UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

CAMPUS ARAGON

"EL ENRUTADOR MARCA CISCO Y SUS PROBLEMAS EN LA RED"

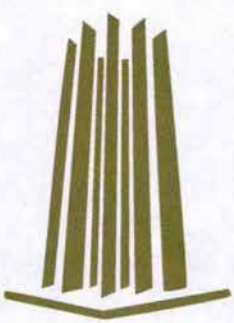
T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A :

JOSE LUIS HERNANDEZ MEDINA



ASESOR: ING. ELEAZAR MARGARITO PINEDA DIAZ

SAN JUAN DE ARAGON EDO. DE MEXICO **2004**

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

SECRETARÍA ACADÉMICA

UNIVERSIDAD NACIONAL AVENOMA DE MEXICO

Ing. RAÚL BARRÓN VERA
Jefe de la Carrera de Ingeniería Mecánica Eléctrica,
Presente.

En atención a la solicitud de fecha 17 de noviembre del año en curso, por la que se comunica que el alumno JOSE LUIS HERNANDEZ MEDINA, de la carrera de Ingeniero Mecánico Electricista, ha concluido su trabajo de investigación intitulado "EL ENRUTADOR MARCA CISCO Y SUS PROBLEMAS EN LA RED", y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 17 de noviembre del 2003
EL SECRETARIO

Lic. ALBERTO IBARRA ROSAS

C p Asesor de Tesis.
C p Interesado.

AIR/

UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN
DIRECCIÓN

DUPLICADO

JOSÉ LUIS HERNÁNDEZ MEDINA
P R E S E N T E

En contestación a su solicitud de fecha 11 de septiembre de 2001, relativa a la autorización que se le debe conceder para que el señor profesor, Ing. ELEAZAR MARGARITO PINEDA DIAZ pueda dirigirle el trabajo de tesis denominado "EL ENRUTADOR MARCA CISCO Y SUS PROBLEMAS EN LA RED", con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobada su solicitud.

Aprovecho la ocasión para reiterarle mi distinguida consideración.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México 10 de noviembre de 2003
LA DIRECTORA

ARQ. LILIA TURCOTT GONZÁLEZ

U.N.A.M. ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN
DIRECCION

Nota: La aceptación del tema de tesis y asesor de la misma fue registrada en la Secretaría Académica de esta Escuela con fecha 19 de septiembre de 2001.

C p Secretaría Académica.
C p Jefatura de la Carrera de Ingeniería Mecánica Eléctrica.
C p Asesor de Tesis.

LTG/AIR/agm

El Enrutador marca Cisco y sus problemas en la red

Índice

Agradecimientos..... I

Introducción II

TEMA 1. Conceptos Generales. 1

1.1 Equipo Cisco..... 1
1.2 La certificación Cisco..... 9
1.3 Administración de la red..... 11
1.4 Seguridad de tráfico y de usuario..... 17
1.5 Tecnologías de redes..... 21

TEMA 2. Redes Cisco..... 28

2.1 Fundamentos..... 28
2.2 Modelo de diseño..... 32
2.3 Método de diseño..... 38
2.4 Necesidades de la red..... 42
2.5 Caracterización de la red..... 43
2.6 La red lógica..... 48
2.7 La red de campo..... 55

TEMA 3. El enrutador Cisco..... 70

3.1 Introducción..... 70
3.2 Puntos de conexión..... 73
3.3 Contraseñas..... 78
3.4 Hardware del Enrutador..... 82
3.4.1 Memorias..... 83
3.4.2 Módulos y puertos del enrutador..... 84

3.5 Software del Enrutador 87
3.5.1 El sistema operativo de redes 87
3.5.2 El archivo de configuración 94
3.6 Configuración del Enrutador 104
3.6.1 Modo Setup 104
3.6.2 Protocolo de descubrimiento de Cisco 108
3.6.3 Aplicaciones de ayuda de configuración 110

TEMA 4. Problemas típicos en las redes Cisco 124

4.1 Introducción 124
4.2 Secuencia de solución 125
4.2.1 Comandos principales para la solución 125
4.2.2 Método de solución 126
4.2.3 Problemas de configuración 128
4.3 Problemas de conectividad 133
4.3.1 Configuración 133
4.3.2 Problemas de conexión 135
4.4 Problemas de enlace 150
4.4.1 El comando show interfaces serial 151
4.4.2 Problemas en la entrada de la línea 153
4.5 Problemas con el equipo 157
4.5.1 Secuencia 157
4.5.2 Inspección física de los dispositivos 158
4.5.3 Pruebas de reinicio 159

Conclusiones 160

Bibliografía 163

Agradecimientos

Quiero agradecer a Dios la oportunidad de existir, con la libertad de pensar y sentir, renovando siempre mi fe en él y en mi, pero sobretodo le agradezco tener, una Excelente e Irremplazable Madre, un Fuerte e Incomparable Padre, muchas gracias Señor.

Mamá, Gracias por todos estos años de buenos consejos, de tus muchos esfuerzos, por tu comprensión, por miles de abrazos y tan tiernos consuelos que me han ayudado a continuar. Mamá, eres parte importante de este logro de vida, gracias por alentarme e impulsarme a ser un buen hombre y un buen profesionista, gracias por enseñarme a valorar el tiempo y las oportunidades, por todo y mucho más. Gracias. Te quiero.

Papá, Gracias por que nunca me has dejado solo y si dejarme estar cerca de ti, gracias por todas las noches de desvelo, gracias por todos tus consejos, gracias por todos los buenos ratos que juntos compartimos dentro y fuera de tu trabajo estoy muy orgulloso de ti, gracias por enseñarme que siempre hay que hacer un buen trabajo, por todo, Gracias. Te quiero.

Gracias a todos mis **C**ompañeros y **C**ompañeras que me hicieron parte de sus vidas, gracias por compartir los bueno y los malos ratos, gracias por su apoyo, por sus consejos, y su fuerza que me animó a no quedarme atrás, gracias a todos ustedes.

Gracias a mis amigos, Gracias ***Bernardino*** por tú alegría que siempre me muestras y contagias, gracias por todos estos años de sincera amistad llenos sinceros consejos, experiencias, y buena música, y por que siempre me has demostrado que puedo confiar en ti en cualquier momento, gracias amigo. Gracias ***Julián*** por recordarme que las cosas no son fáciles, que los errores cuestan caro, y que sin embargo siempre hay que ser fuerte por que muchos dependen de nosotros, gracias por la confianza y el impulso a seguir pero sobretodo por tu sincera y singular amistad, muchas gracias amigo.

Gracias a todos mis **P**rofesores que me hicieron ver que la Ingeniería no es solo números, circuitos, y señales, sino que es entrega y dedicación, nuestra vida, muchas gracias porque me hicieron confiar en ustedes haciéndome sentirlos como unos buenos amigos.
Gracias a mi **A**sesor de tesis, Gracias *Ing. Eleazar Margarito Pineda Díaz*, por su paciencia, su tiempo, su experiencia y sus consejos que me ayudaron a realizar este trabajo de titulación.

Mi eterno agradecimiento a la ***Universidad Nacional Autónoma de México*** que me abrió sus puertas, gracias por alojarme en sus instalaciones donde me enseñó a crecer y a vivir dentro una comunidad comprometida a servir con ética y afrontar sin miedo nuevos obstáculos sin importar que tan adversos sean, Gracias, por estos años llenos de retos, alegrías, y tropiezos pero sobretodo lleno de satisfacciones que me las llevo en el alma, Gracias mi **UNAM**.

Y Gracias a todos aquellos, a y ti, que me ayudaron e inspiraron a ser mejor con sus consejos, su cariño y comprensión, mil gracias.

José Luis Hernández Medina

Ingeniero Mecánico Eléctrico

Introducción

En esta tesis se mostrara los productos Cisco así como su sistema operativo IOS, se describe a grandes rasgos la industria de las telecomunicaciones, se explica como coinciden las líneas de productos Cisco con distintos sectores de la industria de las comunicaciones.

La interconexión de redes es la conjugación de docenas de tecnologías sofisticadas y por lo tanto se describe como funcionan desde lo más básico, comenzando primero con las tecnologías LAN's más importantes tales como Ethernet y Token Ring, hasta las diferencias existentes entre ellas, inclusive las tecnologías básicas de alta velocidad como ATM y Gigabit Ethernet. También se debe diferenciar entre el trabajo de red orientado a la conexión y el trabajo sin conexión, y cómo se traducen los nombres de dominio a direcciones numéricas, además se tratan los elementos fundamentales de la red como el direccionamiento IP y las máscaras de subred, también se tratan las tecnologías de acceso telefónico como DSL, RDSI, así como las tecnologías troncales, T1 y T2, Frame Relay y ATM.

Al igual que otras empresas Cisco tiene un programa de certificación para los ingenieros que trabajan con sus productos, siendo las tres principales: Enrutamiento, Conmutación WAN y Acceso telefónico PSI. Las nuevas certificaciones Cisco para el diseño difieren de las que están vigentes para el soporte de red. Los objetivos de los exámenes para cada certificación son para beneficio de las empresas, para el contrato de personal calificado y del mismo ingeniero.

La administración de redes se ha convertido en un tema muy importante a medida que las redes han ido creciendo en tamaño y complejidad, en el tema se tratan los estándares y las tecnologías que subyacen a los sistemas de administración de redes, se explican los estándares de administración de red, así es como el enfoque de Cisco de su implementación. La seguridad de red que existe más allá de los cortafuegos es la seguridad basada en el usuario, que se utiliza para establecer y reforzar las contraseñas para accesar a las redes y las autorizaciones para utilizar los recursos de red.

Hay ciertos elementos básicos que hay que tener en consideración para un diseño de red, ya sea para toda una nueva red o para la expansión de una ya existente. Es hace un repaso de las interconexiones conmutadas frente a la enrutada, las redes VLAN, la necesidad de redundancia, etc. El modelo jerárquico de tres capas se repasa en términos de lo que hay que buscar en las capas de acceso, se repasan los temas de diseño claves, se explica como realizar un análisis completo de las necesidades de una nueva red y cómo introducirlo en soluciones de diseño utilizando los productos Cisco, tratando los factores de diseño, como los protocolos de enrutamiento, el diseño de direcciones, el enrutamiento frente a la conmutación, los servicios WAN y el equilibrio del tráfico de carga.

En los elementos básicos de los enrutadores de Cisco, se explican los componentes de hardware del enrutador y se detalla cómo los administradores de red pueden iniciar una sesión en los enrutadores Cisco para trabajar con ellos, incluyendo él reinicio para realizar tareas tan básicas como la recuperación de contraseñas. También se tratan los principales componentes software de los enrutadores Cisco, tanto la interfaz de comandos del IOS de Cisco como los conjuntos de características del mismo, se repasa la línea de productos de enrutadores de Cisco. Se toca el sistema operativo de Cisco IOS, la jerarquía de comandos, las utilidades y como utilizar el subsistema de ayuda. Pero la importancia radica en el control de archivo de configuración y como se utiliza para la configuración de los enrutadores en las redes, la sintaxis de los comandos, como leer los estados de los dispositivos y cómo leer los estados de los dispositivos y cómo configurar los parámetros clave de los enrutadores. Se repasan las herramientas software de configuración de Cisco.

Y por último se trata de cómo solucionar y examinar los problemas más típicos de red, así como utilizar la metodología más adecuada para su diagnostico y solución. Además de usar así como los comandos más importantes para encontrar y aislar problemas. También adecuar la métrica de los protocolos de enrutamiento y como solucionar problemas de servicio tales como los vínculos de las líneas serie.

Tema 1 Conceptos Generales

1.1 Equipos de Cisco System.

Lo que ofrece Cisco

Cisco System tiene la más amplia y completa línea de productos en el negocio de las redes. La línea de productos ha fluctuado constantemente durante los últimos años. Esto se debe en gran parte a la implacable introducción de nuevos estándares y tecnologías industriales, que provoca continuos giros en la línea de productos. Pero el flujo tiene mucho que ver con el afán de Cisco de conseguir tecnología mediante la compra de otras organizaciones. Cisco también ha adquirido proveedores de software dedicados a ofrecer soluciones en áreas como el diseño de redes y la administración.

Cisco ha pasado años siendo una de las primeras empresas de la industria vendedora de soluciones para la interconexión de redes y la tendencia natural de la empresa es de adaptarse a la tecnología en vez de luchar contra ella.

La línea de productos Cisco se puede dividir en dos categorías que son: Dispositivos y soluciones.

1. - DISPOSITIVOS. Productos con hardware específico, siendo cinco los tipos principales:

- Enrutadores. Estos dispositivos enrutan datos entre las redes de área local (LAN). Los enrutadores ponen el enter en interconexiones de redes; Sin ellos, Internet no seria posible. Los enrutadores usan direcciones de protocolos de Internet (IP) con el fin de calcular la mejor ruta para los paquetes a través de la red.

- Conmutadores. Estos dispositivos también envían datos entre distintas LAN's. Los conmutadores son más rápidos que los enrutadores, pero no usan direcciones IP y, por lo tanto, no tiene la capacidad de los enrutadores para encontrar trayectorias a través de las redes.

- Contrafuegos. Estos son básicamente enrutadores especialmente preparados para filtrar paquetes con el fin de asegurar el procesamiento de datos dentro de la red interna de una empresa.

- Servidores de acceso. Estos dispositivos dedicados contestan a las llamadas telefónicas de usuarios remotos y los conecta a la red. La mayoría de los servidores de acceso se usan como Proveedores de Servicio de Internet (ISP) para conectar a usuarios particulares y pequeñas empresas a Internet.

- Concentradores. El lento concentrador acepta cables de PC y servidores para crear LAN, y son los bloques básicos para construir una red.

2. - SOLUCIONES. Se refiere a la combinación de hardware, software y que deben ajustarse a las necesidades del cliente.

Las soluciones industriales son parte de su éxito, pero es un buen indicativo de dónde y como Cisco ve funcionando sus productos.
Como se mencionó anteriormente, las características sobresalientes de la línea de productos Cisco es que toda la gama de dispositivos ejecuta el Sistema operativo de redes por sus siglas en ingles (IOS), Cisco le dirá que esto permite a los clientes realizar un mejor trabajo en la configuración de las intranet.

A) Enrutadores.

La línea de productos Cisco se alinea de acuerdo a la escala de clientes. En otras palabras, agrupa y pone el precio a cada modelo del producto de acuerdo al tamaño y la sofisticación del mercado del cliente.

Enrutadores SOHO

SOHO es un término industrial para usuarios de redes muy pequeñas. Los clientes típicos de SOHO tiene uno o dos segmentos LAN en su servicio básico y una conexión PSI a Internet.

El eje de la estrategia SOHO de Cisco son los enrutadores de gama baja. Permitir a las pequeñas organizaciones conectarse a los PSI's enrutador a enrutador, en vez de cómo usuario de acceso telefónico ahorra dinero en conexión telefónica, el rendimiento es mayor y se mejora la fiabilidad. La tabla 1.1 muestra las series de productos SOHO de Cisco. El termino serie significa aquí un chasis que se configura de forma diferente en la planta de fabricación para diferentes modelos del producto, normalmente dependiendo del circuito impreso que se instale en ellos.

Los productos SOHO enfatizan las tecnologías de acceso telefónico SDL y RDSI ya que las pequeñas oficinas y las oficinas en el hogar no tienen enlace WAN dedicados que les conecten a su PSI o a su red empresarial.

Serie de productos	Descripción
Cisco 90	Enrutador de acceso DSL para conectar un usuario, no tiene un IOS que pueda configurar el usuario.
Cisco700	Enrutador de acceso RDSI para conectar hasta 30 usuarios, no tiene un IOS que se pueda configurar el usuario
Cisco 800	Enrutador de acceso RDSI para conectar hasta 20 usuarios, incluye el IOS y tiene capacidad de cifrado VPN.

Tabla 1.1 serie de enrutadores SOHO

Enrutadores Cisco de gama media

Las redes de tamaño pequeño o mediano requieren una amplia variedad de soluciones. Cisco tiene varios niveles de productos de enrutadores de acceso diseñados para que se ajusten a las necesidades de capacidad y equipo de enlace de telecomunicaciones del cliente.

Las series de la tabla 1.2 representan docenas de números de productos individuales. Dependiendo de la serie de productos, puede configurarse varias combinaciones de tecnología LAN y medios WAN. Modular significa que se puede actualizar el chasis insertado uno o más módulos. Los dispositivos no son modulares tienen una configuración fija.

Serie 4000 y 7000 de enrutadores de red troncal.

Cuando Cisco afirma que sobre el 70 por 100 de Internet funciona usando sus enrutadores, éstos son los modelos de los que esta hablando. La serie 4000 es quizás el chasis de enrutadores más distribuidos. La serie 7000 y 12000 son mayores, que se perecen a frigoríficos de habitación en forma y tamaño, y tienen buses de datos en los que se puede instalar tarjetas.

Como no son enrutadores de acceso, los enrutadores de red troncal de Cisco pueden aceptar tantos usuarios de la misma forma que manejan los paquetes. Las tres series de productos se describen en la tabla 1.3, son modulares, dejando a los clientes instalar módulos de acuerdo con la tecnología LAN que se use y de sus requisitos de capacidad. De hecho, estos enrutadores pueden operar con mas de un protocolo simultáneamente con Ethernet y Token Ring. Una ranura es una bahía electrónica en la que se inserta un modulo de placa de circuito impreso.

La interfaz serie de alta velocidad por sus siglas en ingles HSSI, es un estándar de entrada / salida especializado, que se utiliza principalmente con las supercomputadoras.
El enrutador Cisco 12000, es uno de los llamados dispositivos de clase portadora, y que los operadores de red de telecomunicaciones de equipos de portadora utilizan en sus operaciones de conmutación de datos para oficinas.

Todos los enrutadores de Cisco para red troncal tienen importantes capacidades para VPN, seguridad, calidad de servicio (QoS) y administración de red.

Serie de producto	**Descripción**
Serie Cisco 1000	Enrutador de acceso Ethernet para conectar a una RDSI o un vinculo serie WAN
Enrutador Cisco 1401	Enrutador de acceso Ethernet para conectar a una ATM o a una red troncal SDL
Serie Cisco 1600	Enrutador de acceso Ethernet para conectar a una RDSI o un enlace WAN, incluye la capacidad de cifrado VPN
Serie Cisco 2500	Enrutador / concentrador Ethernet o Token Ring o modelos deservicio de acceso telefónico para conectar uno o más segmentos LAN a una RDSI o a un enlace serie
Serie Cisco 2600	Solución modular y de bajo costo para que funcione como enrutador, es conductor de voz / datos o como servidor de acceso telefónico, conecta dos o más LAN Ethernet o Token Ring a vínculos RDSI, canalizado, Ethernet, módem analógico o ATM, también soporta voz / fax y Frame Relay
Serie Cisco 3600	Enrutador modular de alta densidad para acceso telefónico o para enrutador a enrutador, soporta vínculos RDSI, líneas serie TI canalizados, módem digitales y ATM, también soporta voz / fax y Frame Relay

Tabla 1.2 Enrutadores de gama media.

B) Conmutadores.

Conmutadores de acceso, al igual que los concentradores, tienen puertos en su frontal a los que se conectan los diferentes equipos, y un puerto vinculo ascendente en la parte posterior que conducen la jerarquía a un enrutador o un conmutador LAN. Los conmutadores de acceso Cisco se muestran en la tabla 1.4, se puede ampliar significa la capacidad para cablear cajas individuales de forma conjunta y hacerlos funcionar como un único conmutador lógico.

Los MicroSwitches son dispositivos de configuración fija sin acceso a la interfaz de línea de comandos IOS. A medida que crece la popularidad de los conmutadores de acceso, algunos esperan que se expanda la línea de bajo costo de MicroSwitches.

Serie de producto	Descripción
Serie Cisco 4000	Enrutador de tres ranuras que soporta Ethernet, Fast Ethernet, Token Ring, FDDI, HDDI, líneas series, RDSI, TI canalizada y ATM
Serie Cisco 7000	Enrutadores centrales de 4 a 13 ranuras que soporta Ethernet, Token Ring, FDDI, HSSI, líneas serie, RDSI, TI canalizada, paquetes sobre DS3 y ATM.
Serie Cisco 12000	Enrutador conmutador de 8 a 12 ranuras Gigabit Ethernet optimizado para IP, disponible de tarjetas especiales para vínculos WAN OC- 12 y OC-18

Tabla 1.3 Enrutadores de red troncal

Conmutadores de LAN Catalyst de Cisco

Un conmutador LAN es un dispositivo de alta velocidad de la capa 2 que dirige el trafico entre segmentos LAN. No deben confundirse con los conmutadores de accesos como los MicroSwitches o los conmutadores de bajas presentaciones Catalyst, que son dispositivos que conectan los equipos a Intranet de forma muy parecida a los concentradores. Dicho de otra forma, los conmutadores de acceso forman segmentos LAN; los conmutadores LAN conmutan entre ellos.

Como los concentradores forman segmentos LAN con múltiples equipos adjuntos a cada segmento, un conmutador suficientemente potente para conectar concentradores LAN pueden conectar, y lo hacen, equipos que requieren un gran ancho de banda, como servidores e impresoras de red de alta velocidad.

La familia de conmutadores LAN de la serie Catalyst de Cisco es la más amplia de la industria. Los modelos Catalyst van desde un modelo de cuatro puertos hasta el de clase portadora Catalyst 8500. Tabla 1.5

Serie de producto	Descripción
Serie MicroSwitch 1548	Conmutadores de acceso con 8 puertos Ethernet con conectividad autosensible para equipos Ethernet de 10 Mbps y Fast Ethernet de 100 Mbps, y uno preparado suficientemente para soportar la administración remota
Serie Catalyst 1900	Cuatro modelos con 12 o 24 puertos Ethernet y dos vínculos hacia arriba para enlaces Fast Ethernet
Serie Catalyst 2820	Cuatro modelos destinados para agregar concentradores o servidores, tiene 24 puertos Fast Ethernet, además dos ranuras para elegir módulos de alta velocidad, Fast Ethernet, FDDI o ATM

Tabla 1.4 Conmutadores de acceso

La conmutación multicapas aparece por primera vez en la gama media de la línea de conmutación Catalyst que se muestra en la tabla 1.6. Recuerde, los conmutadores multicapa son dispositivos con capacidad de enrutamiento IP incorporada en el hardware del conmutador, por lo tanto combinan algunas de las capacidades lógicas del enrutamiento IP con la tremenda velocidad de la conmutación.

Serie de productos	Descripción
Serie Catalyst 2900	Cuatro modelos con 12 o 48 puertos para Ethernet / Fast Ethernet 10 / 100 autosensible
Serie Catalyst 2900XL	Cinco modelos en dos paquetes básicos con 12 o 24 puertos y dos vínculos hacia arriba de fibra óptica

1.5 Conmutadores de LAN Catalyst de Cisco

Cisco ofrece dos conmutadores de red troncal de altas prestaciones, un para Gigabits Ethernet y otro para ATM. La tabla 1.7 los explica brevemente. Las series Catalyst 6000 y 8000 son dispositivos de conmutación de clase portadora. Tienen una densidad de puerto muy alta para interconectar cientos de segmentos LAN. El 6000 tiene una ranura especial que maneja la funcionalidad de conmutación multicapa. La línea 8500 esta preparada para el tipo de trafica multimedia, como VoIP etc.

Serie de productos	Descripción
Serie Catalyst 3000	Tres modelos de conmutación multicapa con 16 o 24 puertos 10BaseT en configuraciones fijas. Soporta diferentes especificaciones Ethernet y tipos de vínculos WAN, se puede apilar hasta ocho conmutadores en cualquier combinación de modelos
Serie Catalyst 3500XL	Tres modelos con 12 o 24 puertos 10/100 BaseT Ethernet y 2 puertos de vinculación hacia arriba de 2 Gigabit, los 3500XL puede apilar hasta nueve unidades mediante una estructura de conmutador de hasta 10 Gbps, es esta usando para la conectividad de bajas prestaciones de Ethernet Gigabit.
Serie Catalyst 3900	Dos modelos con 20 puertos fijos de Token Ring y dos ranuras para módulos de expansión cada uno con cuatro puertos para soportar más usuarios Token Ring una vinculación hacia arriba ATM o dos vinculaciones hacia arriba Fast Ethernet se pueden apilar hasta 8 conmutadores
Serie Catalyst 4000	Un modelo con un chasis modular de tres ranuras que soportan 10/100/1000 Ethernet, un modulo tiene 32 puertos 10/100 con distintas opciones de vinculaciones hacia arriba de Ethernet Gigabit
Familia Catalyst 5000	Familia de dos series con cinco modelos con chasis modular de 2 a 5 ranuras y entre 48 y 528 puertos soportando 100BaseX, 1000X, ATM, FDDI o Token Ring Backplane de 1.2 Gbps a 3.6 Gbps.

Tabla 1.6 Conmutadores LAN Catalyst de gama media.

C) Concentradores.

Cisco tiene dos lineas de productos de concentradores: las series Microhub y Fasthub. La serie Microhub 1538 es el producto hermano del microswitch1548 , una alternativa de bajo costo y sencillo de utilizar frente a los dispositivos de alta densidad y más configurables. Ambas línea pueden apilar hasta cuatro unidades por pila. Ver tabla 1.8 para mas ejemplos de concentradores.

Lo principal que debe recordar acerca de concentradores frente a los conmutadores de acceso es que los concentradores conectan equipos. Para conseguir una mayor conectividad, un concentrador debe conectarse a un conmutador LAN o directamente a un enrutador.

Serie de producto	**Descripción**
Familia Catalyst 6000	Familia de cuatro modelos de conmutadores de alto rendimiento multicapa con 6 o 9 ranuras que soporta 364 puertos 10/100 y vinculación hacia arriba Ethernet Gigabit esta es la solución de para redes troncales Gigabit
Serie Catalyst 8500	Dos modelos con 5 o 13 ranuras que soporta conmutación ATM multiservicio, optimizado para agregar tráfico multiprotocolo

Tabla 1.7 Conmutadores Catalyst de alta prestaciones de redes troncales

Serie de producto	**Descripción**
Cisco MicroHub 1538	Dispositivo autosensible de ocho puentes 10/100 que viene en variantes administradas y administrables, donde una unidad administrada se puede utilizar para administrar indirectamente otras tres unidades administrables en una pila de cuatro concentradores
Serie Cisco Fast Hub	Cuatro modelos que oscilan entre 12 y 24 puertos con 10/100 puertos autosensibles por chasis

Tabla 1.8 Micro Hub y Fast Hub

1.2 La certificación de Cisco System

Introducción a las certificaciones

El auge que han experimentado las redes ha creado la necesidad imperiosa de más talento técnico para instalar y administrar la infraestructura de las mismas. El factor principal ha sido el inmenso crecimiento de la industria. El número de enrutadores, conmutadores y otros dispositivos de redes han aumentado de forma vertiginosa en los últimos años y son necesarios mas técnicos mas calificados para ocuparse de todo ellos.

La escasez de talentos no es fenómeno nuevo en el mundo tecnológico y es una amenaza seria. Si hay una fuerte demanda de los productos, pero no hay nadie que los instale y mantenga, se recorta el crecimiento del fabricante. La respuesta ha sido la certificación de ingenieros.

Cisco tiene unos de los programas de certificación más amplios de toda la industria de telecomunicaciones. Esto puede resultar sorprendente, el programa de Cisco certifica en tres niveles de experiencia: Asociado, Profesional y Experto. Dentro de estos niveles, puede titularse en varias especialidades. El programa general se llama certificación de carrera de Cisco o vía CCIE.

Introducción a las formas de conseguir la certificación Cisco System.

Cisco ofrece y recomienda cursos de preparación para su programa de certificaciones de carrera. Los cursos recomendados se enseñan en Cisco Training Partner, que debe de utilizar como un curriculum de instrucción de nivel superior estandarizado. Las organizaciones que se encargan de la preparación no puede desviarse del curriculum aprobado y la certificación vienen exclusivamente de USA.

Tres niveles de certificación de Cisco

El programa de certificación esta diseñado para animar a los participantes ofreciendo un camino de aprendizaje progresivo:

- CNNA. Asociado de red certificado de Cisco, el certificado de nivel de ingreso requiere un dominio de los conceptos básicos de red, terminologías, tecnologías, productos y las habilidades de configuración básica.

- CCNP. Profesional de redes certificado de Cisco, el certificado intermedio requiere un dominio practico en la línea de productos Cisco, las tecnologías avanzadas, configuración de los dispositivos, solución de problemas y administración.

- CCIE. Ingeniero de redes certificado de Cisco, el certificado superior requiere un dominio absoluto que solo puede ser producto de años de experiencia y una preparación continua.

Cisco presume de que el CCIE es mejor que los demás programas de certificación de la industria de las telecomunicaciones. Cisco afirma que la experiencia es el factor más importante para obtener un titulo de CCIE. Y con razón, puesto que el examen CCIE es un examen practico de laboratorio que dura dos largos días y que es muy difícil.

1.3 Administración de la red

Introducción a la administración de la red

Ya hemos explicado las principales partes de la tecnología de las redes. Los enrutadores, conmutadores, contrafuegos y servidores de acceso están conectados entre sí para formar topologías de red. La mayoría de las configuraciones funcionan sobre cables de par trenzado que se conectan a redes troncales de fibra óptica que mueven datos a velocidades que oscilan entre los 100 Mbps, hasta 2.5 Gbps.

La infraestructura software de Cisco para que todo funcione es el IOS, que es un paquete de comandos, software de protocolos y archivo de configuración. Los protocolos de enrutamiento permiten a las redes un nivel de autoconciencia y autoadaptación sin que la que no sería práctica las configuraciones a gran escala. Esto se hace creando una jerarquía de LAN y sistemas autónomos para buscar una trayectoria óptima que crucen el recorrido necesario, o que vaya hasta el otro extremo del mundo.

Pero es necesario algo más que rutas óptimas para que las redes funcionen. La habilidad de funcionar de forma autónoma es sólo parte de la administración de redes. Los protocolos de enrutamiento pueden que sean capaces de manejar casi todos los asuntos concretos, pero las redes todavía requieren esfuerzos constantes de administración por parte de las personas. Sin la revisión e intervención constante de los administradores, la habilidad de las redes de funcionamiento autónomo se vería desbordada por deterioros progresivos de las condiciones de funcionamiento. Es necesario tener actualizadas constantemente las redes, e incluso actualizarlas para solucionar problemas, crecimientos y cambios. Los equipos de red necesitan herramientas para administrar y anticipar problemas. Los administradores de red deben monitorizar, volver a configurar y solucionar problemas constantemente. El reciente auge de los usuarios y el aumento de la cantidad de tráfico generado por el usuario ha exigido la mejora de los equipos de redes para mantenerse al nivel. Los posibles protocolos de enrutamiento y otras características automatizadas sólo hacen posible la administración eficaz de las redes. Pero no más fácil. También se necesitan las herramientas de administración de red.

La respuesta de la industria ha sido la creación constante de estándares, tecnología y productos centrados en la configuración y manejo de las redes.

Es necesario planificar las redes, modelarlas, presupuestarlas, diseñarlas, configurarlas, monitorizarlas, analizarlas, optimizarlas, actualizarlas y corregirlas. Esto es mucho, basta decir que los productos de administración de red y los servicios son una industria en sí mismos, compuesta de un complejo conjunto de tecnologías, productos y empresas que proporcionan todo, desde sencillos analizadores de protocolos, que miden un solo enlace, hasta centros de administración de red mundiales.

Las tareas de administración de red siguen un ciclo constante que a continuación se enlistan:

Mantener preciso el inventario de red

Trazar y documentar la topología de la red

Administrar y soportar usuarios

Monitorizar operaciones de red

Solucionar problemas

Revisar y mejorar los procesos de red

Analizar y modelar los requisitos de red

Investigar, presupuestar y planificar la estrategia de red

Comprar y organizar nuevos equipos

Instalar, integrar y probar nuevos equipos

Evolución de las herramientas de administración

Históricamente el problema con las herramientas de administración de equipos ha radicado en el poder ofrecer un soporte para varios fabricantes. En otras palabras, es difícil encontrar una sola herramienta que se pueda usar igual de bien en equipos de diferentes fabricantes. Disponer de equipos de varios fabricantes es la norma en prácticamente todas las infraestructuras por la tecnología de información o por sus siglas en ingles IT de las empresas, debido a las sutiles diferencias de los equipos de cada fabricante.

Las herramientas de administración de equipos han evolucionado tanto en todo lo que se refiere a computación, bajo el control administrativo de una sola herramienta y la prioridad de colocar equipos en las redes es lo que esta llevando en otras direcciones a las herramientas actuales de administración de equipos y sistemas.

Consolas tradicionales de administración de sistemas

Los sofisticados sistemas de administración llamados consolas de sistemas se buscan bajo algunas de las siguientes plataformas.

Plataforma UNIX

Plataforma Mainframe de IBM

Plataformas propietarias heredadas.

Sistemas de administración de red

En la última década, ha aparecido una segunda generación de herramientas en forma de sistemas de administración de red. Estas herramientas se centran en la infraestructura de red en lugar de centro de datos. Utilizan las redes que administran como plataforma para monitorizar eventos y se controlan desde una consola a la que se llama Estación de administración de red por sus siglas en ingles NMS.

La mejor NMS es de Hewlett-Packard (HP), alrededor de los 90´s , HP consideró que era oportuno y unirse a la tecnología UNIX para convertirse en la herramienta dominante de la administración de la red.

La clave del éxito consistió en la habilidad de trabajar con dispositivos de varios fabricantes, pero se tiene una ventaja de diseño incorporada en forma novedosa conocido como protocolo de administración de red simple o por sus siglas en ingles SNMP. En lugar de tener que diseñar docenas de interfaces propietarias se permitió que los fabricantes hicieran equipos conforme al protocolo SNMP.

La diferencia clave entre las consolas de red y de sistemas es el nivel en el que operan. Las herramientas de administración de sistemas se centran en los sistemas operativos, transacciones, archivos de datos y base de datos, tal y como existe en los servidores, controladores de almacenamiento y discos. Las herramientas de administración de red se centran en paquetes y conexiones según existen en los dispositivos de red, interfaces de red y enlaces de transmisión.

Las consolas de sistemas de red y enlace están ahora convergiendo en una única clase de tecnología que algunos llaman herramienta Administración de sistemas de empresa o por sus siglas en ingles ESM, la convergencia en ESM son inevitables, ya que la línea entre la red y las computadoras se difumina y la empresa completa el cambio de arquitectura cliente / servidor que mueve recursos desde el centro a las topologías de redes.

Herramientas actuales de administración

Se ha comprobado que es muy difícil administrar una red usando una única herramienta. El problema ha sido la incapacidad de recopilar datos consistentes desde los distintos que existen en la mayoría de la infraestructura IT de la empresa. El problema no es la confrontación entre los nuevos y antiguos equipos, aunque constituya una parte. El mayor problema es que la mayor parte de los sistemas de administración de red son superficiales en sus implementaciones; en otras palabras, pueden administrar solo unos aspectos del funcionamiento de los dispositivos y no son capaces de administrar en absoluto otro.

La infraestructura base de SNMP está ahí, pero los fabricantes pocas veces la implementan completamente en sus productos, esto se debe a cuatro razones:

- Consumo de Recursos de La Administración de Red. Cada ciclo CPU que se emplea en recoger una medida o enviar un mensaje SNMP es un ciclo que no se utiliza para el tráfico de carga. La administración de red implica un costo, ya que sea en una disminución del rendimiento o en la necesidad de hardware extra.

- Débil Soporte de Estándares Por Parte de Los Fabricantes. Sería muy caro para los fabricantes de dispositivos incorporar una compatibilidad completa en sus productos. Sería necesario mejorar el hardware de dispositivos para mantener el trabajo de SNMP adicional, lo que implicaría una subida de los precios. Además, algunos fabricantes prefieren un poco de incompatibilidad SNMP para obligar a sus clientes a estandarizar su línea de productos para la implementación de SNMP, a partir de un fabricante, es más fácil que tener dispositivos de diferentes fabricantes bajo el mismo régimen de administración.

- Trabajo. Se necesita mucho tiempo y atención para que las empresas implementen y hagan funcionar un sistema de administración de red. Los equipos de administración se ven en apuros para mantener el nivel del crecimiento de la red. Son pocos los que tienen los recursos humanos necesarios para hacer un mejor uso de los sistemas basados en SNMP.

- Clientes Concientes de Los Precios. Los clientes prefieren productos baratos. La mitad de la red de tiendas IT se considera como infraestructura y los administradores exigen una adecuación de los precios. La implacable obsesión de reducir los costos por puerto tiene buen aspecto sobre el papel, pero implica costos ocultos bajo la forma de ventas que prácticamente no se usan.

Por estas razones, la mayor parte de las implementaciones SNMP sólo recopilan información de alto nivel. Muy pocos procesos, llamados Objetos se monitorizan, las muestras son más pequeñas, los ciclos de sondeo son menos frecuentes, etc.

A menudo, incluso cuando una empresa desea realizar más controles de administración de red, todavía aparecen puntos ciegos provocados por dispositivos no compatibles. Los puntos ciegos aparecen cuando no es posible cumplir con una política en una parte de la red porque un dispositivo no la soporta. Los puntos ciegos suelen aparecer en las entradas de las redes troncales, especialmente en las redes troncales conmutadas. Como se muestra en la Fig. 1.1 se ven ejemplos de puntos ciegos.

Dependencia de Hardware. Cualquier computadora estándar debe competir con las distintas arquitecturas que se usan para CPU, buses, interfaces de dispositivos, controladores, etc. Esto implica el proceso de establecer estándares y encarece que los fabricantes lo puedan cumplir. El problema se ha exagerado a causa de la práctica habitual de la interconexión de redes de la industria de utilizar tantas partes en su línea de productos.

Tecnologías de Convergencia. Hasta hace poco tiempo, las telecomunicaciones, redes de datos y computación se consideraban industrias independientes y distintas, con sus propios cuerpos de industria, estándares, etc. Pero actualmente, todos los equipos que fabrican deben ser supervisados por los administradores de red, aumentando el ámbito de los estándares y unir los diferentes campos de ingeniería ha supuesto una gran presión.

Preparación de la Tecnología. El imparable avance de la tecnología en todos los niveles de la computación ha supuesto para el IEFT que es la parte de desarrollo de software un objetivo en constante movimiento. Y un fabricante que haya conseguido una ventaja con gran esfuerzo se niega entonces a caer en la línea de los estándares y facilitarle la vida a los competidores.

Las herramientas específicas más importantes de un fabricante es CiscoWorks, con suficiente funcionalidad como para considerarla un ESM en sí misma, pero sólo siempre que se ejecute con equipos de Cisco. Por esa razón, CiscoWorks siempre se suele incluir en una familia ESM como OpenView o NetView.

Tendencias en la administración de sistemas empresariales

Microsoft ha entrado provisionalmente en la lucha con la introducción de la administración de consolas de Microsoft, en su lanzamiento de Windows 2000, donde MMC es una pieza importante para la estrategia de servidores NT de la compañía y que la informática empresarial debe disponer de capacidades de administración. Es simplemente un marco de trabajo para algunas aplicaciones de Microsoft por ahora, pero todas las empresas siguen las siguientes metas:

- Más Cobertura. Donde se coloque más control de administración en dispositivos y procesos de red, esto exigirá hardware de dispositivos más rápidos.

- Simpleza. Debido al auge de popularidad de las redes en las pequeñas y medianas empresas, los expertos cada vez manejan más redes.

- Automatismo. A medida que avanza la tecnología de administración de red, se automatizan más redes para mejorar la calidad de servicio o QoS.

- Administración Activa. Un tipo de herramienta ayuda a aislar y apartar los problemas incipientes más importantes de red aplicando acciones correctivas en el primer momento.

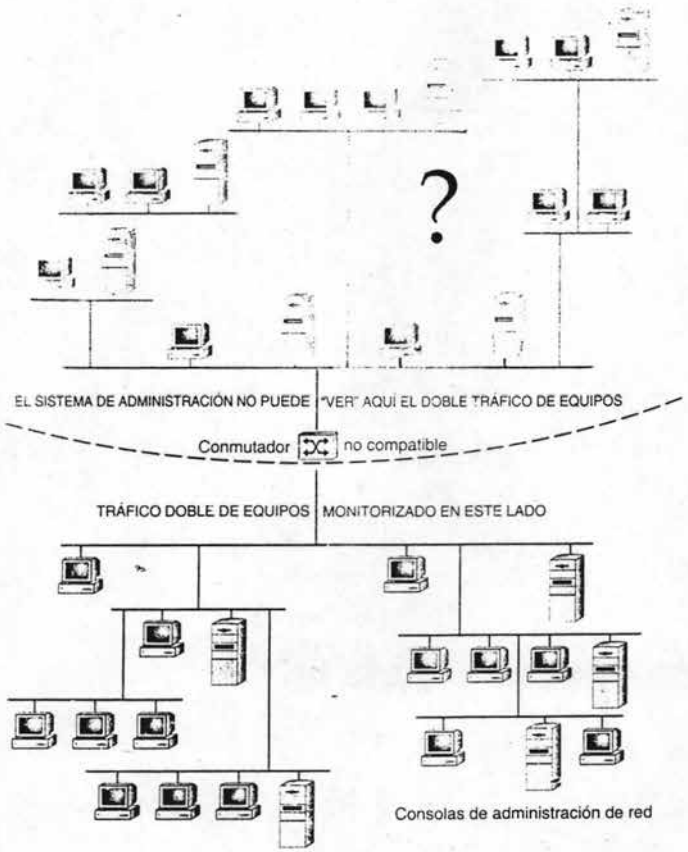


Fig. 1.1 Compatibilidad con SNMP con puntos ciegos de una red

1.4 Seguridad de tráfico y de usuario

Introducción a la seguridad de red

La seguridad de redes es tan importante que todavía se trata por separado. La industria nunca tienen la oportunidad de integrar realmente las aplicaciones de seguridad en familias de NMS como por ejemplo, HP OpenView o Tivoli de IBM.

Pero la seguridad de redes tiene un conflicto natural con la conectividad de redes. Cuanto más se abre al mundo exterior un sistema autónomo, más riesgos tiene. Esto a su vez, requiere que se aplique más esfuerzos a las tareas de refuerzo de seguridad. Tres tendencias han aumentado las pruebas de que seguridad desborda el presupuesto de todo el departamento de IT.

- Las redes crecen y se complican cada vez más
- Siempre hay nuevas amenazas al acecho
- El sistema de seguridad de red típica no es en absoluto un sistema, sino una labor de parches y herramientas específicas del fabricante.

La seguridad de redes es una consideración tan importante que incluso las consolas de administración de red plantean problemas. Como se ha mencionado algunos se preocupan sobre si la propia infraestructura SNMP es lo suficiente segura. Después de todo, robar la cadena de comunidad SNMP adecuada daría a un pirata cibernético un mapa de toda la configuración de una red. Y, a no ser que haya estado viviendo en una cueva, conoce los virus de una computadora que se extienden de distintas formas: bombas de correo electrónico, programas de Java de caballo de Troya, ataques de denegación de servicio y otras nuevas amenazas preocupantes para la seguridad de las computadoras. Basta decir que gran cantidad de tiempo, dinero y esfuerzo se destinan en la seguridad de redes.

La seguridad basada en el tráfico se realiza en contrafuegos y enrutadores, y está relacionada principalmente con las direcciones IP.

Pero un segundo tipo de seguridad opera a nivel de personas. Este tipo de seguridad, llamado seguridad basada en el usuario, usa contraseña y otros controles de acceso para autenticar las identidades de los usuarios antes de que se permita el acceso. Hay dos tipos básicos de seguridad basada en usuarios:

- El acceso remoto de usuario final a los servidores, en el que los empleados accesan telefónicamente a la red de su empresa y los abonados accesan telefónicamente a sus proveedores de servicio de Internet.

- El acceso del administrador de red a los dispositivos de red, en el que los técnicos inician una sesión en el IOS en distintos tipos de dispositivos de red para trabajar en ellos.

La seguridad es el tercer sistema de control importante de las redes, junto con los sistemas de administración de red y los protocolos de enrutamiento. Aunque los sistemas de control tienen distintas misiones, como explica CiscoSecure verá un modelo familiar:

- Comandos Incrustados. Comandos de aplicación creados directamente en IOS que se usa para configurar dispositivos individuales y participar en un sistema de control más grande.

- Protocolo de Control Dedicado. Un protocolo de comunicación que coordina el intercambio de mensajes necesarios para llevar a cabo las tareas de sistema de control de red.

- Servidor y Consola. Un servidor para almacenar los mensajes y una estación de trabajo para proporcionar la interfaz humana a través de la que se maneja en el sistema de control de red.

El tercer sistema de control de redes, los protocolos de enrutamiento, es claramente distinto. Los protocolos de enrutamiento no utilizan servidores porque la información, tablas de enrutamiento es temporal y no es necesario almacenarla en disco. Y no utilizan consolas porque son ampliamente auto-operadas.

Las similitudes estructurales entre la administración de red y la seguridad facilitarán la comprensión de la tecnología de seguridad de red. Simplemente intercambie nombres nuevos protocolos y consolas entenderá la configuración.

Hay dos tipos de seguridad de red. Un tipo se refuerza como proceso de fondo no viable a los usuarios: el otro lo tiene adelante.

- Seguridad Basada en el Tráfico. Las Conexiones de control solicitadas por una aplicación de red, como un explorador Web o una carga de FTP.

- Seguridad Basada en el Usuario. Admisión de controles de individuos a los sistemas para iniciar aplicaciones una vez dentro, normalmente, por el usuario y la contraseña.

Un tipo de seguridad basada en el tráfico es el uso de los contrafuegos para proteger sistemas autónomos comprobando el tráfico de que los equipos en que no se confía. El otro tipo de seguridad basada en el tráfico son las listas de acceso de un enrutador, seguridad basada en el usuario está relacionada, evidentemente, con las personas, no con los equipos. Este tipo de seguridad con el que todos estamos familiarizados, la seguridad basada en el acceso que solicita el usuario el nombre del usuario y la contraseña.

Los dos tipos se completan y aun así funcionan a niveles diferentes. La segunda se basa en el tráfico entra en acción cuando se hace clic en un botón de un explorador Web, se introduce un comando en una pantalla FTP o se utiliza algún otro comando de aplicación. La seguridad basada en el usuario se reafirma cuando un individuo intenta accesar a una red, dispositivo o servicio que ofrece un dispositivo.

Seguridad en el tráfico

La seguridad basada en el tráfico se implementa en una red de Cisco utilizando contrafuegos o lista de acceso de enrutador. Se centra principalmente en el origen y destino de las direcciones IP, números de puerto de aplicación y otra información a nivel de paquetes que se puede utilizar para registrar y controlar las conexiones de red.

Hasta hace poco, los contrafuegos se habían concentrado estrictamente en proteger el sistema autónomo contra intrusos externos. Sin embargo, ahora se están utilizando en tiendas de acceso más sofisticadas para restringir el acceso a los caudales internos sensibles. Las listas de acceso han sido la herramienta tradicional que se ha usado para reforzar la seguridad interna.

Seguridad de tráfico basada en las listas de acceso

Los enrutadores se pueden configurar para reforzar la seguridad de modo muy parecido a los contrafuegos. Todos los enrutadores tienen listas de acceso y se pueden utilizar para controlar los Ids y venidas de tráfico en las interfaces de red del enrutador, y que aplicaciones se pueden utilizar si se aceptan. En realidad, lo que hace una lista de acceso depende, en gran medida, de cómo la configure el administrador de red.

Principalmente, las listas de acceso se utilizan para mejorar el rendimiento de la red aislando el tráfico en su área de inicio. Pero una lista de acceso excesivamente grande puede comportarse como un contrafuego interno, restringiendo el tráfico entre los departamentos.

Seguridad del tráfico basada en contrafuegos

Los contrafuegos son básicamente enrutadores reforzados que comprueba procesos para exigir que se cumpla ciertas reglas de administración de tráfico. Utilizando todo tipo de tácticas para mejorar la seguridad: la traducción de direcciones para ocultar la topología de red de los intrusos; la inspección de la capa de aplicación para asegurar sé que sólo se ejecutan los servicios permitidos; incluso los contadores de elevado / bajo que vigilan cualquier tipo difícil de predecir en ciertos tipos de paquetes para evitar que aparezcan ataques por denegación de servicio.

Los contrafuegos crean un cuello de botella de forma intencionada en el perímetro del sistema autónomo. Mientras pasa el tráfico, el contrafuego inspecciona paquetes conforme llegan y se van a través de las redes conectadas a sus interfaces.

Los contrafuegos leen la dirección origen y destino de los equipos, número de puerto y establecen un contexto para cada conexión par de dirección y número de puerto; deben pertenecer a una sesión válida. Por ejemplo, si un usuario intenta conectarse a un sitio Web para cargar un archivo, el contrafuego comprobará la dirección IP origen del usuario, antes de permitir que pasen los paquetes.

Seguridad basada en el usuario

La seguridad basada en el usuario evoca una imagen diferente: la de una puerta con un guardia de seguridad. Los sistemas más sofisticados de seguridad basada en el usuario, también tiene otro guardia que pregunta lo que intenta hacer y le asigna un distintivo codificado que le da acceso a algunas áreas, pero no a todas.

De este modo, la seguridad en el usuario se emplea donde una persona debe de accesar a un equipo, y la seguridad se presenta en su nombre de usuario y contraseña. En las redes, este tipo de seguridad se utiliza, tanto para impedir se entre en los dispositivos de red, como enrutadores o conmutadores, así para restringir el acceso a los dispositivos de carga como los servidores.

Sin embargo, al contrario que los contrafuegos, la seguridad basada en el usuario atañe tanto a los de dentro como a los de fuera. Los puntos de contraseña inicio de sesión se colocan, generalmente, en cada dispositivo de red y todos los servidores. Como los mecanismos de seguridad basados en el usuario es software, no hardware, se puede distribuir como se quiera dentro de la red, sin que esto afecte demasiado al rendimiento o presupuesto. El equilibrio es cuántas complicaciones desea ocasionar a los usuarios de red, teniendo que iniciar una sesión para poder accesar a distintos servicios. La seguridad en el usuario se aplica en cuatro situaciones principalmente:

- Permitir que empleados remotos usen a la red de la empresa.
- Permitir que empleados locales usen los equipos protegidos y los servicios dentro de la red.
- Permitir que los administradores de red usen a los dispositivos de red.
- Permitir que los PSI concedan el acceso a sus abonados a un portal.

1.5 Tecnologías de redes

Las tecnologías de redes se usan para ejecutar la unidad básica de todas las redes: el segmento LAN. Las tecnologías mas conocidas es Ethernet, pero hay otras muchas, incluyendo el Token Ring, modo de transferencia asíncrona y interfaz de datos distribuidos por fibra.

Las tecnologías de red se implementan en la capa de enlace de datos del modelo de referencia OSI de siete capas. Dicho de otra forma, las tecnologías de red se caracterizan ampliamente por el medio físico que comparten y por cómo controlan el acceso al medio que comparten. La interconexión es conectividad; pero para estar conectado debe aplicarse una orden entre los usuarios que comparten información. Por ello, la capa 2 también recibe el nombre de capa de control de acceso al medio. El formato de unidad de mensaje es este nivel es la trama de datos o trama.

De hecho, las propias tecnologías de red solo pueden manejar direcciones MAC, esos números de serie, que son identificadores de dispositivos. Es necesario un protocolo de la capa de red como IP para enrutar los mensajes a través de la red. Las tecnologías de red independientes solo pueden soportar operaciones de redes conmutadas, que solo son buenas para áreas locales o trayectorias simples sobre largas distancias:

- LAN de acceso. Acepta el cableado de los dispositivos, une grupos de trabajo, comparte recursos como impresoras y servidores departamentales.

- LAN de red troncal. Enlaza las LAN's de acceso y comparte recursos como servidores de base de datos, servidores de correo, etc.

Las LAN's de acceso formadas por concentradores o conmutadores de acceso, permiten a los usuarios y a los dispositivos conectarse a la red a nivel local normalmente dentro de una planta de un edificio de oficina. Las LAN's de red troncal, formada por enrutadores o conmutadores LAN, unen LAN de acceso, normalmente dentro de un edificio o de un campus de oficinas. Las redes enrutadas se suelen usar para distribuir tráfico entre las dos.

Ethernet

Ethernet se ha convertido en el estándar de tecnología de red dominante. Gracias sobre todo a las economías escalables, el costo medio de un puerto Token Ring. Sin embargo se ha convertido más en un estándar ya que muchos fabricantes están integrando NIC Ethernet en las placas madres de las computadoras en un intento de eliminar la necesidad de módulos NIC, independientes.

Arquitectura de Ethernet

Ethernet funciona mediante contención. Los dispositivos que comparten un segmento LAN Ethernet escucha el tráfico que se está transportando sobre el cableado y no transmite un mensaje hasta que el medio este limpio. Si dos estaciones envían a la vez y sus paquetes chocan, ambas transmisiones son abortadas y las estaciones se detienen y esperan un intervalo de tiempo aleatorio antes de volver a transmitir. Ethernet usa el algoritmo múltiple de acceso sin portadora de con detección de colisión para escuchar el tráfico, detectar las colisiones y abortar las transmisiones. El CSMA/CD es el guardia de tráfico que controla lo que de otra forma sería un tráfico aleatorio. Restringe el acceso al cable para asegurar la integridad de las transmisiones.

Como el medio se comparte, cada dispositivo del segmento Lan Ethernet recibe el mensaje y lo comprueba para ver si la dirección destino coincide con su propia dirección. Si es así, el mensaje se acepta y se procesa a través de la pila de siete capas y se realiza una conexión de red. Si la dirección no coincide, los paquetes se desechan.

Ethernet se implementa como la especificación IEEE 802.3.

Implementaciones Ethernet

Incluso fuera de las economías escalables, Ethernet es inherente menos caro gracias a la naturaleza aleatoria de su arquitectura. En otras palabras, la electrónica necesaria para ejecutar Ethernet es más fácil de fabricar, no intenta controlar todo. En términos, sólo se preocupa de las colisiones.

La desventaja obviamente de Ethernet es que se sacrifica mucho ancho de banda para abortar transmisiones. El máximo ancho de banda efectivo de Ethernet se estima en sólo 37 por ciento de la velocidad real del cableado. Sin embargo, el equipamiento es tan barato que Ethernet siempre ha estado en equilibrio con la forma más barata de ancho de banda efectiva. En otras palabras, su simplicidad compensa con creces su inherente ineficacia de ancho de banda.

Ethernet tiene varias opciones de implementación. La especificación original Ethernet funcionaba a 10 Mbps sobre cable coaxial o cable de par trenzado 10 BaseT. La Fast Ethernet funciona a 100 Mbps y opera a 100 BaseTX o cable de fibra óptica. La Gigabit Ethernet funciona a 1000 Mbps sobre cable 1000 BaseTX o 1000 BaseFX. Una elección de configuración muy común es la Lan Fast Ethernet interconectada a través de una red troncal Lan Gigabit Ethernet.

Token Ring

Token Ring es el principal competidor de Ethernet como estándar LAN, difiere superficialmente de Ethernet en su acercamiento a la arquitectura. Es incompatible con Ethernet en términos del tipo de NIC, conectores de cable y software que debe utilizarse. Y no es un estándar abierto.

Token Ring toma su nombre del hecho de que define los equipos conectados en un anillo lógico. Se utiliza lógico para describir Token Ring, ya que un segmento LAN se comporta como un anillo pasando señales de forma circular como si los dispositivos estuviesen realmente conectados a un cable que forma un bucle. Físicamente, sin embargo, las LAN Token Ring pueden configurarse en una topología de concentrar y hablar, llamada topología en estrella. Tenga en cuenta que en Token Ring, el concentrador de acceso se llama unidad de acceso al medio, en vez de concentrador.

Token Ring evita la competición sobre un segmento LAN mediante un protocolo de paso de testigo, que regula el flujo de tráfico mediante el paso de una trama, llamada testigo alrededor del anillo. Sólo al equipo que posee el testigo se le permite transmitir, por tanto, elimina colisiones de paquetes. La arquitectura Token Ring en los negocios reales espera un tiempo para las colisiones, ya que cada estación debe esperar su turno antes de capturar el testigo para transmitir. Sin embargo, la eliminación de la colisión de paquetes incrementa enormemente el uso eficaz del ancho de banda real del Token Ring. Las pruebas muestran que el Token Ring puede usar el 75 % del ancho de banda real, comparando con el máximo teórico de Ethernet, que esta alrededor del 37 %. El problema es que Token Ring sólo sale rentable a partir de ciertos volúmenes de tráfico.

ATM

Modo de transferencia asíncrona o ATM, es una tecnología de red de enlace a datos que, al igual que Ethernet, Token Ring, se especifica en la capa 2 del modelo OSI. Pero aquí es donde termina las similitudes. Las transmisiones ATM envían celdas de 53 bytes en vez de paquetes. Una celda es una unidad de mensaje de longitud fija. Al igual que los paquetes, las celdas son piezas de mensaje, pero el formato de longitud produce ciertas características:

Orientación de Circuitos Virtuales. Las redes basadas en celdas funcionan mejor en modo punto a punto, en el que la estación reporta está preparada para recibir y procesar la celda de forma activa.

Velocidad. El hardware sabe exactamente dónde termina la cabecera y empieza los datos de cada celda, por lo tanto, acelera las operaciones de procesamiento. Las redes ATM funcionan a velocidades de 622 Mbps.

Calidad de Servicio (QoS). La velocidad de salida predecible y los circuitos virtuales permiten a las redes basadas en celdas garantizar mejor los niveles de servicio a tipo de tráfico que son prioritarios.

ATM no tiene una tecnología de control de acceso por sí misma. ATM es una tecnología de conmutación, en la que se establece un llamado circuito virtual antes de que se inicie una transmisión. Esto difiere superficialmente de las tecnologías LAN Ethernet y Token Ring que solo transmiten un mensaje sin una notificación anterior del equipo receptor, dejando a los enrutadores averiguar la mejor trayectoria al receptor.

Comparando al diminuto tamaño de las celdas ATM, el tamaño del paquete Ethernet puede variar desde 64 Bytes hasta alrededor de los 1500 Bytes, hasta 25 veces más grande por unidad de mensaje.

ATM está diseñado para funcionar sobre cables de fibra óptica que funcionen con las especificaciones SONET, el cual es un estándar ANSI que especifica la interfaz física que conecta el cable de fibra óptica a varias velocidades. Trabajan con niveles de transportador óptico diferentes:

OC-1 Cable de fibra óptica a 52 Mbps

OC-3 Cable de fibra óptica a 155 Mbps

OC-12 Cable de fibra óptica a 622 Mbps

OC-24 Cable de fibra óptica a 1.2 Gbps

OC-48 Cable de fibra óptica a 2.5 Gbps

El diseño determinista de ATM cede un ancho de banda efectivo a cambio de su velocidad de cableado real. La sesión efectiva de ATM se dice que es correcta ya que está por encima incluso del 75 por ciento de la Token Ring. La mayoría de las LAN's de red troncal ATM funcionan sobre OC-3 o OC-12. La mayoría de los enlaces entre ciudades funcionan sobre OC-12, aunque los principales proveedores de red troncal de Internet están ahora cableando con OC-48 para cubrir la creciente demanda de ancho de banda.

La mayoría de los troncos de Internet entre ciudades son OC-12 funcionando con ATM, OC-48 en los troncos más cargados. Por ejemplo, UUNET, uno de los proveedores de red troncal de Internet más grandes, usa cableado de fibra óptica a 622 Mbps.

Latencia y sensibilidad de secuencia

Ciertos tipos de tráfico necesitan predectibilidad más que otros. Por ejemplo, una conversación telefónica no puede tolerar retrasos, pues cada participante podría empezar a hablar antes de que haya terminado. Esto se llaman sensibilidad de latencia, otro tipo de sensibilidad de tráfico es la sensibilidad prioritaria, donde el orden en el que se reciben los datos es crítico, por ejemplo, las unidades de una de transmisión de vídeo debe recibirse en el orden correcto para que todas las tramas del vídeo puedan mostrarse en su secuencia correcta.

La figura1.2 representa cómo los problemas de latencia y secuencia dañan la calidad del servicio en aplicaciones de sensibilidad prioritaria, como la videoconferencia.

La videoconferencia se está convirtiendo en una solución popular para aplicaciones como la educación a distancia y las comunicaciones corporativas internas. Muchos sueñan con el día en que la Web desplace a la difusión por televisión

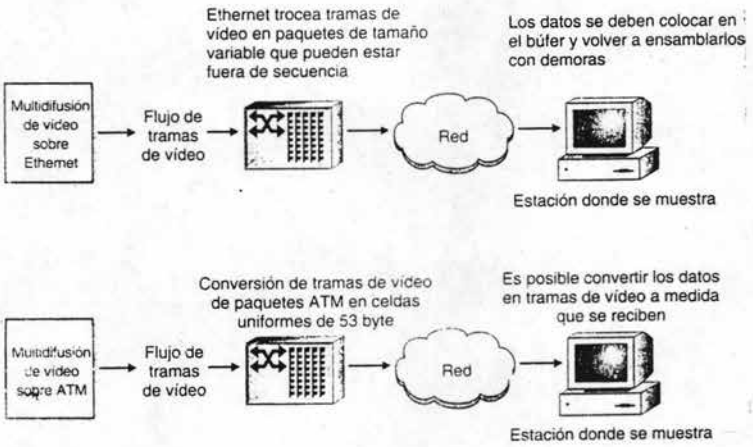


Fig. 1.2 Las aplicaciones de latencia y secuencia.

Multidifusión frente a difusión

Un mensaje difundido va a cada estación que pertenece al dominio de difusión. Por defecto, un dominio de difusión incluye todas las estaciones conectadas al medio compartido de un segmento LAN, aunque se puede extender de forma intencionada usan enrutadores.

Cada estación debe recibir y examinar el mensaje difundido, pero puede llevarlo a la interfaz si está programado para ello, por ejemplo las difusiones pueden ser ventajosas para una red que mantiene las estaciones actualizadas, tanto en cambio como en nuevas direcciones o enlaces caídos. Demasiadas difusiones, sin embargo, pueden minar el ancho de banda con tráfico inútil.

Un mensaje multidifundido va a un subconjunto de estaciones dentro de un dominio de difusión. En términos básicos, cada estación confirma la entrega de mensaje, del tipo de multidifusión que desea compartir.

Un ejemplo clásico de multidifusión es la videoconferencia, en la que se usa un ancho de banda para mover imágenes de vídeo, por lo que sólo las estaciones que quieren participar lo reciben. Tiene sentido usar multidifusión debido a que su formato de celda fija es ideal para aplicaciones multimedia.

Si ATM es mucho mejor que otros protocolos de red, es por que esta basada en el hecho de que la mayoría del tráfico no es sensible a la latencia de transmisión. El gasto añadido y la complejidad de ATM pueden ser suficiente para justificar esto en ausencia de un gran tráfico multimedia, ya que hay suficiente tiempo para volver a empaquetar los mensajes en el extremo receptor.

Los mensajes normales no son particularmente sensibles a retrasos intermitentes o a la secuencia de entrega. Por ejemplo, un correo electrónico con un documento adjunto puede tener un tamaño de 20k. Al usuario no le importa el orden en que se reciben las distintas partes del mensaje, e incluso no se dará cuenta de ningún retraso, por ello, la red puede recibir el correo electrónico como crea más conveniente.

Circuitos virtuales

Como son tan pequeñas, las celdas ATM no contienen la cantidad de información de direccionamiento que se encuentra en la cabecera de un paquete Ethernet. De hecho, ATM usa un esquema de direccionamiento totalmente diferente de las otras tecnologías de red. Esto se debe a que ATM necesita establecer un circuito virtual en el extremo remoto antes de comunicarse. Un circuito virtual es una conexión entre dos puntos, por ejemplo, el circuito telefónico de una casa está cableando directamente a la oficina de conmutación central de una colonia, pasando, sin embargo, a través de diferentes dispositivos de red, como concentradores, conmutadores y enrutadores.

Antes de que la transmisión pueda iniciarse sobre un circuito virtual, cada extremo confirma para qué se realiza la transmisión y también confirmar la trayectoria sobre la que viajará. Esto es completamente diferente de los mensajes de redes, que simplemente se envían al exterior hacia su dirección destino, dejando los detalles sobre cómo llegar allí a uno más enrutadores situados entre el emisor y el receptor.

Simulación de una LAN

Aunque se puede configurar por completo hasta el más pequeño detalle, ATM se usa principalmente para redes troncales, ya sean LAN o de red troncal de un campo de oficina, hasta los enlaces de Internet de todo tipo entre ciudades. ATM es la tecnología más común para redes troncales, debido a que la tecnología subyacente de conmutación de celdas es ideal para enlaces punto a punto de alta velocidad.

Pero algún punto, una red troncal debe hablar el mismo lenguaje que las LAN's de acceso a las que sirve, normalmente, Ethernet o Token Ring. Como ATM se basa en celdas en vez de en paquetes, usa técnicas de encapsulación llamadas LANE o Simulación de LAN. En redes, encapsulación es la técnica de colocar una unidad de mensaje de un formato dentro de otra con formato distinto para que permita atravesar una red que, de otro modo, sería incompatible. LANE encapsula cuadro en el nivel de enlace de datos para establecerlos así llamados circuitos LAN emulados o LANE, en otras palabras LANE juega con los paquetes Ethernet o Token Ring en celda ATM en un extremo y los vuelve a unir en el otro.

Muchos consideran ATM como la respuesta a la escasez de ancho de banda de Internet. Lo están instalando muchas empresas para reemplazar las extremadamente caras redes troncales FDDI. No sólo es la velocidad de ATM a 622 Mbps, sino también su inherente predictibilidad que le asegura al usuario la garantía de la calidad del servicio QoS, es especialmente para aplicaciones multimedia que, por naturaleza, no son lentos. Sin embargo, debido a la necesidad de adaptación LANE, ATM tiene un costo por puerto relativamente alto, también introduce un nuevo protocolo al difícil mundo de las redes, incrementando así la complejidad.

El estándar ATM es coordinado por un grupo industrial internacional sin ánimo de lucro llamado el Forum ATM.

Gigabit Ethernet

El Gigabit Ethernet es una extensión a 1000 Mbps del estándar Ethernet relativamente nuevo como estándar, este termino se conoce a veces con el nombre de 1000BaseX, en referencia a la especificación para el cobre necesario para el cableado de fibra óptica.

El Gigabit Ethernet es el principal competidor de ATM para reemplazar a FDDI como elección de red troncal, su gran ventaja es la gran familiaridad, dado que Ethernet es 1000 Mbps, la Gigabit Ethernet puede escalarse a configuraciones WAN, como Ethernet usa tramas de tamaño variable, que oscila entre los 64 bytes y los 1400 bytes por tramas, no disfruta de las inherentes características de QoS de ATM, sin embargo muchos administradores de red están parcialmente a favor de la Gigabit Ethernet debido a que sus plantillas están familiarizadas con la tecnología presumiblemente no introduce la dificultad añadida de complejidad que requiere la adaptación LANE, al igual que ATM, las redes troncales de Gigabit Ethernet operan sobre distintos tipos de fibra óptica.

Tema 2 Redes de Cisco

2.1 Fundamentos

Hasta ahora hemos visto los componentes que forman parte de una red. El trabajo en redes es geográfico por naturaleza y, por ello, muchas de las tareas del diseño están relacionadas con ajustar la topología a nuestras necesidades. El diseño de una red indica de forma implícita su rendimiento y su escalabilidad. En redes, escalares indica cuánto puede crecer una red sin tener que cambiar la forma básica de su topología, es decir, sin tener que sustituir o volver a configurar excesivamente la infraestructura ya existente.

Es necesario hacer una última revisión de lo que sea mencionado hasta ahora y por lo tanto se inicia con el Segmento LAN; Concentradores y Conmutadores del segmento LAN son los componentes básicos de cualquier red. Un segmento LAN puede ser una LAN de departamento o una red troncal LAN de alta velocidad que da servicio a otros segmentos LAN dentro de una empresa.

Dominios de colisión y difusión, es un medio de red compartido en el que se permite colisionar a los paquetes Ethernet; un dominio de difusión es el área donde se puede enviar mensajes a todas las estaciones usando la llamada dirección de difusión. Es necesario hacer que los dominios de colisión sean pequeños, ya que las colisiones limitan el uso de ancho de banda, cuantos más equipos se conectan al segmento LAN, más lento es el tráfico.

La mayoría de los dominios de colisión están formados por concentradores que conectan dispositivos de equipos a la red. Un dominio de difusión es el área de red en la que se transmiten los mensajes difundidos. Las difusiones usan el número IP decimal reservado 255; algunas difusiones son útiles, pero otras sólo disminuyen la velocidad de la red, saturándola con tráfico inútil, un fenómeno poco deseado que se conoce con el nombre de tormenta de difusión. Los dominios de difusión son, por defecto, lo mismo que los dominios de colisión de una red de medios compartidos, es decir, un concentrador, pero el alcance de las direcciones de difusión puede hacerse menor que un dominio de colisión usando conmutadores. Los enrutadores suelen limitar las difusiones, pero es posible extender un dominio de difusión configurando un enrutador para que deje pasar mensajes de difusión.

El ancho de banda compartido frente a ancho de banda conmutado. Como los conmutadores también conectan equipos a redes, pero de forma totalmente distinta, una red de conmutadores que divide el tiempo en fragmentos accesa a los equipos que tiene conectados de forma que cada puerto conmutado forma un canal con un dominio de colisión. Esto se llama ancho de banda conmutada, al contrario que el ancho de banda compartido son diez veces más rápidas que las redes compartidas en las mismas condiciones.

Por otra parte, las redes conmutadas aceptan LAN virtuales (VLAN's), permitiendo al administrador agrupar usuarios racionalmente en lugar de tener que agruparlos de acuerdo con el concentrador al que se conectan los dispositivos del equipo. Por ejemplo, un concentrador compartido por dos o más equipos forman un dominio de colisiones; Un conmutador no lo hace. Además de formarlos conectados los equipos, los grandes conmutadores conectan segmentos LAN para formar redes mayores. Para evitar la confusión, los dos tipos de conmutadores se llaman a menudo conmutadores de acceso y conmutadores LAN o redes troncales.

Los enrutadores controlan las redes, como el tercer dispositivo básico de una red es el enrutador. Los enrutadores conectan segmentos LAN en lugar de equipos, como lo hacen los concentradores y conmutadores de acceso. Los enrutadores se usan para aislar el tráfico interno y para mantener la seguridad interna. Además puede ampliar los dominios de difusión y multidifusión a segmento LAN específicos, para ayudar a unir esas redes en una unidad funcional.

Los enrutadores se distribuyen tanto en el interior de las redes como en la frontera de sistemas autónomos. Entre los enrutadores, hay algunos llamados enrutadores internos y otros enrutadores de acceso. Los enrutadores que se dedican exclusivamente a las comunicaciones con el exterior se llaman enrutadores finales o de pasarela. Por ejemplo, un Proveedor de servicios de Internet (PSI) usará enrutadores de puerta de acceso para conectarse a Internet. Por el contrario, una gran organización colocará un enrutador interno en cada una de sus divisiones para ayudar a controlar el tráfico interno.

Los enrutadores son más versátiles que los concentradores y los conmutadores porque son capaces de interpretar direcciones de red. Leen las direcciones de red para filtrar el tráfico, controlar el acceso a redes o a servicios y elegir la mejor ruta para alcanzar un destino. Los enrutadores dan sentido a las redes, no es casualidad que los tres dispositivos más importantes para las redes operen en distintos niveles de las siete capas del modelo de referencia OSI.

Los enrutadores operan en la capa de la capa de red, capa 3, hoy la mayoría de las redes usan direcciones de red IP, todos los enrutadores de Internet lo hacen. Pero muchos enrutadores internos todavía deben usar viejos protocolos. Por esa razón, Cisco y sus competidores crean productos multiprotocolos para esas redes.

Los enrutadores utilizan direcciones de red de la capa 3

Ya sea IP o un viejo protocolo de la capa 3, las direcciones de red son inherentemente jerárquicas. Mientras que un enrutador se abre camino a través de una dirección IP, se concentrara en el segmento LAN al que está conectado el equipo destino. En rutas de largo recorrido, el desplazamiento hacia la dirección se realiza mediante saltos entre los enrutadores. Una ruta de un salto sólo requeriría encontrar el segmento LAN en que reside el destino.

Es frecuente resumir las rutas antes de compartirlas con otros enrutadores. Esto mejora el rendimiento, al reducir en gran medida el número de direcciones que transporta una tabla de enrutamiento del enrutador.

El resumen de las rutas, también llamado agregación de ruta, funciona confiando que el enrutador de pasarela conozca la dirección completa del segmento LAN, permitiendo a los enrutadores intermedios transportar menos entradas en sus respectivas tablas de enrutamiento, incrementando así su rendimiento. También se usa con frecuencia la traducción de direcciones, donde las direcciones internas se modifican o agrupan en una dirección global dentro de paquetes enviados al exterior de una red. También utilizan mecanismos como Traducción de Direcciones de puerto PAT (Port Address Translation), y Traducción de direcciones de red NAT (Network Address Translation), en los enrutadores finales o en los cortafuegos para hacer estas traducciones en los campos de direcciones del paquete en ambas direcciones.

Los conmutadores utilizan direcciones MAC de la capa 2

Los conmutadores funcionan en la capa de enlace de datos (capa 2), manejando direcciones MAC en lugar de direcciones de red. Una dirección MAC es un número largo que identifican de forma unívoca dispositivos de hardware. Las direcciones MAC combinan un código de fabricación con un número de serie. Incluso los enrutadores usan direcciones MAC para el último escalón del mensaje, resolviendo una dirección IP a la dirección MAC física para localizar el equipo destino dentro del segmento LAN.

Las direcciones MAC son topologicamente planas. El perfil lógico de una dirección MAC aparece como si todos los equipos estuvieran conectados al mismo cable; no indica nada sobre dónde se ubican los equipos es esencialmente un número de serie. Sin embargo, las redes conmutadas deben operar usando difusiones de direcciones MAC a todos los puertos donde se desconoce un destino MAC.

Las VLAN jerarquizan las redes conmutadas limitando la difusión a grupos reducidos de usuario. Esto cambia la velocidad del ancho de banda conmutada con la topología jerárquica hasta ahora sólo disponible en redes de ancho de banda compartido. Además, las VLAN's asignan a los usuarios de forma flexible a grupos de trabajo lógico en lugar de tener que agrupar los usuarios por concentrador.

Método de optimización

Las redes usan protocolos para enrutar mensajes. Hay tantos cambios dinámicos en las redes, crecimientos, cambios en los modelos de tráfico, un dispositivo que falla, etc., que deben actuar ellos mismos de algún modo actualizando constantemente las tablas de enrutamiento del dispositivo. Las redes enrutadas se basan en protocolos de enrutamiento para hacer un seguimiento de las rutas a través de las redes. Por ejemplo, muchas redes pequeñas usan RIP 2; la mayoría de las grandes usan EIGRP este es propiedad de Cisco u OSPE es un estándar abierto. Estas negocian listas de rutas, la mayoría dentro de sistemas autónomos, que se usan para conectar segmentos LAN. BGP negocia listas de sistemas autónomos y se usan para conectar a Internet.

Las redes mantienen un grado de autómantenimiento mediante los protocolos de descubrimiento, que encuentran nuevos dispositivos y comprueban el estado de los ya conocidos. Estos protocolos, son Protocolo de Descubrimiento de Cisco CDP (Cisco Discovery Protocol) y son los elementos reconocidos de los protocolos de enrutamiento. Cuando sucede un evento se descubre y el aviso se transmite hasta que el conjunto de dispositivos converge en una nueva lista de rutas. A veces se produce un bucle, donde una ruta sugerida vuelve al dispositivo origen, creando rutas sin sentido que disminuyen o incluso bloquean una red. Los protocolos de enrutamiento usan métricas para ajustar de forma más precisa las redes. RIP sólo usa recuento de saltos, pero los protocolos más sofisticados usan métricas estrictas que se pueden combinar con matrices gigantescas para dirigir el tráfico a través de los enlaces deseados.

Las redes conmutadas no son tan complejas. Los conmutadores sólo intercambian listas de direcciones MAC donde la dirección MAC más reciente se coloca en la parte superior, siendo la primera que se elige. Las redes conmutadas usan Protocolos de Expansión de Árbol STP (Spanning Tree Protocol), para evitar bucles.

Aplicaciones y arquitectura de redes

Los requisitos de diseño de la empresa normal han cambiado totalmente. Estos cambios se han realizando en ambos extremos de la topología. En la parte inferior, el uso de concentradores de acceso por parte de la segmentación ha aumentado enormemente el número de segmentos LAN y, por lo tanto, la cantidad de tráfico que pasa a través de la red troncal entre segmentos. En la parte superior, se está estandarizando toda una nueva arquitectura de computación, con Intranet basada en la Web que sustituyen los tradicionales sistemas de administración cliente / servidor, donde las Extranets están transformando los sistemas tradicionales Intercambio electrónico de datos (EDI) y las Redes Privadas Virtuales VPN (Virtual Private Networks), sustituyendo a las redes de áreas anchas WAN concentradas.

La realización de todos estos cambios es lo que ha provocado que las nuevas aplicaciones de red hayan cambiado las características del tráfico. Por ejemplo, se ha popularizado la videoconferencia, aumentando la necesidad de optimizar la configuración para manejar la multidifusión, donde una misma copia de un mensaje se envía a un subconjunto de equipos destino.

2.2 Modelo de diseño

Las topologías jerárquicas y de segmentación son intrínsecamente mejores que las planas por varias razones, la principal es que una jerarquía contiene tráfico hacía su área local. La regla general que usan los diseñadores es que la difusión de tráfico no debe sobrepasar los 20 paquetes por cada enlace, la consecuencia de esa segmentación aumentará, naturalmente, el rendimiento al aislar el tráfico hacia sus usuarios más probables. Esta regla general sólo se aplica a la cantidad de paquetes de difusión que circulan y no se debe confundir con la regla 80/20. La regla 80/20 establece que el 80% del tráfico queda en origen y sólo el 20% transciende el área local.

Una topología plana, en la que cada dispositivo hace más o menos el mismo trabajo, aumenta el número de componentes con los que debe comunicarse un dispositivo individual. Esto aumenta de algún modo la sobrecarga del tráfico que puede aceptar el dispositivo e incrementa enormemente el tráfico total. Por ejemplo, cada vez que un enrutador recibe un mensaje de difusión, el CPU se interrumpe. Para muchas redes pequeñas, es suficiente una topología plana y no está justificado el gasto y la complejidad añadida que requiere la jerarquía. Pero no hacen falta demasiados segmentos LAN para efectuar negativamente el rendimiento y la fiabilidad de una red, con sus dispositivos y equipos entretenidos administrando tráfico innecesario.

Esa es la razón de por qué la industria prefiere un modelo de diseño jerárquico clásico. El modelo tiene tres capas: la capa principal, la de distribución y la de acceso. De esta forma se separa el tráfico local del gran volumen de tráfico que circula entre segmentos LAN y áreas, y permite a los dispositivos de red situados en cada capa, centrarse en sus respectivas tareas. El modelo jerárquico se describe en la figura 2.1.

La jerarquía es posible gracias a la segmentación, la práctica de dividir equipos en segmentos LAN más pequeños. La topología jerárquica y de segmentación tiene varias ventajas:

- Rendimiento. El tráfico se aísla en las áreas de origen, reduciendo así los dominios de colisión de paquetes y aumentando el rendimiento.

- Fiabilidad. Muchos fallos se aíslan en el segmento donde se originó el problema.

- Simplicidad. Al separar áreas diferentes, los elementos de una red se pueden duplicar según sea necesario mejorar la red.

- Escalabilidad. Se puede agregar elementos de diseño modular a medida que la red crece con el tiempo, interfiriendo de forma mínima en las redes ya existentes.

- Seguridad. Los accesos se pueden controlar en uniones bien definidas entre las capas.

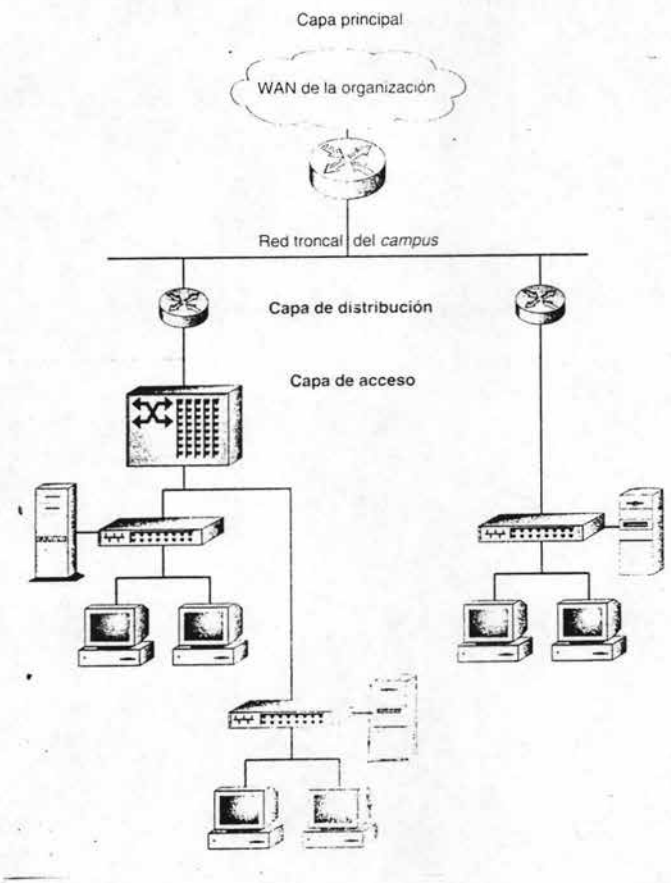


Fig. 2.1 La topología jerárquica de tres capas.

Las redes tienen naturalmente a una jerarquía de dos niveles. Los concentradores y conmutadores conectan equipos en segmentos LAN y la red troncal conecta los dos segmentos a la red local, ya sea dentro de una planta, un edificio, un campus de oficina o incluso en un área metropolitana. Esta es una topología relativamente plana en el sentido de que incluso aunque los dominios de colisión son limitados, un tráfico de difusión excesivo todavía hace uso del ancho de banda disponible. Esto convierte la capa de distribución en lo más importante. Al aislar el tráfico, la capa de distribución también aísla el problema y la complejidad.

La jerarquía ayuda a reducir costos. Al dividir equipos y tráfico, las variaciones se limitan a unos pocos segmentos LAN, o incluso a un único segmento. Las variaciones incluyen aspectos como protocolos de escritorio, volúmenes de tráfico y tipos de tráfico. La jerarquía permite al diseñador de redes ajustar la configuración para cada trabajo en particular. Los ajustes se hacen según el dispositivo de red adquirido y como está configurando el archivo de configuración en términos de memoria, software y parámetros de configuración.

La capa de acceso

Esta capa se compone fundamentalmente de concentradores y conmutadores que sirven para dividir a los dispositivos del equipo, como una PC y servidores, en muchos segmentos LAN compuestos de ancho de banda compartido o conmutada. Aquí es donde se puede realizar el filtrado de capa MAC.

Si una red dispone de sitios remotos, como sucursales u oficinas particulares, la capa de acceso incluirá también servidores de acceso. Las redes WAN deben usar algún tipo de medio de trasmisión a larga distancia. Existen muchos medios, como líneas digitales alquiladas T1 o T3 y redes digitales públicas Frame Relay. Los usuarios de acceso telefónico remoto se conectan llamando a través de líneas analógicas y en ciertas áreas, mediante tecnologías que ofrecen un mayor ancho de banda, como la Línea de Abonado Digital (DSL) Digital Subscriber Line y la Red Digital de Servicios Integrados (RDSI), la figura 2.2 muestra la funcionalidad de la capa de acceso.

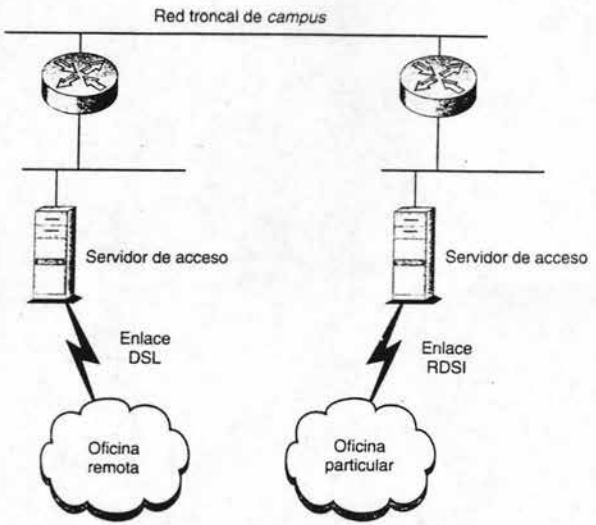


Fig. 2.2 La capa de acceso ofrece conectividad.

En las grandes redes, la capa de acceso puede incluir enrutadores. Estos enrutadores internos se ocupan principalmente de aislar la sobrecarga, controlar el tráfico y mejorar la seguridad interna, la capa de acceso engloba una mezcla de tecnologías en la mayoría de las redes. El Enrutamiento de Acceso Telefónico Bajo Demanda DDR (Dial-on-Demand Routing); se ha hecho habitual para conexiones remotas porque mantienen un enlace inactivo excepto cuando es necesario enviar o recibir datos, reduciendo así los costos de las telecomunicaciones.

La capa de distribución

Esta capa se compone principalmente de enrutadores. Se usan para separar el tráfico local de baja velocidad de la red troncal de alta velocidad. El tráfico en la capa de acceso tiende a usar un gran ancho de banda porque ahí es donde residen la mayoría de las direcciones LAN y equipos. La sobrecarga de red que provoca el tráfico de protocolos para los protocolos de descubrimiento SNMP, los protocolos de enrutamiento y otros sistemas de control de redes es mucho mayor en la capa de acceso.

Como los enrutadores son lo suficientemente rápidos para leer direcciones de red y examinar paquetes, también aumentan el rendimiento al enviar tráfico lo más directamente posible a su destino. Por ejemplo, los enrutadores de la capa de distribución definen los dominios de difusión y multifunción a través de segmentos LAN. Los dominios están, por definición, limitando a segmentos LAN; los enrutadores pueden ampliarse a través de segmentos mientras así lo indique el diseño de la jerarquía. La figura 2.3 describe la funcionalidad de una capa de distribución.

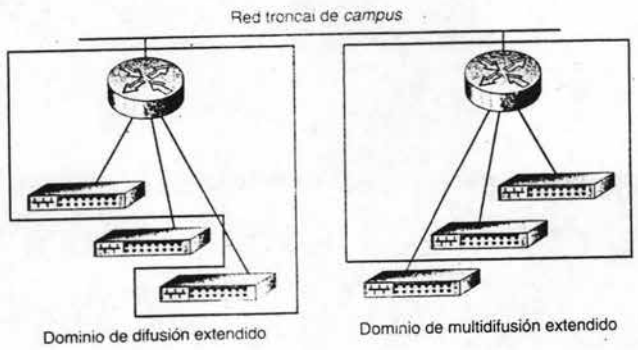


Fig.2.3 La capa de distribución es clave para una buena funcionalidad.

En configuraciones que usan conmutadores multicapa, los dispositivos de cada capa de distribución enrutan mensajes entre las VLAN's. La conmutación multicapa es una tecnología relativamente reciente en la que los paquetes se filtran y envían basándose tanto en las direcciones MAC como en las de red. El Catalyst 5000 es tal vez el mejor ejemplo de un conmutador multicapa, que incorpora Módulos de Conmutación Enrutada RSM (Route Switch Modules); además de los que tiene electrónicamente conmutada convencionalmente.

La mayoría de los servidores con cierto valor añadido los ofrecen los dispositivos en la capa de distribución. La traducción de direcciones se realizan es esta capa, normalmente en un enrutador de puerta de acceso o en un cortafuego. También se hace la agregación de direcciones, así como la agregación de áreas si la red dispone de dominios de enrutamiento OSPF. También se realiza la traducción entre los protocolos como IPX e IP; descifrándolos para transporte de VPN; seguridad basada en el tráfico usando listas de acceso algoritmos de cortafuegos basados en el texto; y seguridad basada en el usuario utilizando protocolos de seguridad como Radius, Tacacs+ y Kerberos.

La capa principal

Es la red troncal en las grandes redes, la capa principal consta de múltiples segmentos desde redes troncales LAN de campo hasta redes regionales. Algunas veces se configuran segmentos principales LAN especiales para manejar un protocolo especifico o tráfico especialmente sensible. Muchos segmentos están ahí para conectar segmentos LAN, normalmente los que están dentro de un edificio particular o campos de oficina. La figura 2.4 muestra una capa principal de una red de una gran empresa.

Para rendir al máximo, una red troncal LAN debería configurarse para sufrir el menor número posible de interrupciones. El objetivo es disponer de tantos ciclos de CPU de dispositivo de una red troncal como sean necesarios para la transferencia de paquetes entre segmentos. La capa de distribución lo hace posible al conectar segmentos LAN de grupos de trabajo y ofrecer servicios de enrutamiento de valor añadido. Debe hacer un mínimo de administración de paquetes en este nivel. Esa es la razón de por qué la mayoría de las redes troncales actuales son LAN conmutadas. La necesidad de interpretación de direcciones en la capa principal se minimiza por el proceso ya realizado por los enrutadores de la capa de distribución.

El Modo de Transferencia Asíncrona ATM (Asynchronus Transfer Mode), y el Gigabit Ethernet están compitiendo duramente para imponer su tecnología de red troncal conmutada. ATM es ideal para aplicaciones multimedia porque utiliza celdas de tamaño fijo en lugar de los paquetes de longitud variable de Ethernet. La notaria ventaja de las redes troncales conmutadas de Gigabit Ethernet es su mayor compatibilidad con los millones de LAN Ethernet ya instaladas en todo el mundo.

ATM es un estándar internacional de transmisión de celdas para servicios como vídeo, voz y datos. La longitud fija de sus celdas de 53 bytes acelera la transferencia de datos al permitir realizar el proceso por hardware. Aunque los productos ATM son para llevar datos directamente hasta su PC, la tecnología está optimizada para funcionar en medio de transmisión a alta velocidad.

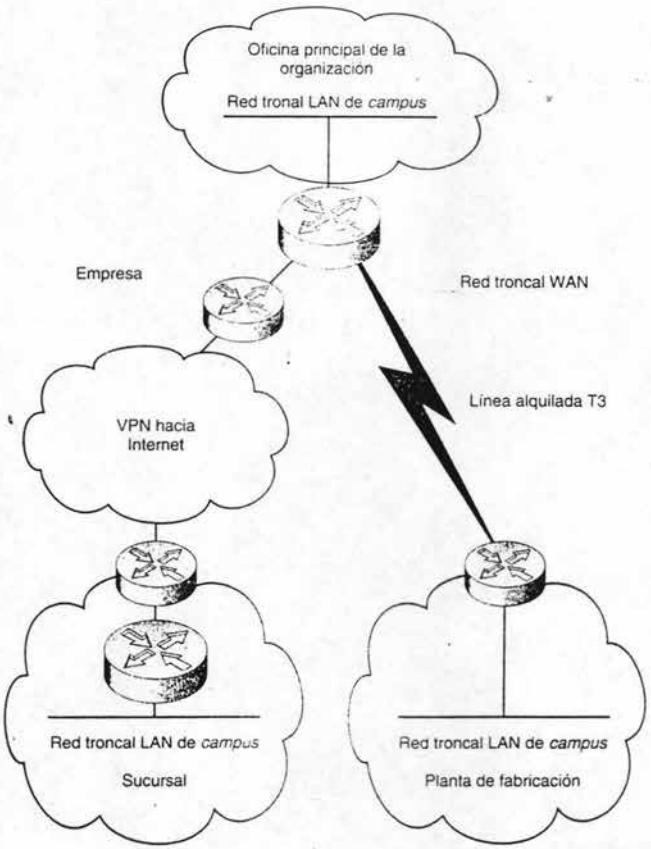


Fig. 2.4 La capa principal incluye redes troncales.

2.3 Método de diseño

Durante años, la industria de redes ha desarrollado todo un conjunto de conceptos y modos de conducta para el diseño de redes. Conforme evolucionan las topologías de redes según las circunstancias y el devenir de los tiempos, se hace más difícil mantener un diseño de red rigurosamente jerárquico, especialmente en grandes empresas con estructuras administrativas distribuidas, o en las que tiene gran rotación de personal de sus plantillas de red.

Equilibrio de carga y redundancia

La redundancia es la práctica de configurar equipos de seguridad. Esto se hace para ofrecer la tolerancia a fallos donde el tráfico se desplazará hacia el dispositivo de seguridad si falla la unidad primaria, un proceso llamado migración tras error. Por ejemplo, muchos segmentos principales de alta velocidad tienen conmutadores de configuración dual en cada extremo por si acaso se cae el conmutador principal. Otra medida de seguridad habitual es tener unidades de energía redundantes dentro de un dispositivo de modo que si una falla, el dispositivo sigue funcionando.

La tecnología de Cisco que soporta redundancia es el Protocolo de Enrutador Activo de Reserva (HSRP), la cual es una familia de comandos dentro del IOS. Activo de reserva es un término de la industria informática que significa que la unidad de seguridad siempre está activa y funcionando, permitiendo así una migración tras un error automáticamente en caso de fallo. HSRP funciona creando un grupo de enrutadores de seguridad, usando la dirección IP del enrutador primario para procesar el tráfico. El enrutador primario lo monitorizan otros del grupo y si falla, la dirección del enrutador de seguridad retomará las tareas del control del tráfico. La migración tras un error se logra sin la intervención humana y se suele realizar en pocos segundos.

Como la configuración redundante es cara, sólo se suele agregar configuraciones tolerantes a fallos a los dispositivos críticos. La redundancia se suele aplicar a los dispositivos de una red troncal y a los cortafuegos donde un fallo de dispositivo tendría efectos de difusión en toda la red.

El equilibrio de una carga es una técnica de configuración que desvía el tráfico a una enlace alternativo si se sobrepasa ciertos límites en el enlace primario. El equilibrio de carga se puede lograr de varias formas, como ajustando de forma precisa la métrica de enrutamiento en los archivos de configuración dentro de los dominios de protocolos de enrutamiento.

El equilibrio de carga se parece a la redundancia en el sentido de que un suceso provoca que el tráfico cambie de dirección y equipos alternativos deban estar presentes en la configuración. Pero en lo que respecta al equilibrio de carga, el equilibrio alternativo no es necesariamente un equipo redundante que sólo funciona en caso de fallo.

Topología de malla

Un buen diseño incorporará una topología de malla para conseguir redundancia y equilibrar una carga. Una malla es cuando dos dispositivos de red, normalmente enrutadores o conmutadores, están conectados directamente. Dentro de una topología completamente en malla, todos los nodos de la red están conectados entre sí dentro de la red ya sea mediante circuitos físicos o virtuales. También podemos tener una topología parcial de malla en la que algunas partes de la topología están completamente en malla, pero algunos nodos se conectan sólo a uno o varios de los demás nodos. Se puede apreciar las ventajas de una topología de malla en lo siguiente:

- Rendimiento. Sólo es necesario realizar un salto para ir de un nodo de la red a otro y cuando menos saltos mayor es la velocidad.

- Disponibilidad. Tener rutas redundantes significa que si alguna se cae, siempre hay disponible una o más rutas alternativas.

- Equilibrio. También se puede usar las rutas alternativas para operaciones normales, donde los parámetros de enrutamiento pueden configurarse para usar rutas alternativas si se excede una carga de tráfico establecida en el enrutador primario.

La red parcialmente en malla de la figura 2.5 no tiene estas ventajas. Por ejemplo, para ir desde el enrutador A al C es necesario pasar por dos enrutadores en vez de uno. Si los enrutadores situados a ambos lados del enrutador F se caen, este no podrá comunicarse con el resto de red. Además, un menor número de conexiones en las mallas reduce las oportunidades de realizar equilibrio de carga, sin embargo, aunque la conexión en malla ofrece ventajas, es necesario tener en cuenta que conlleva un costo:

- Gasto. Cada interfaz de enrutador o conmutador dedicada a crear la malla ya no se puede utilizar para conectar un segmento LAN. La malla consume recursos hardware.

- Sobrecarga de tráfico. Los dispositivos anuncian constantemente sus servicios entre sí. Cuantos más enlaces de malla tiene un dispositivo más paquetes de anuncio difunde, con lo que provoca sobrecarga de ancho de banda.

- Vulnerabilidad. El uso de malla dificulta la aparición de problemas dentro de un área local. Si un dispositivo mal configurado comienza a propagar indiscriminadamente mensajes de difusión, por ejemplo, cada elemento de la malla provocará una tormenta de difusión desde el origen.

- Complejidad. Si se agregan más conexiones, será más difícil aislar los problemas, por ejemplo, será más costoso hacer un seguimiento del dispositivo que provoca una tormenta de difusión en una red completamente o casi completamente en malla, ya que hay demasiados caminos a rastrear.

Por esta razón hay pocas redes de mallas completas. La práctica general es utilizar malla completa en la parte de red troncal de las topologías para proporcionar tolerancia a fallos y equilibrios de carga en estos enlaces críticos, pero utilizar sólo malla parcial en las capas de acceso y distribución.

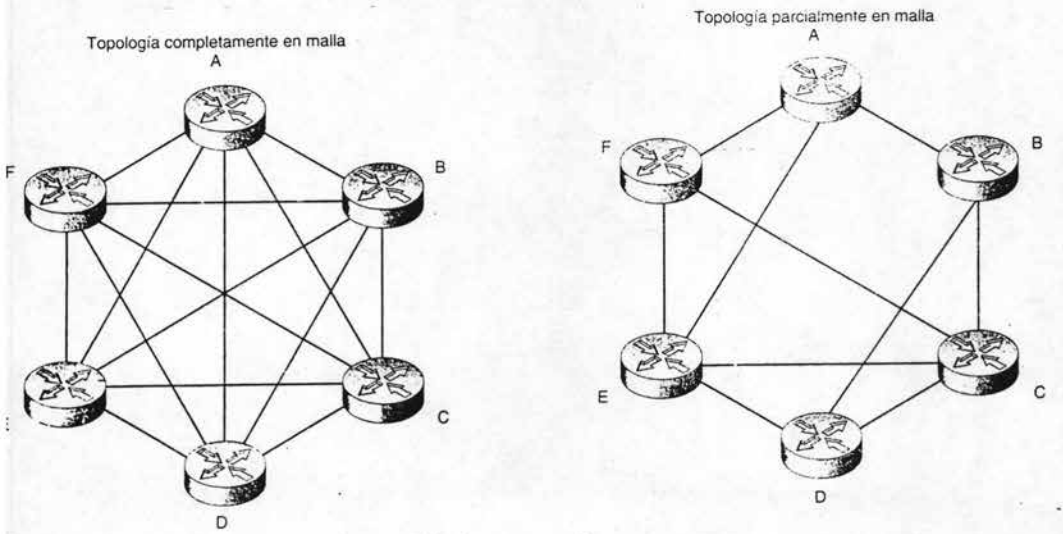


Fig. 2.5 Topología completamente en malla y parcialmente de malla.

Configuración de puerta trasera y cadena

Las circunstancias pueden obligar a desviarse del modelo jerárquico estricto. Las dos desviaciones topológicas más conocidas se llaman Puerta Trasera y Cadenas. Una Puerta trasera es cualquier conexión directa entre dispositivos en la misma capa, normalmente la capa de acceso. Una Cadena es la suma de una o más capas bajo la capa de acceso.

A veces tiene sentido configurar una puerta trasera. Por ejemplo, puede que queramos enlazar directamente dos sitios remotos si los enlaces a los enrutadores de la capa de distribución son costosos o lentos. Las puertas traseras también ofrecen cierto grado de redundancia: Si se cae el enlace de la puerta trasera, los dos sitios remotos pueden migrar después del error a la capa de distribución del enrutador y mantener la comunicación. Con demasiada frecuencia, sin embargo, aparece las puertas traseras y la cadena por la mala planificación de la red, o por un administrador irresponsable que instala equipo sin consultar al resto de la plantilla. La puerta trasera y la cadena se muestran en la figura 2.6.

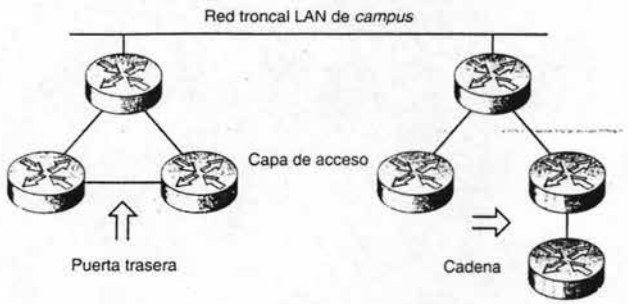


Fig. 2.6 La puerta trasera y la cadena.

2.4 Necesidades de la red

Se sorprendería si supiera cuántas redes, incluso las más grandes y sofisticadas, han crecido sin orden. El crecimiento descontrolado de las redes tiene lugar por varias razones. La más habitual es simplemente, que los acontecimientos suceden demasiado deprisa. Hay que tener en cuenta que algunas realidades habituales, computación cliente / servidor, Intranet, la Web, Extranet, eran sólo conceptos hasta la última década. Esto provoca que muchos administradores IT sin formación realicen planes estratégicos razonados y bien planteados para sus empresas. En muchos casos, un plan tampoco hubiera sido la solución. Las modas en administración vienen y van. La tendencia en administración ha ido buscando estructuras de organización planas, con el menor número de capas entre sí. La mayoría de los departamentos se rigen, en materia de presupuestos, por secciones individuales, grupos o incluso por departamentos. Es otras palabras, las decisiones IT cada vez se toman más desde abajo hacia arriba por la entidad que gestiona el presupuesto, no por el departamento central IT.

Esta manera de tomar las decisiones de forma distribuida ha adquirido relevancia especial debido a la lentitud de muchos departamentos IT para responder a las necesidades crecientes del usuario por culpa de cosas como la reestructuración de los procesos de negocios, fusiones adquisiciones y la creación de cooperativas. Se llegó a un punto en que muchos administradores de usuario final, simplemente, ignoraron la arquitectura técnica corporativa, descolgaron el teléfono y descargaron por sí mismo nuevas redes.

Las tendencias durante los últimos años de los departamentos IT ha sido la de dividir la interconexión de redes en grupo independiente llamado Infraestructura. Por así decirlo, es necesario separar los chips de los cables. Esto se ha realizado porque la interconexión de redes sencillamente se ha hecho demasiado grande y complicada como para dejarla en manos de un administrador que, por ejemplo, sabe algo de COBOL y de administración de proyectos de software de mainframes, las interconexiones de redes requieren dedicación completa, se está convirtiendo rápidamente en una disciplina propia con su propio bagaje de métodos óptimos.

La mayoría son diseños que se realizan sobre otros ya existentes para poder dar servicio a más usuarios o para actualizar la capacidad del ancho de banda, o ambas cosas a la vez. Una actualización habitual, por ejemplo, consiste en implementar una capa de enrutadores entre la red troncal LAN y la capa en la que los equipos pueden accesar a la red. Esto se ha realizado en muchas empresas para mejorar el rendimiento y conseguir un crecimiento controlado. Cualquiera que sea el cambio, es necesario analizar la infraestructura ya existente con detenimiento.

2.5 Características de la red

Hay varios métodos para comprender una red lo suficientemente bien como para plantear un diseño adecuado. Estos métodos se aplican ya sea en una red ya existente o en una topología a construir desde cero. Como los métodos se centran en geografía y tráfico, es decir, donde se ubican los nodos y qué viaja entre ellos. Un nodo es cualquier dispositivo dentro de la topología, incluyendo dispositivos de red, como enrutadores y equipos que soportan la carga, como los servidores. Para nuestros propósitos, al diseñar una red desde cero, la clave es identificar dónde están los usuarios y que utilizan.

Calidad de servicio (QoS)

Saber las características de una red es bueno a la hora de administración y al diseñarla. La industria está promocionando el concepto de Calidad del Servicio QoS (Quality of Service); el cual es un enfoque basado en gran medida en caracterizar el tráfico. Es la técnica de asegurar el rendimiento del tráfico que circula por una red. QoS es más sofisticado que garantiza simplemente que un enlace concreto funcionará a un determinado nivel de rendimiento. La mayoría de garantías QoS se asocian con un tipo concreto de tráfico, es decir, dan prioridad a la multidifusión de vídeo para enseñar a distancia sobre el correo electrónico y otro tráfico menos crítico.

Hay quienes consideran a este servicio como un refinado despliegue de marketing más que un producto real. Y de alguna forma es verdad dado que la complementación de QoS aún tardará un tiempo. Pero existe una serie de comandos QoS ya disponibles en la versión del IOS, la mayoría relacionados con el encolamiento del tráfico.

La política de implementación de QoS se basa fundamentalmente en información obtenida mediante SNMP y RMON, que se muestra a través de consolas NMS y CWSI Campus. Como dichas aplicaciones de consola, QoS utilizan el modelo cliente / servidor guardando una base de datos QoS y pone en práctica políticas mediante subprogramas creados específicamente, como el Policy Manager, Distribution Manager y Cisco Assure.

El policy Manager de Cisco crea comandos abstractos que agrupan comandos individuales del IOS para realizar tareas desde la GUI del Policy Manager de Cisco. Como otros subprogramas de consola NMS, al presionar un botón, uno o más comandos actúan sobre el dispositivo de red del cliente para configurarlo. Algunos subcomandos QoS son comandos genéricos del IOS, otros son específicos de QoS. Los principales comandos abstractos de QoS son:

- Encolamiento Ponderado Preciso (WFQ). Combina los comandos Interface y Fair-Queue para permitir a los administradores de red definir prioridades sobre cómo circulará una mezcla de tráfico a través de la topología. Por ejemplo, el correo electrónico debe tener mayor prioridad en los servidores de Lotus Notes, pero en ningún sitio más.

- Detección Temprana Aleatoria Ponderada (WRED). Combina los comandos Interface y Ramdom-Detect, este último acepta un valor alto para representar la importancia relativa de un tipo de tráfico. Wred trata de controlar la saturación del tráfico cuando comienza a aparecer.

- Intervalo de Acceso Comprometido (CAR). Es la tecnología de control de ancho de banda fundamental de QoS. CAR usa un sofisticado Rmon MIB para reconocer tipos de tráfico, establecer prioridades y limitar velocidad de los paquetes si es necesario.

Las técnicas de QoS se aplican en su mayoría a nivel de interfaz de red y hacen un uso intensivo de las listas de control de acceso para filtrar paquetes. La idea es diferenciar los tipos de tráfico dentro de las áreas de una topología e influir en el comportamiento de la red, una técnica conocida con el nombre de dar forma al tráfico. El objetivo de dar forma al tráfico es garantizar niveles mínimos de servicio punto a punto para diferentes tipos de tráfico. Hay algunos otros comandos QoS abstractos que se refieren a áreas especiales, como enlaces Frame Relay y agregación de ancho de banda Fast Ethernet Channel. Pero hasta ahora muchas áreas operativas carecen todavía de infraestructura QoS con contenido en forma de comandos y Rmon.

Comprender el flujo de tráfico

La comprensión y documentación del flujo de tráfico es el primer paso en el diseño de una red. La características del tráfico son en gran medida una cuestión de direccionalidad, simetría, tamaño de paquetes y volúmenes. Un flujo unidireccional realiza gran parte de la comunicación en una dirección; un flujo bidireccional comunica aproximadamente la misma frecuencia en ambas direcciones de una conexión. Un flujo asimétrico envía más datos en una dirección que en otra; un flujo asimétrico envía aproximadamente la misma cantidad de datos en una dirección que en otra. Por ejemplo, el flujo de una sesión http es bidireccional y asimétrico porque muchos mensajes se envían en las dos direcciones, pero la mayoría de los datos se descargan desde el servidor Web al explorador del usuario.

Identificación de orígenes de tráfico

Para comprender el flujo de tráfico debemos conocer sus orígenes. Esto se realiza identificando grupos de usuarios, no de personas individuales. En términos de metodología de computadoras, grupos de usuarios, a menudo, se conoce como una comunidad. Y para esto debería conseguirse un inventario de características de alto nivel y las aplicaciones utilizadas, la mayoría de los diseñadores de redes mostrarán esta información en una base de datos de herramientas, el siguiente ejemplo muestra una forma que podría usarse para recopilar información del usuario;

Comunidad	No. de personas	Ubicación	Aplicaciones	Tipo de equipo
Contabilidad	27	Polanco	AR, AP, GL	AS/400
Atención al cliente	200	Tlanepantla	Centro de atención	Windows NT 4.0

Tabla 2.1 Forma de recopilar información.

Se puede conseguir cualquier información que queramos. Por ejemplo, puede que no se quiera saber si de antemano todos usan máquinas Pentium o quienes usan variaciones de PC con estaciones UNIX y claro esto sería de mucha ayuda para el cálculo del tráfico.

Identificar orígenes y sumideros de datos

Todas las grades empresas tienen muchos usuarios y los expertos identifican a estos usuarios ávidos de información como sumideros de datos porque resulta útil rastrear los orígenes de datos que usan para ayudar a identificar modelos de tráfico. Las fuentes más comunes son los servidores de base de datos, los conjuntos de discos duros, las bibliotecas, sistemas de inventarios, catálogos en línea, etc. Los sumideros de datos suelen ser usuarios finales, pero a veces, los servidores pueden ser sumideros de datos.

Sumideros de datos	Ubicaciones	Aplicaciones	Comunidad de usuarios
Conjunto de servidores	Polanco	AR, AP, GL	Contabilidad
CCSRV	Tlanepantla	Centro de atención	Atención al cliente

Tabla 2.2 para identificar sumideros de datos.

Documentar que comunidades usan cada sumidero de datos permite entender el tráfico. Ahora podemos empezar a conectar usuarios de equipos de PC a servidores de sumideros de datos. Combinando la información de las dos ilustraciones anteriores podemos dibujar líneas entre clientes y servidores. Relacionar cualquier comunidad de usuarios con cualquier sumidero de datos e implicando y descubriendo un perfil definido de la topología ideal de red.

Identificar las cargas de aplicación y tipos de tráfico

La mayoría de las aplicaciones de red generan el tráfico con unas características específicas. Por ejemplo, FTP genera tráfico asimétrico de grandes archivos en sentido unidireccional. La tabla 2.3 es un ejemplo de tipos de mensajes comunes y su tamaño aproximado.

Tipo de mensaje	Tamaño aproximado
Página Web	50 K
Pantalla gráfica de Windows en un equipo	500 K
Correo electrónico	10 K
Documento de procesador de texto	100 K
Hoja de cálculo	200 K
Pantalla de terminal	5 K
Objeto Multimedia	100 K
Copia de seguridad de una base de datos	1 MB o más

Tabla 2.3 Tamaños normales de mensajes para estimaciones de tráfico.

Además de los niveles de tráfico, también es útil saber el tipo de tráfico. Los tipos de tráfico caracterizan la clase de dispositivos conectados y como fluye el tráfico entre ellos:

- Cliente / Servidor. Normalmente es una PC que se relaciona con un servidor UNIX o NT, esta configuración estándar del tipo cliente / servidor es el tráfico que suele ser asimétrico y bidireccional.

- Servidor / Servidor. Los ejemplos incluyen transparencia en los datos a un servidor redundante que hace una copia de seguridad de otro servidor, servicios de directorio de nombres, etc., este tráfico es bidireccional, pero la simetría depender de la aplicación.

- Terminal / equipo. Muchas aplicaciones basadas en terminal se ejecutan sobre IP, incluso en las conexiones de terminales IBM a Mainframe. Otro ejemplo es Telnet. El tráfico de la terminal es unidireccional, pero la simetría depende de la aplicación.

- Punto a Punto. Algunos ejemplos son la videoconferencia y configuración de la PC para acceder a recursos en otras PC's como impresoras y datos. Este tipo de tráfico es direccional y simétrico.

Comprender el tipo de tráfico que circula por varios enlaces da una idea clara de cómo configurarlo. El siguiente cuadro muestra información que se usa para identificar y caracterizar tipos de tráfico.

Aplicación	Tipo de tráfico	Comunidad de usuarios	Sumideros de datos	Ancho banda necesario	Políticas de QoS
Explorer Web	Cliente / Servidor	Ventas	Servidor de ventas	350 Kbps	CAR
TN3270	Terminal	Compras	AS / 400	200 Kbps	WRED

Tabla 2.4 Tipo de tráfico que circula por una red.

Con frecuencia, un enlace es dominado por uno o dos tipos de tráfico. La columna de ancho de banda necesario en el cuadro anterior se expresa normalmente como un bit por segundo estimado y puede ser Mbps o incluso Gbps.

Una vez que se identifican y caracterizan todas las aplicaciones dentro de una red, el diseñador tiene una línea base para adoptar decisiones de configuración dependiente del volumen. Verificar el tráfico es especialmente útil para saber dónde y como configurar políticas QoS. En otras palabras, debemos identificar que aplicaciones pasan por un enrutador antes de poder aplicar parámetros QoS en su archivo de configuración.

Comprender la carga de tráfico

Una vez documentada y caracterizada las comunidades de usuarios, orígenes y sumideros de datos y los flujos de tráfico, es posible medir los enlaces individuales con más precisión. La información del flujo de tráfico de la siguiente ilustración define perfectamente las rutas a seguir entre el origen y el destino. Antes de totalizar el ancho banda estimado de un enlace, debemos tener en cuenta factores colaterales, como las prioridades de QoS, crecimiento aproximado y a corto plazo, etc.

	Destino 1	
	Enlace	**Mbps**
Origen 1: Contabilidad	Frame Relay	0.056
Origen 2: Centro de atención	Punto a punto	1.54

	Destino 2	
	Enlace	**Mbps**
Origen 1: Contabilidad	Frame Relay	0.256
Origen 2: Centro de atención	Frame Relay	1.54

	Destino 3	
	Enlace	**Mbps**
Origen 1: Contabilidad	Frame Relay	0.256
Origen 2: Centro de atención	Frame Relay	0.512

Fig. 2.7 Comprensión del tráfico en una red.

2.6 La red lógica

Diseñar redes es con mucho una cuestión de elección. Muchas de las elecciones están relacionadas con seleccionar las tecnologías y los productos adecuados con las tareas a realizar, incluso habrá otros elementos del diseño sobre los que no tenemos control que obligará a tomar otras elecciones.

Una vez investigadas y documentadas en profundidad las necesidades presentes y futuras de la empresa, el siguiente paso es elegir las tecnologías para las distintas áreas funcionales:

- Selección de tecnología para la red troncal. Existe varias tecnologías de red troncal y se eligen basándose principalmente en el tamaño de la red y sus características de tráfico.

- Selección de protocolos. Se supone que IP es el protocolo de red, pero todavía es necesario elegir los protocolos de enrutamiento y los demás protocolos que se usarán.

- Selección de tecnología de acceso. Normalmente se plantea una mezcla de concentradores y conmutadores para cubrir perfectamente las necesidades de un grupo de trabajo o de incluso una PC particular.

Una vez escogidas las tecnologías subyacentes hay que configurar los productos específicos para hacerlos funcionar. Después de ese paso hay que realizar más trabajo de diseño para implementar la configuración.

El diseño de redes se realiza en dos niveles; la lógica y el campo. Los diseños de campo cubren la red local de la empresa, desde una PC hasta la red troncal de alta velocidad que sale al exterior. El nivel de empresa abarca múltiples redes de campo y se enfoca sobre configuraciones WAN, ya sea una WAN de línea privada o un sistema basado en Internet que se accesa a través de Internet.

Diseño de redes lógicas

Un diseño de red se define mediante una configuración física y otras lógicas. La parte física es la relacionada con el diseño topológico, dispositivos hardware, software de red, medios de transmisión y otras partes. La configuración lógica debe ajustar perfectamente al diseño físico en tres áreas:

- Direccionamiento IP. Un procedimiento para asignar direcciones de forma racional que pueda conservar el espacio de direcciones y soportar el crecimiento.

- Servicio de nombres. Un procedimiento que permite direccionar equipos y dominios mediante nombres simbólicos en vez de tener que utilizar direcciones IP separadas por puntos.

- Selección de protocolos. Escoger los protocolos a utilizar, especialmente los protocolos de enrutamiento.

El diseño de redes debería empezar con la capa de acceso, porque no es posible direccionar los niveles más altos hasta que se conozca el dispositivo y la población de usuarios. Por ejemplo, estimar la capacidad es virtualmente imposible hasta que se haya identificado y cuantificado todos los equipos, aplicaciones y segmentos LAN y la mayoría de estos elementos ocupan la capa de acceso.

Desde un punto de vista práctico, los tres elementos de diseño lógico, direccionamiento, nombramiento y enrutamiento son una buena base para trazar un boceto de cómo diseñar el hardware físico. Cada uno de ellos requiere reflexión y planificación.

Estrategias de direccionamiento IP

El número de direcciones disponibles se llama espacio de direcciones, las empresas utilizan varios esquemas de direccionamiento para maximizar el espacio de direcciones dentro de un bloque de direcciones IP que les ha asignado su proveedor de Internet. Se han desarrollado varias estrategias de direccionamiento, sólo para maximizar el espacio de direcciones, sino también, para mejorar la seguridad y la administración.

Los bloques privados de direcciones IP, en una empresa se reciben direcciones IP públicas de la organización Autoridad de Asignación de Números de Internet (IANA), que sólo suele asignar direcciones públicas a PSI y a grandes empresas como un intervalo de números, no como una única dirección IP. En la actualidad, la mayoría de las empresas reciben sus direcciones IP públicas de su PSI. Cuando se diseñó IP, el IETF reservó tres intervalos de direcciones IP para uso como direcciones privadas:

- 10.0.0. hasta 10.255.255.255
- 172.16.0.0 hasta 172.31.255.255
- 192.168.0.0 hasta 192.168.255.255

Estos tres bloques de direcciones IP se reservaron para evitar confusión. Podemos usar direcciones dentro de cualquiera de estos bloques reservados sin miedo a que uno de nuestros enrutadores se confunda cuando encuentre la misma dirección en el exterior, porque éstas son direcciones privadas que nunca aparecen en Internet.

Las direcciones IP privadas las asigna el personal de la red a los dispositivos internos. Como nunca se utilizarán en el exterior del sistema independiente, se pueden asignar direcciones privadas mientras permanezcan dentro del espacio asignado. No hace falta autorización del IETF ni de ningún otro organismo coordinador para usar direcciones privadas, que se usan por los siguientes motivos:

- Conservación del espacio de direcciones. A pocas empresas se les asigna un número suficiente de direcciones IP públicas para conectar todos sus nodos dentro de su red.

- Seguridad. Las direcciones privadas se traducen al exterior mediante PAT o NAT. Al no conocerse la dirección privada se dificulta a los intrusos entrar en sistemas independientes haciéndose pasar por un nodo interno.

- Flexibilidad. Una empresa puede cambiar de PSI sin tener que cambiar ninguna dirección privada. Normalmente, sólo hay que cambiar las direcciones de los enrutadores y de los cortafuegos que realizan las traducciones de direcciones.

- Tablas de enrutamiento más pequeñas. Al tener la mayoría de las empresas una única dirección pública o quizá sólo unas pocas direcciones IP, se contribuye a minimizar el tamaño de las tablas de enrutamiento que residen en los enrutadores de Internet, lo que implica una mejora del rendimiento.

El último elemento puede que explique por que el IEFT estableció una dirección IP de 32 bits en lugar de un planteamiento de 64 bits. Si se hubiera distribuido un espacio de direcciones mucho más grandes, hubiera reducido el uso de direcciones privadas. El uso de direcciones IP globales sería enorme, incrementando las tablas de enrutamiento en el proceso. Esto crearía la necesidad de enrutadores con CPU's más rápidos y con mucha más memoria.

Obtener las direcciones públicas IP de la organización sin ánimo de lucro IANA, que es responsable de que no haya dos empresas con la misma dirección IP. Pero pocas empresas obtienen su dirección IP directamente de la IANA; la mayoría las consiguen indirectamente a través de su PSI.

Direccionamiento dinámico, este direccionamiento es una técnica mediante la que se asignan direcciones IP a un equipo terminal cuando se conecta. Novell NetWare y AppleTalk han integrado capacidades de direccionamiento dinámico desde sus comienzos. No obstante, éste no es caso de IP. Recordemos que los protocolos de escritorio como NetWare IPX se diseñaron con el esquema cliente / servidor en mente mientras que IP se diseñó originalmente para conectar un sistema mundial global, la red Internet. El direccionamiento dinámico se hizo popular para cubrir las estaciones de trabajo sin disco duro que carecían de espacio para almacenar direcciones IP permanentes. El protocolo de configuración dinámica de equipo (DHCP) es el estándar consolidado actualmente y utiliza un modelo cliente / servidor en el que un servidor guarda una lista activa de direcciones disponibles y las asigna según sea necesario. DHCP también puede usarse como una herramienta de configuración. Admite asignación permanente automática de direcciones IP a nuevos equipos e incluso se usa para asignación manual de direcciones como forma de comunicarse la nueva dirección al equipo cliente. La figura 2.8 muestra el proceso DHCP.

La asignación dinámica es popular es fácil de configurar y conservar espacio de direcciones. DHCP funciona asignando direcciones durante un periodo de tiempo llamado alquiler, garantizando no asignar la dirección IP a otros equipos mientras dura el alquiler. Cuando el equipo se desconecta de la red, se notifica al servidor DHCP y restaura la dirección a su grupo de direcciones disponibles.

Para asegurar el servicio, se suele configurar múltiples servidores DHCP. Cuando el equipo inicia la sesión, envía un mensaje de descubrimiento por la red al servidor especificando en el campo identificador DHCP del mensaje. El servidor de DHCP responde con un mensaje de ofrecimiento del mismo o pasa la solicitud de descubrimiento a un servidor de reserva. El usuario acepta la oferta enviando un mensaje ACK DHCP como respuesta de recibo.

Si se acepta la oferta, el servidor finaliza el alquiler dentro del grupo de direcciones disponible conservando la asignación en memoria permanente hasta que termine el alquiler. La finalización del alquiler se produce cuando el usuario sale de la red. Si el servidor DHCP identificado está apagado o rechaza la petición, después de un tiempo de espera prefijado, puede que se haya configurado al cliente para enviar una solicitud de descubrimiento a un servidor de reserva. Si el servidor no está en la misma subred, puede configurar un enrutador como estación repetidora DHCP para dirigir el mensaje de petición al segmento LAN en el que reside el servidor.

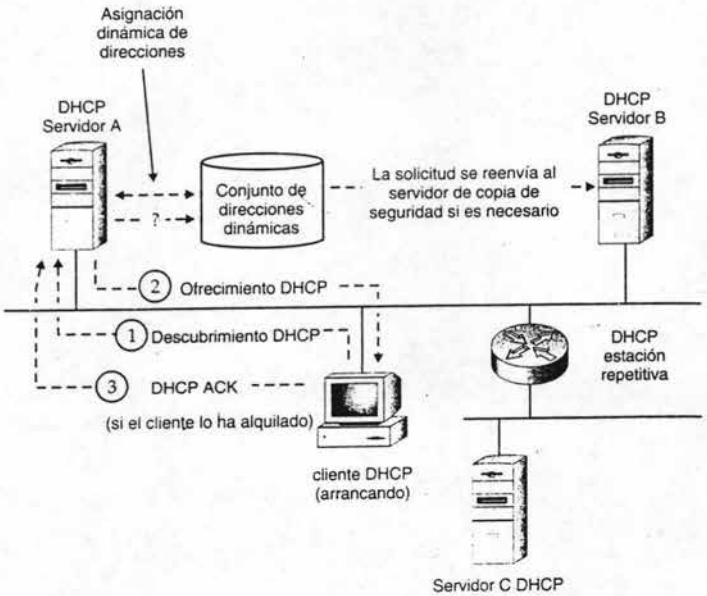


Fig. 2.8 DHCP puede asignar direcciones IP dinámicas.

Sistemas de nombres de dominio

El servicio que se usa para asignar nombres en Internet se denomina Sistema de Nombres de Dominio DNS (Domain Name System). Un nombre DNS tiene dos partes: el nombre del equipo y nombre del dominio.

Para que funcionen los nombres de dominio, en algún momento deben asignarse a una dirección IP de forma que los enrutadores los puedan reconocer. Esta asignación se llama resolución de nombres, una tarea que realizan los servidores de nombres. El sistema de nombres de dominio distribuye base de datos por muchos servidores para poder responder las solicitudes de resolución. Una organización distribuirá su base datos DNS por toda su topología de red. Las personas pueden navegar por Internet porque las bases de datos DNS se distribuyen por todo el mundo. La figura 2.9 describe el proceso de servicio de nombres.

Cuando un cliente necesita mandar un paquete, debe asignar el nombre descriptivo del destino a su dirección IP. El usuario debe tener configurado para esta acción lo que se conoce como software de resolución. El software de resolución del cliente envía una solicitud a un servidor DNS local, recibe la contestación, escribe la dirección IP en el encabezado del paquete y lo transmite. La asignación nombre IP se almacena en la memoria caché del usuario durante un período de tiempo prefijado. Mientras el usuario dispone de la asignación de un nombre en la memoria caché, evita todo este proceso de solicitud.

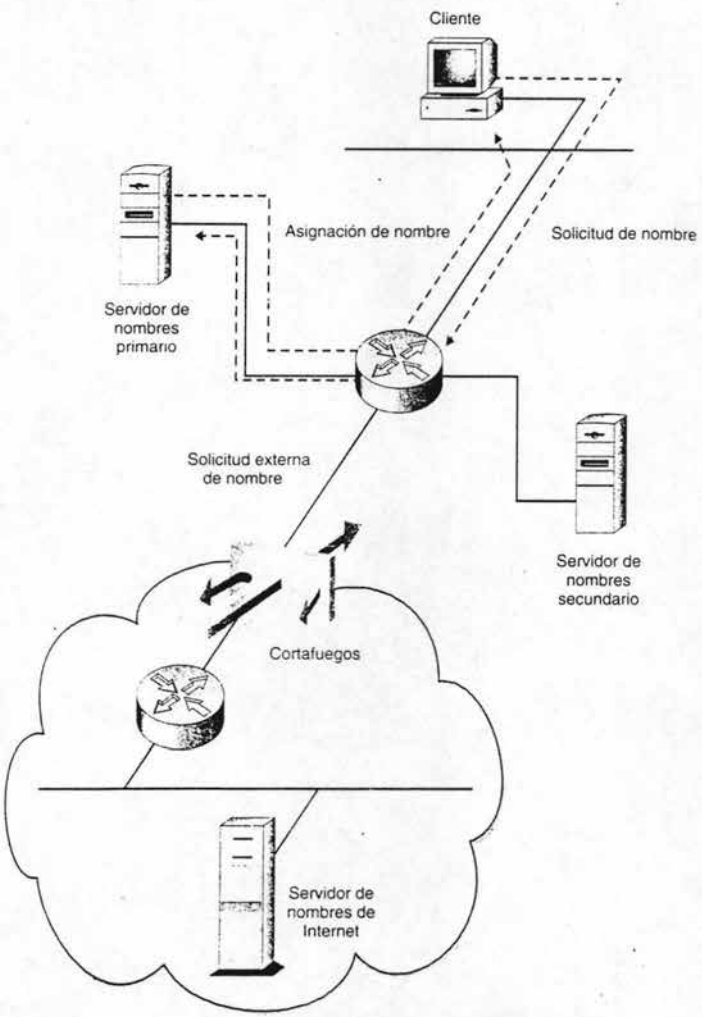


Fig. 2.9 Los nombres de dominio los almacena un servidor de nombres.

Configuración del servidor de nombres

Muchas redes disponen de múltiples servidores DNS por motivos de velocidad y redundancia, especialmente los grandes sistemas autónomos en los que suele contactar y desconectar equipos. Normalmente, muchos servicios se administran desde el servidor central de una red. Por ejemplo, las redes NT tienen algo llamado Controlador de Dominio Primario, que es el responsable de varias tareas de mantenimiento, incluyendo las peticiones de conexión.

Aparte de DNS, los otros dos servicios más importantes son Servicio de Internet de Windows (WINS) y Servicios de información de Red (NIS). Mientras DNS está optimizado para asignaciones de Internet, WINS y NIS administran servicios de nombres a nivel de redes. Los servidores WINS usan DHCP para peticiones de campo porque DNS no puede mejorar nombres dinámicos. NIS realiza una función parecida entre equipos UNIX.

DNS es un estándar importante. Puede ir de un equipo a otro por todo el mundo porque hay cientos de miles de servidores DNS en cualquier parte del globo, intercambiando y guardando en la memoria caché la asignación de nombres a través de dominios de enrutamiento para que tarde lo mínimo en conectarse con un nuevo sitio Web.

2.7 La red de campo

Significa cualquier red local con una red troncal de alta velocidad. Por ejemplo, la red local con una red troncal de una organización situada toda ella en un edificio es un ejemplo de una red de campo, se han desarrollado varios modelos para configurar las redes de campo.

La configuración enrutador / conmutador / concentrador

Esta configuración abarca las capas de acceso y distribución de las tres que hay en el modelo de diseño de red jerárquico. Estas dos capas se tratan juntas porque los enrutadores de distribución se localizan generalmente en el mismo lugar que los dispositivos del equipo a los que se permite accesar a la red.

La configuración de la capa de acceso del modelo jerárquico de tres capas es principalmente una función de la llamada configuración enrutador / conmutador / concentrador. La principal excepción a esto es el acceso remoto. Configurar la capa de acceso es muy importante por que une los equipos de un departamento o la planta de un edificio. Por lo que respecta al medio, supondremos que se usa el cable Par Trenzado sin blindaje (UTP) de categoría 5 para cablear equipos con dispositivos de acceso. Hay que tomar en cuenta dos decisiones al configurar las capas de acceso y de distribución:

- Tipo de red. La mayoría de los segmentos LAN de las capas de acceso que se diseñan en la actualidad funcionan con especificaciones Fast Ethernet, la variante a 100 Mbps del estándar Ethernet. Token Ring ha perdido campo por estas características, limitándose su uso a empresas de usuarios dominadas por IBM.

- Tipo de ancho de banda. Cada vez más segmentos LAN de capas de acceso funcionan sobre el ancho de banda conmutada en lugar de ancho de banda de concentrador compartido. Sin embargo, los conmutadores suelen estar entre un 30 % ó 40% más caros que los concentradores, lo que provoca un uso selectivo del puerto de comunicación en la mayoría de las empresas.

Estas decisiones dictan que producto de Cisco elegir y de algún modo como diseñar nuestra topología.

Seleccionar la tecnología de la capa de acceso, resulta más ventajoso utilizar Fast Ethernet para la capa de acceso. Es rápido, barato y el sector de administradores de red sabe que es la mejor especificación LAN. Si tenemos Token Ring o Ethernet a 10 Mbps, las operaciones son más limitadas. También es necesario tener cuidado de que cualquier cableado de planta cumpla los requisitos físicos especificados por la tecnología LAN.

La forma exacta de proyectar la capa de acceso es un poco más complicada. Si hemos reunido la información sobre las necesidades planteadas anteriormente, se estudiará lentamente hasta que nos informe de dos importantes cuestiones:

- Jerarquía del grupo de trabajo. Los grandes grupos de trabajo homogéneos suelen compartir redes conmutadas planas. Por ejemplo, los grandes departamentos de atención al usuario o departamento de información se inclinan por conectarse a un sólido conjunto de equipos para ejecutar un conjunto de limitado de aplicaciones. Estos establecimientos son buenos candidatos para redes conmutadas planas no VLAN'S.

- Niveles de tráfico. Si el volumen de tráfico es pesado y las políticas de QoS son estrictas, podríamos estudiar las redes conmutadas VLAN, o al menos, las configuraciones de red enrutadas de gran ancho de banda.

La configuración comienza a tomar forma, con bastante frecuencia, el proceso se repite de un lugar a otro. Después de todo, solo hay variaciones de conexiones y administración.

Un conjunto de datos, también llamado armario de cables o centralita, es una pequeña habitación que aloja paneles de revisión que conectan equipos a concentradores o accesan a puertos del conmutador. El panel de revisión es donde se inicia la red. Un panel de revisión es un dispositivo pasivo con hileras de conectores RJ-45, parecidos a los conectores RJ-11 de los teléfonos. El cable UTP del dispositivo del equipo se conecta en un cable de otro conector o puerto de conmutación. Esta disposición modular ofrece flexibilidad a la hora de mover dispositivos entre puertos.

Las señales pasan a través del concentrador o conmutador saliendo del puerto de vínculo ascendente para conectarse al enlace ascendente del edificio. Enlace ascendente se refiere al grupo de cables que viajan por todo el suelo hasta el punto de terminación. Un vínculo ascendente conecta el concentrador o conmutador en sentido lógico, donde el enlace ascendente se encamina hacia una parte más grande del equipo, normalmente un enrutador o un conmutador LAN.

La distribución principal (MDF) es normalmente una habitación de sitio seguro y colocada en el primer piso del edificio. El MDF sirve como punto de terminación para el cableado que proviene de los armarios de datos, a menudo equipados para voz y datos a la vez. La tendencia ha sido la de situar el MDF en la sala de computadoras de la organización, si existe en el edificio. Dependiendo de la distribución del edificio, la red troncal viaja a través de túneles realizados en el suelo o a través de los huecos en el ascensor.

En los grandes edificios, el medio de enlace ascendente es casi siempre cable de fibra óptica. La principal razón para usarla es que puede transmitir datos a más de 100 metros y no le afectan las interferencias eléctricas de los edificios. Pero también hay otra razón de tipo físico: como un enlace ascendente esta colgado, con el paso del tiempo el peso dejará al descubierto el cable de par trenzado desenrollando las tiras de cobre y deteriorando sus propiedades eléctricas. El vidrio de la fibra óptica no sufrirá porque no está trenzado. El siguiente esquema muestra lo dicho anteriormente.

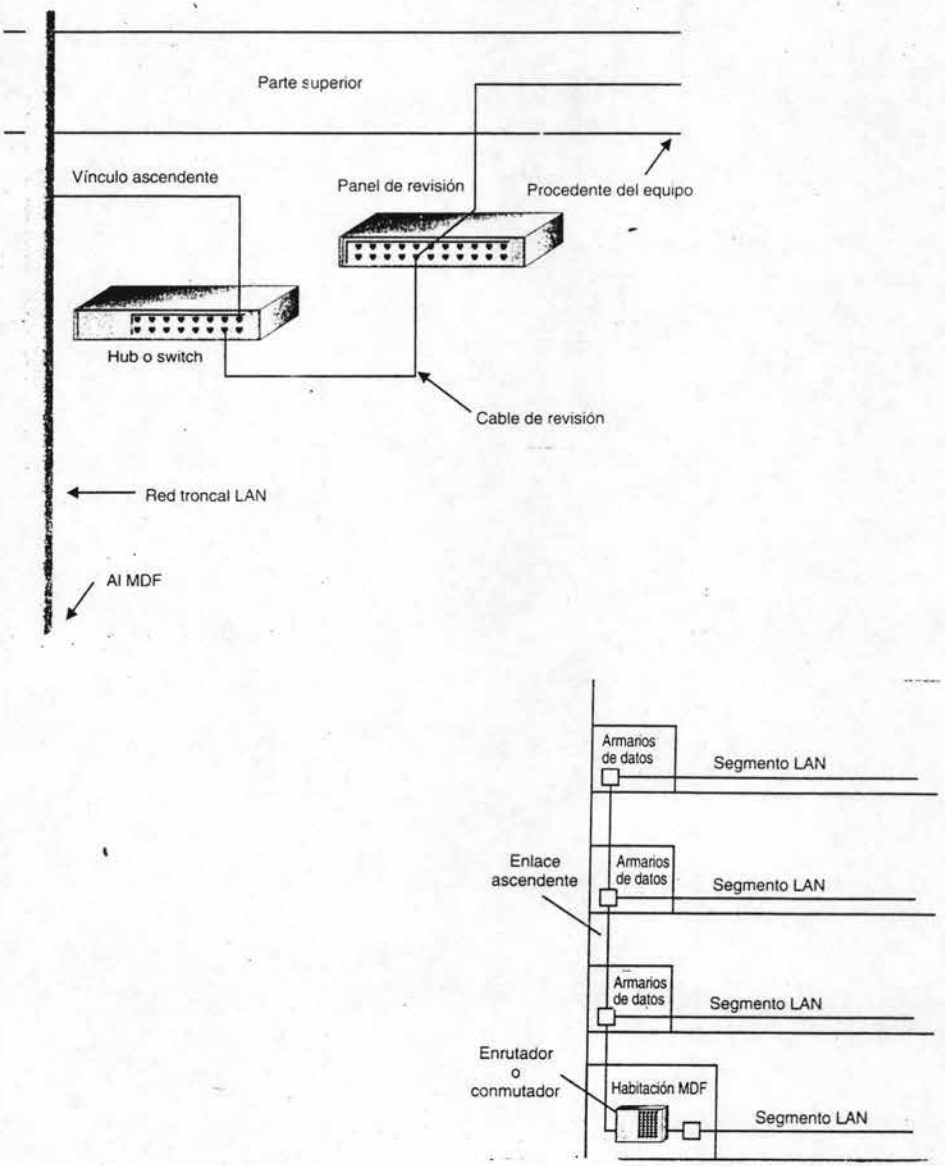


Fig. 2.10 Esquema ilustrativo de diseño.

La configuración del Enrutador / Conmutador / Concentrador. Se aplican varias reglas generales al configurar la capa de acceso. El cable UTP puede extenderse hasta 100 metros del lugar de concentración de datos. Esto suele bastar en el plano horizontal. Si el armario de datos se coloca en el centro de la planta, el tendido real puede ser de 200 metros. Como se muestra en la figura 2.11, no todos los edificios son verticales. Muchos son grandes estructuras horizontales de una o dos plantas, como las plantas industriales y almacenes. Para plantas muy grandes, lo normal es colocar armarios de datos en cada lado.

Desde un punto de vista lógico, no tiene sentido colocar un enrutador o conmutador LAN en cada planta. Hacerlo puede ser un gasto muy grande y lo que es más importante, malgastaría un espacio de direcciones IP, porque cada segmento LAN debe tener una única dirección IP. La estrategia, entonces, es minimizar el número de interfaces enrutadoras que dan servicio a un número dado de equipos. Los concentradores y conmutadores realizan esta tarea.

La figura 2.11 muestra una configuración para organización de tamaño medio con algunos cientos de empleados dentro de un edificio. Para conectar los usuarios en cada planta, se instala al menos un Fast Hub 400 de Cisco en cada armario de datos. El modelo Fast Hub 400 conecta entre 12 y 14 equipos cada uno y se puede apilar hasta cuatro unidades por pila. El tamaño de la pila depende del número de empleados de la planta. El modelo concreto Fast Hub 400 depende de la densidad de equipos: algunos modelos admiten 12 puertos para una densidad de puertos de 48 y otras admiten 24 puertos para una densidad de puertos de 96. Si el número de equipos sobrepasa los 96, basta con colocar otra pila en el armario de datos para incrementar el número de puertos.

La parte inferior izquierda de la figura 2.11 muestra cómo un enlace ascendente no es una red troncal en el estricto sentido del término. El vínculo ascendente que sale del Conmutador Catalyst 5000 de la planta principal expande el grupo de enlaces ascendentes a un total de cinco cables de fibra, que son fundamentales cables largos que se utilizan para evitar tener que colocar un dispositivo terminal en cada planta. Piense en los cables ascendentes como en cables alimentadores en lugar de una red trocal.

La tecnología LAN de todo el edificio de ejemplo es Fast Ethernet, que funciona a 100 Mbps. Esta velocidad es suficiente para conectar la mayoría de los individuales. Hablando claro, esto significa que nuestro enlace ascendente accesa a MDF a una velocidad total de 500 Mbps; por eso es necesario un dispositivo rápido para manejar las conexiones. Hemos colocado un Catalyst 5000 de Cisco para esa tarea. Con un panel posterior de 1.2 Gbps, el Catalyst 5000 tiene suficiente potencia para manejar el flujo de los cinco segmentos LAN. Esta caja tiene cinco ranuras de módulo, pero una simple tarjeta de 12 puertos 100 FX puede manejar los cinco segmentos LAN, dejando gran espacio para el crecimiento. Una segunda ranura se usa para conectar al exterior, quedando tres ranuras vacías.

La figura 2.11 describe las ventajas intrínsecas de la conmutación LAN. Recordemos que un conmutador es generalmente diez veces más rápido cuando contiene una dirección MAC en su tabla de direcciones. Nuestro modelo de organización tiene 300 empleados y el Catalyst 5000 tiene una mayoría y un panel posterior suficientemente rápido como para manejar una tabla de conmutación de ese tamaño. Como el conmutador se relaciona con 300 equipos, permite que se pueda leer sus direcciones MAC.

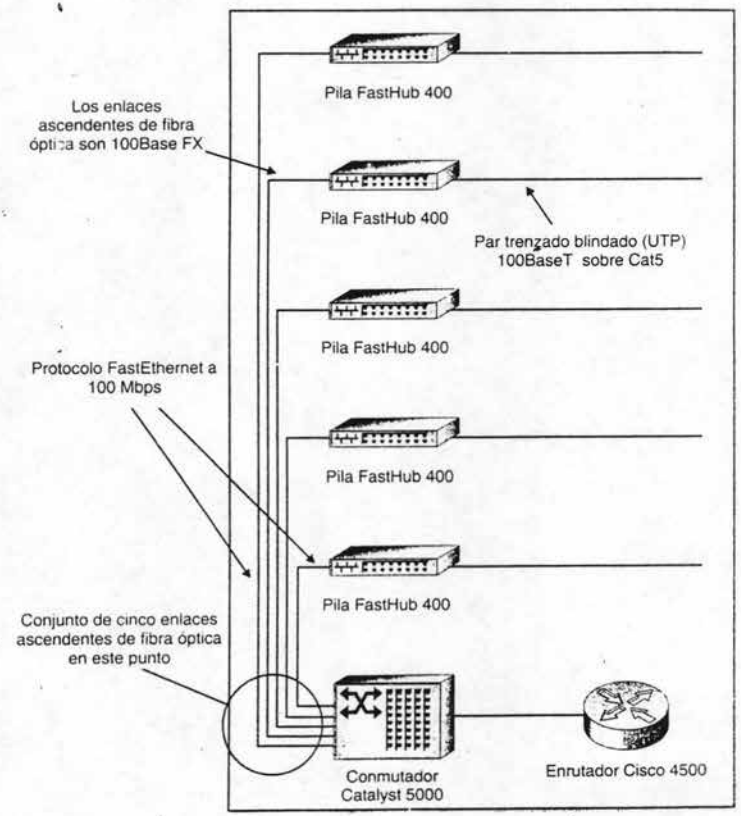


Fig. 2.11 Configuración Enrutador/Conmutador/Concetrador.

La configuración del conmutador de acceso. Los concentradores con el paso del tiempo cederán el paso a los conmutadores y esto se refiere a conmutación de acceso, al contrario que ejemplo de conmutación LAN de la figura 2.11. Un conmutador de acceso hace lo mismo que un concentrador, conecta equipos a segmentos LAN. Esto extiende el ancho de banda conmutada desde el escritorio al servidor. La figura 2.12 muestra una configuración típica de conmutador de acceso.

No sería práctico instalar un cable de fibra óptica desde el MDF hasta cada equipo. Como muestra la figura 2.12, se puede configurar un paso intermedio usando un conmutador de acceso como el Catalyst 1912 de Cisco, capaz de conectar hasta 12 dispositivos. No utilizaremos aquí un conmutador de bajas prestaciones, como el MicroSwitch, porque carece de puerto FX para conectarse a un enlace ascendente de fibra óptica.

El modelo jerárquico prohíbe conectar concentradores a conmutadores. Esto facilita la conectividad a la red troncal, pero equivale a una configuración en cadena. Por ahora, la realidad es que las conexiones concentrador / conmutador se usan habitualmente en diseño de redes porque es una manera fácil de agregar puertos de conexión a una topología.

Es necesario recalcar que en entornos de alta densidad, se indica a los usuarios que configuren conmutadores Catalyst de altas prestaciones en el armario de datos o que instalen cables que vayan hasta MDF.

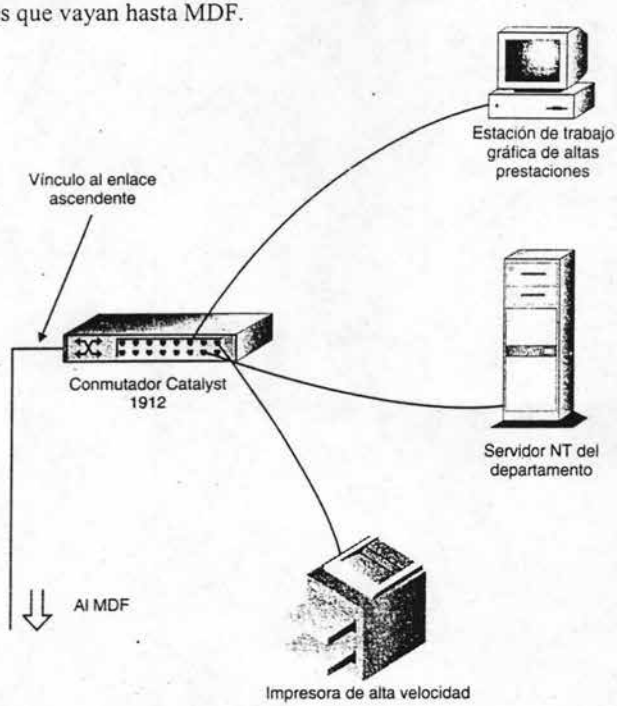


Fig. 2.12 La configuración del conmutador de acceso para más ancho de banda.

La configuración enrutador / conmutador es para poder realizar la interconexión de redes, los usuarios necesitan ser enrutados en algún punto. La práctica habitual es configurar un enrutador local en la sala MDF. De esa forma, los usuarios dentro de la compañía se conectan a la red de la empresa para realizar las conmutaciones internas y al cortafuegos para tener acceso a Internet.

La figura 2.13 amplia la sala MDF de la organización del ejemplo. En este caso se configurará un enrutador Cisco 4500 porque tiene tres ranuras de expansión que pueden albergar módulos LAN o WAN. Una ranura se ocupa con módulo LAN 100BaseTX de un puerto para conectar el conmutador Catalyst 5000; la otra alberga un modulo WAN T1 de un puerto, conectado así al exterior.

Si cree que con todo el ancho de banda circulando por el edificio, un sencillo conducto de 1.544 Mbps exterior puede que no ofrezca suficiente capacidad, tiene razón. Un enlace T1 podría no ser suficiente dependiente de cuanto tráfico local viaja al exterior.

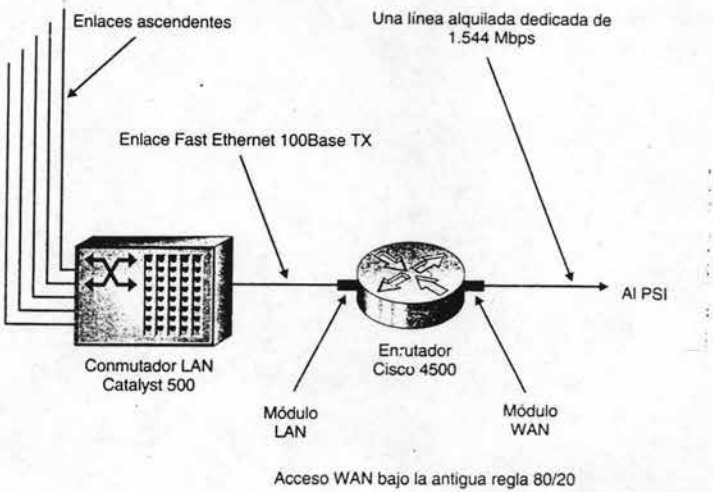


Fig. 2.13 La configuración Enrutador / Conmutador son para conexión al exterior.

La regla 80/20. Se ha hablado tradicionalmente que el 20% del tráfico se realiza con el exterior. Pero las cosas han cambiado. Ahora los expertos dicen que 80% del tráfico puede ser con el exterior, ya que los usuarios accesan a Internet para descargar archivos, hablar con otras secciones de la Intranet de la compañía o incluso negociar con socios comerciales a través de una Extranet.

El principal factor que ha provocado el cambio de tendencia hacia la regla 80/20 es el comercio electrónico, en el que los equipos conectados en red están sustituyendo a las tradicionales ventas interpersonales. El comercio electrónico de negocio a negocio, llamado Intercambio de Datos Electrónicos (EDI), está generando más tráfico IP cada día.

Si se acepta la regla 80/20 en una compañía, la sala MDF podría configurarse sobre las líneas de la figura 2.14, donde un conducto más grueso sale al exterior en forma de línea T3, un medio de enlace WAN de línea digital alquilada de 43 Mbps.

Ahora el enrutador es mayor y el conmutador es más pequeño. Si los usuarios conectaran con el exterior el 80% del tiempo, habría menos necesidades de conmutar el tráfico dentro del edificio. Hemos situado un conmutador Catalyst 3000 de Cisco en lugar del Catalyst 5000 porque es necesario realizar menos trabajo de LAN. En enrutador de altas prestaciones Cisco 7205 está preparado para ofrecer un mayor rendimiento, con un procesador más ágil y cinco ranuras de expansión.

A 45 Mbps, una línea T3 funciona 30 veces más deprisa que una línea T1. Cada vez más empresas optan por T3 para hacer la conexión punto a punto a su PSI. Las pocas, sin embargo, necesitan toda esa capacidad, por eso la mayoría de los PSI's revenden una porción del ancho de banda a usuarios individuales según sus necesidades, una práctica llamada Fraccionalización, en la que el usuario contrata sólo una parte de la capacidad del enlace.

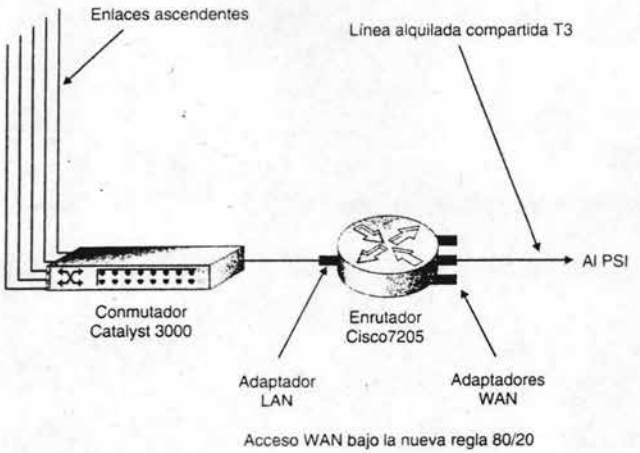


Fig. 2.14 Regla 80/20.

Elección de la red troncal de alta velocidad

Las redes troncales se usan para conectar nodos principales de red. Un enlace de red troncal conecta dos nodos concretos, pero a menudo se utiliza el término red troncal para hablar de una serie de red troncal. Por ejemplo, una red troncal de campo podría extenderse por varios enlaces.

Los enlaces de red troncal sólo transmiten datos entre dispositivos de red troncal, no manejan tráfico entre segmentos LAN dentro de un sitio. Esto se realiza en la capa de distribución del modelo jerárquico de tres capas conmutadas y enrutadores LAN. Las redes troncales se centran en mover el tráfico a alta velocidad a través de una región.

Las redes troncales de campo obviamente cubren un espacio reducido, normalmente mediante un cable de fibra óptica subterráneo. Las redes troncales WAN, que las usan de red troncal WAN los manejan los llamados proveedores de red troncal de Internet, aunque muchas grandes empresas operan sus propios enlaces de larga distancia a alta velocidad. Los enlaces WAN funcionan mediante enlaces de cables de fibra óptica de alta velocidad subterráneos, por torres metálicas.

Están haciendo habitual los enlaces por satélite. A pesar del medio de transporte y si es una red troncal de campo o WAN, comparten las características siguientes:

- Manipulación mínimo de paquetes. La mejora de listas de control de acceso y el filtro de cortafuego no se contempla en las redes troncales para aumentar el rendimiento. Por ello, la mayoría de enlaces de red troncal son conmutados, no enrutados.

- Dispositivos de alta velocidad. Un dispositivo lento, como un Cisco 4500, no se instalaría en una red troncal de alta velocidad. Los dos extremos de un enlace de red troncal suelen funcionar con un enlace Catalyst 5000 o mejor.

- Transporte rápido. La mayoría de las redes troncales de alta velocidad se basan en la tecnología de transporte de 1Gbps o más rápido.

Hoy en día, las dos principales tecnologías de red troncal son ATM y Gigabit Ethernet.

Las redes troncales ATM utilizan un formato de longitud fija al contrario que Ethernet, que usa paquetes de longitud variable. El formato de longitud fija permite un rendimiento de alta velocidad porque el hardware siempre calcula exactamente dónde empieza cada celda. Por ello, ATM ofrece una buena relación entre sobrecarga y el control de red del tráfico general. La arquitectura también permite QoS, un gran valor para manejar enlaces de red troncal crítico.

La figura 2.15 muestra una red troncal de campo construida con ATM. Esta configuración utiliza conmutadores de LAN Catalyst 5000 para el perímetro de un edificio en particular y enrutadores de conmutación multiservicio Catalyst 8500 para manejar el tráfico que llega al conjunto de servidores central de la organización.

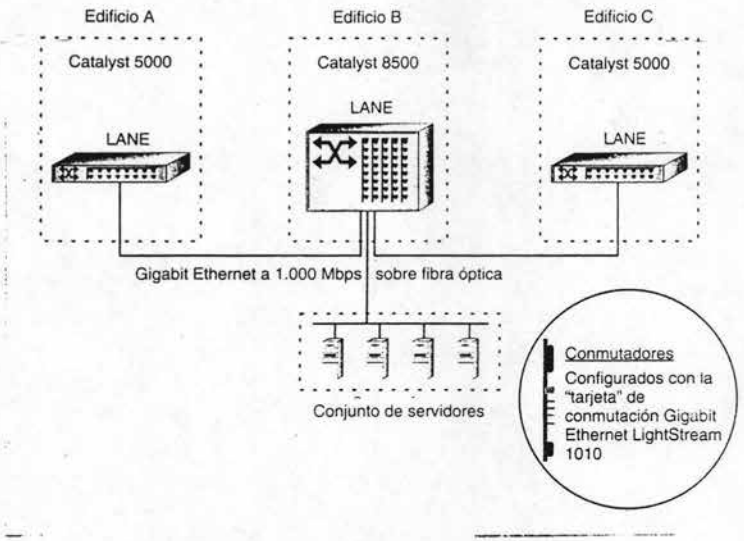


Fig. 2.15 Una red troncal ATM de campo.

Una tarjeta es un término industrial para una gran placa de circuitos impresos que, básicamente, es un dispositivo de red completo en un único módulo. Las tarjetas se introducen en una ranura de expansión, para que un conmutador Catalyst pueda entenderse con ATM, es necesario configurar una tarjeta adaptadora adecuada en el chasis. En este caso se usara la tarjeta LightStream 1010 porque está diseñada para tráfico a corto plazo; existen tarjetas ATM finales para tráfico WAN. Una razón para esto es que Cisco incluya diferentes tecnologías en un solo producto.

Los dispositivos ATM de Cisco usan la tecnología de adaptador Emulación LAN (LANE) para integrarse con redes Ethernet de campo.

Las redes troncales WAN conmutadas funcionan sobre troncos de fibra óptica de muy alta velocidad bajo la especificación SONET. La mayoría de las redes troncales que se instalan son OC-48, que funcionan a unos 2.5 Gbps. La Portadora Óptica (OC) Optical Carrier y la Red Síncrona Óptica (SONET) Synchronous Optical Network son un estándar desarrollado por Bell Communications Research para redes de muy alta velocidad sobre cables de fibra óptica. La especificación SONET más lenta, OC-1 funciona a 52 Mbps, más o menos la velocidad de T3. OC SONET es una tecnología importante porque representa el conducto de la infraestructura de mayor velocidad que necesita Internet para seguir creciendo.

Las redes troncales Gigabit Ethernet es una tecnología reciente de ATM, muchos administradores de red están comenzando a utilizarla en lugar de ATM para cubrir las necesidades de red troncal. La figura 2.16 muestra cómo una red troncal Gigabit Ethernet se puede configurar usando la misma plataforma Catalyst de ATM. Esto se logra configurando tarjetas Gigabit Ethernet en lugar de tarjetas ATM. Se garantiza también que es posible usar el mismo cable de fibra óptica para Gigabit Ethernet, pero hay que cambiar los adaptadores a los diseñados para soportar Gigabit Ethernet en lugar de ATM.

Como cabría imaginar, existen adaptadores y tarjetas específicas que cubren las distintas necesidades electrónicas para procesar tanto Ethernet de longitud variable como celdas ATM de longitud fija.

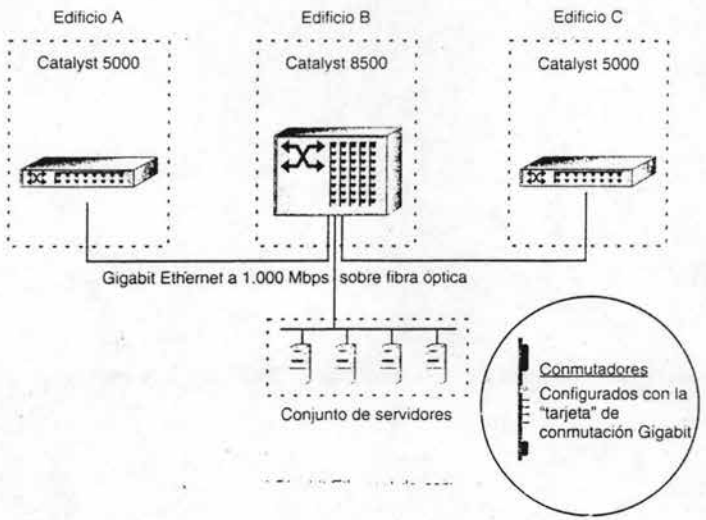


Fig. 2.16 Una red troncal Gigabit Ethernet de campo.

Conectar sitios remotos

Hay dos tipos de ubicaciones remotas: la Sucursal y la Oficina Pequeña SOHO (Small Office/Home Office), la diferencia fundamental entre ambas es el tipo de conexión, los emplazamientos SOHO usan acceso telefónico a redes, mientras que las sucursales utilizan algunas formas de circuitos dedicados. Se pueden utilizar básicamente tres tecnologías de conexión remota.

Frame Relay es ideal para tráfico WAN a ráfagas, en otras palabras, las líneas dedicadas de alquiler como T1 o T3 sólo tienen justificación económica si se usan continuamente. Frame Relay resuelve este problema porque es una Red de Datos de Paquetes Conmutados (PSDN) Packet-Swichted Data Network en donde las conexiones punto a punto son virtuales. Tan sólo hay que comprar un circuito telefónico local entre nuestro sitio remoto y un nodo Frame Relay. Después, los paquetes se mezclan con otros cientos de paquetes de distintas organizaciones.

Normalmente, hace falta un dispositivo llamado FRAD para entenderse con una red Frame Relay. El Ensamblador / Desamblador de Frame Relay (FRAD) traduce el flujo de datos al formato de paquetes propio de Frame Relay. Pero un simple FRAD sólo le conecta, ofreciendo poca administración, seguridad y QoS. Cisco ha incorporado funciones de Frame Relay en muchos de sus enrutadores para conseguir más velocidad de respuesta en las conexiones Frame Relay. La figura 2.17 muestra una configuración típica de Frame Relay usando material de Cisco.

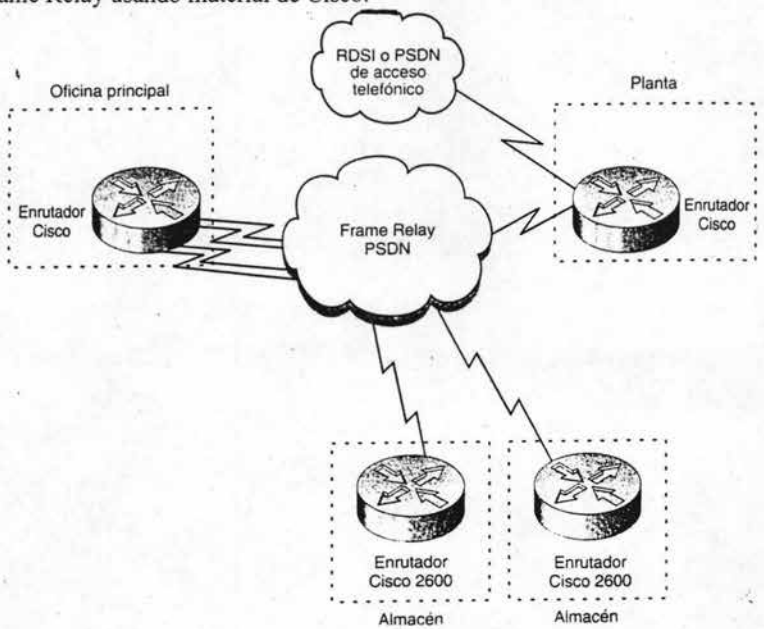


Fig. 2.17 Los enrutadores que soportan Frame Relay.

Como Frame Relay utiliza conexiones normales de líneas series, no hay que instalar interfases especiales en un enrutador para que sea compatible con Frame Relay. El enrutador Cisco 2600 es una solución económica para los almacenes del ejemplo de la figura 2.18 que ofrece un buen rendimiento para manejar el tráfico que estos sitios remotos tienden a generar.

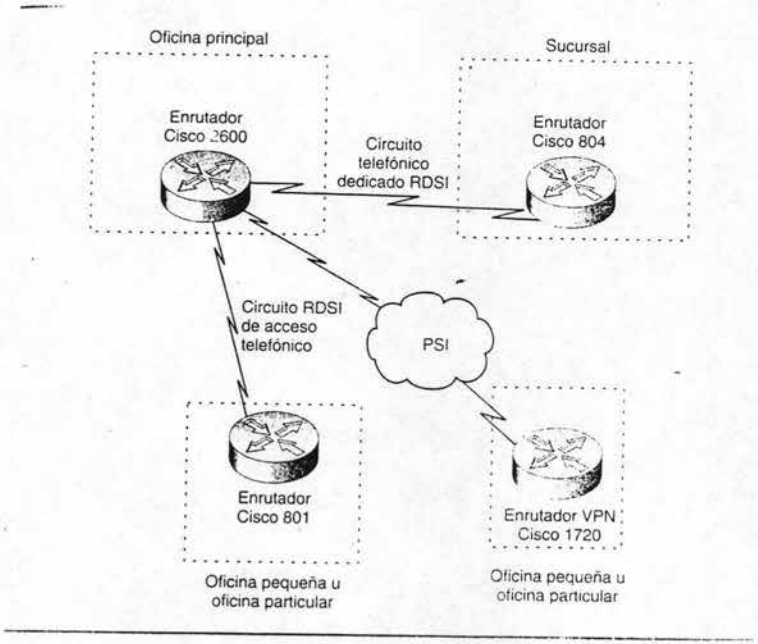


Fig. 2.18 RDSI acepta conexiones de acceso telefónico y circuitos.

La red de servicios integrados (RDSI) puede usar para conexiones telefónicas o para conexiones remotas dedicadas, ofrece mucho más ancho de banda que las habituales conexiones telefónicas analógicas por módem, pero debe estar disponible desde un proveedor local hasta su oficina. La RDSI tiene opciones de canales llamados BRI y PRI. BRI dispone a su vez de dos canales llamados B para ofrecer un ancho de banda de 128 Kbps y se usan normalmente para conexiones telefónicas desde casa o pequeñas oficinas. El PRI ofrece 23 canales B, para conseguir un ancho de banda de 1.48 Mbps y se usa normalmente para conexiones multiusuario a tiempo completo.

La anterior figura 2.18 muestra una configuración RSDI tipica de Cisco. La serie de enrutadores Cisco 800 está preparada para conectar usuarios RDSI. El 804 tiene cuatro puertos y el 801 tiene un puerto. Sin embargo, si se necesita una conexión VPN, es necesario incluir en la configuración el enrutador de acceso 1720 de Cisco. Es más caro pero incorpora la electrónica y el software que hace falta para manejar el cifrado que requieren las interconexiones.

Las líneas de abonado digital (DSL) compiten con RDSI en el sector de la pequeña oficina particular. Para poder usar DSL, debe estar conectado a una centralita telefónica local que admiten DSL y estar a una distancia determinada de la misma, normalmente unos pocos kilómetros. DSL se caracteriza por una transferencia de datos asimétricos, ya que el flujo de datos que produce de la telefónica es mayor de lo que puede enviar el usuario. Esto significa que DSL debe utilizarse teniendo en cuenta está limitación. En otras palabras, cuando el usuario descarga mucho y envía poco. Este caso de la mayoría de usuarios de Internet y DSL se ha hecho muy popular cuando la ofrecieron las compañías telefónicas. La configuración de la figura 2.19 muestra un enrutador de Cisco Speedrunner que es de líneas asimétricas de abanado digital (ADSL) este se parece a un radar detector, pero tiene una interfaz Ethernet en la parte trasera para conectar usuarios locales.

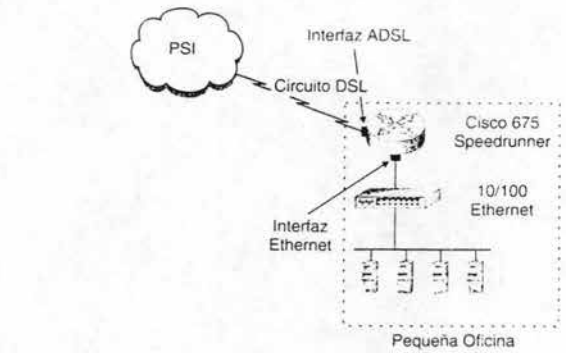


Fig. 2.19 Enrutador Cisco 675 Speedrunner diseñado para conexiones DSL.

TEMA 3 El enrutador Cisco

3.1 Introducción

Un despliegue meramente de hardware, software, medios de telecomunicación y pericia técnica, forma todos los sistemas de interconexión de redes, los cuales pueden ser: Conmutadores, concentradores, contrafuegos, paquetes, pasarelas, puertos, servidores de acceso, interfaces, capas, protocolos, líneas en serie, servicios integrados, tramas, topologías, enrutadores, etc.; la lista puede parecer infinita. De todos ellos en este tema sé describirá el enrutador.

En términos básicos, interconexión de redes no es nada más que enlazar máquinas personales a través de un laberinto de líneas de telecomunicaciones intermediarias y de dispositivos de computación. Esto nos conduce al enrutamiento, que en esencia sólo tiene dos misiones fundamentales: Determinar una trayectoria a lo largo de la que se puede realizar un enlace y transmitir paquetes a lo largo de dicha trayectoria. Debido a estas dos funciones, que ocurren dentro del enrutador, la interconexión de redes se convierte en algo fácil de entender. Esto se debe a que el enrutador, por el sí mismo debe reducir toda la complejidad a un nivel con el que se pueda manejar. El enrutador hace esto trabajando con, un paquete protocolo de Internet (IP) Internet Protocol.

Visto de esta forma, el enrutador es la estructura básica de las redes. De hecho, sin el enrutador, Internet, tal y como lo conocemos, no podría siquiera existir. Esto se debe a sus capacidades únicas, que son:

- Los enrutadores pueden soportar simultáneamente diferentes protocolos como Ethernet, Token Ring, y otros, haciendo de forma efectiva y virtualmente compatibles a todos los equipos en la capa de la red.

- Los enrutadores conectan a la perfección redes locales LAN, a redes de áreas extensas WAN; lo que hace posible la creación de redes a gran escala con una mínima planificación centralizada.

- Los enrutadores filtran al exterior el tráfico no deseado, aislando áreas en las que los mensajes pueden difundir a todos los usuarios de una red.

- Actúan como puertas de seguridad comprobando el tráfico mediante listas de permisos de accesos.

- Los enrutadores aseguran fiabilidad, ofreciendo múltiples trayectorias a través de las redes.

- Dándoles nuevas trayectorias, seleccionan las mejores, eliminan restricciones artificiales para expandir y mejorar las redes.

En otras palabras, los enrutadores hacen posible la existencia de redes. Lo consiguen ofreciendo un entorno unificado y seguro en el que pueden conectarse grandes grupos de personas. Pero existen obstáculos a la hora de enlazar a los usuarios en redes, ya sea en una Intranet corporativa, en una red privada virtual, o en la propia Internet. La siguiente figura 3.1 describe cómo la tecnología de enrutamiento es la clave para superar estos obstáculos, es decir comunicar a diferentes protocolos.

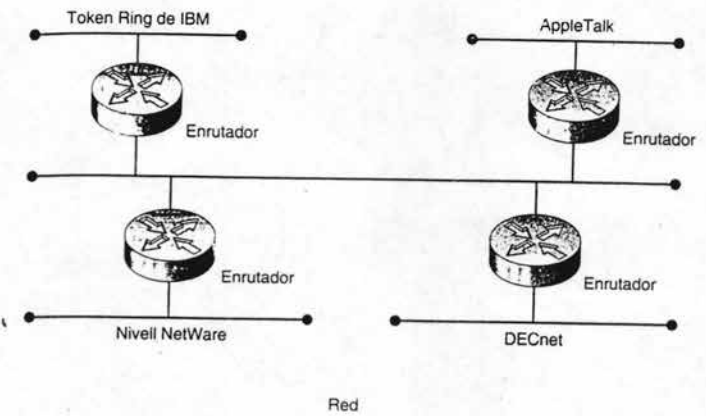


Fig 3.1 Los enrutadores posibilitan la existencia de redes.

La capacidad de los enrutadores para soportar de forma simultánea diferentes protocolos es quizá su característica más importante, ya que esta posibilidad permite a los equipos, ser compatibles con otras marcar y además les permite hablar uno con otro sin que afecte al sistema operativo, el formato de los datos o el medio de comunicación que se utilice. En los últimos años mediante TCP/IP se ha creado una plataforma común mediante la que todos los equipos y las arquitecturas de red pueden intercambiar información libremente.

También es importante para las redes la capacidad de un enrutador de eliminar el tráfico no deseado. Si se bombardea a los usuarios con un gran volumen de mensajes no deseados, o si sienten que es posible acceder fácilmente a sus sistemas, se resistirán a la hora de conectarse a las redes. El filtrado del tráfico y el control de acceso que proporcionan los enrutadores ofrece a los usuarios suficiente privacidad y confidencialidad como para que se anime a conectarse a las redes.

3.2 Comunicación con el Enrutador

La mayoría de las redes no se comunican con enrutadores, se comunican a través de ellos. Los administradores de red, sin embargo, deben manejar directamente enrutadores independientes para instalarlos y administrarlos. Los enrutadores son computadoras construidas a propósito y dedicadas al procesamiento de la interconexión de redes. Son dispositivos importantes que sirven de forma independiente a cientos de miles de usuarios, algunos sirven incluso a más usuarios. Cuando un enrutador falla los usuarios protestan y los administradores de la red tienen que ser capaces de resolver el o los problemas lo más rápido posible.

Los enrutadores no incluyen monitor, ni teclado, ni ratón, por lo que el administrador debe comunicarse con ellos de una de las siguientes formas:

- Desde una terminal que esté en la misma ubicación que el enrutador y esté conectado a él mediante un cable, el medio suele ser una PC o una estación de trabajo funcionando en modo de terminal.

- Mediante la red en la que está situado el enrutador.

En las grandes redes, los administradores de red están físicamente apartados de los enrutadores y deben accesar a ellos mediante una red. Sin embargo, si el enrutador es inaccesible debido a un problema de red, o si hay un problema con el propio enrutador, alguien debe ir a su ubicación e iniciar una sesión directamente en el enrutador. Las tres formas de conseguir acceso administrativo a los enrutadores se describe en la figura 3.2.
Y estos son: directo, puerto auxiliar, y mediante la interfaz de la red.

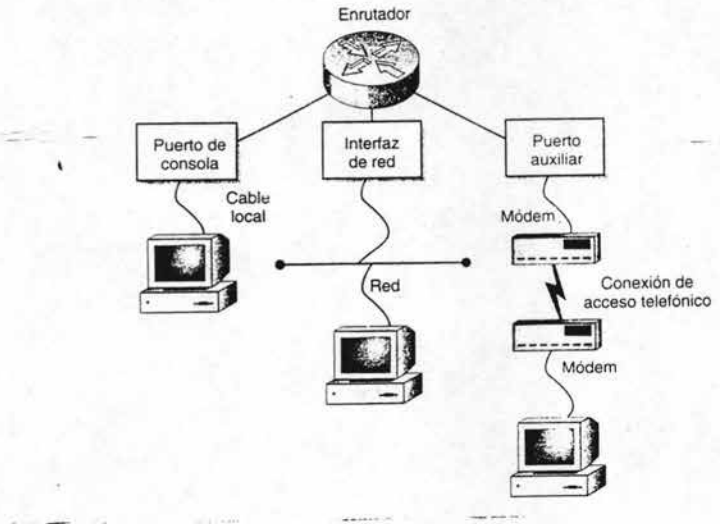


Fig. 3.2 Acceso administrativo a los enrutadores.

Incluso cuando los administradores de red están situados en el propio edificio, todavía prefieren accesar a ellos mediante la red. No tiene sentido tener una terminal conectada a una terminal conectado a cada enrutador, especialmente cuando hay docenas de ellos es muchos más conveniente administrarlos a todos ellos desde una simple PC o estación de trabajo.

Hay varias formas de comunicarse con un enrutador, cada una de las cuales se realiza mediante un protocolo de comunicaciones particular, la tabla 3.1 lista cada uno de los métodos de acceso, protocolo y como se conecta cada uno de ellos.

Método de acceso	Protocolo	Método de conexión
Puerto de consola	EITA/TIA-232	Conexión de línea serie desde un terminal local
Puerto auxiliar	EITA/TIA-232	Conexión terminal de línea serie mediante módem
Telnet	Telnet	Conexión virtual mediante una red TCP/IP
Servidor http	http	Conexión de explorador Web mediante una red TCP/IP
SNMP	SNMP	Protocolo de administración de correo sencillo, conexión terminal virtual a través de una red TCP/IP

Tabla 3.1 Métodos de acceso.

A continuación se hace una breve descripción de cada uno de ellos:

El método de consola

Todos los enrutadores de Cisco tiene un puerto de consola en la parte posterior. Está ahí para ofrecer una forma de conectar un terminal al enrutador y poder trabajar sobre él. El puerto de consola es a veces conocido con el nombre de puerto de administración, porque lo utilizan los administradores para iniciar directamente la sesión en un enrutador, es decir, sin una conexión de red. La consola se debe utilizar para instalar enrutadores en las redes porque, por supuesto, en dicho momento no hay una conexión de red en la que se puede trabajar.

Pero sobre todo, el papel del puerto de consola es estar allí como eventualidad en caso de emergencia. Cuando un enrutador está completamente caído, en otras palabras, cuando ya no está disponible para procesar paquetes de red, no se puede acceder a él mediante la red, o si el enrutador está funcionando y procesando paquetes, pero el segmento de red, por el cual los técnicos deben accesar se ha caído, no es posible utilizar la red para corregir el enrutador. Aquí es donde el puerto de consola ofrece una forma segura de iniciar la sesión en el enrutador para seguir trabajando. Las desventajas, por su puesto, son que alguien debe estar en la misma ubicación física que el enrutador para conectarse a él.

Se puede utilizar como consola un CRT independiente, una PC o una estación de trabajo. Las terminales de la consola deben ejecutar una interfaz de usuarios en modo carácter. No pueden ejecutar una interfaz de usuarios gráficos como GUI, como Microsoft Windows, Mac OS o X Windows. Para poder utilizar un PC o una estación de trabajo como consola, debe usar software de emulador de terminal. Por ejemplo, uno de los emuladores de terminal más conocido es HyperTerminal de Hilgraeve Inc, que incluye todas las versiones de Windows.

Los puertos de consola de los enrutadores de Cisco usan distintos tipos de conectores, Db de 25 pines, RJ-45 ó 9 pines, pero todos ofrecen una conexión sencilla de terminal. Además debe asegurarse de que tiene el cable adecuado antes de probar a conectar una terminal de la consola para trabajar sobre un enrutador.

El puerto auxiliar

La mayoría de los enrutadores de Cisco tienen un puerto secundario en la parte posterior llamados puertos auxiliares, normalmente llamado puerto AUX, de forma abreviada, al igual que el puerto de la consola el puerto AUX posibilita una conexión directa, no de red al enrutador.

En que se diferencia el puerto auxiliar del puerto de consola El puerto AUX usa un tipo de conector al que puede conectarse los módem's, los puertos de consola tienen conectores diseñados para cables de terminal. Si un enrutador situado en un armario de datos lejanos se viene abajo, el administrador de red pregunta a alguien del área que vaya al enrutador y le conecte el módem para poder operar sobre él de forma remota. En configuración más críticas, un módem se suele dejar conectado de forma permanente a un puerto AUX del enrutador. En cualquier caso, el puerto AUX permite el acceso como consola cuando no es práctico enviar un técnico al sitio para trabajar sobre un enrutador a través de una consola local.

Telnet

Una vez instalado el enrutador en una red, casi siempre sé accesa a él mediante sesiones Telnet, no mediante los puertos de consola o AUX. Telnet es una forma de iniciar una sesión en un enrutador como terminal virtual. Las conexiones Telnet se realizan, por el contrario, a través de la red. En términos más básicos, una sesión real en una terminal virtual se compone de paquetes IP que sé enrutan sobre una red, fingiendo ser un flujo de bits sobre una línea serie.

Telnet es una aplicación de red, no un emulador de terminal, como una forma de iniciar sesiones en computadoras remotas para administrarlas, las redes incorporaron Telnet directamente en el protocolo de red TCP/IP como una forma de accesar y administrar dispositivos de redes. Telnet está incluido con cada copia del software IOS de Cisco y la mayoría de los sistemas operativos de computadoras.

Cuando se usa Telnet para accesar a un enrutador, se hace sobre líneas virtuales que ofrece el software IOS de Cisco, estas líneas reciben el nombre de líneas VTY, significa una sesión de terminal virtual dentro del software IOS. IOS soporta hasta cinco líneas de terminal virtual, lo que hace posible tener hasta cinco sesiones de terminal virtual ejecutándose a la vez en un enrutador. Sin embargo, puede que esto sea una exageración. Es raro tener más de una sesión de terminal virtual ejecutándose en un enrutador al mismo tiempo.

El software IOS de Cisco se usa principalmente en el modo de interfaz basado en caracteres, lo que quiere decir que no es un entorno GUI del tipo apuntar y hacer clic Macs de Apple o estación de trabajo UNÍX de X-Windows. Independientemente de quien inicie la sesión en un enrutador mediante el puerto de consola, el puerto AUX o con Telnet, se le direcciona a la interfaz de software IOS basada en caracteres, estos caracteres representan:

- El puerto de consola, al que se accesa mediante una conexión de cable local
- El puerto AUX, al que se accesa mediante una conexión de módem.
- Cinco líneas VTY, a las que se accesa mediante conexiones de red TCP/IP.

Servidor Http

Un método más reciente de acceso al enrutador es el servidor http. Se refiere a una pequeña aplicación software que se ejecuta dentro del software IOS de Cisco. El servidor http estuvo disponible por primera vez con la versión 10.3 del IOS. El servidor http hace posible interactuar con el enrutador a través de un explorador Web.

Usar http para manejar la entrada y salida de la línea de comandos de IOS no es realmente cómoda. La mayoría de los administradores de red todavía prefieren usar el software de IOS en modo basado en caracteres porque es más rápido y más directo.

Pero Cisco puede desplazar gradualmente el IOS hacia una interfaz gráfica de usuario por dos razones. La razón más obvia para ofrecer al menos una alternativa basada en GUI para trabajar con Cisco es que los dispositivos Cisco cada vez los utilizan los expertos.

La otra razón es que conforme crece la complejidad, también crece la necesidad de visualizar el sistema, incluso dentro de un enrutador sencillo.

Usar herramientas de visualización para mostrar condiciones de carga, errores aislados, etc., requerirá, por su puesto, un explorador en vez de la clásica interfaz de pantalla verde de línea de comandos basada en caracteres.

3.3 Contraseñas

Los enrutadores no son muy visibles en las redes, principalmente, porque no tienen Localizador Uniforme de Recursos URL (Uniform Resuorce Locators). Los enrutadores no necesitan tener direcciones descriptivas, ya que los usuarios normales de las redes nunca necesitan saber si un enrutador está allí; simplemente necesitan la conectividad que éste les proporciona.

Las únicas personas que necesitan indicar una sesión directamente en un enrutador son los miembros responsables del equipo de red responsables de su mantenimiento. En las redes TCP/IP, el protocolo sobre el que funciona la mayoría de las redes, los enrutadores se identifican a sí mismo a las redes sólo con sus direcciones IP. Por esta razón, para iniciar una sesión en un enrutador, primero debe conocer que existe y qué dirección IP tiene. Los administradores de red responsables del enrutador, por supuesto conocerán esta información.

No obstante, todavía existe el peligro potencial de abuso por parte de las personas no deseadas, los enrutadores se envían constantemente mensajes entre sí para actualizar y administrar las redes en las que operan. Con las capacidades adecuadas y suficiente determinación, un intruso puede descubrir una dirección IP de un enrutador e intentar luego establecer una conexión Telnet con él. Como los enrutadores son los enlaces que mantienen unidas las redes, es fácil de comprender por qué Cisco y otros fabricantes de equipos de redes diseñan muchas medidas de seguridad dentro de sus productos.

La única intención de las contraseñas del enrutador es evitar el acceso de los intrusos. La protección por contraseña se administra dependiendo del enrutador en particular. En la mayoría de los casos, las contraseñas para accesar a un enrutador se almacenan dentro del propio enrutador. Las grandes redes tienen docenas o incluso cientos de enrutadores, algunos más importantes que otros para operaciones de red, por lo que es una práctica común de los administradores de red permitir sólo a los miembros del equipo de red acceder a ciertos enrutadores, o incluso, a niveles de comandos dentro de los enrutadores.

La tabla 3.2 lista las contraseñas de enrutador y lo que permiten.

En los enrutadores de Cisco se utilizan las contraseñas para restringir el acceso a:

- El propio dispositivo de enrutador.
- La parte EXEC privilegiada del entorno del software IOS.
- El uso de comandos específicos del IOS.

Puerto de control	Tipo de contraseña	Qué está restringido
Puerto de consola	Línea	Iniciar una sesión mediante una línea local a través del puerto de consola
Puerto AUX	Línea	Iniciar una sesión mediante una línea módem o local conectada al puerto auxiliar
Inicio de sesión de red	Terminal virtual	Iniciar la sesión en el enrutador mediante una conexión de red usando Telnet sobre una línea VTY
EXEC privilegiado	Permitido y permitida secreta	Entra al nivel más potente privilegiado EXEC del entorno IOS

Tabla 3.2 Información básica de las contraseñas de enrutador y sus usos.

Contraseñas de línea

Estas contraseñas se usan para controlar quién puede iniciar la sesión en un enrutador. Se usa para definir protección por contraseña en la línea terminal de la consola, la línea AUX y en cualquiera de las cinco líneas (VTY) de terminal virtual.

Es necesario establecer al menos una contraseña para las líneas VYT del enrutador. Si no se define una contraseña de línea cuando intente iniciar la sesión en el enrutador mediante Telnet, aparecerá un mensaje de error password required but none set. Recuerde, cualquiera Internet puede hacer un Telnet a cualquier enrutador, porque definir las contraseñas de línea detendrá a los hackers, excepto a los mejores, de conseguir una forma de introducirse, por debajo, ISO solicita una contraseña, por ejemplo:

```
User Access Verification
Password :

Enrutador>
```

Cuando introduce contraseñas en el IOS, no aparecen asteriscos para enmascarar las letras escritas, algo a lo que la mayoría de nosotros acostumbrados. En el ejemplo anterior, en la línea de comandos Enrutador>, el nombre del Host del enrutador en este ejemplo, se ha introducido la contraseña correcta, se inició la sesión en el enrutador del equipo, pero los asteriscos no aparecen a la derecha de la línea de comandos Password. Esto le puede sorprender en un principio, pero se acostumbrará a ello.

Contraseña permitida y permitida secreta

Una vez que accesa la contraseña de línea, inicia la sesión en el entorno del software IOS del enrutador. El IOS se divide en dos niveles de privilegio, EXEC y Privilegio EXEC.

El nivel EXEC contiene sólo comandos básicos, no destructivos. Estar en modo habilitar permite accesar a más comandos. Los comandos del nivel EXEC, básicamente permiten ver un enrutador. Los comandos del modo habilitar son más potentes en el sentido de que permite volver a configurar el enrutador. Estos comandos son potencialmente destructivos, el comando Erase es un buen ejemplo.

Se puede usar dos tipos de contraseñas para restringir el acceso al Privilegio EXEC, la contraseña Enable y la contraseña Enable Secret. La idea de una contraseña secreta parece una tontería al principio. Por supuesto todas las contraseñas o al menos lo deberían ser. A lo que se refieren los ingenieros de Cisco aquí es al nivel de cifrado que se utiliza para enmascarar la contraseña a usuarios no autorizados.

El nivel privilegio también usa las dos contraseñas. La diferencia entre las dos está en el nivel de cifrado que soportan. El cifrado es una técnica que se utiliza para codificar los datos, haciéndolos incomprensibles a aquellos que no tienen una clave para leerlos. Las contraseñas Enable Secret son inversas y utilizan un complejo algoritmo de cifrado basado en 128 bits para el que no hay técnica conocida de decodificación. El cifrado para la contraseña Enable se basa en un algoritmo menos potente. Cisco recomienda encarecidamente que use la contraseña Enable Secret en lugar de la contraseña Enable.

La contraseña Enable se introdujo en 1997, por lo que todavía se sigue utilizando mucho hardware y software que sólo soporta la contraseña Enable, y los servicios que guardan imágenes de copias de seguridad de IOS suele dar servicio tanto a enrutadores nuevos como antiguos. Cuando se establece los dos la contraseña Enable Secret siempre precede a la contraseña Enable. IOS sólo utilizará contraseña Enable cuando se ejecute una versión antigua del software IOS.

Las contraseñas IOS se almacenan en el archivo de configuración del enrutador. Los archivos de configuración viajan a través de las redes de forma rutinaria cuando se actualizan los enrutadores o se hacen una copia de seguridad. Tener una contraseña Enable significa que un desconocido que use un analizador de protocolos que es un dispositivo de pruebas que puede leer paquetes, tendrá muchos más en decodificar su contraseña. El siguiente ejemplo de archivo de configuración muestra esto:

```
Version 11.2
Service  password-encryption
Service  udp-small-servers
Service  tcp-small-servers
!
enrouter host name
!
enable secret 5 $1$C / q2$ZhtujqzQIuJrRGqFWdwn71
enable password 7 0012000F
```

Tenga en cuenta que la máscara de cifrado de la contraseña Enable en la última línea es mucho más corta que la máscara de cifrado de la contraseña Enable Secret.

Contraseña de encriptación con clave de acceso

Ciertos tipos de contraseñas, como las contraseñas de línea, aparecen por defecto en textos legibles en el archivo configuración. Se puede usar la contraseña de encriptación con clave de acceso para hacerlas más seguras. Una vez que se introduce esta contraseña, cualquier contraseña que se haya definido se cifra automáticamente, por lo que se escribe de forma no muy legible dentro del archivo de configuración, casi igual que las contraseñas disponible y disponible secreta.

La seguridad mediante contraseñas de línea es doblemente importante en las redes en las que se usan servidores TFTP, ya que la copia de seguridad de TFTP implica el movimiento rutinario de archivos de configuración entre redes, y los archivos de configuración, por supuesto contienen las contraseñas de línea.

3.4 Hardware del enrutador

A primera vista, los enrutadores se parecen mucho a una PC, ya que tiene un CPU, memorias y en la parte externa a los puertos e interfaces para conectar periféricos y diferentes medios de comunicación. A veces, incluso tiene un monitor que sirve como consola del sistema.

Pero hay una diferencia con las PC: Los Enrutadores no tienen disco duro, incluso no tienen disco flexible. Si lo piensa tiene sentido ya que un enrutador existe para hacer simplemente eso: Enrutar. No existe para crear, mostrar o almacenar información, auque incluso sea importante. Los enrutadores tienen como única misión la tarea de filtrar los paquetes entrantes y enrutarlos a los destinos correctos.

Otra diferencia está en la clase de módulos complementarios que puede conectar a los enrutadores. Mientras que en la PC típico contiene tarjetas de vídeo, sonido, gráficos u otro propósito, los módulos que se ponen en los enrutadores se utilizan estrictamente para interconexión de redes. Estos módulos se llaman de interfaz, o solamente interfaces. Cuando las personas o los documentos se refieren a una interfaz de enrutador, quieren decir una placa de circuito impreso real, física, que maneja un protocolo particular de redes. E0 y E1, por ejemplo, probablemente significa interfaz Ethernet número 1 y 2 dentro de un enrutador. Los módulos de interfaz son siempre específicos del protocolo del nivel 2. Hay un protocolo por interfaz.

Las interfases se agregan de acuerdo al entorno de red en el que vayan a operar. Por ejemplo, un enrutador puede estar configurando con un módulo de interfaz sólo para Ethernet. Un enrutador que funcione en un entorno de LAN mixta, por el contrario, tendría interfaces tanto para los protocolos Ethernet como para los protocolos Token Ring. Y si el enrutador estuviese actuando como una unión LAN a WAN, también tendría un módulo RDSI.

Hay una última diferencia entre los enrutadores y las computadoras de propósito general, una más sutil: Las líneas de productos de las computadoras se basan casi siempre en una arquitectura de procesador central común CPU, por ejemplo, las PC de Wintel sobre la arquitectura del Intel x 86, las variantes del Motorola 68000 de Apple, el APARC de Sun, etc.

Por el contrario, los enrutadores Cisco usan varios CPU's, cada una de ellas elegidas para que funcione mejor en la misión en la que está destinada. Los enrutadores de la serie 700 de Cisco, por ejemplo, utilizan un CPU 80386 a 25 MHz, Cisco tomó esta elección debido a que la serie 700 está diseñada para el uso de oficinas o en oficinas instaladas en el hogar, donde la carga de actividad suele ser ligera. El CPU 80386 de Intel es fiable, capaz de manejar el trabajo y quizá lo más importante, barato. A continuación se hará una breve descripción de los componentes hardware del enrutador:

3.4.1 Memorias

Los enrutadores usan varias clases de memoria para operar y administrar de forma autónoma. Todas las placas principales de los enrutadores Cisco usan cuatro tipos de memoria, cada una se encarga de una tarea específica.

Todo enrutador Cisco incluye, como mínimo y de forma predeterminada, memoria DRAM y memoria flash de fábrica. Es posible agregar memoria en la fábrica o actualizarse posteriormente. Como regla general, la cantidad de memoria DRAM se puede doblar o cuadriplicar, y la cantidad de memoria flash se puede doblar. Si las cargas de tráfico se incrementa con el tiempo, se puede actualizar la DRAM para incremento del enrutador.

A) RAM / DRAM. Es la memoria de acceso aleatorio / memoria de acceso aleatorio dinámica, también conocida con el nombre de almacenamiento de trabajo, la Ram / Dram la utiliza el procesador central del enrutador para hacer su trabajo, al igual que la memoria de una PC. Cuando un enrutador está funcionando, su RAM/DRAM contiene una imagen del software IOS de Cisco, el archivo de configuración en ejecución, la tabla de enrutamiento, otras tablas y el búfer de paquetes.

B) NVRAM. Es la Ram no volátil, esto significa que la memoria conservará la información después de cortar el suministro de corriente. Los enrutadores Cisco almacenan una copia del archivo de configuración del enrutador en NVRAM. Cuando el enrutador se apaga de forma intencionada, o si hay un corte de suministro eléctrico, la NVRAM permite al enrutador iniciarse con la configuración correcta.

C) Memoria flash. También es no volátil, difiere de la NVRAM en que se puede borrar y volver a programar cuando sea necesario. Originalmente desarrollada por Intel, la memoria flash se utiliza mucho en computadoras y otros dispositivos. En los enrutadores Cisco, la memoria flash se usa para almacenar una o más copias del software IOS. Esta es una característica importante, pues permite a los administradores de red copiar nuevas versiones del IOS en los enrutadores mediante una red y actualizarlos posteriormente todos a la vez con nuevas versiones desde la memoria flash.

D) ROM. También es no volátil. Los enrutadores Cisco usan la ROM para albergar un programa con instrucciones iniciales, que es un archivo que se puede utilizar para iniciar la operación con un estado mínimo de configuración después de la instalación o de un desastre. También se suele conocer a la ROM con el nombre de ROMMON, porque cuando inicia desde ROM, lo primero cosa que verá será el símbolo del sistema rommon>. ROMMON, que significa que es monitor de ROM tiene su origen en el sistema UNIX, que se basa en un ROMMON para reiniciar una computadora en el punto donde, se pudiera escribir los comandos en el monitor de la consola del sistema. En los pequeños enrutadores de Cisco, la ROM contiene un subconjunto de comandos del software IOS de Cisco. La ROM en algunos enrutadores Cisco de la gama alta, dispone de una copia completa de IOS.

3.4.2 Módulos y puertos del enrutador

Una de las ventanas del enrutador hacia la red es a través de sus puertos y módulos. Sin ellos, un enrutador sería un simple chasis. Los puertos y los módulos que se colocan en un enrutador define lo que éste puede hacer.

La interconexión de redes puede ser algo difícil, con una combinación de productos y protocolo, medios, conjuntos de características, estándares, etc., aparentemente sin fin. Los acrónimos aparecen de forma tan rápida y son tan difíciles de recordar que puede ser desesperante aprender cómo configurar correctamente un enrutador. Pero si se elige el producto correcto de enrutador, se reducirá este problema a proporciones manejables. La tabla 3.3 muestra las cinco áreas principales de requisitos que, si se verifican, le guiarán a elegir la mejor solución de enrutador.

Es evidente que Cisco no puede fabricar un modelo de enrutador que encaje en los requisitos específicos de cada cliente. Para hacerlos más flexibles de configurar, los enrutadores se dividen en dos partes principales:

- El chasis. La caja donde se coloca y los componentes básicos dentro de la misma, como la fuente de corriente, los ventiladores, los paneles interiores y posteriores, luces indicadoras y las ranuras.

- Puertos y módulos. Las placas de circuito impreso que se introducen en la caja del enrutador.

La estructura de la línea de productos de los enrutadores de Cisco intenta dirigirle hacia un producto, o al menos una razonable selección centralizada de productos que cumplan todas y cada una de las cinco áreas de requisitos de la tabla 3.3.

Áreas	Requisito de configuración
1 Física	Debe ser compatible a nivel de hardware con el segmento de red físico en el que se colocará el enrutador.
2 Comunicación	El enrutador debe ser compatible con el medio de transporte que se usará como puede ser Frame Relay, ATM, etc.
3 Protocolo	Debe ser compatible con los productos que se utilicen en las redes como, IP, IPX, etc.
4 Misión	El enrutador debe ofrecer la velocidad, fiabilidad, seguridad y características funcionales que requiere el trabajo.
5 Negocio	Debe encajar dentro del presupuesto de compras y de planes de crecimiento de la red.

Tabla 3.3 Requisitos de configuración.

Encontrar el enrutador correcto para sus necesidades es básicamente un proceso de tres pasos. A continuación se ilustra el proceso para seleccionar un enrutador destinado a un área específica de la oficina:

Paso uno, los enrutadores de Cisco se agrupan en familias de productos llamadas series. Elegir una serie de producto de enrutador suele ser cuestión de presupuesto, ya que cada serie refleja un escalón de precio/rendimiento. Los modelos que pertenecen a las series suelen basarse en el mismo chasis, que es el marco de metal y los componentes básicos como fuentes de alimentación, ventiladores, etc. La selección de la serie Cisco 2000, encaja tanto en el presupuesto de compra como en los requisitos de rendimiento para la oficina, ya que reúne las características siguientes: LAN única, enrutador / concentrador, servicios de acceso, línea en serie y LAN dual.

Paso dos. El chasis 2500 es suficientemente versátil para utilizarlo en diversas de situaciones, convirtiéndolo en la gama más popular de enrutadores de grandes oficinas, ya que su característica es para una LAN dual con la configuración siguiente:

Cisco 2513 un puerto de Ethernet y un
Puerto Token Ring.

Cisco 2514 de dos puertos Ethernet.

Cisco 2515 de dos puertos Token Ring.

Paso tres. Selección del Cisco 2514 debido a que tiene dos puertos Ethernet; y tal vez las posibles oficinas ramificadas dispondrán de dos subredes, una para la oficina de servicios al cliente y otra para la oficina de propiamente dicha. Los dos puertos Ethernet permiten separar los departamentos, aislando de esta forma el tráfico.

Categorías de los módulos

Es posible configurar en los enrutadores de Cisco tres categorías principales de módulos, que acepten tanto conectividad LAN como WAN:

- Módulos Ethernet. Para soportar cualquiera de las variantes LAN Ethernet del mercado, incluyendo Novell NetWare, Banyan VINES y AppleTalk.

- Módulos Token Ring. Tecnología LAN de IBM, establecida normalmente en bancos, compañías de seguros y otros entornos corporativos del Furtune 1000.

- Módulos de conectividad WAN. Para soportar una amplia variedad de protocolos WAN, algunos antiguos y otros nuevos. Por ejemplo de tecnologías WAN incluye nuevos protocolos como RDSI, Frame Relay; Modo de transferencia asíncrona ATM y protocolos heredados, como SDLC y X.25.

Las opciones de configuración dependen principalmente de la gama del enrutador concreto de Cisco:

- Los enrutadores de gama baja tienden a tener " configuraciones fijas ", lo que significa que los módulos vienen integrados de fábrica preconfigurados.

- Los enrutadores de gama media, como el Cisco 4500, son "modulares", lo que significa que pueden aceptar distintos tipos de módulos, soportando a menudo diferentes protocolos en la misma caja. Los módulos de interfaz se conectan en esta clase de placas medre de enrutadores.

- Los enrutadores de gama alta, la serie de Cisco 7000 y la serie Cisco 12000, tienen buses, también llamados paneles posteriores, los enrutadores basados en bus aceptan módulos más grandes, normalmente conocidos con el nombre de hojas o tarjetas, que son, en realidad, enrutadores autocontenidos, tienen su propio CPU, unidad de memoria, etc.

3.5 Software del enrutador

Al contrario de las computadoras normales, los enrutadores de Cisco sólo tienen dos archivos principales:

- El archivo de configuración.
- El software IOS de Cisco, que es sistema operativo de redes.

El software IOS de Cisco contiene instrucciones para el enrutador. IOS actúa como el guardia de tráfico que dirige la actividad dentro del enrutador. IOS administra las operaciones internas del enrutador indicándole a los diferentes componentes hardware qué hacer, casi igual que Windows 95 o UNIX con una computadora de propósito general. Los clientes no pueden alterar el contenido del archivo IOS.
El archivo de configuración contiene instrucciones para el enrutador introducidas por el cliente, no por Cisco. Contiene información que describe el entorno de red ente. En una frase, el archivo de configuración indica qué hacer; el IOS le indica el enrutador cómo hacerlo.

Los enrutadores también usan archivos dinámicos, que no se almacenan en la memoria flash del enrutador, sino en NVRAM o en ROM. Por el contrario, los archivos dinámicos se construyen desde cero cuando se inicia un enrutador y son estrictamente reactivos, en el sentido de que sólo contiene información viva, no instrucciones de funcionamiento.

3.5.1 El sistema operativo de redes

Normalmente no pensamos en un sistema operativo como un archivo. Después de todo, el sistema operativo de cualquier PC está formado por miles de archivos, los cuales se sitúan en un directorio de archivos como SYS, EXE, DRV y DLL.

Pero en realidad, IOS está contenida en un único archivo. Cuando envía un archivo IOS a cualquier parte, éste contiene todo lo necesario para hacer funcionar un enrutador. Dependiendo de la versión, una imagen de software del IOS tendrá un tamaño de entre 3 MB hasta 10 MB de tamaño.

Es necesario crear IOS fuertemente unido, porque sus copias, a las que se les conoce con el nombre de imágenes del sistema, se envían de forma rutinaria a través de las redes. Las imágenes del sistema se cargan y descargan sobre enrutadores para copias de seguridad de los enrutadores, actualizan sus capacidades y reiniciarlo después del fallo. No sería práctico enviar miles de archivos de 50 MB. Poder enviar un único, pequeño y autocontenido archivo del IOS hace posible que la administración de la red sea más eficaz.

Conjunto de características del IOS

Los conjuntos de características del IOS son paquetes que intentan simplificar la configuración y la ordenación del software del IOS. En realidad, no hay un único producto de software IOS. Por lo que esté es realmente una plataforma de software común en la que se basa una familia de implementaciones del IOS, cada una de ellas destinadas a cumplir una misión específica. Cisco llama a esto conjuntos de características del paquete IOS, también llamado imágenes software o paquetes de características. Cuando pide un enrutador de Cisco, se elige un conjunto de características del IOS que contenga todas las capacidades que requiere su situación particular. Muchos de estos requisitos están relacionados con el mantenimiento de la compatibilidad con los diferentes dispositivos hardware y protocolos de red en el entorno en el que funcionará el enrutador.

Como se describe en la figura 3.3, las variantes de software IOS de Cisco se definen de dos formas: Mediante conjuntos de características y Mediante versión. Los conjuntos de características definen el trabajo que puede realizar una versión IOS; las versiones se utilizan para administrar el software IOS a lo largo del tiempo.

Los conjuntos de características de Cisco están diseñados para:

- Ser compatible con ciertas plataformas de enrutador.
- Permitir la interoperabilidad entre diferentes protocolos de red como Novell, NetWare, SNA de IBM, AppleTalk, etc.
- Ofrecer características funcionales en forma de servicios de red y aplicaciones para asunto como administración de red, seguridad y multimedia.

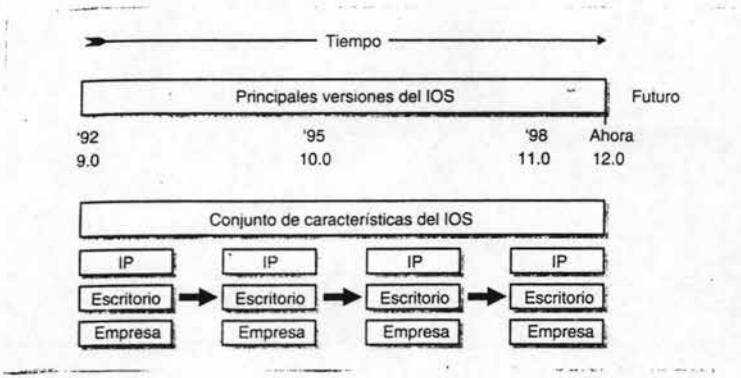


Fig. 3.3 IOS se organiza en versiones y conjuntos de características.

Empaquetar y vender el software IOS de esta forma simplifica las cosas para Cisco y para los clientes. Para el cliente, tener un solo número de parte para hacer los productos pedidos simplifica pensar que software comprar. Para Cisco, ayuda a los ingenieros de productos de la compañía a saber lo que ha sucedido y así el personal de soporte puede saber la causa del error. Recuerde, la interconexión de redes puede convertirse en algo extremadamente complejo debido a que la naturaleza del negocio es permitir que distintas plataformas de computadoras y protocolos de red funcionen conjuntamente y coexistan.

Cómo se crean los conjuntos de características

Como los conjuntos de características de IOS dependen del hardware del enrutador en el que se ejecutan, se aplican dos reglas muy básicas:

- No puede hacer funcionar todos los conjuntos de características en todas las plataformas de enrutador.
- Algunas veces, características específicas de un conjunto de características se ejecutarán o no, dependiendo de la plataforma del enrutador.

Todos los conjuntos de características, de una forma u otra, derivan su funcionalidad de alrededor de una docena de categorías que se listan en la tabla 3.4. Lo importante aquí es comprender que los miles de características y funciones del software IOS puede agruparse en una docena de categorías, más o menos.

Los conjuntos de características del IOS de Cisco intenta combinar características en grupos de forma que se ajusten lo más posible en le mundo real que los requisitos del cliente. Cisco ofrece docenas de conjuntos de características de productos finales en forma de números de productos de software del IOS que puede poner en un pedido de compra. Se agrupan por características generales en las cuatro familias generales de conjuntos de características mostradas en la tabla 3.5. Tenga en cuenta que las dos tablas de las plataformas de computadoras propietarias, como IBM, DEC y Apple, y plataformas propietarias de redes, como Novell y SNA, guían muchas de las necesidades para los conjuntos de características. Todos los enrutadores de Cisco deben cumplir los requisitos de compatibilidad del mundo real del cliente, lo que significa ser capaz de ejecutar con hardware y software heredado. Prácticamente todas las arquitecturas heredadas existen en los productos finales de red.

Esto significa que la mayoría de los equipos propietarios con los cuales los IP deben mantener la compatibilidad funcional sobre LAN o en computadoras situadas en computadoras heredadas propietaria o plataformas especializadas.

Categoría	Ejemplos de características
Soporte de LAN	IP, Novell IPX, AppleTalk, Banyan VINES, DECnet.
Servicios WAN	PPP, emulación LAN ATM, Frame Relay, RSDI, X.25.
Optimización WAN	Acceso telefónico bajo demanda, enrutamiento snapshot, formación del tráfico.
Enrutamiento IP	BGP, RIP, IGRP, IGRP mejorada, OSPF, IS-IS, NAT.
Otro enrutamiento	IPX RIP, AURP, NLSP.
Multimedia y QoS	Formación de tráfico genérico, detección temprana aleatoria, RSVP.
Administración	SNMP, RMON, Cisco Call History MIB, Perfiles virtuales.
Seguridad	Lista de acceso, lista de acceso extendida, bloqueo y clave TACACS+.
Conmutación	Política de enrutamiento de conmutación rápida Apple Talk sobre ISL
Soporte IBM	APPN, Bisync, Frame Relay para SNA, integración SDLC.
Instalación de protocolos	LAT, PPP, X.25.
Nodo remoto	PPP, SLIP, MacIP, Agrupamiento IP, CSLIP, NetBUI sobre PPP.
Servicios de terminal	LAT, Xremote, Telnet, X.25 PAD.

Tabla 3.4 Categorías de las características del software IOS.

En las tablas 3.4 y 3.5 también muestran que grupos de funcionalidad de software van dentro de que productos del conjunto de características del IOS. Por ejemplo, es probable que las empresas multinacionales que estén interesadas en la funcionalidad IBM, como NetBUI sobre PPP y Frame Relay para SNA, probablemente estarán interesadas en uno de los conjuntos de características Empresa / APPN. Al contrario, agencia de publicidad basada en Apple y NT se centraría en los conjuntos de características de escritorio.

Familia de conjunto de características	Entorno de clientes destino
IP	Enrutamiento IP básico.
Escritorio	IP, Novell NetWare IPX, AppleTalk, DECnet.
Empresa	Funcionalidad de gama alta para LAN, WAN y administración.
Empresa / APPN	Igual que empresa, pero muchas características agregadas especificas de IBM.

Tabla 3.5 Familias de conjuntos de características IOS.

Agrupar los conjuntos de características en familias es la forma que tiene Cisco de ofrecer una semblanza de orden a las políticas de precio y trayectorias de actualización. Pedir un solo número de parte de IOS en vez de docenas de ellos ayuda a todo el mundo a evitar errores. La figura 3.4 muestra el proceso de selección del conjunto de características.

Por último, los conjuntos de características también se agrupan en variantes de productos de software:

- Básico. El conjunto de características básico para la plataforma hardware.
- Avanzado. El conjunto de características básico y características adicionales, que dependen de la plataforma hardware seleccionada.
- Cifrado. Agrega una característica de cifrado de 40 bits o bien encima del conjunto de características básico o bien del Avanzado. El objetivo último de los conjuntos de características es guiarle a través del proceso de pedido, por ejemplo, IOS Feature Set Enterprise 56 para Cisco 7500 / RSP que ejecuta la versión 11, sin cometer error que le cueste al proyecto de actualización dos semanas de retraso.

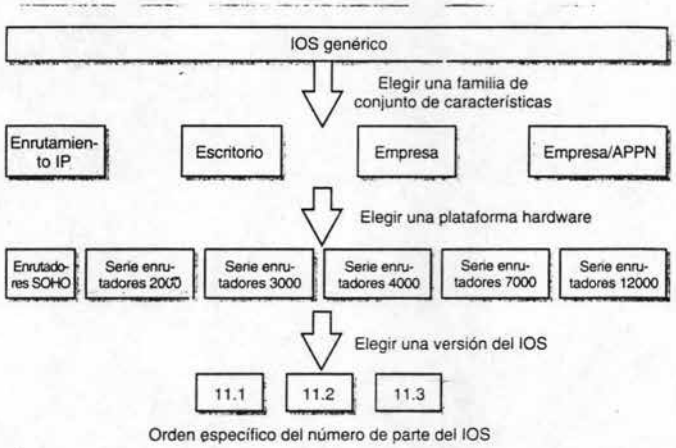


Fig. 3.4 Proceso de selección del IOS.

Anatomía de los números de versión de Cisco

Los números de versión del software de IOS tienen cuatro partes básicas como se muestra en la figura 3.5.

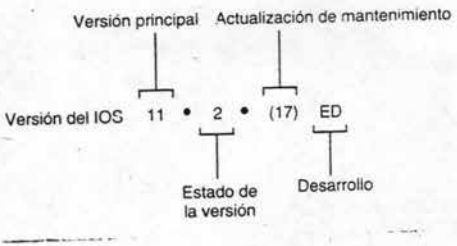


Fig. 3.5 Las cuatro partes principales de un número del IOS.

La primera parte es la versión principal, el "11" de la figura 3.5, que marca la primera versión de cliente, de una versión estable, las versiones principales, se definen mejor de la siguiente forma:

- Estado. El "2" de la figura 3.5 que marca el FCS de varios estados de versión principal, primera versión, versión general de desarrollo, versión de vida corta, etc. Se suele hacer mención a las versiones de los estados en tiempo futuro, cuando todavía están en planificación, pero no se han puesto en funcionamiento.

- Actualización de mantenimiento. El "17" de la figura 3.5, que denota el soporte para otras plataformas o características más allá de las que están disponibles.

La cuarta parte del número de versión es el desarrollo. Una versión desarrollo temprano, ED, que se utilizan para ofrecer nueva funcionalidad o tecnología a los clientes para desarrollar de forma limitada en sus redes. Desarrollo limitado, LD, denotado un ciclo de vida restringido por FCS y GD.

En cualquier momento puede haber varias versiones principales en uso. Por ejemplo, durante 1999, hubo disponibles dos versiones del IOS 12, pero casi todo el mundo utiliza la versión 11.2 o la 11.3. La mayoría de las administraciones de red tiene suficiente con pelearse con una versión que sepan va bien para sus necesidades. Los principales administradores de red utilizan versiones avanzadas del IOS porque necesitan soporte de plataforma o características no disponibles anteriormente. La mayoría de los usuarios están conformes en dejar que los principales administradores ayuden a Cisco a poner a punto las cosas antes de la versión general.

Usar TFTP para actualización y copia de seguridad del IOS

En caso de un desastre en la red, es posible que la imagen del sistema IOS del enrutador se corrompa o se borre de la memoria flash o todo a la vez. El procedimiento estándar es mantener una imagen de seguridad de todas las versiones IOS en uso de la red que se mantienen. Estas imágenes de seguridad se guardan en servidores TFTP o dentro de aplicaciones de administración de red como en los CiscoWorks 2000.

Protocolo de transferencia de archivo trivial TFTP. Este es una aplicación TCP/IP que se deriva de los albores del sistema operativo UNIX. Como puede imaginar, TFTP es una versión filtrada de FTP, el comando que muchos hemos utilizado para descargar archivos en Internet. IOS usa TFTP en vez de FTP porque es más rápido y usa menos recursos del sistema.

Los llamados servidores TFTP son equipos informáticos distribuidos a lo largo de una red que almacena y descarga imágenes de sistema IOS y archivos de configuración.

Se recomienda que se utilice más de un servidor TFTP para hacer copias de seguridad de una red. Esto es por si acaso el propio servidor TFTP se viene abajo o el segmento de red que lo conecta con los dispositivos de los que realiza la copia seguridad deje de estar disponible. Para cargar la nueva imagen del IOS en una memoria flash del enrutador, se usa el comando copy tftp flash.

Como podrá imaginar el servidor TFTP confirmará que tenia una imagen del sistema IOS de sobrescribir la que había en la memoria flash del enrutador. Cada punto de exclamación que aparece en la pantalla indica que se ha copiado con éxito un bloque de un archivo a través de la red, desde el servidor al enrutador.

3.5.2 El archivo de configuración

Administrar un enrutador implica instalación, actualizaciones, copias de seguridad, recuperación y otras tareas controladas por eventos. Pero la mayor parte de la administración de los enrutadores se dedica a su cuidado y a proporcionarle un archivo de configuración del enrutador. El archivo de configuración es la cabina de mando desde donde el administrador de red ejecuta el control del enrutador y todo el tráfico que fluye a través de él. Los archivos de configuración contienen listas de acceso, contraseñas y otras herramientas importantes de administración del enrutador.

La forma más común de ver los archivos de configuración es examinar el estado de un enrutador. Ver casi todo el IOS es pedir una vista de la configuración. El principal comando IOS para ver dicha información es el comando, SHOW. Hay dos tipos de configuración en ejecución de es una imagen ejecutándose en la DRAM, memoria principal, en un momento determinado. El archivo de configuración copia se almacena en la NVRAM y se usa para iniciar el enrutador.

Usar TFTP para configurar actualizaciones y copias de archivo, son al igual que con las copias de seguridad y las actualizaciones de la imagen del sistema IOS, los servidores TFTP se usan para realizar copias de seguridad y actualizar archivos de configuración. Por ejemplo, el comando copy config tftp se usan para realizar una copia de seguridad del archivo de configuración del enrutador en ejecución.

Los comandos TFTP para copias de seguridad o actualización de archivo de configuración son:

- COPY TFTP URNG-CONFIG_. Configura el enrutador directamente copiando desde TFTP directamente a la DRAM del enrutador.

- COPY STARUP-CONFIG TFTP_. Realiza una copia de seguridad de la configuración desde la NVRAM del enrutador al servidor TFTP.

- COPY TFTP STARUP-CONFIG_. Actualiza el archivo de configuración de inicio del enrutador mediante la descarga desde el servidor TFTP y sobrescribe en está almacenando en la NVRAM del enrutador.

Tenga en cuenta que TFTP va delante del tipo de archivo, running-config o star-tup-config, para descargar o actualizar desde el servidor, y detrás del tipo de archivo a cargar como copia de seguridad al servidor. Piense en copy como en copiar desde algún lugar a algún lugar.

Primeros pasos con los enrutadores de Cisco

Para configurar y administrar enrutadores de Cisco, debe poder interactuar con ellos a través de alguna clase de extensión. Primero, debe poder comunicarse de alguna manera con un enrutador, iniciando una sesión o cargando archivo a un enrutador o desde un enrutador. Una vez que haya conseguido conectarse con éxito a un enrutador, debe poder hablar su lenguaje, que en los enrutadores de Cisco son los comandos del IOS.

Comunicación con el IOS

Es posible accesar a un enrutador directamente a través de los puertos de consola o auxiliar, mediante una red usando Telnet o el protocolo http. Los profesionales de las redes suelen usar Telnet por comodidad. Cualquiera de los métodos que utilice, debe acceder al entorno IOS para revisar los archivos e introducir comandos, Telnet se distribuye con todos los sistemas operativos Microsoft Windows. Puede ejecutarlo haciendo click en el botón inicio, elija luego Ejecutar y escriba Telnet en la línea de comandos; aparecerá una pantalla Telnet en blanco. Haga click en la pantalla para conectar, que aparece en el extremo superior izquierdo de la barra de menú e introduzca la dirección IP del enrutador en el que quiera iniciar la sesión bajo la opción sistema remoto. De esta forma accederá al símbolo del sistema de contraseña de línea del enrutador destino.

Se utilizaría una de las direcciones IP remotas si el enrutador se encuentra en un sitio remoto, es decir, por encima de la LAN, pero incluso si se encuentra en la misma red del enrutador, es necesario introducir una contraseña válida para poder accesar al enrutador.

Uso de los comandos del IOS

Cualquier entorno al software de computadoras tiene sus particularidades, e IOS no es ninguna excepción. Por un lado, IOS es un sistema operativo creado con un propósito, al que se le ha despojado de todo menos de lo esencial para hacerlo más sencillo y rápido. Esto es una buena idea, pero tendrá las características de una interfaz de usuario gráfico, por lo contrario, IOS es uno de los sistemas operativos más distribuidos e importantes; Por lo que si se fija todo lo que necesita el usuario para operar lo lleva incorporado.

Jerarquía de comandos del IOS

IOS dispone de cientos de comandos. Algunos se pueden usar en cualquier lugar del IOS, otros sólo dentro de un área especifica. Incluso los especialistas de Cisco no han memorizado todos los comandos IOS. Así que, como cualquier buen sistema operativo IOS organiza sus comandos en jerarquía. La figura 3.6 es una perspectiva general de cómo se estructuran los comandos del IOS.

La primera división dentro de IOS es entre los niveles EXEC de usuario y EXEC privilegiados del IOS. El EXEC de usuarios, por supuesto, contiene sólo un subconjunto de comandos del EXEC privilegiados. El modo EXEC de usuario, que es menos potente, es donde residen connect, login, ping, show y otros comandos inocuos. Estos también están en el EXEC de privilegiado. Pero el modo privilegiado es dónde residen exclusivamente los comandos más poderosos, y potencialmente destructivos, configure, debug, erase, setup y otros.

Dependiendo del conjunto de características IOS instalado, suele haber el doble de comandos en el modo EXEC privilegiado que en el EXEC de usuario. Los comandos en el modo EXEC de usuario tiende a ser planos. En otras palabras, no tienen ramas que apunten a subconjuntos de comandos más bajos en la jerarquía.

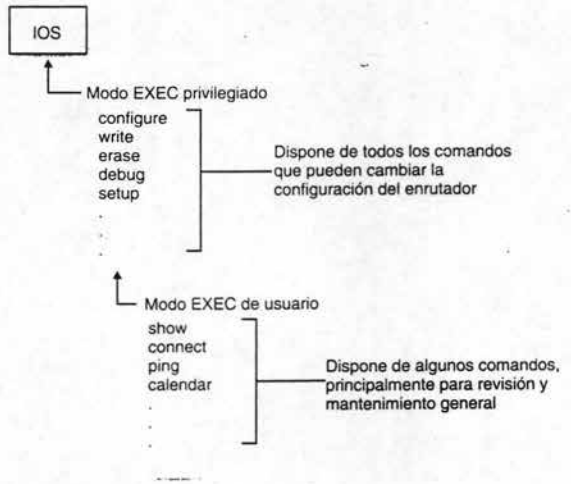


Fig. 3.6 La estructura de comandos del IOS.

Cómo correr el IOS con el sistema de ayuda

IOS tiene incorporado un sistema de ayuda sensible al contexto. Sensible al contexto significa que el sistema de ayuda responde con información basándose en el lugar del sistema donde esté situado el citado usuario en ese momento. Puede conseguir la mejor ayuda sensible al contexto introduciendo simplemente una interrogación en la línea de comandos. Aquí, por ejemplo, tiene un listado de todos los comandos raíz disponible en el nivel EXEC de usuarios de IOS.

También puede conseguir lo que algunos llaman "ayuda de palabra" introduciendo parte del comando, que no conoce, seguido inmediatamente de una interrogación.

La ayuda de palabra es una forma de conseguir definiciones y es especialmente práctica para averiguar lo que significan los comandos truncados, como con show. Otra forma de conseguir ayuda acerca de un comando parcial es simplemente introducirlo, con lo cual el sistema devolverá una instrucción sobre obtener ayuda sobre el comando.

Tenga en cuenta que en la ayuda que sugirió el comando show? Hay un espacio entre el comando y la interrogación. Como se habrá dado cuenta, siempre hay un espacio entre un comando y su modificación, llamado argumento, hacer esto en una solicitud de ayuda siguiente ejemplo, la interrogación solicita todos los argumentos disponibles para show.

Algunas veces, usar la ayuda de esta forma se llama sintaxis de comandos, ya que a completar correctamente un comando con varias partes. La ayuda de sintaxis de comandos es una herramienta potente de aprendizaje porque lista las claves o argumentos disponibles para el usuario en, prácticamente, cualquier momento de las operaciones de comandos IOS. Recuerde, es necesario insertar un espacio entre el comando y la interrogación para usar la ayuda de sintaxis de comandos.

En IOS, la ayuda juega un papel más importante que el sistema de ayuda de los paquetes de aplicaciones de software de negocios o de una PC normal. Estos sistemas de ayuda, también sensibles al contexto, son esencialmente manuales en línea que intenta ayudarle a aprender toda la subsección de la aplicación. La ayuda de IOS es escueta; sólo pretende ayudarle a llegar hasta la siguiente línea de comandos. Esto es alentador. La mayoría de los sistemas de ayuda parecen asumir que el usuario está ansioso por pasar horas leyendo todo sobre un subsistema cuando, de hecho, sólo quiere saber qué hacer a en el momento.

Sintaxis de comandos

Existen más formas de ejecutar los comandos del IOS que simplemente es a través del árbol de subcomandos del comando raíz. Para ejecutar IOS, debe aprender cómo cambiar diferentes comandos, no sólo modificar un único comando, para formar las líneas de comandos que requiere realizar el gran impulso a la administración de red. Pero IOS no es una ciencia extremadamente compleja, como se muestra en el siguiente ejemplo:

```
MyRouter#config
Configuring from terminal, memory, or network [ terminal] ?
```

En la línea de comandos anterior, se entra al modo configurar, e IOS que quiere saber si la configuración se enviará por la red, se copiará desde una imagen almacenada en la memoria Nram del enrutador o se escribirá desde un terminal. Podría haber evitado con facilidad entrar en la línea de comando si solamente se conjuntas los dos en una sola línea de comando:

```
MyRouter#config terminal
```

Esto es la abreviación del IOS, para configurar la terminal, el siguiente paso es apuntar o señalar al objeto a configurar. Por lo cual se configurara una interfaz:

```
MyRouter(config) #interface
% Incomplete command.
```

Pero en vez de preguntar ¿ qué interfaz desea configurar? IOS nos indica de manera automática que el comando no es correcto. Es aquí donde se requiere habilidad del usuario:

MyRouter (config) #interface tokenring1
MyRouter (config-if) #

IOS debe saber que módulo de interfaz física era el que había que configurar. Una vez que se indica que se ha elegido para configurar el puerto número uno del módulo de la interfaz Token Ring, la línea de comandos IOS cambia a MyRouter(config-if)# donde if es la abreviatura de interfaz.

Una vez que apunta a la interfaz de red a configurar, a partir de aquí la configuración del enrutador es simplemente una cuestión de suministrar a IOS los parámetros de configuración para dicha interfaz.

Antes o después se encontrará con líneas de comandos IOS llenas con símbolos aparentemente crípticos, sólo son comandos que los usuarios expertos han truncado para acelerar el proceso de escribir comandos, IOS se parece a DOS pero si el comando truncado no es una cadena de letras idénticas al conjunto de comandos, generará un mensaje de error. Por ejemplo, si se escribe las dos primeras letras de un comando con la que empieza otro comando, obtendrá un mensaje de error como el siguiente:

Router#te
% Ambiguous command : "te"

Este error aparece porque IOS tiene tres comandos que empiezan con la cadena "te" Telnet, terminal y test. Si lo que se quiere es hacer Telnet a algún lugar, agregue un carácter más para solucionar el problema:

Router> tel
Host:

Volver a llamar al historial de comandos

IOS mantiene un registro en ejecución de los comandos recientemente introducidos, es capaz de volver a llamar comandos es útil para:

- Evitar tener que escribir comandos que se introduce repentinamente.
- Evitar tener que recordar líneas de comandos largas y complicadas.

La utilidad del historial (History) registrar cualquier cosa que se introduzca, incluso comandos erróneos. El único limite es la cantidad de búfer de memoria dedicada a mantener el historial. Aquí se muestra un ejemplo:

```
Router#show history
Test
Tel
Exist
Enable
```

Los comandos introducidos más recientemente aparecen más abajo de la línea show history.

También se pueden usar las teclas de flechas para mostrar comandos anteriores. El uso de las teclas de flecha ahorra tener que introducir el comando show history pero sólo muestra los comandos anteriores de uno en uno. Puede pulsar la tecla de flecha para ir hacia arriba o control-p para volver a llamar el primer comando más reciente. Si ya está en algún lugar en la secuencia de comandos anteriores, pulse la tecla flecha hacia abajo o control-n para volver a llamar al primer comando.

Introducción a los modos de enrutador

Los enrutadores Cisco pueden estar en cualquiera de los siete posibles modos operativos, como se muestra en la figura 3.7. Tres de ellos son modos de inicio. En los otros cuatro, los administradores de red están en modo EXEC de usuarios o en modo EXEC privilegiado o en modo de habilitar. Debe pasar por el símbolo de sistema de contraseña en el EXEC de usuario para entrar este mismo comando. Una vez dentro del EXEC privilegiado, se puede realizar los cambios de configuración a todo el dispositivo o a una interfaz de red específica.

Debe realizar un seguimiento del modo de enrutador en que se encuentra en todo momento. Muchos comandos IOS sólo se ejecutarán desde un modo específico.

Como puede verse en la figura 3.7, los modos de enrutador son más específicos y potentes conforme el usuario se desplaza hacia el centro del IOS. Conviene estar atento a la línea de comandos IOS porque siempre indica en qué modo está.

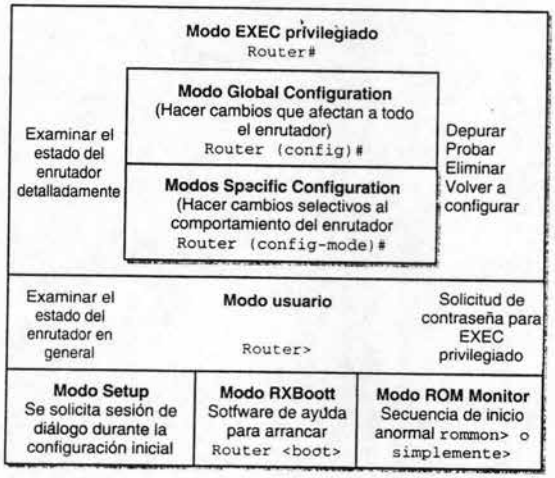


Fig.3.7 Siete posibles modos de operación de los enrutadores Cisco.

Tres grupos de los modos de operación

Los modos operativos del enrutador de Cisco se pueden agrupar tres condiciones generales:

1. Iniciar un sistema.
2. Definir qué comando puede utilizar un usuario.
3. Especificar qué partes de un enrutador se verán afectadas por los cambios realizados al archivo configuración.

En la tabla 3.6 se muestra los diferentes modos IOS y su propósito. A medida que se familiarice con la interconexión de redes de Cisco en general, y con el software IOS en particular, verá que la mayoría de la acción se produce dentro de los diferentes modos de configuración.

Condiciones	Propósito
Inicio	- El modo Setup se usa para realizar un archivo básico de trabajo de configuración - El modo RXBoot ayuda en el inicio de los enrutadores a un estado rudimentario cuando no es posible encontrar en la memoria Flash una imagen operativa del IOS. - El modo ROM monitor lo usa el enrutador si no es posible encontrar la imagen del IOS o si se interrumpió la secuencia normal de inicio.
Usuario	- El modo EXEC de usuario es el primer lugar donde accesa el usuario después de iniciar una sesión; limita a los usuarios a examinar el estado del enrutador. - Se entra al modo EXEC de privilegio utilizando una contraseña de disponibilidad que permite a los usuarios modificar el archivo de configuración, borrar memoria, etc.
Configuración	- El modo Global de configuración parámetros de todas las interfaces. - El modo Comando de Configuración realiza en interfaces concretas

Tabla 3.6 Tres formas generales de modos software del IOS.

Dos tipos de archivo de configuración

Hay dos tipos de configuración para cualquier enrutador:

1. Archivo de configuración de ejecución.
2. Archivo de configuración de inicio.

Como sus nombres indican, la diferencia básica es que el archivo de configuración de ejecución está en pendiente en el sentido de que su imagen está en Ram. Cualquier cambio que se realice al archivo de configuración en ejecución se aplica inmediatamente. El archivo de configuración de inicio se almacena en la Nvram del enrutador, donde la secuencia de inicio del IOS busca los parámetros de configuración de ejecución del enrutador cuando se inicia. El comando copy se usa para guardar y distribuir cambios en el archivo configurar, como puede ver en la parte inferior de la figura 3.8, se puede distribuir un archivo de configuración maestro a otros enrutadores mediante un servidor TFTP.

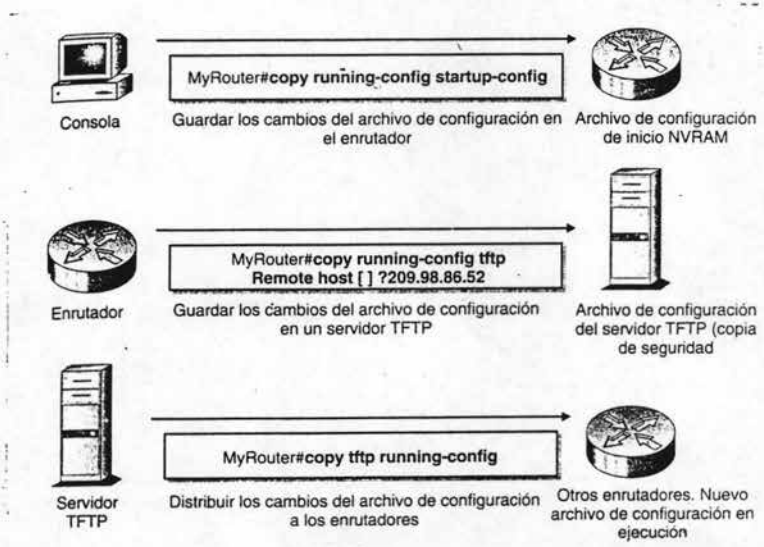


Fig. 3.8 Cada modo de configuración corresponde a una parte del enrutador.

3.6 Configuración del Enrutador Cisco

La configuración del enrutador se realiza mediante los siguientes pasos:

- Introducir cambios directamente en un archivo de configuración en ejecución del enrutador
- Descargar un nuevo archivo de configuración desde un servidor TFTP
- Definir el archivo de configuración desde cero

La mejor forma para aprender a configurar un enrutador es configurar uno desde que se instala. Se mencionara paso a paso a través del modo de configuración aqui, no porque el procedimiento se realice a menudo, sino porque es una forma excelente de revisar los fundamentos de la configuración de enrutadores.

3.6.1 Modo Setup

La configuración se realiza para hacer funcionar el enrutador a un nivel básico. Si el dispositivo es nuevo y por lo tanto nunca se ha configurado o se ha corrompido el archivo de configuración en la NVRAM, el software IOS entra automáticamente al modo setup para reconstruir el archivo de configuración desde cero. Una vez conseguido esto, se puede salir del modo setup y reiniciar el enrutador en modo ISO normal, sobre el que se puede crear un archivo de configuración completa. El modo setup no se ejecuta por sí mismo; el administrador de red debe estar presente para responder a una larga secuencia de preguntas de configuración sobre cómo configurar el enrutador. También, dado que el enrutador no está configurado, no puede ejecutar la configuración mediante una conexión de red. La configuración debe realizarse a través del puerto de la consola o del puerto AUX.

Un enrutador no tiene que ser nuevo o estar para dañado para realizar la configuración. La configuración también puede ser útil en situaciones que no sean de emergencia, los administradores de red a veces usan la configuración cuando un archivo de configuración se ha convertido en un desorden de comandos, tiene más sentido iniciar uno nuevo, como una hoja de papel en blanco. Si se utiliza de esta forma, los parámetros de configuración dados como respuestas durante una sesión de configuración sobrescriben el archivo de configuración existe.

Se entra en el modo de setup y este comando, pero antes de empezar, se conecta el puerto COM de la PC al puerto de la consola del enrutador, luego inicie el software de emulador de terminal que quiera usar, recuerde que un usuario iniciará una sesión en el sistema operativo del enrutador, no en la PC. Las siguientes instrucciones suponen que utilizan una PC con Microsoft de Windows, si no es así, deberá saber como iniciar el emulador de la terminal.

Este es un simple ejemplo de cómo realizar un procedimiento de setup:

1. Haga click en el botón de Inicio.

2. Seleccione programas, luego Accesorios después elija HyperTerminal.

3. Se abrirá una ventana de HyperTerminal, con un cursor parpadeante en la esquina superior izquierda.

4. Pulse Intro, deberá ver la línea de comandos del enrutador.

5. Vaya al modo EXEC privilegiado introduciendo enable, y luego la contraseña de habilitación secreta, setup es, esencialmente un comando de configuración y los archivos configuración no se pueden modificar desde el nivel EXEC de usuario de IOS.

6. Escriba setup y el modo configuración se inicia.

Una vez iniciada la configuración, aparece un titular con instrucciones de comandos, una opción para salir y una opción para revisar un resumen de los módulos de interfaz del enrutador. Al final de una serie de pasos se preguntara si desea continuar con la configuración, en caso de ser así, la configuración empieza configurando los parámetros globales. Esta información es básica, como asignarle un nombre y contraseña al enrutador. Si es un enrutador nuevo o el archivo de configuración en la NVRAM está dañada. Debe introducir nuevos parámetros para estos objetos.

Una vez explicados los principios básicos, setup le lleva a través de una lista de protocolos que puede que quiera configurar globalmente. Esto ofrece una imagen de los protocolos soportados en el conjunto de características IOS de nuestro enrutador. Pero si, por ejemplo, este enrutador tuviera una imagen del conjunto de características Enterprise APPN de IOS establecido en su memoria Flash, el setup mostrará en este momento una lista incluyendo muchos protocolos SNA de IBM.

Varias líneas de comandos preguntan si quiere configurar protocolos heredados. Por ejemplo, la Terminal de Área Local (LAT) Local Area Terminal, es un viejo protocolo que se usaba para cablear terminales en una LAN de DECnet usando servidores de terminal. En la actualidad los protocolos que usará normalmente son IP, Novel IPX, AppleTalk y VINES, más o menos en ese orden.

Si se va a reemplazar un archivo de configuración existente, setup no ignorara por completo la configuración actual del enrutador. Como se podrán imaginar de párrafo anterior las líneas de comandos predeterminadas [yes], que es el archivo de configuración global ya existente esté configurado con IP usando el protocolo de enrutamiento IGRP, configurando para usar el sistema autónomo IGRP número 1. Sin embargo si el enrutador fuera nuevo o el archivo existente estuviera dañado, no notaría los parámetros de configuración existentes, y todas las líneas de comandos tendrían un [no] como valor predeterminado.

Después de realizar estas configuraciones de parámetros globales, la configuración se centra en la configuración específica de la interfaz y empieza a solicitar valores de configuración para módulos de interfaz específicas.

Setup detecta automáticamente los módulos de interfaz presentes físicamente en las ranuras del enrutador, una a una se preguntará si la interfaz está en uso, si contesta si a cualquiera de las líneas de comandos, esto quiere decir que está optando por cambiar dicho valor de configuración del parámetro de administrativo activo. Esto demuestra que el setup puede notar no sólo la presencia y el estado activo / caído, sino también los valores de configuración de la interfaz que él nota que está establecido a 16 Mbps.

Cuando se detecta una interfaz, la configuración quiere establecer sus parámetros, los parámetros se cambian simplemente escribiendo un nuevo valor en vez de tomar los valores predeterminados mediante un entorno de continuidad. Con una dirección IP de la interfaz y un número uno Token Ring se cambia. Una vez tratadas las interfaces, setup presentará al usuario una secuencia de comandos resumiendo el archivo de configuración del enrutador, incluyendo cualquier cambio, y le preguntará si desea seguir adelante y poner a funcionar el archivo recién creado. Si sigue adelante, setup dedica algunos segundos para generar el archivo de configuración, como se ha dicho los archivos de configuración no se modifican de forma interactivo como un archivo de procesador de texto, una vez generado, el usuario para al modo normal de IOS y se le pregunta si desea continuar con la configuración con el comando CONFIG.

Una vez finalizada la sesión de configuración, se ha creado un archivo de configuración básico. A partir de ahora debe seguir un procedimiento normal y entrar al modo EXEC privilegiado y usar el comando CONFIGURE para introducir un archivo de configuración completo.

Cómo asignarle una identidad al enrutador

Tomarse el tiempo adecuado para nombrar y documentar correctamente cada enrutador ayuda a hacer las redes más fáciles de administrar. La información de identificación puede introducirse mediante:

- Dando al enrutador un nombre significativo.
- Documentando individualmente las interfaces del enrutador.
- Poniendo un Mensaje de día MOTD (Message of the day, en el enrutador).

Frecuentemente verá que se usa el nombre de ejemplo "Router" en el ejemplo de configuración, pero no es obligatoria en la línea de comandos de IOS Cisco, un enrutador puede nombrarse simplemente de forma tan fácil como cualquier el más común de los nombres. A los enrutadores se les dan nombres significativos que informan a los administradores de red dónde están los enrutadores y qué hacen.

Debe estar de modo de configuración global y usar el comando HOSTNAME para cambiar el nombre del dispositivo. Cuando se ha introducido un nuevo archivo de configuración, el nuevo nombre MYROUTER se usa de inmediato en la siguiente línea de comandos. Sin embargo, a menos que use el comando WRITE o el comando COPY para almacenar el nuevo nombre o cualquier otro cambio, en la NVRAM, si el enrutador fuese reiniciado, IOS seguiría usando el nombre antiguo. La interfaz de un enrutador puede documentarse específicamente usando el comando DESCRIPTION. Usar descripciones es una gran forma de hacer seguimientos de la red y usuario, a la que da servicio una interfaz. Puede que esto no parezca muy importante, pero las grandes redes tiene miles de interfaces y se configuran frecuentemente. Para introducir una descripción de una interfaz especifica debe ir primero a esa interfaz, introduzca luego el comando DESCRIPTION seguido por la descripción.

Las descripciones pueden tener hasta 80 caracteres de longitud. Para cerrar el ciclo, es posible ver la descripción en la parte del archivo CONFIG dedicada a la interfaz.

Los nombres de enrutadores y las descripciones de interfaz sólo las ven los administradores de red. Una última herramienta de identificación de enrutador, es el titular de mensaje del día, es una forma de dar a conocer información a todas las terminales conectadas al enrutador. Los titulares MOTD son una buena forma de asegurar que todos los usuarios de la red ven los anuncios de administración particulares. Los titulares se suelen utilizar para alertar contra el uso no autorizado, anunciar tiempos de parada programados del sistema y realizar otros tipos de anuncios. Use el comando BANNER MOTD para poner un titular en el enrutador.

Un signo de dólar se puede elegir de forma arbitraria como la marca delimitadora del inicio y fin del mensaje del titular. Es posible utilizar cualquier carácter; basta que se asegure de que usa un carácter que no aparecerá en le propio texto del titular.

El titular aparecerá siempre que alguien inicie una sesión directamente en el enrutador o sé accese al enrutador desde un explorador Web.

Se puede crear atractivos titulares de varias líneas usando los comandos de modo extendido para terminales VT. VT es un estándar de programación de terminales de equipamientos digitales. Una advertencia; no ponga ninguna información sensible en los titulares MOTD, porque cualquiera pueda verlos. Aquí puede haber implicaciones legales si un mensaje Bienvenido a ... da la bienvenida a los piratas mientras accesan a su red.

Examinar el estado de los dispositivos

Examinar las interfases de redes es una técnica básica para obtener información de estado crítico. El comando SHOW INTERFACE hace esto. Las interfases son quienes envían los mensajes de supervivencia, de una o otra en el nivel de enlace para confirmar que el circuito virtual entre ellas sigue activo. La tabla 3.7 resume lo que significan los diferentes informes de estado, usando una interfaz Token Ring como ejemplo.

Mensaje	**Significado**
Token Ring 1, el protocolo de línea esta activo.	Todo funciona perfectamente.
Token Ring 1, está ir.activo, el protocolo de línea está inactivo.	Existe un problema con la interfaz
Token Ring 1 está inactivo de forma administrativa, el protocolo de línea está inactivo.	Deshabilitado.

Tabla 3.7 Definición del informe de estado de la interfaz.

3.6.2 Protocolo de descubrimiento de Cisco

Cisco dispone de una herramienta propia de solución de problemas llamada Protocolo de Descubrimiento de Cisco CDP (Cisco Discovery Protocol), se incluye con todos los equipos Cisco, incluso en los enrutadores. CDP lo utilizan los dispositivos para descubrir y aprender uno sobre el otro en otras palabras saben con que tipo de equipo se esta comunicando. Es independiente del medio y del protocolo. Los dispositivos de Cisco usan el CDP como una forma de dar a conocer su existencia a los otros equipos de una red LAN o al otro extremo de una conexión WAN. Piense en CDP como en una especie de comando Show Configuration, para el conjunto de enrutadores Cisco y otros dispositivos.

CDP se ejecuta en la capa de enlace de datos para ser compatible con dispositivos que ejecutan diferentes protocolos de la capa de red como, IPX, IP, Apple Talk, etc., CDP puede comunicarse con cualquier medio físico que soporte Protocolo de Acceso a Subred (SNAP) Subnetwork Access Protocol, incluyendo medios LAN, Frame Relay y medios ATM. Snap es un protocolo diseñado para permitir que los dispositivos envíen mensajes dentro de una subred como medio de dejarles hacer un seguimiento de lo que sucede en la red.

CDP es automático y es posible conectar cualquier combinación de dispositivos Cisco, encenderlos y tener la seguridad que trabajan bien sin la necesidad de que haya alguien supervisando las acciones de los dispositivos y dejar que se identifiquen unos a otros automáticamente, incluso antes de que se les asigne una dirección de red. CDP es capaz de hacer esto usando un estándar propio llamado Protocolo Propietario de Enlace de Datos de Cisco, la figura 3.9 muestra como CDP también abarca los protocolos que de otra forma serían incompatibles.

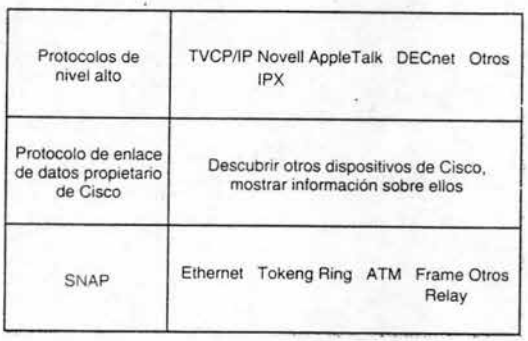


Fig. 3.9 CDP realiza el seguimiento de las redes.

CDP está habilitado de forma predeterminada en todos los dispositivos Cisco. CDP funciona haciendo que todos los dispositivos Cisco de una red conectada de forma directa envíen tramas CDP de uno a otro. La clave para comprender los límites exteriores de CDP reside en las palabras conectadas de forma directa. CDP puede descubrir dispositivos más allá de una LAN, pero sólo tan lejos como las conexiones WAN que no utilicen un dispositivo que no sea de Cisco y por lo tanto no sean compatibles con CDP, para realizar la conexión. Las tramas CDP deben ser capaces de viajar a través de las conexiones de redes para seguir extendiendo su mapa de lo que está conectando a su LAN particular. Use el comando Show CDP para ver cuáles son las configuraciones operativas actuales.

Como podrá imaginar, CDP es capaz de recopilar de forma remota información de configuración detallada sobre dispositivos, CDP se diseño para ser un protocolo eficiente, de baja sobrecarga, así como para hacer uso del preciado ancho de banda y, por tanto realzar toda la línea de productos Cisco. Como CDP es propietario, es capaz de recopilar mucha información sobrecargando muy poco el sistema. Existen otras herramientas para descubrir dispositivos conectados de forma local, las herramientas de administración de red SNMP son importantes para la administración centralizada, pero recopilan menos información granular que CDP en los dispositivos Cisco.

3.6.3 Aplicaciones de ayuda a la configuración

Aplicaciones de software que sirve como herramientas:

- Config Maker. Una herramienta de gama media que se ejecuta sobre Windows 95, 98 y NT 4.0; es una herramienta para configurar las LAN's Ethernet y conectividad WAN, pensada para que la utilicen los administradores o consultores de red que sean bastantes competentes.

- Fast Step. Una herramienta de gama baja que se ejecuta sobre Windows 95, 98 y NT, se utiliza para configurar e instalar pequeños enrutadores y servidores de acceso de Cisco, pensando para que la utilicen los usuarios menos expertos.

Las dos herramientas usan una interfaz gráfica de usuario para ayudar en la tarea de configuración de los enrutadores y hacerlos funcionar. Ninguna herramienta soluciona problemas importantes o complejos de interconexión de redes. Se usa un producto independiente llamado NetSys Baseliner para el modelado y la administración de grandes redes. El uso de Config Maker y Fast Step está prácticamente destinado sólo a usuarios de nivel intermedio y principiantes.

I. Config Maker

Es una herramienta basada en Microsoft Windows que se usa para diseñar y configurar pequeñas redes, funciona tanto para configuraciones LAN como para conectividad WAN. con soporte para un amplio campo de dispositivos y protocolos de Cisco. Config Maker ofrece un entorno de trabajo claro e intuitivo en la PC que consigue un buen equilibrio entre la facilidad de uso y funcionalidad. Pero no está destinado a usuarios sin experiencia, ya que no tiene soporte para dispositivos de la gama alta como los enrutadores de la serie Cisco 7000 o conmutadores de gama alta. Config Maker tampoco soporta el protocolo Token Ring para LAN.

Config Maker se ejecuta sobre Windows 95, 98 y NT 4.0, Cisco lo distribuye sin costo alguno. Para probarlo, descargue una copia desde el sitio Web de Cisco, para el creciente número de personal técnico en pequeñas y medianas empresas que quieren manejar su propia configuración de red, Config Maker es probablemente la solución, con tal de que los dispositivos que forman sus redes prácticamente todos sean de Cisco.

En el centro del escritorio de Config Maker hay un área de diagramas de red en la que se colocan, configuran y enlazan entre sí los objetos de red. Al principio, el área del diagrama de red está vacío, el área de diagrama de red está rodeada de tres ventanas, cada puesta allí para ayudar a generar una red hasta terminarla:

- Ventana de Dispositivos. Origen de dispositivos que arrastrar y colocar en el área de diagrama de red.

- Ventana de Conexión. Origen para conexiones de red de área extendida para arrastrar y colocar en el área de diagrama de red.

- Lista de Comprobación. Esta lista da los pasos cronológicos que deben realizarse en la configuración de la red.

El primer paso es arrastrar y colocar dispositivo desde la ventana de dispositivos al área Network Diagram. Sólo es una idea; basta con elegir cualquier dispositivo que va a formar parte de la red: enrutadores, concentradores, cables LAN, etc. A medida que se coloca cada dispositivo en el diagrama, Config Maker solicita los valores de configuración necesarios para que sea funcional. Las rutinas de solicitud son similares a la rutina Agregar o Quitar hardware en el panel de control de Microsoft Windows.
Una vez colocados los dispositivos en el diagrama, es hora de conectarlos a una red. Esto se hace arrastrado una o más conexiones al diagrama desde la ventana de conexión. Para conectar un dispositivo a la red, primero haga click en la conexión y luego en el dispositivo a conectar. La figura muestra 3.10 muestra el escritorio de Config Maker con los principios de una red Ethernet visualizada en el área de diagrama de red, con dos enrutadores Cisco conectados a una LAN Ethernet. El usuario sigue agregando dispositivos y conexiones hasta que toda la red está representada en el diagrama.

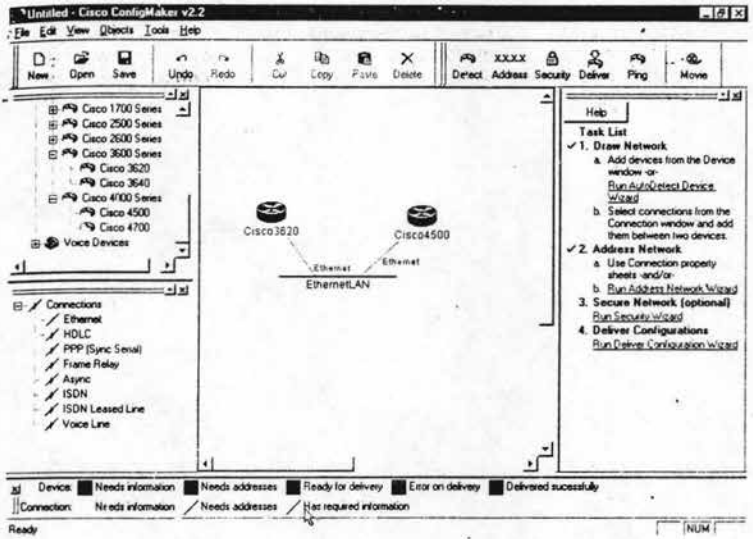


Fig. 3.10 El escritorio de Config Maker.

Metodología de Config Maker

Construir una red mediante esta interfaz gráfica es importante para tener un concepto de la topología de la red, pero Config Maker es algo más que simplemente un programa de diagrama de red. Cada elemento que se coloca en el diagrama en la ventana de dispositivos, a medida que se coloca cada objeto de red, Config Maker pregunta acerca de detalles de los elementos de línea como configuraciones, nombres y cosas similares. Esta información se almacena en una base de datos oculta detrás del diagrama y la usa Config Maker para verificar la consistencia interna. Config Maker impone una metodología para asegurar la calidad sobre el proceso de diseño de red, la cual es:

1. Conforme se agrega un dispositivo a la red, se recopila información sobre él.

2. Se comprueba la consistencia de la información con el resto de la base de datos.

3. Si se produce un error, Config Maker avisa al usuario para que lo corrija.

4. La lógica basada en reglas de Config Maker sigue comprobando toda la red para verificar que es correcta mientras se agrega un nuevo objeto.

Para ver la base de datos que mantiene Config Maker, haga click con el botón derecho sobre cualquier dispositivo y elija propiedades. Este cuadro de diálogo de siete fichas muestra toda la información conocida sobre un dispositivo. La figura 3.10, por ejemplo muestra la ficha de configuración del hardware. La ventana de la izquierda de la ficha contiene todos los módulos posibles que se pueden conectar al dispositivo. La ventana derecha muestra la configuración actual. En este ejemplo, el enrutador Cisco 4500 está configurado con un módulo de seis ranuras Ethernet y un módulo de puerto T1 / ISDN. Config Maker dispone de la lógica para capturar la mayoría de los errores de configuración antes de que ocurran, se indica al usuario que no inserte un módulo de red en un dispositivo incompatible, y una interfaz correcta debe estar en un dispositivo antes de que pueda conectarse a la red. Si se puede apreciar a nuestro ejemplo en las figuras 3.10 y 3.11, al enrutador Cisco 4500 se le permitió conectarse a la red Ethernet ya que configuró en primer lugar con su interfaz de seis puertos Ethernet y podría también ser conectado a una conexión TI / ISDN.

Los cuadros que aparecen en la parte inferior de la pantalla de Config Maker forma una leyenda de condiciones de estado clasificadas por colores, un icono de dispositivo, o las líneas de conexión, cambiaran de color en la pantalla conforme cambie el estado de configuración del objeto.

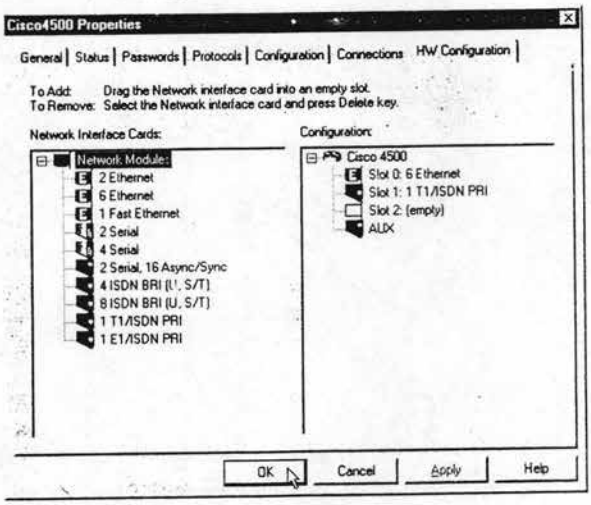


Fig. 3.11 Cuadro de diálogo de las propiedades de Config Maker.

Crear una red con Config Maker

La lista de comprobación es un sistema de ayuda y una lista de comprobaciones todo en uno. La ventana lista de comprobación que aparece a la derecha del diagrama de red. Usa un asistente para guiar al usuario a través de los cuatro pasos principales de la configuración de redes. Una vez finalizada cualquiera de las cuatro tareas de configuración de red, aparece a la izquierda una marca de comprobación. La ventana de lista de comprobación se divide en cuatro partes, cada una con asistente dedicado a un trabajo particular y son:

- Autodetect Device Wizard. Una serie de cuadros de diálogo del tipo agregar o quitar hardware solicitan datos para reunir la descripción y la información necesaria de configuración para los dispositivos de la red.

- Address Network Wizard. La parte de la secuencia de solicitudes de agregar o quitar hardware que recopila información de direccionamiento para dispositivos y sus conexiones.

- Secure Network Wizard. Ayuda a aplicar configuraciones de seguridad para registrar conexiones entre segmentos de red.

- Deliver Configurations Wizard. Descarga automáticamente archivos de configuración a los dispositivos.

Color	Estado de configuración
Gris	Es necesario más configuración en el dispositivo o en la conexión.
Negro	Se necesitan direcciones (direcciones IP, submáscaras, etc.) para el dispositivo.
Azul	El archivo de configuración del dispositivo está listo para ser enviado o la conexión tiene la información necesaria.
Rojo	Se ha enviado el archivo de configuración del dispositivo y se ha encontrado un error.
Verde	Se ha enviado el archivo de configuración con éxito.

Tabla 3.8 Claves de color por estados de seguimientos en una configuración.

El Autodetect Device Wizard. El uso es opcional, si lo usa detectará e identificará automáticamente el tipo de hardware que debe configurarse, Autodetect Device Wizard es práctico si está configurando el dispositivo de forma remota y si no está allí para inspeccionar físicamente los componentes hardware para ver los números de modelo, los módulos de interfaz instalados y demás. El Autodetect Device Wizard soporta tanto redes como conexiones de terminales virtuales (VTY) a los dispositivos que se están configurando.

El Address Network Wizard. Si se ha asignado de antemano las direcciones a los dispositivos de la red, pueden introducirse manualmente. De lo contrario el Address Network Wizard asignará un bloque de direcciones a todos los dispositivos o a dispositivos seleccionados en la red. Si ya existe parte de la red que se está diseñando y por lo tanto, ya tiene direcciones que se querrán mantener, es posible seleccionar la parte nueva del diagrama de red y usar direccionamiento automático sólo para estos dispositivos.

El Security Wizard. Sólo se usa para interconexiones de redes. Por ejemplo no se puede usar para establecer parámetros de seguridad para la red local que se está configurando, porque es un único segmento LAN, no una red. Si un diagrama de red incluye Internet o una Intranet, el Security Wizard ayuda a establecer políticas sobre que LAN pueden accesar y que LAN interna puede accesar a cada una, también usa símbolos del sistema para ayudar a establecer políticas de seguridad básica, cortafuegos e incluso las llamadas Zonas Desmilitarizadas (DMZ) Demilitarised Zone.

Es una LAN a la que el público, Internet entera o la Intranet de una organización, tiene acceso, pero es un problema salir de allí, los operadores de una red usan DMZ para poner a dispositivos del público partes de sus operaciones, sin permitir a los usuarios entrar al resto de la red privada. Los servidores Web y los servidores FTP son los ejemplos más comunes de equipos DMZ.

El Deliver Configurations Wizard. Hace una descarga automática de archivos de configuración creados para Config Maker en los dispositivos destino. Para usar esto, los dispositivos deben estar conectados mediante el puerto de la consola o la red a la PC sobre el que se ejecuta Config Maker.

Revisión del producto Config Maker

Una ventaja de Config Maker es que resulta difícil que los usuarios cometan errores, muchos errores de configuración implican elecciones erróneas para dispositivos particulares, si intenta colocar un dispositivo incompatible en un enrutador particular, aparecerá un mensaje de error. Si se olvida de algo necesario, también lo solicitará. Esta capacidad para asegurar la calidad no sólo ayuda a evitar errores, sino que también ayuda a mantener al usuario actualizado en las opciones del producto, ya que cambian constantemente.

No obstante, quizá la ventaja más importante de Config Maker es que el usuario no necesita conocer la interfaz de línea de comandos del software IOS de Cisco para poder configurar dispositivos de red y conexiones. Cuando necesite introducir algo, las elecciones correctas están justo delante de usted. La GUI basada en Windows lo hace posible. El uso de convenciones de Windows las solicitudes de agregar o quitar hardware, la barra de menú, etc., y las claves de color facilitan su aprendizaje y uso.

Config Maker consigue un equilibrio bastante bueno entre capacidad y facilidad de uso, que hace que tanto los iniciados como los expertos técnicos en redes puedan usarlo. Es un regalo para los no iniciados, no sólo para la configurar una red y ponerla en funcionamiento, sino también, para aprender los principios básicos de la interconexión de redes.

Sin embargo, Config Maker tiene limites, no está pensando para diseñar y administrar redes grandes o complicadas. Por ejemplo, sólo se soportan los enrutadores hasta la serie Cisco 4000, no así la serie de enrutadores de gama alta. Y su funcionamiento no permite simular el componente de red.

II. Fast Step

Fast Step de Cisco es una utilidad de configuración que se incluye con los enrutadores y servidores de acceso de gama baja. Está destinada para que la utilicen el usuario de red principiante con el fin de configurar conexiones punto a punto entre una PC y un proveedor de servicio de Internet (PSI) o Intranet corporativo. Fast Step se ejecuta sobre Microsoft Windows 95, 98 o NT 4.0, se distribuye en un CD-ROM para su instalación en una PC para Windows, también se puede utilizar de dos formas:

1. Para configurar el enrutador interactivamente mientras está conectado al enrutador, ya sea mediante un cable serie desde el puerto COM de la PC al puerto de la consola del enrutador o mediante un enlace Ethernet.

2. Para generar un archivo de configuración con el fin de descargarlo posteriormente al enrutador, o como base para configurar otros enrutadores, es posible leer el archivo mediante el Setup Wizard de Fast Step.

Después de instalar Fast Step, si hace click en el icono se iniciará una secuencia de cuadros de diálogo solicitando al usuario que introduzca información necesaria para configurar e instalar el enrutador. La secuencia puede abarcar alrededor de una docena de cuadros de diálogo, dependiendo de las opciones elegidas. Para ayudar a ordenar las cosas, cada pantalla de Fast Step tiene una ventana de tareas en el lado izquierdo. Usted puede ver su situación en el proceso buscando que tareas están destacadas en la ventana Tasks en la parte izquierda de cada pantalla de Fast Step. Como describe la tabla 3.9 se agrupan las tareas de configuración en cuatro pasos posibles.

Paso	Descripción de las tareas
Encontrar y Conectar	Proporcionar el nombre del enrutador; seleccionar modo de configuración, interactivo o descarga, definir el tipo de conexión, PSI u organización, ofrecer valores de configuración, accesar a la dirección IP y a los números de teléfono, nombre de usuario, contraseña, etc.
Seguridad	Especificar nombre de enrutador, contraseña de sólo lectura del enrutador y contraseña de habilitación secreta del enrutador especificando los tipos de servicio, servidor Web, servidor de correo, servidor FTP.
Dirección de localización	Especificar direcciones IP para conexiones LAN proporcionadas por PSI o por la Intranet de una organización.

Continúa.

Paso	Descripción de las tareas
Instalación y Pruebas	Guardar el archivo de configuración en el enrutador y ponerlo a funcionar, guardar el archivo configuración para usarlo con otros enrutadores.

Tabla 3.9 Fast Step y sus tareas de configuración.

Encontrar y Conectar

Fast Step comienza preguntando información general sobre la sesión de configuración, como el modelo de enrutador a configurar si es necesario crear un nuevo archivo de configuración, o si se usará un archivo configurado previamente.

Luego se solicita información más especifica. Fast Step pide que introduzca su nombre de usuario (PPP) protocolo de punto a punto, que le ha asignado su PSI o su administrador de la Intranet corporativa. El nombre de usuario PPP es sensible a las mayúsculas, por lo que se debe asegurarse de escribirlo exactamente como aparece en la información suministrada por su PSI o administrador de red.

A continuación, introduzca la contraseña PPP. Esta no es la contraseña de inicio de sesión en la red. La contraseña PPP es sólo para acceso telefónico remoto sobre una conexión enrutador a enrutador. Asegúrese de que la contraseña cumpla con los requisitos establecidos por su PSI o de red corporativa, (número mínimo de caracteres, etc.). Esta contraseña, a veces se llama contraseña PAP o CHAP, y es también sensible a las mayúsculas. Por último, introduzca el enrutador central o nombre PPP del enrutador al que esta conectado, no el nombre del enrutador que esta configurando.

La segunda mitad del paso Encontrar y Conectar es proporcionar la información y los valores de configuración necesarios para conectar el enrutador a Internet. Para ello, Fast Step solicita más parámetros implicados, como el tipo de conmutador, SPID de ISDN y números de teléfono de acceso, normalmente un PSI.

Luego las cosas empiezan realmente a complicarse, al menos para el principiante medio. La figura 3.12 muestra Fast Step solicitando la información de dirección IP.

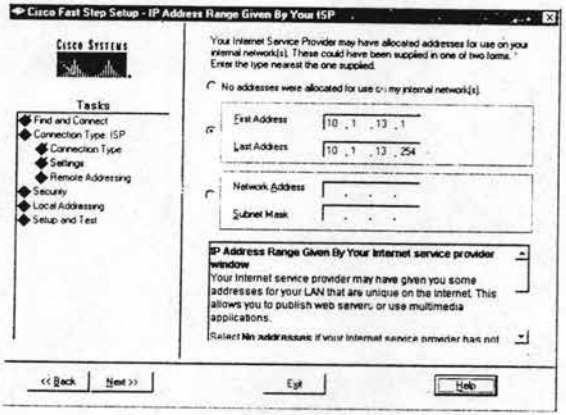


Fig. 3.12 Fast Step información de las direcciones IP.

Sólo puede optar por una de estas tres opciones:

- No ofrecer ninguna porque todavía no la tiene.
- Ofrecer un rango de direcciones que le ha proporcionado el PSI administrador de red de la organización.
- Ofrecer una dirección de red IP y una máscara de subred.

Esta información se usa para identificar el segmento LAN al que el usuario estará conectado con una dirección única de Internet. Fast Step necesita esta información para realizar la conexión a Internet. Estos valores de configuración son, en esencia, la dirección del usuario tal y como muestra al resto de Internet o a toda la Intranet de la organización. Fast Step puede descubrir automáticamente la dirección, pero permite al usuario introducirla directamente si lo desea.

Seguridad

Fast Step solicita los parámetros relacionados con la seguridad del enrutador y la publicación del servidor del enrutador. La figura 3.13 muestra al usuario cuando se le solicita que ponga un nombre al enrutador, una contraseña de sólo lectura y contraseña de habilitación.

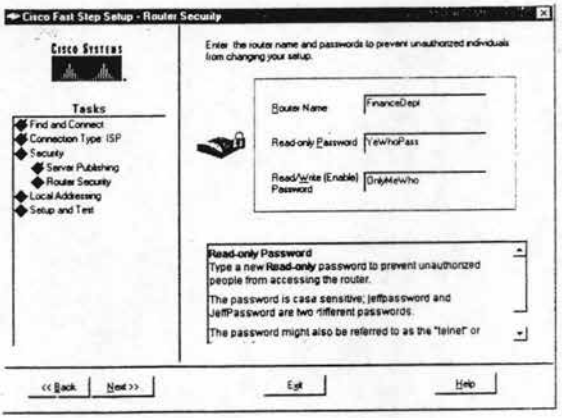


Fig. 3.13 Solicitud del nombre de un Enrutador y contraseña de administración.

Se aplican varias reglas a los nombres y a las contraseñas, de manera que si viola alguna de estas reglas, un mensaje de error le detendrá. El sistema de ayuda en línea indica al usuario que reglas son. Estas contraseñas se aplican para conseguir acceder al propio enrutador con propósitos administrativos. Luego, Fast Step permite que el usuario configure una o todas las opciones de servicios de Internet.

- Servidor sencillo, tanto un servidor Web como un servidor de correo, la opción más común.
- Servidor Web, una página Web sin servicio de correo electrónico.
- Servidor de correo sólo servicios de correo electrónico de Internet.
- Servidor FTP, posibilidad para los usuarios de Internet de descargar información de su sitio.

Los profesionales de las redes suelen llamar a estas opciones servidores. Por ejemplo, si el parámetro para ofrecer descargas FTP desde la LAN del usuario se establece como respuesta a dicha LAN está ejecutando un servidor FTP. Es sólo un término atractivo para un servicio.

Direccionamiento local

Por último, Fast Step solicita las direcciones IP de la red de área extensa a la que está conectada la LAN del usuario. Estas direcciones, que se muestran en la figura 3.14 identifican al PSI o la red corporativa en Internet.

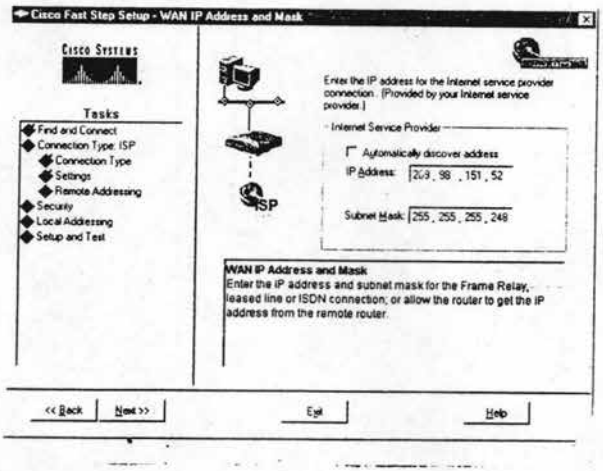


Fig. 3.14 Información de la dirección del SPI.

Si observa las figuras 3.12 y 3.14 verá que Fast Step necesita dos conjuntos de direcciones, que se utilizan para identificar dos segmentos de red independientes que están implicados en conectar la LAN del usuario remoto a Internet. Esto puede confundir, pero tenga en cuenta aquí que el enrutador se conectará al PSI / Intranet mediante una conexión enrutador a enrutador, punto a punto, no sobre una vaga dirección IP de Internet. La información de dirección proporcionada en la figura 3.12 se usa para identificar al enrutador que está configurado Fast Step. Este enrutador es lo que conecta la LAN del usuario a Internet. Como es posible que la LAN tenga más de un usuario a la vez haciendo uso de Internet, Fast Step preguntará por un rango de direcciones, una por usuario, por otro lado, la dirección remota que solicitó se usará para identificar el segmento de red que identifica el PSI / Intranet mediante el que se conectará el usuario, esto aparece en la figura 3.14

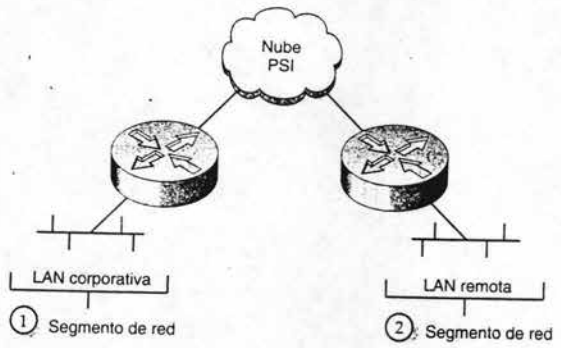


Fig. 3.15 Tres segmentos de red en la conexión remota de una Intranet.

La figura 3.15 ayuda a ordenar estas direcciones. A la LAN local del usuario y al enrutador que se está configurado usando Fast Step. Se le suele asignar un bloque de direcciones IP. El ejemplo de la figura 5.12 tiene un bloque de 254 direcciones emitidas para la red interna del usuario. El PSI o la Intranet corporativa tiene una dirección IP para identificar su segmento de red y una máscara de subred para dicha dirección IP, 255.255.255.248, que permite hasta seis posibles direcciones de equipo dentro de dicha subred.

Si lo que quiere es conectarse a una Intranet corporativa, entra en juego un tercer segmento de red: El segmento de red principal de la organización, que es la parte izquierda de la figura 3.15, para el usuario que está configurando el enrutador, la nube de red de la parte central es el mismo servicio independientemente que si la conexión se realiza a través de una red corporativa privada o a través de un PSI y sólo es posible llegar hasta el segmento de red corporativa del lado izquierdo pasado a través de un cortafuego.

En la última parte de la configuración, Fast Step permite completar el proceso de configuración del enrutador utilizando una de las siguientes opciones:

- Cargando el archivo configuración en el Enrutador.
- Haciendo una copia independiente del archivo configuración.

Si el usuario opta por realizar una copia independiente, está claro que debe de darle nombre el archivo. Puede aguardar el archivo en formato CEG de Fast Step para usarlo en otros enrutadores o guardarlo en un formato de comandos del IOS para usarlo como una plantilla a partir de la que crear archivos configuración algo diferentes para otros enrutadores.

La serie de cuadros de diálogos de Fast Step solicita que el usuario proporcione toda la información necesaria para configurar una conexión punto a punto entre una PC particular o una oficina pequeña y un PSI. Y eso es bueno porque, lo quiera o no, la configuración de las redes puede ser bastante complicada. Pero comparado con Config Maker, si se usan solicitudes es más fácil cometer errores y omisiones. Esto se debe en gran parte a que el trabajo de Fast Step no es el Config Maker.

La extensa modificación de entradas es el punto fuerte de Fast Step. Esto ayuda al usuario a encontrar los errores a medida que suceden. Si el usuario intenta escribir algo ilegal, aparecerá un punto de exclamación a la derecha del campo, así como un mensaje de error en el cuadro de solicitud. Las modificaciones pueden ser buenas o no. Por ejemplo, si intenta introducir una contraseña PPP incorrecta, el cuadro de solicitud le avisa de que, no cumple las reglas aceptadas, y si no supiera cuales son, pulse el botón Help y obtendrá la respuesta, la contraseña es una contraseña de inicio que le proporciona su proveedor de servicio a Internet o su administrador de red, cuando todo lo que en realidad necesitaba saber son las reglas sintácticas. El subsistema de ayuda Fast Step es generalmente bueno, pero a veces es poco claro.

Sin embargo, con las abundantes solicitudes y posibilidades de Fast Step, y con un pequeño esfuerzo, un principiante puede configurar a Internet un enrutador de la gama baja.

Tema 4 Problemas Típicos en Las Redes Cisco

4.1 Introducción

Mantener una red en funcionamiento es un trabajo de tiempo completo, como vimos anteriormente, los problemas aparecen con tanta frecuencia que la industria ha inventado los protocolos de enrutamiento para solucionar estos problemas automáticamente sin esperar la intervención del administrador. Y funcionan muy bien, al menos con problemas que se pueden tratar con desvío a una ruta.

Para que una red funcione de verdad, todos sus dispositivos deben funcionar correctamente el mayor tiempo posible.

Después de todo, ofrecer un ancho de banda aprovechable a los usuarios en circunstancias normales es ya difícil, y sin tener un segmento LAN fuera de servicio o un enrutador a media capacidad, es aun más difícil.

Por este motivo, una gran parte del tiempo del personal de una red se emplea en solucionar problemas.

Los problemas varían desde un usuario incapaz de accesar a un servicio hasta todo un segmento LAN caído.

Solucionar problemas no es sólo una cuestión de buscar y arreglar piezas rotas; la mayor parte se dedica a corregir cuellos de botellas en el funcionamiento de una red.

Cuando surge un problema, el administrador de la red suele desconocer que dispositivo lo provoca. Una vez identificado el dispositivo problemático hay que diagnosticar la posible solución y tomar decisiones.

Hay que adoptar una estrategia metódica para solucionar el problema; de otro modo, se puede perder mucho tiempo intentando imaginar la causa del problema.

La persona que se dedica a solucionar problemas debe reconocer los síntomas, asociarlos con un conjunto de causas posibles y después ir reduciendo la lista hasta identificar finalmente la causa.

A partir de aquí, debe desarrollar e implementar un plan de acción adecuado. A esto se le llama solucionar estratégicamente un problema.

En este tema veremos como solucionar problemas para distintas configuraciones Cisco, analizando varios escenarios con situaciones reales.

Por simplicidad, supondremos que IP es el protocolo de red y que el equipo funciona con Microsoft de Windows. Aunque pueda variar la terminología, los problemas de red son casi siempre los mismos, exceptuando el protocolo o el entorno de los equipos. También restringiremos los ejemplos en solucionar problemas de los enrutadores, que es donde se presenta la mayoría de las fallas.

4.2 Secuencia de solución

4.2.1 Comandos principales para la solución

En redes, el origen de los problemas procede de fallos en dispositivos hardware o de problemas de configuración. La localización de la mayoría de los problemas se puede realizar de forma remota y, hasta cierto punto, se puede diagnosticar los problemas e incluso solucionar de forma remota, pero para ello es necesario que el hardware todavía funcione. Por remoto, nos referimos a no tener que acercarnos, mirar o tocar el dispositivo; no nos referimos necesariamente a estar geográficamente distante. Por ejemplo, si la red de campo de una organización sufre un problema, los administradores de red normalmente realizan la mayor parte de la solución del problema sin abandonar su lugar de trabajo.

En entornos de Cisco, el trabajo remoto se puede realizar a través de una consola de administración de red o iniciando una sesión directamente mediante Telnet en el entorno de línea de comandos del dispositivo. De entrada y de salida IOS como se ha dicho, las consolas NMS de Cisco, usan interfases gráficas para operar indirectamente con comandos del IOS dentro del dispositivo remoto. De este modo, la mayoría de las actuaciones reales en solución de problemas tienen lugar dentro del entorno IOS del dispositivo. A continuación se muestran los principales comandos IOS necesarios (ping, trace y show) para llevar a cabo la mayoría de las tareas de solución de problemas:

- Ping. Indica si los paquetes (ecos) alcanzan el destino y vuelven. Por ejemplo si escribimos ping 10.1.1.1, IOS mostrará el porcentaje de paquetes devueltos desde la interfaz 10.1.1.1.

- Trace. Informa la ruta actual que se usa hacia un destino, por ejemplo, si escribimos trace IP 10.1.1.1, IOS muestra una lista con todos los saltos que hace el mensaje para alcanzar la interfaz destino 10.1.1.1.

- Show. Informa de la configuración y estado de los dispositivos y redes. Por ejemplo, el comando Show Memory muestra la cantidad de memoria asignada a cada dirección de red y cuanta hay libre.

El origen de los problemas puede estar en cada dispositivo o medio de red (cableado, conectores, etc.) incluso si el problema está en un cable, la forma de llegar a este es mediante el IOS. Los comandos ping y trace se usan para localizar problemas. Si el dispositivo todavía funciona, los comandos show y debug se pueden usar para diagnosticarlos. Las reparaciones efectivas se realizan sustituyendo el hardware o su configuración. El comando debug es similar a show, con la excepción de que informa más detalladamente de las operaciones del dispositivo por lo que sí se usa debug se puede alentar el equipo.

4.2.2 Método de solución

Los problemas suelen llegar a la mesa del administrador de la mano del usuario, quien quiere saber por qué no puede accesar a un servicio dentro de la red de la organización, o por qué es tan pobre el rendimiento. El origen y naturaleza de la queja son buenos indicadores de la causa del problema. Muchas veces el administrador sabe inmediatamente lo que funciona mal y cómo arreglarlo. Pero frecuentemente hay que iniciar una investigación para deducir que dispositivo es la causa del problema, cual es la causa y cual es la mejor forma de solucionarlo. El administrador de red debe resolver estas preguntas mediante estrategias de solución de problemas como las que siguen:

- ¿Cuales son los síntomas? Normalmente molesta a los usuarios no poder tener acceso a un destino. Conociendo los extremos de un problema de red, las direcciones de origen y destino, tenemos la información necesaria en la mayoría de las situaciones de solución de problemas.

- ¿Dónde comienzo a buscar? ¿Responde el planteamiento a un modelo conocido que sugiera las posibles causas? Por ejemplo, si un servidor no responde a solicitudes de servicio de un cliente, podría haber un problema en el servidor o en el mismo cliente. Si el servidor responde correctamente a otros clientes, entonces podría ser el dispositivo del cliente. Si no es eso, entonces el problema puede estar en algún lugar entre ambos.

- ¿Por dónde empezar? Hay una regla básica que reduce la lista de posibles causas de un cierto tipo de síntomas. El administrador debe determinar primero la causa más probables. Por ejemplo, si el acceso a un servidor es mediante un enlace WAN y parece que la conexión telefónica de los usuarios es lenta, el enlace podría estar funcionando mal, el uso puede ser elevado, puede faltarle memoria al búfer de la interfaz del enrutador que da servicio al enlace o puede que los equipos estén mal configurados. Una de estas causas posibles puede explicarse en el 95 % de los casos.

- ¿Cuál es el plan de acción? Localizar la causa concreta de un problema en un dispositivo defectuoso significa enfrentarnos a una variable en cada momento, por ejemplo, no tendría sentido sustituir todos los módulos de interfaz de red en un enrutador antes de volver a arrancar. Esto resuelve el problema, pero no define la fuente exacta o incluso la solución. En términos científicos se trata de cambiar una variable cada vez. La mejor forma es tomar referencias e ir cambiando variables una en una. De está forma que se pueda reducir el problema, validar la solución como la apropiada y archivar la causa del problema como referencia para el futuro.

La mayoría de los problemas de red se manifiestan por una reducción importante del rendimiento o como mensajes de tiempo de espera, como destino desconocido. A veces el problema es extenso; otras veces se limita a un segmento LAN, o incluso, a un equipo en concreto. Por lo cual veremos algunos problemas típicos y sus posibles causas. La tabla 4.1 muestra los problemas relacionados con la conectividad del equipo, estos pueden ser PC's pero no necesariamente.

Síntomas	**Posibles causas**
El equipo no puede accesar a la red más allá del segmento LAN local.	Configuraciones erróneas en los dispositivos del equipo, como una dirección IP predeterminada defectuosa o una submáscara de red errónea. Esto significa que el enrutador no funciona correctamente.
El equipo no puede accesar a ciertos servicios más allá del segmento LAN local.	Lista de acceso extendida mal configurada en el enrutador situado entre el equipo y el servidor. El enrutador esta mal configurado, si el sistema está más allá del sistema autónomo.

Tabla 4.1 Muestra síntomas y posibles causas de un mal acceso al equipo.

Por desgracia, la mayoría de los problemas de red no se limitan a un solo equipo. Si existe un problema en un enrutador o se extiende ampliamente por un área, pueden verse afectados muchos usuarios. La tabla 4.2 describe dos problemas de red habituales que son más extensos.

Síntomas	**Posibles causas**
La mayoría de los usuarios no pueden accesar a un servidor.	Especificación de acceso predeterminada mal configurada en el servidor remoto. La lista de acceso mal configurada en el servidor remoto.
No es posible realizar las conexiones a un área cuando la ruta está caída.	El protocolo de enrutamiento no converge dentro del dominio de enrutamiento. No se ha configurado ninguna interfaz del enrutador que maneje rutas alternativas con direcciones IP secundarias (direcciones discontinuas)

Tabla 4.2 Las posibles causas y soluciones de una mala configuración en equipos remotos.

Muchas veces, las redes y los servidores son accesibles, pero el rendimiento es demasiado bajo. La tabla 4.3 muestra algunos factores que pueden influir en el rendimiento de una red local. No se trata de los enlaces WAN. Estos se explican por separado porque las líneas serie conllevan otras tecnologías y problemas diferentes.

Síntomas	**Posibles causas**
Pobres respuestas del servidor; resulta difícil establecer y mantener las conexiones.	Los enlaces de red erróneos, son provocados normalmente por un funcionamiento erróneo del módulo de interfaz de red o medio del segmento LAN. Las listas de acceso no coinciden, en las redes de malla con múltiples rutas. El enlace congestionado, saturado es por demasiado tráfico. El equilibrio de carga pobremente puede estar mal configurado por las métricas del protocolo de enrutamiento.

Tabla 4.3 Problemas de rendimiento de una LAN de campo.

4.2.3 Problemas de configuración

Si un usuario tiene problemas para accesar a servicios y toda la red parece funcionar bien, un buen sitio para comenzar a buscar la causa del problema es el propio equipo de esa persona. Hay un par de cosas que pueden estar mal configuradas en el equipo del usuario:

1. Dirección IP incorrecta. La dirección IP o la máscara de subred pueden haberse perdido o ser incorrectas.

2. Pasarela predeterminada incorrecta. El enrutador de pasarela predeterminado puede estar mal configurado.

Cada equipo tiene una pasarela predeterminada y especificada en las configuraciones de la red del equipo. Una pasarela predeterminada es una interfaz en un enrutador local, que se usa para transmitir mensajes enviados por el equipo a las direcciones fuera de la LAN. Una pasarela predeterminada también de últimos recursos, hay que configurarla porque resulta lógica para un enrutador manejar la mayoría del tráfico que sale de un equipo con vistas a mantener la memoria caché con direcciones IP de destinos y las rutas hacia ellos. Un equipo debe tener al menos una pasarela y se suele configurar una segunda por motivos de redundancia en caso de que la primera se caiga.

Los parámetros de red mal configurados en un equipo de escritorio se atribuyen normalmente a errores cometidos por el usuario final. Recordemos que, en equipos con Windows 9X, al menos, cualquier usuario puede accesar fácilmente y modificar la configuración de red. Para verificar la configuración del equipo, haga click en el botón Inicio de la barra de menú y elija Configuración, Panel de control, Entorno de red para accesar a la ficha Configuración de red Windows 9X. En el cuadro de lista de la ficha de Red, haga doble click en el dispositivo que conecta el equipo con la red. En Windows NT, haga click en la ficha protocolos y, a continuación en propiedades de TCP/IP. Esto nos permitirá configurar la dirección IP y la pasarela predeterminada.

El componente será normalmente una tarjeta de interfaz de red (NIC) que se conecta a al LAN, como es el caso de la tarjeta de la red TCP/IP Ethernet para la PC que se resalta en la figura 4.1, si el equipo se conecta a la red mediante un acceso telefónico, debe seleccionar en su lugar el adaptador de acceso telefónico a redes.

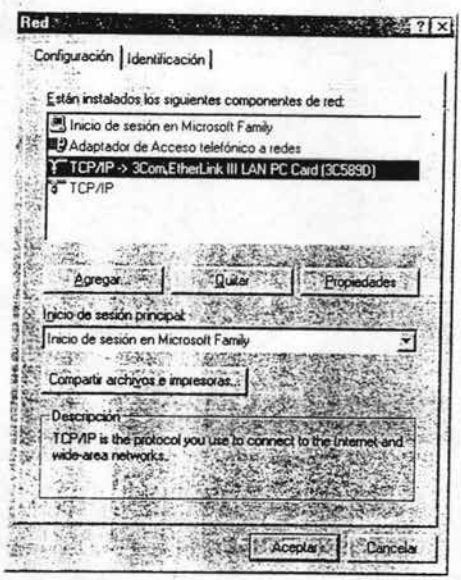
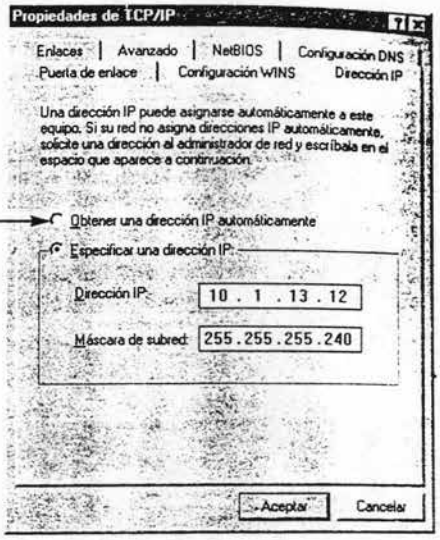


Fig. 4.1 Vea su tarjeta de interfaz de red para empezar la revisión a red.

Una vez seleccionada la NIC adecuada, comience por asegurar que el equipo se identifica a sí mismo correctamente en la red. Para hacerlo haga click en Red / Dirección IP para revisar las configuraciones en la ficha de direcciones IP. El ejemplo de figura 4.2 muestra una dirección IP y de subred definidas de forma estática.



Se utiliza para activar el direccionamiento dinámico, normalmente DHCP en entornos NT y NIS en entornos UNIX

Fig. 4.2 Revise la configuración IP de su equipo como la del enrutador deben coincidir.

Esta debe coincidir con las que hay en el archivo de configuración del enrutador que sirve de pasarela predeterminada. Si está activada la casilla, obtener una dirección IP automáticamente, la dirección IP del equipo la asigna de forma dinámica un servidor de protocolo dinámico de control de equipo (DHCP). Si de usa DHCP o un equivalente, es menos probable que se haya configurado erróneamente la información IP del equipo, pero la persona que se dedica a solucionar los problemas podría confirmar la situación en el servidor de direcciones.

A continuación, asegúrese de que la dirección IP declarada del equipo es la correcta, iniciando una sesión en el enrutador de pasarela e introduciendo un comando show arp. Se recomienda el protocolo de resolución de direcciones (ARP), como una utilidad que se asigna a las direcciones físicas de control de acceso al medio del dispositivo de capa 2 a su dirección IP de la capa 3 con vistas a manejar la etapa final de entrega entre el enrutador de pasarela y el equipo. La figura 4.3 muestra la tabla ARP en el archivo de configuración de nuestro enrutador de la pasarela de ejemplo. La línea sombreada muestra que la interfaz Ethernet tiene, de hacho, una dirección 10.1.13.12 en el archivo, como se indicó en la ficha dirección IP del equipo del equipo sólo identifica por la dirección MAC de su NIC.

Dirección MAC

```
vsigate#show arp
Protocol  address        Age (min)  Hardware Addr   Type   Interface
Internet  10.1.13.11           0   0050.0465.395c  ARPA   Ethernet1
Internet  10.1.11.1            12  0060.3eba.a6a0  SNAP   TokenRing0
Internet  10.1.13.12           9   00a0.c92a.4823  ARPA   Ethernet1
Internet  10.1.11.2            -   0006.f4c5.5f1d  SNAP   TokenRing0
Internet  10.1.11.3          190   0006.c1de.4ab9  SNAP   TokenRing0
Internet  10.1.12.3            -   0006.f4c5.5fdd  SNAP   TokenRing1
Internet  10.1.13.12          15   0050.04d7.1fa4  ARPA   Ethernet1
```

Fig. 4.3 La dirección IP del equipo debe coincidir con la del enrutador.

Otro posible problema con el equipo es la configuración de la propia pasarela predeterminada. Es decir, debemos asegurarnos que el equipo tiene configurada la dirección IP correcta como su enrutador de pasarela predeterminada. Para ello, haga click en la ficha de puerta de enlace dentro del cuadro de diálogo propiedades TCP/IP, como se muestra en la figura 4.4.

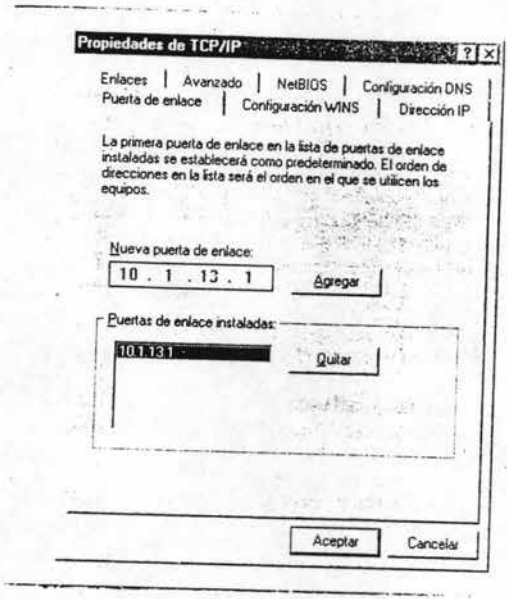


Fig. 4.4 Compruebe la configuración de la puerta de enlace.

La dirección IP de la pasarela predeterminada del equipo debe coincidir con la establecida para el módulo interfaz de red en el enrutador de pasarela. Para verificar esto, vaya al enrutador de pasarela y escriba el comando show interfaces, como se muestra aquí:

```
MyRouter # show interfaces
interface Ethernet1
ip accounting 10.1.13.1   255.255.255.240
ip accounting output-packets
ip nat inside
ip ospf priority 255
media-type 10BaseT
```

Como puede ver, nuestra interfaz Ethernet1 del ejemplo se direcciona por 10.1.13.1 como se declaró en la ficha puerta de enlace del equipo. Aquí podemos comprobar para asegurarnos que la máscara de subred declarada en el equipo coincide con la que hay en el enrutador de pasarela. La máscara 255.255.255.240 también es correcta porque coincide con la declarada en la ficha de dirección IP del equipo. Si esta alguna dirección mal se debe corregir, reiniciar el equipo, por otro lado si la configuración es correcta se debe ver el hardware del equipo.

4.3 Problemas de conectividad

La mayoría de los problemas de red están relacionados con la incapacidad de conectar con un equipo o servicio deseado. Los problemas de conectividad, también llamados problemas de enlace, se presentan de muchas formas: como agotamiento del tiempo de espera de una conexión http, el intento de conexión del terminal no obtiene respuesta, etc. Como se acaba de indicar, el punto de partida para la persona que se dedica a solucionar problemas consiste en asegurarse primero de que el equipo notifique el problema está bien configurado.

4.3.1 Configuración

Si la configuración de red del equipo es correcta, el siguiente paso es trabajar hacia el exterior del equipo y hacia el enrutador de pasarela. Esto se debe realizar incluso si el problema del equipo es una falla en la conexión a un servidor remoto. Mejor que salir afuera, lo mejor es comprobar primero el enlace entre el equipo y el enrutador de pasarela de la siguiente manera:

A) Usar el comando PING. La forma más sencilla de comprobar un enlace es usar el comando ping. Este comando envía paquetes ping a un dispositivo de red específico para ver si es posible el enlace. En terminología técnica, ping envía sus paquetes mediante el protocolo de transporte ICMP en lugar de medio UDP o TCP. En realidad envía varios paquetes, como vemos aquí:

```
MyRouter>>ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-bytes ICMP Echos to 10.1.1.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
MyRouter
```

Tanto los equipos como los dispositivos de red tiene comandos ping. El ejemplo anterior se ha tomado de un enrutador Cisco y el ping alcanzó con éxito sin su destino. Pero también podemos usar el comando ping disponible desde la línea de comandos del equipo. Estamos usando equipos Windows como ejemplo, pero otras plataformas, como las Mac's, las distintas plataformas UNIX, los IBM OS/400 y otras arquitecturas propietarias de servidor, también dispone del comando ping, además de otros comandos de red básicos, incluso en sus sistemas operativos.

Normalmente, la primera prueba ping desde un equipo es el enlace a sus enrutador de pasarela. En un equipo con Windows se puede comprobar haciendo click en el botón inicio en la barra de menú y eligiendo MS-DOS para tener acceso a la línea de comandos DOS. Compruebe después si el enrutador de pasarela responde introduciendo el comando ping, como muestra el siguiente extracto de código:

```
Microsoft® Windows 2000 (TM)
© Copyright 1985 – 1999 Microsoft Corp.

C:\>ping 10.1.13.1 with 32 bytes of data:

Request timed out
Request timed out
Request timed out

C:\>
```

El ejemplo anterior muestra como se envían cuatro paquetes ping al enrutador de pasarela, que falló en la respuesta. Esto indica a la persona que se dedica a solucionar problemas varias cosas:

- El NIC de la PC funciona correctamente; de lo contrario, MS-DOS hubiera devuelto un mensaje de error cuando la tarjeta hubiera fallado al responder al comando ping.

- El segmento de LAN Ethernet podría estar caído, un estado que se suele conocer con el nombre de problema de medios. El medio compartido, aparentemente, no funciona.

- El módulo interfaz de red del enrutador de pasarela podría estar defectuoso.

Si el equipo informa que funciona correctamente, la persona que se dedica a solucionar problemas debe pasar al exterior. Como se ha mencionado, la investigación debe empezar con el enlace al enrutador de pasarela.

B) Usar el comando Show Interfaces. Para comprobar si el problema lo provoca la interfase del enrutador de pasarela o el medio del segmento LAN, conecte al enrutador de pasarela y escriba el comando show interfaces para obtener el siguiente informe:

```
MyRouter>show interfaces
Ethernet is up, line protocol is down
Hardware is MyRouter, address is 0060.2fa3.fabd
(bia 0060.2fa3.fabd)
Internet address is 10.1.13.1/28
```

En el ejemplo anterior, el enrutador informa que el módulo de interfaz de la red Ethernet1 funciona y que el protocolo de línea no funciona. El término protocolo de línea denota tanto al cable del enrutador como al protocolo LAN que funciona sobre él. Cuando un protocolo de línea se dice que es incorrecto probablemente se quiere decir que el medio compartido del segmento LAN, un concentrador, un conmutador de acceso o un cable, está defectuoso. Desde aquí podemos comprobar físicamente el medio para identificar el problema hardware.

Otro inconveniente potencial podría ser que un administrador de red haya apagado la interfaz, la línea a ambos. Esto se hace rutinariamente mientras se repara, se actualiza o sustituye un componente de un equipo. Si comunica al IOS que una parte del equipo no funciona durante el mantenimiento se evita que el enrutador genere mensajes innecesarios. El ejemplo siguiente muestra el informe cuando un modulo de interfaz de red está desconectado por la administración de la red:

```
MyRouter>show interfaces
Ethernet1 is administratively down, line protocol is down
Hardware is MyRouter, address is 0060.2fa3.fabd
(bia 0060.2fa3.fabd)
Internet address is 10.1.13.1/28
```

Si una parte del equipo no funciona debido al diseño o a un mal funcionamiento, seguirá detenido el tráfico. De modo que es importante saber cuando se está revisando una parte del equipo para asegurarse de que hay una ruta alternativa disponible para manejar el tráfico.

Si tanto la interfaz del enrutador de la pasarela como el protocolo de línea están activos y funcionando bien, la causa del problema de conectividad reside en un enlace de otra red.

4.3.2 Problemas de conexión

Las cosas se hacen un poco más complicadas al salir del segmento LAN propio. Si el equipo no puede conectarse con el otro lado del enrutador de pasarela, hay inmediatamente dos orígenes potenciales y más tipos de problemas que comprobar. Lo que entendemos por orígenes potenciales de problemas ahora es que hay que considerar muchos más dispositivos hardware como causas potenciales del problema de conectividad. Lo que se entiende por tipos de problemas potenciales es, a partir de ahora y aparte del hardware: considere elementos como listas de acceso, protocolos de enrutamiento y otros factores.

Usar el comando Trace para determinar con precisión donde está el problema. En lugar de usar ping hacia el exterior del equipo a un enlace cada vez, la ruta entre el equipo y el servidor se puede analizar de una vez usando el comando "trace route". En nuestro equipo con Windows de ejemplo, hágalo haciendo click en el inicio, MS-DOS para tener acceso a los comandos DOS del equipo. Una vez logrado, escriba el comando tracert, la versión Microsoft del comando trace route.

El ejemplo de la figura 4.5 muestra la ruta seguida desde la PC hasta una dirección en Internet, que es un servidor interno de varios saltos. Puede elegir entre usar el nombre de dominio o la dirección IP. Cada línea en el comando tracert representa un salto a la ruta hacia el destino.

```
Microsoft(R) Windows 2000(TM)
(C) Copyright 1985-1999 Microsoft Corp.

C:\>tracert www.PayrollServer.AcmeEnterprises.com

Tracing route to www.PayrollServer.AcmeEnterprises.com [10.1.22.19]
over a maximum of 30 hops:

  1   <10 ms<N  <10 ms <N <10 ms<N 10.1.13.12
  2   <10 ms <N  12 ms   <10 ms <N10.1.5.3
  3    17 ms     20 ms    19 ms  10.1.17.22
  4    22 ms     19 ms    23 ms  10.1.31.2
  5   758 ms    831 ms   790 ms  10.1.49.12
  6    31 ms     40 ms    42 ms  10.1.22.19

Trace complete.

C:\>
```

Enrutador de pasarela del equipo

Una respuesta lenta indica que es probable que este enrutador sea el culpable

Fig. 4.5 Análisis de ruta para un enrutador que detiene el tráfico.

En las redes TCP/IP, los comandos de seguimiento de ruta funcionan enviando tres paquetes de rastreo a cada enrutador cada tres veces registra los intervalos de respuesta del eco. Igual que con el comando ping, los paquetes de rastreo se diferencian de los paquetes ping en que tienen un campo time-to-live que se utiliza para incrementar el flujo de salida del equipo poco a poco. El campo de un TTL provoca la eliminación del paquete cuando el contador indica cero. El comando de seguimiento de ruta usa el campo TTL, enviando el primer paquete de rastreo al enrutador más cercano con un TTL de 1, al siguiente enrutador con un TTL de 2, etc. Este proceso se repite hasta que se alcanza el equipo destino, si es que se puede conectar. El administrador de red puede poner un limite al número de saltos que puede realizar el rastreo, para interrumpir automáticamente el proceso si el destino muestra que no se puede conectar.

Los milisegundos son vitales y lo podemos ver en los enrutadores más cercanos cuando tienden a devolver un eco más rápidamente (10 ms o menos); a partir de 10 ms en adelante se hace lento, pero debemos ajustar la medición del tiempo de acuerdo a la cantidad de saltos que eliminó el enrutador. Como podemos observar, el enrutador de la línea sombreada de la figura 4.5 es el principal objetivo del mal servicio porque sus respuestas son lentas. La explicación más probable es que la interfaz del enrutador o el segmento LAN conectado a este sufra saturación o fallos hardware. El siguiente paso sería conectar a Telnet con el enrutador 10.1.49.12, si es posible, y diagnosticar el sistema, la interfaz de red involucrada, etc. Si no es posible conectar mediante Telnet, la persona que se dedica a solucionar problemas debe hacer uso de la consola o auxiliar, que por supuesto requiere que alguien este presente físicamente frente al dispositivo, a menos que se haya configurado previamente una solución de mantenimiento de acceso telefónico.

A veces, el seguimiento de una ruta localizará un nodo que paraliza todo el tráfico. Se muestra un ejemplo de esto en la figura 4.6 donde 10.1.49.12 emite ahora paquetes de seguimiento de lugar de simplemente devolverlos lamentablemente. Los enrutadores indican un intervalo nulo, porque no regresa nada y se ha insertado el mensaje " tiempo de espera solicitado" o request timed out. Se aprecia que esto no significa necesariamente que el enrutador este completamente bloqueado. Puede ser que sólo este bloqueada la interfaz de red o el segmento LAN que conecta el enrutador o la configuración no pueda responder a pings.

Si es posible conecte a Telnet con el enrutador a través de cualquiera otra de sus interfaces. Si esto no funciona, el siguiente paso depende de la cercanía del enrutador. Si esta cerca, nos desplazamos hasta él y conectamos a través de puerto de consola o auxiliar. Si esta lejos, debería contactar con una persona responsable para manejarlo e instruirlo en los pasos del sistema para futuros diagnósticos y servicios del equipo.

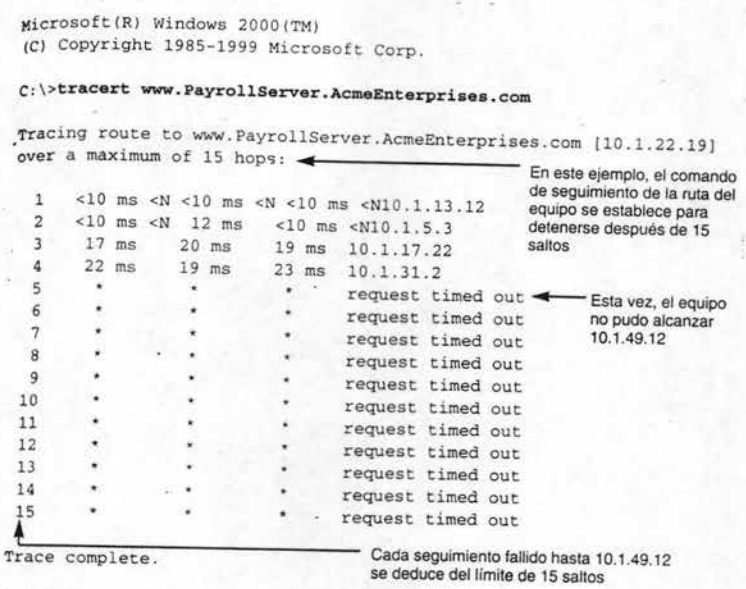


Fig. 4.6 Esto se encuentra cuando un enrutador detiene el tráfico.

Una vez identificado el módulo de interfaz de red que se piensa que esta dando problemas, la persona que se dedica a solucionar problemas debe diagnosticar la causa del problema. La mejor forma de hacerlo es ejecutar el comando show interfaces y repasar las últimas estadísticas de las operaciones de la interfaz. Recuerde, la información no sólo refleja el mismo módulo de interfaz, sino que también ofrece una amplia información de lo que sucede fuera de la red. Un ejemplo de informe de show interfaces se muestra en la figura 4.7.

Este informe es una copia de la interfaz en un momento concreto. Para analizar tendencias, la persona que se dedica a solucionar problemas debe ejecutar el comando show interfaces intermitentemente para buscar cambios. La interfaz se identifica por una dirección IP privada 10.1.49.12/28. Recuerde, normalmente, sólo los enrutadores en la frontera del sistema autónomo, cortafuegos, servidores web, servidores FTP, etc., usan direcciones de Internet públicas. La notación /28 permite a otros enrutadores saber que los segmentos LAN conectados a Remote Router se dividen en subredes usando la máscara de subred 255.255.255.240. La notación usa 28 porque la máscara 255.255.255.2400 tiene 28 bits disponibles para direccionamiento de red, al contrario de los equipos. Como se mencionó anteriormente, las subredes que no coinciden suelen causar problemas.

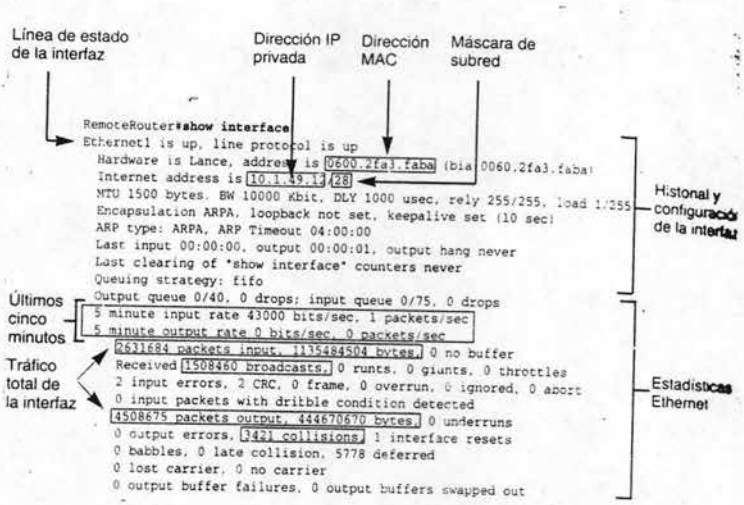


Fig. 4.7 El comando Show Interfaces que se dedica a solucionar problemas.

Lo primero que hay que mirar es la séptima línea del informe show interfaces que dice: last clearing of show interfaces counters never (nunca se ha puesto a cero el contador interfaz), resaltada en la figura 4.7. el ejemplo muestra que nadie ha puesto a cero los contadores del informe desde la última vez que el enrutador se reinició. El tiempo transcurrido desde que se tomaron los datos es muy importante porque la mayoría de los datos son números absolutos, no valores relativos como porcentajes. Es decir, cuando más tarda el IOS en compilar los totales, menos tarda en salir los datos. Por ejemplo, diez portadoras perdidas el mismo día es mucho, pero la misma cantidad en seis meses no lo es. Para ver cuando se realizo el último arranque, use el comando show versión, como se muestra aquí:

```
RemoteRouter>show version
Cisco Internetwork operating system software
IOS ( tm) 4500 software (C4500-IS-M), version 11..2(17)
Release software (fc1)
Copyright © 1986-1999 by Cisco system, inc.
Compiled Mon 04-Jan-99 18:18 by ashan
Image text-base: 0x600088A0, data-base: 0x60604000

ROM: system Bootstrap, version 5.3 (10) [tamb 10] ,
Release software (fci)
Bootflash: 4500 Bootstrap software (C4500-Boot-M), version 10.3 (10),
Release software (fci)

RemoteRouter uptime is 2 weeks, 3 days, 13 hours, 32 minutes
System restarted by power-on
```

Las dos últimas líneas del ejemplo anterior explican que el enrutador ha funcionado durante unas dos semanas y media. Saber esto permite a la persona que se dedica a solucionar problemas, considerar con más precisión si ciertos tipos de error son normales o desproporcionados.

La excepción a esta ventana de prueba son las dos líneas que aparecen en la parte central de la figura 4.7. Esto informa a la interfaz de la entrada y salida, los cinco minutos antes a la ejecución de la petición del informe. La persona que se dedica a solucionar problemas intenta comprender una tendencia en modelos de tráfico debe obtener periódicamente el informe show interfaces y observar sus valores.

Los datos difieren en lo que resulta excesivo. Por ejemplo, Ethernet vigila el control de acceso al medio por colisiones, de modo que es normal que ocurran en algún grado. El valor 3421 colisiones, en el ejemplo de la figura 4.7, es correcto para un período de dos semanas o similar, pero un valor de 50 000 indicará un ancho de banda congestionado. Los paquetes de difusión también son normales, porque realizan funciones positivas como alertar a los enrutadores de cambios en la topología. Hay mucha información por lo cual la persona que se dedica a al solución de problemas debe sacar la experiencia para detectar los datos importantes de los que solo son parte de la información general y redundante del sistema de comunicaciones.

Pero muchos resultados deberían tener un valor muy bajo o incluso cero idealmente. Por ejemplo, runts y glants son paquetes defectuosos provocados a menudo por un funcionamiento incorrecto de la tarjeta de interfaz de red. En un enlace WAN, los eventos de pérdida de portadora indican probablemente una línea sucia o con algún componente de telecomunicaciones defectuoso.

La tabla 4.4 define a los elementos sobre los que se informa cuando se usa el comando show interfaces. Conocer los elementos nos ayudará a comprender como se puede utilizar para diagnosticar el problema.

Datos	Explicación
Intervalo de cinco minutos de entrada o salida (five minutes rates input or output)	El promedio de bits y paquetes que pasan por la interfaz cada segundo, muestreados durante los últimos cinco minutos.
Cancelación (aborts)	Terminación repentina de los paquetes de transmisión de un mensaje.
Fallo del Búfer (buffer failers)	Paquetes desechados por falta de disponibilidad de memoria del búfer del enrutador.
Ancho de banda (BW)	El ancho de banda de la interfaz en Kbps se puede utilizar como una métrica de protocolo de enrutamiento.
Bytes.	Número total de bytes transmitidos a través de la interfaz.
Transiciones de portadora (carrier transitions)	Una portadora es una señal electromagnética modulada por transmisiones de datos sobre líneas en serie. Las transmisiones de portadora son eventos donde se interrumpe la señal, a menudo cuando se reinicia la NIC remota.
Colisiones (Collisions)	Número de mensajes retransmitidos debido a una colisión Ethernet.
Redundancia Cíclica (CRC).	Comprobación de redundancia cíclica, es una técnica común para detectar errores de transmisión. CRC funciona dividiendo el tamaño del contenido de una trampa por un número primo y comparando el resto con el que hay almacenado en la trama por el nodo emisor.
Retardo (DLY).	Demora del tiempo de respuesta de la interfaz, medio en µs, no en milisegundos (ms).

(continúa)

Datos	Explicación
Condiciones de exceso (dribble conditions)	Son tramas que son ligeramente largas, pero que las sigue procesando la interfaz.
Encapsulación (encapsulation)	Método de encapsulación asigna a una interfaz, si existe, el funcionamiento justo de los datos en el inicio del protocolo para direccionar los datos que de otra forma serían incompatibles a través de redes externas. Por ejemplo, Inter-switch link de Cisco ISL; que es el enlace entre conmutadores que encapsulan las tramas de muchos protocolos.
Error entrada o salida (error input or output)	Una condición en la que se descubre que una transmisión no coincide con lo que se esperaba, normalmente está relacionado con el tamaño de la trama o del paquete. Los errores se detectan usando varias técnicas, como CRC.
Trama (frame)	Número de paquetes que tienen un error de CRC y un tamaño de trama parcial. Suele indicar que el dispositivo Ethernet funciona incorrectamente.
Gigantes (giants)	Paquete mayor que el tamaño del paquete máximo que permite la tecnología, 1.518 bytes o más en las redes Ethernet, todos los paquetes gigantes se desechan.
Ignorados (ignored)	Número de paquetes desechados por la interfaz por la falta de búfer de la interfaz con la memoria búfer del enrutador.
Reinicio de la interfaz (interface reset)	Cuando la interfaz se deshace de todos los paquetes y comienza con uno nuevo. El reinicio suele ocurrir cuando el nodo emisor tarda demasiado en transmitir los paquetes.
Mensajes de supervivencia (keepalive)	Mensajes enviados por un dispositivo de red a otro para notificarle que el circuito virtual entre ellos sigue activo.

(continúa)

Datos	Explicación
Ultima entrada o salida (last input or output)	Horas, minutos y segundos desde que la interfaz transmitió o recibió con éxito el último paquete. Es una buena herramienta para determinar cuando ha comenzado el problema.
Carga (load)	Carga de la interfaz como una fracción del número 255. por ejemplo 64/255 representa un 25% de la carga. Se puede utilizar este contador como una métrica del protocolo de enrutamiento.
Ciclo invertido (loopback)	Si se ha activado el ciclo invertido. El loopback es donde se envían las señales desde la interfaz y, luego, se devuelven a ellas desde algún punto de la ruta de comunicación; se utiliza para probar el uso del enlace.
Unidad de Transmisión (MTU).	Unidad de transmisión máxima para que los paquetes que pasan a través de la interfaz, expresado en bytes.
Bloqueo de salida (output hang)	Tiempo transcurrido desde el último reinicio de la interfaz. Toma su nombre del hecho de que la interfaz se bloquea porque la transmisión tarda demasiado tiempo.
Saturación (Overruns)	Número de veces que la interfaz del enrutador satura el nodo receptor enviando más paquetes de los que se puede manejar el búfer del nodo. Toma su nombre del hecho de que la interfaz del enrutador satura al emisor.
Colas de entradas y salidas (queues of input and output)	Número de paquetes en la cola que van a continuación de la barra invertida es el tamaño máximo de la cola.

(continúa)

Datos	explicación
Estrategias de encolamiento (queuing strategy)	Primero en entrar y primero en salir (FIFO) first in first out, que significa que el enrutador maneja paquetes en ese orden. Ultimo en entrar primero en salir (LIFO) last in first out, este último es la estrategia predeterminada.
Confianza (rely)	Fiabilidad de la interfaz como una fracción del número 255. Por ejemplo, 255/255 equivale al 100% de fiabilidad. Se puede utilizar este contador como una métrica del protocolo de enrutamiento.
Diminutos (runts)	Paquetes menor que el tamaño del paquete mínimo que permite la tecnología, de 64 bytes o menos en las redes Ethernet. Todos los paquetes diminutos se desechan.
Aceleradores (throttles)	Número de veces que una interfaz avisa a una NIC emisora que esta siendo saturada por los paquetes que se envían y para reducir el ritmo de envío. Toma su nombre del hecho de que la interfaz pregunta a la NIC que se desacelera.
Agotamientos (underruns)	Número de veces que el nodo emisor satura la interfaz enviando más paquetes de los que puede manejar el búfer. Toma su nombre del hecho de que la interfaz del enrutador agota al enrutador.

Tabla 4.4 Definición de datos de Ethernet.

Una vez que hemos presentado los distintos datos que recopila el informe de show interfaces, pasaremos a revisar como interpretarlas. La figura 4.8 muestra la parte de los datos Ethernet del informe, esta vez con algunas de las variables más importantes resaltantes. Estas son las primeras variables que un administrador de red con experiencia podrá resolver el problema.

Muy a menudo los problemas de conectividad los provoca algún tipo de configuración de Ethernet pero que no afecte a una parte del equipo. Dependiendo del valor de los datos de Ethernet que se haya configurado, la interfaz podría estar saturada de tráfico entrante, tener configurado una tamaño de cola insuficiente, puede tener insufiente memoria de búfer o que no coincida con la velocidad de la entrada que envía la red.

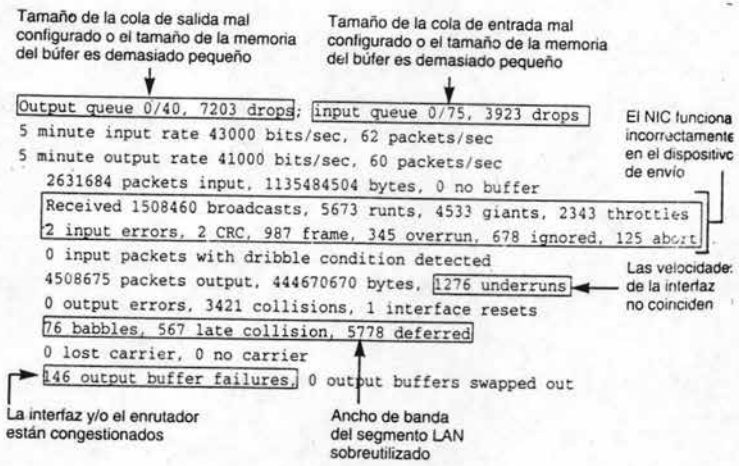


Fig. 4.8 Cada elemento de interfaz tiene razones convincentes para un análisis.

Comprobar las listas de acceso para verificar que se han configurado de forma adecuada, el ejemplo típico de un dispositivo defectuoso, incluso aunque su hardware funcione bien, es la lista de acceso que algunas veces esta mal configurada. Recordemos que las listas de acceso se usan para limitar el tráfico que puede pasar por la interfaz de un enrutador y, como consecuencia, recortar el acceso al segmento LAN conectado a este. Las listas de acceso básicas consigue esto examinando el origen y la dirección IP destino, una forma de controlar quien puede ir y donde. De hecho, las listas de acceso son la forma más clásica de la seguridad de redes, se utilizan como un equipo de cortafuegos internos. No todos los usos de listas de acceso tiene que ver con la seguridad, a veces se usan para dirigir el tráfico por ciertas rutas con el fin de canalizar el tráfico de la forma más equilibrada según el origen de la red.

El primer paso para detectar problemas en las listas de acceso es determinar si el enrutador o una interfaz de un enrutador, está configurado con lista de acceso. Para averiguar esto, conéctese con el enrutador y escriba el comando show access-list para ver si están configuradas todas las listas de acceso

```
RemoteRouter#show access-lists
Extended IP access list 100
Deny IP any host 206.107.120.17
Permit IP any (5308829 matches)
Extended IP access list 101
Access-list 101 permit tcp any host 209.98.208.33 established
Access-list 101 permit tcp udp host 209.98.98.98 host 209.98.208.59
Access-list 101 permit icmp any host 209.98.208.59 echo-reply
Access-list 101 permit tcp any host 209.98.208.59 eq smtp
Access-list 101 permit tcp any host 209.98.208.59 eq pop3
Access-list 101 permit tcp any host 209.98.208.59 eq 65
Access-list 101 permit tcp any host 209.98.208.59 eq telnet
Access-list 101 permit tcp host 209.98.208.34 host 209.98.208.59
Access-list 101 permit tcp any host 209.98.208.32.0.0.0.15 established
Access-list 101 permit icmp any 209.98.208.32.0.0.0.15 echo-reply
```

Si observamos bien al ejemplo anterior, la lista de acceso 100 se opone explícitamente al tráfico a una dirección IP concreta. Esto se hace frecuentemente para interrumpir el tráfico que sale de una conocida dirección IP no deseable, o algún otro tipo de enrutador que pudiera permitir a un intruso un ataque al enrutador final de la organización. La lista de acceso 101 es más sofisticad, con una serie de reglas de autorización para controlar que aplicaciones pueden usarse entre los equipos. El puerto IP de la aplicación se define detrás de cada modificador eq, como eq smtp para el correo electrónico o eq 65 para el servicio de datos TACAS+, algunos puertos se pueden identificar por número. También se puede mencionar que la lista de acceso 101 sólo tiene reglas de autorización. Esto es posible porque si no se permite explícitamente una petición de paquete para un servicio, será denegada por la regla "implicit deny" cuando llegue al final de la lista de acceso.

Puede ser que el problema lo provoque una regla de negación inadvertida o la carencia de regla de autorización. La persona que se dedica a solucionar problemas debe analizar la lista de acceso en busca de cualquier regla que pueda estar causando el problema. Por ejemplo, si una persona no puede conectarse con el servidor de correo, el administrador podría buscar oraciones que contengan eq smtp o la dirección IP del servidor de correo. El siguiente paso sería ir a la interfaz que conecta la red que experimenta el problema para comprobar si se utilizó comando access-group para incluirla en la lista de acceso que podría estar causando problemas. Para hacerlo, debemos entrar en modo privilegio EXEC y pasar a modo configurar interfaz que hace referencia a la interfaz en cuestión, como vemos aquí:

```
MyRouter>enable
Password:
Myrouter#write terminal
.
.
.
interface Ethernet1
ip address 10.1.13.1.255.255.255.240
ip access-group 101 in
ip access-group out
.
.
.
```

Si la lista de acceso problemática esta trabajando la desactivamos temporalmente para comprobar si el tráfico puede pasar por el enrutador sin ella. Hay dos listas de acceso en nuestro ejemplo, por tanto, desactivaremos las dos para ver si el problema lo provoca alguna de ellas. Por lo tanto desactive las listas de acceso en la interfaz de la siguiente manera:

```
MyRouter (config) # interface Ethernet1
MyRouter (config-if) # no ip access-group 100 in
MyRouter (config-if) # access-group 101 out
```

En caso de olvido, el modificador **in** al final de cada frase access-group configura la lista de acceso para aplicarse sólo a paquetes entrantes. Un modificador **out** haría lo contrario; la ausencia de un modificador utiliza a la lista de acceso tanto al tráfico entrante como al saliente.

Una vez desactivadas las listas de acceso, intentaremos conectar el equipo y servidor que no respondía. Si el tráfico fluye con las listas de acceso desactivadas, entonces hay una frase en alguna de las listas de acceso que probablemente causa el problema. El siguiente paso es ver que lista contiene el problema volviendo a activar una de las dos. La lista de acceso 101, con todas sus reglas, es la más sospechosa. Para comprobar si es así, vuelva a activarla con el siguiente comando:

```
MyRouter (config) # ip access-group 101 out
MyRouter (config-if) #
```

Ahora intente conectarse de nuevo con el servidor. Si aparece el problema habremos determinado que este reside en algún lugar de la lista de acceso 101.

Para depurar la lista de acceso debemos repasarla minuciosamente para localizar la regla incorrecta. Podría ser una regla de negación colocada en algún sitio erróneo, pero también el problema podría ser un puerto TCP o UDP perdido dentro de una regla de autorización. Recuerde, cada regla de lista de acceso debe indicar a que protocolo de transporte IP se aplica: TCP, UDP o ICMP. Es muy frecuente, sin embargo, que los puertos de aplicación erróneos sean la fuente del problema, simplemente porque hay demasiados y las aplicaciones de red que se usan cambian muy a menudo. Por ejemplo, si los usuarios tienen problemas para conectarse con el servidor web hay que asegurarse de que el puerto http número 80 esta autorizado entre las direcciones del servidor y el equipo.

También es posible que el tráfico sé este denegando antes de llegar a la regla de autorización designada para permitir el paso. Recuerde que las listas de control de acceso se leen desde arriba hacia abajo hasta que se encuentra una coincidencia. Si este es el caso, el orden en el que se listan las reglas debe ajustarse poniendo en la parte superior las reglas de prioridad.

Redireccionar el tráfico de áreas congestionadas. Algunas veces se satura en un enrutador concreto. Esto puede ser el resultado de agregar nuevos equipos en esa área, la aparición de nuevas aplicaciones de red u otras causas. Cuando ocurra esto, accese al enrutador congestionado y escriba el comando show ip route para generar el siguiente informe:

```
MyRouter # show ip traffic
Ip  statistics:
  Rcvd: 7596385 total, 477543 local destination
        0 format errors, 0 checksum errors, 96 bad hop count
        0 unknown protocol, 1 not a gateway
        0 security failures, 0 bad options, 0 with options
  Opts: 0 end, 0 basic security, 0 loose source route
        0 timestamp, 0 extended security, 0 record route
        0 stream ID, 0 strict source route, 0 alert, 0 cipso
        0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcat:  53238 received, 280 sent
  Mcast: 205899 received, 521886 sent
  Sent:  738759 generated, 6113405 forwarded
         13355 encapsulation failed, 374852 no route
```

Además de informar del tráfico IP, el comando show ip traffic informa del tráfico generado por los protocolos de enrutamiento, solicitudes de traducción ARP e incluso errores de los paquetes. El informe también muestra los mensajes de difusión y multidifusión. Es un modo rápido de comprender la carga que soporta un enrutador y que opciones hay para aligerarla.

Por ejemplo, si el tráfico de difusión parece excesivo podríamos tratar de ajustar las restricciones en las listas de acceso que rigen los enrutadores más cercanos. Pero, si notamos que todo o casi todo el tráfico es legítimo, también hay que analizar el tráfico que afecta a los enrutadores más cercanos. Si hay desigualdad entre las cargas que soportan los enrutadores de capacidad similar, tal vez el equilibrio de carga este regulado. En la mayoría de los casos, esto tiene más sentido que admitir hardware más sofisticado.

Una forma de equilibrar la carga de tráfico entre enrutadores es iniciar una sesión en el enrutador congestionado y entrar en modo config-router, llamando a los protocolos de enrutamiento; luego se establecen métricas de distancia individuales en cada enrutador para dirigir el tráfico lejos del enrutador congestionado hacia otros enrutadores menos congestionados, como se ve en el ejemplo que sigue de IGRP:

```
MyRouter (config) # router igrp 3
MyRouter (config-router) # distance 255
MyRouter (config-router) # distance 120  10.1.13.1  0.0.0.255
MyRouter (config-router) # distance 80   10.1.14.1  0.0.0.3
MyRouter (config-router) #
```

Como se vio anteriormente los protocolos de enrutamiento eligen las mejores rutas basándose en los costos analizados. Los comandos distance del extracto de código anterior, establecen rutas hacia 10.1.13.1 con un costo más elevado que hacia 10.1.14.1 porque aumenta su distancia administrativa con relación a otros enrutadores.

Es decir, la oración router igrp3 coloca al enrutador en modo config-router con vistas a establecer parámetros para el comportamiento del enrutador dentro del número 3 del dominio del protocolo de enrutamiento IGRP. La oración distance 255, al no tener dirección IP, indica al enrutador que ignore todas las actualizaciones de enrutamiento de los enrutadores para los que no se haya establecido distancias administrativas de forma explícita. A continuación, la oración distance 120 10.1.12.1 0.0.0.255 establece la métrica de distancia del enrutador congestionado en 120. Los protocolos de enrutamiento de Cisco utilizan máscaras inversas, de ahí el modificador 0.0.0.255. Por último, la oración distance 80 10.1.14.1 0.0.0.3 establece la métrica de distancia del enrutador más cercano en 80, estimulando su uso un tercio más que el enrutador congestionado. Esta nueva métrica de enrutamiento alejará automáticamente desde 10.1.13.1hacia 10.1.14.1.

4.4 Problemas de enlace

¿Cómo solucionar los problemas de enlace de una red WAN? Bueno esto implica usar un conjunto de herramientas algo distintas. Esto se debe a que la mayoría de las conexiones a enlaces WAN deben realizarse a través de una serie de líneas. Recuerde que una línea serie conecta una unidad CSU/DSU (módem) a un enrutador. Las redes telefónicas no transmiten señales usando una tecnología de red de capa de enlace de datos capa 2 como Ethernet. Los enrutadores no son conmutadores telefónicos, de modo que es necesario realizar transiciones entre las dos tecnologías de alguna forma. La interfaz DSU/DSU a una línea serie da señales comprensibles para el enrutador.

Los enlaces en serie tienen una importancia indiscutible porque extienden las redes más allá del campo de oficina hasta emplazamientos remotos. Un enlace remoto de cualquier tamaño requiere el uso de un circuito telefónico digital de algún tipo, que puede variar desde una línea T1 fraccionada hasta una T3 (DS3) completa. Como se muestra en la siguiente figura 4.9.

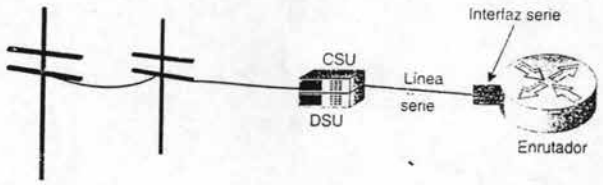


Fig. 4.9 Ruta para realizar un enlace.

Aunque una línea en serie sea sólo un simple hilo de cable, ofrece una ventana a través de la que se puede diagnosticar todo el enlace WAN. En otras palabras, no sólo podemos analizar la línea serie y sus interfaces, sino que observa el tráfico que transporta, también podemos diagnosticar todo el circuito telefónico digital, hasta cierto punto, lo que ocurre en el extremo remoto de enlace.

4.4.1 El comando show interfaces serial

Cisco ofrece una herramienta especial para solucionar problemas de enlace en serie con el comando SIS. Es prácticamente igual que el comando normal show interfaces, pero con algunas diferencias importantes, como se muestra en la figura 4.10.

```
RemoteRouter>show interface serial0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.1.14.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 217/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/390 (size/max/drops); Total output drops: 54920
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/12921 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 39000 bits/sec, 52 packets/sec
  5 minute output rate 36000 bits/sec, 48 packets/sec
     26405 packets input, 1977458 bytes, 0 no buffer
     Received 12385 broadcasts, 0 runts, 0 giants, 0 throttles
     1294 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 397 abort
     4783008 packets output, 2510565558 bytes, 0 underruns
     0 output errors, 0 collisions, 9172 interface resets
     0 output buffer failures, 0 output buffers swapped out
     12 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Fig. 4.10 Centro de atención para solucionar problemas de una línea en serie.

Una diferencia con los enlaces serie es que debe usarse encapsulación sobre circuitos telefónicos digitales cerrados. El protocolo de encapsulación, Control de Enlace de Datos de Alto Nivel HDLC (High level data link control), indicado en el recuadro superior de la figura 4.10. Se hace necesaria la encapsulación para mantener los paquetes Ethernet por encima del enlace telefónico digital. Es posible que a veces se desactive sin querer la encapsulación, por lo que debería activar el campo de encapsulación.

Otra diferencia es en las sesiones que aparecen en el informe de show interfaces serial. Los enlaces WAN tiene menos ancho de banda que los medios compartidos locales. A estar al tanto, de un circuito T1 (DS1) tiene una tasa de transferencia de 1.544 Mbps y un T3 (DS3) de 45 Mbps.

La mayoría de las empresas usan T1 o T3 fraccionadas, adquiriendo canales dentro de ellas (T1 tiene 24 canales y T3 tiene 672 canales). En consecuencia, el ancho de banda de una red WAN es limitada en comparación, digamos, con un segmento LAN y, a veces, una sesión de usuario particular utiliza más de lo que le corresponde. Por consiguiente, cuando busquemos errores en un enlace WAN, resulta útil saber cuantas conversaciones se están realizando. Por si acaso se lo pregunta, el campo Reserved Conversation está relacionado con el protocolo de reserva de recursos (RSVP) que es un estándar industrial incipiente está diseñado para utilizarse en herramientas QoS, con el fin de garantizar la calidad del servicio.

El cuadro de la parte inferior de la figura 4.10 muestra una tercera diferencia en el informe de show interfaces serial. Estos cinco campos son lo mismo que las luces parpadeantes de los módem's externos. Por ejemplo, la terminal de datos preparada (DTR), es un circuito EIA/TIA-232 de la familia RS-232, que se activa para notificar al equipo de comunicaciones, situado al otro extremo, que el equipo esta listo para recibir y enviar datos. La detección de portadora de datos (DCD) es importante porque detecta la señal portadora actual.

Los cinco circuitos de módem se incluyen en el informe de show interfaces serial para solucionar errores de enlace serie que funciona con líneas analógicas / módem en vez de líneas digitales.

Los enlaces serie son distintos por naturaleza de los segmentos LAN, por eso diagnosticarlos sigue un planteamiento. Algunas cosas que se dan por obvio en los enlaces de segmento LAN a menudo son la causa de problemas de rendimiento o incluso, de fallo en enlaces serie. La figura 4.11 resaltan los elementos que busca primero la persona que se dedica a solucionar los problemas cuando se inicia la inspección de una interfaz serie.

Como se puede ver, las soluciones de los problemas en enlaces acentúan la búsqueda de errores y la actividad de las líneas. Es natural, pues la zona media de un enlace WAN, en el circuito telefónico, es prácticamente invisible para un equipo de red.

Si observamos bien la figura 4.11 vemos el caso en el que el tráfico entrante parece ir bien, pero pierden muchos paquetes de salida. Suponiendo que la línea serie se está sobreutilizando, esta funcionando cerca del 80% del ancho de banda disponible, podemos concluir que la causa de las pérdidas es el sobreuso y no un fallo del hardware en el enlace.

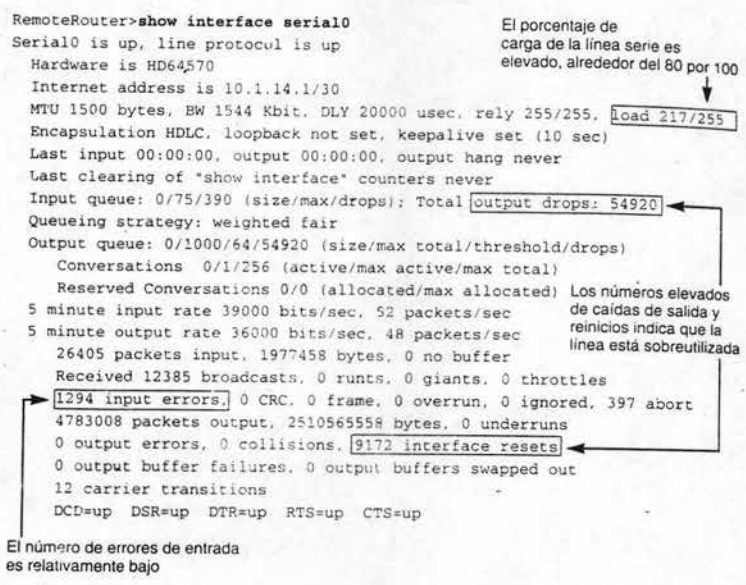


Fig. 4.11 Campos que dan la solución de problemas de líneas serie.

4.4.2 Problemas en la entrada de la línea

Para solucionar los problemas de errores de entrada de líneas serie, las cuales son las causas más frecuentes de problemas en líneas serie son los errores de entrada, en otras palabras, los datos provienen de un sitio remoto. La tabla 4.5 muestra las posibles causas de error de entrada en líneas serie con algunas sugerencias de actuación.

Síntomas de error de entrada	Posibles causas y acciones recomendadas
Errores de entrada junto con errores de trama o CRC	Causa: Una línea sucia, donde el ruido eléctrico interfiere con la señal de datos. El cable serie sobrepasa la longitud máxima especificada por el tipo de circuito telefónico. El cable serie no está blindado. El propio circuito telefónico puede que funcione incorrectamente. Acciones: Reducir la longitud del cable. Instalar cable blindado. Comprobar la línea telefónica con un analizador de señales. Acelerar el reloj en la línea donde la señal de datos de las posiciones de los intervalos de referencia o disminuir el reloj donde los relojes de los dispositivos se han ajustado de forma distinta. Acciones: Asegúrese de que todos los dispositivos están configurados para que utilicen un reloj de línea común.
Errores de entrada junto con cancelaciones	Causa: La transferencia de un paquete terminado en medio de la transmisión. Suele estar provocado por el reinicio de la interfaz del enrutador que se analiza. También se puede deber por el reinicio del enrutador remoto, a un circuito telefónico defectuoso o a un CSU/DSU defectuoso. Acción: Comprobar el hardware local, luego, el hardware remoto. Remplazar el equipo que falla.

Tabla 4.5 Posibles causas de errores de entrada en líneas serie.

Para solucionar los problemas de errores de salida de líneas serie. Otro indicio de problema de línea serie es una tendencia al aumento de paquetes perdidos en la interfaz. Una pérdida sucede cuando se están procesando demasiados paquetes en el sistema y no hay suficiente memoria en el búfer para manejar el paquete. Esto funciona tanto para pérdidas de entradas como de salidas, según se describe en la tabla 4.6.

Las pérdidas que ocurren en una dirección, pero no en la contraria, (entrada frente a la salida), puede indicar a la persona que soluciona problemas el origen del error, si ocurre en ambas direcciones, el enrutador o su interfaz serie es probablemente la parte con el problema.

Sistemas de pérdida de paquetes	Posibles causas y acciones recomendadas
Aumento de la pérdida de paquetes de entrada.	Causa: La caída de la entrada suele ocurrir cuando el tráfico se enruta desde una interfaz local, Ethernet, Token Ring y FDDI, que es más rápida que la interfaz serie. El problema suele suceder durante periodos de tráfico elevado. Acciones: Aumentar el tamaño de la cola mantenida de entrada de la interfaz en el archivo de configuración del enrutador.
Aumento de la pérdida de paquetes de salida.	Causas: Las caídas en la salida suceden cuando no hay disponible un posible búfer del sistema, cuando el enrutador intenta entregar el paquete al búfer de transmisión en momentos de tráfico elevado. Acciones: Aumentar el tamaño de la cola mantenida en la salida de la interfaz. Desactive la conmutación rápida. Implemente el encolamiento prioritario.

Tabla 4.6 Soluciones de errores de salida en líneas de serie.

Para solucionar los problemas de los enlaces en serie, como la mayoría usa módems sabemos que a veces puede fallar, o incluso puede perder la conexión. Esto es valido para líneas serie, normalmente debido a reinicios de interfaz o transiciones de portadora, como se describe en la tabla 4.7.

Síntomas de error en la línea	Posibles causas y acciones recomendadas
Transición creciente de portadora	Causas: Interrupción en la señal portadora. Normalmente se debe al reinicio de las interfaces del extremo remoto del enlace. El reinicio puede provocarlo por causas externas, como tormentas eléctricas, alertas de uso excesivo de las líneas T1 o T3 o hardware defectuoso. Acciones: Utilice las herramientas de desarrollo o el analizador de señales para comprobar el hardware en ambos extremos. Luego, compruebe el hardware del enrutador. Reemplace el hardware que falla según sea necesario. No es necesario realizar ninguna acción si el problema se debe a una causa externa.
Reinicios crecientes de la interfaz	Causas: El reinicio de interfaz lo provocan los mensajes perdidos de supervivencia. Suele estar provocados por transiciones de portadoras, escasez de búfer o un problema con el hardware CSU/DSU. La coincidencia con un aumento de transiciones de portadora o errores de entrada indica un enlace defectuoso o hardware CSU/DSU defectuoso. Acciones: Utilice las herramientas de desarrollo o el analizador de señales para comprobar el hardware en ambos extremos. Contacte con el propietario de la línea alquilada si el hardware está bien.

Tabla 4.7 Solución de los problemas en los enlaces de serie.

Aunque no son segmentos LAN por sí mismos, los enlaces serie son parte integrante de las redes. No se olvide tenerlos en cuenta incluso cuando no se aprecia en un principio un problema con la línea serie. Por ejemplo, al evaluar los problemas de rendimiento, podría ser que un enlace defectuoso este desviando el flujo de tráfico a cualquier sitio dentro de la red.

4.5 Problemas con el equipo

4.5.1 Secuencia

Cuando se identifica la posible localización de un problema. El primer paso es examinar físicamente y probar el dispositivo sospechoso. Esto identificará la causa del problema en muchas situaciones problemáticas. Algunas veces el problema lo causa algo tan simple como un componente suelto; otras veces hay algo dañado de verdad.

Una vez identificado el dispositivo sospechoso hay que inspeccionarlo físicamente. Este es un procedimiento rutinario; incluso cuando un dispositivo sospechoso o con problemas está en un lugar remoto, se envía a una persona de confianza para hacer una inspección. Anteriormente se dijo que la mayoría de las tareas de resolución de problemas se realizan desde la mesa del administrador y esto es verdad. Prácticamente todas las tareas se realizan desde la PC del administrador o en una consola NMS. Sin embargo, no hay sustituto para examinar físicamente el dispositivo y ver lo que sucede. Las dos partes de inspeccionar un dispositivo son observar sus leds e inspeccionar los componentes del dispositivo.

Si el dispositivo todavía está conectado, lo primero que hay que hacer es interpretar sus leds, probablemente reconoceremos los leds como pequeñas luces en un dispositivo electrónico. Casi todos los dispositivos de red tienen leds para ayudar a solucionar problemas. La disposición de los leds depende del diseño del dispositivo:

- Los dispositivos de acceso con un banco de puertos en la parte frontal, con un cable de par trenzado conectado en cada puerto mediante una clavija RJ-45 como la de los teléfonos. Los productos desde el Fast Hub 400 de Cisco hasta el conmutador Catalyst 5000 coinciden con esta descripción. Hay normalmente un led por puerto.

- Enrutadores basados en la placa principal con segmentos LAN conectados en la parte posterior, normalmente mediante un cable de par trenzado, pero también cable de fibra óptica como vínculos ascendentes. El 4500 Router de Cisco cumple con esta descripción. Los leds en estos dispositivos están situados detrás de los paneles de cristal ahumado en la parte frontal de estos aparatos.

- Enrutadores y conmutadores de altas prestaciones de la configuración bus y tarjeta, de nuevo con redes conectadas en la parte trasera, con cables tanto de fibra óptica como de par trenzado. El 7500 Router de Cisco y el conmutador Catalyst 6000 encajan en esta descripción. Los leds de estos aparatos se encuentran tanto detrás de los paneles de cristal ahumado de la parte frontal como en las propias tarjetas en la parte posterior.

Los leds se llaman luces de actividad. Cada led de un dispositivo de acceso representa un equipo. Los leds de los enrutadores y conmutadores LAN representan segmentos LAN completos.

Los leds parpadean y cambian de color en función del estado del puerto. Verde significa correcto y naranja o rojo que el puerto se está activando. Si el puerto está caído, el led se oscurece. El led del puerto parpadea cuando pasan paquetes por él. Una práctica habitual es presionar Reset para ver lo que ocurre. Los leds se vuelven momentáneamente de color naranja o incluso rojo si notan un problema durante el proceso de encendido. Pueden volverse verdes, momentáneamente pero la condición temporal del error puede indicar un error de configuración que no es fatal.

La regla es que si un led esta verde, la línea es buena y el problema debe provenir de algún tipo de problema de configuración. Si la luz es naranja la línea esta trabajando pero funcionado mal. Sí el led esta apagado la línea esta caída.

4.5.2 Inspección física de los dispositivos

El siguiente paso es inspeccionar físicamente el propio dispositivo. Comience asegurándose de que el dispositivo esta bien conectado y a continuación, retire la cubierta de la parte superior del chasis del dispositivo e inspeccione el interior buscando lo siguiente:

- Conexiones sueltas. Busque cualquier tarjeta o módulo suelto. Vuelva a insertarla si estuviera suelta.

- Nueva tarjeta. Si sabemos que alguna tarjeta es nueva, insértela varias veces en su conexión. Las tarjetas nuevas son más proclives a la oxidación o a la acumulación de una capa de carbón en las conexiones del panel posterior.

- Partes quemadas o dañadas. Busque algo componente quemado como cables, cables de cinta o tarjetas. Asegúrese que el panel posterior este bien y compruebe que este bien. Inspecciones cuidadosamente los cables que salen de la fuente de alimentación. Busque también por si hubiera algún cable pelado.

- Interior del un dispositivo sucio. Si el dispositivo acumula suciedad y pelusa en el interior, apague el dispositivo y límpielo. Los dispositivos pueden acumular gran cantidad de sustancias extrañas del ambiente en entornos sucios y esto a veces puede afectar al funcionamiento.

Después de completar la inspección, trate de reiniciar el equipo para ver si el ciclo de encendido arregla el problema. Una precaución importante: no cambie nada en la configuración. Si lo hace antes de reiniciar puede ser mucho más difícil determinar el origen del problema más adelante; sólo agrega más variables al problema.

4.5.3 Prueba de reinicio

Si no se ha encontrado problemas importantes a la hora de inspeccionar el dispositivo, el siguiente paso es intentar una prueba de ciclo de encendido para ver como responde. El ciclo de encendido significa apagar un dispositivo y volverlo a encender, algo que probablemente se conoce como el remedio más común para Microsoft de Windows. Reiniciar los dispositivos pueden indicar mucho acerca del estado de un dispositivo y, en algunos casos, hace que desaparezca el problema.

Cuando reiniciamos, si la configuración en memoria no coincide con el hardware, pueden aparecer varios problemas. Los puertos se pueden colgar, pueden ocurrir errores de tiempo de espera del bus, etc. Si el dispositivo se reinicia y pide una contraseña, los circuitos y la memoria funcionan bien. La tabla 4.8 describe algunos de los síntomas más importantes y sus posibles causas.

Síntomas de reinicio	Posibles causas
No hay respuesta	La fuente de alimentación esta defectuosa, un fusible esta fundido, aislante defectuoso, interruptor de corriente defectuoso, panel posterior defectuoso.
No reinicia	Fuente de alimentación defectuosa o mal conectada, tarjeta de procesador defectuoso o mal instalada, tarjeta de memoria defectuosa, imagen del IOS defectuosa en NVRAM, cables cortados.
Reinicio constante o parcial	Procesador, control o tarjeta de interfaz defectuosa, panel posterior defectuoso, fuente de alimentación defectuosa microcódigo defectuoso.
No aparecen las tarjetas en la pantalla de inicio	Procesador, control o tarjeta de interfaz defectuosa, panel posterior defectuoso, tarjeta no conectadas en el panel posterior, fuentes de alimentación defectuosa.

Tabla 4.8 Problemas típicos de reinicio y sus posibles causas.

Recuerde, cada vez que nos enfrentemos a un problema, el objetivo es seguir el cable y rastrear el origen del problema hasta el fin.

Conclusiones

Cisco como una empresa enfocada al control y manejo de información a través de la red de Internet pone a la disposición de todo el mundo una gran cantidad de dispositivos, sin duda alguna el ROUTER o ENRUTADOR, es una de las herramientas más poderosas y seguras que cualquier empresa en materia de transmisión de datos pueden conseguir si desea estar presente en los primeros lugares de competitividad. Para ello Cisco ha desarrollado los Enrutadores conjugados con el hardware, software y una administración una red puede ser una ventaja para sus clientes y proveedores de servicio.

Esto implica hacer una revisión de los equipos más usados y sus posibles aplicaciones, estos equipos como los Enrutadores de gama baja, media y alta, conmutadores y sus variaciones hacen posible una red de Internet. La actual demanda de servicios que requieren las industrias no termina en la adquisición del mejor equipo y una buena administración, para continuar con una funcionalidad optima se requiere de una atención muy profesional del equipo por lo tanto Cisco ha implantado un sistema de certificación desde principiantes hasta ingenieros expertos en respuesta a las exigencias y requerimientos del mercado por esa razón Cisco capacita a sus ingenieros y la personal que lo desee para una constante profesionalización en los equipos, para mayor atención a los clientes, menor número de fallas que corregir, rapidez en respuesta de atención al cliente y confiabilidad son algunas de las razones por las que Cisco tiene estos programas de certificación.

Otro de los puntos más importantes para Cisco es lo referente a su sistema operativo que es el alma sus equipos para esto Cisco creó el sistema operativo IOS con el cual se pueden configurar los equipos según las necesidades del cliente, además de incluyen los protocolos de ruteo clave para administración de redes. Todo lo anterior no seria posible si no se contara con un buen sistema de seguridad por lo tanto cuidar toda la información que sin duda es muy valiosa se hace posible a través de cortafuegos, seguridad basada en el usuario y la seguridad basada en el tráfico. Como resultado de seguridad que se ha ido mejorando cada vez más se han desarrollado aplicaciones de lo anterior se puede mencionar configuraciones de redes como lo son Ethernet en toda sus versiones Token Ring y por supuesto ATM.

Una de las mejores formas de asegurar por varios años el buen desempeño de la red y la inversión considerable que se hace en ella, para esto se recomienda tomar decisiones con una visión a largo plazo de esto dependerá la confiabilidad, capacidad de transmisión y expansión para nuevas tecnologías que cada día son más poderosas por este motivo Cisco recomienda una serie de medidas adecuadas para implementar una red basada en sus productos. Para iniciar el diseño de una red debemos tener en cuenta los siguientes parámetros y características como son el rendimiento y la escalabilidad para nuevas implementaciones los pasos a realizar pueden ser los siguientes conocer bien los segmentos LAN su dominio y como operan en las distintas capas OSI y la forma de optimizar una arquitectura de red.

El método de diseño puede constar de tres capas las cuales pueden ser diferentes para cada proceso de transmisión, para el diseño el equilibrio de cargas y la redundancia son el principio del diseño por otra parte un buen diseño de malla incorpora lo anterior pero cabe señalar que el diseño que se ajusta a las necesidades reales y pensando en el futuro traerá mejores resultados por eso se tiene que observar la geografía y el tráfico ubicado en los nodos. Además la QoS es otro de los parámetros para tener siempre en cuenta, el flujo constante, bidireccional, asimétrico, origen del tráfico y sus características, grupos de usuarios de donde la información es muy abundante, las bases de datos. Esto también incluye la tecnología para la red, protocolos como el IP, redes de lógica y de campo las cuales incluyen sus propias características como son para campo hay una parte física donde se selecciona el hardware y el software y la red lógica lo forman tres elementos como el direccionamiento, IP, recepción y transmisión de datos

Con el vertiginoso crecimiento de las comunicaciones es muy importante conocer el comportamiento de nuestros equipos su funcionamiento así como sus límites sus procesos adicionales, sus medios de seguridad, programación o instalación de software, expansiones y como puede interactuar con otros equipos, por esta razón Cisco presenta una serie de características muy importantes para que todo administrador de red que desee ocupar estos equipos tenga una ventaja y pueda competir con cualquier compañía y sus redes sea una de las más confiables.

Por eso podemos definir al enrutador como un equipo que tiene dos misiones fundamentales determinar una trayectoria a lo largo de la que se puede realizar un enlace y transmitir paquetes a lo largo de dicha trayectoria.
Soporta simultáneamente varios protocolos lo cual lo hace compatible con otros equipos, une redes LAN y WAN, filtra el tráfico no deseado, actúa como firewall por medio de las listas de acceso, son confiables por las varias rutas que puede usar para transmitir son autónomos porque seleccionan y guardan las mejores trayectorias para transportar el tráfico.
Para trabajar con los enrutadores existen tres formas de conexión que son por medio de la consola, por la red y por el puerto auxiliar. Dentro de las características más importantes del enrutador se encuentra la seguridad ya que sin ella muchos lugares serian dañados o saqueados para perjudicar a una empresa o persona, por eso sus diferentes formas de seguridad de dividen en contraseñas en las diferentes etapas de con el apoyo como es el acceso para firmarse como personas seguras y tienen la intención sola de mantener las conexiones seguras y mantener la optimización de cualquier red. Para asegurarse que uno va elegir un buen enrutador debemos tomar en cuenta los siguientes factores como son el físico que tiene que ser compatible con el segmento de red la comunicación la cual debe ser compatible con el medio de transporte que se usara, el protocolo también debe ser compatible para ofrecer seguridad, velocidad y debe ser rentable a largo plazo.

Una vez elegido el enrutador hay que seguir los pasos apropiados para mantener su funcionalidad y mantener en buen estado el archivo de configuración que es de vital importancia ya que en el se encuentra el control de sus procesos así como las memorias RAM, DRAM, NVRAM, puntos clave para poder realizar los procesos de IOS de Cisco que es el sistema operativo de Cisco el cual forma parte esencial del procesos y controles del enrutador esto implica el manejo de comandos. También cuando se piensa comprar equipo usado el recuperar las contraseñas son esenciales para volverlas o configurar para esto hay varios métodos por ejemplo el uso de comandos en varios niveles del sistema operativo del IOS.
Otros de los puntos para la administración de una son saber configurar el enrutador por eso el sistema operativo IOS y el archivo de configuración son las dos cosas que se deben poner mayor atención para administrar los enrutadores. Estos cambios y movimientos se llevan acabo con comandos. Por su puesto además de dos modos de operación del enrutador que se dividen en siete, las tres primeras son modos de inicio y los cuatro restantes se suelen llamar habilitados, incluso dentro de estos casos hay tres de operación, inicio de sistema que dice que comando hay que usar y que partes del enrutador se van a actualizar. Como pueden ser el config maker herramienta de gama media para LAN y conectividad con WAN, y por último el Fast step de gama baja se utiliza para configurar pequeños enrutadores y servidores de acceso para los que se inician en la administración de sistemas o pequeñas empresas

Y para terminar como en la mayoría de las empresas las fallas se hacen presentes por razones muy diversas por eso es importante tener en cuenta y prevenir fallas desde las más comunes hasta las menos esperadas, saber localizarlas, tener la paciencia y la habilidad de encontrar y resolver fallas, por eso Cisco tiene un sistema muy amigable para interactuar con el software y directamente con el hardware.

El mantenimiento de una red debe ser constante, por eso debemos conocer las fallas y soluciones más comunes para actuar de forma efectiva sin perdida de tiempo y esfuerzo. Los protocolos de enrutamiento solucionan problemas de forma automática sin esperar la intervención del administrador de la red, con esto se prueba que el acceso a través del IOS ayuda enormemente a la solución de problemas por medio de comandos que ayudan a identificar los fallos como son el acceso a equipos, malas configuraciones, rendimientos de la red. La solución puede comenzar desde la más sencilla, como checar direcciones IP, comparándolos con ejecución de comandos para tener buena configuración de debe hacer un ping, estados de conexión, el protocolo de línea prueba si esta bien la interfase de línea, probar la lista de acceso que prueba si se configuro bien el enrutador que son las cuestiones mas comunes. Otra forma de ver el equipo es a través de la inspección física de los equipos checar las interfaces, cables, alimentación, luces y cuando sé más intenso los problemas se requerirá que se haga una inspección interna del equipo para encontrar la falla y recetear el equipo para volverlo a encender.

Bibliografía

 **Libros:**

I. Titulo: Manual de Cisco.

Autor: Tom Shaughnessy.
Toby Velte.

Editorial: Mc Graw Hill.

II. -Titulo: Configuración del Enrutador Cisco

Autor: Rex Hale

Editorial: Mc Graw Hill

 **Web:**

www.cisco.com

www.cisco.com/univercd/cc/td/doc/sicintwk/ita/index.htm

www.zdwebopedia.com/

www.ietf.org