PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS Y COMPUTACIÓN

Diseño de una red LAN /WAN segura para el Tribunal Constitucional aplicando la metodología de 3 capas de CISCO

PABLO XAVIER ARIAS SÁNCHEZ.

DIRECTOR: ING. FRANCISCO RODRÍGUEZ.

QUITO, 2011

AGRADECIMIENTOS

Quiero agradecer a toda mi familia que ha sido un apoyo incondicional en el desarrollo de mi tesis y sobre todo en mi crecimiento personal.

Durante el avance del trabajo conté con amigas y amigos invaluables que aportaron positivamente, muchas gracias.

Tabla de contenido

AGRADECIMIENTOS 2

1. Introducción a las redes LAN/WAN. 9

1.1 Introducción a las Redes LAN. 9

1.1.1 Concepto de Redes 10

1.1.2 Dispositivos LAN 10

1.1.3 Estructura física de una red LAN 12

1.1.4 Estructura de Enlace de Datos. 15

1.1.5 Canales de Datos 15

1.1.6 Auto negociación Ethernet Semidúplex o Dúplex. 16

1.1.7 El Modelo de Referencia OSI 17

1.1.8 Topología de Redes LAN. 20

1.1.9 LAN Virtuales 21

1.2 Ethernet y Cableado 22

1.2.1 Ethernet 802-3. 22

1.2.2 100-Mbps Ethernet. 23

1.2.3 1000-Mbps Ethernet. 25

1.2.4 Normas de Cableado. 25

1.3 Introducción a las redes WAN. 29

1.3.1 Marcación Analógica. 32

1.3.2 RDSI. 33

1.3.3 Línea Alquilada. 34
1.3.4 X.25. 35
1.3.5 Frame Relay. 36
1.3.6 ATM. 37
1.3.7 DSL. 38
1.3.8 Modem por Cable. 39
1.4 Requerimientos de Tráfico. 40
1.4.1 Ancho de Banda. 41
1.4.2 Latencia. 43
1.4.3 Fluctuación de Fase. 44
1.4.4 Voz, Datos Cliente / Servidor, Mensajería, Videoconferencia. 44
1.5 Estándares y Protocolos 45
1.5.1 Protocolo IP. 45
1.5.2 Protocolo de Mensajes de Control en Internet. (ICMP). 47
1.5.3 Protocolo de Resolución de Direcciones (ARP). 50
1.5.4 Protocolo de Resolución Inversa de Direcciones (RARP). 51
1.5.5 Normas WAN. 52
1.5.6 EIA / TIA 232. 52
g1.5.7 EIA / TIA 449 EIA-530. 53
1.5.8 EIA / TIA 612 / 613. 53
1.5.9 V.35. 54
1.6.0 X.21. 54

2. Red Local actual y Requerimientos 55
2.1 Infraestructura Física..... 55
2.1.1 Caso de Estudio 56
2.1.2 Punto de Demarcación (demarc)..... 56
2.1.3 Sala de Telecomunicaciones..... 59
2.1.4 Cableado Backbone y Cableado de Distribución 60
2.1.5 Áreas de Trabajo 61
2.1.6 Sala de Equipos (ER) 63
2.1.7 Administración. 65
2.1.8 Mapa de Red por Pisos Corte Constitucional..... 66
2.2 Infraestructura Lógica..... 71
2.2.1 Diseño Actual 72
2.1.2 Servidores 72
2.1.3 Dominios..... 75
2.1.4 Seguridad y Políticas de Grupo 76
2.1.5 Información..... 78
2.1.6 Relaciones de Confianza..... 84
2.1.7 Unidades Organizativas 84
2.1.8 Direcciones IP 85
2.3 Requerimientos LAN. 88
2.3.1 Metodología..... 88
2.3.2 Requerimientos Físicos de los Usuarios 89

2.3.3 Resultados de las Encuestas y Entrevistas..... 93
2.3.4 Análisis de Requerimientos Físicos..... 94
2.3.4 Requerimientos Lógicos de los Usuarios 95
2.3.5 Análisis de Requerimientos Lógicos..... 102
2.4 Requerimientos WAN. 103
2.4.1 Antecedentes..... 103
2.4.2 Requerimientos WAN de los usuarios..... 103
2.4.3 Requerimientos WAN de Hardware 105
2.4.4 Requerimientos WAN de Software..... 106
2.4.5 Análisis de los Requerimientos WAN..... 107
3. SEGURIDAd eN Redes. 109
3.1 Vulnerabilidades en una Infraestructura de Red..... 110
3.1.1 Amenazas Contra la Seguridad de la Empresa 110
3.1.2 Puntos Inseguros en una Red..... 115
3.2 Bases para Establecer Seguridad Física de Red. 120
3.2.1 Medios Físicos..... 120
3.2.2 Topografía de Red..... 122
3.2.3 Dispositivos de Red. 125
3.2.4 Ambiente de Seguridad. 127
3.3 Bases para Establecer Seguridad Lógica de Red. 128
3.3.1 Instauración de Subredes..... 128
3.3.2 Instauración de Enrutamiento. 130
3.3.3 Autenticación. 131

3.3 Bases para Establecer Integridad. 132
3.3.1 Firewall. 132
3.3.2 Servicios de Red. 133
3.3.3 Autenticación. 134
3.4 Bases para Establecer Confidencialidad. 136
3.4.1 Cifrado. 136
3.4.2 Clave Pública PKI 138
3.4.3 Gestión de claves. 139
3.4.4 Administración de Accesos 140
3.4.5 TCP/IP y Seguridad 142
3.5 Bases para Establecer Procedimientos al Personal. 145
3.5.1 Respaldos de Seguridad. 146
3.5.2 Auditoria. 146
3.5.3 Temas Legales. 146
3.6 Administración de la red y Seguridad. 150
3.6.1 Observaciones para la Implementación de la Seguridad 150
3.6.2 Control de Riesgos 154
3.6.3 Monitoreo de la Red 156
3.6.4 Seguridad vs. Facilidad de Uso 157
3.6.5 Medidas de Control 158
3.6.6 Estrategias Proactivas 158
3.6.7 FCAPS (Fault, Configuration, Acounting, Performance, Security) 160
4 DISEÑO DE RED 163

4.1 Diseño LAN/ WAN 163
4.1.1 RED WAN 163
4.1.2 Direccionamiento WAN. 165
4.1.3 LAN Sucursales propuestas 167
4.2 Diseño LAN Oficina Central. 172
4.2.1 Generalidades 172
4.2.2. Diseño de 3 Capas CISCO 173
4.2.3. Diseño de la Capa de Acceso. 175
4.2.4. Diseño de la capa de distribución. 182
4.2.5 Diseño de la capa Núcleo 193
4.2.6 Localización de los Host 199
4.2.7 Fiabilidad de la Red 199
5 Conclusiones y Recomendaciones 202
5.1 Conclusiones 202
5.2 Recomendaciones 204
Bibliografía. 206
Tabla de Gráficos. 208
Índice de Tablas 211

1. INTRODUCCIÓN A LAS REDES LAN/WAN.

El presente capítulo proporciona un preámbulo que permite un mejor entendimiento del caso de estudio, ***Diseño de una red LAN /WAN segura para el Tribunal Constitucional Aplicando la Metodología de 3 Capas de CISCO***; la información recopilada proviene en su mayor parte de conceptos y fundamentos de redes de los módulos de preparación para la certificación CCNA (Cisco Certified Network Associate); "CISCO es una empresa multinacional con sede en San José (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos telecomunicaciones"[1].

Comenzando por redes de área local se enuncian los conceptos principales relacionados con la parte de transmisión de los datos (aspecto físico), tanto para redes de área local (LAN), como para de área amplia (WAN), para luego, exponer temas de requerimientos de tráfico y por último consideraciones acerca de protocolos (acuerdos) de red.

Una parte importante de este prólogo es el ***modelo de referencia OSI*** que permite simplificar las nociones del transporte de la información, dividiendo todo el proceso en siete capas, cada una con características propias y distintas entre sí. Además, el diseño en capas de la actual disertación tiene su fundamento en la configuración OSI (3 capas).

1.1 Introducción a las Redes LAN.

Las redes de área local (LAN), se caracterizan por compartir recursos o distribuir servicios en un área relativamente pequeña, generalmente, en entornos de oficina. Existen estándares y metodologías para implementar infraestructuras de este tipo, por ejemplo, para que circule la información por un medio físico (cable UTP), no se debe exceder la distancia de 100 metros hasta el medio de difusión (servidor o switch).

[1] Wikipedia. *CISCO Systems*. Internet. http://es.wikipedia.org/wiki/Cisco_Systems Acceso: 01/diciembre 2011.

En lo que sigue del capítulo expondremos conceptos que nos permitan entender las bondades y falencias de las infraestructuras de red local (LAN) y de área extendida (WAN).

1.1.1 Concepto de Redes

Una red es un conjunto de instrumentos (computadoras) dispuestos en un área geográfica, conectados o relacionados entre sí con el objetivo de compartir recursos ya sea en hardware, software o información. Dependiendo del alcance de la red se dividen en redes de área local LAN (varios metros), redes de área metropolitana MAN (dentro de una ciudad) y redes de área amplia WAN (varios kilómetros entre ciudades o países). Por lo expuesto, una red informática es:

> *Un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.*[2]

1.1.2 Dispositivos LAN

Para establecer una red de área local se necesitan varios dispositivos. Se denominan componentes hardware de la LAN y son:

Repetidores.- la principal función de este dispositivo es regenerar y re-sincronizar los datos (bits) enviados por la red para que puedan alcanzar distancias más largas, se emplea cuando en una infraestructura de red existen muchos terminales o si hay escases de cables. Existe una regla que se aplica cuando se requiere extender los segmentos de una red, se denomina ***regla 5-4-3*** y establece que no es permitido enlazar más de cinco segmentos de red extremo a extremo, utilizando cuatro repetidores, y que solo tres segmentos pueden tener terminales. La regla no es muy veraz con switches y arquitecturas de red extendidas.

Hubs.- estos dispositivos son repetidores, pero con varios puertos y se los utiliza con mayor frecuencia en las redes Ethernet 10BASE-T y 100BASE-T. El uso de un hub

---

[2] Tanenbaum Andrew, *Redes de Computadoras*, México, Prentice-Hall, 3ra. Edición, 1997, página 30.

cambia la topología lineal en bus de una red convirtiéndola en una arquitectura en estrella debido a que cuando llega la señal por uno de los puertos, el hub regenera la señal por los otros puertos restantes. Un hub es ***activo*** cuando es necesario conectarlo a una toma de corriente para que pueda ampliara la señal que recibe. Existen hub inteligentes que además de amplificar la señal tienen elementos que ayudan en casos de error o diagnóstico.

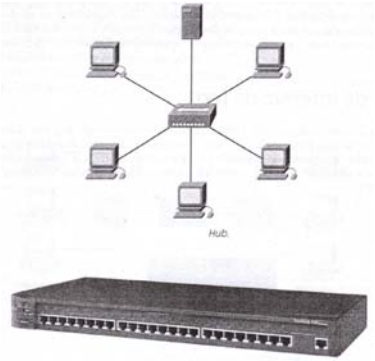


Gráfico 1. 1 Dispositivos LAN Hub.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 75.

Puentes.- cuando es necesario dividir una LAN en segmentos más pequeños se utilizan puentes, son los dispositivos encargados de decidir el envío de señales al segmento, la decisión se basa en el filtrado que es analizar la dirección MAC para verificar si la información de destino se encuentra en la misma sección, si es así, deshabilita cualquier otra sección si, en cambio, el destino está en otra sección la envía y si no conoce el destino transmite a todos los segmentos.

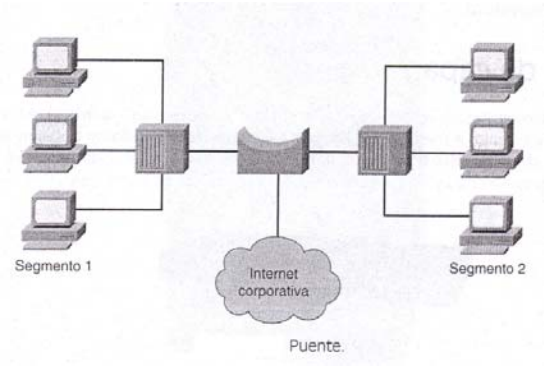


Gráfico 1. 2 Dispositivos LAN Puente.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 77.

Switches.- se puede decir que un switch es un puente multipuerto. Poseen tablas de envío para acordar la entrega de la información. Estos dispositivos trabajan a una velocidad más elevada que un puente. Actualmente, la utilización de switches en un entorno LAN es muy conveniente porque permiten la utilización de segmentos dedicados en un entorno virtual libre de colisiones, lo que maximiza el ancho de banda. Según CISCO un switch es "un dispositivo de red de capa 2 que actúa como punto de concentración para la conexión de estaciones de trabajo, servidores, hubs y otros switches"[3]

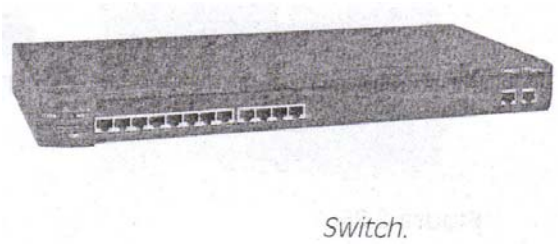


Gráfico 1. 3 Gráfico Dispositivos LAN Switch.

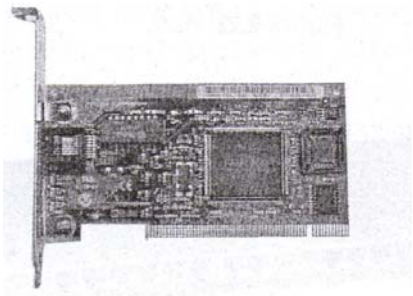
Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 78.

1.1.3 Estructura física de una red LAN

Una red LAN la conforman computadoras (hosts), tarjetas de interfaz de red (NIC / Network Interface Card), dispositivos periféricos, medios de red y dispositivos de red.

[3] Cisco Systems, *Guía del segundo año. CCNA® 3 y 4*. Madrid, Pearson Educación S.A., 3ra edición, 2004. Página 195.

Una ***NIC*** "es un circuito impreso que proporciona capacidad de comunicación entre computadoras"[4]; sirve de enlace entre un medio físico (cable) y un dispositivo (host). Tiene un número expresado en hexadecimal único llamado dirección MAC que sirve de identificador. La tecnología Ethernet utiliza conectores RJ45. Las tarjetas de red son consideradas dispositivos de capa 2 del modelo OSI (modelo de referencia para una red).



Tarjeta de interfaz de red.

Gráfico 1. 4 Dispositivos LAN NIC o Interfaz de red.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 76.

Los ***repetidores*** son dispositivos de que regeneran las señales atenuadas, dicha pérdida, se debe a la longitud del cable.

Un ***hub*** o concentrador es similar a un repetidor con múltiples puertos; generalmente enlazan segmentos de una red LAN repitiendo la señal en cada puerto y ampliando la señal.

El diseño de red más difundido a nivel mundial son las redes conocidas como Ethernet, una de las características principales que ayudaron a establecer este esquema es la adaptación, es decir, la capacidad para integrar mejores velocidades en la misma tecnología así, por ejemplo el mismo protocolo que transportaba datos a 3 megabit por segundo (Mbps), ahora lo hace a 10 gigabits (Gbps).

---

[4] Cisco Systems, *Guía del primer año. CCNA® 1 y 2*. Madrid, Pearson Educación S.A., 3ra edición, 2004. Página 34.

El desarrollo para comunicarse con un mismo medio y acceder a él sin interferencias (colisiones) comenzó con estudios en los años 70; "el proyecto Aloha desarrollado en la Universidad de Hawái"[5] para compartir la banda de radio frecuencia, Ethernet se basó en este estudio para establecer ***acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD, Carrier Sense Multiple Access Collision Detect)*** que es la norma que impide colisiones en el medio***.***

El método ***CSMA/CD*** se focaliza en tres funciones transmitir–recibir, decodificar y detectar paquetes de datos. Es un método de difusión de medio compartido, es decir, antes de transmitir primero detecta un flujo portador; sí, dos hosts transmiten al mismo tiempo, se produce una colisión que se manifiesta por un aumento de la amplitud de la señal, una vez que toda la red a detectado la colisión, cada host ejecuta un ***algoritmo de retardo*** que permite intentar la transmisión nuevamente; sí persiste la colisión se aborta la transmisión.

La primera arquitectura que se implemento en redes LAN Ethernet se denominó DIX (Digital Intel Xerox), DIX sirvió de base para las normas: IEEE 802.3, IEEE802.3u (Fast Ethernet), IEEE 802.3z (Gigabit Ethernet sobre fibra) y 802.3ab (Gigabit Ethernet sobre UTP); estándares implementados por el instituto de ingenieros eléctricos y electrónicos (IEEE). Los estándares y las normas definen el medio físico, los conectores, la forma como se van a comunicar y la manera de encapsular las tramas.

Para una mejor compresión del proceso de comunicación entre host aparece el concepto abstracto de capas; cada una de ellas posee características específicas de acuerdo a la función que realiza, por ejemplo, la capa física se encarga de transportar las condiciones eléctricas o impulsos. En la capa física no se permite la comunicación con capas superiores esto se debe a que en esta capa se transmiten flujos de bits. Para saber el inicio, el fin de la comunicación entre dos hosts, los errores y la sincronización transmisión – recepción es necesario realizar un proceso de entramado (dividir y encapsular la información).

---

[5] Alabau A. y Riera J., *Teleinformática y Redes de Computadores*, Barcelona, Marcombo S.A., 2da. Edición, 1992, Página 20.

1.1.4 Estructura de Enlace de Datos.

Para la comunicación a través del medio, existe como concepto abstracto ***la capa de enlace de datos***, que junto con un estándar conocido como Ethernet IEEE establece dos subcapas:

Control de acceso al medio (MAC) (802.3).- que se encarga del modo de transmitir las tramas por el medio físico, cada dispositivo tiene una sola y única dirección MAC de longitud de 48 bits representada con 12 dígitos hexadecimales necesaria para recibir la información enviada. Los seis dígitos primeros identifican al fabricante, los segundos seis dígitos se refieren al número de serie interfaz. Existen protocolos MAC deterministas y no deterministas, los primeros implementan *Tokens* o datos especiales que permiten transmitir información, son como turnos con tiempo limitado que circulan por la red; los no deterministas utilizan el sistema ***FCFS*** (First-come-first served), es decir, el primero en llegar es el primero en ser servido CSMA / CD es un ejemplo de protocolo de acceso al medio no determinista.

Control de enlace lógico (LLC) (802.2).- en ésta subcapa se reconoce lógicamente las distintas etiquetas o protocolos para su posterior encapsulación. Utiliza un identificador de acceso denominado (SAP). Permite varios protocolos de capa 3 (…) como IP e IPX.

Tanto la MAC como la LLC son componentes importantes para la comunicación con la capa física. En la capa de enlace de datos se incorporan una **cabecera** que almacena datos de capas superiores y una **información final** que corresponde a información de la capa de enlace de datos.

1.1.5 Canales de Datos

Las señales transmitidas pueden propagarse de tres maneras: unidireccional, semiduplex y dúplex. Si hablamos de la primera forma ***unidireccional***, nos referimos a que la información circula en un solo sentido. Las transmisiones de radio y televisión son ejemplos de este modo de transferencia.

Semidúplex es una manera doble de transmisión, es decir, en dos sentidos con el condicionamiento de que la difusión no puede ser al mismo tiempo. Se emplea el método CSMA / CD para ayudar a la prevención de colisiones.

Traslado ***Dúplex*** es en dos direcciones, utiliza dos pares de hilos que permite enviar y recibir al mismo tiempo. Teóricamente la transmisión dúplex brinda 100% de eficacia en ambas direcciones, es decir, con Ethernet a 10 Mbps se puede conseguir 20 Mbps.

1.1.6 Auto negociación Ethernet Semidúplex o Dúplex.

Existen dos modos de transmisión semidúplex y dúplex, el primero generalmente utiliza un medio físico coaxial (cable), mientras que dúplex utiliza UTP o fibra óptica. En el modo de comunicación semidúplex la transmisión de un host se realiza en diferentes intervalos, es decir, no pueden transferir dos host al mismo tiempo, de lo contrario, se generarían choques en la transmisión y consecuentemente errores. En un medio físico de Fibra y UTP la transmisión utiliza pares separados lo que permite que no se solapen las transmisiones, es decir, en el modo dúplex se permite la transmisión al mismo tiempo. La auto negociación evita conflictos cuando dos host utilizan diferentes modos de transmisión. Sí un host necesita transmitir en modo dúplex y tiene velocidades inferiores a 10 Gigabits se puede usar auto negociación o forzando administrativamente el modo de interfaz.

La técnica llamada *auto negociación de velocidades semidúplex o dúplex,* permite armonizar la velocidad entre dos enlaces para obtener un mejor rendimiento. El Ethernet original (10BASE-T) requiere de una transmisión de un pulso de enlace cada 16 milisegundos, siempre y cuando, la terminal no esté ocupada o trasmitiendo. La auto negociación acepta esta marca y la renombra como punto de enlace normal (NLP, Normal Link Pulse), si se transmiten series de NLP’s para la auto negociación, éste conjunto se denomina ráfaga de pulso de enlace rápido (FLP, Fast Link Pulse); cada ráfaga se envía en el mismo intervalo de tiempo que un NLP.

El Ethernet 10BASE-T emplea marcas entre +1 y -1 voltios para la transmisión, en cambio, para una señalización NLP sólo se usa un intervalo de 0 a +1 voltios. La durabilidad de un pulso NLP es de 100 ns. (Nano segundos). La auto negociación se establece transmitiendo 1 ráfaga de impulsos de enlace 10BASE-T desde cada 1 de los 2 socios de enlace, luego que dos host se reconocen, ambos cambian a la configuración común de mayor rendimiento.

Una ráfaga FLP la conforman 33 posiciones de pulso, que simbolizan una palabra código de enlace de 16 bits entramada por 17 pulsos de sincronización, la ausencia de un pulso se interpreta como un cero binario.

Posteriormente de que un enlace a decodificado la palabra código de enlace de su socio, reconoce la recepción de la palabra actual enviando al menos 3 ráfagas de FLP con el conjunto de bits de reconocimiento.

1.1.7 El Modelo de Referencia OSI

A mediados de la década de los ochenta la motivación por los beneficios de compartir recursos e información aumentó el desarrollo de las redes significativamente, sin embargo, el uso de tecnologías entre sistemas de red patentados generó problemas de incompatibilidad, debido a que, los sistemas patentados son de uso y desarrollo exclusivo de quien los crea se volvió muy difícil y costosa la integración de redes.

Para solventar el problema producido por los diferentes esquemas propietarios, la Organización internacional de normalización (ISO, International Organization for Standardization), investiga sistemas de redes como TCP/IP (transfer control protocol), SNA (System Network Architecture), para producir un grupo de normas que permitan a las redes operar entre sí. En consecuencia, en 1984 se propone el **modelo de referencia OSI** (Open System Interconnection), esta norma dividía todo el proceso de envío y recepción de información en 7 capas que son:

Capa 7: capa de aplicación.
Capa 6: capa de presentación.
Capa 5: capa de sesión.
Capa 4: capa de transporte.
Capa 3: capa de red.
Capa 2: capa de enlace de datos.
Capa 1: capa física.[6]

---

[6] Cisco Systems, *Guía del primer año. CCNA® 1 y 2*. Madrid, Pearson Educación S.A., 3ra edición, 2004. Página 65.

Al segmentar todo el proceso de transporte por capas se logra simplificar el entendimiento y la complejidad, hoy en día el avance en el diseño de redes se debe a acuerdos sobre la funcionalidad de los componentes constitutivos implicados y estándares que nos proporcionan un marco de trabajo común para entender los procesos de interconexión de sistemas de información.

A medida que la información recorre las capas del modelo OSI los datos se dividen en segmentos llamados PDU (Protocol Data Unit), que contienen información de origen y destino para cada capa. Existen 2 tipos de PDU's: de control y de datos.

La **capa de aplicación** se relaciona directamente con el usuario, presta servicios de red, impresión de ficheros y no interactúa con ninguna otra capa. Aquí tienen lugar procedimientos para la recuperación de errores. Programas relacionados con esta capa son procesadores de texto, hojas de cálculo, HTTP, entre otros.

Una de las principales funciones de la **capa de presentación**, son los procesos de cifrado y descifrado, también, se verifica que la información que va a llegar a la capa de aplicación de otro sistema se va a poder visualizar correctamente. En esta capa se utilizan formatos comunes como JPEG, PICT, MIDI y MPEG.

En referencia a su nombre la **capa de sesión** administra, sincroniza y gestiona las sesiones entre dos host de comunicaciones, sirve de enlace para las capas de presentación y un eficiente transporte de los datos entre dos dispositivos que se comunican. Aunque no muy usual informa de problemas en las capas de sesión presentación y aplicación con la utilización de puntos de control (checkpoints).

En la **capa de transporte** la finalidad principal es proporcionar fiabilidad en el envío de la información esto se lo hace segmentando los datos (PDU) del host remitente y reordenando el flujo de datos en el host receptor para pasarlos a la capa de red.

El objetivo de la **capa de red** es asegurar que desde el origen al destino los datos lleguen correctamente. También, se lleva un control de congestión que impide la saturación de los procesos de red. Existen dispositivos conocidos como routers que simplifican el trabajo de envío. Sobre esta capa actúan los firewalls para eliminar direcciones MAC. En esta capa se realiza el direccionamiento de los datos y su

receptor IP final. En conclusión se puede decir que esta capa se ocupa del direccionamiento lógico.

La **capa de enlace de datos** se encarga del direccionamiento físico en lo que se refiere a la topología, acceso, distribución y control de flujo de los datos. La PDU de esta etapa se denomina trama.

Cuando nos encontramos en la **capa física** hablamos de las condiciones eléctricas, mecánicas, funcionales necesarias para efectuar la conexión y el envío de información a través de medios guiados (cable) o no-guiados (sin cable). Aquí, se definen el medio de transporte, los materiales, manejo de señales y la transmisión de bits.

En conclusión, la importancia del modelo de referencia aquí expuesto "reside en el hecho de que ha conseguido presentar una visión global y estructurada del problema de la interconexión entre sistemas informáticos"[7].

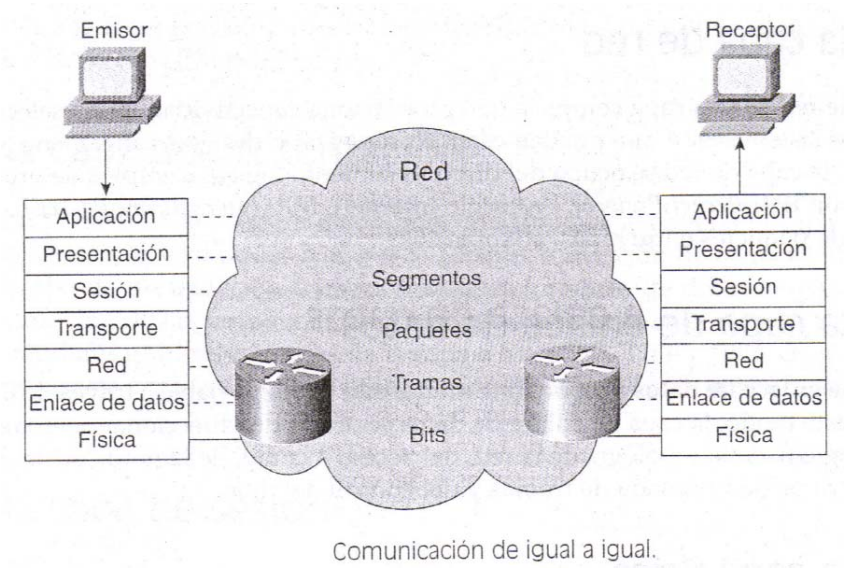


Gráfico 1. 5 Modelo de referencia OSI.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 68.

[7] Alabau A. y Riera J., *Teleinformática y Redes de Computadores*, Barcelona, Marcombo S.A., 2da. Edición, 1992, Página 33.

1.1.8 Topología de Redes LAN.

Cuando hablamos de topología nos referimos a la manera en la que están conectados los dispositivos que forman parte de una red, las rutas por las que la información va a circular[8]. Es muy importante el concepto de la estructura (topología), ya que influye en la transmisión y desenvolvimiento del sistema. Cuando nos referimos a la topología física nos enmarcamos en la distribución de los dispositivos en el sitio donde se encuentran las partes constitutivas de la red. Al indicar la topología lógica aludimos a la manera como los hosts se integran a los medios para enviar datos. Dentro de la topología física tenemos:

- **Bus**.- es una estructura lineal donde todos los terminales se conectan a un cable, al final del cable debe existir un terminador que impida que la señal rebote y pueda generar errores.
- **Anillo**.- en esta topología no existe un principio ni un fin, una de las ventajas es que no produce colisiones, además, los datos circulan por el medio hasta que la información encuentre su destino, si un terminal necesita enviar información solo se adiciona para que se propague hasta su destino. Existen dos tipos de disposiciones anillo simple y doble, la simple utiliza un cable por el cual los datos viajan en un sentido. En un anillo doble nos encontramos con dos anillos por los cuales los datos se desplazan en dos sentidos; una ventaja de una estructura de doble anillo es la tolerancia a fallos, esto se logra gracias a métodos de redundancia.
- **Estrella.-** es la estructura más usada en las redes LAN Ethernet, consiste en un dispositivo central que conecta a cada host con un cable, esto mejora el desenvolvimiento de la red ya que si una terminal falla no afecta a toda la infraestructura.
- **Estrella extendida.-** al ampliar la red de estrella adicionando dispositivos se obtiene una topología extendida.

---

[8] Cisco Systems. *Guía del primer año. CCNA® 1 y 2*. Madrid, Pearson Educación S.A., 3ra edición, 2004. Página 89.

- **Jerárquica.-** es semejante a una arquitectura de estrella extendida, pero difiere en que en vez de utilizar un dispositivo central, implementa un nodo del que parten ramas a otros nodos.
- **Malla.-** en malla existen dos disposiciones completa y parcial al hablar de la primera (completa) todos los host están conectados entre sí para provocar redundancia, sin embargo, la estructura del cableado es muy laboriosa y difícil. En malla parcial al menos uno de los host se conecta con varios nodos. La ventaja de esta topología es que si un camino falla, existen varias opciones para que la información llegue.

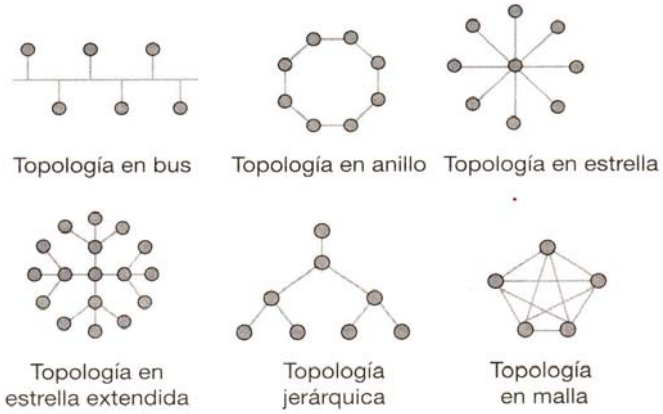


Gráfico 1. 6 Topologías físicas.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 89.

1.1.9 LAN Virtuales.

Ethernet a través de VLAN (Virtual LAN) permite asociar host de trabajo y servidores en agrupaciones lógicas[9] con la utilización de *switches* (dispositivo de enlace), de esta manera, la configuración VLAN funciona como varias LAN individuales.

[9] Cisco Systems. *Guía del segundo año. CCNA® 3 y 4*. Madrid, Pearson Educación S.A., 3ra edición, 2004. Página 282.

Con un *router* en una VLAN se proporciona aspectos como seguridad, administración del flujo de tráfico y filtrado de difusión, mientras que, la VLAN puede encargarse de la escalabilidad, seguridad y administración de la red. Una VLAN no se limita a un segmento físico o switch. El propósito principal de una LAN virtual es segmentar lógicamente a una red, basándose en la funcionalidad y no en su ubicación física o geográfica.

Existen LAN virtuales estáticas conocidas también como agrupación basada en el puerto; cuando un dispositivo se conecta a la red, admite automáticamente la VLAN del puerto. Otra configuración usada son las VLAN dinámicas que son generadas a través de software.

Una asignación dinámica acepta miembros en base a la dirección MAC de origen del dispositivo conectado.

1.2 Ethernet y Cableado.

Para transmitir la información por una red es necesario que las señales, la compartición de dispositivos, Internet o cualquier servicio, se propaguen por un medio, que puede ser el aire en el caso de ondas electromagnéticas o por un cable en el caso de impulsos eléctricos. Cada entorno de propagación tiene distintas propiedades que debemos conocer para mejorar el envío y recepción de información, por ende, se han creado métodos para que las señales que se emiten se acoplen al medio de transmisión.

A continuación, se estudiarán las normas para la transmisión de señales por cable.

1.2.1 Ethernet 802-3.

Es un estándar publicado por primera vez en 1985, en su primera difusión estableció las reglamentaciones para la norma CSMA/CD Carrier Sense Multiple Access with Collision Detection que se traduce como ***acceso múltiple con detección de portadora y detección de colisiones.*** Está conformado por cinco secciones:

La primera parte incluye los artículos del 1 al 20, los Anexos A hasta la H, y La parte 4a. Se incluyen las especificaciones de control de acceso al medio MAC para

operar a 10 Mb/s, y un marco de formato para interfaces usado para cualquier velocidad.

En la segunda sección encontramos las cláusulas 21 hasta la 33, también el Anexo 22a hasta el 33E. Además, incluye especificaciones para la administración y operación a velocidades de 100 Mb/s para múltiples protocolos y velocidades utilizando cable UTP.

Con la Sección tercera nos encontramos con los literales 34 hasta 43, los Anexos 36A hasta 43C. Incluye especificaciones a velocidades de 1000 Mb/s.

Sección cuarta incluye las cláusulas 44 hasta 53, Anexos 44A hasta el 50A. Incorpora especificaciones para 10 Gb/s de velocidad.

La última sección la integran las cláusulas 56 – 67, con Anexos 58A hasta 67A; define servicios y elementos de protocolo que permiten el intercambio de los formatos de trabajo entre estaciones y una subscripción de acceso a la red.

1.2.2 100-Mbps Ethernet.

Esta tecnología es conocida también como ***Fast Ethernet***, existen dos versiones conocidas que son ***100BaseTX y 100BaseFx.*** Estos tres modelos comparten características comunes, específicamente parámetros de temporización, el formato de la trama, fragmentos del proceso de transmisión.

A continuación expondremos algunas características del estándar mencionado, es decir, los elementos que constituyentes:

Parámetro	Valor
Tiempo de bit	10 nanosegundos
Tiempo de ranura	512 tiempos de bit
Espacio entre tramas	96 bits
Límite de intento de colisión	16
Límite de retardo de colisión	10
Tamaño de congestión de colisión	32 bits
Tamaño máximo de la trama sin etiquetar	1518 octetos
Tamaño mínimo de la trama	512 bits (64 octetos)

Tabla 1.1 Parámetros de una operación Ethernet a 100 Mbps.

Referencia: Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 303.

En la versión FastEthernet se experimenta un aumento en la velocidad y, como se envían más bits en menos intervalos de tiempo, el proceso de temporización debe ser meticuloso con el ancho de banda y el ruido (SNR, Signal-to-Noise Ratio). Para evitar el ruido y posibles errores, se emplea un código denominado nibbles (agrupaciones de 4 bits); los datos de 4 bits son transformados en muestras de 5 bits que contienen información de control, éste aumento de 4 a 5 bits implica transmisiones a 125 Mbps. Además, es fundamental comprobar el cable en frecuencias más altas para una transmisión efectiva.

En la versión 100BaseTX apareció una forma de auto negociación para obtener una mayor tasa de transmisión, la norma 802.3u – 1995. 100BaseTX utilizaba cable UTP de categoría 5. Posteriormente, en la norma 802.3x se implementó la transmisión dúplex con switches que controlaban el tráfico de red. La codificación utilizada por la versión 100BaseTX es la 4B/5B para después transformarlos a formato MLT-3

(Multilevel Transmit-Three Levels, Transmisión multinivel-tres niveles), éste método transforma los bits en una onda eléctrica, para después, codificarlos a una línea UTP de categoría 5.

100BaseFX es un modelo de fibra dirigido al empleo de backbone (ruta principal de una red) para ambientes con mucha interferencia, mencionada tecnología no se difundió por la introducción vertiginosa de las normas Gigabit Ethernet de cobre y fibra. La técnica 100BaseFX se basa en la codificación de datos 4B/5B y con codificación NRZI (nonreturn to zero inverted, código sin retorno a cero invertido) que consiste en que las señales conservan rangos de voltaje constantes sin transiciones en la señal, es decir, no vuelve al nivel cero.

1.2.3 1000-Mbps Ethernet.

Conocida como Gigabit –Ethernet (1000BaseX, ó IEEE 802.3z), se lograba enviar datos de 1 Giga dúplex sobre fibra óptica. Es diez veces más rápida que Fast Ethernet, lo que implica, exigencias extras como: tiempo para despachar los bits de un nanosegundo, temporización más minuciosa, frecuencias cercanas al ancho de banda y son muy dispuestas al ruido. Para aplacar las desventajas de transmitir a una velocidad elevada, se utiliza dos codificaciones: de código y de datos; la primera parte de la codificación es un método denominado ***8B1Q4 (8Bit – Quinary quarter)*** para la segunda parte se utiliza la codificación actual de la línea de cobre ***4D-PAM5 (4-dimensional 5 level pulse amplitude modulation)***, además, emplea codificación 8 bits a 10 bits con codificación en línea NRZ de luz sobre fibra óptica.

1.2.4 Normas de Cableado.

Las normas de cableado se aplican en lo que se denomina cableado estructurado, son prácticas que se aplican en arquitecturas de red para que un administrador de red u otros técnicos afines puedan interpretar fácilmente el esquema dispuesto. Con la implementación de un cableado efectivo se persigue una conectividad integral, es decir, que abarque a todos los sistemas y a las futuras tecnologías. Además, se debería prever futuros incrementos de la estructura (escalabilidad), al menos, para 10 años.

Existen 7 subsistemas de cableado estructurados:

1. Punto de demarcación.
2. Sala de telecomunicaciones.
3. Cableado backbone (cableado vertical).
4. Cableado de distribución (cableado horizontal).
5. Área de trabajo.
6. Sala de equipos.
7. Administración.

El ***punto de demarcación*** es el límite entre la infraestructura interna y externa. Existen normas que regulan los aspectos principales que debe cumplir un subsistema, estas normas, son establecidas por La Asociación de la Industria de las telecomunicaciones (TIA), junto con la Asociación de industrias electrónicas (EIA). En el caso del punto de demarcación la ***norma TIA/EIA-569-A*** especifica las condiciones del espacio; en áreas extensas (200 metros cuadrados) se aconseja lugar cerrado, también, utilizar madera contrachapada de 1metro cuadrado por cada área de 20 metros cuadrados de espacio de planta. Los espacios donde se establecerá el hardware de distribución deben estar con madera contrachapada ignífuga, o chapada con dos capas de pintura resistente al fuego y las cubiertas del equipo deben ser de color naranja, esto indica que es un punto de demarcación.

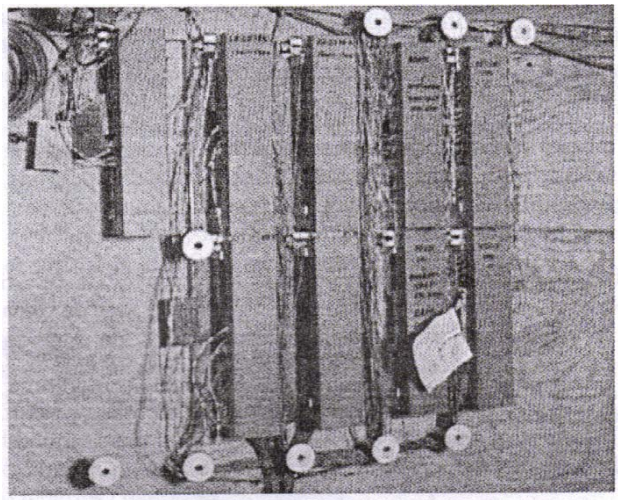
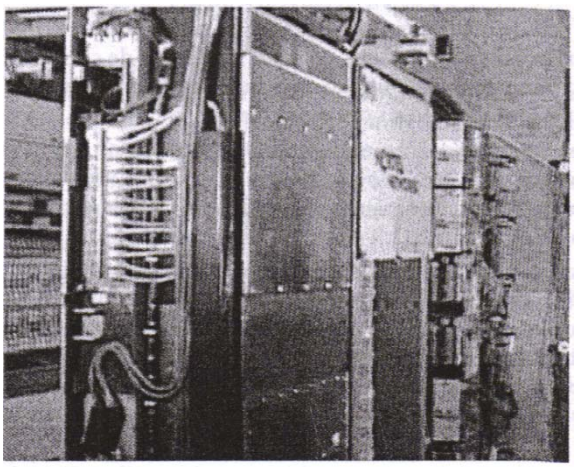


Gráfico 1. 7 Cableado Punto de demarcación.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 812.

En la ***sala de telecomunicaciones*** se encuentra el cuadro de distribución principal, los servidores, routers, switches y demás equipo relacionado. La norma correspondiente a la sala de telecomunicaciones es ***TIA/EIA-569A***. Un hub de cableado y un patch panel se pueden instalar en una pared con un soporte de pared bisagra dejando 48 cm para que el panel se abra fuera de la pared, un rack de distribución debe tener 1 metro mínimo por delante y detrás para poder trabajar o una cabina de equipo completo que necesita 76.2 cm de espacio libre por delante, estos dispositivos suelen medir 1.8 m de alto por 0.74 de ancho.



Recinto de telecomunicaciones.

Gráfico 1. 8 Cableado Sala de telecomunicaciones.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 813.

Para la conexión de cables desde la sala de telecomunicaciones hasta las ***áreas de trabajo*** se debe tomar en cuenta no rebasar los 90 metros (conexión permanente); cada estación (PC) debería tener mínimo dos cables uno para voz y otro para datos.

La ***ANSI/TIA/EIA-568-B*** menciona, que se puede poner una extensión de 5 metros para interconectar patchs panels y 5 metros de cable desde el final del cable en la pared del teléfono o la computadora a esto se le denomina ***canal horizontal***, de esta manera, se cumple los 100 metros que exige la norma (90 de conexión permanente y 10 de canal horizontal).

La conexión cruzada principal (MC, main cross-connect) es la sala de telecomunicaciones principal, la conexión cruzada horizontal (HC, horizontal cross-connect) suministra conexión entre los canales horizontales y el MC y el IC, la conexión cruzada intermedia (IC, intermédiate cross-connect) se refiere a las conexiones entre MC y HC

El cableado ***backbone*** es conocido también como cableado vertical, todas las conexiones entre MC, IC y otra sala de telecomunicaciones, es decir, incluye: conexiones MC a IC, IC a HC, conexiones entre salas de telecomunicaciones y el punto de demarcación y cableado entre edificios.

Entre las principales normas de cableado cabe destacar las siguientes:

TIA/EIA-568-A.- Norma de cableado para edificios comerciales.

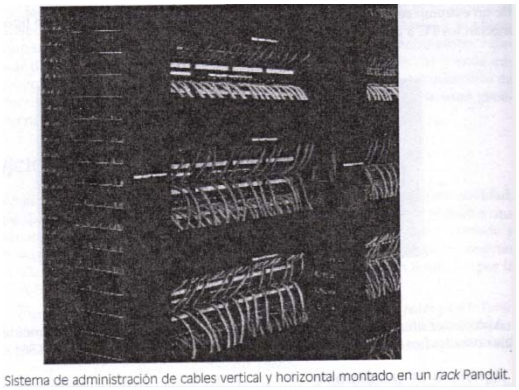
TIA/EIA-568-B.- Norma de cableado.

TIA/EIA-569-A.- Norma edificios comerciales caminos de telecomunicaciones y espacios.

TIA/EIA-570-A.- Norma de cableado para edificios residenciales y comerciales ligeros.

TIA/EIA-606.- Administración de infraestructura de telecomunicaciones de edificios comerciales.

TIA/EIA-607.- Requisitos de toma de tierra y límites de edificios comerciales para las telecomunicaciones.



Sistema de administración de cables vertical y horizontal montado en un *rack* Panduit.

Gráfico 1. 9 Cableado vertical y horizontal.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 818.

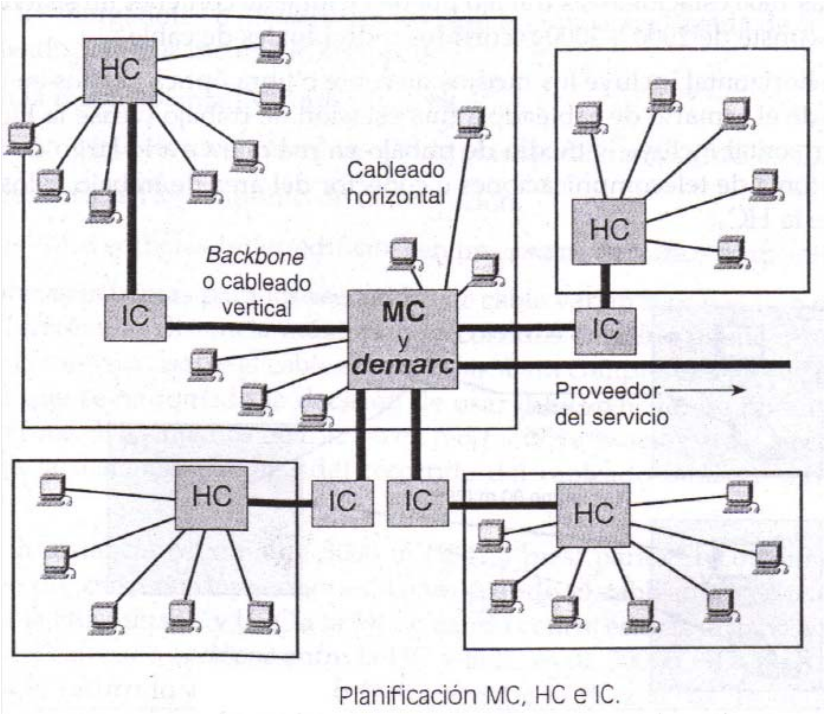


Gráfico 1. 10 Cableado vertical y horizontal.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 819.

1.3 Introducción a las redes WAN.

Enunciando un concepto "una WAN es una red de comunicación de datos que opera más allá de los límites geográficos de una LAN"[10].

Una red de área extendida ***(WAN, wide Area Network)*** permite transmitir datos en un espacio geográfico más amplio que una red de área local ***(LAN, Local Area Network)***. Generalmente, para acceder a un servicio de enlace de datos distante se contrata un proveedor, es decir, otra red WAN que permita la conexión y comunicación entre redes locales alejadas. Un proveedor WAN de enlace puede ser la red telefónica.

[10] Cisco Systems, Inc. Academia de Networking. *Guía del segundo año. CCNA® 3 y 4*. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 375.

Los equipos que se encuentran del lado de la red local se denominan equipo terminal del abonado ***(CPE, Customer Premises Equipment)*** y pueden ser propiedad del proveedor de enlace WAN o del arrendatario. Para enlazar los dispositivos CPE a la oficina central ***(CO, Central Office),*** se utiliza cableado de cobre o fibra, a esta conexión se conoce como "última milla" o bucle local. A través de un bucle local el abonado se conecta a una central particular, que a su vez se enlaza con una central regional, nacional o internacional, así, la información viaja grandes distancias.

Para que un bucle local pueda transmitir los datos necesita de dispositivos que acondicionen los datos; a los instrumentos que colocan datos en el bucle local se los conoce como equipo de terminación de circuito de datos o equipos de comunicación datos ***(DCE, Data Communication Equipment)***. Los equipos de una red local que enlazan los datos de los DCE se denominan equipo terminal de datos ***(DTE, Data Terminal Equipment)***.

Las señales que requieren ser enviadas desde una LAN a través de un proveedor de enlace WAN necesitan pasar a un equipo conocido como ruteador o router. El router cumple con la función de conectividad, rendimiento, control y administración de los recursos en una red. Para acondicionar las señales digitales, se necesita una unidad de servicio de canal ***(CSU, Channel Service Unit)*** y una unidad de servicio de datos ***(DSU, Data Service Unit)*** que se pueden encontrar incorporados en el router. Si las señales son analógicas se requiere de un módem; el módem superpone la señal digital sobre señales de voz analógicas por un proceso de demodulación. Si se utiliza una red digital de servicios integrados ***(RDSI, Integrated Services Digital Network)*** para comunicarse con el exterior, los equipos conectados al bus RDSI deben ser compatibles ya sea en el router si se trata de una red LAN/WAN o en la interfaz para conexiones directas de marcado.

El proceso de transporte requiere de una encapsulación de trama, este proceso se realiza en la capa de enlace de datos, el encapsular datos permite implementar controles. Para entramar los datos se utiliza un protocolo de capa 2 que debe ser configurado en el router dependiendo de la tecnología utilizada en la red WAN. El entramado se fundamenta en el control de enlace de datos de capa superior ***(HDLC)*** que es un estándar orientado al bit que encapsula los datos en enlaces de datos serie síncronos. El estándar permite un transporte seguro sobre medios que no lo son,

señalización y control de errores. Una trama siempre se envía al inicio y al final como una secuencia de 8 bits (01111110), debido a que una secuencia parecida se puede generar en el transporte de datos, el procedimiento inserta un cero en cada secuencia de cinco unos, los ceros sirven como marca (flag) para el próximo segmento.

En una trama encontramos siete campos: Flag, Dirección, Control, Control, Datos, FCS y Flag. No es necesario el campo dirección porque en enlaces WAN generalmente el enlace es punto a punto, en el campo de control se utiliza para conocer el tipo de trama. Existe un campo de secuencia de verificación de trama ***(FCS, Frame Check Sequence)*** que sirve para verificar la redundancia.

Para casos en los que se necesite una conexión de voz los enlaces WAN pueden establecerse como ***circuito conmutado*** utilizando líneas de voz en la red telefónica, o líneas de una red digital, una conexión se logra al activar los switches. Para mejorar el servicio las redes telefónicas ofrecen conexiones dedicadas o alquiladas con enlaces permanentes. Ejemplos de circuitos conmutados son la red telefónica conmutada pública ***(PSTN, Public Switched Telephone Network)***, la red digital integrada de acceso básico ***(RDSI BRI, Basic Rate Interface)*** y la red digital integrada de acceso principal ***(RDSI PRI, Primary Rate Interface)***.

El alto costo de implementación de un enlace conmutado, dio paso a la ***conmutación por paquetes***, que son redes conmutadas que envían los datos señalizados en celdas y aunque los retardos (latencia) y la fluctuación (jitter) son mayores, la tecnología actual permite el transporte adecuado de voz y video. Para el traslado de los datos es necesario definir una ruta, si la ruta se establece al encender el switch, se conoce como circuito virtual permanente ***(PVC, Permanent Virtual Circuit)***. Si el método se ejecuta a medida que se genera un requisito se conoce como circuito virtual conmutado ***(SVC, Switched Virtual Circuit)*** y si la ruta es solucionada por el switch para cada uno de los paquetes, se denomina sin conexión. El enlace necesita de un bucle local cercana al proveedor de servicio, es decir, ***(POP, Punto de Presencia)*** que es una líneal alquilada y dedicada. Frame Relay, X.25 y ATM utilizan conexiones de paquete conmutado.

Existe un método que utiliza un enlace de paquetes y circuitos (circuito conmutado); utilizando la red telefónica y reemplazando los micros teléfonos por módems es posible

enviar datos informáticos. En la central de la red telefónica la información compartirá varios canales por lo que es necesario tecnologías de multiplexión por división de tiempo ***(TDM, Time-División Multiplexing)***; al compartir un medio es necesario marcar o etiquetar los bits en celdas para evitar pérdidas en la entrega. Para determinar a donde se debe enlazar la información existen dos modos: con conexión o sin conexión, en el primer caso, los switches anticipan la ruta para un paquete que contiene un identificador de conexión de enlace de datos ***(DLCI, Data Link Connection Identifiers)***, la predeterminación se realiza consultando el identificador de tablas en los switches, si la ruta física se activa solo cuando circula un paquete se lo llama circuito virtual ***(VC, Virtual Circuit)***. Para métodos sin conexión los paquetes almacenan toda la información de direccionamiento en cada paquete.

1.3.1 Marcación Analógica.

Para una utilización de bajo volumen en la transmisión de información, la tecnología conmutada de acceso telefónico de voz (analógica) es una alternativa viable. La red necesita conectarse a través de un cable de cobre (bucle local); además, el bucle local requiere de un módem para modular (codificar) los bits de datos en señales analógicas y desmodular señales analógicas en datos binarios.

El bucle local determina la velocidad de enlace con la red telefónica conmutada pública que puede ser de unos 33 kbps o 56 kbps si se utiliza una conexión digital.

La sistematización de esta tecnología es conveniente para empresas pequeñas con requerimientos de transferencia de archivos y correo electrónico, los clientes pueden obtener descuentos en las tarifas en horas en las que la red no esté saturada o si la distancia entre los terminales es corta.

El mérito de los modems y de las líneas analógicas es el bajo importe de su instalación, sin embargo, la baja tasa de transferencia y retardo en la conexión son inconvenientes para un tráfico de voz o video.

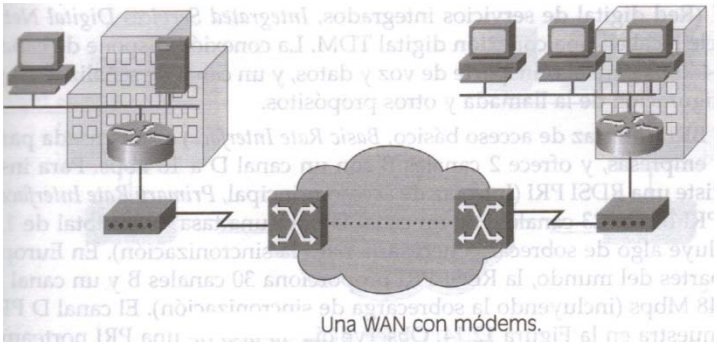


Gráfico 1. 11 Tecnologías WAN modem.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 387.

1.3.2 RDSI.

Las centrales de red telefónica conmutada han evolucionado desde señales multiplexadas y hoy en día pueden transportar señales digitales, luego se pretenderá que el bucle local envíe señales digitales producidas de enlaces conmutados de alta capacidad.

La red digital de servicios integrados ***(ISDN, Integrated Services Digital Network)*** transforma el bucle local en una conexión digital TDM. Por medio de canales principales B de 64 kbps se transporta voz y datos; con un canal delta o D utilizado para señalización es posible configurar llamadas.

La interfaz RDSI de acceso básico ***(BRI, Basic Rate Interface)*** está orientada para entornos reducidos como casas o empresas pequeñas pues, posee 2 canales B con un canal D a 16 kbps. Para ambientes más amplios se emplea interfaz RDSI de acceso principal ***(PRI, Primary Rate Interface)***. En Estados Unidos el servicio PRI presenta 23 canales B y un canal D con tasas de 1.544 Mbps y concuerda con la conexión T1. En Europa y Australia se ofrecen 30 canales B con uno D que contabilizan 2.048 Mbps y concuerda con la conexión E1. 64 kbps le corresponden al canal D PRI.

Algunos proveedores utilizan el canal D BRI para enviar información a 9.6 kbps con enlaces X.25 subvalorando el canal.

Para ambientes WAN geográficamente cortos la RDSI BRI ofrece tiempos de conexión menores al segundo; empleando un canal B a 64 kbps se supera a los enlaces analógicos y para casos donde se necesite mayor capacidad se puede habilitar un segundo canal para obtener 128 kbps más , si bien excelente para el transporte de voz, pero no conveniente para video.

Otro uso de RDSI es para incrementar el volumen de una conexión de línea alquilada previamente establecida para sobrepasar picos de uso.

Con una implementación de interfaz RDSI de acceso principal se pueden establecer muchos canales B entre 2 puntos terminales, posibilitando video conferencia pero a largas distancias producen costos altos.

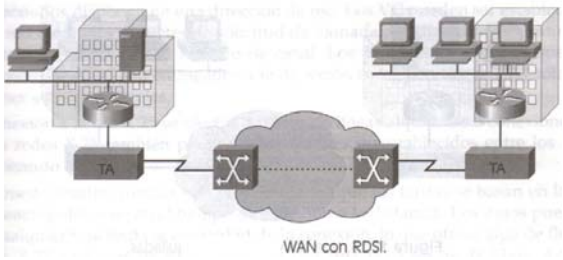


Gráfico 1. 12 Tecnologías WAN RDSI.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 389.

1.3.3 Línea Alquilada.

Las líneas alquiladas pueden ofrecer hasta 2.5 Gbps para conexiones dedicadas; una conexión punto a punto posee una ruta anticipada atravesando una red portadora desde una ubicación local a una remota; una línea alquilada es un enlace punto a punto arrendado a un cliente. Para establecer los precios los propietarios basan el coste de acuerdo al ancho de banda y a la distancia que se debe recorrer para conectar dos puntos. Usualmente éste tipo de conexiones son más caras que las

conexiones punto a punto compartidas como Frame Relay; en una línea alquilada no se genera retardos ni fluctuaciones de fase y se dispone recursos en todo momento.

Para la instalación se requiere de un puerto serie de router, además, de una unidad de canal de servicio, de datos ***(CSU / DSU, Chanell Service Unit / Data Service Unit)*** y el circuito actual desde el proveedor de servicio. El hecho de tener una capacidad fija puede ser una desventaja porque el tráfico en una red WAN es variable y generalmente no se obtiene el ancho de banda necesario, otro inconveniente es que cada punto final necesita de una interfaz en el router, lo que significa que la implementación es cara en un hub de estrella multipunto, sin embargo, multiplexado el enlace los routers pueden ahorrar interfaces. También se puede conectar ramas individuales a una red de paquete conmutado.

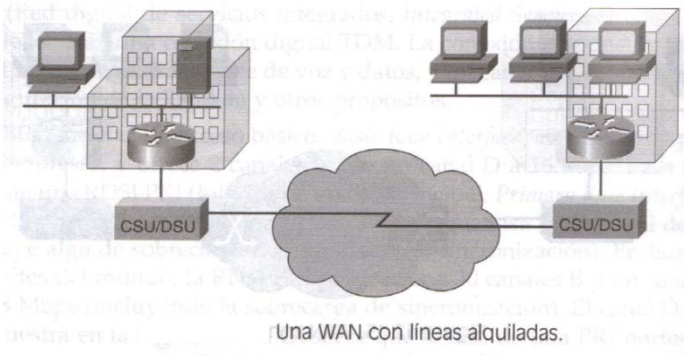


Gráfico 1. 13 Tecnologías WAN Líneas alquiladas.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 390.

1.3.4 X.25.

Como una solución para abaratar costos aparece la tecnología X.25 que son redes de paquete conmutado, es decir, líneas compartidas con una tasa baja de transporte de bits con capacidad variable.

Para establecer el enlace la red se establece un circuito virtual enviando una solicitud a la dirección de recepción y para reconocer la ruta virtual se utiliza un número de canal.

X.25 puede funcionar en un enlace alquilado, conexiones de marcado o a través de canales anticipados (circuitos permanentes).

El precio de los importes se fundamentan en la transferencia de los datos, sin tomar en cuenta el tiempo de conexión ni la distancia y la transferencia de los datos se puede realizar a cualquier tasa dependiendo del enlace que oscila los 48 Kbps Una desventaja de X.25 son los retardos (latencia) y fluctuación de fase (jitter).

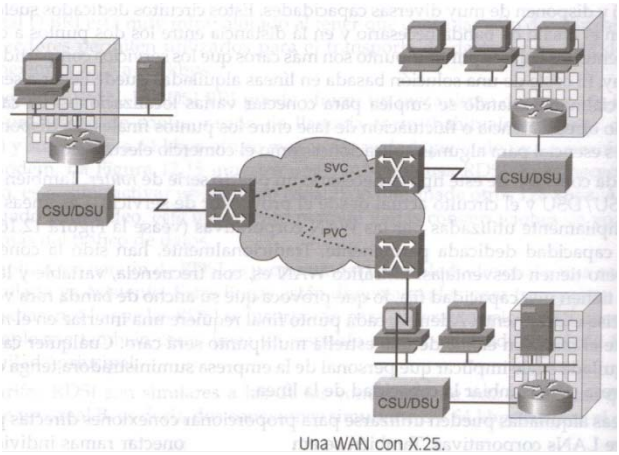


Gráfico 1. 14 Tecnologías WAN X.25.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 390.

1.3.5 Frame Relay.

Con el incremento del flujo de la información se vio la necesidad de una red con un ancho de banda mayor y con retardos menores. Frame Relay se basa en la conmutación de paquetes similar a X.25, con la diferencia de que se puede ofrecer hasta 4Mbps o más en la transferencia.

Frame Relay funciona con un estándar sencillo al enlazar los datos sin implementar el control de flujo o de errores, reduciendo los retardos. Además, la configuración de los switches intermedios reduce la fluctuación de fase.

Una gran parte de los enlaces FR funcionan estableciendo circuitos permanentes y la conexión con el extremo de la red es una línea alquilada. El canal D RDSI se emplea

para establecer un circuito virtual conmutado (SVC) en un canal B. El puerto de conexión en el extremo de la red, y la velocidad de información suscrita ***(CIR, Commited Information Rate)*** determina los importes en Frame Relay.

Conectividad permanente, transmisión de voz, ancho de banda medio, son algunos de los beneficios de esta tecnología, también, es idóneo para interconectar LANs empresariales. El router se configura con una sola interfaz y un bucle local al extremo de la red FR ofrece conexiones mejores y baratas entre LANs dispersas.

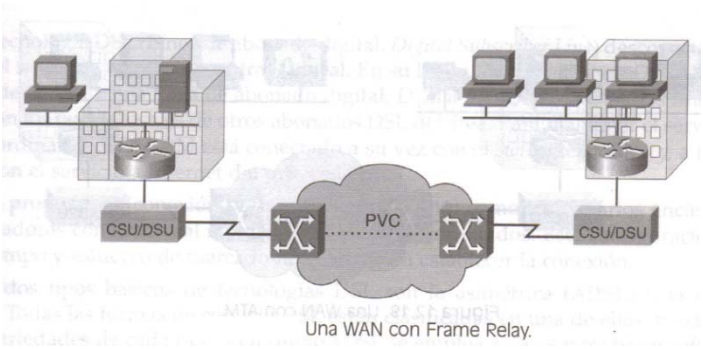


Gráfico 1. 15 Tecnologías WAN Frame Relay.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 391.

1.3.6 ATM.

Modo de transferencia asíncrono ***(ATM, Asynchronous Transfer Mode)*** es una red compartida permanente que aparece para ofrecer mejoras como menor latencia, menor fluctuación de fase y aumento en el ancho de banda llegando a 155 Mbps. ATM es una solución para aplicaciones en las que se necesita una transmisión sin retardos como video o voz, los datos se pueden enviar por redes privadas o públicas por medio de celdas de 53 bytes de longitud que se dividen en una cabecera de 5 bytes con 48 bytes para datos. Las celdas ATM se implementaron con 5 bytes de sobrecarga y cuando los paquetes están divididos, la sobrecarga aumenta por lo que la estructura ATM requiere de un ancho de banda mayor que FR o X.25 para trasladar la misma cantidad de información.

Con ATM se pueden activar circuitos virtuales permanentes o conmutados, siendo los primeros los más usuales.

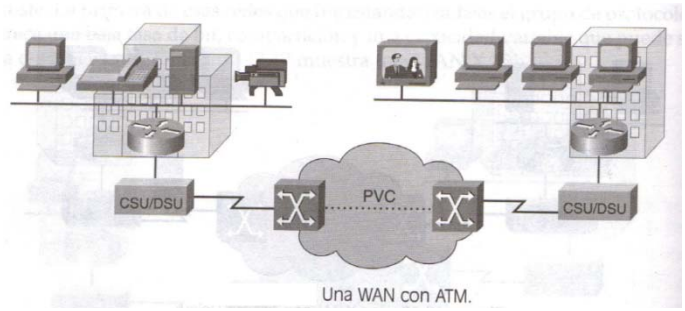


Gráfico 1. 16 Tecnologías WAN ATM.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 392.

1.3.7 DSL.

La utilización de la red telefónica limita el ancho de banda, es por eso que, la tecnología de línea de abonado digital ***(DSL, Digital Subscriber Line)*** desconecta el bucle local propio y de otros abonados del switch en la oficina central (CO) y se conecta a un multiplexor de acceso a una línea de abonado digital ***(DSLAM, Digital Subscriber Line Access Multiplexor)*** que se encuentra enlazado con el switch del servicio telefónico para llamadas telefónicas, y a su vez con ATM para acceder al proveedor de Internet.

La conexión es permanente utilizando DSL, es decir, al momento en que el equipo con un modem se enciende, se establece la conexión, de esta manera se elimina el tiempo de conexión o de marcado.

Existen dos modalidades de DSL, asimétrica o simétrica. Para un DSL asimétrico la velocidad con los que los datos se descargan desde el proveedor es mayor, mientras que para un DSL simétrico tanto la velocidad de descarga (hacia el usuario) como la

velocidad de envío (hacia el proveedor) son iguales. Se suele usar la denominación xDSL indistintamente para cualquier forma de DSL.

El ancho de banda depende de la longitud del bucle local; lo óptimo es 5.5 Kilómetros.

Para que un abonado pueda conectarse a una red necesita de un proveedor de servicio de Internet (ISP) para luego establecer una configuración IP, este hecho, conlleva a inseguridades en la red.

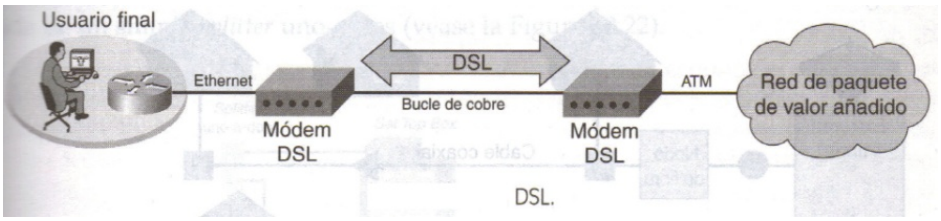


Gráfico 1. 17 Tecnologías WAN DSL.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 393.

1.3.8 Modem por Cable.

Actualmente el uso de redes de televisión por cable ha experimentado un incremento, estas redes permiten el transporte bi-direccional de alta velocidad. Las conexiones utilizan cable coaxial que ofrece un mayor ancho de banda aproximadamente 6.5 veces más que la tecnología T1 y lo que tomaría 2 minutos con una arquitectura RDSI BRI, por cable podemos realizar descargas en 2 segundos.

La implementación de esta arquitectura es simple y de bajo costo, además, ofrece un enlace permanente con velocidades superiores a una línea alquilada, sin embargo, el hecho de estar siempre con conexión genera vulnerabilidades que pueden ser aprovechadas por piratas informáticos. Una medida para controlar el tráfico entrante es la implementación de ***firewall.***

La diferencia entre un módem por cable es de 500 veces más rápido que un módem a 56 Kbps, es decir, entre 30 y 40 Mbps en un canal de 6MHz.

Utilizando un ***splitter*** uno a dos el usuario puede ver la televisión y a la vez navegar por Internet siempre conectándose con el proveedor ISP. Para conectarse a una red empresarial se aplica programas basados en TCP/IP como Telnet. Una limitación de esta tecnología es que varios usuarios comparten el ancho de banda del cable, sí existen muchos abonados, el ancho de banda se reduce considerablemente. El riesgo de intrusiones incluye a los abonados que comparten el cable. Una solución corporativa es la implementación de una red virtual privada (VPN).

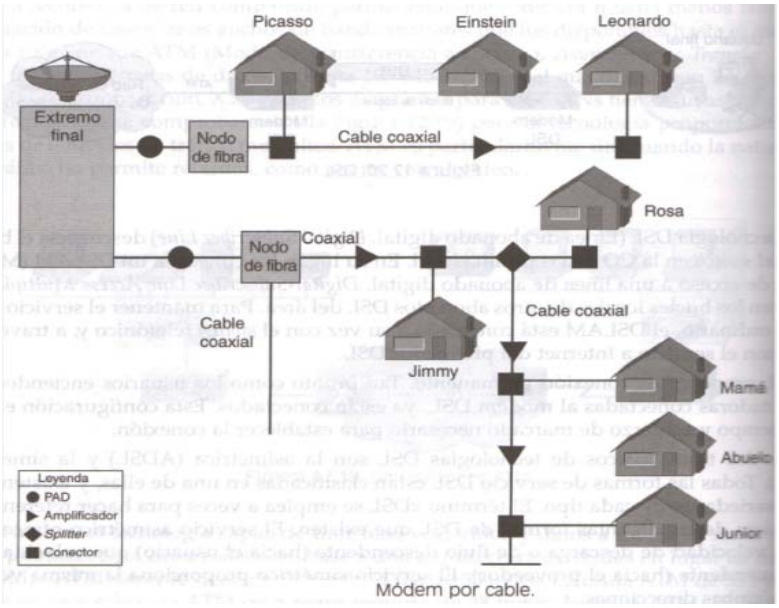


Gráfico 1. 18 Tecnologías WAN Módem por cable.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 394.

1.4 Requerimientos de Tráfico.

En lo que viene del capítulo expondremos los conceptos de ancho de banda, latencia y fluctuación de fase; términos necesarios para comprender el movimiento de los datos dentro de una infraestructura de red. Cada red es diseñada para brindar servicios, dependiendo de los servicios, se debe escoger el medio de transmisión y la tecnología.

1.4.1 Ancho de Banda.

La cantidad de información que se puede enviar a través de una red en un intervalo de tiempo denominamos ancho de banda, dependiendo de factores físicos y de la tecnología empleada en una red se define la tasa de transferencia. Un agente físico es el cableado utilizado, este puede ser, de cobre UTP, líneas telefónicas, frecuencias. La fibra óptica nos provee de un medio ilimitado, sin embargo, actualmente no existe la tecnología que pueda aprovechar mencionada característica. Diferentes tecnologías ofrecen distintos anchos de banda DSL, Frame Relay, T1, E1.

El ancho de banda para redes WAN generalmente lo provee una empresa especializada en el abastecimiento de Internet.

Para evaluar el rendimiento de una red, mejorar una red o diseñar una, es necesario tomar en cuenta el ancho de banda en base a las demandas de los usuarios.

La velocidad de transporte de datos por una red se expresa en bits por segundos ***(bps)***, es así, que podemos hablar de kilobits ***(kbps, 1000 bps)***, megabits ***(Mbps, 1000kbps)*** o gigabits ***(Gbps, 1000Mbps)***. Usualmente se puede transmitir y recibir al mismo tiempo (transmisión dúplex), es decir, si hablamos de una velocidad de 100kbps en realidad decimos 200kbps, 100kbps para transmitir y la misma cantidad para recibir.

Medio de transmisión	Ancho de banda máximo teórico	Distancia física máxima (metros)
Cable coaxial de 50 ohmios (Ethernet 10Base2, ThinNet)	10 Mbps	185 m
Cable coaxial de 50 ohmios (Ethernet 10Base5, ThickNet)	10 Mbps	500 m
Cable UTP de categoría 5 (Ethernet 10Base-T)	10 Mbps	100 m
Cable UTP de categoría 5	100 Mbps	100 m

(Ethernet 100Base-TX)		
Cable UTP de categoría 5 (Ethernet 1000Base-TX)	1000 Mbps	100 m
Fibra óptica multimodo (62.5/125 μm) (Ethernet 100BASE-FX)	100 Mbps	2000 m
Fibra óptica multimodo (62.5/125 μm) (Ethernet 1000BASE-SX)	1000 Mbps	220 m
Fibra óptica multimodo (50/125 μm) (Ethernet 1000BASE-SX)	1000 Mbps	550 m
Fibra óptica multimodo (9/125 μm) (Ethernet 1000BASE-LX)	1000 Mbps	5000 m

Tabla 1. 2 Limitaciones de longitud y anchos de banda máximos.

Referencia: Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, páginas 57-58.

Servicio WAN	Usuario típico	Ancho de banda
Módem	Particulares	56 kbps = 0.056 Mbps
ADSL	Particulares, tele trabajadores y pequeñas empresas	128 kbps a 6.1 Mbps = 0.128 Mbps a 6.1 Mbps

RDSI	Tele trabajadores y pequeñas empresas	128 kbps = 0.128 Mbps
Frame Relay	Pequeñas instituciones (escuelas) y empresas de tamaño medio	56 kbps a 44,736 Mbps (EE.UU.) o 34.368 Mbps (Europa) = 0.056 Mbps a 44.736 Mbps (EE.UU.) 0 34.368 Mbps (Europa)
T1	Grandes entidades	1.544 Mbps
T3	Grades entidades	44.736 Mbps
STS-1 (OC-1)	Compañías telefónicas; backbones de compañías de datos	51.840 Mbps
STS-3 (OC-3)	Compañías telefónicas; backbones de compañías de datos	155.251 Mbps
STS-48 (OC-48)	Compañías telefónicas; backbones de compañías de datos	2.488 Mbps

Tabla 1. 3 Servicios WAN más comunes y el ancho de banda asociado a cada uno.

Referencia: Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, páginas 57-58.

1.4.2 Latencia.

Cuando hablamos de latencia nos referimos a la demora de cada modo de conmutación, y esto se relaciona con la manera en la que envía el switch los paquetes. Una latencia baja corresponde a un rápido traslado de las tramas.

Otra forma de definir la latencia es en términos de “la suma de retardos temporales dentro de una red”[11].

Los modos de conmutación de un switch pueden ser de: almacenamiento y envío ***(store and forward),*** por método de corte ***(cut-through),*** liberación de fragmentos ***(fragment free)*** y envío rápido ***(fast forward)***; cada uno se diferencia por la decisión de conmutar la trama que ingresa al dispositivo. Debe tomarse en cuenta también el tiempo en que los equipos toman decisiones de envío y filtrado.

Es importante poner hincapié en la latencia porque hablamos de tasas de transferencia de 10 Mbps (1 bit por 1 diezmillonésima parte del segundo), 100 Mbps (1 bit por 1 cienmillonésima parte del segundo) o 1 Gbps (1 bit por 1 milmillonésima parte del segundo) por eso cada nanosegundo cuenta.

1.4.3 Fluctuación de Fase.

Durante el envío de paquetes se genera un retraso en la llegada de los mismos este retraso se denomina ***fluctuación de fase***. Cada paquete debe llegar en un mismo intervalo de tiempo, cuando existe este retraso, es necesario reunir los paquetes y retenerlos un intervalo de tiempo prudencial para que aquellos que están retardados lleguen a tiempo para ser enviados en el orden correcto. Es necesario implementar un buffer de fluctuación de fase que disfraza la demora entre los paquetes que llegan, un buffer puede ser estático o dinámico, recomendándose utilizar el segundo para redes con tráfico de voz.

1.4.4 Voz, Datos Cliente / Servidor, Mensajería, Videoconferencia.

El sistema Cliente / Servidor se refiere a que el servidor (una máquina con mayores características que las de su entorno) distribuye las tareas que ha procesado y las reparte en múltiples computadores conectados a él. En un ambiente cliente / servidor los dos se dividen o reparten el procesamiento de las tareas.

---

[11] Wikipedia, *Latencia,* Internet http://es.wikipedia.org/wiki/Latencia. Acceso: 07/diciembre/2011.

Internet es un ejemplo de una relación cliente servidor en la que el usuario manipula datos a nivel de presentación, edición, entradas y diseño. A través de un navegador se envían solicitudes a los servidores web, el mismo que responde proporcionando servicios http o World Wide Web.

El crecimiento de la red World Wide Web (www) ha incrementado aplicaciones que usan multidifusiones IP, servicios como transporte de voz, videoconferencia, mensajería y streaming pueden ser enviados por una misma red de datos. Utilizando un solo medio se consigue optimización, facilidad en la administración, mejor ancho de banda y utilización de una misma infraestructura. Actualmente la tendencia a compartir una misma red para distintas aplicaciones se denomina ***redes convergentes***. Para una red convergente el uso del protocolo IP posibilita disminuir el número de instalaciones WAN, el ancho de banda se puede aumentar paulatinamente y dividirse entre las aplicaciones existentes, además, cuando no se transmite voz o video el ancho de banda puede ser utilizado para el envío de datos.

1.5 Estándares y Protocolos

Con el auge de las redes de computadoras, aparecieron muchas empresas que proporcionaban servicios similares de compartición de recursos y distribución de servicios. Cada fabricante tenía su propia tecnología propietaria, restringiendo la comunicación; por ejemplo, en una misma empresa con 2 sucursales diferentes, se debía tener los mismos equipos con la misma tecnología para poder establecer una comunicación bidireccional. Para solventar incompatibilidades entre diferentes proveedores se crearon estándares o acuerdos de fabricación. Seguidamente, expondremos los más conocidos protocolos utilizados en las infraestructuras de red.

1.5.1 Protocolo IP.

El ***TCP/IP Transmission control protocol/Internet Protocol*** o Protocolo para el control de la transmisión/Protocolo Internet tuvo su origen en el Departamento de Defensa de los Estados Unidos, el objetivo principal era transmitir información a través de una red sin importar las condiciones adversas de algún nodo. “Es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos,

incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN)"[12]

TCP/IP fue diseñado en cuatro capas aplicación, transporte, Internet y de acceso.

La ***capa de aplicación*** maneja protocolos de alto nivel en lo que se refiere a transferencia de archivos, e-mail, correo electrónico, administración de redes, administración de nombres, además, su función es de empaquetar la información para la capa de transporte.

Al transferir archivos se opera con varios protocolos, uno de ellos es el protocolo de transferencia de hipertexto ***(HTTP, Hypertext Transfer Protocol)***, que enmarca la configuración y el modo de transferir los mensajes en la World Wide Web (red de Internet); también, permite interpretar los comandos para que los servidores y navegadores realicen las tareas ingresadas. Protocolo trivial de transferencia de archivos ***(TFTP, Trivial File Transfer Protocol)***, es otra función de transferencia que utiliza el Protocolo de datagrama de usuario (UDP, User Datagram Protocol) para el envío de archivos sin conexión entre sistemas TFTP. El protocolo de transferencia de archivos ***(FTP, File Transfer Protocol)*** es orientado a la conexión entre sistemas FTP, permite transferencia bidireccional de archivos binarios y ASCII. El sistema de archivos de red ***(NFS, Network File System)*** permite el acceso remoto a archivos en una red. Protocolo Simple de transferencia de correo ***(SMTP, Simple Mail Transfer Protocol)*** tiene como tarea principal la transferencia del correo en una red.

Otro servicio de la capa de aplicación es la opción de acceder a una computadora desde una ubicación distante, a esto se conoce como acceder remotamente o ***emulación de terminal (Telnet)***. También, encontramos un protocolo simple de administración de redes ***(SNMP, Simple Network Management Protocol)*** que brinda opciones de configuración, seguridad, estadísticas en una red.

---

[12] Wikipedia, *Familia de protocolos de Internet,* Internet http://es.wikipedia.org/wiki/Latencia. Acceso: 07/diciembre/2011.

Un sistema de denominación de dominio ***(DNS, Domain Name System)*** transforma los nombres de dominio en direcciones IP; este sistema actúa igualmente en la capa de aplicación.

En la ***capa de transporte*** toma importancia el envío y la recepción de la información; y esto se logra al dividir y reordenar los datos de un datagrama de usuario (UDP). Se genera un control de extremo a extremo utilizando números de secuencia y acuses de recibo. Algunas, de las utilidades de esta capa es segmentar y enviar los datos desde un host emisor a un host receptor, ejecución de tareas para asegurar la conexión extremo a extremo, flujo de control (utilizando ventanas deslizantes).

Para la ***capa de internet*** la función principal es fijar y delimitar una ruta de direccionamiento para trasladar paquetes de información utilizando el protocolo adecuado, es en esta capa donde se establece la mejor ruta de destino. Se trabaja con los protocolos:

IP para establecer una ruta para los paquetes de datos, sin tomar en cuenta el contenido de cada paquete.

Protocolo de mensajes de control en Internet ***(ICMP, Internet Control Protocol)*** para manejar adecuadamente servicios de mensajería.

Protocolo de resolución de direcciones ***(ARP, Address Resolution Protocol)*** que asigna direcciones MAC cuando se sabe las direccionesIP.

Protocolo de resolución inversa de direcciones ***(RARP, Reverse Address Resolution Protocol)*** que determina la dirección IP cuando se identifican las direcciones MAC.

En la ***capa de acceso a red*** se pone énfasis en la conexión física de los datos, es decir, que el envío de los paquetes contenga la información necesaria como controladores, direcciones IP físicas. Detalles que dependen de la tecnología que se utilice por ejemplo Ethernet, Fast Ethernet, Proxy ARP, RARP.

1.5.2 Protocolo de Mensajes de Control en Internet. (ICMP).

Sirve para informar de errores, excepciones y mensajes informativos para algunos programas como el uso de ping dentro del protocolo IP.

La entrega de mensajes ICMP se hace a través del protocolo IP. En la capa de red se encapsulan los mensajes en datagramas. Se utiliza el mismo proceso de encapsulación IP, es decir, los mensajes de error también están sujetos a los mismos fallos que los datos.

ICMP no corrige errores encontrados solo informa de ellos.

ICMP se describe en RFC 792 STD 5 como parte de la estructura IP. Los principales mensajes que se pueden producir están relacionados con un ***destino inalcanzable*** de host o de una red, ***protocolo o puerto desconocido*** y la necesidad de ***fragmentar*** (indicador DF activado). Además, avisos de tiempo excedido (TTL) y de procesamiento de paquetes por problemas de encapsulamiento son los principales en ICMP.

Para corregir algunos de los errores se observan mensajes para control de flujo cuando un router está con sobrecarga y re-direccionamiento de un router a otro.

Para solicitudes de información se utiliza ecos (ping), respuestas a marca de hora (tiempo de procesamiento), solicitud y repuesta de máscara de dirección.

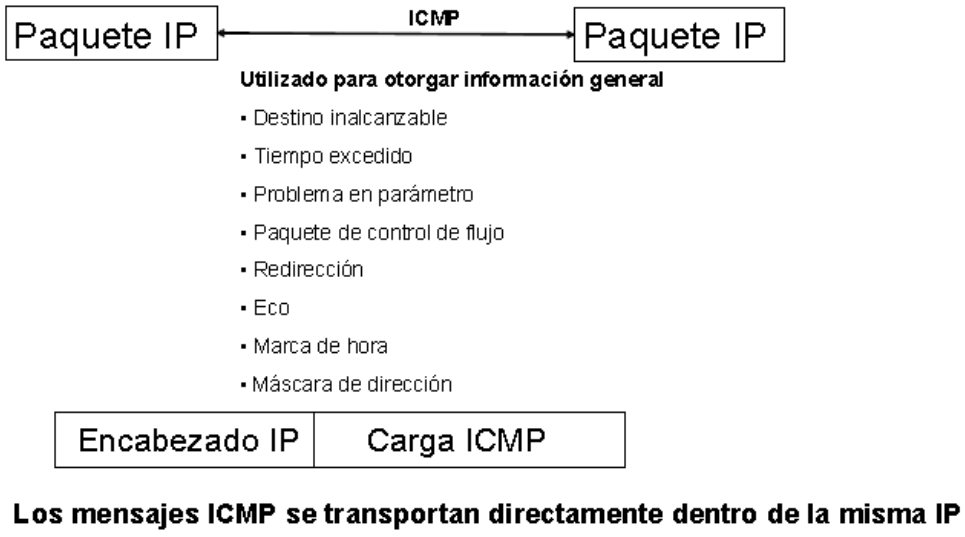
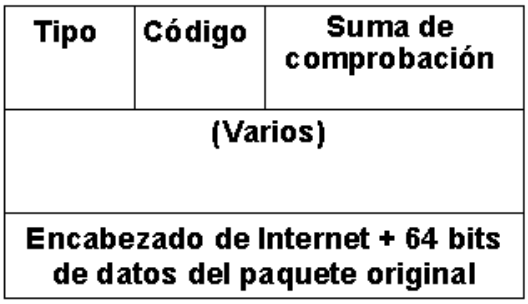


Gráfico 1. 19 Protocolo ICMP.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 6, página 128.

Formato de mensaje ICMP de 12 bytes



Formato general para mensajes ICMP de "error"

Gráfico 1. 20 Protocolo ICMP formato.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 6, página 129.

El formato de mensajes ICMP consiste de 12 bytes los 4 primeros sirven para consulta y error. En el campo ***tipo*** se almacenan valores que corresponden al tipo de mensaje, por ejemplo:

Respuesta de eco (0).

Destino inalcanzable (3).

Control de flujo (4).

Redirección (5).

Eco (8).

Tiempo excedido (11).

Problemas en parámetros (12).

Marca de hora (13).

Respuesta a marca de hora (14).

Solicitud de máscara de dirección (18).

Respuesta a máscara de dirección (19).

En el campo código se almacena información complementaria al campo tipo, por ejemplo, en el mensaje tiempo excedido puede tomar un valor (0) si fue excedido o (1) si expiró el temporizador.

El formato contiene una suma de comprobación parecida a la que se utiliza en el protocolo de Internet (IP).

Los 4 bytes siguientes se utilizan en casos específicos para alojar información variada, en algunos mensajes de error este campo se completa sin información y en otros como, por ejemplo, ***problema en parámetro*** se almacena un puntero en el primer byte que se direcciona al byte donde se registro el problema y en mensajes de ***re-direccionamiento*** se escribe la dirección del router futuro de destino.

Finalmente, el campo final contiene el mensaje IP con 64 bits del paquete original o carga útil, ésta información es procesada por el host de destino para reconstruir la información recibida.

1.5.3 Protocolo de Resolución de Direcciones (ARP).

Las condiciones primordiales antes de que se realice un proceso de envío de datos es conocer las direcciones IP y MAC, sí una máquina no encuentra la dirección MAC de destino, transmite por toda la red una petición denominada petición ARP; esta petición se propaga a través de una dirección de difusión, es decir, una dirección exclusiva para que todos los host puedan verificar si la dirección MAC que se propaga le corresponde. Si un host identifica la petición éste, envía su dirección MAC y establece la conexión con el origen que actualiza su tabla ARP. Una solicitud ARP contiene una cabecera de trama y el mensaje ARP; cuando los datos llegan al destino se examina la cabecera MAC en la capa de enlace de datos y se transfiere los datos a la capa de red en donde las direcciones IP de origen y destino coinciden, entonces transmite los datos a la capa de transporte. Se repite el procedimiento hasta finalizar el envío de la información.

1.5.4 Protocolo de Resolución Inversa de Direcciones (RARP).

El enlace entre las direcciones IP y las direcciones MAC se produce gracias al protocolo de resolución inversa de direcciones (RARP). Los dispositivos que funcionan con protocolo RARP necesitan de un servidor RARP para procesar las solicitudes. Este protocolo es importante cuando un host de origen no conoce su dirección IP en la tabla ARP, es así, que a través de una dirección de difusión se envía a toda la red una solicitud RARP.

La estructura de un mensaje ARP es similar a una de RARP, su diferencia radica en las cabeceras MAC y el código de operación, además, contiene un formato para almacenar las direcciones MAC de origen y destino, en el campo de la dirección IP de origen está vacío.

Una estructura de cabecera de un mensaje ARP/RARP se compone de varias partes:

Tipo de hardware.

Tipo de protocolo de alto nivel proporcionado por el origen.

LongH. Longitud de la dirección hardware.

LongP. Longitud de la dirección de protocolo.

Funcionamiento. Puede tomar los valores 1 – solicitud ARP. 2 – respuesta ARP. 3 – petición RARP. 4 – petición RARP. 5 – petición dinámica RARP. 6 – respuesta dinámica RARP. 7 – error dinámico RARP. 8 – petición InARP. 9 –respuesta InRARP.

Dirección hardware del emisor (HA).

Dirección de protocolo del emisor (PA).

Dirección hardware de destino (HA).

Dirección de protocolo de destino (PA).

1.5.5 Normas WAN.

Las normas utilizadas en las redes WAN se enfocan en las dos capas inferiores del modelo OSI, es decir, capa física y enlace de datos. Además, los estándares también regulan el direccionamiento, el flujo de datos y la encapsulación.

En la capa física se definen como deben ser las conexiones eléctricas, mecanismos de funcionamiento y operación. El equipo a enlazar a la WAN (router) se denomina como DTE, entretanto, el dispositivo en el otro extremo de la conexión quien provee la interfaz con el ISP, se conoce como DCE.

1.5.6 EIA / TIA 232.

Existen organizaciones autorizadas que establecen las normas una de ella es la Asociación de Industrias Electrónicas ***(EIA, Electronic Industries Association)***, Asociación de la Industria de las Telecomunicaciones ***(TIA, Telecommunications Industry Association)*** otra es la Unión Internacional de las Telecomunicaciones ***(ITU, International Telecommunications Union)***.

EIA / TIA 232 admite velocidades de difusión de 64 kbps; es un conector D de 25 pines que se lo conoce también como RS-232 para distancias cortas; en la norma ITU corresponde a ITU.T v.24.

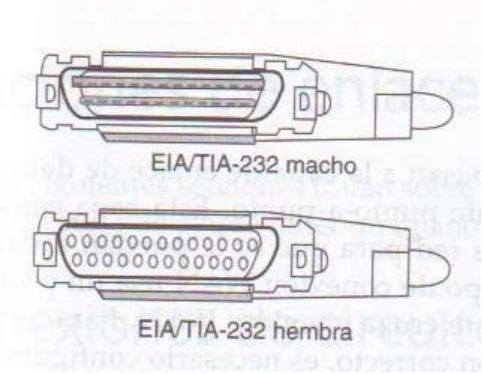


Gráfico 1. 21 Normas WAN EIA / TIA-232.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 381.

g1.5.7 EIA / TIA 449 EIA-530.

Es una versión mejorada de RS-232, es decir, más rápida 2 Mbps, utiliza un conector D de 36 pines que se puede emplear en cables más largos. Se lo conoce también como RS-422 Y RS-423

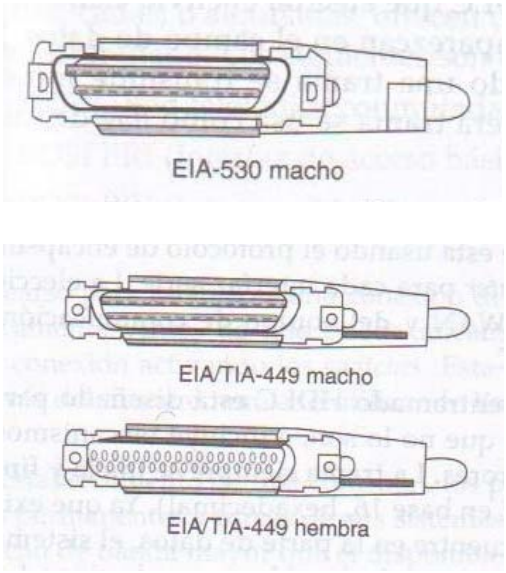


Gráfico 1. 22 Normas WAN EIA / TIA-449 y EIA-530.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 381.

1.5.8 EIA / TIA 612 / 613.

Es una interfaz serie de alta velocidad ***(HSSI, High Speed Serial Interface)***; ofrece una velocidad de hasta 52 Mbps empleando un conector D de 50 pines

Gráfico 1. 23 Normas WAN EIA-613.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 381.

1.5.9 V.35.

Es una norma de la Unión internacional de las telecomunicaciones ITU para la comunicación de datos síncronos de alta velocidad en Estados Unidos esta norma se usa en routers y DSU que conectan a proveedores T1.

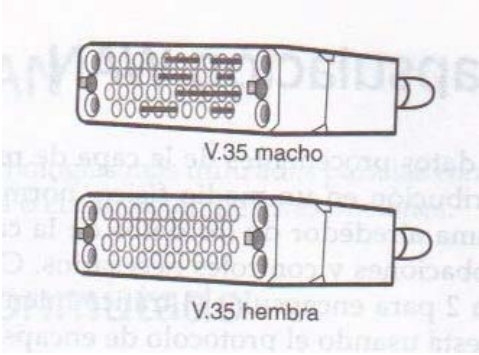


Gráfico 1. 24 Normas WAN V.35.

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 381.

1.6.0 X.21.

Existe un estándar de la Unión internacional de telecomunicaciones – Sector de normalización ITU-T que es aplicable para intercambio de datos digitales síncronos llamado X.21. Utiliza un conector D de 15 pines y es utilizado en Europa y Japón.

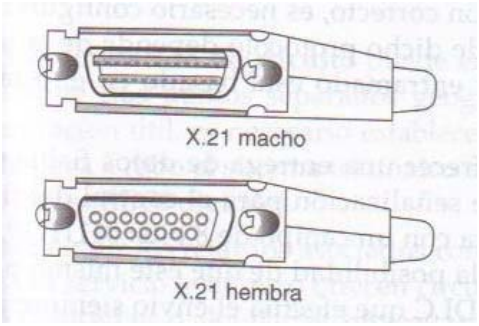


Gráfico 1. 25 Normas WAN

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 381.

2. RED LOCAL ACTUAL Y REQUERIMIENTOS

En el contenido de los próximos apartados se empieza con un diagnóstico de la red local, el análisis abarca la parte física y la lógica, que quiere decir, el vínculo entre elementos conceptuales institucionales y las características del entorno informático. Esta valoración nos permite identificar las debilidades de la infraestructura actual, también, nos coloca en un marco de trabajo del cual partir para establecer los requerimientos locales (LAN) y de la red de área amplia (WAN), dichas demandas, se clasificaron en físicas y lógicas.

La metodología para recolectar información se basa en técnicas de investigación de campo (encuestas y entrevistas) y en herramientas de diagnóstico de red (analizador de protocolos). Los sujetos consultados fueron usuarios de todas las oficinas, específicamente una muestra del 40% (37 personas) y al personal del departamento de sistemas.

Finalmente, examinamos mencionadas exigencias para interpretarlas y traducirlas a términos informáticos.

2.1 Infraestructura Física

En lo que va del capítulo estudiaremos la disposición física con que cuenta la Corte Constitucional, para luego, proponer un mejor diseño o si es el caso, mantener las condiciones actuales.

Para entregar servicios eficientes es necesaria una infraestructura de red que permita una proyección futura que reúna las condiciones adecuadas, estas condiciones, se encuentran normadas por estándares internacionales que también los veremos.

2.1.1 Caso de Estudio

El Tribunal Constitucional ahora Corte Constitucional[13] se encuentra ubicada en la Av. 12 de Octubre N16-114 y Pasaje Nicolás Jiménez, sus instalaciones cubren un área de 11 pisos cada uno con 300 metros aproximadamente. En el piso 2 se encuentra el Departamento de Sistemas que se encarga del mantenimiento del equipo computacional (hardware, software); además, provee de soporte a los funcionarios de la institución en lo relacionado con servicios de red, comunicaciones, software aplicativo, correo electrónico e impresiones.

Para el desarrollo de las actividades se ha implementado una red LAN (local) Fast Ethernet que trabaja a una velocidad de 100 Mbps.

2.1.2 Punto de Demarcación (demarc).

Es el lugar donde los cables del distribuidor externo se conectan con los equipos del cliente interno, "proporciona el punto en el que el cableado exterior conecta con el cableado backbone"[14]; en el caso de la Corte Constitucional existen tres proveedores externos, uno para el servicio de Internet (Telconet), otro para telefonía (Andinatel) y el último para la red eléctrica (Empresa Eléctrica). Los tres grupos de cables tienen su punto demarc en el segundo piso en el departamento de sistemas en un área aproximada de 15 metros cuadrados. Los cables de Telconet ofrecen tecnología de fibra óptica MULTIMODO en la última milla para proveer del servicio de Internet, éste cable va conectado a un router cisco de la serie 800 para que a través de él se distribuya el acceso al World Wide Web (www) por la red local.

---

[13] Corte Constitucional, *Resolución Administrativa No. 004-10-AD-CC*, Internet http://www.corteconstitucional.gob.ec/index.php?option=com_content&view=article&id=220&Itemid=15, Acceso: 08/diciembre/2011.

[14] Cisco Systems, Inc. Academia de Networking. *Guía del primer año. CCNA® 1 y 2*. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 812.

Gráfico 2. 1 Router Cisco Serie 800.

Referencia: Corte Constitucional.

Las conexiones del tendido eléctrico pasan por un conducto y llegan a un tablero principal que reparte el servicio, también, a este tablero están conectados dos sistemas de alimentación interrumpida (UPS), que brindan corriente eléctrica a los servidores en el caso de un corte eléctrico de esta manera se protege las aplicaciones y datos de los usuarios.

Gráfico 2. 2 UPS Firmesa Powerware 9170 Plus.

Referencia: Corte Constitucional.

Gráfico 2. 3 UPS 2 Referencia: Corte Constitucional.

Referencia: Corte Constitucional.

Para el caso de la telefonía los cables llegan a una central telefónica (PBX).

Gráfico 2. 4 Central telefónica Panasonic KX-TDA200 Hybrid IP-PBX.

Referencia: Corte Constitucional.

2.1.3 Sala de Telecomunicaciones.

"La sala de equipos es el centro de la red de voz y de datos. Una sala de equipos es esencialmente un gran recinto de telecomunicaciones …"[15]

Las normas TIA / EIA 569 - A establecen que para edificios con más de 2000 metros cuadrados de trabajo se recomienda un recinto fijo, aislado, exclusivo. Además, por cada 20 metros cuadrados de trabajo se necesita 1 metro cuadrado de madera contrachapada de espacio de planta, en el lugar donde se encuentra el hardware de distribución se aconseja utilizar pintura ignífuga o resistente al fuego y emplear el color naranja para identificar el punto de demarcación; la pintura y un sitio aislado para el demarc. En la institución tanto el punto de demarcación, la sala de telecomunicaciones y los servidores se albergan en el segundo piso.

No se distingue una sala de telecomunicaciones bien definida, debido a que en una misma área se comparte servicios de aplicaciones y distribución del cableado; toda ésta infraestructura se encuentra en el piso dos. Se implementa un rack de distribución panduit que alberga 2 switches, que sirve como punto de distribución principal para el cableado backbone.

[15] Ídem 14.

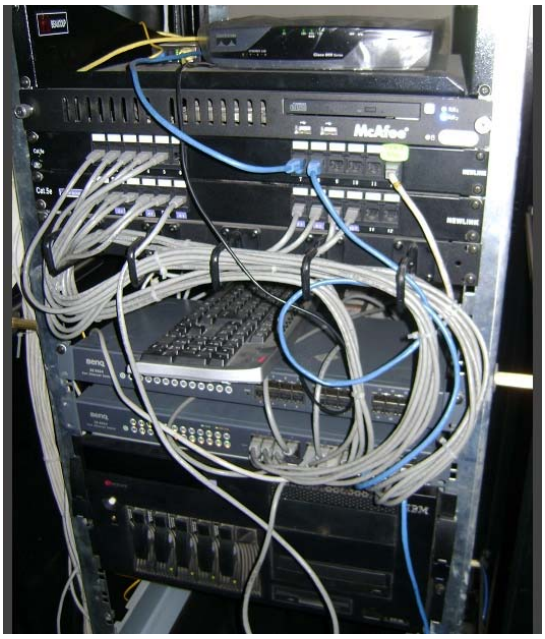


Gráfico 2. 5 Rack de distribución.

Referencia: Corte Constitucional.

2.1.4 Cableado Backbone y Cableado de Distribución

La unidad de distribución principal (MDF) de donde parte el ***cableado backbone*** que atraviesa todo el edificio, está ubicado en el segundo piso del edificio; es un grupo de cables de par trenzado de cobre UTP categoría 5e, que recorren los pisos del edificio en forma vertical hasta llegar a las unidades de distribución intermedia (IDF). En éste caso un IDF que está representado por un switch BenQ SE 0024 Fast Ethernet de 24 puertos conectado a una bandeja NEWLINK Cat 5e de 47 puertos (ver gráfico 2.6), que sirve como medio de expansión del cableado hacia cada host. Al conjunto de cables y equipos utilizados en un área de trabajo se conoce como conexión cruzada horizontal (HCC). Se evidencia que en cada piso a excepción de la planta baja tiene un IDF para cada área de trabajo. El IDF que conecta la conexión cruzada horizontal (HCC) con el MDF, se denomina conexión cruzada intermedia (ICC).

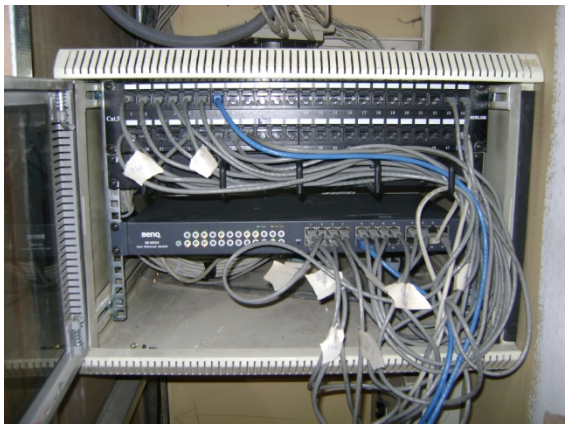


Gráfico 2. 6 Switch con bandeja para distribución horizontal en cada piso.

Referencia: Corte Constitucional.

2.1.5 Áreas de Trabajo

Las ***áreas de trabajo*** se extienden en cada piso del edificio, la conexión permanente (cableado horizontal) no excede los 100 metros de la norma, los cables utilizados son UTP que cumplen con la norma ANSI/TIA/EIA 568 – B. Para proporcionar la ***distribución de cableado*** en cada piso existe un switch BenQ SE0024 Fast Ethernet no administrable (ICC) que sirve de enlace para el cableado horizontal.

Las estaciones de trabajo, en su mayoría presentan las siguientes características.

Marca: Hp compaq

Modelo: dc 220 MT

Sistema operativo: XP Service Pack 2.

Procesador: Intel Pentium III.

Memoria RAM. 1 Gb

Disco Duro: 80 Gb

Monitor: Hp 14’’

Gráfico 2. 7 Unidad central de procesamiento característica.

Referencia: Corte Constitucional.

La mayoría, aproximadamente el 90 por ciento de las computadoras, son de las características arriba mencionadas; en algunas unidades existen notebook o laptop de diferentes marcas y modelos.

Últimamente, se ha adquirido nuevas computadoras de marca Hp, variando algunas características:

Modelo: dc5800.

Procesador: Intel core 2 duo.

Memoria RAM: 2 Gb.

Para las tareas de impresión se utilizan impresoras conectadas a la red. La impresora común en cada área de trabajo tiene las siguientes características:

Marca: Hp.

Modelo: 3005 dn.

Gráfico 2. 8 Impresora característica.

Referencia: Corte Constitucional.

Otras impresoras son:

Marca: EPSON

Modelo: LX 300 +

Marca: Hp

Modelo: 2600n

Marca: Hp

Modelo:1022 dn

Marca: XEROX

Modelo: Phaser 4510.

2.1.6 Sala de Equipos (ER)

La ***sala de equipos (ER)*** está en el Departamento de Sistemas consta de 6 servidores, 1 router, 2 UPS ‘s, 2 switches de 24 puertos cada uno, un patch panel y el PBX. Las condiciones físicas del cuarto son:

Altura de 2,5 metros.

Un área de más de 14 metros cuadrados.

Puertas de 0,91 metros de ancho.

Gráfico 2. 9 Sala de servidores.

Referencia. Corte Constitucional.

#	Marca	Modelo	Procesador	S.O.	Memoria RAM	Disco duro	Función
1	IBM	X series 250	Pentium III	W2000 Server	512 Mb	70 Gb	Aplicaciones
2	Hp compaq	dc5800	Core 2 duo	W2000 Server	1Gb	250 Gb	Antivirus
3	IBM	NetVista	Intel Celeron	Fedora 10.0	384 Mb	40 Gb	Internet
4	IBM	NetVista	Intel Celeron	Red Had 9.0	512 Mb	40 Gb	Correo
5	Acer	Altos G700	x86	W2000 Server	360 Mb	70 Gb	Aplicaciones
6	Mcafee	Gateway 3000	Intel	Linux	512 Mb		Filtro Internet

Tabla 2. 1 Servidores en la sala de equipos.

Referencia: Corte Constitucional.

Gráfico 2. 10 Servidor 6 anti-spam, anti-phishing

Referencia: Corte Constitucional.

2.1.7 Administración.

Los dos servidores de directorio funcionan con Windows server 2000

La ***administración*** se ejerce a través del área de informática. Para cumplir con los requerimientos, el departamento de sistemas cuenta con un equipo de 5 personas, cada una de ellas abarca un ámbito distinto, es decir, un profesional para las áreas de:

- Administración de red.
- Soporte a funcionarios,
- Mantenimiento de equipos (hardware).
- Desarrollo de aplicaciones (software).
- Jefe Administrativo.

La sinergia de este equipo de profesionales es la solución tecnológica a las demandas del entorno empresarial de la Corte Constitucional.

2.1.8 Mapa de Red por Pisos Corte Constitucional.

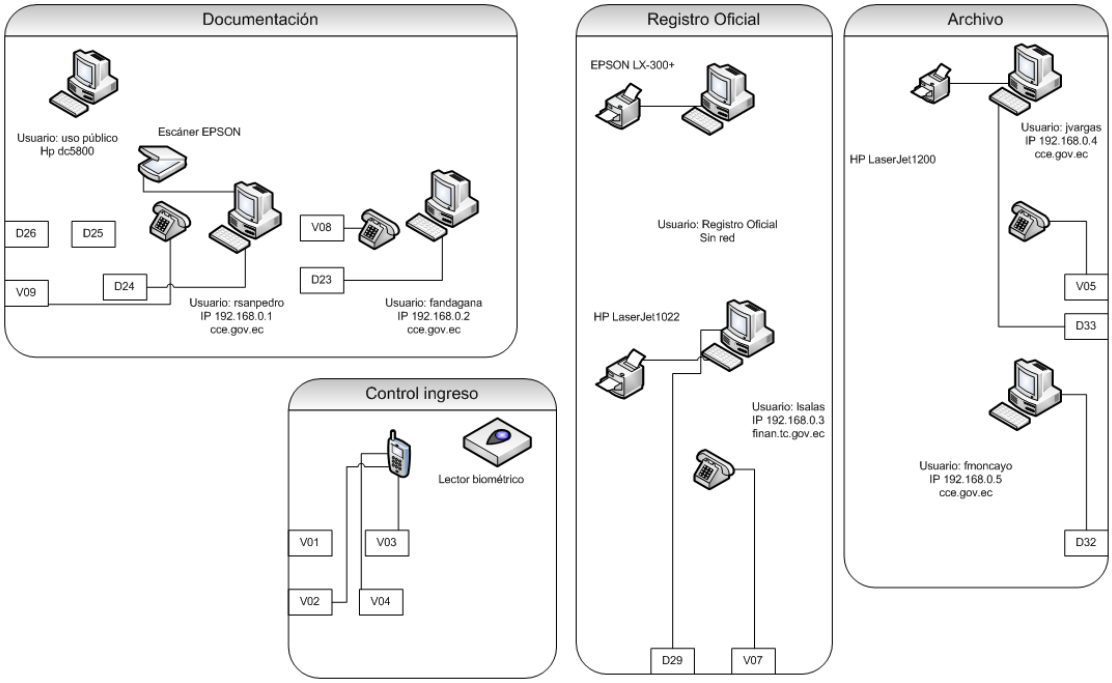


Gráfico 2. 11 Mapa de red Planta Baja.

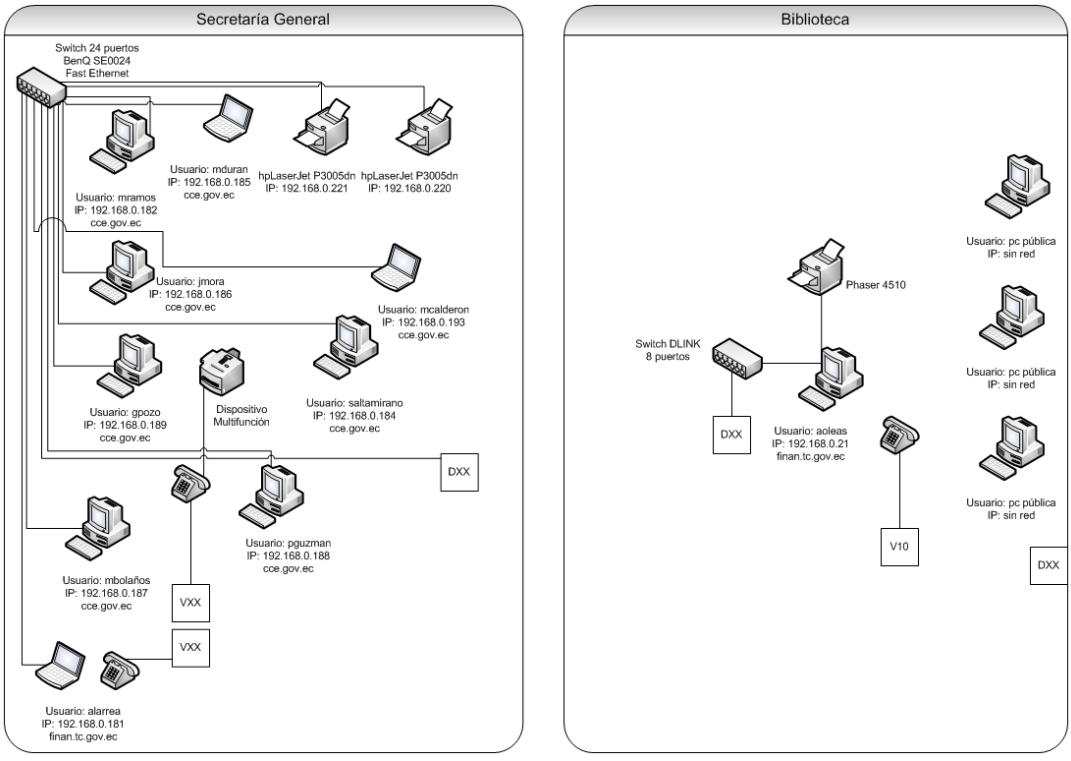


Gráfico 2. 12 Mapa de red Primer piso

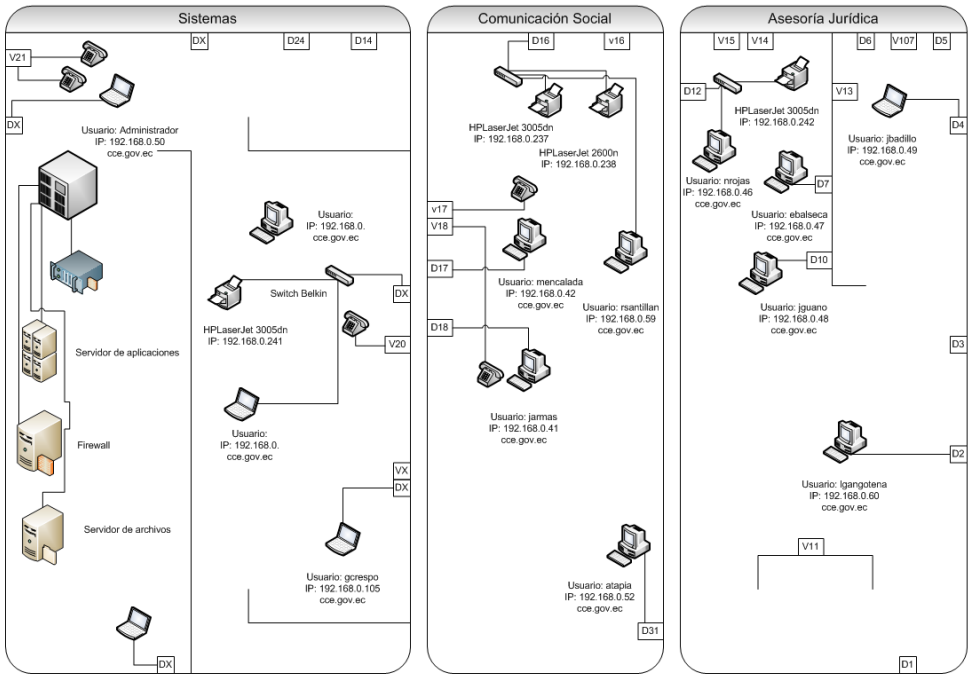


Gráfico 2.13 Mapa de red segundo piso.

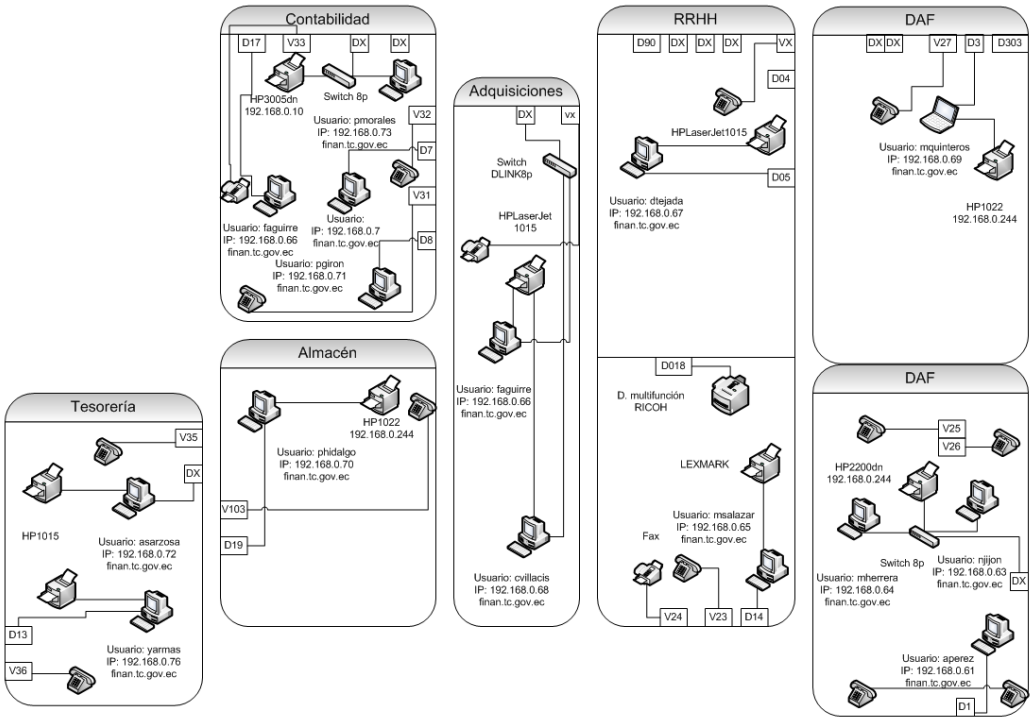


Gráfico 2. 14 Mapa de red tercer piso.

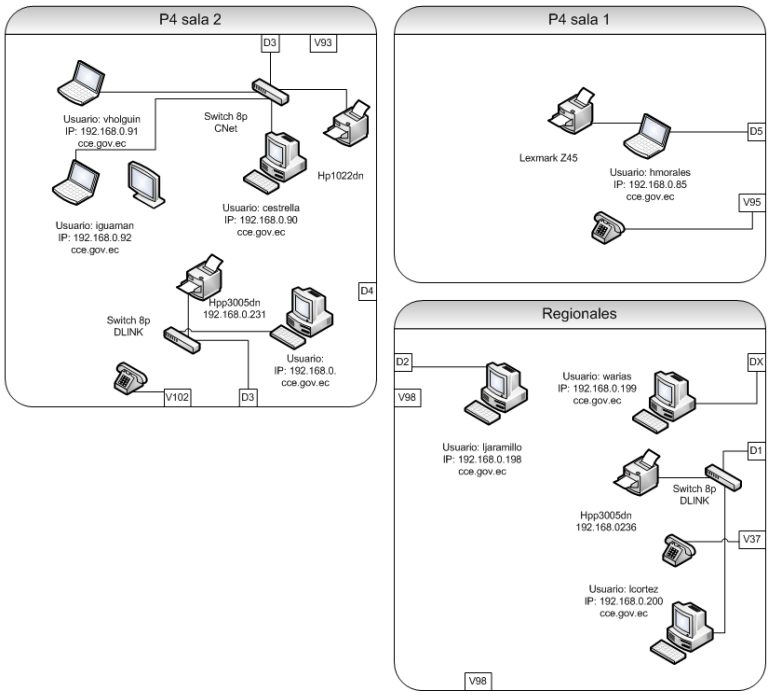


Gráfico 2. 15 Mapa de red cuarto piso

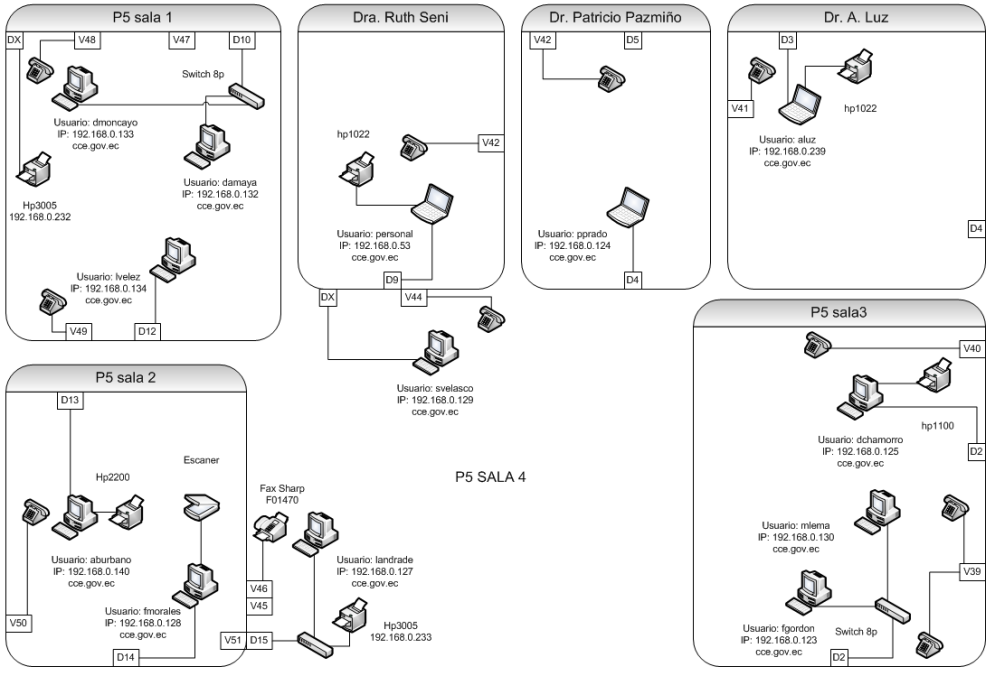


Gráfico 2. 16 Mapa de red quinto piso.

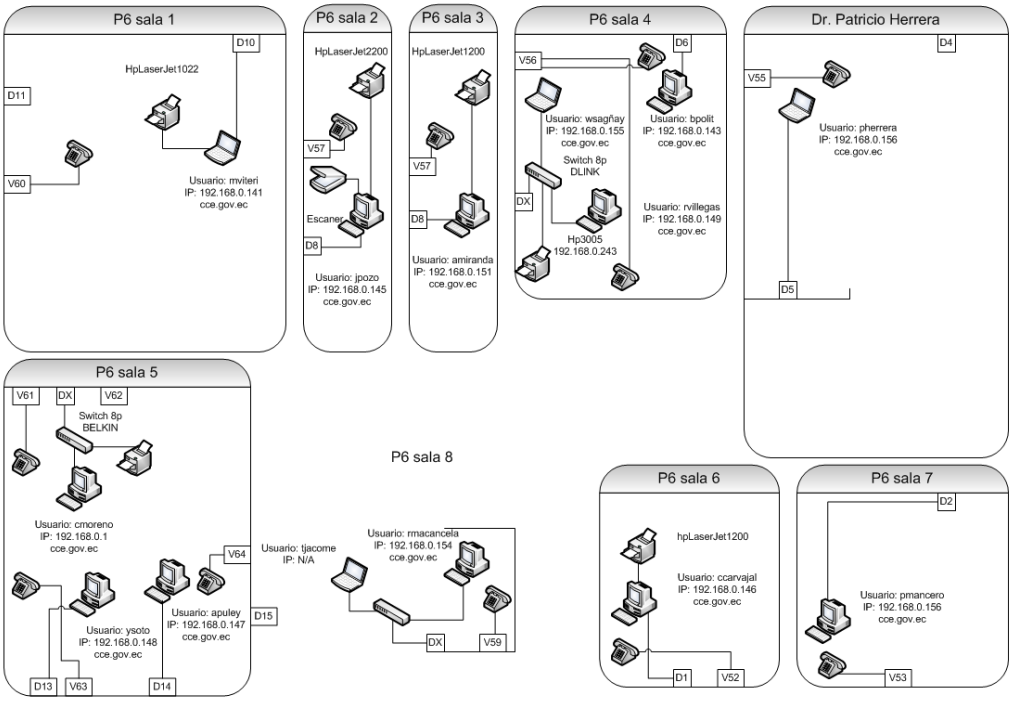


Gráfico 2. 17 Mapa de red sexto piso.

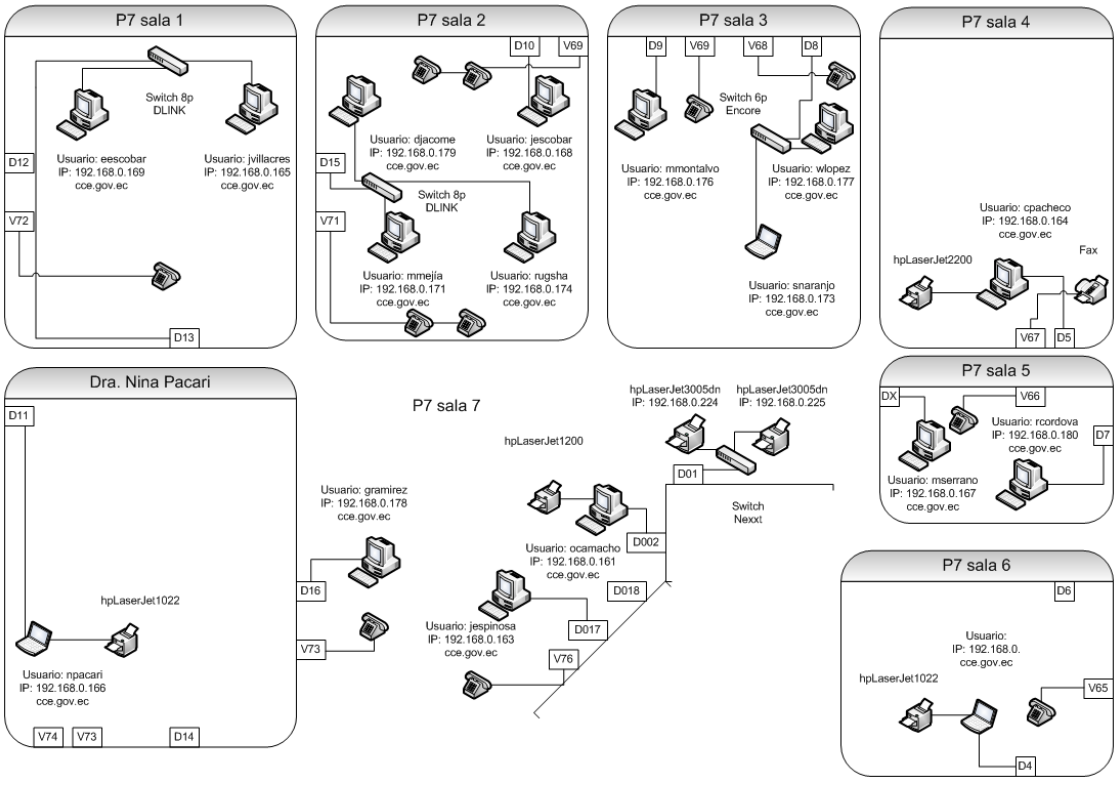


Gráfico 2. 18 Mapa de red séptimo piso

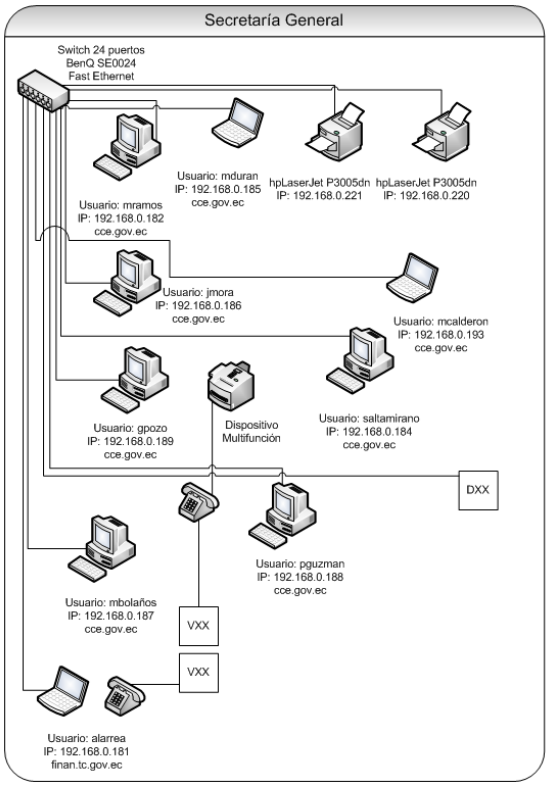


Gráfico 2. 19 Mapa de red octavo piso.

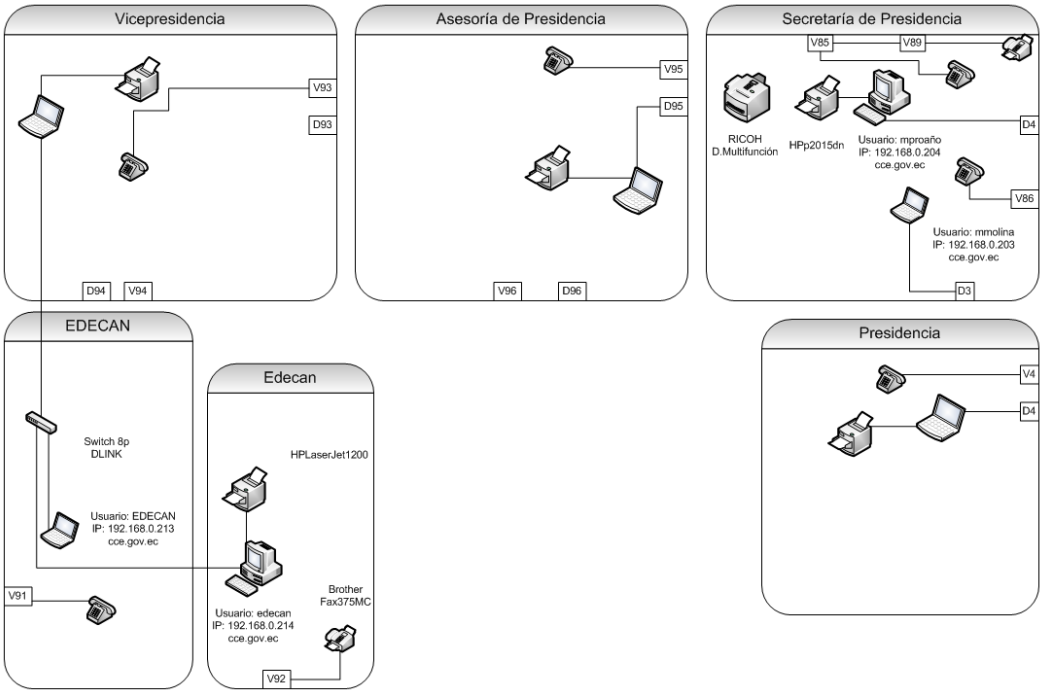


Gráfico 2. 20 Mapa de red noveno piso

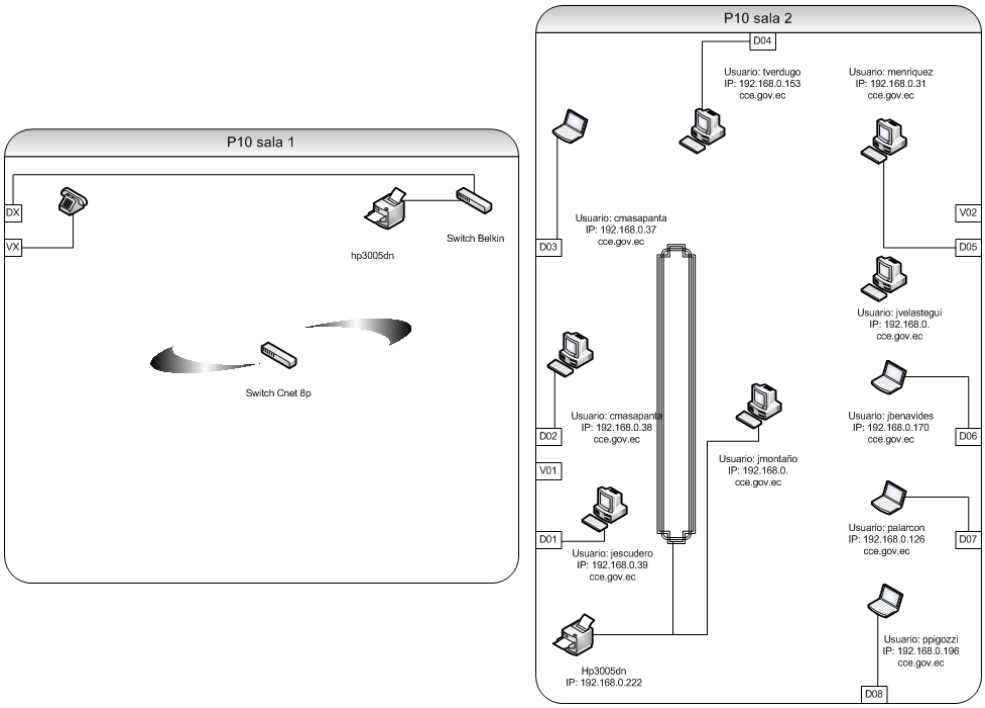


Gráfico 2. 21 Mapa de red décimo piso

2.2 Infraestructura Lógica.

El presente tema se refiere a la forma como se encuentran distribuidos los dispositivos de red, es decir, bajo qué criterio se dispusieron los computadores, servidores y demás equipos para su administración, en otras palabras, con qué criterio fue diseñada la red.

Para identificar cada equipo dentro de la red se utilizan direcciones IP, las mismas que, son utilizadas para entregar el servicio de Internet

2.2.1 Diseño Actual

A continuación, ilustramos en el gráfico la infraestructura lógica.

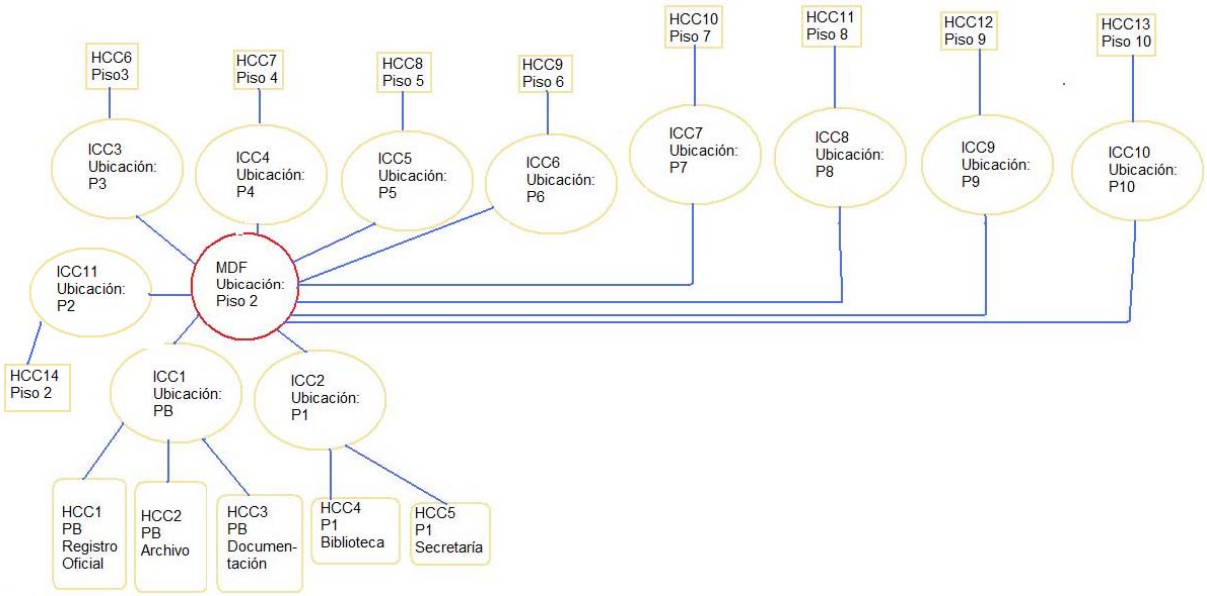


Gráfico 2. 22 Diagrama lógico.

Referencia: Corte Constitucional.

2.1.2 Servidores

Existen 6 servidores (computadoras que proveen servicios) en la sala de equipos, el ***primer servidor*** está dedicado a la administración del sistema de impresión, controlador de dominio (cce.gov.ec), servidor de archivos para lo relacionado con el área jurídica, y gestión de casos que es un software aplicativo de consulta. Es una máquina de marca IBM X Series 250 Xeon III con sistema operativo Windows 2000 Server, 512 en memoria RAM, 5 discos RAID que sumados tienen una capacidad de 70 Gb en dos particiones con el sistema de archivos NTFS. En el equipo que estamos analizando se encuentra instalado del programa Active Directory que es un administrador de directorio en una red distribuida. Los servicios que entrega a las estaciones son:

- File Magister.
- Sistema de gestión de casos.
- Archivos digitales de resoluciones desde 1997 hasta 2004.

- Administración de contenidos (documentos jurídicos) desde 2000 hasta 2006.
- Sistema de sorteo de casos.

El ***segundo servidor*** brinda el servicio de software de antivirus Kaspersky y actualización del mismo en su versión 6.0. El proceso empieza a las 8h30 de la mañana cuando el servidor envía las actualizaciones a cada terminal, además, se realizan análisis de amenazas en estaciones y en servidores.

En el segundo servidor se tiene el servicio de firewall (dispositivo de seguridad) que se identifica con el nombre "iptables" que tiene reglas de acceso.

Para peticiones externas el servidor 2 habilita los siguientes puertos:

Puerto	Aplicación
25	Correo
80	World Wide Web (www)
110	Pop3
443	Certificado de seguridad https
20	ftp
21	ftp
8090	Tomcat Lotus notes
8080	Lotus notes
1000	Webmin
1005	Sin uso

Tabla 2. 2 Puertos habilitados en el segundo servidor.

Referencia: Corte Constitucional.

Para proveer de Internet a la Corte Constitucional se utiliza el ***tercer servidor***, que posee un firewall. Tiene las siguientes características: sistema operativo LINUX Fedora

9.0, kernel versión 2.6. La navegación por Internet emplea dos interfaces eth0 y eth1 para poder enviar tráfico de Internet en eth0 se encuentra la IP pública 190.95.159.26 y en eth1 para distribuir Internet en la red local se maneja la dirección 192.168.0.54.

El ***cuarto servidor*** sirve para ofrecer el servicio de correo electrónico, posee antispam, mailscanner y es también un servidor de nombres de dominio tiene habilitados los puertos:

Puerto	Aplicación
53	Dns
80	http
110	Pop3
143	Imap
443	https
864	X
3306	Mysql

Tabla 2. 3 Puertos habilitados en el tercer servidor.

Referencia: Corte Constitucional.

El sistema operativo es Linux Redhat versión 2.4. Hallamos 5 particiones:

1. /swap.
2. /home.- donde se encuentran los usuarios.
3. /var.- para logearse en el sistema.
4. /usr.- aplicativos del sistema operativo.
5. /temp.- reciclaje.

Para el ***quinto servidor*** se observó que presta servicio para el área financiera, es por esta razón que se tiene otro dominio (finan.gov.ec) tiene instalado el sistema operativo Windows 2000 Server con Active Directory, el equipo es de marca Acer Altos

G700, 360 Kb en RAM, 2 procesadores X86. En la máquina existen 3 particiones: c, f, g, de 15, 25 y 25 Gb. respectivamente. La primera partición es para propósitos del sistema operativo, la segunda es para el aspecto contable y la última para almacenamiento.

Las aplicaciones en este servidor son las siguientes:

- Sistema de inventarios.
- Sistema de nómina.
- Historial de RRHH.
- Control de acceso.

El proceso de filtrado de contenidos provenientes de Internet lo realiza el ***servidor seis***, se lo hace a través de anti spam, anti phishing con un equipo Mcaffe Gateway 3000. A las 8 de la mañana descarga las actualizaciones para realizar sus tareas.

2.1.3 Dominios

En la institución existen dos ***cce.gov.ec*** y ***finan.gov.ec***, sirven para diferenciar la unidad administrativa financiera de las demás.

El dominio que se maneja en el servidor 1 es ***cc.gov.ec***, para identificar a cada uno de los usuarios se usa la unidad administrativa (SG, S1, S2, S3, DGA) seguida de la primera letra del nombre con el primer apellido, por ejemplo, el usuario Pablo Arias que trabaja en Secretaría General se lo identificará con ***sg-parias.cc.gov.ec.*** Éste dominio funciona con direcciones de tipo C **192.168.0.1**.

El segundo dominio ***finan.gov.ec*** se encuentra alojado en el ***quinto servidor***, realiza las tareas necesarias para el área financiera y se utiliza el mismo método para nombrar a los host, es decir, unidad + primera letra del nombre +primer apellido, ***dga-parias.finan.gov.ec***.

Los dos dominios son independientes, es decir, no existe comunicación entre computadoras que no pertenezcan al mismo dominio.

2.1.4 Seguridad y Políticas de Grupo

La seguridad se maneja a través de la interacción de los servidores, por ejemplo, en el primer servidor con el programa Active Directory; aplicativo que es una "implementación de servicio de directorio en una red distribuída"[16]; se manejan políticas para usuarios, en el segundo servidor las actualizaciones de antivirus detectan e impiden amenazas, el sexto servidor produce filtros para el ingreso de la información externa.

Con ***Active Directory*** hay la posibilidad de crear ***grupos integrados*** como grupo de usuarios avanzados, operadores de servidores, operadores de impresiones o de copias de seguridad. En el caso de estudio no existen grupos de ésta naturaleza.

En la opción ***directiva de cuenta*** se puede configurar directivas de contraseñas, bloqueos de cuentas y autenticación kerberos; para las contraseñas tenemos las siguientes restricciones:

La autenticación es permitida en el horario de 8 am hasta 18 pm de lunes a viernes.

La contraseña debe tener 6 dígitos.

Cada 30 días se obliga al usuario a cambiar la contraseñas, se almacenan las últimas cuatro contraseñas para que no se repitan.

Bloqueo de cuentas después de 3 intentos fallidos.

En ***directivas locales*** se puede configurar los derechos de los usuarios. En la Corte Constitucional todos los usuarios comparten los mismos derechos, sí, algún usuario necesita alguna característica adicional, a través de la IP se habilita mencionado requerimiento. A continuación, especificamos otras directivas:

Uso de impresoras restringido para cada unidad, es decir, solo el personal que pertenece a ése departamento puede imprimir en la impresora asignada a esa unidad administrativa.

---

[16] Wikipedia. *Active Directory* Internet. http://es.wikipedia.org/wiki/Active_Directory Acceso: 08/diciembre 2011.

Se permite un máximo de 10 hojas de impresión.

Derechos de usuario acorde a la función que realizan (File server restringido).

En directivas locales se puede configurar el visor de sucesos para habilitar propiedades de auditoría, sin embargo, no se utiliza ésta opción.

Para privilegios de ***inicio de sesión de usuario***, en lo que se refiere a accesos y propiedades del controlador de dominio están configuradas con los valores predeterminados como se indica en la gráfica siguiente:

Asignación de privilegios y derechos de usuario	Estación de trabajo del dominio	Equipo portátil de dominio	DC	Servidor de dominio	WKS independiente	Servidor independiente		
Privilegio	Predeterminado	Modificado						
Tener acceso a este equipo desde la red (Professional/Server)	Administradores Operadores de copia de seguridad Usuarios avanzados Usuarios Todos	Administradores Operadores de copia de seguridad Usuarios avanzados Usuarios Usuarios autenticados	✓	✓		✓	✓	✓
Tener acceso a este equipo desde la red (Controlador de dominio)	Administradores Usuarios autenticados Todos	Administradores Usuarios autenticados			✓			
Inicio de sesión local (Professional)	Administradores Operadores de copia de seguridad Usuarios avanzados Usuarios*Nombreequipo*\Invitado	Administradores Operadores de copia de seguridad Usuarios avanzados Usuarios	✓	✓			✓	
Inicio de sesión local (Server)	Administradores Operadores de copia de seguridad Usuarios avanzados Usuarios *Nombreequipo*\Invitado *Nombreequipo*\TsInte rnetUser	Administradores Operadores de copia de seguridad Usuarios avanzados NOTA: necesitará conceder este privilegio a los usuarios en un servidor de aplicaciones de Terminal Server.				✓		✓
Inicio de sesión local (Controlador de dominio)	Administradores Operadores de cuentas Operadores de copia de seguridad Operadores de impresión Operadores de servidores TsInternetUser	Administradores Operadores de cuentas Operadores de copia de seguridad Operadores de impresión Operadores de servidores			✓			
Agregar estaciones de trabajo al dominio (Controlador de dominio)	Usuarios autenticados	Usuarios autenticados				✓		
Aumentar las cuotas (Controlador de dominio: en la directiva de seguridad de dominio)	(No está definido)	Administradores				✓		
Aumentar la prioridad de programación (Controlador de dominio: en la directiva de seguridad de dominio)	(No está definido)	Administradores				✓		
Cargar y descargar controladores de dispositivo (Controlador de dominio: en la directiva de seguridad de dominio)	(No está definido)	Administradores				✓		
Administrar registros de auditoría y de seguridad (Controlador de dominio: en la directiva de seguridad de dominio)	(No está definido)	Administradores				✓		
Modificar valores de entorno del firmware (Controlador de dominio: en la directiva de seguridad de dominio)	(No está definido)	Administradores				✓		
Perfilar el rendimiento del sistema (Controlador de dominio: en la directiva de seguridad de dominio)	(No está definido)	Administradores				✓		

Apagar el sistema (Clientes)	Administradores Operadores de copia de seguridad Usuarios avanzados Usuarios	Administradores Operadores de copia de seguridad Usuarios avanzados Usuarios autenticados	✓	✓			✓	
Apagar el sistema (Servidores)	Administradores Usuarios avanzados (otros grupos varían dependiendo del tipo de sistema)	Administradores			✓	✓		✓
Tomar posesión de archivos u otros objetos (Controlador de dominio: en la directiva de seguridad de dominio)	(No está definido)	Administradores				✓		

Gráfico 2. 23 Configuración Active Directory para privilegios y derechos de usuario.

Referencia: Internet http://www.microsoft.com/spain/technet/recursos/articulos/secmod220.mspx#EIE.

Otras restricciones son:

- Todos los usuarios se loggean o ingresan a través del Active Directory.
- No existen usuarios con privilegios de administrador.
- No se permite reproducir música y video que no sea localmente.
- Para guardar documentos se concede máximo 8 caracteres.
- Los parches (Service Pack) se descargan todos los días para su inmediata distribución.
- Se realizan respaldos diarios de toda la información en los servidores.

2.1.5 Información

Se maneja varios tipos de información, a continuación, describiremos la información que se distribuye en el dominio ***cce.gov.ec***.

Tenemos el ***Fiel Magister*** que es un programa (software) donde se pueden ver las últimas publicaciones legales. Los terminales ingresan a este servicio a través del puerto 12069. Es una herramienta de información jurídica, a través de ella, se puede consultar las últimas publicaciones legales.

En el sistema de ***Gestión de Casos*** se encuentra almacenada la información de cada una de las peticiones que ingresan a la Institución, por medio de éste aplicativo podemos hacer un seguimiento y conocer del estado de cada uno de los procesos.

Está desarrollado en Visual FoxPro V 7.0, e interactúa con la base de datos relacional ***sql Server 2000.***

Cuando un caso ha llegado a la instancia final, se genera una Sentencia (antes resolución). La publicación de éste documento se digitaliza y se administra para su posterior consulta.

Existe información de Resoluciones desde el año 1997 hasta 2004, mismas que están en un almacén de archivos digitalizados, que se conoce como Repositorio.

Para Resoluciones desde el 2000 hasta el 2006 que necesiten ser estudiadas con opciones de búsqueda se crea el ***Sistema de Administración de Contenidos***.

Para acceder a las publicaciones de los ***Registros Oficiales*** se tiene la aplicación ***ROW***, que contiene los registros digitalizados (ver gráfico 34 y 35).

Cada caso es sometido a un sorteo (***sorteo de causas***) que sirve para asignar el caso a una sala específica (sala 1, sala 2, sala 3), en mencionada unidad se trata el ítem objeto del sorteo (ver gráfico 36).

Gráfico 2. 24 Consultas de Resoluciones.

Referencia: Página Web Corte Constitucional
(http://www.tribunalconstitucional.gov.ec/c_Jurisprudencia.asp).

Gráfico 2. 25 Consultas de Resoluciones.

Referencia: Página Web Corte Constitucional
(http://www.tribunalconstitucional.gov.ec/c_Jurisprudencia.asp)

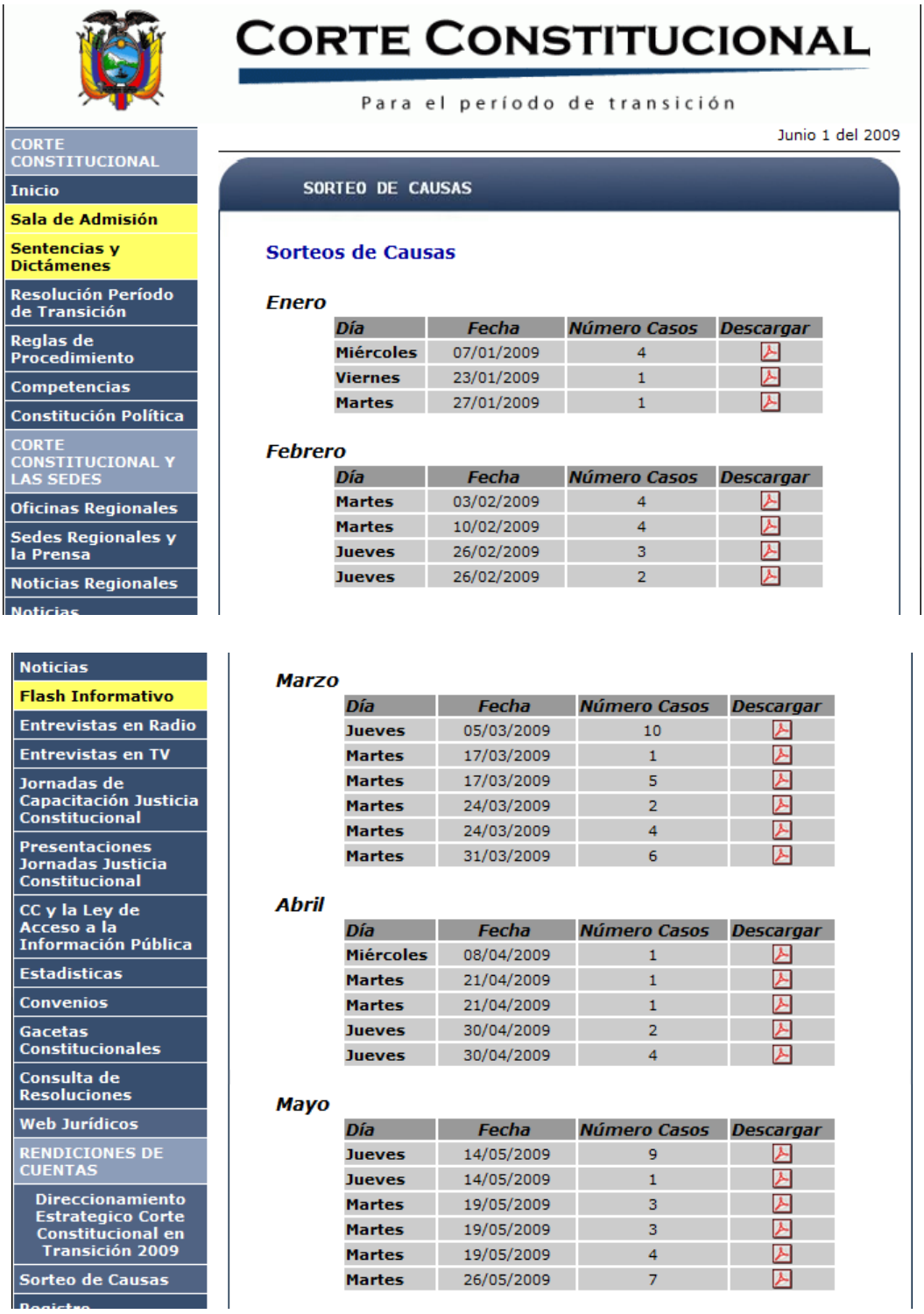


Gráfico 2. 26 Sorteo de Casos.

Referencia: Corte Constitucional página web: http://www.tribunalconstitucional.gov.ec/sorteos.asp

La información de tipo financiera se administra a través del dominio ***finan.gov.ec***. Se tienen los siguientes sistemas:

Sistema de inventarios sirve para controlar los activos muebles e inmuebles de la organización, de ésta manera, se facilitan los procedimientos (depreciación) para realizar transacciones estableciendo valores reales a los equipos.

Para la gestión del personal humano una de las herramientas que se tiene es el ***sistema de nómina,*** en donde se guarda información necesaria para asignación de sueldos, el detalle de los aportes, las deducciones, pagos fiscales, aportes al seguro social, entre otros.

Otro elemento para la gestión del recurso humano es el ***repositorio de RRHH.*** Aquí se almacena información relacionada con el personal como las cargas familiares, hoja de vida; aspectos cualitativos de los funcionarios.

Para el ***control de accesos*** se posee un lector biométrico de manos, con ésta aplicación se puede monitorear los horarios de cada empleado, y si se diera el caso contabilizar las horas extras.

Una vez que hemos separado los servicios por dominios y los hemos enunciado, continuaremos con los servicios que son comunes para todos los usuarios internos.

Un servicio de red común a todos los departamentos de la Corte Constitucional es el ***correo electrónico (e-mail)***. Ésta herramienta se basa en el protocolo simple de transferencia de correo ***(SMTP, Simple Mail Transfer Protocol)*** utilizando mensajes de texto para comunicarse entre sistemas iguales. Debido a un cambio en las competencias de de la institución que antes se enmarcaba como Tribunal y actualmente como Corte se mantienen las direcciones de correo @***tc.gov.ec***, aunque, @***cce.gov.ec*** es actualmente la oficial, es decir por ejemplo, un usuario que antes se identificaba por parias@tc.gov.ec ahora su dirección de correo es parias@cce.gov.ec, pero la correspondencia que le envíen a su dirección anterior también le llegará durante un tiempo para evitar fallos por mencionado cambio.

A menudo se confunde Internet (conjunto de redes interconectadas que emplean el protocolo TCP/IP) con el conjunto de protocolos que permiten la descarga de archivos de hipertexto www World Wide Web. Otros servicios de Internet son: transmisión de

archivos o FTP, conversación en línea o IRC, mensajería instantánea, boletines electrónicos, acceso remoto Telnet, entre los principales. En la Corte Constitucional se utiliza Internet con restricciones a redes sociales, a descargas de música, a descargas de video y con acceso en horario laboral (8h00 a 18h00).

La Intranet es un servicio privado que utiliza Internet para la transmitir información o acceder a ella de una forma segura restringiendo la entrada a algunas aplicaciones propias del negocio para cualquier usuario. Se almacena la información descrita anteriormente como los sorteos de las causas, artículos informativos, datos de la organización, competencias de la Corte Constitucional, misión, visión entre otras (ver gráfico 38).

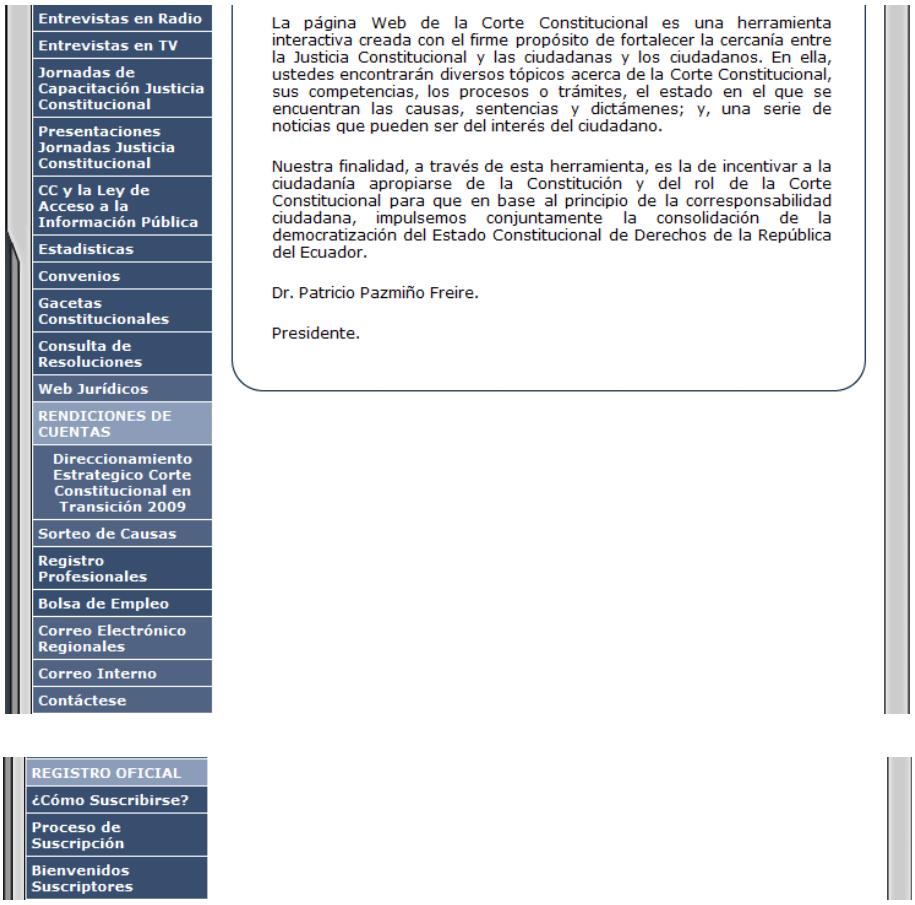


Gráfico 2. 27 Intranet Institucional.

Referencia Corte Constitucional. http://www.tribunalconstitucional.gov.ec/inicio.asp

2.1.6 Relaciones de Confianza

Las relaciones de confianza se establecen para comunicación entre dos dominios. En éste caso no está habilitada esta opción, es decir, no se puede identificar los host que estén en otro dominio.

2.1.7 Unidades Organizativas

Cada unidad organizativa dentro de la institución tiene su grupo de usuarios; podemos citar las siguientes entidades:

- Departamento Jurídico.
- Primera Sala.

- Segunda Sala
- Tercera Sala,
- Secretaría General
- Departamento Financiero.
- Presidencia.

2.1.8 Direcciones IP

Se utiliza la IP pública 190.95.159.26 para acceder a Internet (IP externa); para distribuir Internet en la red local se maneja la dirección 192.168.0.54 (IP interna). Se emplean las IP's en el rango 192.168.0.220 al 139.168.0.244 para reconocer las impresoras en red. Las direcciones comprendidas entre 192.168.0.245 a 192.168.0.254 son utilizadas para los servidores. En la tabla a continuación se evidencia las IP's disponibles y las que son de uso de los funcionarios.

IP	USUARIO
192.168.0.1	rsanpedro
192.168.0.2	fandagana
192.168.0.3	lsalas
192.168.0.4	jvargas
192.168.0.5	fmoncayo
192.168.0.6	1
192.168.0.7	2
192.168.0.9	asarzosa
192.168.0.10	3
192.168.0.21	aoleas
192.168.0.26	4
192.168.0.28	5
192.168.0.34	6
192.168.0.38	cmasapanta
192.168.0.39	jescudero
192.168.0.41	jarmas
192.168.0.42	mencalada
192.168.0.43	7
192.168.0.44	Aoleas
192.168.0.45	8

IP	USUARIO
192.168.0.105	gcrespo
192.168.0.114	13
192.168.0.116	14
192.168.0.122	15
192.168.0.123	mgordon
192.168.0.124	pprado
192.168.0.125	dchamorro
192.168.0.126	palarcon
192.168.0.127	landrade
192.168.0.128	fmorales
192.168.0.129	svelasco
192.168.0.130	mlema
192.168.0.132	damaya
192.168.0.133	dmoncayo
192.168.0.134	lvelez
192.168.0.136	16
192.168.0.140	aburbano
192.168.0.141	mviteri
192.168.0.142	17
192.168.0.143	bpolit

IP	USUARIO
192.168.0.177	Wlopez
192.168.0.178	Jramirez
192.168.0.179	Djacome
192.168.0.180	Rcordova
192.168.0.181	Alarrea
192.168.0.182	Mramos
192.168.0.183	29
192.168.0.184	Saltamirano
192.168.0.185	Mduran
192.168.0.186	Jmora
192.168.0.187	Mbolaños
192.168.0.188	Pguzman
192.168.0.189	Gpozo
192.168.0.193	Mcalderon
192.168.0.196	30
192.168.0.198	Ljaramillo
192.168.0.199	Warias
192.168.0.200	Lcortez
192.168.0.198	Ppigozzi
192.168.0.201	31

192.168.0.46	nrojas	192.168.0.145	jpozo	192.168.0.202	32
192.168.0.47	ebalseca	192.168.0.146	ccarvajal	192.168.0.203	Mmolina
192.168.0.48	iguano	192.168.0.147	18	192.168.0.204	Mproaño
192.168.0.49	jbadillo	192.168.0.148	19	192.168.0.205	33
192.168.0.50	administrador	192.168.0.149	rvillegas	192.168.0.213	EDECAN
192.168.0.52	atapia	192.168.0.150	20	192.168.0.214	Edecán
192.168.0.53	personal	192.168.0.151	amiranda	192.168.0.216	34
192.168.0.59	rsantillan	192.168.0.152	21	192.168.0.220	Impresora
192.168.0.60	lgangotena	192.168.0.153	tverdugo	192.168.0.221	Impresora
192.168.0.61	aperez	192.168.0.154	rmacancela	192.168.0.221	Impresora
192.168.0.62	9	192.168.0.155	wsagñay	192.168.0.224	Impresora
192.168.0.63	njijon	192.168.0.156	pmancero	192.168.0.225	Impresora
192.168.0.64	mherrera	192.168.0.159	22	192.168.0.229	35
192.168.0.65	msalazar	192.168.0.160	23	192.168.0.230	36
192.168.0.66	faguirre	192.168.0.161	ocamacho	192.168.0.231	Impresora
192.168.0.67	dtejada	192.168.0.162	24	192.168.0.232	Impresora
192.168.0.68	cvillacis	192.168.0.163	jespinosa	192.168.0.233	Impresora
192.168.0.69	mquinteros	192.168.0.164	cpacheco	192.168.0.236	37
192.168.0.70	phidalgo	192.168.0.165	jvillacres	192.168.0.237	Impresora
192.168.0.71	pgiron	192.168.0.166	npacari	192.168.0.238	Impresora
192.168.0.72	asarzosa	192.168.0.167	25	192.168.0.239	Aluz
192.168.0.73	pmorales	192.168.0.168	jescobar	192.168.0.240	38

192.168.0.76	yarmas	192.168.0.169	eescobar	192.168.0.241	39
192.168.0.84	10	192.168.0.170	jbenavides	192.168.0.242	Impresora
192.168.0.85	hmorales	192.168.0.171	mmejia	192.168.0.243	Impresora
192.168.0.89	11	192.168.0.172	26	192.168.0.244	Impresora
192.168.0.90	cestrella	192.168.0.173	27	192.168.0.248	Servidor
192.168.0.91	vholguin	192.168.0.174	rugsha	192.168.0.249	Servidor
192.168.0.92	iguaman	192.168.0.175	28	192.168.0.250	Servidor
192.168.0.93	12	192.168.0.176	mmontalvo	192.168.0.251	Servidor
				192.168.0.252	Servidor
				192.168.0.253	Servidor
				192.168.0.254	Servidor

Tabla 2. 4 Rango de IP's utilizados.

Referencia: Corte Constitucional

2.3 Requerimientos LAN.

En este apartado damos a conocer el método empleado para recolectar las necesidades de los usuarios de la red; utilizando herramientas de investigación y un analizador de protocolos, luego analizamos dichos requerimientos

2.3.1 Metodología

Para el estudio de las necesidades en la Corte Constitucional hemos tomado en cuenta tres fuentes, la información recopilada producto del análisis de la red local actual, consulta a los usuarios y entrevistas al personal de sistemas. Comenzamos el estudio de requerimiento local realizando encuestas con los profesionales, para que nos hagan conocer la utilización de los servicios de los que se les provee y cuáles son sus expectativas o sus demandas.

2.3.2 Requerimientos Físicos de los Usuarios

Se realizó encuestas a un grupo representativo de funcionarios (40%) empleando la técnica de ***muestreo de juicio***, es decir, seleccionamos previamente a individuos que pueden aportar con datos sobre el uso de programas, bases de datos, aplicaciones y recursos para que respondan sobre su utilización.

El personal que fue seleccionado para la encuesta, es el que cuenta con experiencia en el empleo de las herramientas a analizar, es decir, quienes han trabajado un largo período en la institución (más de 4 años). Además, los profesionales de sistemas son la fuente especializada en el tema objeto de este estudio que aportará con sugerencias técnicas.

Estudiaremos la encuesta realizada:

Pregunta 1.

¿Qué herramientas de software utiliza para la realización de su trabajo?

Opción 1: File Magister.

Opción 2: Gestión de Casos.

Opción 3: Archivos digitales de resoluciones desde 1997 hasta 2004.

Opción 4: Administración de contenidos (documentos jurídicos) desde 2000 hasta 2006.

Opción 5: Sistema de sorteo de casos.

Opción 6: otros especifique

El objetivo de ésta pregunta es estudiar la localización de los servidores. Los resultados fueron los siguientes:

Ítems	0 Ítems	1 Ítem	2 Ítems	3 Ítems	4 Ítems	5 Ítems	6 Ítems
% Porcentaje	1	2	2	23	31	22	19

Tabla 2 5 Encuesta de los recursos utilizados por los usuarios internos.

Referencia: Corte Constitucional.

En la tabla 2 5 se expresan los resultados de la pregunta 1, se trata sobre las aplicaciones que utilizan, la mayoría de los encuestados (85%) necesita de más de 3 aplicaciones para realizar su trabajo.

Se puede apreciar que un alto porcentaje de los encuestados trabajan compartiendo información; lo que se justifica porque, funcionalmente las 3 salas operan similarmente.

Pregunta 2.

Considera usted que la computadora y equipos informáticos que le han asignado son:

Opción 1: Muy adecuados.

Opción 2: Adecuados.

Opción 3: Poco adecuados.

Opción 4: Nada adecuados.

Con esta interrogante analizaremos el hardware que se está utilizando para evaluar si es necesario una actualización de equipos.

Ítem	Opción 1	Opción 2	Opción 3	Opción 4
% Porcentaje	19	69	10	2

Tabla 2 6 Resultados encuesta del estado de los equipos informáticos.

Referencia: Corte Constitucional.

Nos damos cuenta que el equipo computacional con el que se trabaja es catalogado por los trabajadores como adecuado. Esto se explica porque cada 5 años, según requerimientos de Contraloría, se deben renovar los equipos en las instituciones del Estado.

Pregunta 3.

Cuando realiza una consulta por Internet la respuesta se despliega:

Opción 1 rápidamente.

Opción 2 medianamente rápida.

Opción 3 lentamente.

Opción 4 muy lentamente.

Formulando ésta inquietud deseamos saber si el funcionamiento de la red es óptimo.

Ítem	Opción 1	Opción 2	Opción 3	Opción 4
% porcentaje	5	33	47	15

Tabla 2 7 Resultados encuesta sobre el servicio de Internet.

Referencia: Corte Constitucional.

Vemos que la mayoría de las opiniones se inclinan a la opción de que el Internet se despliega “lentamente”. A pesar de los resultados, tenemos que estudiar el alcance de la pregunta con objetividad, principalmente porque el tema cae en la subjetividad del usuario, además, éste siempre va querer obtener mayor velocidad; sin importar cuán eficiente sea el servicio. Es por esto que debemos diseñar una red que cumpla con estándares para equilibrar las expectativas de los funcionarios.

Pregunta 4.

En su trabajo con cuántas unidades administrativas interactúa, se comunica o comparte información.

Opción 1: solo una.
Opción 2: entre una y tres.
Opción 3: entre tres y cinco.
Opción 4: más de cinco.
Opción 5: ninguna.

Con ésta consulta queremos tomar en cuenta la segmentación en la red.

ÍTEM	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5
% porcentaje	12	46	34	8	0

Tabla 2 8 Resultados de encuesta interacción entre unidades.

Referencia: Corte Constitucional.

Ser registra que un alto porcentaje de funcionarios (46%) se comunica hasta con 3 departamentos.

Para el caso de las regionales se cuenta con 20 equipos distribuidos de la siguiente manera:

Guayaquil 3, Cuenca 2, Riobamba 5, Ibarra 2, Loja 2, Machala 2, Portoviejo 2 y Orellana 2. Todas de marca hp. Con el sistema operativo Windows XP Service Pack 3 con 1Gb de memoria RAM y procesador Intel ® Core 2 Duo.

En las oficinas regionales se realizan trabajos de capacitación e información. Son oficinas recién creadas que cuentan con equipos nuevos acordes a las necesidades mencionadas.

Se debe prever futuras expansiones basándonos en los objetivos de la Corte Constitucional. Previa entrevista con el Coordinador de las regionales, en un futuro las

demandas, causas, información de las resoluciones serían las principales funciones de las oficinas que se encuentran en las provincias.

2.3.3 Resultados de las Encuestas y Entrevistas

Encuesta.

Preguntas	Resultados
1 Sobre las aplicaciones	85 % utiliza más de 2 aplicaciones.
2 Hardware	69% piensa que los equipos son adecuados.
3 Internet	47% opina que es lento el servicio.
4 Interacción	80 % interactúa con todas las aplicaciones.

Entrevista.

Para el presente trabajo hemos aplicado un método de investigación para saber el estado en que se encuentra la red objeto de este estudio. Son preguntas abiertas.

El personal de Sistemas está consciente de algunos de los problemas en la red, se les propuso el siguiente cuestionario:

Pregunta 1:

¿El presupuesto que destina la Institución para el área tecnológica es suficiente y/o adecuado?

Respuesta:

No, en infraestructura tenemos muchas deficiencias, las mismas que se pueden evidenciar en el espacio asignado al Departamento Tecnológico. Además, algunos servidores sobrepasan los 5 años.

Pregunta 2:

¿Cuáles son los problemas más frecuentes en su Institución? Mencione 3.

Problemas con impresión.

Servicio de Internet.

Correo electrónico.

Pregunta 3:

Si, contara con presupuesto, ¿qué proyecto implementaría primero?

Es importante nuevos servidores.

Pregunta 4:

A más de las herramientas con que cuentan, ¿qué utilitario podrían implementar?

Nos gustaría implementar telefonía IP, puesto que, las líneas telefónicas y las extensiones en la central están copadas.

En el aspecto de hardware son equipos nuevos, no requieren de mucha infraestructura de red porque son pocos usuarios y a futuro (mediano plazo) se estima un crecimiento del 30%.

2.3.4 Análisis de Requerimientos Físicos

La mayoría de los funcionarios en la red LAN de Quito trabajan usando Internet, acceden a consultas en File Magister, requieren saber de información de casos, publicaciones en el Registro Oficial y de los sorteos, es decir, comparten información común es por ésta razón que los servidores deberían ir conectados al backbone principal para su mejor difusión (pregunta 1 de la encuesta).

No es necesario actualizar los equipos informáticos como computadoras, impresoras o escáneres debido a que no exceden los 3 años de utilización (pregunta 2 de la encuesta). Además, como es una empresa Estatal por reglamentaciones de Contraloría los equipos se deben cambiar cada 5 años.

Para determinar si una red se está desempeñando correctamente es necesario tomar en cuenta varios factores. En la parte física hay muchos dominios de colisión y

esto desemboca en un bajo servicio de Internet, sin embargo, las razones pueden incluso relacionarse con el proveedor del servicio o problemas con el servidor. Se puede diseñar una red optimizada creando redes virtuales internas denominadas VLAN's.

De la observación realizada en el área de Sistemas evidenciamos que el área de trabajo destinada para la localización de los equipos informáticos y las conexiones eléctricas, no están lo suficientemente aisladas pudiendo afectar el ambiente de trabajo del administrador de la red; inclusive ésta zona es proclive a crear campos eléctricos o magnéticos que podrían perjudicar a los servidores y a la salud.

Para el caso del departamento financiero están muy bien identificados los aplicativos necesarios, es por esta razón que se podría considerar configurar una subred.

En el área financiera se emplea reportes de personal, registros de asistencia e información contable, se podría considerar la opción de alojar un servidor independiente para el uso de éste departamento, sin embargo, por cuestiones físicas y de seguridad, en el área de sistemas estará bien ubicado. Además, sistemas está en 2 piso y el departamento financiero se encuentra en el tercer piso, de tal manera que no existen limitaciones de distancia.

Como se tiene una demanda de pocas computadoras por cada departamento, una alternativa para el diseño de las redes locales sería la utilización de Access point para distribuir Internet las ventajas del diseño inalámbrico son la ***alta disponibilidad, escalabilidad, administración, arquitectura abierta.*** Además, la instalación no requiere de cableado. Una desventaja es que no es tan segura como una LAN, pero como se maneja información no tan sensible es factible la implementación.

2.3.4 Requerimientos Lógicos de los Usuarios

Del estudio de las encuestas realizadas sabemos que gran parte de los departamentos realizan consultas a los servidores de aplicaciones (pregunta 1), lo que supone, que un diseño de red óptimo ayudará en el desenvolvimiento de las labores del servidor.

Por medio de reportes generados por los servidores estudiamos el uso de los mismos en la tabla a continuación:

Recurso	Resoluciones	Contabilidad	Actas	Fiel Magister	Inventario
Porcentaje	33	17	11	27	12

Tabla 2 9 Resumen del uso de aplicaciones.

Referencia: Corte Constitucional reporte del servidor.

En el cuadro anterior omitimos algunos servicios de red, debido a que los analizaremos más adelante. En éste párrafo nos enfocaremos en la información local y vemos que la mayoría de la carga es hacia el servidor que contiene el repositorio de las Resoluciones, seguida por la aplicación Fiel Magister y por último las consultas relacionadas con el área financiera. Es por esto que se debe considerar la comunicación con los servidores como prioridad. Más específicamente se puede considerar el protocolo de transferencia de archivos (FTP), para lo cual, es necesario contar con una red óptima que provea una velocidad de transferencia alta.

Otra herramienta que utilizamos para estudiar los requerimientos lógicos de los usuarios es un sniffer, en éste caso, hemos seleccionado trabajar con el software SoftPerfect Network y específicamente con el analizador de protocolos. Es una versión de prueba que permite monitorear una red local para comprender el tráfico que se genera. Dicha aplicativo “Está dirigido a administradores de sistemas y usuarios en general interesados en la seguridad informática”[17].

[17] SoftPerfect, *Network Scanner*, Internet: http://www.softperfect.com/products/networkscanner/, Acceso: 08/diciembre/2011.

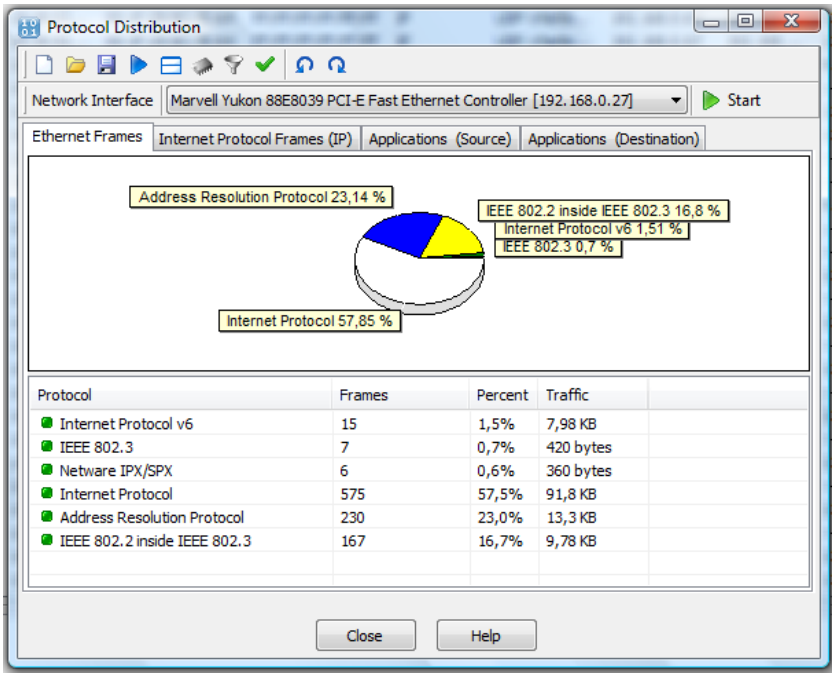


Gráfico 2 28 Analizador de protocolos.

Referencia: Herramienta SoftPerfect aplicada en la red de la Corte Constitucional.

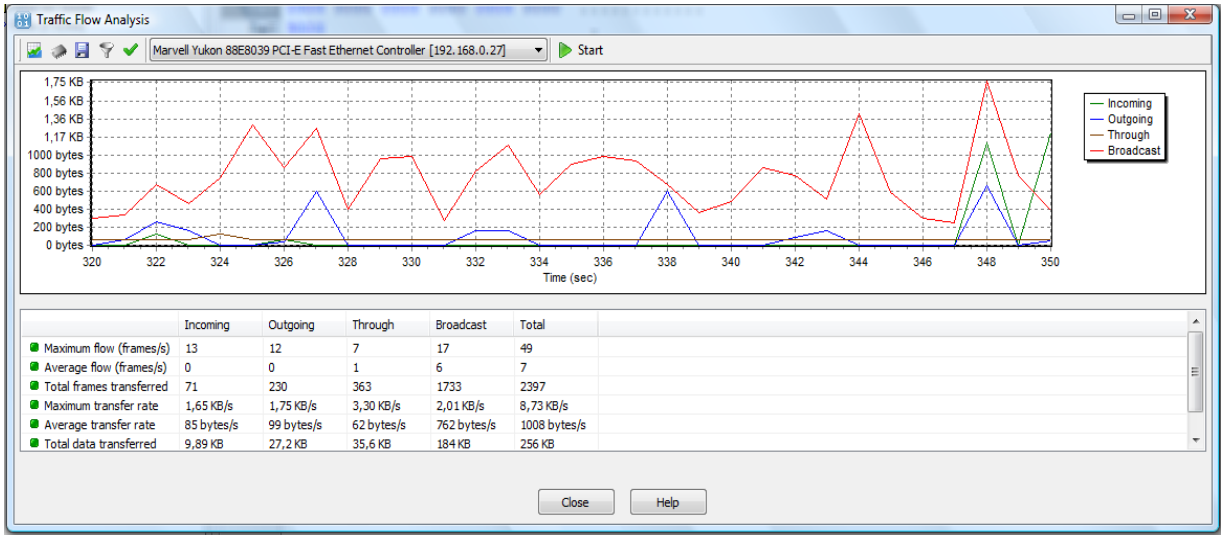


Gráfico 2 29 Análisis de Flujo de Tráfico

Referencia: Herramienta SoftPerfect aplicada en la red de la Corte Constitucional.

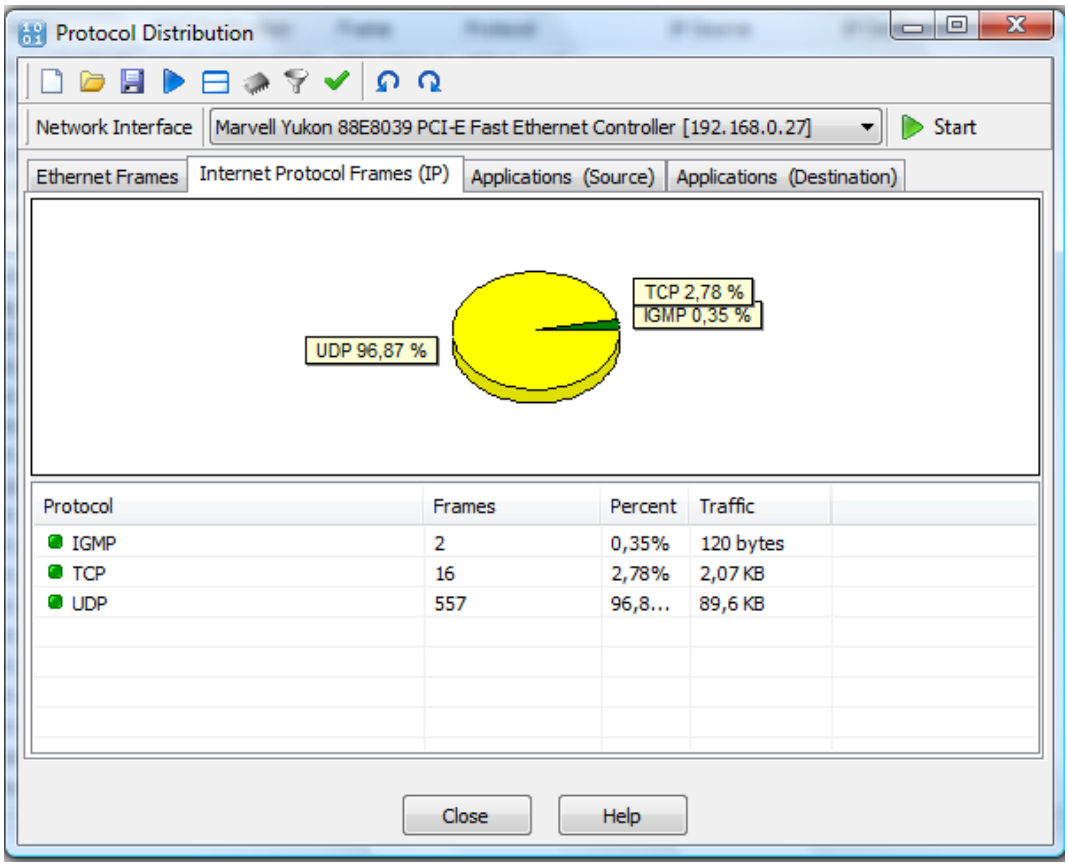


Gráfico 2 30 Análisis tramas de protocolo de internet.

Referencia: Herramienta SoftPerfect aplicada en la red de la Corte Constitucional.

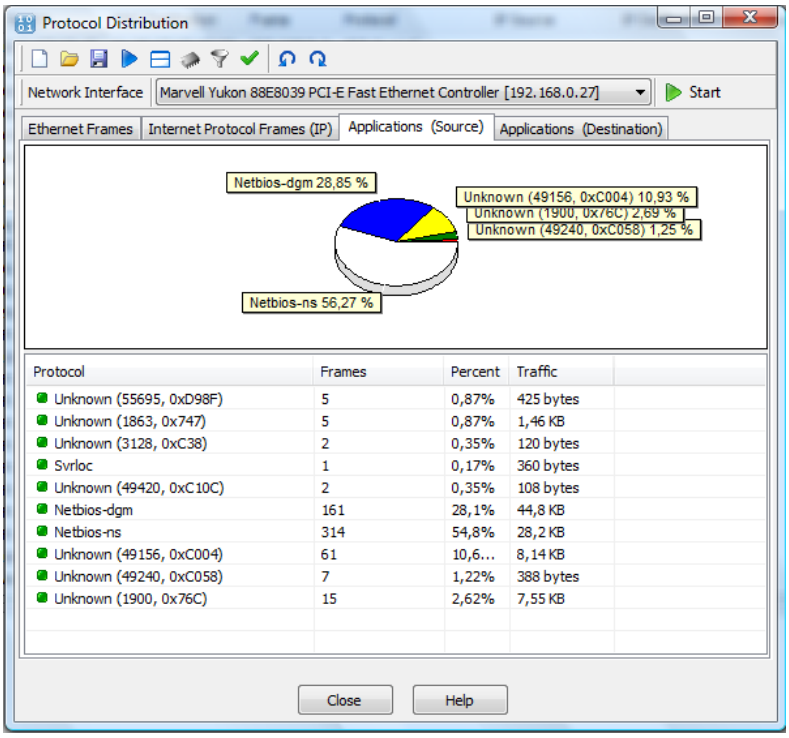


Gráfico 2 31 Análisis de aplicaciones origen

Referencia: Herramienta SoftPerfect aplicada en la red de la Corte Constitucional

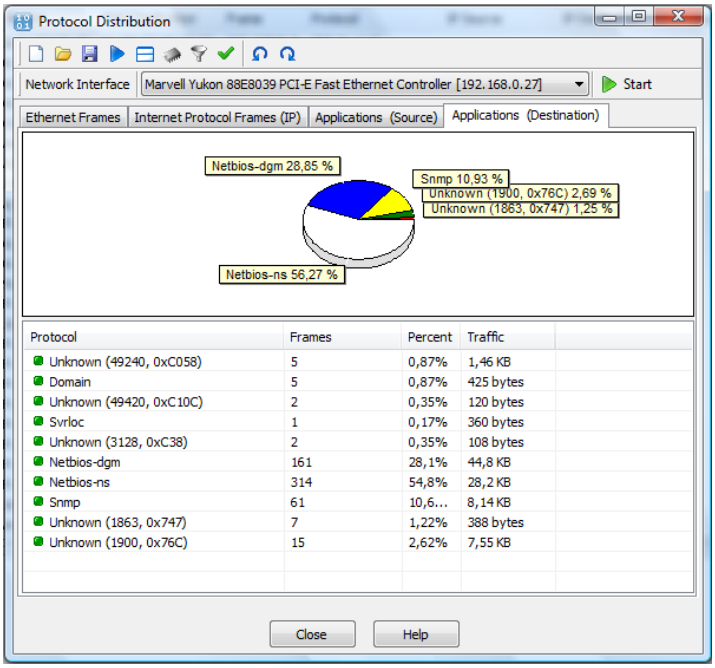


Gráfico 2 32 Análisis de aplicaciones destino.

Referencia: Herramienta SoftPerfect aplicada en la red de la Corte Constitucional.

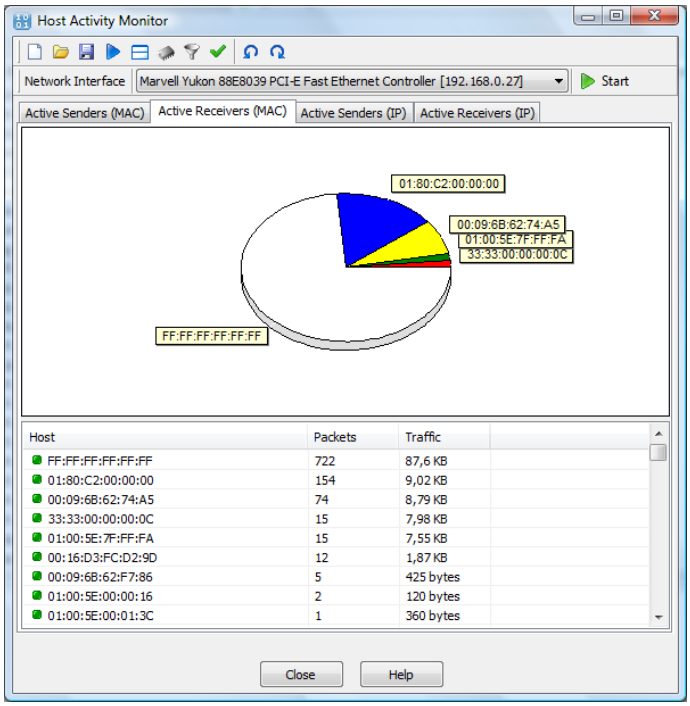


Gráfico 2 33 Recibo activo de MAC.

Referencia: Herramienta SoftPerfect aplicada en la red de la Corte Constitucional

Estudiando los cuadros comparativos de uso de recursos vemos que el protocolo de Internet obtiene un 57,5% de uso, seguido obviamente por el protocolo de resolución de direcciones ARP 23% debido a que son complementarios y actúan conjuntamente. El protocolo IEE 802.3 obtiene un 16% importante para evitar las colisiones en la red.

El edificio cuenta con 11 pisos en cada uno de ellos se encuentra una unidad o subunidad administrativa.

Actualmente los funcionarios se encuentran distribuidos de la siguiente manera:

PISO	UNIDADES	PC's
Planta baja	Documentación / Registro Oficial / Archivo	7
Primer piso	Secretaría / Biblioteca	14
Segundo piso	Sistemas / Comunicación / Asesoría Jurídica	15
Tercer piso	RRHH / Adquisiciones / Contabilidad / Tesorería	15
Cuarto piso	Coordinación regional /	8
Quinto piso	Primera sala	12
Sexto piso	Tercera sala	14
Séptimo piso	Segunda sala	16
Octavo piso	Secretaría (reparación)	----
Noveno piso	Presidencia	7
Décimo piso	Pleno y Asesores	11

Tabla 2 10 Distribución de las Unidades Administrativas por pisos

Referencia: Corte Constitucional.

2.3.5 Análisis de Requerimientos Lógicos

Con la distribución física estudiada debemos partir de las funcionalidades, agrupar las comunes y mejorar el desempeño de la red.

En la institución objeto de éste estudio se ha implementado un switch en cada piso excepto en planta baja donde los host se conectan al equipo ubicado en el primer piso. Temporalmente se trasladó el switch del octavo piso al piso uno por un asunto de remodelación. Es así que, encontramos 10 switches conectados al cableado vertical (backbone), por ende, 10 dominios de difusión. Además, estudiando el mapa detallado de la red, encontramos conectados switches a impresoras, lo que segmenta aún más la red, disminuyendo su desempeño.

La implementación de la red de datos de la Corte Constitucional en su parte lógica se basa en la ubicación geográfica de cada host, lo cual, es recomendable cuando la red no abarca muchas máquinas.

Se puede considerar una mejor distribución lógica con la creación de VLAN's o redes locales virtuales, que optimizan los dominios de difusión, ya que las VLAN's no dependen de la localización de los switches. En una red virtual local los equipos se comunican sólo con otros dispositivos que pertenecen a esa red. También, el hecho de que cada VLAN es independiente, significa que no comparten difusiones, lo que mejora el rendimiento.

Una ventaja de la disposición VLAN es que permite aumentos, cambios sin la utilización de nuevas conexiones, siempre y cuando, los host pertenezcan a la misma red, cualquier nueva distribución es aceptada.

En las regionales se tienen pocas máquinas, las mismas que realizan una labor importante que no demanda mucha infraestructura de red, es así que, con la implementación de una red wireless local se puede satisfacer los servicios de Internet y correo que son los que se emplean para complementación del trabajo.

2.4 Requerimientos WAN.

2.4.1 Antecedentes

Con la aprobación de la nueva Constitución de la República se crea la Corte Constitucional el 20 de octubre de 2008 en el registro oficial 449, artículo 429 con el objetivo de mantener un control, interpretación y administración de justicia constitucional ***con jurisdicción nacional***.

Por los antecedentes enunciados, el rol de la Corte Constitucional se extiende, es así que, se han establecido oficinas estratégicas en: Guayaquil, Cuenca, Riobamba, Ibarra, Loja, Machala, Portoviejo y Orellana para servir de nexo de comunicación con la ciudadanía y proveer información en lo referente a la administración de justicia constitucional. Para la fecha en la que se realiza el estudio, la institución se encuentra en una fase de transición definiendo los alcances de las sucursales zonales. En éste trabajo propondremos una solución para los requerimientos actuales pero, tomando en cuenta la escalabilidad de la red.

2.4.2 Requerimientos WAN de los usuarios

En el Plan operativo del período de transición para el año 2009 publicado en la página Web (http://www.tribunalconstitucional.gov.ec/documentos/Direccionamiento_Estratégico.pdf

), Se menciona como un objetivo primordial el fomentar el acceso a la justicia, es decir, una cultura constitucional y de derechos. También, en el plan estratégico se establece textualmente como directriz la ***"Incorporación de herramientas tecnológicas que soporten mejoras continuas en los servicios de justicia constitucional y gestión interna institucional".***

La creación de las oficinas regionales es reciente; hoy en día, están en un proceso de planificación organizacional y acoplamiento. Para la obtención de los requerimientos se mantuvo entrevistas con el coordinador de las mencionadas dependencias, además, con el asesor jurídico de la Presidencia. En dichas reuniones se manifestó hacia donde

se perfilan los alcances y la relación de los departamentos foráneos con la sede quiteña.

En la actualidad ya está elaborado el reglamento interno, por lo que, nos basamos en su contenido. El deseo es que las sedes realicen las mismas funciones que la unidad administrativa Secretaría General, de esta manera, se aligera el volumen de las causas.

Según el reglamento las funciones de la Secretaría (artículo 54) y por ende las de las regionales (artículo 55) son:

Art. 54.- Funciones del Secretario General.- son funciones de la Secretaría o del Secretario General de la Corte Constitucional las siguientes:

Dirigir la Secretaría General.

Asistir a las deliberaciones de la Sala Plena. Sin voz sin voto.

Coordinar el proceso de elaboración de las actas de las sesiones de la Sala de la Corte.

Coordinar los procesos de archivo y custodia de expedientes y correspondencia de la Corte.

Supervisar el proceso de sorteo de los casos entre las distintas salas y juezas y jueces de la Corte.

Elaborar, bajo la supervisión de la Presidencia o del Presidente, el orden del día de la Sala Plena.

Coordinar, conjuntamente con la Presidencia o Presidente de la Corte el proceso de citación a las juezas y jueces a las sesiones de las diferentes salas de la Corte.

Notificar las providencias de la Corte y ordenar su publicación en la Gaceta Constitucional y el Registro Oficial.

Expedir las certificaciones que correspondan.

Las demás que le asigne la Presidencia o Presidente, La Sala Plena o el reglamento interno de la Corte.

Art. 55.- Oficinas Regionales.- las funciones de la Secretaría General podrán ser desarrolladas de manera desconcentrada a través de oficinas regionales establecidas en el territorio del Ecuador.

Además de las funciones de Secretaría General, estas oficinas ejecutarán un programa de capacitación constitucional para la ciudadanía en el ámbito de su jurisdicción.

Resumiendo; hasta que se tenga un sustento legal y presupuestario de las funciones de las oficinas regionales, éstas se dedicarán a la difusión y capacitación de los derechos constitucionales.

De ésta manera se debe planificar una infraestructura que permita una posible extensión futura.

2.4.3 Requerimientos WAN de Hardware

Por el momento no se requiere de una interacción continua con la sede central en Quito, debido a que, el objetivo de las sucursales es meramente informativo y de capacitación. Sin embargo, en un futuro o a mediano plazo (un año) se planea que cada regional resolverá casos menores, además, recomendará qué causas deberían ser tratadas en última instancia por el Pleno de la Corte.

Entonces, podemos considerar dos escenarios, uno inicial donde se instalen servidores en cada regional para que cada cierto tiempo se sincronicen entre ellos y otra a largo plazo donde se interconecten con la red quiteña que, además, considere la implementación de servicios como videoconferencias, video llamadas y servicios en tiempo real.

Sí, tomamos en cuenta el primer escenario, necesitaríamos adquirir 9 servidores uno para cada una de las regionales. En éste servidor se almacenaría la información para cada caso a tratarse esté a disposición y pueda ser objeto de consulta. En una

fase inicial no es necesario servidores específicos, bastaría computadores de las siguientes características:

Marca: HP

Modelo: DX2400

Procesador: Core 2 Duo E7300 2,6 GHz 1066 MHz 3MB)

Disco: 250 GB SATA

Memoria: 1 Gb.

Red: red Gigabit

Sistema operativo: Windows Vista Downgrade to XP Pro.

Para éste objetivo, se debe conseguir un enlace de 64 Kbps que permita un establecimiento de llamada rápido. No es necesario el transporte de información de video, así que, se podría contratar un enlace BRI RDSI.

Para el segundo posible contexto se necesita contratar un agente de servicios que permita el transporte de datos multimedia (voz, video y datos) ***dedicado*** desde y entre las oficinas principales con las regionales. Luego, se procederá a la compra de los equipos que deben tener tecnología H.323 (multimedia).

Se demanda el tráfico de voz y datos constantemente, mientras que, para video se solicitará hasta un par de veces por mes.

2.4.4 Requerimientos WAN de Software

Del estudio de las competencias y del diálogo con representantes fácilmente deducimos que en lo que se refiere a software las 8 dependencias necesitaran de los mismos programas que se utilizan en el dominio ***cce.gov.ec***, es decir, lo siguiente:

File Magister, lo que no es problema porque es una aplicación no sujeta a cambios es una herramienta netamente de consulta.

Sistema de gestión de casos, aquí recae la sensibilidad del problema porque es información que necesita de actualizaciones.

Archivos digitales de resoluciones desde 1997 hasta 2004. No representa mucho problema ya que es una aplicación de acceso y modificaciones no muy frecuentes.

Administración de contenidos (documentos jurídicos) desde 2000 hasta 2006. Similar al caso anterior de los archivos digitales.

Sistema de sorteo de casos se necesita interacción con las sucursales lejanas lo que dificulta al empatar la información.

2.4.5 Análisis de los Requerimientos WAN

Vamos a considerar dos posibles escenarios para el estudio de la red WAN.

Las funciones de las oficinas regionales se mantienen como informativas y de carácter pedagógico.

Las funciones de las oficinas regionales cambian, pasan a desempeñar las funciones de la Secretaría General y disponen de un presupuesto alto.

En el ***primer caso*** solo es necesario diseñar la red local que comparta información que, por ser pocas máquinas, se aconseja una red Wireless por versatilidad al momento de la instalación, bajo costo y fácil administración.

Sí, se pretende actualizar información interactuando con los servidores no en tiempo real no se necesita enlaces dedicados WAN, bastaría con un enlace de circuito conmutado para sincronizar los servidores.

Para el ***segundo caso*** debemos considerar las especificaciones de voz, las cuales, deben ser:

Determinar los canales de voz.

Elaborar un plan de numeración.

Selección de equipos.

Para las sucursales con las que se cuenta tendremos los siguientes canales:

OFICINAS	CANALES DE VOZ	PUERTOS
Ibarra	1	FXS
Riobamba	1	FXS
Cuenca	1	FXS
Guayaquil	1	FXS
Loja	1	FXS
Machala	1	FXS
Portoviejo	1	FXS
Orellana	1	FXS

Tabla 2 11 Canales de voz.

Referencia: Corte Constitucional.

En cada sucursal tenemos un canal por lo que es necesario un ancho de banda de 64 Kbps.

Para el caso de la videoconferencia a través de redes IP se necesita un ancho de de banda de 128 Kbps. No se necesita entablar conferencias al mismo tiempo (multiconferencia), es decir, tan solo con enlaces punto a punto se satisface la necesidad.

Se puede contratar un ancho de banda de 64 Kbps y para las fechas en que se requiera transmitir videoconferencia llamar al proveedor ISP para aumentar el ancho de banda.

El servicio de tele conferencia abarataría los costos por movilización de los funcionarios y también, porque el servicio se lo puede hacer por Internet cuidando que la diferencia entre retrasos no sea variable y el tiempo de respuesta aceptable eliminando errores en la última milla ***(BER=0, Bit Error Rate)***.

3. SEGURIDAD EN REDES.

El desarrollo de las redes ha incorporado en el ambiente laboral ventajas como la compartición de información y de recursos. Sin embargo, no todos los elementos son de dominio público, hay documentación restringida para el personal interno y externo; es necesario entonces discriminar su uso. La mejor forma de implementar restricciones favorables, es establecer adecuadas normas de seguridad.

Para empezar con el estudio de una red segura empezaremos con identificar:

- ¿Qué componentes son los más sensibles?
- ¿Cuáles son los recursos prioritarios a proteger?
- ¿Cuál es el impacto al implementar normas de seguridad?
- Reconocer las amenazas a las que la red estará expuesta.
- Estudiar los costos versus los beneficios de implementar la seguridad
- Respuestas ante incidentes.

Cuando proporcionamos soluciones a cada uno de los ítems anteriores contribuimos al proceso de mantener la protección de los recursos. Es un proceso continuo que implica monitoreo constante.

En el caso del presente estudio (Corte Constitucional) se identifica como relevante la información que circula por la red interna (Intranet) y externa (Internet). Se manifiesta lo siguiente: "… procesos o trámites, el estado en que se encuentran los autos, sentencias y dictámenes…". (Corte Constitucional, "La Corte Constitucional". Internet. www.tribunalconstitucional.gov.ec. Acceso: (jueves, julio 08, 2010)). En conclusión, puesto que, la Institución cumple con una función de carácter público, la prioridad es la información generada visible a la ciudadanía.

Las consecuencias de no implementar seguridad afecta negativamente al giro del negocio, porque los resultados de los procesos principales se transportan por la red y una pérdida de información implicarían perder todo el trabajo previo; tomemos en cuenta que los pronunciamientos de la Corte obedecen a varias fases y en cada fase se emplea gran cantidad de recursos.

Existen amenazas internas y externas que pueden ser prevenidas con un plan de contingencia adecuado, además, reglas de comportamiento para el personal y acciones proactivas ante incidentes.

El costo en el que se incurra beneficia positivamente en el desempeño de las labores de la Institución.

3.1 Vulnerabilidades en una Infraestructura de Red

El principal motivo de los ataques informáticos es el factor económico, se estima que anualmente se pierden millones de dólares relacionados con el robo de información; existen muchas formas fraudulentas de ataques entre las que podemos citar: reproducir programas o software con derechos de autor, hackear sistemas para obtener información confidencial, ataques de denegación de servicios (DoS), virus, entre otros.

3.1.1 Amenazas Contra la Seguridad de la Empresa

Los ***ataques de repetición*** utilizan componentes que captan contraseñas previamente utilizadas para emplearlas posteriormente y acceder a la aplicación, se recomienda utilizar programas que identifiquen la reutilización, es decir, denieguen la entrada si se registra una entrada ya registrada.

Ataques de diccionario hace referencia cuando un infractor obtiene una lista de contraseñas encriptadas, y debido a que, el registro de una contraseña responde a una función unidireccional fácil de computar pero difícil de decodificar, el atacante busca y compara las contraseñas conocidas encriptadas con la misma función hasta encontrar una contraseña que se repita. Para evitar ésta irregularidad se aconseja seguir las siguientes normas para establecer contraseñas:

- Longitud de al menos ocho caracteres.
- Combinación de minúsculas y mayúsculas.
- Incluir caracteres especiales (¡”#$%&/).
- Combinación de números y letras.

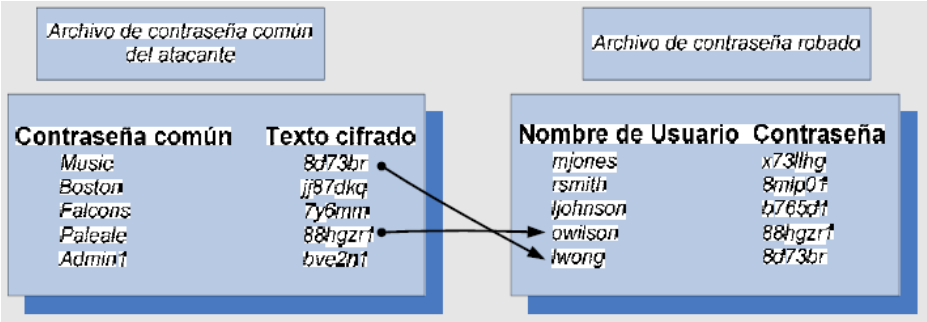


Gráfico 3 1 Ataques de diccionario.

Referencia: Realtime publishers CA., Capítulo 2, Amenazas contra la seguridad de la empresa, página 35.

Alteración y destrucción son amenazas con un alto porcentaje de aparición entre las más comunes se encuentran los ***virus, ataques de negación de servicio, correo fraudulento, explotar un navegador de Internet, spam*** entre otros***.*** Los ataques DoS negación de servicios tienen por objetivo saturar los recursos de un sistema y colapsar a los mismos de manera que los usuarios no accedan a las aplicaciones. Se puede generar DoS inundando de tráfico basura (***packet flooding***), o enviando solicitudes falsas de conexión utilizando IP's ficticias. Últimamente, existen los denominados DDoS que consiste en ataques coordinados desde varios sistemas, la metodología comienza con un atacante que aloja la amenaza en varios dispositivos (***zombies***) y saturan coordinadamente el ataque.

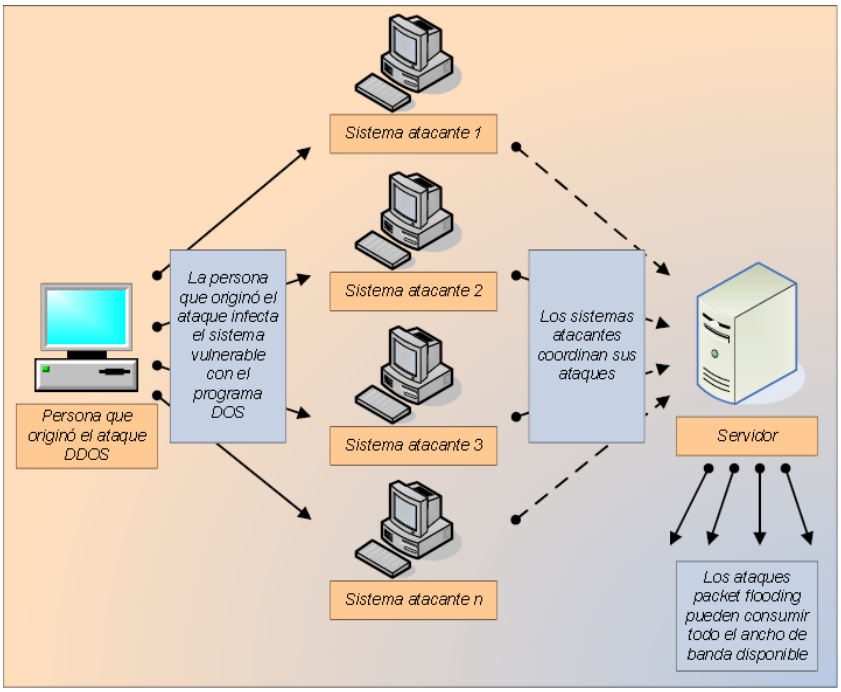


Gráfico 3 2 Ataques DDos. Referencia

Realtime publishers CA., Capítulo 2, Amenazas contra la seguridad de la empresa, página 38.

Riesgos internos y puertas traseras se relacionan con los peligros que se generan dentro de la empresa por empleados insatisfechos y se pueden clasificar entre ataque DoS interno, robo de información confidencial, asignación indebida de privilegios adicionales y fraude.

Domain Spoofing de esta manera se denomina al correo fraudulento; "en términos de seguridad de redes hace referencia al uso de técnicas suplantación de identidad"[18]. Este tipo de ataque afecta al servidor de nombres de dominio DNS desviando el tráfico de un destino correcto a uno no autorizado como se indica en el gráfico a continuación.

[18] Wikipedia. *Spoofing*. Internet. http://es.wikipedia.org/wiki/Spoofing Acceso: 08/diciembre 2011.

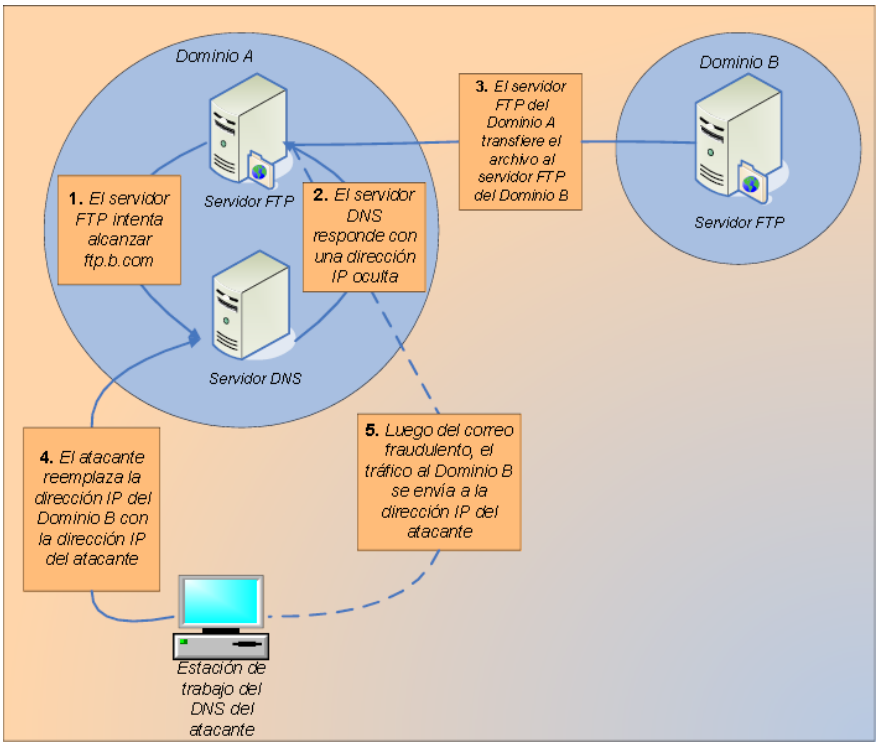


Gráfico 3 3 Ataque Domain spoofing.

Referencia: Realtime publishers CA., Capítulo 2, Amenazas contra la seguridad de la empresa, página 41.

A los virus se los puede clasificar de tres maneras: ***no cifrados o estáticos, cifrados y polimórficos***, mencionada división se debe a la manera en que el virus logra persuadir la detección. Los componentes de un virus son:

1. Carga útil.
2. Método de propagación.
3. Condición de activación.

La carga útil es la acción consecuente del virus, puede ser desde desplegar un mensaje, o hasta borrar archivos importantes. La propagación puede darse a través de copias o infectando cierto tipo de formatos. La activación de un virus puede ocurrir en una fecha previamente escogida, ó al abrir un archivo infectado.

Los virus no cifrados son fáciles de detectar por un antivirus; lo hace detectando patrones de identificación de códigos. Los virus encriptados deben llevar en la carga útil la clave de decodificación y el código de decodificación; códigos que pueden ser detectados por el software antivirus. Los virus polimórficos utilizan un motor de mutación modificando el virus a medida que se propagan; para detectar éste tipo de virus se toma en cuenta patrones de operación, otros métodos incluyen entornos virtuales para que actúe el virus y poder descubrirlo.

Otras formas de malware son el ***spyware*** o software espía, ***Keylogger***, tarjetas para ***captura de video y rootkit***. El spyware procede rastreando los patrones de uso para enviar las preferencias de un usuario a empresas publicitarias o a un atacante. Los keylogger capturan el texto digitado por un usuario utilizando funciones de bajo nivel del sistema operativo como los hooks (conexiones). Las tarjetas de captura de video o screen scrapper almacenan imágenes de documentos o correos contenidos en el buffer de video. Por último, los rootkit permiten ocultar archivos, modificando datos de bajo nivel del sistema operativo; son muy difíciles de detectar.

Spam o correo basura inunda el tráfico en una red y consume los recursos de la misma como el ancho de banda espacio de almacenamiento entre otros, además, el costo para evitarlos son altos. Son correos “no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario”[19]

Existe la posibilidad de encontrarse con virus combinados que poseen varias características, como hace referencia el gráfico a continuación.

[19] Wikipedia. *Spam*. Internet. http://es.wikipedia.org/wiki/Spam Acceso: 08/diciembre 2011.

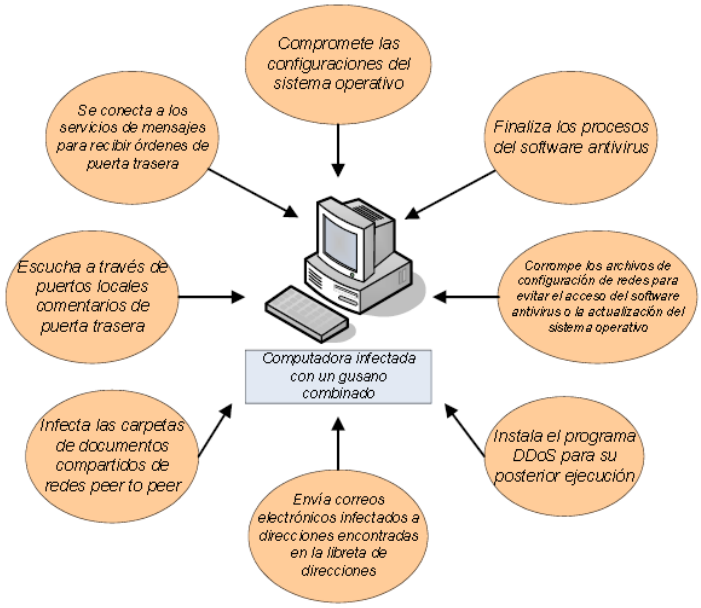


Gráfico 3 4 Ataque combinado.

Referencia: Realtime publishers CA., Capítulo 2, Amenazas contra la seguridad de la empresa, página 48.

Además, del robo de información existe el robo de identidad de marcas denominado ***phishing***, que consiste en falsificar sitios web para obtener datos confidenciales de los usuarios; funciona cuando el atacante envía un correo donde solicita al usuario que ingrese a un sitio web fraudulento diseñado para engañar, haciendo creer que es el sitio oficial de un banco o cualquier sitio que maneje información de la que se pueda sacar ventaja y exige la actualización de datos y contraseñas para utilizarlos en los sitios oficiales. Principalmente, se caracteriza "por intentar adquirir información confidencial de forma fraudulenta"[20]

3.1.2 Puntos Inseguros en una Red

En una infraestructura de red existen muchas debilidades que pueden ser aprovechadas por personas inescrupulosas, sin embargo, podemos dividirlas en tres grandes grupos:

[20] Wikipedia. *Phishing*. Internet. http://es.wikipedia.org/wiki/Phishing Acceso: 08/diciembre 2011.

- Acceso no autorizado.
- Suplantación de identidad
- Denegación de servicio.

A continuación, estudiaremos los puntos vulnerables de algunos protocolos relacionados con una infraestructura de red. Empezaremos con TCP/IP, luego con ICMP, UDP, NNTP, HTTP, SMTP, FTP, NFS/NIS, para finalizar con X Windows.

Para comunicarse a través de TCP/IP en una red, es necesario contactarse (conexión) con el dispositivo de origen de envío de datos (servidor); la comunicación de entre estos dos elementos (cliente - servidor) se realiza en 4 pasos:

El cliente envía un paquete con varios datos, entre ellos, un número de secuencia que debe ser comprobado.

El servidor emite un paquete de respuesta con el número de secuencia recibido aumentado en 1.

El cliente acusa recibo aumentando una unidad en el número de secuencia que recibió del servidor.

Comienza la transmisión de los datos.

El intercambio de números de secuencia no es aleatorio, por lo que, es fácil que un atacante pueda adivinar el proceso. El infractor comenzaría estableciendo una conexión TCP/IP válida con el servidor, registrándose con una IP de origen falsa, que obtuvo de un host confiable, posteriormente, se atacaría al host verdadero con un ***ataque de denegación de servicio*** para imposibilitar su respuesta sí, el intruso logra adivinar la secuencia que envió el servidor, la transmisión de información comenzará; a éste tipo de ataque se lo denomina ***ataque de número de secuencia*****.**

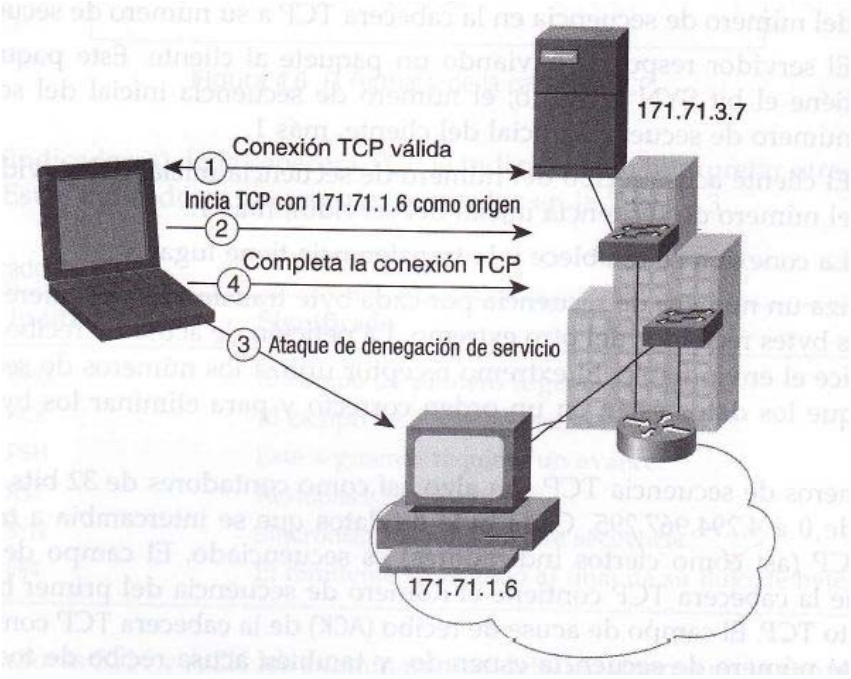


Gráfico 3 5 Ataque de número de secuencia.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 130.

Existe un caso de falseamiento de sesión TCP/IP denominado ***secuestro de sesión*** y se produce cuando un atacante controla una sesión entre dos host enviando información para apropiarse de la sesión de un host legítimo; el intruso continúa enviando información hasta que finalmente, obtiene los mismos privilegios del host auténtico.

Vamos a referirnos a un caso conocido como de ***ataque de SYN (sincronización) de TCP***, que se efectúa durante el proceso de comunicación entre dos host. Cuando un host de destino espera un acuse de recibo de un host de origen, se genera una cola por un tiempo determinado que controla las conexiones TCP. Si, un intruso desea acceder a la cola de conexión con fines maliciosos, el intruso genera paquetes SYN de origen con IP's falsas, para que el host de destino genere paquetes SYN/ACK (acuse de recibo) destinados al host con IP falsa, lo que producirá la cola de conexión y eventualmente un atacante puede denegar las conexiones.

El ***ataque land .c*** se utiliza para ataques de denegación de servicio (DoS). Envía paquetes de sincronización de TCP, tratando de confundir al sistema operativo, propagando la dirección de destino como el origen y el destino, además, utilizando el mismo puerto en el origen y destino. Este hecho genera que algunos sistemas colapsen.

En la capa de transporte del modelo de referencia OSI encontramos al ***protocolo UDP***, mismo que se basa en el envío no fiable de datagramas y no es orientado a conexión, es decir, no registra errores ni ningún tipo de protección. Mencionadas particularidades hacen vulnerables a los datagramas para ser falseados.

ICMP, significa protocolo de mensajes de control de Internet y forma parte del protocolo TCP/IP, la función de éste estándar es de enviar mensajes de error cuando ha ocurrido uno. Problemas como no alcanzar un router o un host y notificar que un servicio no se encuentra disponible; son algunas tareas que realiza ICMP. Debido a que TCP/IP está orientado a la entrega de paquetes, es indispensable encontrar una manera de comunicarse con otro protocolo de un nivel superior indicando la entrega exitosa del mensaje, caso contrario enviar una señal de error.

Una debilidad de ICMP es lo que se conoce como el ***ping de la muerte***, que no es más que, explotar la fragmentación de paquetes ECHO de ICMP (ping). Lo permitido en el paquete de petición ECHO es de 65.507 octetos, la fragmentación permite sobrepasar dicha cifra porque los paquetes se dividen para el envío, pero sólo se procesan hasta que lleguen todos los fragmentos, existiendo la posibilidad de el desbordamiento de variables internas de 16 bits o volcados de kernel.

El ***ataque SMURF*** se produce cuando un agresor envía una gran cantidad de peticiones ECHO de ICMP fraudulentas, con el fin de colapsar el tráfico que puedan generar los equipos que responden a dicho requerimiento.

Otro ataque de fragmentación es ***teardrop.c*** que afecta al re ensamblaje con fragmentos superpuestos para lograr que los sistemas de destino colapsen o no funcionen.

Para el intercambio de noticias entre servidores y lectores se utiliza el ***protocolo de transferencia de noticias de red (NNTP)***, el problema del protocolo es que no

implementa mecanismos de autenticación, haciendo vulnerable la información contenida en los mensajes, dicho de otra forma, se puede alterar las noticias antes de que sean publicadas o eliminar grupos de noticias.

El protocolo ***SMTP o protocolo de simple transferencia*** permite lo que se conoce como el correo electrónico, una debilidad de éste elemento es la carencia de métodos de autenticación, integridad y confidencialidad. Actualmente, existen programas como S/MIME, o Pretty Good Privacy (PGP), que permiten suplir las deficiencias mencionadas.

A través del correo se identifican dos opciones de riesgo para un sistema de red la primera es el demonado ***ataque spam***, que consiste en el envío de correo a cientos de miles de destinatarios, produciendo sobrecarga de las conexiones de red, uso de todos los recursos y sobrecarga del disco duro. En segundo lugar, ***bombing*** se denomina al envío repetido de un correo idéntico a una dirección específica con el objetivo de neutralizar la comunicación.

FTP, protocolo de transferencia de archivos, es uno más, del conjunto de protocolos de TCP/IP que permite almacenar y consumir archivos. Utiliza dos conexiones, una de control y otra de conexión. Cada requerimiento FTP utiliza un número de puerto para cada nueva transferencia, hecho que podría producir inconvenientes al bloqueo de transacciones iniciadas externamente porque, los filtros de paquetes bloquearán los datos entrantes desde el servidor.

En una red corporativa se puede encontrar los servicios ***NFS*** y ***NIS*** (sistema de archivos de red y de información de red, respectivamente). NFS se utiliza para acceso a sistemas de archivos remoto de forma local. NIS sirve para proporcionar servicios a bases de datos centrales, generalmente para el registro de usuarios en un ambiente cliente – servidor. Debido a que los dos aplicativos trabajan con protocolo UDP, el sistema de autentificación tiene limitaciones, por lo que, es altamente recomendable evitar que éste tipo de tráfico circule por los puntos de entrada y salida de la red.

X Window System comparte recursos como teclado, ratón y ventanas a sus clientes X. La interfaz gráfica trabaja bajo el protocolo X11, que carece de métodos de autenticación robustos, por lo que, tráfico X11 debe estar restringido sólo a los host internos.

Por último, el implementar procedimientos seguros para el personal de una empresa ***(ingeniería social)*** es muy importante, porque no importaría cuántos recursos de software o hardware utilicemos, si no se complementa con el medio humano, no se conseguirá el objetivo, una red segura.

3.2 Bases para Establecer Seguridad Física de Red.

Como se comentó anteriormente, para la Corte Constitucional es importante la información que circula por la red de datos, es por eso, que el diseño de una red segura juega un papel prioritario.

Para comenzar hemos de restringir la manipulación de los equipos que abastecen a la red, es decir, implantar controles físicos.

3.2.1 Medios Físicos.

Al decidir implantar una red segura, los medios físicos toman un papel significativo porque existen elementos que proporcionan más fiabilidad que otros. Por ejemplo, el transportar información por un cable de hilos de cobre aislados (UTP par trenzado sin apantallar), es menos seguro que emplear fibra óptica, puesto que, el envío es susceptible a pérdidas. En el otro caso (fibra óptica), el medio es resistente a perdidas y por ende más confiable. De lo expuesto en el párrafo anterior, se deduce, que para los datos sensibles es aconsejable usar tecnología de fibra óptica, mientras que, para servicios de distribución y otros no tan prioritarios podemos ayudarnos del cable UTP. En el caso que nos compete, proponemos utilizar fibra óptica para el backbone de datos, es decir, para la vía principal que enlaza la información y las aplicaciones (servidores) con los conmutadores de cada piso.

Gráfico 3 6 Medios de transmisión

Referencia: Internet
http://electrocentro.com.mx/index.php?num=14&pro=3&nombre=Conductores&PHPSESSID=15841ec67ca196c5143c8eee5f042a32

En el caso de utilizar fibra óptica si una persona irrumpe físicamente sobre el medio de transmisión con el objetivo de obtener datos, denominamos al hecho como una escucha ilegal. Para detectar intromisiones no autorizadas se utiliza un reflectómetro de dominio temporal (TDR), que es un instrumento que identifica la degradación de la que es objeto la red cuando se produce la escucha ilegal.

Por lo mencionado es altamente recomendable utilizar fibra óptica cuando se necesita dirigir grandes cantidades de información (ancho de banda) de manera segura (información confidencial).

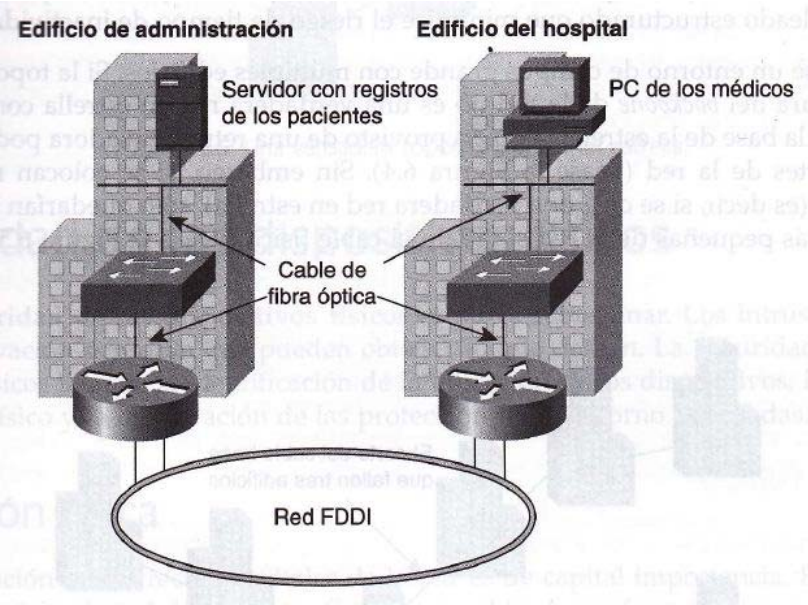


Gráfico 3 7 Uso correcto de medios de transmisión.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 167.

Hoy en día se reportan pocas escuchas ilegales a través de vulneraciones físicas, debido a que, en una red existen tantas estaciones de trabajo que un intruso puede poner a su controlador de red en modo promiscuo (solicitar acceso) para que cuando un usuario autorizado termine su conexión, ingresar lógicamente con una dirección IP permitida.

En conclusión y para el caso de estudio escogeremos fibra óptica para backbone, puesto que, es el canal principal por donde circulara la información y utp categoría 6 para distribuir los demás servicios.

3.2.2 Topografía de Red.

Al hablar de topología de red nos referimos a la ruta o el camino por donde circulará la información.

En lo que se refiere a la topografía de red o a la dirección física de los medios, se aconseja establecer una configuración en estrella, para que en el caso de ruptura de conexión se afecte solo a ese segmento y no a varios puntos.

Gráfico 3 8 Topología no adecuada.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 168.

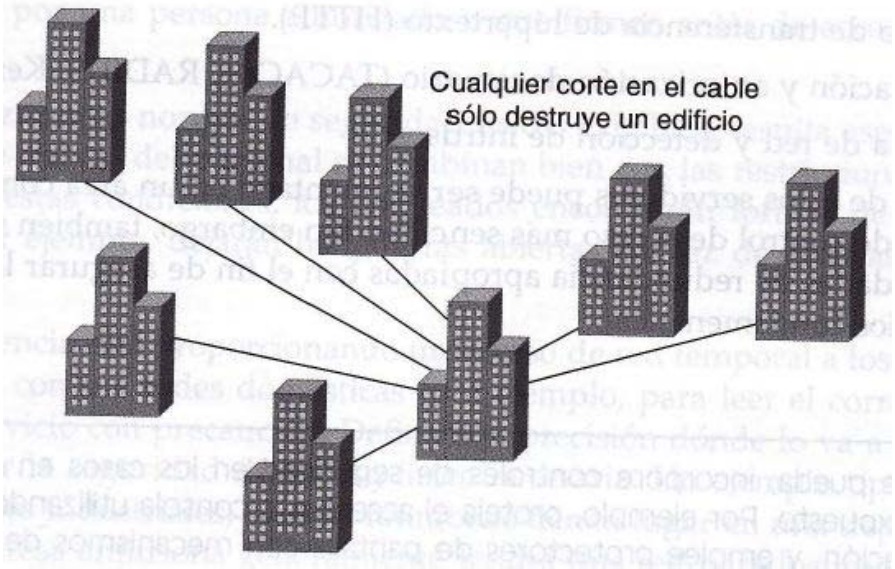


Gráfico 3 9 Topología en estrella.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 169.

Existen muchas configuraciones para establecer la interconexión entre los distintos elementos de la red, sin embargo, se hace necesario tomar en cuenta, que algunas topologías no permiten una tolerancia a fallos, es decir, si, ocurre algún incidente sobre la infraestructura, se afecta a la disponibilidad de los servicios. Para que una infraestructura se recupere de un problema inmediatamente (alta disponibilidad), se recomienda diseñar una red redundante.

Sin embargo, la redundancia puede generar bucles lógicos y físicos prolongados, especialmente si usamos dispositivos de capa 2 (enlace de datos), éstos emiten tramas multicast (señales a todos los dispositivos de red), esto consume el ancho de banda de la red. Para evitar el problema, como solución lógica, se recomienda utilizar el protocolo Spannig tree (STP), dicho protocolo, establece una topología lógica libre de bucles, es decir, una trayectoria activa a la vez.

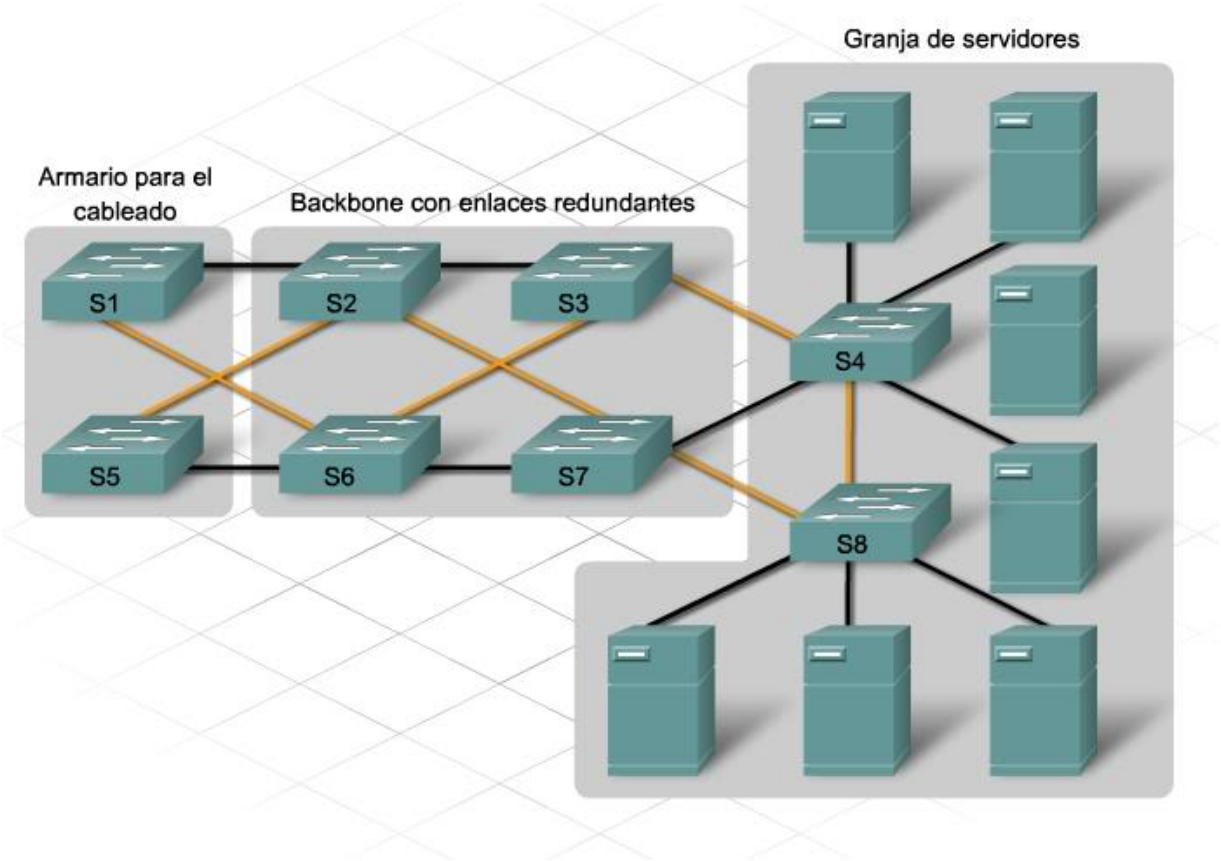


Gráfico 3 10 Topología lógica redundante.

Referencia: Internet. Redundancia .http://blogxdextecnologia.blogspot.com/2009_07_01_archive.html. Acceso:(29/09/2010)

Además, de lo expuesto se debe tomar en cuenta que en la topología física no se diseñen puntos de fallo, es decir, rutas que concentren la entrega de servicios por un solo punto, es necesario diseñar rutas alternativas para que en caso de error, la información pueda llegar, a eso se denomina disponibilidad de la red.

3.2.3 Dispositivos de Red.

Es primordial identificar los dispositivos de la red; comenzaremos incluyendo a los servidores de red (SNMP, DNS, NTP, NFS, HTTP, etc.). Posteriormente, es recomendable limitar el acceso físico y lógico a cada dispositivo, tomando en cuenta todo el entorno en que está ubicado el activo, es decir, aplicar filtros o seguridades globales. Por lo anteriormente escrito, en un entorno empresarial, es aconsejable designar un espacio autónomo para la ubicación de los servidores.

El uso de contraseñas seguras en los dispositivos es un mecanismo de protección y a su vez de autenticación, razón por la cual, se debe enseñar al usuario a elegir password seguros, utilizando contraseñas de un solo uso.

Recomendaciones para la elección de contraseñas:

Escoger una contraseña que sea difícil de adivinar, con una longitud máxima aceptada por el sistema.

Cambiar las contraseñas predeterminadas al reemplazar nuevos equipos de red.

Normar el cambio de claves en cuanto a la frecuencia y qué usuarios deberían cambiar su clave.

Con muchos equipos se puede configurar ***mensajes de bienvenida al sistema*** o ***banner*** al momento que se ingresa a configurar características, por ejemplo:

AVISOAVISO**AVISO**AVISO**AVISO**

HA ACCEDIDO A UN DISPOSITIVO RESTRINGIDO. EL USO DE ESTE DISPOSITIVO SIN AUTORIZACIÓN O PARA FINES NO PREVISTOS EN LA AUTORIZACIÓN ESTÁ PROHIBIDO.

CIERRE SESIÓN INMEDIATAMENTE.

AVISOAVISO**AVISO**AVISO**AVISO**

Además, el acceso debe pasar por un proceso de análisis de riesgos, que definirá el nivel de seguridad a implementarse y de ser necesario implementar seguridad biométrica

Gráfico 3 11 Área autónoma para sala de servidores.

Referencia: Internet. http://www.servitek.com.ar/aires-acondicionados/aire-acondicionado-para-servidores

Gráfico 3 12 Lector biométrico para acceso restringido.

Referencia: Internet.
http://www.kimaldi.com/aplicaciones/control_de_acceso/acceso_biometrico_a_sala_de_servidores

3.2.4 Ambiente de Seguridad.

Es importante considerar que cualquier norma de seguridad comienza con las personas y termina con las personas, en éste sentido, es primordial crear una conciencia de seguridad en la empresa y la mejor forma para que los usuarios internos la cumplan, es hacerles partícipes del proceso de seguridad, formando grupos de trabajo colaborativos, dispuestos a cumplir con las normas exigidas.

Del lado de los profesionales de la infraestructura se debe generar una cultura ***de visibilidad***, es decir, aceptar las sugerencias producidas de los grupos de trabajo, esto permitirá cambios de ambos lados y no unilateralmente. De esta manera, toda la empresa se adaptará rápidamente e informará de los cambios realizados.

Dentro de las normas de seguridad, debe constar un plan de contingencia que por lo menos debería contemplar los siguientes puntos:

- Plan contra incendios.
- Plan contra inundaciones.
- Plan a falta de suministro eléctrico.
- Condiciones de entorno adversas como temperatura y humedad.

- Procedimientos ante desastres naturales como terremotos, tormentas, rayos o maremotos.
- Protección ante campos magnéticos excesivos.
- Mantenimiento adecuado en lo que se refiere a limpieza.

3.3 Bases para Establecer Seguridad Lógica de Red.

Nos referirnos a la seguridad lógica cuando en base a algún criterio, creamos controles o dividimos una infraestructura de red para que cumpla con los parámetros que establecimos en dicho criterio, es decir, creamos restricciones para el acceso a la información.

La ***seguridad lógica*** se refiere principalmente al direccionamiento IP, es decir, se crean límites o grupos de direcciones IP basados en su funcionalidad (VLAN'S), de esta manera, los usuarios con una actividad en común podrán utilizar solo una red adecuada para sus competencias. Sin embargo, es muy fácil falsear una dirección IP, por lo que, se recomienda usar un analizador de paquetes denominado también detector de intrusos en los puntos de entrada y salida más importantes de una red.

3.3.1 Instauración de Subredes.

Para configurar subredes debemos tener en claro los objetivos que se pretenden. Básicamente, el objetivo de crear una infraestructura dividida es para optimizar la red, mejorar la administración y por seguridad.

Una vez creada las subredes se puede controlar el tráfico entre ellas mediante una ***lista de control de accesos, ACL***, que sirve como filtro para el tráfico que se distribuye, es decir, una lista de los servicios que están disponibles.

Una lista de control de acceso

"*es un grupo de sentencias que definen cómo los paquetes hacen lo siguiente:*

- *Entrar en las interfaces de router entrantes.*
- *Retransmitirse a través del router.*

- *Salir de las interfaces de router salientes."*[21]

Los controles de acceso, generalmente, se configuran en los límites de las subredes, es decir, cuando el tráfico de una red aledaña desea circular a otra. Se configuran en dispositivos conmutadores como routers o switches

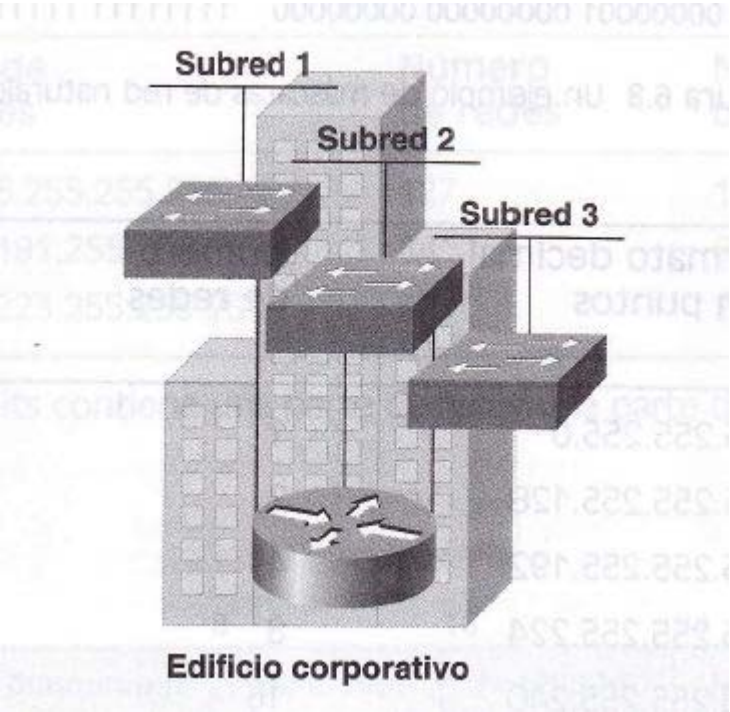


Gráfico 3 13 Límites de subred.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 176.

[21] Cisco Systems. *Guía del primer año. CCNA® 1 y 2*. Madrid, Pearson Educación S.A., 3ra edición, 2004. Página 777.

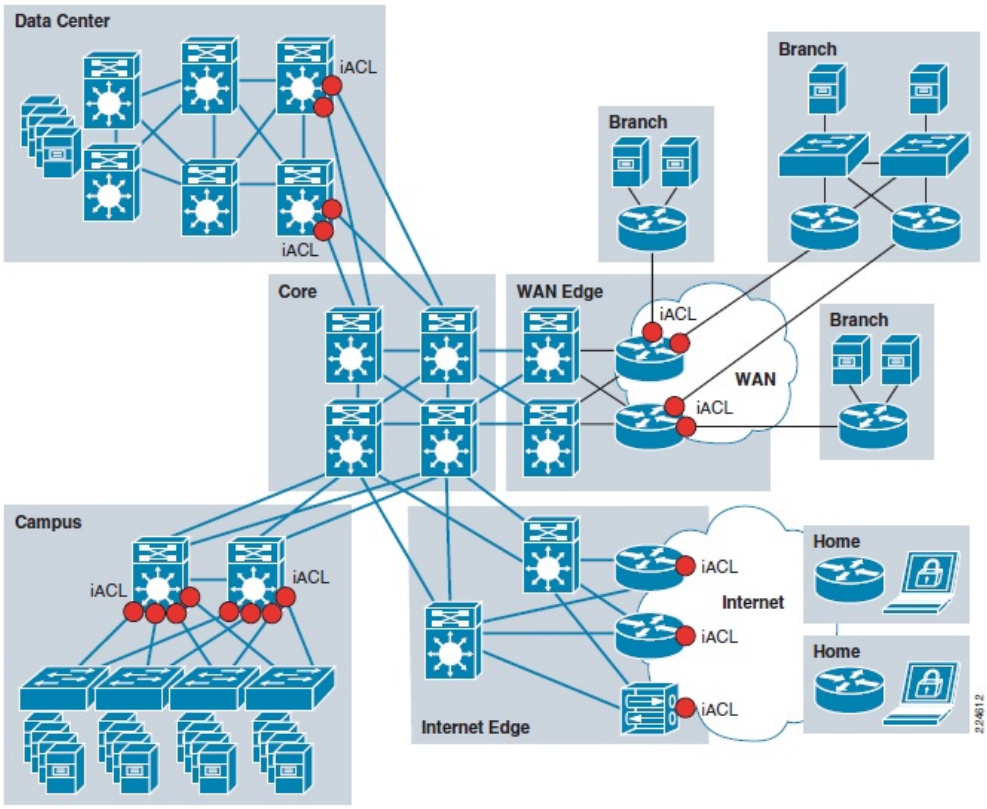


Gráfico 3 14 ACL Control de acceso

Referencia: CISCO, Network Security Baseline, Cisco Systems, Inc. http://www.cisco.com. página 76.

3.3.2 Instauración de Enrutamiento.

Uno de los métodos utilizados para crear seguridad lógica en una red es el enrutamiento, es decir, que por cierta ruta solo se permita el acceso a cierto tipo de tráfico, generalmente, el que consideremos seguro.

Para el transporte entre las subredes se utiliza un protocolo de enrutamiento, que sirve como mecanismo para acceder a los datos de distintas redes. Es así que, ciertos dispositivos permiten denegar o configurar el acceso a redes peligrosas.

Existen protocolos de enrutamiento estático y dinámico se recomienda usar el primero en entornos con pocos host, mientras que, para ambientes grandes la segunda opción es ideal.

Para acceder a una red, un control lógico es implementar comprobaciones exclusivas para cada usuario y controles de detección que registran actividades no permitidas o intentos a sistemas restringidos.

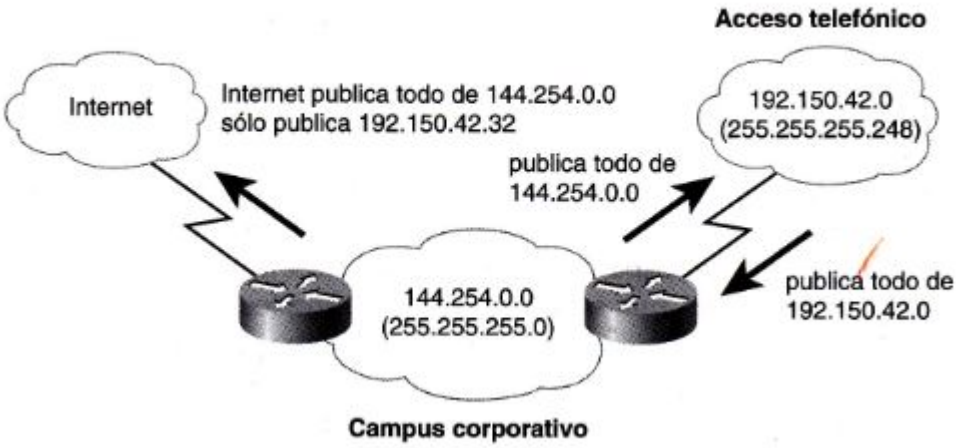


Gráfico 3 15 Enrutamiento Lógico.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 177.

3.3.3 Autenticación.

La ***autenticación*** de usuarios se refiere a la identificación; es importante saber quién quiere acceder a los recursos, así, se le puede ***autorizar*** la realización de ciertas tareas según su perfil o sus necesidades. Los dos conceptos citados están concatenados para establecer el concepto de ***control de accesos o permisos***.

En el proceso de conceder permisos a los usuarios se maneja credenciales, las mismas que se fundamentan en algo que se conoce (contraseña), en algo que se tiene (tarjeta) o que se es (controles biométricos). Existen dos modalidades para autenticar ***localmente*** y ***por un tercero*** (servidor).

Para la implementación de identidad se puede usar ***servicios de directorios,*** estas herramientas, permiten administrar los recursos de una infraestructura corporativa, por ejemplo, compartición de archivos, de impresoras. Entre los principales servicios de

directorios tenemos: Active Directory (AD), Samba con su interfaz web Mandriva Directory.

3.3 Bases para Establecer Integridad.

Cuando hablamos de ***Integridad*** citamos a la seguridad física y lógica en una empresa. Integridad de los dispositivos, acceso a áreas de servidores, implantación de medidas de seguridad, son aspectos significativos que se deben tomar en cuenta. En lo que respecta a la seguridad lógica, es importante restringir el acceso Telnet o de consola instalando un Firewall.

3.3.1 Firewall.

Es un dispositivo de red que sirve como filtro para discriminar la información que llega de una red para ingresar a otra, generalmente, de Internet a la red local de una empresa.

Cuando hablamos de un ***firewall***, implícitamente nos referimos al flujo del tráfico de los servicios de red soportados. Se crean reglas que permiten el ingreso y salida de la información, por esta razón, se los coloca en los puntos de acceso y salida de la red de una empresa. Estos dispositivos cumplen funciones de filtrado de paquetes (TCP, UDP, ICMP e IP), filtrado de circuitos (permiten el flujo comprobando si los paquetes son parte de una conexión previa) y Gateways de aplicación.

- Para establecer un posible control es conveniente analizar:
- Sentido del tráfico.
- Origen del tráfico.
- Dirección IP.
- Números de puerto.
- Autenticación.
- Contenido de la aplicación.

Generalmente se considera como riesgoso al tráfico externo (no fiable), es decir, a la información que quiere entrar a nuestra red (red fiable).

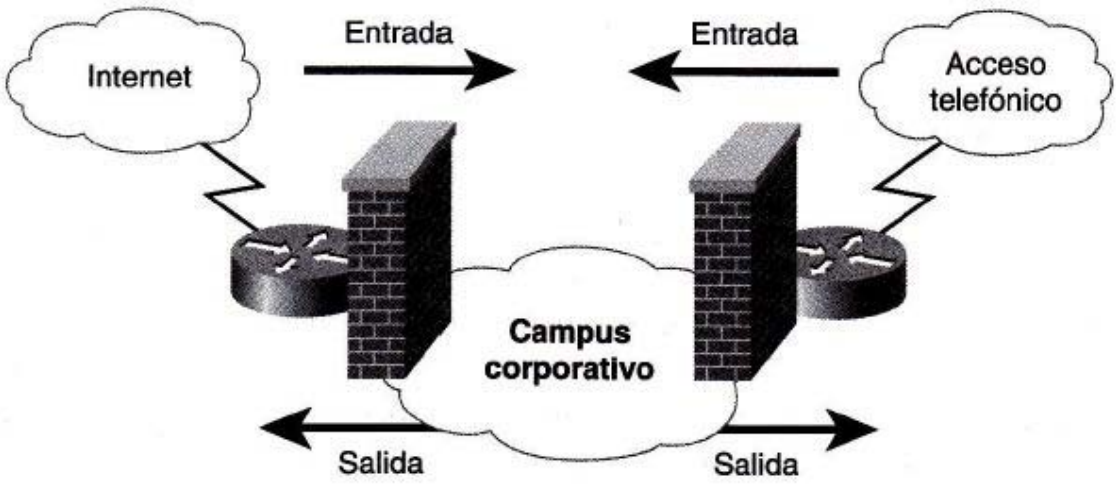


Gráfico 3 16 Implementación Firewall

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 183.

3.3.2 Servicios de Red.

Para precautelar ataques a la infraestructura de red es aconsejable detenerse en el análisis de los ***servicios de red,*** que se refiere al tipo de aplicaciones que funcionarán a través de un determinado puerto. Con el objetivo de la seguridad existen dos métodos de restricción; el primero consiste en ***permitir todo***, y a medida que se detecten amenazas, denegamos el acceso. El segundo mecanismo es ***denegar todo***, y conforme se requiera de un servicio, se lo habilita. Es recomendable utilizar el segundo método porque implica menos riesgo de un ataque.

Los servicios más utilizados son: SNMP, DNS, NTP, WWW, Telnet, FTP, NNTP y SMTP.

Tabla 6.1 Servicios a filtrar de acuerdo a las recomendaciones del CERT.

Protocolo	Número de puerto	Descripción
TCP	53	Zona de transferencia DNS
UDP	69	Tftpd
TCP	87	Enlace (lo suelen usar los intrusos)
TCP	111	SunRPC
UDP	111	SunRPC
TCP	2049	NFS
UDP	2049	NFS
TCP	512	BSD UNIX R-command
TCP	513	BSD UNIX R-command
TCP	514	BSD UNIX R-command
TCP	515	lpd
TCP	540	uucpd
TCP	2000	OpenWindows
UDP	2000	OpenWindows
TCP	6000+	X Windows
UDP	6000+	X Windows

Gráfico 3 17 Servicios a filtrar según las recomendaciones del CERT.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 186.

Hay que tomar en cuenta que cada servicio debe proporcionarse en diferentes equipos pues, puede darse el caso por ejemplo, que un intruso aloje un archivo en el FTP anónimo y si, el servidor WWW se encuentra en la misma máquina, podría configurarse para que el servidor HTTP lo ejecutara.

Una buena práctica es autenticar las actualizaciones de enrutamiento para evitar que un router no autorizado desvíe el tráfico. Además, autenticar los protocolos VLAN. Se puede implementar ***sumas de comprobación*** para evitar ataques de reproducción.

3.3.3 Autenticación.

Para establecer contraseñas seguras se crearon estándares como el ***protocolo S/key*** que cifra el password (contraseña) para que el valor cifrado sea distinto cada

vez, es decir, es de ***un solo uso***, otro protocolo de similar función es el de ***contraseña por tokens***.

S/Key se fundamenta en una estructura cliente – servidor (PC - UNIX) inicializados con la misma frase de paso y un contador de iteración; el contador sirve para determinar las veces que se aplicará una entrada para la función hash. Las contraseñas por tokens utilizan una ***tarjeta inteligente*** (tarjeta de tokens) que se comunica con un servidor; el servidor envía un ***desafío*** (respuesta por desafío) al dispositivo para que se cifre con la clave personal del usuario y calcule una respuesta, mientras, el servidor espera la respuesta, calcula lo que debe recibir y si coinciden los dos datos se permite el acceso. Otra forma es ***autenticación por sincronía***, en éste caso se necesita un elemento (chip) que otorgue la autenticación.

Una gran variedad de protocolos realizan una comprobación previa antes de establecer permisos, es el caso de TACACS+, RADIUS, Kerberos, DCE y FORTEZZA. Kerberos es un estándar que se emplea para identificación de usuarios y servicios en ambientes de infraestructura compartida en Internet. El método se ayuda de un ***tercero de confianza*** conocido como servidor de autenticación o centro de distribución de claves KDC que emite tickets con un tiempo determinado de vida para identificar a un usuario.

La Fundación de software abierto OSF propone DCE que significa ***entorno de computación distribuida***; propone normas para la seguridad (control, identificación y servicios) en ambientes donde los datos se encuentran diseminados. Se basa en un algoritmo parecido a Kerberos versión 5, con la diferencia, de que la implementación la realizan servidores de privilegios y de registros relacionando un ID único universal (UUID) de 128 bits. En la práctica tanto Kerberos como DCE incurren en altos costos de mantenimiento en lo que se refiere a recursos humanos.

FORTEZZA es un recurso de seguridad de red multinivel (MISSI), ideada por la Agencia nacional de seguridad (NSA) para establecer una interoperabilidad entre sistemas de red, puesto que, se fundamenta en estándares comunes de seguridad. Los bloques de construcción de seguridad de sistemas de información multinivel son:

- FORTEZZA y FORTEZZA Plus.
- Firewalls.

- Protecciones.
- Cifradores en línea.
- Computación de confianza.

Los principales servicios de FORTEZZA son la protección para datos sensibles no clasificados en un host dentro de una LAN o WAN, autenticación, confidencialidad, integridad de los datos, irrebatibilidad y compatibilidad entre distintos sistemas operativos.

Una versión implementada para manejo de información clasificada es FORTEZZA Plus, debe complementarse con un servidor seguro de red (SNS) para obtener cifrado.

Existe una tarjeta de cifrado FORTEZZA que se puede adaptar al PC para firmar mensajes, para obtener las opciones mencionadas se necesita combinar aplicaciones FORTEZZA, actualmente, se dispone aplicaciones para correo electrónico, transacciones web seguras, cifradores de archivos, identificación y autenticación.

3.4 Bases para Establecer Confidencialidad.

La ***confidencialidad*** garantiza que tanto la información que se envía, como la que se recibe es totalmente fiable, éste último detalle implica el cifrado. Hay información sensible que puede ser codificada para que sólo quién tenga la clave de decodificación sea capaz de interpretar el contenido.

3.4.1 Cifrado.

Para evitar que un atacante intercepte mensajes se creó el proceso de ***encriptación*** o cifrado, que consiste en codificar un mensaje mediante una clave que solo la conoce el emisor y el receptor de dicho mensaje, consecuentemente, serán los únicos que podrán acceder al mensaje, sin embargo, hay la posibilidad de descifrar el contenido teniendo una copia de un texto original y otro encriptado, de ésta manera el agresor adivina el proceso de ocultamiento; es por esto que se recomienda algoritmos superiores a 56 bits de codificación que son más difíciles de descubrir.

La codificación se la hace a través de una clave que permitirá cifrar, descifrar o firmar datos sensibles; se lo hace aplicando una función matemática (algoritmos DES, 3DES, RC-4 o IDEA), la complejidad del algoritmo matemático está dada por el número

de combinaciones que se puede aplicar con los bits que se dispone, es decir, mientras más bits, más segura y difícil de quebrantar la clave.

Longitud de clave en (bits)	Número de combinaciones
40	$2^{40} = 1.099.511.627.776$
56	$2^{56} = 7,205759403793 \times 10^{16}$
64	$2^{64} = 1, 844674407371 \times 10^{19}$
112	$2^{112} = 5,192296858535 \times 10^{33}$
128	$2^{128} = 3,402823669209 \times 10^{38}$

Tabla 3 1 Combinaciones y longitud de clave.

Referencia. Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, página 6.

Hay tres tipos de cifrado: simétrico, asimétrico y la función hash. Cifrado simétrico utiliza una misma clave para codificar y descodificar, asimétrico emplea una clave pública y otra privada y la función hash que comienza con un tamaño aleatorio de un mensaje como entrada, para crear una salida de longitud fija denominada ***hash***. Un algoritmo hash necesita cumplir con cuatro condiciones para considerarse seguro:

Coherente (misma entrada = misma salida).

Aleatorio (para evitar adivinaciones).

Único (casi imposible utilizar dos mensajes que generen el mismo conjunto de mensajes).

Unidireccional a la salida (imposible obtener el mensaje original).

Los algoritmos hash más conocidos son: Message Digest 4, 5 y hash seguro (MD4, MD5 y SHA).

Las ***firmas digitales*** son un grupo de mensajes cifrados acompañando a un documento. La combinación de cifrado de clave pública y una función hash se conoce como firma digital. Los algoritmos más conocidos son: Ron Rivest, Adi Shamir y Leonard Adleman (RSA) y el algoritmo Digital Signature Standard (DSS, estándar de firma digital). DSS es más rápido para generar claves pero más lento para verificar.

3.4.2 Clave Pública PKI

Una gran variedad de protocolos de seguridad se basan en el ***cifrado de clave pública (PKI)***. El propósito principal de una PKI es gestionar la utilización de certificados y claves de una forma fiable.

Según la norma ***X.509 Public Key Infrastructure PKIX,*** describe a una PKI como: El conjunto de hardware, software, personas, normas y procedimientos necesarios para crear, administrar, almacenar distribuir y revocar los certificados en base al cifrado de clave pública.

Extraído del documento 800-15 del NIST, ***Minimun Interoperability Specification for PKI Components, Version 1,*** septiembre de 1997, de William Burr, Donna Dodson, Noel Nazario y W. Timothy Polk; los 5 elementos presentes en una PKI son:

Las Autoridades de certificados (CA).

Las ***Autoridades de registro organizativo (ORA)*** que controlan la relación entre claves públicas y las entidades del tenedor de certificados.

Los ***Tenedores de certificados*** a los que se les han otorgado certificados con autorización de firmar documentos digitales.

Los usuarios validadores de firmas digitales a partir de una clave pública o una CA confiable.

Los depósitos que conservan y emiten certificados junto con listas de revocación de certificados (CRL).

En el funcionamiento de una PKI se puede mencionar las características de:

Registro, referencia a una CA a cualquier sujeto interesado.

Inicialización trata la configuración inicial de los valores necesarios para utilizar una PKI (clave pública o certificado).

Certificación cuando una CA emite un certificado entregando el mismo o publicándolo en un almacén.

Recuperación de pares de claves en caso de pérdida registra duplicados seguros.

Actualización de las claves cada cierto tiempo para ser reemplazadas por nuevas claves y certificados.

Generación de claves ya sean localmente o por una CA.

Certificación cruzada para permitir la comunicación entre clientes de un tercer sistema administrativo.

Revocación cuando se genera un cambio de nombre, asociación o alteración de la clave.

3.4.3 Gestión de claves.

En la gestión de claves nos enfrentamos a un factor determinante en todo el proceso de la seguridad, el factor humano. Generalmente el mantenimiento de claves y la correcta utilización de las mismas se enmarcan en la subjetividad del poseedor de la clave.

La distribución de claves en empresas grandes se realiza a través de ***"un tercero fiable"*** conocido también como Centro de distribución de claves (KDC). En este esquema se requiere que cada elemento que intercambie información con el KDC tenga una clave secreta compartida, que puede ser asignada al usuario al inicio de la configuración.

Un algoritmo para la creación de claves secretas seguras en un entorno distribuido es el método ***Diffie-Hellman***, que tiene su fundamento en la operación módulo (5 mod 3=2) porque existe un número infinito de resultados que podrían coincidir con la respuesta de la operación.

Para asegurar el intercambio de claves seguras se suele utilizar un par de llaves pública y privada que cumplan con estrictos parámetros estadísticos para que la posibilidad de que se existan dos claves iguales sea casi nula. La tendencia es a la auto-generación de claves, es decir, que la entidad que emite las claves privadas sea la única en conocerlas.

La incógnita principal alrededor de la distribución de claves es cómo confiar en la entidad que genera las claves, para solventar el problema se propuso los ***certificados digitales*** que son la digitalización de información (mensaje) para saber que la clave pública pertenece a un empleado. El formato (estándar X.509) es el siguiente:

- Versión.
- Número de serie del certificado.
- Información sobre el algoritmo emisor.
- Emisor del certificado.
- Válido de tal fecha hasta tal fecha.
- Información sobre el algoritmo de clave pública del asunto del certificado.
- Firma digital de la autoridad emisora.

La autoridad de certificados (CA) es quien se encargaría de manejar la validez del certificado, sin embargo, el debate se centra en quién es la entidad que debería manejar ésta información y si es idóneo concentrar tanta información sensible en un solo lugar. Algunos Gobiernos secundan la idea de permitir escuchas para que instituciones del orden operen con esta información.

Al final, el eslabón más débil en lo que se refiere a la custodia de claves, es el ser humano, puesto que, responde a diferentes intereses, no necesariamente seguros; se puede dar el caso de revelación de claves a cambio de dinero u otros beneficios no comunitarios.

3.4.4 Administración de Accesos

Uno de los objetivos al instaurar políticas de seguridad es conservar la información empresarial; existen tres directrices que permiten alcanzar éste reto.

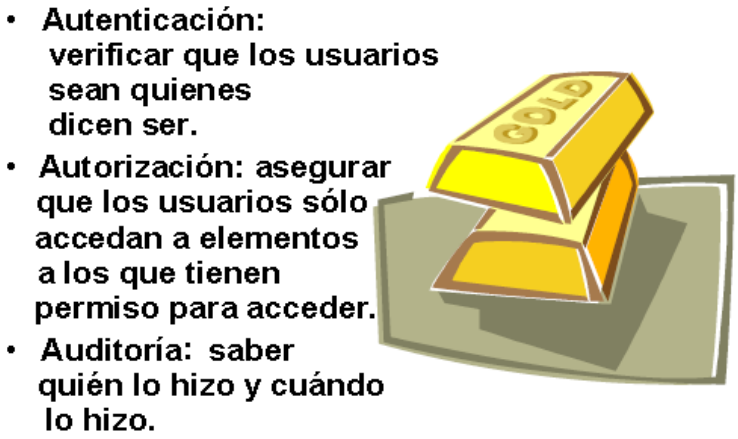


Gráfico 3 18 Acceso a la información.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 9, página 196

Autenticación es el proceso por el cual un miembro de la empresa se identifica a través de un nombre de usuario y una contraseña. Se debe considerar si el nombre de usuario y contraseña son cifradas durante el proceso de envío, o simplemente se transmite como texto sin cifrar. Además, hay que analizar si es suficiente la autenticación para reconocer al usuario y si el método es seguro. Se utiliza autenticación para acceder a una red o a información sensible.

El protocolo de autenticación de contraseña ***(PAP, Password Authentication Protocol)*** , o el de desafío mutuo ***(CHAP, Challenge Handshake Authentication Protocol)***, son usados en muchas empresas; para éstos métodos, se necesita tener la información de usuario y contraseña, lo que se conoce, como ***factor único***.

Como autenticación ***sólida o de dos factores*** se entiende como a la combinación entre lo que se tiene y lo que se conoce; Key fob utiliza ésta técnica generando un símbolo basado en el tiempo (lo que se tiene) relacionándolo con un PIN (lo que se conoce).

La biometría incluye un tercer factor basado en los atributos biológicos de quién ingresa al sistema como escanear la palma de la mano, huellas digitales o la retina el ojo. Sin embargo, el costo es muy alto, por lo que, ahora se está experimentando con técnicas como patrones de uso del teclado u otras conductas.

Luego del procedimiento de autenticación viene la ***autorización*** que consiste en verificar si la información proporcionada coincide con la almacenada en el archivo de seguridad, sí, es la correcta, se produce la asignación del perfil lo que permite que determinados empleados accedan a determinada información; esto se entiende como autorización ***basada en la función***. Se debe poner énfasis en estructurar autorizaciones para entornos como VPN, listas de marcado rápido en VoIP, conferencias, acceso a servidores.

La ***auditoría*** sirve de respaldo para indagaciones sobre problemas, el saber que acciones previas se realizaron ayuda en la correlación de eventos, a saber cómo y cuándo se hicieron cambio de configuraciones en routers o en otros dispositivos. Cada registro debería contener el nombre del usuario, la fecha y la hora tanto de creación como de actualización.

3.4.5 TCP/IP y Seguridad

Cuando la información viaja desde un host de origen a otro de destino, utilizando el protocolo de comunicación TCP/IP, la información se subdivide y pasa por cuatro etapas o capas (aplicación, transporte, red y enlace), cada una de las cuales cumple con un proceso de encapsulación (etiquetación) hasta llegar a la transmisión de impulsos eléctricos a través de una infraestructura de red. En las diferentes capas del modelo mencionado se pueden aplicar normas (protocolos) que proporcionen un transporte seguro de los datos. Así por ejemplo, en la capa de ***aplicación*** se ha creado el método ***protocolo seguro de transporte de hipertexto (SHTTP)***, que establece la protección de las transacciones que se realizan en la web. Además, se puede identificar la integridad, autenticidad y el código de autenticación de mensaje (MAC).

Para implementar SHTTP se debe utilizar la negociación de opciones para que los usuarios y los servidores acuerden el ***modo de transacción, algoritmos de cifrado*** y ***selección de certificados.***

En la etapa de ***transporte*** el protocolo de ***capa de socket segura (SSL)*** brinda seguridad para datos seleccionados de la capa de aplicación (HTTP, Telnet, FTP) y

TCP/IP. Se emplean tres protocolos (intercambio de señales, registro y alerta) para obtener privacidad y fiabilidad.

SSL permite una conexión privada, utiliza clave pública para la identidad del igual y la conexión es fiable empleando MAC (código de autenticación de mensaje) con clave.

SSH (protocolo de Shell seguro) desarrolla un método para un inicio de sesión remoto seguro, transferencia de información y reenvío de tráfico a través de una red no segura. Consiste de tres protocolos:

Capa de transporte para la autenticación, integridad y confidencialidad del servidor.

Autenticación de usuario.

Conexión para cifrar varios canales lógicos.

El protocolo ***SOCKS*** denominado así por ***seguridad de sockets*** funciona como un ***proxy de red*** en la capa de transporte para utilizar confiablemente los servicios de un firewall.

SOCKS Versión 4 permite el tránsito del protocolo TCP/IP a través de firewalls no seguros, en la versión 5 se incluye propiedades de autenticación, UDP, DNS e IPv6.

SOCKS trabaja reemplazando las peticiones de red por llamadas específicas que abren comunicación con un servidor proxy SOCKS por intermedio de un puerto (1080/TCP). Si se logra establecer una conexión, el usuario intercambiará los mecanismos para definir un método de autenticación, para que finalmente, el servidor SOCKS admita o niegue las comunicaciones.

En la ***capa de red*** la seguridad se relaciona con el protocolo IP de seguridad (IPsec), son cuatro especificaciones (RFC2401, RFC2402, RFC2406 y RFC2408), que determinan la manera como el encabezado (cabecera de autenticación) debe guardar los datos, junto con un algoritmo de encriptación, propone una función de cifrado y gestión de clave.

Para la implementación de IPsec es necesario aumentar campos a los datagramas (cabeceras); una cabecera de autenticación (AH) y una de encapsulación de sobrecarga de seguridad (ESP). Pueden funcionar independientemente o en conjunto.

AH y ESP permiten dos modos de utilización ***modo trasporte*** y ***modo túnel.***

En modo transporte, cuando dos host se comunican, la seguridad se enfoca en las capas superiores aumentando los campos mencionados anteriormente.

Un modo túnel permite encapsular los paquetes que están en el protocolo, sin embargo, solo puede ser soportado por equipos finales de datos o Gateway intermedios de seguridad. Se añade una cabecera IP externa e interna que fijan el origen y destino de la información.

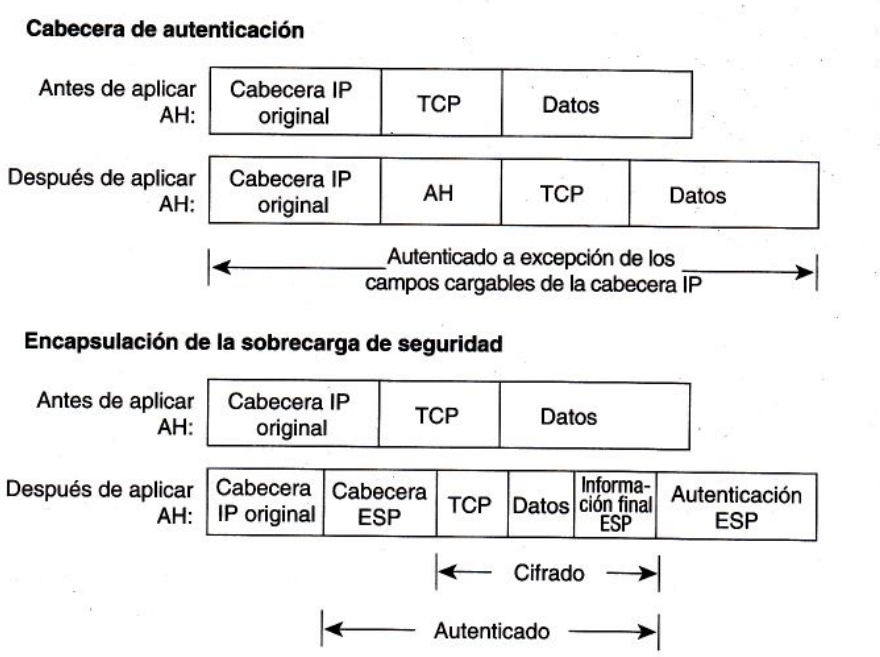


Gráfico 3 19 Modo transporte IPsec IPv4.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, pág70.

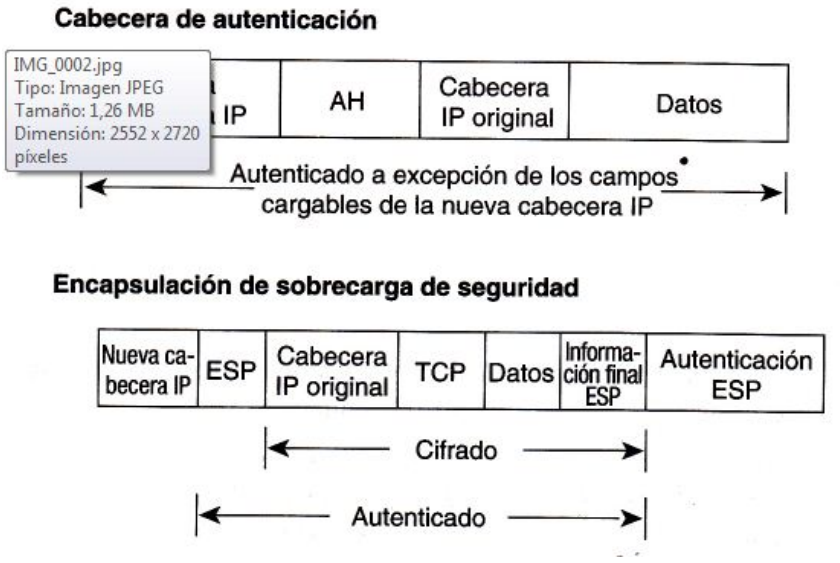


Gráfico 3 20 Modo Túnel IPsec IPv4.

Referencia: Merike Kaeo, Diseño de seguridad en redes, PEARSON EDUCACION, S.A. Madrid 2003, pág70.

Las ventajas de la protección se pueden ver con la utilización del protocolo SSL que es aplicado en el campo de la world wide web con algunas aplicaciones específicas. SSH se emplea para conectarse remotamente vía Telnet. IPsec posibilita su implementación tanto en datagramas UDP, como en IP, además, IPsec oculta los datos que vienen de la capa de transporte.

Es aconsejable una combinación de protocolos de capa de transporte con capa IP.

3.5 Bases para Establecer Procedimientos al Personal.

En cuanto se refiere a las ***normas y procedimientos para el personal*** se necesitan promover y concientizar a los funcionarios que utilizan la infraestructura de red sobre las reglas de seguridad. Uno de los aspectos a tomarse en cuenta son las ***copias de seguridad*** de la información en los servidores, servicios de red y creación de imágenes son primordiales.

Asimismo, cuidar de que el ***uso de las herramientas portátiles*** no implique inseguridades es vital. También, el uso de ***rastros de auditoría*** puede ayudar a

descubrir posibles debilidades, generalmente cuando se visualiza comportamientos distintos al tráfico normal, se puede identificar anormalidades.

Para el ***almacenamiento de los datos*** lo óptimo es que el instrumento en el que se quiere realizar el registro esté enlazado al dispositivo que genera el registro, sin embargo, no siempre se contará con esa posibilidad; en el caso contrario, se debe estimar una ruta segura, es decir, que circule por el menor número de redes o routers.

Además, una parte fundamental son las ***consideraciones legales***, especialmente en lo que se refiere al derecho de la privacidad.

Mencionar que una ***capacitación acerca de la importancia de la seguridad***, es un matiz preponderante es ineludible, porque la mayoría de los usuarios se incomodan cuando un administrador de red establece controles para el ingreso o uso de los servicios de red. Generalmente, los usuarios no conocen los riesgos a los que se exponen, y peor aún, las implicaciones que generan.

Cuando nos referimos a ***ingeniería social***, aludimos a las fallas cometidas por miembros autorizados que entregan información a personas ajenas a la red que, emplean engaños haciéndose pasar por personas debidamente autorizadas.

3.5.1 Respaldos de Seguridad.

3.5.2 Auditoria.

Por medio de la ***auditoria*** podemos evaluar que tan seguro es nuestro entorno de red; cada examen debe ser planificado y deberá contener información relevante que permita mejorar los controles, para lograr este objetivo podemos utilizar filtros de información y auditar solo los aspectos importantes.

3.5.3 Temas Legales.

Existen algunas regulaciones que tanto las empresas públicas como las privadas deben cumplir; una de ellas es SOX que es una ley aprobada en 2002 por el Congreso de Estados Unidos, ley relacionada con procesos de auditoría financiera que es valiosa de entender debido a que establece las bases para la aplicación de principios en la documentación informática. Los principales aspectos que abarca son:

Se crea una compañía pública de supervisión financiera (PCAOB).

Las empresas públicas deben evaluar y notificar la efectividad de sus controles internos.

Los reportes financieros deben ser avalados por los gerentes ejecutivo y financiero.

Empresas que cotizan en la bolsa de valores deben ser supervisadas por comités independientes bajo la acción de auditores.

Se incrementan las sanciones civiles y penales para las violaciones a las normas de seguridad.

En el área de las tecnologías de la información la influencia de esta ley recae en la ***evaluación de los riesgos*** para tomar precauciones que estén acorde con los objetivos de cada departamento y de la empresa en su conjunto.

El aspecto de ***entorno de control*** también se afecta en IT, ya que se determina la manera de actuar del personal, el proceder ético y moral tanto de la compañía como del personal y la administración empresarial. Un entorno debería contemplar una prestación de servicios en la cual los empleados tomen real responsabilidad en los procesos y sean reconocidos por sus éxitos y su buen desempeño. Muchas empresas implementan un período de entrenamiento para empleados en lo que se refiere a diseño, aseguramiento de la calidad y despliegue de la misma, a fin de que puedan participar en el ciclo completo de convergencia de las tecnologías.

Para mitigar la incidencia de una falla se establece el ***control de actividades*** que son procedimientos y políticas documentadas que aseguran el cumplimiento de los servicios. Parte del control es establecer una rutina de tareas, actividades, procedimientos, verificaciones, conciliaciones financieras y métodos de seguridad.

Además, como ya se ha expresado el ***monitoreo*** para saber qué elementos son importantes o sensibles, qué informes se deben presentar ante organismos de control y para obtener un desempeño de calidad.

De suma importancia es el aspecto de la ***comunicación e información***; es un nexo entre el departamento técnico y los usuarios.

Otras leyes relacionadas son la ley financiera ***(GLBA, Gramm – Leach Bliley Act)*** y la ley de información de salud, portabilidad y responsabilidad ***(HIPAA, Health Information Portability & Accountability Act)***; ésta última regulación establece parámetros para los ámbitos de ***administración***, entorno ***físico*** y parte ***técnica*** en una empresa.

En el apartado correspondiente a la administración contempla:

Toda compañía para cumplir las normas HIPAA, debe aprobar por escrito los procedimientos para mantener la privacidad sobre la información personal protegida y asignar un funcionario encargado para éste fin.

En procesos adquisitivos se debe supervisar cada acción y cada control estará acompañado por un proceso claramente documentado basándose en políticas de seguridad.

A los empleados que se les permite trabajar con información personal protegida deben trabajar documentando su accionar y sólo pueden tener acceso a la información estrictamente necesaria para su labor.

Las compañías deben demostrar que han aplicado un programa de formación continua para el manejo de la información personal protegida y que el recurso humano está capacitado para éstas funciones.

A las empresas que trabajan bajo la modalidad de tercerización también se les debe exigir que cumplan las reglas HIPAA, generalmente, a través de cláusulas contractuales.

Las unidades responsables del manejo de la información personal protegida, también, se encargarán del respaldo de los datos, procesos de recuperación, plan de contingencia, análisis de fallos, prioridades, pruebas y control.

HIPAA establece procesos de auditoría interna, revisiones continuas para detectar posibles violaciones. Se debe documentar los objetivos y el alcance de la auditoría e implementar guías con agendas y horarios para la realización de los controles.

Documentar procedimientos para mitigar la brecha de seguridad.

Con la parte física se establece lo siguiente:

La red debe contemplar controles que gobiernen tanto adiciones como eliminaciones en hardware y en software. Los equipos que sobrepasen la vida útil deben ser retirados para que no comprometan la parte física.

El acceso a los sistemas que contienen información protegida debe ser diligentemente monitoreado y controlados.

Solo personal autorizado puede acceder a los sistemas de hardware y software.

Control de accesos deben incluir planes de seguridad, registros de mantenimiento y registro de visitantes.

Las estaciones de trabajo no deben ubicarse en áreas públicas de alto tráfico. Los monitores no pueden estar visibles al público.

A empleados que trabajan bajo contrato, también se les debe entrenar en seguridad empresarial.

Lo que refiere a resguardos técnicos implica:

Deben protegerse de intrusiones a sistemas que albergan información personal protegida. Sí, se trabaja en una red abierta o cerrada, es necesario implementar controles de acceso que eliminen la necesidad de la encriptación.

Asegurar que la información personal protegida no sea vulnerable a ser cambiada o borrada.

La integridad de los datos debe mantenerse implantando seguridades como firmas digitales, claves dobles y chequeos.

Es necesario mensajes de autentificación entre dos entidades que utilizan HIPAA; cada una de las partes debe garantizar la autenticidad de los datos con el empleo de passwords o certificados digitales.

Toda la documentación relacionada con las normas HIPPA, debe estar disponible para verificación.

La documentación relacionada con las tecnologías de la información debe incluir registros escritos de todas las configuraciones y servicios de la red.

Programas de análisis y administración de riesgos requieren ser implementados y documentados.

3.6 Administración de la red y Seguridad.

La Administración adecuada de una infraestructura de red aporta valiosos elementos para el mejoramiento de la seguridad, puesto que, en el proceso de monitoreo se pueden prevenir incidentes y planificar estrategias ante incidentes.

3.6.1 Observaciones para la Implementación de la Seguridad

En administración de incidentes cada fallo tiene un impacto que debe ser superado; la propuesta de ITIL (marco de trabajo de las buenas prácticas para la entrega de servicios de tecnologías de la información) se ilustra en el gráfico a continuación

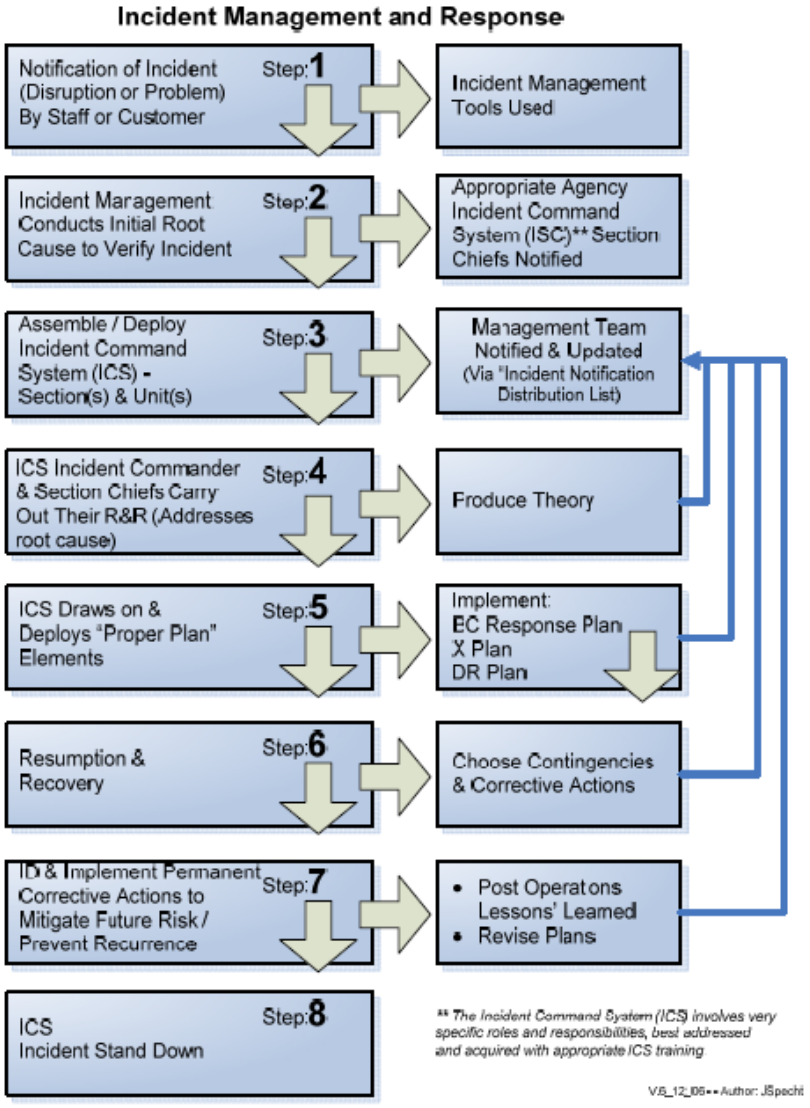


Gráfico 3 21 Respuesta ante un incidente.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 10, página 225.

Del análisis del diagrama de flujo, podemos ver que a cada tarea está respaldada por líneas base contempladas en la documentación correspondiente al plan de contingencias previsto. También se puede establecer una matriz de 3 x 3 para evaluar la gravedad de cada incidente.

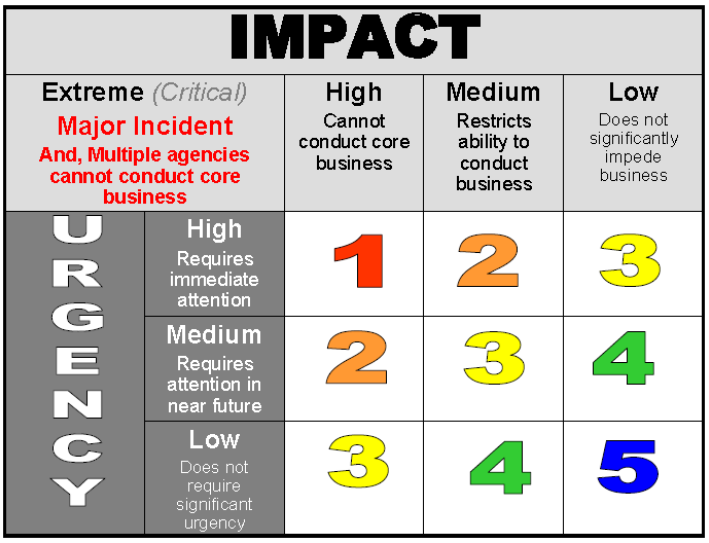


Gráfico 3 22 Valoración de un incidente.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 10, página 226.

Cada valoración de un incidente está relacionada con un tiempo de recuperación que depende de la gravedad del mismo. Como se puede apreciar en el gráfico valores menores requieren de atención inmediata, los intermedios necesitan de una atención en el futuro cercano y los de baja incidencia no son significativamente urgentes.

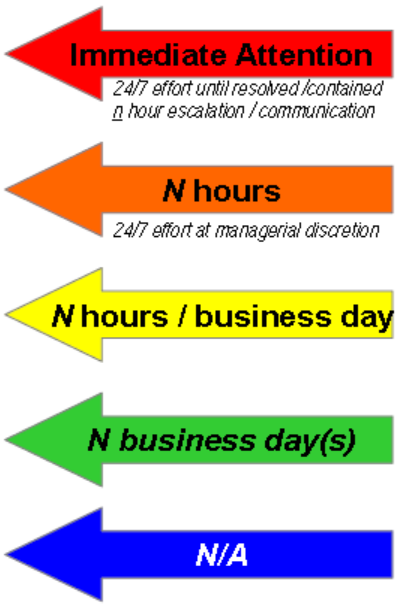


Gráfico 3 23 Tiempo de respuesta ante un incidente.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 10, página 226.

El objetivo de la implantación de los procesos ITIL en una empresa es proveer una respuesta eficiente ante fallas, de ésta manera, la perspectiva del negocio se enfoca al cliente y a la calidad de la entrega de todos los servicios acordados.

Otro elemento digno de estudiar para el manejo de las mejores prácticas de administración es la norma ***ISO 17799,*** que se la conoce como ***Técnicas de seguridad en las tecnologías de la información***; fue revisada en el año 2005. Además, cuenta con el aval de la Organización Internacional para la Estandarización ISO y la Comisión Electrónica Internacional IEC. Plantea lo que se llama planificación continua del negocio ***(BCP, Business Continuity Planning)*** y se enfoca primordialmente en la protección de la confidencialidad, integridad y disponibilidad de los servicios de red.

En su contenido provee de pautas para la recuperación ante incidentes y la manera como una empresa debe planear y prepararse para futuros eventos, son pasos que

sirven para descubrir la debilidad de los procesos. A su vez nos guía en el mejoramiento de la seguridad informática y prácticas para la administración de riesgos.

Básicamente ISO 17799 se resume en seis principales temas:

1. Notificación de desastres.
2. Recuperación del servicio.
3. Retomar las actividades normales.
4. Pruebas de la recuperación del servicio.
5. Manual de mantenimiento.
6. Continuidad en el plan de mantenimiento.

Lo mencionado anteriormente debe ser respaldado por una rutina de procesos técnicos, sistemas de respaldos, sistema para restablecer los registros físicos, implicaciones a terceros y plan de desastres.

Para desarrollar un plan de continuidad se debe tomar en cuenta los siguientes aspectos:

- Análisis.
- Diseño de soluciones.
- Implementación.
- Pruebas y aceptación de la organización.
- Mantenimiento.

3.6.2 Control de Riesgos

Gestionar los posibles riesgos de una empresa requiere de una tarea continua y constante que debe responder a cuatro interrogantes:

1. ¿A qué riesgos está expuesta la empresa?
2. En caso de ocurrencia, ¿Cuál sería el impacto?
3. ¿Con cuánta frecuencia podrían ocurrir éstos incidentes?
4. Qué tan acertadas fueron las respuestas a las primeras preguntas.

El ciclo de administración de riesgos parte de la evaluación de los riesgos hasta finalizar con la reducción o mitigar los mismos. En el proceso intermedio existe un

punto principal donde se enfoca todo el manejar de las vulnerabilidades, para luego crear consciencia en el usuario.

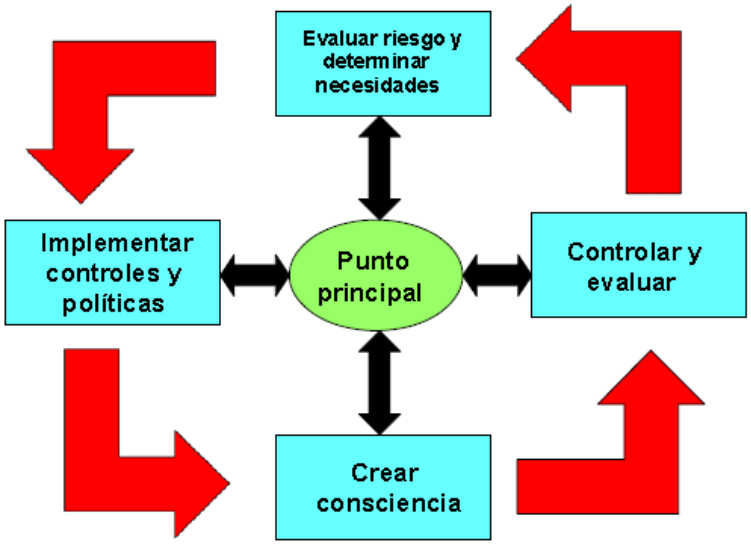


Gráfico 3 24 Administración de riesgos.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 9, página 192.

El tener un equipo de respuesta y un ***plan ante los incidentes***, contribuirá a recuperarse lo más rápido de cualquier inconveniente; lo ideal es prevenir y detectar los errores antes de que se generen. Un equipo de respuesta ***(CIRT, Cyber Incident Response Team)*** debería cumplir con las siguientes tareas:

- Mantener informada a la organización sobre los pasos a seguirse en caso de un incidente.
- Ejecutar un plan documentado ante la ocurrencia de un problema.
- Registro de los procedimientos realizados para mitigar el inconveniente.
- Evitar la propagación del problema (contención).
- Copias de seguridad.
- Restauración de los servicios (continuidad).
- Revisión post mortem.

Gráfico 3 25 Administración de riesgos.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 9, página 194.

3.6.3 Monitoreo de la Red

Para monitorear una infraestructura de red se emplea un sistema de administración de red (NMS), éste sistema circula constantemente por la red registrando las fallas que encuentra, posteriormente notifica a un receptor (Administrador) por medio de un mensaje de correo o algún tipo de alerta o alarma para tomar acciones reactivas. El monitoreo de la conexión a Internet, por ejemplo, se lo puede hacer enviando solicitudes de conexión con el comando ***ping*** al servidor Web cada cierto tiempo para comprobar su funcionamiento. En algunos sistemas con configuraciones más avanzadas se puede programar acciones automáticas para recuperarse de un fallo.

Algunas propiedades que se deben monitorear con NMS son: el uso de CPU, la memoria física, almacenamiento en discos, memoria virtual, servidores de nombres de dominio (DNS), software del servidor web, etc.

Si se tiene la red implementada con voz sobre IP es conveniente monitorear el rendimiento, retardos, puertas de enlace a otras redes, protocolo de iniciación de sesión (SIP), etc.

Además, para el tráfico que se genera por voz sobre IP, es importante registrar las ***llamadas en progreso, llamadas activas, intentos de llamadas y llamadas completas*** para definir parámetros o límites. De ésta manera podremos saber las horas pico y proceder con una planificación. El uso de llamadas exige una interacción con la red pública, por lo que es necesario también monitorear como se establece la conexión.

Con VoIP se genera la posibilidad de realizar conferencias, en este sentido, se debe establecer un límite de secuencias de audio.

El ancho de banda está en función según el tipo de codificación que se va a implementar, por ejemplo, si se decide por el G.711 es requisito poseer 64 Kbps, en los códec que tienen la opción de compresión (G.723 ó G729) se puede reducir el ancho de banda, cuidando que no se sature el canal por una alta afluencia de suscriptores.

Monitorear los retardos o latencia, la oscilación (variación en los retrasos), la pérdida de paquetes y la nota media de opinión (MOS), nos permite mantener una calidad de servicio (QoS). QoS se implementa incluyendo prioridades para cada tráfico de la red.

3.6.4 Seguridad vs. Facilidad de Uso

La seguridad es una característica primordial en una empresa; se fundamenta a partir de conceptos como ***servicios ofrecidos, facilidad de uso y costo de la funcionalidad*** de la infraestructura. Cuando una administrador de red identifica los servicios que va ofrecer evalúa qué tan peligroso es implantar dichas aplicaciones y posterior a ése análisis se decide los posibles niveles de seguridad. En toda institución hay que elegir entre la facilidad de uso y seguridad, por ejemplo, para acceder a la computadora se puede ingresar sin digitar ninguna clave (facilidad de uso) ó entrar con clave (seguridad). Por último el costo de implantar seguridad; tomando el ejemplo anterior, para colocar identificación de accesos es necesario obtener un servidor de seguridad, lo que implica inversión.

3.6.5 Medidas de Control

Es muy recomendable el uso de ***antivirus*** que ayuda en la detección de malware, también, ***detectores de intrusos (IDS)*** y sistemas de ***prevención de intrusos (IPS)***. Los IDS's se enfocan en monitorear los host y la red; los primeros, calculan una función unilateral de los archivos más sensibles cuando se asume que el equipo está libre de virus, a partir de ese estado se va comparando en el futuro; además, utilizan acciones de auditoría y seguimiento de procesos. Los IDS's de red se enfocan en el tráfico de red por medio de rutinas estadísticas, de comparación y algunos en firmas que deben ser actualizadas igual que un antivirus. El proceso estadístico evalúa definiendo un tráfico normal y estudia la concurrencia poco usual. Una buena alternativa es combinar los dos métodos de IDS's.

Las herramientas de prevención de intrusos (IPS'S) se pueden implementar en los host (HIPS) para impedir la ejecución de procesos no autorizados para que ejecuten una respuesta que puede ser la finalización del proceso o el bloque del tráfico de red hacia el host y los NIPS o IPS's de red que se ejecutan a nivel de los servidores de seguridad monitoreando el tráfico de paquetes entrante.

Para el ***filtrado de contenidos*** existen herramientas de ***antispam*** y ***filtro de código*** que actúan de manera eficiente, siempre y cuando, estén delimitadas por procesos de multiniveles para diferenciar correos válidos de los que no lo son, aplicando técnicas heurísticas, estadísticas, listas globales e individuales.

Configurar los servidores de seguridad para que los puertos que no se utilicen estén cerrados, es importante para evitar intrusos en la red.

Todo lo mencionado anteriormente debe enmarcarse en una línea de acción coordinada; determinada por una política de seguridad que englobe: ***uso aceptable*** (equilibrio entre seguridad y facilidad de uso)***, encriptado, antivirus, servidores de seguridad, auditoría y monitoreo, plan de contingencia, filtros para URL's, correo electrónico y contenidos, políticas de contraseñas***.

3.6.6 Estrategias Proactivas

Una infraestructura de red está compuesta por varias capas, generalmente tres, dependiendo del diseño que se haya utilizado, además, con la existencia de muchos

componentes, podemos identificar niveles o capas a las que podemos proteger creando puntos de control.

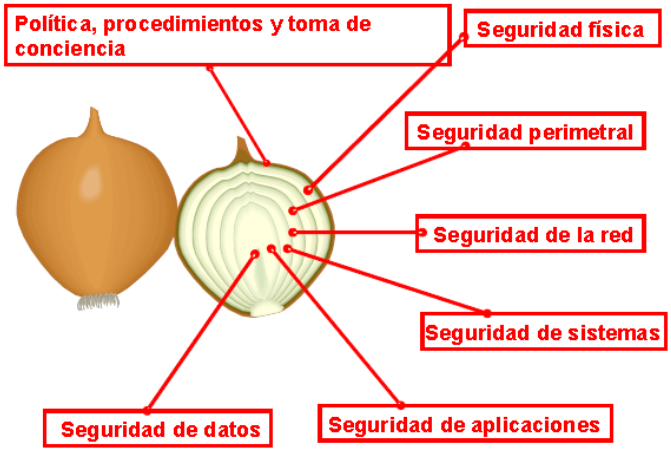


Gráfico 3 26 Seguridad por niveles.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 9, página 195.

La primera línea de control es el perímetro de la red que se identifica localizando el punto de ingreso y egreso de la misma; pueden existir varios puntos en la periferia a más de la conexión con Internet, como extranet y redes virtuales privadas (VPN); sin embargo, no es recomendable puntos de salida porque pueden utilizarse como puertas de entrada para ataques informáticos.

No solo hay una delimitación externa, sino también, interna entre los diferentes departamentos de una empresa, cada uno con diferentes demandas; el objetivo de distinguir áreas determinadas es otorgar permisos adecuados para cada usuario de acuerdo a su función. Para conseguir que no ingrese tráfico malicioso desde el exterior o ingresos indebidos, la técnica que se usa es implantar un servidor de seguridad, o un grupo de ellos, entre las dos zonas distinguidas. También, se pueden usar defensas como:

Combinación de servidores de seguridad internos y externos.

Monitorear y documentar cada acceso a la red.

Utilizar texto encriptado no contenidos planos fáciles de leer.

Cifrar el tráfico de red generado por una VPN utilizando ***SSL, Secure Socket Layer*** y ***SSH, Secure Shell*** (interfaz de usuario segura).

Verificar la autentificación de usuario.

Aplicar filtros.

Pruebas de vulnerabilidad.

En la capa de red se puede implementar detectores de intrusos ***(IDS, Intrusion Detection System)*** para identificar acertadamente las posibles fallas, esto es importante, pues permite tiempos de recuperación menores. Existen también, sistemas de prevención de intrusos ***(IPS, Intrusion Prevention System)*** con la capacidad de configurar otros equipos para impedir el ingreso de tráfico malicioso de manera automática.

Herramientas de monitoreo de tráfico ayudan en la detección de anomalías, generalmente, un cambio repentino de tráfico en el correo puede indicar la presencia de código malicioso.

Las listas de control de acceso ***(ACL, Access Control Lists)*** por medio de bloqueos evita el tráfico a direcciones IP no registradas.

3.6.7 FCAPS (Fault, Configuration, Acounting, Performance, Security)

Para asegurar la entrega de servicios efectivamente, es necesario contar con una base de información que nos permita dilucidar todos los posibles escenarios que puedan afectar el desenvolvimiento normal de la infraestructura de red; para cumplir con el requerimiento anterior necesitamos monitorear, conocer todas las características relacionadas, y lo más importante tener un marco de referencia para obtener lo requerido.

Podemos sustentarnos en estándares ya probados para la administración, como es el caso FCAPS (Fault, Configuration, Acounting, Performance, Security). FCAPS es una norma utilizada en telecomunicaciones que nos sirve de base para adaptar un

formato parecido aplicado a las redes de datos. Los puntos principales que abarca la norma se describen en el cuadro a continuación.

F	C	A	P	S
Fault detection	Resource initialization	Track service / resource usage	Utilization & error rates	Selective resource access
Fault correction	Network provisioning	Cost for services	Consistent performance level	Enable NE functions
Fault isolation	Auto-discovery	Accounting limit	Performance data collection	Access logs
Network recovery	Backup and restore	Combine costs for multiple resources	Performance report generation	Security alarm / event reporting
Alarm handling	Resource shut down	Set quotas for usage	Performance data analysis	Data privacy
Alarm filtering	Change management	Audits	Problem reporting	User access rights checking
Alarm generation	Pre-provisioning	Fraud reporting	Capacity planning	Take care of security breaches & attempts
Clear correlation	Inventory/asset management	Support for different modes of accounting	Performance data & statistics collection	Security audit trail log
Diagnostic test	Copy configuration		Maintaining & examining historical logs	Security related information distributions
Error logging	Remote configuration			
Error handling	Job initiation, tracking & execution			
Error statistics	Automated software distribution			

Gráfico 3 27 FCAPS.

Referencia:

http://www2.tech.purdue.edu/cit/courses/cpt443/resources/assignments/FCAPS_TMN_ITIL.pdf

Para aplicar el estándar FCAPS en una red de datos se puede implementar un modelo simplificado que consiste en cuatro capas:

1. Administración del desempeño / administración de la disponibilidad para asegurar un buen rendimiento y proporcionar los servicios requeridos por los clientes.
2. Administración de la seguridad para prevención de errores y respuesta inmediata a fallos.
3. Administración de configuraciones y vulnerabilidad que permita afinar la red, de manera que exista una correlación con las directivas del negocio.
4. Administración de control de cambios para que solo el personal autorizado realice modificaciones y llevar un control de los mismos.

Para redes convergentes podemos enfocarnos en la administración en conjunto de los siguientes aspectos:

Integridad operativa.

Administración de los servicios.

Cumplimiento de las políticas.

Manejo de riesgos.

En el cuadro a continuación cada una de las acciones se las puede realizar conjuntamente en paralelo. Algunas empresas toman como base ITIL (Information Technology Infrastructure Library) para gobernar los procesos relacionados con las tecnologías de la información y en ocasiones, la información generada en una empresa es compartida con otra para minimizar el costo de la implementación. ITIL se refiere a las mejores prácticas que se pueden aplicar en una empresa para la administración de las plataformas tecnológicas. El objetivo es generar lo que se conoce como un ***modelo de madurez*** que permite trabajar en base a los requerimientos del negocio y a través de procesos continuos para obtener los mejores resultados.

	Performance Management—Availability Management	**Security Management**	**Configuration and Vulnerability Management**	**Change Control Management**
Operational Integrity	Monitor system and network performance	Continually monitor threat environment	Identify vulnerable or exploited systems	Ensure no unauthorized changes are made to operating environment
Service Management	Map performance indicators to business issues	Event correlation of security incidents with performance issues	Benchmark and baseline system configurations	Delegate admin change permission only to approved staff
Policy Compliance	Measure SLAs and compliance	Protect audit trails, monitor and report security violations	Ensure baselines follow corporate standards and policies	Audit logs for all changes to production environment
Risk Management	Forecast and avoid service interruptions	Identify, mitigate, and respond to security incidents	Identify, assess, document, and remediate or accept risks	Test changes before implementation to minimize risk

Gráfico 3 28 Modelo de 4 capas.

Referencia: Realtime publishers CA. The Definitive Guide to Converged Network Management, Capítulo 7, página 148.

4 DISEÑO DE RED

En el diseño que proponemos, establecemos una red local (LAN) implementada con cable para el edificio matriz y una red LAN inalámbrica para las oficinas regionales. Estas a su vez se conectan entre sí por un diseño de red extendido (WAN).

4.1 Diseño LAN/ WAN

Al proponer una solución óptima para brindar el servicio de red, nos basamos en las recomendaciones de CISCO Systems, es decir, en el diseño de tres capas.

En lo que se refiere a la red LAN abarcamos 2 soluciones. La primera se desarrolla para dar una solución a entornos de oficinas reducidos, específicamente, una solución inalámbrica para las sucursales en provincias que poseen menos de 15 equipos. La segunda alternativa LAN es diseñada para el edificio matriz de la Corte Constitucional, aquí, por los servicios que entrega a los usuarios internos y a los equipos que poseen, se recomienda una red que disponga cableado estructurado en su ambiente .

El diseño WAN está orientado a enlazar las sucursales de provincias con la matriz; para cumplir con ese objetivo utilizaremos enlaces de La Compañía Nacional de Telecomunicaciones CNT.

4.1.1 RED WAN

Para el diseño de la red WAN contrataremos los servicios de la empresa Nacional de Telecomunicaciones CNT. El motivo principal para utilizar una red externa es por el costo de la implementación; es decir, optimización de recursos (tiempo, dinero y experiencia).

Generalmente la empresa que provee servicio de red WAN son las empresas de telefonía fija, puesto que, han implementado una red previa punto a punto, o dicho de otra manera, han establecido una ruta (circuito) entre dos puntos geográficos; circuito que puede ser utilizado para otras funcionalidades. CNT es el caso.

CNT maneja una red WAN con protocolo MPLS (MultiProtocol Label Switching), que “es un estándar IP de conmutación de paquetes”[22]; la característica principal de estas redes es que permiten reservar recursos físicos antes de que el paquete llegue a su destino, esto lo hace, asignando una etiqueta (FEC, Forward Equivalence Class) a cada elemento de la tabla de un router o switch dentro de la red MPLS. Al conocer con anterioridad una ruta podemos implementar calidad de servicio (QoS), es decir, asignar niveles de prioridad al transportar la información. Es importante establecer calidad de servicio porque existe información que no puede soportar retardos en la transmisión, es el caso, de las llamadas telefónicas por protocolo IP (VoIP), video conferencias y consultas a motores de bases de datos.

En MPLS existe el concepto de LSP (Label switching Path), que es un camino de tráfico específico a través de una MPLS y que son creados utilizando los LDPs (Label Distribution Protocols), tales como RSVP-TE (ReSerVation Protocol – Traffic Engineering).

En una red MPLS se distinguen 2 tipos de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers). La información de la topología de una red MPLS se intercambia a través de los protocolos usuales OSPF, RIP y BGP.

Los LER se localizan en el borde de la red sirviendo de comunicación entre los dispositivos fuera de la red MPLS y añadiendo etiquetas MPLS que son identificadas por los LSR, que se ubican en el núcleo de la red para realizar encaminamiento de alto rendimiento, como se puede apreciar en la figura a continuación.

[22] Huidobro Moya José Manuel y Millán Tejedor Ramón, *MPLS (MultiProtocol Label Switching)*, Internet: http://www.ramonmillan.com/tutoriales/mpls.php Acceso: 08/diciembre/2011.

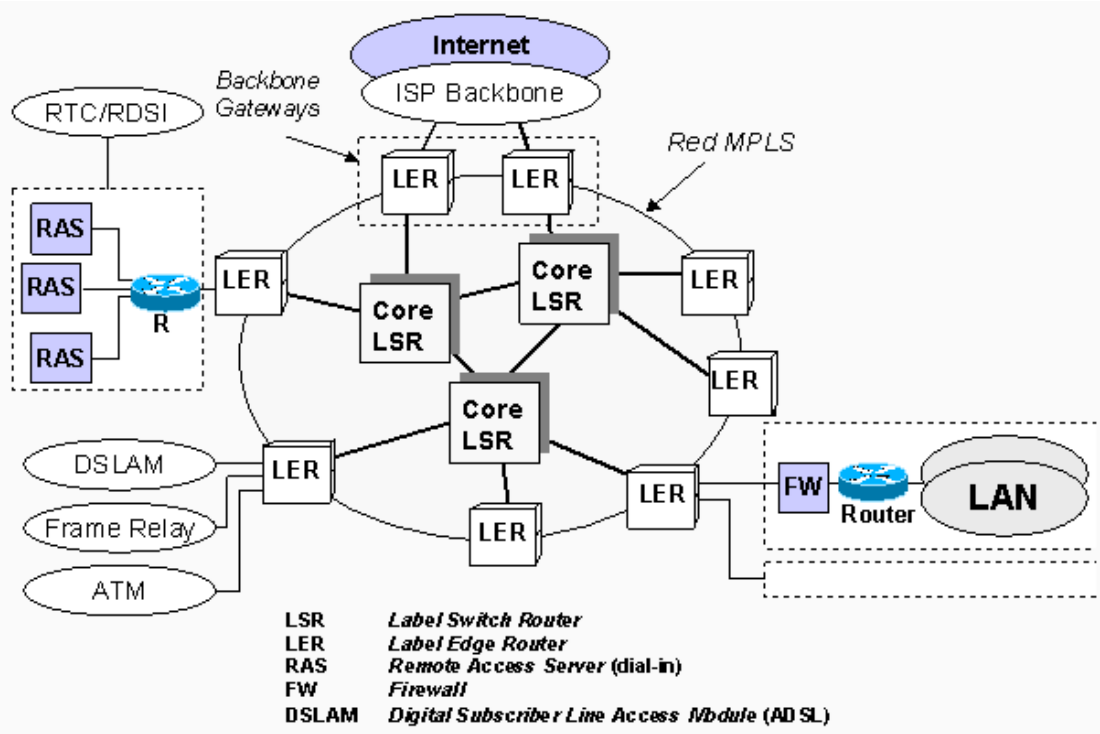


Gráfico 4. 1

Referencia: Internet: http://www.ramonmillan.com/tutoriales/mpls.php. Autor: Ramon Millán, Acceso 09/nov/2011.

4.1.2 Direccionamiento WAN.

Para el direccionamiento WAN tomaremos en cuenta las sucursales a implementar. Las sucursales con las que se cuenta son 8. Utilizaremos la red 192.168.200.x con máscara 255.255.255.252 esto permite tener una subred con 4 IPs en total, sin embargo las subredes utilizables son 2 porque la primera y la última son utilizadas para broadcast

OFICINAS	RED	MASCARA	IP UTILIZABLES
Quito/Ibarra	192.168.200.12	255.255.255.252	2
Quito/Riobamba	192.168.200.28	255.255.255.252	2

Quito/Cuenca	192.168.200.4	255.255.255.252	2
Quito/Guayaquil	192.168.200.0	255.255.255.252	2
Quito/Loja	192.168.200.36	255.255.255.252	2
Quito/Machala	192.168.200.64	255.255.255.252	2
Quito/Portoviejo	192.168.200.48	255.255.255.252	2
Quito/Orellana	192.168.200.112	255.255.255.252	2

Tabla 4. 1 Direccionamiento WAN

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Además, tomamos en cuenta que para poder establecer una red institucional debemos también diseñar un direccionamiento local, esto permite, comunicación bidireccional. Para el caso de estudio, proponemos segmentos dentro de nuestra propia red:

OFICINAS	RED	MASCARA	IP UTILIZABLES
Quito/Ibarra	192.168.16.x	255.255.255.0	254
Quito/Riobamba	192.168.20.x	255.255.255.0	254
Quito/Cuenca	192.168.14.x	255.255.255.0	254
Quito/Guayaquil	192.168.15.x	255.255.255.0	254
Quito/Loja	192.168.22.x	255.255.255.0	254
Quito/Machala	192.168.29.x	255.255.255.0	254
Quito/Portoviejo	192.168.25.x	255.255.255.0	254
Quito/Orellana	192.168.41.x	255.255.255.0	254

Tabla 4. 2 Direccionamiento LAN - Sucursales

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

El direccionamiento propuesto debe ser configurado en los equipos frontera (router de CNT), para establecer la red de la Corte Constitucional.

4.1.3 LAN Sucursales propuestas

Como se enunció en el capítulo anterior, los requerimientos primordiales en las oficinas que se encuentran distantes de la principal, son el acceso a Internet y la sincronización de datos con la oficina matriz en Quito (las regionales son oficinas informativas y pedagógicas).

Son pocas máquinas (3 computadoras) ubicadas en espacios reducidos, por lo mencionado, proponemos sucursales (redes locales) con host enlazados con tecnología wireless, nos enfocaremos en un diseño de alta disponibilidad y escalabilidad.

El diseño óptimo que se apega a las observaciones de CISCO, consiste en la elaboración de capas (modelo jerárquico), cada una de ellas cumple con una función específica; en cada nivel se disponen dispositivos que permite enviar información a la siguiente capa.

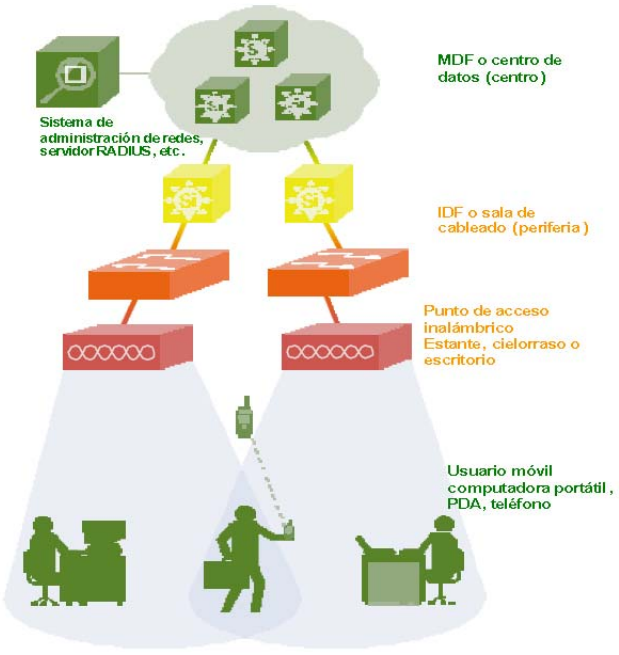


Gráfico 4. 2 *Capas en una red local Wireless.*

Referencia: Infraestructura física de redes LAN inalámbricas empresariales, autor Viswas Purani.

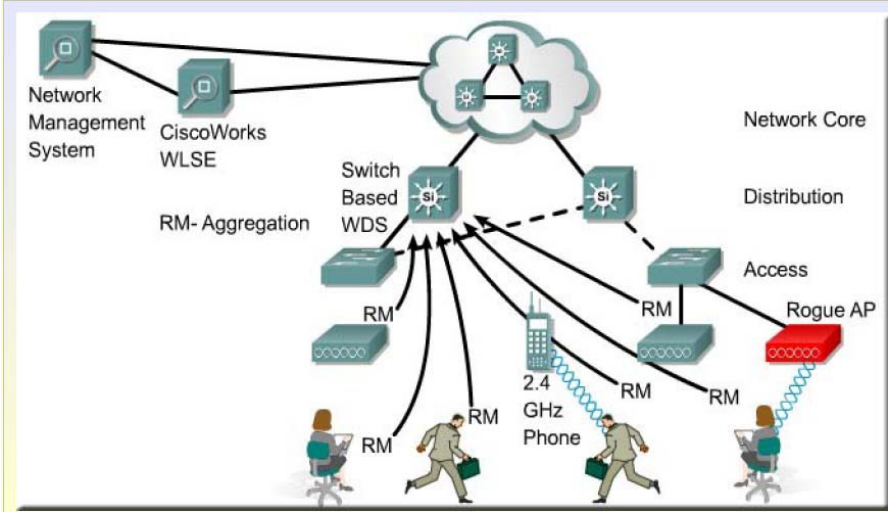


Gráfico 4. 3 *Capas en el desarrollo de una red local Wireless.*

Referencia: Internet: www.cesaercabrera.info, Wireless LAN: Diseño, autor César A. Cabrera E.

Un AP Access point o punto de acceso se puede acoplar en el techo, otros en la pared. La ubicación del AP responde a un tema de difusión y análisis del área o lóbulo de propagación que proporciona la antena, es decir, se lo coloca en el lugar donde la señal sea óptima para cada uno de los equipos involucrados. Uno de los inconvenientes de un punto de acceso (AP) es que depende de la corriente eléctrica, esto hace vulnerable al entorno local externo, es por eso que se aconseja que se instalen dispositivos de almacenamiento eléctrico UPS en caso de un corte energético. Una mejor solución es tomar la alimentación de la red Ethernet mediante los switches que poseen UPS.

Para el diseño tomamos en cuenta los siguientes requerimientos:

Cobertura y velocidad.- al momento se cuenta con 3 equipos o 2 equipos por cada departamento regional, las oficinas no son muy grandes (menos de 40 metros), lo que posibilita que la cobertura de un solo Access point sea suficiente. La velocidad que proporcionan los estándares es de 54 Mbps a 2.4 GHz. Trabajaremos con el estándar 803.11g por motivos de compatibilidad.

Roaming transparente.- al referirnos a roaming expresamos la característica de movilidad, es decir, acceder a los recursos de la red sin importar que cambiemos de

sitio; con transparencia nos referimos a que el usuario no experimente ninguna percepción de cambio en el servicio, aunque éste se produzca. En el caso que estamos estudiando no es necesario diseñar una red que posea ésta característica, debido a que, el área de trabajo es pequeña y la zona de cobertura de un punto de acceso cubre a todo el sector donde se trabaja, sin embargo, hay que prevenir una futura expansión (escalabilidad), y por eso se recomienda la compra de equipos que soporten una ampliación.

Redundancia.- se refiere a la posibilidad de ampliar la cobertura de un access point colocando otro dispositivo con una superposición del 50% sobre el área de cobertura del primer punto de acceso. En el caso de las sucursales regionales, por el momento no es necesario establecer redundancia.

Permisos.- es importante restringir el acceso de personas ajenas a la Corte al uso del Internet. Los dispositivos de entrada (AP) establecen filtros, claves y SSID para autorizar el ingreso.

Disposición de los dispositivos AP.- para delimitar la disposición de los AP tomamos en cuenta la velocidad mínima requerida que en este caso es de 512 Kbps. Un AP nos puede proporcionar desde 11Mbps hasta 54 Mbps dependiendo del estándar utilizado y de la antena que propaga las ondas.

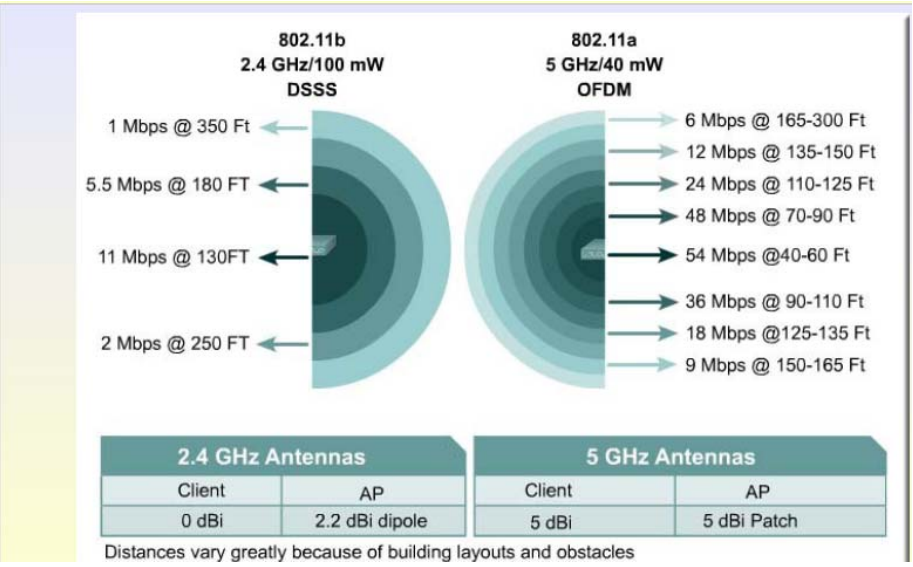


Gráfico 4. 4 *Área de propagación y velocidad de transferencia en un AP.*

Referencia: Internet: www.cesaercabrera.info, Wireless LAN: Diseño, autor César A. Cabrera E.

Para el caso en estudio no se requiere de un análisis a profundidad para la colocación de los AP, debido a que son 3 computadores por oficina. Lo que se aconsejaría es que los computadores estén en un radio de menos de 130 FT para una buena recepción.

Se debe tomar en cuenta las condiciones físicas de las oficinas en especial lo siguiente:

- Inspeccionar obstáculos físicos.
- Analizar posibles interferencias.
- Factibilidad de la cobertura.
- Planos del edificio.
- Infraestructura del edificio.

Para el análisis de la señal, en las tarjetas cisco de la serie 350 se incluyen 2 opciones (passive/active). El modo pasivo estudia el espectro, mientras que, el modo activo envía paquetes para encontrar APs.

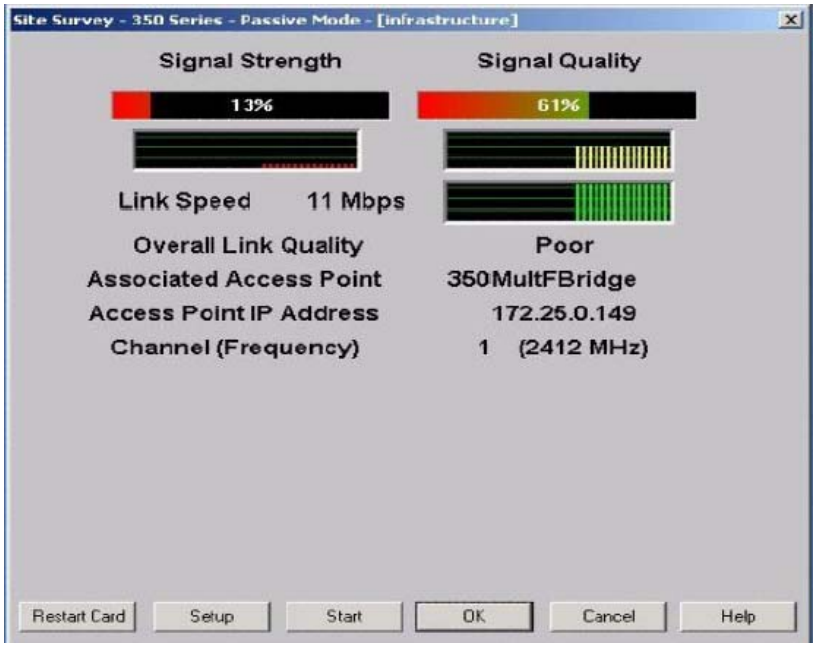


Gráfico 4. 5 *Modo pasivo en una tarjeta inalámbrica.*

Referencia: Internet: www.cesaercabrera.info, Wireless LAN: Diseño, autor César A. Cabrera E.

La topología a utilizar es una infraestructura básica (BSS), es decir, la cobertura es proporcionada por un solo access point, sin embargo, se puede extender la infraestructura colocando otro como se indica en la figura a continuación.

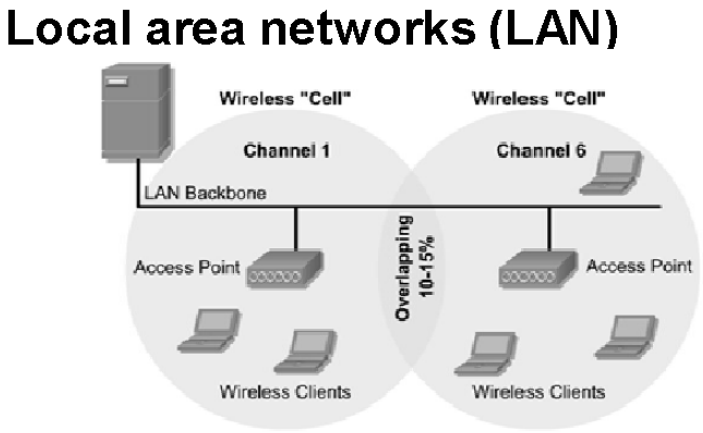


Gráfico 4. 6 *Infraestructura básica inalámbrica LAN.*

Referencia: Internet: www.cesaercabrera.info, Wireless LAN: Diseño, autor César A. Cabrera E.

Inclusive actualmente, las empresas proveedoras del servicio de Internet (ISP), ofrecen modems wireless que se podrían utilizar como Puntos de acceso para una pequeña red WLAN.

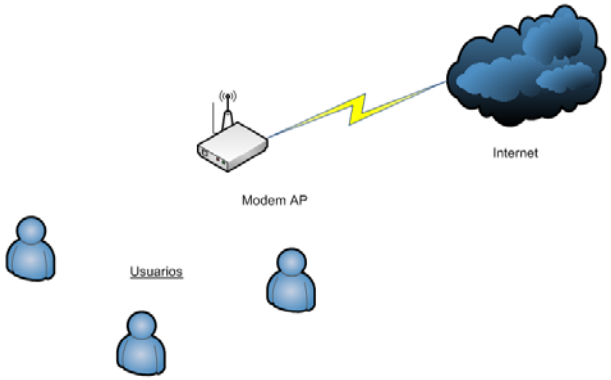


Gráfico 4. 7 *Conexión LAN – WAN.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

El mismo diseño es aplicable a todas las oficinas regionales, debido a que son oficinas con un área de trabajo pequeña con requerimientos mínimos, de hecho son, oficinas de ***carácter pedagógico e informativo,*** diseñadas para promover la cultura constitucional.

4.2 Diseño LAN Oficina Central.

4.2.1 Generalidades

La infraestructura de una red debe ser planificada con el objetivo de que sea segura, fácil de administrar y pensando en futuras expansiones.

Se trata de mejorar la conectividad usuario – aplicación; esto se logra optimizando los recursos en el diseño de red. El cableado de datos se distribuye por los 10 pisos y en cada piso existe un switch, dicho elemento, es importante porque a través de él circularán los datos y se repartirá la información. La solución que sugerimos es adquirir nuevos equipos tanto en switches como en servidores para que el tráfico de la información sea óptimo y en un futuro, si los requerimientos así lo exigen, instaurar asociaciones lógicas (redes virtuales) entre los computadores que tienen al menos una característica en común para que se agrupen en menos segmentos. En el diseño que proponemos no es necesario crear VLANs.

Hay que tomar en cuenta una posible expansión de la empresa, es decir, prever el ingreso de más usuarios, aplicaciones y requerimientos en los equipos.

Que una red sea adaptable, significa que sea capaz de acoplarse a tecnologías futuras, la mejor forma de cumplir con esto es seguir los estándares de las entidades certificadoras, ya que, cualquier nuevo avance se enmarca en los parámetros normalizados que contemplan compatibilidad. Es por esta razón, que en el desarrollo de este trabajo trabajaremos con cableado estructurado siguiendo el estándar TIA/EIA-568-B y para la implementación del centro de procesamiento de datos la norma TIA – 942.

Además, es primordial que tengamos la opción de monitorear fácilmente nuestra red, para que en el caso de algún error, podamos localizar el origen del mismo lo más rápido posible. Por esta razón, más adelante, en este capítulo revisaremos el uso de una herramienta de monitoreo PRTG PAESSLER.

4.2.2. Diseño de 3 Capas CISCO

El modelo de tres capas sugerido por CISCO Systems, es de carácter jerárquico, es decir, una clasificación de las funciones que tiene cada capa, esto permite facilidad en el diseño en lo que se refiere a entendimiento y configuración.

En el modelo por niveles se distinguen tres capas:

El ***Núcleo*** "ofrece conexiones rápidas"[23]; es el nodo central de una empresa, es de donde parten los datos y su objetivo es transportar de manera segura el tráfico que se genera. Para diseñar una capa núcleo eficiente nos debemos orientar en conmutar los paquetes lo más rápido posible. Además, es importante no implementar políticas de red que retrasen el envío de paquetes, y por último, que todos los dispositivos de ésta capa logren alcanzar completamente su destino en la red.

La *capa de* ***distribución*** "ofrece servicios de red a las distintas LAN"[24]; es donde actúan los equipos que sirven para llegar a diferentes partes de la infraestructura física y a los servicios de la misma. Aquí toma importancia el control de paquetes para definir

[23] Cisco Systems, *Guía del segundo año. CCNA® 3 y 4*. Madrid, Pearson Educación S.A., 3ra edición, 2004. Página 405.

[24] Ídem 23.

rutas, minorar los dominios de colisión, accesos a grupos de trabajo o a departamentos, ruteo para redes virtuales y seguridad.

Por último, en la *tercera capa* o nivel de ***acceso*** "proporciona a los usuarios acceso de primera línea a los servicios de red"[25]; se alimenta el tráfico y la comunicación hacia la red a través de equipos en los que trabajan los usuarios. En ésta capa se deben implementar niveles de seguridad, filtros, listas de acceso. Computadores de escritorio, dispositivos y puntos de acceso, cumplen la función de compartir ancho de banda, control de acceso al medio y micro segmentación.

Para el caso de este estudio hemos dividido las capas de la siguiente manera:

- Capa de acceso: conexiones horizontales (HCC), dispositivos y APs.
- Capa de distribución: switches que se encuentran en los IDF.
- Capa núcleo: centro de procesamiento de datos.

A continuación expondremos el diseño lógico de la solución de red propuesta, el mismo que incluye los recintos de cableado, tipo de cableado y áreas de servicio. Tomemos en cuenta los 3 niveles: acceso (áreas de trabajo); distribución (IDF) y núcleo (MDF).

[25] Ídem 24.

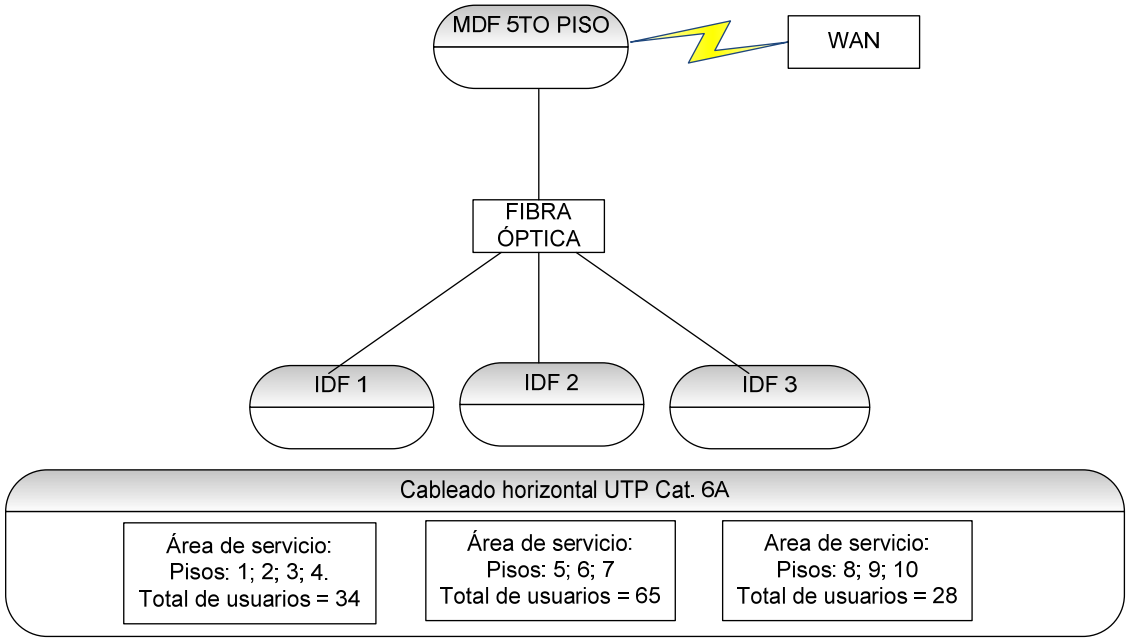


Gráfico 4. 8 *Diagrama lógico de red LAN 3 NIVELES.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

4.2.3. Diseño de la Capa de Acceso.

Como se ha mencionado en el modelo jerárquico la capa de acceso es la encargada de proporcionar servicio a todos los usuarios de una red.

Proponemos una estructura de estrella extendida porque es tolerante a fallos, es decir, sí, una de las máquinas conectadas no responde, la afectación es sólo a esa máquina, además, es fácil de implementar, basta con conectar el host a un conmutador para obtener la funcionalidad requerida.

El cableado que proponemos como óptimo es fibra óptica para el backbone y para las conexiones horizontales utilizaremos cables categoría 6A. Con cable UTP categoría 6A se puede transmitir hasta velocidades Gigabit Ethernet con una frecuencia de 250 MHz en cada par.

La topología que se utilizará es una de estrella extendida con sólo un recinto de cableado principal y 4 secundarios.

Se trata de segmentar la red adecuadamente para conseguir un mejor rendimiento del canal de comunicación. Para el cableado horizontal utilizaremos categoría 6A con capacidad de transmisión de 1000Mbps. Es necesario, hacer un análisis de requerimientos para determinar la cantidad de puertos necesarios, la distribución y ubicación en cada IDF.

Para el análisis de ancho de banda y dominio de colisión tomaremos en cuenta el número de usuarios y la velocidad de acceso al recinto principal MDF que es de donde parten los datos.

Éste recinto proveerá de comunicación a 63 usuarios en 13 oficinas como se detalla a continuación:

Oficina	Usuarios	Oficina	Usuarios
Archivo	3	Comunicación	7
Registro Oficial	3	Sistemas	7
Documentación	3	Asesoría Jurídica	8
Biblioteca	3	Dir. Administrativa	5
RRHH.	4	Adquisiciones	3
Almacén	2	Contabilidad	5
Tesorería	6		

Tabla 4. 3 Usuarios IDF1

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

En total en el IDF1 hay 63 usuarios.

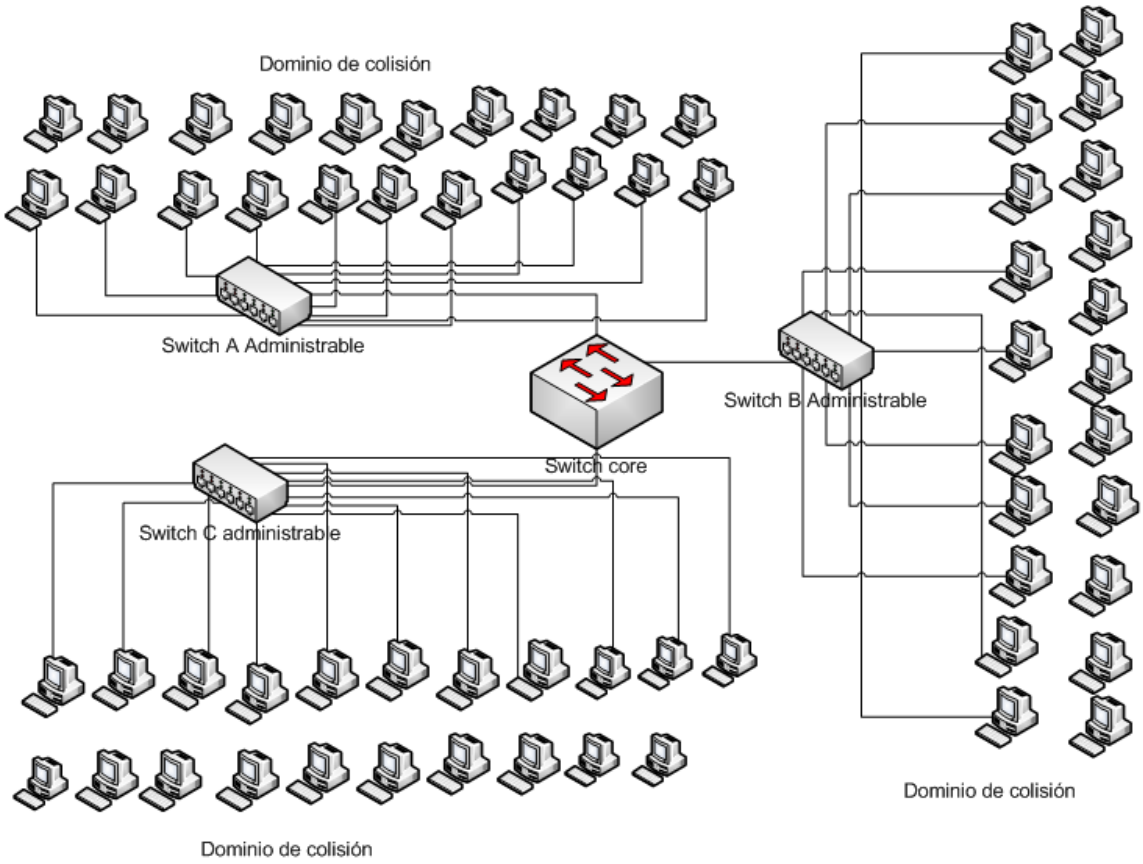


Gráfico 4. 9 *Diagrama dominio de colisión.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Switch A: dominio de colisión = 21 hosts

Promedio ancho de banda = 100 Mbps/21 hosts = 4.762 Mbps por host.

Switch B: dominio de colisión = 21 hosts

Promedio ancho de banda = 100 Mbps/21 hosts = 4.762 Mbps por host.

Switch C: dominio de colisión = 21 hosts

Promedio ancho de banda = 100 Mbps/21 hosts = 4.762 Mbps por host.

Análisis de puertos para el IDF que se encuentra en el MDF

El área de servicio del cableado horizontal que comparte el recinto principal comprende los pisos 5, 6 y 7 de la forma a continuación detallada:

Oficina	Usuarios	Oficina	Usuarios
P5 sala 1	4	P5 sala 3	4
Vocal	2	P6 sala 1	2
Vocal	2	P6 sala 2	2
Vocal	2	P6 sala 3	2
P5 sala 2	2	P6 sala 4	4
P5 sala 4	3	Vocal	2
P6 sala 5	2	P6 sala 8	2
P6 sala 6	2	P7 sala 1	2
P6 sala 7	4	P7 sala 2	4
P7 sala 3	4	P7 sala 4	2
P7 sala 5	3	P7 sala 6	4
P7 sala 7	5	Vocal	2

Tabla 4. 4 Usuarios IDF2

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

En este IDF tenemos un total de 65 usuarios divididos entre los pisos 5, 6 y 7

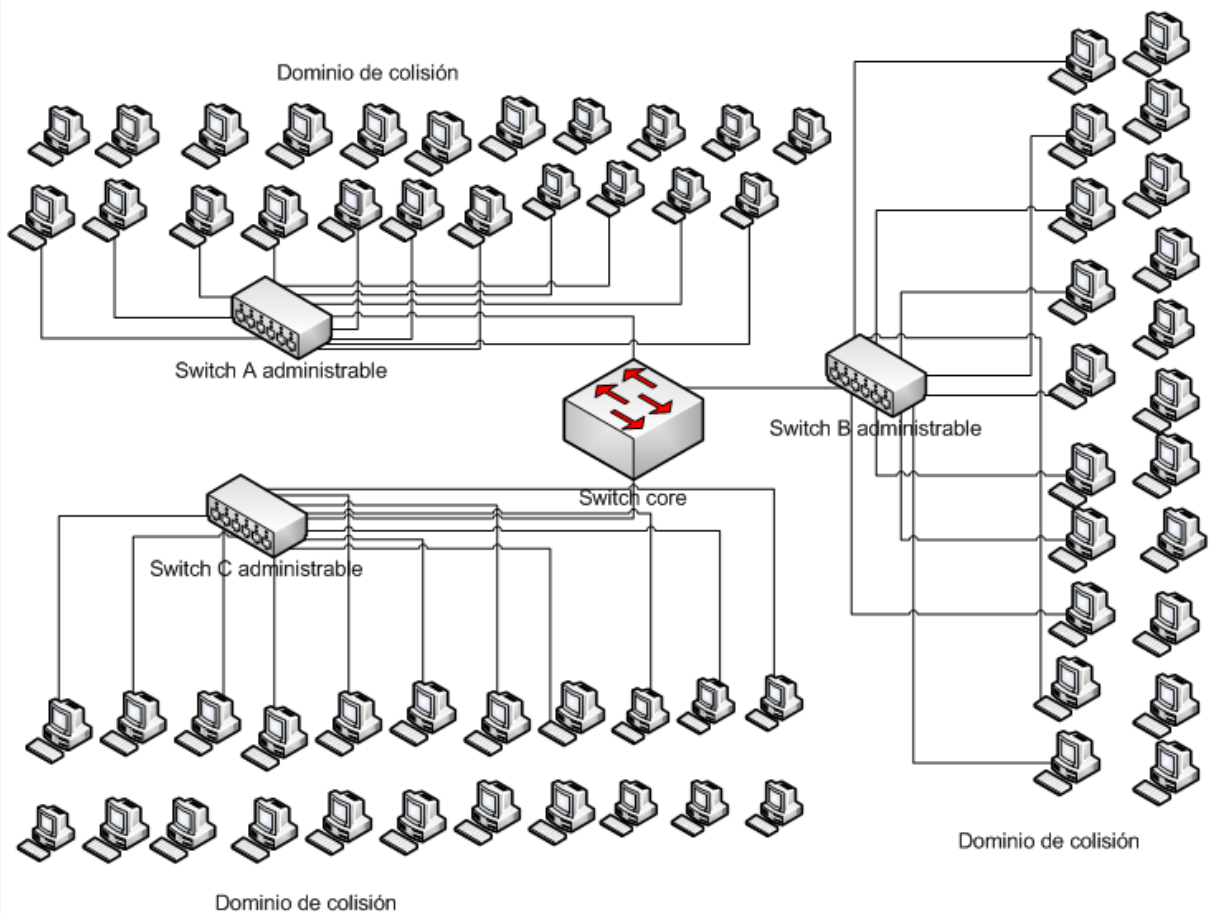


Gráfico 4. 10 *Diagrama dominio de colisión.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Switch A: dominio de colisión = 22 hosts

Promedio ancho de banda = 100 Mbps/22 hosts = 4.545 Mbps por host.

Switch B: dominio de colisión = 21 hosts

Promedio ancho de banda = 100 Mbps/21 hosts = 4.762 Mbps por host.

Switch C: dominio de colisión = 22 hosts

Promedio ancho de banda = 100 Mbps/22 hosts = 4.545 Mbps por host.

Análisis de puertos IDF2.

En éste lugar se atenderá a los pisos 8, 9 y 10 con un total de usuarios repartidos así:

Oficina	Usuarios	Oficina	Usuarios
Secretaría Gral.	15	Secretaría Presidencia	4
Vicepresidencia	2	Seguridad	2
Presidencia	3	P10 sala 1	4
P10 sala 2	12		

Tabla 4. 5 Usuarios IDF3

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Total = 44.

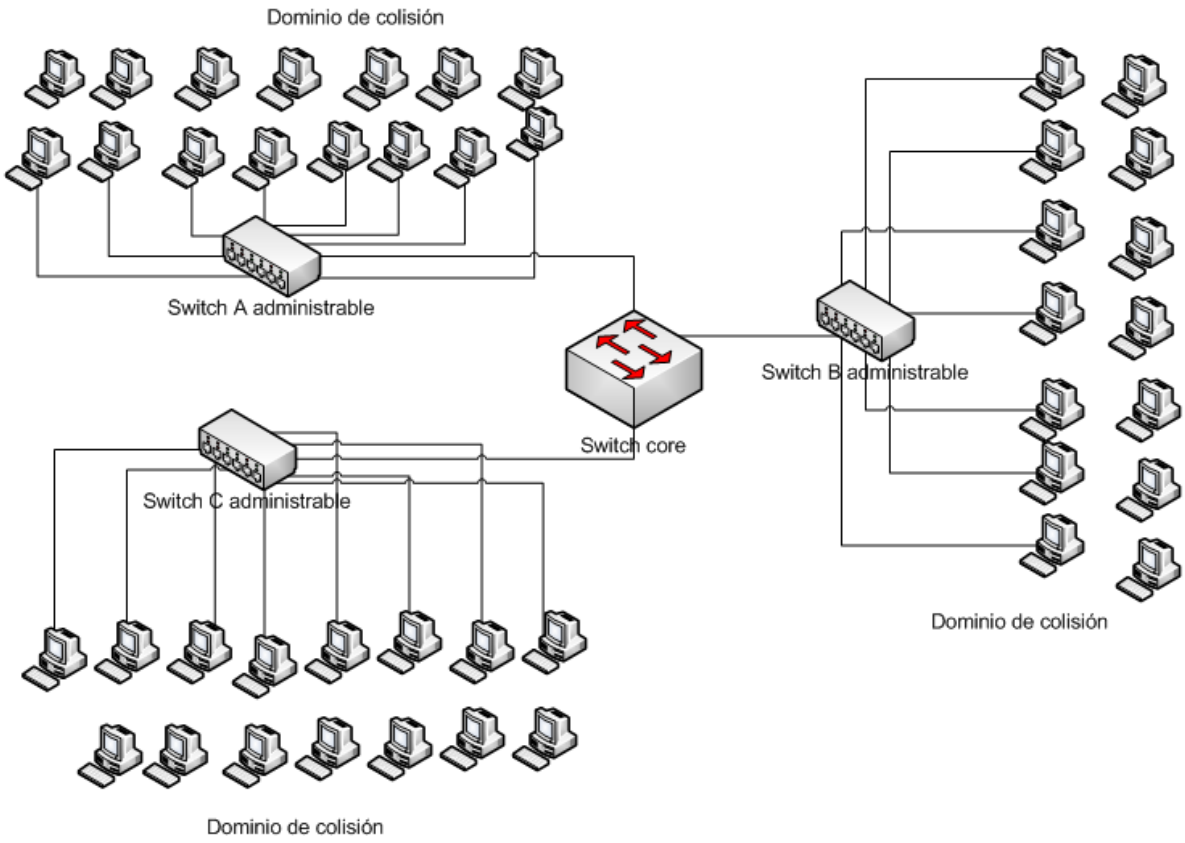


Gráfico 4. 11 *Diagrama dominio de colisión.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Switch A: dominio de colisión = 15 hosts

Promedio ancho de banda = 100 Mbps/15 hosts = 6.667 Mbps por host.

Switch B: dominio de colisión = 14 hosts

Promedio ancho de banda = 100 Mbps/14 hosts = 7.143 Mbps por host.

Switch C: dominio de colisión = 15 hosts

Promedio ancho de banda = 100 Mbps/15 hosts = 6.667 Mbps por host.

En los diagramas no se especifica dispositivos como impresoras ipad, softphone, o puntos de acceso para redes inalámbricas, sin embargo, en el diseño se propone puertos libres que pueden ser utilizados para estas funcionalidades.

4.2.4. Diseño de la capa de distribución.

Es importante tomar en cuenta que el modelo de 3 capas es un concepto que permite diseñar una red, no existen dispositivos específicos para cada capa, es más, equipos del mismo modelo pueden funcionar en distintas capas, es el uso quien determina la jerarquía.

Esta capa permite la conexión entre la capa de acceso y la capa núcleo, aquí se puede implementar políticas de ruteo y seguridad. En nuestro caso a este nivel lo denominamos servicio de distribución intermedia (IDF), aquí, se encuentran 3 switches administrables; recomendamos utilizar la marca CISCO serie Catalyst modelo 2960G-24TC, que tiene la ventaja de poseer 24 puertos con velocidades de conexión 10, 100, 1000 Mbps. Los mismos equipos implementan políticas de ruteo, seguridad y las condiciones necesarias para una buena conmutación.

Vamos a estudiar la implementación del IDF1, tomando en cuenta que la cantidad de usuarios a abastecer es de 63, utilizaremos 3 switches Catalyst serie 2960 de 24 puertos, esto nos permite una escalabilidad del 12.5 % (9 puertos libres). Para conectarse con el nodo central MDF; el IDF se conecta por uno de los puertos con velocidad 1000 Mbps. Los switches restantes se interconectan con el primer switch, esto se conoce como conexión en cascada.

Dispositivo	Enlace	Tipo/Puertos	Cable	IDF
Switch 1	HCC-S1	HCC/puertos 1-21	UTP 6A	1
Switch 1	S1-S2	Cascada/puerto Gbps	UTP 6A	1
Switch 1	IDF1-MDF	VCC1/puerto Fibra	Fibra	1
Switch 2	HCC-S2	HCC/puertos 1-21	UTP 6A	1
Switch 2	S2-S1	Cascada/puerto Gbps	UTP 6A	1
Switch 3	S3-S2	Cascada/puerto Gbps	UTP 6A	1
Switch 3	HCC-S3	HCC/puertos 1-21	UTP 6A	1

Tabla 4. 6SWITCHES Y PUERTOS EN EL IDF1.

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Dispositivo	Enlace	Tipo/Puerto	Cable	IDF
Switch 4	HCC-S4	HCC/puertos 1-22	UTP 6A	2
Switch 4	S4-S5	Cascada/puerto Gbps	UTP 6A	2

Switch 4	IDF4-MDF	VCC4/puerto Fibra	Fibra	2
Switch 5	HCC-S5	HCC/puertos 1-21	UTP 6A	2
Switch 5	S5-S4	Cascada/puerto Gbps	UTP 6A	2
Switch 6	S6-S5	Cascada/puerto Gbps	UTP 6A	2
Switch 6	HCC-S6	HCC/puertos 1-22	UTP 6A	2

Tabla 4. 7 Switches y Etiquetado IDF2.

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Dispositivo	Enlace	Tipo/Puerto	Cable	IDF
Switch 7	HCC-S7	HCC/puertos 1-15	UTP 6A	3
Switch 7	S7-S8	Cascada/puerto Gbps	UTP 6A	3
Switch 7	IDF4-MDF	VCC4/puerto Fibra	Fibra	3
Switch 8	HCC-S8	HCC/puertos 1-14	UTP 6A	3
Switch 8	S8-S7	Cascada/puerto Gbps	UTP 6A	3
Switch 9	S9-S8	Cascada/puerto Gbps	UTP 6A	3
Switch 9	HCC-S9	HCC/puertos 1-15	UTP 6A	3

Tabla 4. 8 Switches en IDF3.

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

A menudo se requiere realizar una división lógica de acuerdo a los criterios funcionales de una institución, con la ayuda de equipos de conmutación se logra conectar, transportar y comunicar los datos en una red y obtener dicho objetivo; con la

utilización de switches administrables, estableceremos VLAN, o como se conocen, redes virtuales para cada departamento.

Los dispositivos Catalyst de la serie 2960 permiten la creación de VLANs; son dispositivos de capa 3 que permiten la comunicación entre segmentos de la red LAN. Dichos switches brindan servicios de filtrado de difusión, seguridad y administración del flujo de tráfico.

El flujo de los datos se discrimina a través del direccionamiento de la capa 3, es decir, la red y la dirección de subred IP. La ventaja de utilizar un switches tipo router se debe a que éste envía datos en base a la información de destino y no emite difusiones LAN como ARP.

En ésta fase del diseño se puede crear redes virtuales VLANS para disminuir los dominios de difusión, además, nos puede servir también para seguridad y escalabilidad.

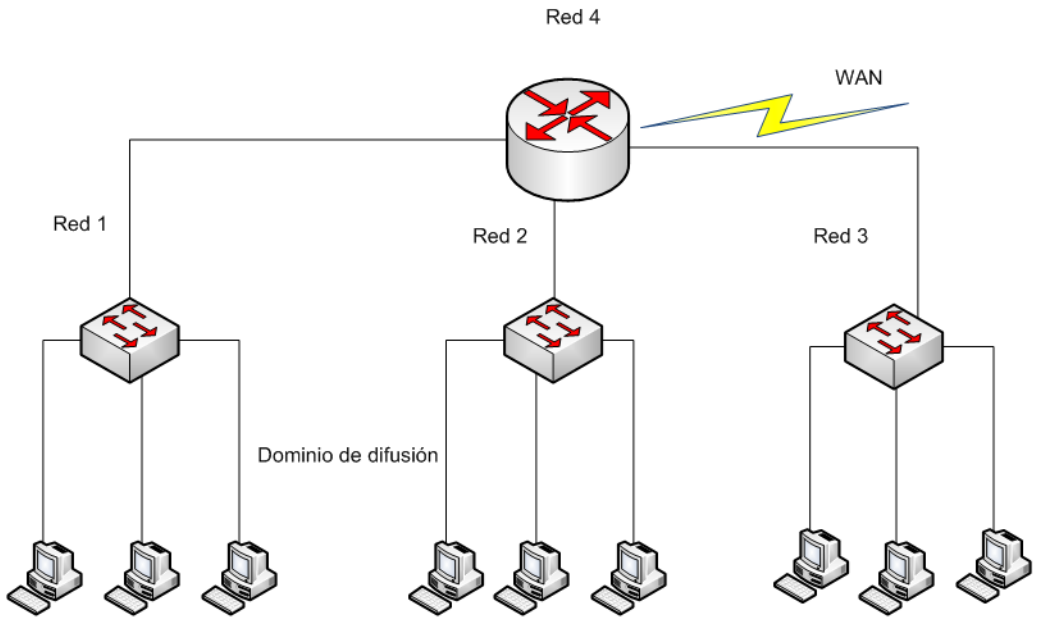


Gráfico 4. 12 *Diagrama capa 3.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Con la implementación de redes virtuales se puede minimizar los dominios de difusión, debido a que, la conmutación que realiza el router se la hace en base a las direcciones de destino, evitando así las excesivas difusiones ARP.

Para el caso en cuestión (Corte Constitucional) proponemos VLAN's asociadas por puerto físico.

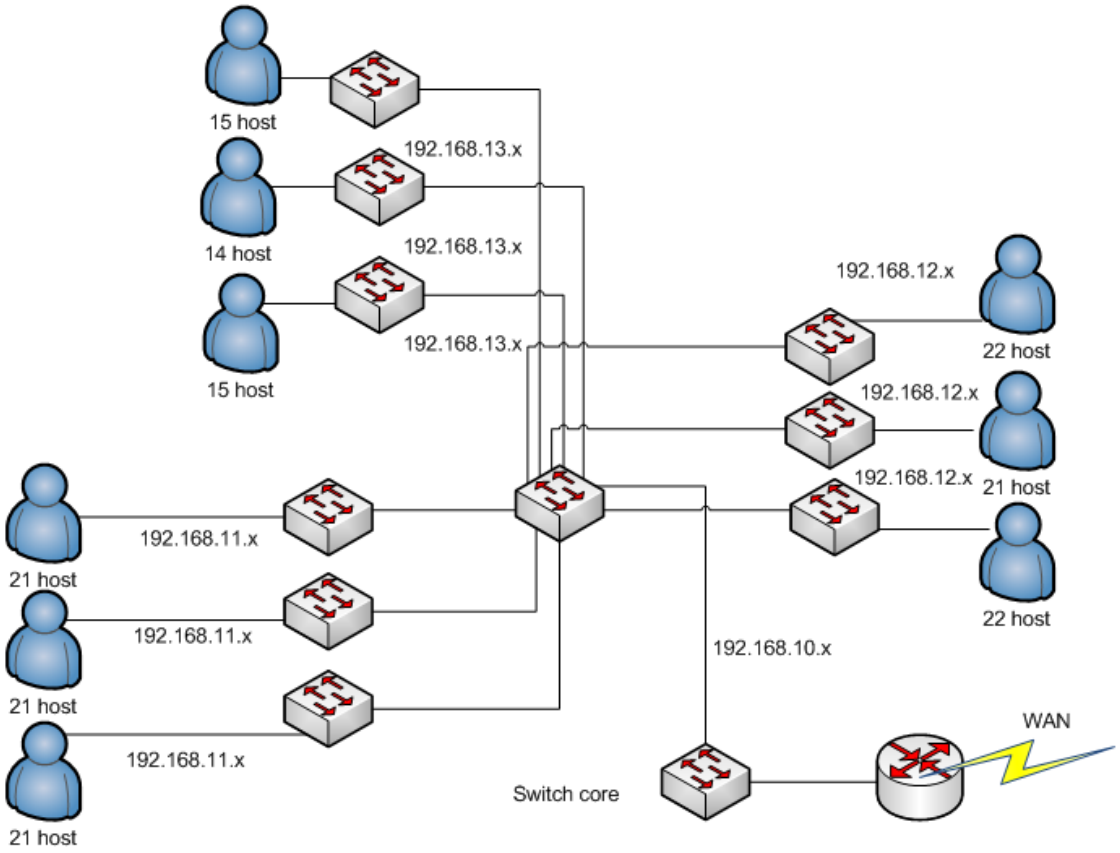


Gráfico 4. 13 *Diagrama de redes CC.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Las redes virtuales que se relacionan con un puerto específico del switch se denominan VLAN estáticas. Cuando un nuevo host necesita conectividad el administrador debe asignar el puerto y la VLAN asociada a este manualmente.

En la Corte Constitucional los usuarios utilizan recursos indistintamente del departamento en el que se encuentren, es decir, el mayor tráfico se registra desde los

servidores hacia los clientes. Por lo mencionado anteriormente, utilizaremos VLAN geográficas lo que implica que para establecerse la comunicación, necesariamente se debe pasar por un router lo que permite rutas perfectamente identificadas, lo que, facilita la administración.

Con la creación de VLAN se facilita la seguridad dentro de una red porque las difusiones se restringen a la VLAN donde se generan sin salir de ella.

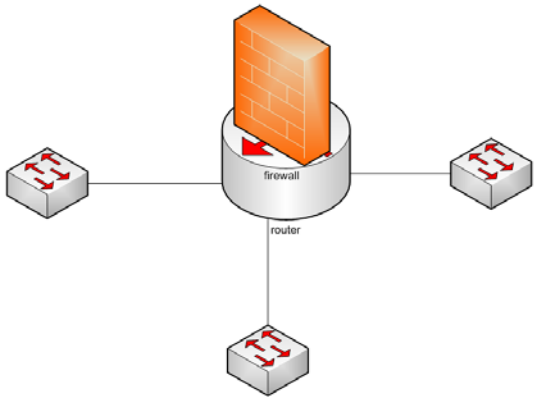


Gráfico 4. 14 *Router y seguridad.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Otra de las ventajas de la implementación de redes virtuales es limitar el número de usuarios, control sobre los nuevos usuarios (se les debe asignar una red previa conectividad).

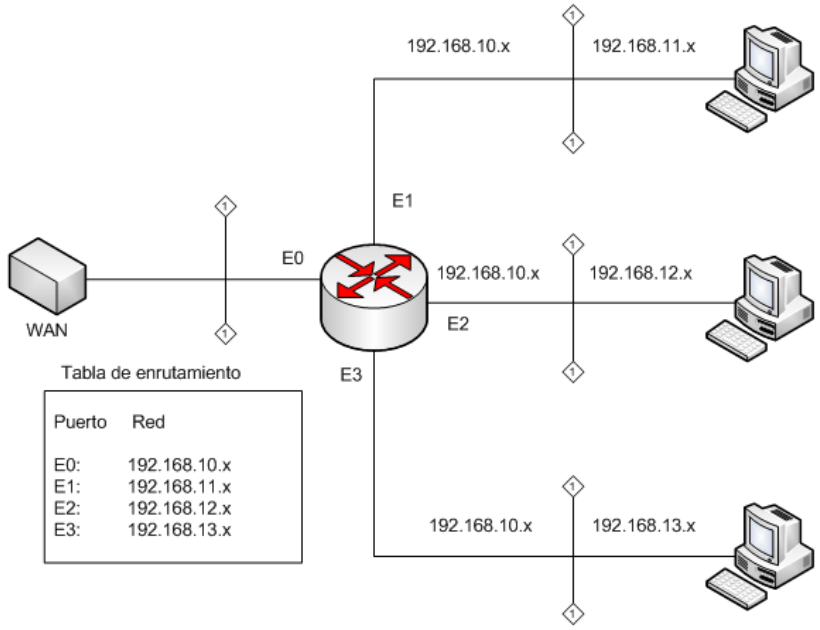


Gráfico 4. 15 *Router y direccionamiento lógico IP.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Se debe documentar el esquema de direccionamiento para identificar cada uno de los equipos en la infraestructura de red.

En la Corte Constitucional nos guiaremos por la siguiente tabla:

Dirección Lógica	Dispositivos de red físicos
192.168.10.0 – 192.168.10.20	Switches LAN
192.168.10.21 – 192.168.10.30	Servidores LAN
192.168.11.0 – 192.168.11.255	VLAN1
192.168.12.0 – 192.168.12.255	VLAN2
192.168.13.0 – 192.168.13.255	VLAN3

Tabla 4. 9 Direcciones IP oficina matriz.

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

E1 192.168.11.0

UNIDAD	# HOST	RANGO IP 192.168.11.X	ETIQUETADO
Archivo	3	192.168.11.31 – 192.168.11.33	D31 – D33
Registro Oficial	3	192.168.11.34 – 192.168.11.36	D34 – D36
Documentación	3	192.168.11.37 – 192.168.11.39	D37 – D39
Biblioteca	3	192.168.11.40 – 192.168.11.42	D40 – D42
Comunicación	7	192.168.11.43 – 192.168.11.49	D43 – D49
Sistemas	7	192.168.11.50 – 192.168.11.56	D50 – D56
Asesoría Jurídica	8	192.168.11.57 – 192.168.11.64	D57 – D64
Dir. Administrativa	7	192.168.11.65 – 192.168.11.71	D65 – D71
RRHH.	4	192.168.11.72 – 192.168.11.75	D72 – D75
Adquisiciones	3	192.168.11.76 – 192.168.11.78	D76 – D78
Almacén	2	192.168.11.79 – 192.168.11.80	D79 – D80
Contabilidad	5	192.168.11.81 – 192.168.11.85	D81 – D85
Tesorería	6	192.168.11.86 – 192.168.11.91	D86 – D91
Piso 4	8	192.168.11.92 – 192.168.11.99	D92 – D99
adicionales	5	192.168.11.100 – 192.168.11.104	D100 – D104
Total - adicionales	65		

Tabla 4. 10 Direcciones IP oficina matriz E1.

E2 192.168.12.0

UNIDAD	# HOST	RANGO IP 192.168.2.X	ETIQUETADO
P5 sala 1	4	192.168.12.106 – 192.168.12.109	D106 – D109
Dra. Ruth Seni	2	192.168.12.110 – 192.168.12.111	D110 – D111
Dr. Patricio Pazmiño	2	192.168.12.112 – 192.168.12.113	D112 – D113
Dr. Luz	2	192.168.12.114 – 192.168.12.115	D114 – D115
P5 sala 2	2	192.168.12.116 – 192.168.12.117	D116 – D117
P5 sala 4	3	192.168.12.118 – 192.168.12.120	D118 – D120
P5 sala 3	4	192.168.12.121 – 192.168.12.124	D121 – D124
P6 sala 1	2	192.168.12.125 – 192.168.12.126	D125 – D126
P6 sala 2	2	192.168.12.127 – 192.168.12.128	D127 – D128
P6 sala 3	2	192.168.12.129 – 192.168.12.130	D129 – D130
P6 sala 4	4	192.168.12.131 –	D131 – D134

		192.168.12.134	
Dr. Patricio Herrera	2	192.168.12.135 – 192.168.12.136	D135 – D136
P6 sala 5	4	192.168.12.137 – 192.168.12.140	D137 – D140
P6 sala 8	2	192.168.12.141 – 192.168.12.142	D141 – D142
P6 sala 6	2	192.168.12.143 – 192.168.12.144	D143 – D144
P6 sala 7	2	192.168.12.145 – 192.168.12.146	D145 – D146
P7 sala 1	2	192.168.12.147 – 192.168.12.148	D147 – D148
P7 sala 2	4	192.168.12.149 – 192.16812.152	D149 – D152
P7 sala 3	4	192.168.12.153 – 192.168.12.156	D153 – D156
P7 sala 4	2	192.168.12.157– 192.168.12.158	D157 – D158
P7 sala 5	3	192.168.12.159 – 192.168.12.161	D159 – D161
P7 sala 6	2	192.168.12.162 – 192.168.12.163	D162 – D163
P7 sala 7	5	192.168.12.164 – 192.168.12.168	D164 – D168

Dra. Nina Pacari	2	192.168.12.169 – 192.168.12.170	D169 – D170
adicionales	10	192.168.12.171 – 192.168.12.180	D171 – D180
Total - adicionales	65		

Tabla 4. 11 Direcciones IP oficina matriz E2

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

E3 192.168.13.0

UNIDAD	HOST	RANGO IP 192.168.2.X	ETIQUETADO
Secretaría General	15	192.168.13.181 – 192.168.13.195	D181 – D195
Vicepresidencia	2	192.168.13.196 – 192.168.13.197	D196 – D197
Asesoría Presidencia	2	192.168.13.198 – 192.168.13.199	D198 – D199
Secretaría presidencia	4	192.168.13.200 – 192.168.13.203	D200 – D203
Edecán	2	192.168.13.204 – 192.168.13.205	D204 – D205
Presidencia	3	192.168.13.206 – 192.168.13.208	D206 – D208
P10 sala 1	4	192.168.13.209 –	D209 – D212

		192.168.13.212	
P10 sala 2	12	192.168.13.213 – 192.168.13.224	D213 – D224
adicionales	10	192.168.13.225 – 192.168.13.234	D225 – D234
Total	44		

Tabla 4. 12 Direcciones IP oficina matriz E3.

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

4.2.5 Diseño de la capa Núcleo

Como se indicó en los apartados anteriores, esta parte del diseño se enmarca en como proporcionar todas las funciones principales de la red, es decir, aquí se encuentran alojados todos los servicios que requieren los usuarios internos y externos.

El principal objetivo es acceder y transmitir los datos de la forma más rápida, es por esta razón, que proponemos que toda la información esté centralizada en un área específica con controles de acceso y condiciones óptimas para asegurar la entrega de la información.

Como aporte al diseño de una red óptima, proponemos la creación de un centro de procesamiento de datos (CPD) o Data Center, es decir, un espacio específico para ubicar los servidores. Además, una nueva estructura de servidores que permita un escalamiento y el acoplamiento futuro de nuevas tecnologías.

En lo que se refiere al diseño del centro de procesamiento de datos, tomaremos como base el estándar TIA – 942. En dicho documento se especifica 4 tipos de CPD según el grado de disponibilidad necesario:

1. CPD Básico: disponibilidad (99.671%).
2. CPD Componentes Redundantes: disponibilidad (99.741%).

3. CDP Mantenimiento Concurrente: disponibilidad (99.982%).
4. CDP Tolerante a Fallos: disponibilidad (99.995%).

Para el caso de estudio propondremos un CPD tipo 1, puesto que, el número de usuarios no es muy grande (menos de 500) y además, consideramos que es un punto de partida para el crecimiento futuro. Para un buen funcionamiento, necesitamos los siguientes elementos logísticos:

- Una sala de equipos independiente.
- UPS.
- Equipos y servidores montados en racks.
- Climatización.
- Control de acceso.
- Redes eléctricas independientes y exclusivas.
- Pisos, techo y paredes no combustibles.

Una funcionalidad importante del Data Center es que abastecerá un entorno virtual para los usuarios, es decir, cada uno de los funcionarios trabajará con una máquina virtual (VM).

Para la adecuación del centro de procesamiento de datos (CPD), diseñamos una arquitectura orientada al servicio, lo que se conoce como infraestructura como servicio (IaaS). Los elementos considerados son: *cálculo de recursos, almacenamiento de recursos, recursos de red y recursos de seguridad*. Es una solución multinivel, lo que permite, afinar la provisión de servicios tecnológicos de acuerdo a perfiles.

Como instrumento metodológico a la implementación de los servidores, dividiremos el estudio en capas:

- Computo virtual.- contiene sistemas unificados de computo (UCS). También, provee de acceso al entorno de red.
- Sistemas de almacenamiento de red (SAN).- soportan canal de fibra (FC), esta capa permite la conexión entre los sistemas de memoria de disco (MDS) y los UCS en la capa de acceso.
- Capa de acceso virtual.- es un camino de acceso para las máquinas virtuales (VM), políticas locales de red como calidad de servicio.

- Capa de acceso.- acceso virtual
- Agregación.- cumple la función de redundancia.
- Capa de servicio.- podemos optar por seguridad (firewall), balance de carga y alta disponibilidad.
- Frontera con la red WAN.- conectividad con internet.

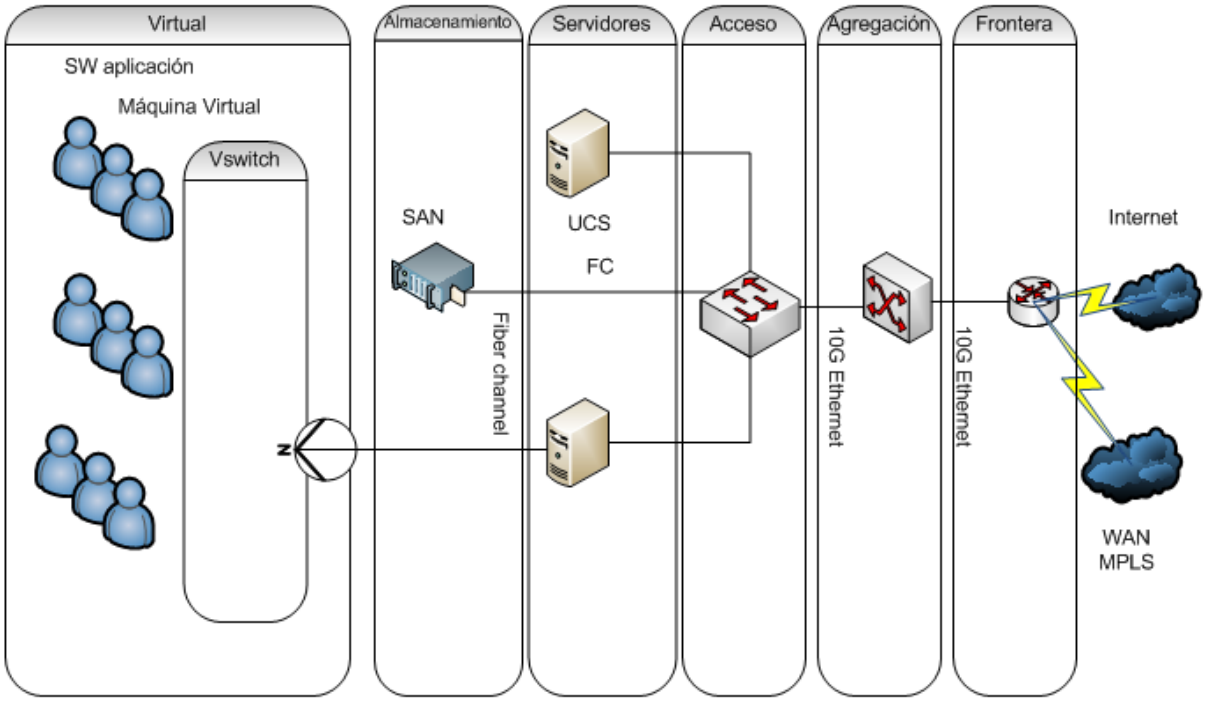


Gráfico 4. 16 *Diseño servidores LAN.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

A continuación, trataremos el tema referido al Sistema Unificado de Cómputo (UCS). Una de las capas en la topología de un centro de procesamiento de datos es el sistema unificado de cómputo, donde interactúan servidores, unidades de almacenamiento, conexiones y acceso a recursos. El equipo que permite la inter-relación con los componentes es un switch con características especiales, la principal, es que posea puertos de alta velocidad de conexión (10Gbits es óptimo), tanto para almacenamiento (fiber channel) como para la red a la que vamos a atender.

Para aprovechar el espacio, reducir el consumo y prever escalamiento, los servidores recomendados son el tipo Blade, el mismo, que posee fuentes de

alimentación redundante, se pueden montar en un rack, posee enfriamiento propio y puertos de red.

Una de las ventajas de esta arquitectura es que permite la administración de todos los componentes involucrados, a través, de una sola consola.

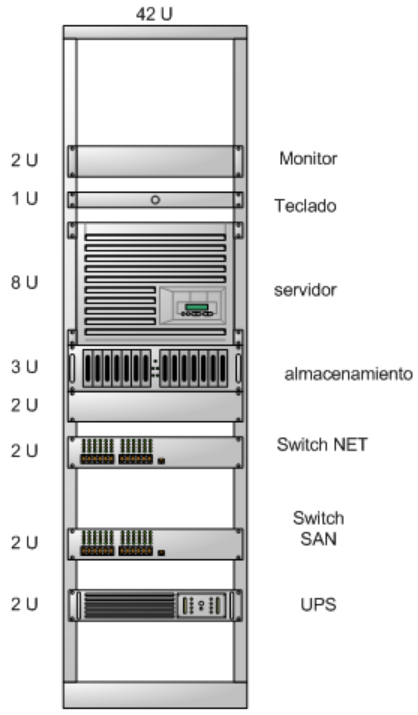


Gráfico 4. 17 *Sistema unificado de computo UCS.*

Referencia: Propuesta de diseño para Corte Constitucional Capítulo 4, Tesis Pablo Arias.

Los servidores se localizan en el sistema unificado de cómputo. En un centro de datos convencional existen varios servidores independientes cada uno con características diferentes de almacenamiento, sistema operativo y procesamiento, este hecho, implica gastos de hardware, consumo eléctrico y altos porcentajes de inversión. Por ejemplo, si, se necesita aumentar un servicio a través de un servidor, en el entorno tradicional, deberíamos adquirir un nuevo hardware con las especificaciones necesarias. Para el diseño que proponemos contaremos con una herramienta de virtualización (plataforma de virtualización) que nos permitirá optimizar recursos, dicha herramienta es VMware vSphere.

La herramienta de virtualización se caracteriza por brindar un ambiente virtualizado de ***servicios de infraestructura*** como por ejemplo, capacidad de computo, almacenamiento y red. Otro elemento agregado es el ***servicio de aplicaciones***, que permiten disponibilidad, seguridad y escalabilidad (tolerancia a fallos).

De vital importancia es ***VMware vCenter Server***, incluida en esta solución, dicho elemento provee de un punto de acceso para administrar los servidores de una empresa permitiendo monitoreo, desempeño y configuración.

Por último, VMware posee una capa de ***acceso*** para los clientes.

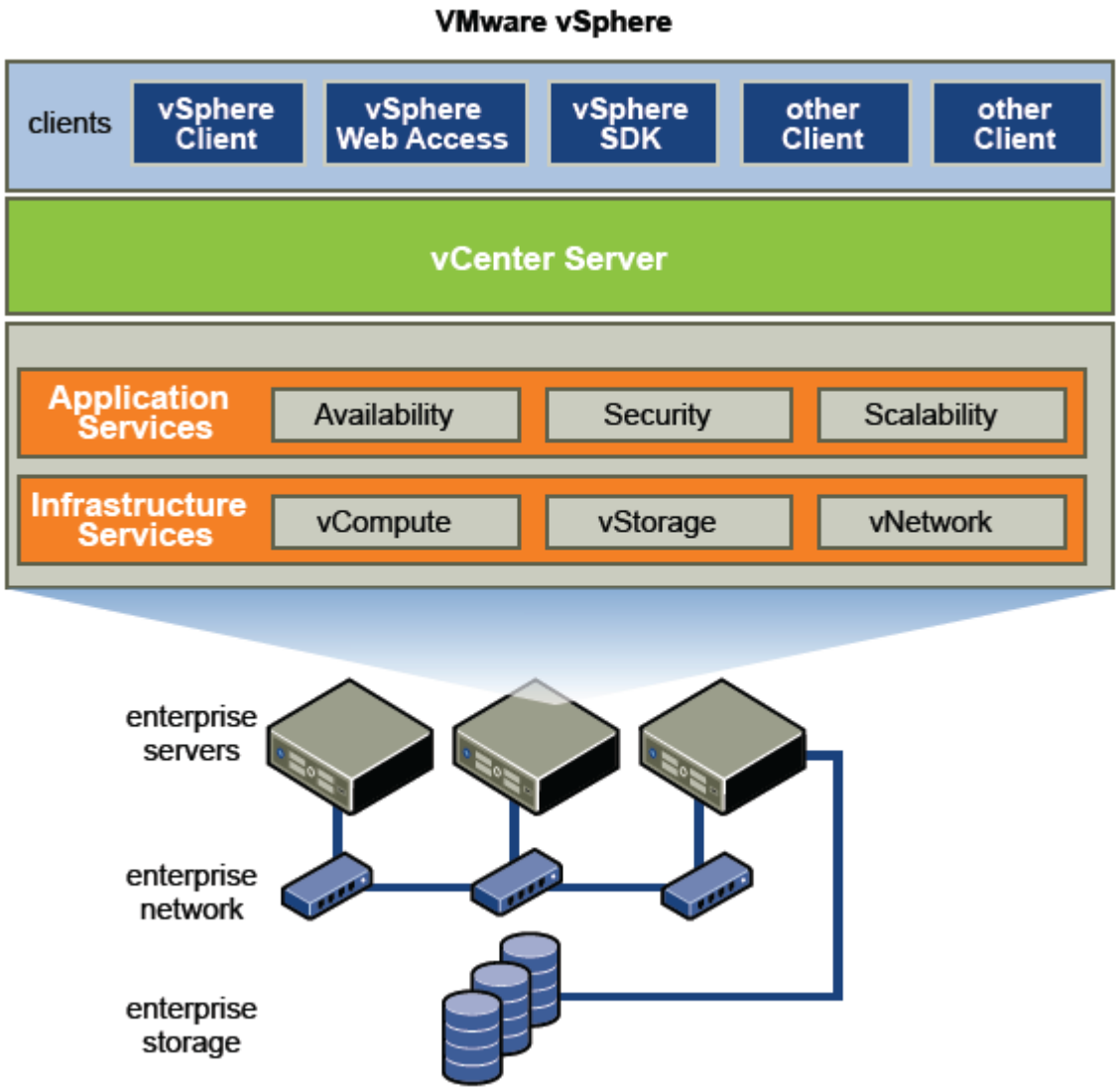


Gráfico 4. 18 *Virtualización con VMware vSphere.*

Referencia: Documentación VMware, empresa Virtual IT.

El centro de datos objeto de este trabajo, consiste en la construcción básica de bloques físicos como virtualización de servidores, matrices de almacenamiento, redes IP, un servidor de administración y los clientes de escritorio.

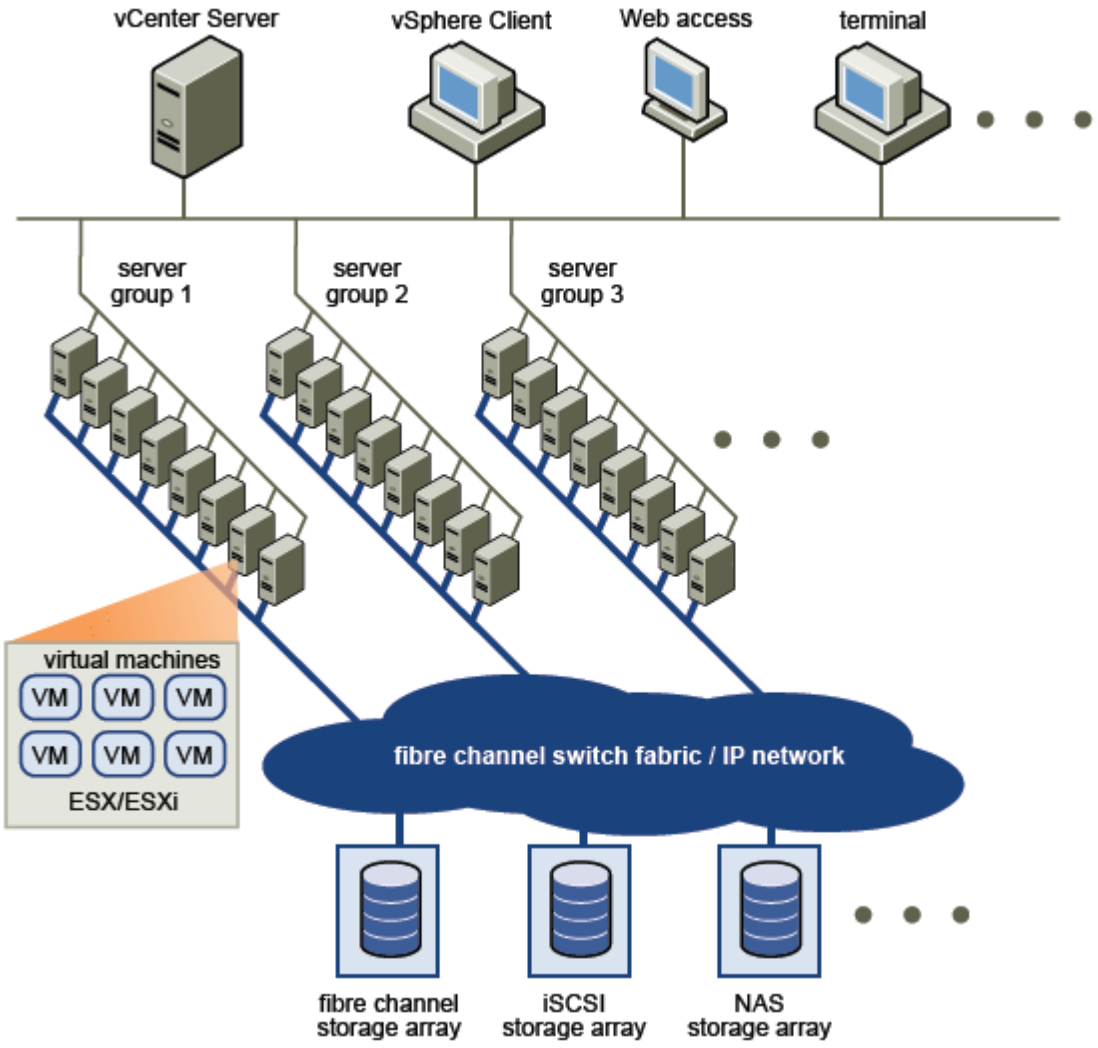


Gráfico 4. 19 *Topología física en un Data Center Virtualizado.*

Referencia: Documentación VMware, empresa Virtual IT.

Apreciando la figura describiremos cada uno de los elementos constitutivos de la topología física de un “data center”.

Servidores virtualizados. Para virtualizar un servidor se utiliza un hipervisor que es un software que se ejecuta directamente sobre el hardware y permite trabajar con distintos sistemas operativos sobre un mismo servidor. En nuestro caso sobre el hipervisor se ejecuta ESX/ESXi que proveen recursos para los elementos virtualizados. Se puede crear agrupaciones de servidores sobre una misma red con sub-sistemas de almacenamiento denominados clustering.

El tema de ***almacenamiento*** esta previsto en la solución de virtualización soporta arreglos de almacenamiento como son fiber channel SAN, iSCSI SAN, y que pueden dimensionarse adecuadamente según el requerimiento.

IP network, cada servidor puede tener múltiples interfaces de red para obtener el ancho de banda necesario.

vCenter Server es un punto para controlar el acceso a los servidores, monitorear y configurar el desempeño. Permite compartir todos los recursos con los servidores alojados. Además, existe una independencia entre servidores virtuales, es decir, si, un servidor se ve afectado, esto no repercute en la funcionalidad de los otros recursos.

Administración de clientes, permite gestionar un servidor desde cualquier sistema operativo final, acezando al centro de datos virtualizado.

4.2.6 Localización de los Host

Se mantiene la misma ubicación actual. Referirse a los gráficos 2 11 hasta 2 21.

4.2.7 Fiabilidad de la Red

El concepto de fiabilidad de una infraestructura radica en la tolerancia a posibles fallos, se trata de obtener una alternativa inmediata que permita un mayor tiempo de actividad en la red. La opción más eficaz es la *redundancia*, es decir, posibilitar a que la información que se transporta por un canal tenga otra alternativa de llegar a su destino. Sin embargo, la implementación de ésta solución acarrea dos problemas la *difusión* y la *inestabilidad de la base de datos MAC*.

Una *tormenta de difusión* se genera cuando dos o más dispositivos de capa 2, generalmente un switch, al no encontrar el destino de una trama, emite multidifusiones por todos los puertos, excepto por el puerto en el que se recibió y sí, en el mismo

segmento se localiza otro switch (para generar redundancia) y tampoco se encuentra el camino el último switch enviará también multidifusiones creando un bucle que degenera el desempeño de la red.

Otro inconveniente que se puede encontrar es la *transmisión múltiple de tramas*, esto sucede cuando una trama se envía por dos segmentos de red que convergen en un mismo dispositivo. Por último otra desventaja es que la base de información MAC (acceso al medio) puede ser inestable e imprecisa almacenando direcciones que no corresponden a las de un puerto.

Para solventar estas contrariedades cada switch posee un *Protocolo de Árbol de extensión (STP)*, que concede la gestión de enlaces de capa 2 libre de bucles *(IEEE802.1d)*. Lo que cada dispositivo hace es monitorear y detectar *lógicamente* los bucles para bloquearlos. STP nos da la elección de establecer una topología física redundante, pero no nos da alternativa de de redundancia lógica.

Cada infraestructura tiene un árbol de extensión y cuando el mismo es estable, decimos que la red converge. El método que se utiliza es, localizar un *puente raíz*, existe un puente raíz por cada puente *no-raíz*, hay un *puerto designado* por segmento, los *no designados* no se utilizan. Un puerto raíz en el más cercano al puente raíz. Al designar un puente raíz los puertos del mismo son puertos designados y están en estado de reenvío. Posteriormente, se elige un puerto raíz en los puentes no-raíz, se lo hace en base al *coste*, es decir, aquel puerto que puede acceder a un mayor ancho de banda desde un puerto no-raíz a la raíz será el designado. También, existe un puerto designado en cada segmento (menor coste). Los puertos no designados están en estado bloqueado lo que le habilita para recibir tráfico pero no enviar.

Para establecer STP usamos bucles puenteados en el nivel de capa 2 con la finalidad de mantener una continuidad en la comunicación.

En éste punto debemos conmutar a la red para que no existan bucles, lo que nos faculta una infraestructura física redundante, más no se puede configurar redundancia lógica. Los mensajes que se envían a través de los dispositivos para saber qué puertos están bloqueados se denominan BPDU (unidad de datos del protocolo de puente), contienen la ruta óptima del árbol de extensión, si ocurre una falla se re-calcula una nueva ruta.

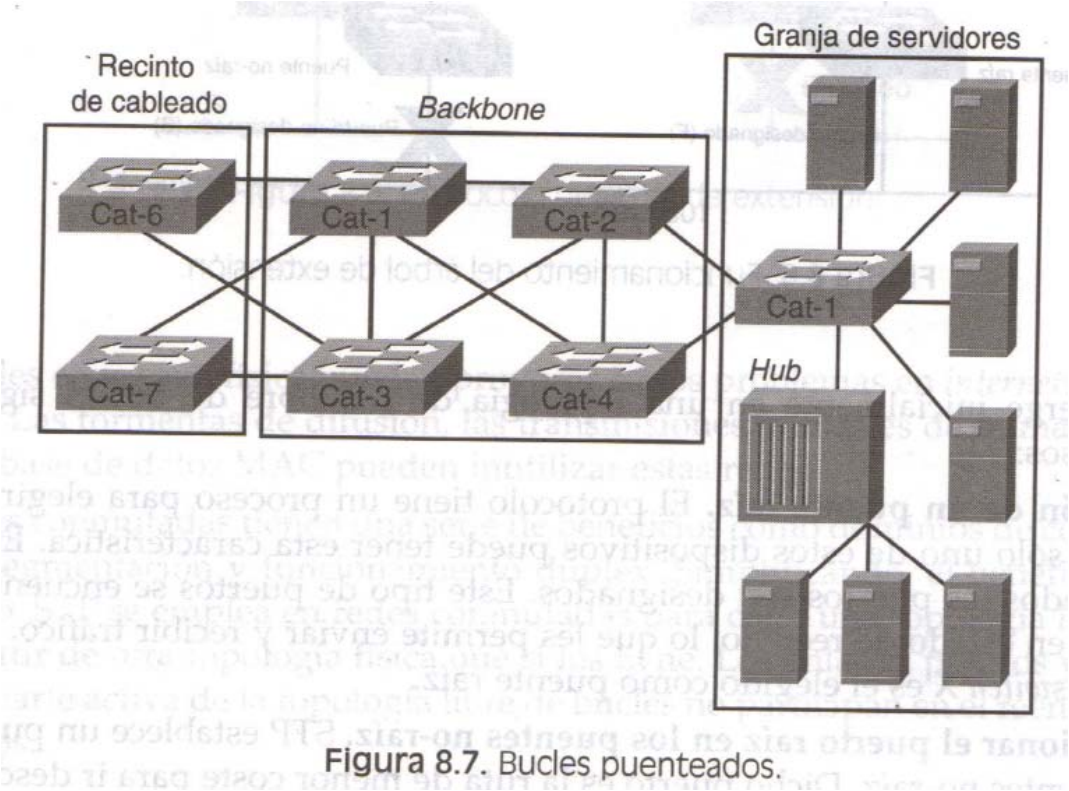


Figura 8.7. Bucles puenteados.

Gráfico 4. 20 *Redundancia física*

Referencia Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 260.

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Luego del estudio realizado en la Corte Constitucional concluimos que:

- La red local actual experimenta una degradación en la entrega de servicios debido a un diseño poco óptimo esto se evidencia al tener dominios de colisión extensos y no establecer subredes.
- Como se especifica en el capítulo 4, establecer VLAN mejora el rendimiento de la red acortando el dominio de colisión y difusión.
- Con la configuración actual no se permite una escalabilidad superior al 3%, esto se evidencia con la ausencia de puertos en los dispositivos.
- La seguridad ante posibles contingencias es nula, es decir, no existe un plan ante eventualidades.
- Es importante establecer un mecanismo de gestión de riesgos como se expone en el capítulo 3 relacionado con la seguridad.
- Se puede mejorar el desempeño de la red segmentando la red con un apropiado diseño lógico.
- Las condiciones actuales del cuarto de servidores no están acorde con los estándares de la industria.
- Se debe hacer un nuevo diseño físico y lógico de la red local.
- Los parámetros observados no cumplen con las especificaciones establecidas por la norma TIA/EIA 569 –A.
- También, la temperatura, humedad e iluminación no están acordes.
- Carecen de un data center adecuado.
- El procesamiento de peticiones a los servidores es del 5 – 10 % razón por la cual es óptimo utilizar ambientes virtualizados.
- Al utilizar distintos servidores con hardware independiente no existe ahorro de energía.
- La virtualización optimiza los recursos de hardware en los servidores.
- Con la virtualización se puede trabajar con grupos de servidores y dimensionar cada uno según sea el requerimiento.

- Implementando un entorno virtual, se puede administrar la escalabilidad de las aplicaciones y la infraestructura de servidores.
- El diseño de un centro de datos es importante para mantener seguridad de la información.
- Es necesario cambiar toda la infraestructura en la capa núcleo, debido a que, es sensible a fallas.
- La adquisición de nuevo equipo permitirá mejorar el entorno de red y por ende, mejorar el servicio.

5.2 Recomendaciones

Recomendamos lo siguiente:

- Para la administración efectiva de los recursos de las tecnologías de la información seguir tres enfoques (FCAPS, TMN, e ITIL). Estos procedimientos son estándares del manejo estratégico de todos los servicios y elementos de la infraestructura de la información reconocidos a nivel mundial.
- Identificar las características claves del rendimiento y de las tecnologías de la información.
- Diseñar arquitecturas de red basadas en los recursos IT disponibles.
- Conocer el por qué se realizan cambios en la configuración para predecirlos.
- Saber los posibles puntos de fallo, es decir, las debilidades de la red monitoreando la misma.
- En el diseño de la red incluir la red de voz.
- Llevar un registro o una bitácora de todos los fallos que presenta la infraestructura con objetivos de planeación y prevención.
- Llevar un inventario del equipo informático que incluya cables y dispositivos de repuesto disponibles.
- Etiquetar todo el cableado de red para identificación de problemas.
- Asignar ancho de banda sobre una base por puerto.
- Por cada dominio es recomendable que existan dos controladores de dominio para balance de carga y tolerancia a fallas.
- En directivas locales se puede configurar el visor de sucesos para habilitar propiedades de auditoría.
- Destinar un espacio específico para los equipos eléctricos como está en la norma 568 – A.
- Establecer un plan estratégico acorde con los objetivos de la Institución para proyectar los futuros servicios de red.
- Es aconsejable una combinación de protocolos de capa de transporte con capa IP.

- Para evitar un ataque de número de secuencia se recomienda habilitar los filtros de puntos de entrada externos evitando el ingreso de paquetes que pretendan identificarse como internos, y permitir sólo la salida de paquetes internos.
- La utilización de un firewall que haga de proxy evita ataques de sincronización (SYN) y asegura las conexiones TCP.
- Para evitar un ataque al protocolo de transferencia de noticias, se recomienda usar servidores seguros que implementen algoritmos de seguridad para autorizar la publicación de noticias en base a un ID de usuario o IP de red.

- Una forma de evitar el ataque ***spaming y bombing*** es implementar un firewall en los puntos de entrada y salida de la red corporativa a Internet, esto permitirá filtrar el correo en base a reglas o publicaciones de servidores que contienen una base de datos con los posibles correos fraudulentos.
- Si se desea implementar un servidor FTP, se recomienda usar el modo FTP pasivo para las transacciones externas, junto con un firewall de filtrado, de otra manera, se bloquearían la transferencia de datos.
- Configurar el firewall para que los host no accedan al tráfico externo, a menos, que estos inicien una conexión saliente de algún tipo.
- Colocar los servicios web, correo y FTP en una zona desmilitarizada (DMZ) de la red, en vez de la red interna.
- Verificar que se están creando copias de seguridad para todas las configuraciones.
- Crear, comparar, corregir y almacenar las copias de seguridad.
- Con la adquisición de equipos adecuados se puede mejorar la administración de los recursos.
- En el caso de planes de contingencia proyectar la movilidad de cargas virtualizadas para Data Center, es decir, planificar un Data Center de respaldo.
- Lo que se aconsejaría es que los computadores estén en un radio de menos de 130 FT para una buena recepción.

Bibliografía.

- Abad, Alfredo. Redes de área local. Madrid. McGraw-Hill. 2001.
- Ariganello, Ernesto. Las tres capas del Modelo Jerárquico de CISCO. Internet. **http://www.aprenderedes.com/?p=25** Acceso: (abril 2008).
- Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004.
- Cisco Systems, Inc. Academia de Networking. Guía del segundo año. CCNA® 3 y 4. Madrid, Pearson Educación S.A., 3ra edición, 2004.
- Comer, Douglas. Redes Globales de Información con Internet y TCP/IP. México. Prentice Hall. 3ra. Edición. 1996.
- Domínguez, Alejandra; Viruel Daisy; Romero, José y Toledo Fernando. Como Implementar una Red. Internet. **http://usuarios.lycos.es/aledomiisa/red.php** Acceso (Marzo 2008).
- Guevara, José. Diseño de la Red LAN-CAMPUS. Internet. **http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/Ingenie/Guevara_J_J/cap5.pdf** Acceso: (abril 2008).
- Gutiérrez, Abraham. Curso de Elaboración de Tesis y Actividades Académicas. Quito, Ediciones Serie Didáctica A.G., 1992.
- Gutiérrez, Abraham. Curso de Técnicas de Investigación y Metodología del Estudio. Quito, Ediciones Serie Didáctica A.G., 4ta edición, 1995.
- Hallberg, Bruce. Fundamentos de Redes. México. McGraw-Hill. 2003.
- IEEE. Standard for Information technology …. Internet. **http://www.ieee.org/portal/site** Acceso: (abril 2008)
- Izquierdo, Enrique. Investigación Científica. Loja, Imprenta Cosmos.
- López, Mariano. Teoría de las Redes Informáticas. Internet. **http://redesafull.galeon.com/** Acceso: (marzo 2008).
- Martínez, Evelio. Estándares de Telecomunicaciones. Internet. **http://www.eveliux.com/mx/index.php?option=com_content&task=view&id=9**

- Metodología para la Implementación de Redes de Área Local. Internet. **http://garg0la.tripod.com/Redes/Unidad4.html** Acceso: (marzo 2008).
- Peluffo, Luis. Diseño de Redes Convergentes Corporativas. Internet. **http://www.citel.oas.org/newsletter/2005/agosto/disenoredes_e.asp** Acceso: (marzo 2008).
- Reyes, Isidora. Método de Recolección de Datos. Internet. **http://www.monografias.com/trabajos16/recoleccion-datos/recoleccion-datos.shtml** Acceso (abril 2008).
- Rodríguez, Alfonso; Fernández, Eduardo y Piattini, Mario. Elicitación de Requisitos de Seguridad en Procesos de Negocio. Internet. **http://alarcos.inf-cr.uclm.es/pnis/articulos/pnis-07-Rodriguez-RFMP.pdf** Acceso: (mayo 2008).
- Salazar, Edison. Metodología de la Investigación. Quito, S.M. Editores, 2da edición, 2004.
- Tanenbaum Andrew, "Redes de Computadoras", México, Prentice-Hall, 3ra. Edición, 1997
- Trilithic. VOIP Settings. Internet. **http://www.trilithic.com/media/broadband_instruments/manuals/860_DSPi_Espanol/860_DSPi_Manual_Espanol_Seccion_IV_Capitulo_2_Subdivisiones_15.pdf?hGA=1** Acceso: (abril 2008).

Tabla de Gráficos.

Gráfico 1. 1 Dispositivos LAN Hub. 11
Gráfico 1. 2 Dispositivos LAN Puente. 11
Gráfico 1. 3 Gráfico Dispositivos LAN Switch. 12
Gráfico 1. 4 Dispositivos LAN NIC o Interfaz de red. 13
Gráfico 1. 5 Modelo de referencia OSI. 19
Gráfico 1. 6 Topologías físicas. 21
Gráfico 1. 7 Cableado Punto de demarcación. 26
Gráfico 1. 8 Cableado Sala de telecomunicaciones. 27
Gráfico 1. 9 Cableado vertical y horizontal. 28
Gráfico 1. 10 Cableado vertical y horizontal. 29
Gráfico 1. 11 Tecnologías WAN modem. 33
Gráfico 1. 12 Tecnologías WAN RDSI. 34
Gráfico 1. 13 Tecnologías WAN Líneas alquiladas. 35
Gráfico 1. 14 Tecnologías WAN X.25. 36
Gráfico 1. 15 Tecnologías WAN Frame Relay. 37
Gráfico 1. 16 Tecnologías WAN ATM. 38
Gráfico 1. 17 Tecnologías WAN DSL. 39
Gráfico 1. 18 Tecnologías WAN Módem por cable. 40
Gráfico 1. 19 Protocolo ICMP. 48
Gráfico 1. 20 Protocolo ICMP formato. 49
Gráfico 1. 21 Normas WAN EIA / TIA-232. 52
Gráfico 1. 22 Normas WAN EIA / TIA-449 y EIA-530. 53
Gráfico 1. 23 Normas WAN EIA-613. 53
Gráfico 1. 24 Normas WAN V.35. 54
Gráfico 1. 25 Normas WAN 54

Gráfico 2. 1 Router Cisco Serie 800. 57
Gráfico 2. 2 UPS Firmesa Powerware 9170 Plus. 57
Gráfico 2. 3 UPS 2 Referencia: Corte Constitucional. 58

Gráfico 2. 4 Central telefónica Panasonic KX-TDA200 Hybrid IP-PBX. 58
Gráfico 2. 5 Rack de distribución. 60
Gráfico 2. 6 Switch con bandeja para distribución horizontal en cada piso. 61
Gráfico 2 7 Unidad central de procesamiento característica. 62
Gráfico 2 8 Impresora característica. 63
Gráfico 2 9 Sala de servidores. 64
Gráfico 2 10 Servidor 6 anti-spam, anti-phishing 65
Gráfico 2 11 Mapa de red Planta Baja. 66
Gráfico 2 12 Mapa de red Primer piso 66
Gráfico 2 13 Mapa de red segundo piso. 67
Gráfico 2 14 Mapa de red tercer piso. 67
Gráfico 2 15 Mapa de red cuarto piso 68
Gráfico 2 16 Mapa de red quinto piso. 68
Gráfico 2 17 Mapa de red sexto piso. 69
Gráfico 2 18 Mapa de red séptimo piso 69
Gráfico 2 19 Mapa de red octavo piso. 70
Gráfico 2 20 Mapa de red noveno piso 70
Gráfico 2 21 Mapa de red décimo piso 71
Gráfico 2 22 Diagrama lógico. 72
Gráfico 2 23 Configuración Active Directory para privilegios y derechos de usuario. 78
Gráfico 2 24 Consultas de Resoluciones. 79
Gráfico 2 25 Consultas de Resoluciones. 80
Gráfico 2 26 Sorteo de Casos. 81
Gráfico 2 27 Intranet Institucional. 84
Gráfico 2 28 Analizador de protocolos. 97
Gráfico 2 29 Análisis de Flujo de Tráfico 97
Gráfico 2 30 Análisis tramas de protocolo de internet. 98
Gráfico 2 31 Análisis de aplicaciones orígen 99
Gráfico 2 32 Análisis de aplicaciones destino. 99
Gráfico 2 33 Recibo activo de MAC. 100

Gráfico 3 1 Ataques de diccionario. 111
Gráfico 3 2 Ataques DDos. Referencia 112

Gráfico 3 3 Ataque Domain spoofing. 113
Gráfico 3 4 Ataque combinado. 115
Gráfico 3 5 Ataque de número de secuencia. 117
Gráfico 3 6 Medios de transmisión. 121
Gráfico 3 7 Uso correcto de medios de transmisión. 122
Gráfico 3 8 Topología no adecuada. 123
Gráfico 3 9 Topología en estrella. 123
Gráfico 3 10 Topología lógica redundante. 124
Gráfico 3 11 Área autónoma para sala de servidores. 126
Gráfico 3 12 Lector biométrico para acceso restringido. 127
Gráfico 3 13 Límites de subred. 129
Gráfico 3 14 ACL Control de acceso. 130
Gráfico 3 15 Enrutamiento Lógico. 131
Gráfico 3 16 Implementación Firewall 133
Gráfico 3 17 Servicios a filtrar según las recomendaciones del CERT. 134
Gráfico 3 18 Modo transporte IPsec IPv4. 144
Gráfico 3 19 Modo Túnel IPsec IPv4. 145
Gráfico 3 20 Respuesta ante un incidente. 151
Gráfico 3 21 Valoración de un incidente. 152
Gráfico 3 22 Tiempo de respuesta ante un incidente. 153
Gráfico 3 23 Administración de riesgos. 155
Gráfico 3 24 Administración de riesgos. 156
Gráfico 3 25 Seguridad por niveles. 159
Gráfico 3 26 FCAPS. 161
Gráfico 3 27 Modelo de 4 capas. 162

Gráfico 4. 1 165
Gráfico 4. 2 *Capas en una red local Wireless.* 167
Gráfico 4. 3 *Capas en el desarrollo de una red local Wireless.* 168
Gráfico 4. 4 *Área de propagación y velocidad de transferencia en un AP.* 169
Gráfico 4. 5 *Modo pasivo en una tarjeta inalámbrica.* 170
Gráfico 4. 6 *Infraestructura básica inalámbrica LAN.* 171
Gráfico 4. 7 *Conexión LAN – WAN.* 172

Gráfico 4. 8 *Diagrama lógico de red LAN 3 NIVELES.* 175
Gráfico 4. 9 *Diagrama dominio de colisión.* 177
Gráfico 4. 10 *Diagrama dominio de colisión.* 179
Gráfico 4. 11 *Diagrama dominio de colisión.* 181
Gráfico 4. 12 *Diagrama capa 3.* 185
Gráfico 4. 13 *Diagrama de redes CC.* 186
Gráfico 4. 14 *Router y seguridad.* 187
Gráfico 4. 15 *Router y direccionamiento lógico IP.* 188
Gráfico 4. 16 *Diseño servidores LAN.* 195
Gráfico 4. 17 *Sistema unificado de computo UCS.* 196
Gráfico 4. 18 *Virtualización con VMware vSphere.* 197
Gráfico 4. 19 *Topología física en un Data Center Virtualizado.* 198
Gráfico 4. 20 *Redundancia física* 201

Índice de Tablas

Tabla 1 1 Parámetros de una operación Ethernet a 100 Mbps. 24
Tabla 1 2 Limitaciones de longitud y anchos de banda máximos. 42
Tabla 1 3 Servicios WAN más comunes y el ancho de banda asociado a cada uno. 43

Tabla 2 1 Servidores en la sala de equipos. 64
Tabla 2 2 Puertos habilitados en el segundo servidor. 73
Tabla 2 3 Puertos habilitados en el tercer servidor. 74
Tabla 2 4 Rango de IP’s utilizados. 88
Tabla 2 5 Encuesta de los recursos utilizados por los usuarios internos. 90
Tabla 2 6 Resultados encuesta del estado de los equipos informáticos. 90
Tabla 2 7 Resultados encuesta sobre el servicio de Internet. 91
Tabla 2 8 Resultados de encuesta interacción entre unidades. 92
Tabla 2 9 Resumen del uso de aplicaciones. 96
Tabla 2 10 Distribución de las Unidades Administrativas por pisos 101
Tabla 2 11 Canales de voz. 108

Tabla 3 1 Combinaciones y longitud de clave. 137

Tabla 4. 1 Direccionamiento WAN 166
Tabla 4. 2 Direccionamiento LAN - Sucursales 166
Tabla 4. 3 Usuarios IDF1 176
Tabla 4. 4 Usuarios IDF2 178
Tabla 4. 5 Usuarios IDF3 180
Tabla 4. 6SWITCHES Y PUERTOS EN EL IDF1. 183
Tabla 4. 7 Switches y Etiquetado IDF2. 184
Tabla 4. 8 Switches en IDF3. 184
Tabla 4. 9 Direcciones IP oficina matriz. 188
Tabla 4. 10 Direcciones IP oficina matriz E1. 189
Tabla 4. 11 Direcciones IP oficina matriz E2 192
Tabla 4. 12 Direcciones IP oficina matriz E3. 193