Capítulo 1

Conceptos de OSPFv2 de área única

Características y funciones de OSPF

Introducción a OSPF

- El protocolo OSPF es un protocolo de routing de estado de enlace desarrollado como alternativa del protocolo de routing por vector de distancias, RIP. OSPF presenta ventajas importantes en comparación con RIP, ya que ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes.
- OSPF es un protocolo de routing sin clase que utiliza el concepto de áreas para realizar la escalabilidad. Un administrador de red puede dividir el dominio de enrutamiento en áreas distintas que ayudan a controlar el tráfico de actualización de enrutamiento.
  - Un vínculo es una interfaz de un router, un segmento de red que conecta dos routers o una red auxiliar, como una LAN Ethernet conectada a un único router.
  - La información acerca del estado de dichos enlaces se conoce como estados de enlace. Toda la información del estado del vínculo incluye el prefijo de red, la longitud del prefijo y el costo.
- Este módulo cubre implementaciones y configuraciones básicas de OSPF de área única.

Características y funciones de OSPF

- Todos los protocolos de routing comparten componentes similares. Todos usan mensajes de protocolo de routing para intercambiar información de la ruta. Los mensajes contribuyen a armar estructuras de datos, que luego se procesan con un algoritmo de routing.
- Los routers que ejecutan OSPF intercambian mensajes para transmitir información de routing por medio de cinco tipos de paquetes.
  - Paquete de saludo
  - Paquete de descripción de la base de datos
  - Paquete de solicitud de estado de enlace
  - Paquete de actualización de estado de enlace
  - Paquete de acuse de recibo de estado de enlace
- Estos paquetes se usan para descubrir routers vecinos y también para intercambiar información de routing a fin de mantener información precisa acerca de la red.

Características y funciones de OSPF

Componentes de OSPF

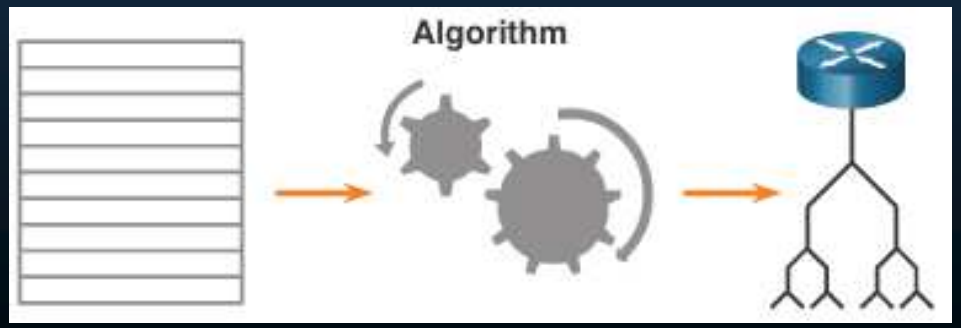
Los mensajes OSPF se utilizan para crear y mantener tres bases de datos OSPF, como se indica a continuación:

Base de datos	Tabla	Descripción
Base de datos de adyacencia	Tabla de vecinos	•Lista de todos los routers vecinos con los que un router estableció comunicación bidireccional. •Esta tabla es única para cada router. •Se puede ver con el **comando** show ip ospf neighbor
Base de datos de estado de enlace (LSDB)	Tabla de topología	•Muestra información sobre todos los otros routers en la red. •Esta base de datos representa la topología de la red. •Todos los routers dentro de un área tienen LSDB idénticas. •Se puede ver con el**comando** show ip ospf database
Base de datos de reenvío	Tabla de routing	•Lista de rutas generada cuando se ejecuta un algoritmo en la base de datos de estado de enlace. •La tabla de routing de cada router es única y contiene información sobre cómo y dónde enviar paquetes para otros routers. •Se puede ver con el **comando** show ip route.

Características y funciones de OSPF

Componentes de OSPF

- El router arma la tabla de topología; para ello, utiliza los resultados de cálculos realizados a partir del algoritmo SPF (Primero la ruta más corta) de Dijkstra. El algoritmo SPF se basa en el costo acumulado para llegar a un destino.
- El algoritmo SPF crea un árbol SPF posicionando cada router en la raíz del árbol y calculando la ruta más corta hacia cada nodo. Luego, el árbol SPF se usa para calcular las mejores rutas. OSPF coloca las mejores rutas en la base de datos de reenvío, que se usa para crear la tabla de routing.



Características y funciones de OSPF

Operación Link-State

A fin de mantener la información de routing, los routers OSPF realizan el siguiente proceso genérico de routing de estado de enlace para alcanzar un estado de convergencia: Los siguientes son los pasos de enrutamiento de estado de vínculo que completa un router:

1. Establecimiento de adyacencias de vecinos
2. Intercambio de anuncios de estado de enlace
3. Crear la base de datos de estado de vínculo
4. Ejecución del algoritmo SPF
5. Elija la mejor ruta

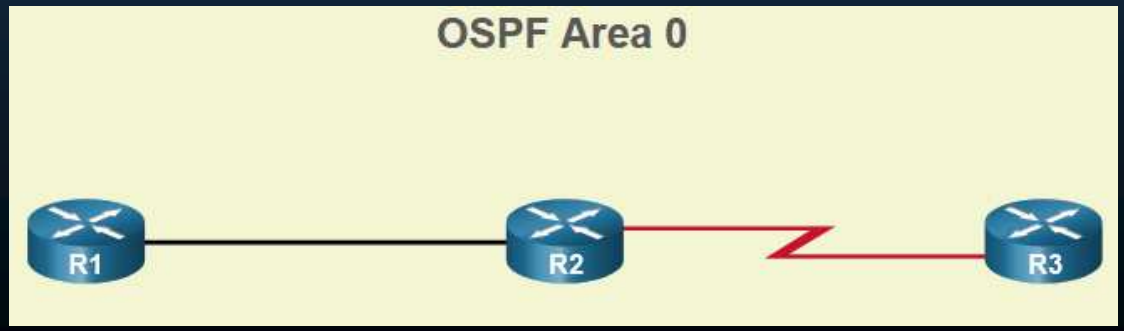
Características y funciones de OSPF

OSPF área única y multiárea

Para que OSPF sea más eficaz y escalable, este protocolo admite el routing jerárquico mediante áreas. Un área OSPF es un grupo de routers que comparten la misma información de estado de enlace en sus LSDB. El OSPF se puede implementar de una de estas dos maneras:

- **OSPF de área única**: todos los routers están en un área. La mejor práctica es usar el área 0.
- **Multiarea OSPF** - OSPF se implementa mediante varias áreas, de manera jerárquica. Todas las áreas deben conectarse al área troncal (área 0). Los routers que interconectan las áreas se denominan “routers fronterizos de área” (ABR).

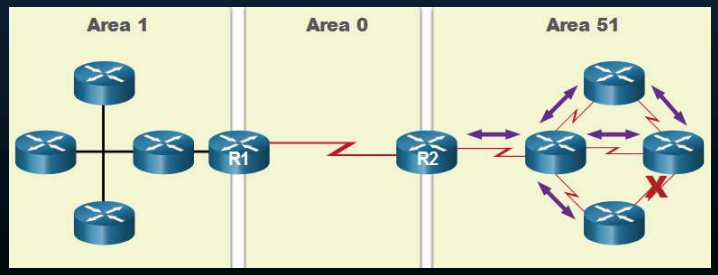
Este capítulo se centra en OSPF de área única.



Características y funciones de OSPF

Multiarea OSPF

- Las opciones de diseño de topología jerárquica con OSPF multiárea pueden ofrecer estas ventajas:
  - **Tablas de enrutamiento más pequeñas** : las tablas son más pequeñas porque hay menos entradas de tabla de enrutamiento. Esto se debe a que las direcciones de red se pueden resumir entre áreas. La sumarización de ruta no está habilitada de manera predeterminada.
  - **Sobrecarga de actualizaciones de estado de enlace reducida** - el diseño de OSPF multiárea con áreas más pequeñas minimiza el procesamiento y los requisitos de memoria.
  - **Menor frecuencia de cálculos de SPF** -– Multiarea OSPF localiza el impacto de un cambio de topología dentro de un área. Por ejemplo, minimiza el impacto de las actualizaciones de routing debido a que la saturación con LSA se detiene en el límite del área.



Características y funciones de OSPF

OSPFv3

- OSPFv3 es el equivalente a OSPFv2 para intercambiar prefijos IPv6. OSPFv3 intercambia información de routing para completar la tabla de routing de IPv6 con prefijos remotos.
  - **Nota**: con la característica de familias de direcciones de OSPFv3, esta versión del protocolo es compatible con IPv4 e IPv6. En este currículo no se hablará de familias de direcciones de OSPF.
- OSPFv3 tiene la misma funcionalidad que OSPFv2, pero utiliza IPv6 como transporte de la capa de red, por lo que se comunica con peers OSPFv3 y anuncia rutas IPv6. OSPFv3 también utiliza el algoritmo SPF como motor de cómputo para determinar las mejores rutas a lo largo del dominio de routing.
- OSPFv3 tiene procesos diferentes de los de su equivalente de IPv4. Los procesos y las operaciones son básicamente los mismos que en el protocolo de routing IPv4, pero se ejecutan de forma independiente.

Paquetes OSPF

Tipos de Paquetes OSPF

La tabla resume los cinco tipos diferentes de paquetes de estado de enlace (LSP) utilizados por OSPFv2. OSPFv3 tiene tipos de paquetes similares.

Tipo	Nombre del paquete	Descripción
1	Saludo	Descubre los vecinos y construye adyacencias entre ellos
2	Descriptores de bases de datos (DBD)	Controla la sincronización de bases de datos entre routers.
3	Solicitud de link-state (LSR)	Solicita registros específicos de estado de enlace de router a router
4	Actualización de link-state (LSU)	Envía los registros de estado de enlace específicamente solicitados
5	Acuse de recibo de estado de enlace (LSAck)	Reconoce los demás tipos de paquetes

Paquetes OSPF

Actualizaciones de estado de enlace

- Los paquetes LSU también se usan para reenviar actualizaciones de routing OSPF. Un paquete LSU puede contener 11 tipos de LSA OSPFv2 OSPFv3 cambió el nombre de varias de estas LSA y también contiene dos LSA adicionales.
- LSU y LSA a menudo se utilizan indistintamente, pero la jerarquía correcta es que los paquetes LSU contienen mensajes LSA.

LSUs

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	DBD	Checks for database synchronization between routers
3	LSR	Requests specific link-state records from router to router
4	LSU	Sends specifically requested link-state records
5	LSAck	Acknowledges the other packet types

LSAs

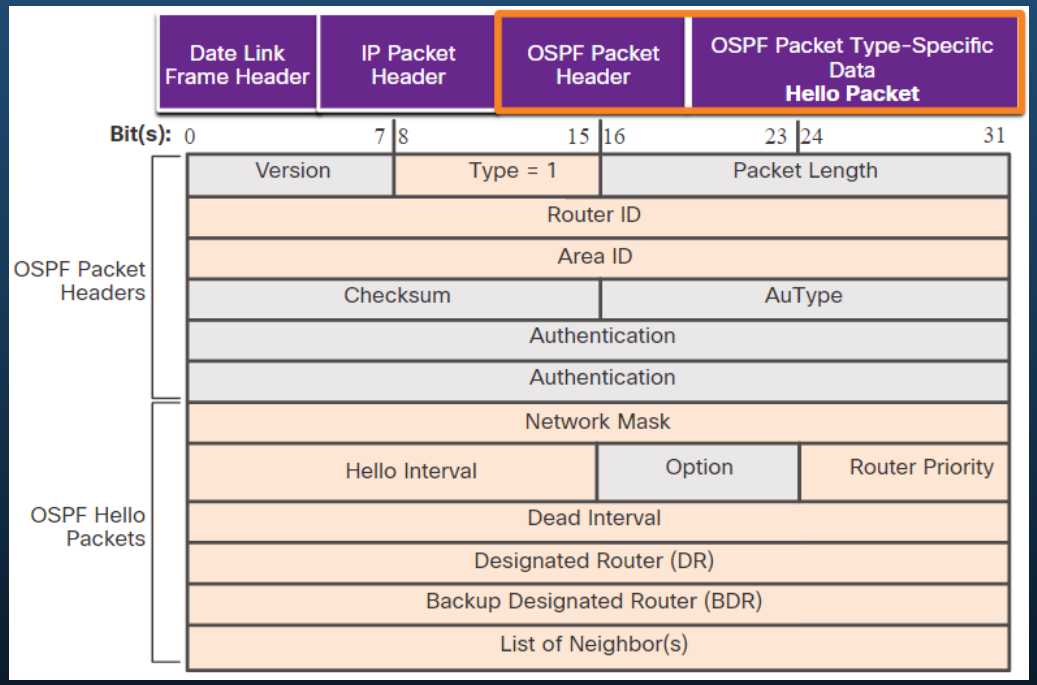
LSA Type	Description
1	Router LSAs
2	Checks for database synchronization between routers
3 or 4	Summary LSAs
5	Autonomous System External LSAs
6	Multicast OSPF LSAs
7	Defined for Not-So-Stubby Areas
8	External Attributes LSA for Border Gateway Patrol (BGPs)

Paquetes OSPF

Paquete de saludo

El paquete OSPF de tipo 1 es el paquete de saludo. Los paquetes Hello se utilizan para hacer lo siguiente:

- Descubrir vecinos OSPF y establecer adyacencias de vecinos.
- Publicar parámetros en los que dos routers deben acordar convertirse en vecinos.
- Elige el router designado (DR) y el router designado de respaldo (BDR) en redes multiacceso, como Ethernet. Los enlaces punto a punto no requieren DR o BDR.



Funcionamiento de OSPF

Estados operativos de OSPF

Estado	Descripción
Estado inactivo	•Ningún paquete de saludo recibido = Down. •El router envía paquetes de saludo. •Transición al estado Init.
Estado Init	•Se reciben los paquetes de saludo del vecino. •Estos contienen la ID del router emisor. •Transición al estado Two-Way.
Estado Two-Way	•En este estado, la comunicación entre los dos routers es bidireccional. •En los enlaces de acceso múltiple, los routers eligen una DR y una BDR. •Transición al estado ExStart.

Funcionamiento de OSPF

Estados operativos de OSPF

Estado	Descripción
Estado ExStart	En redes punto a punto, los dos routers deciden qué router iniciará el intercambio de paquetes DBD y deciden sobre el número de secuencia de paquetes DBD inicial.
Estado de intercambio	•Los routers intercambian paquetes DBD. •Si se requiere información adicional del router, se realiza la transición a Loading; de lo contrario, se realiza la transición al estado Full.
Estado Loading	•Las LSR y las LSU se usan para obtener información adicional de la ruta. •Las rutas se procesan mediante el algoritmo SPF. •Transición al estado Full.
Estado Full	La base de datos de estado de vínculo del router está completamente sincronizada.

Funcionamiento de OSPF

Establecimiento de adyacencias de vecinos

- Para determinar si hay un vecino OSPF en el vínculo, el router envía un paquete Hello que contiene su ID de router fuera de todas las interfaces habilitadas para OSPF. El paquete Hello se envía a la dirección de multidifusión IPv4 224.0.0.5 reservada- Todos los routers OSPF. Sólo los enrutadores OSPFv2 procesarán estos paquetes.
- El proceso OSPF utiliza la ID del router OSPF para identificar cada router en el área OSPF de manera exclusiva. La ID de router es un número de 32 bits con formato similar a una dirección IP que se asigna para identificar un router de forma exclusiva entre pares OSPF.
- Cuando un router vecino con OSPF habilitado recibe un paquete de saludo con una ID de router que no figura en su lista de vecinos, el router receptor intenta establecer una adyacencia con el router que inició la comunicación.

Funcionamiento de OSPF

Establecimiento de adyacencias de vecinos

Los routers de proceso utilizan para establecer adyacencia en una red multiacceso:

1	Down to Init State	Cuando OSPFv2 está habilitado en la interfaz, R1 pasa de Down a Init y comienza a enviar OSPFv2 Hellos fuera de la interfaz en un intento de descubrir vecinos.
2	Estado Init	Cuando un R2 recibe un saludo del router R1 previamente desconocido, agrega el ID del router R1 a la lista de vecinos y responde con un paquete Hello que contiene su propio ID de router.
3	Estado Two-Way	R1 recibe saludo de R2 y nota que el mensaje contiene el ID del enrutador R1 en la lista de vecinos de R2. R1 agrega el ID del enrutador de R2 a la lista de vecinos y realiza transiciones al estado de dos vías. Si R1 y R2 están conectados con un enlace punto a punto, pasan a ExStart Si R1 y R2 están conectados a través de una red Ethernet común, se produce la elección DR/BDR.
4	Elección del DR y el BDR	Se produce la elección de DR y BDR, donde el router con el ID de router más alto o la prioridad más alta se elige como DR, y el segundo más alto es el BDR

Funcionamiento de OSPF

Sincronización de las bases de datos OSPF

Después del estado Two-Way, los routers pasan a los estados de sincronización de bases de datos. Este es un proceso de tres pasos, como sigue:

- Decidir primer router: el router con el ID de router más alto envía su DBD primero.
- DBDs de Exchange: tantos como sea necesario para transmitir la base de datos. El otro router debe reconocer cada DBD con un paquete LSack.
- Enviar un LSR: Cada router compara la información DBD con el LSDB local. Si el paquete DBD tiene una entrada de estado de enlace más actual, el router pasa al estado Loading.

Después de cumplir con todas las LSR para un router determinado, los routers adyacentes se consideran sincronizados y en estado Full. Se envían actualizaciones (LSU):

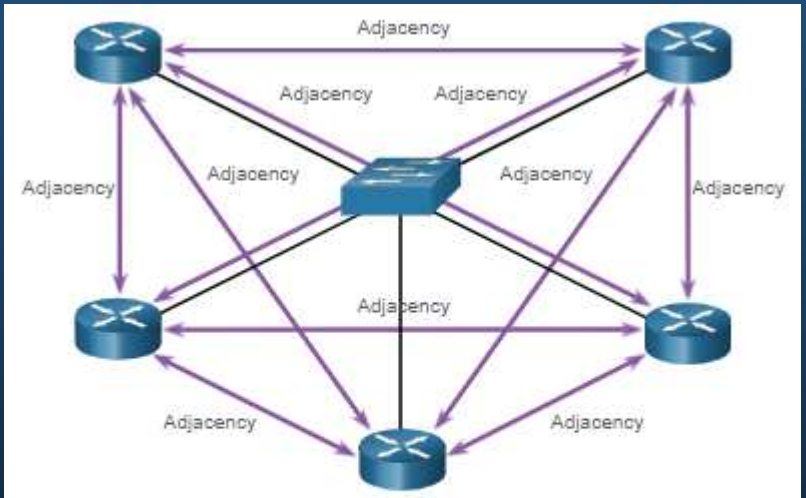
- Cuando se percibe un cambio (actualizaciones incrementales).
- Cada 30 minutos.

Funcionamiento de OSPF

La necesidad de una recuperación ante desastres

Las redes multiacceso pueden crear dos retos para OSPF en relación con la saturación de las LSA:

- **Creación de varias adyacencias** -las redes Ethernet podrían interconectar muchos routers OSPF con un enlace común. La creación de varias adyacencias con cada router conduciría al intercambio de una cantidad excesiva de LSA entre routers en la misma red.
- **Saturación intensa con LSA** - Los routers de estado de enlace saturan con sus LSA cada vez que se inicializa OSPF o cuando se produce un cambio en la topología. Esta saturación puede llegar a ser excesiva.



Funcionamiento de OSPF

LSA Inundación con DR

- Un aumento en el número de routers en una red multiacceso también aumenta el número de LSA intercambiados entre los routers. Esta inundación de LSA afecta significativamente el funcionamiento de OSPF.
- Si cada router en una red multiacceso tuviera que saturar y reconocer todas las LSA recibidas a todos los demás routers en la misma red multiacceso, el tráfico de la red se volvería bastante caótico.
- En las redes multiacceso, OSPF elige un DR como punto de recolección y distribución de las LSA enviadas y recibidas. También se elige un BDR en caso de que falle el DR. Todos los otros routers se convierten en DROTHER. Un DROTHER es un router que no funciona como DR ni como BDR.
- **Nota**: El DR se utiliza solo para la transmisión de LSA. El router seguirá usando el mejor router de siguiente salto indicado en la tabla de routing para el reenvío de los demás paquetes.

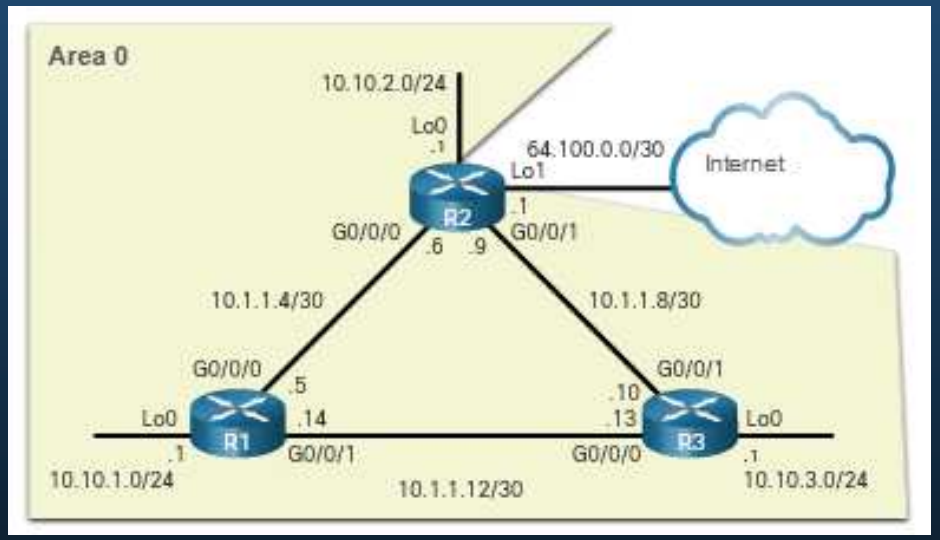
Capítulo 2

Configuración OSPFv2 de área única

Router ID de OSPF

Topología OSPF de referencia

En la ilustración, se muestra la topología que se usa para configurar OSPFv2 en este módulo. Los routers en la topología tienen una configuración inicial, incluidas las direcciones de interfaz. En este momento, ninguno de los routers tiene configurado enrutamiento estático o enrutamiento dinámico. Todas las interfaces en los routers R1, R2 y R3 (excepto la interfaz loopback en el R2) se encuentran dentro del área troncal de OSPF. El router ISP se usa como gateway a Internet del dominio de enrutamiento



Router ID de OSPF

Modo de configuración del router OSPF

OSPFv2 se habilita con el comando **router ospf** *process-id* del modo de configuración global. El valor de *process-id* representa un número entre 1 y 65 535, y lo elige el administrador de redes. El valor de *process-id* es localmente significativo. Se considera una práctica recomendada utilizar el mismo *process-id* en todos los routers OSPF.

```
R1(config)# router ospf 10
R1 (config-router) # ?
  area OSPF: Parámetros del area
  auto-cost: Calcula el costo de la interfaz OSPF según el ancho de banda
  default-information: Controla la distribución de la información predeterminada
  distance: Define una distancia administrativa
  exit: Salir del modo de configuración del protocolo de enrutamiento
  log-adyacency-changes: Registra cambios en estado de adyacencia
  neighbor: Especifica un router vecino
  network: Habilita el enrutamiento en una red IP
  no: Negar un comando o establecer sus valores predeterminados
  passive-interface: Suprime las actualizaciones de enrutamiento en una interfaz
  redistribute: Redistribuye información desde otro protocolo de enrutamiento
  router-id: router-id para este proceso OSPF
R1(config-router)#
```

Router ID de OSPF

Router ID

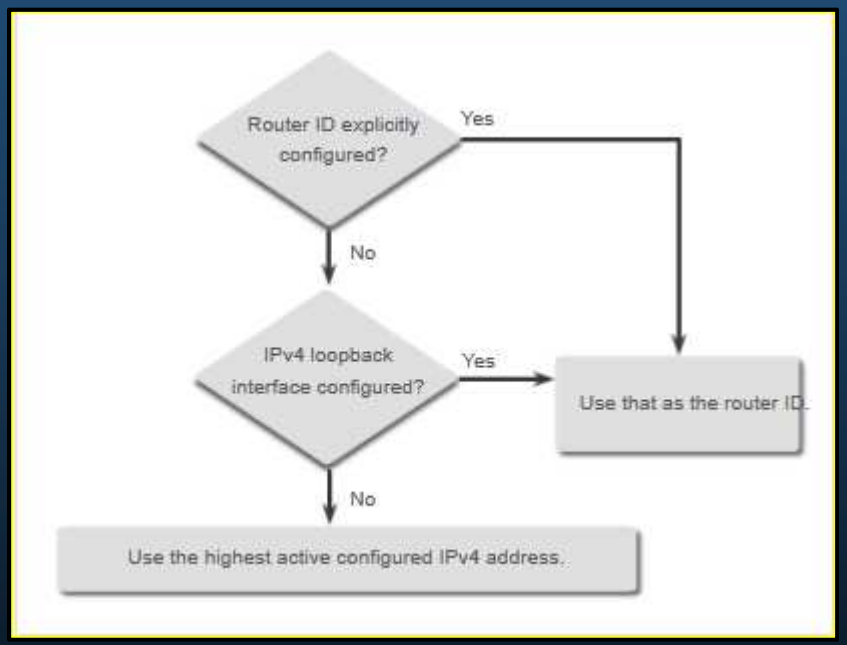
- El router ID de OSPF es un valor de 32 bits, representado como una dirección IPv4. Se utiliza para identificar de forma única un router OSPF y todos los paquetes OSPF incluyen el router ID del router de origen.
- Para participar en un dominio OSPF, cada router requiere de un router ID. Puede ser definido por un administrador o asignado automáticamente por el router. El router ID es utilizado por un router habilitado por OSPF para hacer lo siguiente:
  - **Participar en la sincronización de bases de datos OSPF** : durante el estado de Exchange, el router con el router ID más alto enviará primero sus paquetes de descriptor de base de datos (DBD).
  - **Participar en la elección del router designado (DR)** - En un entorno LAN multiacceso, el router con el router ID más alto se elige el DR. El dispositivo de enrutamiento con el segundo router ID más alto, se elige como el router designado de respaldo (BDR).

Router ID de OSPF

Orden de precedencia del Router ID

Los routers Cisco derivan el router ID según uno de los tres criterios, en el siguiente orden preferencial:

1. El router ID se configura explícitamente utilizando el comando **router-id** *rid* router de modo de configuración. Este es el método recomendado para asignar un router ID
2. El router elige la dirección IPv4 más alta de cualquiera de las interfaces de loopback configuradas.
3. El router elige la dirección IPv4 activa más alta de cualquiera de sus interfaces físicas.



Router ID de OSPF

Uso de una interfaz de bucle invertido como router ID

En lugar de confiar en la interfaz física, el router ID se puede asignar a una interfaz loopback. Normalmente, la dirección IPv4 para este tipo de interfaz loopback debe configurarse utilizando una máscara de subred de 32 bits (255.255.255.255). Esto crea una ruta de host. Una ruta de host de 32 bits no se anuncia como ruta a otros routers OSPF.

OSPF no necesita estar habilitado en una interfaz para que esa interfaz se elija como el router ID.

```
R1(config-if)# interface Loopback 1
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

Router ID de OSPF

Configure explícitamente un Router ID

En nuestra topología de referencia, el router ID para cada router se asigna de la siguiente manera:

- R1 usa el router ID 1.1.1.1
- R2 usa el router ID 2.2.2.2
- R3 usa el router ID 3.3.3.3

Utilice el comando **router-id***rid* router para asignar manualmente un router ID. En el ejemplo, el router ID 1.1.1.1 se asigna a R1. Utilice el comando **show ip protocols** para verificar el router ID.

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
*May 23 19:33:42.689: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

Router ID de OSPF

Modifique el router ID

- Después de que un router selecciona el router ID, un router OSPF activo no permitirá que el router ID cambie, hasta que el router se reinicie o el proceso de OSPF sea restablecido.
- El método preferido para restablecer el router ID es borrar el proceso OSPF.

```
R1# show ip protocols | include Router ID
Router ID 10.10.1.1
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
R1(config-router)# end
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
*Jun 6 01:09:46.975: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/1 from FULL to
DOWN, Neighbor Down: Interface down or detached
*Jun 6 01:09:46.981: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/1 from LOADING
to FULL, Loading Done *
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

Redes punto a punto OSPF

La sintaxis del comando de red

- Puede especificar las interfaces que pertenecen a una red punto a punto configurando el comando **network** . También puede configurar OSPF directamente en la interfaz con el comando **ip ospf** .
- La sintaxis básica del comando **network** es la siguiente:

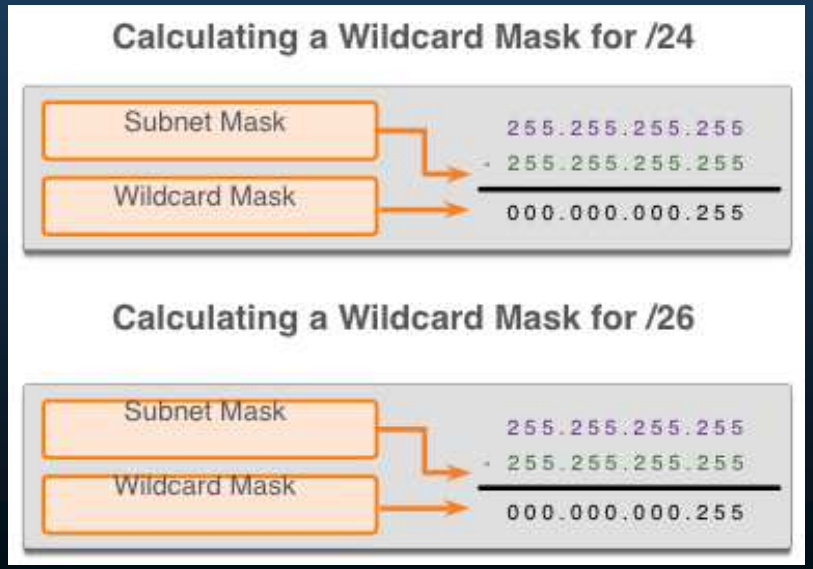
```
Router(config-router)# network network-address wildcard-mask area area-id
```

- La sintaxis *de wildcard mask de dirección de red* se utiliza para habilitar OSPF en las interfaces. Cualquier interfaz en un router que coincida con esta parte del comando está habilitada para enviar y recibir paquetes OSPF.
- La sintaxis del **area** *area-id* se refiere al área OSPF. Al configurar OSPFv2 de área única, el comando **network** debe configurarse con el mismo valor de *area-id* en todos los routers. Si bien se puede usar cualquier ID de área, es aconsejable utilizar una ID de área 0 con OSPFv2 de área única. Esta convención facilita la tarea si posteriormente se modifica la red para admitir OSPFv2 multiárea.

Redes punto a punto OSPF

El Wildcard Mask

- El wildcard mask suele ser la inversa de la máscara de subred configurada en esa interfaz.
- El método más fácil para calcular un wildcard mask es restar la máscara de subred de red de 255.255.255.255, como se muestra para las máscaras de subred / 24 y / 26 en la figura.



Redes punto a punto OSPF

Configurar OSPF mediante el comando network

Dentro del modo de configuración de enrutamiento, hay dos formas de identificar las interfaces que participarán en el proceso de enrutamiento OSPFv2.

- En el primer ejemplo, el wildcard mask identifica la interfaz en función de las direcciones de red. Cualquier interfaz activa configurada con una dirección IPv4 perteneciente a esa red participará en el proceso de enrutamiento OSPFv2.
- **Nota**: Algunas versiones de IOS permiten introducir la máscara de subred en lugar del wildcard mask. Luego, IOS convierte la máscara de subred al formato del wildcard mask.

```
R1(config)# router ospf 10
R1 (config-router) # network 10.10.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.4 0.0.0.3 area 0
R1 (config-router) # network 10.1.1.12 0.0.0.3 area 0
R1(config-router)#
```

Redes punto a punto OSPF

Configure OSPF mediante el comando network

- Como alternativa, OSPFv2 se puede habilitar especificando la dirección IPv4 exacta de la interfaz usando un wildcard mask cuádruple cero. Al ingresar **network 10.1.1.5 0.0.0.0 area 0** en R1 le dice al router que habilite la interfaz Gigabit Ethernet 0/0/0 para el proceso de enrutamiento.
- La ventaja de especificar la interfaz es que no se necesita calcular el wildcard mask. Observe que en todos los casos, el argumento **area** específica el área 0.

```
R1(config)# router ospf 10
R1 (config-router) # network 10.10.1.1 0.0.0.0 area 0
R1 (config-router) # network 10.1.1.5 0.0.0.0 area 0
R1 (config-router) # network 10.1.1.14 0.0.0.0 area 0
R1(config-router)#
```

Redes punto a punto OSPF

Configure OSPF mediante el comando ip ospf

Para configurar OSPF directamente en la interfaz, utilice el comando en modo de configuración **ip ospf** interface. La sintaxis es la siguiente:

```
Router(config-if)# ip ospf process-id area area-id
```

Elimine los comandos de red utilizando la forma **no** del comando. Luego vaya a cada interfaz y configure el comando **ip ospf**

```
R1(config)# router ospf 10
R1 (config-router) # no network 10.10.1.1 0.0.0.0 area 0
R1 (config-router) # no network 10.1.1.5 0.0.0.0 area 0
R1 (config-router) # no network 10.1.1.14 0.0.0.0 area 0
R1(config-router)# interface GigabitEthernet 0/0/0
R1 (config-if) # ip ospf 10 área 0
R1(config-if)# interface GigabitEthernet 0/0/1
R1 (config-if) # ip ospf 10 área 0
R1(config-if)# interface Loopback 0
R1 (config-if) # ip ospf 10 área 0
R1(config-if)#
```

Redes punto a punto OSPF

Configurar interfaces pasivas

De manera predeterminada, los mensajes OSPF se reenvían por todas las interfaces con OSPF habilitado. Sin embargo, estos mensajes solo necesitan enviarse por las interfaces que se conectan a otros routers con OSPF habilitado.

El envío de mensajes innecesarios en una LAN afecta la red de tres maneras:

- **Uso ineficaz del ancho de banda** -se consume el ancho de banda disponible con el transporte de mensajes innecesarios.
- **Uso ineficaz de los recurso:** - Todos los dispositivos en la LAN deben procesar el mensaje y, finalmente, descartarlo.
- **Mayor riesgo de seguridad** : sin configuraciones de seguridad OSPF adicionales, los mensajes OSPF se pueden interceptar con software de detección de paquetes. Las actualizaciones de routing se pueden modificar y enviar de regreso al router, lo que daña la tabla de routing con métricas falsas que direccionan erróneamente el tráfico.

Redes punto a punto OSPF

Configure las interfaces pasivas

- Utilice el comando **passive-interface** del modo de configuración del router para evitar la transmisión de mensajes de routing a través de una interfaz del router y permitir que se anuncie esa red a otros routers.
- El comando **show ip protocols** se utiliza para verificar que la interfaz Gigabit Ethernet es pasiva.

```
R1(config)# router ospf 10
R1(config-router)# passive-interface loopback 0
R1(config-router)# end
R1#
*May 23 20:24:39.309: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip protocols
*** IP Routing is NSF aware ***
(output omitted)
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Loopback0
    GigabitEthernet0/0/1
    GigabitEthernet0/0/0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      01:01:48
    2.2.2.2              110      01:01:38
  Distance: (default is 110)
R1#
```

Redes punto a punto OSPF

OSPF Punto a Punto

De forma predeterminada, los routers Cisco eligen DR y BDR en las interfaces Ethernet, incluso si solo hay otro dispositivo en el enlace. Puede verificarlo con el comando **show ip ospf interface** . El proceso de elección de DR/ BDR es innecesario ya que solo puede haber dos routers en la red punto a punto entre R1 y R2. Observe en la salida que el router ha designado el tipo de red como Broadcast.

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
        0 1 no no Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 10.1.1.6
  Backup Designated router (ID) 1.1.1.1, Interface address 10.1.1.5
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
```

Redes punto a punto OSPF

Redes OSPF punto a punto

Para cambiar esto a una red punto a punto, utilice el comando de configuración de interfaz **ip ospf network point-to-point** en todas las interfaces en las que desee deshabilitar el proceso de elección DR/BDR.

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf network point-to-point
*Jun 6 00:44:05.208: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
*Jun 6 00:44:05.211: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from
LOADING to FULL, Loading Done
R1(config-if)# end
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
```

Redes punto a punto OSPF

Loopbacks y Redes OSPF punto a punto

- Utilice loopbacks para proporcionar interfaces adicionales para una variedad de propósitos. De forma predeterminada, las interfaces loopback se anuncian como rutas de host /32.
- Para simular una LAN real, la interfaz de loopback se puede configurar como una red punto a punto para anunciar la red completa.
- Lo que R2 ve cuando R1 anuncia la interfaz de loopback tal cual:

```
R2# show ip route | include 10.10.1
O 10.10.1.1/32 [110/2] via 10.1.1.5, 00:03:05, GigabitEthernet0/0/0
```

- Cambio en la configuración en R1:

```
R1(config-if)# interface Loopback 0
R1(config-if)# ip ospf network point-to-point
```

- Resultado en R2:

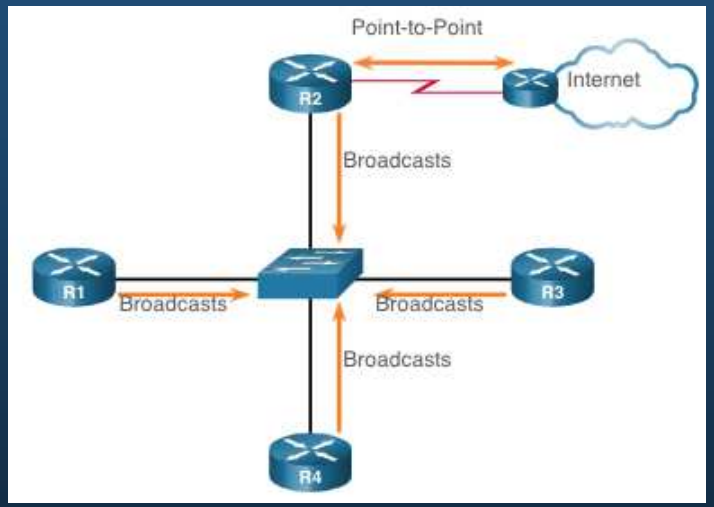
```
R2# show ip route | include 10.10.1
O 10.10.1.0/24 [110/2] via 10.1.1.5, 00:03:05, GigabitEthernet0/0/0
```

Redes OSPF de acceso múltiple

Tipos de red OPSF

Otro tipo de red que utiliza OSPF es la red OSPF multiacceso. Las redes OSPF multiacceso son únicas, ya que un router controla la distribución de los LSA.

El router elegido para este rol debe ser determinado por el administrador de red a través de la configuración adecuada.



Redes OSPF de acceso múltiple

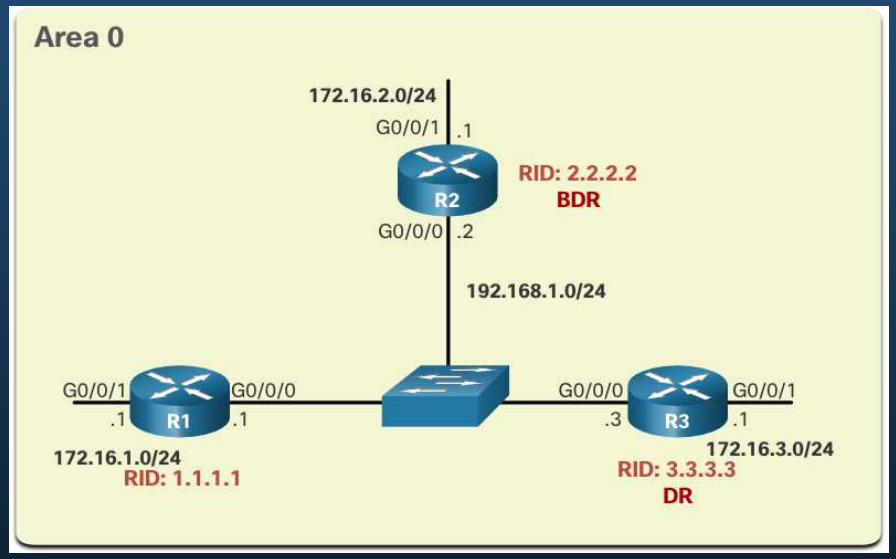
Router designado

- En redes multiacceso, OSPF elige un DR y un BDR. El DR es responsable de recolectar y distribuir los LSA enviados y recibidos. El DR usa la dirección multicast de IPv4 224.0.0.5 que está destinada a todos los routers OSPF.
- También se elige un BDR en caso de que falle el DR. El BDR escucha este intercambio en forma pasiva y mantiene una relación con todos los routers. Si el DR deja de producir paquetes Hello, el BDR se asciende a sí mismo y asume la función de DR.
- Todos los demás routers se convierten en DROTHER (un router que no es DR ni BDR). Los dispositivos de acceso múltiple utilizan la dirección 224.0.0.6 (todos los routers designados) para enviar paquetes OSPF a DR y BDR. Sólo DR y BDR escuchan 224.0.0.6.

Redes OSPF de acceso múltiple

Topología de referencia de multiacceso OSPF

- En la topología de acceso múltiple que se muestra en la figura, hay tres routers interconectados a través de una red de acceso múltiple Ethernet común, 192.168.1.0/24.
- Debido a que los routers están conectados a través de una red de acceso múltiple común, OSPF ha elegido automáticamente un DR y BDR. R3 ha sido elegido como DR porque su router ID es 3.3.3.3, que es la más alta en esta red. El R2 es el BDR porque tiene el segundo router ID más alta en la red.



Redes OSPF de acceso múltiple

Verificar las funciones del router OSPF

Para comprobar las funciones del OSPFv2, utilice el comando **show ip ospf interface**.

El resultado generado por R1 confirma que lo siguiente:

- El R1 no es el DR ni el BDR, sino un DROTHER con una prioridad predeterminada de 1. (Línea 7)
- El DR es el R3 el router ID 3.3.3.3 en la dirección IPv4 192.168.1.3; el BDR es el R2 con el router ID 2.2.2.2 en la dirección IPv4 192.168.1.2. (Líneas 8 y 9)
- El R1 tiene dos adyacencias: una con el BDR y otra con el DR. (Líneas 20 a 22)

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  (output omitted)
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  (output omitted)
  Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
  Adjacent with neighbor 3.3.3.3 (Designated Router)
  Suppress hello for 0 neighbor(s)
R1#
```

Redes OSPF de acceso múltiple

Verificanr las funciones del router OSPF

El resultado generado por R2 confirma lo siguiente:

- El R2 es el BDR, con una prioridad predeterminada de 1. (Línea 7)
- El DR es el R3 el router ID 3.3.3.3 en la dirección IPv4 192.168.1.3; el BDR es el R2 con el router ID 2.2.2.2 en la dirección IPv4 192.168.1.2. (Líneas 8 y 9)
- El R2 tiene dos adyacencias, una con un vecino que tiene el router ID 1.1.1.1 (R1) y la otra con el DR. (Líneas 20 a 22)

```
R2# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.2/24, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  (output omitted)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated Router (ID) 2.2.2.2, Interface address 192.168.1.2
  (output omitted)
  Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 1.1.1.1
  Adjacent with neighbor 3.3.3.3 (Designated Router)
  Suppress hello for 0 neighbor(s)
R2#
```

Redes OSPF de acceso múltiple

Verificar las funciones del router OSPF

El resultado generado por R3 confirma lo siguiente:

- El R3 es el DR, con una prioridad predeterminada de 1. (Línea 7)
- El DR es el R3 el router ID 3.3.3.3 en la dirección IPv4 192.168.1.3; el BDR es el R2 con el router ID 2.2.2.2 en la dirección IPv4 192.168.1.2. (Líneas 8 y 9)
- El R3 tiene dos adyacencias, una con un vecino que tiene el router ID 1.1.1.1 (R1) y la otra con el BDR. (Líneas 20 a 22)

```
R3# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.3/24, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  (output omitted)
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated Router (ID) 2.2.2.2, Interface address 192.168.1.2
  (output omitted)
  Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 1.1.1.1
  Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R3#
```

Redes OSPF de acceso múltiple

Verifique adyacencias DR/BDR

Para comprobar las adyacencias OSPFv2, utilice comando **show ip ospf neighbor** El estado de los vecinos en las redes de acceso múltiple puede ser el siguiente:

- **FULL/DROTHER** - Este es un router DR o BDR que está completamente adyacente con un router que no sea DR o BDR Estos dos vecinos pueden intercambiar paquetes Hello, actualizaciones, consultas, respuestas y acuses de recibo.
- **FULL/BDR** - El router está completamente adyacente con el vecino DR indicado Estos dos vecinos pueden intercambiar paquetes Hello, actualizaciones, consultas, respuestas y acuses de recibo.
- **FULL/BDR** - El router es completamente adyacente con el vecino BDR indicado. Estos dos vecinos pueden intercambiar paquetes Hello, actualizaciones, consultas, respuestas y acuses de recibo.
- **2-WAY/DROTHER** - El router que no es DR o BDR tiene una relación vecina con otro router no DR o BDR Estos dos vecinos intercambian paquetes Hello.

En general, el estado normal de un router OSPF es FULL. Si un router está atascado en otro estado, es un indicio de que existen problemas en la formación de adyacencias. La única excepción a esto es el estado 2-WAY, que es normal en una red broadcast multiacceso.

Redes OSPF de acceso múltiple

Verificar adyacencias DR/BDR

El resultado generado por R2 confirma que R2 tiene adyacencias con los siguientes routers:

- El R1 con el router ID 1.1.1.1 está en estado Full, y su función no es ni DR ni BDR.
- El R3 con el router ID 3.3.3.3 está en estado Full y cumple la función de DR.

```
R2# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
1.1.1.1 1 FULL/DROTHER 00:00:31 192.168.1.1 GigabiteThernet0/0/0
3.3.3.3 1 FULL/DR  00:00:34 192.168.1.3 GigabitEthernet0/0/0 R2#
```

Redes OSPF de acceso múltiple

Proceso de elección de DR/BDR predeterminado

La decisión de elección del DR y el BDR OSPF se hace según los siguientes criterios, en orden secuencial:

1. Los routers en la red seleccionan como DR al router con la prioridad de interfaz más alta. El router con la segunda prioridad de interfaz más alta se elige como BDR.
   - La prioridad puede configurarse para que sea cualquier número entre 0 y 255.
   - Si el valor de prioridad de la interfaz se establece en 0, esa interfaz no se puede elegir como DR ni BDR.
   - La prioridad predeterminada de las interfaces broadcast de acceso múltiple es 1.
2. Si las prioridades de interfaz son iguales, se elige al router con la ID más alta como DR. El router con el segundo router ID más alto es el BDR.

- El proceso de elección tiene lugar cuando el primer router con una interfaz habilitada para OSPF está activo en la red. Si no terminaron de arrancar todos los routers en la red multiacceso, es posible que un router con un router ID más bajo se convierta en el DR.
- La adición de un router nuevo no inicia un nuevo proceso de elección.

Redes OSPF de acceso múltiple

Error y recuperación de DR

Una vez que se elige el DR, permanece como tal hasta que se produce una de las siguientes situaciones:

- El DR falla.
- El proceso OSPF en el DR falla o se detiene.
- La interfaz multiacceso en el DR falla o se apaga.

Si el DR falla, el BDR se asciende automáticamente a DR. Esto ocurre así incluso si se agrega otro DROTHER con una prioridad o router ID más alta a la red después de la elección inicial de DR/BDR. Sin embargo, después del ascenso de un BDR a DR, se lleva a cabo otra elección de BDR y se elige al DROTHER con la prioridad o la ID de router más alta como el BDR nuevo.

Redes OSPF de acceso múltiple

El comando ip ospf priority

- Si las prioridades de interfaz son iguales en todos los routers, se elige al router con la ID más alta como DR.
- En vez de depender del router ID, es mejor controlar la elección mediante el establecimiento de prioridades de interfaz. Esto también permite que un router sea el DR en una red y un DROTHER en otra.
- Para establecer la prioridad de una interfaz, utilice el comando **ip ospf priority** *value* , donde value es de 0 a 255.
  - Un valor de 0 no se convierte en DR o BDR.
  - Un valor de 1 a 255 en la interfaz hace más probable que el router se convierta en DR o BDR.

Redes OSPF de acceso múltiple

Configurar la prioridad OSPF

El ejemplo muestra los comandos que se utilizan para cambiar la prioridad de interfaz R1 G0/0/0 de 1 a 255 y, a continuación, restablecer el proceso OSPF.

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf priority 255
R1(config-if)# end
R1#  clear ip ospf process
Reset ALL OSPF processes? [no]: y
R1# *Jun 5 03:47:41.563: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
```

Modificar OSPFv2 de área única

Métrica de costos OSPF de Cisco

- Recuerde que un protocolo de enrutamiento utiliza una métrica para determinar la mejor ruta de un paquete a través de una red. El protocolo OSPF utiliza el costo como métrica. Un costo más bajo indica un mejor camino.
- El costo de Cisco de una interfaz es inversamente proporcional al ancho de banda de la interfaz. Por lo tanto, cuanto mayor es el ancho de banda, menor es el costo. La fórmula que se usa para calcular el costo de OSPF es la siguiente:

  Costo = ancho de banda de referencia / ancho de banda de la interfaz
- El ancho de banda de referencia predeterminado es 10^8 (100,000,000); por lo tanto, la fórmula es la siguiente:

  Costo = 100.000.000 bps/ancho de banda de la interfaz en bps
- Debido a que el valor del costo OSPF debe ser un número entero, las interfaces FastEthernet, Gigabit Ethernet y 10 GigE comparten el mismo costo. Para corregir esta situación, puede:
  - Ajuste el ancho de banda de referencia con el comando **auto-cost reference-bandwidth** en cada router OSPF.
  - Establezca manualmente el valor de coste OSPF con el comando **ip ospf cost** en las interfaces necesarias.

Modificar OSPFv2 de área única

Métrica de costos OSPF de Cisco

Consulte la tabla para obtener un desglose del cálculo de costos.

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gigabit Ethernet 10 Gbps	100,000,000	÷	10,000,000,000	0.01 = 1
Gigabit Ethernet 1 Gbps	100,000,000	÷	1,000,000,000	0.1 = 1
Fast Ethernet 100 Mbps	100,000,000	÷	100,000,000	1
Ethernet 10 Mbps	100,000,000	÷	10,000,000	1

Same Costs due to reference bandwidth

Modificar OSPFv2 de área única

Ajustar el ancho de banda de referencia

- El valor de coste debe ser un entero. Si se calcula un valor menor que un número entero, OSPF redondea al número entero más cercano. Por lo tanto, el costo OSPF asignado a una interfaz Gigabit Ethernet con el ancho de banda de referencia predeterminado de 100.000.000 bps equivaldría a 1, porque el entero más cercano para 0.1 es 0 en lugar de 1.

  Costo = 100.000.000 bps/1.000.000.000 = 1
- Por esta razón, todas las interfaces más rápidas que Fast Ethernet tendrán el mismo valor de costo de 1 que una interfaz Fast Ethernet.
- Para ayudar a OSPF a determinar la ruta correcta, se debe cambiar el ancho de banda de referencia a un valor superior a fin de admitir redes con enlaces más rápidos que 100 Mbps.

Modificar OSPFv2 de área única

Ajuste el ancho de banda de referencia

- El cambio del ancho de banda de referencia en realidad no afecta la capacidad de ancho de banda en el enlace, sino que simplemente afecta el cálculo utilizado para determinar la métrica.
- Para ajustar el ancho de banda de referencia, use el comando de configuración del router **auto-cost reference-bandwidth** *Mbps*
  - Se debe configurar este comando en cada router en el dominio OSPF.
  - Observe en el comando que el valor se expresa en Mbps; por lo tanto, para ajustar los costos de Gigabit Ethernet, utilice el comando **auto-cost reference-bandwidth 1000.** Para 10 Gigabit Ethernet, use el comando**auto-cost reference-bandwidth 10000.**
  - Para volver al ancho de banda de referencia predeterminado, use el comando **auto-cost reference-bandwidth 100**.
- Otra opción es cambiar el costo en una interfaz específica mediante el comando **ip ospfcost** .

Modificar OSPFv2 de área única

Ajuste el ancho de banda de referencia

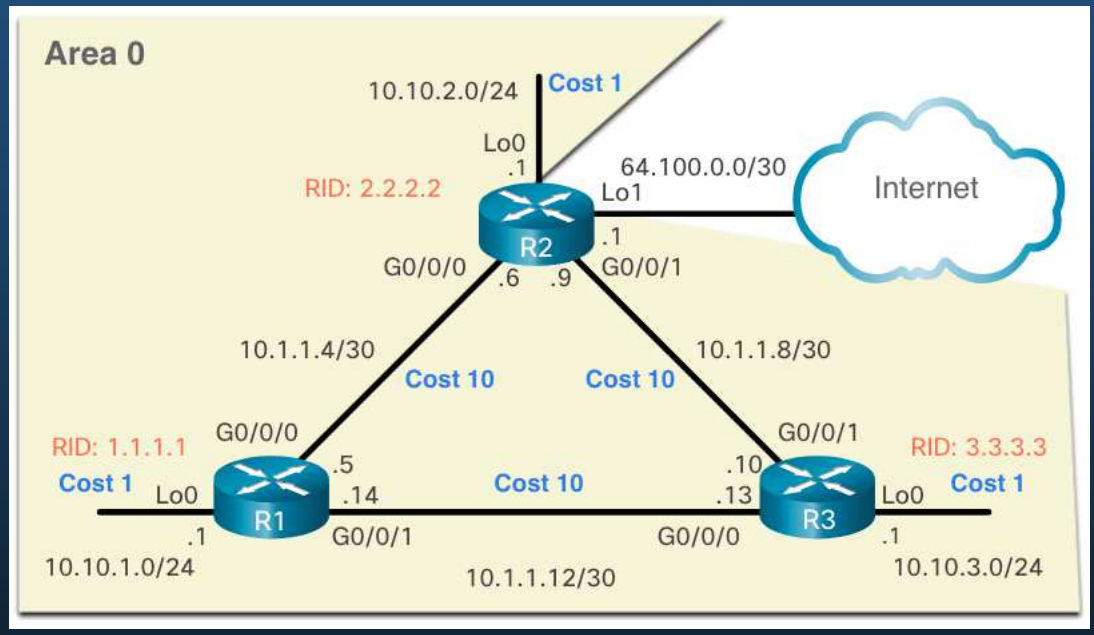
- Cualquiera que sea el método utilizado, es importante aplicar la configuración a todos los routers en el dominio de enrutamiento OSPF.
- La tabla muestra el costo de OSPF si el ancho de banda de referencia se ajusta para acomodar enlaces de 10 Gigabit Ethernet. El ancho de banda de referencia debe ajustarse cada vez que haya enlaces más rápidos que FastEthernet (100 Mbps).
- Utilice el comando **show ip ospf interface** para verificar el costo de OSPFv2 actual asignado a una interfaz.

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gigabit Ethernet 10 Gbps	10,000,000,000	÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	10,000,000,000	÷	1,000,000,000	10
Fast Ethernet 100 Mbps	10,000,000,000	÷	100,000,000	100
Ethernet 10 Mbps	10,000,000,000	÷	10,000,000	1000

Modificar OSPFv2 de área única

OSPF acumula costos

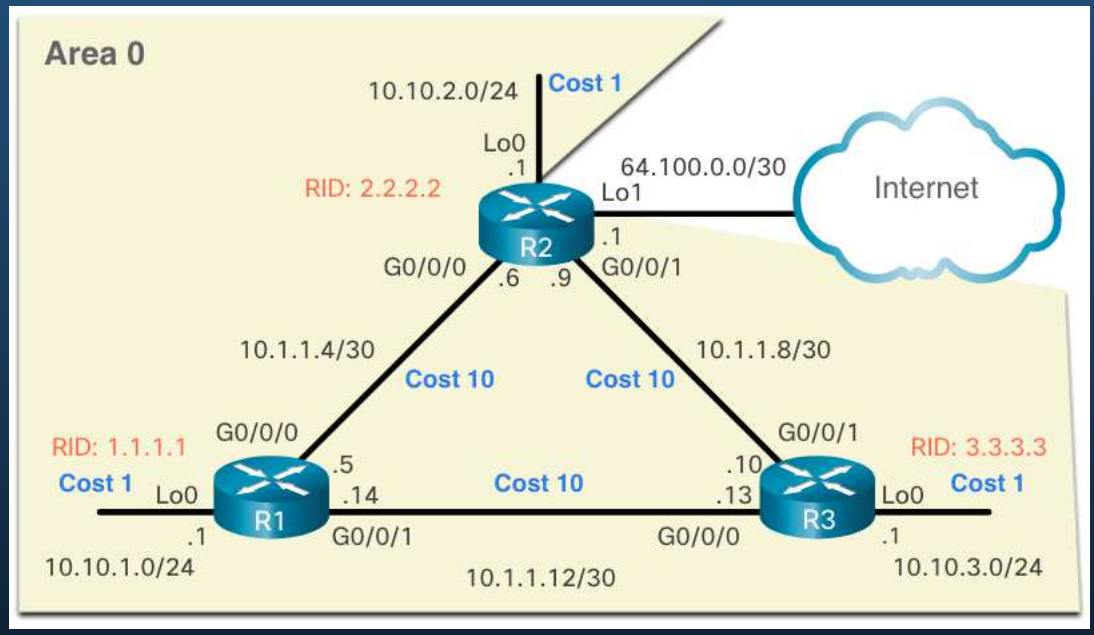
- El costo de una ruta de OSPF es el valor acumulado desde un router hasta la red de destino.
- Suponiendo que el comando **auto-cost reference-bandwidth 10000** se haya configurado en los tres routers, el costo de los enlaces entre cada router es ahora 10. Las interfaces de loopback tienen un costo predeterminado de 1.



Modificar OSPFv2 de área única

OSPF acumula costos

- Puede calcular el costo de cada router para llegar a cada red.
- Por ejemplo, el costo total de R1 para alcanzar la red 10.10.2.0/24 es 11. Esto se debe a que el vínculo al costo R2 = 10 y el costo predeterminado del bucle invertido = 1. 10 + 1 = 11.
- Esto se puede verificar mediante el comando **show ip route**.



Modificar OSPFv2 de área única

OSPF acumula costos

Verificación del costo acumulado de la ruta a la red 10.10.2.0/24:

```
R1# show ip route | include 10.10.2.0
O 10.10.2.0/24 [110/11] via 10.1.1.6, 01:05:02, GigabitEthernet0/0/0
R1# show ip route 10.10.2.0
Routing entry for 10.10.2.0/24
  Known via "ospf 10", distance 110, metric 11, type intra area
  Last update from 10.1.1.6 on GigabitEthernet0/0/0, 01:05:13 ago
  Routing Descriptor Blocks:
  * 10.1.1.6, from 2.2.2.2, 01:05:13 ago, via GigabitEthernet0/0/0
          Route metric is 11, traffic share count is 1
R1#
```

Modificar OSPFv2 de área única

Establezca manualmente el valor de costo OSPF

Las razones para establecer manualmente el valor de costo incluyen:

- Es posible que el Administrador desee influir en la selección de rutas dentro de OSPF, lo que provoca que se seleccionen rutas diferentes de lo que normalmente daría costos predeterminados y acumulación de costos.
- Conexiones a equipos de otros proveedores que utilizan una fórmula diferente para calcular el costo OSPF.

Para cambiar el valor de costo notificado por el router OSPF local a otros routers OSPF, utilice el comando de configuración de interfaz **ip ospf cost** *value*.

```
R1 (config) # interfaz g0/0/1 R1 (config-if) #
ip ospf cost 30 R1 (config-if) # interface lo0
R1 (config-if) # ip ospf cost 10 R1 (config-if)
# end
R1#
```

Modificar OSPFv2 de área única

Prueba OSPFv2 de área única a la ruta de respaldo

¿Qué sucede si el enlace entre R1 y R2 cae? Puede simular esto apagando la interfaz Gigabit Ethernet 0/0/0 y verificando que la tabla de enrutamiento se actualiza para usar R3 como router de salto siguiente. Observe que R1 ahora puede llegar a la red 10.1.1.4/30 a través de R3 con un valor de costo de 50.

```
R1# show ip route ospf | begin 10
          10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
O 10.1.1.4/30 [110/50] via 10.1.1.13, 00:00:14, GigabitEthernet0/0/1
O 10.1.1.8/30 [110/40] via 10.1.1.13, 00:00:14, GigabitEthernet0/0/1
O 10.10.2.0/24 [110/50] via 10.1.1.13, 00:00:14, GigabitEthernet0/0/1
O 10.10.3.0/24 [110/40] via 10.1.1.13, 00:00:14, GigabitEthernet0/0/1
R1#
```

Modificar OSPFv2 de área única

Hello OSPFv2 de área única

- Los paquetes Hello OSPFv2 se transmiten a la dirección multicast 224.0.0.5 (todos los routers OSPF) cada 10 segundos. Este es el valor predeterminado del temporizador en redes multiacceso y punto a punto.

Nota: Los paquetes Hello no se envían en las interfaces configuradas como pasivas mediante el comando **passive-interface**

- El intervalo Dead es el período que el router espera para recibir un paquete Hello antes de declarar al vecino como inactivo. Si el intervalo Dead caduca antes de que los routers reciban un paquete Hello, OSPF elimina ese vecino de su base de datos (LSDB). El router satura la LSDB con información acerca del vecino inactivo por todas las interfaces con OSPF habilitado. Cisco utiliza un intervalo predeterminado de cuatro veces el intervalo Hello: Esto es 40 segundos en redes de acceso múltiple y punto a punto.

Modificar OSPFv2 de área única

Modifique losIntervalos de Hello y Dead OSPFv2 de área única

- Los intervalos de Hello y Dead de OSPF pueden configurarse por interfaz.
- Los intervalos de OSPF deben coincidir, de lo contrario, no se crea una adyacencia de vecino.
- Para verificar los intervalos de la interfaz OSPFv2 configurados actualmente, use el comando **show ip ospf interface**. Los intervalos Hello y Dead Gigabit Ethernet 0/0/0 están configurados en los 10 segundos y 40 segundos predeterminados, respectivamente.

```
R1# show ip ospf interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 10
  Topology-MTID Cost Disabled Shutdown Topology Name
              0 10 no no Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
(output omitted)
```

Modificar OSPFv2 de área única

Modifique losIntervalos de Hello y Dead OSPFv2 de área única

Utilice el comando **show ip ospf neighbor** para ver el intervalo Dead contando atrás desde 40 segundos. De manera predeterminada, este valor se actualiza cada 10 segundos cuando R1 recibe un Hello del vecino.

```
R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time  Address Interface
3.3.3.3 0 FULL/ - 00:00:35 10.1.1.13 GigabiteThernet0/0/1
2.2.2.2 0 FULL/ - 00:00:31 10.1.1.6 GigabiteThernet0/0/0
R1#
```

Modificar OSPFv2 de área única

Modifique los intervalos OSPFv2

- Quizá se deseen cambiar los temporizadores de OSPF para que los routers detecten fallas en las redes en menos tiempo. Esto incrementa el tráfico, pero a veces la necesidad de convergencia rápida es más importante que el tráfico adicional que genera.

Nota: **los intervalos de Hello y Dead predeterminados se basan en prácticas recomendadas y solo deben alterarse en situaciones excepcionales.**

- Los intervalos de Hello y Dead de OSPFv2 pueden modificarse manualmente mediante los siguientes comandos del modo de configuración de interfaces:

```
Router(config-if) # ipospf hello-interval segundos
Router(config-if)# ip ospf dead-interval seconds
```

- Utilice los comandos **no ip ospf hello-interval** y **no ip ospf dead-interval** para restablecer los intervalos al valor predeterminado.

Modificar OSPFv2 de área única

Modifique los intervalos OSPFv2

- En el ejemplo, el intervalo Hello para el enlace entre R1 y R2 se cambia a 5 segundos. Cisco IOS modifica automáticamente el intervalo Dead a cuatro veces el intervalo Hello. Sin embargo, puede documentar el nuevo intervalo Dead en la configuración, configurándolo manualmente en 20 segundos, como se muestra.
- Cuando caduca el temporizador Dead en R1, R1 y R2 pierden adyacencia. R1 y R2 deben configurarse con el mismo intervalo Hello. Use el comando **show ip ospf neighbor** en el R1 para verificar las adyacencias de vecinos.

```
R1(config)# interface g0/0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
R1(config-if)#
*Jun 7 04:56:07.571: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)# end
R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
3.3.3.3 0 FULL/ - 00:00:37 10.1.1.13 GigabitEthernet0/0/1
R1#
```

Propagación de la ruta predeterminada

Propagación de una ruta estática predeterminada

Para propagar una ruta predeterminada, el router de borde (R2) debe configurarse con lo siguiente:

- Una ruta estática predeterminada, mediante el comando**ip route 0.0.0.0 0.0.0.0** [*next-hop-address* | *exit-intf*]
- El comando de configuración del router **default-information originate**. Esto ordena al R2 que sea el origen de la información de la ruta predeterminada y que propague la ruta estática predeterminada en las actualizaciones OSPF.

En el ejemplo, R2 se configura con un loopback para simular una conexión a Internet. Se configura una ruta predeterminada y se propaga a todos los demás routers OSPF del dominio de enrutamiento.

```
R2 (config) # interface lo1
R2 (config-if) # ip address 64.100.0.1 255.255.255.252
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback 1
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# end
R2#
```

Propagación de la ruta predeterminada

Verifique la ruta predeterminada propagada

- Puede verificar la configuración de ruta predeterminada en R2 usando el comando **show ip route** También puede verificar que R1 y R3 hayan recibido una ruta predeterminada.
- Observe que la fuente de ruta en R1 es **O*E2**, lo que significa que se aprendió utilizando OSPFv2. El asterisco indica que esa ruta es una buena candidata para la ruta predeterminada. La designación “E2” indica que se trata de una ruta externa. El significado de E1 y E2 está fuera del alcance de este módulo.

```
R2# show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S* 0.0.0.0/0 is directly connected, Loopback1
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
(output omitted)
```

```
R1# show ip route | begin Gateway
Gateway of last resort is 10.1.1.6 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 10.1.1.6, 00:11:08, GigabitEthernet0/0/0
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
(output omitted)
```

Verificar OSPFv2 de área única

Verifique los vecinos de OSPF

Después de configurar OSPFv2 de área única, deberá verificar sus configuraciones. Los dos comandos siguientes son particularmente útiles para verificar el enrutamiento:

- **show ip interface brief** - Esto verifica que las interfaces deseadas estén activas con el direccionamiento IP correcto.
- **show ip route**- Esto verifica que la tabla de enrutamiento contiene todas las rutas esperadas.

Entre los comandos adicionales para determinar que OSPF funciona como se esperaba se incluyen los siguientes:

- **show ip ospf neighbor**
- **show ip protocols**
- **show ip ospf**
- **show ip ospf interface**

Verificar OSPFv2 de área única

Verifique los vecinos de OSPF

- Utilice el comando **show ip ospf neighbor** para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra el router ID vecino o si este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPFv2.

Nota: Un router que no sea DR o BDR que tenga una relación de vecino con otro router que no sea DR o BDR mostrará una adyacencia bidireccional en lugar de completa.

- El siguiente resultado del comando muestra la tabla vecina de R1.

```
R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time  Address Interface
3.3.3.3 0 FULL/ - 00:00:35 10.1.1.13 GigabitEthernet0/0/1
2.2.2.2 0 FULL/ - 00:00:31 10.1.1.6 GigabitEthernet0/0/0
R1#
```

Verificar OSPFv2 de área única

Verifique los vecinos de OSPF

Dos routers pueden no formar una adyacencia OSPFv2 si ocurre lo siguiente:

- Las máscaras de subred no coinciden, esto hace que los routers se encuentren en redes separadas.
- Los temporizadores de tiempo de Hello y Dead del protocolo OSPFv2 no coinciden.
- Los tipos de redes OSPFv2 no coinciden.
- Falta un comando de red OSPFv2 o es incorrecto.

Verificar OSPFv2 de área única

Verifique configuración del protocolo OSPF

El comando **show ip protocols** es una forma rápida de verificar información vital de configuración de OSPF, como se muestra en el ejemplo del comando. Esto incluye la ID del proceso OSPFv2, el router ID, las interfaces configuradas explícitamente para anunciar las rutas OSPF, los vecinos desde los que el router recibe actualizaciones y la distancia administrativa predeterminada, que es 110 para OSPF.

```
R1# show ip protocols
*** IP Routing is NSF aware ***
(output omitted)
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
          Loopback0
          GigabitEthernet0/0/1
          GigabitEthernet0/0/0
  Routing Information Sources:
          Gateway Distance Last Update
          3.3.3.3 110 00:09:30
          2.2.2.2 110 00:09:58
  Distance: (default is 110)
R1#
```

Verificar OSPFv2 de área única

Verifique la información de proceso OSPF

El comando **show ip ospf** también se puede usar para examinar la ID del proceso OSPFv2 y el router ID, como se muestra en el siguiente resultado. Este comando muestra información de área OSPFv2 y la última vez que se ejecuto el algoritmo SPF.

```
R1# show ip ospf
Routing Process "ospf 10" with ID 1.1.1.1
Start time: 00:01:47.390, Time elapsed: 00:12:32.320
 (output omitted)
Cisco NSF helper support enabled
Reference bandwidth unit is 10000 mbps
          Area BACKBONE(0)
                    Number of interfaces in this area is 3
                    Area has no authentication
                    SPF algorithm last executed 00:11:31.231 ago
                    SPF algorithm executed 4 times
                    Area ranges are
                    Number of LSA 3. Checksum Sum 0x00E77E
                    Number of opaque link LSA 0. Checksum Sum 0x000000
                    Number of DCbitless LSA 0 Number of indication LSA 0
                    Number of DoNotAge LSA 0 Flood list length 0
R1#
```

Verificar OSPFv2 de área única

Verifique la configuración de la interfaz de OSPF

El comando **show ip ospf interface** proporciona una lista detallada de cada interfaz habilitada para OSPFv2. Especifique una interfaz para mostrar la configuración de esa interfaz. Este comando muestra el ID de proceso, el router ID local, el tipo de red, el costo OSPF, la información de DR y BDR en vínculos de acceso múltiple (no se muestra) y los vecinos adyacentes.

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 10

<output omitted>

  Neighbor Count is 1, Adjacent neighbor count is 1
          Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
R1#
```

Verificar OSPFv2 de área única

Verifique la configuración de la interfaz de OSPF

Para obtener un resumen rápido de las interfaces habilitadas para OSPFv2, use el comando **show ip ospf interface brief** como se muestra en el resultado del comando. Este comando es útil para ver información importante, incluyendo:

- Las interfaces están participando en OSPF
- Redes que se anuncian (Dirección IP/Máscara)
- Costo de cada enlace
- Estado de la red
- Número de vecinos en cada enlace

```
R1# show ip ospf interface brief
Interface PID Area IP Address/Mask Cost State Nbrs F/C
Lo0 10 0 10.10.1.1/24 10 P2P 0/0
Gi0/0/1 10 0 10.1.1.14/30 30 P2P 1/1
Gi0/0/0 10 0 10.1.1.5/30 10 P2P 1/1
R1#
```

Capítulo 3

Conceptos de Seguridad de Redes

Estado actual de la ciberseguridad

Estado actual de los casos

- Los Delincuentes Cibernéticos ahora tienen la experiencia y las herramientas necesarias para derribar la infraestructura y los sistemas críticos. Sus herramientas y técnicas continúan evolucionando.
- Mantener una red segura garantiza la seguridad de los usuarios de la red y protege los intereses comerciales. Todos los usuarios deben conocer los términos de seguridad en la tabla.

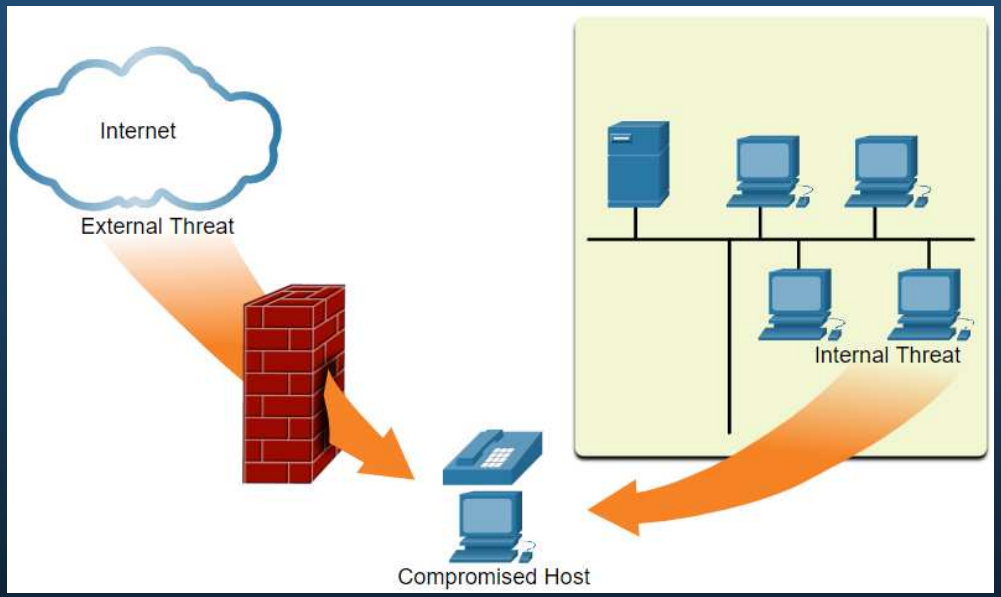
Términos de seguridad	Descripción
Activos	Un activo es cualquier cosa de valor para la organización. Incluye personas, equipos, recursos y datos.
Vulnerabilidad	Una vulnerabilidad es una debilidad en un sistema, o su diseño, que podría ser explotada por una amenaza.
Amenaza	Una amenaza es un peligro potencial para los activos, los datos o la funcionalidad de la red de una empresa.
Exploit	Un exploit es un mecanismo para tomar ventaja de una vulnerabilidad.
Mitigación	La mitigación es la contra-medida que reduce la probabilidad o la severidad de una posible amenaza o riesgo. La seguridad de Redes consiste en técnicas de mitigación múltiples.
Riesgo	El riesgo es la probabilidad de que una amenaza explote la vulnerabilidad de un activo, con el objetivo de afectar negativamente a una organización. El riesgo se mide utilizando la probabilidad de ocurrencia de un evento y sus consecuencias.

Estado actual de la ciberseguridad

Vectores de ataques de red

- Un vector de ataque es una ruta por la cual un atacante puede obtener acceso a un servidor, host o red. Los vectores de ataque se originan dentro o fuera de la red corporativa, como se muestra en la figura.

- Las amenazas internas tienen el potencial de causar mayores daños que las amenazas externas porque los usuarios internos tienen acceso directo al edificio y a sus dispositivos de infraestructura.



Estado actual de la ciberseguridad

Pérdida de datos

Pérdida o filtración de datos son los términos utilizados para describir cuándo los datos se pierden con o sin intención, son robados o se filtran fuera de la organización. La pérdida de datos puede generar:

- Daño de la marca/pérdida de la reputación
- Pérdida de la ventaja competitiva
- Pérdida de clientes
- Pérdida de ingresos
- Acciones legales que generen multas y sanciones civiles
- Costo y esfuerzo significativos para notificar a las partes afectadas y recuperarse de la transgresión

Los profesionales de seguridad de red deben proteger los datos de la organización. Se deben implementar varios controles de prevención de pérdida de datos (DLP) que combinen medidas estratégicas, operativas y tácticas.

Estado actual de la ciberseguridad

Pérdida de datos

Vectores de pérdida de datos	Descripción
Correo electrónico / Redes sociales	El correo electrónico o los mensajes de mensajería instantánea interceptados podrían capturarse y descifrar el contenido.
Dispositivos no encriptados	Si los datos no se almacenan utilizando un algoritmo de cifrado, entonces el ladrón puede extraer datos confidenciales de valor.
Dispositivos de almacenamiento en la nube	Los datos confidenciales se pueden perder si el acceso a la nube se ve comprometido debido a ajustes débiles en la seguridad.
Medios extraíbles	Un riesgo es que un empleado pueda realizar una transferencia no autorizada de datos a un dispositivo USB. Otro riesgo es que el dispositivo USB que contiene datos corporativos de valor se puede extraviar.
Respaldo físico	Los datos confidenciales deben triturarse cuando ya no sean necesarios.
Control de Acceso Incorrecto	Las contraseñas o contraseñas débiles que se hayan visto comprometidas pueden proporcionar al atacante un acceso fácil a los datos corporativos.

Atacantes

El Hacker

Un hacker es un término común usado para describir a un atacante.

Tipo de Hacker	Descripción
Hackers de Sombrero Blanco	Son hackers éticos que utilizan sus habilidades de programación para fines buenos, éticos y legales. Las vulnerabilidades en la seguridad se informan a los desarrolladores para que las corrijan antes de que las vulnerabilidades puedan aprovecharse.
Hackers de Sombrero Gris	Son personas que cometen delitos y hacen cosas probablemente poco éticas, pero no para beneficio personal o ni para causar daños. Un hacker de sombrero gris puede divulgar una vulnerabilidad de la organización afectada después de haber puesto en peligro la red.
Hackers de sombrero negro	Son delincuentes poco éticos que violan la seguridad de una computadora y una red para beneficio personal o por motivos maliciosos, como ataques a la red.

Atacantes

La evolución de los Hackers

La tabla muestra los términos de piratería moderna y una breve descripción de cada una.

Término de Piratería	Descripción
Script kiddies	Estos son adolescentes o hackers inexpertos que corren scripts, ejecutan herramientas y exploits existentes para ocasionar daño, pero generalmente no para obtener ganancias.
Agentes de Vulnerabilidad	Son generalmente hackers de sombrero gris que intentan descubrir los exploits e informarlos a los proveedores, a veces a cambio de premios o recompensas.
Hacktivistas	Estos son hackers de sombrero gris que protestan en público contra las organizaciones o gobiernos mediante la publicación de artículos, videos, la filtración de información confidencial y la ejecución de ataques a la red.
Delincuentes cibernéticos	Son hackers de sombrero negro que independientes o que trabajan para grandes organizaciones de delito cibernético.
Patrocinados por el estado	Son hackers de sombrero blanco o sombrero negro que roban secretos de gobierno, recopilan inteligencia y sabotean las redes. Sus objetivos son los gobiernos, los grupos terroristas y las corporaciones extranjeras. La mayoría de los países del mundo participan en algún tipo de hacking patrocinado por el estado.

Atacantes

Cibercriminales

Se calcula que, en todo el mundo, los cibercriminales roban miles de millones de dólares de los consumidores y las empresas.

Los cibercriminales operan en una economía clandestina donde compran, venden e intercambian herramientas de ataque, código de explotación de día cero, servicios de botnet, troyanos bancarios, keyloggers y mucho más.

También compran y venden la información privada y la propiedad intelectual que roban de sus víctimas.

Los cibercriminales apuntan a pequeñas empresas y consumidores, así como a grandes empresas e industrias.

Atacantes

Hacktivistas

Dos ejemplos de hacktivistas son Anonymous y el Ejército Electrónico Sirio.

Aunque la mayoría de los grupos hacktivistas no están bien organizados, pueden causar problemas importantes para los gobiernos y las empresas.

Los hacktivistas tienden a confiar en herramientas bastante básicas y de libre acceso.

Atacantes

Hackers patrocinados por el estado (State-Sponsored)

Los hackers informáticos patrocinados por el estado crean un código de ataque avanzado y personalizado, a menudo utilizando vulnerabilidades de software previamente no descubiertas llamadas vulnerabilidades de día cero.

Un ejemplo de un ataque patrocinado por el estado involucró el malware de Stuxnet diseñado para dañar la planta de enriquecimiento nuclear de Irán.

Herramientas del atacante

Introducción a las herramientas de Ataque

Para explotar una vulnerabilidad, un actor de amenazas debe tener una técnica o herramienta.

Con los años, las herramientas de ataque se han vuelto más sofisticadas y altamente automatizadas.

Estas nuevas herramientas requieren menos conocimiento técnico para su implementación.

Herramientas del atacante

Evolución de las herramientas de seguridad

La tabla destaca categorías de herramientas comunes de prueba de penetración. Observe cómo algunas herramientas son utilizadas por hackers de sombrero blanco y de sombrero negro. Tenga en cuenta que esta lista no es definitiva, ya que se desarrollan nuevas herramientas constantemente.

Herramientas de pruebas de penetración	Descripción
Decodificadores de contraseñas	Las herramientas para descodificar contraseñas a menudo se les conoce como herramientas de recuperación de contraseña y pueden ser usadas para decodificar o recuperar una contraseñar. Los decodificadores de contraseñas hacen intentos repetidos para averiguar la contraseña. Algunos ejemplos de herramientas para decodificar contraseñas son: John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack y Medusa.
Herramientas de Hacking Inalámbrico	Las herramientas de hacking inalámbrico se utilizan para hackear intencionalmente una red inalámbrica con el fin de detectar vulnerabilidades en la seguridad. Algunos ejemplos de herramientas de hacking inalámbrico son: Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and ViStumbler.
Escaneo de Redes y Herramientas de Hacking	Las herramientas de análisis de red se utilizan para sondear dispositivos de red, servidores y hosts para puertos TCP o UDP abiertos. Algunos ejemplos de herramientas de escaneo: Nmap, SuperScan, Angry IP Scanner y NetScanTools.
Herramientas para elaborar paquetes de prueba	Estas herramientas se utilizan para sondear y probar la solidez de un firewall usando paquetes especialmente diseñados. Algunos ejemplos son: Hping, Scapy, Socat, Yersinia, Netcat, Nping y Nemesis.
Sniffers de paquetes	Estas herramientas se utilizan para capturar y analizar paquetes dentro de redes tradicionales LAN Ethernet o WLAN. Algunas herramientas son las siguientes: Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy y SSLstrip.

Herramientas del atacante

Evolución de las Herramientas de Seguridad

Herramientas de Pruebas de Penetración	Descripción
Detectores de Rootkits	Se trata de un comprobador de integridad de archivos y directorios utilizado por hackers de sombrero blanco para detectar rootkits instalados. Algunos ejemplos de herramientas: AIDE, Netfilter y PF: OpenBSD Packet Filter.
Fuzzers para buscar Vulnerabilidades	Los fuzzers son herramientas usadas por los atacantes cuando intentan descubrir las vulnerabilidades de seguridad de una computadora. Algunos ejemplos de fuzzers: Skipfish, Wapiti y W3af.
Herramientas de Informática Forense	Estas herramientas son utilizadas por los hackers de sombrero blanco para detectar cualquier rastro de evidencia existente en una computadora. Algunos ejemplos de herramientas: Sleuth Kit, Helix, Maltego y Encase.
Depuradores	Los hackers de sombrero negro utilizan estas herramientas para aplicar ingeniería inversa en archivos binarios cuando programan ataques. También las utilizan los sombreros blancos cuando analizan malware. Algunas herramientas de depuración son las siguientes: GDB, WinDbg, IDA Pro e Immunity Debugger.
Sistemas Operativos para Hacking	Estos son sistemas operativos especialmente diseñados precargados con herramientas optimizadas para hacking. Algunos ejemplos de sistemas operativos especialmente diseñados para hacking son Kali Linux, BackBox Linux.
Herramientas de Cifrado	Las herramientas de encriptación utilizan esquemas de algoritmo para codificar los datos a fin de prevenir el acceso no autorizado a los datos encriptados. Algunos ejemplos de estas herramientas son VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN y Stunnel.
Herramientas para Atacar Vulnerabilidades	Estas herramientas identifican si un host remoto es vulnerable a un ataque de seguridad. Algunos ejemplos de herramientas de explotación de vulnerabilidades son Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit y Netsparker.
Escáneres de vulnerabilidades	Estas herramientas analizan una red o un sistema para identificar puertos abiertos. También pueden utilizarse para escanear vulnerabilidades conocidas y explorar máquinas virtuales, dispositivos BYOD y bases de datos de clientes. Algunos ejemplos de herramientas son Nipper, Core Impact, Nessus, SAINT y OpenVAS.

Herramientas del atacante

Tipos de ataques

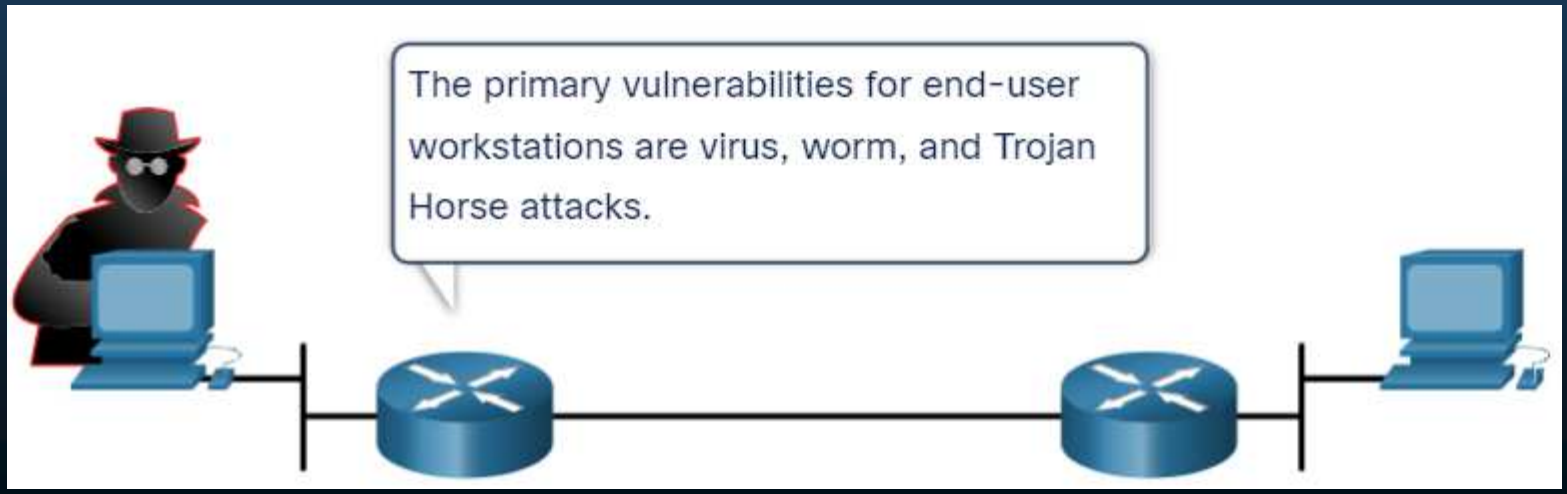
Tipo de Ataque	Descripción
Ataque de intercepción pasiva (eavesdropping)	Esto sucede cuando un hacker captura y "escucha" el tráfico de red. Este ataque también se conoce como sniffing o snooping.
Ataque de Modificación de Datos	Si los hackers han obtenido tráfico de la empresa, pueden alterar los datos en el paquete sin el conocimiento del remitente o del receptor.
Ataque de suplantación de dirección IP	Un atacante crea un paquete IP que parece provenir de una dirección válida dentro de la intranet corporativa.
Ataques basados en contraseñas	Si los harckers descubren una cuenta válida de usuario, los hackers tienen los mismos derechos que el usuario real. Los hackers pueden usar una cuenta válida para obtener listas de otros usuarios, información de red, cambios de servidor y configuraciones de red, y modificar, redirigir o borrar datos.
Ataque de Denegación de Servicio	Un ataque de DoS impide el uso normal de una computadora o red por parte de usuarios válidos. Un ataque de DoS también puede saturar una computadora o toda la red con tráfico hasta que se apaguen por sobrecarga. Un ataque de DoS también puede bloquear tráfico; eso deriva en la pérdida de acceso a recursos de red por parte de usuarios autorizados.
Ataque man-in-the-middle	Este ataque se produce cuando los hackers se colocan entre un origen y un destino. Entonces ahora pueden monitorear, capturar y controlar la comunicación en forma activa y transparente.
Ataque de Claves Comprometidas	Si un atacante obtiene una clave secreta, esa clave se conoce como una clave de riesgo. Una clave comprometida puede utilizarse para obtener acceso a una comunicación asegurada sin que el emisor ni el receptor se enteren del ataque.
Ataque de analizador de protocolos	Un analizador de protocolos es una aplicación o un dispositivo que puede leer, monitorear y capturar intercambios de datos en la red y leer paquetes de red. Si los paquetes no están cifrados, un analizador de protocolos permite ver por completo los datos que los componen.

Malware

Descripción General del Malware

- Ahora que conoce las herramientas que usan los hackers, este tema le presenta los diferentes tipos de malware que utilizan los hackers para obtener acceso a dispositivos finales.

- Los terminales son especialmente propensos a ataques de malware. Es importante saber acerca del malware porque los atacantes confían en que los usuarios instalen malware para explotar las brechas de seguridad.



Malware

Virus y Caballos de Troya

- El primer tipo de malware informático y el más común son los virus. Los virus requieren una acción humana para propagarse e infectar otros equipos.
- Se ocultan al adjuntarse al código informático, al software o a los documentos en la computadora. Cuando se abre, el virus se ejecuta e infecta el equipo.
- Los virus pueden:
  - Modificar, dañar, eliminar archivos o borrar discos duros completos.
  - Causar problemas de arranque del equipo y dañar aplicaciones.
  - Capturar y enviar información confidencial a los atacantes.
  - Acceder a cuentas de correo electrónico y utilizarlas para propagarse.
  - Permanecer inactivo hasta que el atacante lo requiera.

Malware

Virus y Caballos de Troya

Los virus modernos se desarrollan con intenciones muy específicas, como las indicadas

Tipos de virus	Descripción
Virus en el sector de arranque	El virus ataca el sector de arranque, la tabla de particiones de archivos o el sistema de archivos.
Virus de firmware	El virus ataca el firmware del dispositivo.
Virus de macros	El virus utiliza la función de macros de MS Office con fines maliciosos.
Virus del programa	El virus se introduce en otro programa ejecutable.
Virus de script	El virus ataca al intérprete del SO que se utiliza para ejecutar los scripts.

Malware

Virus y Caballos de Troya

Los atacantes usan caballos de Troya para comprometer a los hosts. Un Troyano es un programa que parece útil pero también transporta código malicioso. Los Troyanos a menudo se proporcionan con programas gratuitos en línea, como los juegos de computadora. Existen varios tipos de caballos de Troya como se describen en la tabla.

Tipo de Caballo de Troya	Descripción
Acceso remoto	El Troyano activa el acceso remoto no autorizado.
Envío de datos	El Troyano le proporciona al atacante datos confidenciales, como contraseñas.
Destructivo	El Troyano daña o elimina archivos.
Proxy	El Troyano usará el equipo de la víctima como dispositivo de origen para lanzar ataques y realizar otras actividades ilegales.
FTP	El Troyano habilita servicios no autorizados de transferencia de archivos en dispositivos finales.
Desactivador de software de seguridad	El Troyano detiene el funcionamiento de los programas antivirus o firewall.
Denegación de servicio (DoS)	Caballo de Troya de DoS: retarda o detiene la actividad de red.
Keylogger	El Troyano intenta activamente robar información confidencial, como números de tarjetas de crédito, registrando las pulsaciones de teclas efectuadas en un formulario web.

Malware

Otros Tipos de Malware

Malware	Descripción
Adware	•El Adware se suele distribuir en las descargas de software. •El Adware puede mostrar anuncios no solicitados mediante ventanas emergentes del navegador web, nuevas barras de herramientas o redireccionamientos inesperados a un sitio web diferente •Las ventanas emergentes pueden ser difíciles de controlar, ya que las modernas son más rápidas que la mano del usuario.
Ransomware	•El Ransomware generalmente cifra los archivos de la PC para que el usuario no pueda acceder a ellos y luego presenta un mensaje donde se exige un rescate para suministrar la clave de descifrado. •Los Usuarios sin copias de respaldo actualizadas deben pagar el rescate para descifrar sus archivos. •Por lo general, el pago se hace mediante transferencia bancaria o divisas criptográficas como bitcoines.
Rootkit	•Los atacantes usan los Rootkits para obtener acceso a nivel de cuenta de administrador a una PC. •Son muy difíciles de detectar porque pueden alterar el firewall, la protección antivirus, los archivos del sistema e incluso los comandos del SO para ocultar su presencia. •Pueden proveer una puerta trasera para que los atancantes accedan al equipo, carguen archivos e instalen nuevo software para utilizarlo en un ataque DDoS. •Se deben utilizar herramientas especiales para eliminar los rootkits y a veces es necesario reinstalar el sistema completo.
Spyware	•Es similar al adware, pero se utiliza para recopilar información sobre el usuario y enviarla sin su consentimiento a los atacantes. •El Spyware puede ser una amenaza menor que recopile datos de navegación, o bien, puede ser una amenaza importante que recopile información personal y financiera.
Gusano	•Es un programa que se replica a sí mismo y se propaga automáticamente sin participación del usuario, al aprovechar vulnerabilidades de software legítimo. •Utiliza la red para buscar otras víctimas con la misma vulnerabilidad. •El objetivo de los gusanos suele ser quitar velocidad o interrumpir las operaciones de redes.

Ataques de red habituales

Resumen de los Ataques de Red Habituales

- Cuando se entrega e instala malware, la carga útil puede usarse para causar una variedad de ataques relacionados con la red.
- Para mitigar los ataques, es útil comprender los tipos de ataques. Al clasificarlos, es posible abordar los ataques por tipo, en lugar de abordarlos individualmente.
- Las redes son susceptibles a los siguientes tipos de ataques:
  - Ataques de sondeo
  - Ataques de Acceso
  - Ataques de DoS

Ataques de red habituales

Ataques de Sondeo

- El sondeo se conoce como recopilación de información.
- Los atacantes utilizan ataques de sondeo para realizar la detección no autorizada y el análisis de sistemas, servicios o vulnerabilidades. Los ataques de sondeo preceden los ataques de acceso o DoS attacks.

Ataques de red habituales

Ataques de Sondeo

En la tabla se describen algunas de las técnicas utilizadas por los atacantes para realizar ataques de sondeo.

Técnica	Descripción
Realizar una consulta de información de un objetivo	El atacante está buscando información inicial sobre un objetivo. Se pueden usar varias herramientas, incluida la búsqueda de Google, páginas web de organizaciones, whois y más.
Iniciar un barrido de ping de la red de destino	La consulta de información generalmente revela la dirección de red del objetivo. El atacante ahora puede iniciar un barrido de ping para determinar cuál dirección IP está activa.
Iniciar un análisis de puertos de las direcciones IP activas	Esto se utiliza para determinar qué puertos o servicios están disponibles. Algunos ejemplos de escáneres de puertos incluyen Nmap, SuperScan, Angry IP Scanner y NetScan Tools.
Ejecutar escáneres de vulnerabilidades	Útil para consultar los puertos identificados para determinar el tipo y la versión de la aplicación y el sistema operativo que el host está ejecutando. Algunos ejemplos de herramientas son Nipper, Core Impact, Nessus, SAINT y OpenVAS.
Ejecutar herramientas de ataque	El atacante ahora intenta descubrir servicios vulnerables que pueden ser abusados. Una variedad de herramientas de explotación de vulnerabilidades existen, incluyendo: Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit y Netsparker.

Ataques de red habituales

Ataques de acceso

- Los ataques de acceso aprovechan vulnerabilidades conocidas en servicios de autenticación, servicios FTP y servicios web. El propósito de este tipo de ataques es obtener acceso a cuentas web, bases de datos confidenciales y otra información confidencial.
- Los atacantes usan ataques de acceso en dispositivos de red y computadoras para recuperar datos, obtener acceso o escalar privilegios de acceso al rol de administrador.
- **Ataques de contraseña:** En un ataque de contraseña, el atacante intenta descubrir contraseñas críticas del sistema utilizando varios métodos. Los ataques de contraseña son muy comunes y pueden iniciarse utilizando una variedad de herramientas para descifrar contraseñas.
- **Ataque Spoofing o de falsificación:** En los ataques de falsificación, el dispositivo del atacante intenta hacerse pasar por otro dispositivo falsificando datos. Los ataques comunes de suplantación de identidad incluyen suplantación de IP, suplantación de MAC y suplantación de DHCP. Estos ataques de suplantación se analizarán con más detalle más adelante en este módulo.
- Otros ataques de acceso incluyen:
  - Ataque de confianza
  - Redireccionamiento de puertos
  - Ataques de man-in-the-middle
  - Ataques de desbordamiento de búfer o Buffer overflow

Ataques de red habituales

Ataques de Ingeniería Social

- La ingeniería social es un ataque de acceso que intenta manipular a las personas para que realicen acciones o divulguen información confidencial. Algunas técnicas son presenciales, mientras que otras pueden ser por teléfono o Internet.

- Los ingenieros sociales, a menudo, se aprovechan de la disposición que tienen las personas a ayudar. También se aprovechan de las debilidades de los demás.

Ataques de red habituales

Ataques de Ingeniería Social

Ataques de Ingeniería Social	Descripción
Pretexto	Un atacante finge necesitar datos personales o financieros para confirmar la identidad del destinatario.
Suplantación de identidad (phishing)	El atacante envía un mensaje fraudulento que parece ser de una fuente legítima y confiable, para hacer que el destinatario instale malware en su dispositivo o revele información personal o financiera.
Suplantación de identidad focalizada (spear phishing)	El atacante crea un ataque de suplantación de identidad (phishing) dirigido específicamente a una persona u organización.
Correo electrónico no deseado	También conocido como correo basura, es correo electrónico no solicitado que suele contener enlaces nocivos, malware o información engañosa.
Algo por algo (something for something)	A veces se denomina "quid pro quo" y es cuando el atacante solicita información personal a cambio de algo como un obsequio.
Carnada (Baiting)	Un atacante deja deliveradamente una unidad flash infectada con malware en un sitio público. Una víctima encuentra la unidad, la coloca en su equipo portátil y sin darse cuenta instala malware.
Simulación de identidad (Impersonation)	Este tipo de ataque es donde un atacante finge ser alguien más para ganarse la confianza de la víctima.
Infiltración (tailgating)	Es un tipo de ataque presencial en el cual el atacante sigue muy de cerca a una persona autorizada para poder acceder a un área protegida.
Espiar por encima del hombro (shoulder surfing)	Es un tipo de ataque presencial en el cual el atacante mira con disimulo sobre el hombro de una persona para robar sus contraseñas u otra información.
Inspección de basura (Dumpster diving)	Tipo de ataque presencial en el cual el atacante hurga en la basura en busca de documentos confidenciales.

Ataques de red habituales

Ataques de Ingeniería Social

- El Kit de herramientas de ingeniería social (SET, Social Engineering Toolkit) fue diseñado por TrustedSec para ayudar a los hackers de sombrero blanco y a otros profesionales de seguridad de la red a crear ataques de ingeniería social para poner a prueba sus propias redes.
- Las empresas deben capacitar y educar a sus usuarios sobre los riesgos de la ingeniería social, y desarrollar estrategias para validar las identidades por teléfono, por correo electrónico o en persona.
- En la figura, se presentan las prácticas recomendadas que deben seguir todos los usuarios.

Ataques de red habituales

Ataques de DoS y DDoS

- Un ataque de Denegación de Servicio (DoS) crea algún tipo de interrupción de los servicios de red para usuarios, dispositivos o aplicaciones. Existen dos tipos principales de ataques de DoS:
  - **Cantidad abrumadora de tráfico**- el atacante envía una gran cantidad de datos a una velocidad que la red, el host o la aplicación no puede manejar. Esto hace que los tiempos de transmisión y respuesta disminuyan. También puede bloquear un dispositivo o servicio.
  - **Paquetes Mal Formateados**- El atacante envía un paquete malicioso formateado a un host o una aplicación y el receptor no puede manejarlo. Esto hace que el dispositivo receptor funcione muy lentamente o se detenga.

- Los ataques de DoS son un riesgo importante porque pueden interrumpir fácilmente la comunicación y causar una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de ejecutar, incluso si lo hace un agente de amenaza inexperto.

- Un ataque de DoS distribuida (DDoS) es similar a un ataque de DoS pero proviene de múltiples fuentes coordinadas.

Vulnerabilidades y amenazas de IP

IPv4 e IPv6

- El protocolo IP no valida si la dirección IP de origen contenida en un paquete realmente provino de esa fuente. Por eso, los atacantes pueden enviar paquetes con una dirección IP de origen falsa. Los analistas de seguridad deben entender los diferentes campos en los encabezados IPv4 e IPv6.
- Algunos de los ataques relacionados con IP más comunes se muestran en la tabla.

Técnicas de Ataque IP	Descripción
Ataques ICMP	Los atacantes utilizan paquetes de eco (pings) del protocolo de mensajería de control de Internet (ICMP) para detectar subredes y hosts en una red protegida para generar ataques de saturación de DoS y para modificar las tablas de routing de los hosts.
Ataques de Amplificación y reflexión	Los atacantes intentan impedir que usuarios legítimos tengan acceso a información o servicios.
Ataques de suplantación de direcciones	Los atacantes suplantan la dirección IP de origen en un paquete de IP para realizar suplantación blind o non-blind.
Ataques man-in-the-middle (MITM)	Los atacantes se posicionan entre un origen y un destino para monitorear, capturar y controlar la comunicación en forma transparente. Simplemente pueden escuchar en silencio mediante la inspección de paquetes capturados o modificar paquetes y reenviarlos a su destino original.
Secuestros de sesiones	Los atacantes obtienen acceso a la red física y, luego, usan un ataque de MITM para secuestrar una sesión.

Vulnerabilidades y amenazas de IP

Ataques ICMP

- Los agentes de amenaza utilizan el ICMP para los ataques de reconocimiento y análisis. Esto les permite iniciar ataques de recopilación de información para conocer la disposición de una topología de red, detectar qué hosts están activos (dentro del alcance), identificar el sistema operativo del host (identificación del SO) y determinar el estado de un firewall. Los atacantes también usan ICMP para ataques DoS.

- **Nota**: ICMP para IPv4 (ICMPv4) e ICMP para IPv6 (ICMPv6) son susceptibles a ataques similares.

- Las redes deben tener filtros estrictos de lista de control de acceso (ACL) en el perímetro de la red para evitar sondeos de ICMP desde Internet. En el caso de redes grandes, los dispositivos de seguridad (como firewalls y sistemas de detección de intrusiones o IDS) deben detectar este tipo de ataques y generar alertas para los analistas de seguridad.

Vulnerabilidades y amenazas de IP

Ataques ICMP

Los mensajes comunes de ICMP de interés para los atacantes se enumeran en la tabla.

Mensajes ICMP utilizados por los Hackers	Descripción
"Echo request" y "echo reply" de ICMP	Esto se utiliza para realizar la verificación del host y los ataques DoS.
"Unreachable" de ICMP	Se usa para realizar ataques de reconocimiento y análisis de la red.
"Mask reply" de ICMP	Se utiliza para alcanzar una red IP interna.
"Redirect" de ICMP	Se utiliza para lograr que un host de destino envíe todo el tráfico a través de un dispositivo atacado y crear un ataque de MITM.
"Router discovery" de ICMP	Se usa para inyectar rutas falsas en la tabla de routing de un host de destino.

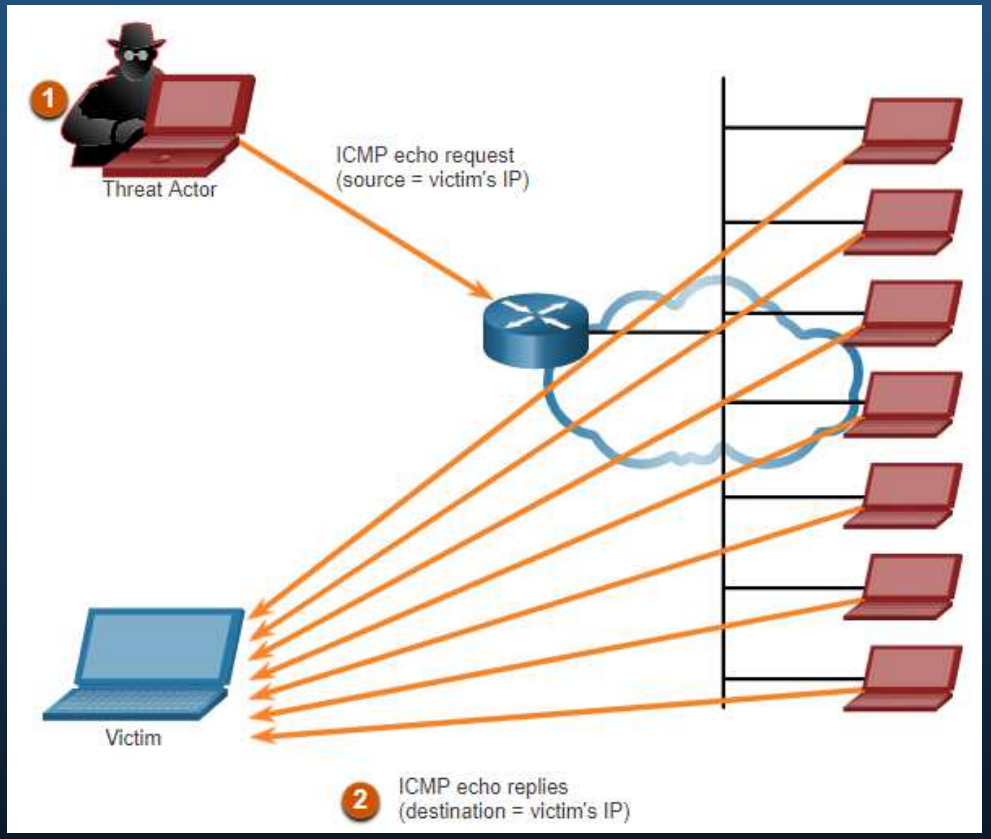
Vulnerabilidades y amenazas de IP

Ataques de reflejo y amplificación

- Los atacantes suelen usar técnicas de amplificación y reflejo para crear ataques de DoS. En la figura se ilustra cómo se usa un ataque "Smurf" para abrumar un host objetivo.

Nota: Ahora se utilizan nuevas formas de ataques de amplificación y reflejo, como ataques de amplificación y reflejo con base en DNS y ataques de amplificación de NTP.

- Los atacantes también utilizan ataques de agotamiento de recursos de un host objetivo a fin de que deje de funcionar o para consumir los recursos de una red.



Vulnerabilidades y amenazas de IP

Ataques de Suplantación de Direcciones

- Los ataques de suplantación de dirección IP se producen cuando un atacante crea paquetes con información falsa de la dirección IP de origen para ocultar la identidad del remitente o hacerse pasar por otro usuario legítimo. La suplantación de dirección IP suele formar parte de otro ataque denominado ataque Smurf.

- Los ataques de Suplantación pueden ser "blind" (ciegos) o "non-blind" (no ciegos):
  - **Suplantación no ciega (Non-blind spoofing)**: El atacante puede ver el tráfico que se envía entre el host y el destino. Esta técnica determina el estado de un firewall y la predicción del número de secuencia. También puede secuestrar una sesión autorizada.
  - **Suplantación ciega (blind spoofing)**: El atacante no puede ver el tráfico que se envía entre el host y el destino. Este tipo de ataque se utiliza en ataques de DoS.

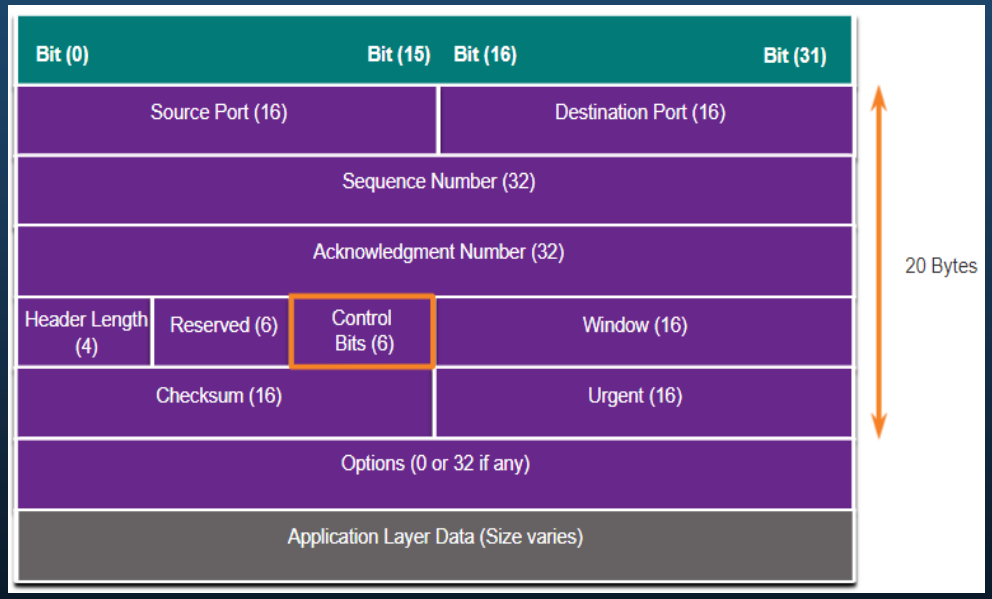
- Los ataques de suplantación de dirección MAC se utilizan cuando los atacantes tienen acceso a la red interna. Los atacantes cambian la dirección MAC de su host para que coincida con otra dirección MAC conocida de un host de destino.

Vulnerabilidades de TCP y UDP

Encabezado de segmento TCP

- La información de segmento de TCP aparece inmediatamente después del encabezado de IP. Los campos del segmento de TCP y Bits de control aparecen en la figura.

- Los siguientes son los seis bits de control del segmento TCP:
  - **URG** - campo indicador urgente significativo
  - **ACK** - campo de reconocimiento significativo
  - **PSH** - función de empuje
  - **RST**- restablecer la conexión
  - **SYN**- sincronizar números de secuencia
  - **FIN** - no hay más datos del emisor



Vulnerabilidades de TCP y UDP

Servicios TCP

El TCP ofrece los siguientes servicios:

- **Entrega confiable**- TCP incorpora reconocimientos para garantizar la entrega. Si no se recibe un acuse de recibo oportuno, el emisor retransmite los datos. Requerir acuses de recibo de los datos recibidos puede causar retrasos sustanciales. Algunos ejemplos de los protocolos de capa de aplicación que hacen uso de la confiabilidad de TCP incluyen HTTP, SSL/TLS, FTP y transferencias de zona DNS.

- **Control de flujo**- el TCP implementa el control de flujo para abordar este problema. En lugar de confirmar la recepción de un segmento a la vez, varios segmentos se pueden confirmar con un único acuse de recibo.

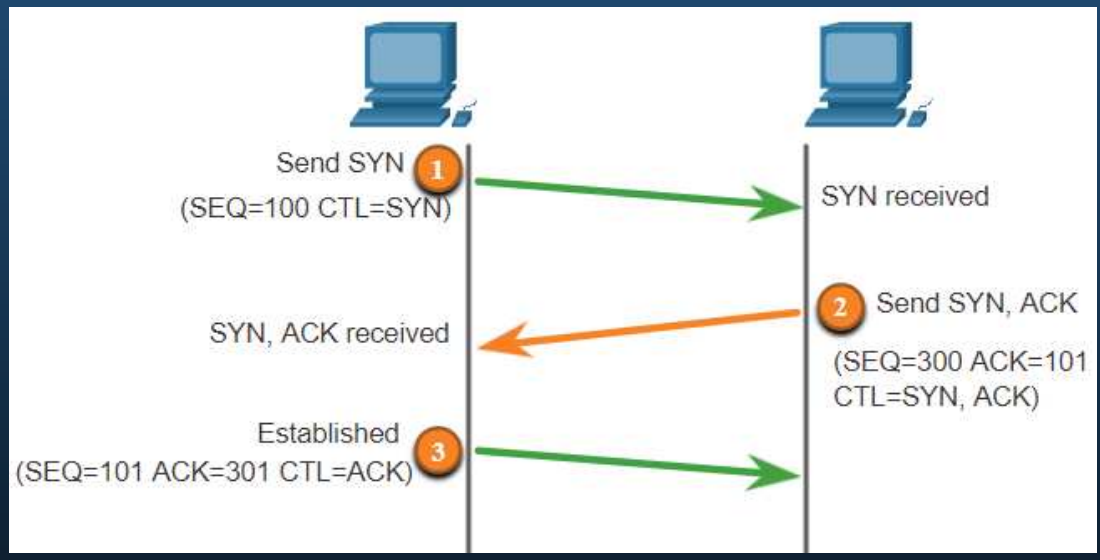
- **Comunicación con estado**- la comunicación con estado del TCP entre dos partes ocurre gracias a la comunicación tridireccional de TCP.

Vulnerabilidades de TCP y UDP

Servicios TCP

Una **conexión TCP** se establece en tres pasos:

1. El cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.
2. El servidor acusa recibo de la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.
3. El cliente de origen acusa recibo de la sesión de comunicación de servidor a cliente.

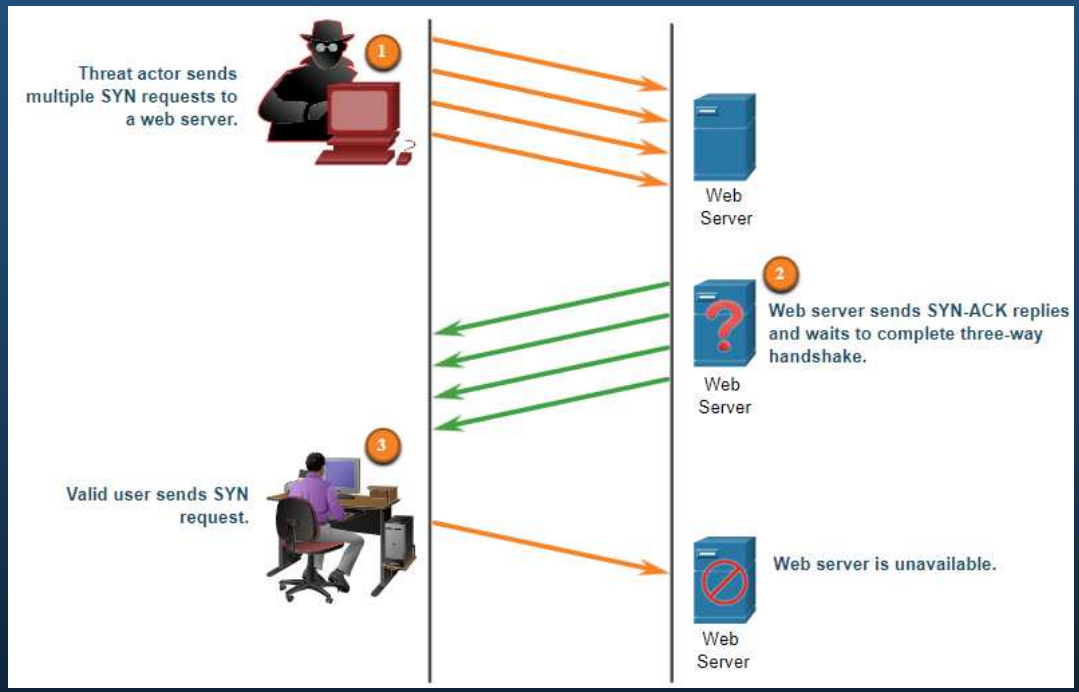


Vulnerabilidades de TCP y UDP

Ataques de TCP

Ataque de Inundación SYN a TCP

1. El atacante envía múltiples solicitudes SYN a un servidor web.
2. El servidor web responde con SYN-ACK para cada solicitud SYN y espera para completar el protocolo de enlace de tres vías. El actor de la amenaza no responde a los SYN-ACK.
3. Un usuario válido no puede acceder al servidor web porque el servidor web tiene demasiadas conexiones TCP a medio abrir.



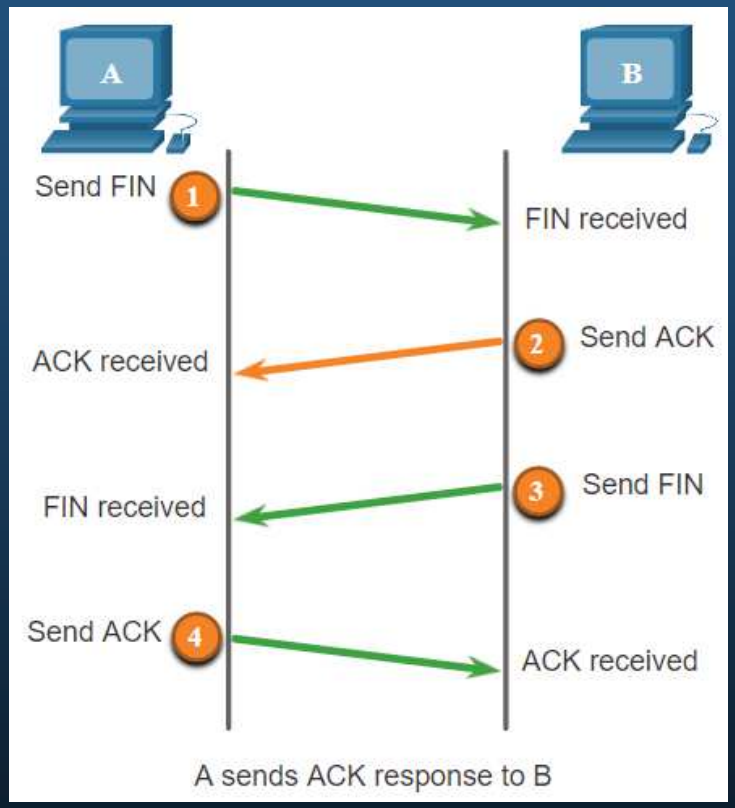
Vulnerabilidades de TCP y UDP

Ataques de TCP

La finalización de una sesión TCP utiliza el siguiente proceso de intercambio de cuatro vías:

1. Cuando el cliente no tiene más datos para enviar en la transmisión, envía un segmento con el indicador FIN establecido.
2. El servidor envía un ACK para acusar recibo del FIN para terminar la sesión de cliente a servidor.
3. El servidor envía un FIN al cliente para terminar la sesión de servidor a cliente.
4. El cliente responde con un ACK para dar acuse de recibo del FIN desde el servidor.

Un atacante podría efectuar un ataque de restablecimiento de TCP y enviar un paquete falso con un RST de TCP a uno o ambos terminales.



Vulnerabilidades de TCP y UDP

Ataques de TCP

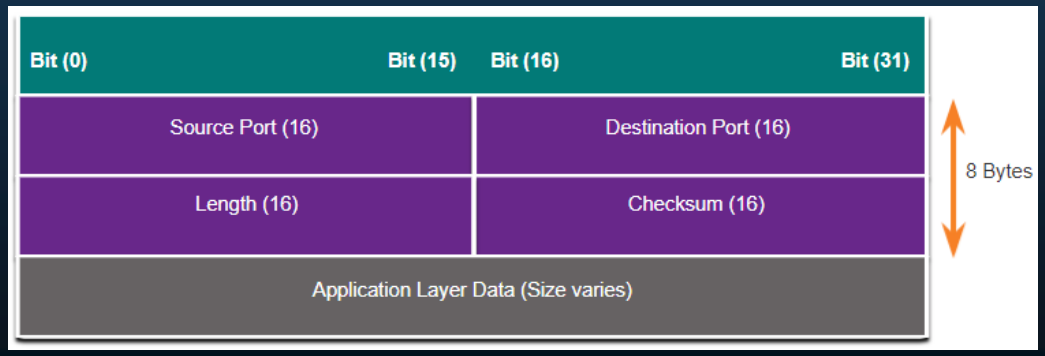
Otra vulnerabilidad es el secuestro de sesiones de TCP. Aunque es difícil de realizar, permite que un atacante tome el control de un host ya autenticado mientras se comunica con el destino.

El atacante tendría que suplantar la dirección IP de un host, predecir el siguiente número de secuencia y enviar un ACK al otro host. Si tiene éxito, el atacante puede enviar, pero no recibir, datos desde el dispositivo de destino.

Vulnerabilidades de TCP y UDP

Encabezado de segmento TCP y Funcionamiento

- DNS, TFTP, NFS y SNMP utilizan comúnmente UDP. También lo utilizan aplicaciones en tiempo real, como la transmisión multimedia o VoIP. UDP es un protocolo de capa de transporte sin conexión. Tiene una sobrecarga mucho menor que TCP ya que no está orientado a la conexión y no proporciona los mecanismos sofisticados de retransmisión, secuenciación y control del flujo que ofrecen confiabilidad.
- Significa que estas funciones no las proporciona el protocolo de la capa de transporte, y se deben implementar aparte si es necesario.
- La baja sobrecarga del UDP es muy deseable para los protocolos que realizan transacciones simples de solicitud y respuesta.



Vulnerabilidades de TCP y UDP

Ataques de UDP

- UDP no está protegido por ningún tipo de encriptación. Puede agregar cifrado a UDP, pero no está disponible de forma predeterminada. La falta de encriptación permite que cualquiera vea el tráfico, lo modifique y lo envíe a su destino.

- **Ataques de UDP Flood:** El atacante debe usar una herramienta como UDP Unicorn o Low Orbit Ion Cannon. Estas herramientas envían una avalancha de paquetes UDP, a menudo desde un host falsificado, a un servidor en la subred. El programa analiza todos los puertos conocidos intentando encontrar puertos cerrados. Esto hace que el servidor responda con un mensaje de puerto ICMP inaccesible. Debido a que hay muchos puertos cerrados en el servidor, esto crea mucho tráfico en el segmento, que utiliza la mayor parte del ancho de banda. El resultado es muy similar al de un ataque de DoS.

Servicios IP

Vulnerabilidades de ARP

- Los hosts transmiten una solicitud de ARP a otros hosts del segmento para determinar la dirección MAC de un host con una dirección IP específica. El host con la dirección IP que coincide con la de la solicitud de ARP envía una respuesta de ARP.

- Cualquier cliente puede enviar una respuesta de ARP no solicitada llamada “ARP gratuito”. Cuando un host envía un ARP gratuito, otros hosts en la subred almacenan en sus tablas de ARP la dirección MAC y la dirección IP que contiene dicho ARP.

- Esta característica de ARP también significa que cualquier host puede afirmar ser el dueño de cualquier IP o MAC que elija. Un atacante puede envenenar la caché de ARP de los dispositivos en la red local y crear un ataque de MITM para redireccionar el tráfico.

Servicios IP

Envenenamiento de caché de ARP

El envenenamiento de caché ARP se puede usar para lanzar varios ataques de MITM.

1. La PC-A necesita la dirección MAC de su gateway predeterminado (R1) y, por lo tanto, envía ARP request para obtener la MAC de 192.168.10.1.
2. El R1 actualiza su caché de ARP con la IP y MAC de la PC-A y envía una respuesta ARP, la cual, a su vez, actualiza su caché de ARP con la IP y MAC del R1.
3. El atacante envía dos gratuitous ARP falsos usando su propia dirección MAC para la IP de destino indicada. La PC-A actualiza su caché de ARP y, ahora, el gateway predeterminado apunta hacia la MAC del host del atacante. El R1 también actualiza su caché de ARP con la dirección IP de la PC-A y comienza a apuntar a la dirección de MAC del atacante.

El envenenamiento ARP puede ser pasivo o activo: Pasivo cuando los atacantes roban información confidencial. Activo cuando los atacantes modifican datos en tránsito o inyectan datos maliciosos.

Servicios IP

Ataques de DNS

- El protocolo de Servicio de Nombres de Dominio (DNS) define un servicio automatizado que coincide con los nombres de recursos, como www.cisco.com, con su dirección de red numérica, ya sea dirección IPv4 o IPv6. Incluye el formato para las consultas, respuestas y datos, y usa registros de recursos (RR) para identificar el tipo de respuesta de DNS.

- La protección de DNS suele pasarse por alto. Sin embargo, es fundamental para el funcionamiento de una red y debe protegerse correctamente.

- Los ataques DNS incluyen lo siguiente:
  - Ataques de resolución abierta de DNS
  - Ataques sigilosos de DNS
  - Ataques de domain shadowing de DNS
  - Ataques de tunelización de DNS

Servicios IP

Ataques de DNS

Ataques de resolución abierta de DNS: Responde las consultas de clientes fuera de su dominio administrativo. Son vulnerables a múltiples actividades maliciosas descritas en la tabla.

Vulnerabilidades de resolución de DNS	Descripción
Ataque de envenenamiento de caché DNS	Los atacantes envían registros de recursos (RR) falsificados a una "DNS resolver" para redirigir a los usuarios de sitios legítimos a sitios maliciosos. Estos ataques se pueden utilizar para informar a la resolución de DNS que utilice un servidor de nombre malicioso que proporciona información del RR para actividades maliciosas.
Ataque de amplificación y reflexión de DNS	Los atacantes usan ataque DoS o DDoS para aumentar el volumen de ataques y para ocultar la verdadera fuente de un ataque. Los atacantes envían mensajes de DNS a las resoluciones abiertas utilizando la dirección IP de un host de destino. Estos ataques son posibles porque la resolución abierta responde las consultas de cualquiera que pregunte.
Ataques de recursos disponibles de DNS	Un ataque DoS que consume los recursos de los DNS open resolvers. Este ataque de DoS consume todos los recursos disponibles para afectar negativamente las operaciones de la resolución de DNS abierta. El impacto de este ataque de DoS puede requerir el reinicio de la resolución de DNS abierta o la interrupción y el reinicio de los servicios.

Servicios IP

Ataques de DNS

Ataques de DNS Sigilosas: Para ocultar su identidad, los atacantes también utilizan las técnicas de DNS sigilosas descritas en la siguiente tabla.

Técnicas de sigilo DNS	Descripción
Flujo Rápido	Los atacantes utilizan esta técnica para ocultar sus sitios de entrega de phishing y malware en una red de hosts DNS atacados que cambia rápidamente. Las direcciones IP de DNS cambian constantemente en apenas minutos. A menudo, los botnets emplean técnicas de flujo rápido para ocultar con eficacia servidores maliciosos y evitar su detección.
Flujo IP Doble	Los atacantes utilizan esta técnica para cambiar rápidamente el nombre de host para las asignaciones de dirección IP y también cambiar el servidor de nombres autorizados. Esto aumenta la dificultad para identificar el origen del ataque.
Algoritmos de generación de dominio	Los atacantes utilizan esta técnica en malware para generar aleatoriamente nombres de dominio que puedan utilizarse como puntos de encuentro de sus servidores de comando y control (C&C).

Servicios IP

Ataques de DNS

Ataques de Domain Shadowing de DNS: El domain shadowing implica que el atacante reúna credenciales de la cuenta de dominio para crear silenciosamente múltiples subdominios para usar durante los ataques.

Estos subdominios generalmente apuntan a servidores maliciosos sin alertar al propietario real del dominio principal.

Servicios IP

Túnel de DNS

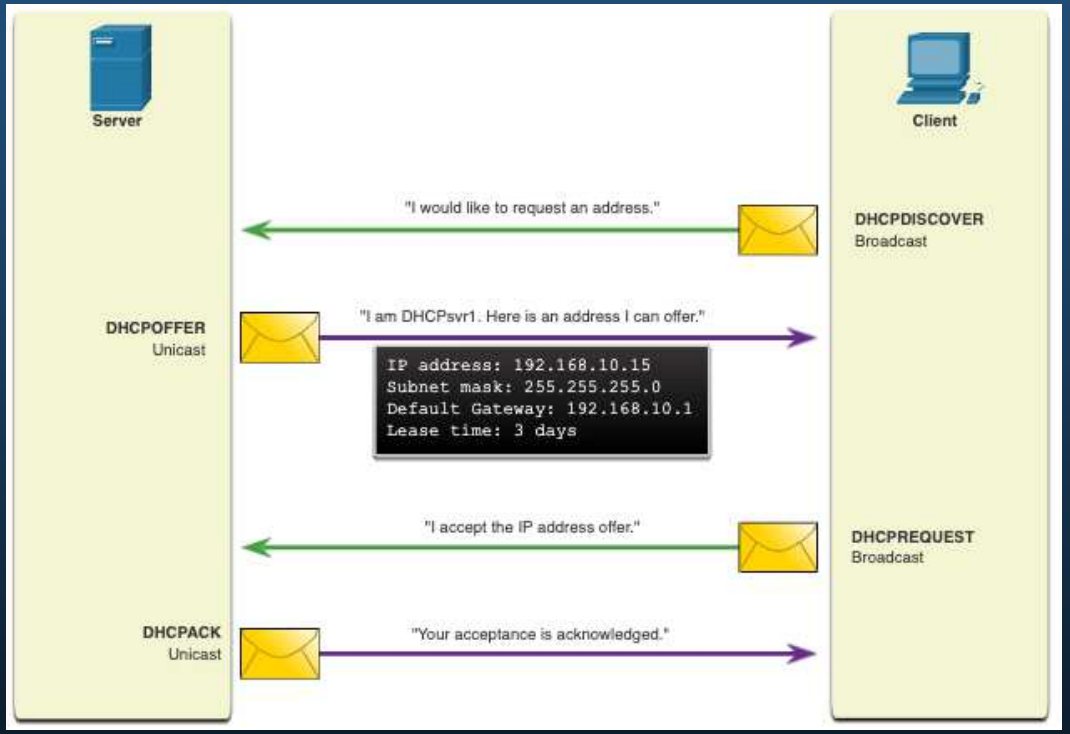
- Los atacantes que utilizan la tunelización de DNS colocan tráfico que no es DNS en tráfico DNS. Este método a menudo evita las soluciones de seguridad cuando un atacantes desea comunicarse con bots dentro de una red protegida, o extraer datos de la organización. Así es como funciona el túnel DNS para los comandos CnC enviados a una botnet:
  1. Los datos se dividen en varias partes codificadas.
  2. Cada parte se coloca en una etiqueta de nombre de dominio de nivel inferior de la consulta de DNS.
  3. Dado que no hay ninguna respuesta del DNS local o en red para la consulta, la solicitud se envía a los servidores DNS recursivos del ISP.
  4. El servicio de DNS recursivo reenvía la consulta al servidor de nombres autorizado del atacante.
  5. El proceso se repite hasta que se envían todas las consultas que contienen las partes.
  6. Cuando el servidor de nombre autorizado del atacante recibe las consultas de DNS de los dispositivos infectados, envía las respuestas para cada consulta de DNS, las cuales contienen los comandos CnC encapsulados y codificados.
  7. El malware en el host atacado vuelve a combinar las partes y ejecuta los comandos ocultos dentro del registro DNS.
- Para detener el túnel DNS, el administrador de la red debe usar un filtro que inspeccione el tráfico DNS. Preste especial atención a las consultas de DNS que son más largas de lo normal, o las que tienen un nombre de dominio sospechoso.

Servicios IP

DHCP

- Los servidores DHCP proporcionan dinámicamente información de configuración de IP a los clientes.

- En la figura, un cliente transmite un mensaje de descubrimiento de DHCP. El servidor DHCP le responde directamente con una oferta que incluye información de direccionamiento que el cliente puede usar. El cliente transmite una solicitud DHCP para decirle al servidor que el cliente acepta la oferta. El servidor le responde directamente con un reconocimiento aceptando la solicitud.



Servicios IP

Ataques de DHCP

- Un **ataque de suplantación de DHCP** se produce cuando un servidor DHCP malicioso se conecta a la red y brinda parámetros de configuración IP falsos a los clientes legítimos. Un servidor malicioso puede proporcionar una variedad de información engañosa:

- **Gateway predeterminado incorrecto**: El atacante proporciona un gateway no válido o la dirección IP de su host para crear un ataque de MITM. Esto puede pasar totalmente inadvertido, ya que el intruso intercepta el flujo de datos por la red.

- **Servidor DNS incorrecto**: El atacante proporciona una dirección del servidor DNS incorrecta que dirige al usuario a un sitio web malicioso.

- **Dirección IP incorrecta**: El atacante proporciona una dirección IP no válida, una dirección IP de puerta de enlace predeterminada no válida o ambas. Luego, el agente de amenaza crea un ataque de DoS en el cliente DHCP.

Servicios IP

Ataques de DHCP

Supongamos que un atacante conecta con éxito un servidor DHCP malicioso a un puerto de switch en la misma subred de los clientes objetivos. El objetivo del servidor malicioso es proporcionarles a los clientes información de configuración de IP falsa.

1. El cliente emite una solicitud de detección de DHCP en busca de una respuesta de un servidor DHCP. Ambos servidores recibirán el mensaje.
2. El servidor DHCP malicioso y el legítimo responden ambos con parámetros de configuración de IP válidos. El cliente responde a la primera oferta recibida.
3. El cliente recibió primero la oferta del servidor malicioso y emite una solicitud de DHCP aceptando los parámetros. El servidor legítimo y el dudoso recibirán la solicitud.
4. Solamente el servidor malicioso emite una respuesta individual al cliente para acusar recibo de su solicitud. El servidor legítimo deja de comunicarse con el cliente porque la solicitud ya ha sido reconocida.

Mejores Prácticas en Seguridad de Redes

Confidencialidad, Disponibilidad e Integridad

- La Seguridad de la Red consiste en proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados.

- La mayoría de las organizaciones siguen la triada de seguridad de la información (CIA, por sus siglas en inglés):

  - **Confidencialidad**: Solamente individuos, entidades o procesos autorizados pueden tener acceso a información confidencial. Puede requerir el uso de algoritmos de cifrado criptográfico como AES para cifrar y descifrar datos.
  - **Integridad**: Se refiere a proteger los datos de modificaciones no autorizadas. Requiere el uso de algoritmos de hashing criptográficos como SHA.
  - **Disponibilidad**: Los usuarios autorizados deben tener acceso ininterrumpido a los recursos y datos importantes. Requiere implementar servicios puertas de enlace y enlaces redundantes.

Mejores Prácticas en Seguridad de Redes

El Enfoque de Defensa en Profundidad

- Para garantizar comunicaciones seguras en redes públicas y privadas, el primer objetivo es proteger los dispositivos como routers, switches, servidores y hosts. La mayoría de las organizaciones emplean un enfoque de defensa en profundidad para la seguridad. Esto requiere una combinación de dispositivos y servicios de red que trabajen en conjunto.
- Se implementan varios dispositivos de seguridad y servicios:
  - **VPN**
  - **Firewall ASA**
  - **IPS**
  - **ESA/WSA**
  - **Servidor AAA**
- Todos los dispositivos red incluyendo el router y los switches son fortalecidos.
- Además se deben proteger los datos a medida que viajan a través de varios enlaces.

Mejores Prácticas en Seguridad de Redes

Firewalls

Un firewall es un sistema o grupo de sistemas que impone una política de control de acceso entre redes.

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

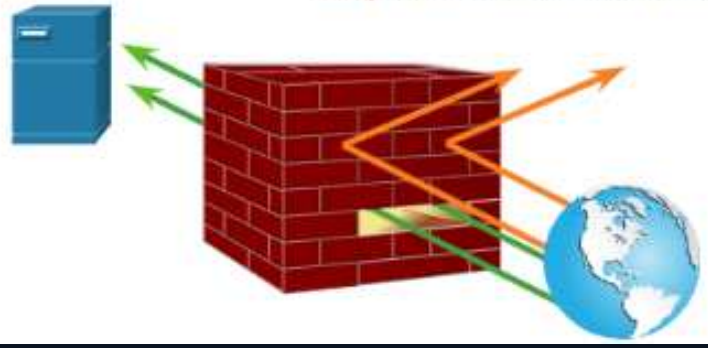
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.



Mejores Prácticas en Seguridad de Redes

IPS

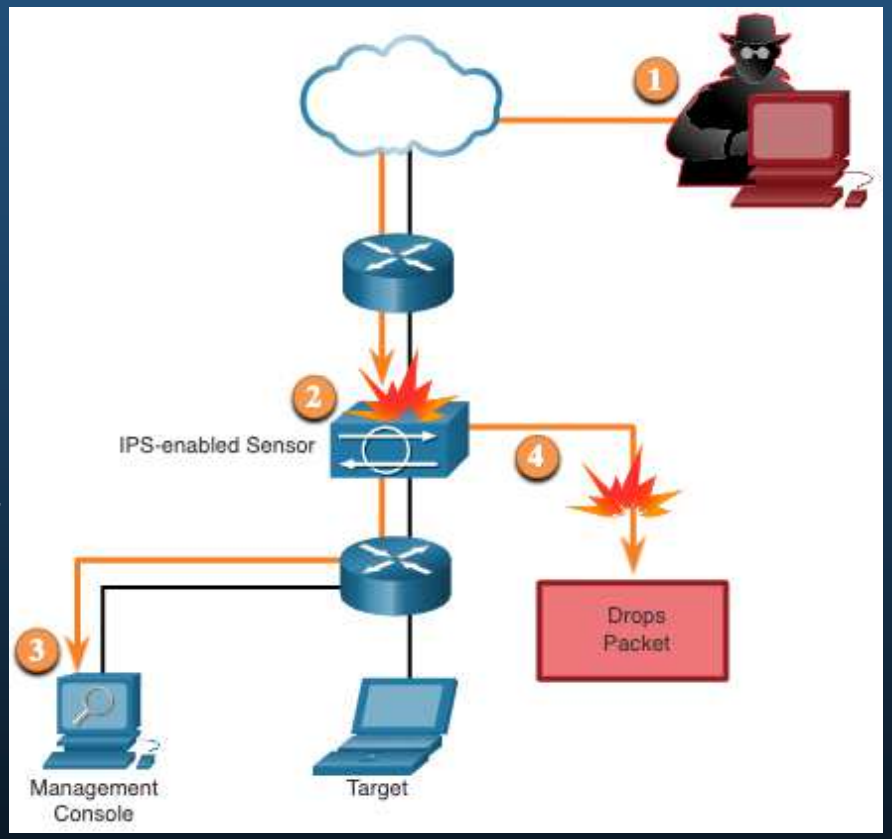
- Para defenderse de los ataques rápidos y cambiantes, se podrían necesitar sistemas rentables de detección y prevención integrados en los puntos de entrada y salida de la red.
- Las tecnologías IDS e IPS comparten varias características. Ambas tecnologías se implementan como sensores. Un sensor IDS o IPS puede adoptar la forma de varios dispositivos diferentes:
  - Un router configurado con el software IPS de Cisco IOS.
  - Un dispositivo diseñado específicamente para proporcionar servicios de IDS o IPS exclusivos.
  - Un módulo de red instalado en un dispositivo de seguridad adaptable (ASA, Adaptive Security Appliance), switch o router.
- IDS e IPS identifican patrones en el tráfico de la red utilizando un conjunto de reglas llamadas firmas para detectar actividad maliciosa. Las tecnologías IDS e IPS pueden detectar patrones de firma atómica (paquete individual) o patrones de firma compuesta (varios paquetes).

Mejores Prácticas en Seguridad de Redes

IPS

La figura muestra cómo un IPS maneja el tráfico denegado.

1. El atacante envía un paquete destinado a la computadora portátil objetivo.
2. El IPS intercepta el tráfico y lo evalúa contra amenazas reconocido y las políticas configuradas.
3. El IPS envía un mensaje de registro a la consola de administración.
4. El IPS desecha el paquete.



Mejores Prácticas en Seguridad de Redes

Dispositivos de Seguridad de Contenido

- El dispositivo de seguridad de correo electrónico de Cisco (ESA) es un dispositivo especial diseñado para monitorear el protocolo simple de transferencia de correo (SMTP). Cisco ESA se actualiza constantemente por fuentes en tiempo real del Cisco Talos. Cisco ESA extrae estos datos de inteligencia de amenazas cada tres o cinco minutos.

- Cisco Web Security Appliance (WSA) es una tecnología de mitigación para amenazas basadas en la web. Cisco WSA combina protección avanzada contra malware, visibilidad y control de aplicaciones, controles de políticas de uso aceptable e informes.

- Cisco WSA proporciona un control total sobre cómo los usuarios acceden a internet. La WSA puede marcar URLs en lista negra, filtrar URLs, escanear malware, categorizar URLs, filtrar aplicaciones web y encriptar y desencriptar tráfico web.

Criptografía

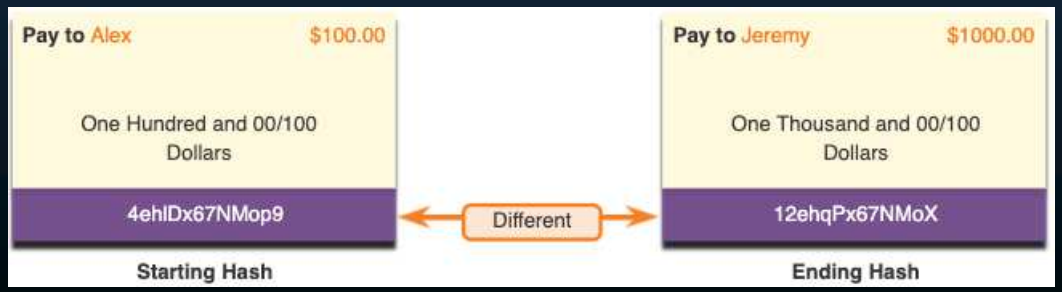
Comunicaciones Seguras

- Las organizaciones deben proporcionar soporte para proteger los datos a medida que viajan a través de enlaces. Esto puede incluir el tráfico interno, pero la mayor preocupación es proteger los datos que viajan fuera de la organización.
- Estos son los cuatro elementos de las comunicaciones seguras:
  - **Integridad de los datos**: Garantiza que el mensaje no se haya modificado. La integridad se garantiza mediante la aplicación de los algoritmos de generación de hash Message Digest versión 5 (MD5) o Secure Hash (SHA).
  - **Autenticación de Origen**: Garantiza que el mensaje no sea falso y que provenga de quien dice ser. Muchas redes modernas garantizan la autenticación con protocolos, como el código de autenticación de mensaje hash (Hash Message Authentication Code (HMAC).
  - **Confidencialidad de los datos**: Garantiza que solamente los usuarios autorizados puedan leer el mensaje. La confidencialidad de los datos se implementa utilizando algoritmos de encriptación simétrica y asimétrica.
  - **Imposibilidad de Negación de los Datos**: Garantiza que el remitente no pueda negar ni refutar la validez de un mensaje enviado. La imposibilidad de negación se basa en el hecho de que solamente el remitente tiene características únicas o una firma de cómo tratar el mensaje.
- La criptografía puede usarse casi en cualquier lugar donde haya comunicación de datos. De hecho, la tendencia marcha hacia un mundo donde toda la comunicación será cifrada.

Criptografía

Integridad de los Datos

- Las funciones de hash se utilizan para garantizar la integridad de un mensaje. Garantizan que los datos del mensaje no hayan cambiado accidental o intencionalmente.
- En la Figura, el remitente envía una transferencia de USD 100 a Alex. El emisor quiere asegurarse de que el mensaje no se altere en su recorrido hasta el receptor:
  1. El dispositivo de envío introduce el mensaje en un algoritmo de hash y calcula un hash de longitud fija de 4ehiDx67NMop9.
  2. Luego, este hash se adjunta al mensaje y se envía al receptor. El mensaje y el hash se transmiten en texto sin formato.
  3. El dispositivo receptor elimina el hash del mensaje e introduce el mensaje en el mismo algoritmo de hash. Si el hash calculado es igual al que se adjunta al mensaje, significa que el mensaje no se modificó durante su recorrido. Si los hash son no iguales, ya no es posible garantizar la integridad del mensaje.



Criptografía

Funciones Hash

- Existen tres funciones de hash muy conocidas:
  - **MD5 con una síntesis de 128 bits:**MD5 es una función unidireccional que genera un mensaje de hash de 128 bits. MD5 es un algoritmo heredado que solo debe usarse cuando no hay mejores alternativas disponibles. Use SHA-2 en su lugar.
  - **SHA:** SHA-1 es muy similar a las funciones de hash MD5. SHA-1 crea un mensaje hash de 160 bits y es un poco más lento que MD5. SHA-1 tiene defectos conocidos y es un algoritmo obsoleto. Use SHA-2 cuando sea posible.
  - **SHA-2:** Esto incluye SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit), and SHA-512 (512 bit). SHA-256, SHA-384 y SHA-512 son algoritmos de última generación y deben utilizarse siempre que sea posible.

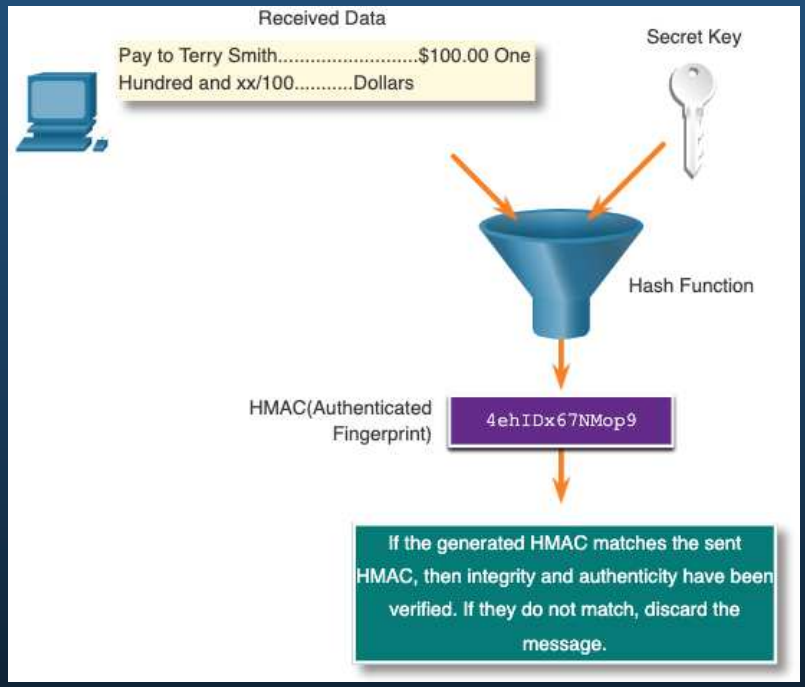
- Mientras que el hash se puede utilizar para detectar modificaciones accidentales, no brinda protección contra cambios deliberados. Esto significa que cualquier persona puede calcular un hash para los datos, siempre y cuando tengan la función de hash correcta.

- Por lo tanto, el hash es vulnerable a los ataques man-in-the-middle y no proporciona seguridad a los datos transmitidos.

Criptografía

Autenticación de Origen

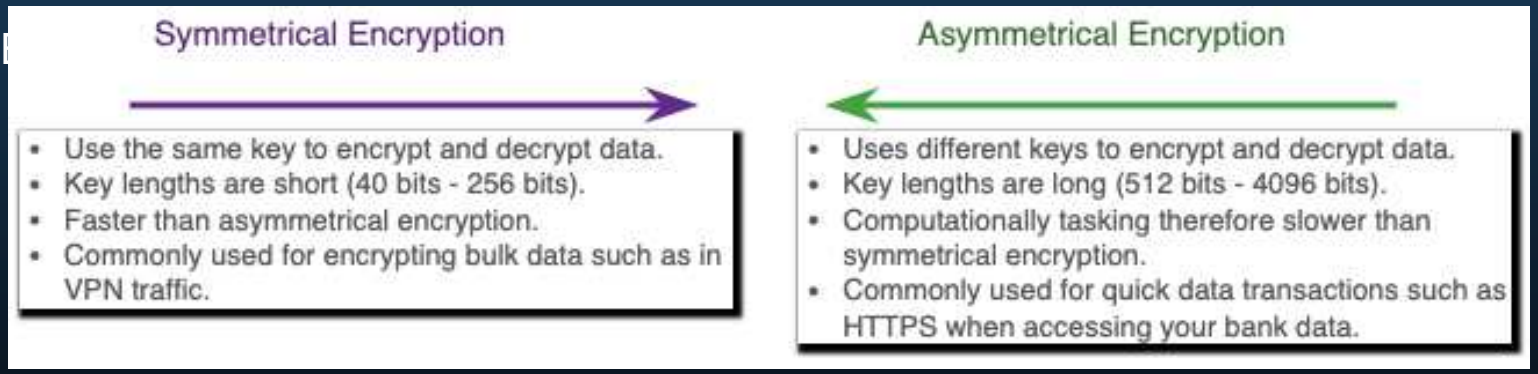
- Para agregar autenticación al control de integridad se usa un código de autenticación de mensajes hash con clave (HMAC).
- Un HMAC se calcula utilizando cualquier algoritmo criptográfico que combine una función hash criptográfica con una clave secreta.
- Solo las partes que tienen acceso a esa clave secreta pueden calcular el compendio de una función de HMAC. Esta característica derrota los ataques man-in-the-middle y proporciona autenticación del origen de los datos.



Criptografía

Confidencialidad de Datos

- Hay dos clases de encriptación utilizadas para brindar confidencialidad de los datos. Estas dos clases se diferencian en cómo utilizan las claves:
- Los algoritmos de cifrado simétricos como (DES), 3DES y el Estándar de cifrado avanzado (AES) se basan en la premisa de que cada parte que se comunica conoce la clave precompartida. La confidencialidad también se puede garantizar utilizando algoritmos asimétricos, como Rivest, Shamir y Adleman (RSA) y la infraestructura de clave pública (PKI).
-



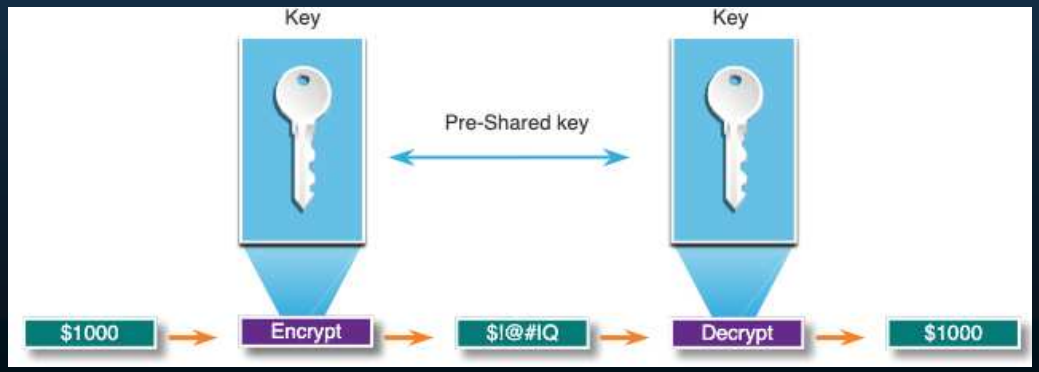
Criptografía

Cifrado Simétrico

- Los algoritmos simétricos utilizan la misma clave precompartida, también llamada una clave secreta, para encriptar y desencriptar datos. Antes de que ocurra cualquier comunicación encriptada, el emisor y el receptor conocen la clave precompartida.

- Los algoritmos simétricos cifrados se usan normalmente con el tráfico de VPN porque utilizan menos recursos de CPU que los algoritmos de encriptación asimétrica.

- Al utilizar algoritmos de encriptación simétrica, mientras más larga sea la clave, más tiempo demorará alguien en descubrirla. Para garantizar que la encriptación sea segura, se recomienda una longitud mínima de clave de 128 bits.



Criptografía

Cifrado simétrico

Algoritmos de Encriptación Simétrica	Descripción
Algoritmo de Cifrado de Datos (DES)	Este es un algoritmo de cifrado simétrico heredado. Puede utilizarse en el cifrado de flujo, pero suele funcionar en el cifrado por bloques al encriptar de datos en bloques de 64 bits. Un cifrado de flujo encripta un byte o un bit a la vez.
3DES (triple DES)	Esta es una versión más reciente del DES, pero repite el proceso de algoritmo de DES tres veces. Se considera muy confiable cuando se implementa con claves de duración muy breve.
Estándar de encriptación avanzada (AES)	AES es un algoritmo seguro y más eficiente que 3DES. Es un algoritmo de cifrado simétrico popular y recomendado. Ofrece nueve combinaciones de longitud de clave y bloque, utilizando una longitud de clave variable de 128, 192 o 256 bits para encriptar los bloques de datos que son de 128, 192 o 256 bits de largo.
Algoritmo de Cifrado Optimizado por Software (SEAL)	SEAL es un algoritmo de cifrado simétrico rápido y alternativo para DES, 3DES y AES. Usa un llave de cifrado de 160 bit y tiene un menor impacto en la CPU en comparación con otros algoritmos basados en software.
Rivest ciphers (RC) para flujos	Este algoritmo fue desarrollado por Ron Rivest. Se han desarrollado numerosas variantes, pero RC4 es la de uso más frecuente. RC4 es un cifrado de flujo y se utiliza para proteger el tráfico web de SSL y TLS.

Criptografía

Cifrado Asimétrico

- Los algoritmos asimétricos, también llamados algoritmos de claves públicas, están diseñados para que la clave de encriptación y la de desencriptación sean diferentes.

- Los algoritmos asimétricos utilizan una clave pública y una privada. La clave complementaria emparejada es requerida para la desencriptación. Los datos encriptados con la clave privada requieren la clave pública para desencriptarse. Los algoritmos asimétricos logran confidencialidad, autenticación e integridad mediante el uso de este proceso.

- Debido a que ninguno de los participantes comparte un secreto, las longitudes de clave deber ser muy largas. La encriptación asimétrica puede utilizar longitudes de claves entre 512 y 4096 bits. Longitudes de clave mayores o iguales a 1024 bits son confiables, y mientras que las claves más cortas no.

Criptografía

Cifrado Asimétrico

- Entre algunos de los ejemplos de protocolos en los que se utilizan algoritmos de claves asimétricos se incluyen los siguientes:
  - **Intercambio de claves por Internet (IKE):** Es un componente fundamental de las VPN con IPsec..
  - **Secure Socket Layer (SSL):** Ahora se implementa como Seguridad de la capa de transporte (TLS) estándar de IETF.
  - **Secure Shell (SSH):** Este protocolo proporciona una conexión segura de acceso remoto a dispositivos de red.
  - **Pretty Good Privacy (PGP):** Este programa de computadora proporciona privacidad y autenticación criptográfica. A menudo, se utiliza para aumentar la seguridad de las comunicaciones por correo electrónico.
- Los algoritmos asimétricos son sustancialmente más lentos que los simétricos. Su diseño se basa en problemas informáticos, como la factorización de números demasiado grandes o el cálculo de logaritmos discretos de números demasiado grandes.

- Dado que carecen de velocidad, los algoritmos asimétricos se utilizan típicamente en criptografías de poco volumen, como las firmas digitales y el intercambio de claves.

Criptografía

Cifrado Asimétrico

Algoritmo de Cifrado Asimétrico	Longitud de la Clave	Descripción
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	Permite que ambas partes acuerden una clave que pueden utilizar para cifrar los mensajes que quieren enviarse. La seguridad de este algoritmo depende de la presunción de que resulta sencillo elevar un número a una determinada potencia, pero difícil calcular qué potencia se utilizó sabiendo el número y el resultado.
Estándar de firmas digitales (Digital Signature Standard, DSS) y Algoritmo de firmas digitales (Digital Signature Algorithm, DSA)	512 - 1024	DSS especifica DSA como el algoritmo para firmas digitales. DSA es un algoritmo de clave pública basado en el esquema de firmas ElGamal. La velocidad de creación es similar a la RSA, pero es de 10 a 40 veces más lenta para la verificación.
Algoritmos de cifrado Rivest, Shamir y Adleman (RSA)	Entre 512 y 2048	Usado para criptografía de clave pública que se basa en la dificultad actual de factorización de números muy grandes. Es el primer algoritmo apto tanto para firmas como para cifrados. Es ampliamente utilizado en protocolos de comercio electrónico y se considera seguro si se utilizan claves suficientemente prolongadas e implementaciones actualizadas.
ElGamal	512 - 1024	Usado para criptografía de claves públicas basado en el acuerdo de claves Diffie-Hellman. Una desventaja del sistema ElGamal es que el mensaje cifrado se vuelve muy grande (aprox. el doble del tamaño del original). Por ello sólo se utiliza con mensajes pequeños como claves secretas.
Técnicas de curvas elípticas	160	Se puede utilizar para adaptar muchos algoritmos de cifrado, como los de Diffie-Hellman o ElGamal. La principal ventaja es que las claves pueden ser mucho más pequeñas.

Criptografía

Diffie-Hellman

- Algoritmo matemático asimétrico que permite que dos computadoras generen una clave secreta idéntica compartida sin antes haberse comunicado. El emisor y el receptor nunca intercambian realmente la nueva clave compartida.

- Estos son tres ejemplos de casos en los que el algoritmo de DH suele utilizarse:
  - Se intercambian datos en una VPN con IPsec
  - Se encriptan datos en Internet usando SSL o TLS
  - Se intercambian datos de SSH

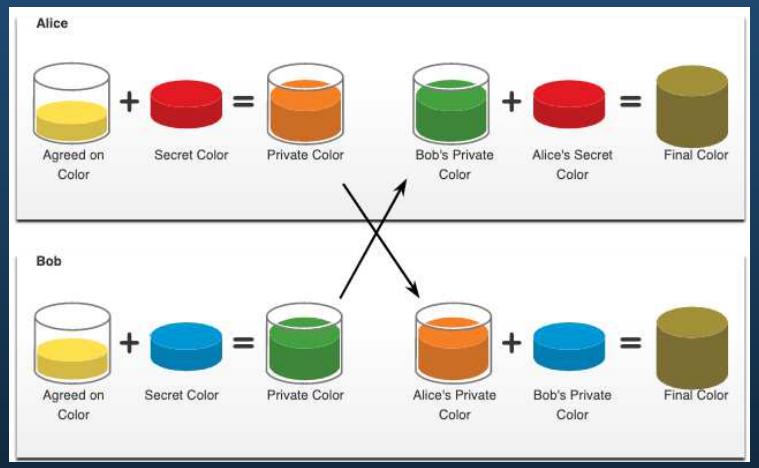
- La seguridad de DH utiliza números increíblemente grandes en sus cálculos.

- Desafortunadamente, los sistemas de clave asimétrica son extremadamente lentos para cualquier tipo de encriptación masiva. Por esto, es común encriptar la mayor parte del tráfico utilizando un algoritmo simétrico (como 3DES o AES) y dejar el algoritmo de DH para crear claves que serán utilizadas por el algoritmo de encriptación.

Criptografía

Diffie-Hellman

- Los colores en la figura se utilizarán en lugar de números para simplificar el proceso de acuerdo de claves del algoritmo de DH. El intercambio de claves del algoritmo de DH comienza con Alice y Bob eligiendo arbitrariamente un color en común que no tienen que mantener en secreto. El color acordado en nuestro ejemplo es el amarillo.
- Luego, Alice y Bob seleccionan un color secreto cada uno. Alice eligió rojo y Bob, azul. Nunca compartirán estos colores secretos con nadie. El color secreto representa la clave privada secreta que cada participante eligió.
- Ahora, Alice y Bob mezclan el color común compartido (amarillo) con su color secreto respectivo para generar un color privado. Por lo tanto, Alice mezcla el amarillo con el rojo para obtener el anaranjado como color privado. Bob mezcla el amarillo y el azul para obtener verde como color privado.
- Alice envía su color privado (anaranjado) a Bob y Bob le envía el suyo (verde) a Alice.
- Alice y Bob mezclan cada uno el color que recibieron con su propio color secreto original (rojo para Alice y azul para Bob). El resultado es una mezcla final de color marrón que es idéntica a la mezcla final del otro participante. El color marrón representa la clave secreta que comparten Bob y Alice.



Capítulo 4

Conceptos de ACL

Proposito de las ACLs

Que es una ACL?

Una ACL es una serie de comandos de IOS que se utilizan para filtrar paquetes según la información que se encuentra en el encabezado del paquete. De forma predeterminada, un Router no tiene ninguna ACL configurada. Cuando se aplica una ACL a una interfaz, el Router realiza la tarea adicional de evaluar todos los paquetes de red a medida que pasan por la interfaz para determinar si el paquete se puede reenviar.

- Una ACL utiliza una lista secuencial de declaraciones de permiso o denegación, conocidas como entradas de control de acceso (ACE).

Nota: Las ACE también se denominan comúnmente declaraciones de ACL.

- Cuando el tráfico de red pasa a través de una interfaz configurada con una ACL, el Router compara la información dentro del paquete con cada ACE, en orden secuencial, para determinar si el paquete coincide con una de las ACE. Este proceso se denomina filtrado de paquetes.

Proposito de las ACLs

Que es una ACL?

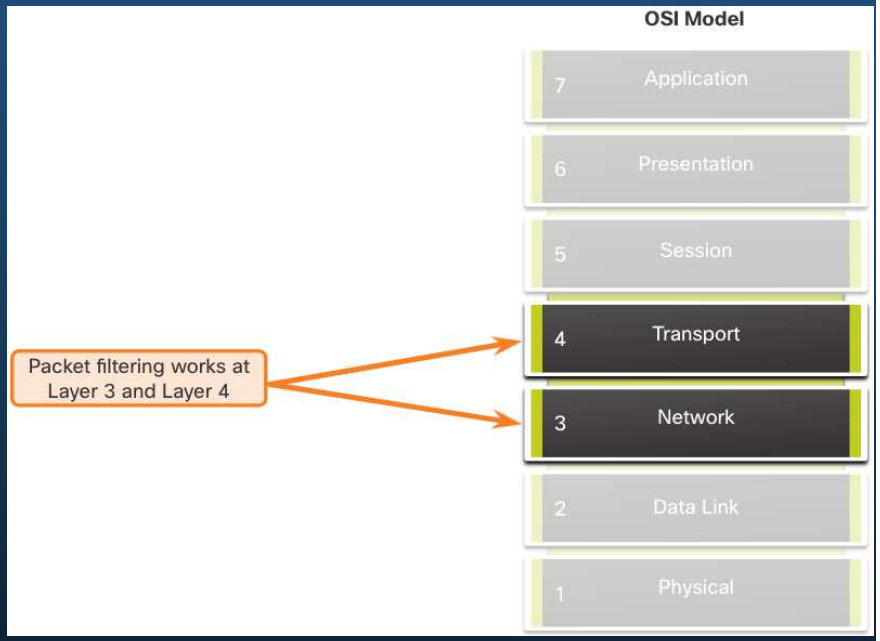
Varias tareas realizadas por los Routers requieren el uso de ACL para identificar el tráfico:

- Limite el tráfico de la red para aumentar el rendimiento de la red
- Proporcionar control de flujo de tráfico
- Proporcionar un nivel básico de seguridad para el acceso a la red.
- Filtrar el tráfico según el tipo de tráfico
- Examinar hosts para permitir o denegar el acceso a los servicios de red
- Dar prioridad a determinadas clases de tráfico de red

Proposito de las ACLs

Filtrado de paquetes

- El filtrado de paquetes controla el acceso a una red analizando los paquetes entrantes y / o salientes y enviándolos o descartándolos según criterios dados.
- El filtrado de paquetes puede ocurrir en la capa 3 o la capa 4.
- Los routers Cisco admiten dos tipos de ACL:
  - ACL estándar: las ACL solo se filtran en la capa 3 utilizando solo la dirección IPv4 de origen.
  - ACL extendidas: las ACL se filtran en la capa 3 utilizando la dirección IPv4 de origen y / o destino. También pueden filtrar en la Capa 4 utilizando TCP, puertos UDP e información de tipo de protocolo opcional para un control más preciso.



Proposito de las ACLs

Funcionamiento de ACL

- Las ACL definen el conjunto de reglas que brindan control adicional para los paquetes que ingresan a las interfaces entrantes, los paquetes que se transmiten a través del Router y los paquetes que salen de las interfaces salientes del Router.
- Las ACL se pueden configurar para que se apliquen al tráfico entrante y saliente.
- Nota: las ACL no actúan sobre los paquetes que se originan en el Routerr.
- Una ACL entrante filtra los paquetes antes de que se enruten a la interfaz de salida. Una ACL entrante es eficaz porque ahorra la sobrecarga de las búsquedas de enrutamiento si se descarta el paquete.
- Una ACL saliente filtra los paquetes después de ser enrutados, independientemente de la interfaz de entrada

Proposito de las ACLs

Funcionamiento de ACL

Cuando se aplica una ACL a una interfaz, sigue un procedimiento operativo específico. Estos son los pasos operativos que se utilizan cuando el tráfico ingresa a una interfaz de Router con una ACL IPv4 estándar entrante configurada:

1. El Router extrae la dirección IPv4 de origen del encabezado del paquete.
2. El Router comienza en la parte superior de la ACL y compara la dirección IPv4 de origen con cada ACE en un orden secuencial.
3. Cuando se hace una coincidencia, el Router ejecuta la instrucción, ya sea permitiendo o denegando el paquete, y las ACE restantes en la ACL, si las hay, no se analizan.
4. Si la dirección IPv4 de origen no coincide con ninguna ACE en la ACL, el paquete se descarta porque hay una ACE de denegación implícita que se aplica automáticamente a todas las ACL.

La última declaración ACE de una ACL es siempre una denegación implícita que bloquea todo el tráfico. Está oculto y no se muestra en la configuración.

Nota: Una ACL debe tener al menos una declaración de permiso; de lo contrario, se denegará todo el tráfico debido a la declaración de denegación ACE implícita.

Wildcard Mask en ACLs

Revisión Wildcard Mask

Una Wildcard Mask es similar a una máscara de subred en el sentido de que utiliza el proceso AND para identificar qué bits de una dirección IPv4 deben coincidir. A diferencia de una máscara de subred, en la que el 1 binario es igual a una coincidencia y el 0 binario no es una coincidencia, en una Wildcard Mask ocurre lo contrario.

Una ACE de IPv4 utiliza una máscara comodín de 32 bits para determinar qué bits de la dirección se deben examinar en busca de una coincidencia.

Las Wildcard Mask utilizan las siguientes reglas para hacer coincidir unos y ceros binarios:

- Wildcard Mask bit 0: coincide con el valor de bit correspondiente en la dirección
- Wildcard Mask bit 1: ignore el valor de bit correspondiente en la dirección

Wildcard Mask en ACLs

Revisión Wildcard Mask

Wildcard Mask	Last Octet (in Binary)	Meaning (0 - match, 1 - ignore)
0.0.0.0	**00000000**	Match all octets.
0.0.0.63	**00111111**	•Match the first three octets •Match the two left most bits of the last octet •Ignore the last 6 bits
0.0.0.15	**00001111**	•Match the first three octets •Match the four left most bits of the last octet •Ignore the last 4 bits of the last octet
0.0.0.248	**11111100**	•Match the first three octets •Ignore the six left most bits of the last octet •Match the last two bits
0.0.0.255	**11111111**	•Match the first three octet •Ignore the last octet

Wildcard Mask en ACLs

Tipos de Wildcard Mask

Wildcard Mask para hacer coincidir un host:

- **Suponga que ACL 10 necesita una ACE que solo permita el host con la dirección IPv4 192.168.1.1. Recuerde que "0" es igual a una coincidencia y "1" es igual a ignorar. Para hacer coincidir una dirección IPv4 de host específica, se requiere una Wildcard Mask que consta de todos ceros (es decir, 0.0.0.0).**
- **Cuando se procesa el ACE, la Wildcard Mask permitirá solo la dirección 192.168.1.1. La ACE resultante en ACL 10 sería el permiso de la lista de acceso 10 192.168.1.1 0.0.0.0.**

	Decimal	Binary
IPv4 address	192.168.1.1	`11000000.10101000.00000001.00000001`
Wildcard Mask	0.0.0.0	`00000000.00000000.00000000.00000000`
Permitted IPv4 Address	**192.168.1.1**	`11000000.10101000.00000001.00000001`

Wildcard Mask en ACLs

Tipos de Wildcard Mask

Wildcard Mask para que coincida con una subred IPv4

- **ACL 10 necesita una ACE que permita todos los hosts en la red 192.168.1.0/24. La Wildcard Mask 0.0.0.255 estipula que los primeros tres octetos deben coincidir exactamente, pero el cuarto octeto no.**
- **Cuando se procesa, la Wildcard Mask 0.0.0.255 permite todos los hosts en la red 192.168.1.0/24. La ACE resultante en ACL 10 sería el permiso de la lista de acceso 10 192.168.1.0 0.0.0.255.**

	Decimal	Binary
IPv4 address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Permitted IPv4 Address	**192.168.1.0/24**	11000000.10101000.00000001.00000000

Wildcard Mask en ACLs

Tipos de Wildcard Mask

Wildcard Mask para que coincida con un rango de direcciones IPv4

ACL 10 necesita una ACE que permita todos los hosts en las redes 192.168.16.0/24, 192.168.17.0/24,…, 192.168.31.0/24.

Cuando se procesa, la Wildcard Mask 0.0.15.255 permite todos los hosts en las redes 192.168.16.0/24 a 192.168.31.0/24. La ACE resultante en ACL 10 sería el permiso de la lista de acceso 10 192.168.16.0 0.0.15.255.

	Decimal	Binary
IPv4 address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Permitted IPv4 Address	**192.168.16.0/24 to 192.168.31.0/24**	11000000.10101000.00010000.00000000 11000000.10101000.00011111.00000000

Wildcard Mask en ACLs

Calculo de Wildcard Mask

El cálculo de Wildcard Mask puede resultar complicado. Un método de atajo es restar la máscara de subred de 255.255.255.255. Algunos ejemplos:

Suponga que desea una ACE en ACL 10 para permitir el acceso a todos los usuarios de la red 192.168.3.0/24. Para calcular la Wildcard Mask, reste la máscara de subred (255.255.255.0) de 255.255.255.255. Esto produce la Wildcard Mask 0.0.0.255. El ACE sería el permiso de la lista de acceso 10 192.168.3.0 0.0.0.255.

Suponga que desea una ACE en ACL 10 para permitir el acceso a la red para los 14 usuarios en la subred 192.168.3.32/28. Reste la subred (es decir, 255.255.255.240) de 255.255.255.255. Esto produce la Wildcard Mask 0.0.0.15. El ACE sería el permiso de la lista de acceso 10 192.168.3.32 0.0.0.15.

Suponga que necesita una ACE en ACL 10 para permitir solo las redes 192.168.10.0 y 192.168.11.0. Estas dos redes podrían resumirse como 192.168.10.0/23, que es una máscara de subred de 255.255.254.0. Reste la máscara de subred 255.255.254.0 de 255.255.255.255. Esto produce la máscara comodín Wildcard Mask 0.0.1.255. El ACE sería el permiso de la lista de acceso 10 192.168.10.0 0.0.1.255.

Wildcard Mask en ACLs

Palabras clave de Wildcard Mask

Cisco IOS proporciona dos palabras clave para identificar los usos más comunes de Wildcard Mask. Las dos palabras clave son:

- host: esta palabra clave sustituye a la máscara 0.0.0.0. Esta máscara indica que todos los bits de dirección IPv4 deben coincidir para filtrar solo una dirección de host.
- any: esta palabra clave sustituye a la máscara 255.255.255.255. Esta máscara dice que se ignore la dirección IPv4 completa o que se acepte cualquier dirección.

Indicaciones para crear ACLs

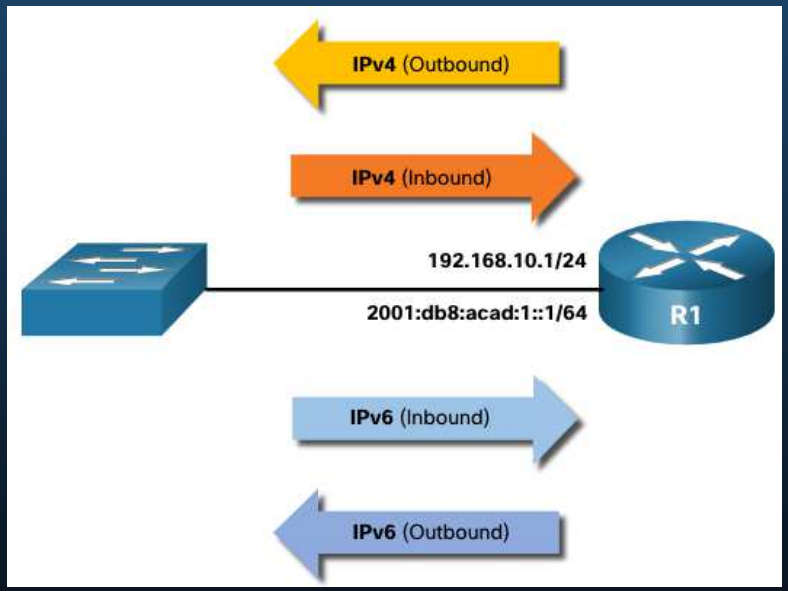
Número limitado de ACL por interfaz

Existe un límite en la cantidad de ACL que se pueden aplicar en una interfaz de Router. Por ejemplo, una interfaz de Router de doble protocolo (es decir, IPv4 e IPv6) puede tener aplicadas hasta cuatro ACL, como se muestra en la figura.

Específicamente, una interfaz de Router puede tener:

- Una ACL IPv4 saliente.
- Una ACL IPv4 entrante.
- Una ACL IPv6 entrante.
- Una ACL IPv6 saliente.

Nota: las ACL no tienen que configurarse en ambas direcciones. La cantidad de ACL y su dirección aplicada a la interfaz dependerá de la política de seguridad de la organización.



Indicaciones para crear ACLs

Mejores prácticas para ACL

El uso de ACL requiere atención a los detalles y mucho cuidado. Los errores pueden ser costosos en términos de tiempo de inactividad, esfuerzos de solución de problemas y servicio de red deficiente. Se requiere una planificación básica antes de configurar una ACL.

Guideline	Benefit
Base ACLs on the organizational security policies.	This will ensure you implement organizational security guidelines.
Write out what you want the ACL to do.	This will help you avoid inadvertently creating potential access problems.
Use a text editor to create, edit, and save all of your ACLs.	This will help you create a library of reusable ACLs.
Document the ACLs using the **remark** command.	This will help you (and others) understand the purpose of an ACE.
Test the ACLs on a development network before implementing them on a production network.	This will help you avoid costly errors.

Tipos de ACLs IPv4

ACLs estandar y extendidas

Hay dos tipos de ACL de IPv4:

- ACL estándar: permiten o deniegan paquetes basándose únicamente en la dirección IPv4 de origen.
- ACL extendidas: permiten o rechazan paquetes según la dirección IPv4 de origen y la dirección IPv4 de destino, el tipo de protocolo, los puertos TCP o UDP de origen y destino, y más.

Tipos de ACLs IPv4

Numeración y nombramiento de ACLs

ACL numeradas

Las ACL numeradas del 1 al 99 o 1300-1999 son ACL estándar, mientras que las ACL numeradas del 100-199 o 2000-2699 son ACL extendidas.

```
R1(config)# access-list ?
  <1-99> IP standard access list
  <100-199> IP extended access list
  <1100-1199> Extended 48-bit MAC address access list
  <1300-1999> IP standard access list (expanded range)
  <200-299> Protocol type-code access list
  <2000-2699> IP extended access list (expanded range)
  <700-799> 48-bit MAC address access list
  rate-limit Simple rate-limit specific access list
  template Enable IP template acls
Router(config)# access-list
```

Tipos de ACLs IPv4

Numeración y nombramiento de ACLs

ACL con nombre

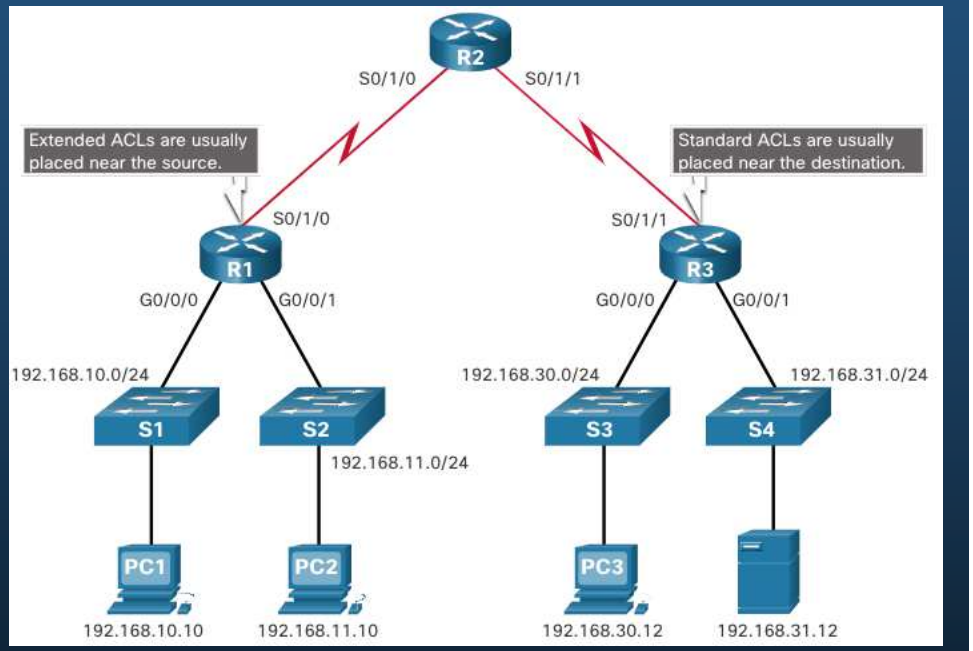
- **Las ACL con nombre son el método preferido para usar al configurar las ACL. Específicamente, las ACL estándar y extendidas se pueden nombrar para proporcionar información sobre el propósito de la ACL. Por ejemplo, nombrar un ACL FTP-FILTER extendido es mucho mejor que tener un ACL 100 numerado.**
- **El comando de configuración global ip access-list se utiliza para crear una ACL con nombre, como se muestra en el siguiente ejemplo.**

```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
R1(config-ext-nacl)#
```

Tipos de ACLs IPv4

Dónde colocar las ACL

- Cada ACL debe colocarse donde tenga el mayor impacto en la eficiencia.
- Las ACL extendidas deben ubicarse lo más cerca posible de la fuente del tráfico que se filtrará.
- Las ACL estándar deben ubicarse lo más cerca posible del destino.



Tipos de ACLs IPv4

Dónde colocar las ACL

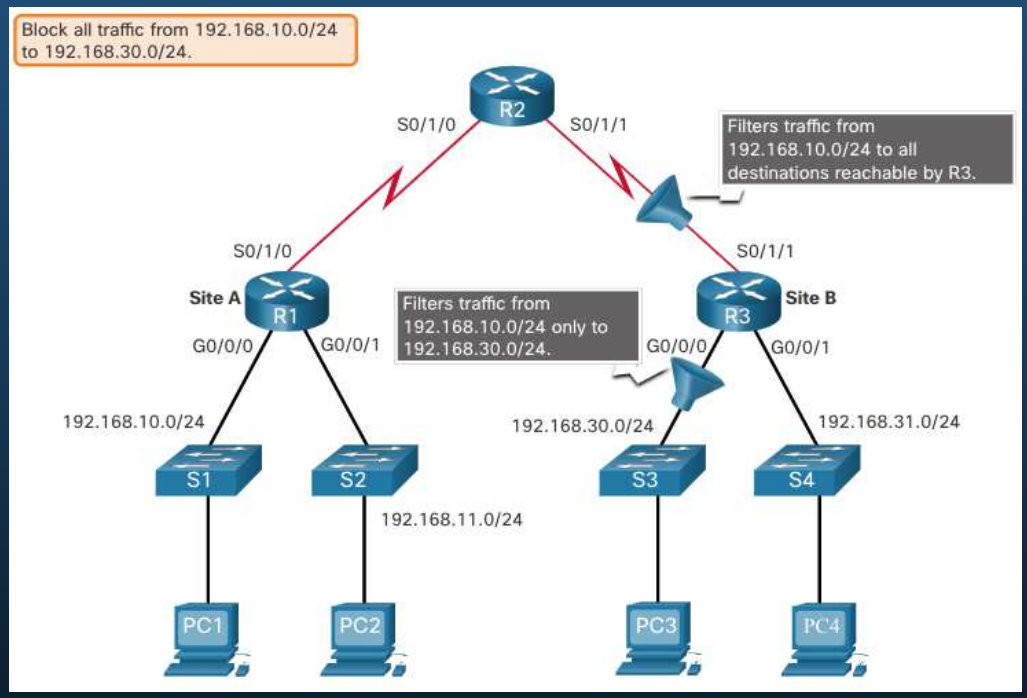
Factors Influencing ACL Placement	Explanation
The extent of organizational control	Placement of the ACL can depend on whether or not the organization has control of both the source and destination networks.
Bandwidth of the networks involved	It may be desirable to filter unwanted traffic at the source to prevent transmission of bandwidth-consuming traffic.
Ease of configuration	•It may be easier to implement an ACL at the destination, but traffic will use bandwidth unnecessarily. •An extended ACL could be used on each router where the traffic originated. This would save bandwidth by filtering the traffic at the source, but it would require creating extended ACLs on multiple routers.

Tipos de ACLs IPv4

Ejemplo de colocación de ACL estándar

En la figura, el administrador quiere evitar que el tráfico que se origina en la red 192.168.10.0/24 llegue a la red 192.168.30.0/24.

Siguiendo las pautas básicas de ubicación, el administrador colocaría una ACL estándar en el Router R3.

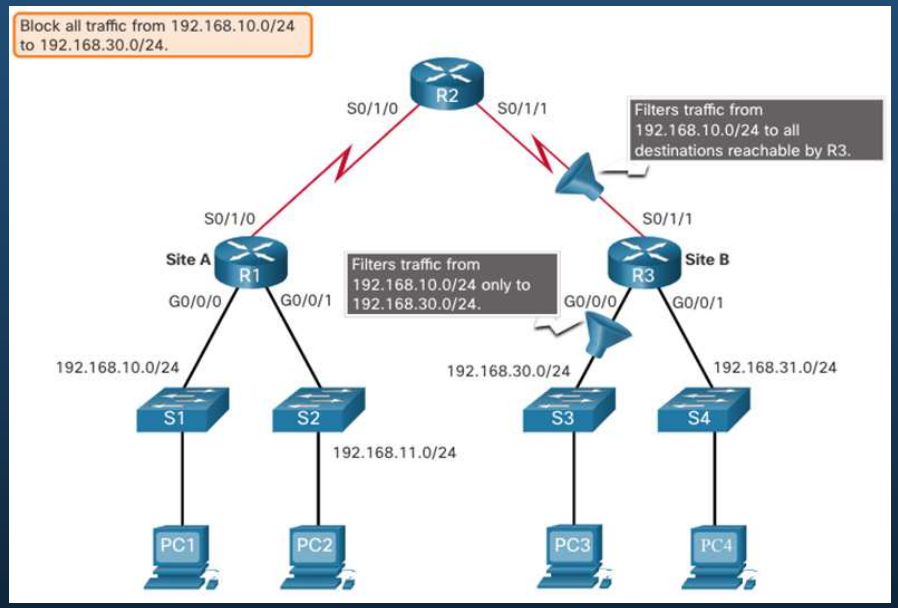


Tipos de ACLs IPv4

Ejemplo de colocación de ACL estándar

Hay dos interfaces posibles en R3 para aplicar la ACL estándar:

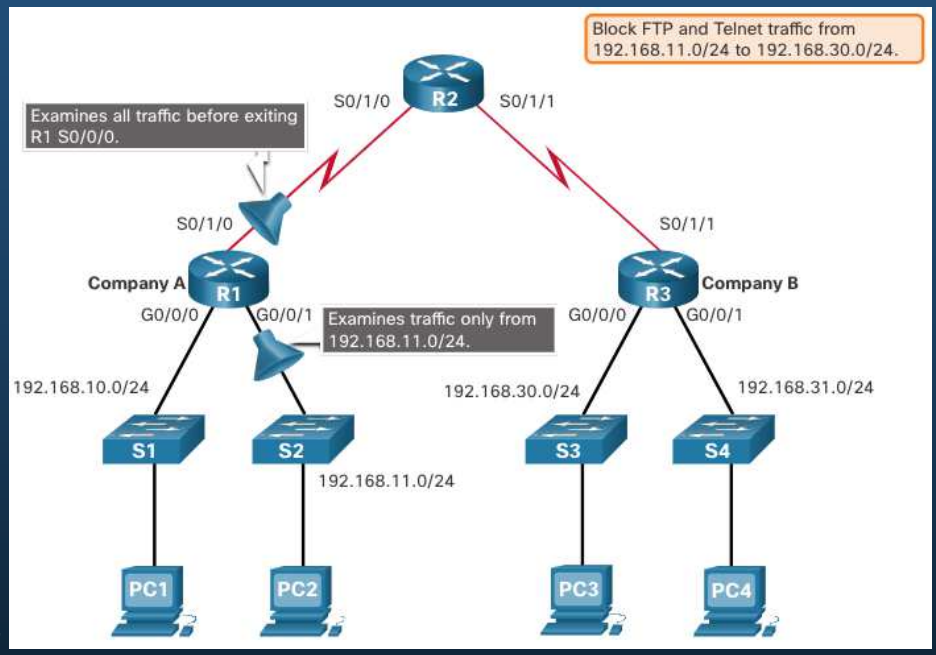
- Interfaz R3 S0 / 1/1 (entrante): la ACL estándar se puede aplicar entrante en la interfaz R3 S0 / 1/1 para denegar el tráfico de la red .10. Sin embargo, también filtraría el tráfico .10 a la red 192.168.31.0/24 (.31 en este ejemplo). Por lo tanto, la ACL estándar no debe aplicarse a esta interfaz.
- Interfaz R3 G0 / 0 (saliente): la ACL estándar se puede aplicar saliente en la interfaz R3 G0 / 0/0. Esto no afectará a otras redes accesibles por R3. Los paquetes de la red .10 aún podrán llegar a la red .31. Esta es la mejor interfaz para colocar la ACL estándar para cumplir con los requisitos de tráfico.



Tipos de ACLs IPv4

Ejemplo de colocación de ACL extendida

- Las ACL extendidas deben ubicarse lo más cerca posible de la fuente.
- Sin embargo, la organización solo puede colocar ACL en los dispositivos que controlan. Por lo tanto, la ubicación de ACL extendida debe determinarse en el contexto de dónde se extiende el control organizacional.
- En la figura, por ejemplo, la Compañía A quiere denegar el tráfico Telnet y FTP a la red 192.168.30.0/24 de la Compañía B desde su red 192.168.11.0/24, mientras permite el resto del tráfico.



Tipos de ACLs IPv4

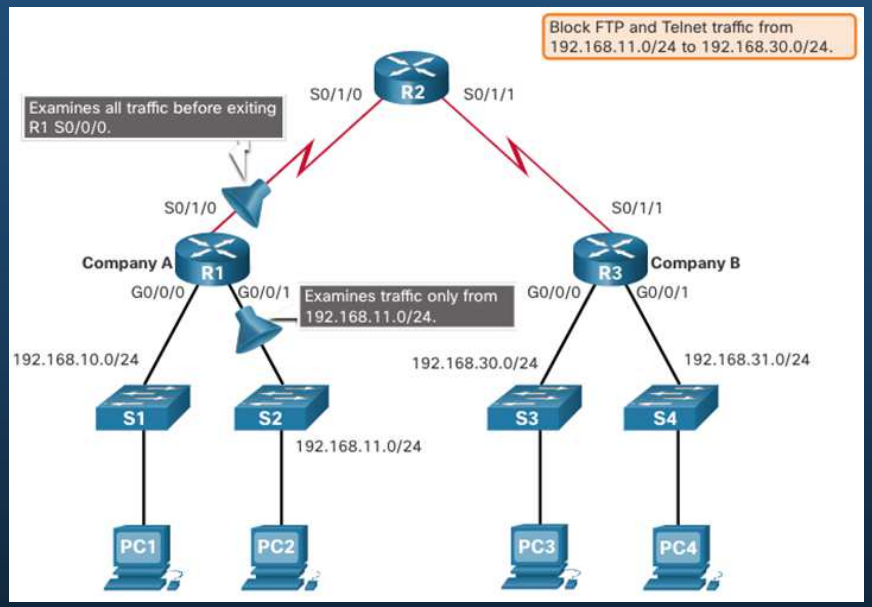
Ejemplo de colocación de ACL extendida

Una ACL extendida en R3 lograría la tarea, pero el administrador no controla R3. Además, esta solución permite que el tráfico no deseado atraviese toda la red y se bloquee en el destino.

La solución es colocar una ACL extendida en el R1 que especifique las direcciones de origen y destino.

Hay dos interfaces posibles en el R1 para aplicar la ACL extendida:

- Interfaz R1 S0 / 1/0 (saliente): la ACL extendida se puede aplicar saliente en la interfaz S0 / 1/0. Esta solución procesará todos los paquetes que salen de R1, incluidos los paquetes de 192.168.10.0/24.
- Interfaz R1 G0 / 0/1 (entrante): la ACL extendida se puede aplicar entrante en G0 / 0/1 y solo los paquetes de la red 192.168.11.0/24 están sujetos al procesamiento de ACL en R1. Debido a que el filtro se limitará solo a los paquetes que salen de la red 192.168.11.0/24, aplicar la ACL extendida a G0 / 1 es la mejor solución.



Capítulo 5

ACL para configuración IPv4

Configurar ACL IPv4 estándar

Crear una ACL

Todas las listas de control de acceso (ACL) deben planificarse. Al configurar una ACL compleja, se sugiere que:

- Utilice un editor de texto y escriba los detalles de la política que se va a implementar.
- Agregue los comandos de configuración del IOS para realizar esas tareas.
- Incluya comentarios para documentar la ACL.
- Copie y pegue los comandos en el dispositivo.
- Pruebe siempre exhaustivamente una ACL para asegurarse de que aplica correctamente la política deseada.

Configurar ACL IPv4 estándar

Sintaxis de una ACL de IPv4 estándar numerada

Para crear una ACL estándar numerada, utilice el comando **access-list** .

```
Router(config)# access-list access-list-number {deny | permit | remark text} source [source-wildcard]
[log]
```

Parámetro	Descripción
número-acl	El rango de números es de 1 a 99 o de 1300 a 1999
deny	Deniega el acceso si se dan las condiciones.
permit	Permite el acceso si se dan las condiciones.
texto **de observación**	(Opcional) entrada de texto para fines de documentación
origen	Identifica la red de origen o la dirección de host que se va a filtrar
comodín-origen	(Optativo) Máscara wildcard de 32 bits para aplicar al origen.
registrar	(Opcional) Genera y envía un mensaje informativo cuando el ACE coincide

Nota: Utilice el comando de configuración global **no access-list** *access-list-number* para eliminar una ACL estándar numerada.

Configurar ACL IPv4 estándar

Sintaxis de una ACL de IPv4 estándar con nombre

Para crear una ACL estándar numerada, utilice el **comando** ip access-list standard

- Los nombres de las ACL son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos.
- No es necesario que los nombres de las ACL comiencen con mayúscula, pero esto los hace destacarse cuando se observa el resultado de show running-config.

```
Router(config)# ip access-list standard access-list-name
```

```
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
R1(config-std-nacl)#
```

Configurar ACL IPv4 estándar

Aplicación de la ACL IPv4 estándar

Después de configurar una ACL IPv4 estándar, debe vincularse a una interfaz o entidad.

- El comando **ip access-group** se utiliza para enlazar una ACL IPv4 estándar numerada o nombrada a una interfaz.
- Para eliminar una ACL de una interfaz, primero introduzca el comando **no ip access-group** interface configuration.

```
Router(config-if) # ip access-group {access-list-number | access-list-name} {in | out}
```

Configurar ACL IPv4 estándar

Ejemplo de ACL estándar numerado

El ejemplo ACL permite el tráfico desde el host 192.168.10.10 y todos los hosts de la interfaz de salida de red 192.168.20.0/24 serial 0/1/0 en el router R1.

```
R1(config)# access-list 10 remark ACE permits ONLY host 192.168.10.10 to the internet
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
R1(config)#
```

```
R1(config)# access-list 10 remark ACE permits all host in LAN 2
R1(config)# access-list 10 permit 192.168.20.0 0.0.0.255
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1(config)#
```

```
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group 10 out
R1(config-if)# end
R1#
```

Configurar ACL IPv4 estándar

Ejemplos de ACL estándar numeradas

- Use el **comando** show running-config para revisar el ACL en la configuración.
- Use el **comando** show ip interface para verificar que el ACL esta aplicado a a interfaz

```
R1# show run | section access-list
access-list 10 remark ACE permits host 192.168.10.10
access-list 10 permit 192.168.10.10
access-list 10 remark ACE permits all host in LAN 2
access-list 10 permit 192.168.20.0 0.0.0.255
R1#
```

```
R1# show ip int Serial 0/1/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is 10
  Inbound Common access list is not set
  Inbound  access list is not set
R1#
```

Configurar ACL IPv4 estándar

Ejemplo de ACL estándar denominada

El ejemplo ACL permite el tráfico desde el host 192.168.10.10 y todos los hosts de la interfaz de salida de red 192.168.20.0/24 serial 0/1/0 en el router R1.

```
R1(config)# no access-list 10
R1(config)# ip access-list standard PERMIT-ACCESS
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)#
```

```
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)# remark ACE permits all hosts in LAN 2
R1(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)#
```

```
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group PERMIT-ACCESS out
R1(config-if)# end
R1#
```

Configurar ACL IPv4 estándar

Ejemplos de ACL numeradas estandar

- Use el **comando show access-list** show access-list para revisar el ACL en la configuración.
- Use el **comando** show ip interface para verificar que el ACL está aplicado a la interfaz.

```
R1# show access-lists
Standard IP access list PERMIT-ACCESS
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1# show run | section ip access-list
ip access-list standard PERMIT-ACCESS
 remark ACE permits host 192.168.10.10
 permit 192.168.10.10
 remark ACE permits all hosts in LAN 2
 permit 192.168.20.0 0.0.0.255
R1#
```

```
R1# show ip int Serial 0/1/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is PERMIT-ACCESS
  Inbound Common access list is not set
  Inbound  access list is not set
R1#
```

Modificación de ACL IPv4

Dos métodos para modificar una ACL

Después de configurar una ACL, es posible que deba modificarse. Las ACL con varias ACE pueden ser complejas de configurar. A veces, el ACE configurado no produce los comportamientos esperados.

Hay dos métodos que se deben utilizar al modificar una ACL:

- Utilice un editor de texto.
- Utilice números de secuencia

Modificación de ACL IPv4

Método de editor de textos

Las ACL con varias ACE deben crearse en un editor de texto. Esto permite crear o editar la ACL y luego pegarla en la interfaz del router. También simplifica las tareas para editar y corregir una ACL.

Para corregir un error en una ACL:

- Copie la ACL de la configuración en ejecución y péguela en el editor de texto.
- Realice las ediciones o cambios necesarios.
- Elimine la ACL configurada previamente en el router.
- Copie y pegue la ACL editada de nuevo en el router.

```
R1# show run | section access-list
access-list 1 deny   19.168.10.10
access-list 1 permit 192.168.10.0 0.0.0.255
R1#
```

```
R1(config)# no access-list 1
R1(config)#
R1(config)# access-list 1 deny 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#
```

Modificación de ACL IPv4

Método secuencia de números

Una ACE ACL se puede eliminar o agregar utilizando los números de secuencia ACL.

- Utilice el comando **ip access-list standard** para editar una ACL.
- Las instrucciones no se pueden sobrescribir con el mismo número de secuencia que el de una instrucción existente. La instrucción actual debe eliminarse primero con el comando **no 10**. A continuación, se puede agregar el ACE correcto utilizando el número de secuencia.

```
R1# show access-lists
Standard IP access list 1
    10 deny   19.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

Modificación de ACL IPv4

Modificar una ACL con nombre Ejemplo

Las ACL con nombre también pueden utilizar números de secuencia para eliminar y agregar ACE. En el ejemplo se agrega una ACE para denegar hosts 192.168.10.11.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
```

```
R1# configure terminal
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# 15 deny 192.168.10.5
R1(config-std-nacl)# end
R1#
R1# show access-lists
Standard IP access list NO-ACCESS
    15 deny   192.168.10.5
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

Modificación de ACL IPv4

Estadísticas de una ACL

El comando **show access-lists** del ejemplo muestra las estadísticas de cada sentencia que se ha coincidente.

- El ACE de denegación se ha igualado 20 veces y el ACE de permiso se ha igualado 64 veces.
- Tenga en cuenta que la declaración deny any implícita no muestra ninguna estadística. Para realizar un seguimiento de cuántos paquetes denegados implícitos se han asociado, debe configurar manualmente el comando **deny any** .
- Utilice el comando **clear access-list counters** para borrar las estadísticas de ACL.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10  (20 matches)
    20 permit 192.168.10.0, wildcard bits 0.0.0.255  (64 matches)
R1# clear access-list counters NO-ACCESS
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

Puertos VTY con ACL IPv4 estándar

El comando access-class

Una ACL estándar puede proteger el acceso administrativo remoto a un dispositivo mediante las líneas vty implementando los dos siguientes pasos:

- Cree una ACL para identificar a qué hosts administrativos se debe permitir el acceso remoto.
- Aplique la ACL al tráfico entrante en las líneas vty.

```
R1(config-line)# access-class {access-list-number | access-list-name} { in | out }
```

Puertos VTY con ACL IPv4 estándar

Ejemplo de acceso seguro a VTY

En este ejemplo se muestra cómo configurar una ACL para filtrar el tráfico vty.

- En primer lugar, se configura una entrada de base de datos local para un usuario **ADMIN** y una **clase** de contraseña.
- Las líneas vty en R1 están configuradas para utilizar la base de datos local para la autenticación, permitir el tráfico SSH y utilizar la ACL ADMIN-HOST para restringir el tráfico.

```
R1(config)# username ADMIN secret class
R1(config)# ip access-list standard ADMIN-HOST
R1(config-std-nacl)# remark This ACL secures incoming vty lines
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# access-class ADMIN-HOST in
R1(config-line)# end
R1#
```

Puertos VTY con ACL IPv4 estándar

Verificar que el puerto VTY esté asegurado

Después de configurar la ACL para restringir el acceso a las líneas VTY, es importante verificar que funcione correctamente.

Para verificar las estadísticas de ACL, ejecute el comando **show access-lists** .

- La coincidencia en la línea permit del resultado es producto de una conexión SSH correcta de la PC192.168.10.10.
- La coincidencia en la instrucción deny se debe al intento fallido de una PC, a un dispositivo en la red , de establecer una conexión SSH.

```
R1#
Oct  9 15:11:19.544: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 192.168.10.10]
[localport: 23] at 15:11:19 UTC Wed Oct 9 2019
R1# show access-lists
Standard IP access list ADMIN-HOST
    10 permit 192.168.10.10  (2 matches)
    20 deny   any  (2 matches)
R1#
```

Configuración de ACL IPv4 extendidas

ACL extendidas

Las ACL extendidas proporcionan un mayor rango de control. Pueden filtrar por dirección de origen, dirección de destino, protocolo (es decir, IP, TCP, UDP, ICMP) y número de puerto.

Las ACL extendidas se pueden crear como:

- **ACL extendida numerada:** creada mediante el comando de configuración global **access-list** *access-list-number*.
- **Llamada ACL extendida:** creada usando el **nombre de lista de acceso extendido de ip access-list** .

Configuración de ACL IPv4 extendidas

Protocolos y puertos de ACL IPv4 extendidos

Las ACL extendidas se pueden filtrar por protocolo y número de puerto. Usar el símbolo **"?"** para obtener ayuda al ingresar a un ACE complejo. Los cuatro protocolos resaltados son las opciones más populares.

Opciones de protocolo

```
R1(config)# access-list 100 permit ?
  <0-255>        An IP protocol number
  ahp            Authentication Header Protocol
  dvmrp          dvmrp
  eigrp          Cisco's EIGRP routing protocol
  esp            Encapsulation Security Payload
  gre            Cisco's GRE tunneling
  icmp           Internet Control Message Protocol
  igmp           Internet Gateway Message Protocol
  ip             Any Internet Protocol
  ipinip         IP in IP tunneling
  nos            KA9Q NOS compatible IP over IP tunneling
  object-group   Service object group
  ospf           OSPF routing protocol
  pcp            Payload Compression Protocol
  pim            Protocol Independent Multicast
  tcp            Transmission Control Protocol
  udp            User Datagram Protocol
R1(config)# access-list 100 permit
```

Configuración de ACL IPv4 extendidas

Protocolos y puertos de ACL IPv4 extendidos

La selección de un protocolo influye en las opciones de puerto. Muchas opciones de puerto TCP están disponibles, como se muestra en la salida.

```
R1(config)# access-list 100 permit tcp any any eq ?
  <0-65535>     Port number
  bgp           Border Gateway Protocol (179)
  chargen       Character generator (19)
  cmd           Remote commands (rcmd, 514)
  daytime       Daytime (13)
  discard       Discard (9)
  domain        Domain Name Service (53)
  echo          Echo (7)
  exec          Exec (rsh, 512)
  finger        Finger (79)
  ftp           File Transfer Protocol (21)
  ftp-data      FTP data connections (20)
  gopher        Gopher (70)
  hostname      NIC hostname server (101)
  ident         Ident Protocol (113)
  irc           Internet Relay Chat (194)
  klogin        Kerberos login (543)
  kshell        Kerberos shell (544)
  login         Login (rlogin, 513)
  lpd           Printer service (515)
  msrpc         MS Remote Procedure Call (135)
  nntp          Network News Transport Protocol (119)
  onep-plain    Onep Cleartext (15001)
  onep-tls      Onep TLS (15002)
  pim-auto-rp   PIM Auto-RP (496)
  pop2          Post Office Protocol v2 (109)
  pop3          Post Office Protocol v3 (110)
  smtp          Simple Mail Transport Protocol (25)
  sunrpc        Sun Remote Procedure Call (111)
  syslog        Syslog (514)
  tacacs        TAC Access Control System (49)
  talk          Talk (517)
  telnet        Telnet (23)
  time          Time (37)
  uucp          Unix-to-Unix Copy Program (540)
  whois         Nicname (43)
  www           World Wide Web (HTTP, 80)
```

Configuración de ACL IPv4 extendidas

Ejemplos de configuración de números de puerto y protocolos de ACL IPv4 extendidos

Las ACL extendidas pueden filtrar en diferentes opciones de número de puerto y nombre de puerto.

En este ejemplo se configura una ACL 100 extendida para filtrar el tráfico HTTP. El primer ACE utiliza el nombre del puerto **www**. El segundo ACE utiliza el número de puerto **80**. Ambas ACE logran exactamente el mismo resultado.

```
R1(config)# access-list 100 permit tcp any any eq www
!or...
R1(config)# access-list 100 permit tcp any any eq 80
```

La configuración del número de puerto es necesaria cuando no aparece un nombre de protocolo específico, como SSH (número de puerto 22) o HTTPS (número de puerto 443), como se muestra en el siguiente ejemplo.

```
R1(config)# access-list 100 permit tcp any any eq 22
R1(config)# access-list 100 permit tcp any any eq 443
R1(config)#
```

Configuración de ACL IPv4 extendidas

Aplicar una ACL IPv4 extendida numerada

En este ejemplo, la ACL permite que el tráfico HTTP y HTTPS de la red 192.168.10.0 vaya a cualquier destino.

Las ACL extendidas se pueden aplicar en varias ubicaciones. Sin embargo, normalmente se aplican cerca del origen. Aquí ACL 110 se aplica entrante en la interfaz R1 G0/0/0.

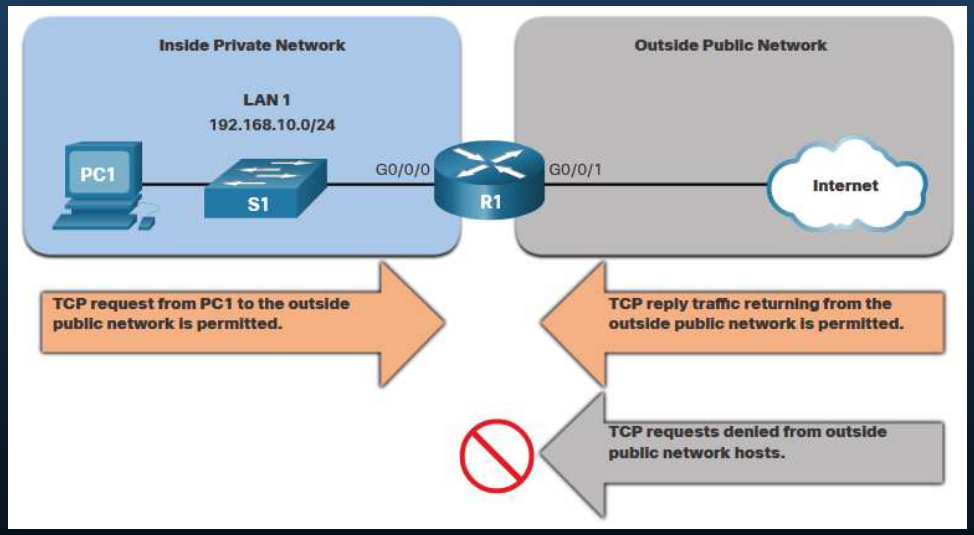
```
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 110 in
R1(config-if)# exit
R1(config)#
```

Configuración de ACL IPv4 extendidas

TCP Establecida ACL extendida

TCP también puede realizar servicios básicos de firewall con estado usando la **palabra clave TCP establecida**.

- **La palabra clave establecida** permite que el tráfico interno salga de la red privada interna y permite que el tráfico de respuesta devuelta entre en la red privada interna.
- Se deniega el tráfico TCP generado por un host externo e intentando comunicarse con un host interno.



Configuración de ACL IPv4 extendidas

TCP Establecida ACL extendida

- ACL 120 está configurado para permitir sólo devolver tráfico web a los hosts internos. A continuación, la ACL se aplica saliente en la interfaz R1 G0/0/0.
- El comando **show access-lists** muestra que los hosts internos están accediendo a los recursos web seguros desde Internet.

Nota: Si el segmento TCP que regresa tiene los bits ACK o de restablecimiento (RST) establecidos, que indican que el paquete pertenece a una conexión existente, se produce una coincidencia TCP.

```
R1(config)# access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 120 out
R1(config-if)# end
R1# show access-lists
Extended IP access list 110
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (657 matches)
Extended IP access list 120
    10 permit tcp any 192.168.10.0 0.0.0.255 established (1166 matches)
R1#
```

Configuración de ACL IPv4 extendidas

Creación de ACL extendidas denominadas

La asignación de nombres a las ACL hace más fácil comprender su función. Para crear una ACL extendida con nombre, utilice el comando **ip access-list extended** configuration.

En el ejemplo, se crea una ACL extendida con nombre llamada NO-FTP-ACCESS y el indicador cambia a modo de configuración ACL extendida con nombre. Las sentencias ACE se introducen en el modo de subconfiguración de ACL extendido con nombre.

```
Router(config)# ip access-list extended access-list-name
```

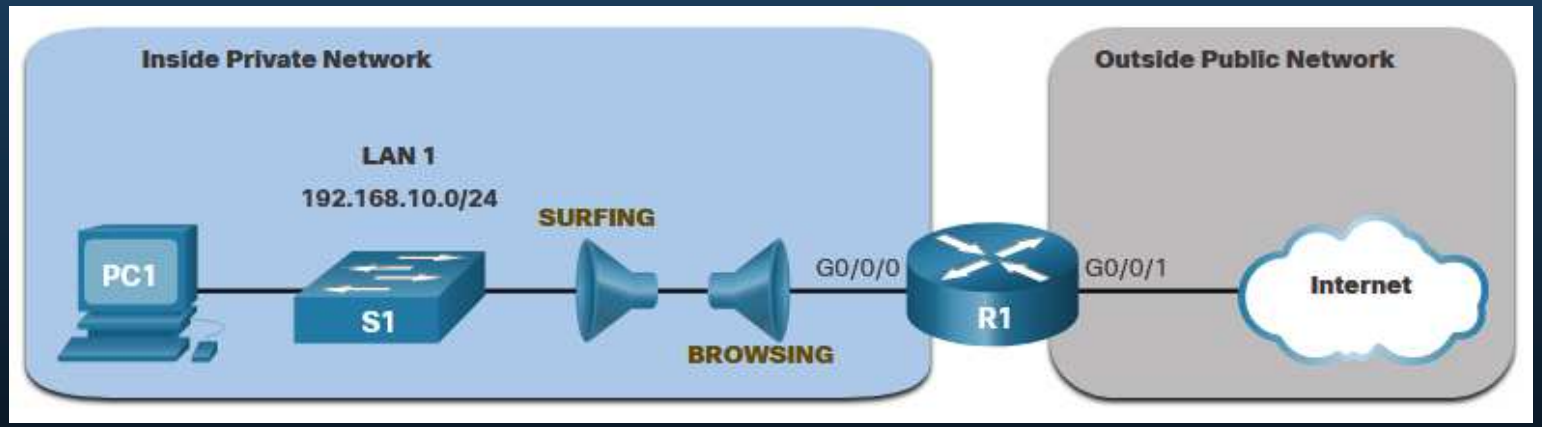
```
R1(config)# ip access-list extended NO-FTP-ACCESS
R1(config-ext-nacl)#
```

Configuración de ACL IPv4 extendidas

Creación de ACL extendidas denominadas

La topología a continuación se utiliza para demostrar la configuración y aplicación de dos ACL IPv4 extendidas con nombre a una interfaz:

- **SURF** - Esto permitirá que dentro del tráfico HTTP y HTTPS salga a Internet.
- **Navegación** - Esto solo permitirá devolver tráfico web a los hosts internos mientras que todo el resto del tráfico que sale de la interfaz R1 G0/0/0 está implícitamente denegado.



Configuración de ACL IPv4 extendidas

Creación de ACL extendidas denominadas

- La ACL de SURF permite que el tráfico HTTP y HTTPS de los usuarios internos salga de la interfaz G0/0/1 conectada a Internet. La ACL de navegación permite que el tráfico web que regrese de Internet vuelva a la red privada interna.
- La ACL de SURF se aplica entrante y la ACL de navegación se aplica saliente en la interfaz R1 G0/0/0.

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# Remark Permits inside HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# Remark Only permit returning HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
R1(config-if)# end
R1# show access-lists
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (124 matches)
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established (369 matches)
R1#
```

Configuración de ACL IPv4 extendidas

Creación de ACL extendidas denominadas

Para verificar las estadísticas de ACL, ejecute el comando show access-lists. Observe que los contadores HTTPS seguros de permiso (es decir, eq 443) en la ACL de SURF y los contadores de retorno establecidos en la ACL de navegación han aumentado.

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

Configuración de ACL IPv4 extendidas

Edición de ACL extendidas

Una ACL extendida se puede editar utilizando un editor de texto cuando se requieren muchos cambios. O bien, si la edición se aplica a una o dos ACE, se pueden utilizar números de secuencia.

Por ejemplo:

- El número de secuencia ACE 10 de la ACL de SURF tiene una dirección de red IP de origen incorrecta.

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

Configuración de ACL IPv4 extendidas

Edición de ACL extendida

- Para corregir este error, la sentencia original se elimina con el comando **no** *sequence_#* y la sentencia corregida se agrega reemplazando la sentencia original.
- El resultado del comando **show access-lists** verifica el cambio de configuración.

```
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config-ext-nacl)# end
```

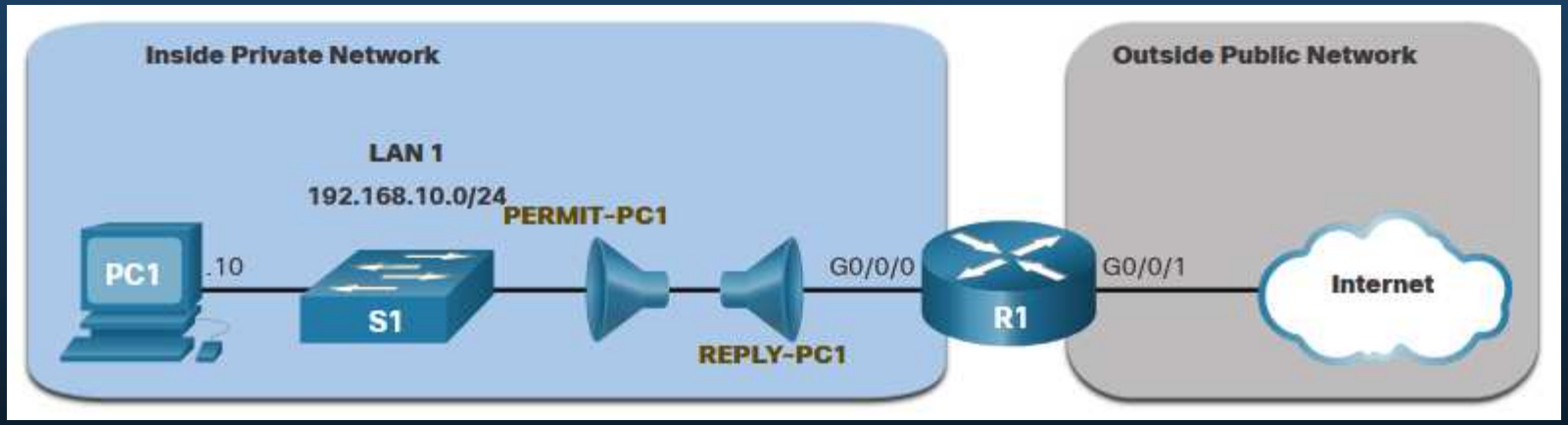
```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

Configuración de ACL IPv4 extendidas

Otro ejemplo de ACL IPv4 Extendida

Se crearán dos ACL extendidas con nombre:

- **PERMIT-PC1** - Esto sólo permitirá el acceso TCP PC1 a Internet y denegará todos los demás hosts de la red privada.
- **REPLY-PC1** - Esto sólo permitirá que el tráfico TCP devuelto especificado a PC1 deniegue implícitamente todo el resto del tráfico.



Configuración de ACL IPv4 extendidas

Otro ejemplo de ACL IPv4 Extendida

- La **ACL PERMIT-PC1** permite el acceso TCP PC1 (192.168.10.10) al tráfico FTP, SSH, Telnet, DNS, HTTP y HTTPS.
- La ACL **REPLY-PC1** permitirá el tráfico de retorno a PC1.
- La **ACL PERMIT-PC1** se aplica entrante y la ACL **REPLY-PC1** se aplica saliente en la interfaz R1 G0/0/0.

```
R1(config)# ip access-list extended PERMIT-PC1
R1(config-ext-nacl)# Remark Permit PC1 TCP access to internet
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 20
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 21
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 22
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 23
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 53
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 80
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 443
R1(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 any
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended REPLY-PC1
R1(config-ext-nacl)# Remark Only permit returning traffic to PC1
R1(config-ext-nacl)# permit tcp any host 192.168.10.10 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group PERMIT-PC1 in
R1(config-if)# ip access-group REPLY-PC1 out
R1(config-if)# end
R1#
```

Configuración de ACL IPv4 extendidas

Verificación de ACL extendidas

El comando **show ip interface** se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is REPLY-PC1
  Inbound  access list is PERMIT-PC1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
R1#
R1# show ip interface g0/0/0 | include access list
Outgoing access list is REPLY-PC1
Inbound access list is PERMIT-PC1
R1#
```

Configuración de ACL IPv4 extendidas

Verifique ACLs extendidas

El comando **show access-lists** se puede utilizar para confirmar que las ACL funcionan como se esperaba. El comando muestra contadores estadísticos que aumentan cada vez que se hace coincidir una ACE.

Nota: Se debe generar tráfico para verificar el funcionamiento de la ACL.

```
R1# show access-lists
Extended IP access list PERMIT-PC1
10 permit tcp host 192.168.10.10 any eq 20
20 permit tcp host 192.168.10.10 any eq ftp
30 permit tcp host 192.168.10.10 any eq 22
40 permit tcp host 192.168.10.10 any eq telnet
50 permit tcp host 192.168.10.10 any eq domain
60 permit tcp host 192.168.10.10 any eq www
70 permit tcp host 192.168.10.10 any eq 443
80 deny ip 192.168.10.0 0.0.0.255 any
Extended IP access list REPLY-PC1
10 permit tcp any host 192.168.10.10 established
R1#
```

Configuración de ACL IPv4 extendidas

Verifique ACLs extendidas

El comando **show running-config** se puede utilizar para validar lo que se configuró. El comando también muestra las observaciones configuradas.

```
R1# show running-config | begin ip access-list
ip access-list extended PERMIT-PC1
remark Permit PC1 TCP access to internet
permit tcp host 192.168.10.10 any eq 20
permit tcp host 192.168.10.10 any eq ftp
permit tcp host 192.168.10.10 any eq 22
permit tcp host 192.168.10.10 any eq telnet
permit tcp host 192.168.10.10 any eq domain
permit tcp host 192.168.10.10 any eq www
permit tcp host 192.168.10.10 any eq 443
deny ip 192.168.10.0 0.0.0.255 any
ip access-list extended REPLY-PC1
remark Only permit returning traffic to PC1
permit tcp any host 192.168.10.10 established
!
```

Capítulo 6

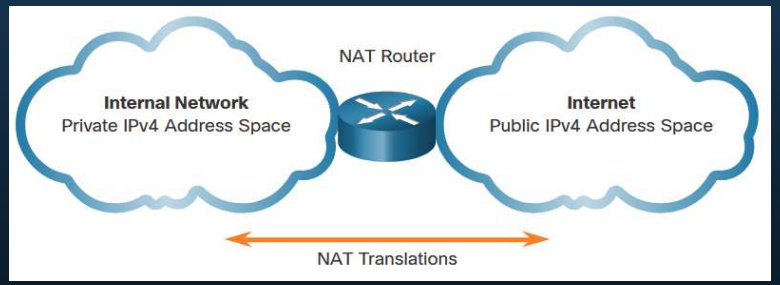
NAT para IPv4

Caracteristicas de NAT

Espacio de direcciones IPv4

- Las redes suelen implementarse mediante el uso de direcciones IPv4 privadas, según se definen en RFC 1918.
- Las direcciones IPv4 privadas no se pueden enrutar a través de Internet y se usan dentro de una organización o sitio para permitir que los dispositivos se comuniquen localmente.
- Para permitir que un dispositivo con una dirección IPv4 privada acceda a recursos y dispositivos fuera de la red local, primero se debe traducir la dirección privada a una dirección pública.
- NAT proporciona la traducción de direcciones privadas a direcciones públicas.

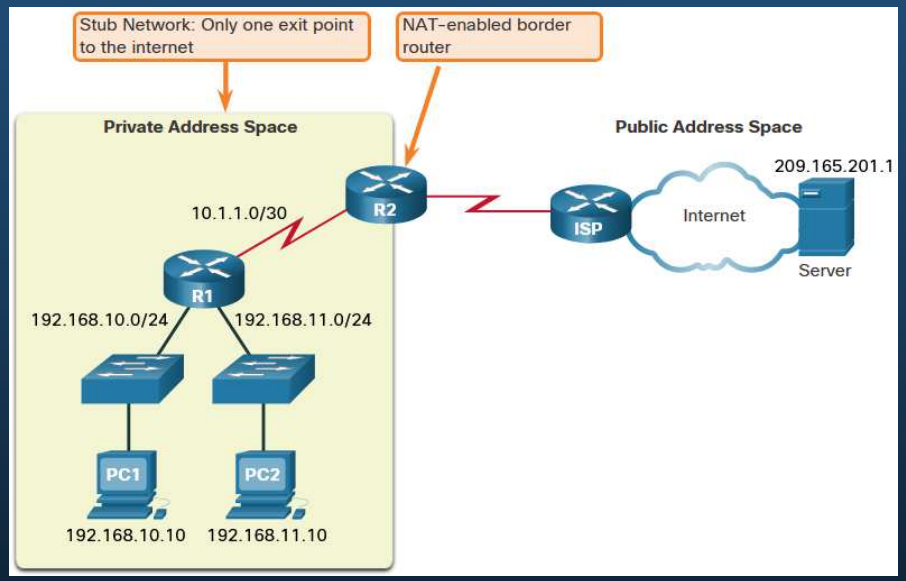
Clase	Tipo de actividad	Nombre de la actividad
servidor	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16



Caracteristicas de NAT

¿Qué es NAT?

- El uso principal de NAT es conservar las direcciones IPv4 públicas.
- NAT permite que las redes utilicen direcciones IPv4 privadas internamente y las traduce a una dirección pública cuando sea necesario.
- En general, los routers NAT funcionan en la frontera de una red de rutas internas.
- Cuando un dispositivo dentro de la red auxiliar desea comunicarse con un dispositivo fuera de su red, el paquete se reenvía al enrutador fronterizo que realiza el proceso NAT, traduciendo la dirección privada interna del dispositivo a una dirección pública, externa y enrutable.



Caracteristicas de NAT

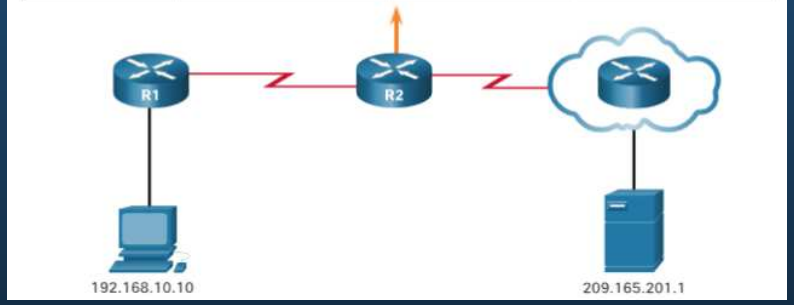
¿Cómo funciona NAT?

PC1 quiere comunicarse con un servidor web externo con dirección pública 209.165.201.1.

1. La PC1 envía un paquete dirigido al servidor web.
2. R2 recibe el paquete y lee la dirección IPv4 de origen para determinar si necesita traducción.
3. R2 agrega la asignación de la dirección local a la global a la tabla NAT.
4. El R2 envía el paquete con la dirección de origen traducida hacia el destino.
5. El servidor web responde con un paquete dirigido a la dirección global interna de la PC1 (209.165.200.226).
6. El R2 recibe el paquete con la dirección de destino 209.165.200.226. El R2 revisa la tabla de NAT y encuentra una entrada para esta asignación. El R2 usa esta información y traduce la dirección global interna (209.165.200.226) a la dirección local interna (192.168.10.10), y el paquete se reenvía a la PC1.

NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



Caracteristicas de NAT

Terminología de NAT

NAT incluye cuatro tipos de direcciones:

- Dirección local interna
- Dirección global interna
- Dirección local externa
- Dirección global externa

La terminología NAT siempre se aplica desde la perspectiva del dispositivo con la dirección traducida:

- **Dirección interna -** La dirección del dispositivo que NAT está traduciendo.
- **Dirección externa -** La dirección del dispositivo de destino.
- **Dirección local -** Una dirección local es cualquier dirección que aparece en la parte interna de la red.
- **Dirección global -** Una dirección global es cualquier dirección que aparece en la parte externa de la red.

Caracteristicas de NAT

Terminología de NAT

Dirección local interna

La dirección de la fuente vista desde dentro de la red. Normalmente, es una dirección IPv4 privada. La dirección local interna de PC1 es 192.168.10.10.

Direcciones globales internas

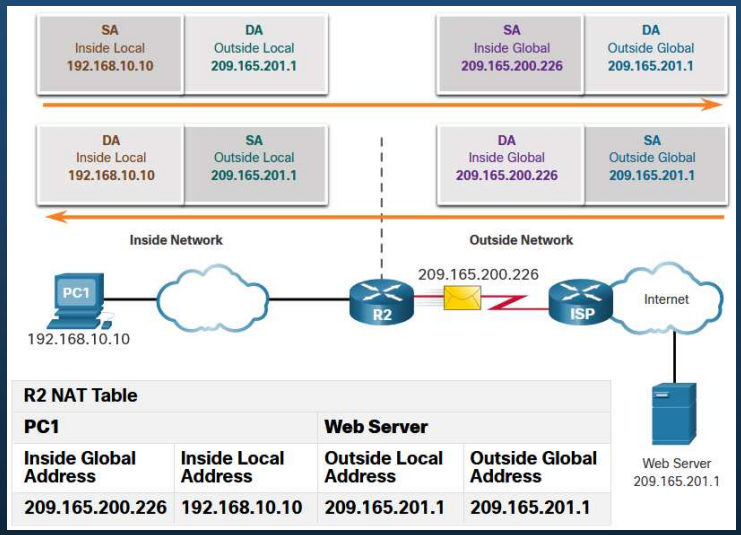
La dirección de origen vista desde la red externa. La dirección global interna de PC1 es 209.165.200.226

Dirección global externa

La dirección del destino vista desde la red externa. La dirección global externa del servidor web es 209.165.201.1

Dirección local externa

La dirección del destino como se ve desde la red interna. La PC1 envía tráfico al servidor web en la dirección IPv4 209.165.201.1. Si bien es poco frecuente, esta dirección podría ser diferente de la dirección globalmente enrutable del destino.



R2 NAT Table

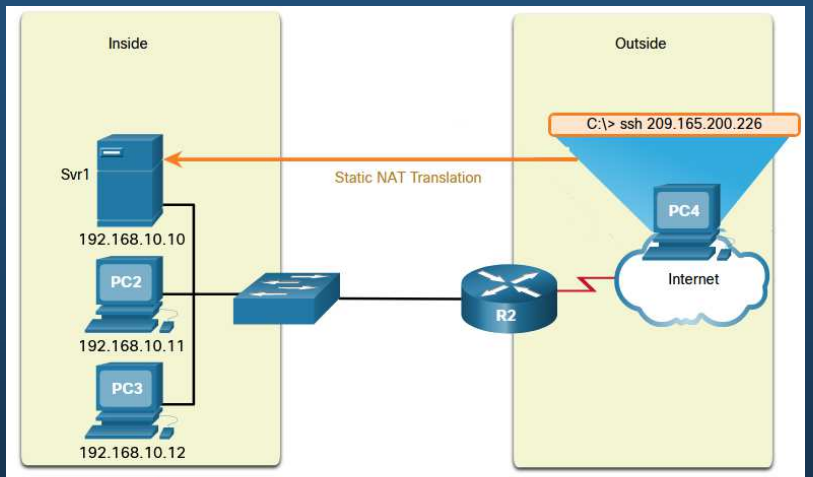
PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

Tipos de NAT

NAT estático

La NAT estática utiliza una asignación uno a uno de direcciones locales y globales configuradas por el administrador de la red que permanecen constantes.

- La NAT estática es útil para servidores web o dispositivos que deben tener una dirección coherente a la que se pueda acceder desde Internet, como un servidor web de la empresa.
- También es útil para dispositivos que deben ser accesibles por personal autorizado cuando se encuentra fuera del sitio, pero no por el público en general en Internet.



Static NAT Table

Inside Local Address	Inside Global Address – Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Nota: NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer el número total de sesiones de usuario simultáneas.

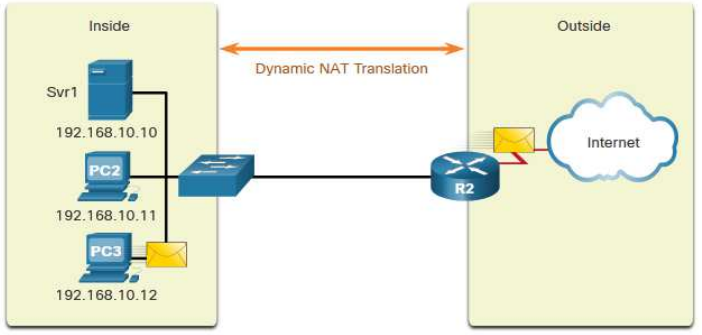
Tipos de NAT

NAT Dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada.

- Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto.
- Las otras direcciones del grupo todavía están disponibles para su uso.

Nota: NAT dinámica requiere que haya suficientes direcciones públicas disponibles para satisfacer el número total de sesiones de usuario simultáneas.



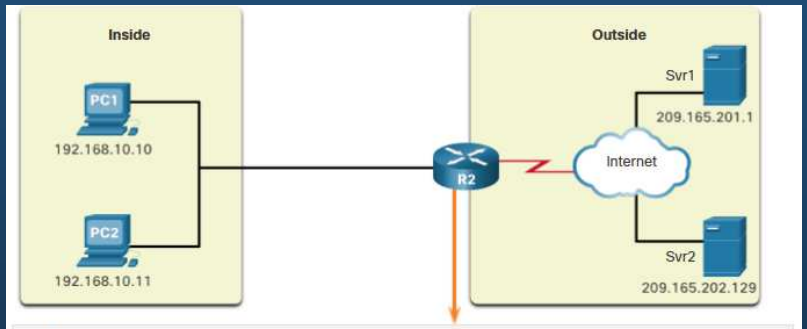
IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool - Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

Tipos de NAT

Traducción de dirección de puerto

La traducción de la dirección del puerto (PAT), también conocida como “NAT con sobrecarga”, asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o a algunas direcciones.

- Con PAT, cuando el router NAT recibe un paquete del cliente, utiliza el número de puerto de origen para identificar de forma exclusiva la traducción NAT específica.
- PAT garantiza que los dispositivos usen un número de puerto TCP diferente para cada sesión con un servidor en Internet



NAT Table with Overload

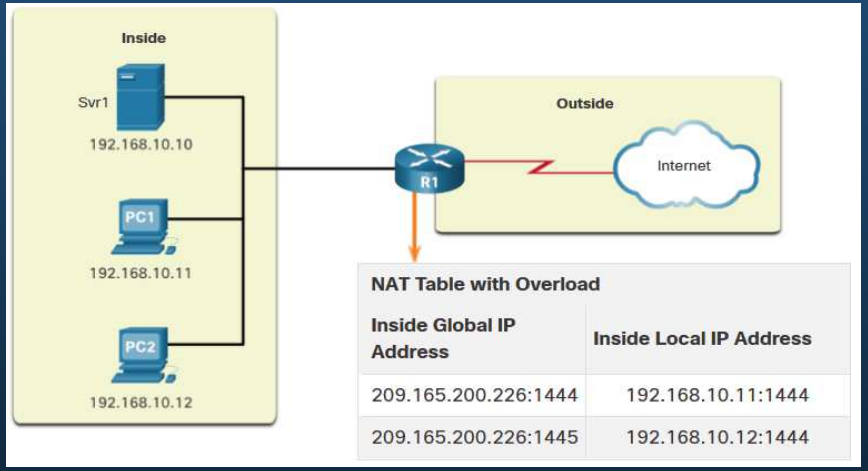
Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

Tipos de NAT

Siguiente puerto disponible

PAT intenta conservar el puerto de origen inicial. Si el puerto de origen original ya está en uso, PAT asigna el primer número de puerto disponible a partir del comienzo del grupo de puertos apropiado 0-511, 512-1,023 o 1,024-65,535.

- Cuando no hay más puertos disponibles y hay más de una dirección externa en el conjunto de direcciones, PAT avanza a la siguiente dirección para intentar asignar el puerto de origen inicial.
- El proceso continúa hasta que no haya más puertos disponibles o direcciones IPv4 externas en el grupo de direcciones.



Tipos de NAT

Comparación entre NAT y PAT

Resumen de las diferencias entre NAT y PAT.

NAT : solo modifica las direcciones IPv4

Dirección global interna	Dirección local interna
209.165.200.226	192.168.10.10

PAT - PAT modifica tanto la dirección IPv4 como el número de puerto.

Dirección global interna	Dirección local interna
209.165.200. 226:2031	192.168.10. 10:2031

NAT	PAT
Mapeo uno a uno entre las direcciones Local interna y Global interna.	Una dirección global interna se puede asignar a muchas direcciones locales internas.
Utiliza sólo direcciones IPv4 en el proceso de traducción.	Utiliza direcciones IPv4 y números de puerto de origen TCP o UDP en el proceso de traducción.
Se requiere una dirección global interna única para cada host interno que acceda a la red externa.	Muchos hosts internos que acceden a la red externa pueden compartir una única dirección global interna única.

Tipos de NAT

Paquetes sin un segmento de capa 4

Algunos paquetes no contienen un número de puerto de Capa 4, como mensajes ICMPv4. PAT maneja cada uno de estos tipos de protocolos de manera diferente.

Por ejemplo, los mensajes de consulta, las solicitudes de eco y las respuestas de eco de ICMPv4 incluyen una ID de consulta. ICMPv4 utiliza la ID de consulta para identificar una solicitud de eco con su respectiva respuesta.

Nota: Otros mensajes ICMPv4 no usan la ID de consulta. Estos mensajes y otros protocolos que no utilizan los números de puerto TCP o UDP varían y exceden el ámbito de este currículo.

Ventajas y desventajas de NAT

Ventajas de NAT

NAT proporciona muchos beneficios:

- NAT conserva el esquema de direccionamiento legalmente registrado al permitir la privatización de las intranets.
- NAT conserva las direcciones mediante la multiplexación de aplicaciones en el nivel de puerto.
- NAT aumenta la flexibilidad de las conexiones a la red pública.
- NAT proporciona coherencia a los esquemas de direccionamiento de red interna.
- NAT permite mantener el esquema de direcciones IPv4 privadas existente a la vez que facilita el cambio a un nuevo esquema de direccionamiento público.
- NAT oculta las direcciones IPv4 de los usuarios y otros dispositivos.

Ventajas y desventajas de NAT

Desventajas de NAT

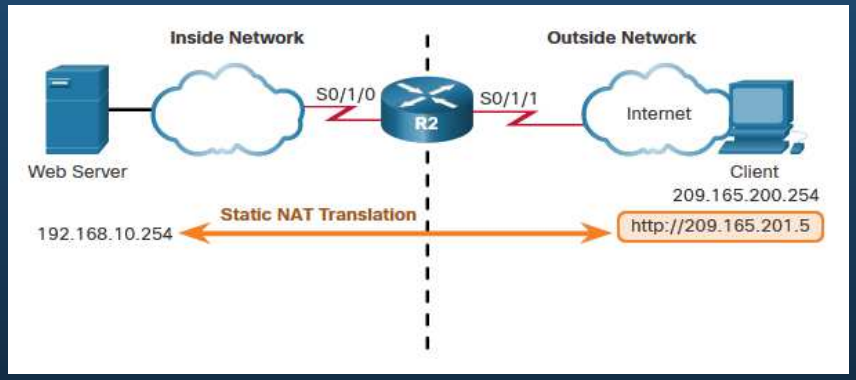
NAT tiene inconvenientes:

- NAT aumenta los retrasos de reenvío.
- Se pierde el direccionamiento de extremo a extremo.
- Se pierde la trazabilidad IPv4 de extremo a extremo.
- NAT complica el uso de protocolos de túnel, como IPSec.
- Los servicios que requieren que se inicie una conexión TCP desde la red externa, o "protocolos sin estado", como los servicios que utilizan UDP, pueden interrumpirse.

NAT estático

Escenario NAT estático

- La NAT estática es una asignación uno a uno entre una dirección interna y una dirección externa.
- La NAT estática permite que los dispositivos externos inicien conexiones a los dispositivos internos mediante la dirección pública asignada de forma estática.
- Por ejemplo, se puede asignar una dirección global interna específica a un servidor web interno de modo que se pueda acceder a este desde redes externas.



NAT estático

Configurar NAT estático

Hay dos tareas básicas al configurar traducciones NAT estáticas:

- **Paso 1** - Crear una asignación entre la dirección local interna y las direcciones globales internas utilizando el comando ip nat inside source static.
- **Paso 2** - Las interfaces que participan en la traducción se configuran como dentro o fuera en relación con NAT con los comandos ip nat dentro y ip nat outside.

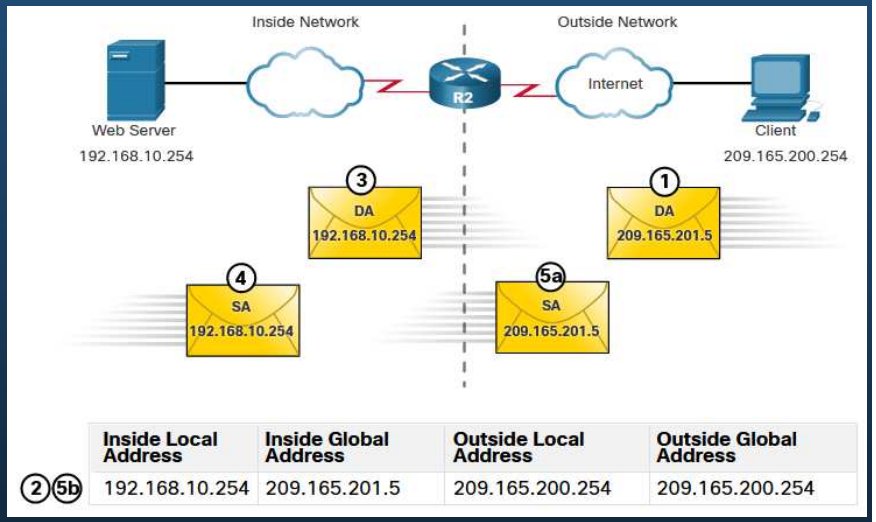
```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)#
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

NAT estático

Analizar NAT estático

El proceso de traducción NAT estática entre el cliente y el servidor web:

1. El cliente envía un paquete al servidor web.
2. R2 recibe paquetes del cliente en su interfaz NAT externa y verifica su tabla NAT.
3. R2 traduce la dirección global interna de la dirección local interna y reenvía el paquete hacia el servidor web.
4. El servidor web recibe el paquete y responde al cliente utilizando su dirección local interna.
5. (a) R2 recibe el paquete del servidor web en su interfaz interna NAT con la dirección de origen de la dirección local interna del servidor web y (b) traduce la dirección de origen a la dirección global interna.



	Inside Local Address	Inside Global Address	Outside Local Address	Outside Global Address
2 5b	192.168.10.254	209.165.201.5	209.165.200.254	209.165.200.254

NAT estático

Verificación de NAT estático

Para verificar la operación NAT, emita el comando **show ip nat translation**.

- Este comando muestra las traducciones NAT activas.
- Debido a que el ejemplo es una configuración NAT estática, siempre figura una traducción en la tabla de NAT, independientemente de que haya comunicaciones activas.
- Si el comando se emite durante una sesión activa, la salida también indica la dirección del dispositivo externo.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
— 209.165.201.5 192.168.10.254 — —
Total number of translations: 1
```

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.201.5 192.168.10.254 209.165.200.254 209.165.200.254 209.165.200.254
--- 209.165.201.5 192.168.10.254 --- ---
Total number of translations: 2
```

NAT estático

Verificación de NAT

Otro comando útil es **show ip nat stats**.

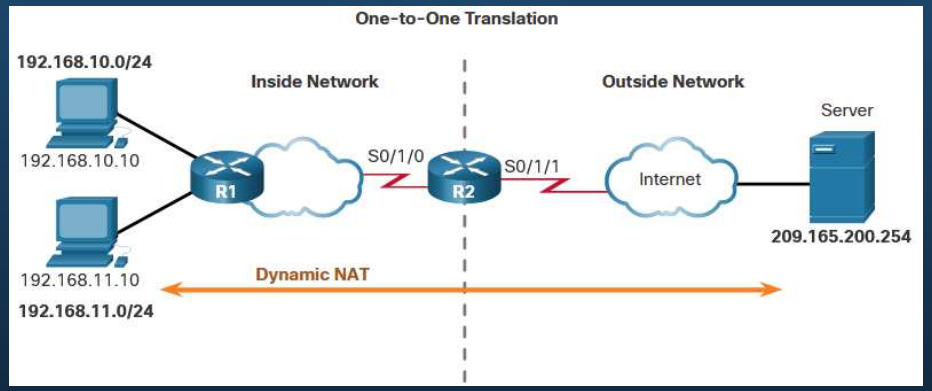
- Muestra información sobre el número total de traducciones activas, los parámetros de configuración de NAT, el número de direcciones en el grupo y el número de direcciones que se han asignado.
- Para verificar que la traducción NAT está funcionando, es mejor borrar las estadísticas de cualquier traducción anterior utilizando el comando **clear ip nat statistics** antes de realizar la prueba.

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4 Misses: 1
(resultado omitido)
```

NAT dinámico

Escenario NAT dinámico

- NAT dinámico asigna automáticamente dentro de direcciones locales a direcciones globales dentro.
- NAT Dinámica utiliza un grupo de direcciones globales internas.
- El conjunto de direcciones globales internas está disponible para cualquier dispositivo en la red interna por orden de llegada.
- Si todas las direcciones del grupo están en uso, un dispositivo debe esperar una dirección disponible antes de poder acceder a la red externa.



NAT dinámico

Configurar NAT dinámico

Hay cinco tareas para configurar las traducciones NAT estáticas.

- **Paso 1:** Defina el conjunto de direcciones que se utilizarán para la traducción con el comando **ip natpool**.
- **Paso 2 -** Configure una ACL estándar para identificar (permitir) solo aquellas direcciones que se traducirán.
- **Paso 3** - Enlazar la ACL al grupo, utilizando el comando ip nat inside source list.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

NAT dinámico

Configurar NAT dinámico

Hay cinco tareas para configurar las traducciones NAT estáticas.

- **Paso 4** - Identifique qué interfaces están dentro.
- **Paso 5** - Identifique qué interfaces están fuera.

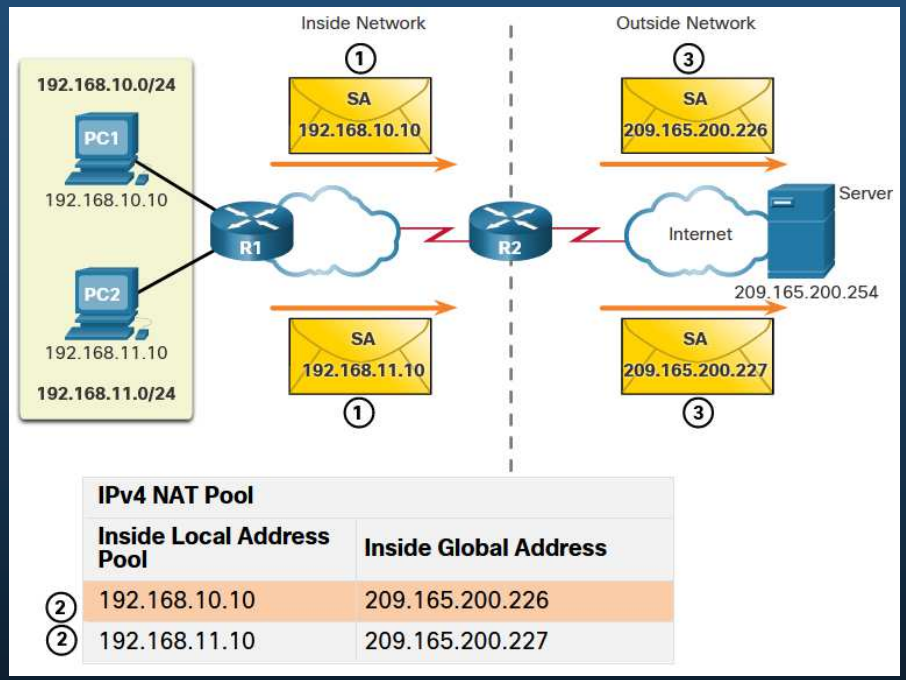
```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

NAT dinámico

Analizar NAT dinámico: interior a exterior

Proceso de traducción de NAT dinámica:

1. PC1 y PC2 envían paquetes solicitando una conexión al servidor.
2. R2 recibe el primer paquete de PC1, comprueba el ALC para determinar si el paquete debe traducirse, selecciona una dirección global disponible y crea una entrada de traducción en la tabla NAT.
3. El R2 reemplaza la dirección de origen local interna de la PC1, 192.168.10.10, por la dirección global interna traducida 209.165.200.226 y reenvía el paquete. (El mismo proceso ocurre para el paquete de PC2 usando la dirección traducida de 209.165.200.227.)



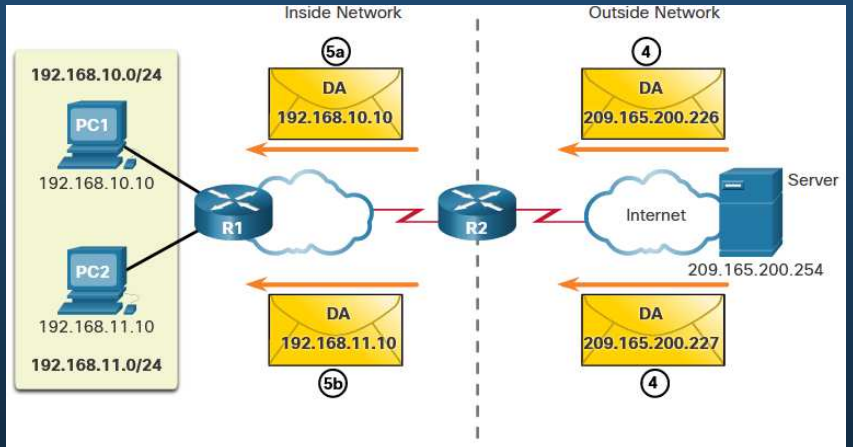
IPv4 NAT Pool	
Inside Local Address Pool	**Inside Global Address**
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227

NAT dinámico

Analizar NAT dinámico: de exterior a interior

Proceso de traducción de NAT dinámica:

4. El servidor recibe el paquete de PC1 y responde con la dirección de destino 209.165.200.226. El servidor recibe el paquete de PC2, responde utilizando la dirección de destino 209.165.200.227.
5. (a) Cuando R2 recibe el paquete con la dirección de destino 209.165.200.226; realiza una búsqueda de tabla NAT y traduce la dirección de vuelta a la dirección local interna y reenvía el paquete hacia PC1.
   (b) Cuando R2 recibe el paquete con la dirección de destino 209.165.200.227; realiza una búsqueda de tabla NAT y traduce la dirección de vuelta a la dirección local interior 192.168.11.10 y reenvía el paquete hacia PC2.



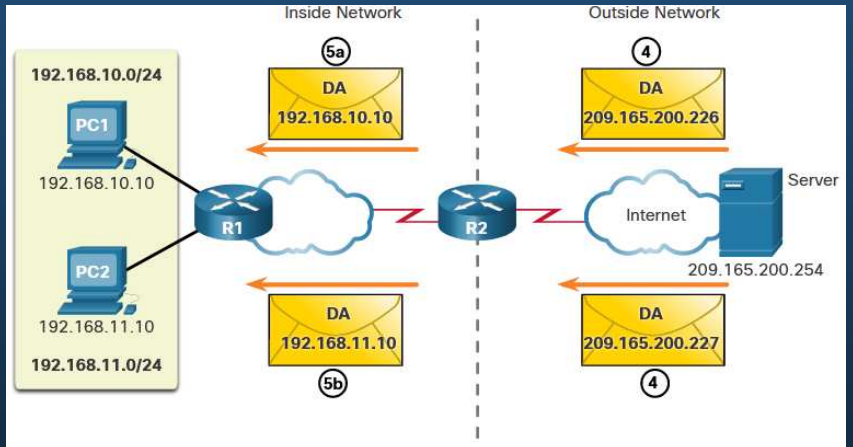
IPv4 NAT Pool		
	Inside Local Address Pool	Inside Global Address
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

NAT dinámico

Analizar NAT dinámico: de afuera hacia adentro

Proceso de traducción de NAT dinámica:

6. La PC1 y la PC2 reciben los paquetes y continúan la conversación. El router lleva a cabo los pasos 2 a 5 para cada paquete.



IPv4 NAT Pool		
	Inside Local Address Pool	Inside Global Address
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

NAT dinámico

Verificar NAT dinámico

La salida del comando **show ip nat translation** muestra todas las traducciones estáticas que se han configurado y cualquier traducción dinámica que haya sido creada por el tráfico.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.228 192.168.10.10 --- ---
— 209.165.200.229 192.168.11.10 — —
R2#
```

NAT dinámico

Verificar NAT dinámico

Si se agrega la palabra clave **verbose**, se muestra información adicional acerca de cada traducción, incluido el tiempo transcurrido desde que se creó y se utilizó la entrada.

```
R2# show ip nat translation verbose
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.228 192.168.10.10 — —
    create 00:02:11, use 00:02:11 tiempo de espera: 86400000, left 23:57:48, Map Id (In): 1,
    flags:
none, use_count: 0, entry-id: 10, lc_entries: 0
tcp 209.165.200.229 192.168.11.10 — —
    create 00:02:10, use 00:02:10 tiempo de espera: 86400000, left 23:57:49, Map Id (In): 1,
    flags:
none, use_count: 0, entry-id: 12, lc_entries: 0
R2#
```

NAT dinámico

Verificar NAT dinámico

De forma predeterminada, las entradas de traducción expiran después de 24 horas, a menos que los temporizadores se hayan reconfigurado con el comando **ip nat translation timeout** *timeout-seconds* en el modo de configuración global. Para borrar entradas dinámicas antes de se exceda el tiempo de espera, utilice el comando **clear ip nat translation** en modo EXEC con privilegios.

```
R2# clear ip nat translation *
R2# show ip nat translation
```

Comando	Descripción
clear ip nat translation *	Elimina todas las entradas de traducción dinámica de direcciones de la tabla de traducción NAT.
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Borra una entrada de traducción dinámica simple que contiene una traducción interna o ambas, traducción interna y externa.
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	Elimina una entrada de traducción dinámica extendida.

NAT dinámico

Verificar NAT dinámico

El comando **show ip nat statistics** muestra información sobre el número total de traducciones activas, los parámetros de configuración de NAT, el número de direcciones en el grupo y cuántas de las direcciones se han asignado.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 0 extended)
Peak translations: 4, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 47 Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 4
 pool NAT-POOL1: netmask 255.255.255.224
            inicio 209.165.200.226 fin 209.165.200.240
            type generic, total addresses 15, allocated 2 (13%), misses 0
(resultado omitido)
R2#
```

NAT dinámico

Verificar NAT dinámico

El comando **show running-config** muestra los comandos NAT, ACL, interface o pool con los valores requeridos.

```
R2# show running-config | include NAT
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
ip nat inside source list 1 pool NAT-POOL1
```

PAT

Configurar PAT para usar una única dirección IPv4

Para configurar PAT para que utilice una sola dirección IPv4, agregue la palabra clave **overload** al comando **ip nat inside source** .

En el ejemplo, todos los hosts de la red 192.168.0.0/16 (coincidencia ACL 1) que envían tráfico a través del router R2 a Internet se traducirán a la dirección IPv4 209.165.200.225 (dirección IPv4 de la interfaz S0 / 1/1). Los flujos de tráfico se identificarán mediante números de puerto en la tabla NAT porque la palabra clave de **overload** está configurada.

```
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2 (config) # interfaz serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2 (config) # interfaz Serial0/1/1
R2(config-if)# ip nat outside
```

PAT

Configurar PAT para usar un grupo de direcciones

Un ISP puede asignar más de una dirección IPv4 pública a una organización. En este escenario, la organización puede configurar PAT para utilizar un grupo de direcciones públicas IPv4 para la traducción.

Para configurar PAT para un grupo de direcciones NAT dinámico, simplemente agregue la palabra clave **overload** al comando **ip nat inside source** .

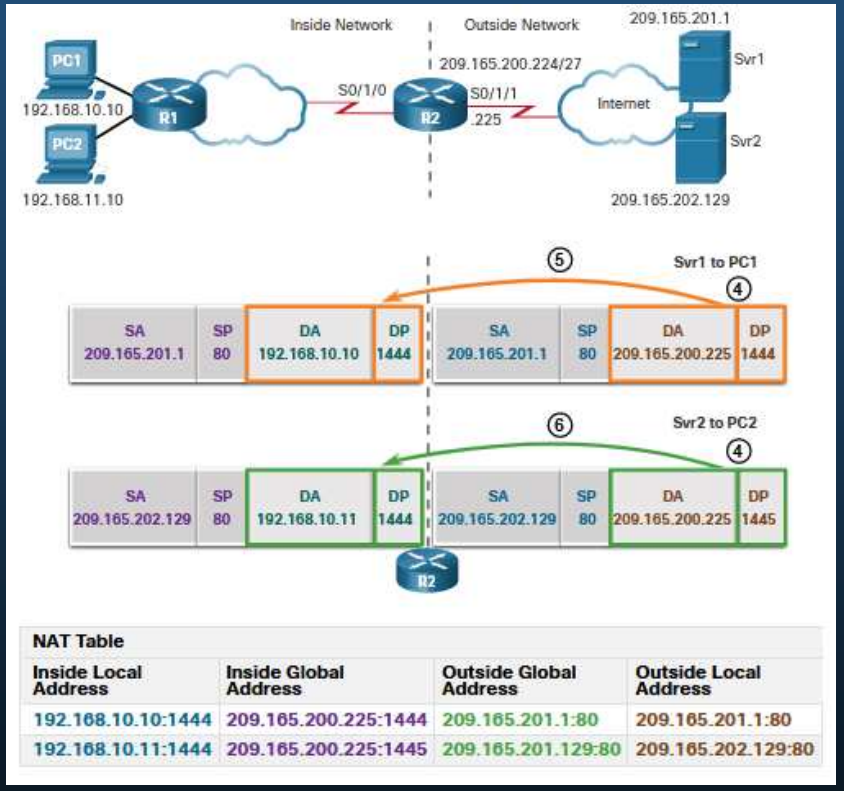
En el ejemplo, NAT-POOL2 está enlazado a una ACL para permitir la traducción de 192.168.0.0/16. Estos hosts pueden compartir una dirección IPv4 del grupo porque PAT está habilitado con la palabra clave **overload**.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2 (config-if) # interfaz serial0/1/0
R2(config-if)# ip nat outside
```

PAT

Analizar PAT - Servidor a PC

1. PC1 y PC2 envían paquetes a Svr1 y Svr2.
2. El paquete de la PC1 llega primero al R2. R2 modifica la dirección IPv4 de origen a 209.165.200.225 (dirección global interna). El paquete se reenvía a Svr1.
3. El paquete de la PC2 llega a R2. PAT cambia la dirección origen IPv4 de la PC2 a la dirección global interna 209.165.200.225. La PC2 tiene el mismo número de puerto de origen que la traducción para PC1. PAT aumenta el número de puerto de origen hasta que sea un valor único en su tabla. En este caso, 1445.



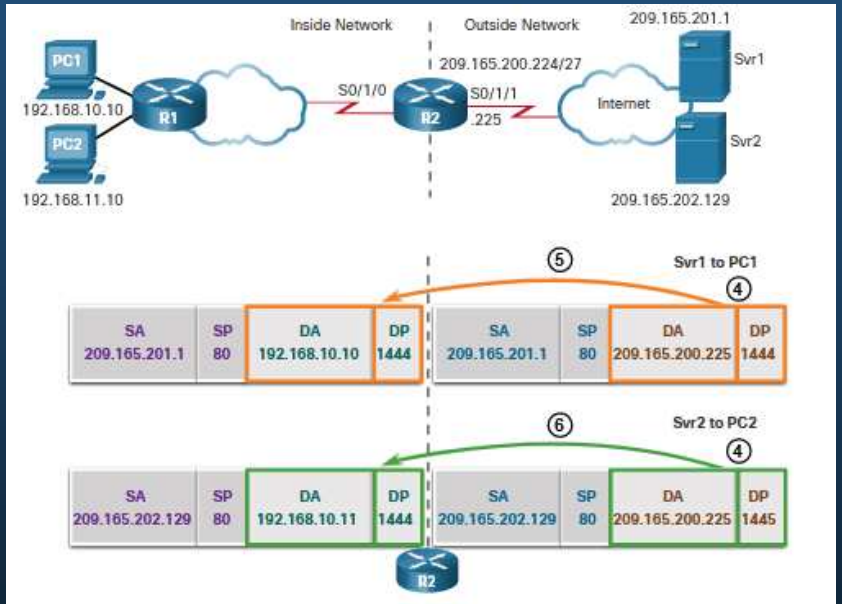
NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

PAT

Analizar PAT - Servidor a PC

1. PC1 y PC2 envían paquetes a Svr1 y Svr2.
2. El paquete de la PC1 llega primero al R2. R2 modifica la dirección IPv4 de origen a 209.165.200.225 (dirección global interna). El paquete se reenvía a Svr1.
3. El paquete de la PC2 llega a R2. PAT cambia la dirección origen IPv4 de la PC2 a la dirección global interna 209.165.200.225. La PC2 tiene el mismo número de puerto de origen que la traducción para PC1. PAT aumenta el número de puerto de origen hasta que sea un valor único en su tabla. En este caso, es 1445.



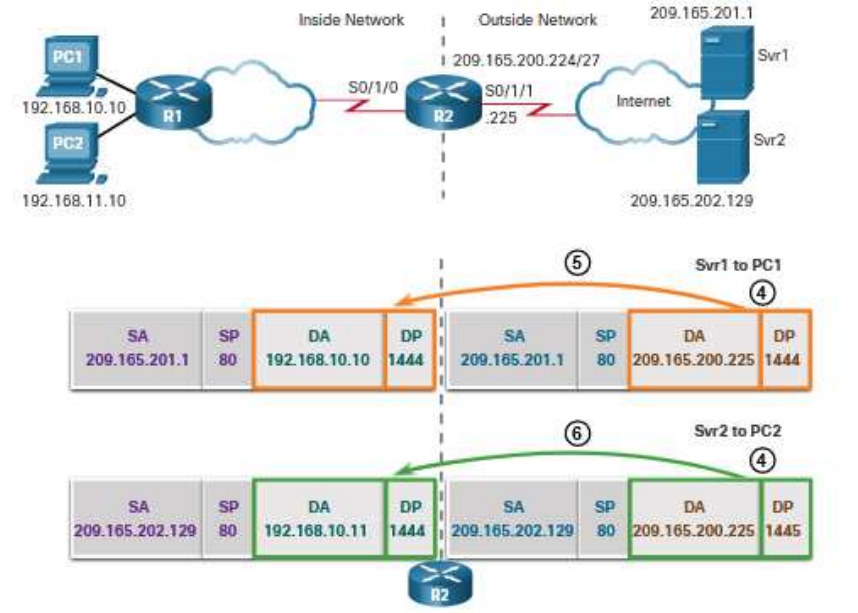
NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

PAT

Analizar PAT - Servidor a PC

1. Los servidores usan el puerto de origen del paquete recibido como puerto de destino y la dirección de origen como dirección de destino para el tráfico de retorno.
2. R2 cambia la dirección IPv4 de destino del paquete de Srv1 de 209.165.200.225 a 192.168.10.10 y reenvía el paquete hacia PC1.
3. R2 cambia la dirección de destino del paquete de Srv2. de 209.165.200.225 a 192.168.10.11. y modifica el puerto de destino a su valor original de 1444. Luego, el paquete se reenvía hacia la PC2.



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

PAT

Verificar PAT

Los mismos comandos utilizados para verificar NAT estático y dinámico se utilizan para verificar PAT. El comando **show ip nat translations** muestra las traducciones de dos hosts distintos a servidores web distintos. Observe que se asigna la misma dirección IPv4 209.165.200.226 (dirección global interna) a dos hosts internos distintos. Los números de puerto de origen en la tabla de NAT distinguen las dos transacciones.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200. 225:1444 192.168.10. 10:1444 209.165.201. 1:80 209.165.201. 1:80
tcp 209.165.200. 225:1445 192.168.11. 10:1444 209.165.202. 129:80 209.165.202. 129:80
R2#
```

PAT

Verificación PAT

El comando **show ip nat statistics** verifica que NAT-POOL2 haya asignado una única dirección para ambas traducciones. También se muestra la cantidad y el tipo de traducciones activas, los parámetros de configuración de NAT, la cantidad de direcciones en el grupo y cuántas se han asignado.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4 Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
 pool NAT-POOL2: netmask 255.255.255.224
           start 209.165.200.225 end 209.165.200.240
           type generic, total addresses 15, allocated 1 (6%), misses 0
(resultado omitido)
R2#
```

NAT64

¿NAT 64 para IPv6?

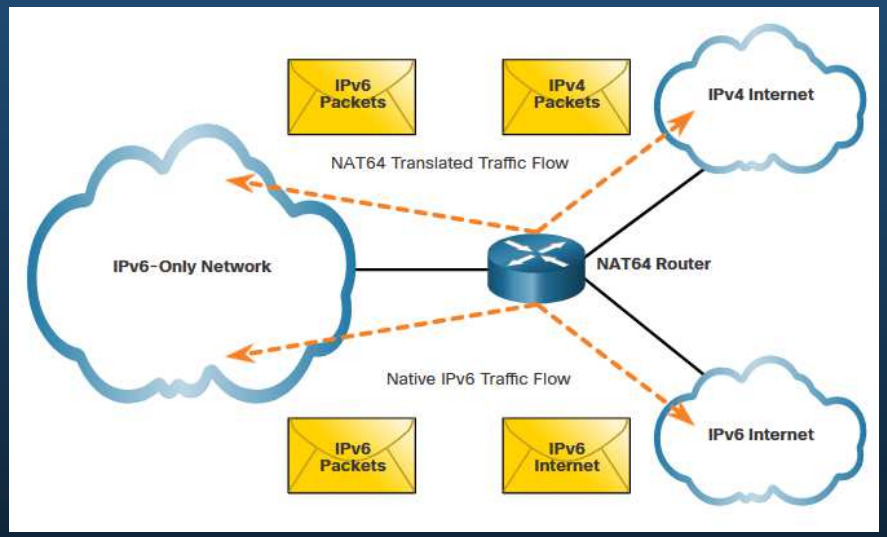
IPv6 se desarrolló con la intención de que la NAT para IPv4 con su traducción entre direcciones IPv4 públicas y privadas resulte innecesaria.

- Sin embargo, IPv6 sí incluye su propio espacio de direcciones privadas IPv6, direcciones locales únicas (ULA).
- Las direcciones IPv6 locales únicas (ULA) se asemejan a las direcciones privadas en IPv4 definidas en RFC 1918, pero con un propósito distinto.
- Las direcciones ULA están destinadas únicamente a las comunicaciones locales dentro de un sitio. Las direcciones ULA no están destinadas a proporcionar espacio de direcciones IPv6 adicional ni a proporcionar un nivel de seguridad.
- IPv6 proporciona la traducción de protocolos entre IPv4 e IPv6 conocida como NAT64.

NAT64

NAT64

- NAT para IPv6 se usa en un contexto muy distinto al de NAT para IPv4.
- Las variedades de NAT para IPv6 se utilizan para proporcionar acceso transparente entre redes de solo IPv6 e IPv4, como se muestra. No se utiliza como forma de traducción de IPv6 privada a IPv6 global.
- NAT para IPv6 no debe usarse como una estrategia a largo plazo, sino como un mecanismo temporal para ayudar en la migración de IPv4 a IPv6.



Capítulo 7

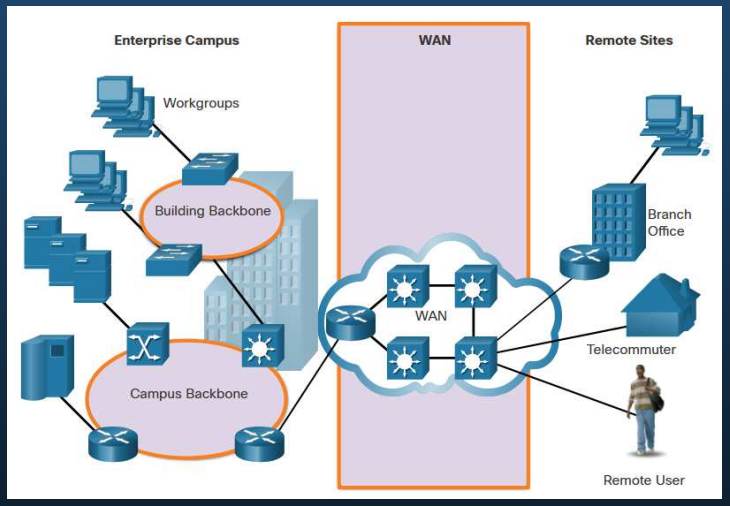
Conceptos de WLAN

Propósito de las WAN's

LANs y WANs

Una WAN es una red de telecomunicaciones que abarca un área geográfica relativamente grande y se requiere para conectarse más allá del límite de la LAN.

Redes de área local (LAN)	Redes de área extensa (WAN)
Las LAN proporcionan servicios de red dentro de un área geográfica pequeña.	Una red de proveedor de servicios puede cubrir grandes áreas geográficas.
Las LAN se utilizan para interconectar equipos locales, periféricos y otros dispositivos.	Las WAN se utilizan para interconectar usuarios, redes y sitios remotos.
Una LAN es propiedad de una organización o un usuario doméstico y la administra.	Las WAN son propiedad y administradas por proveedores de servicios de Internet, teléfono, cable y satélite.
Aparte de los costos de infraestructura de red, no hay tarifa por usar una LAN.	Los servicios WAN se proporcionan por un suplemento.
Las LAN proporcionan altas velocidades de ancho de banda mediante servicios Ethernet y Wi-Fi por cable.	Los proveedores de WAN ofrecen velocidades de ancho de banda bajas a altas, a largas distancias.



Propósito de las WAN's

Privadas y Públicas

Una WAN privada es una conexión dedicada a un único cliente.

Las WAN privadas proporcionan lo siguiente:

- Nivel de servicio garantizado
- Ancho de banda consistente
- Seguridad

Normalmente, un ISP o un proveedor de servicios de telecomunicaciones que utiliza Internet proporciona una conexión WAN pública. En este caso, los niveles de servicio y el ancho de banda pueden variar, y las conexiones compartidas no garantizan la seguridad.

Propósito de las WAN's

Topologías WAN

Las WAN se implementan utilizando los siguientes diseños de topología lógica:

- Topología punto a punto
- Topología de estrella (hub and spoke)
- Topología de doble conexión
- Topología de malla completa
- Topología parcialmente mallada

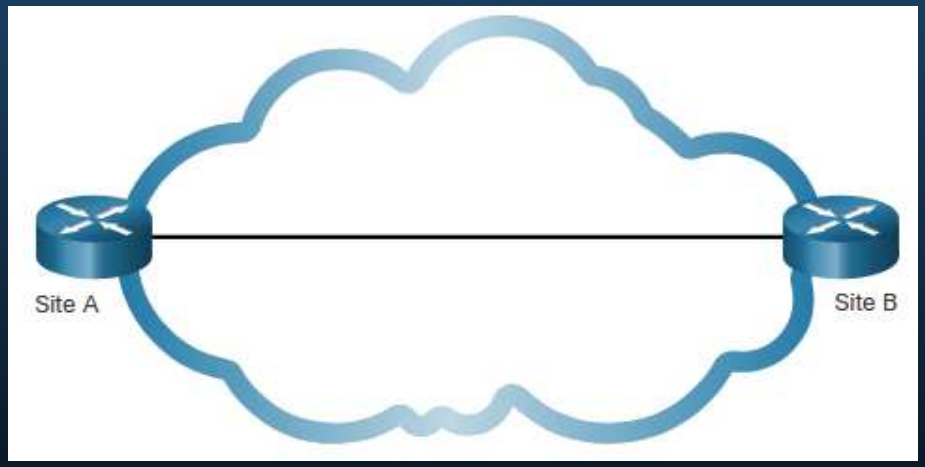
Nota: Las redes grandes suelen implementar una combinación de estas topologías.

Propósito de las WAN's

Topologías WAN

Topología punto a punto

- Emplea un circuito punto a punto entre dos terminales.
- Implica un servicio de transporte de capa 2 a través de la red del proveedor de servicios.
- La conexión punto a punto es transparente para la red del cliente.



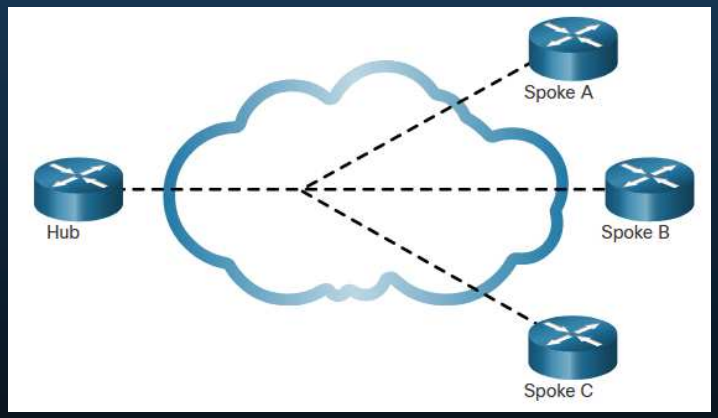
Nota: Puede resultar costoso si se requieren muchas conexiones punto a punto.

Propósito de las WAN's

Topologías WAN

Topología de estrella (hub and spoke)

- Permite que una sola interfaz al hub puede ser compartida por todos los circuitos de radio.
- Los sitios radiales se pueden interconectar a través del sitio de hub mediante circuitos virtuales y subinterfaces enrutadas del hub.
- Los routers radiales solo pueden comunicarse entre sí a través del router concentrador.



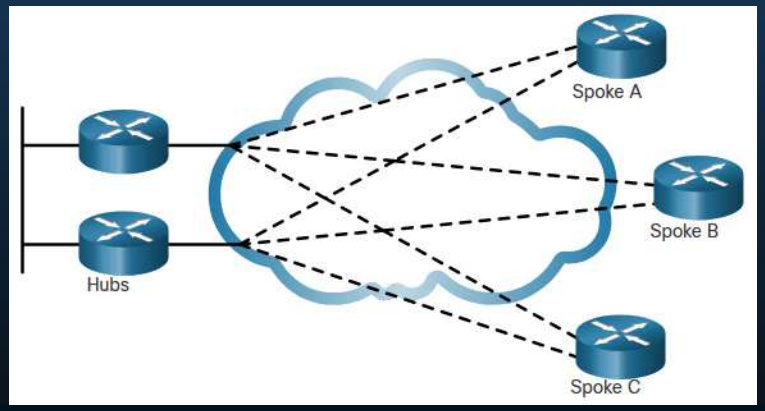
Nota: El router central (concentrador) representa un punto único de falla. Si falla, la comunicación entre radios también falla.

Propósito de las WAN's

Topologías WAN

Topología de doble conexión

- Ofrecen redundancia de red mejorada, equilibrio de carga, computación o procesamiento distribuido y la capacidad de implementar conexiones del proveedor de servicio de respaldo.
- Más caro de implementar que las topologías de un solo hogar. Esto es porque requieren hardware de red, como routers y switches adicionales.
- Además, son más difíciles de implementar porque requieren configuraciones adicionales y más complejas.

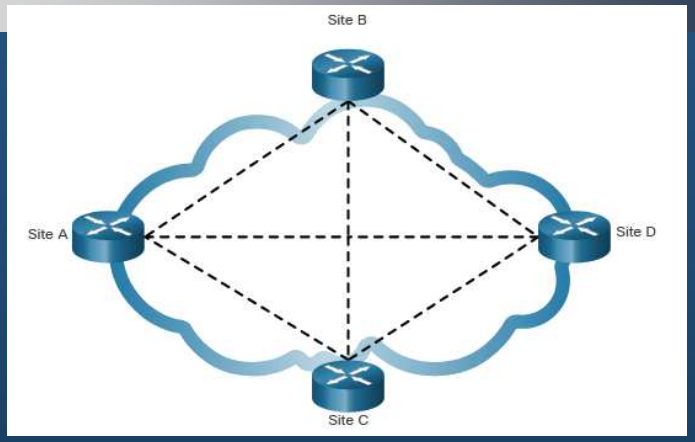


Propósito de las WAN's

Topologías WAN

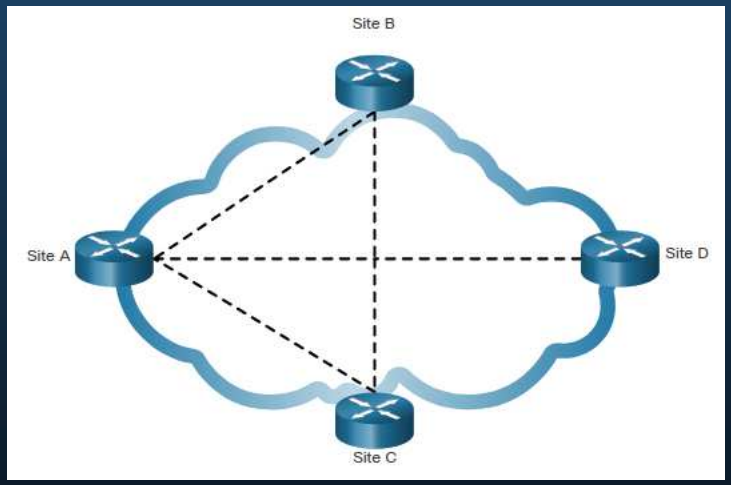
Topología de malla completa

- Utiliza múltiples circuitos virtuales para conectar todos los sitios
- La topología más tolerante a errores



Topología parcialmente mallada

- Conecta muchos sitios pero no todos



Propósito de las WAN's

Conexiones de operador

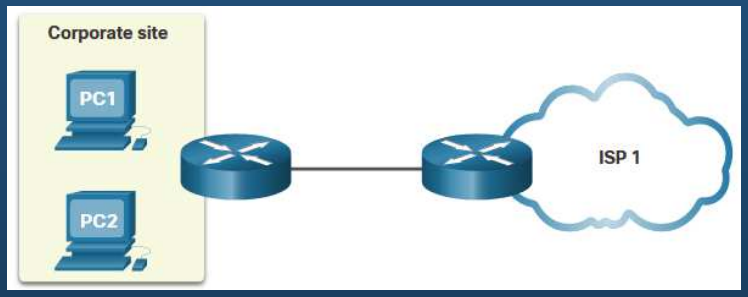
Otro aspecto del diseño WAN es cómo una organización se conecta a Internet. Por lo general, una organización firma un acuerdo de nivel de servicio (SLA) con un proveedor de servicios. El SLA describe los servicios esperados relacionados con la fiabilidad y disponibilidad de la conexión.

El proveedor de servicios puede o no ser el transportista real. Un transportista posee y mantiene la conexión física y el equipo entre el proveedor y el cliente. Normalmente, una organización elegirá una conexión WAN de un solo operador o de dos portadoras.

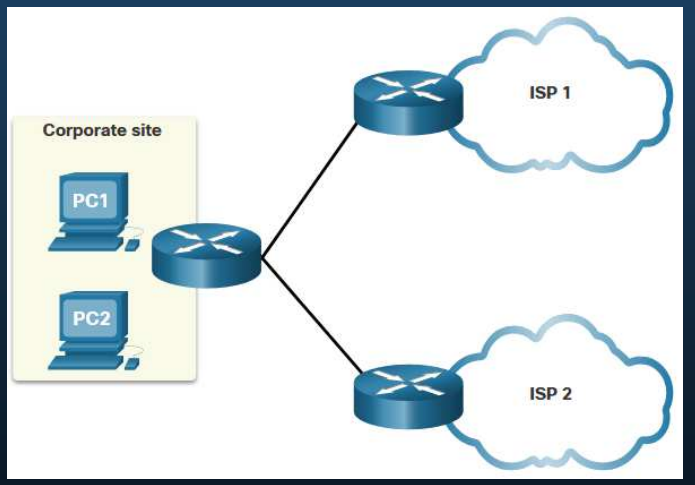
Propósito de las WAN's

Conexiones de operador

Una conexión de operador único es cuando una organización se conecta a un único proveedor de servicios. Un SLA se negocia entre la organización y el proveedor de servicios.



Una conexión de doble operador proporciona redundancia y aumenta la disponibilidad de la red. La organización negocia acuerdos de nivel de servicio independientes con dos proveedores de servicios diferentes.



Propósito de las WAN's

Evolución de las redes

Los requisitos de red de una empresa pueden cambiar significativamente a medida que la empresa crece con el tiempo.

- Una red no solo debe satisfacer las necesidades operativas diarias de la empresa, sino que debe ser capaz de adaptarse y crecer a medida que la empresa cambia.
- Los diseñadores de redes y los administradores pueden abordar estos desafíos eligiendo cuidadosamente las tecnologías de red, los protocolos y los proveedores de servicios.
- Las redes se pueden optimizar mediante el uso de una variedad de técnicas y arquitecturas de diseño de red.

Para ilustrar las diferencias entre el tamaño de la red, utilizaremos una empresa ficticia llamada SPAN Engineering a medida que crece de un pequeño negocio local a una empresa global.

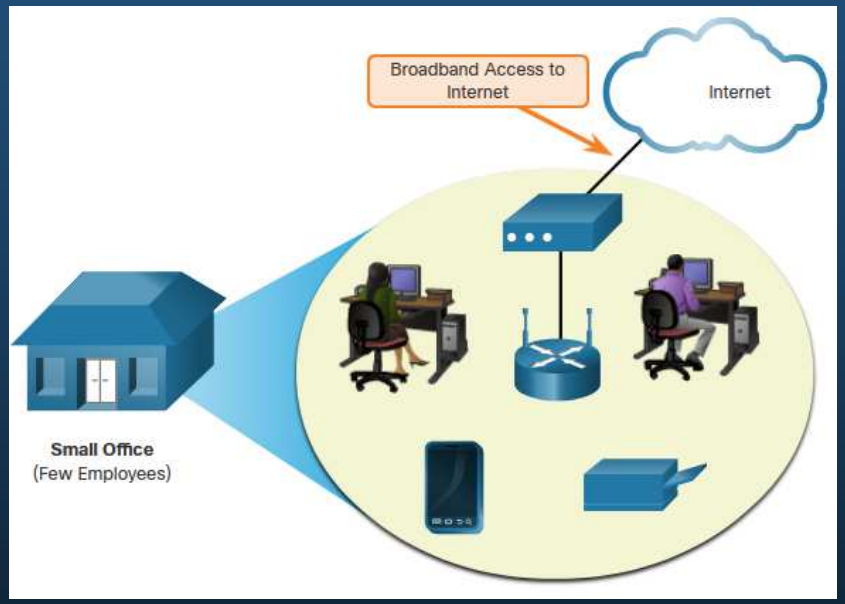
Propósito de las WAN's

Evolución de las redes

Redes pequeñas

SPAN, una pequeña empresa ficticia, comenzó con unos pocos empleados en una pequeña oficina.

- Utiliza una única LAN conectada a un router inalámbrico para compartir datos y periféricos.
- La conexión a Internet se realiza a través de un servicio de banda ancha común denominado línea de suscriptor digital (DSL.
- El soporte de TI se contrata con el proveedor de DSL.



Propósito de las WAN's

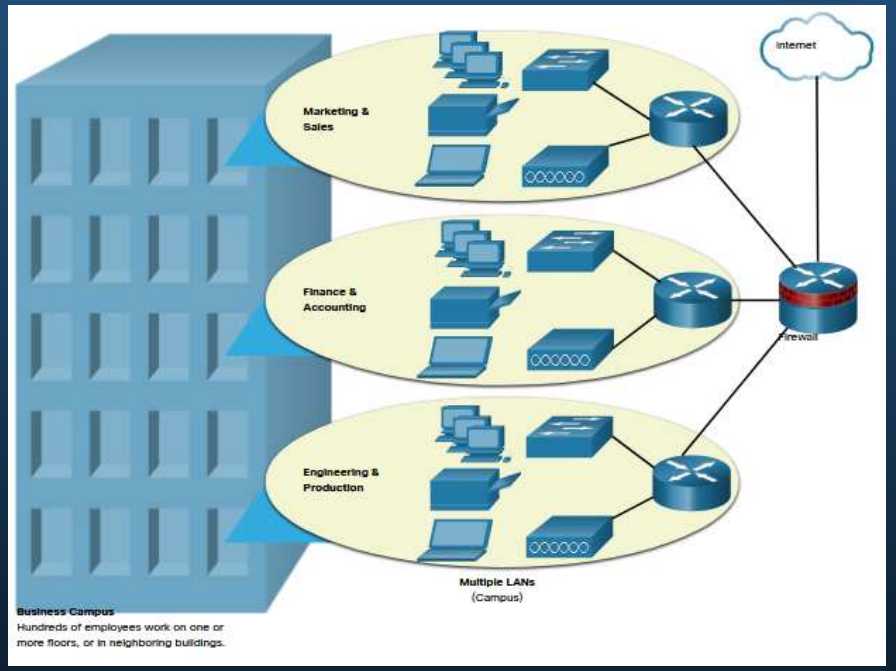
Evolución de las redes

Red de campus

Dentro de unos años SPAN creció y requirió varios pisos de un edificio.

La empresa necesitaba ahora una red de área de campus (CAN).

- Un firewall asegura el acceso a Internet a los usuarios corporativos.
- La empresa cuenta con personal interno de TI para dar soporte y mantenimiento a la red.

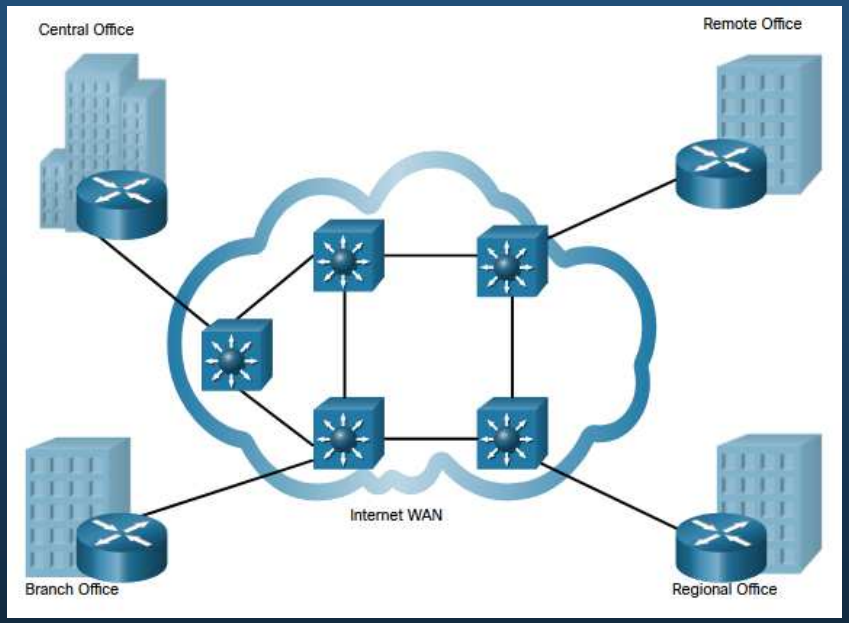


Propósito de las WAN's

Evolución de las redes

Red de la sucursal

- Unos años más tarde, la compañía se expandió y agregó una sucursal en la ciudad, y sitios remotos y regionales en otras ciudades.
- La compañía necesitaba ahora una red de área metropolitana (MAN) para interconectar sitios dentro de la ciudad.
- Para conectarse con la oficina central las sucursales que están en ciudades usan líneas privadas dedicadas a través de su proveedor de servicios local.



Propósito de las WAN's

Evolución de las redes

Red distribuida

- SPAN Ingeniería tiene 20 años de operación y cuenta con miles de empleados distribuidos en oficinas en todo el mundo.
- Las redes privadas virtuales (VPN) de sitio a sitio y de acceso remoto permiten que la empresa use Internet para conectarse de manera fácil y segura con los empleados y las instalaciones en todo el mundo.

Funcionamiento de WAN

Estándares WAN

Varias autoridades reconocidas definen y administran los estándares de acceso WAN:

- **TIA/EIA** - Asociación de la Industria de Telecomunicaciones y Alianza de Industrias Electrónicas
- **ISO** - Organización Internacional de Estandarización.
- **IEEE** - Instituto de Ingenieros en Electricidad y Electrónica

Funcionamiento de WAN

WAN en el modelo OSI

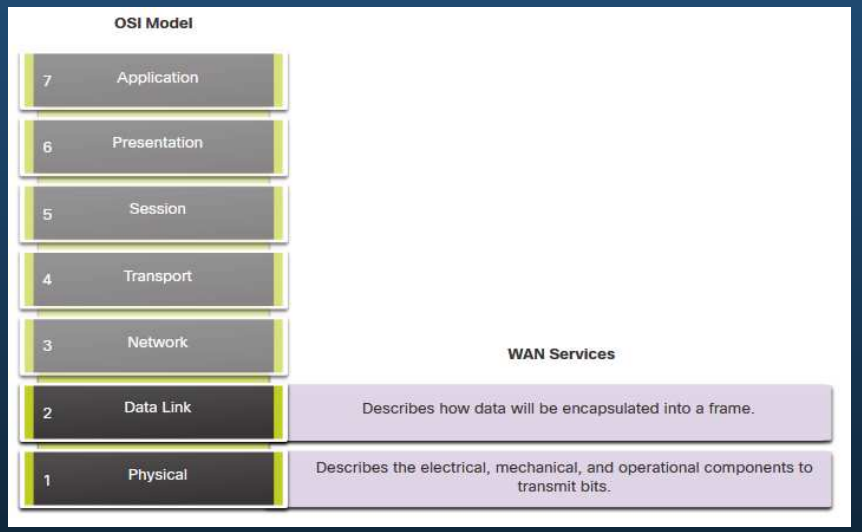
La mayoría de los estándares WAN se centran en la capa física y la capa de enlace de datos.

Protocolos de capa 1

- Jerarquía digital sincrónica (SDH, Synchronous Digital Hierarchy)
- Red óptica síncrona (SONET)
- Multiplexado por división de longitud de onda densa (DWDM)

Protocolos de capa 2

- Banda ancha (es decir, DSL y cable)
- Conexión inalámbrica
- WAN Ethernet (Metro Ethernet)
- Switching por etiquetas multiprotocolo (MPLS)
- Protocolo punto a punto (PPP) (menos usado).
- Control de enlace de datos de alto nivel (HDLC, High-Level Data Link Control)(menos usado).
- Frame Relay (heredado)
- Modo de transferencia asíncrona (ATM, asynchronous transfer mode)

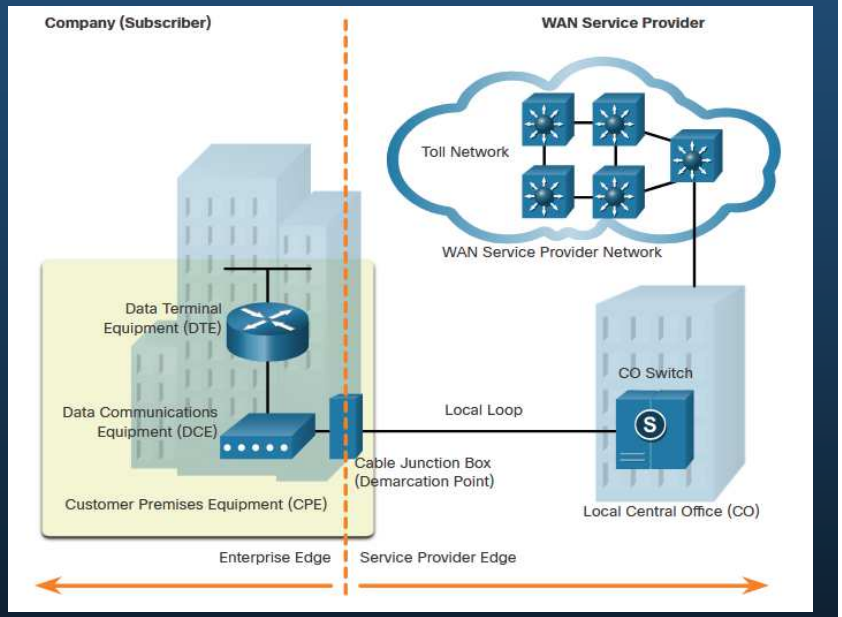


Funcionamiento de WAN

Terminología común WAN

Existen términos específicos utilizados para describir las conexiones WAN entre el suscriptor (es decir, la empresa/cliente) y el proveedor de servicios WAN.

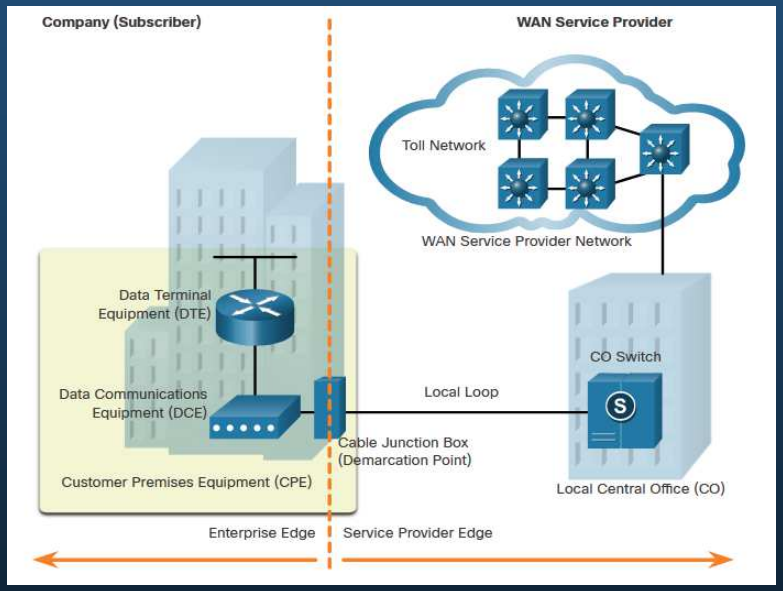
Término relacionado con WAN	Descripción
Equipo terminal de datos (DTE)	Conecta las LAN del suscriptor al dispositivo de comunicación WAN
Equipo de comunicación de datos (DCE)	Dispositivo utilizado para comunicarse con el proveedor
Equipo de las instalaciones del cliente (CPE)	Se trata de los dispositivos DTE y DCE ubicados en el perímetro empresarial
Punto de presencia (POP)	Este punto en que el suscriptor se conecta a la red de los proveedores de servicios
Punto de demarcación	La ubicación física en un edificio o complejo que separa oficialmente el CPE del equipo del proveedor de servicios.



Funcionamiento de WAN

Terminología común WAN

Término relacionado con WAN	Descripción
Loop local (última milla)	Cable de cobre o fibra propiamente dicho que conecta el CPE a la CO del proveedor de servicios.
Oficina central (CO)	Oficina centraL: Instalación o edificio del proveedor de servicios local que conecta el CPE a la red del proveedor.
Red con cargo	Red interurbana: consta de líneas de comunicación y otros equipos digitales, de largo alcance y de fibra óptica dentro de la red del proveedor de servicios WAN.
Red de backhaul	conectan varios nodos de acceso de la red del proveedor de servicios.
Red troncal	Redes grandes y de alta capacidad utilizadas para interconectar redes de proveedores de servicios y crear una red redundante.

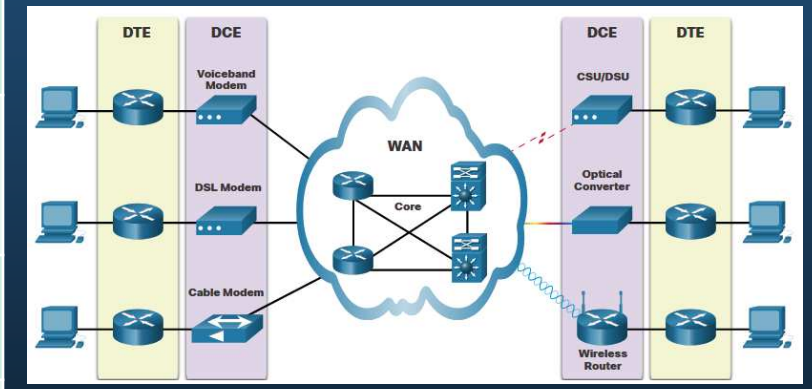


Funcionamiento de WAN

Dispositivos WAN

Existen muchos tipos de dispositivos que son específicos de los entornos WAN:

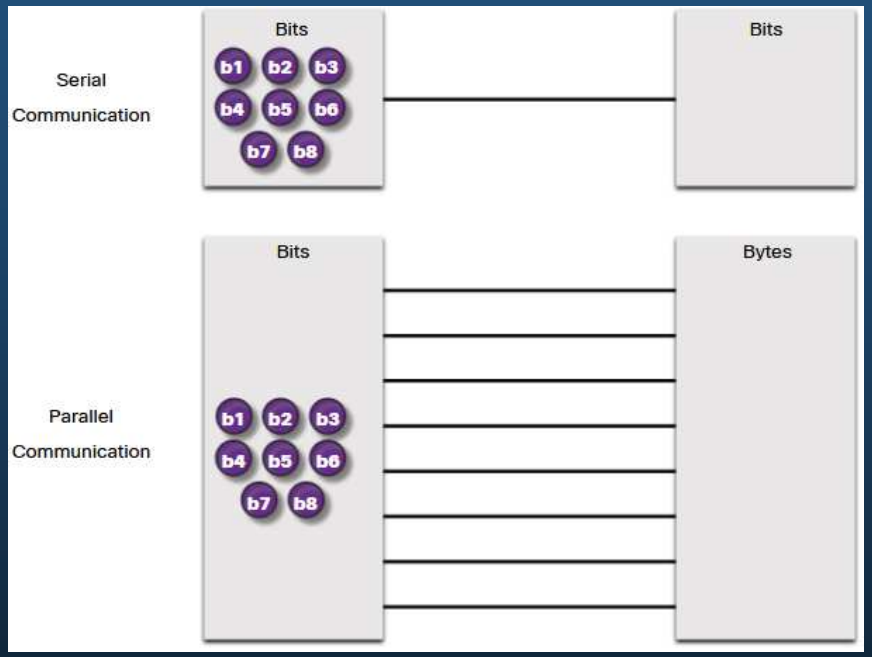
Dispositivos WAN	Descripción
Módem de banda de voz	Módem de acceso telefónico: utiliza líneas telefónicas Dispositivo heredado
Módem DSL/Módem por cable	Conocidos colectivamente como módems de banda ancha, estos módems digitales de alta velocidad se conectan al router DTE mediante Ethernet.
CSU/DSU	Las líneas arrendadas digitales requieren una CSU y una DSU. Conecta un dispositivo digital a una línea digital.
Convertidor óptico	Conecte medios de fibra óptica a medios de cobre y convierta señales ópticas a impulsos electrónicos.
El enrutador inalámbrico/punto de acceso	Los dispositivos se utilizan para conectarse de forma inalámbrica a un proveedor WAN.
Dispositivos WAN	La red troncal WAN consta de múltiples routers de alta velocidad y switches de nivel 3.



Funcionamiento de WAN

Comunicación en serie

- Casi todas las comunicaciones de red se producen mediante una entrega de comunicaciones en serie. La comunicación serial transmite los bits secuencialmente a través de un solo canal.
- Por el contrario, las comunicaciones paralelas transmiten simultáneamente varios bits utilizando varios cables.
- A medida que aumenta la longitud del cable, la sincronización entre varios canales se vuelve más sensible a la distancia. Por esta razón, la comunicación paralela se limita a distancias muy cortas

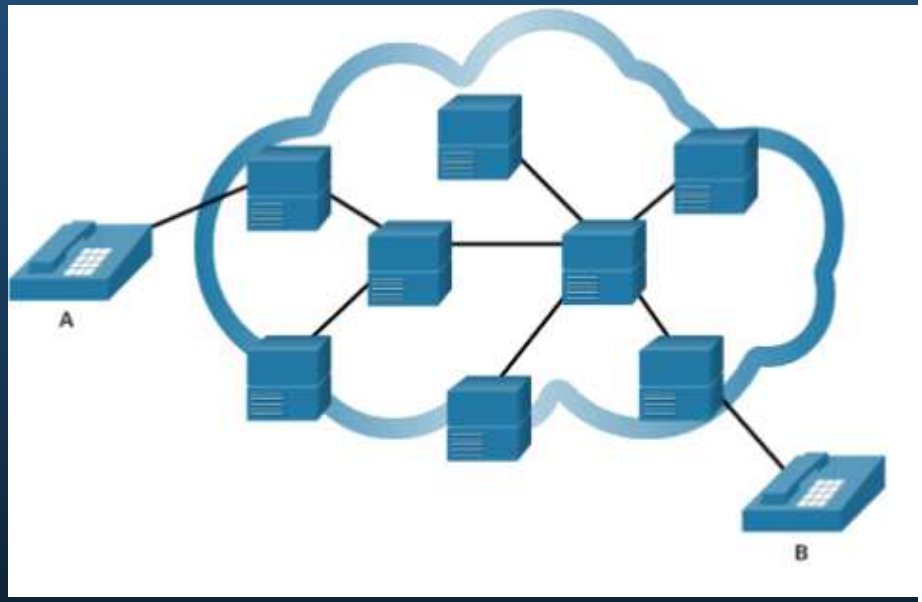


Funcionamiento de WAN

Comunicación Conmutada por Circuito

Las red de conmutación de circuitos son aquellas que establecen un circuito (o canal) dedicado entre los nodos y las terminales antes de que los usuarios se puedan comunicar.

- La tecnología ATM requiere el establecimiento de una conexión a través de una red de proveedor de servicios antes de que se pueda iniciar la comunicación.
- Todas las comunicaciones usan la misma ruta.
- Los dos tipos más comunes de tecnologías WAN de conmutación de circuitos son la red pública de telefonía de conmutación (PSTN) y la red digital de servicios integrados (ISDN).

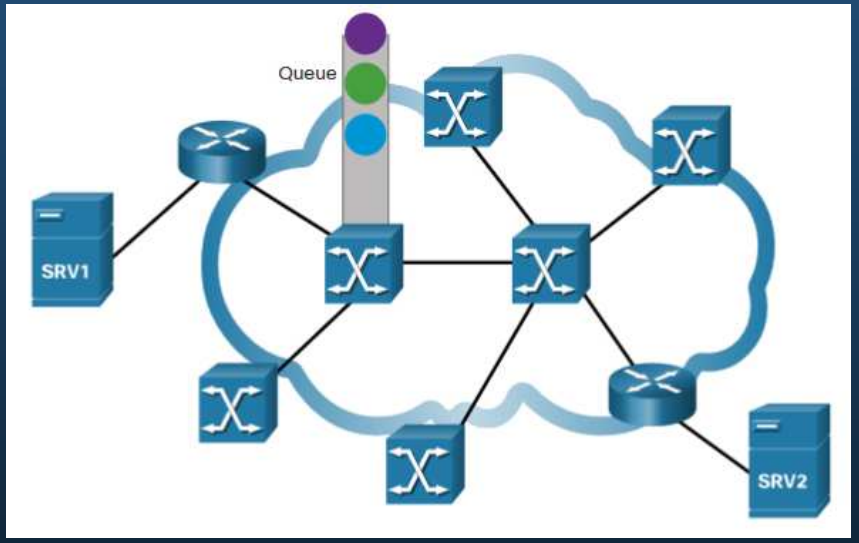


Funcionamiento de WAN

Comunicación Conmutada por Paquetes

La comunicación de red se implementa con mayor frecuencia mediante la comunicación conmutada por paquetes.

- La conmutación por paquetes divide el tráfico en paquetes que se enrutan a través de una red compartida.
- Mucho menos costoso y más flexible que la conmutación de circuitos.
- Los tipos comunes de tecnologías WAN conmutadas por paquetes son:
  - WAN Ethernet (Metro Ethernet),
  - Switching por Etiquetas MItiprotocolo (MPLS)
  - Frame Relay
  - Asynchronous Transfer Mode (ATM).



Funcionamiento de WAN

SDH, SONET y DWDM

Las redes de proveedores de servicios utilizan infraestructuras de fibra óptica para transportar datos de usuarios entre destinos. El cable de fibra óptica es muy superior al cable de cobre para transmisiones de larga distancia debido a su atenuación e interferencia mucho menor.

Hay dos estándares OSI capa 1 de fibra óptica disponibles para los proveedores de servicios:

- **SDH** - Synchronous Digital Hierarchy (SDH) es un estándar global para el transporte de datos a través de cable de fibra óptica.
- **SONET** - Red óptica síncrona (SONET) es el estándar norteamericano que ofrece los mismos servicios que SDH.

SDH/SONET definen cómo transferir múltiples comunicaciones de datos, voz y video a través de fibra óptica mediante láseres o diodos emisores de luz (LED) por grandes distancias.

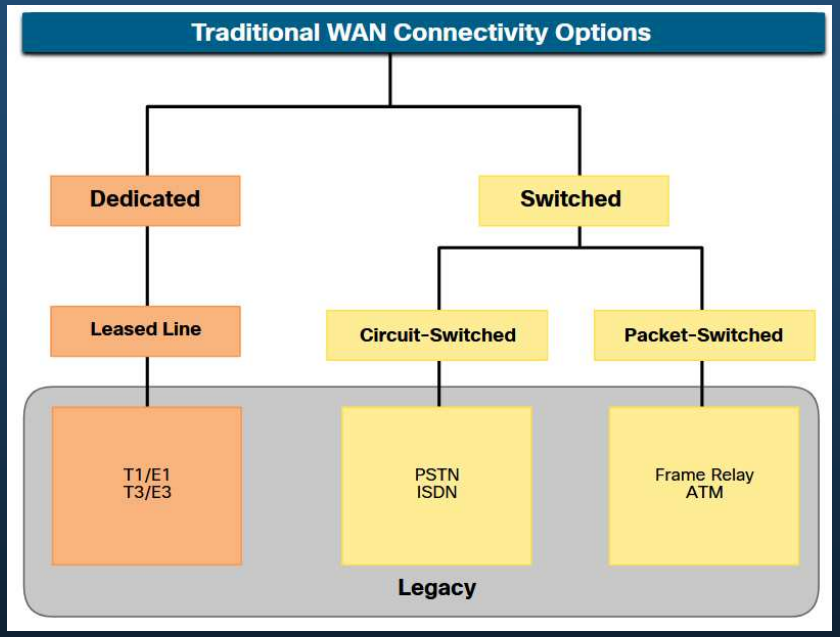
La multiplexación por división de longitud de onda densa (DWDM) es una tecnología más reciente que aumenta la capacidad de transmisión de datos de SDH y SONET al enviar simultáneamente múltiples flujos de datos (multiplexación) utilizando diferentes longitudes de onda de luz.

Conectividad de la WAN tradicional

Opciones de conectividad WAN tradicionales

Para entender las WAN de hoy, ayuda saber por dónde comenzaron.

- Cuando las LAN aparecieron en la década de 1980, las organizaciones comenzaron a ver la necesidad de interconectarse con otras ubicaciones.
- Para ello, necesitaban sus redes para conectarse al bucle local de un proveedor de servicios.
- Esto se logró mediante el uso de líneas dedicadas o mediante el uso de servicios conmutados de un proveedor de servicios.



Conectividad de la WAN tradicional

Terminología WAN común

Por lo general, un proveedor de servicios arrienda las líneas punto a punto, que se llaman “líneas arrendadas”. El término "línea arrendada" hace referencia al hecho de que la organización paga una tarifa mensual de arrendamiento a un proveedor de servicios para usar la línea.

- Hay líneas arrendadas disponibles de distintas capacidades y, por lo general, su precio depende del ancho de banda necesario y de la distancia entre los dos puntos conectados.
- Hay dos sistemas utilizados para definir la capacidad digital de un enlace serie de medios de cobre:
  - **T-carrier** - Utilizado en América del Norte, T-carrier proporciona enlaces T1 que admiten ancho de banda de hasta 1.544 Mbps y enlaces T3 que soportan ancho de banda de hasta 43,7 Mbps.
  - **E-carrier** — Utilizado en Europa, e-carrier proporciona enlaces E1 que admiten ancho de banda de hasta 2.048 Mbps y enlaces E3 que admiten ancho de banda de hasta 34.368 Mbps.

Conectividad de la WAN tradicional

Terminología WAN común

En esta tabla se resumen las ventajas y desventajas delas lineas arrendadas.

Ventajas	
Simplicidad	Los enlaces de comunicación punto a punto requieren conocimientos mínimos de instalación y mantenimiento.
Calidad	Los enlaces de comunicación punto a punto generalmente ofrecen una alta calidad de servicio si tienen un ancho de banda adecuado.
Disponibilidad	La disponibilidad constante es esencial para algunas aplicaciones, como el comercio electrónico. Los enlaces de comunicación punto a punto proporcionan la capacidad dedicada permanente que se necesita para VoIP o para video sobre IP.

Desventajas	
Costo	Los enlaces punto a punto son el tipo de acceso WAN más costoso. Cuando se usan para conectar varios sitios a través de distancias cada vez mayores, el costo de las soluciones de línea arrendada puede ser significativo.
Flexibilidad limitada	El tráfico WAN suele ser variable, y las líneas arrendadas tienen una capacidad fija, de modo que el ancho de banda de la línea rara vez coincide con la necesidad de manera precisa.

Conectividad de la WAN tradicional

Opciones de conexiones conmutadas por circuitos

Las conexiones conmutadas por circuitos son proporcionadas por los operadores de la Red Telefónica de Servicio Público (PSTN). El bucle local que conecta el CPE al CO es un medio de cobre.

Hay dos opciones tradicionales de conmutación de circuito:

Conexiones para la Red de telefonía de servicio público (PSTN)

- El acceso a la WAN de acceso telefónico utiliza la RTC como su conexión WAN. Los bucles locales tradicionales pueden transportar datos informáticos binarios a través de la red telefónica de voz mediante un módem.
- Las características físicas del bucle local y su conexión a la PSTN limitan la velocidad de señal a menos de 56 kbps.

Red digital de servicios integrados (ISDN)

- ISDN es una tecnología de conmutación de circuitos que permite al bucle local PSTN transportar señales digitales. Esto proporcionó conexiones conmutadas de mayor capacidad que el acceso telefónico. ISDN proporciona velocidades de datos de 45 Kbps a 2.048 Mbps.

Conectividad de la WAN tradicional

Opciones de conmutación por paquetes

La conmutación por paquetes divide el tráfico en paquetes que se enrutan a través de una red compartida. Permite que muchos pares de nodos se comuniquen a través del mismo canal.

Hay dos opciones tradicionales (heredadas) de conmutación de circuitos:

Frame Relay

- La retransmisión de tramas (Frame Relay) es una tecnología WAN multiacceso sin difusión (NBMA) simple de capa 2 que se utiliza para interconectar las redes LAN de una empresa.
- Frame Relay crea PVC que se identifican únicamente por un identificador de conexión de enlace de datos (DLCI).

Modo de Transferencia Asíncrona (ATM, asynchronous transfer mode)

- La tecnología del Modo de Transferencia Asíncrona (ATM) puede transferir voz, video y datos a través de redes privadas y públicas.
- ATM construye sobre una arquitectura basada en celdas, en vez de una arquitectura basada en tramas. Las celdas ATM tienen siempre una longitud fija de 53 bytes.

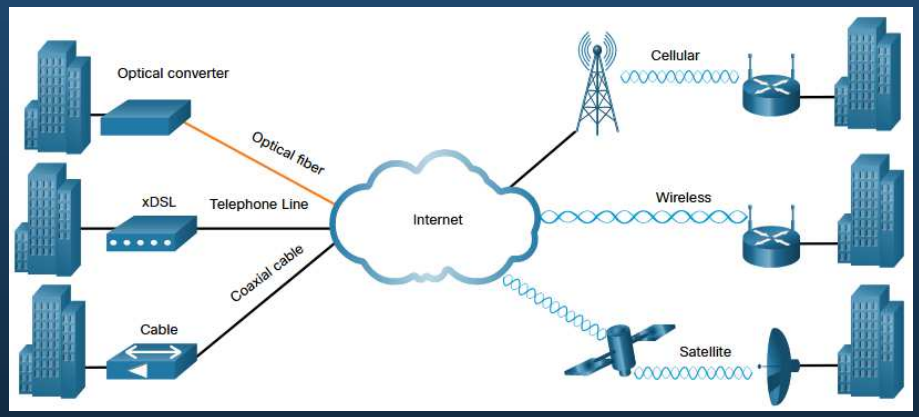
Nota: Las redes de Frame Relay y ATM han sido reemplazadas en gran medida por soluciones Metro Ethernet más rápidas y basadas en Internet.

Conectividad WAN moderna

WAN Modernas

Las WANS modernas tienen más opciones de conectividad que los WAN tradicionales.

- Las empresas ahora requieren opciones de conectividad WAN más rápidas y flexibles.
- Las opciones de conectividad WAN tradicionales han disminuido rápidamente en uso porque ya no están disponibles, son demasiado caras o tienen un ancho de banda limitado.



La figura muestra las conexiones de bucle local más probable que se encuentran hoy en día.

Conectividad WAN moderna

Opciones de conectividad WAN modernas

Las nuevas tecnologías están surgiendo continuamente. La figura resume las opciones modernas de conectividad WAN.

Banda ancha dedicada

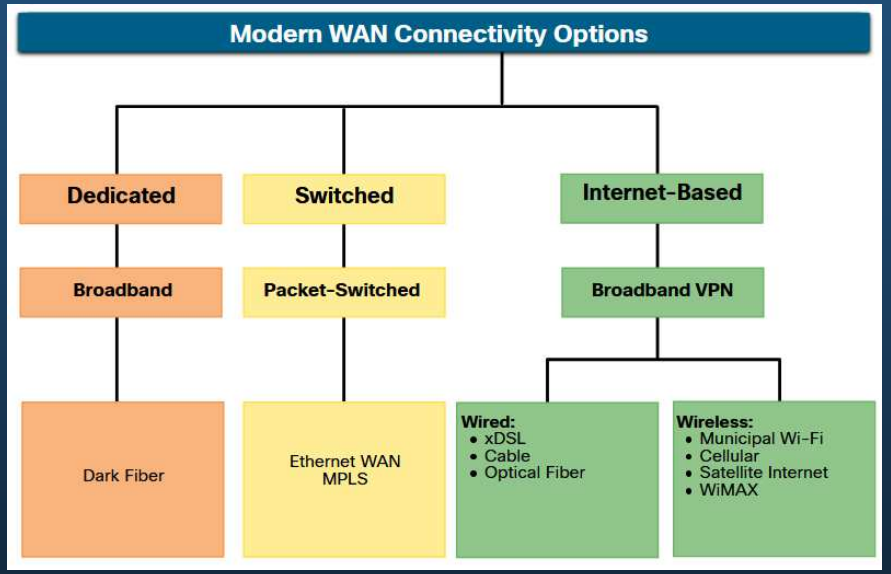
- Una organización puede instalar fibra de forma independiente para conectar ubicaciones remotas directamente entre sí.
- La fibra oscura se puede alquilar o comprar a un proveedor.

Conmutada por paquetes

- Metro Ethernet — Reemplazar muchas opciones WAN tradicionales.
- MPLS: permite que los sitios se conecten al proveedor independientemente de sus tecnologías de acceso.

Banda ancha basada en Internet

- Actualmente, las organizaciones utilizan habitualmente la infraestructura global de Internet para la conectividad WAN.



Conectividad WAN moderna

Ethernet WAN

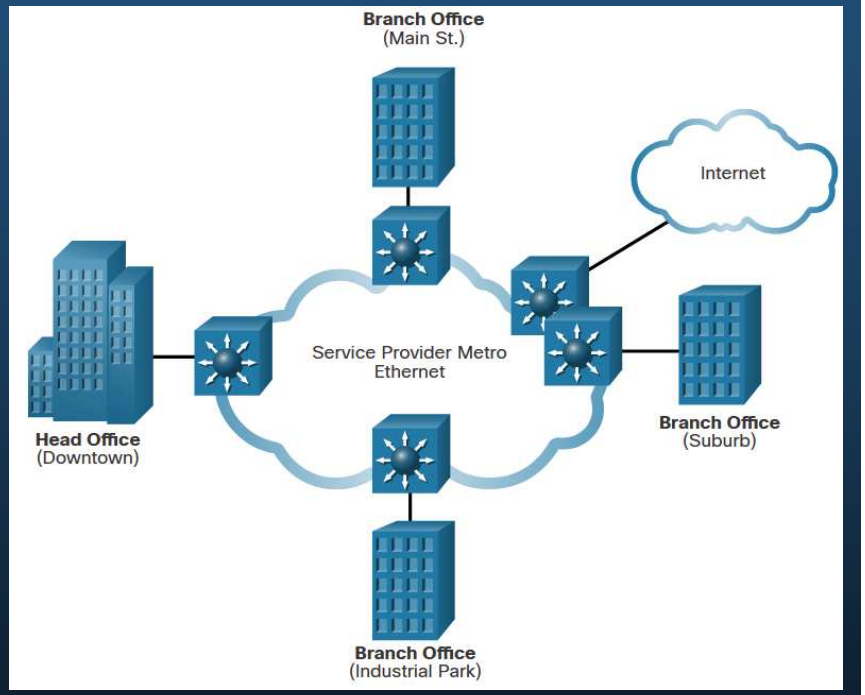
Los proveedores de servicios ahora ofrecen servicio WAN Ethernet con cableado de fibra óptica.

El servicio WAN Ethernet puede ir por muchos nombres, incluidos los siguientes:

- **Ethernet metropolitana (MetroE)**
- **Ethernet sobre MPLS**
- **Servicio de LAN privada virtual (VPLS)**

Existen varios beneficios de una WAN Ethernet:

- **Gastos y administración reducidos.**
- **Fácil integración con las redes existentes.**
- **Mejoramiento de la productividad de la empresa.**



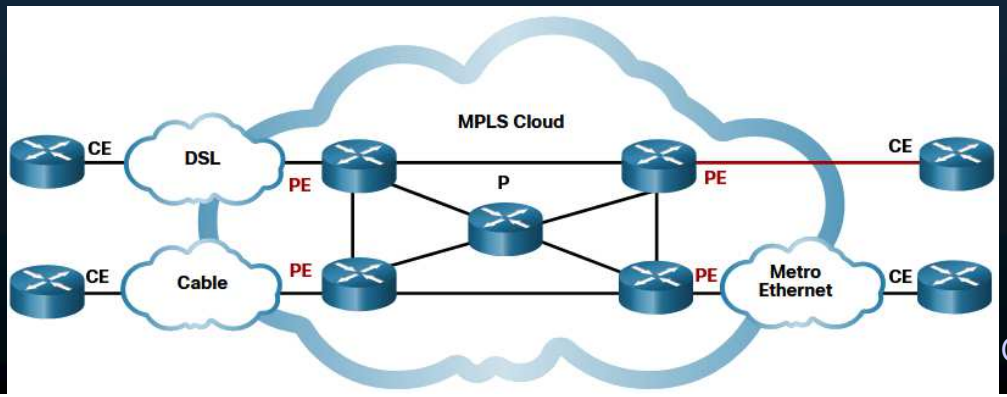
Nota:las WAN Ethernet ganaron popularidad y ahora se usan comúnmente para reemplazar los tradicionales enlaces de Frame Relay y WAN ATM..

Conectividad WAN moderna

MPLS

Multiprotocol Label Switching (MPLS) es una tecnología de enrutamiento WAN de proveedor de servicios de alto rendimiento para interconectar clientes sin tener en cuenta el método de acceso o la carga útil.

- MPLS soporta una variedad de métodos de acceso de cliente (por ejemplo, Ethernet, DSL, Cable, Frame Relay).
- MPLS puede encapsular todos los tipos de protocolos, incluido el tráfico IPv4 e IPv6.
- Un router MPLS puede ser un router de borde de cliente (CE), un router de borde de proveedor (PE) o un router de proveedor interno (P).
- Los routers MPLS también se denominan routers conmutados por etiquetas (LSR). Adjuntan etiquetas a paquetes que luego son utilizados por otros routers MPLS para reenviar tráfico.
- MPLS también proporciona servicios para soporte QoS, ingeniería de tráfico, redundancia y VPNs.



7.5 Conectividad basada en Internet

Conectividad basada en Internet

Opciones de conectividad basada en Internet

La conectividad de banda ancha basada en Internet es una alternativa al uso de opciones WAN dedicadas.

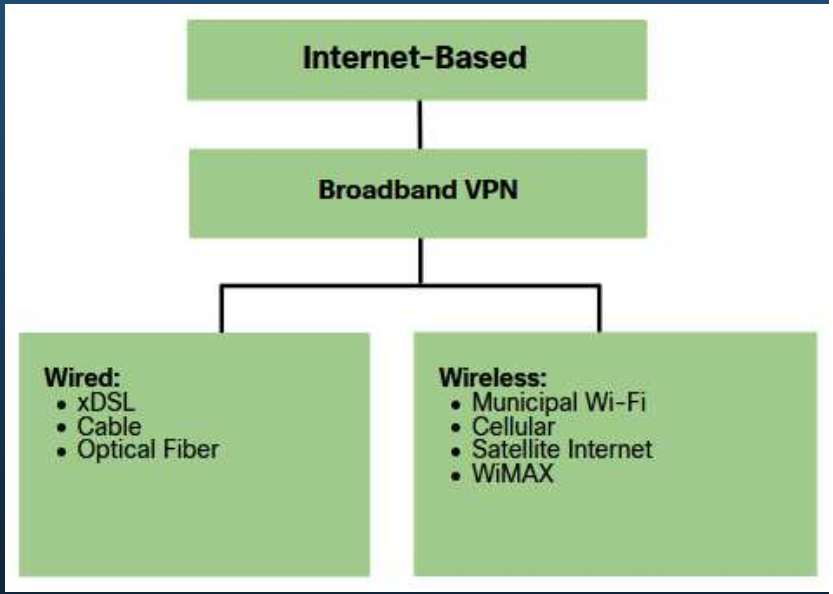
La conectividad basada en Internet se puede dividir en opciones cableadas e inalámbricas.

Opciones con cable

- Las opciones cableadas utilizan cableado permanente (por ejemplo, cobre o fibra) para proporcionar ancho de banda consistente y reducir las tasas de error y la latencia. Ejemplos: DSL, las conexiones de TV por cable y las redes de fibra óptica.

Opciones inalámbricas

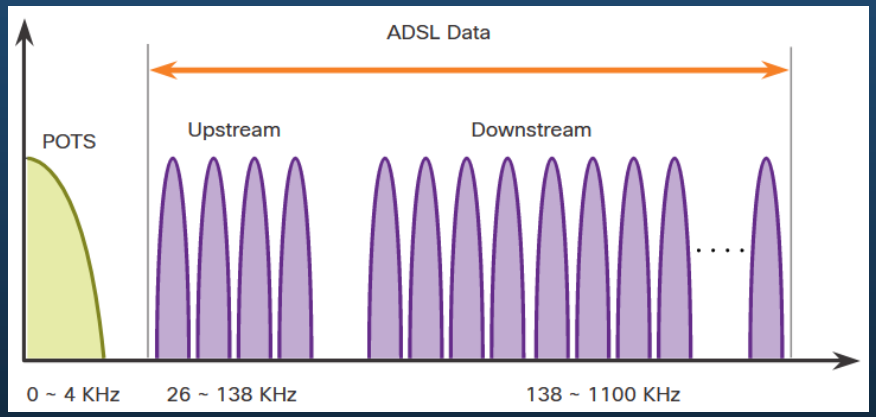
- Las opciones inalámbricas son menos costosas de implementar en comparación con otras opciones de conectividad WAN porque utilizan ondas de radio en lugar de medios cableados para transmitir datos. Ejemplos: los servicios de Internet celulares 3G/4G/5G o satelitales.
- Las señales inalámbricas pueden verse afectadas negativamente por factores como la distancia de las torres de radio, la interferencia de otras fuentes y el clima.



Conectividad basada en Internet

Tecnología DSL

La tecnología DSL es una tecnología de conexión permanente que usa las líneas telefónicas de par trenzado existentes para transportar datos con un ancho de banda elevado y proporciona servicios IP a los suscriptores.



Los DSL se clasifican como DSL asimétrico (ADSL) o DSL simétrico (SDSL).

- ADSL y ADSL2 + proporciona mayor ancho de banda descendente al usuario que el ancho de banda de carga.
- SDSL proporciona la misma capacidad en ambas direcciones.

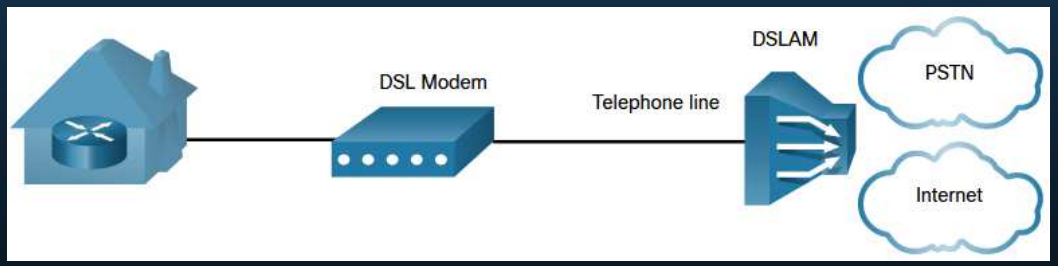
Las velocidades de transferencia DSL dependen de la extensión real del bucle local, y del tipo y la condición del cableado.

Conectividad basada en Internet

Conexiones DSL

Los proveedores de servicios implementan conexiones DSL en el bucle local. La conexión se configura entre el módem DSL y el multiplexor de acceso DSL (DSLAM).

- El módem DSL convierte las señales Ethernet del dispositivo de teletrabajador en una señal DSL, que se transmite a un multiplexor de acceso DSL (DSLAM) en la ubicación del proveedor.
- Un DSLAM es el dispositivo ubicado en la oficina central (CO) del proveedor y concentra las conexiones de varios suscriptores de DSL.
- DSL no es un medio compartido. Cada usuario tiene su propia conexión directa al DSLAM. Agregar usuarios no impide el rendimiento.



Conectividad basada en Internet

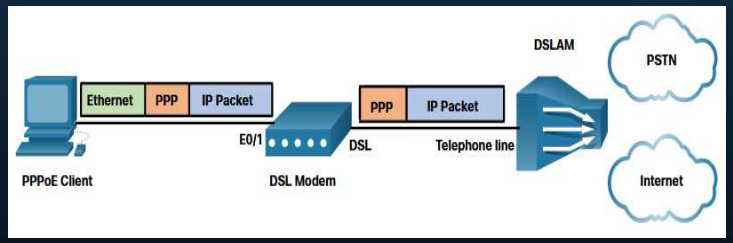
DSL y PPP

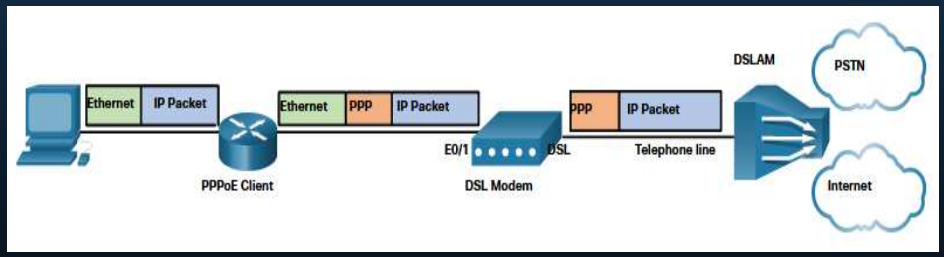
Los ISP suelen usar PPP como protocolo de enlace de datos a través de las conexiones de banda ancha.

- PPP se puede utilizar para autenticar al suscriptor.
- PPP puede asignar una dirección IPv4 pública al suscriptor.
- El PPP también incluye la función de administración de calidad de enlace.

Hay dos maneras de implementar PPP sobre Ethernet (PPPoE):

- **Host con cliente PPoE** - El software cliente PPPoE se comunica con el módem DSL mediante PPPoE y el módem se comunica con el ISP mediante PPP.
- **Cliente PPPoE** Router - El router es el cliente PPPoE y obtiene su configuración del proveedor.





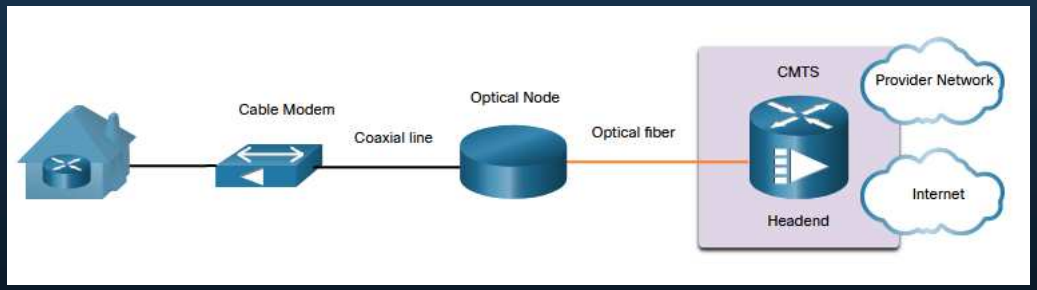
Conectividad basada en Internet

Tecnología de cable

La tecnología de cable es una tecnología de conexión siempre activa de alta velocidad que utiliza un cable coaxial de la compañía de cable para proporcionar servicios IP a los usuarios.

La especificación de interfaz del servicio de datos por cable (DOCSIS) es el estándar internacional para agregar datos de ancho de banda de alta velocidad a un sistema de cables existente.

- El nodo óptico convierte las señales de RF en impulsos de luz sobre el cable de fibra óptica.
- El medio de fibra permite que las señales viajen a largas distancias hasta la cabecera del proveedor donde se encuentra un sistema de terminación de módem por cable (CMTS).
- El encabezado contiene las bases de datos necesarias para proporcionar acceso a Internet, mientras que el CMTS es responsable de comunicarse con los módems por cable.



Nota:Todos los suscriptores locales comparten el mismo ancho de banda de cable.Fuzzy match 80% - Approved A medida que se unen más usuarios al servicio, es posible que el ancho de banda disponible caiga por debajo de la velocidad esperada.

Conectividad basada en Internet

Fibra óptica

Muchos municipios, ciudades y proveedores instalan cable de fibra óptica en la ubicación del usuario. Esto se conoce comúnmente como Fiber to the x (FTTx) e incluye lo siguiente:

- **Fiber to the Home (FTTH)** - La fibra alcanza el límite de la residencia.
- **Fiber to the Building (FTTB)** - La fibra alcanza el límite del edificio con la conexión final con el espacio de vida individual que se realiza a través de medios alternativos.
- **Fiber to the Node/Neighborhood (FTTN)** : el cableado óptico llega a un nodo óptico que convierte las señales ópticas a un formato aceptable para par trenzado o cable coaxial a la premisa.

Nota: FTTx puede ofrecer el ancho de banda más alto de todas las opciones de banda ancha.

Conectividad basada en Internet

Banda ancha inalámbrica basada en Internet

Para enviar y recibir datos, la tecnología inalámbrica usa el espectro de radio sin licencia.

- **Wi-Fi Municipal** -Algunas de estas redes proporcionan acceso a Internet de alta velocidad de manera gratuita o por un precio sustancialmente inferior al de otros servicios de banda ancha..
- **Celular** – Cada vez se utiliza más para conectar dispositivos a Internet mediante ondas de radio para comunicarse a través de una torre de telefonía móvil cercana. 3G/4G/5G y la evolución a largo plazo (LTE) son tecnologías celulares.
- **Internet satelital** - Generalmente utilizada por usuarios en áreas rurales, donde no hay cable ni DSL. Específicamente, un router se conecta a un plato satelital que apunta al satélite de un proveedor de servicios. Los árboles y las fuertes lluvias pueden impactar la señal satelital.
- **WiMAX** - Interoperabilidad mundial para acceso por microondas que proporciona un servicio de banda ancha de alta velocidad con acceso inalámbrico y una amplia cobertura, como una red de telefonía celular, en vez de pequeñas zonas de cobertura inalámbrica Wi-Fi.

Conectividad basada en Internet

Tecnología VPN

Cuando un trabajador remoto o un trabajador en una oficina remota utilizan un servicio de banda ancha para acceder a la WAN corporativa a través de Internet, se generan riesgos de seguridad y por eso son necesarias las VPN.

Una VPN es una conexión cifrada entre redes privadas a través de una red pública. Los túneles VPN se enrutan a través de Internet desde la red privada de la empresa al sitio remoto o al host del empleado.

Existen varios beneficios en el uso de VPN:

- **Ahorro de costes**- Esto elimina los enlaces WAN dedicados y costosos, y los bancos de módem.
- **Seguridad** -Los protocolos de encriptación y autenticación protegen los datos del acceso no autorizado..
- **Escalabilidad** – Las organizaciones pueden agregar una gran cantidad de capacidad sin necesidad de aumentar considerablemente la infraestructura.
- **Compatibilidad con la tecnología de banda ancha** - Los proveedores de servicio de banda ancha, como DSL y cable, admiten la tecnología VPN.

Las VPN se implementan comúnmente de la siguiente manera:

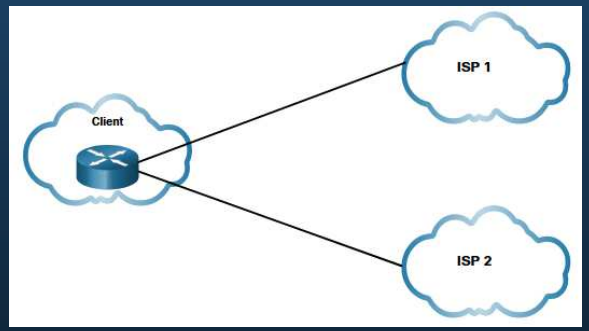
- **VPN de sitio a sitio** - La configuración de VPN se configura en los routers. Los clientes no saben que sus datos están siendo cifrados.
- **Acceso remoto** - El usuario es consciente e inicia la conexión de acceso remoto. Por ejemplo, usar HTTPS en un navegador para conectarse a su banco. Alternativamente, el usuario puede ejecutar software cliente VPN en su host para conectarse y autenticarse con el dispositivo de destino.

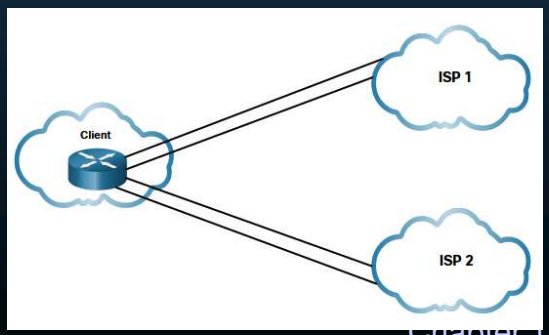
Conectividad basada en Internet

Opciones de conectividad de ISP

Hay diferentes maneras en que una organización puede conectarse a un ISP. La elección depende de las necesidades y el presupuesto de la organización.

- **Una sola conexión** - Una sola conexión al ISP mediante un enlace. No proporciona redundancia y es la solución menos costosa.
- **Dual-homed** - Se conecta al mismo ISP mediante dos enlaces. Proporciona redundancia y equilibrio de carga. Sin embargo, la organización pierde conectividad a Internet si el ISP experimenta una interrupción.
- **Multihomed** - El cliente se conecta a dos ISP diferentes. Este diseño proporciona una mayor redundancia y permite equilibrar la carga, pero puede ser costoso.
- **Dual-MultiHomed** - Dual-MultiHomed es la topología más resistente de las cuatro mostradas. El cliente se conecta con vínculos redundantes a varios ISP. Esta topología proporciona la mayor redundancia posible. Es la opción más cara de los cuatro.





Conectividad basada en Internet

Comparación de soluciones de banda ancha

Todas las soluciones de banda ancha tienen ventajas y desventajas. Si hay varias soluciones de banda ancha disponibles, se debe llevar a cabo un análisis de costos y beneficios para determinar cuál es la mejor solución.

Entre otros de los factores que se deben considerar se incluyen los siguientes:

- **Cable**- Ancho de banda es compartido por muchos usuarios. Por lo tanto, el ancho de banda se comparte entre diversos usuarios; las velocidades de datos ascendentes suelen ser lentas durante las horas de alto uso en áreas con sobresubscripción.
- **DSL**- El ancho de banda es limitado y se ve afectado por la distancia. La tasa de carga es proporcionalmente menor en comparación con la tasa de descarga.
- **Fibra hasta el hogar**- Requiere la instalación de la fibra directamente en el hogar.
- **Datos móviles-** La cobertura a menudo representa un problema; incluso dentro de una SOHO, en donde el ancho de banda es relativamente limitado.
- **Wi-Fi Municipal**- la mayoría de las municipalidades no cuentan con una red de malla implementada. Si está disponible y en rango, entonces es una opción viable.
- **Satélite** - Es costoso, tiene una capacidad limitada por suscriptor. Normalmente se utiliza cuando no hay otra opción disponible.

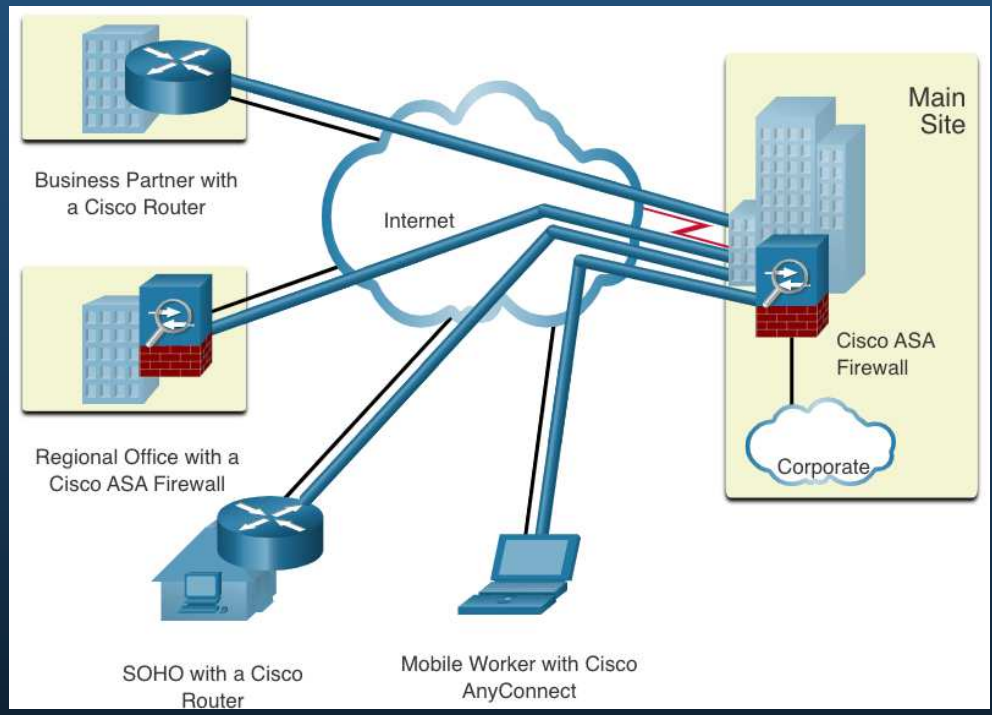
Capítulo 8

Conceptos de VPN e IPsec

Tecnología VPN

Redes privadas virtuales

- Redes privadas virtuales (VPNs) para crear conexiones de red privada de punto a punto (end-to-end).
- Una VPN es virtual porque transporta la información dentro de una red privada, pero, en realidad, esa información se transporta usando una red pública.
- Una VPN es privada porque el tráfico se encripta para preservar la confidencialidad de los datos mientras se los transporta por la red pública



Tecnología VPN

Beneficios VPN

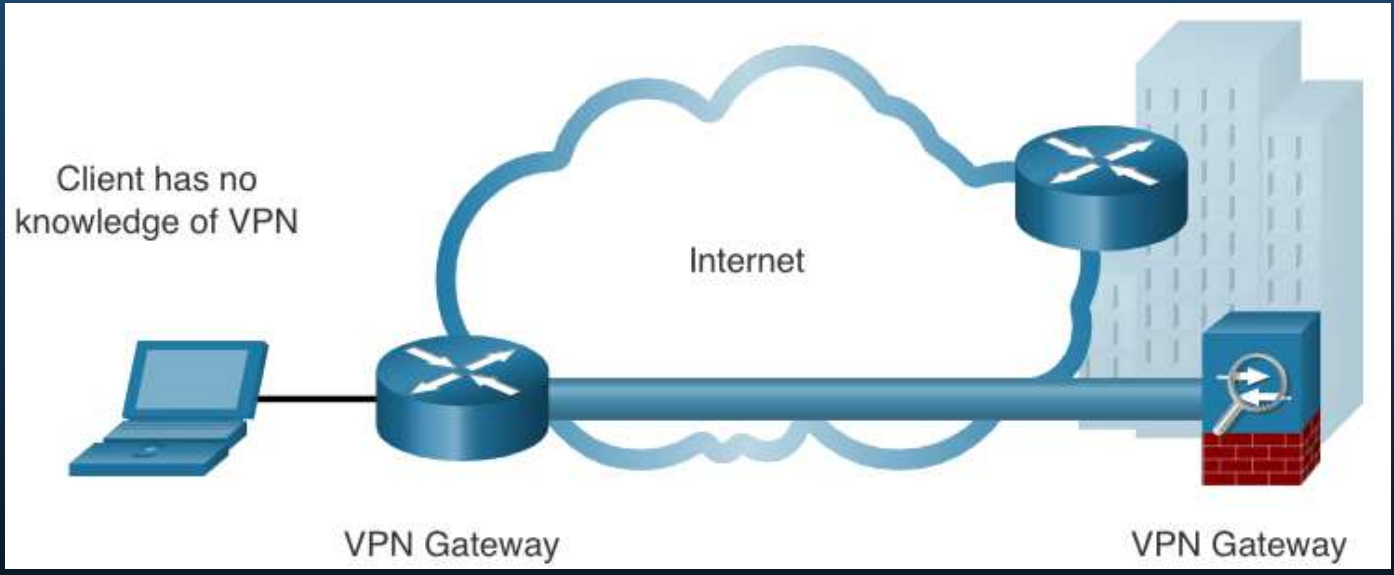
- Las VPN modernas ahora admiten funciones de encriptación, como la seguridad de protocolo de Internet (IPsec) y las VPN de capa de sockets seguros (SSL) para proteger el tráfico de red entre sitios.
- Los principales beneficios de las VPN se muestran en la tabla.

Ventaja	Descripción
Ahorro de costos	Las organizaciones pueden usar VPN para reducir sus costos de conectividad y al mismo tiempo aumentar el ancho de banda de la conexión remota.
Seguridad	Los protocolos de encriptación y autenticación protegen los datos del acceso no autorizado.
Escalabilidad	Las VPN proporcionan escalabilidad, lo que permite a las organizaciones usar Internet, lo que facilita agregar nuevos usuarios sin agregar una infraestructura significativa.
Compatibilidad	Las VPN se pueden implementar en una amplia variedad de opciones de enlace WAN, incluidas las tecnologías de banda ancha. Los trabajadores remotos pueden usar estas conexiones de alta velocidad para obtener acceso seguro a las redes corporativas.

Tecnología VPN

VPN de sitio a sitio y acceso remoto

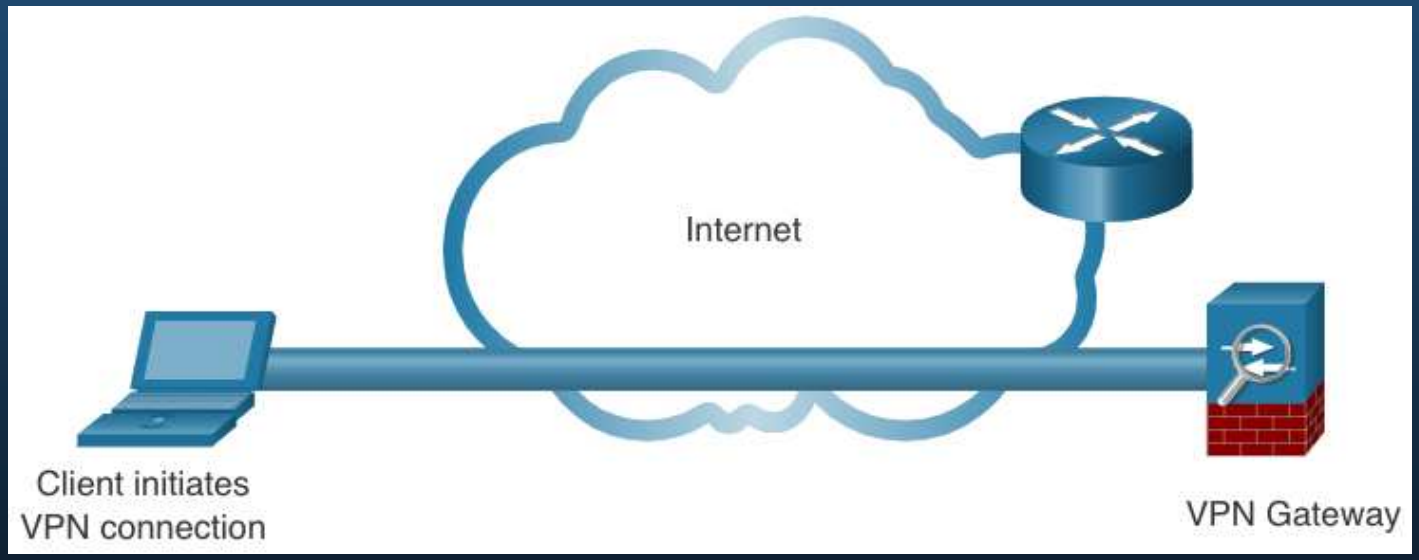
Una VPN de sitio a sitio finaliza en las puertas de enlace VPN. El tráfico VPN solo se cifra entre las puertas de enlace. Los hosts internos no tienen conocimiento de que se está utilizando una VPN.



Tecnología VPN

VPN de sitio a sitio y acceso remoto

Una VPN de acceso-remoto se crea dinámicamente para establecer una conexión segura entre un cliente y un dispositivo de terminación de VPN.



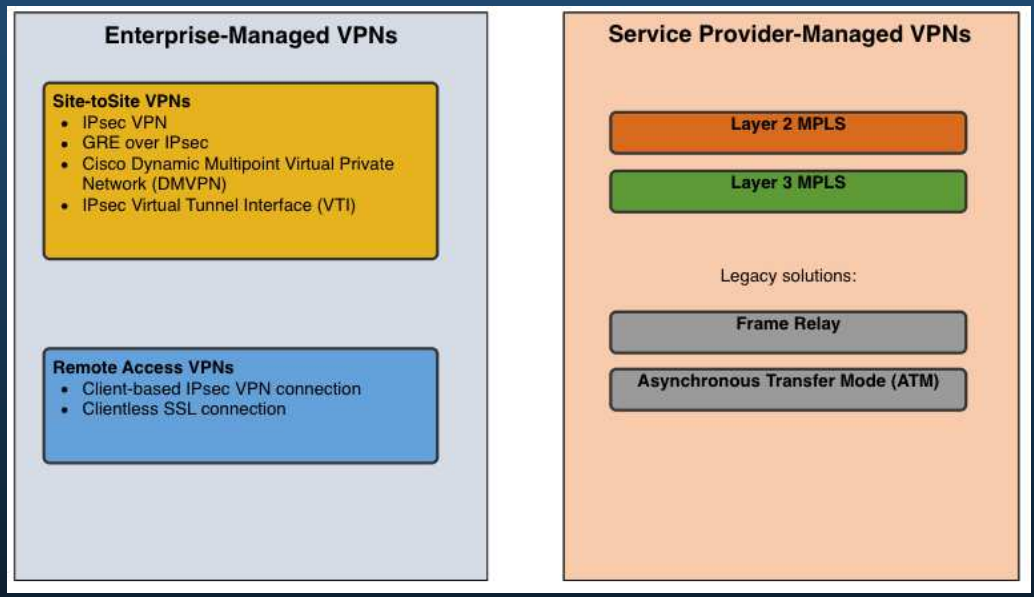
Tecnología VPN

VPN para empresas y proveedores de servicios

Las VPN se pueden administrar e implementar como:

- **VPN empresariales:** solución común para proteger el tráfico empresarial a través de Internet. Las VPN de sitio a sitio y de acceso remoto son creadas y administradas por la empresa utilizando tanto VPN IPsec como SSL.

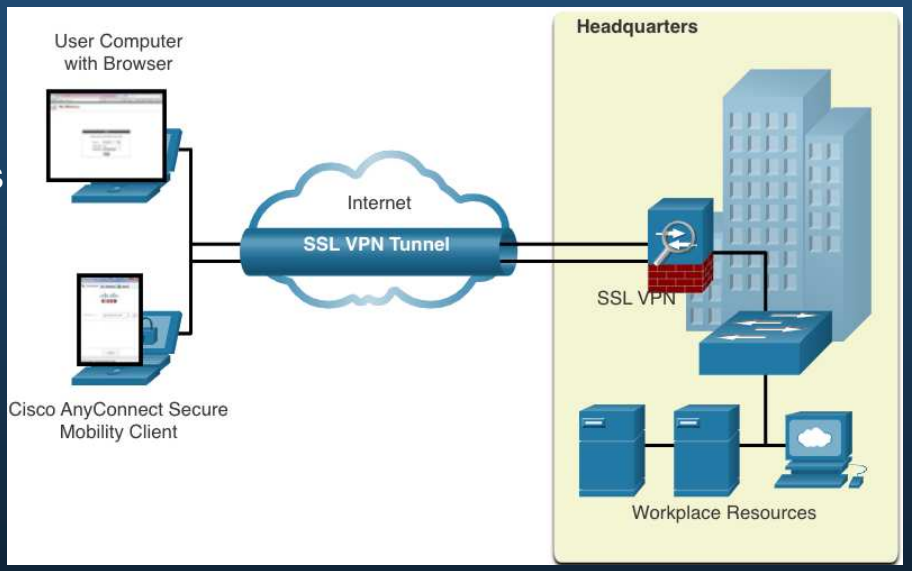
- **VPN de proveedores de servicios:** creados y administrados por la red de proveedores. El proveedor utiliza la conmutación de etiquetas multiprotocolo (MPLS) en la capa 2 o la capa 3 para crear canales seguros entre los sitios de una empresa, segregando efectivamente el tráfico del tráfico de otros clientes.



Tipos de VPN

VPN de acceso remoto

- Las VPN de acceso remoto permiten a los usuarios remotos y móviles conectarse de forma segura a la empresa.
- Las VPN de acceso remoto generalmente se habilitan dinámicamente por el usuario cuando es necesario y se pueden crear utilizando IPsec o SSL.
- **Conexión VPN sin cliente** - La conexión se asegura utilizando una conexión SSL de navegador web.
- **Conexión VPN basada en el cliente** - El software de cliente VPN, como Cisco AnyConnect Secure Mobility Client, debe instalarse en el dispositivo final del usuario remoto.



Tipos de VPN

SSL VPNs

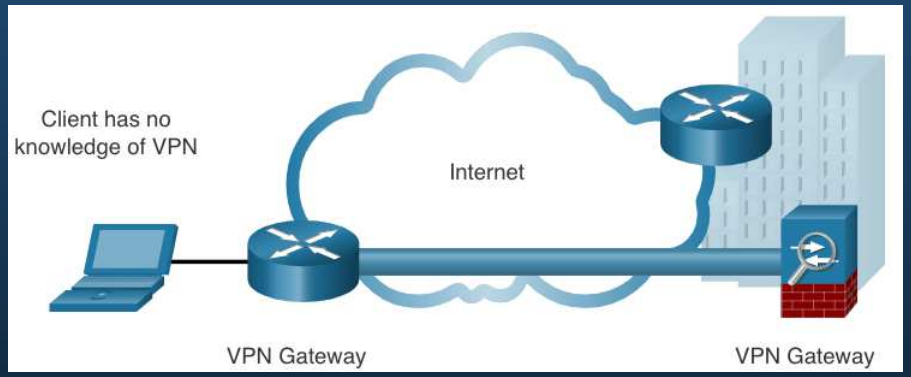
SSL utiliza la infraestructura de llave pública y los certificados digitales para autenticar a sus pares. El tipo de método VPN implementado se basa en los requisitos de acceso de los usuarios y en los procesos de TI de la organización. La tabla compara las implementaciones de acceso remoto IPsec y SSL.

Característica	IPsec	SSL
Aplicaciones compatibles	**Extensiva** – Todas las aplicaciones basadas en IP son compatibles.	**Limitada** – Solo aplicaciones y archivos compartidos basados en la web
Fuerza de autenticación	**Fuerte:** – autenticación bidireccional con claves compartidas o certificados digitales	**Moderado** – Uso de autenticación unidireccional o bidireccional
Fuerza de encriptación	**Fuerte** – Longitudes de clave 56 - 256 bits	**Moderado a fuerte**- Longitudes de clave 40 - 256 bits
Complejidad de conexión	**Medio:** – Requiere un cliente VPN instalado en un host	**Bajo:** – Requiere un navegador web en un host
Opción de conexión	**Limitado:** – Solo se pueden conectar dispositivos específicos con configuraciones específicas	**Extenso:** – Cualquier dispositivo con un navegador web puede conectarse

Tipos de VPN

VPN de IPsec de sitio a sitio

- Las VPN de sitio a sitio se utilizan para conectar redes a través de otra red no confiable como Internet.
- Los hosts finales envían y reciben tráfico TCP / IP sin cifrar normal a través de una puerta de enlace VPN.
- La puerta de enlace VPN encapsula y cifra el tráfico saliente de un sitio y envía el tráfico a través del túnel VPN a la puerta de enlace VPN en el sitio de destino. Al recibirlo, la puerta de enlace VPN receptora despoja los encabezados, desencripta el contenido y retransmite el paquete hacia el usuario de destino dentro de su red privada.



Tipos de VPN

GRE sobre IPsec

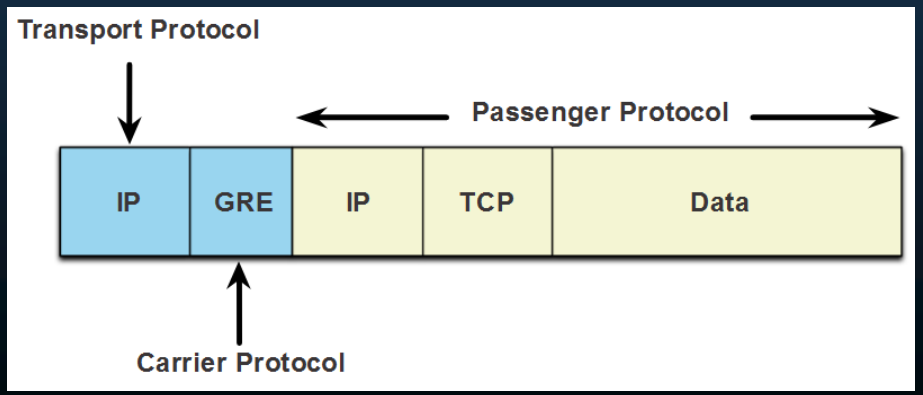
- Generic Routing Encapsulation (GRE) es un protocolo de túnel de VPN de sitio a sitio básico y no seguro.
- Un túnel GRE puede encapsular varios protocolos de capa de red, así como tráfico multicast y broadcast.
- Sin embargo, GRE no admite de forma predeterminada el encriptado; y por lo tanto, no proporciona un túnel VPN seguro.
- Un paquete GRE puede encapsularse en un paquete IPsec para reenviarlo de forma segura a la puerta de enlace VPN de destino.
- Una VPN IPsec estándar (no GRE) solo puede crear túneles seguros para el tráfico de unicast.
- Encapsular GRE en IPsec permite asegurar las actualizaciones del protocolo de enrutamiento de multidifusión a través de una VPN.

Tipos de VPN

GRE sobre IPsec

Los términos utilizados para describir la encapsulación de GRE sobre el túnel IPsec son protocolo pasajero (passenger protocol), protocolo operador (carrier protocol) y protocolo transporte (transport protocol).

- **Protocolo del Pasajero** – Este es el paquete original que debe ser encapsulado por GRE. Podría ser un paquete IPv4 o IPv6, una actualización de enrutamiento y más.
- **Protocolo del Operador** – GRE es el protocolo del operador que encapsula el paquete original de pasajeros.
- **Protocolo de transporte:** – Este es el protocolo que realmente se usará para reenviar el paquete. Esto podría ser IPv4 o IPv6.

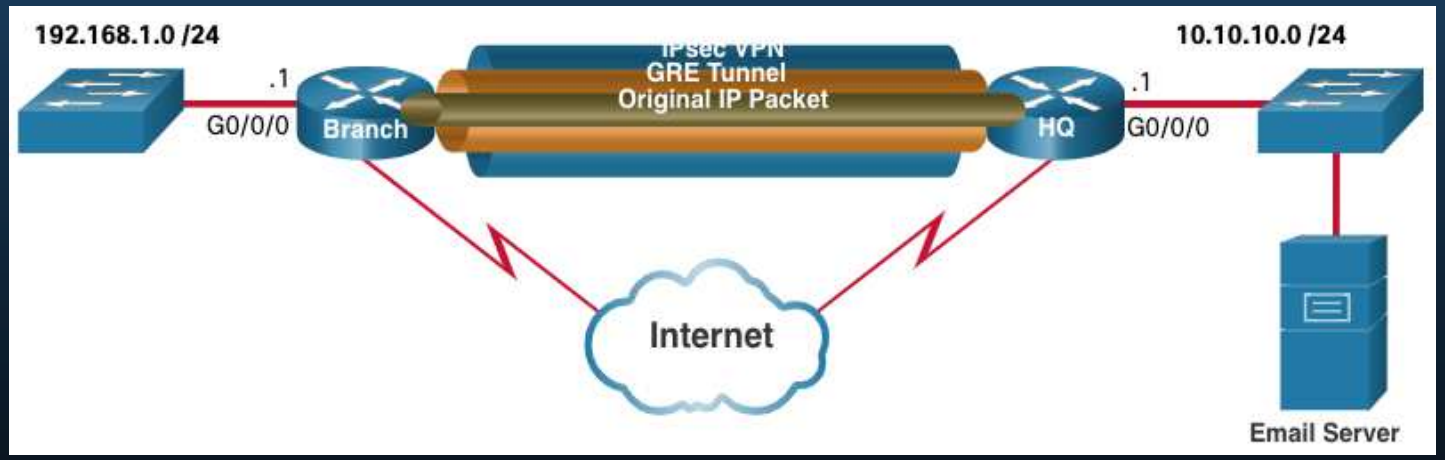


Tipos de VPN

GRE sobre IPsec

Por ejemplo, Branch y HQ necesitan intercambiar información de enrutamiento OSPF sobre una VPN IPsec. Por lo tanto, GRE sobre IPsec se usa para admitir el tráfico del protocolo de enrutamiento sobre la VPN de IPsec.

Específicamente, los paquetes OSPF (es decir, el protocolo del pasajero) serían encapsulados por GRE (es decir, el protocolo del operador) y posteriormente encapsulados en un túnel VPN IPsec.



Tipos de VPN

VPN dinámicas multipunto

Las VPN de IPsec de sitio a sitio y GRE sobre IPsec no son suficientes cuando la empresa agrega muchos más sitios. La VPN dinámica multipunto (DMVPN) es una solución de Cisco para crear VPN múltiples de forma fácil, dinámica y escalable.

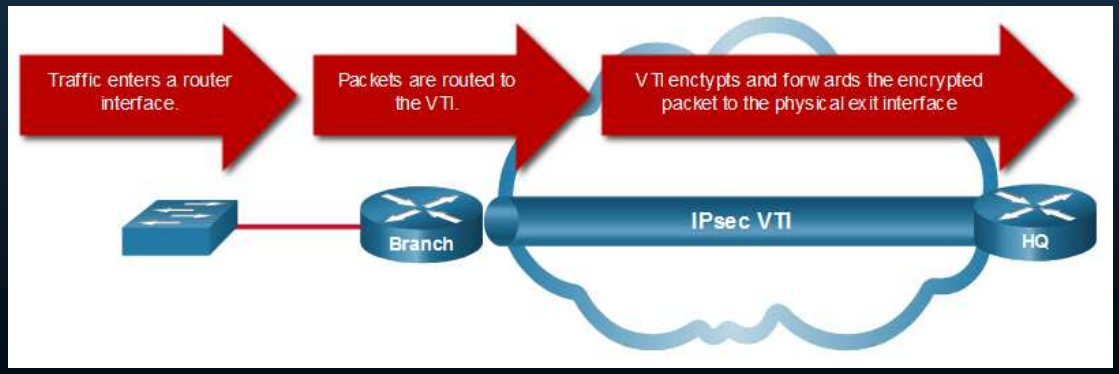
- DMVPN simplifica la configuración del túnel VPN y proporciona una opción flexible para conectar un sitio central con sitios de sucursales.
- Utiliza una configuración de hub-and-spoke para establecer una topología de malla completa (full mesh).
- Los sitios de spoke establecen túneles VPN seguros con el sitio central, como se muestra en la figura.
- Cada sitio se configura usando Multipoint Generic Routing Encapsulation (mGRE). La interfaz del túnel mGRE permite que una única interfaz GRE admita dinámicamente múltiples túneles IPsec.
- Los sitios de radios también pueden obtener información unos de otros y, alternativamente, construir túneles directos entre ellos (túneles de radio a radio).

Tipos de VPN

Interfaz de túnel virtual IPsec

Al igual que los DMVPN, IPsec Virtual Tunnel Interface (VTI) simplifica el proceso de configuración requerido para admitir múltiples sitios y acceso remoto.

- Las configuraciones de IPsec VTI se aplican a una interfaz virtual en lugar de la asignación estática de las sesiones de IPsec a una interfaz física.
- IPsec VTI es capaz de enviar y recibir tráfico IP encriptado de unicast y multicast. Por lo tanto, los protocolos de enrutamiento son compatibles automáticamente sin tener que configurar túneles GRE.
- IPsec VTI se puede configurar entre sitios o en una topología de hub-and-spoke.



Tipos de VPN

VPN de MPLS del proveedor de servicios

Hoy, los proveedores de servicios usan MPLS en su red principal. El tráfico se reenvía a través de la red troncal MPLS mediante etiquetas. Al igual que las conexiones WAN heredadas, el tráfico es seguro porque los clientes del proveedor de servicios no pueden ver el tráfico de los demás.

- MPLS puede proporcionar a los clientes soluciones VPN administradas; por lo tanto, aseguran el tráfico entre los sitios del cliente es responsabilidad del proveedor del servicio.
- Hay dos tipos de soluciones VPN MPLS compatibles con los proveedores de servicios:
  - **VPN MPLS Capa 3** -El proveedor de servicios participa en el enrutamiento del cliente al establecer un intercambio entre los enrutadores del cliente y los enrutadores del proveedor.
  - **VPN MPLS Capa 2** -El proveedor de servicios no participa en el enrutamiento del cliente. En cambio, el proveedor implementa un servicio de LAN privada virtual (VPLS) para emular un segmento LAN de acceso múltiple de Ethernet a través de la red MPLS. No hay enrutamiento involucrado. Los enrutadores del cliente pertenecen efectivamente a la misma red de acceso múltiple.

IPSec

Tecnologías IPsec

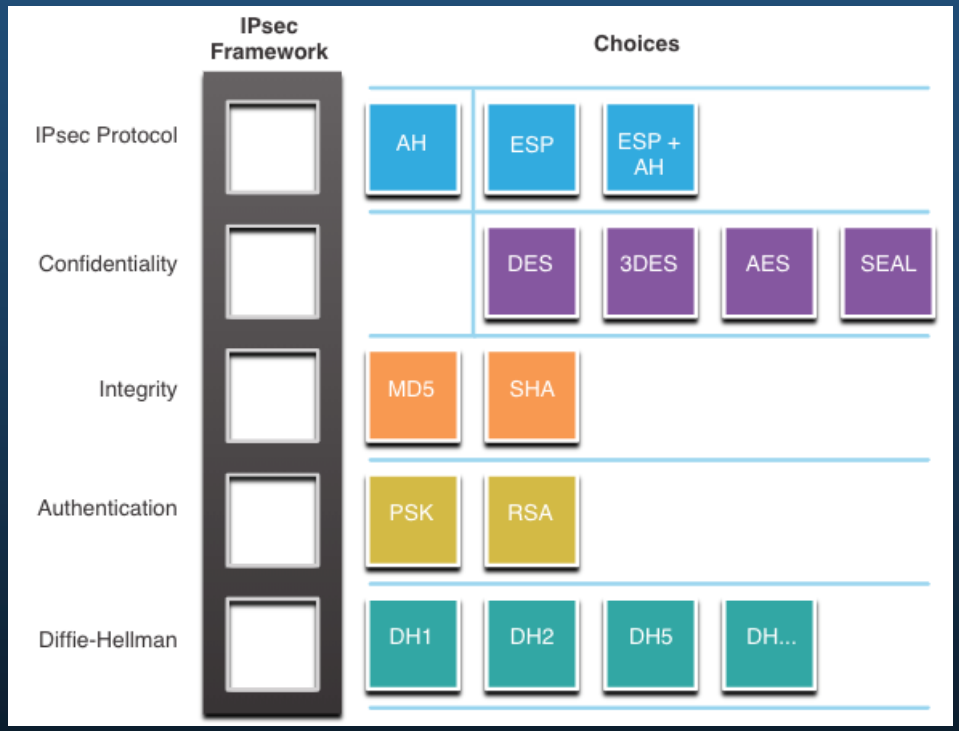
IPsec es un estándar IETF (RFC 2401-2412) que define cómo se puede asegurar una VPN a través de redes IP. IPsec protege y autentica los paquetes IP entre el origen y el destino y proporciona estas funciones de seguridad esenciales:

- **Confidencialidad** - IPsec utiliza algoritmos de encriptación para evitar que los delincuentes cibernéticos lean el contenido del paquete.
- **Integridad** - Psec utiliza algoritmos de hash para garantizar que los paquetes no se hayan modificado entre el origen y el destino.
- **Autenticación de Origen** - IPsec utiliza el protocolo de intercambio de claves de Internet (IKE) para autenticar el origen y el destino.
- **Diffie-Hellman** – se utiliza para asegurar el intercambio de claves.

IPSec

Tecnologías IPsec

- IPsec no está sujeto a ninguna regla específica para comunicaciones seguras.
- IPsec puede integrar fácilmente nuevas tecnologías de seguridad sin actualizar los estándares existentes de IPsec.
- Las ranuras abiertas que se muestran en el marco de IPsec en la figura pueden llenarse con cualquiera de las opciones disponibles para esa función de IPsec para crear una asociación de seguridad (SA) única.



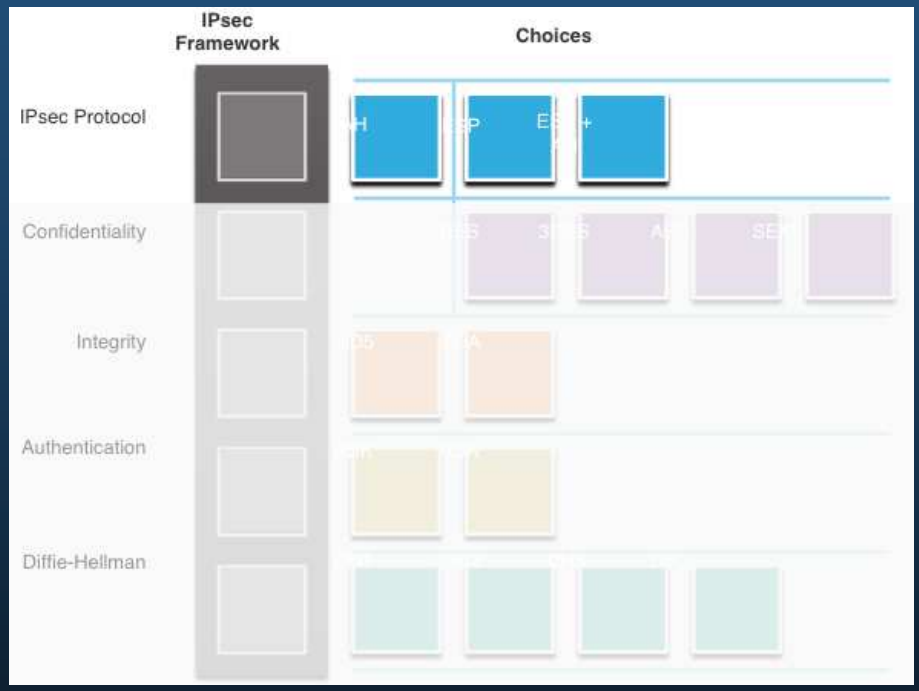
IPSec

Protocolo de Encapsulación IPsec

La elección del protocolo de encapsulación IPsec es el primer bloque de construcción del marco.

- IPsec encapsula paquetes usando el Encabezado de autenticación (AH) o el Protocolo de seguridad de encapsulación (ESP).

- La elección de AH o ESP establece que otros bloques de construcción están disponibles:
  - AH es apropiado solo cuando la confidencialidad no es requerida o permitida.
  - ESP proporciona confidencialidad y autenticación.

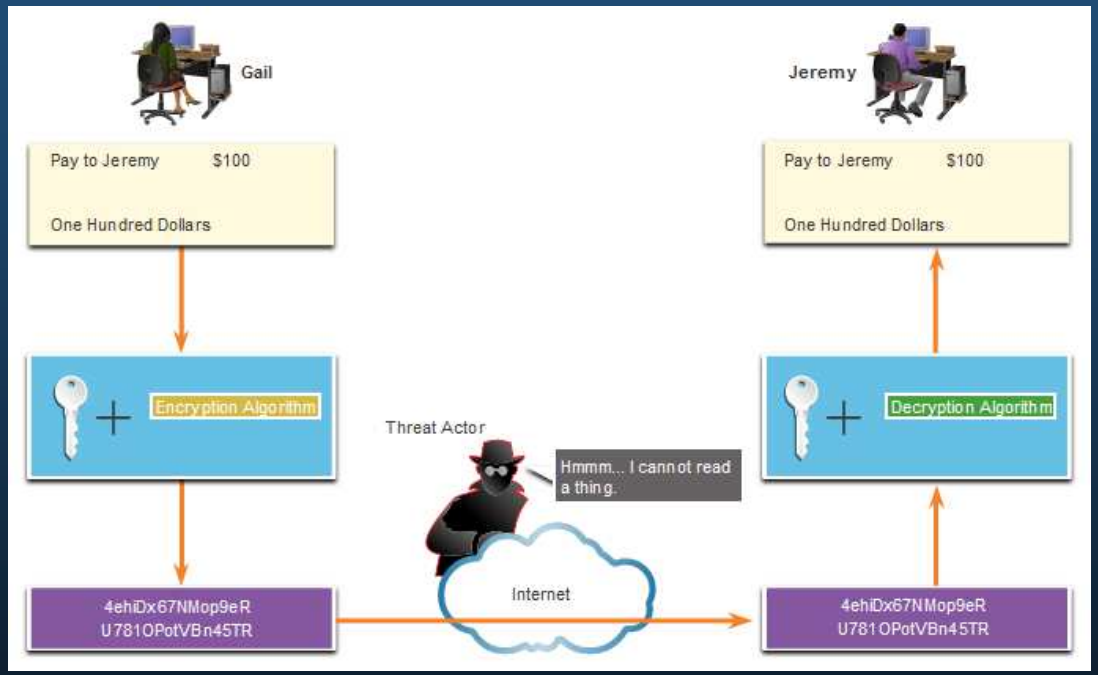


IPSec

Confidencialidad

El grado de confidencialidad depende del algoritmo de encriptación y la longitud de la llave utilizada en el algoritmo de encriptación.

La cantidad de posibilidades para intentar hackear la clave es una función de la longitud de la clave: cuanto más corta es la clave, más fácil es romperla.

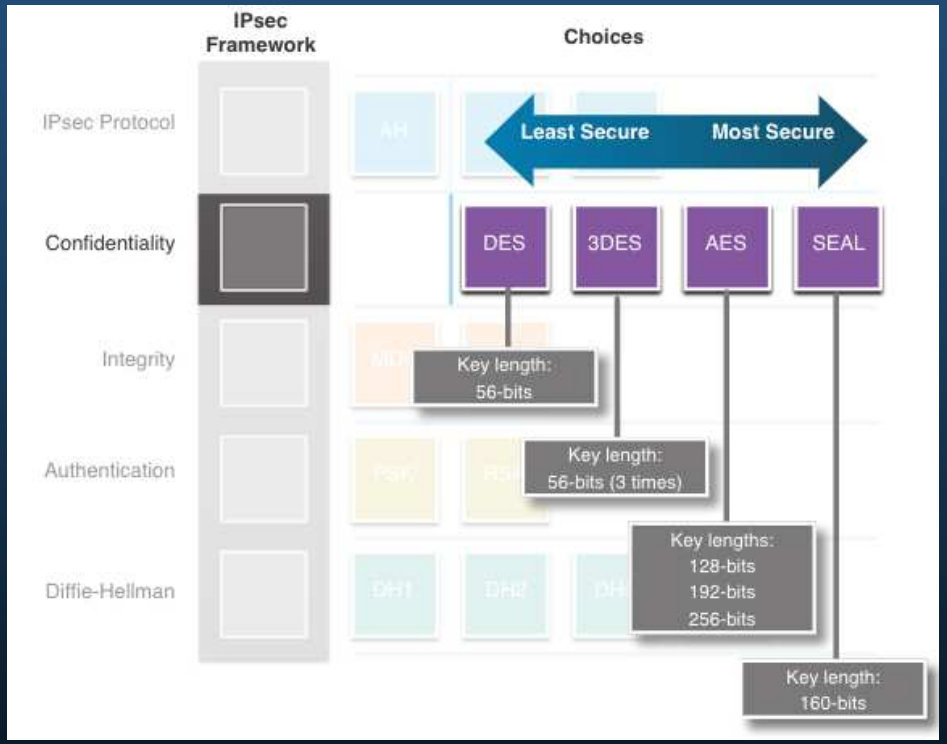


IPSec

Confidencialidad

Los algoritmos de encriptación resaltados en la figura son todos criptosistemas de llave simétrica:

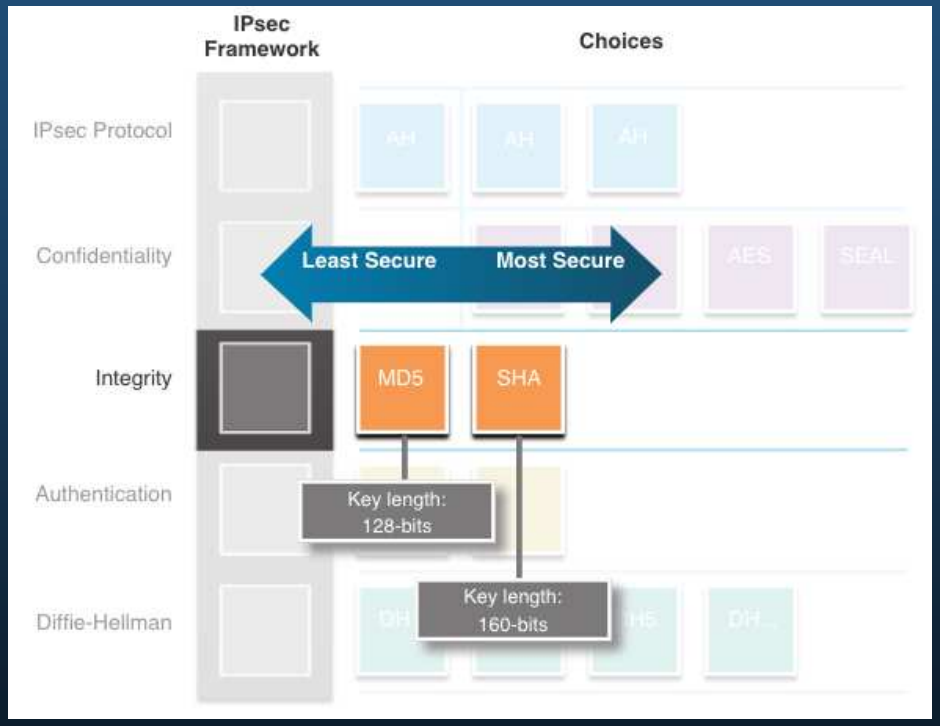
- DES usa una llave de 56 bits.
- 3DES utiliza tres claves de cifrado independientes de 56 bits por bloque de 64 bits.
- AES ofrece tres longitudes de llave diferentes: 128 bits, 192 bits y 256 bits.
- SEAL es un cifrado de flujo, lo que significa que encripta datos continuamente en lugar de encriptar bloques de datos. SEAL utiliza una llave de 160 bits.



IPSec

Integridad

- La integridad de los datos significa que los datos no han cambiado en tránsito.
- Se requiere un método para probar la integridad de los datos.
- El Código de autenticación de mensajes hash (HMAC) es un algoritmo de integridad de datos que garantiza la integridad del mensaje utilizando un valor hash:
  - **Message-Digest 5 (MD5)** utiliza una llave secreta compartida de 128 bits.
  - **El algoritmo de seguro de hash (SHA por sus siglas en inglés)** utiliza una llave secreta de 160 bits.



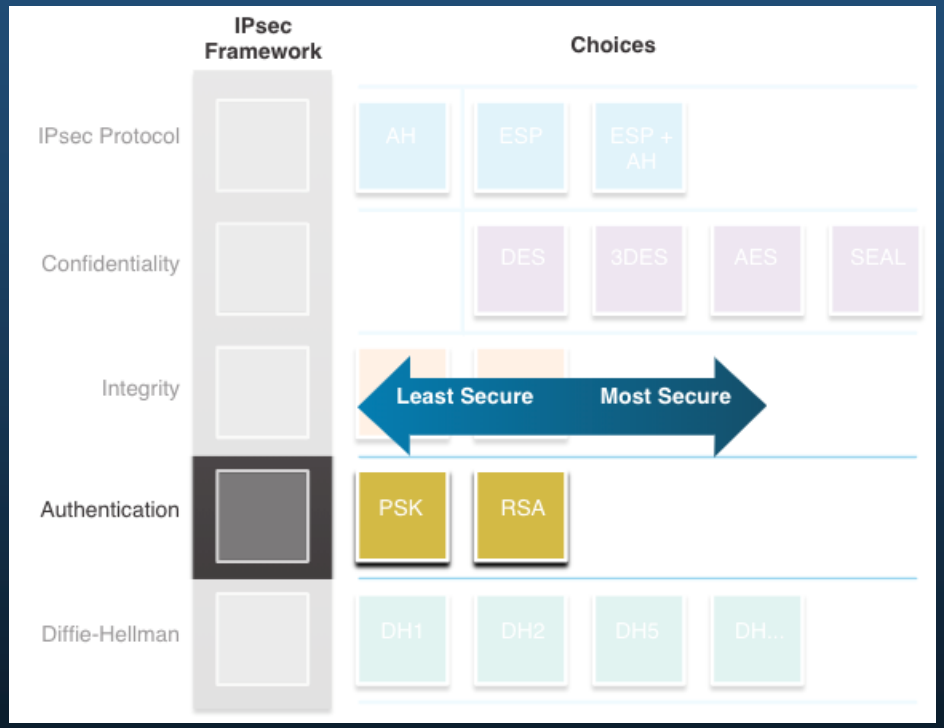
IPSec

Autenticación

Existen dos métodos de autenticación de pares de IPsec:

1. **(PSK) Un valor de llave secreta precompartida**- (PSK) se ingresa manualmente en cada par.
   - Fácil de configurar manualmente.
   - No escala bien.
   - Debe configurarse en cada par.

2. **Rivest, Shamir y Adleman (RSA):**- la autenticación utiliza certificados digitales para autenticar a los pares.
   - Cada par debe autenticar a su par opuesto antes de que el túnel se considere seguro.



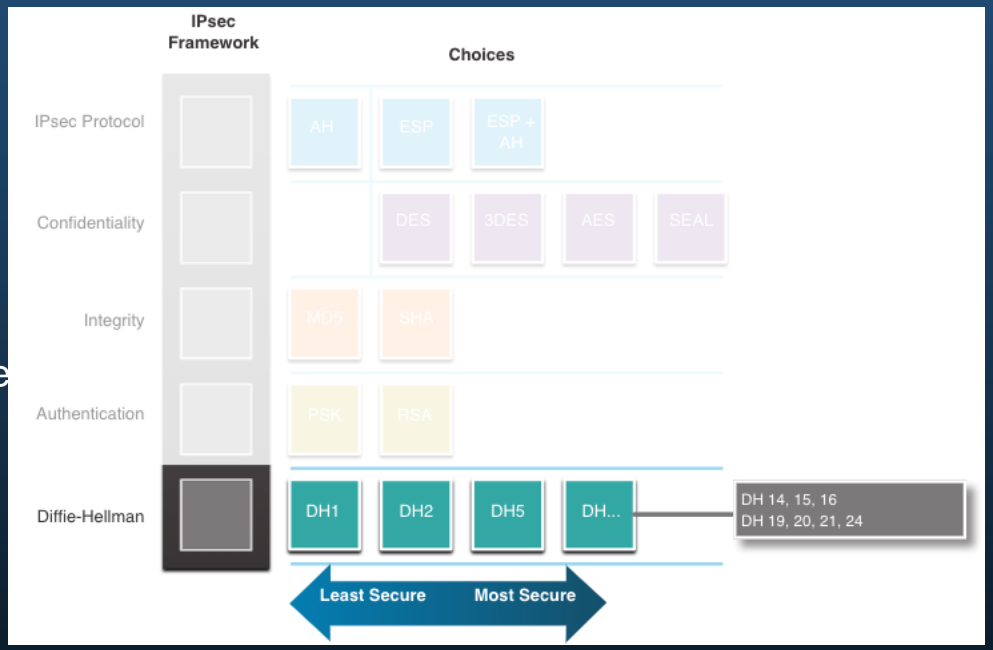
IPSec

Intercambio seguro de llaves con Diffie-Hellman

DH proporciona que dos pares puedan establecer una clave secreta compartida a través de un canal inseguro.

Las variaciones del intercambio de llaves DH se especifican como grupos DH:

- Los grupos DH 1, 2 y 5 ya no deberían usarse.
- Los grupos DH 14, 15 y 16 usan tamaños de clave más grandes con 2048 bits, 3072 bits y 4096 bits, respectivamente.
- Los grupos DH 19, 20, 21 y 24 con tamaños de llave respectivos de 256 bits, 384 bits, 521 bits y 2048 bits admiten la criptografía de curva elíptica (ECC), que reduce el tiempo necesario para generar llaves.



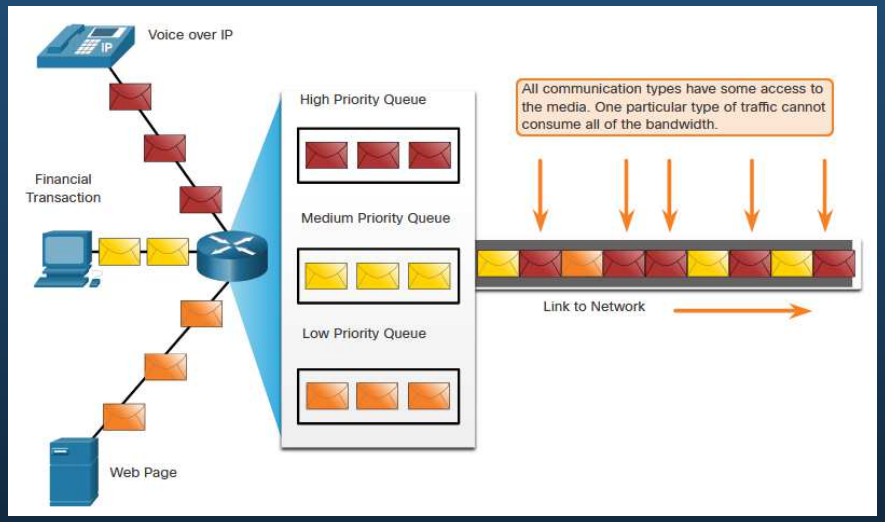
Capítulo 9

Conceptos de QoS

Calidad de la transmisión de red

Priorización del tráfico

- Cuando el volumen de tráfico es mayor de lo que se puede transportar a través de la red, los dispositivos ponen en cola (retienen) los paquetes en la memoria hasta que los recursos estén disponibles para transmitirlos.
- Los paquetes en cola causan retrasos, dado que los nuevos paquetes no se pueden transmitir hasta que no se hayan procesado los anteriores.
- Si sigue aumentando la cantidad de paquetes que se pondrán en cola, la memoria del dispositivo se llenará y los paquetes se descartarán.
- Una técnica de QoS que puede ayudarlo con este problema es la clasificación de datos en varias colas, como se muestra en la figura.

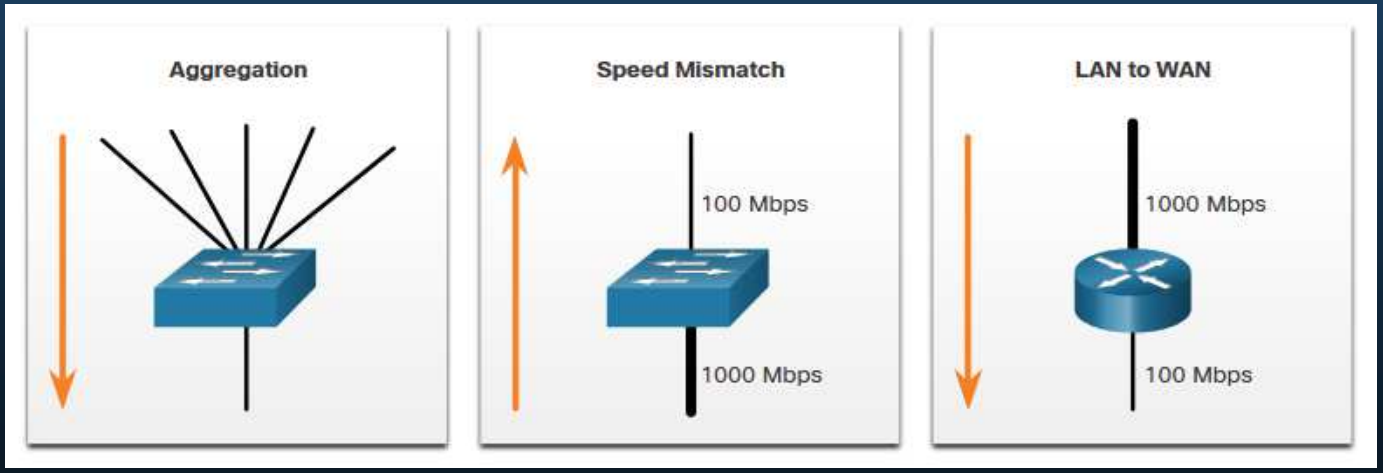


Nota: Un dispositivo implementa QoS solo cuando experimenta algún tipo de congestión

Calidad de la transmisión de red

Ancho de banda, Congestión, Demora, y Jitter

- El ancho de banda de la red es la medida de la cantidad de bits que se pueden transmitir en un segundo, es decir, bits por segundo (bps).
- La congestión de la red produce demoras. Una interfaz experimenta congestión cuando tiene más tráfico del que puede gestionar. Los puntos de congestión de la red son candidatos ideales para los mecanismos de QoS.
- Los puntos de congestión típicos son agregación, desajuste de velocidad y LAN a WAN.



Calidad de la transmisión de red

Ancho de banda, Congestión, Demora, y Jitter

La demora o la latencia se refiere al tiempo que demora un paquete en viajar de origen a destino.

- El retraso fijo es la cantidad de tiempo que tarda un proceso específico, como el tiempo que lleva colocar un bit en el medio de transmisión.
- El retraso variable lleva una cantidad de tiempo no especificada y se ve afectado por factores como la cantidad de tráfico que se procesa.
- Jitter es la variación del retraso de los paquetes recibidos.

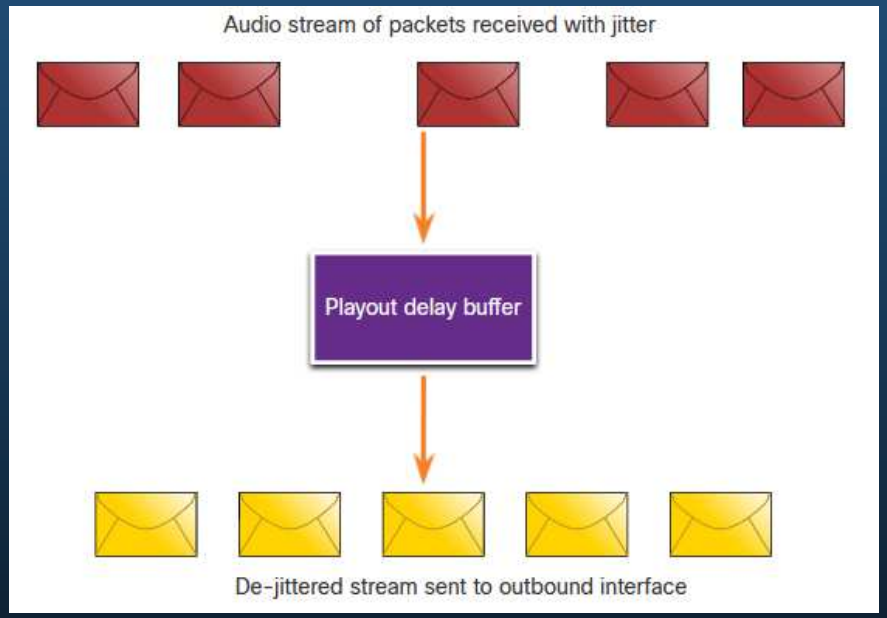
Demora	Descripción
Demora de código	La cantidad fija de tiempo dedicado a comprimir los datos en el origen antes de transmitir el primer dispositivo de interconexión de redes, generalmente un switch.
Demora de paquetización	El tiempo fijo que demora la encapsulación de un paquete con toda la información de encabezado necesaria.
Demora de asignación de cola	La cantidad de tiempo variable que una trama o un paquete espera para transmitirse en el enlace.
Demora de serialización	La cantidad fija de tiempo que lleva transmitir una trama al cable.
Demora de propagación	La cantidad de tiempo variable que demora la trama para pasar enrte el origen y el destino.
Demora de de-jitter (eliminación de fluctuación)	La cantidad fija de tiempo que se demora en el almacenamiento en búfer de un flujo de paquetes y en el envío de estos a intervalos uniformes.

Calidad de la transmisión de red

Pérdida de paquetes

Sin mecanismos de QoS, los paquetes sensibles al tiempo, como el video y la voz en tiempo real, se descartan con la misma frecuencia que los datos que no son sensibles al tiempo.

- Cuando un router recibe una transmisión de audio digital del Protocolo en tiempo real (RTP) para Voz sobre IP (VoIP), compensa el Jitter que se encuentra al usar un búfer de retardo de reproducción.
- El búfer de retardo de reproducción almacena estos paquetes y luego los reproduce en un flujo constante.

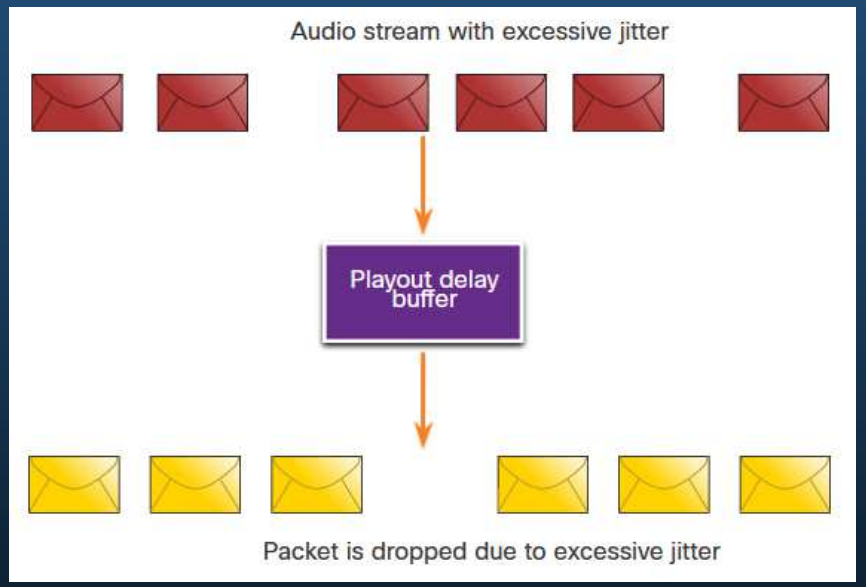


Calidad de la transmisión de red

Pérdida de paquetes

Si el jitter es tan grande que hace que los paquetes se reciban fuera del rango del búfer de reproducción, los paquetes fuera del rango se descartan y se escuchan abandonos en el audio.

- En el caso de pérdidas pequeñas de un paquete, el procesador de señales digitales (DSP) extrapola la información faltante del audio para que el usuario pueda escucharlo sin problemas.
- Cuando el jitter excede lo que el DSP puede hacer para compensar los paquetes faltantes, se escuchan problemas de audio.



Nota: En una red diseñada adecuadamente, la pérdida de paquetes debe ser cercana a cero.

Características del tráfico

Tendencias del tráfico de red

A principios de la década del 2000, los tipos de tráfico IP predominantes eran voz y datos.

- El tráfico de voz tiene una necesidad de ancho de banda predecible y tiempos de llegada de paquete conocidos.
- El tráfico de datos no es en tiempo real, y tiene una necesidad impredecible de ancho de banda.
- El tráfico de datos puede tener estallidos temporalmente, como cuando se descarga un archivo grande. Este estallido puede consumir todo el ancho de banda de un enlace.

Más recientemente, el tráfico de video se ha vuelto cada vez más importante para las comunicaciones y las operaciones empresariales.

- Según el Índice de redes visuales de Cisco (VNI), el tráfico de video representó el 70% de todo el tráfico en 2017.
- Para 2022, el video representará el 82% de todo el tráfico.
- El tráfico de video móvil alcanzará 60,9 exabytes por mes para 2022.

Los tipos de demandas de voz, video y tráfico de datos en la red son muy diferentes.

Características del tráfico

Voz

El tráfico de voz es predecible y fluido y muy sensible a retrasos y paquetes descartados.

- Los paquetes de voz deben recibir una prioridad mayor a la de otros tipos de paquetes.
- Los productos de Cisco utilizan el rango de puerto de 16384 a 32767 de RTP para priorizar el tráfico de voz.

La voz puede tolerar una cierta cantidad de latencia, jitter y pérdida sin ningún efecto notable.

La latencia no debe superar los 150 milisegundos (ms).

- El jitter no debe superar los 30 ms y la pérdida de paquetes no debe superar el 1%.
- El tráfico de voz requiere al menos 30 Kbps de ancho de banda.

Características del tráfico de voz	Requerimientos de sentido único
• Fluida • Favorable • Sensible a las caídas • Sensible al retraso • Prioridad UPD	• Latencia ≤ 150 ms • Jitter ≤ 30 ms • Pérdida ≤ 1% ancho de banda (30-128 Kbps)

Características del tráfico

Video

El tráfico de video tiende a ser impredecible, inconsistente y explosivo. En comparación con la transmisión de voz, el video es menos resistente a pérdidas y tiene un mayor volumen de datos por paquete.

- La cantidad y el tamaño de los paquetes de video varían cada 33 ms según el contenido del video.
- Los puertos UDP, como el 554, se utilizan para el Protocolo de transmisión en tiempo real (RSTP) y se les debe dar prioridad sobre otro tráfico de red menos sensible al retraso.
- La latencia no debe ser superior a 400 milisegundos (ms). El jitter no deben ser de más de 50 ms, y la pérdida de paquetes de video no debe ser superior al 1%. El tráfico de video requiere al menos 384 Kbps de ancho de banda.

Características del tráfico de video	Requisitos unidireccionales
• Explosivo • Codicioso • Sensible a las caídas • Sensible al retraso • Prioridad UPD	• Latencia ≤ 200-400 ms • Jitter ≤ 30-50 ms • Pérdida ≤ 0.1 – 1% • BandwidthAncho de banda (384 Kbps - 20 Mbps)

Características del tráfico

Datos

Las aplicaciones de datos que no toleran la pérdida de datos, como el correo electrónico y las páginas web, utilizan TCP para garantizar que si los paquetes se pierden en tránsito, se reenviarán.

- El tráfico de datos puede ser fluido o puede tener estallidos.
- El tráfico de control de red generalmente es elegante y predecible.

Algunas aplicaciones TCP pueden consumir una gran parte de la capacidad de la red. El FTP ocupará tanto ancho de banda como pueda obtener cuando usted descargue un archivo grande, como una película o un juego.

Características del tráfico de datos
• Suave/explosivo • Benigno /codicioso • Insensible a las caídas • Insensible al retraso • Retransmisiones de TCP

Características del tráfico

Datos

El tráfico de datos es relativamente insensible a las caídas y demoras en comparación con la voz y el video. La calidad de la experiencia o QoE es importante tener en cuenta con el tráfico de datos.

- ¿Los datos provienen de una aplicación interactiva?
- ¿Es la misión de datos crítica?

Factor	Misión crítica	Misión no crítica
Interactivo	Prioriza la demora más baja de todo el tráfico de datos y se esfuerza por un tiempo de respuesta de 1 a 2 segundos.	Las aplicaciones podrían beneficiarse con una demora más baja.
No interactivo	La demora puede variar enormemente siempre que se suministre el ancho de banda mínimo necesario.	Obtiene cualquier ancho de banda sobrante una vez que hayan satisfecho todas las necesidades de voz, video y de otras aplicaciones de datos.

Algoritmos de puesta en cola

Resumen de colas

La política de la QoS implementada por el administrador de la red se activa cuando se produce una congestión en el enlace. La puesta en cola es una herramienta administrativa para la congestión que puede almacenar en búfer, priorizar, y, si corresponde, reordenar los paquetes antes de que estos se transmitan al destino.

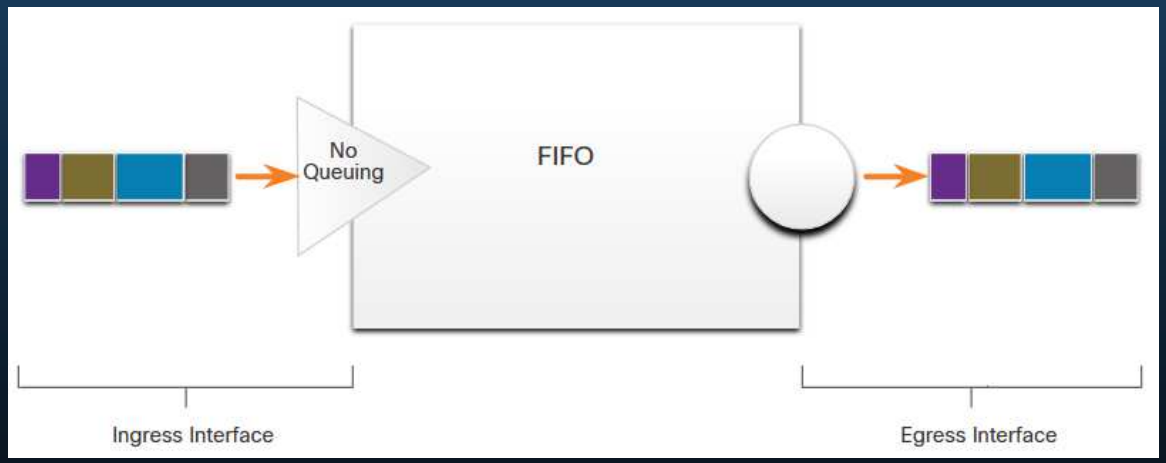
Hay varios algoritmos de colas disponibles:

- Primero en entrar, primero en salir (FIFO)
- Mecanismo de cola equitativo ponderado (WFQ)
- Mecanismo de cola de espera equitativo y ponderado basado en clases (CBWFQ)
- Mecanismo de cola de baja latencia (LLQ)

Algoritmos de puesta en cola

Primero en entrar, primero en salir

- Primero en entrar, primero en salir (FIFO) almacenando buffers y reenviando paquetes en el orden de llegada.
- FIFO no tiene concepto de prioridad ni clases de tráfico, por lo que no toma decisiones sobre la prioridad de los paquetes.
- Hay una sola cola, y todos los paquetes se tratan por igual.
- Los paquetes se envían a una interfaz en el orden de llegada.

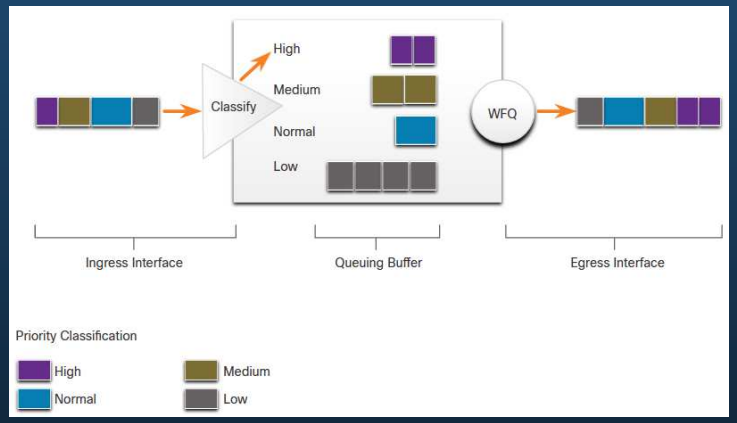


Algoritmos de puesta en cola

Mecanismo de cola equitativo ponderado (WFQ)

Las colas justas ponderadas (WFQ) son un método de programación automatizado que proporciona una asignación justa de ancho de banda a todo el tráfico de red.

- WFQ aplica prioridad, o pesos, al tráfico identificado, lo clasifica en conversaciones o flujos y, a continuación, determina cuánto ancho de banda se permite cada flujo en relación con otros flujos.
- WFQ clasifica el tráfico en diferentes flujos según las direcciones IP de origen y destino, las direcciones MAC, los números de puerto, el protocolo y el valor del Tipo de servicio (ToS).
- WFQ no se utiliza con los túneles y el encriptado porque estas funciones modifican la información de contenido de paquete requerida por WFQ para la clasificación.



Algoritmos de puesta en cola

Mecanismo de Cola de Espera Equitativo y Ponderado Basado en Clases (CBWFQ)

La ponderación equitativa ponderada basada en clases (CBWFQ) amplía la funcionalidad estándar WFQ para proporcionar soporte para las clases de tráfico definidas por el usuario.

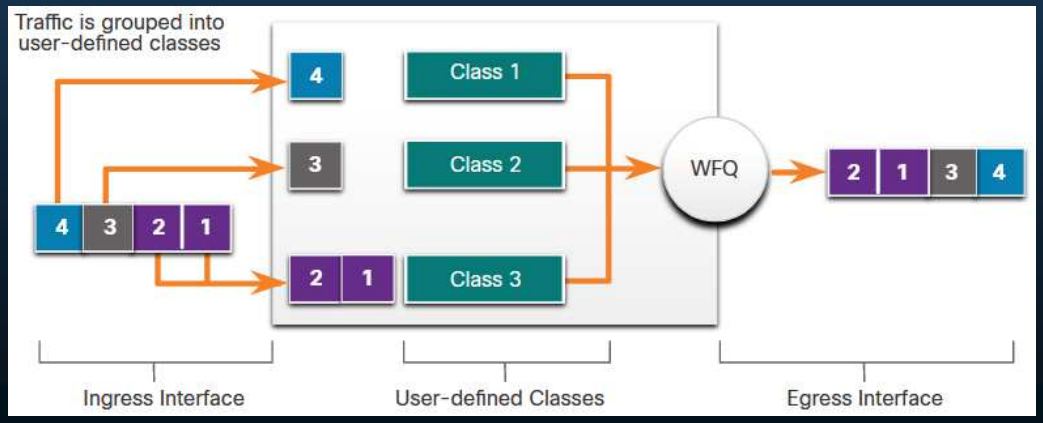
- Las clases de tráfico se definen en función de criterios de coincidencia que incluyen protocolos, listas de control de acceso (ACL) e interfaces de entrada.
- Los paquetes que cumplen los criterios de coincidencia para una clase constituyen el tráfico para esa clase.
- Se reserva una cola FIFO para cada clase, y el tráfico que pertenece a una clase se dirige a la cola para esa clase.
- Se pueden asignar características a una clase, como ancho de banda, peso y límite máximo de paquetes. El ancho de banda asignado a una clase es el ancho de banda garantizado entregado durante la congestión.
- Los paquetes que pertenecen a una clase están sujetos a los límites de ancho de banda y de cola, que es el número máximo de paquetes que se permite acumular en la cola, que caracterizan a la clase.

Algoritmos de puesta en cola

Mecanismo de Cola de Espera Equitativo y Ponderado Basado en Clases (CBWFQ)

Una vez que una cola haya alcanzado su límite de cola configurado, el agregado de más paquetes a la clase hace que surtan efecto el descarte de cola o el descarte de paquetes, según cómo esté configurada la política de clase.

- La caída de cola descarta cualquier paquete que llegue al final de una cola que haya agotado completamente sus recursos de retención de paquetes.
- Esta es la respuesta de espera predeterminada para la congestión. El descarte de extremo final trata a todo el tráfico de la misma manera y no diferencia entre clases de servicios.

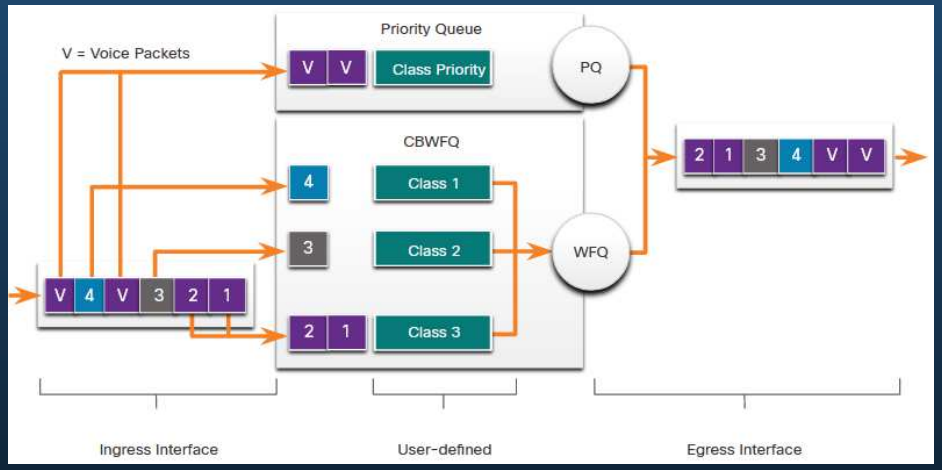


Algoritmos de puesta en cola

Mecanismo de cola de baja latencia (LLQ)

La función de cola de baja latencia (LLQ) trae cola de prioridad estricta (PQ) a CBWFQ.

- La estricta PQ permite que los paquetes sensibles al retraso, como la voz, se envíen antes que los paquetes en otras colas.
- LLQ permite que los paquetes sensibles al retraso, como la voz, se envíen primero (antes que los paquetes en otras colas), dando a los paquetes sensibles al retraso un tratamiento preferencial sobre otro tráfico.
- Cisco recomienda que sólo el tráfico de voz se dirija a la cola de prioridad.



Modelos de QoS

Selección de un modelo adecuado de política de la QoS

Existen tres modelos para implementar QoS. QoS se implementa en una red utilizando IntServ o DiffServ.

- IntServ ofrece la mayor garantía de QoS, requiere muchos recursos y, por lo tanto, no es fácilmente escalable.
- DiffServ requiere menos recursos y es más escalable.
- IntServ y DiffServ a veces se implementan conjuntamente en implementaciones de QoS de red.

Modelo	Descripción
Modelo de mejor esfuerzo	• No es una implementación ya que QoS no está configurado explícitamente. • Se utiliza cuando no se requiere QoS.
Servicios integrados (IntServ)	• Proporciona QoS muy alta a los paquetes de IP con garantía de entrega. • Define un proceso de señalización para que las aplicaciones envíen señales a la red que requieren QoS especiales durante un período y que el ancho de banda debe reservarse. • IntServ puede limitar severamente la escalabilidad de una red.
Servicios diferenciados (DiffServ)	• Proporciona alta escalabilidad y flexibilidad en la implementación de QoS. • Los dispositivos de red reconocen las clases de tráfico y proporcionan distintos niveles de QoS a diferentes clases de tráfico.

Modelos de QoS

Mejor Esfuerzo

El diseño básico de Internet es la entrega de paquetes de mejor esfuerzo y no ofrece garantías.

- El modelo de mejor esfuerzo trata todos los paquetes de red de la misma manera, por lo que un mensaje de voz de emergencia se trata de la misma manera que se trata una fotografía digital adjunta a un correo electrónico.
- Beneficios e inconvenientes del modelo de mejor esfuerzo:

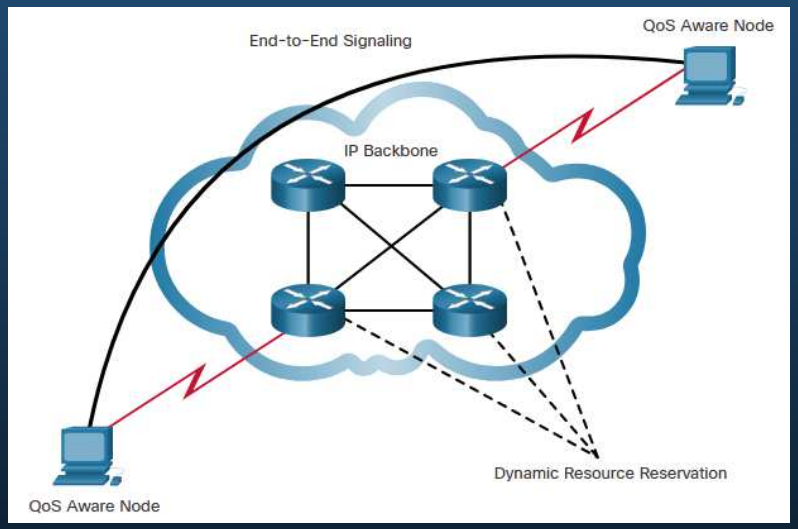
Beneficios	Desventajas
Este modelo es el más escalable.	No hay garantías de entrega.
La escalabilidad solo está limitada por el ancho de banda disponible, en cuyo caso todo el tráfico se ve igualmente afectado.	Los paquetes llegarán cuando puedan y en cualquier orden posible, si es que llegan.
No se requieren mecanismos de QoS especiales.	Ningún paquete tiene trato preferencial.
Es el modelo más fácil y rápido de implementar.	Los datos críticos se tratan del mismo modo que el correo electrónico informal.

Modelos de QoS

Servicios integrados

IntServ ofrece la QoS end-to-end que requieren las aplicaciones en tiempo real.

- Administra explícitamente los recursos de red para proporcionar QoS a flujos o flujos individuales, a veces denominados microflujos.
- Utilizan la reserva de recursos y mecanismos de control de admisión como módulos de construcción para establecer y mantener la QoS.
- Utiliza un enfoque orientado a la conexión. Cada comunicación individual debe especificar explícitamente su descriptor de tráfico y los recursos solicitados a la red.
- El router perimetral realiza el control de admisión para garantizar que los recursos disponibles son suficientes en la red.



Modelos de QoS

Servicios diferenciados

En el modelo de IntServ, la aplicación solicita a un tipo específico de servicio a la red antes de enviar datos.

- La aplicación informa a la red su perfil de tráfico y solicita a un tipo particular de servicio que puede abarcar requisitos de ancho de banda y retraso.
- IntServ utiliza el Protocolo de reserva de recursos (RSVP) para señalar las necesidades de la QoS del tráfico de una aplicación junto con los dispositivos en la ruta de extremo a extremo a través de la red.
- Si los dispositivos de red a lo largo de la ruta pueden reservar el ancho de banda necesario, la aplicación de origen puede comenzar a transmitir. Si reserva solicitada falla a lo largo de la ruta, la aplicación de origen no envía ningún dato.

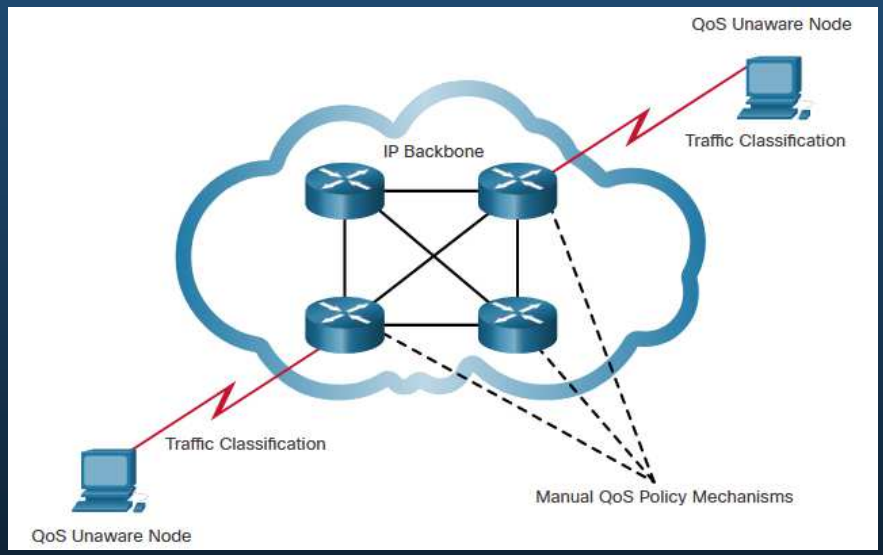
Beneficios	Desventajas
• Control explícito de admisión de recursos de extremo a extremo • Control de admisión de políticas por solicitud • Señalización de números de puerto dinámicos	• Uso intensivo de recursos debido al requisito de arquitectura activa para la señalización continua. • Enfoque basado en el flujo no escalable a grandes implementaciones como Internet.

Modelos de QoS

Servicios diferenciados

El modelo de QoS de servicios diferenciados (DiffServ) específica un mecanismo simple y escalable para clasificar y gestionar el tráfico de red.

- No es una estrategia de QoS de extremo a extremo porque no puede hacer cumplir las garantías de extremo a extremo.
- Los hosts reenvían el tráfico a un router que clasifica los flujos en agregados (clases) y proporciona la política de QoS adecuada para las clases.
- Refuerza y aplica mecanismos de QoS salto por salto, aplicando de manera uniforme el significado global a cada clase de tráfico para proporcionar flexibilidad y escalabilidad.



Modelos de QoS

Servicios diferenciados

- DiffServ divide el tráfico de red en clases según los requisitos de la empresa. Se puede asignar a un nivel diferente de servicio a cada una de las clases.
- A medida que los paquetes atraviesan una red, cada uno de los dispositivos de red identifica la clase de paquete y brinda servicios al paquete según esa clase.
- Con DiffServ, es posible elegir muchos niveles de servicio.

Beneficios	Desventajas
• Gran escalabilidad • Proporciona distintos niveles de calidad	• Sin garantía absoluta de la calidad del servicio • Requiere un conjunto de mecanismos complejos para trabajar en conjunto en la red

Técnicas de implementación de QoS

Prevención de la pérdida de paquetes

La pérdida de paquetes es generalmente el resultado de la congestión en una interfaz. La mayoría de las aplicaciones que utilizan el TCP experimentan una disminución de velocidad debido a que el TCP se ajusta automáticamente a la congestión en la red. Los segmentos caídos del TCP hacen que las sesiones del TCP reduzcan su tamaño de ventana. Algunas aplicaciones no utilizan TCP y no pueden manejar las caídas (flujos frágiles).

Los enfoques siguientes pueden prevenir los descartes en las aplicaciones sensibles:

- Aumenta la capacidad de enlace para facilitar o evitar la congestión.
- Garantiza el suficiente ancho de banda y aumenta el espacio en búfer para acomodar las ráfagas de tráfico de flujos frágiles. WFQ, CBWFQ y LLQ pueden garantizar ancho de banda y proporcionar reenvío priorizado a aplicaciones sensibles a caídas.
- Los paquetes de baja prioridad de descartan antes de que se presente la congestión. Cisco IOS QoS proporciona mecanismos de colas, como la detección temprana aleatoria ponderada (WRED), que comienzan a descartar paquetes de menor prioridad antes de que ocurra la congestión.

Técnicas de implementación de QoS

Herramientas de QoS

Hay tres categorías de herramientas de QoS, como se describe en la tabla.

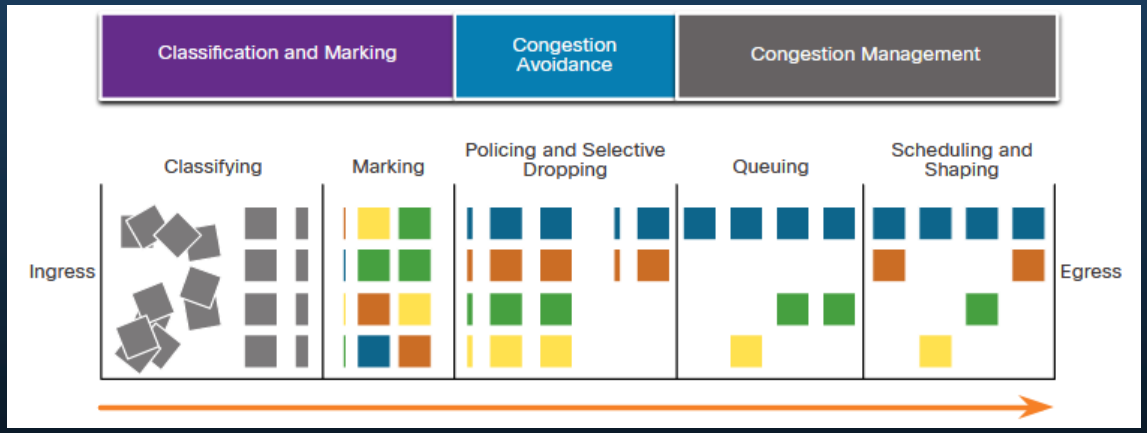
Herramientas de QoS	Descripción
Herramientas de clasificación y marcación	• Las sesiones, o flujos, se analizan para determinar a qué clase de tráfico pertenecen. • Cuando se determina la clase de tráfico, se marcan los paquetes.
Herramientas para evitar la congestión	• A las clases de tráfico se les asignan porciones de recursos de red según lo definido por la política de QoS. • La política de QoS también identifica cómo se puede descartar, demorar o volver a marcar selectivamente parte del tráfico para evitar la congestión. • La herramienta principal para evitar la congestión es WRED y se utiliza para regular el tráfico de datos del TCP de manera eficiente según el ancho de banda antes de que se descarten paquetes en la cola ocasionadas debido a desbordamientos de la cola.
Herramientas de administración de congestión	• Cuando el tráfico excede los recursos de red disponibles, el tráfico se pone en cola para esperar la disponibilidad de recursos. • Las herramientas comunes de administración de congestión basadas en Cisco IOS incluyen los algoritmos CBWFQ y LLQ.

Técnicas de implementación de QoS

Herramientas de QoS

La figura muestra la secuencia de herramientas de QoS utilizadas cuando se aplica a los flujos de paquetes.

- Los paquetes de entrada se clasifican y su encabezado IP respectivo está marcado.
- Para evitar la congestión, luego se asignan recursos a los paquetes en base a las políticas definidas.
- Los paquetes son luego puestos en la cola y reenviados a la interfaz de egreso según la política definida de modelado y regulación de tráfico de la QoS.



Nota: La clasificación y el marcado se pueden realizar en la entrada o salida, mientras que otras acciones de QoS, como la formación de colas y la configuración, generalmente se realizan en la salida.

Técnicas de implementación de QoS

Clasificación y Marcación

Antes de que a un paquete se le pueda aplicar una política de la QoS, el mismo tiene que ser clasificado.

La clasificación determina la clase de tráfico al cual los paquetes o tramas pertenecen. Solo pueden aplicarse las políticas al tráfico después del marcado.

Cómo se clasifica un paquete depende de la implementación de la QoS.

- Los métodos de clasificación de flujos de tráfico en la capa 2 y 3 incluyen el uso de interfaces, ACL y mapas de clase.
- El tráfico también se puede clasificar en las capas 4 a 7 mediante el uso del Reconocimiento de Aplicaciones Basado en la Red (NBAR).

Técnicas de implementación de QoS

Clasificación y marcación

La forma en la que se marca el tráfico generalmente depende de la tecnología. La decisión de marcar el tráfico de las capas 2 o 3 (o ambos) no es despreciable y debe tomarse tras considerar los siguientes puntos:

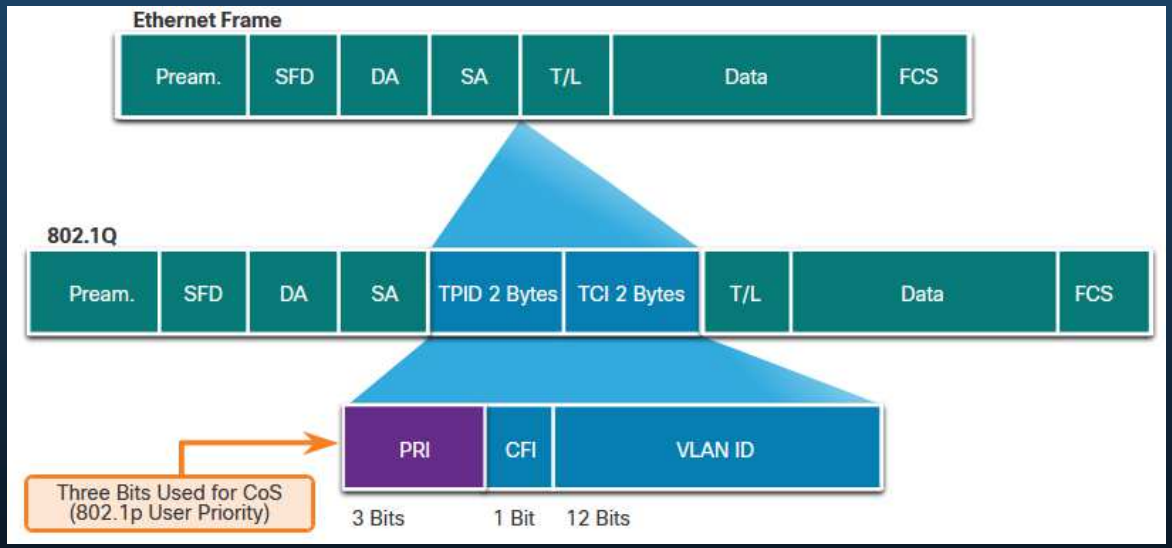
- Se puede marcar la Capa 2 de las tramas para el tráfico no IP.
- El marcado en la capa 2 de las tramas es la única opción de la QoS disponible para los switches que no tienen "reconocimiento de IP".
- El marcado de Capa 3 llevará la información de la QoS de extremo a extremo.

Herramientas de QoS	Capa	Campo de marcación	Ancho en bits
Ethernet (802.1q, 802.1p)	2	Clase de servicio (CoS)	3
802.11 (Wi-Fi)	2	Identificador de tráfico (TID) de Wi-Fi	3
MPLS	2	Experimental (EXP)	3
IPv4 e IPv6	3	Precedencia de IP (IPP)	3
IPv4 e IPv6	3	Punto de código de servicios diferenciados (DSCP)	6

Técnicas de implementación de QoS

Marcación en la capa 2

802.1Q es el estándar IEEE que admite etiquetado VLAN en la capa 2 de las redes Ethernet. Cuando se implementa 802.1Q, se insertan dos campos en la trama Ethernet que sigue al campo de la dirección MAC de origen.



Técnicas de implementación de QoS

Marcación en la capa 2

El estándar 802.1Q también incluye el esquema de priorización de la QoS conocido como IEEE 802.1p. El estándar 802.1p usa los tres primeros bits del campo de información de control de etiqueta (TCI). Conocido como campo de prioridad (PRI), este campo de 3 bits identifica las marcas de clase de servicio (CoS).

Tres bits significa que una trama Ethernet de capa 2 se puede marcar con uno de los ocho niveles de prioridad (valores 0-7).

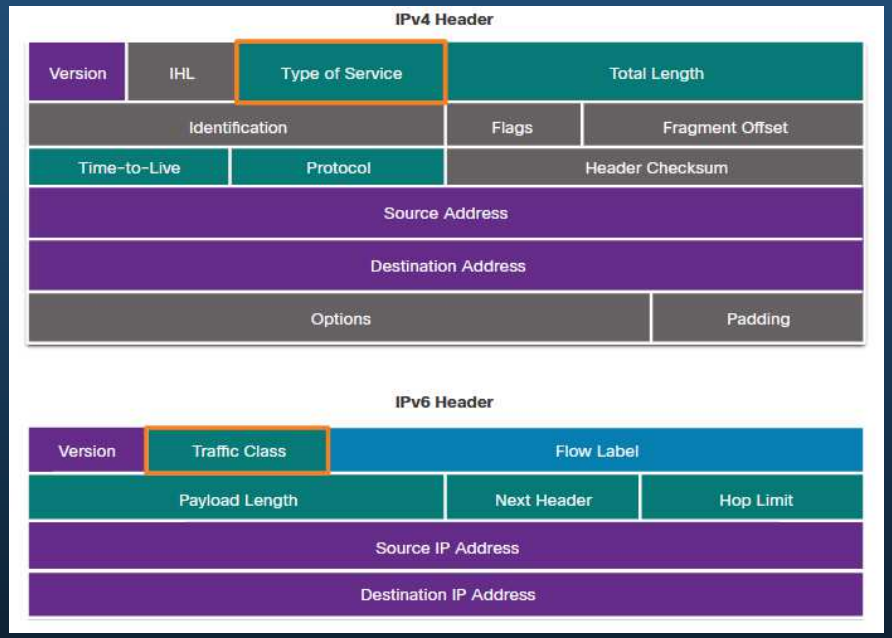
Valor de CoS	Valor binario de CoS	Descripción
0	000	Datos de mejor esfuerzo
1	001	Datos de prioridad media
2	010	Datos de alta prioridad
3	011	Señalización de llamadas
4	100	Videoconferencia
5	101	Portador de voz (tráfico de voz)
6	110	Reservado
7	111	Reservado

Técnicas de implementación de QoS

Marcación en la capa 3

IPv4 e IPv6 especifican un campo de 8 bits en sus encabezados de paquetes para marcar los paquetes.

Tanto IPv4 como IPv6 admiten un campo de 8 bits para marcar: el campo Tipo de servicio (ToS) para IPv4 y el campo Clase de tráfico para IPv6.

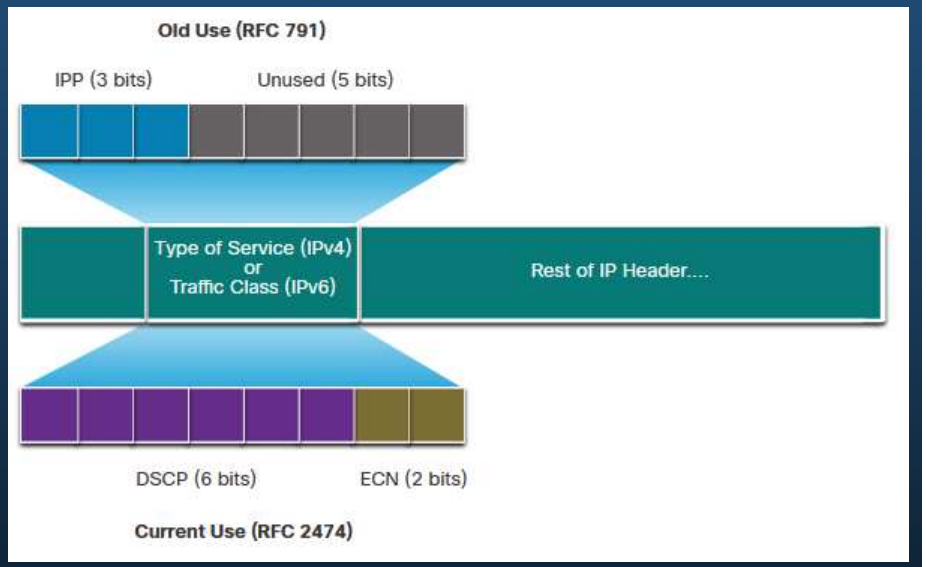


Técnicas de implementación de QoS

Tipo de servicio y campo de clase de tráfico

El tipo de servicio (IPv4) y la clase de tráfico (IPv6) llevan el marcado de paquetes según lo asignado por las herramientas de clasificación de QoS.

- RFC 791 especificó el campo de precedencia de IP de 3 bits (IPP) que se utilizará para las marcas de QoS.
- RFC 2474 reemplaza a RFC 791 y redefine el campo ToS renombrando y extendiendo el campo IPP a 6 bits.
- Conocido como campo de punto de código de servicios diferenciados (DSCP), estos seis bits ofrecen un máximo de 64 clases de servicio posibles.
- Los dos bits restantes de notificación de congestión extendida (ECN) de IP pueden usarse en los routers con reconocimiento de ECN para marcar paquetes en vez de descartarlos.



Técnicas de implementación de QoS

Valores DSCP

Los 64 valores de DSCP se organizan en tres categorías:

- **Mejor esfuerzo (BE)** - Este es el valor predeterminado para todos los paquetes IP. El valor de DSCP es 0. El comportamiento por salto es enrutamiento normal. Cuando un router experimenta congestión, estos paquetes se descartan. No se implementa plan de la QoS.
- **Reenvío Acelerado (EF)** - RFC 3246 define EF como el valor decimal DSCP 46 (binario**101**110). Los primeros 3 bits (101) se asocian directamente al valor 5 de CoS de capa 2 que se utiliza para el tráfico de voz. En la capa 3, Cisco recomienda que EF solo se use para marcar paquetes de voz.
- **Reenvío asegurado (AF)** - Reenvío asegurado (AF): RFC 2597 define el AF para usar los 5 bits DSCP más significativos para indicar las colas y la preferencia de descarte.

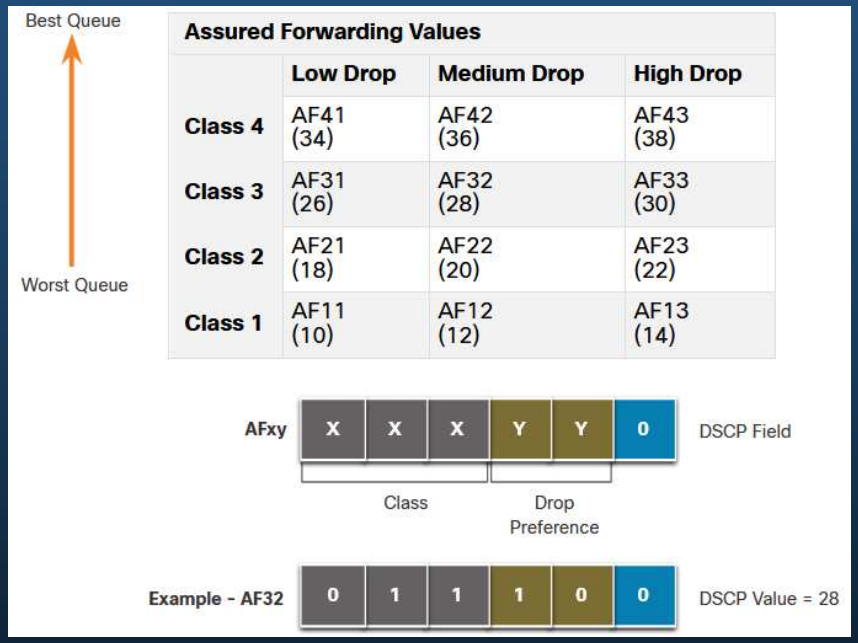
Técnicas de implementación de QoS

Valores DSCP

Los valores de reenvío asegurado se muestran en la figura.

La fórmula **AFXy** se especifica de la siguiente manera:

- Los primeros 3 bits más significativos se utilizan para designar la clase. La clase 4 es la mejor cola y la clase 1 es la peor.
- El 4to y 5to bit más significativos se usan para indicar la preferencia de descarte.
- El 6to bit más significativo se establece en cero.



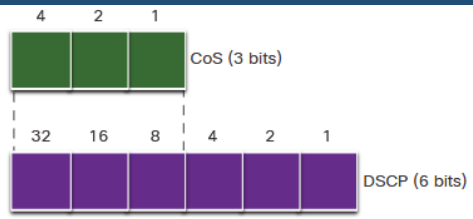
Por ejemplo: AF32 pertenece a la clase 3 (binario 011) y tiene una preferencia de caída media (binario 10). El valor de DSCP completo es 28 porque se incluye el 6to bit en 0 (binario 011100).

Técnicas de implementación de QoS

Bits selectores de clase

Bits de selector de clase (CS):

- Los primeros 3 bits más significativos del campo DSCP e indican la clase.
- Asigne directamente a los 3 bits del campo CoS y el campo IPP para mantener la compatibilidad con 802.1p y RFC 791.



CoS values, Class Selectors, and corresponding DSCP 6-bit value

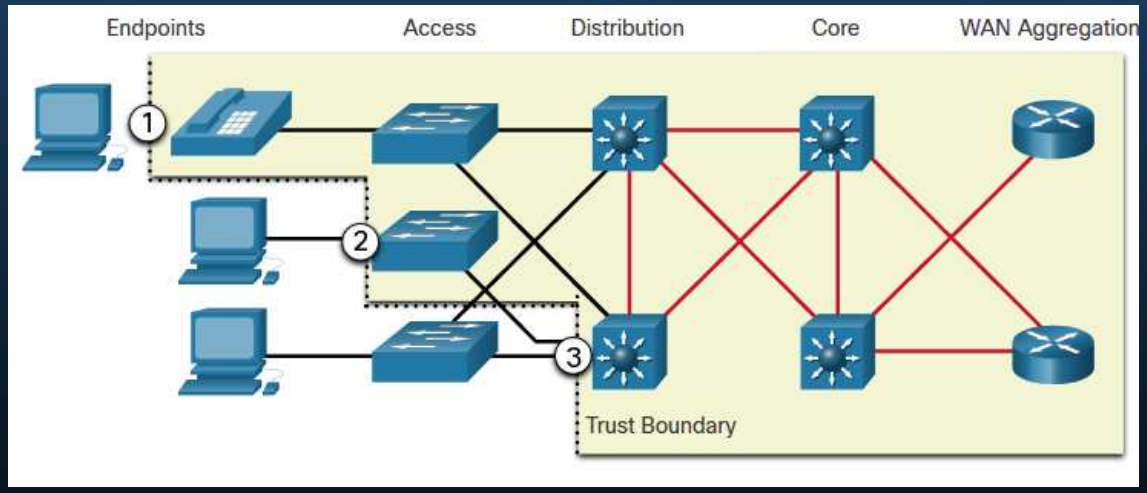
CoS Value	CoS Binary Value	Class Selector (CS)	CS Binary	DSCP Decimal Value
0	000	CS0*/DF	000 000	0
1	001	CS1	001 000	8
2	010	CS2	010 000	16
3	011	CS3	011 000	24
4	100	CS4	100 000	32
5	101	CS5	101 000	40
6	110	CS6	110 000	48
7	111	CS7	111 000	56

Técnicas de implementación de QoS

Límites de confianza

El tráfico se debe clasificar y marcar lo más cerca su origen como sea técnicamente y administrativamente posible. Esto define el límite de confianza.

1. Los terminales confiables tienen las capacidades y la inteligencia para marcar el tráfico de aplicaciones con las CoS de capa 2 apropiadas y/o los valores de DSCP de la Capa 3.
2. Los terminales seguros pueden hacer que el tráfico se marque en el switch de la capa 2.
3. El tráfico también puede marcarse en los switches/routers de la capa 3.



Técnicas de implementación de QoS

Prevención de la congestión

Las herramientas para evitar la congestión monitorean las cargas de tráfico de la red en un esfuerzo por anticipar y evitar la congestión en la red común y los cuellos de botella entre redes antes de que la congestión se convierta en un problema.

- Las cargas de tráfico de la red, en un esfuerzo por anticipar y evitar la congestión en los cuellos de botella de la red común y de internetwork antes de que la congestión se convierta en un problema.
- Ellas monitorean la profundidad promedio de la cola. Cuando la cola está por debajo del umbral mínimo, no hay descartes. A medida que la cola alcanza el umbral máximo, se descarta un pequeño porcentaje de paquetes. Cuando se supera el umbral máximo, se descartan todos los paquetes.

Algunas técnicas para evitar la congestión brindan un tratamiento preferencial para el cual los paquetes se descartan.

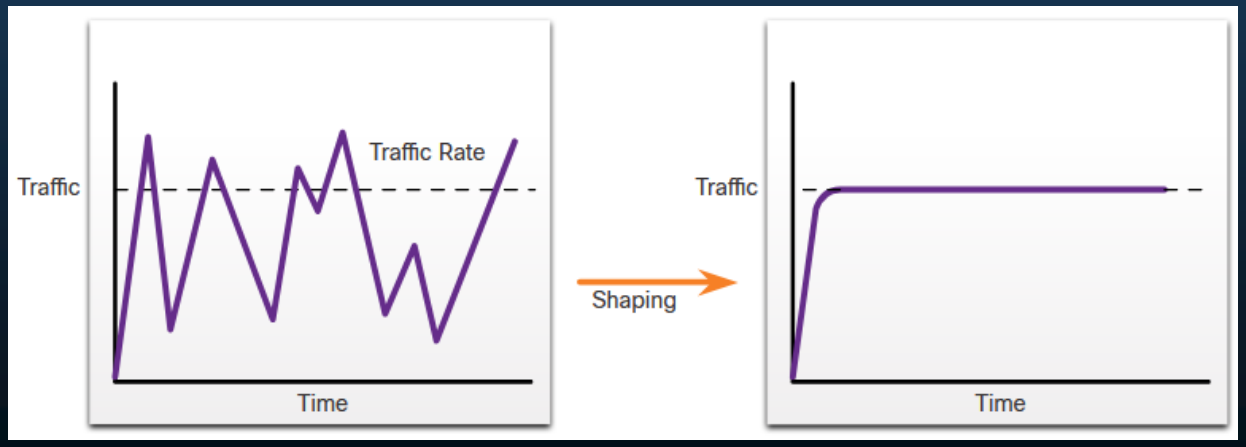
- La detección temprana aleatoria ponderada (WRED) permite evitar la congestión en las interfaces de red al proporcionar una gestión de la memoria intermedia y permitir que el tráfico TCP disminuya o se acelere antes de que se agoten las memorias intermedias.
- WRED ayuda a evitar caídas de cola y maximiza el uso de la red y el rendimiento de las aplicaciones basadas en TCP.

Técnicas de implementación de QoS

Modelado y políticas

Las políticas de modelado y de vigilancia del son dos mecanismos proporcionados por el software Cisco IOS QoS para evitar la congestión.

- El modelado del tráfico conserva los paquetes en exceso en una cola y luego programa el exceso para la transmisión posterior en incrementos de tiempo. El modelado del tráfico da como resultado una tasa de salida de paquetes suavizada.
- El modelado es un concepto saliente; los paquetes que salen de una interfaz se almacenan en cola y pueden modelarse. Por el contrario, la vigilancia se aplica al tráfico entrante de la interfaz.



Técnicas de implementación de QoS

Moldear y vigilar

Se puede aplicar la vigilancia al tráfico entrante en una interfaz. Los proveedores de servicios suelen implementar la vigilancia para aplicar una tasa de información de clientes (CIR) por contrato. Sin embargo, el proveedor de servicios también puede permitir el estallido por CIR si la red del proveedor de servicios no tiene congestión en la actualidad.

Técnicas de implementación de QoS

Pautas de política de QoS

Las directivas QoS deben tener en cuenta la ruta completa desde el origen hasta el destino.

Algunas pautas que ayudan a garantizar la mejor experiencia para los usuarios finales incluyen las siguientes:

- Habilite la puesta en cola en todos los dispositivos de la ruta entre el origen y el destino.
- Clasifique y marque el tráfico lo más cerca posible de la fuente.
- Modele (Shape) y controle (police) el flujo del tráfico tan cerca del origen como sea posible

Capítulo 10

Administración de redes

Detección de dispositivos con CDP

Descripción general de CDP

CDP es un protocolo de Capa 2 propiedad de Cisco que se utiliza para recopilar información sobre dispositivos Cisco que comparten el mismo enlace de datos. El CDP es independiente de los medios y protocolos y se ejecuta en todos los dispositivos Cisco, como routers, switches y servidores de acceso.

El dispositivo envía mensajes periódicos del CDP a los dispositivos conectados. Estos mensajes comparten información sobre el tipo de dispositivo que se descubre, el nombre de los dispositivos, y la cantidad y el tipo de interfaces.

Detección de dispositivos con CDP

Configuración y verificación del CDP

- Para los dispositivos Cisco, el CDP está habilitado de manera predeterminada. Para verificar el estado de CDP y mostrar información sobre CDP, ingrese el comando **show cdp** .
- Para deshabilitar CDP en una interfaz específica, ingrese **no cdp enable** en el modo de configuración de la interfaz. El CDP aún se encuentra habilitado en el dispositivo; sin embargo, no se enviarán más mensajes a la interfaz. Para habilitar CDP en la interfaz específica nuevamente, ingrese **cdp enable.**
- Para habilitar CDP globalmente para todas las interfaces compatibles en el dispositivo, ingrese **cdp run** en el modo de configuración global. CDP se puede deshabilitar para todas las interfaces en el dispositivo con el comando **no cdp run** en el modo de configuración global.
- Utilice el comando **show cdp interface** para mostrar las interfaces que están habilitadas en CDP en el dispositivo. También se muestra el estado de cada interfaz.

Detección de dispositivos con CDP

Detección de dispositivos mediante CDP

- Con CDP habilitado en la red, el comando **show cdp neighbors** se puede usar para determinar el diseño de la red, como se muestra en el ejemplo.
- La salida muestra que hay otro dispositivo Cisco, S1, conectado a la interfaz G0/0/1 en R1. Además, S1 está conectado a través de su F0/5

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                                  S - Switch, H - Host, I - IGMP, r -
Repeater, P - Phone,
                                  D - Remote, C - CVTA, M - Two-port Mac
Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
S1 Gig 0/0/1 179 S I WS-C3560- Fas 0/5
```

Detección de dispositivos con CDP

Detección de dispositivos mediante CDP

El administrador de red utiliza **show cdp neighbors detail** para descubrir la dirección IP de S1. Como se muestra en la salida, la dirección de S1 es 192.168.1.2.

```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C3560-24TS, Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

(output omitted)
```

Detección de dispositivos con LLDP

Descripción general de LLDP

El protocolo de detección de capa de enlace (LLDP) es un protocolo de detección de vecinos similar al CDP que es independiente del proveedor. El LLDP funciona con los dispositivos de red, como routers, switches, y puntos de acceso inalámbrico LAN. Este protocolo anuncia su identidad y capacidades a otros dispositivos y recibe la información de un dispositivo de capa 2 conectado físicamente.

Detección de dispositivos con LLDP

Configuración y verificación del LLDP

- LLDP puede estar habilitado por defecto. Para habilitar LLDP a nivel global en un dispositivo de red Cisco, ingrese el comando **lldp run** en el modo de configuración global. Para deshabilitar el LLDP, ingrese el comando **no lldp run** en el modo de configuración global.
- LLDP se puede configurar en interfaces específicas. Sin embargo, LLDP debe configurarse por separado para transmitir y recibir paquetes LLDP.
- Para verificar que LLDP esté habilitado, ingrese el comando **show lldp** en modo EXEC privilegiado.

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
Switch# show lldp
Global LLDP Information:
   Status: ACTIVE
   LLDP advertisements are sent every 30 seconds
   LLDP hold time advertised is 120 seconds
   LLDP interface reinitialisation delay is 2 seconds
```

Detección de dispositivos con LLDP

Detección de dispositivos mediante LLDP

Con LLDP habilitado, los vecinos del dispositivo se pueden descubrir mediante el comando **show lldp neighbors** .

```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID Local Intf Hold-time Capability Port ID
R1 Fa0/5 117 R Gi0/0/1
S2 Fa0/1 112 B Fa0/1
Total entries displayed: 2
```

Detección de dispositivos con LLDP

Detección de dispositivos mediante LLDP

Cuando se necesitan más detalles sobre los vecinos, el comando **show lldp neighbors detail** puede proporcionar información, como la versión del IOS vecino, la dirección IP y la capacidad del dispositivo.

```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id: 848a.8d44.49b0
Port id: Gi0/0/1
Port Description: GigabitEthernet0/0/1
System Name: R1
System Description: Cisco IOS Software [Fuji], ISR Software (X86_64_LINUX_.....,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:09 by mcpre

Time remaining: 111 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses - not advertised
(output omitted)
```

NTP

Servicios de Tiempo y Calendario

- El reloj del software en un router o un switch se inicia cuando se inicia el sistema. Es la principal fuente de tiempo para el sistema. Es importante sincronizar la hora en todos los dispositivos de la red. Cuando no se sincroniza la hora entre los dispositivos, será imposible determinar el orden de los eventos y la causa de un evento.
- Normalmente, la configuración de fecha y hora de un router o switch se puede establecer mediante uno de los dos métodos. Puede configurarse manualmente la fecha y la hora, como se muestra en el ejemplo, o configurar el Protocolo de tiempo de red (NTP).

```
R1# clock set 20:36:00 nov 15 2019
R1#
*Nov 15 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been
updated from 21:32:31 UTC Fri Nov 15 2019 to 20:36:00 UTC Fri Nov 15
2019, configured from console by console.
```

NTP

Servicios detiempo y calendario NTP

A medida que la red crece, se hace difícil garantizar que todos los dispositivos de infraestructura estén funcionando con tiempo sincronizado utilizando el método manual.

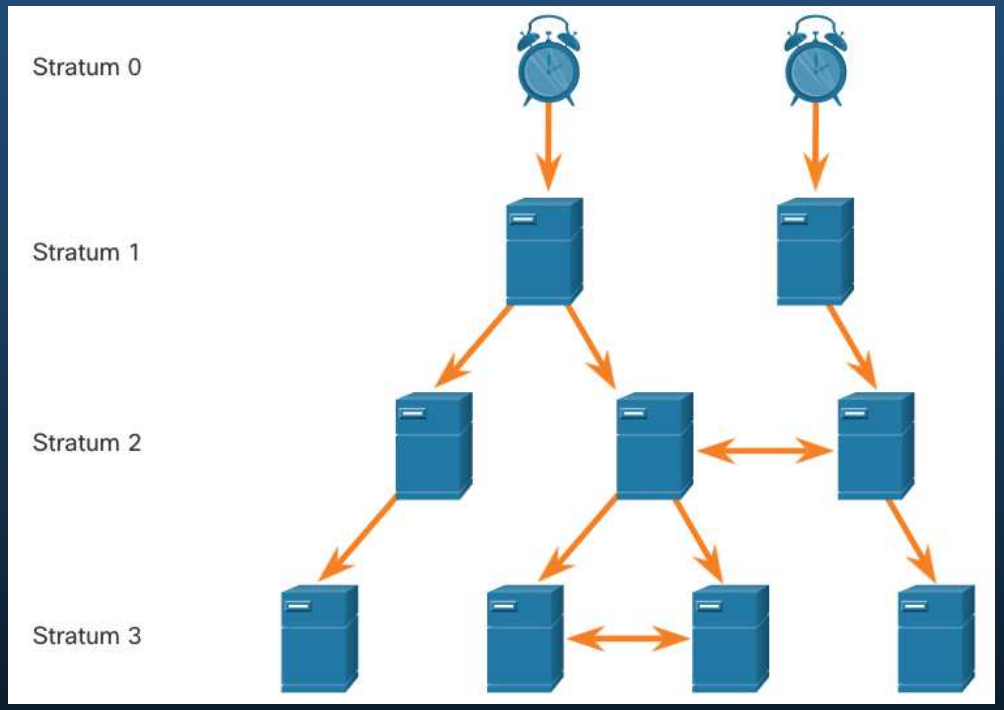
Una mejor solución es configurar el NTP en la red. Este protocolo permite a los routers de la red sincronizar sus configuraciones de hora con un servidor NTP, lo que proporciona configuraciones de hora más consistentes. NTP puede configurarse para sincronizarse con un reloj maestro privado, o puede sincronizarse con un servidor NTP disponible públicamente en Internet. NTP utiliza el puerto 123 de UDP y se documenta en RFC 1305.

NTP

Operación NTP

Las redes NTP utilizan un sistema jerárquico de fuentes horarias. Cada nivel en este sistema jerárquico se denomina estrato. El nivel de estrato se define como la cantidad de saltos desde la fuente autorizada. El tiempo sincronizado se distribuye a través de la red mediante NTP.

El recuento de saltos máximo es 15. El estrato 16, el nivel de estrato inferior, indica que un dispositivo no está sincronizado.



NTP

Operación NTP

- **Stratum 0:** Estas "fuentes de tiempo autorizadas" son dispositivos de cronometraje de alta precisión que se supone son precisos y con poco o ningún retraso asociado con ellos.
- **Stratum 1:** Dispositivos que están directamente conectados a las fuentes de tiempo autorizadas. Actúan como el estándar horario de la red principal.
- **Stratum 2 e inferiores:** los servidores del estrato 2 están conectados a los dispositivos del estrato 1 a través de conexiones de red. Los dispositivos de stratum 2, como los clientes NTP, sincronizan su tiempo utilizando los paquetes NTP de los servidores de stratum 1. Podrían también actuar como servidores para dispositivos del stratum 3.

Los servidores en el mismo nivel de Stratum, pueden configurarse para actuar como un par con otros servidores horarios en el mismo nivel de estratos, esto con la finalidad de verificar o respaldar el horario.

NTP

Configuración y verificación del NTP

- Antes de configurar NTP en la red, el comando **show clock** muestra la hora actual en el reloj del software. Con la opción de **detail** , observe que la fuente de tiempo es la configuración del usuario. Esto significa que la hora se configuró manualmente con el comando **clock** .
- El comando **ntp server** *ip-address* se emite en modo de configuración global para configurar 209.165.200.225 como el servidor NTP para R1. Para verificar que la fuente de tiempo esté establecida en NTP, use el comando **show clock detail** . Observe que ahora la fuente de tiempo es NTP.

```
R1# show clock detail
20:55:10 .207 UTC Vie Nov 15 2019
Time source is user configuration
R1# config t
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34 .563 UTC Vie Nov 15 2019
Time source is NTP
```

NTP

Configurar y verificar NTP

Los comandos **show ntp associations** y **show ntp status** se utilizan para verificar que R1 esté sincronizado con el servidor NTP en 209.165.200.225. Observe que el R1 está sincronizado con un servidor NTP de Stratum 1 en 209.165.200.225, que se sincroniza con un reloj GPS. El comando **show ntp status** muestra que R1 ahora es un dispositivo del Stratum 2 que está sincronizado con el servidor NTP en 209.165.220.225.

```
R1# show ntp associations

address ref clock st when poll each delay offset disp
*~209.165.200.225 .GPS.           1 61 64 377 0,481 7,480 4,261
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
(output omitted)
```

NTP

Configurar y verificar NTP

- El reloj de S1 está configurado para sincronizarse con R1 con el comando **ntp server** y la configuración se verifica con el comando **show ntp associations** .
- La salida del comando **show ntp associations** verifica que el reloj en S1 ahora esté sincronizado con R1 en 192.168.1.1 a través de NTP. Ahora S1 es un dispositivo de Stratum 3, que puede proporcionar el servicio NTP a otros dispositivos en la red, por ejemplo terminales.

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations
address ref clock st when poll reach delay offset disp
*~192.168.1.1 209.165.200.225 2 12 64 377 1.066 13.616 3.840
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
(output omitted)

S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
(output omitted
```

SNMP

Introducción a SNMP

SNMP fue desarrollado para permitir a los administradores administrar nodos en una red IP. Permite que los administradores de redes monitoreen y administren el rendimiento de la red, detecten y resuelvan problemas de red y planifiquen el crecimiento de la red.

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:

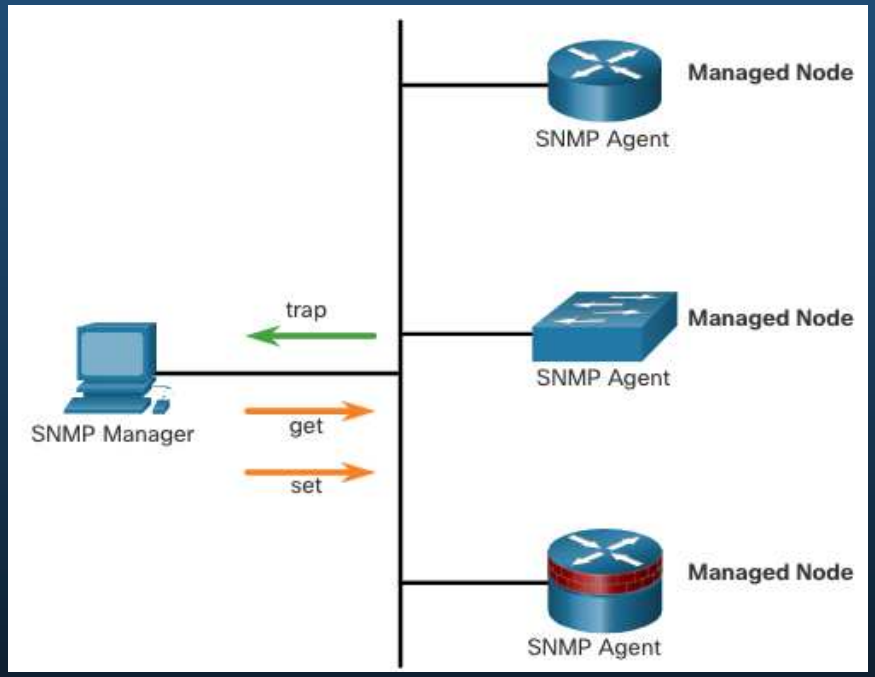
- Administrador de SNMP
- Agentes SNMP (nodo administrado)
- Base de información de administración (MIB)

SNMP define cómo se intercambia la información de administración entre las aplicaciones de administración de red y los agentes de administración. El administrador de SNMP sondea los agentes y consulta la MIB para los agentes de SNMP en el puerto UDP 161. Los agentes de SNMP envían todas las notificaciones de SNMP al administrador de SNMP en el puerto UDP 162.

SNMP

Introducción a SNMP

- El administrador de SNMP forma parte de un sistema de administración de red (NMS). El administrador SNMP puede recopilar información de un agente SNMP mediante la acción "GET" y puede cambiar las configuraciones de un agente mediante la acción "SET". Los agentes SNMP pueden reenviar información directamente a un administrador de red mediante el uso de "TRAPS".
- El agente de SNMP y MIB se alojan en los dispositivos del cliente de SNMP. Las MIB almacenan datos sobre el dispositivo y estadísticas operativas y deben estar disponibles para los usuarios remotos autenticados. El agente de SNMP es responsable de brindar acceso a la MIB local.



SNMP

Operación de SNMP

- Los agentes SNMP que residen en dispositivos administrados recopilan y almacenan información sobre el dispositivo y su funcionamiento localmente en la MIB. El administrador de SNMP luego usa el agente SNMP para tener acceso a la información dentro de la MIB.
- Existen dos solicitudes principales de administrador de SNMP: get y set. Además de la configuración, un conjunto puede provocar que se produzca una acción, como reiniciar un router.

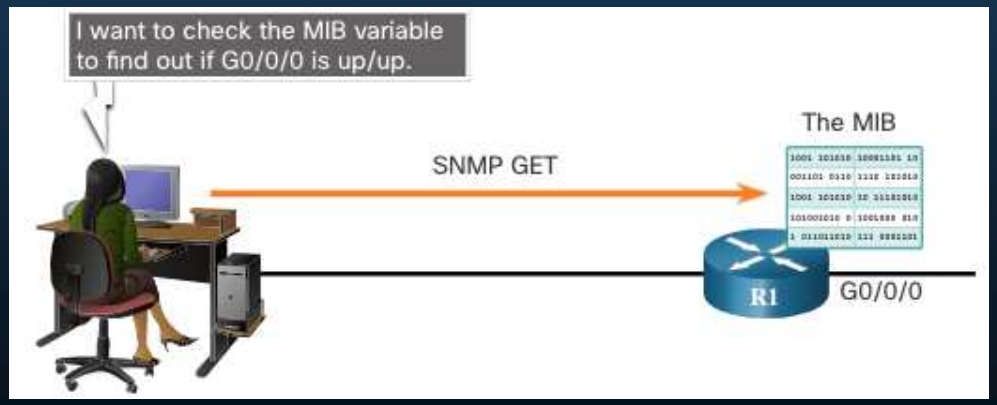
Operación	Descripción
get-request	Recupera un valor de una variable específica.
get-next-request	Recupera un valor de una variable dentro de una tabla; el administrador de SNMP no necesita saber el nombre exacto de la variable. Se realiza una búsqueda secuencial para encontrar la variable necesaria dentro de una tabla.
get-bulk-request	Recupera grandes bloques de datos, como varias filas en una tabla, que de otra manera requerirían la transmisión de muchos bloques pequeños de datos. (Solo funciona con SNMPv2 o más reciente).
get-response	Responde a una operación **get-request, get-next-request** y **set-request** que envió NMS.
set-request	Almacena un valor en una variable específica.

SNMP

Operación SNMP

El agente SNMP responde a las solicitudes del administrador de SNMP de la siguiente manera:

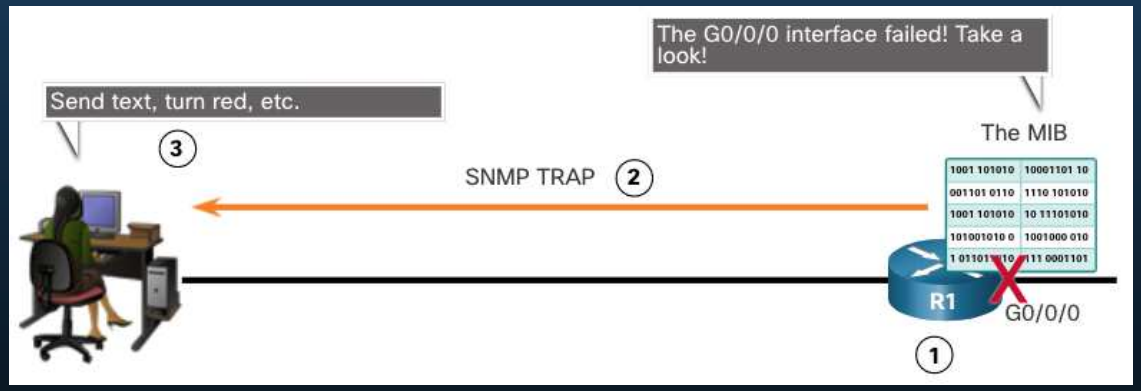
- **Obtener una variable MIB:** - el agente SNMP realiza esta función en respuesta a una GetRequest-PDU del administrador de red. El agente obtiene el valor de la variable de MIB solicitada y responde al administrador de red con dicho valor.
- **Establecer una variable MIB:** - el agente SNMP realiza esta función en respuesta a una PDU SetRequest del administrador de red. El agente de SNMP cambia el valor de la variable de MIB al valor especificado por el administrador de red. La respuesta del agente SNMP a una solicitud set incluye la nueva configuración en el dispositivo.



SNMP

Traps del agente SNMP

- Las traps son mensajes no solicitados que alertan al administrador de SNMP sobre una condición o un evento en la red. Las notificaciones dirigidas a trampas reducen los recursos de la red y del agente al eliminar la necesidad de algunas solicitudes de sondeo SNMP.
- La figura ilustra el uso de una trampa SNMP para alertar al administrador de la red que la interfaz G0/0/0 ha fallado. El software de NMS puede enviar un mensaje de texto al administrador de red, mostrar una ventana emergente en el software de NMS o mostrar el ícono del router en color rojo en la GUI de NMS.



SNMP

Versiones de SNMP

- SNMPv1 - Estándar heredado definido en RFC 1157. Utiliza un método de autenticación simple basado en cadenas de comunidad. No debe utilizarse debido a riesgos de seguridad.
- SNMPv2c - Definido en RFC 1901-1908. Utiliza un método de autenticación simple basado en cadenas de comunidad. Proporciona opciones de recuperación masiva, así como mensajes de error más detallados.
- SNMPv3 - Definido en RFC 3410-3415. Utiliza la autenticación de nombre de usuario, proporciona protección de datos mediante HMAC-MD5 o HMAC-SHA y el cifrado mediante DES, 3DES o AES.

SNMP

Community Strings

SNMPv1 y SNMPv2c usan cadenas de comunidad que controlan el acceso a la MIB. Las cadenas de comunidad son contraseñas de texto no cifrado. Las cadenas de la comunidad de SNMP autentican el acceso a los objetos MIB.

Existen dos tipos de cadenas de comunidad:

- **Sólo lectura (ro) - Este tipo proporciona acceso a las variables MIB, pero no permite cambiar estas variables, sólo lectura.** Debido a que la seguridad es mínima en la versión 2c, muchas organizaciones usan SNMPv2c en modo de solo lectura.
- **Read-write (rw)** - Este tipo proporciona acceso de lectura y escritura a todos los objetos en la MIB.

Para ver o establecer variables de MIB, el usuario debe especificar la cadena de comunidad correspondiente para el acceso de lectura o escritura.

SNMP

MIB Id. de objeto

La MIB organiza variables de manera jerárquica. Formalmente, la MIB define cada variable como una ID de objeto (OID). Las OID identifican de forma exclusiva los objetos administrados. La MIB organiza las OID según estándares RFC en una jerarquía de OID, que se suele mostrar como un árbol.

- El árbol de la MIB para un dispositivo determinado incluye algunas ramas con variables comunes a varios dispositivos de red y algunas ramas con variables específicas de ese dispositivo o proveedor.
- Las RFC definen algunas variables públicas comunes. La mayoría de los dispositivos implementan estas variables de MIB. Además, los proveedores de equipos de redes, como Cisco, pueden definir sus propias ramas privadas del árbol para admitir las nuevas variables específicas de sus dispositivos.

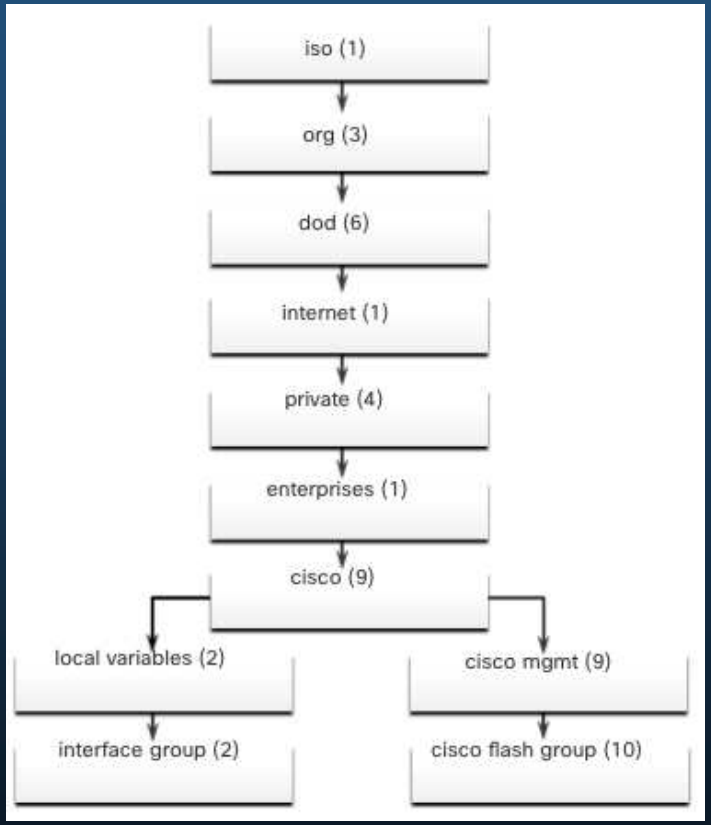
SNMP

Id. de objeto MIB SNMP

La figura muestra partes de la estructura MIB definida por Cisco. Observe cómo se puede describir el OID en palabras o números para ayudar a localizar una variable particular en el árbol.

Los OID de Cisco se numeran de la siguiente manera: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9).

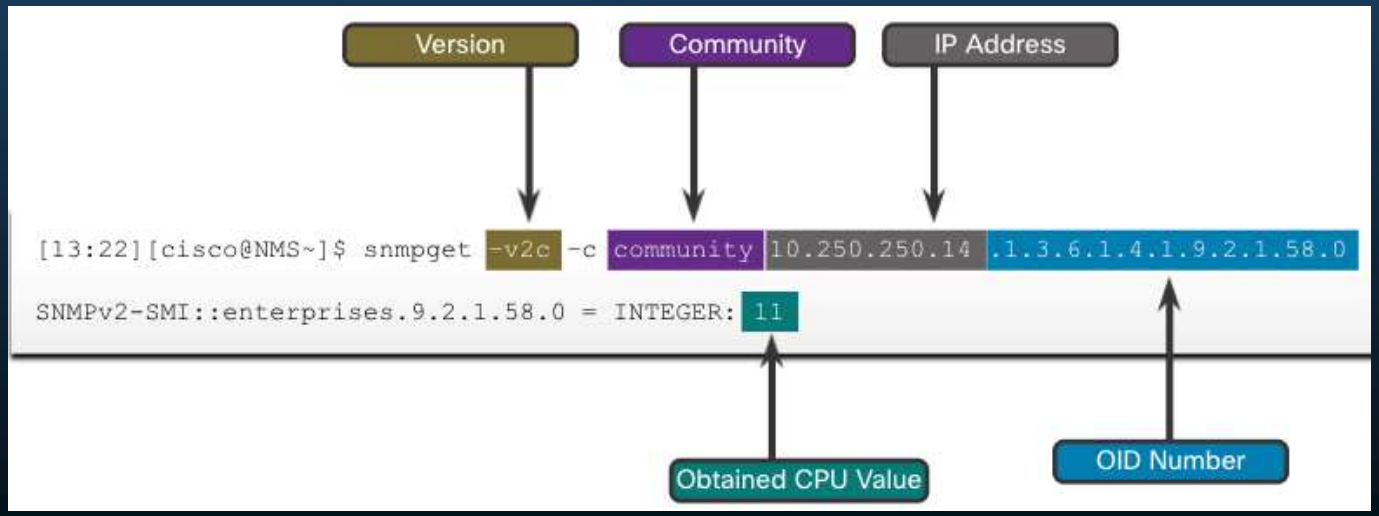
Por lo tanto, el OID es 1.3.6.1.4.1.9.



SNMP

Escenario de sondeo SNMP SNMP

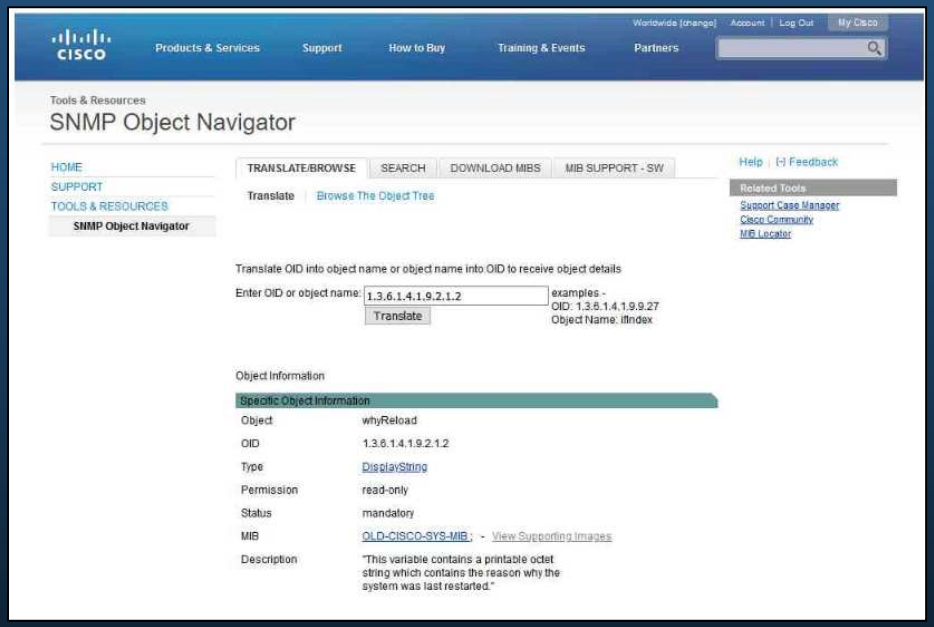
- SNMP se puede utilizar para observar la utilización de la CPU durante un período de tiempo mediante dispositivos de sondeo. Las estadísticas de la CPU se pueden compilar en el NMS y graficar. Esto crea una línea de base para el administrador de red.
- Los datos se recuperan mediante la utilidad snmpget, que se emite en NMS. Con la utilidad snmpget, puede recuperar manualmente datos en tiempo real o hacer que el NMS ejecute un informe. Este informe le daría un período de tiempo en el que podría utilizar los datos para obtener el promedio.



SNMP

Navegador de objeto SNMP

La utilidad snmpget da una idea de la mecánica básica de cómo funciona SNMP. Sin embargo, trabajar con nombres de variables de MIB largos como 1.3.6.1.4.1.9.2.1.58.0 puede ser problemático para el usuario promedio. Más comúnmente, el personal de operaciones de la red utiliza un producto de administración de red con una GUI fácil de usar, lo que hace que el nombre completo de la variable de datos MIB sea transparente para el usuario.



Cisco SNMP Navigator en el sitio web http://www.cisco.com permite a un administrador de red investigar detalles sobre un OID en particular.

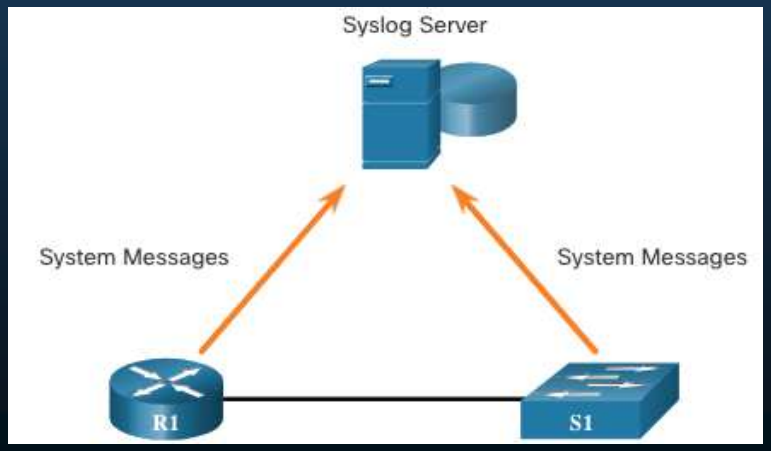
Syslog

Introducción a Syslog

Syslog utiliza el puerto UDP 514 para enviar mensajes de notificación de eventos a través de redes IP a recopiladores de mensajes de eventos, como se muestra en la figura.

El servicio de registro de syslog proporciona tres funciones principales:

- La capacidad de recopilar información de registro para el control y la solución de problemas
- La capacidad de escoger el tipo de información de registro que se captura
- La capacidad de especificar los destinos de los mensajes de syslog capturados



Syslog

Operación Syslog

El protocolo syslog comienza enviando mensajes del sistema y resultados de **debug** a un proceso de registro local. La configuración de Syslog puede enviar estos mensajes a través de la red a un servidor syslog externo, donde se pueden recuperar sin necesidad de acceder al dispositivo.

Por otra parte, los mensajes de syslog se pueden enviar a un búfer interno. Los mensajes enviados al búfer interno solo se pueden ver mediante la CLI del dispositivo.

El administrador de red puede especificar que solo se envíen ciertos tipos de mensajes del sistema a varios destinos. Los destinos populares para mensajes de syslog incluyen los siguientes:

- Búfer de registro (RAM dentro de un router o switch)
- Línea de consola
- Línea de terminal
- Servidor de syslog

Syslog

Formato de mensaje de Syslog

Los dispositivos de Cisco generan mensajes de syslog como resultado de los eventos de red. Cada mensaje de syslog contiene un nivel de severidad y su origen.

Cuanto más bajos son los números de nivel, más fundamentales son las alarmas de syslog. El nivel de severidad de los mensajes se puede establecer para controlar dónde se muestra cada tipo de mensaje (es decir, en la consola o los otros destinos). La lista completa de niveles de syslog se muestra en la tabla.

Nombre de la Severidad	Nivel de Severidad	Explicación
Emergency	Nivel 0	El sistema no se puede usar.
Alert	Nivel 1	Se necesita una acción inmediata.
Critical	Nivel 2	Condición crítica.
Error	Nivel 3	Condición de error.
Warning	Nivel 4	Condición de advertencia.
Notification	Level 5	Condición normal pero importante.
Informational	Nivel 6	Mensaje informativo.
Debugging	Nivel 7	Mensaje de depuración.

Syslog

Servicios de Syslog

Además de especificar la gravedad, los mensajes de syslog también contienen información sobre el sistema/proceso que lo origino. Estos últimos, son identificadores de servicios que identifican y categorizan los datos de estado del sistema para informar los mensajes de error y de eventos. Las opciones registro disponibles son específicas del dispositivo de red.

Algunas registros comunes de mensajes de syslog que se informan en los routers con IOS de Cisco incluyen los siguientes:

- IP
- Protocolo OSPF
- Sistema operativo SYS
- Seguridad IP (IPsec)
- IP de interfaz (IF)

Syslog

Instalaciones de Syslog

De manera predeterminada, el formato de los mensajes de syslog en el software IOS de Cisco es el siguiente:

%facility-severity-MNEMONIC: description

Por ejemplo, el resultado de ejemplo de un switch Cisco para un enlace EtherChannel que cambia al estado activo es el siguiente:

```
%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Aquí la instalación es LINK, y el nivel de gravedad es 3, con con MNEMONIC UPDOWN.

Syslog

Configurar Syslog Timestamp

De manera predeterminada, los mensajes no tienen marca de hora. Los mensajes deben tener marcas de hora, así cuando se envían a otro destino, como un servidor syslog, haya un registro del momento en el que se generó el mensaje. Use el comando **service timestamps log datetime** para forzar que los eventos registrados muestren la fecha y la hora.

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0/0
R1(config-if)# no shutdown
*1 de mar 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Mar 1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Mar 1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
R1(config-if)#
```

Mantenimiento de Routers y Switches

Sistemas de archivos del router

El Sistema de archivos Cisco IOS (IFS) permite al administrador navegar a diferentes directorios y enumerar los archivos en un directorio. El administrador también puede crear subdirectorios en memoria flash o en un disco. Los directorios disponibles dependen del dispositivo.

El ejemplo muestra la salida del comando **show file systems** , que enumera todos los sistemas de archivos disponibles en un router Cisco 4221.

```
Router# show file systems
File Systems:
      Size(b)       Free(b)      Type  Flags  Prefixes
            -             -    opaque     rw   system:
            -             -    opaque     rw   tmpsys:
*  7194652672    6294822912      disk     rw   bootflash: flash:
   256589824     256573440      disk     rw   usb0:
  1804468224    1723789312      disk     ro   webui:
            -             -    opaque     rw   null:
            -             -    opaque     ro   tar:
            -             -   network     rw   tftp:
            -             -    opaque     wo   syslog:
     33554432      33539983     nvram     rw   nvram:
            -             -   network     rw   rcp:
            -             -   network     rw   ftp:
            -             -   network     rw   http:
            -             -   network     rw   scp:
            -             -   network     rw   sftp:
            -             -   network     rw   https:
            -             -    opaque     ro   cns:
Router#
```

El asterisco indica el sistema de archivos predeterminado actual. El signo de número (#) indica un disco de arranque. Ambos están asignados al sistema de archivos flash de forma predeterminada

Mantenimiento de Routers y Switches

Sistemas de archivos del router

Ya que la memoria flash es el sistema de archivos predeterminado, el comando **dir** enumera el contenido de flash. La última lista es de interés específico. Se trata del nombre del archivo de imagen de Cisco IOS actual, que se ejecuta en la memoria RAM.

```
Router# dir
Directory of bootflash:/
   11  drwx            16384   Aug 2 2019 04:15:13 +00:00  lost+found
370945  drwx             4096    Oct 3 2019 15:12:10 +00:00  .installer
338689  drwx             4096    Aug 2 2019 04:15:55 +00:00  .ssh
217729  drwx             4096    Aug 2 2019 04:17:59 +00:00  core
379009  drwx             4096   Sep 26 2019 15:54:10 +00:00  .prst_sync
80641  drwx              4096   Aug 2 2019 04:16:09 +00:00  .rollback_timer
161281  drwx             4096    Aug 2 2019 04:16:11 +00:00  gs_script
112897  drwx            102400   Oct 3 2019 15:23:07 +00:00  tracelogs
362881  drwx             4096   Aug 23 2019 17:19:54 +00:00  .dbpersist
298369  drwx             4096    Aug 2 2019 04:16:41 +00:00  virtual-instance
   12  -rw-               30   Oct 3 2019 15:14:11 +00:00  throughput_monitor_params
 8065  drwx              4096   Aug 2 2019 04:17:55 +00:00  onep
   13  -rw-               34   Oct 3 2019 15:19:30 +00:00  pnp-tech-time
249985  drwx             4096   Aug 20 2019 17:40:11 +00:00  Archives
   14  -rw-            65037   Oct 3 2019 15:19:42 +00:00  pnp-tech-discovery-summary
   17  -rw-          5032908   Sep 19 2019 14:16:23 +00:00
isr4200_4300_rommon_1612_1r_SPA.pkg
   18  -rw-        517153193   Sep 21 2019 04:24:04 +00:00  isr4200-
universalk9_ias.16.09.04.SPA.bin
7194652672 bytes total (6294822912 bytes free)
Router#
```

Mantenimiento de Routers y Switches

Sistemas de archivos del router

Para ver el contenido de NVRAM, debe cambiar el sistema de archivos predeterminado actual mediante el comando **cd** (cambiar directorio), como se muestra en el ejemplo.

El comando actual del directorio de trabajo es **pwd**. Este comando verifica que estamos viendo el directorio NVRAM. Finalmente, el comando **dir** enumera los contenidos de NVRAM. Si bien se enumeran varios archivos de configuración, el de mayor interés específicamente es el archivo de configuración de inicio.

```
Router#
Router# cd nvram:
Router# pwd
nvram:/
Router# dir
Directory of nvram:/
32769  -rw-             1024                    startup-config
32770  ----               61                    private-config
32771  -rw-             1024                    underlying-config
    1  ----                4                    private-KS1
    2  -rw-             2945                    cwmp_inventory
    5  ----              447                    persistent-data
    6  -rw-             1237                    ISR4221-2x1GE_0_0_0
    8  -rw-               17                    ecfm_ieee_mib
    9  -rw-                0                    ifIndex-table
   10  -rw-             1431                    NIM-2T_0_1_0
   12  -rw-              820                    IOS-Self-Sig#1.cer
   13  -rw-              820                    IOS-Self-Sig#2.cer
33554432 bytes total (33539983 bytes free)
Router#
```

Mantenimiento de Routers y Switches

Sistemas de archivos del switch

Con el sistema de archivos flash del switch Cisco 2960, se pueden copiar los archivos de configuración y archivar (subir y descargar) imágenes de software.

El comando para ver los sistemas de archivos en un switch Catalyst es el mismo que en un router Cisco: **show file systems.**

```
Switch# show file systems
File Systems:
       Size(b)     Free(b)      Type  Flags  Prefixes
*    32514048    20887552     flash     rw    flash:
           -           -    opaque     rw       vb:
           -           -    opaque     ro       bs:
           -           -    opaque     rw   system:
           -           -    opaque     rw   tmpsys:
       65536       48897     nvram     rw    nvram:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -    opaque     rw     null:
           -           -    opaque     ro      tar:
           -           -   network     rw     tftp:
           -           -   network     rw      rcp:
           -           -   network     rw     http:
           -           -   network     rw      ftp:
           -           -   network     rw      scp:
           -           -   network     rw    https:
           -           -    opaque     ro      cns:
Switch#
```

Mantenimiento de Routers y Switches

Utilice un archivo de texto para realizar una copia de seguridad de una configuración

Los archivos de configuración se pueden guardar en un archivo de texto utilizando Tera Term:

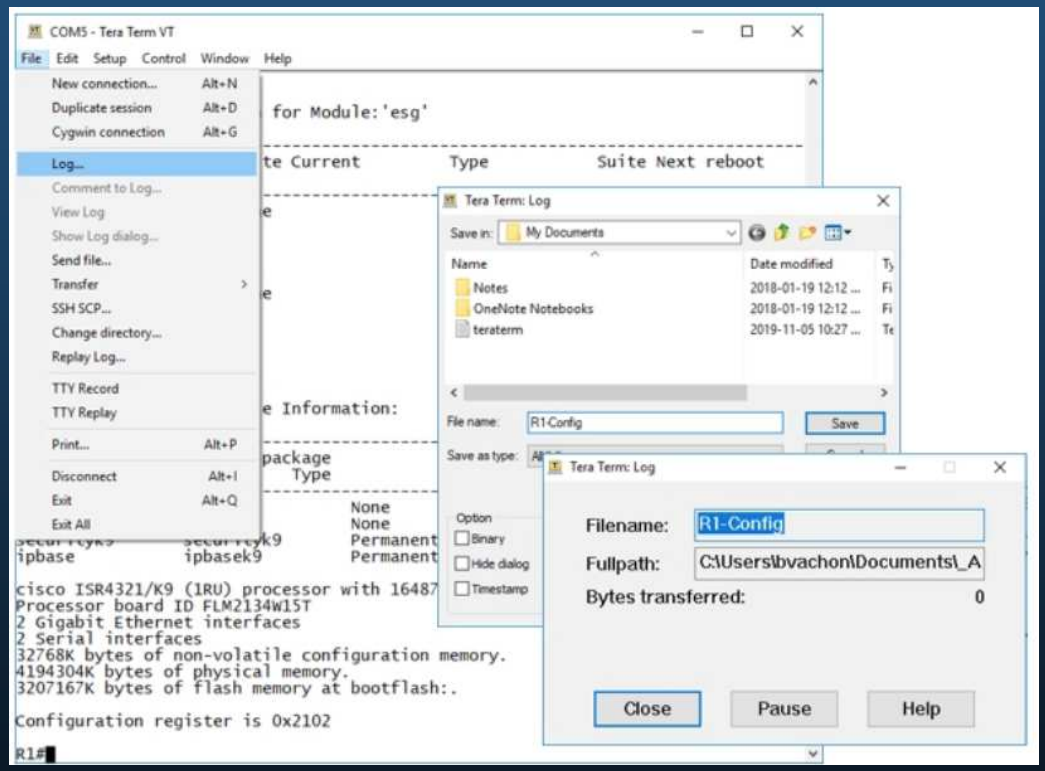
Paso 1. En el menú Archivo (File menu), haga clic en **Log**.

Paso 2. Elija la ubicación para guardar el archivo. Tera Term comenzará a capturar texto.

Paso 3. Después de iniciar la captura, ejecute el comando **show running-config** o **show startup-config** en el indicador EXEC privilegiado. El texto que aparece en la ventana del terminal se dirigirá al archivo elegido.

Paso 4. Cuando se complete la captura, seleccione **Close** en la ventana Tera Term: Log.

Paso 5. Observe el archivo para verificar que no esté dañado.



Mantenimiento de Routers y Switches

Usar un archivo de texto para restaurar una configuración

Se puede copiar una configuración de un archivo y luego pegarla directamente en un dispositivo. TEl archivo requerirá edición para garantizar que las contraseñas cifradas estén en texto sin formato y que se eliminen los textos que no sean de comando, como **--More--** y los mensajes IOS.

Además, es posible que desee agregar **enable** y **configure terminal** al comienzo del archivo o entrar en el modo de configuración global antes de pegar la configuración. En lugar de copiar y pegar, una configuración se puede restaurar a partir de un archivo de texto utilizando Tera Term. Al usar Tera Term, los pasos son los siguientes:

Paso 1. En el menú File (Archivo), haga clic en **Send file (Enviar archivo)**.
Paso 2. Ubique el archivo que debe copiar en el dispositivo y haga clic en **Open (Abrir)**.
Paso 3. Tera Term pegará el archivo en el dispositivo.

El texto en el archivo se aplicará en forma de comandos en la CLI y pasará a ser la configuración en ejecución en el dispositivo.

Mantenimiento de Routers y Switches

Creación de copias de seguridad y restauración mediante TFTP

Siga estos pasos para realizar una copia de respaldo de la configuración en un servidor TFTP:

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

Siga estos pasos para restaurar la configuración en ejecución desde un servidor TFTP:

Paso 1. Introduzca el comando **copy tftp running-config** .
Paso 2. Introduzca la dirección IP del host en el que está almacenado el archivo de configuración.
Paso 3. Introduzca el nombre que se asignará al archivo de configuración.
Paso 4. Presione **Enter** para confirmar cada elección.

```
R1# copy running-config tftp
Remote host []? 192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jan-2019
Write file R1-Jan-2019 to 192.168.10.254? [confirm]
Writing R1-Jan-2019 !!!!!! [OK]
```

Mantenimiento de Routers y Switches

Uso de puertos USB en un router Cisco

La característica de almacenamiento de bus serial universal (USB) habilita a determinados modelos de routers Cisco para que admitan unidades flash USB. La característica flash USB proporciona una capacidad de almacenamiento secundario optativa y un dispositivo de arranque adicional. Los puertos USB de un Cisco 4321 Router se muestran en la figura.

Utilice el comando **dir** para ver el contenido de la unidad de memoria flash USB.

Mantenimiento de Routers y Switches

Uso de USB para realizar copias de seguridad y restaurar una configuración

- **Ejecute el comando show file systems** para verificar que la unidad USB está allí y confirmar su nombre. Para este ejemplo, el sistema de archivos USB se denomina **usbflash0:**.
- Utilice el comando **copy run usbflash0:/** para copiar el archivo de configuración en la unidad flash USB. Asegúrese de utilizar el nombre de la unidad flash tal como se indica en el sistema de archivos. La barra es optativa, pero indica el directorio raíz de la unidad flash USB.
- El IOS le solicitará el nombre de archivo. Si el archivo ya existe en la unidad flash USB, el router solicitará que se sobrescriba.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? Configuración R1-
%Warning:There is a file already existing with this name
          Do you want to over write? [confirm]

 5024 bytes copiados en 1.796 segundos (2797 bytes/seg)
                          R1#
```

Mantenimiento de Routers y Switches

Uso de USB para realizar copias de seguridad y restaurar una configuración

Utilice el comando **dir** para ver el archivo en la unidad USB, y el comand **more** para ver el contenido

Para restaurar configuraciones con una unidad flash USB, será necesario editar el archivo USB R1-Config con un editor de texto. Suponiendo que el nombre del archivo es **R1-Config**, use el comando **copy usbflash0:/R1-Config** *running-config* para restaurar una configuración en ejecución.

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config
4050042880 bytes total (3774144512 bytes free)
R1#
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
no ipv6 cef
R1#
```

Mantenimiento de Routers y Switches

Procedimientos de recuperación de contraseña

Las contraseñas de los dispositivos se utilizan para evitar el acceso no autorizado. Las contraseñas encriptadas, como las contraseñas generadas mediante "enable secret", se deben reemplazar después de su recuperación. Dependiendo del dispositivo, el procedimiento detallado para la recuperación de contraseña varía.

Sin embargo, todos los procedimientos de recuperación de contraseña siguen el mismo principio:

Paso 1. Ingrese en el modo ROMMON.
Paso 2. Cambie el registro de configuración.
Paso 3. Copie el startup-config en la running-config.
Paso 4. Cambie la contraseña.
Paso 5. Guarde el running-config como el nuevo startup-config.
Paso 6. Reinicie el dispositivo.

Mantenimiento de Routers y Switches

Procedimientos para recuperación de contraseñas

Paso 1. Ingresar en el modo ROMMON. Con el acceso a la consola, el usuario puede acceder al modo ROMMON mediante una secuencia de interrupción durante el proceso de arranque o eliminando la memoria flash externa cuando el dispositivo está apagado.

Cuando se realiza correctamente, se muestra el mensaje **rommon 1 >** , como se muestra en el ejemplo.

```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Mantenimiento de Routers y Switches

Ejemplo de recuperación de contraseña

Paso 2. Cambiar el registro de configuración. El comando confreg 0x2142 permite al usuario establecer el registro de configuración en 0x2142, lo que hace que el dispositivo ignore el archivo de configuración de inicio durante el inicio.

Después de establecer el registro de configuración en 0x2142, escriba **reset** en el indicador para reiniciar el dispositivo. Introduzca la secuencia de interrupción mientras el dispositivo esté reiniciando y descomprimiendo el IOS. El ejemplo muestra la salida del terminal de un router 1941 en el modo ROMMON después de usar una secuencia de interrupción durante el proceso de arranque.

```
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

Mantenimiento de Routers y Switches

Ejemplo de recuperación de contraseña

Paso 3. Copie el startup-config en la running-config. Una vez que el dispositivo haya terminado de iniciar nuevamente, emita el comando **copy startup-config running-config** .

PRECAUCIÓN: no ingrese **copy running-config startup-config**. Este comando borra la configuración de inicio original.

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
R1#
```

Mantenimiento de Routers y Switches

Ejemplo de recuperación de contraseña

Paso 4. Cambie la contraseña. Dado que está en el modo EXEC privilegiado, ahora puede configurar todas las contraseñas necesarias.

Nota: la contraseña **cisco** no es una contraseña segura y se usa aquí solo como ejemplo

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# enable secret cisco
```

Mantenimiento de Routers y Switches

Ejemplo de recuperación de contraseña

Paso 5. Guarde el running-config como el nuevo startup-config. Después de configurar las nuevas contraseñas, vuelva a cambiar el registro de configuración a 0x2102 mediante el comando **config-register 0x2102** en el modo de configuración global. Guarde el running-config en startup-config.

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration... [OK]
R1#
```

Administración de imágenes de IOS

Servidores TFTP como ubicación de copia de seguridad

A medida que una red crece, las imágenes y los archivos de configuración del software IOS de Cisco pueden almacenarse en un servidor TFTP central. Esto ayuda a controlar la cantidad de imágenes del IOS y las revisiones a dichas imágenes del IOS, así como los archivos de configuración que deben mantenerse.

Las internetworks de producción suelen abarcar áreas extensas y contienen varios routers. Para cualquier red, es una buena práctica mantener una copia de seguridad de la imagen del software Cisco IOS en caso de que la imagen del sistema en el router se dañe o se borre accidentalmente.

Los routers distribuidos ampliamente necesitan una ubicación de origen o de copia de seguridad para las imágenes del software IOS de Cisco. Utilizar un servidor TFTP de red permite cargar y descargar imágenes y configuraciones por la red. El servidor TFTP de la red puede ser otro router, una estación de trabajo o un sistema host.

Mantenimiento de Routers y Switches

Ejemplo de copia de seguridad de la imagen del IOS en el servidor TFTP

Para mantener las operaciones de red con el mínimo tiempo de inactividad, es necesario implementar procedimientos para realizar copias de seguridad de las imágenes del IOS de Cisco. Esto permite que el administrador de red copie rápidamente una imagen a un router en caso de que la imagen esté dañada o borrada. Utilice los siguientes pasos:

Paso 1. Haga ping al servidor TFTP. Haga ping al servidor TFTP para probar la conectividad.

Paso 2. Verifique el tamaño de la imagen en flash. Verifique que el servidor TFTP tenga suficiente espacio en disco para admitir la imagen del software IOS de Cisco. Use el comando **show flash0:** en el router para determinar el tamaño del archivo de imagen Cisco IOS.

Paso 3. Copie la imagen al servidor TFTP. Copie la imagen en el servidor TFTP mediante el comando **copy***source-url destination-url* . Después de emitir el comando utilizando las URL de origen y destino especificadas, se le solicita al usuario el nombre del archivo de origen, la dirección IP del host remoto y el nombre del archivo de destino. A continuación, se inicia la transferencia.

Mantenimiento de Routers y Switches

Copie una imagen IOS a un dispositivo Ejemplo

Paso 1. Haga ping al servidor TFTP. Haga ping al servidor TFTP para probar la conectividad.

Paso 2. Verifique la cantidad de flash libre. Asegúrese de que hay suficiente espacio flash en el dispositivo que se está actualizando mediante el**comando show flash:. Compare el espacio disponible en la memoria flash con el tamaño del nuevo archivo de imagen.**

Paso 3. Copie el archivo de imagen IOS del servidor TFTP al router utilizando el comando **copy tftp: flash:** . Después de emitir este comando, se le solicitará al usuario la dirección IP del host remoto, el nombre del archivo de origen y el nombre del archivo de destino.

```
R1# copy tftp: flash:
Address or name of remote host []? 2001:DB8:CAF:100: :99
Source filename []? isr4200-universalk9_ias.16.09.04.SPA.bin
Destination filename [isr4200-universalk9_ias.16.09.04.SPA.bin]?
Accessing tftp://2001:DB8:CAFE:100::99/ isr4200- universalk9_ias.16.09.04.SPA.bin...
Loading isr4200-universalk9_ias.16.09.04.SPA.bin from 2001:DB8:CAFE:100::99 (via
GigabitEthernet0/0/0): !!!!!!!!!!!!!!!!!!!

[OK - 517153193 bytes]
517153193 bytes copied in 868.128 secs (265652 bytes/sec)
```

Mantenimiento de Routers y Switches

Comando boot system

Durante el inicio, el código de arranque analiza el archivo de configuración de inicio en NVRAM para los comandos **boot system** que específican el nombre y la ubicación de la imagen del software Cisco IOS para cargar. Si no hay comandos **boot system** de manera secuencial para proporcionar un plan de arranque que tenga tolerancia a fallas.

Si no hay comandos **boot system** en la configuración, de manera predeterminada, el router carga y ejecuta la primera imagen válida del IOS de Cisco en la memoria flash.

Para actualizar a la imagen IOS copiada después de que esa imagen se guarde en la memoria flash del router, configure el router para cargar la nueva imagen mediante el comando **boot system** . Guarde la configuración. Vuelva a cargar el router para que arranque con la nueva imagen.

```
R1# configure terminal
R1 (config) # boot system flash0:isr4200-
universalk9_ias.16.09.04.SPA.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```