Universidad Israel

DEPARTAMENTO: Ciencias de la Ingeniería **PROFESOR:** Mg.Tannia Mayorga.
CARRERA: Sistemas de Información **ESTUDIANTE:** Marco Antonio Ayala Lituma
CURSO: Séptimo **PARALELO:** "A" **DESCRIPCIÓN:** Diario de Ingeniería
ASIGNATURA: Plataformas de Desarrollo 1

Diario de Ingeniería Completo

Contenido

Capítulo 1 – Las Redes en la actualidad

Hablando en la actualidad del año 2020 las redes son la base fundamental de la comunicación, de igual manera es fuente productiva económicamente a nivel mundial, dicho así las redes nos permiten de manera digital comunicarnos de varias maneras o herramientas como mensajes instantáneos, juegos simultáneos sin importar en el lugar donde te encuentres o comúnmente realizar videos llamadas y muchas cosas aún mas como saber información de muchas fuentes de publicación en varios idiomas gracias a internet que es el resultado de la red en la actualidad.

Hoy en día gracias a las redes podemos realizar muchas actividades cotidianas que lo hacíamos desde un lugar en específico pero en cambio con los avances de tecnología como en la actualidad que vivimos una pandemia todo se transformó y simplemente con la utilización de media base de redes, su adaptación y la continuidad tanto el académico, trabajo, incremento de software de comunicación y otros recursos según la necesidad del ambiente del día a día siendo así que no existe límites de comunicaciones.

Entonces para formar parte de las redes de comunicaciones en el mundo actual, puede ser de varias maneras o desde distintas herramientas a esto lo llamamos usuario final y puede ser desde un computador personal, una tablet o celular inteligente pero también existe otras como dispositivos IoT (Internet de las cosas) o Relojes inteligentes, Dispositivos de geoposicionamiento o GPS, y muchas más, ahora bien todos estas debe estar conectados a internet o dependiendo su necesidad forman parte de una red.

Para conectarse a una red existen varias maneras como son medios inalámbricos o mediante cables de varios tipos, entre los mas comunes o de la actualidad es fibra óptica que son como su nombre lo indica son filamentos de fibra que pueden ser de vidrio o plástico y su mecanismo son por pulsaciones de luz también existe la común o tradicional que el cobre o el cable de red que son micro cables que su composición lo hace mas rustico y su mecanismo de funcionamiento son los impulsos eléctricos.

Ya hemos mencionado los dispositivos cliente y sobre la conectividad, también existe otro componente que son los dispositivos intermedios que sirven para conectar a más dispositivos y es el que administra, controla, da seguridad y varias funciones sobre la utilización de la red.

Ahora bien, hemos descrito sobre la actualidad de las redes pero si aterrizamos en un ejemplo muy claro sobre las redes y su utilización de una empresa pequeña que puede estar conectado un router al servidor que esta funcionado el sistema de facturación, mientras en la contra parte los usuarios finales o computadores de los empleados está conectado también al router para estar comunicados con el sistema de igual manera el sistema de telefonía está conectado al router, dicho así el esto se conoce como una red LAN, ahora si pensamos que la empresa pequeña crece y necesita una sucursal esta tendría también que estar conectada y también tendría que tener conexión interna y externa para esta comunicados toda la organización esto se conoce como red WAN

La arquitectura de una red debe tener ciertas características como tolerancia a fallas, ya que puede haber desperfecto o desconfiguraciones en la misma que pueda ser solventada rápidamente, de igual manera una estabilidad es decir que su diagrama de arquitectura debe ser claro y abierto a incremento de equipos conectados a la misma red, ahora tenemos la calidad de servicio que es un elemento muy importante y depende de los dos elementos anteriores para que su calidad o buen servicio sea optimo, finalmente tenemos un elemento también importante ya que los equipos debe estar con las seguridades de acceso ya que si hubiera un acceso abierto podemos tener fallos internos tanto técnicamente como perdida de información de negocio de la organización u otra índole.

Con la Evolución de las comunicaciones de igual manera las maneras de conectarse a la red generan nuevas herramientas de trabajo u cotidianidad del ambientes digital es mismo como son el dispositivo móvil que portan muchas personas tanto de manera personal como de trabajo, siendo así que las tendencias de recientes hacen que la colaboración en línea se mas practica e instantánea, de igual forma podemos decir sobre la domótica con casa inteligentes y el lo profesional como la computación en la nube que es un concepto transformando para tener organización digitalizadas de forma que puedan administrar desde cualquier parte del mundo en todos sus procesos, todos estos conceptos hace que una red conectada vía internet este intercomunicada de manera privada y publica de manera de controlarse desde la palma de la mano.

Un concepto muy importante de red también es la seguridad de la información ya que esta sin no tener controles puede ser muy sensible para los usuarios vulnerables, en la actualidad no existe alguna solución estándar, pero si herramientas que previene dichos ataques; a los componentes básicos de seguridad que puede ser de tipo antivirus y antispyware o el filtrado de firewall.

Siendo las redes conceptos externos y que ingenieros que construyeron esta arquitectura para formar todas las comunicaciones del mundo de igual forma un profesional de redes es muy cotizado ya que siendo en una organización su conectividad debe estar administrada y el modulo de CCNA otorga su aprendizaje y certifica la preparación de un experto.

Capítulo 2 - Configuración básica de switches y dispositivos finales

En este Capitulo se habla sobre su configuración siendo que son equipos técnicos cada dispositivos final o equipo de red contiene un software base o sistema operativo mismo que contiene de manera lógica o intangible los funciones como actuara el equipo configurado, y par acceder al mismo se puede utilizar varias herramientas de emulación de la terminal como puTTY, Tera Term o SecureCRT estas herramientas con facilitan el acceso de manera remora es decir a una consola que mediante comandos podemos visualizar y modificar parámetros de acuerdo la configuración que se desee, también existen herramientas propias y de tercero que nos ayudan acceder de manera visual a las configuración.

Para Navegar en el equipo se tiene un concepto de modos la cual nos permite navegar de cierta manera limitada según la administración es decir si la ejecución de comando es de un usuario normal que quiero visualizar información pues podrá ejecutar los comandos normales, pero si necesita realizar modificaciones o actualización de parámetros debe ingresar con el modo privilegiado.

Ahora puede ingresar al equipo mediante consola o ambiente gráfico, dicho está pero la utilización de comandos debe tener una estructura y orden de ejecución así que se debe tener en cuenta su sintaxis de forma general para realizar las configuraciones necesarias, de igual manera desde la herramientas que utilice la comprobación de las palabras claves que utilizara se validara internamente y cuando la ejecute si la escribió bien se procederá con la acción caso contrario mostrar un error, para esto debe aprender algunos comando básicos como colocar nombres a los equipos, colocar claves en los equipos, encriptar sus credenciales, configuración de direcciones IP, validación de conectividad, restricciones de acceso, entre otras y guardar información de respaldo de dichas configuraciones.

Aquí aprendimos a utilizar la herramienta Packet Tracert la misma que nos permitió crear ambiente de redes, configurar y probar dicha conexión colocando un computador y switch conectado, a esto ejecutamos los comandos de privilegios dando nombre al equipo, asignado direcciones y agregando seguridades.

Capítulo 3 – Protocolos y Modelos

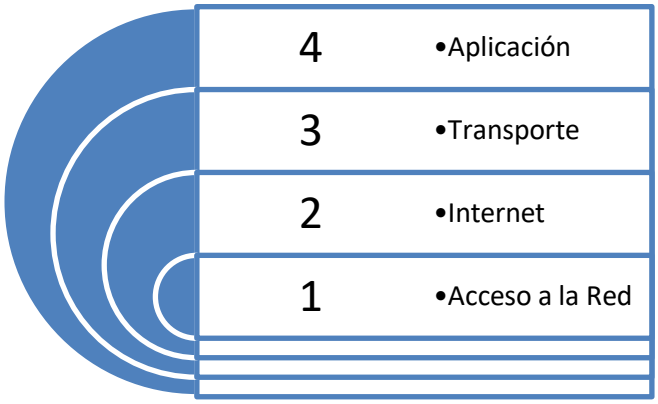
En este modulo nos enseñó la parte técnica interna como la red entra en funcionamiento y como validamos que las configuraciones realizadas están ejecutándose en el mismo hecho tenemos las reglas como deben aplicarse a la base de la comunicación desde el emisor y el receptor como se manipulan los mensajes, tamaño de mensajes, tiempo de duración y la forma de entrega de dichos menajes.

Entonces ya hemos descrito que se necesita reglas para establecer comunicación entre dispositivos esto conlleva hablar de protocolos, esto significa que la comunicación debe tener al menos los protocolos de comunicación de a red como son HTTP,UDP, TCP entre otros, también debemos tener en cuenta un protocolo de seguridad y es la que se encarga sobre la integridad de la información, encriptación de datos que se envía, de igual manera sobre la autenticación con credenciales y se utilizan protocolos estándares como SSH, SSL, TSL.

Existe varios protocolos de comunicación de los cuales los más utilizados de acuerdo a la utilización o necesidad en base lo es TCP/IP del más común ya que nos permite tener un conjunto de sub-protocolos que lo hace potente para trabajar con en la transferencia de datos de manera confiable

Diagrama de modelo OSI y TCP

En respecto al modelo TPC /IP solo tiene cuatro capas



De acuerdo con el modelo OSI la segmentación de mensajes tiene características importantes ya que al enviar mensajes esta se puede dividir en varias partes y en cada capa se encarga de secuenciar cada segmente para que el protocolo de datos PDU lo pueda utilizar.

Ahora bien, cuando la información ha llegado a la capa de acceso de datos este contiene ya la transformación íntegra en su destino de dirección IP. Ya que el remitente y quien recepta los paquetes en la dirección IP deben estar en la misma red, aquí también existe otro concepto importante como lo es una dirección única del medio de red o cliente que son una dirección de control de acceso a medios internet o MAC. Cuando el remitente del paquete está en una red diferente a la del receptor, las direcciones IP de origen y destino representarán hosts en diferentes redes. La trama de Ethernet debe enviarse a otro dispositivo conocido como enrutador o puerta de enlace predeterminada.

Capítulo 4 – Capa Física

De acuerdo con el modelo OSI la capa física es la ultima como lo detallamos en el anterior capitulo, entonces nos referimos a la parte tangible lo que sino tenemos los equipos o dispositivos conectados físicamente no existiría una conectividad de red. Claro está que también existen dispositivos inalámbricos, pero si no existiera una interfaz de cualquier medio esta no cumpliría con el concepto de red, entonces regresando al punto de la capa física esta tiene como propósito establecer una conectividad en los medios otorgados como hardware y será en intermediario para que dicha comunica se establezca.

Tres tipos de cableado de cobre son : UTP, STP y cable coaxial (coaxial). El cable STP utiliza cuatro pares de cables, cada uno envuelto en un blindaje de lámina, que luego se envuelve en una trenza o lámina metálica en general. Cable coaxial, o coaxial para abreviar, recibe su nombre del hecho de que hay dos conductores que comparten el mismo eje. El cable coaxial se utiliza para conectar antenas a dispositivos inalámbricos. Los proveedores de Internet por cable utilizan cable coaxial dentro de las instalaciones de sus clientes.

El cable UTP no usa blindaje para contrarrestar los efectos de EMI y RFI. El cableado UTP cumple con los estándares establecidos conjuntamente por la TIA / EIA. Las características eléctricas del cableado de cobre están definidas por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). El cable UTP suele terminar con un conector RJ - 45.

El cable de fibra óptica puede transmitir señales con menos atenuación que el cable de cobre y es completamente inmune a EMI y RFI. La fibra óptica es una hebra transparente, flexible, pero extremadamente delgada, de vidrio muy puro, no mucho más grande que un cabello humano. Hay cuatro tipos de conectores de fibra óptica: ST, SC, LC y LC multimodo dúplex. Los cables de

conexión de fibra óptica incluyen SC - SC multimodo, LC - LC monomodo, ST - LC multimodo y SC - ST monomodo.

La tecnología inalámbrica tiene algunas limitaciones, que incluyen: área de cobertura, interferencia, seguridad y los problemas que ocurren con cualquier medio compartido. Los estándares inalámbricos incluyen los siguientes: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16) y Zigbee (IEEE 802.15. La LAN inalámbrica (WLAN) requiere un AP inalámbrico y adaptadores NIC inalámbricos.

Capítulo 5 Sistema Numéricos

Este tema presentó algunas formas de convertir decimal a binario y binario a decimal. Sistema numérico hexadecimal, Así como el decimal es un sistema numérico de base diez, el hexadecimal es un sistema de base dieciséis. El sistema de numeración hexadecimal se utiliza en redes para representar direcciones IPv6 y direcciones MAC Ethernet. Las direcciones IPv6 tienen una longitud de 128 bits y cada 4 bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales. Para convertir hexadecimal a decimal, primero debe convertir el hexadecimal a binario, luego convertir el binario a decimal. Para convertir decimal a hexadecimal, primero debe convertir el decimal a binario.

Capítulo 6 – Capa de Enlace de Datos

Objetivo de la capa de enlace de datos.

La capa de enlace de datos del modelo OSI (Capa 2) elabora los datos de la red para la red física.

Sin la capa de enlace de datos, un protocolo de capa de red, de la misma forma que IP, tendría que tomar medidas para conectarse con todos los tipos de medios que tengan la posibilidad de existir durante la ruta de envío.

Se usa un procedimiento conveniente de control de ingreso a los medios para entrar a cada enlace.

La capa de enlace de datos “ve” la topología lógica de una red al mantener el control de el ingreso de datos a los medios.

La topología lógica influye en el tipo de trama de red y el control de ingreso a medios usado.

Hay 2 procedimientos básicos de control de ingreso para medios compartidos: el ingreso con base en contencion y el ingreso controlado.

La capa de enlace de datos elabora los datos encapsulados (generalmente un paquete IPv4 o IPv6) para el transporte por medio de los medios locales encapsulándolos con un encabezado y un trailer para generar una trama.

El protocolo de enlace de datos es responsable de las comunicaciones de NIC a NIC en la misma red.

Hay varios protocolos diferentes de capa de enlace de datos que describen marcos de capa de enlace de datos, cada tipo de marco tiene 3 piezas primordiales: encabezado, datos y trailer.

De acuerdo con el ámbito, la proporción de información de control que es necesario en la trama cambia para llevar a cabo con los requisitos de control de ingreso al medio de la topología lógica y de los medios.

La capa de enlace de datos otorga direccionamiento usado para transportar un marco por medio de medios locales compartidos.

El direccionamiento de la capa de enlace de datos está contenido en el encabezado de la trama y especifica el nodo de destino de la trama en la red local.

La dirección de la capa de enlace de datos solo se utiliza para la entrega local.

En una red TCP/IP, todos los protocolos de capa 2 del modelo OSI funcionan con la dirección IP en la capa 3.

No obstante, el protocolo de capa 2 específico que se utilice es dependiente de la topología lógica y de los medios físicos

Cada protocolo ejecuta el control de ingreso a los medios para las topologías lógicas de Capa 2 que se especifican

Los protocolos de capa de enlace de datos incluyen: Ethernet, 802.11 Wireless, PPP, HDLC y Frame Relay.

Capítulo 7 - Switching Ethernet

Ethernet funciona en la capa de enlace de datos y en la capa física.

Ethernet usa las subcapas LLC y MAC de la capa de enlace de datos para operar.

Los campos de trama Ethernet son: delimitador de trama de preámbulo y inicio, dirección MAC de destino, dirección MAC de procedencia, EtherType, datos y FCS.

La dirección MAC se usa para detectar los dispositivos físicos de procedencia y destino (NIC) en el segmento de red local.

El direccionamiento MAC da un procedimiento para la identificación del dispositivo en la capa de enlace de datos del modelo OSI.

Una vez que un dispositivo reenvía un mensaje a una red Ethernet, el encabezado Ethernet incluye las direcciones MAC de procedencia y destino.

En Ethernet, se aplican diferentes direcciones MAC para las comunicaciones de unicast, broadcast y multicast de capa 2.

La tabla de direcciones MAC.

Un switch Ethernet de capa 2 toma sus elecciones de reenvío basándose únicamente en las direcciones MAC Ethernet de capa 2.

El switch arma la tabla de direcciones MAC de forma dinámica luego de analizar la dirección MAC de procedencia de las tramas recibidas en un puerto.

El switch reenvía las tramas luego de buscar una coincidencia entre la dirección MAC de destino de la trama y una entrada de la tabla de direcciones MAC.

Mientras un switch obtiene tramas de diferentes dispositivos, puede terminar la tabla de direcciones MAC examinando la dirección MAC de cada trama.

Una vez que la tabla de direcciones MAC del switch tiene la dirección MAC de destino, puede filtrar la trama y reenviar un solo puerto.

Capítulo 8 – Capa de Red

IP encapsula el segmento de la capa de transporte añadiendo un encabezado IP, que se usa para dar el paquete al host de destino.

Los campos significativos del encabezado IPv6 incluyen: versión, DS, suma de comprobación de encabezado, TTL, protocolo y direcciones IPv4 de procedencia y destino.

Los campos en el encabezado del paquete IPv6 incluyen: versión, clase de tráfico, etiqueta de flujo, longitud de la carga eficaz, siguiente encabezado, límite de salto y las direcciones IPv6 de procedencia y destino.

Un host puede mandar un paquete a él mismo, a otro host local y a un host remoto.

En IPv4, el dispositivo de procedencia usa su propia máscara de subred junto con su propia dirección IPv4 y la dirección IPv4 de destino para decidir si el host de destino está en la misma red.

En IPv6, el router local anuncia la dirección de red local (prefijo) a todos los dispositivos de la red, para hacer esta decisión.

En una red, una puerta de enlace predeterminada frecuenta ser un router que tiene una dirección IP local en el mismo rango de direcciones que otros hosts de la red local, puede admitir datos en la red local y reenviar datos fuera de la red local, y enrutar el tráfico a otras redes.

Una tabla de enrutamiento de host principalmente incluirá una puerta de enlace predeterminada.

En IPv4, el host obtiene la dirección IPv4 de la puerta de enlace predeterminada de manera dinámica por medio de DHCP o se configura manualmente.

En IPv6, el router anuncia la dirección de la puerta de enlace predeterminada o el host se puede configurar manualmente.

¿En un host de Windows, el comando route print o netstat -r se puede utilizar para demostrar la tabla de enrutamiento del host?

Una vez que un host envía un paquete a otro host, consulta su tabla de enrutamiento para establecer dónde mandar el paquete.

Si el host de destino está en una red remota, el paquete se reenvía a la puerta de enlace predeterminada, que principalmente es el router local.

El router revisa la dirección IP de destino del paquete y busca en su tabla de enrutamiento para decidir dónde reenviar el paquete.

La tabla de enrutamiento tiene una lista de cada una de las direcciones de red conocidas (prefijos) y a dónde reenviar el paquete.

La tabla de enrutamiento de un router almacena 3 tipos de entradas de ruta: redes conectadas de manera directa, redes remotas y una ruta predeterminada.

El comando EXEC mode espectáculo ip route privilegiado se usa para ver la tabla de enrutamiento IPv4 en un router Cisco IOS

Al inicio de una tabla de enrutamiento IPv4 hay un código que se usa para detectar el tipo de ruta o cómo se aprendió la ruta:

- L - Dirección IP de interfaz local conectada directamente
- C - Red conectada directamente
- S - La ruta estática fue configurada manualmente por un administrador
- O - Open Shortest Path First (OSPF)
- D - Enhanced Interior Gateway Routing Protocol (EIGRP)

Capítulo 9 – Resolver Direcciones

Las direcciones físicas de capa 2 (es decir, las direcciones MAC de Ethernet) se usan para dar la trama de enlace de datos con el paquete IP encapsulado de una NIC a otra NIC que está en la misma red.

Si la dirección IP de destino está en la misma red, la dirección MAC de destino es la del dispositivo de destino.

Una vez que la dirección IP de destino (IPv4 o IPv6) está en una red remota, la dirección MAC de destino va a ser la dirección de gateway predeterminada del host (es decir, la interfaz del router).

Si el dispositivo del siguiente salto es el destino final, la dirección MAC de destino es la de la NIC Ethernet del dispositivo?

Cada dispositivo IP de una red Ethernet tiene una dirección MAC Ethernet exclusiva.

Una vez que un dispositivo envía una trama de capa 2 de Ethernet, tiene estas 2 direcciones: dirección MAC de destino y dirección MAC de procedencia.

Un dispositivo usa ARP para establecer la dirección MAC de destino de un dispositivo local una vez que conoce su dirección IPv4.

La solicitud ARP se encapsula en una trama Ethernet usando esta información de encabezado: direcciones MAC de procedencia y destino y tipo.

Solo un dispositivo de la LAN tiene la dirección IPv4 que coincide con la dirección IPv4 objetivo de la solicitud de ARP.

Cuando obtiene la respuesta de ARP, el dispositivo añade la dirección IPv4 y la dirección MAC que corresponde a su tabla ARP.

Una vez que la dirección IPv4 de destino no está en la misma red que la dirección IPv4 de procedencia, el dispositivo de procedencia debería mandar la trama al gateway establecido.

Al igual que ARP para IPv4, los dispositivos IPv6 usan IPv6 ND para solucionar la dirección MAC de un dispositivo en una dirección IPv6 exitosa.

Capítulo 10 – Configuración Básica de un Router

Para que se logre llegar a los routers, se debería configurar la interfaz de router.

Las labores para configurar una interfaz de router resultan muy semejantes a un SVI de gestión en un switch.

La interfaz además debería estar conectada a otro dispositivo , como un switch o un router, para que la capa física se active.

Para que un terminal se comunique por medio de la red, se debería configurar con la información de dirección IP idónea, incluida la dirección de gateway establecido.

Generalmente, la dirección de gateway establecido es la dirección de la interfaz de router conectada a la red local del host.

La dirección IP del dispositivo host y la dirección de interfaz de router tienen que estar en la misma red.

Para configurar un gateway establecido en un switch, use el comando ip default-gateway ip-address de configuración universal Use la dirección IPv4 de la interfaz del enrutador local que está conectada al conmutador.

Estos son los pasos que debe seguir para configurar el router.

Las siguientes tareas deben completarse al configurar la configuración inicial en un enrutador.

- Configure el nombre del dispositivo.
- Proteja el modo EXEC con privilegios.
- Proteger el modo EXEC de usuario
- Proteger el acceso remoto por Telnet y SSH
- Proteja todas las contraseñas del archivo de configuración.
- Proporcione una notificación legal.

- Guarde la configuración.
- Configurar interfaces

De manera técnica:

```
R1 (config) # nombre de host R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1 (config) # cifrado de contraseña de servicio
R1 (config) # banner motd #
Escriba un mensaje de texto. Termina con una nueva línea y el #
**************************************************
WARNING: Unauthorized access is prohibited!
**************************************************
R1(config)# exit
R1# copy running-config startup-config
```

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.

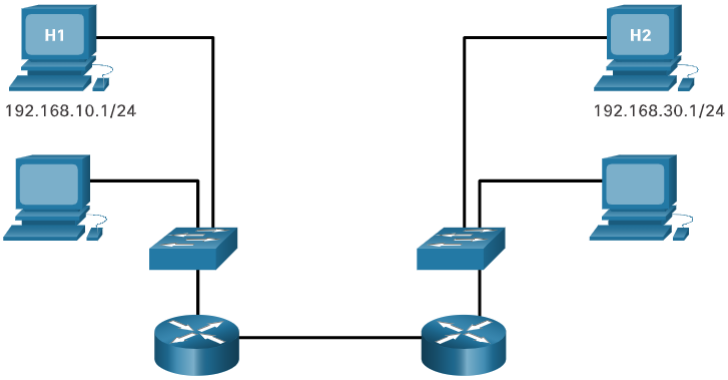
Con el aumento en el número de dispositivos móviles, los proveedores de telefonía móvil han liderado el camino en la transición a IPv6. Los dos principales proveedores de telefonía móvil de Estados Unidos informan que más del 90% de su tráfico se realiza a través de IPv6.

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.

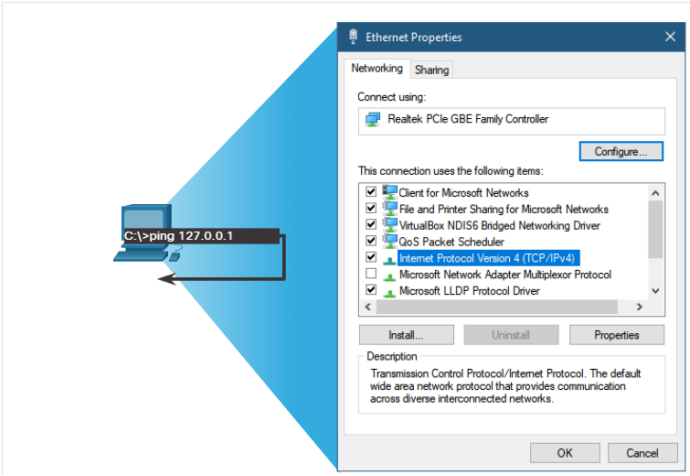
ICMPv6 contiene cuatro mensajes nuevos como parte del protocolo de descubrimiento de vecinos (ND o NDP).

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 01 febrero del 2021 de https://www.netacad.com/portal/learning