DEPARTAMENTO: Ciencias de la Ingeniería **PROFESOR:** Mg. Tannia Mayorga.
CARRERA: Sistemas de Información **ESTUDIANTE:** Marco Antonio Ayala Lituma
CURSO: Séptimo **PARALELO:** "A" **DESCRIPCIÓN:** Diario ingeniería – S5
ASIGNATURA: Redes de Datos I

Contenido

TEMA:

Resumen un las partes importantes de cada capitulos de CCNA 11 al 13

El presente documento representa el resumen de la plataforma NetACad sobre los módulos de requeridos.

Capítulo 11 – Asignación de Direcciones IPv4

Una dirección IPv4 es una dirección jerárquica de 32 bits, compuesta por una parte de red y una parte de host. Para todos los dispositivos de la misma red, los bits de la parte de red de la dirección deben ser los mismos. Los bits en la parte de host de la dirección deben ser únicos para identificar un host específico en la red. El host necesita una dirección IPv4 única y una máscara de subred para mostrar el host o la parte de red de la dirección. La longitud del prefijo es el número de bits establecido en 1 en la máscara de subred. Está escrito usando "notación de barra diagonal" (es decir, "/" seguido del número de dígitos establecido en 1). La operación lógica AND es una comparación de dos bits. Solo 1 Y 1 producirán 1, todas las demás combinaciones producirán 0. Cualquier otra combinación producirá 0. Cada red tiene una dirección de red, una dirección de host y una dirección de transmisión.

Hablando sobre Brodcast y Multicast, la transmisión unidifusión se refiere a un dispositivo que envía un mensaje a otro dispositivo en comunicación uno a uno. Un paquete de unidifusión es un paquete con una dirección IP de destino, que es una dirección de unidifusión como una única dirección de destinatario. Difusión Difusión se refiere a un dispositivo que envía mensajes a todos los dispositivos de la red a través de una comunicación uno a uno. La dirección IPv4 de destino del paquete de transmisión contiene solo el número uno (1) en la parte del host. La transmisión por secuencias de multidifusión reduce el tráfico al permitir que los hosts envíen un solo paquete a grupos de hosts seleccionados que están suscritos al grupo de multidifusión. Un paquete de multidifusión es un paquete con una dirección IP de destino, es decir, una dirección de multidifusión. La dirección reservada IPv4 varía de 224.0.0.0 a 239.255.255.255 como rango de multidifusión.

Utilice uno o más bits de host como bits de red para crear una subred IPv4. Esto se hace extendiendo la máscara de subred para tomar prestados algunos bits de la parte del host de la dirección para crear otros bits de red. Cuantos más bits de host se tomen prestados, más subredes se pueden definir. Tomar prestados más bits para aumentar el número de subredes reducirá el número de hosts por subred.

La red es más fácil de subdividir en límites de / 8/16 y / 24 bytes. Esta tabla identifica estas longitudes de prefijo. Tenga en cuenta que el uso de una longitud de prefijo más larga reducirá la cantidad de hosts por subred.

Mascaras de subred en límites de octeto

Longitud de prefijo	Máscara de subred	Máscara de subred en sistema binario (n=red, h=host)	# de hosts
/8	255.0.0.0	nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.00000000	16777214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.00000000	65534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000	254

Sería útil saber cómo dividir en subredes en los límites de los octetos. El siguiente ejemplo muestra este proceso. Suponga que una empresa elige la dirección privada 10.0.0.0/8 como su dirección de red interna. Dicha dirección de red puede conectar 16777214 hosts en el dominio de transmisión. Obviamente, tener más de 16 millones de hosts en una sola subred no es lo ideal.

Como se muestra en la tabla, la empresa puede subdividir aún más la dirección 10.0.0.0/8 en un límite de 16 octetos. Esto permitirá a la empresa definir hasta 256 subredes (es decir, 10.0.0.0/16-10.255.0.0/16), cada una de las cuales puede conectar 65.534 hosts. Observe cómo los dos primeros octetos identifican la parte de red de la dirección y los dos últimos octetos se utilizan para la dirección IP del host.
Red de sibredes 10.0.0.0/8 usando un /16

Dirección de subred (256 subredes posibles)	Rango de host (65.534 posibles hosts por subred)	Dirección
10.0.0.0/**16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
...	...	...
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

La planificación de la subred de la red requiere analizar los requisitos de uso de la red de la organización y la estructura de la subred. El punto de partida es realizar una investigación sobre los requisitos de la red. Esto significa mirar toda la red, incluidas Intranet y DMZ, y determinar cómo dividir cada zona. El plan de direcciones incluye determinar dónde se debe reservar la dirección (generalmente dentro de la DMZ) y dónde se requiere más flexibilidad (generalmente dentro de la intranet).

Cuando sea necesario reservar direcciones, el plan debe determinar cuántas subredes se necesitan y cuántos hosts por subred. Como se mencionó anteriormente, el espacio de direcciones IPv4 públicas en la DMZ generalmente lo requiere. Esto puede incluir el uso de VLSM.

En la intranet de una empresa, la reserva de direcciones no suele ser un problema. Esto se debe principalmente al uso de direcciones IPv4 privadas (incluida 10.0.0.0/8) y más de 16 millones de direcciones IPv4 de host.

Para la mayoría de las organizaciones, la cantidad de direcciones internas (intranet) permitidas por direcciones IPv4 privadas es más que suficiente. Para muchas organizaciones grandes e ISP,

incluso el espacio de direcciones IPv4 privado no es suficiente para satisfacer sus necesidades internas. Esta es otra razón para que la organización haga la transición a IPv6.

Para la intranet que usa direcciones IPv4 privadas y la DMZ que usa direcciones IPv4 públicas, es importante planificar y asignar direcciones.

Capítulo 12 – Asignación de Direcciones IPv6

IPv6 está diseñado como sucesor de IPv4. IPv6 tiene un espacio de direcciones de 128 bits más grande y puede proporcionar 340 decimales (es decir, 340 seguidos de 36 ceros). Sin embargo, IPv6 es más que direcciones más largas.

Cuando el IETF comenzó a desarrollar productos sucesores de IPv4, aprovechó la oportunidad para corregir las limitaciones de IPv4 e incluir mejoras. Un ejemplo es la versión 6 del Protocolo de mensajes de control de Internet (ICMPv6), que incluye la resolución de direcciones y la configuración automática de direcciones no ICMP para IPv4 (ICMPv4).

El agotamiento del espacio de direcciones IPv4 es un factor en la migración a IPv6. Dado que África, Asia y el resto del mundo están cada vez más conectados a Internet, las direcciones IPv4 no son suficientes para adaptarse a este crecimiento. Como se muestra en la figura, cuatro quintas partes de los RIR se quedan sin direcciones IPv4.

En teoría, IPv4 tiene hasta 4,3 mil millones de direcciones. La combinación de direcciones privadas y traducción de direcciones de red (NAT) es esencial para reducir la latencia del espacio de direcciones IPv4. NAT es problemático para muchas aplicaciones, causa retrasos y tiene limitaciones que dificultan gravemente la comunicación entre pares.

Con el aumento en el número de dispositivos móviles, los proveedores de telefonía móvil han liderado el camino en la transición a IPv6. Los dos principales proveedores de telefonía móvil de Estados Unidos informan que más del 90% de su tráfico se realiza a través de IPv6.

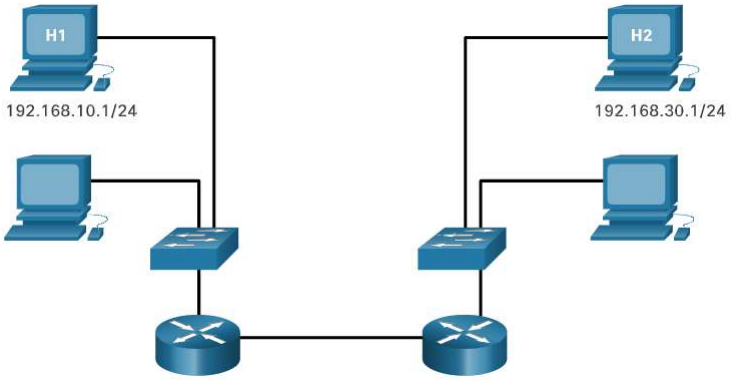
La mayoría de los principales proveedores de Internet y de contenido, como YouTube y Netflix, también han realizado la transición. Muchas empresas como Microsoft, Facebook y LinkedIn solo realizan la transición a IPv6 internamente. En 2018, el ISP de banda ancha Comcast (Comcast) informó un despliegue de más del 65%, y British Sky Broadcasting (British Sky Broadcasting) desplegó más del 86%.

Capítulo 13 – ICMP

Al comunicarse con otro dispositivo IP, la suite TCP / IP proporciona mensajes de error y mensajes de referencia. Estos mensajes se envían a través del servicio ICMP. Estos mensajes están destinados a proporcionar respuestas a temas relacionados con el procesamiento de paquetes IP bajo ciertas condiciones, no a hacer IP confiable. Los mensajes ICMP no son obligatorios y generalmente no se permiten dentro de la red por razones de seguridad. El protocolo ICMP se puede utilizar para IPv4 e IPv6. El protocolo de mensajes de IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero también incluye otras funciones. En este curso, el término ICMP se utilizará para hacer referencia a ICMPv4 e ICMPv6. Los tipos de mensajes ICMP y sus motivos para enviarlos son extensos. Los mensajes ICMP comunes de

ICMPv4 e ICMPv6 discutidos en este módulo incluyen: Accesibilidad del anfitrión Destino o servicio no accesible tiempo extraordinario

Los mensajes de eco ICMP se pueden utilizar para probar la accesibilidad de los hosts en la red IP. El host local envía una solicitud de eco ICMP al host. Si el host está disponible, el host de destino responde con una respuesta de eco. En la ilustración, haga clic en el botón "Reproducir" para ver la animación de la solicitud / respuesta de eco ICMP. Este uso de mensajes de eco ICMP es la base de la utilidad ping.



Mensajes ICMPv6

La información y los mensajes de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y error implementados en ICMPv4. Sin embargo, ICMPv6 tiene funciones nuevas y mejoradas que no se encuentran en ICMPv4. Los mensajes ICMPv6 se encapsulan en IPv6.

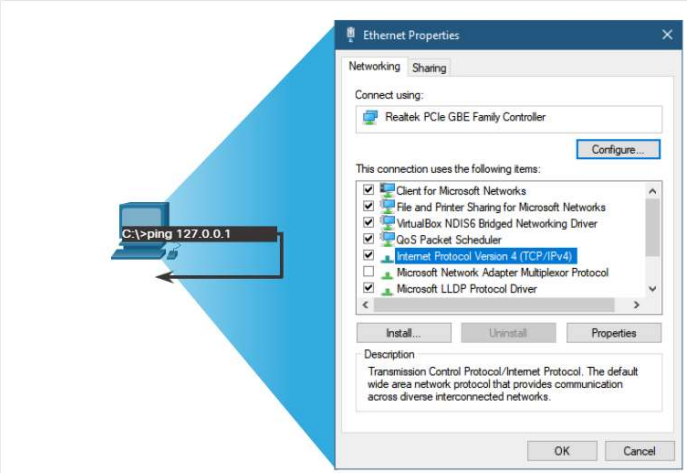
ICMPv6 contiene cuatro mensajes nuevos como parte del protocolo de descubrimiento de vecinos (ND o NDP).

Los mensajes entre los enrutadores IPv6 y los dispositivos IPv6, incluida la asignación dinámica de direcciones, son los siguientes:

Mensaje de solicitud de enrutador (RS)
Mensaje de anuncio de enrutador (RA)
Los mensajes entre dispositivos IPv6, incluida la detección de direcciones duplicadas y la resolución de direcciones, son los siguientes:

Solicitud de vecinos (NS)
Mensaje de anuncio de vecino (NA)

Para probar la conectividad con otro host en la red, use el siguiente comando para enviar una solicitud de eco a la dirección de ese host. ping Si el host en la dirección especificada recibe una solicitud de eco, responderá con una respuesta de eco. Después de recibir cada respuesta de eco, ping proporcionará información sobre el tiempo entre el envío de la solicitud y la recepción de la respuesta. Esto puede medir el rendimiento de la red.



Ping (utilizado por IPv4 e IPv6) utiliza la solicitud de eco ICMP y los mensajes de respuesta de eco para probar la conectividad entre los hosts. Para probar la conectividad con otro host en la red, use el comando ping para enviar una solicitud de eco a la dirección del host. Si el host en la dirección especificada recibe una solicitud de eco, responderá con una respuesta de eco. Después de recibir cada respuesta de eco, el comando ping proporcionará información sobre el tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. Después de enviar todas las solicitudes, la utilidad Ping proporcionará un resumen que incluye la tasa de éxito y el tiempo promedio de ida y vuelta al destino. Ping se puede utilizar para probar la configuración interna de IPv4 o IPv6 en el host local.

Haga ping a la dirección de bucle invertido local 127.0.0.1 para IPv4 (para IPv6 ::: 1). Utilice ping para probar la capacidad del host para comunicarse en la red local haciendo ping a la dirección IP de la puerta de enlace predeterminada del host. 1 Un ping exitoso a la puerta de enlace predeterminada significa que, de forma predeterminada, la interfaz del host y el enrutador actúan como la puerta de enlace predeterminada. El comando ping también se puede utilizar para probar la capacidad del host local para comunicarse a través de interconexiones. El host local puede ser un host desconectado de IPv4 en una red remota. Traceroute (tracert) genera una lista de saltos alcanzados con éxito en el camino.

Esta lista proporciona información de verificación y solución de problemas. Si los datos llegan al destino, la traza indicará la interfaz de cada enrutador que aparece en la ruta entre los hosts. Si los datos fallan en cualquier salto del proceso, la dirección del último enrutador en el seguimiento de respuesta puede indicar el problema o la restricción de seguridad. El tiempo de ida y vuelta es el tiempo que tarda un paquete de datos en llegar al host remoto y el host responde. Traceroute utiliza el campo TTL en IPv4 y el campo de límite de salto IPv6 en el encabezado de la capa 3 y la función de los mensajes de tiempo de espera ICMP.

BIBLIOGRAFÍA

Networking Academy CCNAv7 Recuperado el 10 de enero del 2021 de https://www.netacad.com/portal/learning