

Resumen Modulo 17

Crear una red pequeña

17.1 Dispositivos de una red pequeña

• **Topologías de redes pequeñas** → Un dispositivo de red pequeña es simple. La cantidad y tipo de dispositivos incluidos se reducen en comparación con una red grande.

Las redes grandes requieren un departamento de TI para mantener, proteger y solucionar problemas de red y proteger los datos de la organización. La administración de una red pequeña requiere muchas habilidades para administrar redes más grandes.

• **Selección de dispositivos para redes pequeñas** → Las redes requieren planificación y diseño para cumplir los requisitos del usuario. Las consideraciones de diseño es el tipo de dispositivos intermedios que se utilizarán para dar soporte a la red. **costo** → Los costos se determinan sobre las capacidades y características. Incluye la cantidad y los tipos de puertos disponibles, además de backplane. También se toma en cuenta el cable necesario para conectar cada dispositivo.

Velocidad y tipos de puertos/interfaces → Elegir la cantidad y tipo de puertos o switch es una cosa por tomar en cuenta. Algunos servers pueden tener puertos de 10 Gbps.

Capacidad de expansión → Los dispositivos de red incluyen configuraciones físicas modulares y fijas. Las configuraciones fijas tienen un tipo y cantidad específica de puertos que no aumentan.

Características y servicios de los sistemas operativos → Deben tener S.O. que admitan requisitos de organizaciones como: switching capa 3, NAT, DHCP, seguridad, QoS, VoIP.

• **Asignación de direcciones IP para redes pequeñas** → Todos los hosts dentro de una red interna deben tener una dirección exclusiva. Entre los dispositivos que se incluirán en el esquema de direccionamiento IP se incluye lo siguiente:

Dispositivos de usuario final: número y tipo de conexión. **Servidores y periféricos**: impresoras, etc.
Dispositivos intermedios: switches, access point.

Se recomienda planificar, documentar y mantener un esquema de direccionamiento IP basado en el tipo de dispositivo.

• **Redundancia en redes pequeñas** → Otra parte importante es la confiabilidad. Para mantener un alto grado de confiabilidad, se requiere **redundancia** en el diseño de red. La redundancia ayuda a eliminar puntos de error únicos. La redundancia se puede obtener la instalación de equipos duplicados, pero también se puede obtener al suministrar

enlaces de red duplicados en áreas fundamentales.

- **Administración del tráfico** → El objetivo del diseño de la red, es aumentar la productividad de empleados y reducir el tiempo de inactividad de la red. Los routers y switches en una red pequeña se deben configurar para admitir el tráfico en tiempo real, voz y video, de forma independiente del tráfico de otros datos. Prioridad: **Voz, SMTP, Mensajería instantánea, FTP**

17.2 Protocolos y aplicaciones de redes pequeñas

- **Aplicaciones comunes** → La utilidad de las redes dependen de las aplicaciones que se encuentran en ellas. Hay 2 programas que proporcionan acceso a la red:

Aplicaciones de red → Programas de software que se utilizan para comunicación. Algunas apps de usuario final reconocen la red, lo que significa que implementan protocolos de capa de aplicación. Clientes de correo y navegadores web son ejemplo.

Servicios de capa de aplicación → Los distintos tipos de datos, texto, gráfico o video requieren distintos servicios de red para asegurar que estén preparados para que los procesen las funciones de capas inferiores. Cada aplicación utilizará protocolos que definen los estándares y formatos de datos que se deben utilizar.

- **Protocolos comunes** → Los protocolos de red admiten servicios y aplicaciones que usan los usuarios. Las 2 soluciones de acceso remoto más comunes son Telnet y secure shell (SSH). SSH utiliza para conexiones remotas. **Dispositivo de red** → router, switch, debe admitir SSH para proporcionar acceso remoto a servicios de servidor SSH a clientes.

Servidor → Debe admitir servicios de Servidor SSH de acceso remoto a clientes.

Servidor web → HTTP y HTTPS.

Servidor DHCP → DHCP

Servidor de correo → SMTP, POP, IMAP.

Servidor DNS → DNS

Servidor FTP → FTP y SFTP

Definen los procesos en cualquier extremo de una sesión de comunicación, tipos de mensajes, sintaxis de los mensajes, campos informativos, como se envían los mensajes y respuesta e interacción con la siguiente capa inferior.

- **Aplicaciones de voz y video** → **Infraestructura** → La infraestructura de red debe admitir aplicaciones en tiempo real, dispositivos existentes y cableado deben ser probados y validos, productos de red recientes. **VoIP** → convierten la señal analógica de los teléfonos en paquetes IP digitales, más económico que una solución de telefonía IP integrada.

Telefonía IP → Un teléfono IP la conversión de voz a IP con el uso de un servidor dedicado para el control de llamadas y señalización.

Aplicaciones en tiempo real → Debe admitir mecanismos de calidad para minimizar latencia de aplicaciones. RTP y RTCP.

17.3 Escalar hacia redes más grandes

- Crecimiento de las redes pequeñas → El crecimiento de una red se denomina **escalar una red**. Para extender una red, se requieren varios elementos:
Documentación de la red → Topologías física y lógica. **Inventarios de dispositivos** → Lista de dispositivos que utilizan o forman la red. **Presupuesto** → Presupuesto de TI detallado. **Ánálisis de tráfico** → Se deben registrar los protocolos, aplicaciones, servicios y requisitos tráfico.
Ánálisis de protocolos → Es importante saber el tipo de tráfico que atraviesa la red así como el flujo de tráfico. Hay varias herramientas de administración de red que se pueden utilizar para este propósito. También se puede utilizar un analizador de protocolos simple como Wireshark. Para determinar los patrones de flujo de tráfico es importante capturar tráfico en horas de uso pico para obtener buena representación de tipos de tráfico y realizar la captura de diferentes segmentos de red y dispositivos. La información recopilada se evalúa de acuerdo al origen y destino del tráfico y con el tipo de tráfico que se envía. Puede ayudar a la toma de decisiones para administrar el tráfico.
Utilización de la red por parte de los empleados → Muchos S.O. proporcionan herramientas de red para mostrar dicha información. Estas herramientas se pueden utilizar para capturar una «instantánea» de la información como: **SO y versión SO, utilización de CPU, utilización de RAM, utilización de unidades, aplicaciones que no usan red y aplicaciones de red**. Documentar instantáneas es muy útil para identificar los requisitos de crecimiento y flujos de tráfico asociados. La herramienta uso de datos se accede mediante **Settings > Network & Internet > Data usage > network interface**.

17.4 Verificar la conectividad

- Verificar la conectividad con Ping → El ping es comando más eficaz de probar rápidamente la conectividad de capa 3 entre origen y destino. Muestra estadísticas acerca del tiempo de ida y vuelta. Usa los mensajes eco del protocolo de mensajes de control de internet (ICMP tipo 8) y respuesta eco (ICMP tipo 0). Indicadores de ping los:
! Recepción correcta, • el tiempo expiró en espera de un mensaje de eco, U un router

en mayúsculas indica un router a lo largo de la ruta respondió "unreachable".

● Ping extendido → Un estándar ping utiliza la IP de origen más cercana y toma la destino como origen de ping. El modo "extendido". Permite al usuario crear un tipo especial de pings ajustando los parámetros relacionados con la operación de comando. Se ingresa en modo EXEC privilegiado escribiendo ping sin una IP de destino. Selecciónarán varias indicaciones para personalizar el extendido ping.

● Verificar la conectividad con traceroute → Ping es útil para determinar rápidamente si existe un problema de conectividad de capa 3. No identifica dónde se encuentra el problema a lo largo de la ruta. Un traceroute proporciona una lista de saltos cuando un paquete se enruta a través de una red. Se podrá utilizar para identificar el punto a lo largo de la ruta donde se puede encontrar el problema. traceroute ip / traceroute *
Se usa ctrl-c para interrumpirlo en windows. Un * significa que el router del siguiente salto no respondió.

● Traceroute extendido → Permite ajustar los parámetros relacionados con la operación del comando. Sirve para solucionar bades de enrutamiento, determinando el router de siguiente salto o dónde los paquetes son descartados. La opción para cisco permite al usuario crear un tipo especial de traceroute ajustando los parámetros relacionados con la operación del comando. Es solo en EXEC privilegiado Solo traceroute.

● Línea base de red → La medición del rendimiento en distintos momentos y con distintas cargas ayuda a tener una idea más precisa del rendimiento de la red. Un método para iniciar una línea base es copiar y pegar los resultados de ping, traceroute, en un.txt. Se deben considerar. Hay herramientas que almacenan y mantienen la información de línea de base. Las mejores prácticas de cisco Se encuentran como "mejores prácticas de proceso Baseline".

17.5 Comandos de host y de los

● Configuración de IP en un host windows → Los comandos de host e los pueden determinar el problema está relacionado con el direccionamiento IP de sus dispositivos, que es un problema común de red. En windows 10, puedes acceder a los detalles de la IP desde network and sharing center. Se visualiza dirección, máscara, router y DNS. Con comando se utiliza ipconfig en el cmd. También se usa el comando ipconfigall para visualizar la MAC y datos capa 3.

Si un host está configurado como cliente DHCP, la configuración de la IP se puede renovar utilizando los comandos `ipconfig /release` `ipconfig /renew`. El comando `ipconfig /displaydns` muestra todas las entradas DNS en caché en un sistema Windows.

Configuración de IP en un host Linux → La verificación de la configuración IP usando la GUI en una máquina Linux variará dependiendo de la distribución Linux y la interfaz de escritorio. En la terminal se usa el comando `ifconfig` para mostrar el estado de las interfaces activas y su IP. El comando `ip address` se utiliza para mostrar direcciones y sus propiedades.

Configuración de IP en un host macOS → Network preferences > advanced. El comando `ifconfig` también se puede utilizar para verificar la configuración IP de la interfaz. Otros comandos para verificar la configuración incluyen: `networksetup -listallnetworkservices` y `networksetup -getinfo <network service>`

El comando arp → Este comando se ejecuta desde el cmd, enumera todos los dispositivos que se encuentran en la caché ARP del host, incluye dirección IPv4, dirección física y tipo de direccionamiento (estático/dinámico) para cada dispositivo. El comando `arp -a` muestra los vínculos entre la dirección IP y la dirección MAC. Solo muestra información de dispositivos a los que se ha accedido recientemente. Para borrar la caché mediante `netsh interface ip delete arpcache` en caso de llenarla con información actualizada.

Reaso de comandos show comunes → Verifica...

`Show running-config`

Configuración actual

`Sh interfaces`

Estado de la interfaz y mensajes de error

`Sh ip interface`

información de la capa 3 de una interfaz

`Sh arp`

lista de hosts conocidos en LAN locales

`Sh ip route`

información de enrutamiento de capa 3

`Sh protocols`

Protocolos estás operativos

`Sh version`

Memoria, las interfaces y licencias del dispositivo

Comando `Show cdp neighbors` → Se ejecuta en la capa de enlace de datos. Descubre automáticamente los dispositivos vecinos que ejecutan ese protocolo. Intercambia información del hardware y software del dispositivo con sus vecinos. Brinda:

Identificadores, lista de direcciones, identificador del puerto, lista de capacidades, plataforma. `Show cdp neighbor`, `Show cdp neighbors detail`, `No cdp run`, `No cdp enable`.

El comando show ip interface brief → Show ip interface brief proporciona un resultado más abreviado que el sh ip int. Muestra todas las interfaces del router, la dirección IP asignada a cada interfaz y su funcionamiento. También se puede utilizar para verificar el estado de las interfaces del switch.

17.6 Metodologías para la solución de problemas

Enfoques básicos para la solución de problemas → Se visualizarán por pasos:

- 1- Identificar el problema,
- 2- Establecer una teoría de causas probables,
- 3- Poner a prueba la teoría para determinar la causa,
- 4- Establecer un plan de acción e implementar la solución,
- 5- Verificar la solución e implementar medidas preventivas,
- 6- Registrar hallazgos, acciones y resultados.

Solucionar o escalar? Un problema debería escalarse cuando requiere la decisión del gerente, experiencia específica, nivel de acceso a la red, no esté disponible para el técnico que soluciona el problema. Por ejemplo un técnico que ocupa cambiar un router, el problema debe escalar para la aprobación del gerente. Puede escalar más.

Comando debug → Permite que el administrador muestre los mensajes en tiempo real para su análisis. Se usan en el modo exec de privilegio. Solo se usan para trabajar **problemas específicos**. Puede usar debug ip icmp para ver el estado de mensajes de ICMP en un router. Para depurarlo sin debug ip icmp, undebug ip icmp para la misma función. undebug all.

Monitor terminal de comandos → Puede haber 2 conexiones para otorgar acceso:

Localmente → Requieren acceso físico a router o switch a través de un cable.

Remotamente → Requiere SSH para establecer conexión a dispositivos.

Se puede utilizar **terminal monitor** para realizar mensajes largos en la terminal, se usa en modo privilegiado. Se detienen con terminal no monitor.

17.7 Escenarios de resolución de problemas

Problemas de funcionamiento dúplex y discordancia → Cuando se trata de comunicación de datos, **dúplex** se refiere a la dirección de la transmisión de datos entre dos dispositivos. Hay 2 formas de comunicación dúplex:



Half duplex → El intercambio de datos es a una dirección a la vez.

Full duplex → Se permite enviar y recibir simultáneamente.

Las interfaces de interconexión Ethernet deben funcionar en el mismo dúplex para un mejor rendimiento de comunicación. Los dispositivos primero **anuncian sus capacidades utilizadas** y luego eligen el modo de mayor rendimiento soportado por los extremos. Una incongruencia duplex suelen ser difíciles de resolver mientras los dispositivos se comunican entre sí.

● Problemas de asignación de direcciones IP en dispositivos IOS → Dos causas comunes de IPv4 son los errores manuales o problemas con DHCP. La asignación manual se realiza a servers y routers. Para comprobación de IPv4 use **show int br**.

● Problemas de asignación de direcciones IP en terminales → Si un equipo windows no se comunica con un DHCP, windows asigna una dirección del rango **169.254.0.0/16**. Se denomina **Dirección IP Privada automática (APIPA)** y facilita comunicación dentro de la LAN. No podrá comunicarse con otros dispositivos de la LAN porque no pertenecen a la misma LAN. Puede usar **ipconfig** para ver las ip que tiene, máscara de subred y gateway.

● Problemas con el gateway → El gateway es el dispositivo (router) de red más cercano que puede reenviar tráfico. Si un host no tiene bien el gateway no podrá comunicarse. Los problemas suelen relacionarse con la configuración incorrecta o DHCP. Para resolverlos asegúrese que el dispositivo tenga bien configurado el gateway. Si es dinámica asegúrese que el dispositivo pueda comunicarse con DHCP. Puede usar los comandos: **ipconfig, show route, show begin gateway**.

● Solución de problemas DNS → DNS hace coincidir los nombres de una página con la IP. Los servidores DNS mantenidos por un ISP son asignados a los clientes SOHO mediante DHCP. Para verificar que DNS usa la computadora use el comando **ipconfig /all**. También el comando **nslookup** puede usarse para mostrar el resultado de una consulta para una página.