ESCUELA POLITÉCNICA DEL EJERCITO

FACULTAD DE INGENIERIA ELECTRÓNICA

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TITULO EN INGENIERIA ELECTRÓNICA

REDISEÑO DE LA RED DE DATOS DE ANDINATEL PARA EL ÁREA METROPOLITANA DE QUITO.

ROBERTO ALMEIDA GUTIERREZ

QUITO – ECUADOR

2005

CERTIFICACIÓN

Certificamos por medio de la presente que el Proyecto de Grado para la obtención del Título en Ingeniería Electrónica denominado “Rediseño de la Red de Datos para el Área Metropolitana de Quito” fue realizado en su totalidad y bajo nuestra supervisión por el Sr. Roberto Almeida Gutiérrez.

Atentamente

Ing. Fabián Sáenz
Director de Tesis

Ing. Alejandro Chacón
Codirector de Tesis

AGRADECIMIENTO

A Concepción y Hugo, mis padres

A Hugo y Tatiana, mis hermanos

A Ximena y Roberto, mis amigos

Al San Gabriel, mi Colegio

A la Dolorosa, mi Guía.

DEDICATORIA

I Para Vicente, Marcelo, Jaime,
William, Diego por compartir
Su amistad y camaradería.

II Para Roberto y Ximena
Mis amigos de penas y glorias.

III Para Paola y Verónica
Gracias por su gran amistad
Y su cálido y abierto cariño.

IV Para Mauricio, Álvaro y los Carlos
Por ayudar a sobrellevar los
Momentos amargos.

V Johanna
Llegaste en el momento justo
Con tu luz, tu gracia y alegría
Hasta siempre, amiga mía.

VI Alexandra
Me hiciste soñar y también escribir
Eres ángel de luz, ángel de ensueño
Vuela con tus alas. Vuela libre.
Libre como quien no tiene dueño.

VII Margarita
Por ser de las pocas mujeres
Que alegraron mi pupila.

VIII Alexandra
Será que algún día te olvido?
Ojalá que no, porque espero
Que tú tampoco lo hagas.

IX Para todos los que de alguna forma
Me conocieron y me apoyaron.

PRÓLOGO

Durante los últimos años viene sonando en el mundo de las redes de comunicación de datos, el término convergencia. Lo que primero empezó con el transporte de la voz sobre el Internet, se ha ido perfeccionando poco a poco y ahora se estima que en los próximos años las redes de datos empresariales estarán transportando la totalidad de las comunicaciones telefónicas internas de las organizaciones. El transporte en tiempo real de video de alta calidad es una realidad y las corporaciones han percibido las ventajas competitivas que la aplicación de esta tecnología les brinda.

Voz, video y datos integrados en una sola red IP configuran el nuevo escenario en el cual se desenvolverán las nuevas redes de comunicaciones. Con esta visión, el presente trabajo se enfoca en el rediseño de la red de datos de Andinatel, para lograr la convergencia transparente de los servicios de voz, video y datos en una única infraestructura, con calidad de servicio de extremo a extremo y además facilitando la administración de configuración, fallos y reportes de los equipos de red, garantizando un óptimo servicio a los clientes internos y externos, así como la protección de la inversión presente y futura en equipos de red.

Roberto Almeida G., CCNA

ÍNDICE

CAPITULO I

INTRODUCCIÓN

ANTECEDENTES

Hasta el año de 1998, la red de datos interna de Andinatel se basaba en la red de teleprocesos, la cual no era la adecuada para prestar servicios de calidad tanto para los clientes internos como para los externos, debido a la limitada velocidad de transmisión de 9.6 Kbps y al limitado flujo de tráfico de datos que ésta red podía soportar, debido a la arquitectura de servidor y terminales tontos, además de los inconvenientes de inestabilidad y poca confiabilidad; factores que deterioraban la imagen corporativa de la empresa, que cada vez demandaba de mayores prestaciones en la red, debido al incremento de los clientes tanto externos que superaban los 800.000 abonados, así como del desarrollo de nuevas aplicaciones orientadas a mejorar los servicios a los clientes, ya que la plataforma de servicios desarrollada sobre Fortran empezaba a ser obsoleta.

Con la modernización de la empresa, la antigua red de teleprocesos se reemplazó por una nueva red de datos que cumplía con los estándares de networking vigentes a la época de la instalación, tales como ethernet para el acceso de las máquinas a la red y fastethernet en los enlaces troncales. Desde entonces, la actual red de datos que interconecta todas las dependencias de Andinatel, tanto las operativas como las administrativas, ha crecido de forma sostenida, a un ritmo de 6 puntos de red promedio por semana, tanto por la inclusión de nuevos usuarios a la red, así como debido a la reubicación de los ya existentes, sin que existan registros actualizados de dichas instalaciones o cambios.

La falta de actualización de dichos registros, menos del 5% de la red horizontal está documentada y no existe un registro de la utilización de los puertos en los equipos, provoca la subutilización de equipos activos en unos casos y en otros su saturación; el desconocimiento de cuáles y cuántos puntos ya no se utilizan o no podrían utilizarse por razones varias, dónde se localizan éstos puntos y qué acciones se deberían tomar en caso de ser necesaria una rehabilitación; qué equipos son los utilizados para interconectar a los clientes de la red, y cómo se interconectan entre sí, además de si guardan compatibilidad para ejecutar protocolos de configuración, monitoreo y mantenimiento de red. Dentro de la red coexiste ethernet, fastethernet y gigabit ethernet, así como hubs y switches de marcas tales como Cisco, 3COM, IBM, NetGear, DLink, Allied Telesyn, entre otros.

Los problemas anteriormente mencionados dificultan la administración de la red y por ende toda planificación para el mejoramiento de la calidad de servicio de la red de datos o la implementación de nuevas arquitecturas de red, porque muchos de los equipos ya son descontinuados por el fabricante, su sistema operativo ya no es actualizable o porque no están diseñados para interactuar con equipos de otras marcas.

La inexistencia de diagramas físicos y lógicos de la implementación de la red, trae como resultado que la solución de problemas de conectividad sea una tarea llevada a cabo con cierta dificultad, porque se requiere “saltar” de equipo activo en equipo activo para encontrar el daño, lo que requiere y consume demasiados recursos de personal. El desconocimiento de cuánto material y equipos se necesitarían para en el futuro migrar a nuevos estándares, o si en efecto los materiales adquiridos han sido instalados en la red de datos son otros problemas latentes.

El objetivo del presente proyecto es crear las bases necesarias para mejorar la calidad de los servicios que actualmente ofrece la red de datos interna de Andinatel, al estandarizar los procesos internos del Departamento de Redes, así como el preparar las condiciones necesarias para futuras mejoras. Para ello, se realizará una investigación de campo en todas los edificios y dependencias de Andinatel, comprendidos en el área de jurisdicción del Distrito Metropolitano de Quito, para realizar los respectivos diagramas horizontales y verticales de la red instalada, certificando la calidad de los enlaces. Además se propondrá y ejecutará, por vez primera, un plan de identificación unificado para todos los puntos de

conexión de red, para facilitar el registro de nuevos puntos de conexión y solución de problemas de conectividad.

Las dependencias sobre las cuales tiene injerencia, el presente proyecto son las siguientes:

1. Central de Conmutación y Centro de Recaudación de Quito Centro.
2. Central de Conmutación y Centro de Recaudación de Iñaquito.
3. Central de Conmutación y Centro de Recaudación de Villaflora.
4. Central de Conmutación y Centro de Recaudación de La Luz.
5. Central de Conmutación y Centro de Recaudación de Tumbaco.
6. Central de Conmutación y Centro de Recaudación de San Rafael.
7. Central de Conmutación y Centro de Recaudación de Sangolquí.
8. Central de Conmutación y Centro de Recaudación de Cotocollao.
9. Central de Conmutación de Carcelén.
10. Central de Conmutación de El Pintado.
11. Central de Conmutación de Mariscal.
12. Oficinas Administrativas en el Edificio Banco del Pacífico.
13. Oficinas Administrativas en el Edificio Droira
14. Oficinas Administrativas en el Edificio Estudio Z.
15. Oficinas Administrativas en el Edificio Andinanet – Informática
16. Oficinas Administrativas y de Servicio al Cliente en el Edificio El Doral.

Como segundo punto para el mejoramiento integral de la red, se realizará un inventario de todos los equipos activos de red, hubs, switches y routers; de sus capacidades, tanto instaladas como ocupadas, de sus configuraciones, si las tuvieren, y de ser el caso reprogramarlos o repotenciarlos por medio de la actualización de su IOS. Todas las configuraciones, antiguas y nuevas, se las pondrá a disposición de los mismos equipos y del personal encargado de la red, a través de un servidor TFTP, para que pueden utilizarse como respaldo ante una eventual emergencia o funcionamiento incorrecto de la red.

Documentada la red, tanto de forma física como lógica, se procederá a realizar un estudio del tráfico de red, con el fin de disminuir el dominio de broadcast, mediante la implementación de redes Lan Virtuales (VLANs), que se adapten a las necesidades

presentes y futuras de la red. Con este estudio, también se realizará una priorización del tráfico, para que aplicaciones consideradas críticas, tales como los sistemas de atención al cliente, sean más rápidas, efectivas y seguras, con el afán de mejorar el servicio al cliente externo. Además se restringirá tráfico innecesario y tráfico no deseado, para aliviar la presión sobre los enlaces y mejorar la seguridad de la red.

JUSTIFICACIÓN E IMPORTANCIA

El presente proyecto es importante para Andinatel como empresa, ya que de los resultados obtenidos se lograría el conocimiento preciso de todos los equipos activos de red instalados, así como de la cantidad de material instalado y utilizado, lo que permitiría un inventario total de la red de datos interna para detectar faltantes o sobrantes, o simplemente facilitar la tarea de reemplazo del material utilizado en los puntos de conexión . Además con el conocimiento exacto de la red, como se constituye de forma física y lógica, cuántos usuarios ocupan la red, y a qué servicios acceden, se puede elaborar nuevas propuestas para el mejoramiento de la calidad de servicio y la diversificación de servicios que en la actualidad ofrece la red, mejorando las relaciones con los clientes tanto internos como externos.

Con el conocimiento de quién y para qué se usa la red, se puede mejorar los sistemas de gestión de red, para priorizar tráfico, establecer rutas redundantes, mejorar servicios al usuario final, y actuar de forma más rápida y efectiva para la solución de problemas de conectividad, especialmente cuando se traten de aplicaciones críticas, tales como los sistemas de facturación.

Para los clientes externos también existe el beneficio, ya que al priorizar tráfico, y establecer rutas redundantes, los sistemas de facturación y consulta aumentarán su disponibilidad desde el 99.85% hasta el 99.99%.

CAPITULO II

SITUACIÓN ACTUAL DE LA RED

Se proporciona la siguiente información:

- Plan de identificación de cableado estructurado.
- Diagrama vertical de la red.
- Tipo de equipos instalados en la red.
- Configuraciones actuales de los equipos.
- Configuración lógica de la red.
- Protocolos enrutados dentro de la red.
- Servicios de la red.

El actual sistema de cableado estructurado de Andinatel S.A. tiene su base en el diseño ejecutado e implementado por parte de una empresa privada en el año de 1998. A lo largo del tiempo, aquel diseño ha sido modificado por parte del departamento de redes, para adecuar la red física a las necesidades empresariales, ya sea aumentando puntos de red, o reubicando los existentes, a tasa promedio semanal de 6 puntos de red, sin que exista una base de datos actualizada de dichas instalaciones o cambios.

Por el contrario, el departamento de redes no posee los planos originales de la ubicación de dichos puntos, no sabe cuántos de dichos puntos todavía están en funcionamiento, cuántos fueron reubicados y a dónde, o cuántos puntos se dejaron de utilizar porque las oficinas fueron reubicadas o remodeladas. Tampoco se guarda un registro de los puntos nuevos, ni se realiza un seguimiento de su utilización, a lo que hay que sumar que muchas veces las reubicaciones son reportadas como instalaciones nuevas o viceversa.

La falta de información actualizada, menos del 5% de la red horizontal está documentada, impide un eficiente manejo de recursos y dificulta la solución de problemas. La nomenclatura utilizada en los puntos de red, aunque un 8% de los puntos no está etiquetado, no responde a ningún ordenamiento jerárquico ni indica el origen de los mismos, por lo que la localización de fallos se torna dificultosa y consume muchos recursos. Menos del 2% de los cuartos de comunicaciones están a punto de saturarse debido a la presencia de un elevado número de puntos muertos. Por ejemplo, en un cuarto de comunicaciones del edificio El Doral, el 52% de los puntos instalados no están en funcionamiento.

No se conserva sino un sistema tradicional de nombrar a los cuartos de comunicaciones en base a la oficina en la que se ubican, aunque dicha correspondencia ya no exista. Por ejemplo el cuarto de comunicaciones de Back Office no se encuentra en Back Office, sino en Andinadatos. Tampoco se cuenta con un registro centralizado de las certificaciones de los puntos de red, por lo que no se puede garantizar la calidad de las instalaciones, y no se pueden predecir posibles fallos relacionados con ruido eléctrico, distancias fuera de norma, o incluso, roturas de cables.

De existir estas certificaciones, se podría predecir si un punto se lo puede reubicar en otra localización, cuánto se necesitaría para reemplazar un cable defectuoso, o cuánto se necesita para instalar uno contiguo. Cabe mencionar que se certifica el 40% de las nuevas instalaciones si son menos de 8 puntos y el 100% de las instalaciones si supera esa cantidad. El problema es que no existe una normativa sobre que hacer con estas certificaciones.

Lo anteriormente expuesto tiene que ver con los diagramas horizontales de la red. En cuanto a los diagramas verticales, estos desde el inicio del proyecto se han actualizado hasta llegar al 97%, por lo que relativamente fácil aislar segmentos de red para solucionar problemas, excepto en el caso en el cual el segmento no esté documentado. Los enlaces no documentados son aquellos para los cuales se utilizan bridges no administrables.

Para descubrir equipos activos dentro de la red, se cuenta con un protocolo de descubrimiento de equipos, como es el Cisco Discovery Protocol, por lo que no se puede descubrir equipos que no sean de marca Cisco. Si a esto se le suma que algunos equipos presentan direcciones IP duplicadas (7% al iniciar el proyecto, 0% en la actualidad), no válidas (2% al iniciar el proyecto, 0% en la actualidad), o no configuradas (4% al iniciar el proyecto), las tareas de administración de equipos de red es más compleja de lo que debería ser.

En cuanto a la implementación lógica de la red, ésta es totalmente plana para los equipos bajo la administración directa de Andinatel. Al no existir ningún nivel de jerarquía dentro de la red, ésta es un único dominio de broadcast, con todas las implicaciones directas, tales como mayor probabilidad de inundación de tráfico, mayor vulnerabilidad a ataques, entre los más indeseables. A nivel de capa 2, coexisten ethernet (10 Mbps) y fastethernet (100 Mbps) en la capa de acceso de la red, aunque también hay que mencionar a los bridges con velocidades de 2.048Mbps. En el backbone coexisten fastethernet (100 Mbps) y GigaBit ethernet (1000 Mbps).

El direccionamiento de capa 3 se basa en una única dirección IP de clase B para toda la red MAN, lo que en teoría proporciona capacidad para alojar a 65534 hosts, aunque en la actualidad se necesita espacio de direccionamiento para alrededor de 1300 hosts. Existen tantos dominios de colisión, como puertos en los switches de la red, sin embargo hay que contar una cantidad no determinada de hubs, aunque desde el inicio de este proyecto se han ido reemplazando paulatinamente por switches.

Si bien las colisiones las manejan de forma eficiente los switches, en este tipo de red no es posible una contención del broadcast y multicast, lo que significa que todos los hosts en la red “oyen” y procesan todos los paquetes de este tipo que se transmiten por la red, que representa entre el 52 y 54% del tráfico dentro de la red. Si se toma en cuenta este dato de los paquetes broadcast o multicast, se notará que el desempeño de la red es pobre, y que los procesadores de los hosts necesitan dedicar recursos para procesar entre 105 y 110 paquetes por segundo que no estaban dedicados a ellos.

El impacto de esta cantidad de tráfico sobre cada host varía en función del procesador y la memoria instalada. Desde el inicio del proyecto, la red de datos ha quedado inutilizada en tres ocasiones debido a este tipo de tráfico. En dos ocasiones se debió a pruebas con servidores de contenido y la otra debido a un ataque del tipo DoS (Denial of Service) generado por medio de paquetes ICMP.

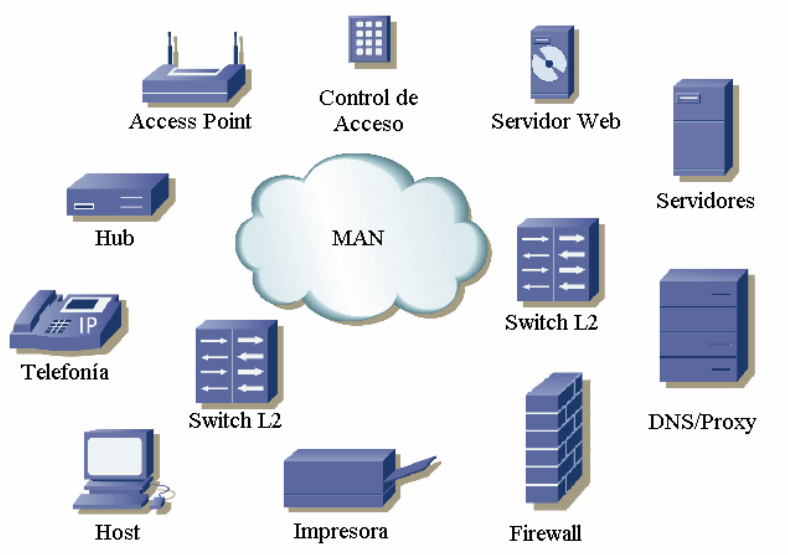


Figura 2.1. Implementación lógica de la red

En la figura 2.1 se observa con mayor claridad la implementación lógica de la red. Todos los servidores, equipos de acceso (hubs y switches), y hosts (PCs, impresoras, dispositivos de control de acceso) tienen la misma jerarquía dentro de la red. La ventaja de esta implementación es que la adición de nuevos hosts a la red es una tarea sumamente sencilla, no hay que configurar ningún parámetro en equipo activo alguno. La enorme desventaja, es que cada vez se amplía más el dominio de broadcast, y se degrada el desempeño de la red, notándose este efecto con mayor gravedad en los hosts de menores capacidades, o en los conectados a equipos activos de menores prestaciones.

Dentro de la red existe una gran variedad de marcas y modelos de equipos instalados, en su mayoría son equipos de marca Cisco, aunque también existen equipos de otras marcas tales como Allied Telesyn, NetGear, 3Com, IBM y Bay Networks. Sin contar los switches Cisco, los equipos de red no tienen configurada una dirección IP válida para administrarlos (13% de los casos), ya sea por que no son administrables (4% de los casos), o porque

nunca se la ha configurado (2% de los casos), o la dirección está duplicada (7% de los casos).

Dado que la mayoría de equipos son de marca Cisco, es posible realizar un inventario preliminar de los equipos instalados en la red. Como se verá en el Capítulo 4, existe un protocolo propietario de Cisco, llamado Cisco Discovery Protocol –CDP por sus siglas en inglés– que sirve para descubrir dispositivos Cisco dentro de la red. Con la ayuda de este protocolo, al inicio de este proyecto se detectaron los equipos detallados en la tabla 2.1.

Equipo	Modelo	Cantidad
Switch	C5505	2
Switch	C3550-12G	2
Switch	C2950C-24	3
Switch	C2950G-24-EI	33
Switch	C2950G-48-EI	3
Switch	C2924M-XL	5
Switch	C2924C-XL	6
Switch	C2924-XL	9
Switch	C2912-XL	2
Switch	C1924C-EN	9
Switch	C1924-A	1
Switch	C1912-A	1
Switch	1548M	1
Access Point	AIR-AP1230B-A-K9	9
Total de Equipos:		86

Tabla. 2.1. Resumen de equipos de red Cisco

Para el análisis de las configuraciones de los equipos de la red, se toma como universo a los equipos de la tabla 2.1., ya que representan a la gran mayoría de los equipos administrables dentro de la red, debido a sus características técnicas.

En cuanto a las configuraciones de los equipos (86 configurables al momento de realizar este proyecto), se revisaron los siguientes parámetros:

1. Mensaje de advertencia sobre el ingreso a sistema.
2. Duración del periodo de inactividad durante las sesiones.
3. Sincronización de relojes con equipos de la red.

4. Marca de tiempo de los eventos ocurridos dentro del equipo.
5. Intercambio de información sobre VLANs.
6. Programación para gestión SNMP.
7. Soporte para manejo de lazos.

Cuando se iniciaba una sesión en un equipo cualquiera, ya sea por la terminal de consola o sesión Telnet, el mensaje que se recibía del equipo (76% de los casos) era del siguiente tipo:

ANDINATEL S.A.
VP DE TECNOLOGIA Y ANDINANET
Tipo de equipo, marca y modelo.
Ubicación.

La utilidad de este mensaje es meramente informativa, ya que brinda el modelo y la ubicación de un equipo dado, sin embargo no advierte que el acceso a este equipo esta restringido al personal encargado de la administración de la red, por consiguiente, este es una falla de seguridad. Por ello, se modificó este mensaje de inicio de sesión por el siguiente:

ANDINATEL S.A.
VP DE TECNOLOGIA Y ANDINANET
Tipo de equipo, marca y modelo.
Ubicación.
EL USO DEL SISTEMA SE RESTRINGE
A USUARIOS AUTORIZADOS

Para efectuar este cambio en los equipos de marca Cisco se debe introducir el siguiente comando desde el modo de configuración global:

Switch(config)# banner motd d mensaje d

Donde d es un caracter limitador, el cual no podrá ser utilizado dentro del mensaje; mensaje es el mensaje que se imprimirá en la pantalla cada vez que se quiera ingresar a la consola del equipo.

Con este mensaje se deja en claro, en el 86% de los equipos, que solo el personal de redes puede entrar a modificar la configuración del equipo, o a monitorear el mismo. Las violaciones a este principio se consideran atentatorias contra la propiedad de la empresa y las personas que violen el sistema no pueden alegar que éste era abierto o que no hubo advertencia de las implicaciones que conllevan dichos actos.

Otro problema de seguridad relacionado es la duración de los periodos de inactividad de las sesiones. En todos los equipos de la red, no existía ningún limitante sobre la duración de una sesión abierta. Existe la posibilidad de que por descuido se deje una sesión abierta en un equipo, por lo que es vulnerable a ataques. De la misma forma, ya que cada equipo acepta un número finito de sesiones, es posible que se abran y no se cierren, tantas sesiones como están permitidas, negándose el acceso al equipo. Es por ello que en la totalidad de los equipos se configurará como período de inactividad máximo de 2 minutos, para minimizar las posibilidades anteriores.

Para efectuar este cambio en los equipos de marca Cisco se debe introducir el siguiente comando desde el modo de configuración de línea, tanto para la consola como para las líneas VTY (sesiones telnet):

Switch(config)# line console 0
Switch(config)# exec-timeout 2 0
Switch(config)# line vty 0 4
Switch(config)# exec-timeout 2 0

Con ello tanto en la línea de consola (line console 0), como en las líneas VTY o sesiones telnet (line VTY 0 4) se limita el período de inactividad a 2 minutos 0 segundos.

Para tareas administrativas y de control, el 86% equipos tienen la capacidad de guardar en una base de datos interna, los eventos que ocurren dentro de ellos, tales como interfaces que cambian de estado, identidad del usuario que cambia la configuración, fallos en el software, entre otros. Todos ellos tienen una marca de tiempo, sin embargo ésta no es útil si todos los equipos los equipos de red no tienen sincronizados sus relojes internos con un servidor dedicado al sincronismo de red.

Para lograr dicha sincronización se utiliza el protocolo Network Timing Protocol –NTP por sus siglas en inglés–. En la figura 2.2 se observan los resultados obtenidos al verificar la configuración de dicho protocolo. Logrado el sincronismo de los equipos de red, ahora es importante que los eventos se marquen con el tiempo real en el que ocurrieron (el tiempo dado por el servidor de tiempo) y no los marquen con relación al tiempo transcurrido desde el encendido del equipo, tal como sucede con todos los equipos en la actualidad.

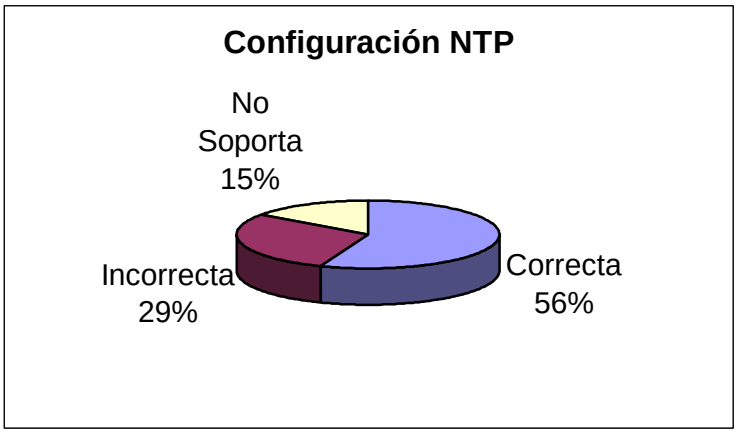


Figura 2.2. Resumen de configuración NTP

Para segmentar y jerarquizar la red se implementarán redes de área local virtuales (VLANs por sus siglas en inglés). Cabe anotar que dentro de la infraestructura de Andinatel ya existen seis (6) VLANs, implementadas para separar los centros de gestión de red de Alcatel, Siemens, Ericsson, Huawei y Andinadatos de la red de Andinatel. Ya que la implementación de VLANs se la realiza a través de software en los equipos, es importante que todos los equipos conozcan que VLANs manejarán y como identificarlas.

Una forma rápida y eficiente es a través de un servidor VTP (Virtual Trunking Protocol), en el cual se configuran las VLANs existentes para que éste se encargue de propagar dicha información. En las figuras 2.3 y 2.4 se resumen las configuraciones de los equipos con respecto a este protocolo.

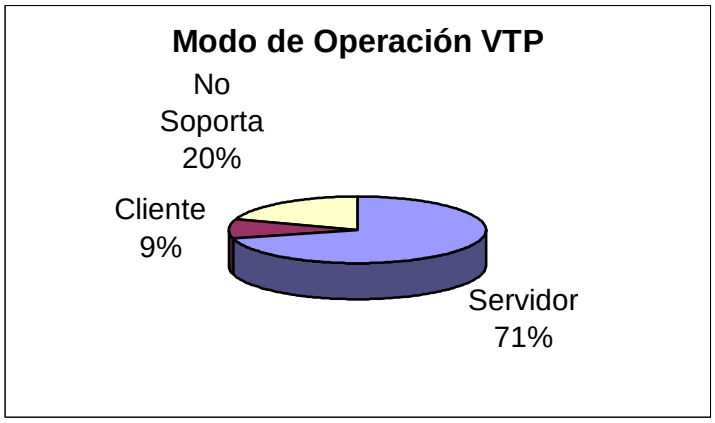


Figura 2.3. Modo de Operación VTP

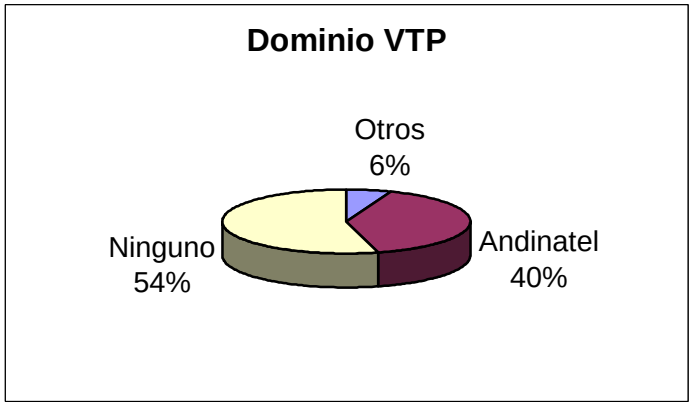


Figura 2.4. Dominio VTP

De la figura 2.3 se desprende que el 20% de los equipos no soporta VTP, por lo que la configuración de las VLANs deberá ser hecha de forma manual. Habrá que cambiar el modo de operación en el 69% de los switches, para tener un servidor de VTP principal y uno de respaldo. De la figura 2.4 se infiere que la mayor parte de los equipos de la red no posee la información sobre las VLANs configuradas, ya que no comparten el mismo dominio Andinatel en el 60% de los casos, por lo que habrá que reconfigurar este parámetro. Otros dominios existentes son laboratorio, cursow, andina y prue.

Para la gestión SNMP será necesario la reconfiguración del 100% de los equipos, ya que envían los mensajes a servidores diferentes, o tienen el servicio deshabilitado, sin contar que no existen comunidades de lectura y escritura estandarizadas dentro de la red. También será necesario un servidor que recoja todos estos mensajes, los procese y los almacene. Para el manejo de lazos en la red existe el protocolo de árbol extendido (Spanning Tree Protocol –STP por sus siglas en inglés–) que lo soportan todos los equipos indicados en la tabla 2.1. No se ha cambiado la configuración de fábrica por lo que realizado el diagrama vertical de las conexiones, es decir, conocidos los puertos de interconexión entre switches, se deberá cambiar la configuración de este protocolo. La configuración correcta de este protocolo es importante, ya que en algunas ocasiones los usuarios realizan conexiones no autorizadas y el comportamiento normal de la red se ve afectado debido a la presencia de lazos físicos y lógicos en la topología. Desde el inicio de este proyecto, los lazos provocados por conexiones no autorizadas han inutilizado la red por una ocasión.

En cuanto a los protocolos enrutados existen varios de ellos, a pesar de que en la red deberían circular únicamente paquetes IP para la comunicación entre hosts, paquetes NetBios para la resolución de nombres de hosts dentro de la red y paquetes EIGRP para la comunicación entre ruteadores. En la figura 2.5 se muestra la distribución de los protocolos enrutados. Para ello se analizaron un aproximado de 50 millones de paquetes de tráfico de la red, con la versión educativa del software *Protocol Inspector* de FLUKE Networks ©.

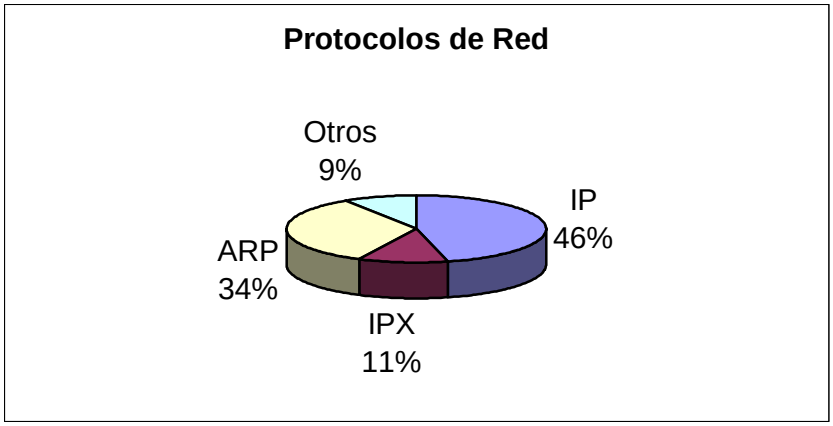


Figura 2.5. Protocolos enrutados

A primera vista, se puede inferir de la figura 2.5 que casi la tercera parte de la muestra es tráfico de tipo broadcast, ya que el protocolo ARP es tráfico tipo broadcast que generan los hosts para resolver las direcciones físicas a partir de las direcciones lógicas. Una quinta parte del tráfico se debe a protocolos de poca utilidad dentro de la red, ya que la implementación lógica de la red se basa en el conjunto de protocolos TCP/IP. El tráfico IPX se debe en gran parte a problemas de configuraciones de los equipos, en especial las impresoras en red, en las que viene activado por defecto este protocolo. El nueve por ciento etiquetado como otros, incluye tráfico del tipo NetBEUI, CDP, STP, entre otros.

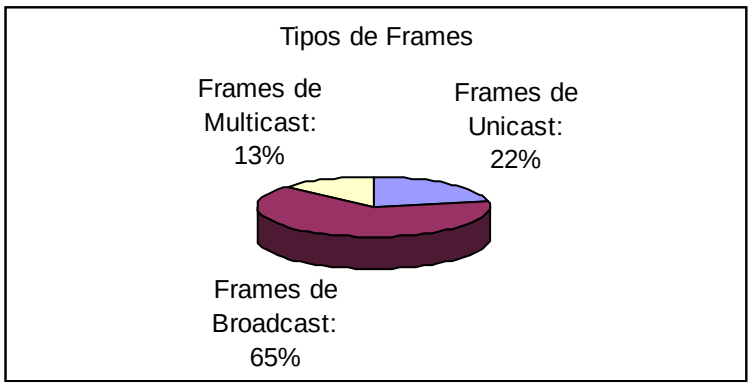


Figura 2.6. Estadísticas presentadas por los Equipos

En la figura 2.6 se muestra el tipo de frames dentro de la muestra de estudio. Al realizar el análisis de cuántas tramas no son del tipo broadcast o multicast, se llega al resultado impresionante de que únicamente el 22% (aprox) es tráfico del tipo unicast, mientras que el restante 78% (aprox) es del tipo broadcast o multicast. Ello se debe en gran medida a que los servicios de impresión se basan en NetBIOS. Este protocolo se encapsula en paquetes IP y por ello aparece en las estadísticas de la figura 2.5 como tráfico IP. Debido al menor tamaño de las tramas de broadcast y multicast, el tráfico unicast medido en bytes aumenta hasta el rango de entre el 46 y 48% del tráfico total.

En cuanto a los servicios que ofrece la red, éstos son variados y limitados únicamente a nivel de servidor, por lo que en teoría, todos los usuarios tienen acceso potencial a todos

los servicios de red, o generar tráfico dirigido hacia ellos. Los servicios que ofrece la red son: servicio de correo electrónico, servicio de Internet, servicio de Intranet, servicio de impresión, acceso a bases de datos y archivos compartidos entre usuarios. En forma incipiente, y solo en el edificio de la Vicepresidencia de Tecnología, se ofrece el servicio de voz sobre IP (VoIP por sus siglas en inglés) y existe el proyecto de implementar multidifusión de video. Debido a la naturaleza plana de la red, es bastante difícil implementar de forma exitosa nuevos servicios, tales como la mencionada multidifusión de video o la de audio, sin comprometer el desempeño de otras aplicaciones, tales como el acceso a la base de datos de facturación. Durante las pruebas de funcionamiento de la multidifusión de video, la red colapsó debido a la cantidad de tráfico multicast generado.

Para llevar a cabo tareas de monitoreo de red, tales como respuesta de equipos activos, tiempo de respuesta de servidores activos, uso de ancho de banda en el backbone, utilización de puertos troncales, entre otras, no existe ningún software o equipo especializado que lleve a cabo estas tareas. La mayor parte de las fallas dentro de la red no son detectadas a tiempo, sino cuando los usuarios finales las reportan, y al no existir una documentación detallada de la red, las tareas de solución de problemas conllevan más tiempo del que deberían.

CAPITULO III

MEJORAMIENTO DE LA RED A NIVEL DE LA CAPA 1 DEL MODELO DE REFERENCIA OSI

Se proporciona la siguiente información:

- Descripción de las configuraciones de canal y enlace básico.
- Explicaciones de las pruebas de cables para LAN.
- Procedimientos fundamentales de diagnóstico en cables de LAN.
- Plan de identificación del cableado estructurado de la red de Andinatel.
- Diagrama Vertical de la red MAN de Andinatel.

CONEXIONES DE ENLACE BÁSICO Y DE CANAL

Las pruebas de los enlaces de cableado estructurado pueden incluir o no, lo cables de conexión para equipo y conexiones adicionales de transición en el armario de telecomunicaciones y en el área de trabajo. El segmento de cable instalado permanentemente entre el armario y el primer receptáculo de distribución en la pared del área de trabajo es el enlace básico, tal como se muestra en la figura 3.1 . Como se define en el TSB-67, el enlace básico consiste de hasta 90 metros de cable horizontal, un conector de transición en cada extremo y dos cables de conexión de equipo, cuya longitud individual no superará los 2 metros.

Este tipo de certificación de cableado estructurado es el que se lleva a cabo actualmente dentro de la red de Andinatel, en un 40% de las instalaciones nuevas menores a ocho puntos de red, y en el 100% de las instalaciones nuevas si supera dicha cantidad, por lo que

no se puede garantizar que el 100% de los puntos nuevos instalados cumplan con todos los estándares. Resultado de ello, es que existen problemas de conectividad con ciertas tarjetas de red en lugares específicos, en especial con las instaladas en los equipos del tipo Laptop.

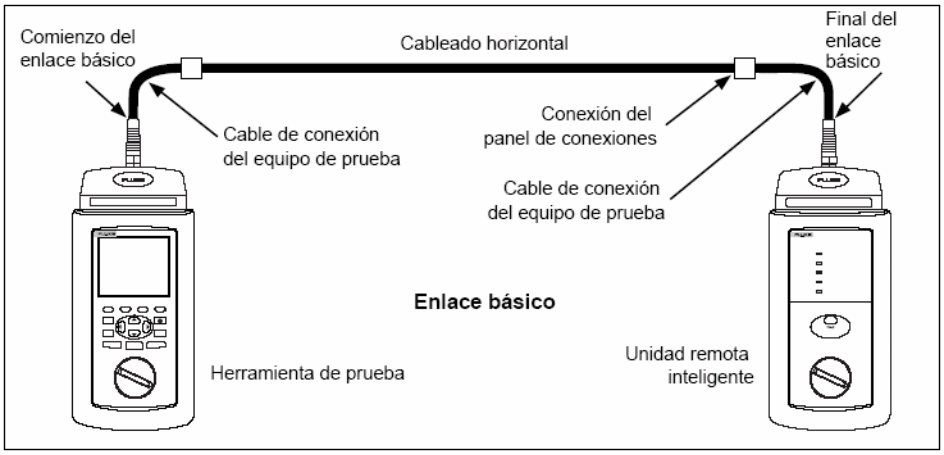


Figura. 3.1. Conexiones de prueba para enlace básico

Ya que las pruebas de enlace básico no incluyen los cables de conexión de equipos, éstos pueden originar los fallos de conectividad y llevar a conclusiones erróneas en cuanto a la ubicación y tipo del problema. Es por ello que existe otra forma de certificar las instalaciones de cableado estructurado, que es la prueba de enlace de canal.

El enlace de canal incluye los conectores de transición y los cables de conexión de equipos agregados al segmento del enlace básico. El canal se prueba de extremo a extremo para comprobar el rendimiento de todos los componentes. En este caso se utiliza los cables de conexión de equipos para conectar la herramienta de prueba al canal, tal como se muestra en la figura 3.2. El TSB-67 define el canal como un enlace básico más un conector de transición adicional en cada extremo y hasta 10 metros de cables de conexión de equipos. Debido a los conectores y cables de conexión adicionales, los límites de prueba para un canal son menos exigentes que para el enlace básico, sin embargo, se garantiza la no existencia de fallos de extremo a extremo de la conexión.

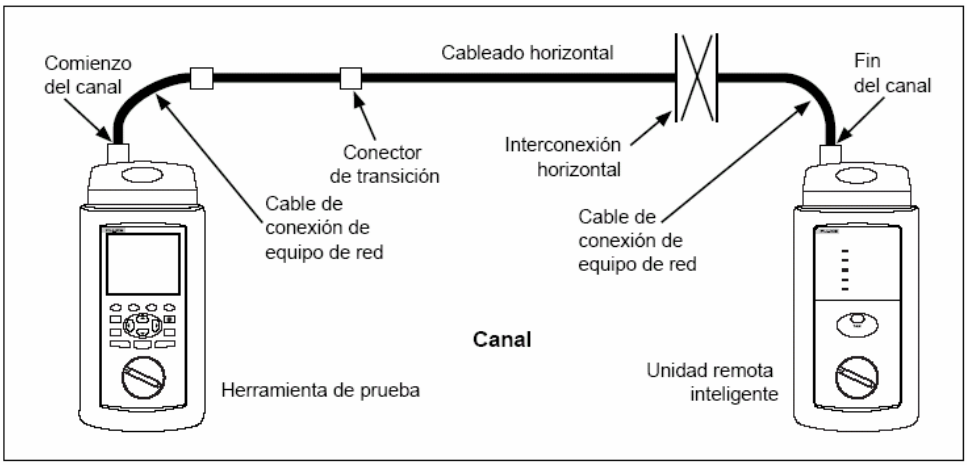


Figura. 3.2. Conexiones de prueba para canal

Este tipo de certificación es el más adecuado para el ámbito empresarial, ya que garantiza que todos los componentes físicos de las conexión funcionarán adecuadamente y no se presentarán inconvenientes con equipos activos, cualquiera que sea el fabricante.

PRUEBAS DE CABLE PARA LAN

Cualquier cable de LAN instalado correctamente, debe cumplir con pruebas básicas, tales como longitud, atenuación y paradiafonía. Sin embargo, existen otros factores, tales como la presencia de ruido, la impedancia característica, la telediafonía, la razón de la atenuación a la diafonía y la pérdida de retorno, que deben probarse, para asegurar el desempeño correcto de las instalaciones, especialmente para la actualización a estándares de mayores velocidades de transmisión. Tal es el caso que determina que instalaciones que cumplan con los estándares de Categoría 5, puedan soportar sin inconvenientes, velocidades de 100 Mbps.

Atenuación

La atenuación, también conocida como pérdida de inserción, es una disminución de la intensidad de la señal a lo largo del cable, tal como se muestra en la figura 3.3. La atenuación se origina por dos factores: la pérdida de energía eléctrica en la resistencia del cable y la fuga de energía a través del material aislante del cable.

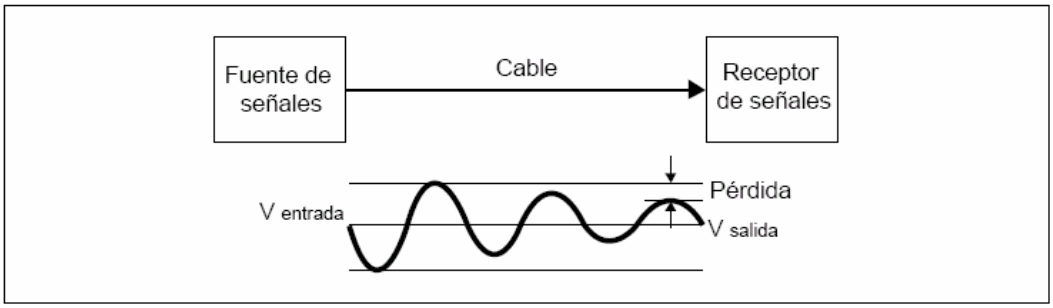


Figura. 3.3. Atenuación de una señal

Esta pérdida de energía se expresa en decibelios, y es por ello que un mejor rendimiento del cable corresponde a valores bajos de atenuación. La atenuación de las señales dentro de un cable, la determina la construcción del cable, la longitud del cable y las frecuencias de las señales dentro del cable.

Ruido Eléctrico

El ruido eléctrico son señales eléctricas no deseadas que alteran la forma de las señales transmitidas por un cable de LAN. La figura 3.4. muestra un ejemplo de cómo el ruido afecta la forma de una señal. Las señales muy distorsionadas por el ruido pueden originar errores de comunicación en una LAN, tales como tramas incompletas, tramas de que no tienen la longitud mínima (runts) o exceden la máxima (giants) e incluso que se detecten falsas colisiones.

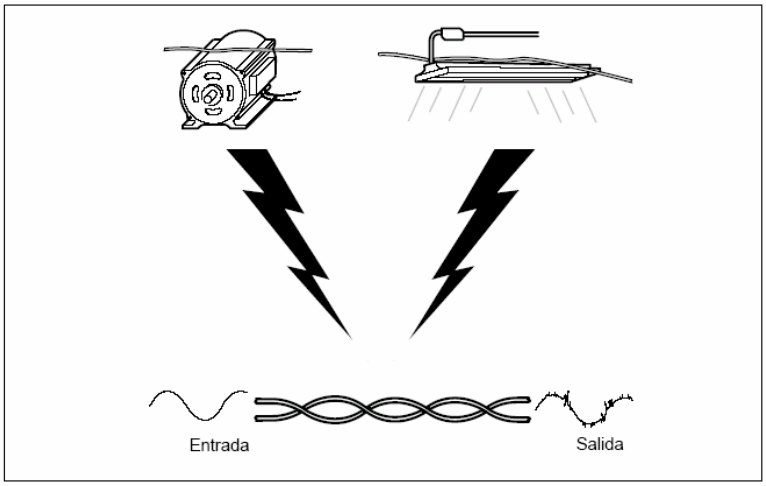


Figura. 3.4. Fuentes de ruido eléctrico

Impedancia Característica

La impedancia característica es la impedancia que tendría un cable si tuviera una longitud infinita. El funcionamiento adecuado de la red depende de tener una impedancia característica constante en todos los cables y conectores del sistema. Los cambios repentinos en la impedancia característica causan reflexiones de las señales, que pueden distorsionar las señales transmitidas por los cables de la LAN y dar lugar a fallos en la red. Estas reflexiones podrían generar colisiones, o atenuaciones excesivas en las tramas transmitidas, por lo que es necesario minimizar la falta de continuidad de la impedancia.

Minimización De La Falta De Continuidad De La Impedancia

Las conexiones y las terminaciones de los cables generalmente alteran ligeramente la impedancia característica al igual que los dobleces agudos en el cable de la LAN. Las redes pueden funcionar con faltas de continuidad pequeñas porque las reflexiones resultantes de la señal son pequeñas y se atenúan en el cable. Las faltas de continuidad mayores pueden interferir en la transmisión de las tramas, y son causadas por un mal contacto eléctrico, terminaciones inadecuadas de los cables, cables o conectores que no concuerden y por perturbaciones en el patrón de trenzado del cable de par trenzado.

Se pueden evitar problemas de falta de continuidad de la impedancia observando las siguientes precauciones:

- No mezclar nunca cables con impedancias características distintas.
- Al destrenzar pares de cables para instalar conectores o para efectuar conexiones en bloques de conexión, mantener las secciones destrenzadas lo más cortas posible.
- No doblar en forma aguda el cable. Consultar las especificaciones del fabricante del cable para conocer el radio mínimo de doblez.
- Manejar el cable para LAN con precaución durante la instalación. No pisar el cable ni comprimirlo con ataduras para cable demasiado ajustadas.

Diafonía

La diafonía es una transmisión de señales indeseables de un par de cables a otro par cercano, lo que puede crear problemas de comunicación en las redes. De todas las características de la operación de redes LAN, la diafonía es la que tiene el mayor efecto en el rendimiento de una red.

Paradiafonía

La paradiafonía (NEXT por sus siglas en inglés) se mide aplicando una señal de prueba a un par de cables y midiendo la amplitud de las señales de diafonía que se reciben en el otro par de cables. El valor de la NEXT, expresado en decibelios, se calcula como la diferencia en la amplitud entre la señal de prueba y la señal de diafonía medida en el mismo extremo del cable. Los valores altos de la NEXT corresponden a una menor diafonía y a un mejor rendimiento del cable.

Telediafonía

La telediafonía (FEXT por sus siglas en inglés) es la diferencia entre la amplitud de una señal de prueba del extremo lejano aplicada a un par y la paradiafonía resultante en un par diferente. Al igual que la NEXT, la FEXT se expresa en decibelios y los valores más altos de la FEXT corresponden a mejor rendimiento del cable.

Como todas las señales FEXT recorren la misma distancia, tienden a sumarse en fase. Puede existir una diferencia entre la NEXT y la FEXT de un enlace, especialmente en la conexión de hardware. La diferencia se debe a la naturaleza de las corrientes capacitivas e inductivas que originan la diafonía. En la fuente de una señal (el extremo cercano) estas corrientes pueden restarse. Si las corrientes se restan en el extremo cercano, éstas se suman en el extremo lejano.

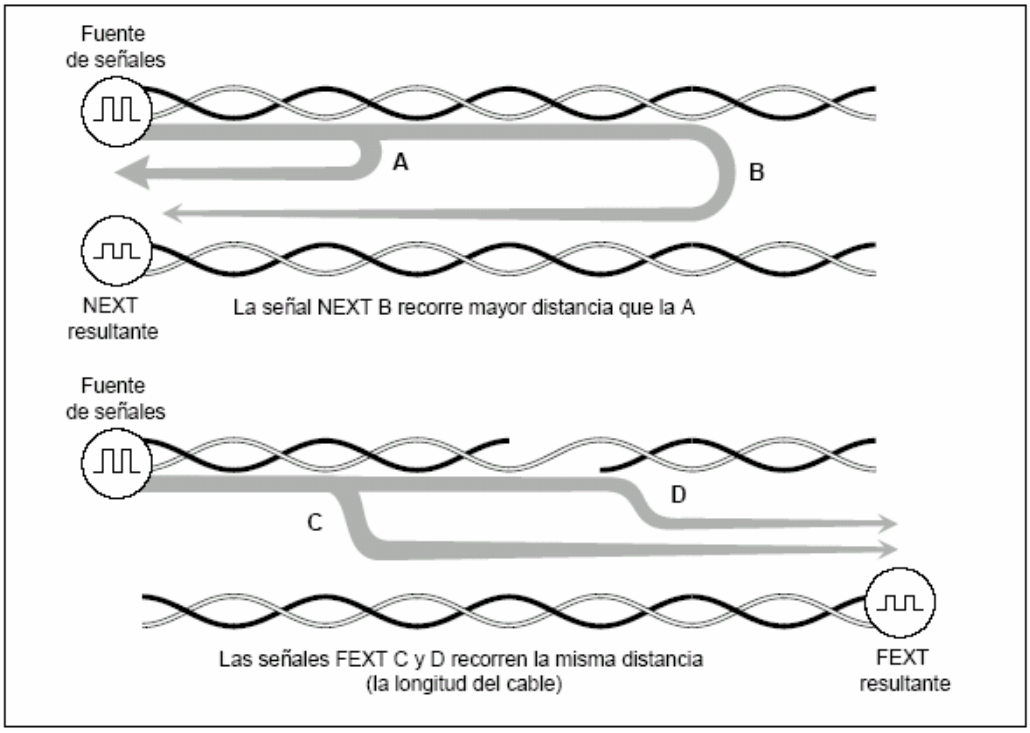


Figura. 3.5. Atenuación de las señales FEXT

Minimización De La Diafonía

Los problemas de diafonía se minimizan trenzando juntos los dos hilos en cada par de cables. El objetivo de trenzar los dos hilos juntos es la cancelación de los campos electromagnéticos alrededor de los hilos, no dejando prácticamente ningún campo externo que transmita señales a los pares de cables cercanos.

Se pueden evitar problemas de diafonía observando las siguientes precauciones:

- Al destrenzar pares de cables para instalar conectores o para efectuar conexiones en los bloques de conexión, procurar que las secciones destrenzadas sean lo más cortas posible.
- Poner atención al efectuar las conexiones del cableado. Los errores en el cableado pueden causar pares partidos que dan lugar a graves problemas de diafonía.
- No doblar en forma aguda el cable.
- Manejar el cable para LAN con precaución durante la instalación.

Técnicas Fundamentales De Diagnóstico

Los diagnósticos en las instalaciones de LAN son necesarios durante la instalación o la modificación del cableado. Cuando el cable se maneja e instala correctamente, casi siempre dará servicio sin problemas durante años. Según fabricantes, como Panduit y Belden, el tiempo de vida útil de una instalación de cableado estructurado debe fluctuar entre los 10 y 12 años.

Una regla general para encontrar fallos en los cables es la siguiente: *Con muy pocas excepciones, los fallos ocurren en las conexiones de los cables.* Las conexiones de los cables incluyen las salidas de telecomunicación, los tableros de conexiones, los bloques de conexión y los conectores de transición. Las conexiones son los lugares más propensos para los fallos por tres razones: (1) las conexiones siempre alteran la impedancia del camino de la transmisión, (2) las conexiones son propensas a fallos por los errores de cableado y la instalación defectuosa o incompatibilidad de equipo y (3) las conexiones siempre causan algo de diafonía debido al destrenzado de los pares del cable.

Cuando un cable se maneja sin cuidado, pueden ocurrir fallos a mitad del cable. Estos fallos pueden ocurrir cuando se pisa el cable, se dobla en forma aguda, se oprime por ataduras para cable u otros herrajes o cuando se somete a esfuerzo mecánico de alguna otra forma.

RESULTADOS DE PRUEBAS DE CERTIFICACIÓN

Como muestra se tomaron cien puntos de red ubicados en el Centro de Cómputo, instalados por personal del departamento de redes, durante la remodelación del mismo. El tipo de prueba realizada fue la de enlace básico y el cable utilizado en la instalación es de categoría 5E, de marca Belden. El equipo certificador es de marca Fluke, modelo 4100.

La elección de esta muestra se debió a que en esta área se concentran los servidores empresariales y que el cableado debe cumplir con todas las pruebas de certificación para

garantizar que no existan fallos físicos que impidan, bloqueen o degraden la comunicación entre los clientes y los servidores instalados.

Por ser un área de continua reubicación, adición y remoción de servidores, ya sea para redundancia, balanceo de carga, adición de servicios, o por mantenimiento, es indispensable que la infraestructura física no presente problemas de ninguna índole. Hay que puntualizar que dichos cambios los realiza el Departamento de Servidores, por lo que la conexión de equipos no debe representar una tarea en la que se requiera personal del Departamento de Redes, sino únicamente en los casos en que se necesite habilitar o configurar puertos en los equipos activos.

Con los antecedentes anteriores, los resultados fueron los siguientes: el 12% de los puntos de la muestra está identificado en ambos extremos. El 100% de los puntos etiquetados tiene una denominación que no corresponde a un ordenamiento lógico ni secuencial de los racks en los cuales se ubica los servidores. La meta es crear un plan de identificación de cableado estructurado e identificar como mínimo el 90% de los puntos ya instalados y el 100% de las nuevas instalaciones.

El 54% de los puertos de los equipos activos tienen una identificación de qué servidor se conecta en ellos. La meta es identificar el 100% de los puertos de conexión de los servidores, al menos el 95% de los puertos de conexión de equipos activos y el 95% de los puertos de conexión de los usuarios de red.

A pesar de ser la instalación más reciente, el 7% de los puntos de la muestra no pasaron las pruebas de certificación de cableado estructurado, lo que permite inferir un manejo no adecuado de la instalación. En la actualidad, el 100% de los puntos de la muestra pasan la prueba de certificación del cableado estructurado. Debido al porcentaje de fallos en las instalaciones, se piensa extender las pruebas de certificación a toda la infraestructura de la empresa. En las páginas siguientes se presenta un resultado típico de la prueba de certificación de cableado estructurado para cuando el punto pasa y no pasa la prueba.

Prueba Exitosa Típica

```
Cable ID: CC-R5-D03                              Test Summary: PASS
ANDINATEL S.A.                                   HEADROOM: 3.7 dB (NEXT @ Remote 36-45)
SITE: Centro de Computo                          Date / Time: 07/08/2004  02:39:56pm
OPERATOR: Roberto Almeida                        Test Standard: TIA Cat 5e Perm. Link
Standards Version: 4.9                           Cable Type: UTP 100 Ohm Cat 5e
Software Version: 3.8                            FLUKE DSP-4000   S/N: 7931020 LIA011
NVP: 69.0%   FAULT ANOMALY THRESHOLD: 15%        FLUKE DSP-4000SR S/N: 7931020 LIA011
SHIELD TEST: N/A

Wire Map PASS                    Result    RJ45 PIN:       1 2 3 4 5 6 7 8 S
                                                           | | | | | | | | |
                                           RJ45 PIN:       1 2 3 4 5 6 7 8
```

	Length		Prop. Delay		Delay Skew		Resistance		Impedance			Attenuation		
Pair	(ft)	Limit	ns	Limit	ns	Limit	ohms	Limit	ohms	Limit	Anom. (ft)	Result (dB)	Freq. MHz	Limit (dB)
12	67	295	99	498	1	44						4.4	100.0	21.0
36	69	295	101	498	3	44						4.4	100.0	21.0
45	69	295	102	498	4	44						4.4	100.0	21.0
78	67	295	98	498	0	44						4.6	100.0	21.0

	Main Results						Remote Results					
	Worst Margin			Worst Value			Worst Margin			Worst Value		
Pair	Result (dB)	Freq. MHz	Limit (dB)	Result (dB)	Freq. MHz	Limit (dB)	Result (dB)	Freq. MHz	Limit (dB)	Result (dB)	Freq. MHz	Limit (dB)
RETURN LOSS												
12	22.5	63.8	14.0	22.0	77.8	13.1	22.1	71.8	13.5	22.0	76.8	13.1
36	17.4	63.0	14.1	17.4	63.2	14.0	16.0*	63.0	14.1	16.0	63.2	14.0
45	22.7	48.2	15.2	22.7	48.2	15.2	19.7	48.4	15.2	19.7	48.4	15.2
78	19.9	44.2	15.6	18.5	100.0	12.0	17.6	44.8	15.5	15.5	95.2	12.2
PSNEXT												
12	36.7	95.6	29.7	36.7	95.6	29.7	39.3	58.8	33.1	38.2	80.4	30.9
36	37.2	95.2	29.7	37.2	95.2	29.7	35.0	95.0	29.7	35.0	95.0	29.7
45	40.1	58.6	33.1	38.0	96.8	29.6	37.8	58.8	33.1	35.7	95.4	29.7
78	41.1	65.4	32.4	39.0	96.0	29.6	38.7	87.4	30.3	38.7	87.4	30.3
PSACR												
12	56.9	6.5	43.5	32.4	95.6	9.2	55.9	6.5	43.5	34.3	80.4	12.2
36	58.9	6.2	44.0	32.9	95.2	9.2	52.2	11.9	37.5	30.7	95.0	9.3
45	56.7	5.7	44.8	33.7	96.8	8.9	55.4	6.0	44.3	31.4	95.4	9.2
78	65.4	3.3	49.6	34.5	96.0	9.1	65.4	3.3	49.6	34.6	87.4	10.7
NEXT												
12-36	38.1	90.2	33.1	38.1	90.2	33.1	39.9	90.0	33.1	39.9	90.0	33.1
12-45	42.2	58.4	36.2	40.4	96.8	32.6	40.1	58.8	36.1	40.1	58.8	36.1
12-78	47.6	40.0	38.8	42.8	96.0	32.6	43.1	80.6	33.9	42.8	85.6	33.5
36-45	42.3	69.0	35.0	41.3	93.4	32.8	36.4	94.6	32.7	36.4	94.6	32.7
36-78	41.8	66.6	35.3	41.8	66.6	35.3	41.2	67.2	35.2	41.2	72.4	34.6
45-78	44.9	89.2	33.2	44.9	89.2	33.2	42.3	89.4	33.2	42.3	89.4	33.2
ACR												
12-36	54.8	11.7	40.7	34.0	90.2	13.2	54.4	12.1	40.3	35.8	90.0	13.2
12-45	58.8	5.7	47.8	36.1	96.8	11.9	57.2	5.9	47.5	36.8	59.0	20.4
12-78	70.3	2.8	54.0	38.3	96.0	12.1	72.2	2.2	55.9	38.7	85.6	14.1
36-45	61.5	6.1	47.1	37.0	93.4	12.6	62.6	5.5	48.1	32.1	94.6	12.3
36-78	66.0	4.3	50.3	38.2	66.6	18.4	68.3	3.6	51.9	37.4	72.4	17.1
45-78	63.3	7.2	45.5	40.6	89.2	13.4	61.2	7.6	45.0	38.0	89.4	13.4
ELFEXT												
12-36	49.1	30.8	28.9	42.2	92.8	19.3	49.2	30.8	28.9	42.2	92.8	19.3
12-45	64.8	5.5	43.8	41.9	92.6	19.3	64.8	5.5	43.8	41.9	92.6	19.3
12-78	79.6	1.8	53.5	46.2	95.6	19.0	79.6	1.8	53.5	46.4	95.6	19.0
36-12	46.6	46.0	25.4	41.6	99.6	18.6	46.6	46.0	25.4	41.6	99.6	18.6
36-45	35.8	94.6	19.1	35.8	94.6	19.1	35.8	94.6	19.1	35.8	94.6	19.1
36-78	40.7	96.6	18.9	40.7	97.4	18.8	40.8	97.6	18.8	40.8	97.6	18.8
45-12	75.9	1.6	54.6	41.8	99.2	18.7	75.9	1.6	54.6	41.8	99.2	18.7
45-36	35.5	94.6	19.1	35.5	94.6	19.1	35.5	93.8	19.2	35.5	94.6	19.1
45-78	70.8	2.8	49.7	46.8	65.0	22.3	70.8	2.8	49.7	46.9	74.0	21.3
78-12	79.1	1.5	55.1	46.0	95.2	19.0	79.2	1.5	55.1	45.8	95.2	19.0
78-36	42.5	92.8	19.3	42.3	100.0	18.6	42.4	92.8	19.3	42.1	100.0	18.6
78-45	74.8	1.6	54.6	46.2	78.0	20.8	74.8	1.6	54.6	46.2	98.2	18.8
PSELFEXT												
12	43.9	46.0	22.4	38.3	100.0	15.6	47.1	31.1	25.8	38.7	99.6	15.6
36	34.1	93.6	16.2	34.1	93.6	16.2	34.3	94.8	16.1	34.3	94.8	16.1
45	34.9	94.8	16.1	34.9	94.8	16.1	34.6	93.8	16.2	34.6	94.6	16.1
78	43.6	56.6	20.6	39.1	96.6	15.9	74.1	1.6	51.6	39.8	100.0	15.6

* Measurement is within the accuracy limits of the instrument.

Prueba Típica de Fallo

```
Cable ID: CC-R3-D05                              Test Summary: FAIL
ANDINATEL S.A.                                   HEADROOM: 2.6 dB (NEXT @ Remote 36-45)
SITE: Centro de Computo                          Date / Time: 07/08/2004  01:28:54pm
OPERATOR: Roberto Almeida                        Test Standard: TIA Cat 5e Perm. Link
Standards Version: 4.9                           Cable Type: UTP 100 Ohm Cat 5e
Software Version: 3.8                            FLUKE DSP-4000   S/N: 7931020 LIA011
NVP: 69.0%   FAULT ANOMALY THRESHOLD: 15%        FLUKE DSP-4000SR S/N: 7931020 LIA011
SHIELD TEST: N/A

Wire Map PASS                    Result    RJ45 PIN:       1 2 3 4 5 6 7 8 S
                                                           | | | | | | | |
                                           RJ45 PIN:       1 2 3 4 5 6 7 8
     |Length      |Prop.     |Delay    |Resistance |Impedance          |Attenuation          |
     |            |Delay     |Skew     |           |             Anom.|Result  Freq. Limit|
Pair |(ft)   Limit|ns  Limit |ns Limit |ohms  Limit|ohms Limit    (ft)| (dB)   MHz    (dB)|
12   |60     295  |88   498  |0   44   |           |                  | 3.9   100.0  21.0 |
36   |61     295  |90   498  |2   44   |           |                  | 4.2   100.0  21.0 |
45   |60     295  |89   498  |1   44   |           |                  | 3.9   100.0  21.0 |
78   |61     295  |90   498  |2   44   |           |                  | 4.0   100.0  21.0 |
      |              Main Results                 |          Remote Results                |
      |Worst Margin        |Worst Value           |Worst Margin        |Worst Value        |
      |Result  Freq. Limit |Result  Freq. Limit   |Result  Freq. Limit |Result  Freq. Limit |
Pair  | (dB)   MHz    (dB) | (dB)   MHz    (dB)  | (dB)   MHz    (dB) | (dB)   MHz    (dB) |
RETURN LOSS FAIL           |                      |                    |                    |
12    | 17.7    73.4  13.4 | 17.4    84.8  12.7   | 16.6    85.0  12.7 | 16.6    85.0  12.7 |
36    | 13.4*F  71.8  13.5 | 13.4    71.8  13.5   | 14.7    97.4  12.1 | 14.7    97.4  12.1 |
45    | 16.7    83.6  12.8 | 16.7    83.6  12.8   | 15.6    83.4  12.8 | 15.6    83.4  12.8 |
78    | 14.3*   70.4  13.6 | 14.3    70.6  13.5   | 19.7    70.2  13.6 | 19.7    70.2  13.6 |
PSNEXT                     |                      |                    |                    |
12    | 39.8    58.2  33.2 | 37.7    95.6  29.7   | 41.2    58.4  33.1 | 39.1    95.6  29.7 |
36    | 35.4    80.8  30.8 | 35.3    87.2  30.3   | 36.0    74.8  31.3 | 36.0    74.8  31.3 |
45    | 35.5    86.8  30.4 | 35.5    88.0  30.3   | 35.4    74.6  31.3 | 35.4    74.6  31.3 |
78    | 37.8    74.6  31.3 | 36.2   100.0  29.3   | 37.3    75.2  31.3 | 36.3    91.8  30.0 |
PSACR                      |                      |                    |                    |
12    | 65.7     2.7  51.3 | 33.9    95.6   9.2   | 56.9     9.5  39.8 | 35.3    95.6   9.2 |
36    | 52.8     9.9  39.4 | 31.2    97.6   8.8   | 52.7     9.7  39.6 | 32.5    74.8  13.5 |
45    | 55.1     8.3  41.2 | 31.9    88.0  10.6   | 54.4     8.5  41.0 | 32.1    74.6  13.5 |
78    | 61.4     5.0  45.9 | 32.2   100.0   8.3   | 54.0    10.5  38.8 | 32.5    91.8   9.9 |
NEXT                       |                      |                    |                    |
12-36 | 49.2    32.8  40.3 | 43.5    80.0  33.9   | 48.7    33.2  40.2 | 43.7    96.6  32.6 |
12-45 | 43.5    58.2  36.2 | 40.7    94.2  32.8   | 42.7    94.0  32.8 | 42.7    94.0  32.8 |
12-78 | 43.1    58.4  36.2 | 40.3    97.4  32.5   | 43.3    58.4  36.2 | 41.5    97.0  32.6 |
36-45 | 36.7    87.0  33.4 | 36.7    87.2  33.3   | 37.0    74.6  34.4 | 37.0    74.6  34.4 |
36-78 | 40.0    70.2  34.9 | 38.2   100.0  32.3   | 46.6    32.2  40.4 | 41.2    92.0  33.0 |
45-78 | 42.9    73.4  34.5 | 42.1    91.0  33.0   | 38.2    91.8  33.0 | 38.2    91.8  33.0 |
ACR                        |                      |                    |                    |
12-36 | 67.9     2.7  54.3 | 39.8    80.0  15.3   | 58.4    10.2  42.1 | 39.6    96.6  12.0 |
12-45 | 59.7     8.4  44.1 | 36.9    94.2  12.4   | 60.7     8.4  44.1 | 39.0    94.2  12.4 |
12-78 | 72.7     1.9  56.9 | 36.4    97.4  11.8   | 72.6     2.0  56.6 | 37.6    97.0  11.9 |
36-45 | 67.9     2.8  54.0 | 33.1    87.2  13.8   | 56.6     8.9  43.5 | 33.7    74.6  16.6 |
36-78 | 50.6    15.9  37.4 | 34.2   100.0  11.3   | 51.2    15.8  37.5 | 37.4    92.0  12.9 |
45-78 | 56.4    11.7  40.7 | 38.3    91.0  13.0   | 55.1    12.1  40.3 | 34.4    91.8  12.9 |
ELFEXT                     |                      |                    |                    |
12-36 | 71.8     1.7  54.0 | 37.7    94.8  19.1   | 71.7     1.7  54.0 | 38.0    94.8  19.1 |
12-45 | 74.8     2.7  50.0 | 44.4   100.0  18.6   | 74.8     2.7  50.0 | 44.4   100.0  18.6 |
12-78 | 76.0     1.7  54.0 | 47.8    94.2  19.1   | 76.0     1.7  54.0 | 47.9    94.2  19.1 |
36-12 | 67.2     2.8  49.7 | 37.9    87.2  19.7   | 67.2     2.8  49.7 | 37.7    94.0  19.1 |
36-45 | 35.3    81.0  20.5 | 34.7    90.8  19.4   | 35.1    81.0  20.5 | 34.5   100.0  18.6 |
36-78 | 69.1     2.7  50.0 | 38.4    99.8  18.6   | 69.2     2.7  50.0 | 38.2    99.8  18.6 |
45-12 | 72.8     2.8  49.7 | 43.2    95.8  19.0   | 72.8     2.8  49.7 | 43.2    95.8  19.0 |
45-36 | 32.6    97.6  18.8 | 32.6    97.6  18.8   | 33.0    97.6  18.8 | 33.0    97.6  18.8 |
45-78 | 71.6     2.8  49.7 | 50.7    98.0  18.8   | 71.7     2.8  49.7 | 50.9    98.0  18.8 |
78-12 | 72.4     2.8  49.7 | 48.2   100.0  18.6   | 72.3     2.8  49.7 | 48.1   100.0  18.6 |
78-36 | 66.6     2.8  49.7 | 37.0    99.6  18.6   | 66.5     2.8  49.7 | 37.2    99.6  18.6 |
78-45 | 75.4     2.7  50.0 | 47.6    90.8  19.4   | 75.3     2.7  50.0 | 47.5    90.8  19.4 |
PSELFEXT                   |                      |                    |                    |
12    | 65.2     2.8  46.7 | 36.8    94.2  16.1   | 70.1     1.7  51.0 | 36.9    94.4  16.1 |
36    | 30.5    97.6  15.8 | 30.5    97.6  15.8   | 32.8    81.6  17.4 | 31.9   100.0  15.6 |
45    | 34.9    81.0  17.5 | 34.1    90.8  16.4   | 32.6    97.6  15.8 | 32.6    97.6  15.8 |
78    | 67.7     2.7  47.0 | 37.9   100.0  15.6   | 65.4     2.8  46.7 | 36.8    99.6  15.6 |
* Measurement is within the accuracy limits of the instrument.
```

PLAN DE IDENTIFICACIÓN DE CABLEADO ESTRUCTURADO

Como se expuso en el capítulo 2: Situación actual de la red MAN, la inexistencia de un plan de identificación de cableado estructurado, ha provocado que se tenga un conocimiento empírico y casi rudimentario de la localización de los puntos de red. Para ubicar fallos y problemas en la infraestructura instalada, hay que utilizar grandes cantidades de tiempo, lo que provoca una ineficiente utilización de los recursos humanos del departamento de redes.

Es por ello, que para ahorrar recursos en futuras reparaciones, y para conocer de forma exacta dónde y cuántos puntos de red existen, y sobre todo, de qué cuarto de comunicaciones se originan, es indispensable que la identificación de los mismos, lleve una codificación fácil de interpretar, en la que se aprecie en qué armario de comunicación se encuentra el otro extremo del cable y un número secuencial que los identifique. Además se deben numerar los cuartos de comunicaciones, para dejar de llamarlos por las oficinas que están cerca, que en varios casos ya no lo están.

Con los criterios anteriormente citados, la identificación de los puntos de red actuales y futuros constará de ocho (8) caracteres: en los tres primeros se identificará el cuarto de comunicaciones, que en adelante se llamará IDF (Intermediate Distribution Facility), dónde se encuentra el primer extremo del cable; el cuarto caracter será un guión que separe la parte de identificación del IDF de la numeración del punto en sí; el quinto caracter será una letra D, si el punto se lo instaló para transmisión de datos, o una letra V si el punto es para transmisión de señales de voz, dejando así tres caracteres para la numeración secuencial del punto. En la práctica, la identificación de un punto desde la implementación de este proyecto, se verá así:

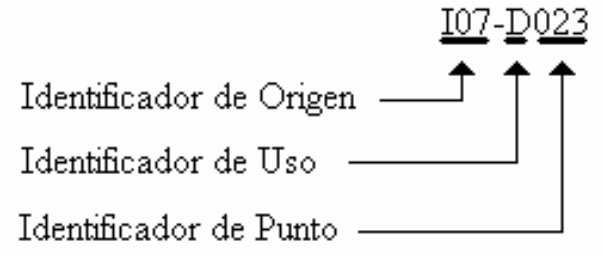


Figura. 3.6. Identificación de puntos de red

DIAGRAMA HORIZONTAL DE LA RED DE ANDINATEL

Debido a la complejidad y constantes cambios físicos de la red, debido a la instalación de nuevos puntos, reubicación de los mismos, o a la remodelación de oficinas y ambientes, es casi imposible llevar un registro arquitectónico actualizado de la configuración física de la red de datos. Para sobrellevar esta limitación, se identifica el puerto de conexión de cada host, y se lo actualiza como una descripción en la interfaz del switch en el cual se conecta el host. El primer paso para realizar dicha operación es obtener la dirección MAC del host y la identificación del punto de red al que se conecta.

Acto seguido se busca dicha dirección en los switches hasta encontrar el puerto de conexión del host, y se actualiza la descripción del puerto. Para ello son necesarios los siguientes comandos:

Switch# show mac-address-table address <dirección MAC del host>

La salida del comando asocia la dirección MAC a un puerto del switch. Ahora en dicho puerto se ingresa la información necesaria por medio de los comandos:

Switch(config)# interface fast 0/x donde x es el puerto en el que se encontró al host
Switch(config-if)# description I0x-Dxxx <Area> donde x es un número de acuerdo a la nomenclatura y Area es el departamento en el que se encuentra el punto. Por ejemplo:

Switch(config-if)# description I03-D023 Marketing

DIAGRAMA VERTICAL DE LA RED DE ANDINATEL

En la figura 3.7 se aprecia el detalle de velocidad y tipo de medio instalado en los enlaces principales que conforman la red MAN de Andinatel S.A. El detalle de las redes LAN en cada edificio de los identificados en el diagrama, no se presenta por motivos de seguridad, aunque vale aclarar que a partir del switch principal de la LAN, el resto de equipos activos se conectan formando la topología de estrella, o estrella extendida, dependiendo del edificio en el que se encuentren. Entre Quito Centro y Mariscal existe una fibra monomodo, la cual no se utiliza, por lo que no se la presenta en la figura 3.7.

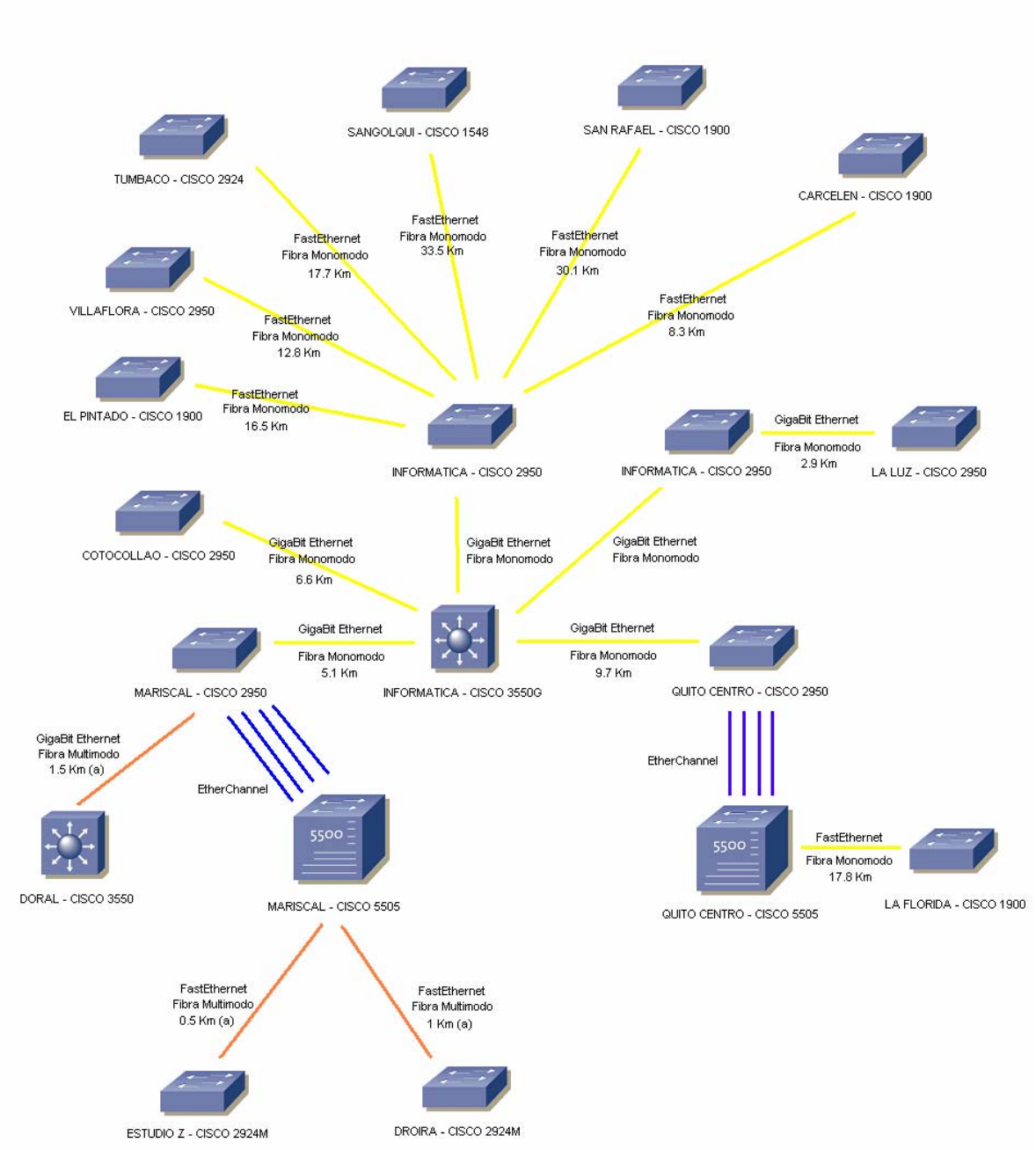


Figura 3.7 Backbone de la Red de Andinatel

CAPITULO IV

MEJORAMIENTO DE LA RED A NIVEL LÓGICO

Se proporciona la siguiente información:

- Implementación del Network Timing Protocol.
- Implementación del Simple Network Management Protocol.
- Implementación de Remote Monitoring.
- Implementación de Spanning Tree Protocol.
- Implementación de Virtual Trunk Protocol.
- Implementación de Cisco Discovery Protocol.

Conocidas las capacidades de los equipos instalados y operativos dentro de la red de Andinatel, y determinada la topología exacta de la red interna de datos, el siguiente paso es configurar los protocolos básicos en los equipos, para que funcionen al unísono, facilitando de esta forma el monitoreo de la red, para prevenir y corregir fallos en el sistema.

NETWORK TIMING PROTOCOL

La definición completa de la arquitectura, algoritmos y protocolos utilizados, y entidades, se lo encuentra en el RFC 1305. El Network Timing Protocol es un protocolo que provee los mecanismos necesarios para sincronizar los relojes internos dentro de un conjunto de servidores y clientes, con una precisión teórica del orden de los nanosegundos, además de proveer una fecha no ambigua. Este protocolo no mejora las prestaciones de la red, sino que provee una herramienta para mejorar la administración de la red.

IMPLEMENTACIÓN DE NTP EN LA RED DE ANDINATEL

El departamento de redes de Andinatel S.A. posee para la sincronización de los relojes de los equipos de red un daemon instalado en un servidor Linux, sin embargo únicamente el 56% de los equipos presentaban una configuración correcta. Para mejorar y facilitar las tareas administrativas, a todos los equipos que soportan este protocolo se les ha configurado como clientes de dicho equipo, hasta llegar a la sincronización del 85% de los equipos de red. Cabe recalcar que esta configuración se la ha realizado únicamente en equipos Cisco, ya que son los únicos equipos dentro de la red que permiten la configuración de este protocolo.

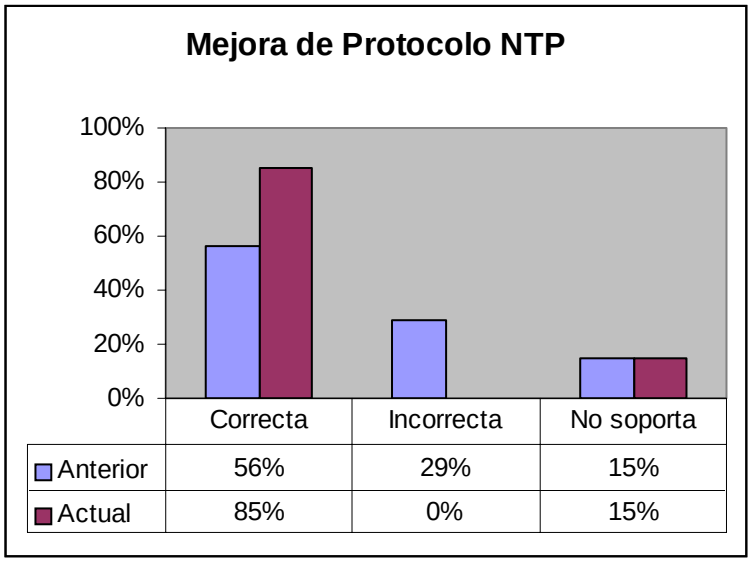


Tabla 4.1. Mejora de protocolo NTP

Es importante verificar el sincronismo entre los clientes y el servidor, ya que esto permite monitorear con exactitud los diferentes eventos que se suceden dentro de los equipos y monitorear condiciones anómalas que afecten simultáneamente a varios equipos. Logrado el sincronismo, es importante variar la forma en que se marca el tiempo del suceso, ya que de ello depende la adecuada administración de la red.

Con la configuración actual, se logra que el monitoreo de los eventos que suceden en los equipos sea llevado a cabo con mayor facilidad y que se logre determinar fácilmente la hora y fecha en que sucedieron los eventos, para correlacionarlos con otros, para inferir

posibles causas de los fallos. Con la configuración anterior, al recuperar el archivo de eventos de los equipos, la salida del mismo es como la siguiente:

19w3d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down

Como se observa, si bien es cierto que el reloj tiene una hora y fecha válidas y sincronizadas con el resto de equipos de red, es casi imposible determinar a qué fecha y hora se sucedieron los eventos expuestos. Con la configuración actual, al recuperar el archivo de eventos de los equipos, la salida es la siguiente:

May 5 12:33:06.457 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down

Como se observa, ahora la marca de tiempo corresponde a la fecha y hora con las cuales el equipo está sincronizado, lo que permite una administración más amigable y sencilla, lo que además permite correlacionar eventos externos, tales como la adición de nuevos equipos en la red, cambios de topología y si éstos influyeron negativamente en la red.

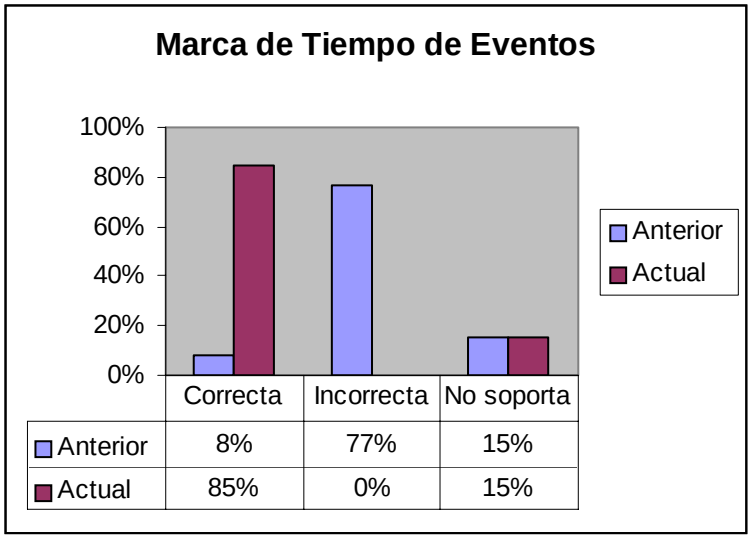


Tabla 4.2. Mejora en la Marca de Tiempo de Eventos

SIMPLE NETWORK MANAGEMENT PROTOCOL

El Simple Network Management Protocol (SNMP por sus siglas en inglés), es un protocolo de la capa de aplicación, parte del conjunto de protocolos TCP/IP, que facilita el intercambio de información de administración, entre dispositivos de red. SNMP permite a la administración de red, el manejo del rendimiento de la red, la localización y solución de problemas de red, y la planificación del crecimiento de la red.

IMPLEMENTACIÓN DE SNMP EN LA RED DE ANDINATEL

Esta sección se relaciona directamente con el proyecto de compra de software especializado para gestión de red que lleva adelante la Vicepresidencia de Sistemas de Andinatel S.A. Luego de entendido el funcionamiento del protocolo, la implementación del mismo, debe abarcar los siguientes aspectos:

- Definición de un servidor para realizar las peticiones y almacenar los reportes.
- Definición de las comunidades de lectura y escritura, para todos los elementos que actuarán como agentes. Por seguridad, y para prevenir que personas no autorizadas modifiquen la configuración de los equipos, se configurará únicamente la clave de lectura, la cual permite tomar estadísticas de los equipos.
- Definición de los eventos que deben reportar los agentes al NMS.

El servidor y la aplicación NMS los adquirirá Andinatel S.A., por lo que hay que definir qué dirección IP se le asignará a dicho servidor. Por motivos de seguridad, dicha dirección no se la puede publicar en este documento, al igual que la comunidad de lectura. La comunidad de escritura no se configurará en ningún equipo, para impedir que personas no autorizadas traten de cambiar la configuración de los equipos. En cuanto a los eventos que los equipos reporten, éstos deben ser del tipo trap dirigida, ya que todos los equipos tienen un gran número de objetos, por lo que sería impráctico recoger información de cada objeto en cada dispositivo manejado.

La solución es que el agente notifique al NMS, sin necesidad de alguna solicitud, enviándole una trap del evento. Las notificaciones del tipo trap dirigidas, ahorran recursos

en cuanto a la utilización del agente y de la red, al seleccionar cuáles eventos relevantes serán anunciados. En cuanto a los eventos de importancia que se quieren analizar se tienen los siguientes: Authentication, linkdown, linkup, coldstart, syslog y config. La primera, *Authetication*, controla el envío de notificaciones de fallos en la autenticación snmp, con los que se logra identificar equipos que estén realizando peticiones SNMP dentro de la red de Andinatel; las dos siguientes, *linkdown* y *linkup*, informan qué puertos se han encendido o apagado, lo que permite identificar patrones de comportamiento de usuarios; la cuarta alarma, *coldstart*, tiene que ver con la reinicialización del equipo y por ende del agente, lo que proporciona información valiosa sobre fallos eléctricos en la red, o bugs en el sistema operativo; la quinta alarma, *syslog*, envía mensajes de notificación de errores, y la última tiene que ver con el cambio en la configuración del equipo.

Con estas consideraciones, la configuración de SNMP se realizó a cabo en todos los equipos de red que soportan este protocolo. La utilidad de este protocolo tiene que ver con la administración del sistema, ya que no reduce ni mejora las prestaciones de la red, solo informa los eventos que suceden dentro de ella.

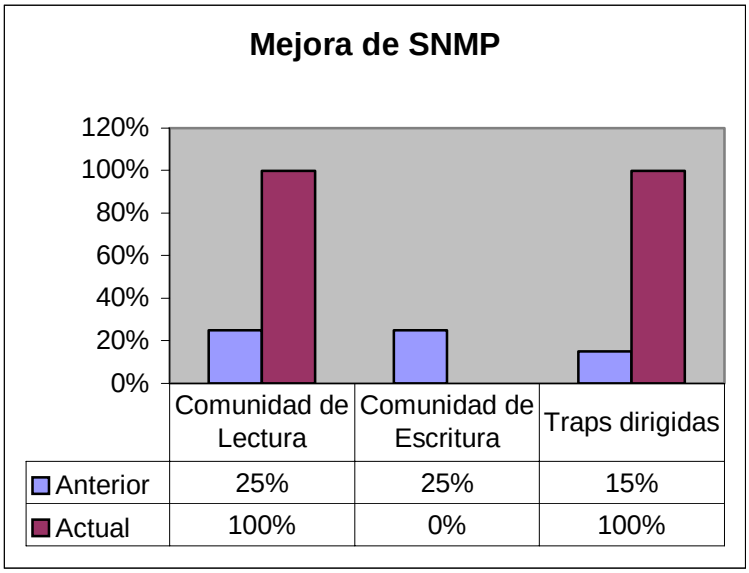


Tabla 4.3. Mejora en el protocolo SNMP

Ahora todos los equipos tienen la misma comunidad de lectura, lo que facilita la implementación de un software especializado para la administración de redes. Al eliminar la comunidad de escritura, se reducen las posibles fallas de seguridad, impidiendo

configuraciones no autorizadas. Al informar los eventos a través de operaciones del tipo trap, se obtiene un monitoreo en tiempo real de los eventos generados dentro de la red.

REMOTE MONITORING

El monitoreo remoto (RMON por sus siglas en inglés), es una especificación estándar de monitoreo, que permite que varios monitores de red y sistemas de consola, intercambien datos de monitoreo de red, tales como estadísticas. RMON provee a los administradores de red la libertad de elegir sondas de monitoreo de red y consolas con características que satisfagan sus necesidades particulares, en cuanto a diagnóstico de fallas de red, e información de rendimiento.

IMPLEMENTACIÓN DE RMON EN LA RED DE ANDINATEL

El protocolo RMON trabaja en conjunto con SNMP, por lo cual no es necesario configurarlo en todas las interfaces de los equipos, ya que se generaría más carga de procesamiento en ellos, lo que puede causar un deterioro en el rendimiento de la red, debido a la cantidad de datos que se deben procesar y almacenar, lo que aumentaría la latencia provocada por los equipos. Este protocolo se configurará únicamente en los puertos troncales de los todos switches de la red que estén en capacidad de soportar este protocolo, ya que es por ellos por donde pasa la totalidad de tráfico de cada segmento de red hacia el Centro de Cómputo.

Con estas consideraciones, la configuración de este protocolo en los equipos de red se la realiza en todos los enlaces troncales que lo soportan para recoger información estadística del tráfico en las interfaces, y así evaluar el desempeño de la red, y detectar a tiempo enlaces conflictivos, al mismo tiempo de planificar aumento en la capacidad de los enlaces.

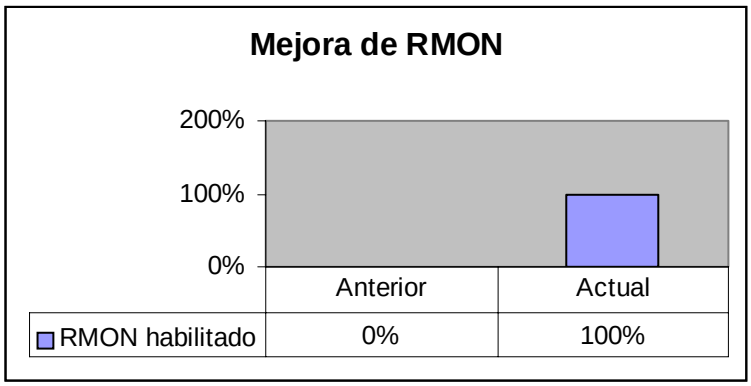


Tabla 4.4. Mejora en el protocolo RMON

El 100% es en referencia a los enlaces entre equipos, no a la totalidad de los equipos.

SPANNING TREE PROTOCOL

Spanning tree es un protocolo de capa 2 de administración de enlaces, que provee redundancia, al mismo tiempo que evita lazos indeseados en la red. Para que una red ethernet funcione de forma adecuada, solo debe existir un camino activo entre dos estaciones. Cuando se diseña redes tolerantes a fallos, se debe tener enlaces libres de lazos entre todos los nodos de la red. El algoritmo de Spanning Tree calcula el mejor camino libre de lazos a través de una red conmutada. Los switches envían y reciben tramas de spanning tree a intervalos regulares; no las retransmiten, pero con ellas construyen el camino libre de lazos.

Spanning tree define un árbol con un switch raíz, y un camino libre de lazos desde la raíz hacia todos los switches en la red. Spanning tree coloca los caminos redundantes en un estado de bloqueo (standby). Si el segmento de red activo falla, y existe un camino redundante, el algoritmo de spanning tree recalcula la topología de spanning tree y activa el camino que estaba en estado de standby.

IMPLEMENTACIÓN DE STP EN LA RED DE ANDINATEL

Aunque pareciera que STP es un protocolo que no necesita ningún tipo de configuración, debido a que las decisiones las toman automáticamente los equipos, es

necesario llevar a cabo configuraciones que impidan que conexiones no autorizadas desencadenen lazos indeseados en la red, con resultados inesperados dentro del funcionamiento normal de la red, entre los cuales no se puede descartar la inutilización de la red, debido a tormentas de broadcast, generadas a partir de lazos físicos.

Además, identificados y documentados los puertos de conexión de todos los hosts dentro de la red de Andinatel, se puede obviar el paso de cada puerto a través de los cinco estados del protocolo, que en total se demora unos 35 segundos, y reducir el tiempo que demora el reconocimiento del host por parte del switch a unos 2 segundos, al mismo tiempo de impedir que en un puerto del switch se conecte otro sin que se otorgue el permiso correspondiente.

Por política interna del departamento de redes, no existen caminos redundantes entre los equipos, por lo que por el momento, la elección del switch raíz se la deja al funcionamiento normal del protocolo dentro de los equipos. Cuando se presente la propuesta de rediseño de la red, los switches centrales deberán ser los switches raíces y se deberá garantizar un ancho de banda mínimo para cada usuario hasta el primer dispositivo de capa 3. Para ello se deberá utilizar EtherChannels entre equipos o enlaces Gigabit. Por lo pronto se realizará la configuración respectiva en todos los puertos de acceso para disminuir el tiempo de reconocimiento de los hosts por parte del switch, así como se impide que se conecten nuevos switches, sin el consentimiento de la administración de la red.

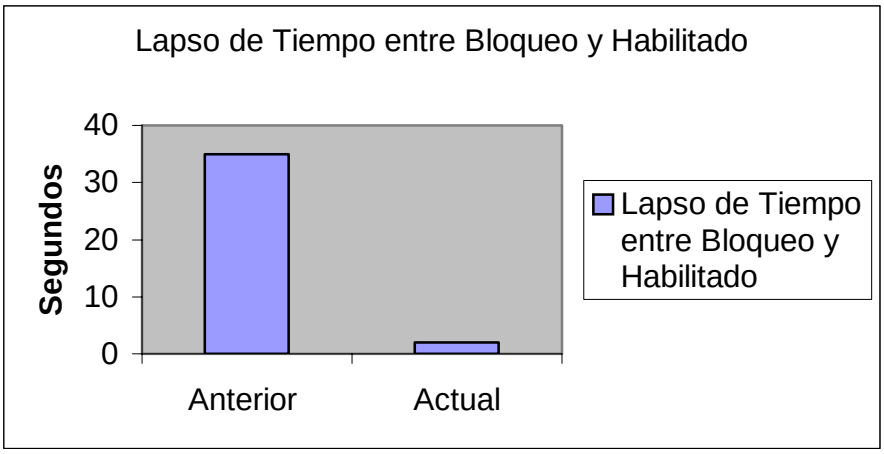


Tabla 4.5. Mejora en el Lapso de Tiempo entre Bloqueo y Habilitado

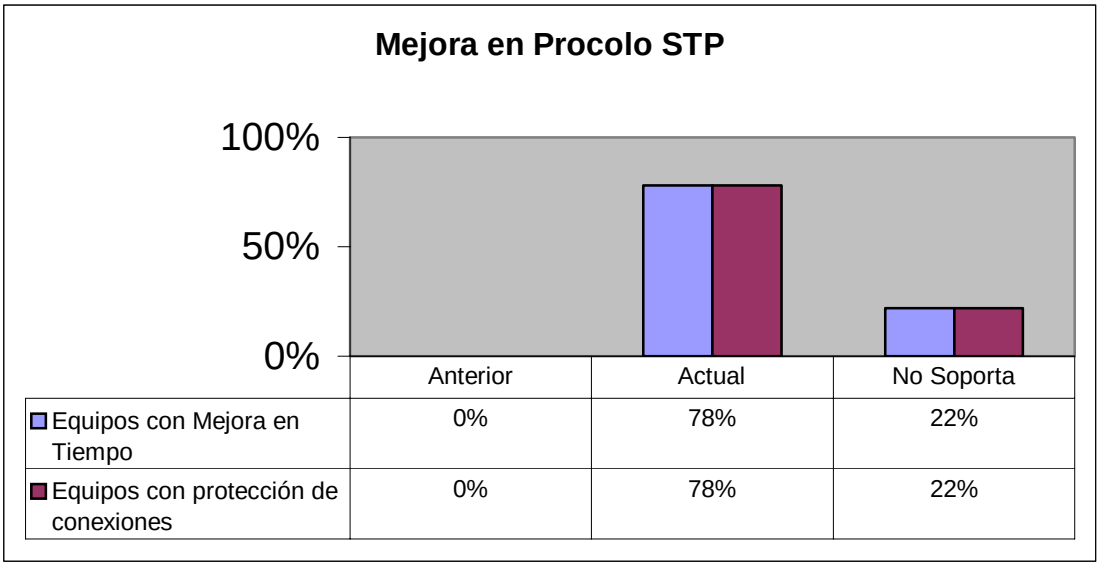


Tabla 4.6. Mejora en el Protocolo STP

Con la reducción del lapso de tiempo que un puerto del switch necesita para pasar del estado bloqueado al de habilitado, se mejora el tiempo de arranque de los hosts conectados a dichos puertos. Al proteger a las equipos de conexiones no autorizadas, se mejora la estabilidad de la red y se tiene un mayor control sobre los dispositivos conectados y por conectarse.

VIRTUAL TRUNK PROTOCOL

Virtual Trunk Protocol (VTP por sus siglas en inglés) es un protocolo de capa 2 que maneja la creación, eliminación y nombres de VLANs con el objetivo de mantener la consistencia de configuración de VLANs dentro de la red. El VTP minimiza las malas configuraciones e inconsistencias en las configuraciones, que pueden causar varios problemas, tales como nombres duplicados de VLANs y violaciones de seguridad. Al utilizar VTP, se pueden realizar cambios de forma centralizada en un solo switch, ya que éstos serán comunicados al resto de switches de la red.

IMPLEMENTACIÓN DE VTP EN LA RED DE ANDINATEL

Establecidas ya las conexiones verticales dentro de la red de Andinatel, el primer paso para configurar este protocolo, es definir como puertos troncales (trunking) a todos los puertos de los switches que definen la red vertical. El puerto al cual se lo va a troncalizar, debe determinarse a partir del diagrama vertical de la red, por lo que pudiera ser cualquiera, aunque se recomienda que sea el primer puerto del switch, y de existir más de un equipo conectado, se debe escoger siempre los primeros puertos. En algunos equipos, no es necesario especificar el tipo de encapsulación que se utilizará ni tampoco las VLANs admitidas, ya que por defecto tienen la encapsulación 802.1q y admiten todas las VLANs de la 1 a la 1005.

Troncalizados todos los puertos de conexión vertical, se debe configurar a los equipos que servirán como servidores VTP: uno principal y otro de respaldo, en segmentos diferentes de la red, para proporcionar redundancia y supervivencia en caso de fallo del principal. Al resto de equipos se los configurará como clientes, y sobre todo, hay que configurarlos a todos, tanto clientes como servidores, dentro del mismo dominio. Por políticas de seguridad, el nombre del dominio no se presenta en este documento escrito, ya que es para uso exclusivo del personal del departamento de redes de Andinatel.

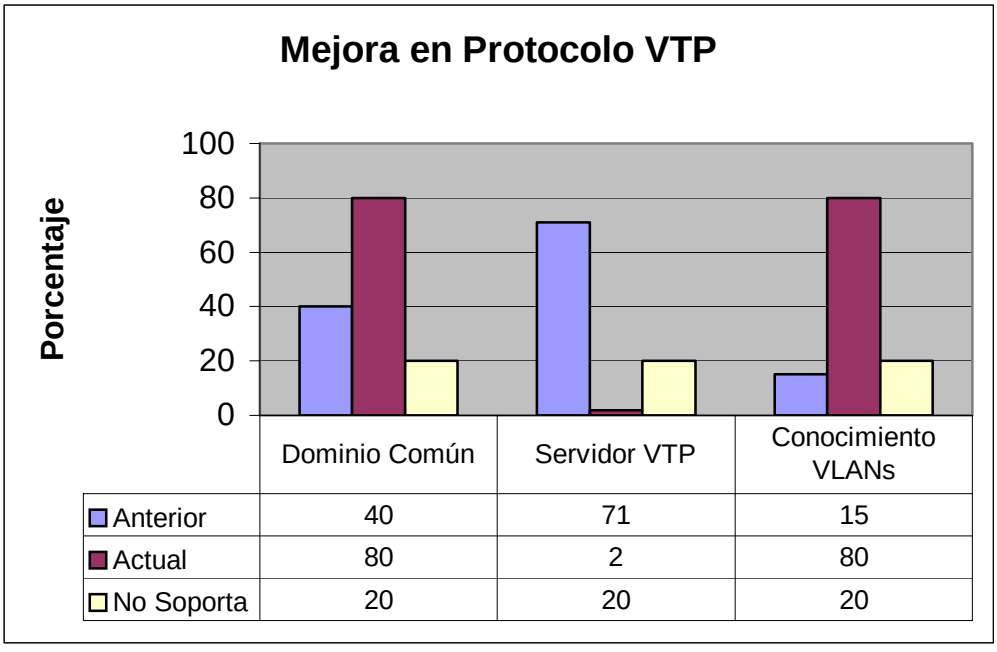


Tabla 4.7. Mejora en el Protocolo VTP

Los resultados de la configuración del protocolo VTP se muestran en la tabla 4.7. Al consolidar todos los equipos capaces en un solo dominio VTP, se logra una visión uniforme y coherente de todas las VLANs configuradas. Al permitir únicamente que dos equipos sean servidores, se racionaliza y facilita la administración de las VLANs creadas. Los beneficios conseguidos con este protocolo son meramente administrativos, pero de suma importancia para el diseño definitivo de la red.

CISCO DISCOVERY PROTOCOL

El Cisco Discovery Protocol (CDP por sus siglas en inglés) es un protocolo de capa 2, independiente de medios y red, utilizado para descubrir información acerca de dispositivos vecinos. Por operar en la capa de Enlace de Datos, no necesita de protocolos de red como IP o IPX para transportar datos. Los dispositivos en los que está habilitado CDP envían avisos periódicos a la dirección MAC de multicast 0100.0ccc.cccc, cada treinta segundos por defecto. El holdtime por defecto es de 180 segundos; si no se recibe avisos durante este lapso de tiempo, la entrada CDP se borra de la tabla CDP.

CDP opera en todos los equipos de marca Cisco, incluidos routers, switches, bridges, access servers y teléfonos IP. Recolecta información acerca de los dispositivos vecinos, tal como el tipo de dispositivo, el nombre del dispositivo, si está configurado, la versión de software, el tipo y número del puerto local y remoto de conexión, el número de segundos que es válido el aviso y la dirección de la capa de red, si ésta está configurada. Los datos obtenidos los almacena en una tabla localizada en la memoria RAM del equipo.

IMPLEMENTACIÓN DE CDP EN LA RED DE ANDINATEL

Determinados y documentados los puertos de conexión de los hosts, servidores y equipos activos dentro de la red de Andinatel, para disminuir el tráfico innecesario que se dirige hacia los servidores, se opta por suprimir los avisos periódicos que envía el protocolo en mención por los puertos a los cuales se conectan los servidores empresariales, ya que no existe la posibilidad de que en estos puertos se conecten otros equipos activos.

CAPITULO V

RED INALÁMBRICA LAN

Se proporciona la siguiente información:

- Introducción a las LAN inalámbricas.
- Tecnología Spread Spectrum.
- Arquitectura de la Red.
- Implementación de Red.

INTRODUCCIÓN A LAS LAN INALÁMBRICAS

Las redes LAN inalámbricas se desarrollaron con el propósito de ser un punto de acceso a las redes alámbricas, al tiempo que ofrecen una solución específica para un problema difícil: la movilidad de usuarios. Y es que las LANs inalámbricas son relativamente rápidas, baratas y se pueden instalar virtualmente en todo lugar.

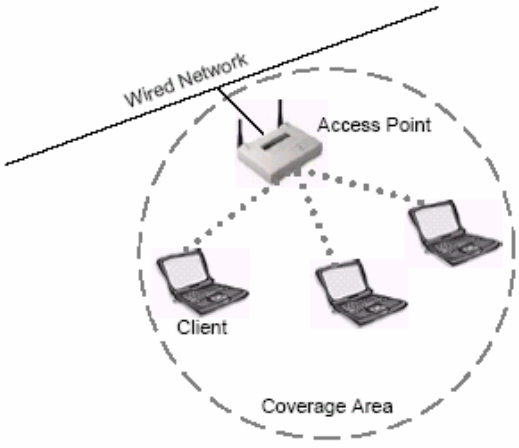


Figura. 5.1. Rol de las LANs inalámbricas

Extensión De Red

Las redes inalámbricas sirven como una extensión de la red alámbrica, ya que en muchos casos, la extensión de la red alámbrica necesitaría cables y ductería adicionales, de costos prohibitivos, debido a la necesidad de nuevas obras civiles, que causen molestias a otros usuarios, internos o externos a la organización. Además, en el caso de distancias considerables, es posible que la LAN no pueda extenderse por razones obvias, y que la fibra óptica no sea la solución adecuada, tanto técnica como económica, ya sea porque los equipos instalados no poseen interfaces de fibra, o porque la relación costo beneficio de la instalación no amerita la inversión. Las LANs inalámbricas pueden instalarse fácilmente para brindar conectividad a áreas remotas de un edificio como se ilustra en la figura 5.2.

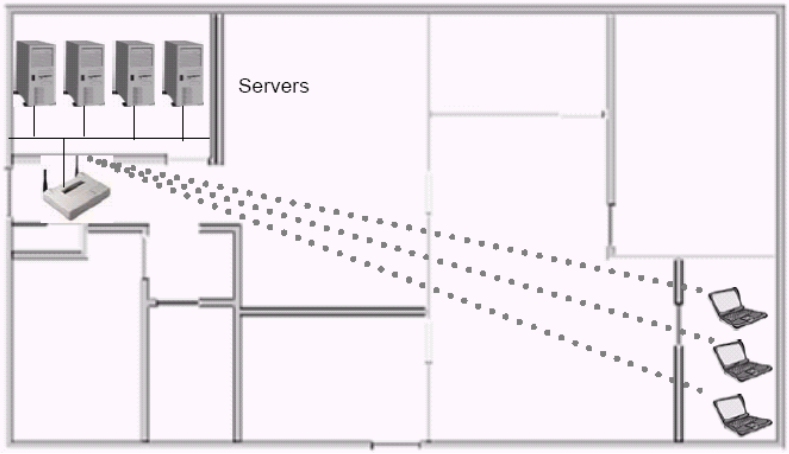


Figura. 5.2. Extensión de Red

Movilidad

Las redes inalámbricas no pueden reemplazar a las alámbricas por cuanto las velocidades de transmisión son todavía inferiores (100 Mbps de FastEthernet contra 54 Mbps de 802.11a), sin embargo, la gran ventaja de las redes inalámbricas es su capacidad de ofrecer movilidad a los clientes, sacrificando velocidad. Además las redes inalámbricas permiten realizar roaming automático, o lo que es lo mismo, moverse físicamente de un área de cobertura inalámbrica, a otra, sin perder conectividad, tal como si se tratara de clientes de telefonía celular.

Oficinas Móviles

Las oficinas móviles permiten que los usuarios empaquen sus equipos y se trasladen rápidamente a otro lugar. Esto resulta particularmente útil para salas de sesiones, despachos gerenciales, y oficinas administrativas, donde se deben llevar a cabo reuniones o juntas de trabajo, y el costo de incrementar y mantener la infraestructura de cableado estructurado es alta, tomando en cuenta, que su uso es esporádico. Este es el principal motivo por el cual se pretende instalar una red inalámbrica dentro de la infraestructura física de Andinatel S.A.

En otras ocasiones, debido al crecimiento propio de la empresa, o al mejoramiento de la infraestructura física, es necesario trasladar de forma temporal a los trabajadores a otras oficinas, en donde la infraestructura de telecomunicaciones es limitada. La instalación de un nuevo sistema de cableado estructurado resultaría demasiado oneroso, tomando en cuenta, el tiempo que se demora en instalar, y el tiempo que estará en uso.

TECNOLOGÍA SPREAD SPECTRUM

Es una técnica de comunicación que se caracteriza por el amplio ancho de banda y baja potencia pico. Utiliza varias técnicas de modulación en las redes inalámbricas y posee varias ventajas sobre su precursora, la comunicación de banda estrecha. Las señales de spread spectrum son parecidas al ruido, difíciles de detectar, y aún más de interceptar o demodular sin el equipo apropiado.

La comunicación de banda estrecha es una tecnología de comunicación que solamente utiliza el espectro de frecuencias suficiente para transmitir la portadora digital. El spread spectrum es el opuesto a esto, ya que utiliza una banda de frecuencia mucho más amplia que la necesaria para transmitir la información. Este es el primer requisito que debe cumplir una señal para considerarse spread spectrum.

La figura 5.3. ilustra la diferencia entre las transmisiones de banda estrecha y spread spectrum. La característica de la transmisión de banda estrecha es la alta potencia pico,

necesaria para la transmisión libre de errores en un rango pequeño de frecuencias. Para recibir las señales, éstas deben permanecer sobre el umbral de ruido con un margen apreciable.

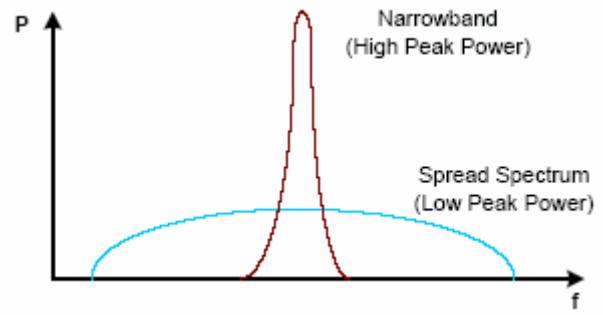


Figura. 5.3. Spread Spectrum vs Banda Estrecha en Dominio de la Frecuencia

Aparte de la gran potencia necesaria, las transmisiones de banda estrecha pueden interferirse o anularse fácilmente, ya que otras señales en la misma banda, incluido el ruido, pueden eliminar completamente la información al superponerse a la señal original.

Tecnología Spread Spectrum

La tecnología spread spectrum permite tomar la cantidad de información que se transmitiría en una portadora de banda estrecha, y esparcirla en una rango de frecuencias mucho más amplio. Por ejemplo, en banda estrecha se puede utilizar una portadora de 1 MHz y 10 W, pero en spread spectrum se puede utilizar 20 MHz y 100 mW, ya que al ensanchar el espectro de frecuencias, la probabilidad de que los datos se corrompan o interfieran, se reduce.

Mientras que el ancho de banda de spread spectrum es amplio, la potencia pico de la señal es baja, siendo éste el segundo requisito para que una señal sea considerada spread spectrum. Las dos características de spread spectrum, ancho de banda amplio y baja potencia, hacen que las señales sean percibidas como ruido por la mayoría de receptores, por lo que no intentarán demodular o interpretar las señales recibidas, creando así una comunicación más segura.

Spread Spectrum De Secuencia Directa

Spread Spectrum de Secuencia Directa (Direct Sequence Spread Spectrum – DSSS – por sus siglas en inglés) es el tipo de spread spectrum más ampliamente conocido y difundido, debido a la facilidad de implementación y altas velocidades de transmisión de datos. DSSS es un método de transmisión de datos en el cual los sistemas de transmisión y recepción operan dentro de un conjunto de canales de frecuencias de 22 MHhz de ancho.

Funcionamiento de DSSS

DSSS combina la señal digital de la estación de transmisión, con una secuencia de datos de mayor velocidad, conocida como el código de chip, o ganancia del proceso. Una alta ganancia de proceso, incrementa la resistencia de la señal a las interferencias. El proceso de secuencia directa empieza cuando la portadora se modula con un código secuencial. El número de "chips" en el código determinarán cuánto ensanchamiento se produce y el número de chips por bit y la velocidad del código (en chips por segundo) determinarán la velocidad de datos.

Sistemas de Secuencia Directa

En la banda de 2.4 GHz, la IEEE especifica el uso de DSSS a una velocidad de 1 ó 2 Mbps bajo el estándar 802.11, ó 5.5 y 11 Mbps bajo el estándar IEEE 802.11b. Los dispositivos que operan bajo el estándar IEEE 802.11b pueden comunicarse con dispositivos que operen bajo el estándar IEEE 802.11, ya que son totalmente compatibles. Recientemente se aprobó el estándar IEEE 802.11g, en el que se especifica velocidades de hasta 54 Mbps, totalmente compatible con el estándar IEEE 802.11b, a diferencia del estándar IEEE 802.11a que opera en la banda de los 5 GHz.

Canales

Los sistemas de DSSS utilizan una definición convencional de canales: Cada canal es una banda de frecuencias contiguas de 22 MHz de ancho con una portadora de 1MHz. Por ejemplo el Canal 1 opera de 2.401 GHz a 2.423 GHz (2.412 GHz ± 11 MHz), el canal 2

opera desde los 2.406 GHz a 2.4028 GHz (2.417 GHz ± 11 MHz), y así sucesivamente hasta el canal 11. La figura 5.4. ilustra la relación de los canales.

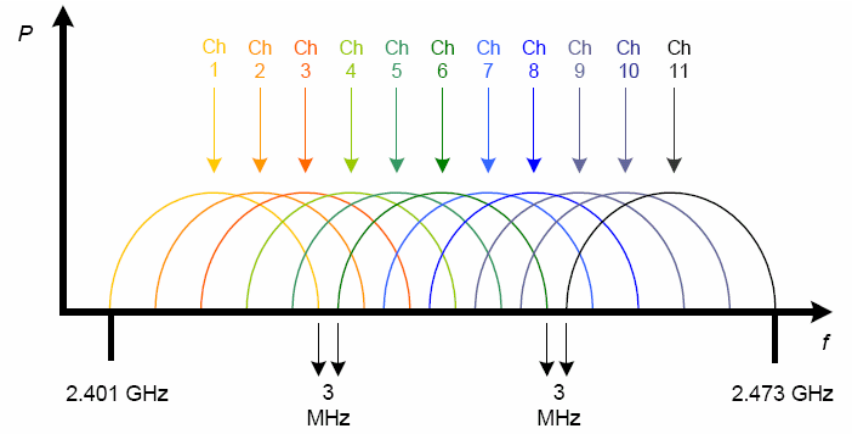


Figura 5.4. Canales DSSS y relación espectral.

La tabla 5.1. tiene una lista completa de los canales que se utilizan en Estados Unidos y Europa. La Comisión Federal de Comunicaciones (FCC por su siglas en inglés) especifica únicamente 11 canales para el uso en Estados Unidos. Como se puede apreciar, los canales 1 y 2 se sobreponen (overlap) de forma significativa, siendo norma general la superposición significativa de los canales adyacentes. Cada una de las frecuencias de la tabla 5.1 es una frecuencia central, por lo que hay que añadir y restar 11 MHz para obtener el canal utilizable de 22 MHz.

Canal	Frecuencia GHz EE.UU.	Frecuencia GHz Europa
1	2.412	N / A
2	2.417	N / A
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457	2.457
11	2.462	2.462

Tabla 5.1. Asignación de canales DSSS

El uso de sistemas DSSS con canales sobrepuestos, en el mismo espacio físico, causaría interferencia entre los sistemas, por lo que esta práctica debe evitarse, ya que la interferencia causaría una drástica reducción en la velocidad del sistema, y en el peor de los casos, no habría conectividad.

Dado que las frecuencias centrales están separadas únicamente por 5 MHz, cuando el ancho del canal es de 22 MHz, se podrán activar dos canales únicamente si el número del canal es superior en 5: los canales 1 y 6 no sobreponen, los canales 2 y 7 no se sobreponen, etcétera. Hay un máximo de 3 canales que pueden activarse de forma simultánea en el mismo espacio físico. Estos son los canales 1, 6 y 11, que teóricamente no se superponen. La figura 5.5. muestra la relación entre estos canales.

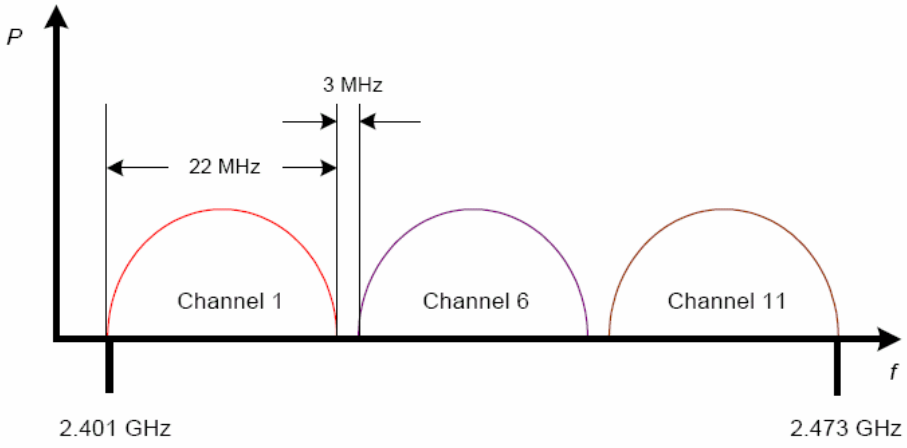


Figura. 5.5. Canales no superpuestos

ARQUITECTURA DE LA RED

Esta sección cubre conceptos clave de la arquitectura de la red 802.11, establecidos en los respectivos estándares, para de esta forma introducir los pasos elementales del diseño y administración de redes inalámbricas.

Localización De Red Inalámbrica

Cuando se instala y configura un dispositivo cliente de red inalámbrica, tal como un cliente USB o una tarjeta PCMCIA, el cliente automáticamente “escucha” para informarse si está dentro de los límites de una red inalámbrica. También intenta asociarse a esa red. Ese proceso de “escuchar”, no es más que la búsqueda de la red, que es el primer proceso, ya que de esta forma, es como se encuentra a la red.

Hay dos tipos de búsqueda: búsqueda activa y búsqueda pasiva. Un Access Point deja un rastro para que las estaciones cliente puedan encontrarlo. Estos rastros son los Service Set Identifiers (SSID por sus siglas en inglés) y los beacons, herramientas que permiten la localización de los Access Points.

Service Set Identifier

El SSID es un valor alfanumérico único, de longitud variable entre 2 y 32 caracteres, que representa al nombre de la red inalámbrica. El manejo de nombres se utiliza para segmentar redes, como medida de seguridad, y en el proceso de asociarse a una red. El valor del SSID se lo envía en los beacons y otros tipos de trama. Una estación cliente debe tener el SSID correcto para que pueda conectarse al Access Point. Si los clientes deben conectarse a través de varios Access Points, los clientes y los Access Points deben configurarse con SSID iguales. El punto más importante de un SSID es la correspondencia exacta entre el valor que posee el cliente, y el configurado en el Access Point.

Beacons

Son tramas cortas enviadas desde el Access Point a las estaciones (modo de infraestructura) o de estación a estación (modo Ad Hoc) para organizar y sincronizar la comunicación inalámbrica dentro de la red inalámbrica. Los beacons sirven para varias funciones, entre las que se incluyen:

Sincronización

Se sincroniza a los clientes por medio de una marca de tiempo (time-stamp) al momento exacto de la transmisión. Cuando el cliente recibe el beacon, cambia su reloj, para reflejar el reloj del Access Point, sincronizándose de esto modo. La sincronización de los relojes asegura que las funciones sensibles al tiempo se ejecuten sin error. El beacon también contiene el intervalo de beacon, que informa a la estación la periodicidad con la que recibirá los beacons.

Información De SSID

Las estaciones cliente buscan dentro del beacon, el valor del SSID de la red a la cual quieren conectarse. Cuando se encuentra la información, la estación busca la dirección MAC del origen del beacon y envía una petición de asociación para asociarse con el Access Point. Si la estación está configurada para aceptar cualquier SSID, la estación intentará conectarse a la red a través del primer access point que envíe un beacon, o el que tenga la mejor señal, si existen múltiples Access Points.

Mapa De Identificación De Tráfico

El Mapa de Identificación de Tráfico (TIM por sus siglas en inglés), se utiliza como un indicador de cuáles estaciones dormidas tienen paquetes en la cola, dirigidos al Access Point. Esta información se pasa a todas las estaciones asociadas a través del beacon. Mientras duermen, las estaciones sincronizadas encienden sus receptores, analizan el TIM para ver si están en lista, y si no lo están, apagan sus receptores y continúan durmiendo.

Velocidades Aceptadas

Dentro de las redes inalámbricas, existen varias velocidades aceptadas, que dependen del hardware utilizado. Por ejemplo, un dispositivo que cumpla la norma 802.11b, soporta las velocidades de 11, 5.5, 2 y 1 Mbps. Esta información se pasa en los beacons para informar a las estaciones cuáles son las velocidades aceptadas por el Access Point.

Búsqueda Pasiva

La búsqueda pasiva (pasive scanning) es el proceso de escuchar los beacons en cada canal, por un tiempo determinado, luego de la inicialización de la estación, hasta que se oiga un beacon en el que se encuentre el SSID de la red a la cual se desea conectarse. Ubicado el beacon, la estación intenta conectarse a la red a través del Access Point del que recibió el beacon. La búsqueda pasiva se ilustra en la figura 5.6.

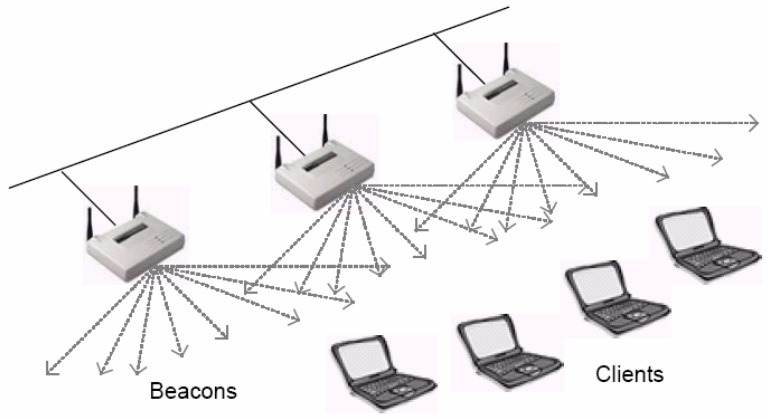


Figura 5.6. Búsqueda Pasiva

Los clientes continúan con la búsqueda pasiva incluso después de asociarse a un Access Point. Este tipo de búsqueda ahorra tiempo al reconectarse a la red, ya que en caso de que el cliente se desconecte de la red, por cualquier circunstancia, éste mantiene una lista de los Access Points disponibles y sus características, tales como canal, potencia de señal, y SSID, y tratará de localizar al mejor Access Point disponible.

Los clientes harán el “roaming” de un Access Point a otro luego de que la potencia de la señal de radio sea menor a un nivel mínimo, con el fin de permanecer conectados a la red. La información obtenida a través de la búsqueda pasiva se la utiliza para localizar el mejor Access Point para mantener la conexión. Es por ello que la superposición entre celdas debe corresponder a aproximadamente del 20 al 30%, para efectuar el “roaming” de forma transparente.

Búsqueda Activa

En la búsqueda activa, se envía una trama de petición desde los clientes. Esta sonda se envía para buscar de forma activa una red a la cual conectarse, por ello se incluye el SSID de la red a la cual se desea conectar. Esta petición será contestada por el Access Point que tenga un SSID concordante con la petición, como se ilustra en la figura 5.7.

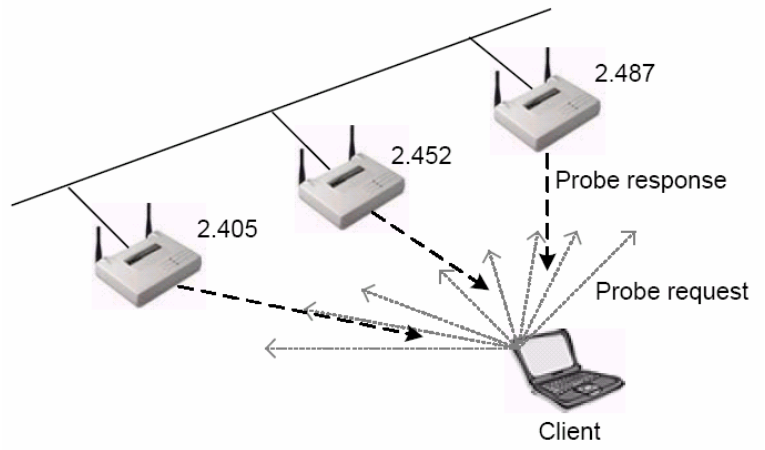


Figura. 5.7. Búsqueda Activa

La respuesta que recibe la estación es casi idéntica a un beacon, salvo que no tiene la marca de tiempo, ni el mapa de tráfico. La potencia de la señal recibida, además ayuda a determinar al Access Point con la mejor calidad de señal, mejor relación señal a ruido, y menor BER, para intentar asociarse a éste.

AUTENTICACIÓN Y ASOCIACIÓN

El proceso de conexión a una red inalámbrica consta de dos subprocesos, que ocurren siempre en el mismo orden, y se los conoce como autenticación y asociación. La asociación se refiere a la conectividad de capa 2, y la autenticación se refiere a la tarjeta de red, mas no al usuario. Los pasos de conexión de los clientes son cruciales en la seguridad, solución de problemas y manejo de las redes inalámbricas.

Autenticación

Es el primer paso para la conexión. Es el proceso a través del cual la red valida la identidad del cliente inalámbrico que intenta conectarse. Algunas veces el proceso es nulo, lo que significa que aunque el cliente y el Access Point tienen que proceder con la autenticación, no se necesita ninguna identidad especial para establecer la asociación.

El cliente envía una trama de petición de autenticación al Access Point para iniciar el proceso de autenticación. El Access Point acepta o niega esta petición, y notifica su decisión con una trama de respuesta de asociación. Un Access Point puede realizar el proceso de autenticación, o pasar la responsabilidad a un servidor de autenticación, tal como un servidor RADIUS. El servidor RADIUS efectuará la autenticación en base a una lista de criterios; envía los resultados al Access Point, para que éste los reenvíe al cliente.

Asociación

Luego de que un cliente se ha autenticado, se asocia a un Access Point. La asociación es el estado en el cual se permite al cliente enviar información a través del Access Point. Si un cliente se asocia a un Access Point, está conectado a ese Access Point y por ende a la red. El proceso de asociación es el siguiente: cuando un cliente se desea conectar a la red, envía una petición de autenticación al Access Point y recibe una respuesta de autenticación. Luego de completar el proceso de autenticación, el cliente envía una petición de asociación al Access Point, y recibe una respuesta de asociación, lo que le permite la asociación o la no asociación.

Estados De Autenticación Y Asociación

El proceso completo de autenticación y asociación tiene tres estados:

No autenticado y no asociado. Es el estado inicial, en el cual el cliente está desconectado de la red y no puede transmitir tramas a través del Access Point.

Autenticado y No Asociado. En este segundo estado, el cliente culminó el proceso de autenticación pero todavía no está asociado. Al cliente todavía no se le permite enviar o recibir datos a través del Access Point.

Autenticado Y Asociado. En el estado final, el cliente está completamente conectado a la red y es capaz de enviar y recibir datos a través del Access Point al cual está asociado.

MÉTODOS DE AUTENTICACIÓN

El estándar IEEE 802.11 especifica dos métodos de autenticación, autenticación de sistema abierto (Open System) y la autenticación de llave compartida (Shared Key). La más simple y segura es la de sistema abierto.

Autenticación De Sistema Abierto

Es un método de autenticación nula especificada por el estándar IEEE 802.11 como el valor por defecto en el equipo de red inalámbrica. Si se utiliza este método, un cliente se puede asociar a cualquier Access Point con autenticación de sistema abierto, con la sola condición de tener exactamente el mismo SSID.

Proceso De Autenticación De Sistema Abierto

- El cliente envía una petición para asociarse al Access Point.
- El Access Point autentica al cliente, envía una respuesta positiva por lo que el cliente se asocia (conecta).

Es un proceso muy simple, que no necesita de configuración tanto en el cliente como en el Access Point, ya que tiene soporte en todos los equipos que cumplan con la norma IEEE 802.11.

Autenticación De Llave Compartida

Es un método de autenticación en el que es necesario el uso de WEP. El cifrado WEP utiliza llaves introducidas tanto en el cliente como en el Access Point. Ambas llaves deben concordar en ambos lados para que funcione de forma adecuada.

Proceso De Autenticación De Llave Compartida

- El cliente pide asociarse al Access Point.
- El Access Point emite un desafío al cliente. Este desafío (challenge) se genera de forma aleatoria, y se lo envía al cliente en forma de texto llano (plain text).
- El cliente responde al desafío. Cifra el texto con su llave WEP y lo envía al Access Point.
- El Access Point responde a la respuesta del cliente. Descifra la respuesta cifrada del cliente para verificar que el texto fue cifrado con una llave WEP concordante. A través de este proceso, el Access Point determina si el cliente tiene la llave WEP correcta.

Si la llave WEP del cliente es correcta, el Access Point autenticará al cliente, caso contrario lo dejará en el estado de no autenticado y no asociado.

Seguridad De Autenticación

No se considera segura a la autenticación de llave compartida porque el Access Point envía el desafío en texto llano y recibe el mismo texto cifrado con la llave WEP. Esto permite que un hacker utilice un sniffer para ver el desafío en texto llano y cifrado, lo que le permitiría obtener la llave WEP, con lo que podría descifrar todo el tráfico. Es por ello

que se considera a la autenticación de sistema abierto como un método más seguro de autenticación de clientes.

PROTOCOLOS DE AUTENTICACIÓN EMERGENTES

Actualmente existen nuevas soluciones y protocolos de seguridad entre los cuales se incluyen a las VPNs y 802.1x con el Protocolo de Autenticación Extensible (EAP por sus siglas en inglés). Muchas de estas soluciones utilizan servidores de autenticación para permitir o denegar el acceso a la red. Durante la fase de autenticación, el access point mantiene en espera al cliente hasta recibir la contestación del servidor.

802.1x y EAP

El estándar 802.1x, que se encarga del control de acceso a la red basado en puerto, es relativamente nuevo y los dispositivos que lo soportan permiten la conexión a la red, a nivel de capa 2, únicamente si la autenticación del usuario es exitosa. Este protocolo funciona bien en los access points que necesitan mantener a los usuarios desconectados si se supone que éstos no deben conectarse a la red. EAP es un protocolo de capa 2 que es un reemplazo flexible para PAP y CHAP, ya que permite plug-ins en cualquier extremo de la conexión, por lo que varios métodos de autenticación pueden utilizarse.

La autenticación de usuarios se la realiza a través a través de un servidor RADIUS (Remote Authentication Dial In User Service) y algún tipo de base de datos de usuario, tal como Native Radius, NDS, Active Directory entre otras. Ya que la seguridad en redes inalámbricas es esencial, los fabricantes están añadiendo rápidamente nuevas implementaciones de EAP a sus productos.

IMPLEMENTACIÓN DE LA RED WIRELESS EN ANDINATEL

Desde el primer semestre del año 2004, el Departamento de Redes de Andinatel está implementando la LAN inalámbrica en lugares específicos de la infraestructura física. El proyecto piloto contempla la totalidad del edificio de la Vicepresidencia de Tecnología, la Presidencia Ejecutiva, la Vicepresidencia de Operaciones, la Vicepresidencia de Desarrollo Organizacional y la Vicepresidencia de Negocios. En un principio la red inalámbrica se pensó para habilitar salas de reuniones en todos los lugares indicados, en donde los usuarios seleccionados, usualmente los Vicepresidentes y Gerentes, pueden reunirse y compartir información a través de la red, sin necesidad de aumentar puntos de red en dichas salas, lo que brinda una mayor flexibilidad y adaptabilidad de la red a las necesidades de los usuarios, ya que éstos con su misma laptop pueden laborar en sus oficinas y luego reunirse en otra, sin desconectarse de la red, y sin la necesidad de instalar nuevos puntos de red en las salas de reuniones.

Lo anteriormente expuesto propende a ahorros en infraestructura física, ya que no se instalan nuevos puntos ni se tienen conectados éstos a puertos de switches, lo que representa un ahorro en equipos. Además, aparte de las salas de reuniones temporales, se puede brindar acceso a la red a ciertos usuarios que debido a sus actividades cotidianas necesitan moverse constantemente, pero al mismo tiempo necesitan acceder a la red desde cualquier lugar, como es el caso del personal de soporte informático. Un tercer grupo de clientes son aquellos que debido a trabajos emergentes de obras civiles necesitan moverse a otro lugar donde no existe cableado estructurado, y sería muy oneroso realizar una instalación debido al tiempo que permanecerán alejados de sus oficinas. Por último, y aunque menos probable, es el acceso de clientes que de otra forma no pudieran hacerlo debido a la imposibilidad de instalar cableado estructurado en sus dependencias.

Este capítulo es el complemento al proyecto de red inalámbrica ejecutado por el departamento de redes, dentro del cual no se contempló el diseño de las celdas de cobertura, de la reutilización de canales, ni de la colocación de los equipos activos. Para llevar a cabo este proyecto, se cuenta con una solución de Cisco, la cual incluye access points, antenas y tarjetas inalámbricas, compatibles con la norma 802.11b.

Las características técnicas de los equipos se resumen en las tablas 5.2 para el caso de los access points y 5.3 para el caso de los clientes inalámbricos.

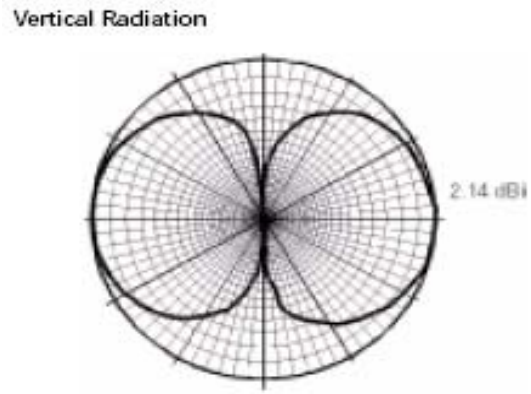
ACCESS POINT	
Marca:	Cisco
Modelo:	Aironet 1200 Series
Potencia de Salida:	100, 50, 30, 20, 5 o 1 mW
Frecuencia:	2.400 a 2.497 GHz
Rango:	Interiores: 45 m (150 ft) a 11 Mbps 106 m (450 ft) a 1 Mbps
	Exteriores: 243 m (800 ft) a 11 Mbps 609 m (2000 ft) a 1 Mbps
Modulación:	Espectro Ensanchado de Secuencia Directa Direct Sequence Spread Spectrum (DSSS)
Tasas de Transmisión:	1, 2, 5.5 y 11 Mbps
ANTENAS	
Modelo:	AIR-ANT4941
Tipo:	Dipolo
Ganancia:	2.2 dBi
Aplicación:	Cobertura omnidireccional para interiores.
VSWR	Menor que 2:1
Haz de Media Potencia:	360 H 65 V 

Tabla 5.2. Características de los Access Points

CLIENT ADAPTERS	
Marca:	Cisco
Modelo:	Aironet 350 Series
Potencia de Salida:	100, 50, 30, 20, 5 o 1 mW
Frecuencia:	2.400 a 2.497 GHz
Rango:	Interiores: 45 m (150 ft) a 11 Mbps 106 m (450 ft) a 1 Mbps
	Exteriores: 243 m (800 ft) a 11 Mbps 609 m (2000 ft) a 1 Mbps
Modulación:	Espectro Ensanchado de Secuencia Directa Direct Sequence Spread Spectrum (DSSS)
Tasas de Transmisión:	1, 2, 5.5 y 11 Mbps
Protocolo de Acceso al Medio:	Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA -
Sensibilidad:	1 Mbps: - 94 dBm 2 Mbps: - 91 dBm 5.5 Mbps: - 89 dBm 11 Mbps: - 85 dBm
Delay:	1 Mbps: 500 ns 2 Mbps: 400 ns 5.5 Mbps: 300 ns 11 Mbps: 140 ns

Tabla 5.3. Características de los Clientes

Con dicha solución, se establecen los siguientes criterios de diseño que se deben satisfacer para la implementación de la red:

- Cobertura total en el primer, segundo, tercer y cuarto piso del edificio de Informática.
- Cobertura en la oficina del Presidente Ejecutivo, y Secretaría General del Edificio Estudio Z
- Cobertura en la oficina del Vicepresidente de Operaciones
- Cobertura en la oficina del Vicepresidente de Desarrollo Organizacional y Gerencia de Comunicación e Imagen Corporativa, en el Edificio El Doral.
- Cobertura en la oficina del Vicepresidente de Negocios, Gerencia de Andinadatos y Gerencia Comercial, en el Edificio El Doral.
- En las zonas de cobertura, la velocidad debe ser la máxima que permitan los equipos.
- El sistema de autorización y autenticación no debe permitir el ingreso de usuarios no autorizados a la red.

- La señal debe ser difícilmente detectable en los exteriores de las dependencias antes mencionadas.
- En los edificios en los que existiere más de un Access Point, las señales de éstos no deben interferirse, pero el roaming debe ser transparente para los usuarios.

Con estas premisas, se analizará la implementación realizada en el edificio de Informática, que presenta la mayor cantidad de Access Points instalados en un solo edificio de Andinatel.

IMPLEMENTACIÓN DE LA RED WIRELESS EN EL EDIFICIO DE INFORMÁTICA

El edificio de Informática es un edificio de seis pisos, de base rectangular de aproximadamente 20 x 24 mts. La altura aproximada de los pisos es de 3.5 mts, de losa a losa, existiendo entre la losa del piso y del techo un techo falso que cuelga a aproximadamente 0.50 mts del techo verdadero. Las paredes exteriores del lado más largo del rectángulo son una combinación de bloque y vidrio, siendo la parte de bloque de aproximadamente 0.50 mts y el resto de vidrio. Las paredes exteriores del lado más corto son de bloque en su totalidad. Las divisiones interiores dentro de cada piso son vidrio, aluminio, madera o paredes delgadas de bloque. La descripción física de la composición del edificio es útil, para realizar un cálculo aproximado de las atenuaciones provocadas por el material, que se presentan en la tabla 5.4.

Obstrucción	Pérdida (dB)
Espacio Libre	0
Vidrio sin polarizar	3
Vidrio polarizado	5 a 8
Pared delgada	5 a 8
Pared de madera	10
Pared ancha	15 a 20
Muro	20 a 25
Piso / tumbado	15 a 20
Piso / tumbado ancho	20 a 25

Tabla 5.4. Atenuación provocada por material

Para cumplir con el requisito de cobertura total dentro del piso, se opta por instalar un access point por piso, en la parte central del mismo, o en la línea del eje central, con las siguientes características de transmisión:

Potencia: 100 mW (20 dB)
Canal: 1 u 11 dependiendo de los access points vecinos.
Antena: 2 antenas dipolo omnidireccionales de 2.2 dBi de ganancia
Potencia Radiada: 22.2 dB

Al tener un access point por piso, se garantiza un uso racional de los recursos, y una potencia y calidad adecuada de la señal que se transmite y recibe, ya que la pérdida total entre el emisor y el receptor, para garantizar la tasa máxima de transmisión de datos debe ubicarse entre los 105 y 107 dB, dado que la sensibilidad para los 11 Mbps es de –85 dB, según la tabla 5.3, proporcionada por el fabricante. Al configurar el canal de transmisión en 1 u 11, se obtiene una separación de 50 Mhz entre las frecuencias centrales de los canales, y una separación efectiva de 28 Mhz entre los canales, lo que garantiza que las señales de las celdas no se interfieran destructivamente entre sí.

El trade-off de configurar los equipos para transmitir a la máxima potencia y garantizar la tasa máxima de transmisión de datos, es que parte de la señal sale de las dependencias de Andinatel y podría ser detectada y utilizada como una vulnerabilidad para que personas no autorizadas intenten ingresar a la red de datos. Como medida preventiva, se configura por medio del software del equipo, que acepte únicamente conexiones de 11 y 5.5 Mbps (-85 y –89 dB de sensibilidad), lo que permite controlar el radio desde el cual se pueden intentar conexiones, y ubicarlas dentro del perímetro de las dependencias de Andinatel.

Definido el radio físico desde el cual se pueden intentar conexiones a la red, el siguiente paso es definir SSID únicos y exclusivos para el uso dentro de Andinatel, y que sean de difícilmente obtenidos por personas a las cuales no se les haya autorizado el acceso a la red por esta vía. El SSID será una cadena de 10 caracteres definidos por la administración de la red, y tendrá el mismo tratamiento de seguridad que una contraseña: cadena alfanumérica, que combine dígitos con caracteres mayúsculos, minúsculos y especiales que

no represente palabra alguna conocida, o que tengan sentido como fechas, o eventos, o que sean fácilmente adivinables.

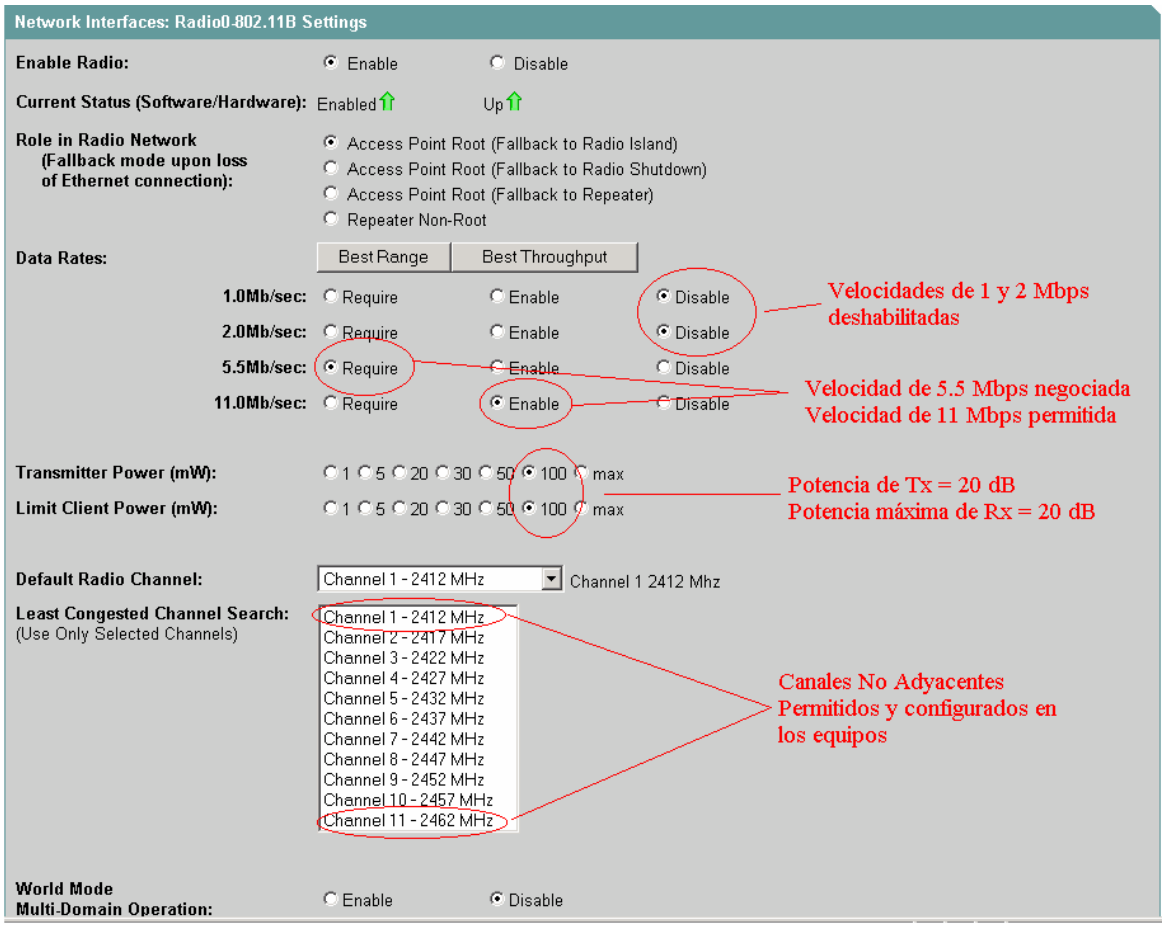


Figura 5.8. Configuración de los parámetros de Transmisión.

El siguiente paso es el método de autenticación. Dentro de la solución Cisco que adquirió Andinatel, existen varios métodos de autenticación, tales como sistema abierto, llave compartida y una implementación propia de Cisco de EAP, llamada LEAP (Lightweight Extensible Authentication Protocol), que provee seguridad durante el intercambio de credenciales, cifrado de datos mediante llaves WEP generadas dinámicamente y soporta autenticación mutua.

Debido a la mayor grado de seguridad que ofrece, se escoge la autenticación LEAP, con el uso del nombre de usuario y contraseña que el usuario utiliza para ingresar a la red corporativa de datos. Con ello, el proceso de ingresar a la red de datos, por medio de la red

inalámbrica se simplifica para los usuarios, ya que deben ingresar como habitualmente lo realizaban.

Además LEAP permite un control más estricto sobre quiénes pueden acceder a la red de datos, ya que además del nombre de usuario y contraseña correctas, se necesita privilegios de usuario remoto en el servidor de dominio para poder ingresar a la red. Con ello se permite que únicamente los usuarios seleccionados puedan ingresar a la red por este medio, y al mismo tiempo se evita que personas que pudiesen tener acceso a las máquinas a las cuales se les instaló la tarjeta inalámbrica puedan ingresar a la red, aún cuando pertenezcan a la organización y tengan un nombre de usuario y contraseña válidas para el acceso a la red.

Con el cumplimiento de los puntos expuestos en los párrafos anteriores se ha logrado que el acceso inalámbrico sea una solución factible en todas las áreas en las que se ha implementado esta solución. En las áreas que no pertenecen al edificio de Informática la implementación sigue las mismas guías en cuanto a ubicación y características de transmisión de los access points. Ahora en todas las áreas mencionadas en los criterios de diseño existe una sala de reuniones virtual, ya que todos los access points comparten los mismos SSID, lo que permite que los usuarios se puedan conectar a la red corporativa de datos desde cualquier área en la que existe cobertura, sin contratiempos, y con toda la flexibilidad y confiabilidad que permite este sistema.

En cuanto a la seguridad, si bien han existido y existirán intentos de usuarios por ingresar a la red por este medio, el sistema de seguridad siempre los ha rechazado de forma exitosa, mostrando la fortaleza de este modelo de seguridad, que únicamente permite el ingreso de usuarios que estén dentro de la infraestructura de Andinatel, que conozcan un SSID válido, que tengan un nombre de usuario y contraseña válida para ingresar a la red corporativa de datos y que además tengan privilegios dentro del servidor de dominio.

El próximo paso es aumentar el número de usuarios inalámbricos, que en la actualidad es de 12 personas, entre Vicepresidentes, Gerentes, Responsables y usuarios seleccionados, para aprovechar la infraestructura actualmente instalada. Los próximos

usuarios inalámbricos serían los ingenieros de soporte informático, que debido a su actividad deben moverse continuamente dentro de la infraestructura de Andinatel. En la etapa final, la cobertura inalámbrica debería extenderse a todos los edificios de Andinatel, pero con tecnología 802.1g, que permita mejores velocidades de acceso, además de compatibilidad con la red inalámbrica ya instalada.

CAPITULO VI

SEGMENTACIÓN DE LA RED MAN

Se proporciona la siguiente información:

- Segmentación de red.
- Arquitecturas de Red.
- Descripción de conmutación a nivel de la capa 2 y de la capa 3 del modelo de referencia OSI.
- Descripción de funcionamiento de VLANS.
- Priorización de tráfico.
- Protocolos de Enrutamiento
- Protocolos de Clase y No Clase
- Diseño de Red

SEGMENTACIÓN DE RED

En la actualidad, la LAN esta cada vez más congestionada y sobrecargada, debido a una población de usuarios de red en constante crecimiento, los mismos que se conectan y demandan mayores recursos de red, especialmente de las aplicaciones cliente / servidor. La actual topología es plana, implementada mayoritariamente con switches, tal como se vio en el capítulo II: Situación Actual de la red MAN, por lo que únicamente existe un dominio de broadcast para casi toda la red MAN, lo que afecta el desempeño no solo de la red, sino de los hosts conectados a ella, ya que deben procesar ingentes cantidades de paquetes que no le son útiles.

En la actual condición de la red, el ruido normal de fondo se ubica entre los 100 y 130 paquetes por segundo, con un valor más estable en los 120 paquetes por segundo. Según Cisco, en su Internetworking Design Guide, el porcentaje de pérdida de procesamiento del CPU de un host, es del orden del 0.96% por cada 1000 hosts en un mismo dominio de broadcast. Aunque el valor parece insignificante, durante tormentas de broadcast, este valor puede superar varias veces el promedio y paralizar al equipo. En segmentos de red con menos de 100 hosts, el el porcentaje de pérdida de procesamiento del CPU de un host disminuye al 0.14%.

Con la segmentación de la red, se lograrán los siguientes beneficios: a) incremento del ancho de banda disponible por cada usuario, al disminuir el ruido de fondo que recibe cada host, lo que a su vez disminuirá el porcentaje de pérdida de procesamiento del CPU; b) el uso de VLANs para agrupar a los usuarios en grupos de trabajo lógicos, independientes de su localización física, lo que permitirá mejorar la seguridad dentro de la red y establecer prioridades de tráfico; y c) preparar la red para aplicaciones multimedia futuras, tales como videoconferencia, video bajo demanda, video en tiempo real y voz sobre IP (VoIP), en las que se necesita establecer niveles de calidad de servicio.

ARQUITECTURAS DE RED

A medida que las intranets corporativas evolucionan, los administradores de red encuentran una gran cantidad de opciones para construir y modificar sus redes. El diseño tradicional de las redes ha sido una LAN única a la cual se le agregan nuevos usuarios simplemente conectándolos en cualquier parte de la misma, tal como es el caso de la red actual de Andinatel. Con esta arquitectura, muy pocas consideraciones de diseño se necesitan para proveer acceso al usuario hacia el backbone de la red. De hecho, los usuarios físicamente adyacentes se conectan al mismo dispositivo de acceso para minimizar el número de enlaces hacia el backbone.

Los mayores problemas con la arquitectura tradicional son la disponibilidad y el rendimiento, problemas relacionados con el ancho de banda disponible. En un dominio de colisión único, las tramas son visibles para todos los dispositivos de la LAN y colisionan libremente. Los dispositivos multipuerto de Capa 2, como los switches, segmentan a la

LAN en dominios de colisión discretos y transmiten tramas de Capa 2 hacia el segmento de red que contiene la dirección de destino.

Sin embargo, las tramas que contienen la dirección MAC de broadcast inundan la red, por lo que una sola máquina puede inundar toda la red con “ruido” e inutilizarla. Este tipo de ataques pueden ser premeditados o intencionales, pero en ambos casos, es un grave problema. Para evitar esto, se utilizan dispositivos de Capa 3, ya que son capaces de hacer decisiones inteligentes tomando en cuenta el flujo de datos hacia un segmento de red. El tráfico que afecta el rendimiento de la red es aquel que interroga a la red acerca del estado de un componente o de sus disponibilidad y avisa el estado de un componente o su disponibilidad.

Los tipos comunes de broadcast que interrogan a la red son las peticiones del Protocolo de Resolución de Direcciones IP (ARP) y las peticiones de nombre NetBIOS. Estos broadcast se propagan a través de la subred entera y esperan que el dispositivo objetivo responda directamente a la petición. Este tráfico no puede ser eliminado del todo, por cuanto servicios de red, tal como el servicio de impresión, depende de este tipo de broadcast. Adicionalmente, el tráfico de multicast consume una gran cantidad del ancho de banda disponible. Este tráfico se propaga a un grupo específico de usuarios. Dependiendo del número de usuarios en un grupo multicast o del tipo de datos de aplicación encapsulados en el paquete multicast, este tipo de broadcast puede consumir la mayoría de los recursos de red. De hecho, un solo servidor de multicast, dentro de una red no preparada para multicast, puede congestionar todos los enlaces.

Existen dos métodos para manejar el problema de broadcast en grandes redes LAN conmutadas (switched LANs). El primero es usar ruteadores para crear subredes y segmentar lógicamente el tráfico, ya que el broadcast no pasan a través de los ruteadores. Aunque este modelo contiene el tráfico de broadcast, el CPU de un ruteador tradicional debe procesar cada paquete, lo que puede provocar un cuello de botella en la red. La segunda opción es implementar VLANs dentro de la red. El beneficio principal de los switches con VLANs es que contienen de forma efectiva el tráfico de broadcast.

Reglas para el Tráfico de Red

De forma ideal, los usuarios finales con intereses o patrones de trabajo comunes se colocan en la misma red lógica, al igual que los servidores a los que acceden. La mayor parte del tráfico dentro de esta red lógica se mantiene dentro del segmento local, lo que minimiza la carga en el backbone de la red. La regla del 80/20 indica que el 80 % del tráfico de un segmento de red debe ser local, y no más del 20% debe atravesar el backbone de la red. Esta fue la premisa bajo la cual se implemento la actual red de datos.

Debido a la evolución de las redes, los patrones de tráfico se modifican, hasta llegar a un nuevo modelo, en el cual solo el 20% del tráfico es local en el segmento de red, mientras que el 80% restante abandona la red local. Los factores que contribuyen a este cambio en el patrón de tráfico son:

Internet. Con las aplicaciones web, las PCs se utilizan para publicar y acceder información, por lo que ésta puede provenir de cualquier parte de la red, creando ingentes cantidades de tráfico que atraviesa los límites de las subredes. En la actualidad, por citar un ejemplo, la gestión de las centrales telefónicas de toda la región de Andinatel, se la realiza a través de servidores instalados en Quito, que generan más tráfico hacia fuera de la red que en la misma red.

Servicios Centralizados. La centralización de servidores se debe a medidas de seguridad, facilidad de manejo y costos reducidos de mantenimiento. Todo el tráfico desde las redes de los clientes hacia estos servidores debe atravesar a través del backbone. Todos los clientes de acceden al mismo servidor de correo, de formas, DNS, DHCP, etcétera, sin embargo el rendimiento de los mismos se ve afectado por la cantidad de paquetes innecesarios que deben procesar.

Sin embargo, el cambio en los patrones de tráfico necesita que el rendimiento de los dispositivos de Capa 3 se aproxime al de los dispositivos de Capa 2. Debido a que el enrutamiento es un proceso que hace uso intensivo del CPU, éste puede crear cuellos de botella dentro de la red.

REQUISITOS BÁSICOS DE LA ARQUITECTURA DE RED

Convergencia Rápida. La red debe adaptarse rápidamente a los cambios en la topología de red, tales como enlaces que fallan o inserción de nuevos dispositivos o extracción de dispositivos existentes. En ello juega un papel importante la implementación del protocolo de enrutamiento y la implementación del Spanning Tree Protocol.

Redundancia. Debe existir un mecanismo, tal como enlaces, dispositivos o módulos redundantes que garanticen que la red opere todo el tiempo, para todos los usuarios.

Escalabilidad. La infraestructura de la red debe adaptarse al crecimiento de la red y la adición de nuevas aplicaciones, así como del incremento de tráfico y de usuarios.

Aplicaciones Centralizadas. Están disponibles para la mayoría, o para todos los usuarios de la red, por lo que hay que considerar la *regla del 20/80*, la cual se enfoca en el cambio de los patrones de tráfico.

Multicasting. Este requisito apunta a que las redes deben soportar tráfico multicast además del tráfico unicast.

CONMUTACIÓN DE CAPA 2 Y CAPA 3

Existen dos métodos de conmutación de tramas de datos: la conmutación a nivel de Capa 2 y la de Capa 3. La conmutación es el proceso de tomar una trama que llega de una interfaz y enviar a través de otra interfaz. Los routers utilizan la conmutación de Capa 3 para enrutar un paquete; los switches (switches de Capa 2) utilizan la conmutación de Capa 2 para enviar tramas.

La diferencia entre la conmutación de Capa 2 y Capa 3 es el tipo de información que se encuentra dentro de la trama y que se utiliza para determinar la interfaz de salida correcta. Con la conmutación de Capa 2, las tramas se conmutan tomando como base la información

de la dirección MAC; con la conmutación de Capa 3, las tramas se conmutan tomando como base la información de la capa de red.

La conmutación de Capa 3 opera a nivel de la capa de red. Examina la información del paquete y los envía tomando como base las direcciones destino de la capa de red. Si los usuarios cambian sus posiciones físicas, sus estaciones finales obtienen nuevas direcciones de Capa 3, pero sus direcciones de Capa 2 permanecen iguales.

Como los routers operan a nivel de Capa 3 del modelo de referencia OSI, pueden adoptar y crear una estructura de direccionamiento jerárquico. El flujo de tráfico en una red conmutada (plana) es por lo tanto inherentemente diferente del flujo de tráfico en una red enrutada (jerárquica). Las redes jerárquicas permiten un flujo de tráfico más flexible que las redes planas ya que pueden usar la jerarquía de red para determinar las rutas óptimas y contener los dominios de broadcast. Es por ello que el diseño de la red propenderá a una estructura jerárquica, para limitar el número de usuarios a máximo 128 por subred, y con restricciones de los servicios y redes a los cuales puede acceder, pero con garantía en la calidad de servicio ofrecida por la red.

REDES VIRTUALES DE AREA LOCAL

Una red virtual de área local (VLAN por sus siglas en inglés), consiste de varios sistemas terminales, ya sean hosts o equipos de red, todos los cuales son miembros de un mismo dominio lógico de broadcast, a diferencia del dominio de broadcast físico. El soporte para VLANs está presente en varios equipos de red, que soportan protocolos de troncalización de VLANs.

Las VLAN se utilizan para agrupar a un conjunto de usuarios relacionados, sin importar su conectividad física. Los usuarios que pertenecen a una VLAN son del mismo departamento o desempeñan las mismas funciones, o porque su patrón de flujo de datos hace pensar en agruparlos. La configuración de la VLAN se la realiza en el switch a través de software propietario del fabricante, ya que las VLAN no están estandarizadas.

En la figura 6.1 se muestra la topología típica de VLAN, donde los usuarios se agrupan por departamentos, o grupos lógicos, sin importar su localización física.

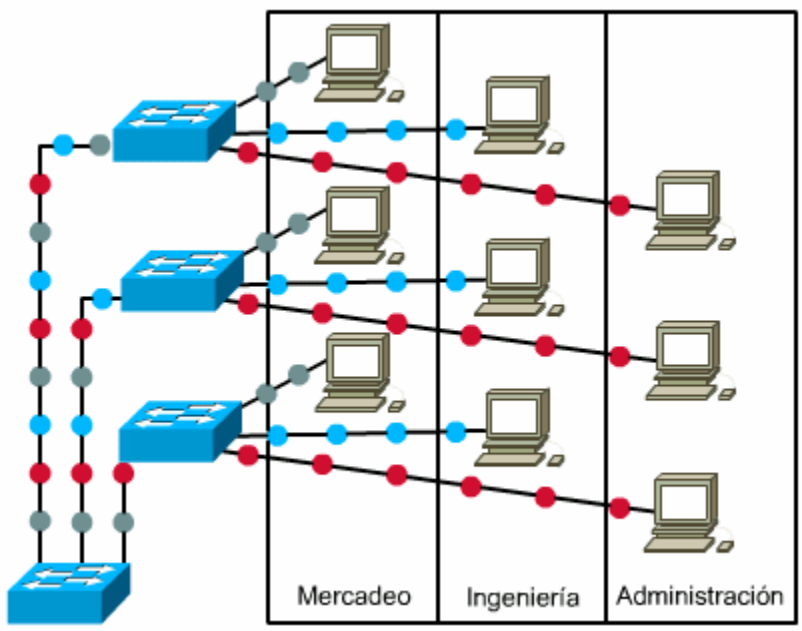


Figura. 6.1. Topología típica de VLAN

Beneficios de las VLAN

Las VLANs ofrecen las siguientes características:

Control de Broadcast. Una VLAN es un dominio de broadcast y todo tráfico de broadcast o multicast se mantiene dentro de la VLAN, ofreciendo un completo aislamiento entre VLANs. En cada dominio de broadcast se incluirá como máximo a 128 usuarios.

Seguridad. Los usuarios que necesiten alta seguridad pueden agruparse en una VLAN, y a ningún otro usuario fuera de la VLAN puede permitírsele la comunicación. La comunicación entre VLANs se logra a través de un dispositivo de capa 3, lo que permite realizar funciones de seguridad y filtrado. Esta seguridad se implementará en las redes de los Centros de Operación, Mantenimiento y Gestión de las Centrales Telefónicas, que por la naturaleza de la información que manejan, debe ser tratada con mucho cuidado.

Desempeño. El agrupamiento lógico de usuarios permite crear redes de usos específicos, adecuados a las necesidades de cada grupo de usuarios, mejorando así, el desempeño de la red, y de los hosts conectados a la misma.

Manejo de red. El agrupamiento lógico de usuarios, sin importar su localización física, permite facilitar la administración de la red, ya que los cambios, mudanzas y la inclusión de nuevos usuarios se logran a través de la configuración de un puerto en la VLAN apropiada.

Implementación de VLANs

Las VLANs que se implementen, se las definirá p*or Puerto*. Cada puerto de cada uno de los switches de la red de datos de Andinatel soportará una y solo una VLAN. Todo el tráfico dentro de la VLAN es conmutado, y el tráfico entre VLANs es ruteado. Este tipo de VLAN también se conoce como VLAN basada en segmento. Esta definición de VLANs se prefiere sobre la De Protocolo o Por Usuario debido a su simplicidad de configuración y que se obtiene un mayor control sobre los usuarios.

PRIORIZACIÓN DE TRÁFICO

Definidas las VLANs que se utilizarán dentro de cada edificio de la organización, es conveniente que el tráfico generado por las mismas sea manejado de forma distinta, para priorizar el tráfico generado por diferentes segmentos de red. La mayoría de equipos con los que se cuenta en la actualidad (80% de la plataforma instalada), pueden configurarse para ofrecer calidad de servicio (QoS por sus siglas en inglés) a partir del estándar IEEE 802.1p Class of Service (CoS). QoS utiliza la clasificación y programación para transmitir tráfico de red de una forma predecible. QoS clasifica las tramas asignándoles valores indexados de prioridad CoS y da preferencia a tráfico de mayor prioridad tal como las llamadas telefónicas. De forma general, cada puerto confiará en el valor de CoS que reciba de los equipos, y a las tramas que no contengan un valor de CoS, se les asignará uno dependiendo de la función del personal agrupado en dicha VLAN.

PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento son reglas que gobiernan el intercambio de información de enrutamiento entre routers. La arquitectura abierta y popularidad de TCP/IP ha impulsado el desarrollo de varios protocolos de enrutamiento de IP, cada uno de los cuales tiene sus fortalezas y debilidades, en aspectos relacionados con el tiempo de convergencia, el overhead dentro de la red, y las características de escalabilidad.

Un router aprende las rutas configuradas estáticamente por un administrador, o las aprende de forma dinámica a través de otros routers, por medio de protocolos de enrutamiento. Los routers arman una tabla de enrutamiento, que utilizan para la tomar las decisiones de cómo transmitir los paquetes. Las principales ventajas y desventajas del enrutamiento estático y dinámico se muestran en la tabla 6.1.

Enrutamiento	Ventajas	Desventajas
Estático	Poco uso del procesador. Se necesita routers con menos memoria y capacidad de procesador.	Alto mantenimiento. Se debe configurar todas las rutas manualmente.
	No se gasta ancho de banda en mantener actualizadas las tablas de enrutamiento.	No es adaptable a los cambios en los estados de los enlaces.
	Predictabilidad. Se conoce exactamente por donde se enviaran los paquetes.	
Dinámico	Alta adaptabilidad a los cambios en el estado de los enlaces y de la topología de la red.	Alto uso del procesador y de la memoria del router.
	Bajo mantemiento. La configuración se limita al protocolo de enrutamiento.	Utilización de ancho de banda para mantener las tablas de enrutamiento actualizadas.
	Los routers avisan sobre el estado de los enlaces, o sobre el cambio de topologías.	

Tabla 6.1. Características del enrutamiento estático y dinámico

Los protocolos de enrutamiento pueden clasificarse como vector-distancia o estado-enlace, dependiendo del algoritmo utilizado para calcular e intercambiar la información de enrutamiento.

Protocolos de Enrutamiento de Vector Distancia

Los routers que utilizan este tipo de protocolos de enrutamiento envían su tabla completa de enrutamiento a intervalos regulares, por todas sus interfaces, a no ser que se les indique lo contrario. Las ventajas de los protocolos vector-distancia son su facilidad de configuración en los equipos, y la menor necesidad de procesamiento y memoria presentes en los equipos, además de que la mayoría de los equipos lo soporta. Las desventajas son su poca escalabilidad, ya que no soportan VLSM (Variable Length Subnet Masking) o supernetting, y su lentitud para converger en comparación con los protocolos de vector-distancia.

Protocolos De Enrutamiento De Estado Enlace

Ofrecen una mayor escalabilidad y menores tiempos de convergencia con el costo de un mayor poder de procesamiento y memoria en los equipos. Su funcionamiento se base en el estado de las interfaces de enlace hacia los otros routers de la red. Se construye una base de datos completa de todos los enlaces dentro de la red, desde la perspectiva de cada router, identificando los mejores caminos hacia las otras redes, los cuales se instalan en la tabla de enrutamiento. Las actualizaciones de las tablas de enrutamiento ocurren al existir un cambio en el estado de un enlace, en cuyo caso se envía inmediatamente una actualización parcial, o si no ha existido ningún cambio durante un intervalo específico de tiempo. Además soportan características como CIDR (Classless Inter Domain Routing), VLSM (Variable Length Subnet Masking) y subnetting, lo que los convierte en la mejor solución para escalar redes complejas.

PROTOCOLOS DE ENRUTAMIENTO DE CLASE Y NO CLASE

En una red de subredes de máscaras variables, los routers deben propagar en sus actualizaciones las máscaras de red, ya que sin ellas, el equipo únicamente tendría las direcciones recibidas a través de las actualizaciones y la máscara de red de las interfaces conectadas directamente, para decidir la ruta que tomará el paquete. Solo los protocolos de enrutamiento que ignoren las reglas del direccionamiento de clase (classfull) y utilicen prefijos de no clase (classless) funcionan apropiadamente con CIDR y VLSM.

Entre los protocolos de enrutamiento de clase (classfull) se encuentran el RIPv1 (Routing Information Protocol versión 1), y el IGRP (Interior Gateway Routing Protocol). En cuanto a los protocolos de no clase (classless) se pueden nombrar a la versión 2 de RIP, al protocolo propietario de Cisco EIGRP (Enhanced Interior Gateway Routing Protocol), a OSPF (Open Shortest Path First), protocolo de estado enlace basado en estándares abiertos y a IS-IS (Intermediate System to Intermediate System), protocolo de estado enlace de amplio uso en los ISPs.

DISEÑO DE RED

Como se explicó en el Capítulo II Situación Actual de la Red, la topología lógica de la red es plana, lo que significa que no existe ningún tipo de jerarquía dentro de la misma. Con la convergencia de servicios dentro de la red, tales como voz, video en tiempo real, video bajo demanda, y los datos, el diseño de la red debe ser lo suficientemente flexible para adaptarse y soportar estos nuevos servicios que demandan los usuarios. Es por ello que el diseño de la red debe ser jerárquico, para diferenciar equipos que demandan servicios de los que los ofrecen, y además manejar de forma óptima los patrones de tráfico que se generen con la convergencia de servicios.

El diseño jerárquico de la red incluye tres capas: acceso, distribución y núcleo. La *Capa de Acceso* es el punto en el cual los usuarios finales se conectan a la red. Utiliza listas de control de acceso (ACLs) para optimizar las necesidades de cada grupo de usuarios. Sus funciones son compartir el ancho de banda, filtrar el tráfico de Capa 2, y la microsegmentación de la red.

La *Capa de Distribución* divide la capa de acceso del núcleo, a la vez que define límites y es el donde ocurre la manipulación de paquetes. Sus funciones son la agregación de direcciones o áreas, la definición de dominios de broadcast, el enrutamiento entre VLANs, y seguridad. En resumen, esta capa proporciona conectividad basada en políticas.

La *Capa de Núcleo*, debe ser un backbone de alta velocidad y debe diseñarse para conmutar los paquetes tan rápido como sea posible. No debe realizar ninguna

manipulación de paquetes, tal como filtrado con listas de control de acceso, ya que disminuiría la velocidad de conmutación de los paquetes. Se prefiere que sea un ambiente de conmutación exclusivamente de Capa 3.

Con estas consideraciones, ahora la propuesta de rediseño de la red interna de datos seguirá la siguiente secuencia: diseño del Núcleo, esquema de direccionamiento, protocolo de enrutamiento en el núcleo, diseño de la capa de Distribución, políticas de conectividad en la capa de distribución, diseño de la capa de acceso, políticas de acceso, seguridad básica en la red y priorización del tráfico.

Diseño del Núcleo

Es común pensar que las tres capas: acceso, distribución y núcleo, deben diferenciarse claramente y existir en diferentes dispositivos físicos, sin embargo este no es el caso. La forma en que se implementan las capas depende de las necesidades de la red, pero hay que recordar que para que la red funcione adecuadamente, y se adapte a los cambios futuros, ésta debe ser jerárquica. El proyecto “Ampliación del Backbone de Fibra Óptica” del departamento de redes de Andinatel, contempla la adquisición de tres switches de capa 3, que junto a los dos switches que ya posee, conformarían el backbone de la red. La propuesta de la ubicación y reubicación de los switches es la mostrada en la figura 6.2.

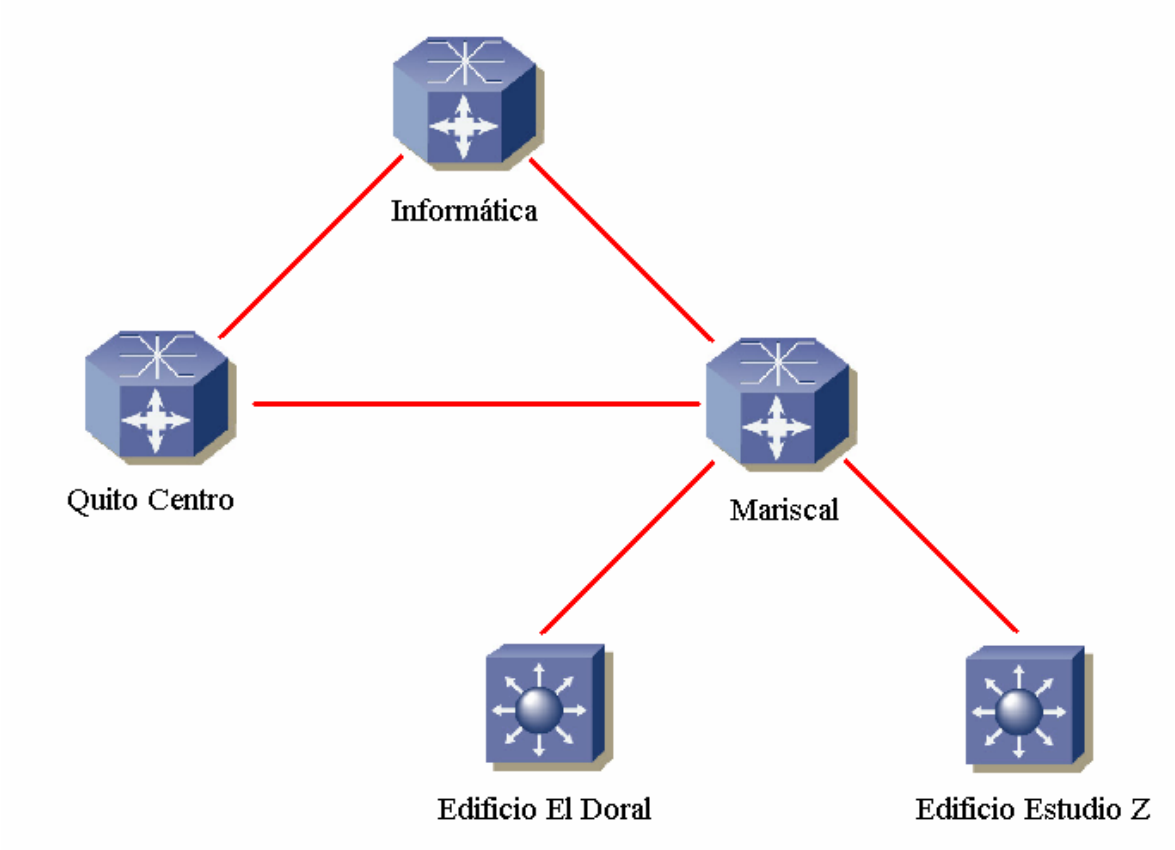


Figura 6.2. Propuesta de Ubicación de Switches de Capa 3

En la actualidad, los switches de capa 3 se ubican en el edificio de Informática y El Doral, pero no están configurados para que sus enlaces sean de capa 3. En esta propuesta, todos los enlaces son de capa 3, con velocidad de 1000 Mbps (1 Gbps). Se propone utilizar la fibra instalada entre Quito Centro y Mariscal, que en la actualidad no esta utilizada, para dar redundancia a parte del núcleo, así como hacer balanceo de cargas. En el Edificio El Doral y Estudio Z se ubican los otros switches de capa 3 debido a la cantidad representativa de usuarios en cada edificio. En el Doral el número de usuarios supera los 450 y en el Estudio Z los 180.

Esquema de Direccionamiento

Se mantendrá la actual dirección de clase B, sin embargo, por medio de VLSM se la partirá en subredes más pequeñas. Específicamente, la actual dirección de clase B se segmentará en 256 redes de clase C, que se repartirán de la manera indicada en la tabla 6.2.

Edificio	Redes Clase C	Redes Enlaces	Edificios Atendidos	Dirección Inicio	Dirección Final	Dirección Sumarizada
Mariscal	32	1	Mariscal	172.xx.0.0	172.xx.31.0	172.xx.0.0 / 19
			Bco. del Pacífico			
			Droira			
Estudio Z	32	0	Estudio Z	172.xx.32.0	172.xx.63.0	172.xx.32.0 / 19
El Doral	64	0	El Doral	172.xx.64.0	172.xx.127.0	172.xx.64.0 / 18
Informática	64	0	Informática	172.xx.128.0	172.xx.191.0	172.xx.128.0 / 18
			Carcelén			
			Cotocollao			
			El Pintado			
			Iñaquito			
			La Luz			
			San Rafael			
			Sangolquí			
			Tumbaco			
			Villaflora			
Quito Centro	32	0	Quito Centro	172.xx.192.0	172.xx.223.0	172.xx.192.0 / 19
Reserva	32	0		172.xx.224.0	172.xx.255.0	172.xx.224.0 / 19

Tabla 6.2. Plan de direccionamiento

Se debe notar que cada bloque de direcciones es una potencia de 2, lo que facilitará la sumarización de las rutas. Se deja un bloque de direcciones como reserva para futuras ampliaciones de la red.

Protocolo de Enrutamiento

Para simplificar las tareas administrativas, se opta por un protocolo de enrutamiento para que actualice dinámicamente los cambios que surgen en la red. Este protocolo debe soportar CDIR y VLSM, su convergencia debe ser rápida y debe ser escalable. Bajo estas características, no es apropiado ningún protocolo de vector distancia, por lo que las opciones se reducen a los protocolos de estado enlace EIGRP, propietario de Cisco, que técnicamente es un protocolo híbrido, y OSPF e IS-IS, que son protocolos abiertos, es decir, definidos en estándares públicos.

Debido a su característica de trabajar con áreas, lo que lo convierte en un protocolo altamente escalable, se prefiere OSPF, para ser configurado como multiárea.

Open Shortest Path First

La escalabilidad de OSPF radica en su diseño jerárquico y el uso de áreas. Al definir áreas en una red diseñada correctamente, se puede reducir el número de actualizaciones necesarias para la convergencia, lo que mejora el desempeño de la red. OSPF, en comparación con los protocolos de estado enlace mejora la velocidad de convergencia, al no transmitir la tabla completa de enrutamiento, sino únicamente los cambios ocurridos, lo que además reduce el uso del ancho de banda de los enlaces; soporta VLSM, lo que permite un manejo más flexible del direccionamiento y de la sumarización de rutas; se adapta fácilmente a redes bastante amplias, ya que selecciona la mejor ruta en base al ancho de banda disponible en los enlaces, lo que optimiza la transmisión de paquetes; y segmenta la red al crear grupos de routers dentro de la red.

Para que los routers puedan intercambiar la información de enrutamiento, es necesario que establezcan relaciones de adyacencia, las cuales dependen del tipo de red dentro de la cual estén los routers. Los tipos de red pueden ser Acceso Múltiple por broadcast, tal como el caso de ethernet; Punto a Punto y Acceso Múltiple sin broadcast como en el caso de Frame Relay o X.25. En el caso del núcleo propuesto, los enlaces son del tipo Punto a Punto, por lo que la formación de adyacencia es con únicamente con su par.

En la figura 6.3 se presenta la propuesta de la implementación de OSPF. Como se observa existen 6 áreas de OSPF. El área 0 es el área de backbone, que es la que conoce todas las rutas existentes dentro de la red. Los switches de capa 3 de Informática y de Quito Centro inyectan en el área 0 la sumarización de sus respectivas áreas, tal como se indicó en la tabla 6.2. El switch de capa 3 de Mariscal inyecta en el área 0 la sumarización de las áreas 2, 3, 4, en cuyo caso la dirección de sumarización sería 172.xx.0.0 / 17. Un beneficio adicional de la sumarización, es la estabilización de las rutas y de las tablas de enrutamiento. Por ejemplo, si una ruta en el área 4 deja de existir, esta información se propaga solo dentro del área 4, y no desencadena ninguna actualización en otra área, ya que la ruta sumarizada publicada por el switch de capa 3 de Mariscal, nunca dejó de existir.

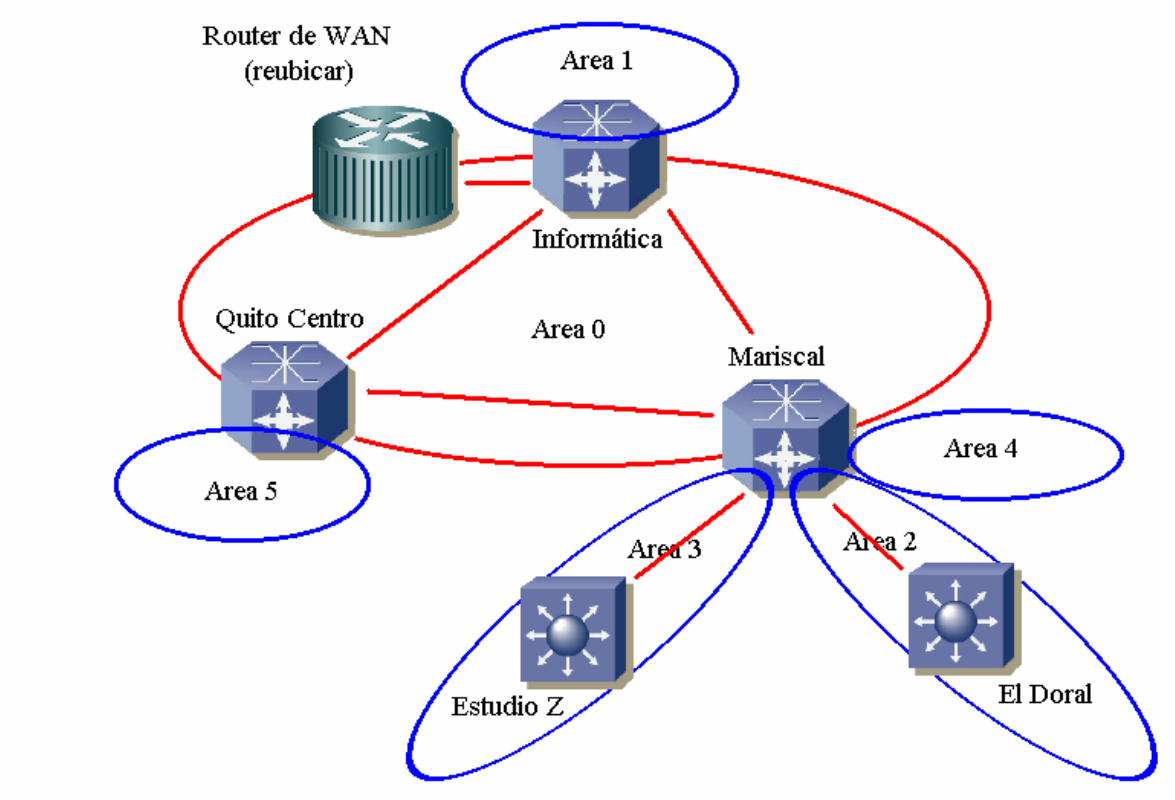


Figura 6.3. Implementación de OSPF

Con esta implementación de OSPF, en el área 0 o de backbone se conocen cuatro redes, en vez de las 256 en las que se dividió la dirección de clase B. Las direcciones son las inyectadas por los switches de capa 3 de Informática, Mariscal y Quito Centro, y la red que se utiliza para los enlaces entre los switches de capa 3. Aparte se conocen las redes inyectadas por el router de WAN, el mismo que debe ser trasladado desde Quito Centro, hacia el edificio de Informática, para centralizar el monitoreo de los enlaces.

En cuanto a la Capa de Distribución, esta se encargará del enrutamiento entre VLANs. Existirán VLANs a las que se restrinja el tráfico, debido a la naturaleza de información o de equipos que contengan. Por ejemplo, se permitirá que solo las VLANs asignadas a los Centros de Operación, Mantenimiento y Gestión de Centrales acceda hacia las centrales, para prevenir ataques contra las mismas. Del mismo modo existen servidores restringidos a cierto de grupo de usuarios, en cuyo caso también hay que filtrar el tráfico. Este filtro de tráfico se lo realizará en todos los switches de capa 3, por medio de Listas de Control de Acceso, en todos los casos necesarios. En este capa es donde se realiza la asignación de subred por VLAN, lo que significa que existirán tantas VLANs como subredes.

Parte de la capa de acceso ya fue configurada, como se explica en el Capítulo IV. Ahora solo resta asignar los puertos de los switches de acceso a las VLANs adecuadas para agrupar de forma lógica a los usuarios, y aumentar los dominios de broadcast dentro de la red de Andinatel. La distribución de VLANs por edificio no puede ser difundida, por políticas de seguridad, pero el modelo de la red reflejará la estructura organizacional de la empresa. Así por ejemplo, si en un edificio coexisten una Vicepresidencia, tres gerencias, y 16 departamentos, existirá una VLAN para la Vicepresidencia, una VLAN para cada una de las Gerencias y los departamentos se tratará de unificar bajo el criterio de similitud de patrones de tráfico, para disminuir el uso de VLANs y acomodar hasta 128 usuarios en la misma VLAN.

En la figura 6.4 se muestra la arquitectura general de red que se desea. Los servidores se separan en tres grupos: acceso público, acceso general y acceso limitado. Con esta diferenciación se tiene mayor control de quién puede acceder a qué recursos de la red. En Acceso Público se colocarán los servidores que pueden ser vistos tanto desde adentro como desde afuera de la red, como el caso de los servidores Web; en Acceso General se concentrarán los servidores a los que todos los miembros de la organización tienen acceso libre, como el caso de los servidores DHCP y DNS, y en acceso limitado se colocarán los servidores hacia los cuales solo ciertos grupos de usuarios pueden acceder, como el caso del servidor de Recursos Humanos. Con esta diferenciación de servicios, lo que se logra es direccionar el tráfico hacia segmentos específicos de la red, disminuyendo el tráfico de broadcast que debe procesar cada servidor, lo que aumentará su eficiencia y disminuirá el tiempo necesario para cada transacción.

Como se observa, las VLANs segmentan de forma lógica la red, al poder agrupar a los usuarios con patrones de tráfico semejantes, y darles privilegios y restricciones comunes para acceder a distintos segmentos lógicos dentro de la red.

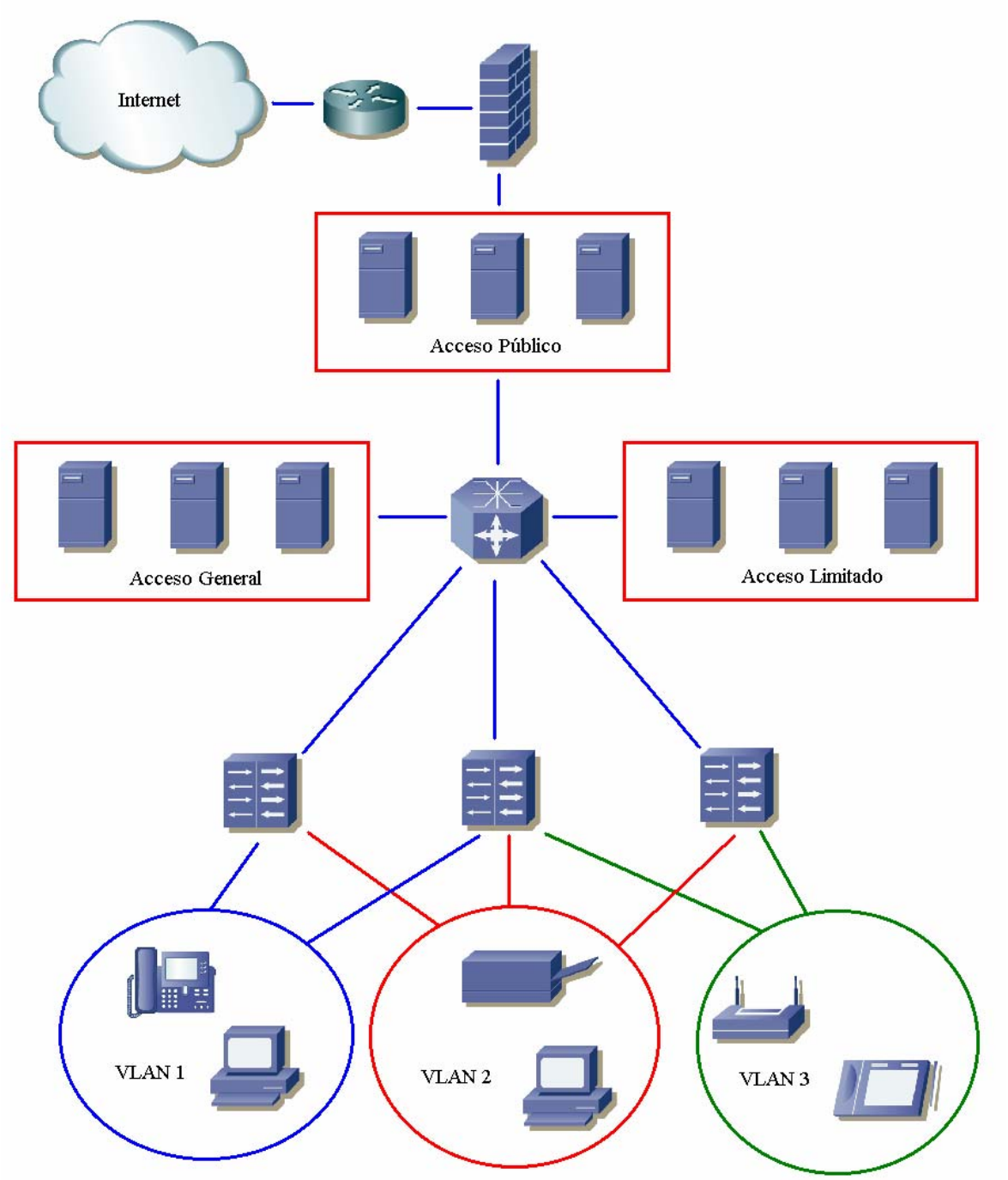


Figura 6.4. Arquitectura General de Red

Con la implementación de VLANs y el filtrado de tráfico en la Capa de Distribución, se ha aumentado la seguridad dentro de la red, al permitir o denegar el acceso a segmentos de la red a grupos de usuarios, lo que con la arquitectura anterior de la red no era posible. Sin embargo, todavía falta solucionar el problema de la adición de nuevos hosts sin la autorización previa. Ya que el sistema operativo de red actual, Windows 2000, no permite

realizar una autenticación de los hosts (con Windows XP Profesional sería posible por medio del protocolo 802.1x), lo que se controlará es que en cada puerto del switch se conecte una sola máquina. Para ello se configura los puertos de cada uno de los switches de la red para que acepten únicamente una dirección MAC y se apaguen en caso de que ingrese más de una por el puerto.

Priorización del Tráfico

Al disminuir notablemente el broadcast que circula en cada segmento de red, y debido a los enlaces de alta velocidad dentro del backbone (1 Gbps), la priorización del tráfico se la realizará a través del estándar 802.1p Class of Service. Al configurar este parámetro este parámetro en las interfaces de los switches, se asigna a la trama un valor de prioridad del 0 al 7, siendo el 0 la menor prioridad y 7 la mayor prioridad. Las tramas etiquetadas con valores del 0 al 3 se envían a la cola de prioridad normal, mientras que las etiquetadas con valores del 4 al 7 se envían a la cola de alta prioridad. Los valores 6 y 7 son reservados para señalización de la red (por ejemplo BPDUs o LSAs). El valor de 5 corresponde a paquetes de VoIP, por lo que el valor más alto asignable es 4. Dentro de la arquitectura general de red mostrada en la figura 6.4, se definieron VLANs en base a patrones de tráfico y servicios de red demandados.

Al asignar cada puerto a una VLAN particular, hay que asignar la prioridad que tendrá el puerto basado en los siguientes criterios: si es una VLAN en la que existan hosts de atención al cliente externo, o sea un puerto de conexión de un Access Point o servidor, la prioridad será de 4 (máxima prioridad asignable); si es un puerto de conexión de hosts que continuamente acceden a aplicaciones ubicadas en servidores, la prioridad será de 4; si es un puerto de conexión de hosts que acceden, pero no de forma constante, a aplicaciones ubicadas en servidores, la prioridad será de 3. Para el resto de casos, la prioridad será de 1.

Con esta configuración se logra que cuando exista congestión en la red, las tramas de mayor prioridad, asociadas a las aplicaciones críticas, salgan primero de la cola y lleguen primero al destino deseado.

CAPITULO VII

CONCLUSIONES Y RECOMENDACIONES

En este trabajo se presenta un diseño basado en tecnologías Gigabit Ethernet y Fast Ethernet para la red MAN de Andinatel S.A. Se realiza un estudio de la situación actual de la red, tanto en su implementación física como lógica, y cómo esta impide un mejor aprovechamiento de los recursos instalados.

La arquitectura de red presentada es la de una red de datos jerárquica, sólida, segura y confiable que garantiza la integridad en el transporte de datos de extremo a extremo, así como la disponibilidad de los servicios de red a todos los usuarios, en base a políticas predefinidas que garantizan la confidencialidad de las comunicaciones y su integridad.

Se explica la solución propuesta, indicando las ventajas e inconvenientes que motivan la elección. Se parte del hecho concreto de la existencia de proyectos para adquirir nuevos equipos y se explica cómo integrarlos a la red, para optimizar el funcionamiento de los ya instalados, mejorando el desempeño general de la red.

Se presentan las políticas de direccionamiento, seguridad y gestión de la red, para las necesidades corporativas actuales. Es importante empezar a proyectar las necesidades de la empresa, para adaptar la arquitectura de red a éstas, y lograr soluciones integrales en el mediano y largo plazo.

Se aprovechan de mejor forma los recursos ya instalados dentro de la infraestructura de red y que antes de iniciar el proyecto se encontraban subutilizados. Al realizar configuraciones avanzadas en los equipos de red, se explota la mayoría de sus recursos, justificando de este modo los gastos de inversión realizados en los mismos.

Se empieza la evaluación de las tecnologías inalámbricas en la capa de acceso de la red. Se debe monitorear y evaluar este proyecto piloto constantemente para introducir mejoras, y sobre todo para ampliar su uso hacia personas que continuamente deben trasladarse entre los edificios de la empresa, como es el caso del personal de asistencia técnica.

Se empieza a diferenciar servicios, y a establecer prioridades de tráfico dentro de la red, en especial de los hosts utilizados para atención al cliente externo. Esta política espera mejorar la productividad de los colaboradores internos y disminuir el tiempo de espera de las transacciones que realizan los clientes externos, mejorando y realzando la imagen corporativa de la empresa.

La propuesta presentada simplifica la integración de nuevos servicios en la red, tales como Voz sobre IP (VoIP), y video en tiempo real y video bajo demanda. Durante la fase de evaluación e implementación de estos servicios, hay que extender los estudios sobre el tráfico multicast y cómo reacciona esta arquitectura de red con este tipo de tráfico. Si es necesario, además de la implementación de 802.1p CoS, se deberá configurar QoS dentro de la red de datos.

Se presenta un modelo de seguridad que previene e impide el acceso de usuarios no autorizados hacia los equipos de red. También se impide que se agreguen nuevos hosts sin las respectivas autorizaciones, sin embargo no existe un monitoreo de las actividades realizadas por cada host. El modelo de gestión de red deja preparado el camino para la integración del software especializado en la gestión de red. Actualmente se están probando varias alternativas de centralización del monitoreo de los equipos de red.

Toda red de datos está expuesta a ataques informáticos que pretendan inutilizarla o paralizarla. También es probable que los equipos sufran averías y pierdan su configuración, por lo que es imprescindible contar con planes de contingencia para paliar esta situación. Como medida preventiva, existe un servidor TFTP en el cual se almacenan todas las configuraciones de los equipos, pero hay que elaborar un plan detallado de contingencias.

Se recomienda impulsar el proyecto de Ampliación del Backbone de Fibra, el cual contempla la adquisición de los switches de capa 3 que serán colocados en el núcleo de la red de datos. Sin esos equipos, la jerarquización de la red sería una tarea imposible de realizarla de forma adecuada.

Se recomienda impulsar el proyecto de implementación del Sistema de Detección de Intrusos (IDS por sus siglas en inglés), el cual aumentará la seguridad de la red al monitorear la actividad dentro de la misma. Este sistema detecta actividades sospechosas y corta dichas comunicaciones antes de que surjan los efectos negativos de un ataque informático.

Se recomienda impulsar el proyecto de la adquisición de un Network Management Station, con el cual se centralizaría el monitoreo de la red. Dicho sistema recogería e interpretaría la información enviada por los equipos de red a través del protocolo SNMP.

Se recomienda estandarizar el sistema operativo de red de todos los hosts hacia uno que soporte el estándar 802.1x para la autenticación. Con ello se puede crear una base de datos de todas las direcciones MAC de los hosts pertenecientes a la red de Andinatel, y permitir el acceso a la red única y exclusivamente a los hosts registrados en esta base de datos. Con ello se logrará una mayor seguridad en el acceso hacia la red.

Todos los beneficios y ventajas de las tecnologías de información no pueden aprovecharse a cabalidad si no se cuenta con el personal técnico calificado para administrar estos recursos, por lo que la capacitación técnica especializada de los recursos humanos encargados del mantenimiento y administración de la infraestructura de red se vuelve indispensable. En este proceso se deben involucrar las empresas y universidades para garantizar la inversión en la infraestructura de telecomunicaciones.

REFERENCIAS BIBLIOGRÁFICAS

BRUNO, Anthony, *CCDA Exam Certification Guide,* Cisco Press, Indianapolis, Indiana, 2002.

GOUGH, Clare, *CCNP BSCI Exam Certification Guide*, Cisco Press, Indianapolis, Indiana, 2002.

ODOM, Wendel, *Cisco CCNA Exam #640-607 Certification Guide*, Cisco Press, Indianapolis, Indiana, 2002.

VARIOS, *Certified Wireless Network Administrator*, Planet3 Wireless Inc, Bremen Georgia, 2002.

VARIOS, *Cisco IOS Desktop Switching Software Configuration Guide*, Cisco Press, San José, California, Abril 2000.

VARIOS, *Internetwork Design Guide*, Cisco Press, Indianapolis, Indiana, 2001.

VARIOS, *Internetworking Terms and Acronym*, Cisco Press, Indianapolis, Indiana, 2001.

VARIOS, *Curriculum CCNA 3: v*ersion 2.13

VARIOS, *Curriculum CCNP 1: Building Scalable Cisco Internetworks*, version 3.0

VARIOS, *Curriculum CCNP 3: Building Cisco Multilayer Switched Networks*, version 3.0

ANEXO 1

MODELO DE REFERENCIA OSI

El modelo de referencia OSI (Open System Interconnection) es un modelo conceptual de siete capas que describe como la información de las aplicaciones de software de un computador se transmite a través de la red hacia otras aplicaciones de software en otra computadora. El modelo fue desarrollado por la ISO en 1984 y se considera como el modelo primario para las comunicaciones entre computadoras.

El modelo OSI divide la tarea de transportar la información entre computadores en siete grupos de tareas más pequeños y manejables, con lo cual se puede implementar cada tarea de forma independiente, lo que ayuda a la actualización de cada tarea sin afectar a las otras.

Las siguientes son las capas del modelo de referencia OSI:

Capa 7. Aplicación. Es la más cercana al usuario y se encarga de identificar los pares para la comunicación, determinar la disponibilidad de recursos y sincronizar la comunicación.

Capa 6. Presentación. Esta capa provee las funciones de codificación y conversión aplicables a los datos entregados por la capa de aplicación. Se incluye los formatos de representación de datos, la conversión de los formatos de representación de caracteres, los esquemas de compresión de datos y los esquemas de cifrado de los datos.

Capa 5. Sesión. La capa de sesión establece, mantiene y cierra las sesiones de comunicación. Una sesión se compone de los servicios de petición y los servicios de respuestas que ocurren entre diferentes dispositivos de una red.

Capa 4. Transporte. Esta capa segmenta los datos recibidos de la capa de sesión para transportarlos a través de la red. Generalmente se encarga de la transmisión libre de errores y en la secuencia apropiada.

Capa 3. Red. Esta capa es la encargada de determinar el mejor camino para el flujo de la información.

Capa 2. Enlace de datos. Esta capa define la topología lógica de la red.

Capa 1. Física. Esta capa define las características eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre los sistemas que se comunican a través de la red.

ANEXO 2

NETWORK TIMING PROTOCOL

La definición completa de la arquitectura, algoritmos y protocolos utilizados, y entidades, se lo encuentra en el RFC 1305. El Network Timing Protocol es un protocolo enrutable (puerto UDP 123) que provee los mecanismos necesarios para sincronizar los relojes internos dentro de un conjunto de servidores y clientes, con una precisión teórica del orden de los nanosegundos, además de proveer una fecha no ambigua, válida hasta mediados de este siglo (XXI).

El protocolo incluye previsiones que especifican las características y estiman el error del reloj local y servidor de tiempo (time server) a los cuales se sincroniza la red. La precisión a la que puede llegar NTP depende fuertemente del hardware del reloj local y del estricto control de la latencia del dispositivo y procesos.

Modos De Operación

Una asociación NTP se forma cuando dos pares intercambian mensajes, y uno, o ambos, crean y mantienen una instancia del proceso del protocolo; excepto cuando se trabaja en el modo de broadcast. La asociación puede operar en cualquiera de los cinco modos de operación: activo simétrico, pasivo simétrico, cliente, servidor y broadcast.

Activo Simétrico. Un host que opere en este modo envía mensajes periódicos, sin importar la disponibilidad de su par, para anunciar que desea sincronizar y sincronizarse con su par.

Pasivo Simétrico. De forma ordinaria, este tipo de asociación se crea al recibir un mensaje de un par que opere en el modo simétrico activo y persiste mientras el par esté

disponible y operativo, de lo contrario, la asociación se disuelve. Sin embargo, la asociación persistirá si al menos se ha enviado un mensaje de respuesta. En este modo, el host anuncia que desea sincronizar y sincronizarse con su par.

Cliente. Un host que opera en este modo, usualmente una estación de trabajo de la LAN, envía mensajes periódicos, sin importar la disponibilidad de su par, para anunciar que quiere que su par lo sincronice.

Servidor. Este tipo de asociación se crea con la llegada de un mensaje de petición de un cliente, y existe solamente para responder a esa petición. Un host que opera en este modo, un servidor de tiempo de la LAN, anuncia que quiere sincronizar a su par.

Broadcast. Este tipo de asociación permite que un host, usualmente un servidor de tiempo de la LAN, en un medio de broadcast de alta velocidad, anuncie a sus pares que desea sincronizarlos, pero que ninguno de ellos lo sincronice.

ANEXO 3

SIMPLE NETWORK MANAGEMENT PROTOCOL

El Simple Network Management Protocol (SNMP por sus siglas en inglés), es un protocolo de la capa de aplicación, parte del conjunto de protocolos TCP/IP, que facilita el intercambio de información de administración, entre dispositivos de red. SNMP permite a la administración de red, el manejo del rendimiento de la red, la localización y solución de problemas de red, y la planificación del crecimiento de la red.

Componentes Básicos

Una red administrada con SNMP, tiene tres componentes clave: dispositivos administrados, agentes, y sistemas de administración de red (NMSs por su siglas en inglés). Un *dispositivo administrado* es un nodo que tiene un agente SNMP y que pertenece a una red administrada. Recolectan y guardan información de administración, para ponerla a disposición de los NMSs, a través del SNMP. Los dispositivos administrados, también llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, desktops o impresoras.

Un *agente* es un módulo de software de administración de red, residente en un dispositivo administrado. Tiene conocimiento local de la información de administración y la traduce a una forma compatible con SNMP. Un *NMS* ejecuta aplicaciones que monitorean y controlan los dispositivos administrados. Provee el grueso del procesamiento y recursos de memoria necesarios para la administración de red. La figura 3.1. ilustra la relación de los componentes.

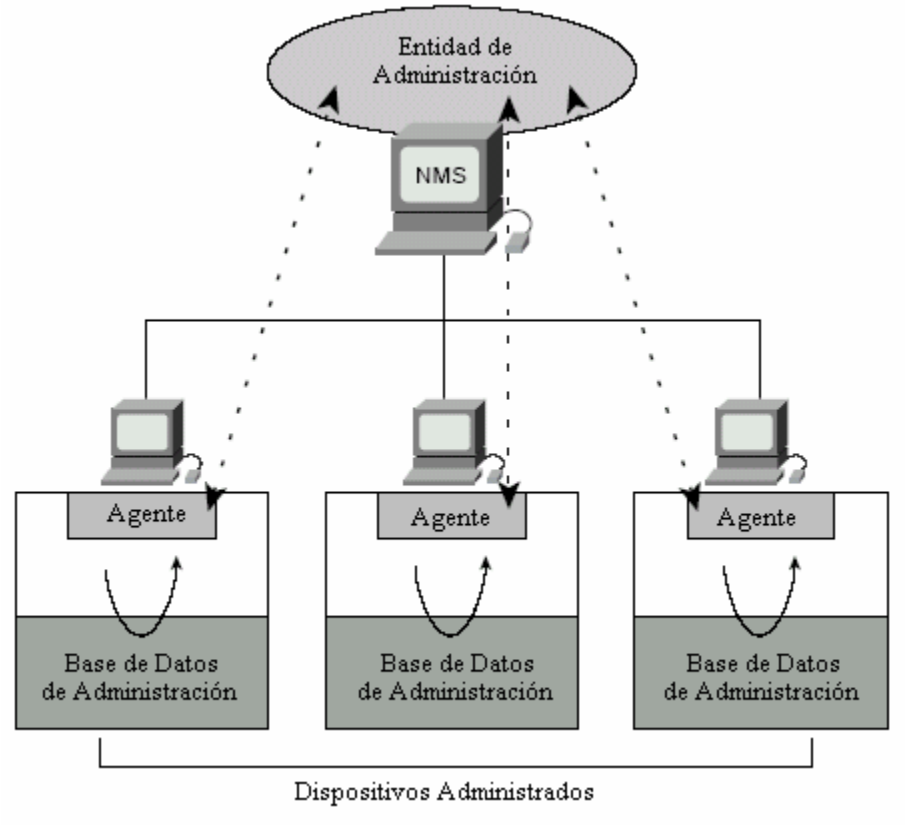


Figura. 3.1. Red administrada por SNMP

Existen dos versiones de SNMP: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas comparten varias características comunes, pero SNMPv2 ofrece mejoras, tales como operaciones adicionales.

Comandos Básicos

Los dispositivos administrados se monitorean y controlan mediante cuatro comandos básicos: lectura (read), escritura (write), trampas (traps) y operaciones transversales. Un NMS utiliza el comando **read** para monitorear los dispositivos administrados. Éste examina distintas variables almacenadas por los dispositivos administrados. El comando **write** se lo utiliza para controlar a los dispositivos administrados. Con este comando, un NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados. El comando trap lo utilizan los dispositivos administrados para reportar eventos de forma asíncrona a un NMS. Las operaciones transversales se utilizan para

determinar que variables soporta un dispositivo administrado y para recolectar información de forma secuencial en tablas de variables.

Base De Datos De Información De Administración

La Base de datos de información de administración (MIB por sus siglas en inglés), es un conjunto de información organizada jerárquicamente, a la que se accede a través de un protocolo de administración de red, tal como el SNMP, que abarca objetos administrados identificados por identificadores de objetos.

Un **objeto administrado**, llamado también objeto MIB, objeto, o MIB, es cualquiera de las características específicas de un dispositivo administrado. Los objetos administrados abarcan una o más instancias de objeto, que son esencialmente variables. Existen dos tipos de objetos administrados: *escalares*, si definen una instancia de un solo objeto, y *tabulares* si definen múltiples instancias de objetos relacionados, agrupados en tablas MIB.

Un **identificador de objeto**, identifica de forma única a un objeto administrado dentro de la jerarquía MIB, la que puede representarse como un árbol con una raíz sin nombre. Los niveles los asignan varias organizaciones. La figura 3.2. ilustra al árbol MIB.

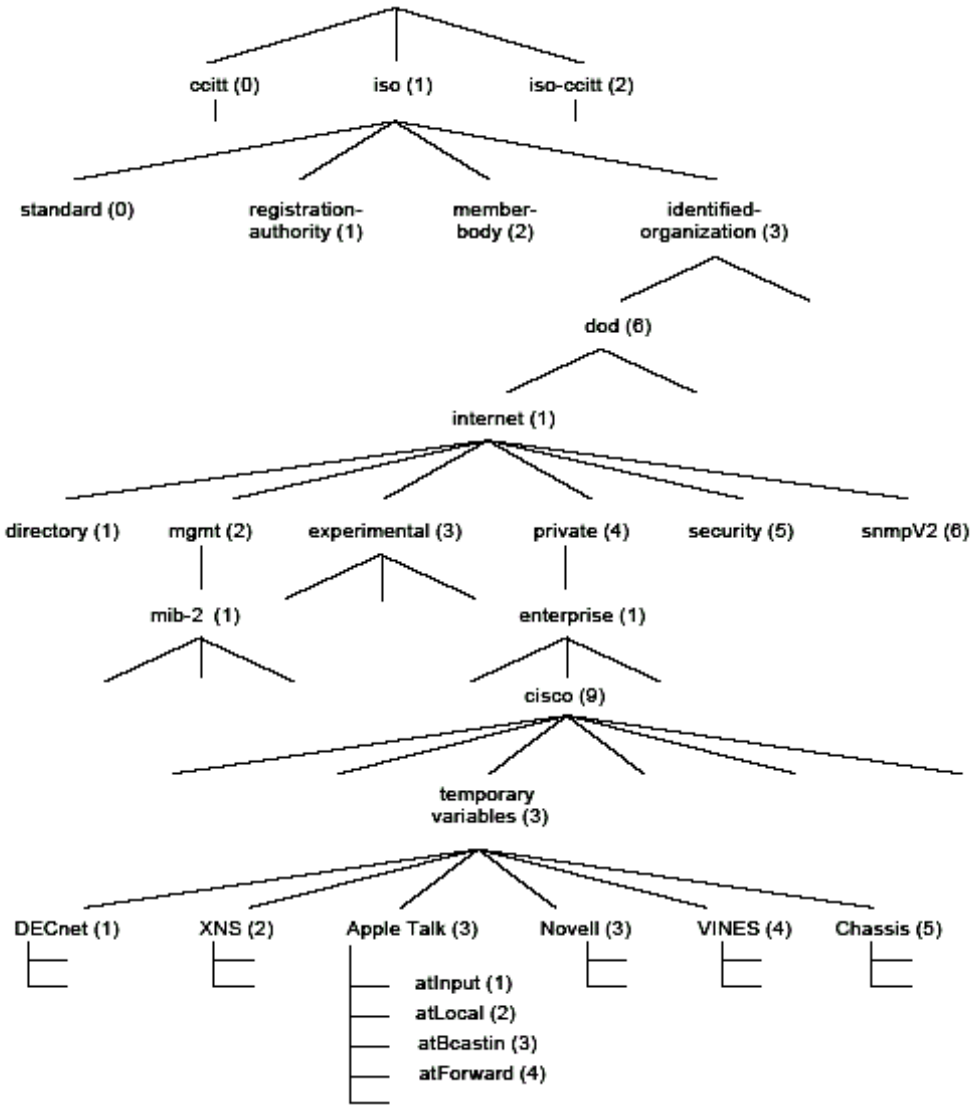


Figura. 3.2. Árbol MIB

Los identificadores de objeto del primer nivel pertenecen a diferentes organizaciones de estándares, mientras que los niveles inferiores son asignados por organizaciones asociadas. Los vendedores pueden definir ramas privadas para incluir objetos administrados para sus propios productos. Las MIBs no estándares se posicionan en la rama experimental. Los objetos manejados pueden ser identificados ya sea por el nombre del objeto, o la descripción equivalente del objeto.

Representación de Datos

SNMP debe tomar en cuenta y ajustar las incompatibilidades entre dispositivos administrados. Computadores diferentes utilizan diferentes técnicas de representación de datos, lo que podría comprometer la capacidad de SNMP para intercambiar información entre dispositivos administrados. Para posibilitar la comunicación, SNMP utiliza un subconjunto del *Abstract Syntax Notation One* (ASN.1).

Operación Del Protocolo

SNMP es un protocolo simple de petición / respuesta. El NMS emite peticiones, y los dispositivos administrados responden. Este comportamiento es la implementación de una de cuatro operaciones del protocolo: Get, GetNext, Set y Trap.

El NMS utiliza la operación **Get** para recuperar el valor de una o más instancias de objeto desde un agente. Si el agente que responde a la operación Get no puede devolver los valores de todas las instancias de objeto en una lista, entonces no devuelve ninguno. La operación **GetNext** se utiliza para recuperar el valor del siguiente objeto de la tabla o lista dentro de un agente; la operación **Set** se utiliza para dar valores a los objetos dentro del agente; la operación **Trap** se utiliza para informar de forma asíncrona al NMS de eventos significativos.

Los comandos anteriores son válidos tanto para SNMPv1 como para SNMPv2, sin embargo este último define dos nuevas operaciones de protocolo: GetBulk e Inform. La primera se utiliza para recuperar grandes bloques de datos, como por ejemplo, múltiples columnas en una tabla. Si el agente que responde no puede proveer valores para todas las variables de la lista, entonces provee resultados parciales. El segundo comando (Inform), permite que un NMS envíe información a otro NMS para luego recibir respuestas.

Administración SNMP

SNMP es un protocolo de administración distribuida. Un sistema puede operar como NMS o como agente, o como ambos a la vez. Cuando opera de esta forma, otro NMS

necesitará que el sistema le provea de la información aprendida de los dispositivos manejados, o que reporte la información almacenada localmente.

Seguridad SNMP

SNMP carece de cualquier capacidad de autenticación, por lo que es vulnerable a varias amenazas de seguridad, entre las que se encuentran el enmascaramiento, modificación de información, modificaciones a la secuencia de mensajes y temporización, y descubrimientos.

El enmascaramiento consiste en los intentos de una entidad no autorizada para ejecutar operaciones de administración al asumir la identidad de una entidad administrativa autorizada. La modificación de información involucra a una entidad no autorizada, la cual intenta alterar los mensajes enviados por una entidad autorizada, de forma tal que se ejecuten operaciones administrativas. Las modificaciones a la secuencia de mensajes y temporización ocurren cuando una entidad no autorizada, reordena, retrasa, o copia y luego envía mensajes generados por una entidad autorizada. Los descubrimientos ocurren cuando una entidad no autorizada, extrae valores almacenados en objetos administrados, o aprende eventos al monitorear los intercambios entre los administradores y agentes.

Ya que SNMP no implementa autenticación, algunos vendedores no implementan las operaciones de Set, por lo que SNMP funciona únicamente para monitoreo.

ANEXO 4

REMOTE MONITORING

El monitoreo remoto (RMON por sus siglas en inglés), es una especificación estándar de monitoreo, que permite que varios monitores de red y sistemas de consola, intercambien datos de monitoreo de red, tales como estadísticas. RMON provee a los administradores de red la libertad de elegir sondas de monitoreo de red y consolas con características que satisfagan sus necesidades particulares, en cuanto a diagnóstico de fallas de red, e información de rendimiento.

La figura 4.1. ilustra una sonda RMON capaz de monitorear un segmento Ethernet y transmitir información estadística hacia la consola RMON.

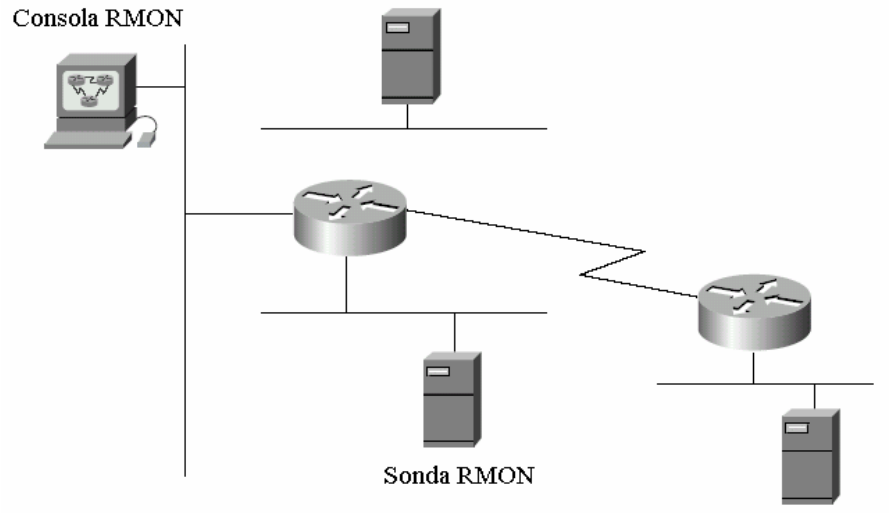


Figura. 4.1. Sonda y consola RMON

Grupos RMON

RMON entrega información en nueve grupos de elementos de monitoreo, cada uno de los cuales provee un conjunto específico de datos que cumplen con requisitos comunes de monitoreo de red. Algunos grupos RMON necesitan el soporte de otros grupos RMON para funcionar de forma adecuada. La siguiente tabla resume los 9 grupos de monitoreo.

Grupo RMON	Función	Elementos
Estadísticas (Statistics)	Contener estadísticas medidas por la sonda para cada interfaz monitoreada en el dispositivo	Paquetes descartados, paquetes enviados, bytes enviados, paquetes de broadcast, errores de CRC, runts, giants, fragmentos, colisiones y contadores de paquetes.
Historial (History)	Grabar muestras estadísticas periódicas de la red, y guardarlas para peticiones posteriores	Período de muestra, número de muestras, ítems muestreados.
Alarma (Alarm)	Tomar muestras estadísticas periódicas de variables en la sonda y compararlas con umbrales preestablecidos. Generar eventos si la variable monitoreada supera el umbral.	Tabla de alarmas. Necesita al grupo de eventos. Tipo de alarmas, intervalo, umbral de inicio, umbral de parada.
Host (Host)	Contener estadísticas asociadas con cada host descubierto en la red.	Dirección de host, paquetes y bytes transmitidos recibidos, así como los broadcasts, multicasts y paquetes de error.
HostTopN	Preparar tablas que describen a los hosts que sobresalen en una lista.	Estadísticas, host (s), período de inicio y fin de muestreo, duración.
Matriz (Matrix)	Almacenar estadísticas de conversaciones entre conjuntos de dos direcciones.	Pares de dirección de origen y destino. Paquetes, bytes y errores de cada par.
Filtros (Filters)	Permitir la comparación de paquetes por medio de una ecuación de filtro. Las coincidencias pueden capturarse o generar eventos.	Tipo de filtro, expresiones de filtro, expresiones condicionales.
Captura de Paquetes	Permitir la captura de paquetes luego de que han atravesado un canal.	Tamaño del búfer para los paquetes capturados, estado de llenado (alarma), número de paquetes capturados.
Eventos (Events)	Controlar la generación y notificación de eventos desde este dispositivo.	Tipo de evento, descripción, último envío de evento.

Grupos de Monitoreo RMON

ANEXO 5

SPANNING TREE PROTOCOL

Spanning tree es un protocolo de capa 2 de administración de enlaces, que provee redundancia, al mismo tiempo que evita lazos indeseados en la red. Para que una red ethernet funcione de forma adecuada, solo debe existir un camino activo entre dos estaciones. Cuando se diseña redes tolerantes a fallos, se debe tener enlaces libres de lazos entre todos los nodos de la red.

El algoritmo de Spanning Tree calcula el mejor camino libre de lazos a través de una red conmutada. Los switches envían y reciben tramas de spanning tree a intervalos regulares; no las retransmiten, pero con ellas construyen el camino libre de lazos.

Múltiples caminos activos entre estaciones, causan lazos en la red, provocando que las estaciones reciban mensajes duplicados, o que los switches aprendan las direcciones MACs de las estaciones en múltiples interfaces, lo que causa la inestabilidad de la red.

Spanning tree define un árbol con un switch raíz, y un camino libre de lazos desde la raíz hacia todos los switches en la red. Spanning tree coloca los caminos redundantes en un estado de bloqueo (standby). Si el segmento de red activo falla, y existe un camino redundante, el algoritmo de spanning tree recalcula la topología de spanning tree y activa el camino que estaba en estado de standby.

Cuando dos puertos de un switch son parte de un lazo, los valores de la prioridad de puerto y costo de enlace (spanning tree port priority & port cost), determinan cuál puerto será el que transmita y cuál pasará al estado de bloqueo. El valor de la prioridad de puerto representa la localización de una interfaz en una topología de red, mientras que el costo del enlace representa la velocidad.

Elección De La Raíz

Todos los switches de la red participan en la recolección de datos acerca de los otros switches de la red a través del intercambio de mensajes conocidos como Bridge Protocol Data Units (BPDUs por las siglas en inglés), lo que provoca las siguientes acciones:

- La elección de un único switch como raíz del spanning tree.
- La elección de un switch designado para cada segmento de LAN.
- La eliminación de lazos en la red, al bloquear las interfaces conectadas a los enlaces redundantes.

Para cada VLAN, se elige al switch con la mayor prioridad (menor valor numérico de prioridad) como el switch raíz. Si todos los switches están configurados con la prioridad por defecto (32768), el switch con la dirección MAC más baja se convierte en la raíz.

El switch raíz es el centro lógico de la topología de spanning tree de la red. Todos los enlaces no necesarios para comunicarse con el switch raíz desde cualquier parte de la red, se colocan en el estado de bloqueo.

Las BPDUs contienen información acerca del switch que transmite y de sus puertos. Se transmite la dirección MAC del switch, su prioridad, la prioridad de los puertos y el costo del enlace. Spanning tree usa esta información para elegir al switch raíz y puerto raíz de la red, así como el puerto raíz y el puerto designado para cada segmento de la red.

Estado De Los Puertos En Spanning Tree

Los retardos de propagación ocurren cuando la información del protocolo se transmite a través de una red conmutada. Cuando una interfaz pasa del estado de no participación en la topología de spanning tree al estado de transmisión, puede crear lazos temporales. Los puertos deben esperar a que se propague nueva información de la topología a través de la

LAN antes de poder transmitir tramas. Deben permitir que expire el tiempo de vida de las tramas transmitidas con la topología anterior.

Cada interfaz del switch que utilice spanning tree, trabaja en uno de los cinco estados siguientes:

- Bloquear. La interfaz no transmite tramas.
- Escuchar. Primer estado de transición después del bloqueo. Spanning tree determina que la interfaz debe transmitir tramas.
- Aprender. La interfaz se prepara para transmitir tramas.
- Transmitir. La interfaz transmite tramas.
- Deshabilitar. La interfaz no participa en spanning tree y no transmite tramas.

Una interfaz pasa a través de los cinco estados de la siguiente manera:

- De inicialización a bloqueo.
- De bloqueo a escucha o deshabilitado.
- De escucha a aprendizaje o a deshabilitado.
- De aprendizaje a transmisión o a deshabilitado.
- De transmisión a deshabilitado.

ANEXO 6

VIRTUAL TRUNK PROTOCOL

Virtual Trunk Protocol (VTP por sus siglas en inglés) es un protocolo de capa 2 que maneja la creación, eliminación y nombres de VLANs con el objetivo de mantener la consistencia de configuración de VLANs dentro de la red. El VTP minimiza las malas configuraciones e inconsistencias en las configuraciones, que pueden causar varios problemas, tales como nombres duplicados de VLANs y violaciones de seguridad. Al utilizar VTP, se pueden realizar cambios de forma centralizada en un solo switch, ya que éstos serán comunicados al resto de switches de la red.

Dominio VTP

Un dominio VTP, llamado también dominio de administración de VLAN, es uno o varios switches interconectados que comparten el mismo dominio VTP. Un switch se configura para que pertenezca a un solo dominio VTP; el switch por defecto está en el modo de servidor VTP, pero no propaga la información de VLANs hasta que se configure o aprenda el nombre del dominio de administración.

Cuando un switch recibe un aviso VTP a través de un enlace troncal (trunk), éste lee el nombre del dominio de administración y el número de revisión de la configuración. Se ignoran los avisos con un nombre del dominio de administración diferente, o con un número de revisión de configuración anterior.

Cuando se realizan cambios a la configuración de VLANs en el servidor VTP, los cambios se propagan a todos los switches del dominio VTP, a través de todos los enlaces troncales, ya sean del tipo ISL (Inter. Switch Link), IEEE 802.1Q, IEEE 802.10 y Modo de Transferencia Asíncrono (ATM) emulación de LAN (LANE).

Modos VTP

Un switch se puede configurar para que trabaje en uno de los siguientes modos:

- Servidor VTP. Modo por defecto. En este modo se pueden crear, modificar y eliminar VLANs y especificar otros parámetros de configuración para el dominio VTP entero. Los servidores VTP publican la configuración de VLANs a través de los enlaces troncales, al resto de switches de la red.

- Cliente VTP. En este modo, se comporta como un servidor VTP, pero no se pueden crear, modificar o eliminar VLANs.

- Transparente. En este modo, los switches no publican su configuración de VLAN ni la sincronizan con los avisos recibidos. Sin embargo, si se transmiten los avisos recibidos de otros switches. Se pueden crear, modificar y eliminar VLANs.

Avisos VTP

Cada switch en el dominio VTP envía estos avisos periódicos de configuración global desde cada puerto troncal a una dirección reservada de multicast. Los switches vecinos reciben estos avisos y actualizan su configuración VTP y de VLAN de ser necesario. La información de dominio que se distribuye en los avisos VTP es la siguiente: nombre del dominio VTP, número de revisión de configuración VTP, identidad de actualización y de marca de tiempo (timestamp) y resumen MD5.

La información que se distribuye de cada VLAN configurada, en cada aviso VTP es la siguiente: identificación de VLAN, nombre de VLAN, tipo de VLAN, estado de VLAN e información adicional de la configuración de VLAN específica al tipo de VLAN.

INDICE DE FIGURAS

INDICE DE TABLAS

GLOSARIO

ACE *Access Control Entry*. Cada una de las condiciones de las que se compone una Lista de Control de Acceso.

ACL *Access Control List*. Lista configurada en los routers para controlar el acceso desde y hacia el router a ciertos servicios o segmentos de red.

AP *Access Point*. Equipo activo de red que sirve de punto de acceso para los clientes inalámbricos.

ARP *Address Resolution Protocol*. Protocolo del stack TCP/IP que resuelve una dirección IP en una dirección MAC.

AS *Autonomous System*. Conjunto de redes bajo una administración común que comparten una estrategia de enrutamiento.

BPDU *Bridge Protocol Data Unit*. Paquete hello de Spanning Tree Protocol que se envía de forma periódica para intercambiar información entre lo bridges de la red.

CDP *Cisco Discovery Protocol*. Protocolo de descubrimiento de dispositivos independiente de medios y de protocolos que corre en todos los equipos de Cisco.

CHAP *Challenge Handshake Authentication Protocol*. Característica de seguridad en líneas con encapsulación PPP que previene el acceso no autorizado.

CIDR *Classless Interdomain Routing*. Técnica que se basa en la agregación de rutas. Permite a los routers agrupar rutas para reducir la cantidad de información de enrutamiento que atraviesa a través de la red.

CoS *Class of Service*. Indicador de cómo los protocolos de las capas superiores deben tratar los mensajes de los protocolos de las capas inferiores.

dB *Decibel*. Unidad para expresar relaciones de potencia relativas en términos de pérdidas o ganancias. Las unidades se expresan en términos del logaritmo en base 10 de la relación expresada usualmente en vatios.

dBi dB relativo a un radiador isotrópico, el cual teóricamente tiene un patrón de radiación simétrico.

dBm *Decibelios por milivatios*. 0 dBm se define como 1 mW a 1 kHz de frecuencia y a 600 ohmios de impedancia.

DHCP *Dynamic Host Configuration Protocol*. Provee un mecanismo para la asignación dinámica de direcciones IP.

DNS *Domain Name System*. Sistema que traduce nombres de nodos de red a direcciones.

DSSS *Direct Sequence Spread Spectrum*. Spread Spectrum de Secuencia Directa.

EAP *Extensible Authentication Protocol*. Arquitectura que soporta múltiples mecanismos de autenticación opcionales como texto llano, challenge – response y secuencias arbitrarias de diálogo.

EIGRP *Enhanced Internal Gateway Routing Protocol*. Versión avanzada de IGRP desarrollada por Cisco. Provee mejoras en la convergencia y eficiencia de operación, al combinar las ventajas de los protocolos de estado enlace y los de vector distancia.

FEXT *Far End Cross Talk*. Diafonía en el extremo lejano o paradiafonía.

FHSS *Frequency Hop Spread Spectrum*. Spread Spectrum de Salto de Frecuencia.

Gbps Giga bit per second.

Ghz Giga hetz

Gigabit Ethernet. Estándar para ethernet de alta velocidad aprobado por el estándar 802.3z de la IEEE en 1996.

Hz *Hertz*. Medida de la frecuencia, sinónimo de ciclos por segundo.

IDF *Intermediate Distribution Facility*. Cuarto de comunicaciones que no es el principal.

IDS *Intrusion Detection System*. Sistema de detección de intrusos. Detecta y bloquea actividades sospechosas o no autorizadas dentro de la red.

IEEE *Institute of Electrical and Electronic Engineers*. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes.

IGRP *Interior Gateway Routing Protocol*. Protocolo desarrollado por Cisco para manejar los problemas asociados con el enrutamiento dentro de grandes redes heterogéneas.

IP *Internet Protocol*. Protocolo de la capa de red que provee servicio no orientado a la conexión. Provee características de direccionamiento, especificación de Tipo de Servicio, fragmentación y reensamblado y seguridad.

IS-IS *Intermediate System – Intermediate System*. Protocolo OSI jerárquico de enrutamiento de estado enlace.

ISO *International Standards Organization*. Organización internacional responsable de una amplia gama de estándares, entre los que se incluyen los de redes. Desarrolló el modelo de referencia OSI.

LAN *Local Area Network*. Red de datos de alta velocidad y baja tasa de error que cubre un área geográfica relativamente pequeña.

LEAP *Light Extensible Authentication Protocol*. Implementación EAP propuesta e implementada por Cisco Systems en sus equipos de acceso inalámbrico.

LSA *Link State Advertisement*. Paquete del tipo broadcast utilizados por los protocolos de estado enlace el cual contiene información acerca de los vecinos y los costos de las rutas.

MAN *Metropolitan Area Network*. Red de datos que se extiende a través de un área metropolitana. Generalmente es mayor que una LAN, pero menor que una WAN.
Mbps Mega bit per second. Megabits por Segundo.

MDF *Main Distribution Facility*. Cuarto de comunicaciones principal.

MHz Mega hertz.

MIB *Management Information Base*. Base de datos de información administrativa de la red usada y mantenida por un protocolo de administración de red.

mW Mili Watt

NEXT *Near End Cross Talk*. Diafonía de extremo cercano.

NTP *Network Timing Protocol*. Protocolo que asegura el mantenimiento del tiempo local en referencia a relojes de alta precisión.

OSI *Open Systems Interconnection*. Programa de estandarización internacional creado por la ISO y la ITU-T para desarrollar estándares de networking que faciliten la interoperabilidad de equipos de diferentes vendedores.

OSPF *Open Shortest Path First*. Algoritmo de enrutamiento jerárquico de estado enlace propuesto como el sucesor de RIP.

PAP *Password Authentication Protocol*. Protocolo de autentiación que permite a los pares PPP autenticar el uno al otro.

PPP *Point to Point Protocol*. Provee conexiones router a router y host a red sobre circuitos síncronos y asíncronos.

QoS *Quality of Service*. Medida del rendimiento de un sistema de transmisión que refleja la calidad de la transmisión y la disponibilidad del servicio.

RADIUS *Remote Access Dial In User Server*. Base de datos para autenticar conecciones y llevar registros de la duración de las mismas.

RFC *Request For Comment*. Series de documentos utilizados para propagar información acerca del Internet. La mayoría provee especificaciones de protocolos, pero algunos son únicamente de carácter histórico.

RIP *Routing Information Protocol*. Protocolo de enrutamiento que utiliza como métrica los saltos.

RMON *Remote Monitoring*. Especificación que provee múltiples capacidades para monitoreo, detección y reporte de problemas.

SNMP *Simple Network Management Protocol*. Provee las herramientas para monitorear y controlar dispositivos de red, administrar configuraciones, y almacenar estadísticas de rendimiento.

SPF *Shortest Path First*. Algoritmo de enrutamiento que realiza iteraciones en la longitud de un camino para determinar el camino más corto.

SSID *Service Set Identifier*. El SSID es un valor alfanumérico único, de longitud variable entre 2 y 32 caracteres, que representa al nombre de la red inalámbrica

STP *Spanning Tree Protocol*. Protocolo de capa 2 que impide la formación de lazos físicos dentro de una red switcheada.

TCP/IP *Transfer Control Protocol*. Protocolo de la capa de transporte orientado a la conexión el cual provee transmisiones confiables full dúplex.

TFTP *Trivial File Transfer Protocol*. Versión simplificada de FTP que permite la transmisión de archivos sin el uso de autenticación de cliente.

UDP *Unreliable Datagram Protocol*. Protocolo de la capa de transporte no orientado a la conexión.

VLAN *Virtual Local Area Network*. Grupo de dispositivos en una o más LANs que están configuradas para que puedan comunicarse como si estuvieran conectados al mismo segmento de red.

VLSM *Variable Length Subnet Mask*. Capacidad para especificar diferentes máscaras de subred para la misma red.

VoIP *Voice over Internet Protocol*. Capacidad para llevar la voz a través de una red IP con las características de funcionalidad, calidad y confiabilidad que el sistema telefónico común.

VPN *Virtual Private Network*. Permite transportar el tráfico IP de forma segura a través de una red pública de un host a otro. Las VPNs utilizan la tunelización para cifrar el tráfico entre los extremos.

VTP *Virtual Trunking Protocol*. Protocolo de capa 2 que maneja la creación, eliminación y nombres de VLANs con el objetivo de mantener la consistencia de configuración de VLANs dentro de la red

WAN *Wide Area Network*. Red de comunicación de datos utilizada por usuarios a través de un área geográfica extensa. Los tipos de encapsulación más comunes son Frame Relay, PPP y HDLC.

WLAN *Wireless Local Area Network*. Red Inalámbrica de área local.

Sangolquí _____

Elaborado por

Ángel Roberto Almeida Gutiérrez

Decano

Ing. Marcelo Gómez C.
TCRN de E.M.

Secretario Académico

Ab. Jorge Carvajal R.