"CIENCIA Y TECNOLOGÍA AL SERVICIO DEL HOMBRE"

ASIGNATURA: Int. De tecnologías WAN

TEMA: Resumen Capitulo 7

DOCENTE: Juan Alberto Vivas Burgos

ESTUDIANTE: Alex Ricardo Puc Kumul

CARRERA: Ingeniería informática

Fecha de entrega: 19 de Noviembre del 2019

Internet y las tecnologías de IP han crecido con rapidez. Una de las razones de este crecimiento es en parte la flexibilidad del diseño original. Sin embargo, ese diseño no anticipó la popularidad de Internet con la demanda resultante de direcciones IP. Por ejemplo, cada host y cada dispositivo conectado a Internet requiere una dirección IP versión 4 (IPv4) única. A causa del enorme crecimiento, la cantidad de direcciones IP disponibles se está acabando con rapidez.

Para poder compensar esta falta de direcciones IP, se desarrollaron diferentes soluciones a corto plazo. Dos de estas soluciones a corto plazo son las direcciones privadas y la traducción de direcciones de red (NAT, Network Address Translation).

Normalmente un host interno recibe su dirección IP, máscara de subred, dirección IP del gateway predeterminado, dirección IP del servidor DNS y otra información de un servidor de protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol). En lugar de proporcionar a los hosts internos direcciones IP de Internet válidas, el servidor de DHCP normalmente proporcionas direcciones IP de un conjunto de direcciones privado. El problema es que puede ocurrir que estos hosts necesiten direcciones IP válidas para poder tener acceso a los recursos de Internet. Aquí es donde entra en juego NAT.

NAT permite a los hosts de red internos tomar prestada una dirección IP de Internet legítima al conectarse a los recursos de Internet. Cuando el tráfico solicitado regresa, la dirección IP legítima se libera y vuelve a estar disponible para la siguiente solicitud de Internet que haga un host interno. Al usar NAT, los administradores de red sólo necesitan una o algunas direcciones IP para que el router proporcione a los hosts, en lugar de una dirección IP única para cada cliente que se une a la red. Si bien este método no parece ser eficaz, en realidad sí lo es, porque el tráfico de los hosts se traslada con mucha rapidez.

Si bien las direcciones privadas con DHCP y NAT han colaborado para reducir la necesidad de direcciones IP, se estima que para el año 2010 se agotarán las direcciones IPv4 únicas. Por este motivo, a mediados de la década del 90, el IETF solicitó propuestas para un nuevo esquema de direccionamiento IP. Así recibió la respuesta del grupo IP de próxima generación (IPng, IP Next Generation). Para 1996, el IETF comenzó a publicar una serie de RFC que definen el IPv6.

¿Qué es DHCP?

Cada dispositivo que se conecta a una red necesita una dirección IP. Los administradores de red asignan direcciones IP estáticas a los routers, los servidores y otros dispositivos de red que es poco probable que cambien de ubicación (física y lógica). Los administradores ingresan las direcciones IP estáticas de manera manual al configurar los dispositivos que se conectarán a la red. Las direcciones estáticas también permiten a los administradores administrar esos dispositivos de manera remota.

Sin embargo, las computadoras de una organización con frecuencia cambian de ubicación, tanto física como lógica. Los administradores no pueden asignar nuevas direcciones IP cada vez que un empleado se muda a otra oficina o cubículo. Los clientes de escritorio no requieren direcciones estáticas. Por el contrario, una estación de trabajo puede utilizar cualquier dirección perteneciente a un rango de direcciones. Este rango se encuentra por lo general dentro de una subred IP. Una estación de trabajo perteneciente a una subred específica puede recibir cualquier dirección perteneciente a un rango especificado. Otros elementos, como la máscara de subred, el gateway predeterminado y el servidor del sistema de nombres de dominios (DNS, Domain Name System)

reciben un valor que es común para esa subred o toda la red administrada. Por ejemplo, todos los hosts dentro de la misma subred reciben diferentes direcciones IP de host, pero reciben la misma máscara de subred y la misma dirección IP de gateway predeterminado.

Funcionamiento de DHCP

La asignación de direcciones IP a los clientes es la tarea más fundamental que realiza un servidor de DHCP. DHCP incluye tres mecanismos diferentes para la asignación de direcciones a fin de proporcionar flexibilidad al momento de asignar direcciones IP:

- Asignación manual: El administrador asigna una dirección IP asignada previamente al cliente y DHCP sólo comunica la dirección IP al dispositivo.
- Asignación automática: DHCP asigna automáticamente una dirección IP estática permanente a un dispositivo; la dirección es seleccionada de un conjunto de direcciones disponibles. No hay arrendamiento y la dirección se asigna permanentemente al dispositivo.
- Asignación dinámica: DHCP asigna automáticamente una dirección IP dinámica, o arrendada, tomada de un grupo de direcciones IP por un período limitado seleccionado por el servidor o hasta que el cliente informe al servidor de DHCP que ya no necesita la dirección.

BOOTP y DHCP

El protocolo Bootstrap (BOOTP), definido en RFC 951, es el predecesor del protocolo DHCP y comparte con éste algunas características funcionales. BOOTP es una manera de descargar configuraciones de dirección e inicio para estaciones de trabajo sin disco. Una estación de trabajo sin disco no tiene unidad de disco duro ni sistema operativo. Por ejemplo, muchos sistemas de cajas registradoras automatizadas de los supermercados son estaciones de trabajo sin disco. Tanto DHCP como BOOTP se basan en la relación cliente/servidor y utilizan los puertos UDP 67 y 68. Estos puertos todavía se conocen como puertos BOOTP.

DHCP y BOOTP tienen dos componentes, como se muestra en la figura. El servidor es un host con dirección IP estática que asigna, distribuye y administra las asignaciones de IP y los datos de configuración. Cada asignación (IP y datos de configuración) se almacena en el servidor en un conjunto de datos llamado asignación. El cliente es algún dispositivo que utilice DHCP como método de obtención de direccionamiento IP o soporte de información de configuración.

Para comprender las diferencias funcionales entre BOOTP y DHCP, tenga en cuenta los cuatro parámetros básicos de IP necesarios para conectarse a una red:

1. Dirección IP
2. Dirección de gateway
3. Máscara de subred
4. Dirección de servidor DNS

Configuración de un servidor de DHCP

Los routers Cisco que ejecutan el software IOS de Cisco son plenamente compatibles para actuar como servidores de DHCP. El servidor de DHCP que ejecuta IOS de Cisco administra direcciones IP de conjuntos de direcciones especificados en el router y las asigna a los clientes de DHCP.

Los pasos para configurar un router como servidor de DHCP son los siguientes:

- Paso 1. Definición de un rango de direcciones que DHCP no debe asignar. Normalmente estas direcciones son las direcciones estáticas reservadas para la interfaz del router, la dirección IP de administración del switch, los servidores y las impresoras de red locales.
- Paso 2. Creación del pool de DHCP con el comando ip dhcp pool.
- Paso 3. Configuración de los parámetros específicos del pool.

Una mejor práctica consiste en configurar las direcciones excluidas en un modo de configuración global antes de crear el pool de DHCP. Esto garantiza que DHCP no asigne direcciones reservadas por accidente.

Es necesario especificar las direcciones IP que el servidor de DHCP no debe asignar a los clientes. Normalmente, algunas direcciones IP pertenecen a dispositivos estáticos de la red, por ejemplo, servidores o impresoras. DHCP no debe asignar estas direcciones IP a otros dispositivos. Una mejor práctica consiste en configurar las direcciones excluidas en un modo de configuración global antes de crear el pool de DHCP. Esto garantiza que DHCP no asigne direcciones reservadas por accidente. Para excluir direcciones específicas, utilice el comando ip dhcp excluded-address.

¿Qué es NAT?

NAT es como el recepcionista de una oficina grande. Imagine que le indica al recepcionista que no le pase ninguna llamada a menos que se lo solicite. Más tarde, llama a un posible cliente y le deja un mensaje para que le devuelva el llamado. A continuación, le informa al recepcionista que está esperando una llamada de este cliente y le solicita que le pase la llamada a su teléfono.

El cliente llama al número principal de la oficina, que es el único número que el cliente conoce. Cuando el cliente informa al recepcionista a quién está buscando, el recepcionista se fija en una tabla de búsqueda que indica cuál es el número de extensión de su oficina. El recepcionista sabe que el usuario había solicitado esta llamada, de manera que la reenvía a su extensión.

Entonces, mientras que el servidor de DHCP asigna direcciones IP dinámicas a los dispositivos que se encuentran dentro de la red, los routers habilitados para NAT retienen una o varias direcciones IP de Internet válidas fuera de la red. Cuando el cliente envía paquetes fuera de la red, NAT traduce la dirección IP interna del cliente a una dirección externa. Para los usuarios externos, todo el tráfico que entra a la red y sale de ella tiene la misma dirección IP o proviene del mismo conjunto de direcciones.

NAT tiene muchos usos, pero la utilidad clave es el ahorro de direcciones IP al permitir que las redes utilicen direcciones IP privadas. NAT traduce direcciones internas, privadas y no enrutables a direcciones públicas enrutables. NAT tiene el beneficio adicional de agregar un nivel de privacidad y seguridad a una red porque oculta las direcciones IP internas de las redes externas.

Sobrecarga de NAT

La sobrecarga de NAT (a veces llamada Traducción de la dirección del puerto, [PAT, Port Address Translation]) asigna varias direcciones IP privadas a una única dirección IP pública o a un grupo pequeño de direcciones IP públicas. Es lo que hacen la mayoría de los routers. El ISP asigna una dirección al router doméstico, y varios integrantes de la familia pueden navegar por Internet de manera simultánea.

Con la sobrecarga de NAT, es posible asignar varias direcciones a una o sólo algunas direcciones porque cada dirección privada también se identifica por un número de puerto. Cuando un cliente abre una sesión TCP/IP, el router NAT asigna un número de puerto a la dirección de origen correspondiente. La sobrecarga de NAT asegura que los clientes utilicen un número de puerto TCP diferente para cada sesión de cliente con un servidor en Internet. Cuando se recibe una respuesta del servidor, el número de puerto de origen, que pasa a ser el número de puerto de destino en la respuesta, determina a qué cliente se enrutan los paquetes. Además valida que los paquetes entrantes fueron solicitados, lo que agrega seguridad a la sesión.

NAT estática

Recuerde que la asignación NAT estática es una asignación uno a uno entre una dirección interna y una dirección externa. La NAT estática permite conexiones iniciadas por dispositivos externos dirigidas a dispositivos internos. Por ejemplo, puede asignar una dirección global interna a una dirección local interna específica que está asignada al servidor Web.

La configuración de las traducciones NAT estáticas es una tarea simple. Debe definir las direcciones que desea traducir y a continuación configurar NAT en las interfaces correspondientes. Los paquetes que llegan a una interfaz interna provenientes de la dirección IP identificada se someten al proceso de traducción. Los paquetes que llegan a una interfaz externa dirigidos a la dirección IP identificada se someten al proceso de traducción.

Configuración de NAT dinámica

Mientras que la NAT estática proporciona una asignación permanente entre una dirección interna y una dirección pública específica, la NAT dinámica asigna direcciones IP privadas a direcciones públicas. Estas direcciones IP públicas provienen de un conjunto de NAT. La configuración NAT dinámica difiere de la NAT estática, pero también tiene algunas similitudes. Como la NAT estática, requiere que la configuración identifique cada interfaz como interfaz interna o externa. Sin embargo, en lugar de crear una asignación estática a una única dirección IP, se utiliza un conjunto de direcciones globales internas.

Motivos para usar IPv6

El movimiento para pasar de IPv4 a IPv6 ya comenzó, en particular en Europa, Japón y la región del Pacífico asiático. Estas áreas están agotando las direcciones IPv4 que tienen asignadas, lo que hace que IPv6 sea más atractivo y necesario. Japón comenzó el cambio oficialmente en el año 2000, cuando el gobierno japonés exigió la incorporación de IPv6 y estableció una fecha límite en el año 2005 para actualizar los sistemas existentes de todas las empresas del sector público. Corea, China y Malasia han lanzado iniciativas similares.

La posibilidad de expandir las redes para exigencias futuras requiere un suministro ilimitado de direcciones IP y una mayor movilidad que no se pueden satisfacer sólo con DHCP y NAT. IPv6 satisface los requisitos cada vez más complejos del direccionamiento jerárquico que IPv4 no proporciona.

Dada la enorme base instalada de IPv4 en todo el mundo, no es difícil apreciar que la transición de IPv4 a IPv6 es un desafío. Sin embargo, hay una variedad de técnicas, entre ellas una opción de configuración automática, para facilitar la transición. El mecanismo de transición que debe utilizar depende de las necesidades de su red.

La figura compara las representaciones binarias y alfanuméricas de las direcciones IPv4 e IPv6. Una dirección IPv6 es un valor binario de 128 bits, que se puede mostrar como 32 dígitos hexadecimales. IPv6 debería proporcionar una cantidad de direcciones suficiente para las necesidades de crecimiento futuras de Internet durante muchos años más. La cantidad de direcciones IPv6 disponibles permiten asignar a cada persona del planeta un espacio de direcciones de Internet equivalente al espacio total de IPv4.

IPv6 no existiría si no fuera por el agotamiento evidente de las direcciones IPv4 disponibles. Sin embargo, más allá del mayor espacio de direcciones IP, el desarrollo de IPv6 presentó oportunidades para aplicar lo aprendido a partir de las limitaciones de IPv4 y crear así un protocolo con funciones nuevas y mejoradas.

La mayor simplicidad de la arquitectura de encabezados y el funcionamiento del protocolo significa que se reducen los gastos operativos. Las funciones de seguridad incorporadas posibilitan prácticas de seguridad más sencillas que muchas redes actuales necesitan. Sin embargo, tal vez la mejora más importante ofrecida por IPv6 son las funciones de configuración automática de direcciones que ofrece.

Direccionamiento IP mejorado

Un espacio de direcciones más grande ofrece varias mejoras, entre ellas:

- Más posibilidad de conexión y flexibilidad global.
- Mejor agrupación de los prefijos IP anunciados en las tablas de enrutamiento.
- Hosts con múltiples conexiones. La multiconexión es una técnica para aumentar la confiabilidad de la conexión a Internet de una red IP. Con IPv6, un host puede tener varias direcciones IP a través de un enlace ascendente físico. Por ejemplo, un host puede conectarse a varios ISP.

- Configuración automática que puede incluir direcciones de capa de enlace de datos en el espacio de la dirección.
- Más opciones plug-and-play para más dispositivos.
- Redireccionamiento de extremo a extremo de público a privado sin traducción de direcciones. Esto hace que las redes entre peers (P2P) sea más funcional y fácil de implementar.
- Mecanismos simplificados para renumeración y modificación de direcciones.

Stack doble

El método de stack doble es un método de integración en el que un nodo tiene implementación y conectividad para redes IPv4 e IPv6. Es la opción recomendada y requiere que se ejecuten IPv4 e IPv6 simultáneamente. El router y los switches se configuran para admitir ambos protocolos; el protocolo preferido es IPv6.

Tunneling

La segunda técnica de transición más importante es el tunneling. Existen varias técnicas de tunneling, entre ellas:

- Tunneling manual de IPv6 sobre IPv4: un paquete de IPv6 se encapsula dentro del protocolo IPv4. Este método requiere routers de stack doble.
- Tunneling dinámico 6to4: establece automáticamente la conexión de islas de IPv6 a través de la red IPv4, normalmente Internet. Aplica dinámicamente un prefijo IPv6 válido y único a cada isla de IPv6, lo que posibilita la implementación rápida de IPv6 en una red corporativa sin recuperación de direcciones de los ISP o los registros.