Universidad Nacional Autónoma de México

Facultad de Ingeniería

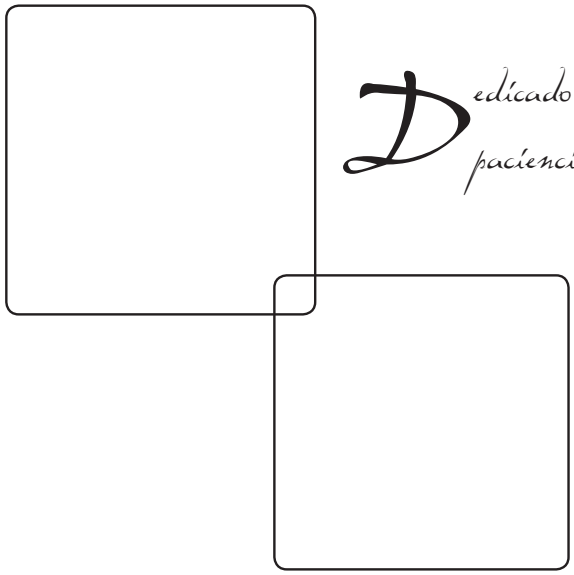
Implementación, mantenimiento y renovación de la Red Corporativa de Datos Telmex

Trabajo profesional
que para obtener el título de:
Ingeniero en Telecomunicaciones

Presenta:
Carlos Josue Hernández Cruz

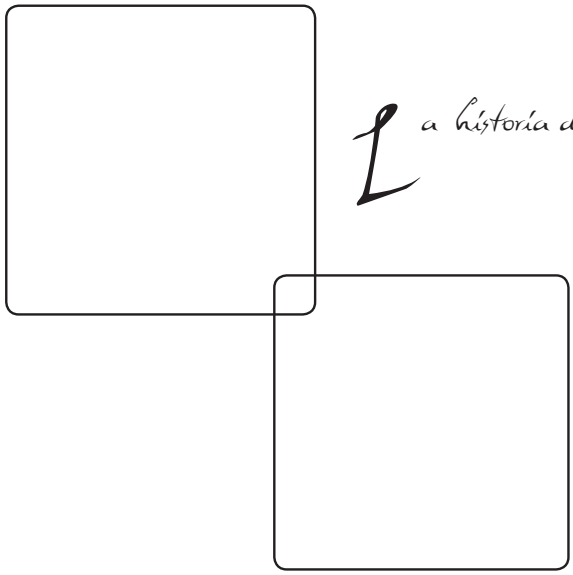
Director:
Dr. Miguel Moctezuma Flores

Ciudad Universitaria, D.F., 2010



Dedicado a mi familia, por su inagotable paciencia y apoyo en la noches de duda.

Gracias a tí porque lo hiciste posible, Mizuki, que eres el brillo de plata sobre el agua obscura.



La historia del mundo debe cumplirse en cada hombre.

Los teólogos

Índice

Objetivo

TELMEX es una compañía internacional líder que ofrece servicios avanzados de telecomunicaciones que incluyen transmisión de voz, datos y video, acceso a Internet y soluciones integrales para todos los segmentos del mercado de las telecomunicaciones; desde telefonía pública, rural y residencial, hasta la atención de clientes de la pequeña y mediana empresa, así como para grandes corporativos nacionales e internacionales, gracias a la gran capacidad técnica y de cobertura que brindan sus redes de acceso y transporte, que le han permitido un constante nivel de crecimiento en los productos y servicios que ofrece al mercado.

Tiene presencia en cinco países de América del Sur y en Estados Unidos y conexión por fibra óptica con 39 países en el mundo, lo que ha hecho que se consolide como una empresa líder en los países de América latina donde tiene presencia.

Por lo cual a asegurado su crecimiento y modernización de su infraestructura desarrollando una plataforma totalmente digital con el respaldo de una de las redes más avanzadas a nivel mundial de fibra óptica la cual incluye interconexiones submarinas internacionales. Esta infraestructura está organizada en anillos de alta capacidad los cuales permiten alta redundancia lo que se refleja en una garantía del servicio ya que en caso de falla el cliente no lo percibirá dado que se cuenta con un camino alterno que garantiza la continuidad del transporte.

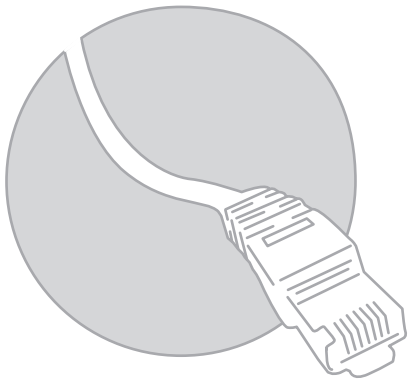
La fortaleza financiera de TELMEX y su pertenencia al principal grupo empresarial de México así como su capacidad tecnológica para innovar productos y servicios con base en su amplio conocimiento de los mercados que atiende, permiten a Telmex fortalecer su expansión internacional, buscando con esto inversiones de largo plazo para el desarrollo de infraestructura y servicios de telecomunicaciones en cada uno de los países en los que opera, en beneficio de los sectores productivos que compiten en el nuevo entorno de globalización mundial.

Debido al enorme desarrollo de la empresa, esta se divide en dos entidades: Uninet y la Red Corporativa de Datos Telmex (RCDT). La primera se encarga de la planeación, implementación y operación de los servicios masivos. La RCDT tiene como objetivo garantizar la comunicación corporativa teniendo como responsabilidad la red de datos en su planeación, implementación, operación y expansión asegurando alta disponibilidad; y provee la gestión de los equipos de comunicaciones. Todo esto bajo un esquema de control de

cambios y ajustándose a los procesos definidos para cada proyecto.

Dada la importancia e impacto de las aplicaciones y servicios ofrecidos por RCDT se necesita personal capacitado, responsable con iniciativa y comprometido con los objetivos establecidos en conjunto con las diferentes áreas en que se divide la RCDT.

Ser egresado de la carrera de telecomunicaciones me permitirá desarrollar y valuar las posibles soluciones a los requerimientos actuales de la red de datos, así como la integración de estas a la red operativa de tal forma que la afectación al servicio sea mínima. Esto será posible supervisando que los elementos tales como adquisición, planeación, ingeniería e implantación se encuentren listos para la recepción e integración de la solución técnica.



Capítulo 1

Antecedentes

Son varios los aspectos generales que se deben tener en cuenta al momento de diseñar una red de datos y en especial si es una de grandes dimensiones debido al flujo de tráfico, la interconexión entre ciudades de toda la república y el impacto en las aplicaciones que soporta.

Dentro de los factores a contemplar destacan el modelo de referencia, tipo de arquitectura, selección del equipo a utilizar, protocolos de ruteo y el desarrollo de políticas, es decir, un conjunto de reglas y estándares para la homologación de la red.

Modelo de referencia

El modelo utilizado es el TCP/IP el cual tiene como base el modelo de referencia OSI que fue creado para estandarizar los protocolos de la red de datos que permiten la comunicación de dispositivos finales. El modelo de TCP/IP fue definido después de los protocolos y por lo que se adecúan perfectamente. No es complejo, tiene apoyo para broadcast. Tiene como objetivos la conexión de redes múltiples y la capacidad de mantener conexiones aun cuando una parte de la subred esté perdida. También la red es packet-switched y está basada en un nivel de internet sin conexiones.

Este modelo es dividido en cuatro partes que desempeñan funciones específicas:

Capa de Acceso de a la red. Maneja los aspectos que requiere un paquete ip para efectuar un enlace físico real con los medios de la red. Sus protocolos son:

- ARP: Conseguir dirección física a partir de una dirección ip
- RARP: Asignar una dirección ip a partir de una dirección física

Capa de Internet. Los hosts pueden introducir paquetes en la red, los cuales viajan independientemente al destino. No hay garantías de entrega ni de orden. Este nivel define el Internet Protocol (IP), que provee el ruteo y control de congestión.

Capa de Transporte. Permite que pares en los hosts de fuente y destino puedan conversar. Hay dos protocolos:

Transmission Control Protocol (TCP). Provee una conexión confiable que permite la entrega sin errores de un flujo de

bytes desde una máquina a alguna otra en la internet. Parte el flujo en mensajes discretos y lo monta de nuevo en el destino. Maneja el control de flujo.

User Datagram Protocol (UDP). Es un protocolo no confiable y sin conexión para la entrega de mensajes discretos. Se pueden construir otros protocolos de aplicación sobre UDP. También se usa UDP cuando la entrega rápida es más importante que la entrega garantizada.

Capa de Aplicación. Maneja aspectos de representación, codificación y control de dialogo. Sus protocolos son FTP, TFTP, NFS, SMTP.

Arquitectura de red

La topología de la RCDT está basada en un modelo jerárquico de tres niveles, siendo estos Dorsal, Distribución y Acceso (también conocida como topología en árbol) puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Éste árbol tiene nodos periféricos individuales que requieren transmitir a y recibir de otro nodo solamente y no necesitan actuar como repetidores o regeneradores. Al contrario que en las redes en estrella, la función del nodo central se puede distribuir.

Como en las redes en estrella convencionales, los nodos individuales pueden quedar aislados de la red por un fallo puntual en la ruta de conexión del nodo. Si falla un enlace que conecta con un nodo individual, este queda aislado; si falla un enlace con un nodo que no sea aislado, la sección entera queda aislada del resto. Cada nivel de esta topología desempeña funciones específicas que se describen a continuación:

- Nivel Dorsal: Este nivel constituye la red de alta capacidad de conmutación de datos, está conformado por un conjunto de enrutadores que conforman un backbone nacional. Este nivel esta implementado lógicamente única y exclusivamente sobre el protocolo IP.

- Nivel Distribución: El nivel de distribución realiza funciones de transporte de tráfico a nivel regional. Siendo su capacidad de ancho de banda menor respecto al ancho de banda implementado en el nivel dorsal. El nivel de distribución es frecuentemente el nivel que delimita los dominios regionales. Tiene una distribución nacional con poco más de 90 enrutadores. Este nivel esta implementado lógicamente única y exclusivamente sobre el protocolo IP.

- Nivel Acceso: Este nivel es el que permite la integración de usuarios directamente a la red de datos, se conforma por un gran conjunto de nodos (2500 enrutadores aproximadamente) de distintas plataformas distribuidos a nivel nacional en los que se provee presencia RCDT. Estos nodos permiten la interconexión de distintos tipos de interfaces físicas y protocolos.

En base a lo anterior resulta indispensable homogenizar los tipos de conexiones que se establecen por dispositivos de usuarios sobre los nodos de acceso, ya que mientras mayor sea el número de distintas interfaces y protocolos permitidos, mas complejo se vuelve para la RCDT mantener stock de refacciones, definir y actualizar versiones IOS que omitan bugs para cada protocolo y hardware específico, mantener el desempeño y recursos (CPU, memoria y buffers) de los nodos, establecer métodos de encapsulamiento para cada protocolo diferente a IP, etc.

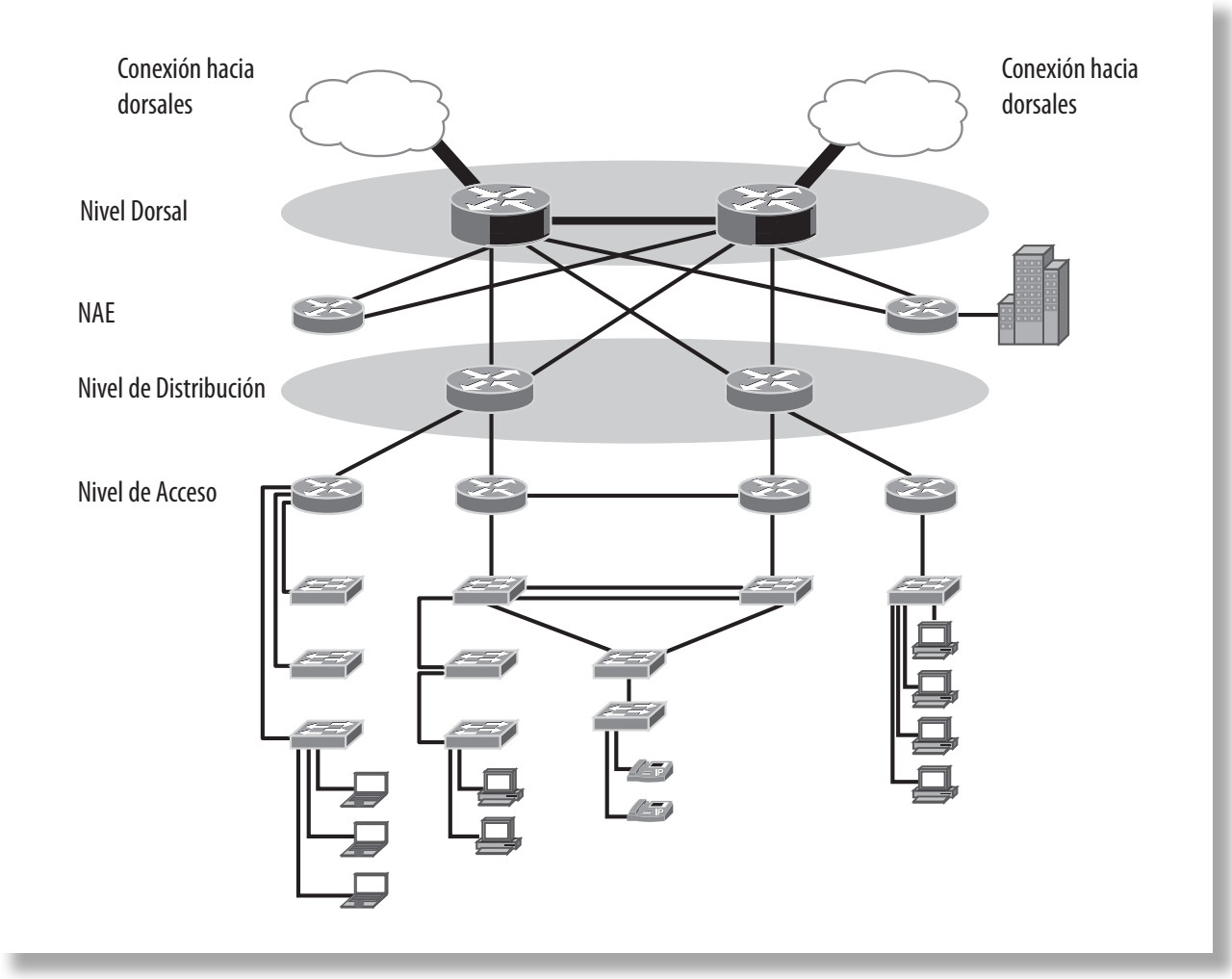


Figura 1.

Dispositivos de red

Debido a que la RCDT está basada fundamentalmente sobre el protocolo IP y protocolos relacionados al stack TCP/IP, es muy recomendable que los dispositivos a gestionar a través de la RCDT funcionen sobre el protocolo IP en cuanto a lo que especta a su gestión, de manera que su integración en el aspecto lógico sea transparente.

RCDT tiene definidas arquitecturas LAN en Centrales para soportar de manera ordenada, segura y eficiente la integración de dispositivos de usuario típicos de central. Estos modelos de red permiten agrupar y separar dispositivos que operan en protocolo IP de los que operan en protocolo CLNS. El equipo de comunicaciones que interconecta a los dispositivos de usuario es un switch LAN con puertos 10/100BaseT para cable UTP en conector RJ-45.

Como una estrategia de administración de la inversión, RCDT ha establecido en sus modelos de red para aplicaciones de Central la convivencia lógica de la mayoría de las aplicaciones que se ajusten al "Protocolo e Interface" homologados. De tal manera que la funcionalidad particular de cada aplicación deberá ser lo más simple en cuanto a funcionalidades con el fin de poder convivir con otras aplicaciones.

La RCDT ha definido, dentro de las tareas de reingeniería de la red, estructuras estándares de LAN basadas en switches que proporcionan alta eficiencia en el manejo de tráfico y simplifican la administración. Dentro de las estructuras LAN mencionadas existen dos grandes esquemas: Topologías de Edificios Corporativos y Topologías de Centrales Telefónicas.

Para edificios corporativos, se utiliza una topología que consiste en colapsar los switches de nivel acceso Catalyst 1900 en switches de nivel distribución Catalyst 2950:

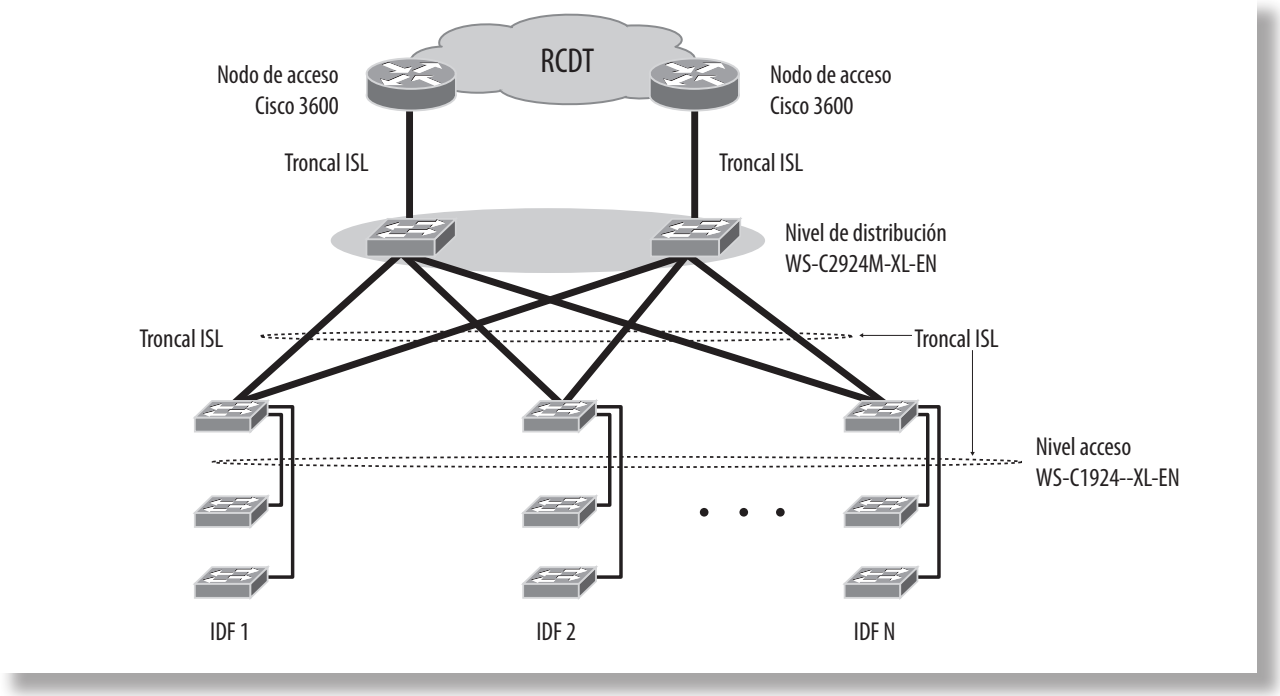


Figura 2. Topología para edificios corporativos.

Para el caso de Centrales, se tienen dos modelos, ver figura 3:

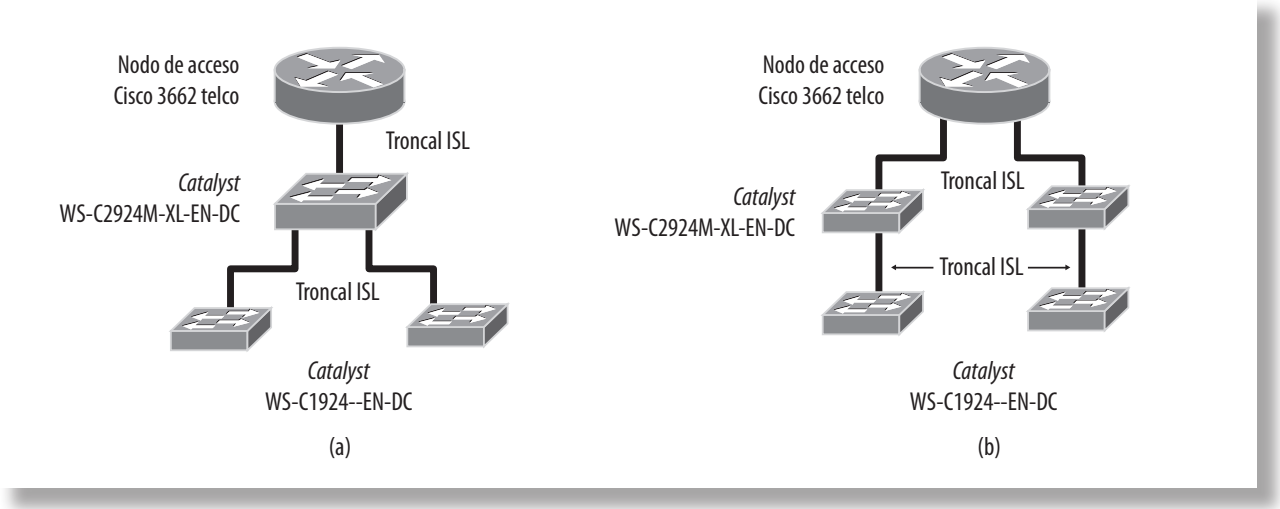


Figura 3. Topología para centrales de TELMEX.

Catalyst 2950

El switch Cisco Catalyst 2950-24 es un switch independiente, de configuración fija, que proporciona conectividad para redes de tamaños pequeños a medios. Este switch Desktop ofrece funcionalidades del IOS Cisco para servicios básicos de datos, video y voz a nivel acceso. El Catalyst 2950-24 contiene 24 puertos 10/100.

La versión de software 12.1.6EA2c para esta plataforma contiene las funcionalidades de las imágenes estándar y mejorada, No obstante, el switch catalyst 2950-24 únicamente soporta la imagen estándar. La imagen enhanced incluye las funcionalidades mejoradas para calidad de servicio, tales como clasificación, policing y marking.

Catalyst 3550

La serie Cisco Catalyst 3550 de switches Ethernet inteligentes es una línea nueva de productos de clase enterprise, apilable, multicapa, que proporcionan alta disponibilidad, escalabilidad, seguridad y control para mejorar la operación de una red. Con un amplio rango de configuraciones Ethernet y Gigabit Ethernet, la serie 3550 puede utilizarse como un switch poderoso en la capa de acceso para corporativos medianos y como switch de backbone para redes de tamaño medio. A través de estos productos, se puede desplegar un amplio rango de servicios inteligentes, como calidad de servicio (QoS, Quality of Service) avanzada, limitación de tasa de transmisión, listas de control de acceso Cisco, administración multicast, y enrutamiento IP de alto rendimiento, manteniendo la simplicidad del switcheo LAN tradicional.

En el 3550-24 se puede incluir la imagen estándar (SMI, Standard Multilayer Image) o la imagen mejorada (EMI, Enhanced Multilayer Image). La imagen mejorada proporciona un conjunto de características de clase enterprise, que incluyen ruteo IP (unicast y multicast) basado en hardware, ruteo entre VLAN's, Routed Access List Control (RALC's), y HSRP (Hot Standby Router Protocol), como se puede observar en la tabla 1.

Características de Capa3 para el Catalyst 3552-24-EMI	
Equal Cost Routing	Para balanceo de carga y redundancia
RACL´s (Router ACL´s)	Para definir políticas de seguridad en routed interfaces para el tráfico del plano de control y el palno de datos
CEF (Cisco Express Forwading)	Arquitectura de ruteo basada en hardware para entregar ruteo IP de alto rendimiento
Soporte para protocolos estándar de ruteo IP unicats (RIPv1, RIPv2, OSPF, IGRP, EIGRP)	Para balanceo de carga y construcción de LAN´s escalables
Ruteo estático IP	Con el que se puede construir manualmente la tabla de ruteo
Ruteo entre VLAN´s	Para ruteo de capa 3 entre dos o más VLAN´s
PIM (Protocol Independent Multicast)	A través del cual se rutea el tráfico multicast dentro de una red, permite que se reciba una petición de alimentación multicast y reenvío de este tráfico hacia switches que no participan
DVMRP tunneling (Distance Vector Multicast Routing protocol)	Para conectar dos redes multicast a través de una red que no lo es
Fallback bridging	Para reenviar tráfico que no es IP entre dos o más VLAN´s
HSRP (Hot standby Router Protocol)	Para crear topologías redundantes

Tabla 1. Características de la Capa 3 soportadas por el C3550-24.

Caracteríticas de seguridad				
Funcionalidad	**1924**	**2924**	**2950-24**	**3550-24**
Private VLAN edge			✓	✓
Soporte para *port secure*	✓	✓	✓	✓
Seguridad multinivel en el acceso a la consola	✓	✓	✓	✓
Modo de aprendizaje de direcciones elegible por el usuario	✓	✓	✓	✓
Autenticación TACACS+	✓	✓	✓	✓
STP root guard		✓	✓	✓
Autenticación RADIUS				✓
Autenticación 802.1x				✓
Listas de acceso Cisco de seguridad para VLAN en todas las VLAN´s				✓
Listas de acceso basadas en tiempo				✓
BPDU *guard*				✓

Tabla 2. Funcionalidad para la implementeción de seguridad en las plataformas Catalyst.

Calidad de servicio				
Funcionalidad	**1924**	**2924**	**2950-24**	**3550-24**
Clase de servicio (CoS) 802.1p		✓	✓	✓
Cuatro colas de egreso por puerto, soportadas en *hardware*			✓	✓
Algoritmo de encolamiento WRR (*Weighted Round Robin*)			✓	✓
Configuración de encolamiento *Stric Priority*			✓	✓
WRED (*Weighted Random Early Detection*)				✓
Listas de acceso QoS para el plano de control y plano de datos en todos los puertos				✓
Funcionalidad Cisco CIR (*Committed Information Rate*)				✓

Tabla 3. Funcionalidad para la implementeción de calidad de servicio en las plataformas Catalyst.

Calidad de servicio				
Switch	**1924**	**2924**	**2950-24**	**3550-24**
Encapsulación ISL	✓	✓	×	✓
Encapsulación 802.1Q	×	✓	✓	✓

Tabla 4. Encapsulaciones soportadas por las diferentes plataformas.

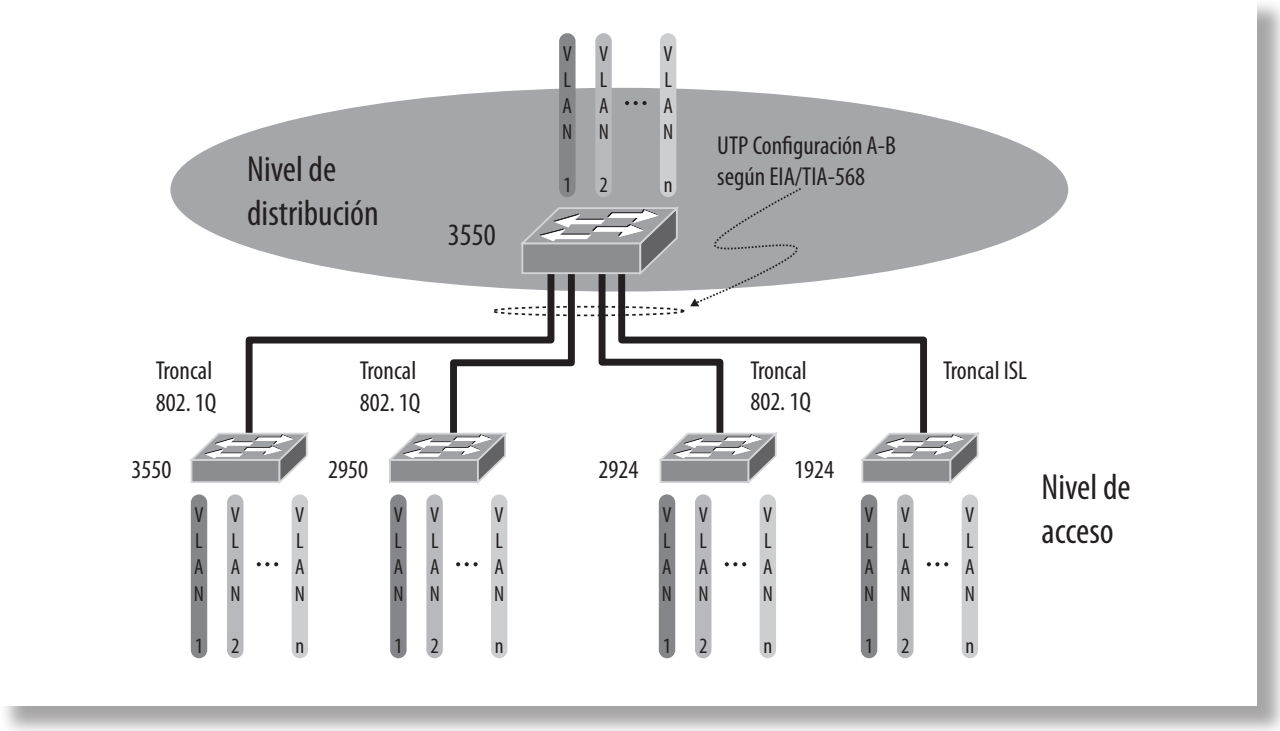


Figura 4. Conectividad entre switches de nivel distribución y acceso por troncales.

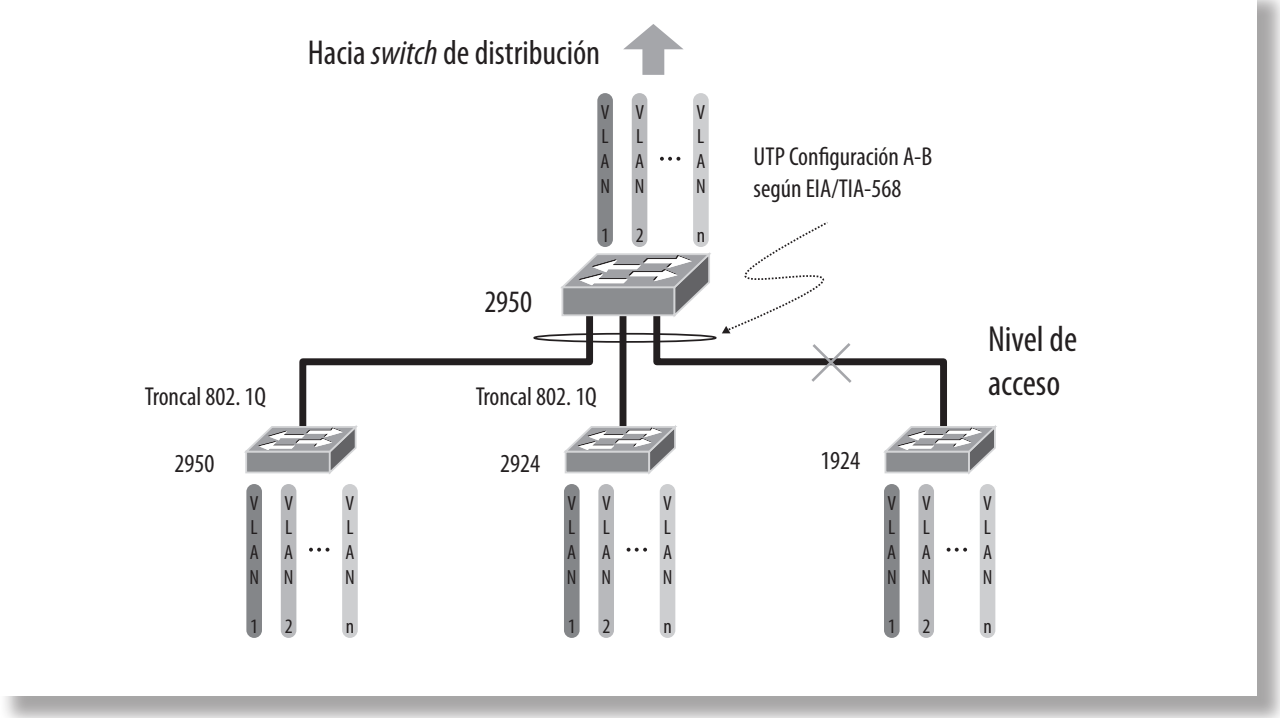


Figura 5. Conectividad entre switches de nivel distribución y acceso.

Políticas de configuración

Una VLAN (acrónimo de Virtual LAN, red de área local virtual) es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión (broadcast) y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3).

Una VLAN consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

VLAN nativa en 802.1Q

Las tramas 802.1Q de una VLAN contienen una etiqueta en el encabezado, se trata de cuatro bytes de datos. La etiqueta se inserta en el frame después de la dirección MAC fuente; se compone del TPID de 2 bytes (EtherType Identifier, que para el caso de 802.1Q corresponde el valor 0x8100), 3 bits de prioridad que se utilizan en el estándar 802.1p, 1 bit que es el Canonical Format Identifier y 12 bits que representan el VLAN ID. Las troncales 802.1Q están configuradas para transmitir todos los frames etiquetados y desechan aquellos que no tienen etiqueta de VLAN. Existe una VLAN nativa encargada de transportar el tráfico no etiquetado, para el caso de los routers y switches Cisco, la VLAN nativa por default es la 1.

Para una correcta operación de las troncales es necesario que la VLAN nativa en ambos extremos sea la misma. Existen algunos conflictos en cuanto a configuración de la VLAN nativa en un Router que dependen de la versión de IOS. Las versiones homologadas en la RCDT no tienen opción de cambiar la VLAN nativa (12.0.9 y 12.1.13). Por eso, se ha decidido utilizar la configuración default para esta VLAN, de tal forma que para asignación de usuarios la primera VLAN operativa será la 2.

VLAN de gestión

La VLAN de gestión por default en los switches 2950 Y 3550 es la 1, en las topologías LAN de la RCDT se definió la VLAN 255 como VLAN de gestión para equipos de comunicaciones, esta política seguirá utilizándose como hasta ahora para las cuatro plataformas.

VLAN de gestión en 1924

Los switches 1924 soportan un máximo de 64 instancias de Spanning Tree y por default se encuentran operativas en las primeras 64 VLAN's. Por lo que, cuando se requiera habilitar spanning tree en una VLAN fuera del rango 1-64 (por ejemplo la VLAN 255 de gestión), es necesario dar de baja SPT en alguna de las VLAN's que no sean operativas, y habilitarlo en la VLAN que se requiera. Los comandos para hacerlo son los siguientes:

```
Switch(conf)#no spantree 64
Switch(conf)#spantree 255
```

La primera línea de comandos da de baja STP en la VLAN 64, mientras que la segunda lo habilita en la VLAN 255. De

esta forma se respeta el máximo número de instancias de Spanning Tree soportadas por el switch.

Configuración de switch raíz en STP

Spanning Tree Protocol (STP) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos) Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE 802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.

Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de lazos. STP es transparente a las estaciones de usuario.

La definición de switches raíz primario y secundario para las topologías redundantes que se utilizan en la RCDT, se realizará mediante el ajuste del parámetro de prioridad que utiliza Spanning Tree. Por default los switches tienen un valor de 32768. Para lograr que un switch del nivel distribución (ver figura 6) sea raíz, se configurarán valores de prioridad como sigue:

```
Para switch raíz primario: 8192.
Para switch raíz secundario: 16384.
```

Configuración de puertos para usuarios

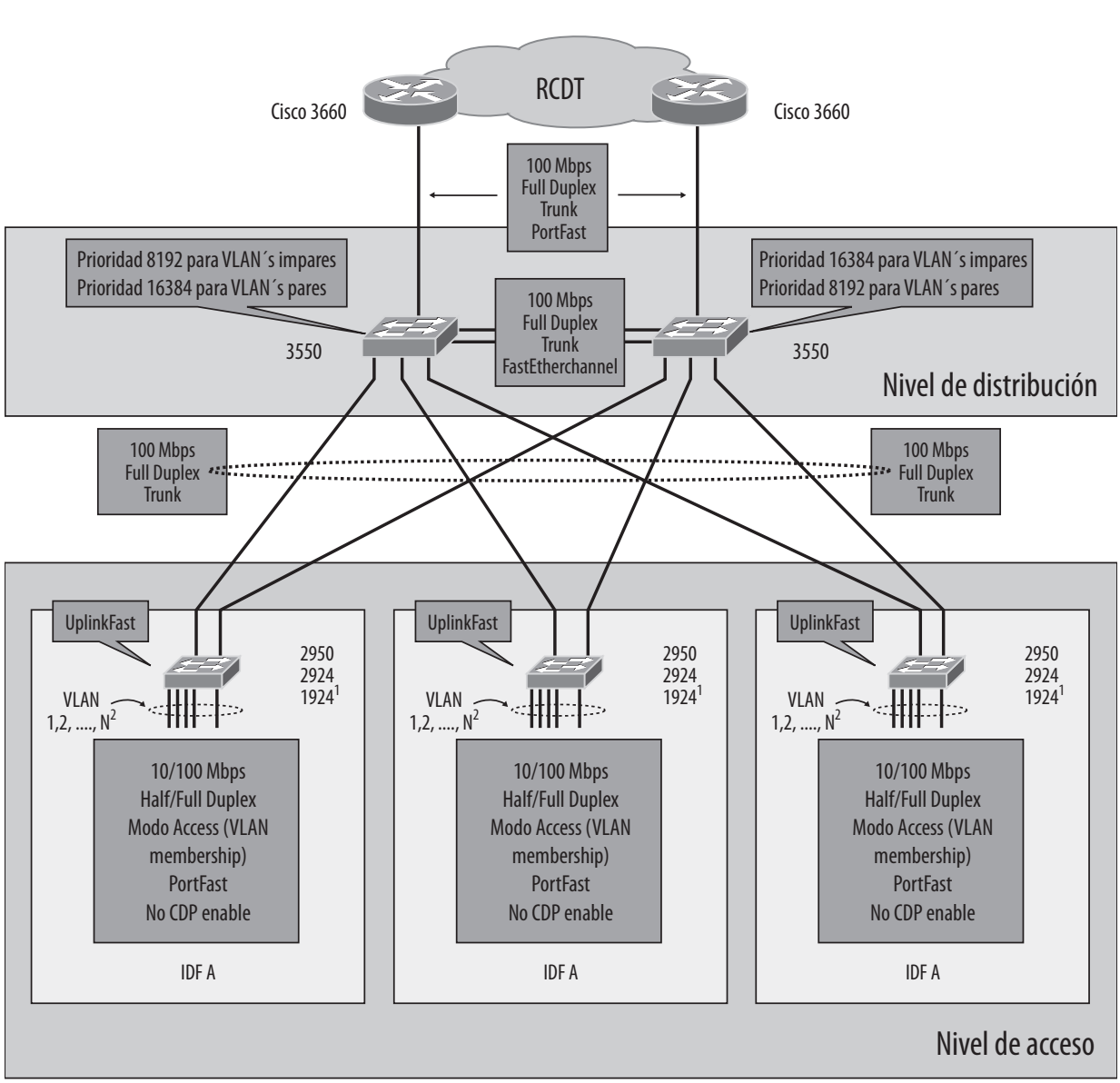
Para evitar que los puertos del switch destinados a usuarios entren en el proceso de spanning tree, deberá habilitarse en ellos la opción de PortFast.

Para las versiones de software de los switches 3550 (12.1(8)EA1c) y 2950 (12.1.6.EA2c), los puertos se encuentran en modo dynamic desirable. Es necesario configurar los puertos de usuarios en modo access, con su pertenencia a la VLAN respectiva.

Direccionamiento IP

Una máscara de red nos ayuda a conocer que parte de direcciones identifican la red y que parte de direcciones identifican los nodos. Las clases de red A, B y C tienen mascaras por default también conocidas como su mascara natural:

```
Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0
```



1. En este caso se configurará ISL para trunking, ya que 1924 únicamente soporta esta tipo de encapsulación, en cualquier otro caso se configurará 802. 1Q.
2. La VLAN 1 será reservada como VLAN nativa en 802. 1Q, en este caso la primera VLAN operativa para usuarios será la VLAN 2.

Figura 6.

Una dirección IP sobre una red de clase A que no ha sido subneteada podría tener un par mascara/dirección similar a 8.20.15.1 / 255.0.0.0. Para ver como la masca ayuda a identificar la parte de red y el nodo de las direcciones convertimos la dirección y mascara a números binarios:

```
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
```

Una vez que tenemos las direcciones y la mascara representada en binario entonces podremos identificar la parte del identificador de red y de host. Los bits de direccionamiento que tienen su correspondiente mascara de bits puestos en 1 representan el identificador de red. Los bits de direccionamiento que tiene su correspondiente mascara de bits puesta en 0 representan el identificador de nodo.

```
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
-----------------------------------
Red id | Host id
redid  = 00001000 = 8
hostid = 00010100.00001111.00000001 = 20.15.1
```

Subneteo

El subneteo nos permite crear múltiples redes lógicas que existen con una simple red clase A, B o C. Si no se aplicara el subneteo, solo se podría habilitar una sola red, lo cual no resulta práctico.

En cada enlace de la red se debe tener un único id, y cada nodo al que pertenece ese link también será un miembro de al misma red. Si se rompe una red grande (Clase A, B o C) en pequeñas subredes, se permitirá la creación de una red de interconexión de redes. Entonces cada enlace en esta red podría tener un único identificador de red/subred. Cualquier dispositivo o gateway, que conecta N redes/subredes tendrá N ip's distintas, una por cada red/subred que interconecta.

Para subnetear una red, se extiende la mascara natural usando algunos de los bits de la porción de direcciones de host para crear los identificadores de subred. Por ejemplo, dada la red de clase C 204.15.5.0 la cual tiene una mascara natural de 255.255.255.0, se puede crear subredes de la siguiente manera:

```
204.15.5.0      – 11001100.00001111.00000101.00000000
255.255.255.224 – 11111111.11111111.11111111.11100000
                  -------------------------|sub|----
```

Extendiendo la mascara a 255.255.255.224, se tienen tres bits (indicado por sub) de la porción original de la direcciones y se usan para crear subredes. Con estos tres bits, es posible crear ocho subredes Con los cinco restantes bits de host cada subred podrá tener 32 direcciones de host, 30 de las cuales podrán ser asignadas a los dispositivos con excepción de la primera y ultima dirección de este segmento. Con esto en mente, se tendrán las siguientes subredes:

```
204.15.5.0   255.255.255.224 host rango de direcciones 1   a 30
204.15.5.32  255.255.255.224 host rango de direcciones 33  a 62
204.15.5.64  255.255.255.224 host rango de direcciones 65  a 94
204.15.5.96  255.255.255.224 host rango de direcciones 97  a 126
204.15.5.128 255.255.255.224 host rango de direcciones 129 a 158
204.15.5.160 255.255.255.224 host rango de direcciones 161 a 190
204.15.5.192 255.255.255.224 host rango de direcciones 193 a 222
204.15.5.224 255.255.255.224 host rango de direcciones 225 a 254
```

Existen dos maneras de representar estas mascaras. La primera desde que tu estas usando tres bits mas de la mascara natural de la red clase de C, tu puedes denotar estas direcciones teniendo 3 bits mascara de subred. O la segunda, la mascara de 255.255.255.224 puede también ser representada como /27 porque hay 27 bits que están siendo utilizados en la mascara. Este segundo método es comúnmente usado con CIDR. Usando este método, una de esas redes puede ser descrita con una notación de prefijo/longitud. Por ejemplo, 204.15.5.32/27 describe la red 204.15.5.32 255.255.255.224.

El esquema de subneteo usa ocho subredes, la red podría ser como se muestra:

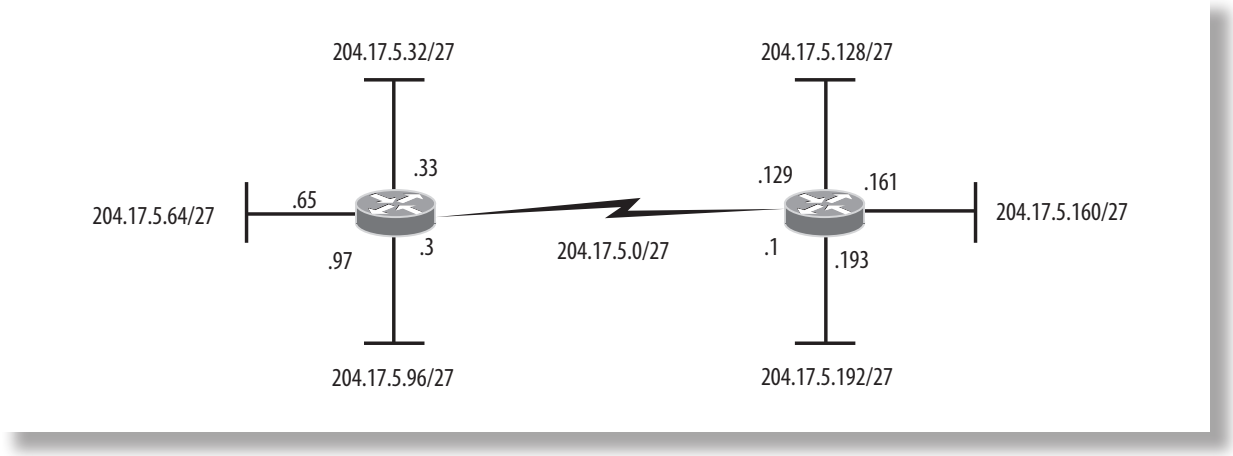


Figura 7.

Se observa que cada ruteador esta asociado a cuatro subredes, una de ellas es común a ambos ruteadores. Así, cada ruteador tiene un dirección IP para cada subred a las cual esta asociado. Cada subred podría potencialmente soportar 30 direcciones de host. Esto nos muestra un punto interesante: A mayor numero de subredes, menor numero de host y viceversa.

Antes existía una limitación en el uso de la subred 0 (todos las bits estaban puestos en 0) y todas las subredes 1 (todos los bits en 1). Algunos dispositivos no permitían el uso de estas subredes. Los dispositivos Cisco permiten su uso mediante el comando ip subnet zero.

VLSM

Variable Length Subnet Masks (VLSM) permite usar diferentes mascaras para cada subred usando de esta manera el espacio de direccionamiento eficientemente.

En el ejemplo anterior la mascara de subred fue aplicada a todas las subredes, pero hacerlo implica un desperdicio de direcciones ya que algunos segmentos no serán utilizados en su totalidad.

Para ejemplo anterior tendremos un mejor uso de direcciones si segmentamos de la siguiente manera:

```
redA: debe soportar 14 hosts
redB: debe soportar 28 hosts
redC: debe soportar 2  hosts
redD: debe soportar 7  hosts
redE: debe soportar 28 host
```

Se determina que mascara puede permitir el número requerido de host:

```
redA: requiere una mascara de /28 (255.255.255.240) para soportar 14 hosts
redB: requiere una mascara de /27 (255.255.255.224) para soportar 28 hosts
redC: requiere una mascara de /30 (255.255.255.252) para soportar 2  hosts
redD: requiere una mascara de /28 (255.255.255.240) para soportar 7  hosts
redE: requiere una mascara de /27 (255.255.255.224) para soportar 28 hosts
```

La manera más fácil de asignar subredes es asignar primero el segmento mas extenso primero. Por ejemplo de la siguiente manera:

```
redB: 204.15.5.0/27  rango de direcciones de host de 1  a 30
redE: 204.15.5.32/27 rango de direcciones de host de 33 a 62
redA: 204.15.5.64/28 rango de direcciones de host de 65 a 78
redD: 204.15.5.80/28 rango de direcciones de host de 81 a 94
redC: 204.15.5.96/30 rango de direcciones de host de 97 a 98
```

CIDR

Classless Interdomain Routing (CIDR) fue introducido para implementar en conjunto utilización del espacio de direccionamiento y escalabilidad de ruteo en Internet. Fue necesario por lo rápido del crecimiento de Internet y del crecimiento de las tablas de ruteo IP contenidas en los ruteadores de Internet.

CIDR sale de las tradicionales clases IP (clase A, clase B, clase C, etc). En CIDR, una red IP es representado por un prefijo, el cual es una dirección IP y alguna indicación de la longitud de de la mascara. La longitud significa el numero de bits contiguos a la mascara natural que serán encendidos. Entonces la red 172.16.0.0 255.255.0.0 es representada por 172.16.0.0/16. CIDR también representa una arquitectura de Internet más jerárquica donde cada dominio toma su direccionamiento IP de un nivel superior. Esto hace posible la sumarización de los dominios en un nivel superior.

Las necesidades de direccionamiento de la RCDT varían según algunos parámetros a considerar como el número de usuarios, ips de gestión de equipos, numero de enlaces entre dispositivos de la red, etc.

La administración del direccionamiento comienza por dividir un gran segmento de direcciones IP para cada divisional (Se trabaja con la red clase A 10.0.0.0) después de haber hecho un estudio de la proyección de crecimiento y necesidades de cada una de ellas, esto con la finalidad de ahorrar procesamiento a los ruteadores dorsales. Y a partir de ahí se segmentan en otros mas pequeños que son otorgados de manera mas regional en el nivel de distribución (Ciudades); Finalmente en la capa de acceso se subnetea hasta segmentos de máximo /24 para direccionamiento de usuario.

Generalmente se otorga un segmento de direcciones de /28 para gestión de equipos de conmutación y de usuarios (aquí pueden ser dos segmentos dependiendo de la cantidad de equipos a gestionar y el numero de usuarios), 1 dirección de loopback para cada equipo ruteador con mascara de /32, un segmento de /30 para direccionamiento de enlaces hacia equipos distribuidores, dorsales o de acceso.

Cada subinterface, que sirve como gateway de cada vlan posee la dirección mas alta del segmento utilizado (por ejemplo xx.xx.yy.254 / 24) y las ip asignadas la usuario (host) comenzaran desde la primera ip valida inferior (por ejemplo xx.xx.yy.1).

Protocolos de ruteo

Un protocolo es un juego formal de reglas y convenciones que gobiernan el hecho de como las computadoras intercambian información sobre un medio de red. Un protocolo implementa las funciones de una o más capas del modelo de referencia OSI. Hay una gran variedad de protocolos de comunicación. Estos protocolos caen dentro de uno de los siguientes grupos:

- Protocolos de ruteo: Son protocolos de la capa de red que son responsables de la determinación de rutas y conmutación de tráfico.

- Protocolos ruteables: Son protocolos típicos de las capas superiores en una suite protocolaria dada.

Los protocolos de ruteo determinan la ruta óptima a través de la red usando algoritmos de ruteo e información de transporte sobre estas rutas. Los protocolos de ruteo funcionan en la capa de red del modelo de referencia OSI. Ellos usan información específica de la capa de red, incluyendo direcciones de red, para mover unidades de información a través de la red.

Los algoritmos de los protocolos de ruteo actúan en dos funciones primarias

- Determinación de la ruta permite a un ruteador seleccionar la interfaz más apropiada para enviar un paquete.

- Conmutación de la ruta permite a un ruteador a aceptar un paquete en una interfaz y mandarlo por una segunda interfaz.

Los protocolos ruteables son transportados por los protocolos de ruteo sobre una red. Los protocolos ruteables actúan en una variedad de funciones requeridas para la comunicación entre dispositivos de una aplicación de usuario fuente y un destino.

Enrutamiento estático en nivel acceso.

Un equipo terminal típico (de usuario) debe ser capaz de manejar enrutamiento estático, lo cual simplifica el enrutamiento en RCDT, ya que solo se distribuyen las rutas pertenecientes al usuario final

En el caso de nodos de acceso, por cuestiones de aseguramiento de la calidad de los servicios ofrecidos, no deber utilizar enrutamiento dinámico para TCP/IP. Su operación se fundamenta sobre enrutamiento estático.

Por condición de diseño no es recomendable la utilización de 2 protocolos de enrutamiento para el mismo protocolo enrutado. La RCDT utiliza EIGRP en sus niveles dorsal y distribución, y los nodos de acceso son configurados de manera estática, por lo que no es conveniente utilizar un protocolo de enrutamiento adicional como lo es RIP dados los siguientes puntos:

- La habilitación de protocolos dinámicos en los enrutadores de acceso exige recursos de memoria DRAM y CPU. Este consumo puede ser considerable según el tamaño de las tablas de enrutamiento que están en función del tamaño de la red.

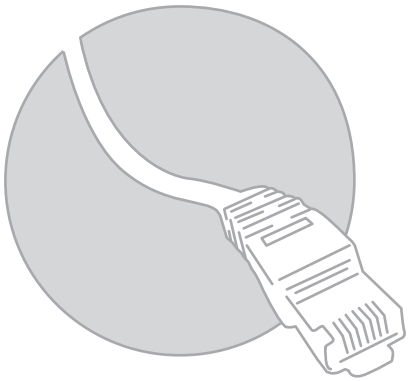
- Activar protocolos de enrutamiento como es el caso de RIP en los enrutadores de acceso, establece la posibilidad de que los dispositivos del usuario conectados a la red, inyecten rutas invalidas a la red, lo cual puede provocar puntos de falla a las aplicaciones existentes también sobre la red.

La consecutiva habilitación de protocolos a nivel acceso vuelve ms complejo el proceso de upgrade de versión IOS en los enrutadores. El proceso normal para esta actualización, consiste en revisar exhaustivamente los bugs asociados a cada protocolo. La existencia de más protocolos complica este proceso debido a que en ocasiones se presenta el caso de realizar un upgrade para solucionar una falla detectada en un protocolo, pero la nueva versión tiene nuevos bugs que afectan a la operación de otros protocolos en el mismo enrutador.

El tener enrutadores de acceso configurados con múltiples protocolos de enrutamiento hace más compleja la carga administrativa en la operación, debido a la necesidad de llevar un control de direccionamientos, configuraciones, tablas, bugs, etc.

La interconexión de dispositivos a través de enrutamientos dinámicos, establece la posibilidad de inyección de paquetes de actualización de rutas sobre los enrutadores de acceso. Este mecanismo puede llegar a ser intenso e impactar los procesos normales de la red.

Cualquier funcionalidad que se introduzca en la red debe cumplir con estándares y RFCs internacionales. Si un equipo no permite realizar una configuración estática para IP, no cumple con los principios básicos.



Capítulo 2

Definición de criterios administrativos y operativos

Por lo mencionado anteriormente, los dispositivos de usuario de Central deben ajustarse a los siguientes criterios:

1. Implementar una interface física de gestión 10BaseT o 100BaseTX.
   Posibilidad de fijar la velocidad del puerto ya sea en 10 Mbps o 100 Mbps.
   Posibilidad de fijar el modo duplex de transmisión ya sea en "half" o "full".

2. Implementar en capa 2 (enlace de datos) respecto al modelo de referencia OSI, el protocolo Ethernet II con encapsulamiento Ethernet.

3. Implementar capacidad de configuración de comandos de enrutamiento estático en el puerto de gestión, cuando requiera instalar enrutamiento dinámico dentro de la arquitectura del lado usuario.

4. No Implementar o desactivar funciones de boot remoto vía BOOTP/DHCP.

5. No Implementar o desactivar funciones de enrutamiento dinámico en el puerto de Gestión.

6. No Implementar o desactivar funciones de multicast ó broadcast en capa 3

7. No Implementar o desactivar funciones de multicast ó broadcast en capa 2 de protocolos diferentes a Ethernet II.

En base a las necesidades específicas de interconectividad de los distintos nodos de acceso y a fin de homologar infraestructuras tipo, se definen cinco tipos básicos de nodos de acceso:

1. Nodo de acceso de una Central mininodo

2. Nodo de acceso de una Central pequeña

3. Nodo de acceso de una Central mediana

4. Nodo de acceso de una Central grande

5. Nodo de acceso para un CTT, CTR u OCO

Un nodo de acceso de central mininodo es la nueva versión de un nodo de acceso RCDT pequeño, donde solamente se requiere acceso a la red para 9 equipos de central vía protocolo IP o CLNS.

Un nodo de acceso de central pequeña, mediana o grande topológicamente es el mismo nodo, el nodo consiste de un

enrutador, de un switch de IP, un switch CLNS, puertos para redes administrativas y aplicaciones seriales. La diferencia de un nodo de central pequeña, mediana y grande radica en la plataforma del enrutador a emplear en cada caso, cada uno de los tres diferentes nodos de acceso para central varía en el número de puertos para host LAN y WAN disponibles.

Un nodo de acceso de un Centro Telefónico (CTT), Centro de Trabajo (CTR) o de una Oficina Comercial (OCO), consiste básicamente de un enrutador y de un switch para redes LAN Administrativas.

Actualmente en la planta se tienen instalados para estos tipos de nodos enrutadores Cisco de la plataforma 2600, 3600, 3700, 3800; modelos 2610XM, 2620XM, 3620, 3640 y 3662, 2811, 3825, 3845. Cisco ha anunciado el EOS (End Of Sale) para sus modelos 3620 y 3640, entre otros, por lo cual es necesario definir las infraestructuras con los nuevos equipos Cisco que sustituyen a los modelos referidos.

Los nuevos modelos utilizados son de la familia 2800 (sólo mininodos), 3700 y 3800 en cada una de las infraestructuras tipo de nodo de acceso se define la distribución de módulos y el equipamiento que debe llevar cada enrutador. Los nuevos nodos de acceso deben ser enrutadores de las familias 2800 (sólo mininodos), 3700 ó 3800, el modelo dependerá del tipo de nodo de acceso a instalar, ya sea un Centro Telefónico (CTT), Centro de Trabajo (CTR), una Oficina Comercial (OCO) ó una Central (CTL). Cisco menciona que la mayoría de los módulos utilizados en la plataforma 3600 son soportados por las plataformas 3700 y 3800, pero no implica que un módulo de plataforma 3600 por defecto sea soportado en ambas plataformas. Adicional a la salida de venta de modelos de enrutadores también se tiene EOS (End Of Sale) de ciertos módulos, el archivo de control donde se tiene el ciclo de vida de enrutadores.

Anteriormente cada aplicación con puerto de gestión Ethernet en Centrales Telefónicas era implementada a través de puertos Ethernet exclusivos en los Nodos de Acceso, vía una conexión directa al nodo o mediante Hubs. Esta forma de asignación de puertos para aplicaciones propicia una subutilización de puertos en el enrutador, agregación de dispositivos de red por aplicación, acceso libre a intrusiones no deseadas, aumento del impacto económico en relación con el costo unitario por puerto Ethernet de enrutador y exige el constante crecimiento de equipos de mayor capacidad en puertos de acceso.

Debido a lo anteriormente mencionado, el área de ingeniería realizó una Solución Técnica que define las políticas de instalación y uso de Switches LAN en Centrales Telefónicas, los cuales fueron evaluados y designados como nodos de acceso LAN de alta disponibilidad. El uso de switches permite integrar adecuadamente a las principales aplicaciones LAN en un sólo nodo satisfaciendo los requerimientos de interconexión, logrando periodos mínimos de interrupción del servicio de red y ventajas como:

- Optimización de la inversión de equipamiento (costo/beneficio) en precio por puerto.
- Gestión y monitoreo eficientes al centralizar las aplicaciones en switches.
- Mayor seguridad al tener el control de la activación de puertos y el aseguramiento por dirección MAC.
- Mejor desempeño al proveer ancho de banda dedicado y dominio de broadcast.

- Instalación y mantenimiento más eficiente al considerar alimentación en –48 VDC y cumplimiento de las normas NEBS (equipos para TELCO).

- Soporte local y remoto sobre las infraestructuras definidas.

La primera aplicación de Central Telefónica en fase de implantación fue el proyecto Telefonía Pública con una cobertura nacional, por lo cual se aprovechó su implementación para crear la infraestructura LAN en Centrales Telefónicas y posteriormente integrar las demás La integración de varias aplicaciones de Central a través del Switch LAN, exige establecer políticas de configuración y uso de los Switches que normen su instalación. Estos Switches se denominarán como: "Switches IP de Central" de alta disponibilidad; en función de las necesidades se tendrá un Switch Primario y un Secundario si es requerido.

Con base en la experiencia obtenida en emisiones anteriores y la implementación de estos switches IP de Central, es posible obtener una retroalimentación de las situaciones presentadas en este proceso. Algunos de los puntos observados fueron:

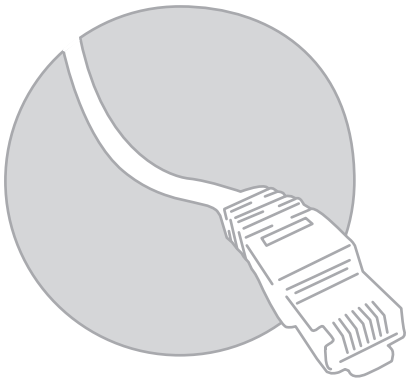
1. No hay coincidencias de aplicaciones en Centrales con relación uno a uno, por lo que la asignación permanente de aplicaciones en puertos del switch genera que existan puertos en el mismo que nunca se ocuparán.

2. La asignación de una 6ª UC de telefonía pública fue una necesidad común en bastantes centrales.

3. Pueden coincidir aplicaciones iguales en algunas Centrales, con la variante de que una es LADA y otra es de la Divisional (local), como sucede con sincronía.

4. La implementación de un Switch de Central en un sólo Nodo de Acceso, implica que en ocasiones todos los dispositivos de aplicaciones se tengan que cablear hasta un punto donde puedan excederse más de 100 mts.

5. Necesidad de redundancia para aplicaciones IP en CTI's, lo que origina proveer una topología robusta y de alta disponibilidad a las mismas, que así lo requieran.



Capítulo 3

Análisis y procedimientos de implementación e integración

Criterios de diseño

Una vez analizados los puntos anteriores, podemos establecer una serie de criterios para garantizar un proceso de implementación más ágil y eficiente de estos switches. Por lo tanto, se han considerado los siguientes criterios:

- La definición de una franja de puertos libres más amplia para integrar nuevas aplicaciones, los cuales se asignarán conforme se presente la necesidad de conectar esas aplicaciones a la RCDT en cada Central.
- La interconexión de UC de telefonía pública en el Switch IP de Central ser en los puertos de franja libre del switch primario secundario.
- Construcción (Src) podrá instalar Switches IP de Central en ms de un Nodo de Acceso en Centrales, esta instalación se debe justificar en base a distancia o factibilidad del cableado.
- Infraestructura redundante para aplicaciones IP de central que lo requieran en CTIs.
- Mayor disponibilidad de puertos en switches IP de central en CTIs

Tomando en consideración cada una de las aplicaciones existentes en la planta y de acuerdo a los requerimientos de interconexión, las topologías LAN posibles de interconexión de switches IP son las mostradas:

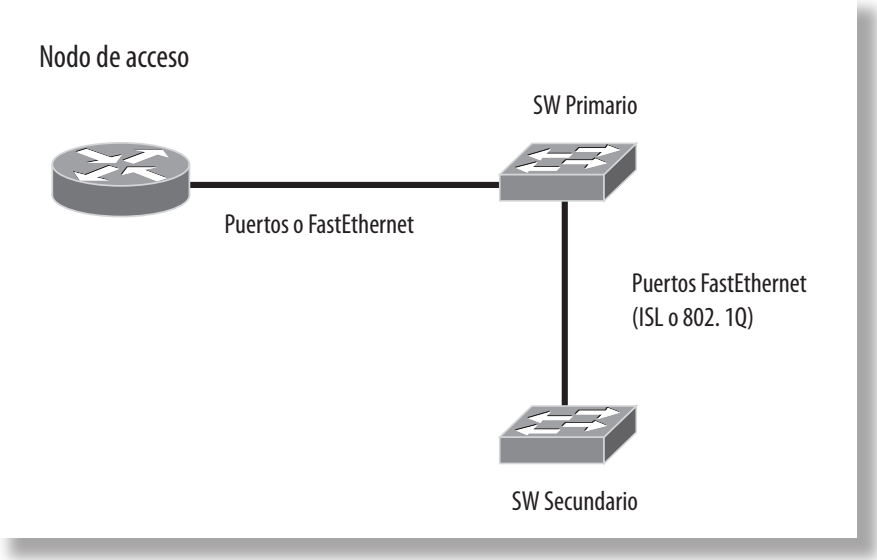


Figura 8. Topología LAN de un switch primario y un swicht secundario.

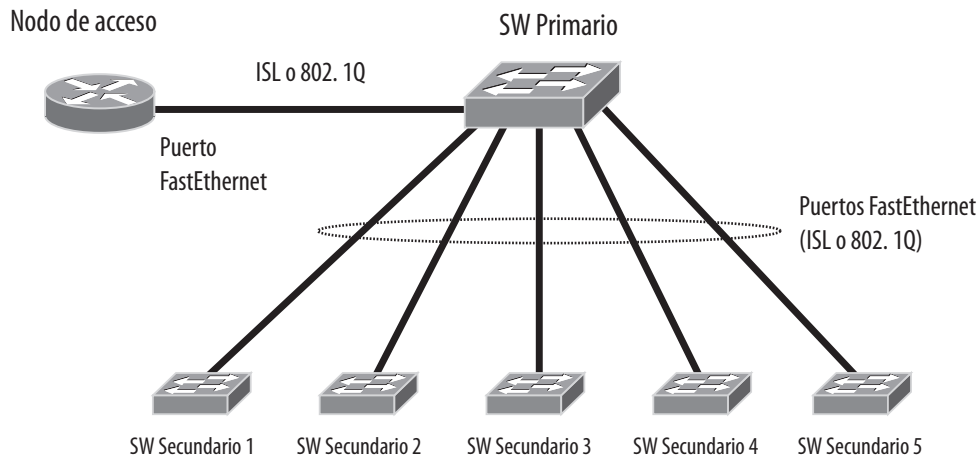


Figura 9. Topología básica de un switch primario y ms de un switch secundario.

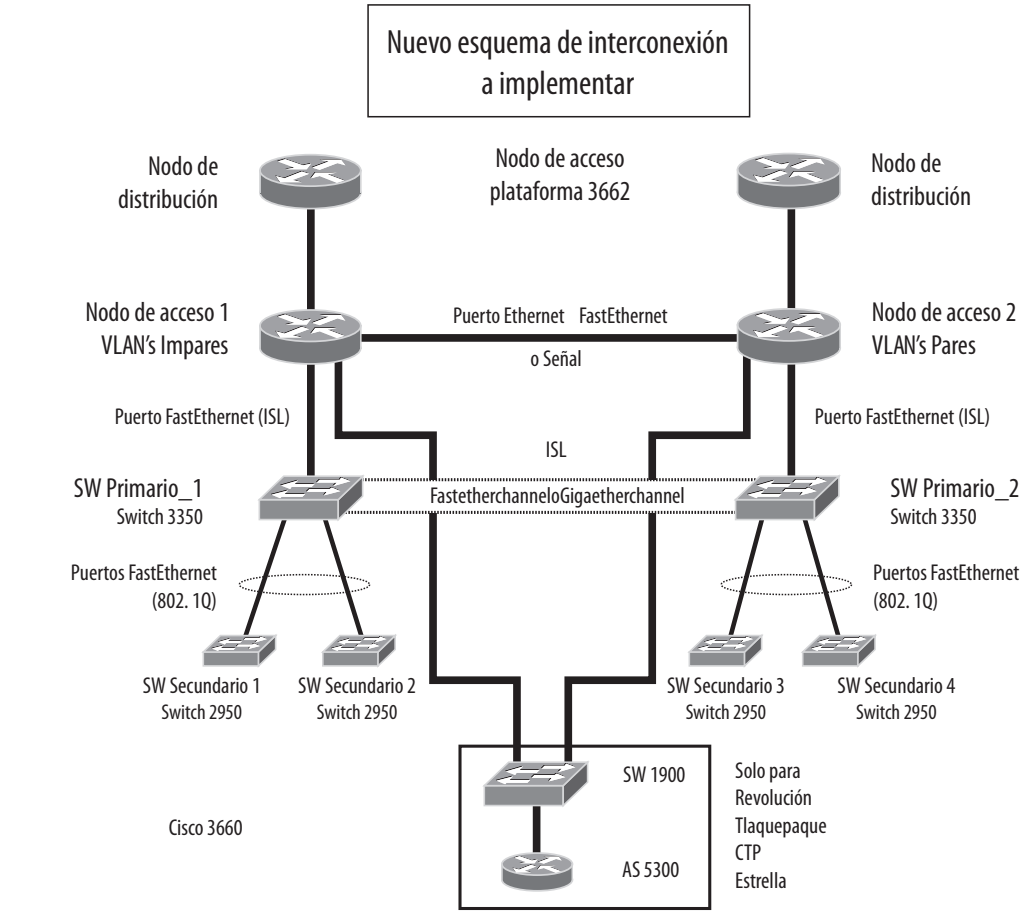


Figura 10. Topología LAN en CTIs.

Es necesario definir y normar los aspectos generales de configuración de gestión y de tráfico para cada uno de los equipos de la red, esto con el fin de recabar información estadística, sincronización de dispositivos, control del sistema operativo de la plataforma y también para evitar puntos de vulnerabilidad que faciliten intrusiones. Dentro de estas consideraciones tenemos SNMP, NTP, TACACS+, líneas de acceso TTY y versión del IOS.

Identificación de características del dispositivo

Dado que los routers y switches son parte integral de la infraestructura de la red es necesario que, con objeto de determinar la relación de comandos apropiados para la configuración de los parámetros de administración (SNMP, NTP y TACACS), se identifiquen algunas características básicas del dispositivo a configurar, esto con el fin de recabar información estadística, sincronización de dispositivos, control del sistema operativo de la plataforma y también para evitar puntos de vulnerabilidad que faciliten intrusiones.

SNMP (Simple Network Management Protocol)

Es un protocolo de capa de aplicación diseñado para facilitar el intercambio de información de administración entre dispositivos de red. Usando datos de SNMP (como paquetes por segundo y tasas de error de red), los administradores de red pueden administrar el rendimiento y planear el crecimiento de la red, asi como encontrar y solucionar problemas de red.

TACACS/TACACS+ (Terminal Access Controller Access Control System)

Protocolo de autenticación, que suministra autenticación de acceso remoto y servicios relacionados, como por ejemplo el registro de eventos. Las contraseñas de usuario se administran en una base de datos central en lugar de administrarse en los dispositivos de forma individual.

NTP (Network Time Protocol)

Es un protocolo de comunicación que permite sincronizar los relojes de un dispositivo que este conectado a la red con un servidor central de tiempo. Con ello se consigue una exactitud del orden de milisegundos en una red local.

Routers

Jerarquía del equipo: Verificar la jerarquía del equipo, la cual puede ser; _do_, _doc_, _di_, _ae_, _naea_, _nas_, _ai_,_ ax_, _ncc_, _ce_, _rr_, _AS_, _cc_ o _ac_

- Versión de IOS: Verificar la versión del sistema operativo (IOS) del equipo, mediante el uso del comando: show Versión De acuerdo a la versión de IOS existen algunas diferencias.

- Password de Enable: Requerido para accesar al nivel privilegiado del equipo Es necesario que el password de enable del dispositivo cumpla con las recomendaciones para la definición de un password seguro, de no cumplir con estas hay que cambiarlo por uno seguro mediante el uso del comando: enable password 0 xxxxxxxx

- Líneas TTY: El uso de TACACS+ en cualquier equipo hace que automáticamente se realice la autenticación en todos los tipos de líneas que existen en el mismo y dado que existen aplicaciones que utilizan las líneas TTY para acceder directamente a sus servidores, es necesario que a

fin de evitar problemas con dichas aplicaciones, en equipos con líneas TTY se deben considerar las líneas adicionales de TACACS+ indicadas en la documentación de las aplicaciones.

Switches

- Importancia del equipo: Verificar si el la jerarquía del equipo, la cual puede ser; _swe_, _swi_, _bb_sw_, _sw_ (edificio importante) o _sw_ (edificio no importante)

- Modelo del equipo: Verificar el modelo del equipo, mediante el uso del comando: show versión De acuerdo al modelo del equipo existen algunas diferencias, siendo las principales la versión de IOS, memoria y capacidad de procesamiento.

Configuración del Dispositivo dentro del servidor de Cisco Secure.

Una vez que se determino que el tipo de autenticación que utilizara el equipo, será TACACS+, se procede a configurar el mismo dentro de la base de datos de CiscoSecure, siguiendo los pasos indicados en el Instructivo para la Configuración de Equipos en CiscoSecure de la RCDT.

Procedimiento de configuración para switches

Se definió una configuración mínima y el procedimiento para implantarla en switches 2950-24 no gestionados por la RCDT, con el fin de minimizar problemas de operación.

La RCDT proporciona a las áreas de sistemas de las Direcciones Divisionales switches modelo 2950-24 para ser integrados a sus infraestructuras de red local, estos switches no son instalados, configurados ni gestionados por la RCDT si no por los administradores de redes locales de cada área. Por sus características inherentes los switches 2950-24 pueden presentar problemas en su operación si no cuentan con una adecuada configuración. Se ha decidido definir una configuración mínima para los equipos 2950-24 no gestionados por la RCDT que evite los problemas detectados y reduzca al mínimo las intervenciones de los administradores de red.

Criterios

A continuación los criterios considerados para definir la configuración mínima:

- Los switches proporcionados por la RCDT a las Divisionales tienen como objeto el reemplazo de concentradores (HUB) en operación.

- La configuración empleada debe deshabilitar todos los parámetros de autonegociación del switch para evitar que éste cambie de su estado originalmente configurado ante la presencia de otro switch, otro concentrador o algún evento de red como un loop, evitando así la intervención del administrador de red local para restaurarlo a su estado original.

- La configuración debe de evitar que el switch vaya al estado de deshabilitación por errores en puertos, disminuyendo así la intervención de los administradores de red en labores de diagnóstico y restablecimiento del equipo o sus puertos.

- Los switches para áreas externas sólo podrán gestionarse localmente por consola, en ellos no se configurarán direcciones IP de gestión reduciendo así la complejidad de la configuración, las posibilidades de conflictos de direcciones y las posibles violaciones de seguridad.

Procedimiento

A continuación se presentan el procedimiento para configurar los switches de las Divisionales que no son gestionados por la RCDT, éste está dividido en 4 pasos: Conexión, Restauración a valores originales, Configuración y Guardado de la configuración.

Conexión

Con el switch 2950 se entrega un cable con un conector RJ-45 y un conector DB-9, este cable es conocido como "De Consola", el extremo RJ-45 se conecta en el puerto "Console" ubicado en la parte posterior del switch y el extremo DB-9 se conecta en el puerto serial de cualquier PC o Lap Top que se vaya a emplear para realizar la configuración del equipo (véase figura 11). Para configurar al equipo es necesario que una vez que el switch esté conectado a la PC o Lap Top se inicie una sesión del programa Hyper Terminal siguiendo la siguiente ruta de menús

Inicio> Programa> Accesorios> Comunicaciones> Hyper Terminal (véase figura 11).

Al dar click en el menú Hyper Terminal se abrirá una carpeta, dentro de ésta aparecerá un ícono con el nombre Hyper Terminal, al dar click en éste arrancará una sesión del programa, ésta solicitará un nombre para identificar a la sesión (véase figura 12), en este caso se empleará "Cisco", al presionar el botón "Aceptar" aparecerá la ventana "conectar con" (véase figura 12):

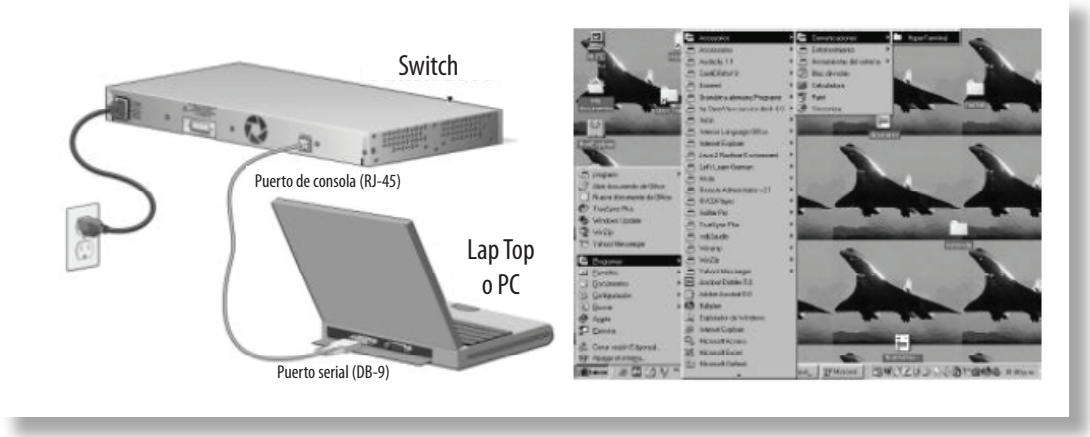


Figura 11.

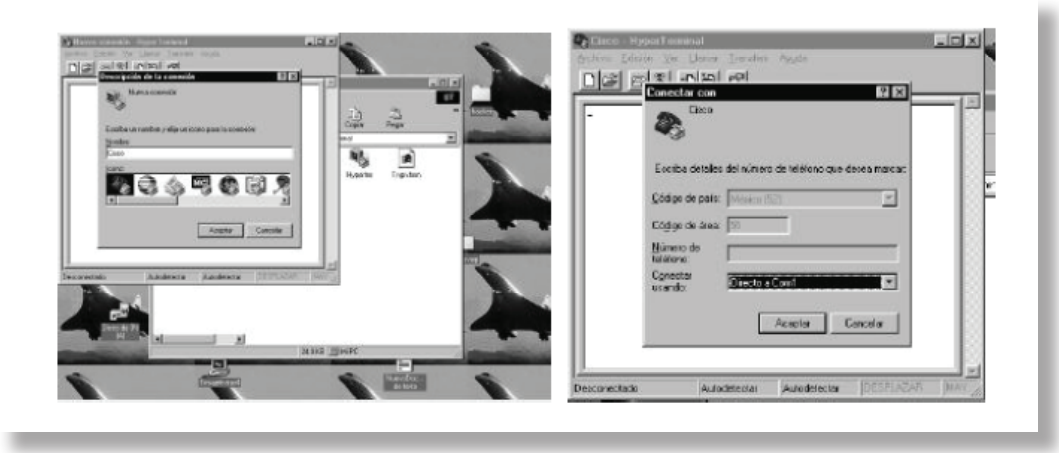


Figura 12.

Dentro de la ventana 4 el parámetro "Conectar usando" debe fijarse a "Directo a Com1", al dar el botón "Aceptar" aparecerá la ventana "Propiedades de COM1" (figura 12) en la que se configurarán los siguientes parámetros:

Bits por segundo	9600
Bits de datos	8
Bits de parada	1
Control de flujo	Ninguno

Configurados los parámetros, al dar el botón "Aceptar" aparecerá la ventana "Cisco-Hyper Terminal" (figura 13), empleando ésta se puede configurar al switch por medio de texto.

Si la conexión al switch se ha establecido exitosamente aparecerá en la ventana el prompt:

"switch>".

El resto del procedimiento y las configuraciones se realizarán empleando la ventana que aparece en la figura 13, se le denominará ventana Hyper Terminal.

Nota: Si en el switch ha sido configurado un password de acceso, el equipo lo solicitará cuando se inicie la ventana de Hyper Terminal, este password de acceso será proporcionado por el administrador que configuró al switch previamente.

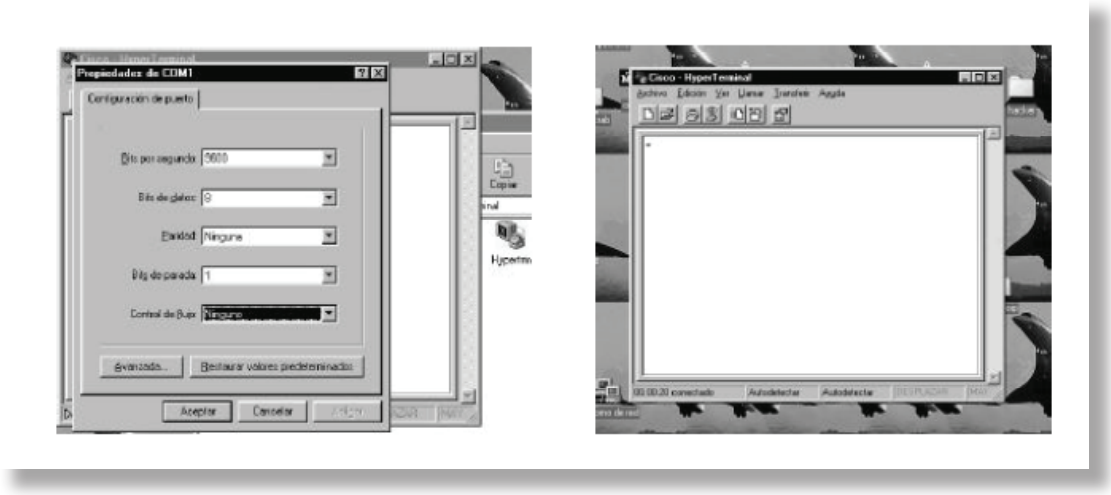


Figura 13.

Restauración a valores originales

Una vez que se tiene conexión al switch por Hyper Terminal se procede a configurarlo a sus valores originales o default, este paso causa que todas las VLANs creadas en el equipo diferentes a la 1 y todas las configuraciones que el equipo tenía sean eliminadas.

Cuando la ventana Hyper Terminal presente el prompt de usuario "switch>" corte de este documento y pegue en ella los comandos sombreados tal y cual aparecen a continuación.

```
enable

delete flash:vlan.dat

erase startup-config

reload
```

El switch se reiniciará a valores de fábrica, durante este proceso que durará aproximadamente 2 minutos aparecerán múltiples mensajes, la indicación de que ha terminado será la aparición del siguiente mensaje: Lo anterior indica que el equipo está listo para ser configurado, y se procederá al siguiente paso que es la configuración.

```
Would you like to enter
the initial configuration
dialog? [yes/no]:
```

Configuración

Para configurar al switch en la ventana Hyper Terminal se deben usar tal y como aparecen aquí los comandos a continuación.

```
no
enable
config terminal
¡
hostname SWITCH
!
! Los siguientes comandos apagan la gestión por HTML del equipo.
!
no ip http server
no ip finger
!
! Con el siguiente comando se configura el password de enable del equipo,
se recomienda usarlo
! por protección.
! enable password XXXX
!
! El siguiente comando evita que el equipo de baja puertos por errores detectados
en ellos.
!
no errdisable detect cause all
¡
! Los siguientes comandos fuerzan al switch a recuperar cualquier puerto dado de
baja después de
! 30 segundos.
!
errdisable recovery cause all
errdisable recovery interval 30
¡
¡ Los siguientes comandos evitan que el switch adquiera una dirección IP en la
¡ Vlan 10, 15 o 255.
¡
interface Vlan1
```

```
 no ip address
 shutdown
¡
¡ Los siguientes comandos configuran la direccion de gestion del switch.
¡
interface Vlan10
 description VLAN DE GESTION
 ip address 10.XX.XX.254 255.255.255.0
 no shutdown
¡
¡ Los siguientes comandos evitan que el switch adquiera una dirección IP.
¡ Con los siguientes comandos se configura a todas las interfaces para que sean
compatibles con
¡ concentradores y para que omitan la autonegociación.
¡
interface range FastEthernet0/1 - 24
description USUARIOS
switchport access vlan 1
switchport mode access
switchport nonegotiate
spanning-tree portfast
no shutdown
¡
! Con estos comandos se obliga al equipo a solicitar un password cuando detecta una
conexión
¡ en su puerto de consola, se recomienda emplear password para evitar accesos no
autorizados.
!
line CON 0
password XXXX
login
!
! Con estos comandos se obliga al equipo a solicitar un password cuando detecta
! una conexión por sesion remota, se recomienda emplear password para
! evitar accesos no autorizados.
!
line VTY 0 - 15
history size 100
exec-timeout 60
password XXXX
login XXXX
!
end
copy running-config startup-config
¡
wr mem
```

Durante la configuración se desplegarán múltiples mensajes, cuando el switch quede configurado su prompt cambiará a:

```
SWITCH#
```

Guardado de la configuración

Para asegurar que el switch guarde la configuración se deben proporcionar los siguientes comandos en el prompt:

```
SWITCH# copy running-config startup-config
```

Para salir del equipo se da el comando "exit" como se muestra a continuación:

```
SWITCH# exit
```

Ahora el equipo se puede emplearse para conectar hosts de usuarios, enrutadores así como pilas de concentradores sin causar problemas.

Se puede salvar la sesión de Hyper Terminal para posteriormente emplearla en la configuración de otros equipos, para esto terminada la configuración en la ventana Cisco-Hyper Terminal se va a la barra de menús y se da "Archivo> Salvar".

Procedimiento de configuración básica para Routers

Se definirá una configuración mínima y el procedimiento para implantarla en Router con una versión de IOS mayor a 12a con el fin de agilizar el proceso de entrega por parte del ingeniero en sitio evitando problemas de conexión con el equipo.

Además de estandarizar algunos aspectos de etiquetación de puertos y uso de interfaces.

Criterios

A continuación los criterios considerados para definir la configuración mínima:

- Los ruteadores implantados por la RCDT a las Direcciones Divisionales tienen como objeto el reemplazo de equipos que no cumplen con las funcionalidades requeridas o que serán parte de una nueva solución para brindar conectividad a la red corporativa.

- La configuración básica empleada debe habilitar el acceso al equipo así como deshabilitar todos los parámetros relacionados a una configuración previa (equipos de rehuso) para evitar problemas de duplicidad de direccionamiento, de listas de acceso, configuración de puertos (Auto negociación), así como parámetros en la conexión de líneas virtuales (gestión) y en general que causen algún evento de red como un loop.

- La configuración debe de evitar que ruteador vaya al estado de auto negociación en puertos, disminuyendo así la probabilidad de una posible desconexión y en consecuencia la pérdida de su gestión.

- Los ruteadores serán gestionados localmente por consola y remotamente por lineas virtuales con usuario y pas-

sword para evitar intrusiones y configuraciones no deseadas.

- En ellos se configurará una dirección IP de gestión a través de una loopback de administración disminuyendo las posibilidades de perdida de conexión por falla en un enlace (en caso de tener dos o mas), además de ser necesario para facilitar tareas de administración.

Procedimiento

A continuación se presentan el procedimiento básico para configurar los ruteadores de las Direcciones Divisionales que son gestionados por la RCDT, éste está dividido en 4 pasos: Conexión, Restauración a valores originales, Configuración y Guardado de la configuración.

Conexión

Con el ruteador se entrega un cable con un conector RJ-45 y un conector DB-9, este cable es conocido como "De Consola", el extremo RJ-45 se conecta en el puerto "Console" ubicado en la parte posterior del switch y el extremo DB-9 se conecta en el puerto serial de cualquier PC o Lap Top que se vaya a emplear para realizar la configuración del equipo (véase figura 1). Para configurar al equipo es necesario que una vez que el switch esté conectado a la PC o Lap Top se inicie una sesión del programa Hyper Terminal siguiendo la siguiente ruta de menús.

Inicio> Programa> Accesorios> Comunicaciones> Hyper Terminal (véase figura 14):

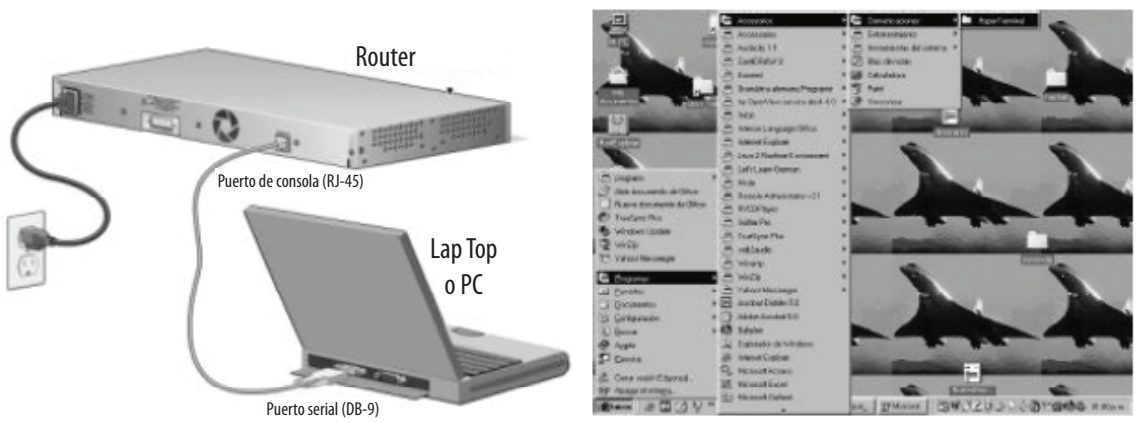


Figura 14.

Al dar click en el menú Hyper Terminal se abrirá una carpeta, dentro de ésta aparecerá un ícono con el nombre Hyper Terminal, al dar click en éste arrancará una sesión del programa, ésta solicitará un nombre para identificar a la sesión (véase figura 15), en este caso se empleará "Cisco", al presionar el botón "Aceptar" aparecerá la ventana "conectar con" (véase figura 15):

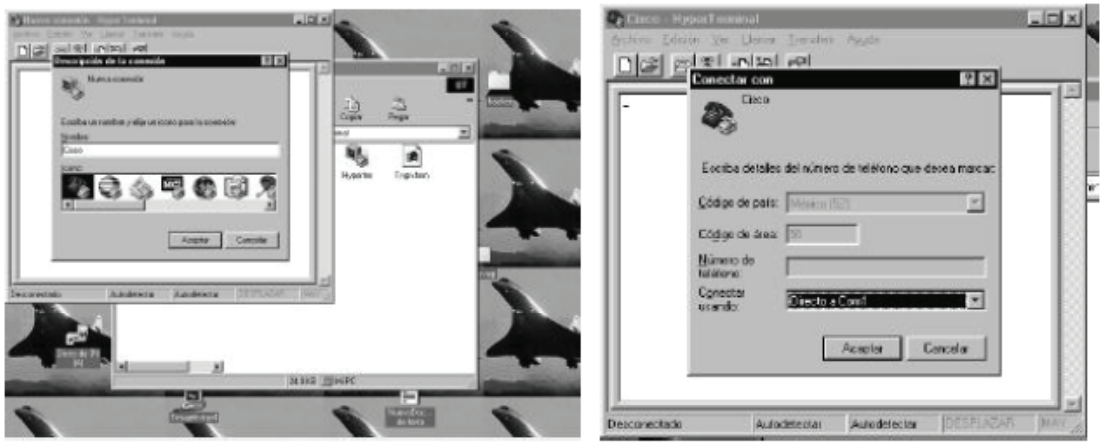


Figura 15.

Dentro de la ventana 4 el parámetro "Conectar usando" debe fijarse a "Directo a Com1", al dar el botón "Aceptar" aparecerá la ventana "Propiedades de COM1" (figura 16) en la que se configurarán los siguientes parámetros:

Bits por segundo	9600
Bits de datos	8
Bits de parada	1
Control de flujo	Ninguno

Configurados los parámetros, al dar el botón "Aceptar" aparecerá la ventana "Cisco-Hyper Terminal" (figura 16), empleando ésta se puede configurar al switch por medio de texto.

Si la conexión al switch se ha establecido exitosamente aparecerá en la ventana el prompt:

"router>".

El resto del procedimiento y las configuraciones se realizarán empleando la ventana que aparece en la figura 16, se le denomina ventana Hyper Terminal.

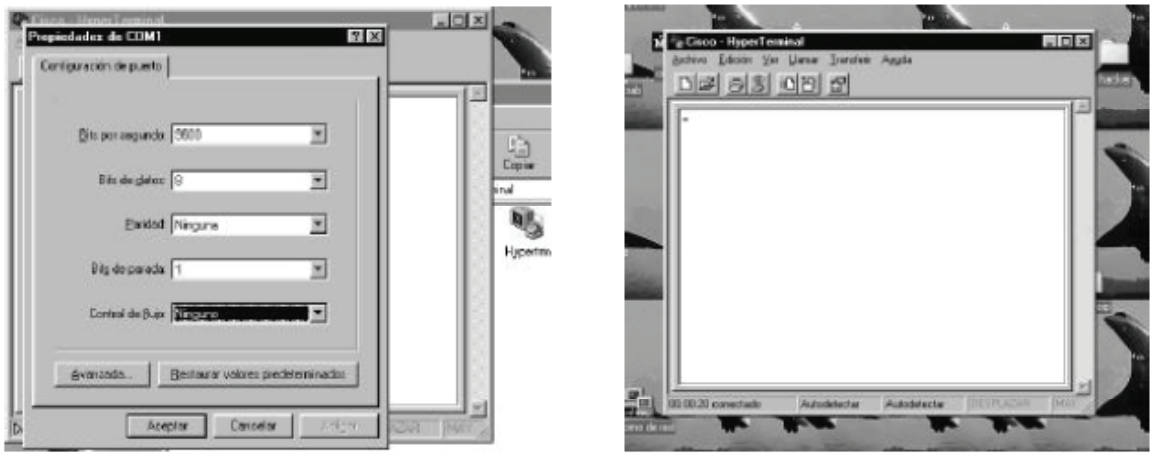


Figura 16.

Nota: Si en el router ha sido configurado un password de acceso, el equipo lo solicitará cuando se inicie la ventana de Hyper Terminal, este password de acceso será proporcionado por el administrador que configuró al router previamente.

Restauración a valores originales

Una vez que se tiene conexión al router por Hyper Terminal se procede a configurarlo a sus valores originales o default, este paso causa que todas las configuraciones que el equipo tenía sean eliminadas.

Cuando la ventana Hyper Terminal presente el prompt de usuario "router>" corte de este documento y pegue en ella los comandos sombreados tal y cual aparecen a continuación.

```
enable

erase startup-config

reload
```

El router se reiniciará a valores de fábrica, durante este proceso que durará aproximadamente 2 minutos aparecerán múltiples mensajes, la indicación de que ha terminado será la aparición del siguiente mensaje:

```
Would you like to enter the initial
configuration dialog? [yes/no]:
```

Lo anterior indica que el equipo está listo para ser configurado, no responda a la pregunta ni proporcione ningún comando y proceda al siguiente paso "Configuración".

Configuración

Para configurar al router en la ventana Hyper Terminal se deben introducir los comandos sombreados a continuación modificando los direccionamientos de enlaces:

```
no
enable
config terminal
¡
hostname ROUTER
!
! Los siguientes comandos apagan la gestión por HTML del equipo.
!
no ip http server
no ip finger
no ip domain lookup
ip subnet-zero
!
! Con el siguiente comando se configura el password de enable del equipo, se
! recomienda usarlo por protección.
!
```

```
enable password XXXX
!
!
! Con las siguientes lineas de comandos se configura la Interface loopback del
equipo.
!
interface Loopback10
 description ROUTER S/N: #########
 ip address 10.XX.XX.ZZ 255.255.255.255
!
! Se configura la interface para que la velocidad sea fijo y no se propensa a
! desconexiones por autonegociacion
!
!
interface FastEthernet0/0
 description ENLACE BACK-TO-BACK HACIA SWITCH
 duplex half
 speed 100
!
! Es necesario definir una subinterface para la gestion por la VLAN 10 o VLAN 255 o
! VLAN 15 con la finalidad de estandarizar los nodos de acceso.
!
interface FastEthernet0/0.10
 description VLAN DE GESTION
 ip address 10.XX.XX.YY 255.255.255.0
 duplex half
 speed 100
!
! Se configura controladora para la gestion del enlace (Generalmente E1).
!
controller E1 0/1/0
 framing NO-CRC4
 channel-group 1 timeslots 1-30
 description ENLACE BACK-TO-BACK A ROUTER DISTRIBUCION
!
! Se configura una ruta enlace hacia el equipo de distribución.
!
interface Serial0/1/0
 description ENLACE BACK-TO-BACK A ROUTER DISTRIBUCION
 bandwidth 256
 ip address 10.XX.XX.WW 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
```

```
 no ip route-cache cef
 no ip route-cache
 fair-queue
!
! Se configura una ruta de salida para el equipo superior de distribución.
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
!
! Con estos comandos se obliga al equipo a solicitar un password cuando detecta
! una conexión en su puerto de consola, se recomienda emplear password para
! evitar accesos no autorizados.
!
line CON 0
history size 100
exec-timeout 60
password XXXX
login XXXX
!
!
! Con estos comandos se obliga al equipo a solicitar un password cuando detecta
! una conexión por sesion remota, se recomienda emplear password para
! evitar accesos no autorizados.
!
line VTY 0 – 15
history size 100
exec-timeout 60
password XXXX
login XXXX
!
end
copy running-config startup-config
¡
wr mem
```

Durante la configuración se desplegarán múltiples mensajes, cuando el switch quede configurado su prompt cambiará a:

```
ROUTER#
```

Guardado de la configuración

Para asegurar que el router guarde la configuración se deben proporcionar los siguientes comandos en el prompt:

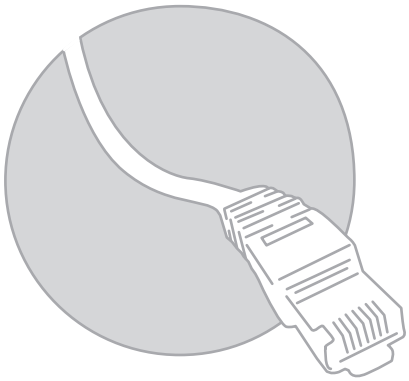
```
ROUTER# copy running-config startup-config
```

Para salir del equipo se da el comando “exit” como se muestra a continuación:

```
ROUTER# exit
```

Ahora el equipo se puede emplearse para conectar hosts de red, enrutadores así como pilas de switches sin causar problemas.

Se puede salvar la sesión de Hyper Terminal para posteriormente emplearla en la configuración de otros equipos, para esto terminada la configuración en la ventana Cisco-Hyper Terminal se va a la barra de menús y se da “Archivo> Salvar”.



Capítulo 4

Integración de solución técnica

El objetivo de la Subgerencia de administración de configuraciones de la RCDT es la de verificar, aprobar, ejecutar y administrar los cambios que se harán a la red.

El área de clientes inicia el proceso al establecer alguna solución técnica para los requerimientos de alguna de las áreas de edificios corporativos, centros telefónicos, centros de trabajo, oficinas comerciales, etc. Se estiman el número de usuarios, el costo/beneficio de la inversión, tipo de equipo a solicitar, la proyección de crecimiento entre otros aspectos.

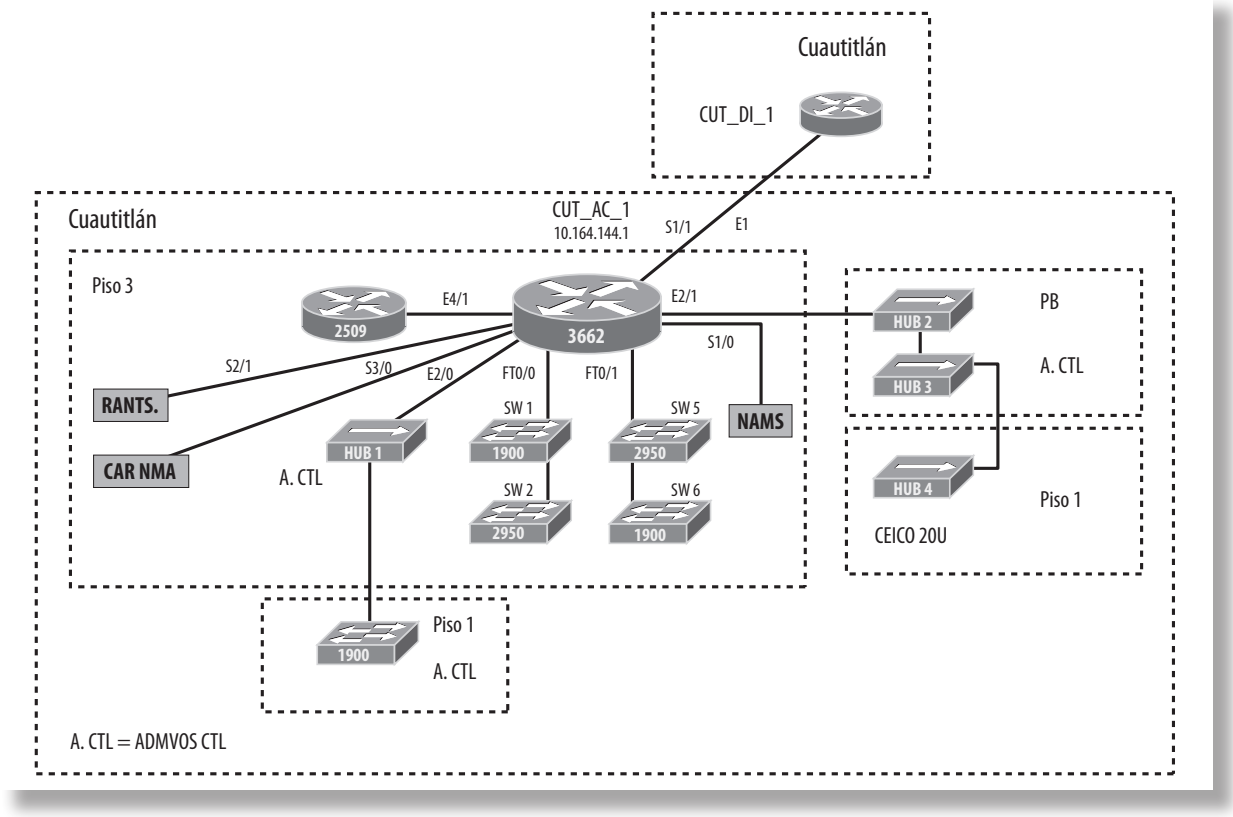


Figura 17. Situación inicial de la central Cuautitlán

Una vez que se ha aprobado la solución, el Área de Ingeniería se encargara de diseñar la solución final, lo cual incluye las pruebas a la topología, cargas de tráfico, seguridad, calidad de servicio, redundancia, alta disponibilidad (si es que lo requiere), etc.

Se elabora un documento en donde se plasma el proyecto final, que incluye todos los aspectos los requerimientos del cliente, el equipo requisitado, su ubicación, conexión y administración, responsabilidad de actividades y finalmente los detalles de configuración y sistema operativo.

Por cada actividad se generara una orden de trabajo a través del sistema HP Openview, el cual es una herramienta que integra una base de datos de los objetos de la red, de los trabajos que en ellos se realiza o las actividades que se desempeñan en cada área. Esta orden de trabajo será asignada a un ingeniero del área de configuraciones (Srrc) quien estará como responsable de la correcta implantación y operación de este cambio. Por lo tanto mis actividades consistían la implementación de la solución técnica en la parte de configuración y gestión central.

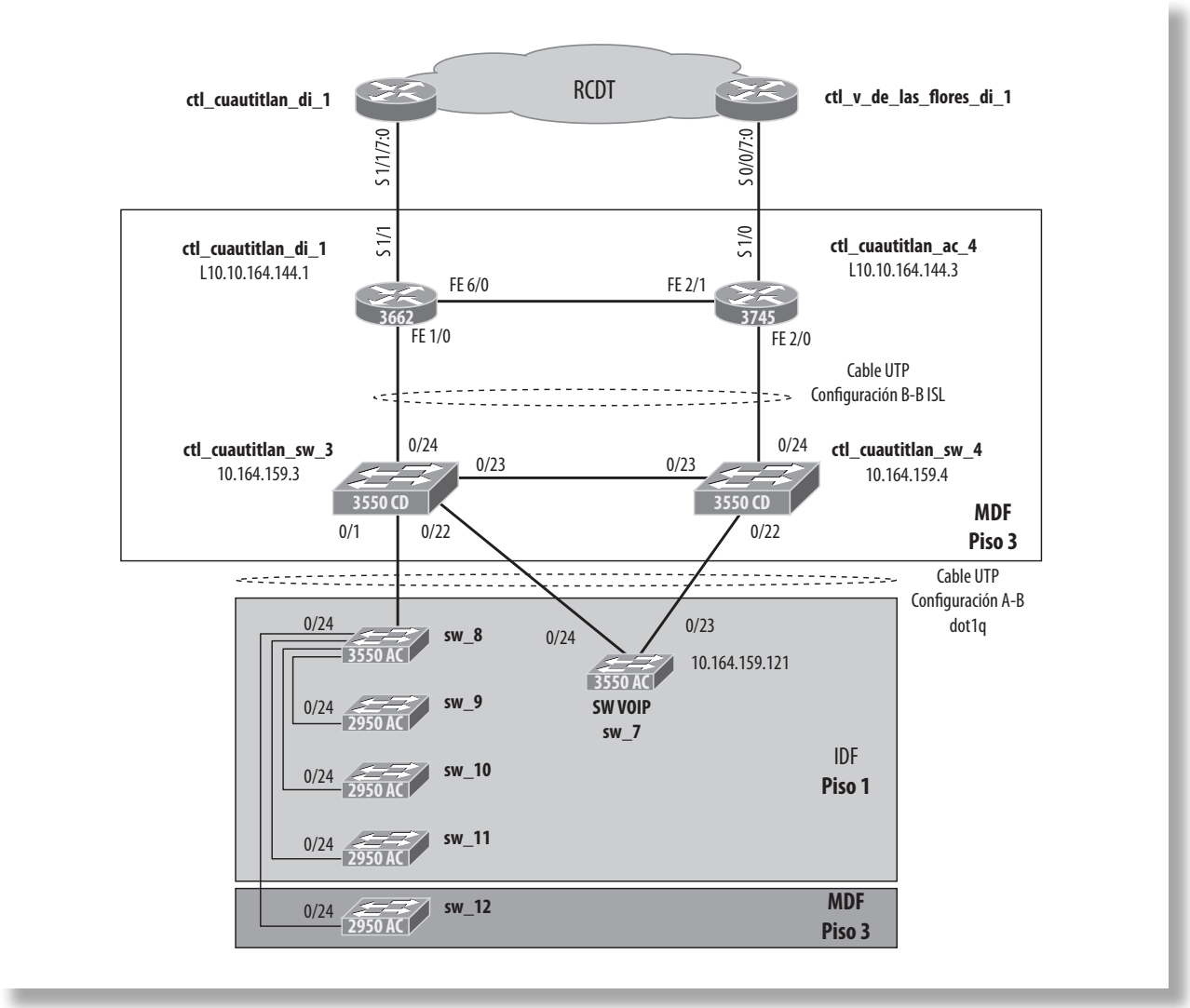


Figura 18. Topología propuesta VoIP-AT

El primer punto era revisar la solución final y verificar que todas las partes tuvieran congruencia para poder ser implementadas, es decir, que al momento de ser ejecutadas los direccionamientos fueran correctos, se hubieran pedido el número de equipos y módulos necesarios y correctos, la versión de sistema operativo soportara la lógica de conexión y carga de proceso, también era necesario verificar la asignación de direccionamiento lógico (su asignación, su reutilización, las redes dadas de baja, el direccionamiento automático, además de revisar el direccionamiento de usuario).

En caso de encontrar algún detalle, es necesario notificar al área respectiva y solicitar la generación de un nuevo documento (una revisión), con la corrección y o solución de de error o inconsistencia observada.

En cuanto a la actividad también deben ser notificadas las entidades de monitoreo central de la red: Centro de Operación de la Red Nacional (CORN), Centro Regional (CAR) y CNS, esto con el fin de enterarlos de las actividades programadas y acordar una fecha para su ejecución (con esto se evita el traslape de actividades o afectación a los servicios), esto debe ser hecho con un mínimo de 72 horas de anticipación, y se programaran en un calendario general de actividades.

La mayor parte de las actividades necesitan del apoyo de un ingeniero del área de construcción o personal regional de administración de esa red, ya que se puede presentar algún problema con la gestión remota de los equipos y será necesaria la intervención en sitio para aminorar los efectos de una posible falla en el servicio.

Para optimizar el desarrollo de la actividad es necesario preconfigurar los equipos para lo cual se le enviara esta configuración base a los ingenieros de sitio que se encargaran entregar los switches o routers para su gestión y termino de configuración remota. También son encargados de revisar que la infraestructura este totalmente adecuada (cableado estructurado, sites, entrega de enlaces, energía eléctrica, clima, etc)

Por mi parte, es necesario preparar la configuración de los equipos, su integración a los sistemas de seguridad, revisión de aplicaciones, protocolos y segmentos de red.

Los horarios para las intervenciones a la red son en su mayor parte nocturnos, debido a que en este periodo las afectaciones son menores por haber un menor número de usuarios activos. Dependiendo de la magnitud y criticidad de la actividad se otorga lo que se conoce como una ventana de mantenimiento, que es el tiempo estimado de impacto a la red por el trabajo planeado y durante este periodo se desactivaran los sistemas de monitoreo y alarmas de los equipos afectados.

Una vez llegado el día y hora acordado, se procedía a la notificación de inicio a las tres entidades de operación y mantenimiento (CAR, CNS, CORN)

Una vez comenzada la actividad se realizaban los siguientes puntos:

Integración

- Añadir a gestor (Cisco Works)
- Checar configuración básica (conexión, direccionamiento, administración)
- Revisión de hardware, software.
- Configuración de puertos, QoS, seguridad y acceso remoto.
- Validar rutas, tráfico, gestión y conectividad de equipos en puertos.
- Notificar fin de la actividad.
- Agregar a inventario.

Migración (reingeniería)

- Respaldar configuración actual de cada equipo al iniciar la actividad.
- Modificar/añadir a gestor (Cisco Works)
- Checar configuración básica (conexión, direccionamiento, administración)
- Revisión de hardware, software.
- Configuración de puertos, QoS, seguridad y acceso remoto.
- Validar rutas, tráfico, gestión y conectividad de equipos en puertos.
- Notificar fin de la actividad y documentar cambios y detalles.
- Actualizar inventario.

Baja

- Respaldar configuración actual de cada equipo al iniciar la actividad.
- Remover del gestor (Cisco Works)
- Eliminar configuración en nodos vecinos.
- Notificar fin de la actividad y documentar baja de equipo.
- Actualizar inventario.

Al finalizar las actividades el primer punto es volver a verificar el hardware y versión de sistema operativo (IOS) que has sido entregado: Modelo del equipo, tarjetas instaladas, módulos instalados, memoria FLASH, registro de configuración, versión de IOS correspondiente a la última versión recomendada por el proveedor CISCO.

```
ctl_cuautitlan_ac_1#sh run
Building configuration...

Current configuration 29028 bytes
!
Last configuration change at 02:02:23 MEXICO Fri Jan 13 2006 by mexusc08
NVRAM config last updated at 05:02:54 MEXICO Fri Jan 13 2006 by mexusc33
!
version 12.3
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname ctl_cuautitlan_ac_1
!
boot-start-marker
boot system flash:c3660-telcoent-mz.123-9a.bin
boot system flash slot0:c3660-telcoent-mz.121-1.T.bin
boot-end-marker
!
card type e1 5
logging buffered 4096 debugging
```

```
enable password 7 XXXXXXXXXXXXXXXXX
!
!
!
!
!
[LINEAS OMITIDAS]
!
end

ctl_cuautitlan_ac_1#sh ver
Cisco Internetwork Operating System Software
IOS (tm) 360Software (C3660-TELCOENT-M), Version 12.3(9a), RELEASE SOFTWARE (fc4)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Thu 22-Jul-04 17:1by kellythw
Image text-base0x60008AF4, data-base0x620A0000

ROMSystem Bootstrap, Version 12.0(6r)T, RELEASE SOFTWARE (fc1)

ctl_cuautitlan_ac_1 uptime is 34 weeks, 2 days, 8 hours, 23 minutes
System returned to ROM by power-on
System restarted at 22:17:28 MEXICO Tue May 17 2005
System image file is flash:c3660-telcoent-mz.123-9a.bin

cisco 3660-telco (R527x) processor (revision 1.0) with 116736K/14336K bytes of memory

.
Processor board ID JMX0619K5PZ
R527x CPU at 225MHz, Implementation 40, Rev 10.0, 2048KB L2 Cache
Channelized E1, Version 1.0.
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 199by Meridian Technology Corp).
TN327Emulation software.
Primary Rate ISDN software, Version 1.1.


366Chassis typeTELCO
6 Ethernet/IEEE 802.3 interface(s)
4 FastEthernet/IEEE 802.3 interface(s)
45 Serial network interface(s)
4 Channelized E1/PRI port(s)
DRAM configuration is 64 bits wide with parity disabled.
```

```
125K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)
16384K bytes of processor board PCMCIA Slotflash (Read/Write)

Configuration register is 0x2102
!
End
```

El siguiente paso es revisar la configuración correcta del equipo, (running-config, starup-config), la gestión del equipo local y remoto, su direccionamiento de gestión y de usuarios (en el caso de dispositivos de capa 3); y finalmente la vecindad con los equipos que están conectados directamente (la cantidad de equipos iniciales debe ser igual a la cantidad de equipos finales).

```
ctl_cuautitlan_ac_1#sh cdp n d
-------------------------
Device IDctl_cuautitlan_ac_4.edo.mex
Entry address(es)
IP address10.190.3.173
Platformcisco 3745,CapabilitiesRouter Switch
InterfaceFastEthernet6/0,Port ID (outgoing port)FastEthernet2/1
Holdtime 132 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 370Software (C3745-JS-M), Version 12.3(6e), RELEASE SOFTWARE (fc3)
Technical Supporthttp://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Fri 01-Apr-05 02:27 by hqluong

advertisement version2
VTP Management Domain''
Duplexfull
-------------------------
Device IDctl_cuautitlan_sw_3.edo.mex
Entry address(es):

!
!
[LINEAS OMITIDAS]
```

```
ctl_cuautitlan_ac_1#sh run
Building configuration...

Current configuration 29028 bytes
!
Last configuration change at 02:02:23 MEXICO Fri Jan 13 2006 by mexusc08
NVRAM config last updated at 05:02:54 MEXICO Fri Jan 13 2006 by mexusc33
!
!
[LINEAS OMITIDAS]
!
!
interface FastEthernet1/0
 description ENLACE BACK-TO-BACK A CTL_CUAUTITLAN_SW_2 (CJHC, 12/01/06)
 no ip address
 speed 100
 full-duplex

interface FastEthernet1/0.2
 description PUERTO ASIGNADO A PROYECTOSVOIP CEICOS++ (CJHC, 12/01/06)
 encapsulation isl 2
 ip address 13.49.117.252 255.255.255.secondary
 ip address 10.164.158.125 255.255.255.128
 no ip redirects
 standby 2 ip 10.164.158.126
 standby 2 ip 13.49.117.254 secondary
 standby 2 timers 8 24
 standby 2 priority 95
 standby 2 preempt
 standby 2 authentication VLAN2
 standby 2 track Serial1/1:5
!
interface FastEthernet1/0.3
 description PUERTO ASIGNADO A PROYECTOSRED LOCAL++ (CJHC, 12/01/06)
 encapsulation isl 3
 ip address 13.49.140.254 255.255.255.secondary
 ip address 10.164.158.254 255.255.255.128
 no ip redirects
!
interface FastEthernet1/0.255
 description PUERTO ASIGNADO A PROYECTOSVLAN ADMON++ (CJHC, 12/01/06)
 encapsulation isl 255
 ip address 10.164.159.61 255.255.255.192
 no ip redirects
```

```
 standby 255 ip 10.164.159.62
 standby 255 timers 8 24
 standby 255 preempt
 standby 255 authentication VLAN255
 standby 255 track Serial1/1:8
!
!
[LINEAS OMITIDAS]
!
end

ctl_cuautitlan_ac_1#sh arp
ProtocolAddressAge (min)Hardware Addr Type Interface
Internet10.164.159.61 - 0008.e395.b0d ARPA FastEthernet1/0.255
Internet10.164.159.6 30011.9399.8181ARPA FastEthernet1/0.255
Internet13.73.72.1 30004.75e7.2d14ARPA FastEthernet0/0.2
Internet10.164.157.62 - 0008.e395.b0c ARPA FastEthernet0/0.4
Internet13.73.72.2000b.ab05.9e6aARPA FastEthernet0/0.2
Internet10.164.159.62 - 0000.0c07.acffARPA FastEthernet1/0.255
Internet13.49.140.16228 0080.4545.f8ecARPA FastEthernet1/0.3
Internet10.190.3.174- 0008.e395.b12 ARPA FastEthernet6/0
Internet10.190.3.173182 0011.9399.8182ARPA FastEthernet6/0
Internet10.164.158.16 6 0009.6bd8.657aARPA FastEthernet1/0.2
Internet13.134.82.251 2 0012.0152.2c8 ARPA FastEthernet0/1.15
Internet13.134.82.252 0014.6af9.7c8 ARPA FastEthernet0/1.15
!
!
[LINEAS OMITIDAS]
!
```

Correcta activación de interfaces y subinterfaces (puertos, loopback , vlans). Es importante dejar desactivados los puertos que no son usados para evitar ataques al equipo y a la red o intrusiones de usuarios no permitidos que se reflejan en un consumo del ancho de banda.

```
ctl_cuautitlan_ac_1#sh ip int br
InterfaceIP-AddressOK? Method StatusProtocol
FastEthernet0/ unassignedYES NVRAMupup
FastEthernet0/0.1unassignedYES manual deleted down
FastEthernet0/0.213.73.72.254YES NVRAMupup
```

```
FastEthernet0/0.313.72.95.254YES NVRAMupup
FastEthernet0/0.410.164.157.62 YES manual upup
FastEthernet0/0.110.164.150.254YES NVRAMupup
FastEthernet0/0.31 10.164.156.6YES manual upup
FastEthernet0/1unassignedYES NVRAMupup
FastEthernet0/1.1unassignedYES NVRAMdeleted down
FastEthernet0/1.2unassignedYES unsetupup
FastEthernet0/1.313.72.234.254 YES NVRAMupup
FastEthernet0/1.5unassignedYES unsetupup
FastEthernet0/1.6unassignedYES unsetdeleted down
FastEthernet0/1.7unassignedYES unsetupup
FastEthernet0/1.8unassignedYES unsetupup
FastEthernet0/1. unassignedYES unsetupup
FastEthernet0/1.1unassignedYES unsetupup
FastEthernet0/1.11 unassignedYES unsetupup
FastEthernet0/1.15 13.134.82.254 YES manual upup
FastEthernet1/ unassignedYES manual upup
FastEthernet1/0.210.164.158.125YES manual upup
FastEthernet1/0.310.164.158.254YES manual upup
FastEthernet1/0.25510.164.159.61 YES manual upup
Serial1/0: 10.164.153.6YES NVRAMupup
Serial1/0:110.164.153.14 YES NVRAMupup
Loopback110.164.144.1YES NVRAMupup
Loopback80 10.164.144.48 YES manual upup
Loopback80210.164.144.5YES NVRAMupup
Loopback80310.164.144.51 YES manual upup
Tunnel5unassignedYES NVRAMupup
Tunnel70 unassignedYES NVRAMupup
Tunnel701unassignedYES NVRAMupup
!
!
[LINEAS OMITIDAS]
```

Revisión de los parámetros de seguridad (TACACS), listas de acceso(IP's permitidas), estadísticas (SNMP), reloj (NTP), así como la revisión de líneas de configuración de QoS y la baja del segmento de red 13.0.0.0.

```
ctl_cuautitlan_ac_1#sh run
Building configuration...
```

```
Current configuration 29028 bytes
!
Last configuration change at 02:02:23 MEXICO Fri Jan 13 2006 by mexusc08
NVRAM config last updated at 05:02:54 MEXICO Fri Jan 13 2006 by mexusc33
!
!
!
!
!
aaa authentication fail-message ^CC
Su Acceso a Tacacs+ es incorrecto,
Verifique sus Datos o su cuenta sera desactivada. ^C
aaa authentication password-prompt Introduzca-su-Password:
aaa  authentication  username-prompt  Servidor-de-Tacacs+-fuera-de-servicio-
introduzca-s
u-usuario-local:
aaa authentication login default group tacacs+ enable local
aaa authentication enable default group tacacs+ enable
aaa authorization config-commands
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
!
!
!
[LINEAS OMITIDAS]
!
!
tacacs-server host 13.12.176.XX
tacacs-server host 13.12.176.XX
tacacs-server host 10.108.129.XX
tacacs-server directed-request
tacacs-server key XXXXXXXXXXX
!
!
!
access-list 1 permit 10.108.129.XX 0.0.0.127
access-list 1 permit 10.105.25.XX 0.0.0.127
access-list 2 permit 10.108.129.XX
```

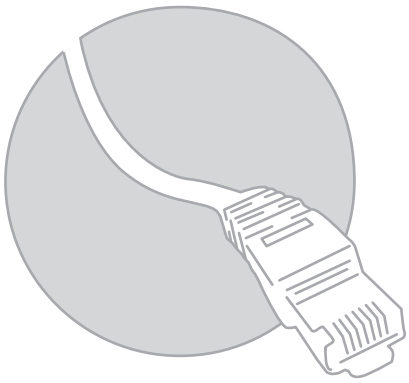
```
access-list 2 permit 10.108.129.XX
access-list 2 permit 10.108.129.XX
access-list 2 permit 10.108.129.XX
!
!
!
[LINEAS OMITIDAS]
!
!
snmp-server engineID local 00000009020000602FA44D09
snmp-server community XXXXXXXXX RO 2
snmp-server community XXXXXXXXX RW 2
snmp-server community XXXXXXXXX RO 1
snmp-server trap-source Loopback10
snmp-server location DIRECCION Y CONTACTO DE LA RCDT
snmp-server enable traps tty
snmp-server host 10.105.XX.XX XXXXXXXXX
snmp-server host 13.12.XX.XX XXXXXXXXX

!
ntp authentication-key 2 md5 XXXXXXXXXXX 7
ntp authenticate
ntp trusted-key 2
ntp clock-period 17180385
ntp source Loopback10
ntp server 10.111.XX.XX key 2 source Loopback10
ntp server 10.111.XX.XX key 2 source Loopback10
!
[LINEAS OMITIDAS]
!
End
```

Una vez hecha la revisión, se notifica del término de la actividad ha cada una de las entidades involucradas las cuales validaran el correcto funcionamiento de sus aplicaciones y de sus gestores, ademas tendrán conocimiento que se han hecho cambios a la topología de la red.

Una vez puesto en operación se procede al llenado de una base de datos en los cuales se capturan los datos de los equipos involucrados en la actividad, esto con el fin de llevar un control estadístico y de consulta de cada uno de los dispositivos tanto físicamente (hardware) como lógicamente (gestión, direccionamiento, interfaces lógicas como vlans, loopbacks; proyectos involucrados, versiones de software, etc).

Finalmente se verifica el correcto poleo de configuración, estadísticas y alarmas a través del gestor Cisco Secure.



Capítulo 5

Resultados

Mi formación como ingeniero en la carrera de telecomunicaciones, me ha permitido desarrollar una visión para la integración de soluciones y adecuaciones a la red de telecomunicaciones que han cumplido la meta de ofrecer servicios de alta disponibilidad y tecnología de punta enfocados tanto a clientes corporativos como al mercado masivo.

Gracias a la integración de nuevas soluciones, se ha estandarizado la red a un modelo por niveles, con lo cual se han optimizado los recursos otorgando una mayor disponibilidad y un rápido acceso al usuario final, sin mencionar una mayor eficiencia en el consumo de procesamiento en la parte de ruteo.

Estas acciones permitirán hacer uso de nuevas tecnologías como lo es VoIP ya que se cuenta con equipos de mayor capacidad, un esquema eficiente de ruteo que mejora los tiempos de respuesta en la comunicación; en la parte de acceso la integración de QoS a las soluciones es fundamental para diferenciar el tipo de tráfico y asignarle una prioridad diferente según sea su importancia.

En la parte de conmutación siempre es importante la definición de redes virtuales para separar el tráfico y no interferir con la red virtual nativa que utilizan los mismo switches para realizar sus procesos. Con las soluciones integradas las aplicaciones y soluciones que ya se encontraban operativas tengan acceso a la red bajo una estandarización, lo que permite brindar una seguridad inicial de conexión, disponibilidad de puertos, minimizar tráfico entre redes e integración de proyectos a la red. Cabe resaltar que a la par se optimizo la asignación de recursos lo cual evita un desperdicio de asignación de puertos y/o equipos a proyectos específicos que no los utilizaran en su totalidad.

Para realizar esta adecuación de servicios fue necesaria la migración de los equipos de centrales para que soportaran una mayor carga de procesos lo que significa migraciones de plataforma, actualización en las versiones de sistema operativo, incremento en la capacidad de hardware como tarjetas procesadoras, numero de puertos, dispositivos de almacenamiento como flash y discos, capacidad de tarjetas de enlace.

Estos cambios fueron soportados por la adecuación del sitio en cuanto a requerimientos de potencia (fuerza), dimensiones de los sitios de comunicaciones, sustitución o implementación de cableado estructurado y finalmente la puesta en punta de enlaces de alta capacidad para la salida de tráfico de comunicaciones.

Es necesario mencionar la organización logística, pues se debe de afectar lo menos posible los servicios. Así que se debe coordinar con los clientes y las diversas entidades corporativas el momento adecuado de ejecución de las actividades. Este aspecto es de vital importancia y que de acuerdo al calendario actividades como facturación, envió de información entre servidores, ejecuciones de otros trabajos planeados, y la productividad misma de las áreas comerciales puede mermarse o en el mejor de los casos degradarse y provocar conflictos de ejecución en el caso de los otros trabajos planeados. De la fecha y duración de la ventana de mantenimiento depende también la disponibilidad de los recursos ya que los ingenieros que asisten a sitio tienen una agenda de actividades y si una actividad no es programada con anticipación puede desencadenar un desfasamiento en la ejecución de todas las actividades que tienen asignados la gente en sitio.

Como resultado de la consideración de cada uno de los aspectos anteriormente mencionados se tiene la integración a un nuevo esquema de operación de un gran número de centrales, centros de trabajo, centrales telefónicas, oficinas comerciales, oficinas administrativas y oficinas corporativas a lo largo de toda la republica que permite a los usuarios y aplicativos realizar sus funciones de una manera optima en cuanto a comunicación se refiere garantizándose la entrega de información, calidad de comunicación por voz y video, confiabilidad de acceso a la intranet e internet optimizando los recursos asignados y explotando su capacidad lo más posible.

Conclusiones

Como consecuencia del crecimiento de la RCDT, se debe de analizar, comparar e implementar nuevas soluciones tecnológicas que permitan un desempeño cada vez mas eficiente, confiable y seguro del transporte de la información en conjunto con la calidad de servicio que se requiere para las diversas aplicaciones y servicios de usuario.

Las consideraciones necesarias para la migración de servicios de datos contemplan los aspectos de preparación, planeación, diseño, implementación, operación y optimización.

En primer lugar se debe establecer una justificación financiera para el tipo de negocio. Y se debe proyectar el crecimiento para reducir re-trabajos por un corto alcance de la solución o una alta proyección que a la larga significan recursos que podrían no ser utilizados.

La planeación es evaluar los sitios y redes con los que actualmente se cuentan y desarrollar un plan de gestión del proyecto.

El diseño reduce riesgos y re-trabajos y optimiza los tiempos de implementaciones exitosas. También significa conjugar los requerimientos financieros con los requerimientos técnicos de manera comprensiva y detallada.

Como parte de la implementación se deben integrar las soluciones sin interrupciones en los servicios de la red que actualmente opera o sin crear brechas de seguridad (puntos de vulnerabilidad).

Un aspecto importante en el crecimiento de la red es considerar el operación que mantendrá la alta disponibilidad de los recursos y reducirá gastos por fallas no atendidas. Dicho de otra manera el mantenimiento también brinda el aspecto preventivo ante posibles fallas y desviaciones.

Con visión a largo plazo se podrá contemplar la optimización de la red lo que implica aumentar el rendimiento, la disponibilidad, capacidad y la seguridad de la red. Con esto se alcanzara la excelencia operativa a través de la mejora continua del rendimiento y funcionalidad de la red.

Glosario

ARP. Protocolo de Resolución de Dirección (*Address Resolution Protocol*). Protocolo que empleado para correlacionar una dirección IP con una dirección de hardware (MAC).

Bug. Un bug es un error o un defecto en el software o hardware que hace que un programa funcione incorrectamente.

CLNS. Es una abreviatura de Servicio No Orientado a Conexión (*Connectionless Network Service*) Este protocolo no requiere un circuito a ser establecido antes de que se transmitan los datos. CLNS encamina mensajes a su destino independientemente de cualquier otro mensaje.

DB9. El conector DB9 (originalmente DE-9) es un conector analógico de 9 clavijas de la familia de conectores D-Subminiature (D-Sub o Sub-D). Se utiliza principalmente para conexiones en serie, ya que permite una transmisión asíncrona de datos según lo establecido en la norma RS-232 (RS-232C).

EIGRP. Es un protocolo de encaminamiento híbrido, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

Ethernet. Es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI. La Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3. Usualmente se toman Ethernet e IEEE 802.3 como sinónimos

FTP. El Protocolo de Transferencia de Archivos (*File Transfer Protocol*) se utiliza para la transferencia de archivos entre sistemas conectados a una red TCP (*Transmission Control Protocol*), basado en la arquitectura cliente-servidor.

Gateway. Nodo en una red de datos que sirve de punto de acceso a otra red

Gestión de red. Es el monitoreo y control de los recursos de una red con el fin de evitar que llegue a funcionar incorrectamente provocando perdida o degradación del servicio.

HSRP. Es un protocolo propiedad de Cisco Systems para manejar redundancia de capa 3 en el gateway de la LAN.

Hub. Es un concentrador es un equipo de redes que permite conectar entre sí otros equipos y sólo retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Los hubs ya no son utilizados, debido al gran nivel de colisiones y tráfico de red que propician.

IEEE. Corresponde a las siglas de Instituto de Ingenieros Electricistas y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas

Interfaz. Es el puerto por el cual se envían o reciben señales desde un sistema hacia otros.

IOS. Sistema Operativo de Interconexión de Redes (Internetwork Operating System) Sistema operativo creado por Cisco Systems para programar y mantener equipos de transporte en redes de datos.

IP. El Protocolo de Internet (Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados sin garantizar su entrega haciendo uso de la técnica del mejor esfuerzo.

LAN. Una red de área local o red local (*Local Area Network*) es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Está enfocada a conectar campus, edificios o áreas corporativas.

Loop. El bucle (*loop*) se presenta cuando en una red los paquetes pasan por una parte de la trayectoria de la cual no pueden salir porque siempre regresan al punto de partida sin importar el camino que tomen. Pueden ser físicos o lógicos.

Loopback. Es un interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado.

MAC. Control de acceso al medio (*Media Access Control*) es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única de identificación física de un dispositivo de red.

Memoria flash. Es una forma desarrollada de la memoria EEPROM que permite que múltiples posiciones de memoria sean escritas o borradas en una misma operación de programación mediante impulsos eléctricos.

OSI. El modelo de referencia de Interconexión de Sistemas Abiertos (*Open System Interconnection*) fue el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, fue un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Multicast. Es el envío de la información en una red a múltiples déstinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

NFS.El Sistema de archivos de red (Network File System) es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local.

OSPF. *Open Shortest Path First* es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (*LSA - Link State Algorithm*) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (*link-state database, LSDB*) idéntica en todos los enrutadores de la zona.

Packet switching. (Conmutación de paquetes) Es un principio básico en las comunicaciones en donde se dice que determinado paquete de información que forma parte de un mensaje, traza su recorrido entre los sistemas

anfitriones (*hosts*), sin que este camino (*path*) esté predeterminado.

QoS. Calidad de Servicio (*Quality of Service*) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*). Es especialmente importante para ciertas aplicaciones tales como la transmisión de video o voz ya que requieren de una garantía de entrega por tiempo.

RARP. Protocolo de Resolución de Dirección de Retorno (*Reverse Address Resolution Protocol*). Protocolo de bajo nivel que asigna direcciones IP a ordenadores desde un servidor en una red.

RFC. La Petición De Comentarios (*Request for comments*) es una serie de notas sobre Internet que comenzaron a publicarse en 1969. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

RIPO. Protocolo de información de enrutamiento. El IGP más común de la Internet. RIP utiliza el número de saltos como métrica de enrutamiento.

RJ-45. Es una interfaz física (*Registered Jack*) comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). Es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado. Es utilizada comúnmente con estándares norma A y B, que define la disposición de los pines.

Running-config. La configuración actual (que está en ejecución) de la RAM en un equipo CISCO

Rutas estáticas. Establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino y se definen administrativamente.

SMTP. El Protocolo Simple de Transferencia de Correo (*Simple Mail Transfer Protocol*), es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos Está definido en el RFC 2821 y es un estándar oficial de Internet.

Startup-config. La configuración de arranque que está guardada en la NVRAM (*Non-volatile random access memory*) y mantiene la información incluso si se interrumpe la corriente.

Subinterfaz. Es una interfaz virtual que hace uso de una interfaz física individual.

Telnet. Es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor). Utiliza el protocolo TCP y envía los datos en formato ASCII.

TFTP. Son las siglas de Protocolo de transferencia de archivos trivial (*Trivial file transfer Protocol*). Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. Utiliza UDP (en el puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza el puerto 21 TCP).

Topología de red. Es la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se la llama mixta.

Troncal. Enlace troncal Conexión lógica y física entre dos dispositivos de red a través de los cuales viaja el tráfico.

Upgrade. Nombre en inglés que reciben las nuevas versiones de una aplicación o un hardware y son diseñadas para reemplazar una versión previa del mismo producto.

VoIP. Son las siglas de Voz sobre Protocolo de Internet o Telefonía IP (*Voice over Internet Protocol*), una categoría de hardware y software que permite a la gente utilizar Internet como medio de transmisión de llamadas telefónicas, enviando datos de voz en paquetes usando el IP (Paquetes conmutados) en lugar de los circuitos de transmisión telefónicos (Circuitos conmutados).

WAN. Una Red de Área Amplia (*Wide Area Network*), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 km hasta unos 1000 km, dando el servicio a una región, país o un continente.

802.1Q. Es un protocolo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas. Fue un proyecto del grupo de trabajo 802 de la IEEE.

Bibliografía

Interconnecting Cisco Networking Devices
Version 1.0 Part 1
Cisco Systems, Inc.
Canada, 2006

Interconnecting Cisco Networking Devices
Version 1.0 Part 2
Cisco Systems, Inc.
Canada, 2006

Exploration Routing Networking Academy
Cisco Systems, Inc.
Canada, 2006

Cisco IOS IP Command Reference, Volume 1
Release 12.2
Cisco Systems, Inc.
Canada, 2006

Cisco IOS IP Command Reference, Volume 2
Release 12.2
Cisco Systems, Inc.
Canada, 2006

Cisco IOS IP Command Reference, Volume 3
Release 12.2
Cisco Systems, Inc.
Canada, 2006

Catalyst 3750 Switch Software Configuration Guide Cisco IOS Release 12.2(37)SE
Cisco Systems, Inc.
May 2007

Documentos internos

Srda-007 Políticas de Configuración y uso de Switches IP en Centrales Rev.6

Srda-128 Normatividad de protocolos e interfaces en RCDT Rev.4

Srda-130 Solución técnica para la integración de switches en la RCDT

Srda-171 Homologación de NA RCDT Rev.2

Srda-260 Solución Técnica Infraestructura de red de la Central Cuautitlán para suministrar el servicio de VoIP de Atención Telefónica. Versión 1.0

Sitios Web

http://es.wikipedia.org/wiki/Wikipedia:Portada

http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html

Documentos electrónicos

CCNA Ciscopedia V3.1
Bases de enrutamiento Red Uno / Uninet