



Cisco Networking Academy

Cisco Devnet

Módulo #5: Fundamentos de la Red

Autor: Paco Aldarias
francisco.aldarias@aulammentor.es

Fecha:
13-03-2022

Licencia:
Creative Commons v.2.0



Reconocimiento - NoComercial - CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

¿Qué aprenderá en este módulo?



Título del módulo: Fundamentos de la red

Objetivo del módulo: Aplicar los procesos y dispositivos que admiten la conectividad de red.

Objetivo	Objetivo del tema
Introducción a los fundamentos de la red	Explique los términos y procesos básicos de las redes.
Capa de interfaz de la red	Explique las características y las funciones de la capa de red de OSI.
Capa de internetwork	Explique las características y las funciones de la capa de interconexión de red de OSI.
Dispositivos de red	Explique las características y las funciones de los dispositivos de red comunes.
Protocolos de red	Explique los protocolos de red comunes.
Solución de problemas de conectividad de aplicaciones	Solución de los problemas de conectividad de la red básica.

5.1 Introducción a los aspectos básicos de las redes

¿Qué es una red?

- Una red consta de dispositivos finales, como equipos, dispositivos móviles e impresoras, conectados por dispositivos de red, como conmutadores y enrutadores.
- La red permite que los dispositivos se comuniquen entre sí y compartan datos.
- Los métodos de LAN más comunes para conectarse a una red son LAN Ethernet cableadas (IEEE 802.3) o LAN inalámbricas (IEEE 802.11). Los dispositivos finales se conectan a la red mediante Ethernet o una tarjeta de interfaz de red inalámbrica (NIC Network Interface Controller).

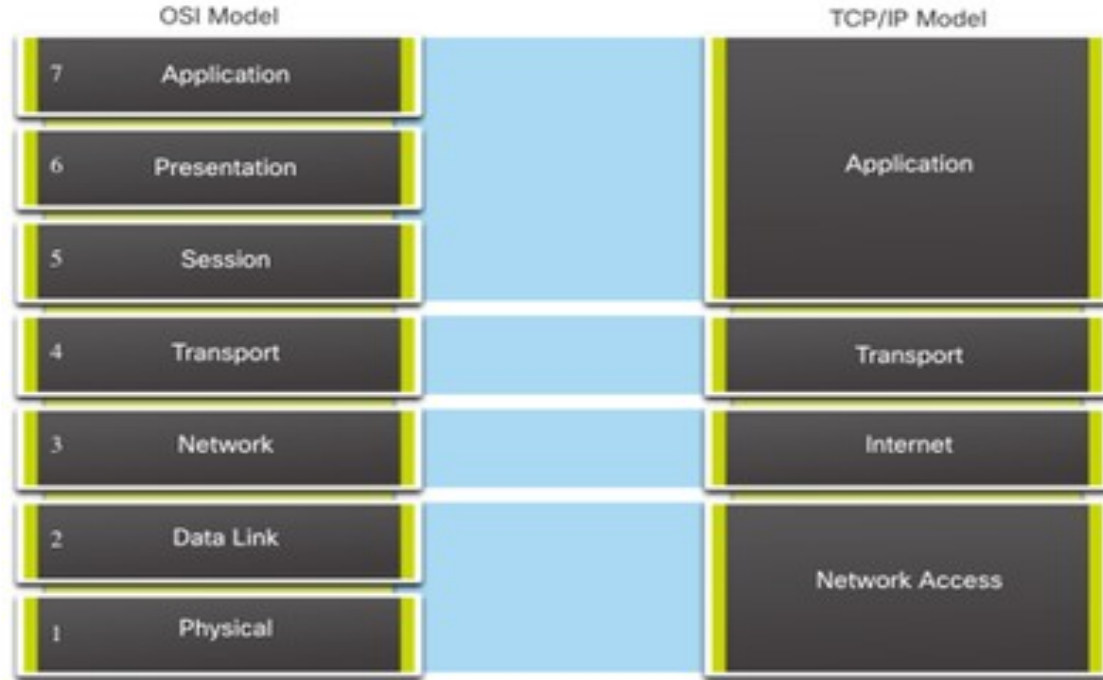
Suite de protocolos

Un conjunto de protocolos es un conjunto de protocolos que funcionan juntos para proporcionar servicios de comunicación de red integrales, como:

- Suite de protocolo de Internet o TCP/IP
- Protocolos de interconexión de sistemas abiertos (OSI)
- AppleTalk (ahora reemplazado por TCP/IP)
- Novell NetWare (ahora reemplazado por TCP/IP)

¿Qué es una red? (Continuación)

- Tanto el modelo OSI como el modelo TCP/IP usan capas para describir las funciones y servicios que pueden ocurrir en esa capa.
- Ambos modelos se pueden utilizar con las siguientes diferencias:
 - El modelo OSI numera cada capa.
 - El modelo TCP/IP utiliza una sola capa de aplicación para hacer referencia a las capas de aplicación, presentación y sesión OSI.
 - El modelo TCP/IP utiliza una única capa de acceso a la red para hacer referencia al vínculo de datos OSI y a las capas físicas.
 - El modelo TCP/IP se refiere a la capa de red OSI como capa de Internet.



5.1.- Fundamentos de redes

5.1.1. *Qué es una red*

Los dispositivos finales implementan protocolos para toda la «pila» de capas.

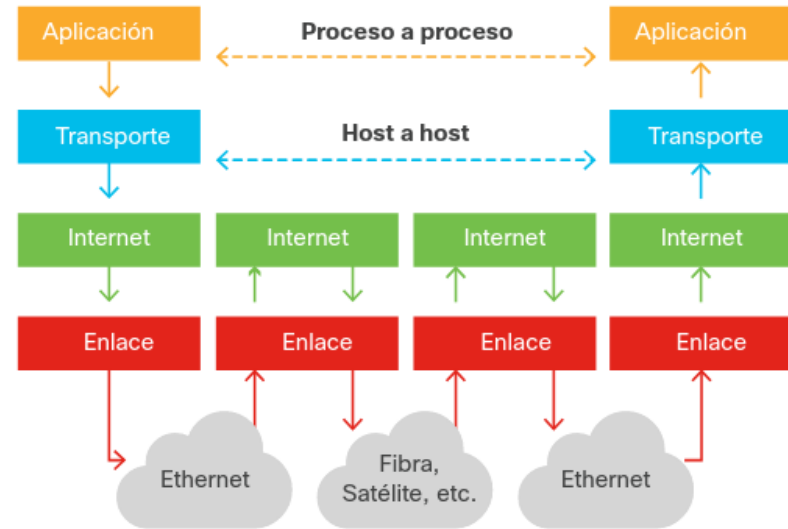
Capa Enlace. Trabaja con MAC, Ejemplo Switch.

Capa Internet. Interconecta redes usando enrutamiento y usando IPs. Ejemplo Routers

Topología de la red



Flujo de datos

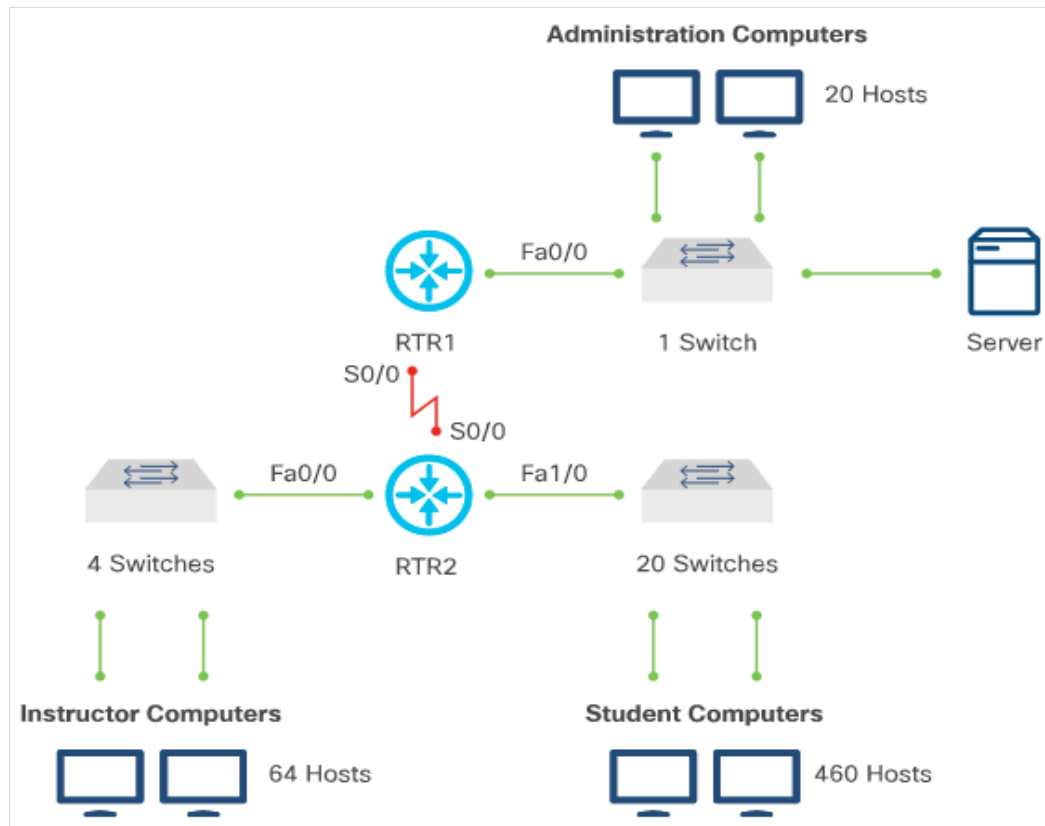


5.2 Capa de interfaz de red

Comprensión de la capa de interfaz de red

Topología de la red

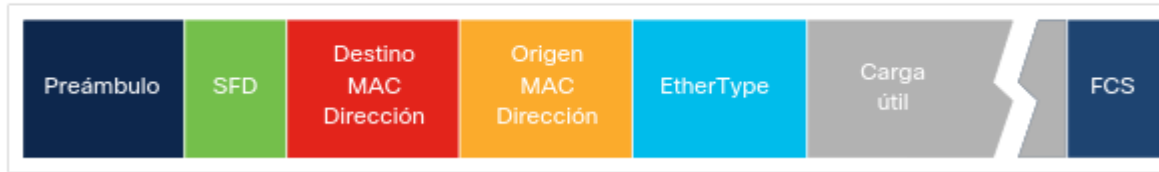
- La red permite que los dispositivos se comuniquen entre sí y compartan datos.
- Todos los dispositivos host y de red que están interconectados, dentro de un área física cercana, forman una red de área local (LAN).
- Los dispositivos de red que conectan LAN, a grandes distancias, forman una red de área ampliada (WAN).



5.2.- Capa de interface de la red

5.2.2. Ethernet

Trama de Ethernet



Ethernet es un estandar de red que incluye cableado y distancias entre segmentos.

Los bits que se transmiten a través de la LAN Ethernet se organizan en tramas que es donde van los datos. La comunicación es de mac a mac.

Categorías de cable ethernet

<https://www.igus.es/info/cable-ethernet>

Cat 5 = 100Mbps || Cat 5e = 1Gbps ||

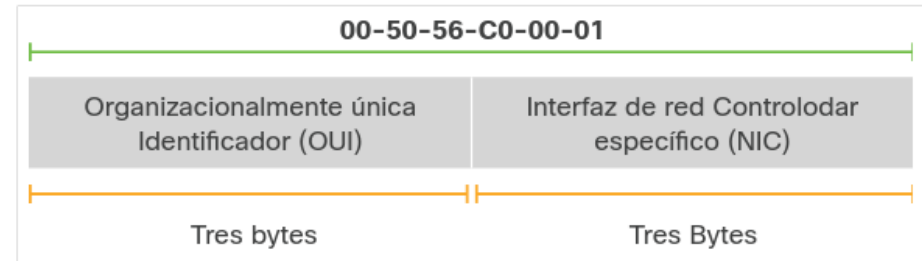
Cat 6 = 10 Gbps



DevNet Associate

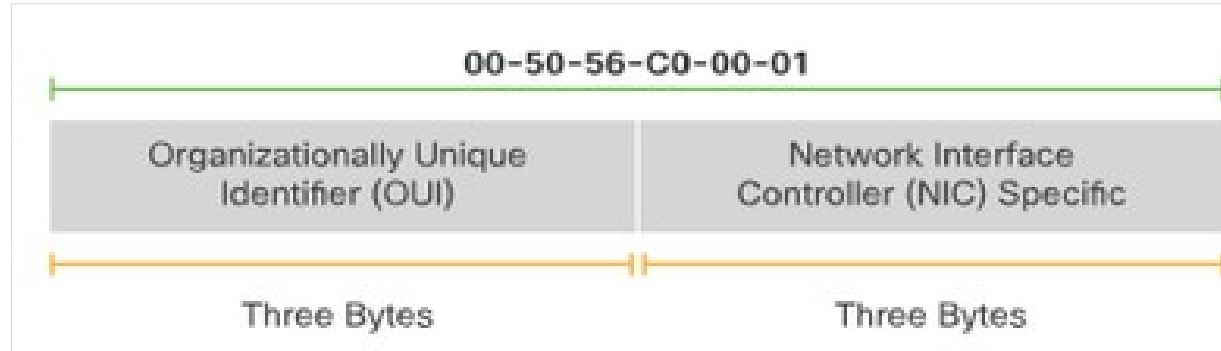
v1.0

Formato de dirección MAC



Direcciones MAC de capa de interfaz de red

- Todos los dispositivos de red en la misma red deben tener una dirección MAC única.
- La dirección MAC es el medio por el cual los datos se dirigen al dispositivo de destino adecuado.
- Una dirección MAC se compone de 12 números hexadecimales. Hay dos componentes principales de un MAC:
 - **24-bit OUI** - El OUI identifica al fabricante de la NIC.
 - **24-bit, asignado por el proveedor, dirección de la estación final** - Esta parte identifica de forma exclusiva el hardware Ethernet.
- Las direcciones MAC de destino incluyen los tres tipos principales de comunicaciones de red:
 - Unidifusión
 - Difusión
 - Multidifusión

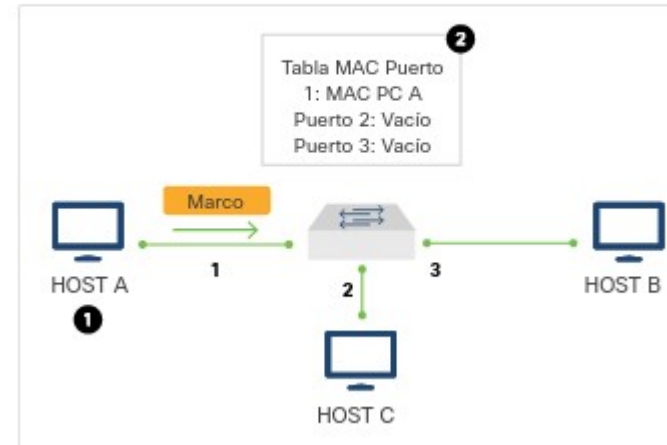


5.2.- Capa de interface de la red

5.2.4. Switching

El switch interconecta por cable dispositivos de una red y dispone de una tabla que identifica cada puerto con la mac que tiene para un mayor rendimiento. El switch crea dinámicamente la tabla de direcciones MAC, examinando la dirección MAC de origen de las tramas recibidas en un puerto. Si la dirección MAC de destino está en la tabla de direcciones MAC, la enviará por el puerto especificado. De lo contrario, lo inundará todos los puertos excepto el puerto entrante.

Proceso de switching



5.2.- Capa de interface de red

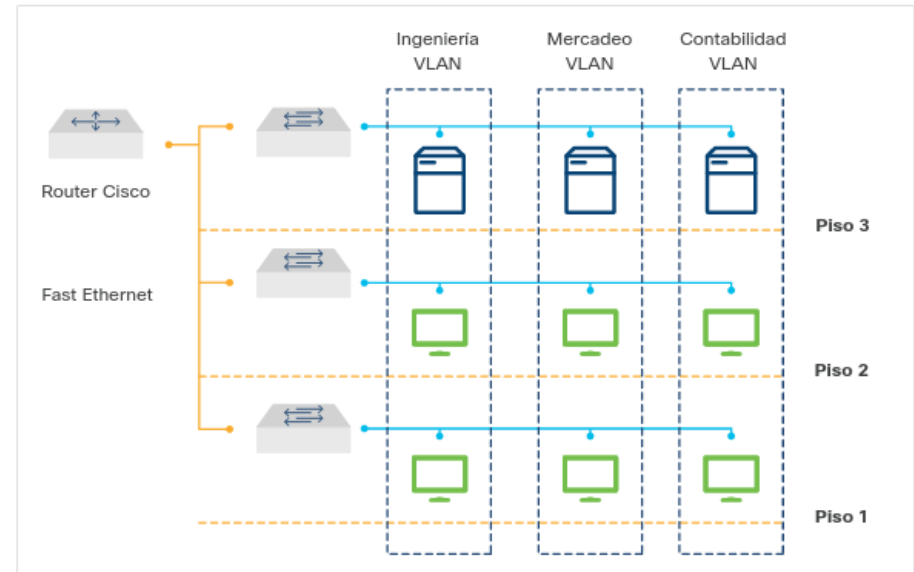
5.2.5. VLAN

Una LAN virtual (VLAN) se utiliza para segmentar diferentes dominios de difusión de Capa 2 en uno o más conmutadores. Una VLAN agrupa dispositivos en una o más LAN que están configuradas para comunicarse como si estuvieran conectados al mismo cable, cuando en realidad están ubicados en varios segmentos de LAN diferentes.

Por ejemplo, en la figura, el administrador de red creó tres VLAN basadas en la función de sus usuarios: ingeniería, mercadeo y contabilidad. Tenga en cuenta que los dispositivos no necesitan estar en el mismo piso.

Puede definir una o varias VLAN dentro de un switch. Cada VLAN que cree en el switch define un nuevo **dominio de difusión**. El tráfico no puede pasar directamente a otra VLAN (entre dominios de difusión)

VLAN



LAN virtuales de capa de interfaz de red (VLAN) (Cont.)

- Las VLAN definen los dominios de broadcast de Capa 2. Las VLAN en los conmutadores de Capa 2 crean dominios de difusión según la configuración del conmutador.
- Para interconectar dos VLAN diferentes, se debe utilizar un switch o un router de Capa 3.
- Las VLAN suelen asociarse con redes IP o subredes.
- La siguiente tabla explica que las VLAN están organizadas en tres rangos: reservada, normal y extendida.

VLAN	Alcance	Uso
0, 4095	Reservado	Solo para uso del sistema. No puede visualizar o utilizar estas VLAN.
1	Normal	Cisco predeterminado. Puede utilizar esta VLAN, pero no puede eliminarla.
2 - 1001	Normal	Se utiliza para VLAN Ethernet; puede crear, usar y eliminar estas VLAN.
1002 - 1005	Normal	Valores predeterminados de Cisco para FDDI y Token Ring. Las VLAN 1002 - 1005 no se pueden eliminar.
1006 - 4094	Extendida	Para VLAN Ethernet únicamente.

5.3 Capa de interconexión de red

Direcciones

IPv4 de capa entre redes

- Cada dispositivo de una red tiene una dirección IP única.
- Una dirección IPv4 es de 32 bits, con cada octeto (8 bits) representado como un valor decimal separado por un punto. Esta representación se denomina notación decimal punteada.
- Hay tres tipos de direcciones IPv4:
 - Dirección de red
 - Direcciones de host
 - Dirección de broadcast
- La máscara de subred IPv4 (o la longitud del prefijo) se usa para diferenciar la porción de red de la porción de host de una dirección IPv4.
- Una red se puede dividir en redes más pequeñas llamadas subredes. Se pueden proporcionar subredes a unidades organizativas individuales para simplificar la red. La subred proporciona un rango específico de direcciones IP para que un grupo de hosts utilice.
- Los dispositivos que utilizan direcciones IPv4 privadas pueden acceder a Internet a través de la traducción de direcciones de red (NAT) y la traducción de direcciones de puerto (PAT).

5.3.- Capa de internetworking



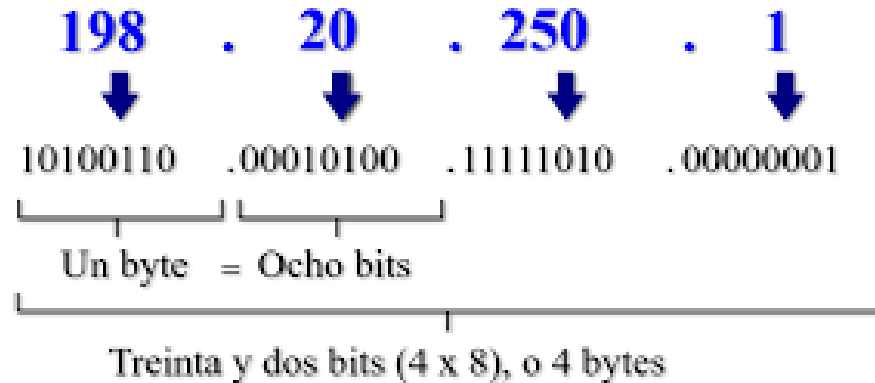
5.3.2 Direcciones IPv4

Notación

203.0.113.1/24 = 203.0.113.1/255.255.255.0

- Dirección de red. 203.0.113.0
- Dirección de host. 203.0.113.1
- Dirección de broadcast. 203.0.113.255

Estructura de una dirección IPv4



5.3.- Capa de internetworking



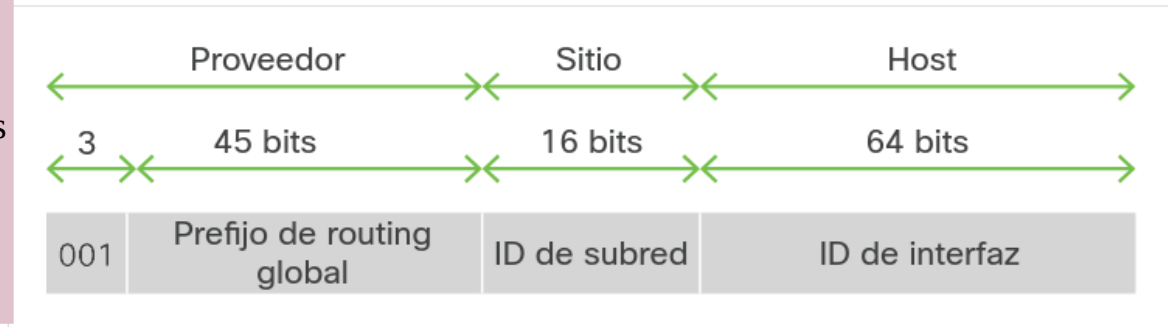
5.3.3. Direcciones IPv6

Ipv4 = 32 || Ipv6 = 128 bits

Las direcciones IPv6 se representan como una serie de campos hexadecimales de 16 bits (hexteto) separados por dos puntos (:) en el formato: x: x: x: x: x: x: x: x.

El formato preferido incluye todos los valores hexadecimales.

Formato GUA IPv6



DevNet Associate

v1.0

IPv6 está diseñado para ser el sucesor de IPv4.

5.3.- Capa de internetworking

5.3.3 Direcciones IPv6

Hay dos reglas que se pueden utilizar para reducir la representación de la dirección IPv6:

1. Omitir ceros a la izquierda en cada hexteto
2. Reemplazar una sola cadena de hextetos de cero por dos puntos (::)

Se pueden omitir ceros a la izquierda en cada hexteto de 16 bits. Por ejemplo:

Recomendado:

2001:0db8:0000:1111:0000:0000:0200

Sin ceros a la izquierda: 2001:db8:0:1111:0:0:0:200

Las direcciones IPv6 suelen contener campos hexadecimales sucesivos de ceros. Se pueden usar dos puntos (::) para comprimir campos hexadecimales sucesivos de ceros.

Recomendado:

2001:0db8:0000:1111:0000:0000:0200

Sin ceros a la izquierda:

2001:db8:0:1111::200

5.3.- Capa de internetworking



5.3.3 Direcciones IPv6

Tipo de dirección IPv6	Formato preferido	Formato comprimido
Unidifusión	2001:0:0:db8:800:200c:417a	2001::db8:800:200c:417a
Multidifusión	ff01:0:0:0:0:0:0:101	ff01::101
Bucle de retorno	0:0:0:0:0:0:0:1	::1
Sin especificar	0:0:0:0:0:0:0:0	::



5.3.- Capa de internetworking

5.3.5 Routers y Enrutamiento

El enrutamiento implica el reenvío de paquetes entre diferentes redes. Cuando un router recibe un paquete entrante en una de sus interfaces, verifica la dirección IP de destino en el paquete y busca la mejor coincidencia entre la dirección de destino y las direcciones de red en su tabla de enrutamiento.

Una entrada coincidente indica que el destino está conectado directamente al enrutador o que se puede alcanzar reenviando el paquete a otro router.

Ese router se convierte en el router de salto siguiente hacia el destino final del paquete. Si no hay ninguna entrada que coincida, el router envía el paquete a la ruta predeterminada. Si no hay una ruta predeterminada, el router descarta el paquete.

```
~ : bash — Konsole
Nueva pestaña Separar vista izquierda/derecha Separar vista arriba/abajo Copiar Pegar Buscar
paco@lliurex-e70sff:~$ route -n
Tabla de rutas IP del núcleo
Destino      Pasarela      Genmask      Indic Métric Ref      Uso Interfaz
0.0.0.0      172.29.24.1   0.0.0.0      UG    100    0        0 eth0
169.254.0.0  0.0.0.0      255.255.0.0  U     1000   0        0 eth0
172.29.24.0  0.0.0.0      255.255.255.0 U     100    0        0 eth0
paco@lliurex-e70sff:~$
```

Enrutamiento y enrutadores de capas entre redes

- El enrutador es un dispositivo de red que funciona en la capa de Internet del modelo TCP / IP o en la capa de red de Capa 3 del modelo OSI.
- Los routers utilizan una tabla de routing para el routing entre redes.
- Por lo general, un router realiza dos funciones principales:

Determinación de ruta

La determinación de ruta es el proceso mediante el cual los enrutadores usan sus tablas de enrutamiento para determinar dónde reenviar los paquetes.

- Cuando un router recibe un paquete entrante, verifica la dirección IP de destino en el paquete y busca la mejor coincidencia en su tabla de enrutamiento.
- Una entrada coincidente indica que el destino está conectado directamente al enrutador. Ese router se convierte en el router de salto siguiente hacia el destino final del paquete.
- Si no hay ninguna entrada que coincida, el router envía el paquete a la ruta predeterminada. Si no hay una ruta predeterminada, el router descarta el paquete.

Reenvío de Paquetes

Una vez que el router determina la ruta correcta para un paquete, reenvía el paquete a través de una interfaz de red hacia la red de destino.

Una tabla de enrutamiento puede contener los siguientes tipos de entradas:

- Redes conectadas directamente
- Rutas estáticas
- Rutas dinámicas
- Rutas predeterminadas

5.4 Dispositivos de red

5.4.1 Swichers Ethernet

- Un concepto clave en la conmutación Ethernet es el dominio de broadcast. Un dominio de broadcast es una división lógica en la que todos los dispositivos de una red pueden comunicarse entre sí mediante broadcast en la capa de enlace de datos.
- Los conmutadores Ethernet pueden transmitir y recibir datos simultáneamente. Este modo se denomina dúplex completo, que elimina los dominios de colisión.
- Los switches tienen las siguientes funciones:
 - Operar en la capa de acceso a la red del modelo TCP / IP y la capa de enlace de datos de Capa 2 del modelo OSI
 - Filtrar o inundar tramas en función de las entradas de la tabla de direcciones MAC
 - Tener una gran cantidad de puertos de alta velocidad y dúplex completo
- La figura muestra un ejemplo de conmutadores con múltiples puertos de alta velocidad y dúplex completo.



Routers

- Los routers son necesarios para llegar a dispositivos que no están en la misma LAN y utilizar tablas de enrutamiento para enrutar tráfico entre diferentes redes.
- Los routers tienen las siguientes funciones:
 - Operan en la capa de Internet del modelo TCP / IP y la capa de red de la capa 3 del modelo OSI.
 - Enrutan paquetes entre redes en función de las entradas de la tabla de enrutamiento.
 - Tienen soporte para una gran variedad de puertos de red, incluidos varios puertos de medios LAN y WAN.
- La figura muestra un router modular con puertos de switch integrados.



Firewalls

- Un firewall es un sistema de hardware o software que evita el acceso no autorizado dentro o fuera de una red.
 - Los firewalls se utilizan para evitar que usuarios de Internet no autorizados accedan a las redes internas.
- Todos los datos que entran o salen de la intranet protegida deben atravesar el cortafuegos para llegar a su destino, y cualquier dato no autorizado se bloquea.
- La figura muestra un ejemplo de un firewall de hardware.



Equilibradores de carga de dispositivos de red

- El equilibrio de carga mejora la distribución de las cargas de trabajo en varios recursos informáticos, como servidores, clústeres de servidores, enlaces de red, etc.
- El equilibrio de carga del servidor ayuda a garantizar la disponibilidad, la escalabilidad y la seguridad de las aplicaciones y los servicios al distribuir el trabajo de un único servidor entre varios servidores.
- A nivel de dispositivo, el equilibrador de carga proporciona las siguientes características para admitir una alta disponibilidad de red:
 - Redundancia de dispositivos
 - Escalabilidad
 - Seguridad
- En el nivel de servicio de red, un equilibrador de carga proporciona los siguientes servicios avanzados:

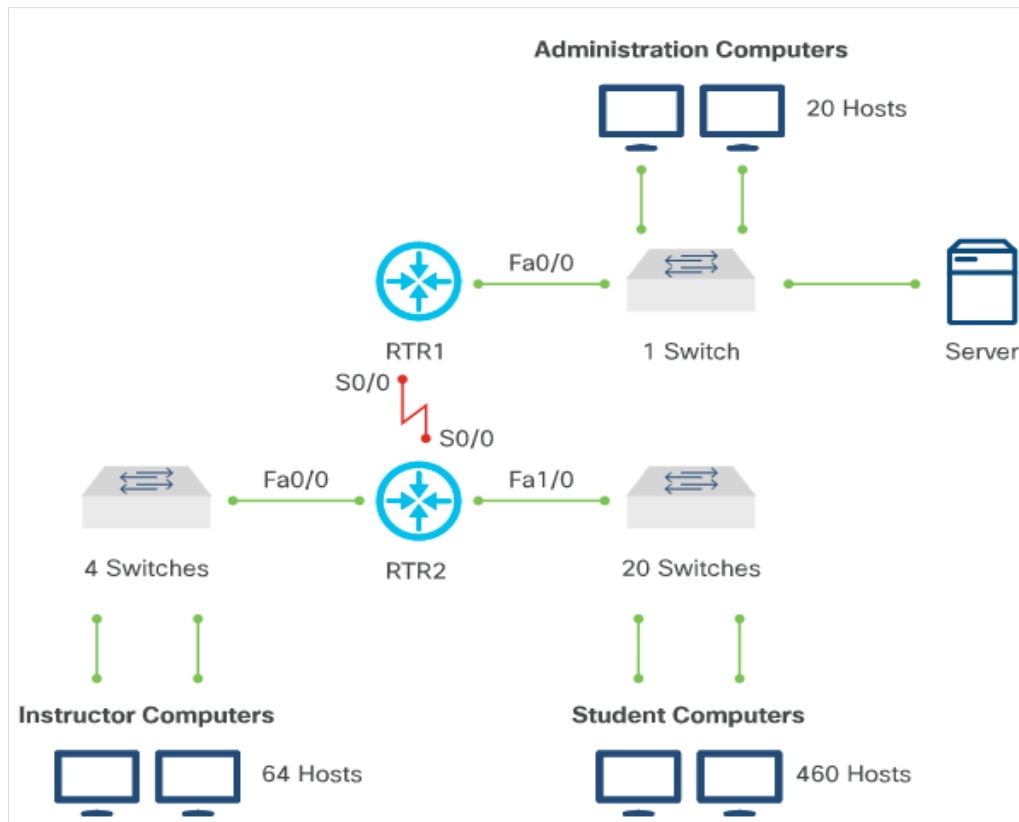
Alta disponibilidad de servicios	Escalabilidad	Seguridad a nivel de servicio
Esto permite la distribución de solicitudes de cliente entre servidores físicos y granjas de servidores.	La virtualización permite el uso de algoritmos avanzados de equilibrio de carga para distribuir las solicitudes de los clientes entre los dispositivos virtuales.	Esto permite establecer y mantener una sesión de Secure Sockets Layer (SSL) entre el equilibrador de carga y su par.

Diagramas de red de dispositivos de red

- Los diagramas de red son parte de la documentación que acompaña a la implementación de una red y también juegan un papel importante cuando la documentación entra en el código de programación.
- Muestran una representación visual e intuitiva de la red, mostrando cómo están conectados todos los dispositivos y qué interfaz se conecta a cada dispositivo, etc.
- Generalmente hay dos tipos de diagramas de red:
 - **Diagramas de conectividad física de capa 2:** Estos son los diagramas de red que representan la conectividad del puerto entre los dispositivos en la red.
 - **Diagramas de conectividad lógica de capa 3:** Estos son los diagramas de red que muestran la conectividad IP entre dispositivos en la red.

Diagramas de red de dispositivos de red (cont.)

- Aquí se muestra un diagrama de red de capa 2 simplificado.
- Este diagrama da una idea general de cómo los clientes se conectan a la red y cómo los dispositivos de red se conectan entre sí para que se logre la conectividad de extremo a extremo entre todos los clientes.



Packet Tracer – Explore una red simple

- En este Packet Tracer, hará lo siguiente:
- **Parte 1:** Agregar equipos a la topología
- **Parte 2:** Pruebe la conectividad en toda la red
- **Parte 3:** Cree una página web y visualícela
- **Parte 4:** Examine las listas de acceso de FIREWALL

5.5 Protocolos de red

Protocolos de red

- Es esencial comprender los protocolos de red estándar para una comunicación eficaz y la resolución de problemas.

Telnet y Secure Shell (SSH)

- Estos protocolos se utilizan para conectarse e iniciar sesión en un equipo remoto.
- SSH utiliza cifrado para proteger los datos a través de una conexión de red y, por lo tanto, se utiliza con mayor frecuencia.
- Telnet solo debe usarse en entornos que no sean de producción.
- De forma predeterminada, SSH utiliza el puerto 22 y Telnet utiliza el puerto 23.

HTTP y HTTPS

- HTTP significa Hyper Text Transfer Protocol y HTTPS es la versión segura de HTTP. HTTP usa puerto 80, y el https el 443.
- Estos protocolos son reconocidos por los navegadores web y se utilizan para conectarse a sitios web.
- HTTPS utiliza TLS o SSL para establecer una conexión segura.

NETCONF and RESTCONF

- NETCONF utiliza el puerto 830. RESTCONF no tiene un valor de puerto reservado.
- Para tener varias operaciones de red, asegúrese de que cada protocolo tenga un puerto predeterminado y utilice estándares para tratar de evitar conflictos.

DHCP

- DHCP funciona dentro de un modelo cliente / servidor, donde los servidores DHCP asignan direcciones IP y entregan información de configuración a dispositivos que están configurados para solicitar información de direccionamiento de forma dinámica.
- Además de la dirección IP del propio dispositivo, un servidor DHCP también puede proporcionar información adicional, como la dirección IP del servidor DNS, el enrutador predeterminado y otros parámetros de configuración.
- Algunos de los beneficios de usar DHCP en lugar de las configuraciones manuales son tareas y costos de configuración de clientes reducidos y administración centralizada
- DHCP asigna direcciones IP de tres formas: asignación automática, asignación dinámica, asignación manual.

Retransmisión DHCP

- En los casos en que el cliente y el servidor DHCP se encuentran en diferentes subredes, se puede utilizar un agente de retransmisión DHCP entre ellos.
- Los agentes de retransmisión DHCP se encuentran en la interfaz.



Protocolos de red

DNS

- En las redes de datos, los dispositivos se etiquetan con direcciones IP numéricas para enviar y recibir datos a través de las redes. Los nombres de dominio (DNS) se crearon para convertir la dirección numérica en un nombre simple y reconocible.
- El protocolo DNS define un servicio automatizado que hace coincidir los nombres de dominio con las direcciones IP.
- Incluye el formato de consultas, respuestas y datos. DNS utiliza un único formato denominado mensaje DNS.

Formato de mensaje DNS

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Algunos de estos tipos de registros son los siguientes:

- A - Una dirección IPv4 de dispositivo final
- NS - Un servidor de nombres autorizado
- AAAA: - Una dirección IPv6 de dispositivo final (pronunciada quad-A)
- MX - Un registro de intercambio de correo

DNS (Cont.)

- Cuando un cliente realiza una consulta a su servidor DNS configurado, el servidor DNS primero mira sus propios registros para resolver el nombre. Si no puede resolverlo con los registros almacenados, contacta a otros servidores para hacerlo.
- Una vez que se encuentra una coincidencia y se devuelve al servidor solicitante, el servidor almacena temporalmente la dirección en caso de que se vuelva a solicitar el mismo nombre.
- Como se muestra en la siguiente tabla, DNS usa el mismo formato de mensaje entre servidores

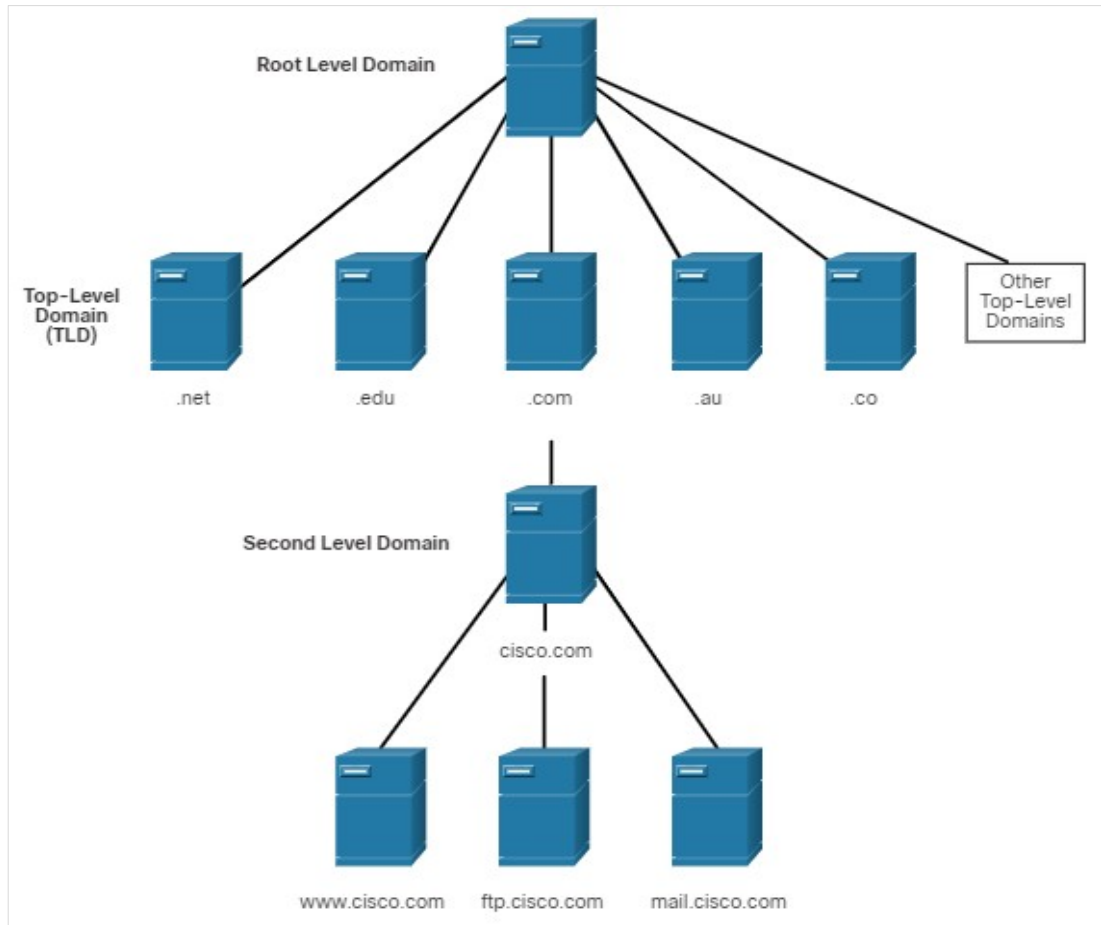
Sección de mensajes DNS	Descripción
Pregunta	La pregunta para el servidor de nombres
Respuesta	Registros de recursos que responden la pregunta
Autoridad	Registros de recursos que apuntan a una autoridad
Adicional	Registros de recursos que poseen información adicional

Protocolos de red

DNS (Cont.)

Jerarquía DNS

- DNS utiliza un sistema jerárquico basado en nombres de dominio para crear una base de datos que proporcione resolución de nombres.
- La estructura de nomenclatura se divide en zonas pequeñas y manejables.
- Cuando un servidor DNS recibe una solicitud de traducción de nombre que no está dentro de su zona DNS, reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para la traducción.



SNMP

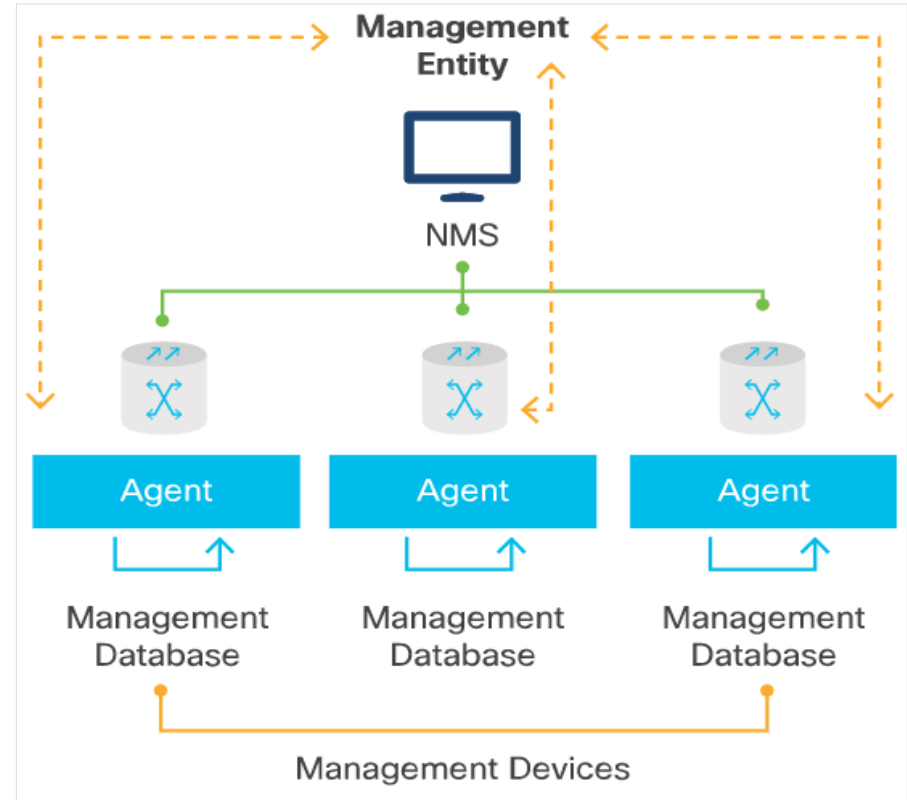
- SNMP se desarrolló para permitir a los administradores gestionar dispositivos como servidores, estaciones de trabajo, enrutadores, conmutadores y dispositivos de seguridad en una red IP.
- SNMP es un protocolo de capa de aplicación que proporciona un formato de mensaje para la comunicación entre administradores y agentes.
- El sistema SNMP consta de tres elementos:
 - Sistema de Administración de Red (Network Management System-NMS)
 - Agentes SNMP (nodo administrado)
 - Base de información de administración (MIB)

Protocolos de red

SNMP (Cont.)

Componentes SNMP

- Para configurar SNMP en un dispositivo de red, primero es necesario definir la relación entre el administrador y el agente.
- El administrador de SNMP forma parte de un sistema de administración de red (Network Management System NMS).
- Puede recopilar información de un agente SNMP mediante la acción get y puede cambiar las configuraciones de un agente mediante la acción set.
- Además, los agentes SNMP pueden reenviar información directamente al administrador SNMP mediante trampas.



SNMP (Cont.)

Funcionamiento de SNMP

- Un agente s SNMP que se ejecuta en un dispositivo recopila y almacena información sobre el dispositivo y su funcionamiento. Luego, el administrador SNMP usa el agente SNMP para acceder a la información dentro de la MIB y realizar cambios en la configuración del dispositivo.
- Hay dos solicitudes principales del administrador SNMP, **get** y **set**. Una solicitud **get** es utilizada por el administrador SNMP para consultar datos del dispositivo. Una solicitud **set** es utiliza por el administrador SNMP para cambiar las variables de configuración en el dispositivo del agente.

Sondeo SNMP

- El NMS se puede configurar para que los administradores SNMP sondeen periódicamente a los agentes SNMP.
- Con este proceso, la información se recopila para monitorear las cargas de tráfico y verificar las configuraciones de los dispositivos administrados.
- Los datos se pueden graficar o se pueden establecer umbrales para activar un proceso de notificación cuando se superan los umbrales.

SNMP (Cont.)

Trampas del protocolo SNMP

- Las encuestas periódicas SNMP tienen algunos inconvenientes.
 - Retraso entre el momento en que ocurre un evento y el momento en que el NMS lo detecta (mediante sondeo)
 - compensación entre la frecuencia de sondeo y el uso del ancho de banda
- Para mitigar las desventajas, los agentes SNMP generan y envían trampas para informar al NMS inmediatamente de ciertos eventos.

Cadenas de comunidad SNMP

- Para que SNMP funcione, NMS debe tener acceso a la MIB.
- SNMPv1 y SNMPv2c utilizan cadenas de comunidad (contraseñas de texto sin formato) que controlan el acceso a la MIB.
- Las cadenas de comunidad SNMP autentican el acceso a los objetos MIB.
- Hay dos tipos de cadenas de comunidad: Solo lectura (ro) y lectura-escritura (rw)

SNMP (Cont.)

Base de información para administración (MIB, Management Information Base)

- El agente captura datos de MIB, que son estructuras de datos que describen elementos de red SNMP como una lista de objetos de datos.
- El MIB está organizado en una estructura de árbol con variables únicas representadas como hojas terminales.
- Un identificador de objeto (OID) es una etiqueta numérica larga. Se utiliza para distinguir cada variable de forma única en el MIB y en los mensajes SNMP.
- Las variables que miden elementos como la temperatura de la CPU, los paquetes entrantes en una interfaz, la velocidad del ventilador y otras métricas, tienen valores OID asociados.
- Las capturas SNMP se utilizan para generar alarmas y eventos que están ocurriendo en el dispositivo. Las trampas contienen:
 - OID que identifican cada evento y lo hacen coincidir con la entidad que generó el evento
 - Gravedad de la alarma (crítica, mayor, menor, información o evento)
 - Una marca de fecha y hora

SNMP (Cont.)

Comunidades SNMP

- Los nombres de comunidad SNMP se utilizan para agrupar destinos de captura SNMP.
- Cuando se asignan nombres de comunidad a capturas SNMP, la solicitud del administrador SNMP se considera válida si el nombre de la comunidad coincide con el configurado en el dispositivo administrado; de lo contrario, SNMP descarta la solicitud.

Mensajes SNMP

SNMP utiliza los siguientes mensajes para comunicarse entre el administrador y el agente:

- **Get y GetNext** - Los mensajes Get y GetNext se utilizan cuando el administrador solicita información para una variable específica.
- **GetResponse** - Cuando el agente recibe un mensaje Get o GetNext, enviará un mensaje GetResponse al administrador.
- **Set** - El administrador utiliza un mensaje Set para solicitar que se realice un cambio en el valor de una variable específica.
- **Trap** - El agente usa el mensaje Trap para informar al gerente cuando ocurren eventos importantes.

NTP

- La función principal del Protocolo de tiempo de red (NTP) es sincronizar la hora de los dispositivos en la red.
- NTP permite que un dispositivo actualice su reloj desde una fuente de tiempo de red confiable. Un dispositivo que recibe tiempo autorizado se puede confirmar para que sirva tiempo a otras máquinas, lo que permite que los grupos de dispositivos estén estrechamente sincronizados.
- NTP se ejecuta sobre UDP utilizando el puerto 123 como origen y destino.
- Una fuente de tiempo autorizada suele ser un reloj de radio, o un reloj atómico conectado a un servidor de tiempo. El servidor autorizado en NTP es una fuente de tiempo muy precisa. Es la función de NTP distribuir el tiempo a través de la red.
- NTP utiliza el concepto de estratos (capas) para describir qué tan lejos está un host de una fuente de tiempo autorizada. Las fuentes más autorizadas están en el estrato 1.

NTP (Cont.)

- NTP evita la sincronización con servidores ascendentes cuya hora no es precisa mediante estas dos formas:
 - NTP nunca se sincroniza con un servidor NTP que no esté sincronizado.
 - NTP compara la hora informada por varios servidores NTP y no se sincronizará con un servidor cuya hora sea un valor atípico.
- Los clientes normalmente se sincronizan con el servidor de estrato más bajo al que pueden acceder. Pero NTP también incorpora salvaguardas: prefiere tener acceso a al menos tres fuentes de tiempo de estrato inferior porque esto le ayuda a determinar si alguna fuente es incorrecta.

Modos de asociación NTP - Los servidores NTP pueden asociarse en varios modos, que incluyen:

- Cliente/Servidor
- Simétrico activo / pasivo
- Broadcast

NTP (Cont.)

Cliente / Modo seguro

- Este es el modo más común en el que un cliente o servidor dependiente puede sincronizarse con un miembro del grupo, pero no al revés, protegiendo contra ataques de protocolo o mal funcionamiento.
- Las solicitudes de cliente a servidor se realizan mediante llamadas a procedimientos remotos asincrónicas.
- En este modo, un cliente solicita tiempo desde uno o más servidores y procesa las respuestas tal como se recibieron. El servidor cambia las direcciones y los puertos, sobrescribe los campos de mensajes, recalcula la suma de comprobación y devuelve el mensaje inmediatamente.
- La información incluida en el mensaje NTP permite al cliente determinar el sesgo entre el servidor y la hora local, lo que permite ajustar el reloj.
- El mensaje también incluye información para calcular la precisión y fiabilidad esperadas, así como ayudar al cliente a seleccionar el mejor servidor.

NTP (Cont.)

Modo simétrico activo/pasivo

- En este modo, un grupo de pares de estrato bajo trabajan como copias de seguridad entre sí. Cada par obtiene tiempo de una o más fuentes de referencia primarias o de servidores secundarios confiables.
- El modo simétrico/activo generalmente se confirma declarando un par en el archivo de configuración, indicando al par que uno desea obtener tiempo de él, y proporcionar tiempo atrás si es necesario.
- Los modos simétricos se utilizan con mayor frecuencia para interconectar dos o más servidores que funcionan como un grupo mutuamente redundante.

NTP (Cont.)

Modo de difusión y/o multidifusión

- Cuando solo existen requisitos modestos de precisión, los clientes pueden usar modos de difusión y/o multidifusión NTP, donde muchos clientes se confían de la misma manera, y un servidor de difusión (en la misma subred) proporciona tiempo para todos ellos.
- La configuración de un servidor de difusión se realiza mediante el comando broadcast y, a continuación, se proporciona una dirección de subred local. El comando broadcast client permite al cliente broadcast responder a los mensajes de difusión recibidos en cualquier interfaz.
- Este modo no se puede utilizar más allá de una sola subred. Este modo siempre debe estar autenticado porque un intruso puede hacerse pasar por un servidor de transmisión y propagar valores de tiempo falsos.

NAT

- La traducción de direcciones de red (NAT) ayuda con el problema del agotamiento de direcciones IPv4. NAT funciona asignando miles de direcciones IPv4 internas privadas a un rango de direcciones públicas.
- NAT identifica el tráfico hacia y desde un dispositivo específico, traduciendo entre direcciones IPv4 externas/públicas e internas/privadas.
- Permite a una organización cambiar fácilmente de proveedor de servicios o reenumerar voluntariamente los recursos de red sin afectar su espacio de direcciones IPv4 públicas.
- NAT también oculta a los clientes en la red interna detrás de un rango de direcciones públicas, proporcionando una sensación de seguridad contra los dispositivos que son atacados directamente desde el exterior.

Tipos de NAT

- Traducción de direcciones estáticas (NAT estática)
- Traducción dinámica de direcciones (NAT dinámica)
- Sobrecarga (también llamada traducción de direcciones de puerto o PAT)

NAT (Cont.)

- IPv6 se desarrolló con la intención de hacer que NAT no fuera necesario.
- IPv6 proporciona traducción de protocolos entre IPv4 e IPv6. Esto se conoce como NAT64. NAT para IPv6 se usa en un contexto muy distinto al de NAT para IPv4.
- Las variedades de NAT para IPv6 se usan para proporcionar acceso de manera transparente entre redes solo IPv6 y redes solo IPv4.

Cuatro direcciones NAT

NAT incluye cuatro tipos de direcciones:

- **Dirección interior** - Esta es la dirección del dispositivo que está siendo traducido por NAT.
- **Dirección exterior** - Esta es la dirección del dispositivo de destino.
- **Dirección local** - Esta es cualquier dirección que aparezca en la parte interior de la red.
- **Dirección global** - Esta es cualquier dirección que aparezca en la parte exterior de la red.

Protocolos de red

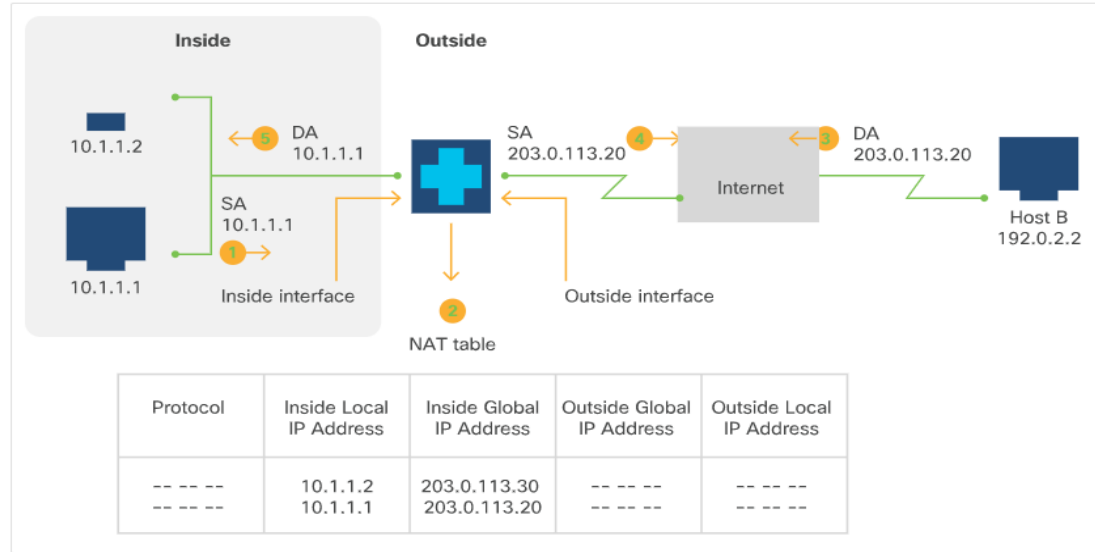
NAT (Cont.)

Traducción de direcciones de origen interno

Las direcciones IPv4 se pueden traducir a direcciones IPv4 globales únicas cuando se comunican fuera de la red interna. Hay dos opciones para lograr esto:

- **Traducción estática** - Este método establece un mapeo uno a uno entre una dirección local interna y una dirección global interna; útil cuando se debe acceder a un host en el interior desde una dirección exterior fija.
- **Traducción dinámica** - Este método se asigna entre direcciones locales internas y un grupo de direcciones globales.

La figura muestra un dispositivo que traduce una dirección de origen dentro de una red a una dirección de origen fuera de la red.

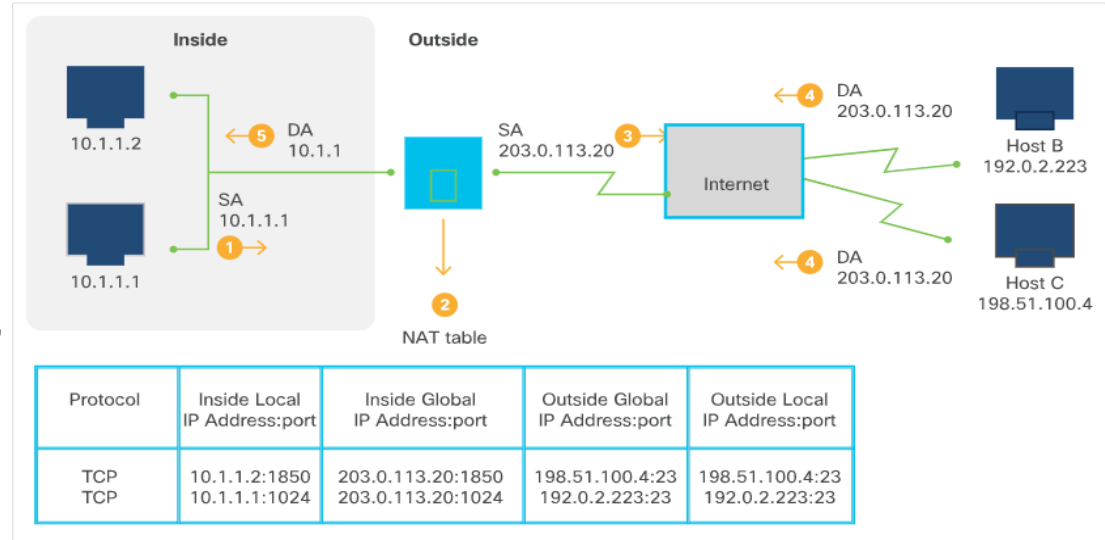


Protocolos de red


NAT (Cont.)

Sobrecarga de direcciones globales internas

- El uso de una sola dirección global para varias direcciones locales se conoce como sobrecarga.
- Cuando se configura la sobrecarga, el dispositivo NAT recopila información de protocolos de nivel superior (por ejemplo, números de puerto TCP o UDP) para traducir las direcciones globales a direcciones locales correctas.
- Para asignar varias direcciones locales a una dirección global, se utilizan números de puerto TCP o UDP para distinguir las direcciones locales. Este proceso NAT se denomina traducción de direcciones de puerto (PAT).



Packet Tracer – Explore los protocolos de red

- En este Packet Tracer, hará lo siguiente:
 - **Parte 1:** Configurar DNS
 - **Parte 2:** Configurar DHCP
 - **Parte 3:** Configurar NTP
 - **Parte 4:** Usar SSH para Configurar un Switch
 - **Parte 5:** Usar SNMP
 - **Parte 6:** Configurar HTTPS
 - **Parte 7:** Configurar EMAIL
 - **Parte 8:** Configurar FTP
- 

5.6 Solución de problemas

Problema de conectividad de la aplicación

Solución de problemas comunes de conectividad de red

- La solución de problemas de red suele seguir las capas OSI.
- Puede comenzar de arriba a abajo comenzando en la capa de aplicación y haciendo su camino hacia abajo a la capa física. O puedes ir de abajo a arriba.
- Soluciones como Cisco AppDynamics pueden ofrecer una visión más profunda del rendimiento de las aplicaciones y el análisis de la causa raíz de los problemas de las aplicaciones.

Solución de problemas comunes de conectividad de red (contd.)

- Una sesión típica de resolución de problemas que comienza desde la capa física y avanza por la pila de capas hacia la capa de aplicación:
 - Determine cómo el cliente se conecta a la red: ¿es una conexión cableada o inalámbrica?
 - Si el cliente se conecta a través de un cable Ethernet, asegúrese de que la NIC se conecte y que haya señales eléctricas que se intercambien con el puerto del switch al que está conectado el cable.
 - Si la NIC está conectada, la capa física funciona como se esperaba.
 - Si la NIC no está conectada o habilitada, verifique la configuración en el conmutador. El puerto al que se conecta el cliente puede estar apagado, o tal vez el cable que conecta al cliente al puerto de red de la pared esté defectuoso, o el cable que conecta el puerto de red desde la pared hasta el switch puede estar defectuoso.
 - La resolución de problemas en la capa física consiste en garantizar que haya cuatro pares ininterrumpidos de cables de cobre trenzados entre el cliente de red y el puerto del conmutador.
 - Si el cliente utiliza una conexión inalámbrica, compruebe si la interfaz de red inalámbrica está activada y asegúrese de permanecer dentro del alcance del punto de acceso inalámbrico.

Solución de problemas comunes de conectividad de red (cont.)

- Subiendo a la capa de enlace de datos, o Capa 2, asegúrese de que el cliente pueda aprender la MAC de destino, asegúrese de que las direcciones (usando ARP) y también que el conmutador al que se está conectando el cliente pueda aprender las direcciones MAC recibidas en su puertos.
- Si puede verificar que ambas tablas son exactas, puede pasar a la siguiente capa.
- Si el cliente no puede ver ninguna dirección MAC en su tabla ARP local, compruebe si hay listas de control de acceso de Capa 2 en el puerto del switch que puedan bloquear este tráfico. También asegúrese de que el puerto del conmutador esté configurado para la VLAN de cliente correcta.
- En la capa de red, o Capa 3, asegúrese de que el cliente obtenga la dirección IP correcta del servidor DHCP o de que esté configurado manualmente con la dirección IP correcta y la puerta de enlace predeterminada correcta.
- Si no se puede establecer la conectividad de Capa 3, compruebe las listas de acceso IP en las interfaces del router, compruebe la tabla de enrutamiento tanto en el cliente como en el router de puerta de enlace predeterminado y asegúrese de que el tráfico se enrute correctamente.
- Si la conectividad de Capa 3 se puede establecer desde el cliente hasta el destino, pase a la solución de problemas a la capa de transporte o a la Capa 4.
- Si no se puede establecer la conectividad de Capa 3, compruebe las listas de acceso IP en las interfaces del router, compruebe la tabla de enrutamiento tanto en el cliente como en el router de puerta de enlace predeterminado y asegúrese de que el tráfico se enrute correctamente.

Solución de problemas comunes de conectividad de red (cont.)

- Si no se puede establecer una conexión de transporte, compruebe los firewalls y los dispositivos de seguridad que se colocan en la ruta de tráfico para las reglas que bloquean el tráfico en función de los puertos TCP y UDP.
- Verifique si el balanceo de carga está habilitado y si el balanceador de carga funciona como se esperaba, o si algún servidor proxy que intercepte el tráfico está filtrando y denegando la conexión.
- La carga de tráfico y el retraso de la red son los más difíciles de solucionar. La implementación de QoS en toda la red puede ayudar con estos problemas.
- Si a pesar de la solución de problemas de red, no ha podido identificar ningún problema, existe una buena probabilidad de que el problema no sea con la red.

Herramientas de red: uso de ifconfig

`ifconfig` es una utilidad de software para sistemas operativos basados en UNIX. También existe una utilidad similar para los sistemas operativos basados en Microsoft Windows llamada `ipconfig`.

El objetivo principal de esta utilidad es administrar, configurar y supervisar las interfaces de red y sus parámetros.

`Ifconfig` se ejecuta como una herramienta de interfaz de línea de comandos y viene instalado por defecto con la mayoría de los sistemas operativos.

Los usos comunes de `ifconfig` son:

Configure la dirección IP y la máscara de subred para las interfaces de red.

Consulta el estado de las interfaces de red.

Habilitar o deshabilitar interfaces de red.

Cambie la dirección MAC en una interfaz de red Ethernet.

Solución de problemas de conectividad de aplicaciones

Herramientas de red —

Uso de ifconfig (Contd.)

- Al ejecutar el comando `ifconfig --help` en la interfaz de línea de comandos, se mostrarán todas las opciones disponibles con esta versión de `ifconfig`.

`ifconfig` nos da la opción de agregar (add) o del (eliminar) direcciones IP y su máscara de subred (longitud de prefijo) a una interfaz de red específica.

- El `hw ether` nos da la opción de cambiar la dirección MAC de Ethernet.

```
devasc@labvm:~$ ifconfig --help
Usage:
  ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
  [add <address>[/<prefixlen>]]
  [del <address>[/<prefixlen>]]
  [[-]broadcast [<address>]] [[-]pointopoint [<address>]]
  [netmask <address>] [dstaddr <address>] [tunnel <address>]
  [outfill <NN>] [keepalive <NN>]
  [hw <HW> <address>] [mtu <NN>]
  [[-]trailers] [[-]arp] [[-]allmulti]
  [multicast] [[-]promisc]
  [mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
  [txqueuelen <NN>]
  [[-]dynamic]
  [up|down] ...
<output omitted>
```

Herramientas de red: uso de ifconfig (cont.)

- Si `ifconfig` se emite sin ningún parámetro, simplemente devuelve el estado de todas las interfaces de red en ese host.
- MTU es la Unidad de transmisión máxima y especifica el número máximo de bytes que la trama puede transmitirse en este medio antes de ser fragmentada.
- Los paquetes RX y los bytes RX contienen los valores de los paquetes y bytes recibidos respectivamente en esa interfaz.

```
devasc@labvm:~$ ifconfig
dummy0: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 1500
    inet 192.0.2.1  netmask 255.255.255.255  broadcast 0.0.0.0
    inet6 fe80::48db:6aff:fe27:4849  prefixlen 64  scopeid 0x20<link>
    ether 4a:db:6a:27:48:49  txqueuelen 1000  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 12293  bytes 2544763 (2.5 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fee9:3de6  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:e9:3d:e6  txqueuelen 1000  (Ethernet)
    RX packets 280055  bytes 281957761 (281.9 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 112889  bytes 10175993 (10.1 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 46014  bytes 14094803 (14.0 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 46014  bytes 14094803 (14.0 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

devasc@labvm:~$
```

Herramientas de red: uso de ifconfig (cont.)

- Los paquetes TX y los bytes TX contienen los valores de los paquetes y bytes transmitidos en esa interfaz específica.
- **Nota:** El comando `ifconfig` se ha utilizado en Linux durante muchos años. Sin embargo, algunas distribuciones de Linux han desaprobado el comando `ifconfig`. El comando `ip address` se está convirtiendo en la nueva alternativa. Verá el comando `ip address` utilizado en algunas de las prácticas de laboratorio de este curso.

```
devasc@labvm:~$ ifconfig
dummy0: flags=195<UP,BROADCAST,RUNNING,NOARP> mtu 1500
    inet 192.0.2.1 netmask 255.255.255.255 broadcast 0.0.0.0
    inet6 fe80::48db:6aff:fe27:4849 prefixlen 64 scopeid 0x20<link>
    ether 4a:db:6a:27:48:49 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12293 bytes 2544763 (2.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fee9:3de6 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e9:3d:e6 txqueuelen 1000 (Ethernet)
    RX packets 280055 bytes 281957761 (281.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112889 bytes 10175993 (10.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 46014 bytes 14094803 (14.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46014 bytes 14094803 (14.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

devasc@labvm:~$
```

Uso de ping

- **ping es una utilidad de software que se utiliza para probar la accesibilidad de la red IP para hosts y dispositivos conectados a una red específica.**
- **Está disponible virtualmente en todos los sistemas operativos y es extremadamente útil para solucionar problemas de conectividad.**
- **La utilidad de ping utiliza el Protocolo de mensajes de control de Internet (ICMP) para enviar paquetes al host de destino y luego espera las respuestas de eco ICMP.**
- **Con base en este intercambio de paquetes ICMP, el ping informa errores, pérdida de paquetes, tiempo de ida y vuelta, tiempo de vida (TTL) para los paquetes recibidos, etc.**

Solución de problemas de conectividad de aplicaciones

Uso de ping (cont.)

- En Windows 10, ingrese el comando `ping` para ver su información de uso.
- La salida debe verse similar a la figura al lado.

```
C:\> ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
          [-4] [-6] target_name

Options:
  -t          Ping the specified host until stopped.
              To see statistics and continue - type Control-Break;
              To stop - type Control-C.
  -a          Resolve addresses to hostnames.
  -n count    Number of echo requests to send.
  -l size     Send buffer size.
  -f          Set Don't Fragment flag in packet (IPv4-only).
  -i TTL      Time To Live.
  -v TOS      Type Of Service (IPv4-only. This setting has been deprecated
              and has no effect on the type of service field in the IP
              Header).
  -r count    Record route for count hops (IPv4-only).
  -s count    Timestamp for count hops (IPv4-only).
  -j host-list Loose source route along host-list (IPv4-only).
  -k host-list Strict source route along host-list (IPv4-only).
  -w timeout  Timeout in milliseconds to wait for each reply.
  -R          Use routing header to test reverse route also (IPv6-only).
              Per RFC 5095 the use of this routing header has been
              deprecated. Some systems may drop echo requests if
              this header is used.
  -S srcaddr  Source address to use.
  -c compartment Routing compartment identifier.
  -p          Ping a Hyper-V Network Virtualization provider address.
  -4          Force using IPv4.
  -6          Force using IPv6.
```

C:\>

Uso de ping (cont.)

- En MacOS Catalina, ingrese el comando `ping` para ver su información de uso.
- El resultado debe parecerse a lo siguiente

```
$ ping
usage: ping [-AaDdfnoQqRrv] [-c count] [-G sweepmaxsize]
           [-g sweepminsize] [-h sweepincrsz] [-i wait]
           [-l preload] [-M mask | time] [-m ttl] [-p pattern]
           [-S src_addr] [-s packetsize] [-t timeout] [-W waittime]
           [-z tos] host
ping [-AaDdfLnoQqRrv] [-c count] [-I iface] [-i wait]
     [-l preload] [-M mask | time] [-m ttl] [-p pattern] [-S src_addr]
     [-s packetsize] [-T ttl] [-t timeout] [-W waittime]
     [-z tos] mcast-group
Apple specific options (to be specified before mcast-group or host like all options)
-b boundif          # bind the socket to the interface
-k traffic_class    # set traffic class socket option
-K net_service_type # set traffic class socket options
-apple-connect      # call connect(2) in the socket
-apple-time         # display current time
```

Uso de ping (cont.)

- En su Máquina Virtual DEVASC, agregue la opción `-help` para ver su información de uso.
- La salida debe verse similar a la figura al lado.

```
devasc@labvm:~$ ping -help

Usage
  ping [options] <destination>

Options:
  <destination>    dns name or ip address
  -a              use audible ping
  -A              use adaptive ping
  -B              sticky source address
  -c <count>      stop after <count> replies
  -D              print timestamps
  -d              use SO_DEBUG socket option
  -f              flood ping
  -h              print help and exit
<output omitted>

IPv4 options:
  -4              use IPv4
  -b              allow pinging broadcast
  -R              record route
  -T <timestamp>  define timestamp, can be one of <tsonly|tsandaddr|tsprespec>

IPv6 options:
  -6              use IPv6
  -F <flowlabel>  define flow label, default is random
  -N <nodeinfo opt> use icmp6 node info query, try <help> as argument

For more details see ping(8).
devasc@labvm:~$
```


Uso de ping (cont.)

- Por defecto, `ping` (`ping -help` en Linux) mostrará todas las opciones disponibles. Algunas de las opciones que puede especificar incluyen:
 - Recuento de cuántas solicitudes de eco ICMP desea enviar
 - Dirección IP de origen en caso de que haya varias interfaces de red en el host
 - Tiempo de espera para esperar un paquete de respuesta de eco
 - Tamaño del paquete, si desea enviar tamaños de paquete mayores que los 64 bytes predeterminados. Esta opción es muy importante a la hora de determinar cuál es la MTU en una interfaz.
- Si no recibe ninguna respuesta del destino al que está tratando de llegar con `ping`, no significa que el host esté apagado o no sea accesible. Simplemente podría significar que los paquetes de solicitud de eco ICMP están filtrados por un firewall y no se les permite llegar al destino del host.

Uso de traceroute

- traceroute muestra la ruta que toman los paquetes para mostrar la accesibilidad del host en la red
- traceroute utiliza paquetes ICMP para determinar la ruta al destino.
- En Windows 10, utilice tracert para ver las opciones disponibles como se muestra en la salida al lado.

```
C:\> tracert
```

```
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name
```

```
Options:
```

-d	Do not resolve addresses to hostnames.
-h maximum_hops	Maximum number of hops to search for target.
-j host-list	Loose source route along host-list (IPv4-only).
-w timeout	Wait timeout milliseconds for each reply.
-R	Trace round-trip path (IPv6-only).
-S srcaddr	Source address to use (IPv6-only).
-4	Force using IPv4.
-6	Force using IPv6.

```
C:\>
```

Nota: En lugar de ICMP, de forma predeterminada, Linux usa UDP y un rango de puertos alto (33434 - 33534). Los destinos a lo largo de la ruta responden con mensajes inalcanzables del puerto ICMP en lugar de las respuestas de eco enviadas en traceroutes basados en ICMP.

Uso de traceroute (Cont.)

- En MacOS, utilice `traceroute` para ver las opciones disponibles como se muestra en el siguiente resultado

```
$ traceroute
Version 1.4a12+Darwin
Usage: traceroute [-adDeFIInrSvx] [-A as_server] [-f first_ttl] [-g gateway] [-i iface]
      [-M first_ttl] [-m max_ttl] [-p port] [-P proto] [-q nqueries] [-s src_addr]
      [-t tos] [-w waittime] [-z pausesecs] host [packetlen]
```

Uso de traceroute (Cont.)

- En su Máquina Virtual DEVASC, utilice `traceroute --help` para ver las opciones disponibles como se muestra en el siguiente resultado

```
devasc@labvm:~$ traceroute --help
Usage: traceroute [OPTION...] HOST
Print the route packets trace to network host.

  -f, --first-hop=NUM      set initial hop distance, i.e., time-to-live
  -g, --gateways=GATES     list of gateways for loose source routing
  -I, --icmp               use ICMP ECHO as probe
  -m, --max-hop=NUM        set maximal hop count (default: 64)
  -M, --type=METHOD      use METHOD ('icmp' or 'udp') for traceroute
                           operations, defaulting to 'udp'
  -p, --port=PORT          use destination PORT port (default: 33434)
  -q, --tries=NUM          send NUM probe packets per hop (default: 3)
                           --resolve-hostnames    resolve hostnames
  -t, --tos=NUM            set type of service (TOS) to NUM
  -w, --wait=NUM           wait NUM seconds for response (default: 3)
  -?, --help              give this help list
                           --usage               give a short usage message
  -V, --version            print program version

Mandatory or optional arguments to long options are also mandatory or optional
for any corresponding short options.

Report bugs to <bug-inetutils@gnu.org>.
devasc@labvm:~$]
```

Uso de traceroute (Cont.)

- Hay varias opciones disponibles con `traceroute` que incluyen:
 - Especificar el valor TTL del primer paquete enviado. Por defecto, esto es 1.
 - Especificación del valor TTL máximo. De forma predeterminada, aumentará el valor TTL hasta 64 o hasta que se alcance el destino.
 - Especificar la dirección de origen en caso de que haya varias interfaces en el host.
 - Especificación del valor QoS en el encabezado IP.
 - Especificación de la longitud del paquete.

Uso de traceroute (Cont.)

- Puede utilizar el comando `tracert` desde su dispositivo Windows o `traceroute` desde su dispositivo MacOS.
- La salida al lado es de un dispositivo MacOS dentro de la red corporativa de Cisco que rastrea la ruta a uno de los servidores web de Yahoo

```
$ traceroute www.yahoo.com
traceroute: Warning: www.yahoo.com has multiple addresses; using 98.138.219.232
traceroute to atsv2-fp-shed.wg1.b.yahoo.com (98.138.219.232), 64 hops max, 52 byte packets
 1  sjc2x-dtbb.cisco.com (10.1x.y.z)  2.422 ms  1.916 ms  1.773 ms
 2  sjc2x-dt5.cisco.com (12x.1y.1z.1ww)  2.045 ms
    sjc2x-dt5-01.cisco.com (12x.1y.1z.15w)  2.099 ms  1.968 ms
 3  sjc2x-sbb5.cisco.com (1xx.1x.1xx.4y)  1.713 ms  1.984 ms
    sjc2x-sbb5-10.cisco.com (1xx.1x.1y.4w)  1.665 ms
 4  sjc2x-rbb.cisco.com (1xx.1y.zz.yyy)  1.836 ms  1.804 ms  1.696 ms
 5  sjc1x-rbb-7.cisco.com (1xx.zz.y.ww)  68.448 ms  1.880 ms  1.939 ms
 6  sjc1x-corp-0.cisco.com (1xx.yy.z.w)  1.890 ms  2.660 ms  2.793 ms
 7  * * *
 8  * * *
 9  * * *
...
61  * * *
62  * * *
63  * * *
64  * * *
```

Nota: La salida anterior se ha modificado por razones de seguridad, pero la salida debería tener tanto nombres de host como direcciones IP válidos.

Uso de nslookup

- nslookup es otra utilidad de línea de comandos utilizada para consultar DNS para obtener el nombre de dominio a la asignación de dirección IP. Esta herramienta es útil para determinar si el servidor DNS configurado en un host específico funciona como se esperaba y realmente resuelve nombres de host en direcciones IP.
- Ejecute el comando `nslookup www.cisco.com 8.8.8.8` para resolver la dirección o direcciones IP del servidor web de Cisco y especifique que desea utilizar el servidor DNS de Google en 8.8.8.8 para realizar la resolución.

```
devasc@labvm:~$ nslookup www.cisco.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e2867.dsca.akamaiedge.net.
Name:      e2867.dsca.akamaiedge.net
Address: 23.204.11.200
Name:      e2867.dsca.akamaiedge.net
Address: 2600:1404:5800:392::b33
Name:      e2867.dsca.akamaiedge.net
Address: 2600:1404:5800:39a::b33

devasc@labvm:~$
```

Packet Tracer - Solucionar problemas de red comunes

En este Packet Tracer, completará estos objetivos:

- **Parte 1:** Prueba de conectividad
- **Part 2:** Solucionar problemas en R3
- **Part 3:** Solucionar problemas en R1
- **Part 4:** Solucionar problemas en el DNS

Lab 5.6.7- Herramientas de resolución de problemas de red

En este laboratorio, hará lo siguiente:

- **Parte 1:** Iniciar la máquina virtual (Virtual Machine) de DEVASC.
- **Parte 2:** Explore la herramienta de resolución de problemas de **ifconfig**
- **Parte 3:** Explore la herramienta de resolución de problemas de **ping**
- **Parte 4:** Explore la herramienta de resolución de problemas de **tracert**
- **Parte 5:** Explore la herramienta de resolución de problemas de **nslookup**

5.7 Resumen de los fundamentos de redes

¿Qué aprendí en este módulo?

- Una red consta de dispositivos finales, como equipos, dispositivos móviles e impresoras, conectados por dispositivos de red, como conmutadores y enrutadores.
- Tanto los modelos de referencia OSI como TCP/IP utilizan capas para describir las funciones y servicios que pueden ocurrir en esa capa.
- Todos los dispositivos de red en la misma red deben tener una dirección MAC única.
- Cada dispositivo de una red tiene una dirección IP única. Una dirección IP y una dirección MAC se utilizan para el acceso y la comunicación en todos los dispositivos de red.
- Mientras que los conmutadores se utilizan para conectar dispositivos en LAN, los routers se utilizan para enrutar tráfico entre diferentes redes.
- Un firewall es un sistema de hardware o software que evita el acceso no autorizado dentro o fuera de una red.

¿Qué aprendí en este módulo? (Continuación)

- El equilibrio de carga mejora la distribución de las cargas de trabajo en varios recursos informáticos, como servidores, clústeres de servidores, enlaces de red, etc.
- El equilibrio de carga del servidor ayuda a garantizar la disponibilidad, la escalabilidad y la seguridad de las aplicaciones y los servicios al distribuir el trabajo de un único servidor entre varios servidores.
- Los diagramas de red muestran una representación visual e intuitiva de la red.
- Existen varias operaciones de red que utilizan diferentes protocolos como SSH, Telnet, DNS, http, NETCONF y RESTCONF. Cada protocolo tiene un puerto predeterminado.
- ping es una utilidad de software utilizada para probar la accesibilidad de la red IP para hosts y dispositivos conectados a una red específica.
- traceroute utiliza paquetes ICMP para determinar la ruta al destino.
- nslookup es otra utilidad de línea de comandos utilizada para consultar DNS para obtener la asignación de nombres de dominio a direcciones IP.

