivo, con frecuencia se usan símbolos tales como “#".

Para configurar un MOTD, ingrese el comando banner motd desde el modo de configuración global:

Switch(config)#banner motd # message #

Una vez que se ha ejecutado el comando, aparecerá el aviso en todos los intentos posteriores de acceso al dispositivo hasta que el aviso se elimine.

13.6 Actividad
Actividad 11.2.2 (4)

14. Administración de archivos de configuración

La modificación de la configuración en ejecución afecta la operación del dispositivo en forma inmediata. Después de hacer cambios en una configuración, considere estas opciones como siguiente paso:
Convertir la configuración cambiada en la nueva configuración de inicio.
Volver a la configuración original del dispositivo.
Eliminar toda la configuración del dispositivo.

14.1 Convertir la configuración cambiada en la nueva configuración de inicio

Ya que la configuración en ejecución se almacena en la RAM, se encuentra temporalmente activa mientras se ejecuta (se encuentra encendido) el dispositivo Cisco. Si se corta la energía al router o si se reinicia el router, se perderán todos los cambios de configuración a menos que se hayan guardado. Al guardar la configuración en ejecución en el archivo de configuración de inicio en la NVRAM se mantienen los cambios como la nueva configuración de inicio.
Utilice el comando copy running-config startup-config en la petición de entrada del modo EXEC privilegiado.
Switch#copy running-config startup-config

Una vez ejecutado, el archivo de configuración en ejecución reemplaza al archivo de configuración de inicio.

14.2 Volver a la configuración inicial del dispositivo

Si los cambios realizados en la configuración en ejecución no tienen el efecto deseado, puede ser necesario volver a la configuración previa del dispositivo.

Suponiendo que no se ha sobreescrito la configuración de inicio con los cambios, se puede reemplazar la configuración en ejecución por la configuración de inicio.

La mejor manera de hacerlo es reiniciando el dispositivo con el comando reload ante la petición de entrada del modo EXEC privilegiado.

Cuando se inicia una recarga, el IOS detectará que la configuración en ejecución tiene cambios que no se guardaron en la configuración de inicio.

Aparecerá una petición de entrada para preguntar si se desean guardar los cambios realizados. Para descartar los cambios, ingrese n o no.

Aparecerá otra petición de entrada para confirmar la recarga. Para confirmar, presione la tecla Intro. Si se presiona cualquier otra tecla, se cancelará el procedimiento. Por ejemplo:

Router#reload
Systemconfiguration has been modified. Save? [yes/no]: n
Proceed with reload? [confirm]
*Apr 13 01:34:15.758: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2004 by cisco Systems, Inc.
Versión PLD 0x10
Versión GIO ASIC 0x127
Procesador c1841 con 131072 KB de memoria principal

La memoria principal se encuentra configurada en modo 64 bits con la paridad deshabilitada

14.3 Eliminar toda la configuración del dispositivo

Si se guardan cambios no deseados en la configuración de inicio, posiblemente sea necesario eliminar todas las configuraciones. Esto requiere borrar la configuración de inicio y reiniciar el dispositivo. La configuración de inicio se elimina con el uso del comando **erase startupconfig.**

Para borrar el archivo de configuración de inicio utilice erase NVRAM:startup-config o erase startup-config en la petición de entrada del modo EXEC privilegiado:
Router#erase startup-config. Una vez que se ejecuta el comando, el router solicitará la confirmación:
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
Confirm es la respuesta predeterminada. Para confirmar y borrar el archivo de configuración de inicio, presione la tecla Intro. Si se presiona cualquier otra tecla, se cancelará el proceso.

14.4 Actividad
Actividad 11.2.3

15. Configuración de interfaces

La Interfaz Ethernet del router se utiliza como gateway para los dispositivos finales en las LAN conectadas directamente al router. Cada Interfaz Ethernet debe contar con una dirección IP y máscara de subred para enrutar los paquetes IP.

Para configurar una interfaz Ethernet, siga estos pasos:
1. Ingrese al modo de configuración global.
2. Ingrese al modo de configuración de interfaz.
3. Especifique la dirección de la interfaz y la máscara de subred.
4. Active la interfaz.

Configure la dirección IP de Ethernet mediante los siguientes comandos:

```
Router(config)#interface FastEthernet 0/0
Router(config-if )#ip address ip_address netmask
Router(config-if )#no shutdown
```

Por defecto, las interfaces se encuentran deshabilitadas. Para habilitar una interfaz, ingrese el comando no shutdown en el modo de configuración de interfaz. Si es necesario desactivar una interfaz por cuestiones de mantenimiento o para resolver problemas, use el comando shutdown.

15.1 Configuración de interfaces seriales

Las interfaces seriales se usan para conectar WAN a routers en un sitio remoto o ISP.

Para configurar una interfaz serial siga estos pasos:
1. Ingrese al modo de configuración global.
2. Ingrese al modo de interfaz.
3. Especifique la dirección de la interfaz y la máscara de subred.
4. Si el cable de conexión es DCE, fije la frecuencia de reloj. Omita este paso si el cable es DTE.
5. Active la interfaz.

Cada interfaz serial conectada debe tener una dirección IP y una máscara de subred para enrutar paquetes IP. Configure la dirección IP con los siguientes comandos:

```
Router(config)#interface Serial 0/0/0
Router(config-if )#ip address ip_address netmask
```

Las interfaces seriales requieren una señal de reloj para controlar la temporización de las comunicaciones. En los enlaces seriales interconectados directamente, como en nuestro entorno de laboratorio, un extremo debe operar como DCE para proporcionar la señal del reloj. Se activa el reloj y la velocidad se especifica con el comando clock rate.
Los comandos que se utilizan para establecer una frecuencia de reloj y habilitar una interfaz serial son:

```
Router(config)#interface Serial 0/0/0
Router(config-if )#clock rate 56000
Router(config-if )#no shutdown
```

15.2 Descripción de interfaces

Así como el nombre del host ayuda a identificar el dispositivo en una red, una descripción de interfaz indica el propósito de la interfaz. Una descripción de lo que una interfaz hace o dónde está conectada debe ser parte de la configuración de cada interfaz. Esta

descripción puede resultar útil para la resolución de problemas. La descripción de interfaz aparecerá en el resultado de estos comandos:
show startup-config, show running-config y show interfaces.

Por ejemplo, esta descripción provee información valiosa sobre el propósito de la interfaz: *Esta interfaz es el gateway para la LAN administrativa.*

Una descripción puede ayudar a determinar los dispositivos o las ubicaciones conectadas a la interfaz. A continuación, se proporciona otro ejemplo: *La interfaz F0/0 está conectada al switch principal en el edificio administrativo.*

Para crear una descripción, utilice el comando **description**. Este ejemplo muestra los comandos utilizados para crear una descripción para una interfaz FastEthernet:

HQ-switch1#configure terminal
HQ-switch1(config)#interface fa0/0
HQ-switch1(config-if)#description Conectarse al switch principal del Edificio A

Una vez que se aplica la descripción a la interfaz, utilice el comando show interfaces para verificar que la descripción sea correcta.

16. Configuración de una interfaz de switch

Un switch LAN es un dispositivo intermediario que interconecta segmentos dentro de una red. Por lo tanto, las interfaces físicas en el switch no tienen direcciones IP. A diferencia de un router en el que las interfaces están conectadas a diferentes redes, una interfaz física en un switch conecta dispositivos dentro de una red.

Las interfaces de switch están habilitadas en forma predeterminada. Podemos asignar descripciones pero no es necesario activar la interfaz. Para poder administrar un switch, se asigna una dirección a una interfaz virtual representada como una interfaz LAN virtual (VLAN). En la mayoría de los casos, esta es la interfaz VLAN 1

Una vez que se asigna la dirección, se accede al switch con telnet, ssh o serviciosWeb.
Al igual que las interfaces físicas de un router, también se debe activar esta interfaz con el comando no shutdown. Como cualquier otro host, el switch necesita una dirección de gateway definida para comunicarse fuera de la red local. Este gateway se asigna con el comando ip default-gateway.

17. Verificación de interfaces de un router

Del mismo modo que se usan comandos y utilidades para verificar la configuración de un host, se deben aprender los comandos para verificar las interfaces de dispositivos intermediarios. El IOS provee comandos para verificar la operación de interfaces de router y switch. Uno de los comandos más utilizados es el comando show ip interface brief. Este proporciona un resultado más abreviado que el comando show ip interface. Ofrece además un resumen de la información clave de todas las interfaces.

Si se observa la figura del Router 1, se puede ver que este resultado muestra todas las interfaces conectadas al router, la dirección IP, si la hay, asignada a cada interfaz y el estado operativo de la interfaz.

Si se observa la línea de la interfaz FastEthernet 0/0, se ve que la dirección IP es 192.168.254.254.
Si se observan las dos últimas columnas, se advierte el estado de la interfaz de Capa 1 y Capa 2. up en la columna de estado muestra que esta interfaz está en funcionamiento en la Capa 1. up en la columna de protocolo señala que el protocolo de Capa 2 está funcionando.
En la misma figura, se observa que la interfaz serial 0/0/1 no ha sido habilitada. La indicación correspondiente es administratively down en la columna de estado.

Esta interfaz puede activarse con el comando no shutdown.

18. Verificación de interfaces de un switch

Al examinar la figura del Switch 1 se puede ver el uso del comando show ip interface brief para verificar la condición de las interfaces del switch. Como se aprendió anteriormente, la dirección IP para el switch se aplica a una interfaz VLAN (Red de área local virtual).

En este caso, se asigna una dirección IP 192.168.254.250 a la interfaz Vlan1. También se puede observar que esta interfaz está activada y en funcionamiento. Al examinar la interfaz FastEthernet0/1, se puede detectar que esta interfaz está desactivada. Esto quiere decir que no hay un dispositivo conectado a la interfaz o que la interfaz de red de los dispositivos conectada no está funcionando.
Por otro lado, los resultados de las interfaces FastEthernet0/2 y FastEthernet0/3 muestran que están en funcionamiento. Esto se indica en el Estado y en el Protocolo, cuando ambos se muestran activos.

19. Conexiones del switch

Una herramienta adicional que puede resultar útil es un mapeo de cómo están conectados los hosts a un switch. Dicho mapeo se puede obtener emitiendo el comando show macaddress-table.
Por medio de una línea de comandos de un switch, ingrese el comando show con el argumento mac-address-table : Sw1-2950#showmac-address-table

20. Prueba del siguiente salto en la ruta

En un router, use el IOS para probar el siguiente salto de las rutas individuales. La tabla de enrutamiento muestra el siguiente salto de cada ruta. Para determinar el siguiente salto, examine la tabla de enrutamiento desde el resultado del comando show ip route.
Los paquetes que trasladan tramas y que se dirigen a la red destino indicada en la tabla de enrutamiento se envían al dispositivo que representa el siguiente salto. Si el siguiente salto es inaccesible, el paquete se descarta. Para probar el siguiente salto, determine la

ruta apropiada al destino y trate de hacer ping al gateway por defecto o al siguiente salto apropiado para esa ruta en la tabla de enrutamiento.

Una falla en el ping indica que puede existir un problema de configuración o de hardware. Sin embargo, el ping también puede estar prohibido por la seguridad del dispositivo.

21. Rastreo e implementación de los resultados de rastreo

Ver secuencia de prueba: Unificación Punto 11.3.5(2) de la máquina virtual
Actividades
Actividad 11.2.4
Actividad 11.3.5(3)
Actividad 11.5.1
Actividad 11.6.1
Examen Tema 11 CISCO