CAPÍTULO III

3. ANÁLISIS Y DISEÑO PROPUESTO PARA LA RED LAN - WAN

3.1. DESCRIPCIÓN DE LA SITUACIÓN ACTUAL DE LA RED DE DATOS

En todas las dependencias municipales existen redes de área local, las que son utilizadas para compartir recursos de hardware, aplicaciones locales de software, además para acceder hacia las aplicaciones localizadas en servidores situados en el Data Center, en las instalaciones que funciona la Dirección Metropolitana de Informática (Centro Histórico de Quito).

En la siguiente tabla, se resumen los datos referentes a la situación actual de todas las redes de área local en las diferentes dependencias municipales.

Entidades Municipales	**Cableado Estructurado**	
	SI	**NO**
Adm. Zona Norte		x
Adm. Zona Sur		x
Adm. Zona Valle de los Chillos	x	
Adm. Zona Valle de Tumbaco	x	
Adm. Zona La Delicia	x	
Direc. M. Administrativa	x	
Direc. M de RRHH	x	
Direc. M. Financiera		x

Direc. M. de Informática	x	
Adm. Zona Centro	x	
Direc. M. de Territorio y Vivienda	x	
Direc. M. de Medio Ambiente	x	
Direc. M. de Avalúos y Catastros	x	
SRIM	x	
Direc. M. de Desarrollo Humano	x	
Administración General	x	
Admin. Zona Quitumbe	x	
Alcaldía	x	
Direc. M. de Comercialización	x	
Recaudaciones	x	
Comité de Fiestas	x	
Comunicación Social, Dialogo	x	
Procuraduría	x	
Concejales	x	
Patronato Zona Centro	x	
Patronato Zona Norte	x	x
EMASEO	x	
Fonsal	x	
COSPE	x	

Tabla 3.1: Situación Actual de las Redes

Esta información se obtuvo al realizar encuestas[2] a cada una de las personas encargadas de la administración del área informática, además se realizó una verificación mediante la observación directa y la ayuda de software especializado.

[2] Ver Anexo: Modelo y Resultado de las Encuestas

Las redes de área local que tiene el Municipio del Distrito Metropolitano de Quito son de topología física en estrella y en estrella extendida, en ciertos segmentos trabajan como redes tipo bus a nivel lógico (presencia de hubs). Se tratan de redes que a nivel de capas inferiores está implementado Ethernet de 10 Mbps o 100 Mbps, sobre las cuales están implementados servicios de la pila de protocolos TCP/IP.

3.1.1. Descripción Física de la Red de Datos

Dentro de la descripción física de la red de área local del Municipio del Distrito Metropolitano de Quito se debe considerar la parte pasiva y la parte activa.

3.1.1.1 Parte Pasiva

En la mayoría de dependencias municipales las redes LAN no cuentan con cableado estructurado, lo único con lo que disponen en el mejor de los casos es con cableados ordenados, los cables de datos son enrutados sin las debidas protecciones; pocas dependencias tienen un cableado estructurado (detalle se puede observar en la Tabla 3.1), es decir, la mayoría de redes LAN no cumplen con las normas del sistema de cableado estructurado.

Se observa que en una gran parte de dependencias municipales se tiene acceso directo hacia los closets de telecomunicaciones, además no existe etiquetación en los elementos, tampoco cuentan con la documentación

necesaria para una correcta administración del sistema de cableado, actualmente la administración del sistema de cableado depende de la memoria del administrador de sistemas de la dependencia municipal.

En las dependencias municipales que disponen de sistemas de cableado estructurados se han realizado cambios, movimientos, aumento de áreas de trabajo, sin tomar la precaución de arreglar de manera adecuada todos los cables y elementos, ni tampoco documentar estas modificaciones, por lo que podemos deducir que no se ha realizado mantenimiento del sistema de cableado estructurado.

Los equipos que cumplen funciones de servidores de Bases de Datos y de Comunicaciones, se encuentran ubicados en sitios en los cuales no se controla la temperatura ambiental, ni la humedad relativa, tampoco se tiene un control de acceso a los mismos, es decir no se cumplen la norma ANSI/EIA/TIA 569.[3]

En las instalaciones de las dependencias municipales no existen circuitos eléctricos para uso exclusivo de equipos de computación, peor aun sistemas eléctricos con fuentes ininterrumpibles de energía (UPS), en algunas dependencias ni siquiera se dispone de estos equipos para proteger los servidores.

3.1.1.2. Parte Activa

[3] ANSI/EIA/TIA 569 Estándar de Rutas y Espacios para Edificios Comerciales

La parte activa de la redes de área local está constituida tanto por las interfaces de red, así como los equipos concentradores de señales (Hub o Switch).

Los computadores personales tienen instaladas interfaces Ethernet de 10 o 100 Mbps de velocidad, que no tienen la capacidad de ser administrados vía protocolo SNMP, no así en el caso de las impresoras de red, routers y servidores, cuyas interfaces si son administrables con velocidades de acceso de 10, 100 o 1000 Mbps

En cuanto al diseño de las redes casi en su totalidad se tratan de redes con topología en estrella y en estrella extendida, en el centro de la estrella se encuentran switches de tipo administrables en capa 2 y capa 3 y no administrables capa 2 donde predomina la marca 3com. El crecimiento de las redes LAN en las dependencias municipales ha sido desorganizado, ya que no se ha tomado en cuenta ningún diseño modular que mejore el rendimiento de la red de datos LAN, de esta manera se puede encontrar switches administrables (mejor rendimiento) en segmentos departamentales, y el switch no administrable lo ubican como principal; con excepción de la redes LAN que son administradas directamente por la Dirección Metropolitana de Informática, en las cuales se encuentra redes bien dispuestas.

En las redes LAN de ciertas dependencias municipales, como se muestra en la Tabla 3.2, que disponen de switches administrables en los que no se ha realizado configuración alguna.

Entidades Municipales	Switch	
	Adm.	No Adm.
Adm. Zona Norte	x	
Adm. Zona Sur		x
Adm. Zona Valle de los Chillos	x	
Adm. Zona Valle de Tumbaco		x
Adm. Zona La Delicia	x	
Direc. M. Administrativa	x	
Direc. M de RRHH	x	
Direc. M. Financiera	x	
Adm. Zona Centro		
Direc. M. de Territorio y Vivienda	x	
Direc. M. de Medio Ambiente	x	x
Direc. M. de Informática	x	
Direc. M. de Avalúos y Catastros	x	
SRIM	x	
Direc. M. de Desarrollo Humano	x	
Administración General	x	
Admin. Zona Quitumbe	x	x
Alcaldía	x	x
Admin. Zona Calderón	x	x
Direc. M. de Comercialización	x	
Recaudaciones		x
Comité de Fiestas		x
Comunicación Social, Dialogo		x
Procuraduría		x
Concejales		x
Patronato Zona Centro	x	
Patronato Zona Sur		x
Patronato Zona Norte		x
EMASEO		x
Fonsal	x	

COSPE	x	

Tabla 3.2: Switches de las Entidades

Los switchs administrables, no están definidos los parámetros para su administración, como son: dirección IP, dirección de correo del administrador, restricción de manejo, ni siquiera se ha cambiado el password que viene configurado de fábrica para el usuario administrador, peor aún establecer parámetros de control de equipos y rendimiento de red, como son: VLANS, tráfico permitido, que esto a su vez trae como consecuencia que las redes sean inseguras y no tengan el rendimiento adecuado, y el usuario común lo interpreta como lentitud en el procesamiento de los servidores.

En el Switch principal 3com 7750 están definidas VLANS que protegen a las redes LAN de la Alcaldía; Concejales y conexiones provenientes de las dependencias municipales que mantienen enlace con la red de datos principal del Municipio.

3.1.2. Descripción Lógica de la Red de Datos

Dentro de la descripción lógica de la red de área local del Municipio del Distrito Metropolitano de Quito se debe considerar varios tópicos como son:

3.1.2.1. Administración de la Red de Datos

En lo relación a la Administración de Redes, la mayoría de los administradores de sistemas no utilizan ninguna herramienta para realizar monitoreo de red, recordando que este es un instrumento de ayuda para la prevención de ataques, además que los reportes que arrojan estas herramientas contribuyen a mejorar el rendimiento de la red de datos. El departamento de redes de la Dirección Metropolitana de Informática, dispone de varios paquetes que sirven para controlar las redes y verificar la seguridad en equipos o servidores, estos deben ser impartidos en todas las dependencias municipales con su respectiva capacitación.

De igual manera podemos mencionar que en las dependencias municipales, los administradores de sistemas han cumplido en mayor parte los lineamientos establecidos por la Dirección Metropolitana de Informática, en cuanto a la creación de cuentas de usuarios en servidores y en computadores personales, nombres de máquinas, direccionamiento IP. Es necesario que se realicen auditorias periódicas, a fin de corroborar que las políticas sean cumplidas en su totalidad, ya que existen casos aislados en donde se ha comprobado que los nombres de PCS no son los correctos y por la falta de seguimiento no se hacen las rectificaciones respectivas.

La mayoría del personal que administra los sistemas informáticos, tienen los conocimientos necesarios para el trabajo que demanda la mayor cantidad de tiempo, como es el servicio de Help Desk, en lo que respecta a conocimientos técnicos de redes de datos si existen diferencias entre el personal y eso se da a notar en el mejor funcionamiento y administración de

unas redes LAN sobre otras. Adicionalmente es importante señalar que en ciertas dependencias el personal técnico también cumple funciones asignadas a otros departamentos, lo que de alguna manera desvía su atención en procesos que no son su responsabilidad.

3.1.2.2. Licenciamiento

Este es un punto que más atención requiere de las autoridades del Municipio del Distrito Metropolitano de Quito, ya que únicamente el Fondo de Salvamento del Patrimonio Cultural (FONSAL) cuenta con casi todos los licenciamientos correspondientes, el resto de entidades no poseen licenciamiento, en el mejor de los casos para el Sistema Operativo de computadores personales poseen el 40% de licencias, para Microsoft Office el 20%; no disponen de licenciamiento de sistemas operativos para los servidores, ni tampoco para Autocad ni para Symantec Antivirus.

Este es un punto que aparentemente no tiene influencia directa sobre el rendimiento en la red de datos, pero en realidad constituye uno de los aspectos más relevantes desde el punto de vista de control del buen funcionamiento del computador personal y de los servidores. Es vital que el sistema operativo y los paquetes utilitarios de oficina se encuentren totalmente actualizados y parchados, de esta manera se cierran vulnerabilidades propias del software y se evitan ataques que aprovechan estas vulnerabilidades que finalmente generan un aumento significativo del tráfico en la red de datos.

3.1.2.3. Aplicaciones

Las dependencias municipales cuentan con aplicaciones de software de acceso local, y aplicaciones centralizadas que disponen en el Data Center ubicado en la Dirección Metropolitana de Informática (Centro Histórico de Quito); a continuación se detalla las aplicaciones centralizadas como son:

- **Acceso a Internet**, para brindar este servicio la Dirección Metropolitana de Informática, dispone de un enlace inalámbrico centralizado contratado con la empresa Impsat, el control de navegación está regulado en el servidor Proxy (sistema operativo Linux Centos), mediante autorización a través de la dirección IP del equipo que desea el servicio, por ello los usuarios de las dependencias municipales que requieren navegar en Internet, deben solicitar este servicio a la Dirección Metropolitana de Informática.

  A continuación se presenta un gráfico que muestra el acceso a Internet.

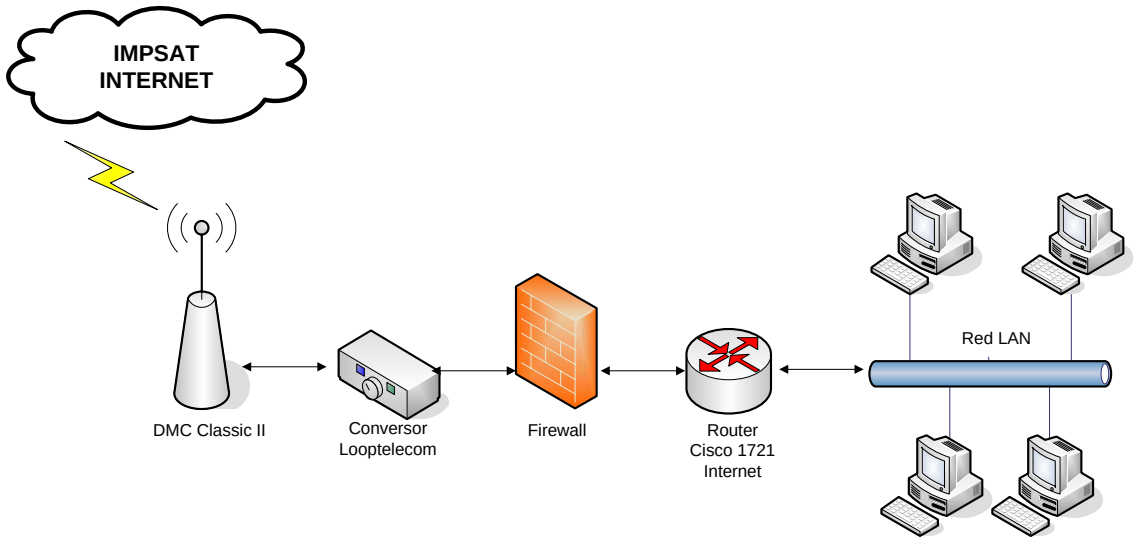


Figura 3.1: Acceso a Internet

A fin de proteger la red interna de ataques provenientes de la red externa, se tiene implementado un Firewall 3Com, en el cual adicionalmente se realiza un filtro de sitios no permitidos para su navegación, así como puertos y servicios permitidos o no.

Existen dependencias municipales que cuentan con enlaces propios para salir hacia el Internet: Patronato Centro, Patronato Norte, EMASEO, Fondo de Salvamento del Patrimonio Cultural (FONSAL), las que consideraron que el enlace centralizado no era suficiente para sus necesidades, el control de navegación es local y realizado por el administrador de sistemas.

- **Correo,** otra de las aplicaciones muy utilizadas por los usuarios es el servicio de correo electrónico que de igual manera está instalado sobre un servidor con sistema operativo Linux, ubicado en el Data Center de la Dirección Metropolitana de Informática, en este servidor está instalado y configurado el servidor de correo Lotus Notes mediante protocolo POP3, este constituye el único servidor para los usuarios de todas las dependencias municipales, en este servidor se ha incorporado el control antispam mediante negación a listas negras, la administración de este servicio está a cargo del Departamento de Redes de la Dirección Metropolitana de Informática. En cuanto al estado de este servicio es inseguro debido a que en cada uno de los usuarios no se controla el espacio del servicio de correo.

- **Aplicaciones Críticas,** las podemos dividir en aplicaciones que trabajan en ambiente cliente-servidor (SQL y Oracle), y aplicaciones centralizadas OS390, la administración de estas aplicaciones es centralizada y depende de la Dirección Metropolitana de Informática, el acceso es autorizado mediante un rango de direcciones IP previamente definidas, es decir el funcionamiento de las aplicaciones criticas se da a través de la autorización a un determinado rango de IP's para acceder a los servidores.

- **Backup,** definitivamente en las dependencias municipales no existe la política de respaldar la información tanto de usuarios como de servidores, peor aun tener respaldadas configuraciones de equipos de comunicación como un posible plan de contingencia ante un desastre informático.

3.2. ANÁLISIS DE LAS REDES LAN - WAN

Para realizar el análisis de la cantidad y del tipo de tráfico que circula en los diferentes segmentos de red LAN de las dependencias municipales, se utilizaron varios herramientas de software apropiadas, una de las que se utilizó fue el MRTG, sistema que sirve para supervisar la carga de tráfico en los enlaces de red, de igual manera para identificar el tipo de tráfico se utilizaron programas libres como el Ethereal y el Software EtherDetect, estos paquetes de software fueron instalados sobre equipos con sistemas operativos Linux y Windows.

3.2.1. Resultados de la Medición de Tráfico LAN

Observando los resultados obtenidos por estas herramientas se puede determinar que existe un excesivo tráfico de broadcast, debido a que se encuentra habilitado el protocolo Netbios, este sistema relaciona el nombre de máquina no jerárquico y la dirección IP y para su funcionamiento utiliza la difusión a todo el segmento de red, el problema se genera cuando los computadores personales buscan al servidor de nombres Netbios y al no existir este tipo de servidor, los computadores lo envían hacia todo el segmento de red mediante tráfico de broadcast, además casi en la totalidad de las redes LAN de las dependencias municipales se pueden encontrar paquetes Netbios malformados, la causa de este tipo de tráfico es que se utilizan caracteres inválidos dentro de los nombres Netbios de máquinas, o la presencia de este tipo de tramas se deba a la presencia de virus dentro de la red de datos.

A continuación se presenta un gráfico que muestra los errores de paquetes Netbios.

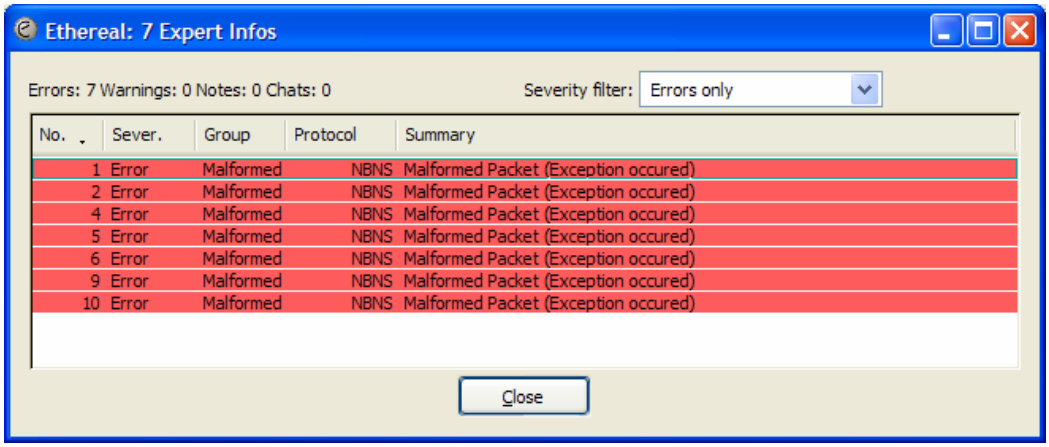


Figura 3.2: Errores de Paquetes Netbios

En ciertas redes LAN aun disponen de Hubs, lo que se evidencia con el excesivo tráfico, debido a que el principio de funcionamiento de estos sistemas son a través de la difusión a todos los puertos de paquetes que generan los dispositivos, es conveniente su reemplazo por switchs, los cuales manejan de mejor manera el trafico de la red con la configuración adecuada.

La red de datos no cuenta con herramientas anti-sniffer, además en las redes LAN y MAN circula información no cifrada, por lo que es posible capturar datos importantes como direccionamiento IP, dirección MAC, nombres de usuarios y password mediante software especializado (Sniffers), estos datos vitales pueden ser utilizados en un ataque informático.

El cliente de correo habilitado en las dependencias municipales es Microsoft Outlook y también Outlook Express, el cual para conectarse hacia cualquier servidor de correo, debe hacerlo a través de la Dirección Metropolitana de Informática, ya que aquí se encuentra centralizado el sistema Lotus Notes sobre Linux, para ello se utiliza el protocolo de llamada a procedimiento remoto (RPC), para este efecto es necesario que el puerto 139 (netbios) se encuentre abierto, sin embargo, de acuerdo al actual sistema de correo esto produce una causa más para el tráfico de difusión en las redes LAN y MAN.

3.2.2. Resultados de la Medición de Tráfico WAN

Para Interconectar las redes LAN en las diferentes Administraciones Zonales, la Dirección Metropolitana de Informática ha contratado los servicios

de dos empresas proveedoras de transmisión de datos: Andinadatos y PuntoNet, además posee enlaces propios de fibra óptica, enlaces por cable UTP y enlaces inalámbricos con equipamiento adquirido por el Ilustre Municipio de Quito, estos sistemas trabajan con la banda de frecuencias de uso libre.

Mediante herramientas de software especializado no intruso para la red (no genera tráfico), como PRTG Traffic Grapher y WANguard Network, se recopila la información producida en los enlaces durante un período de 3 días, de igual forma se emiten reportes detallados de tráfico recreacional y tráfico crítico.

Para recolectar datos de utilización y rendimiento de aplicaciones se ha instalado en la red de datos del Municipio de Quito, un computador personal que tiene instalado el software mencionado, se habilita el protocolo SNMP en los routers de cada uno de los proveedores, estos datos proveen la base del servicio, los cuales son analizados para determinar los problemas en el rendimiento de aplicaciones y además identificar que aplicaciones consumen mayor cantidad de ancho de banda.

3.2.3. Proveedor Andinadatos

Este proveedor ofrece los servicios de interconexión de sitios remotos (Figura 3.3) hacia la Dirección Metropolitana de Informática, para este efecto utiliza la infraestructura telefónica existente como enlace de última milla tanto en el lado del sitio remoto como en el caso del sitio central, sobre

esta infraestructura física tiene implementado un enlace ATM sobre tecnología ADSL.

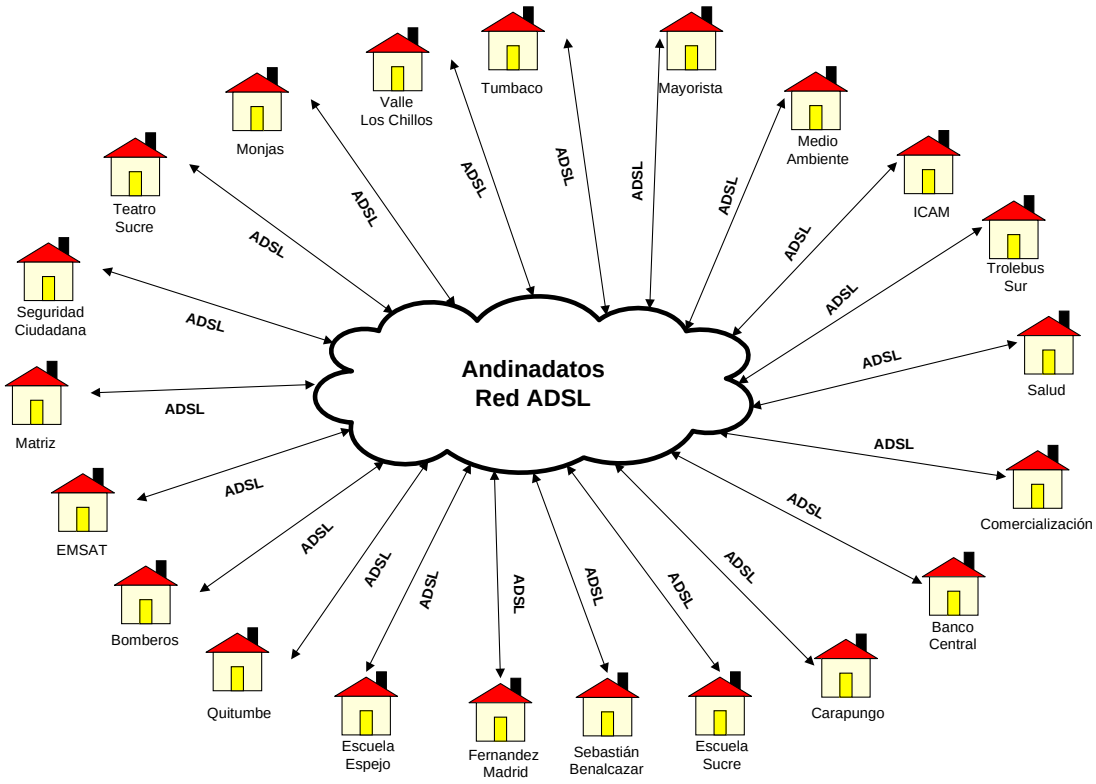


Figura 3.3: Proveedor de Andinadatos

3.2.3.1. Resultados de la Medición de Tráfico

El objetivo de este análisis es identificar las aplicaciones más utilizadas, determinar el ancho de banda usado por cada una de ellas, ya que generalmente la mayor cantidad de ancho de banda está dividido entre estas aplicaciones.

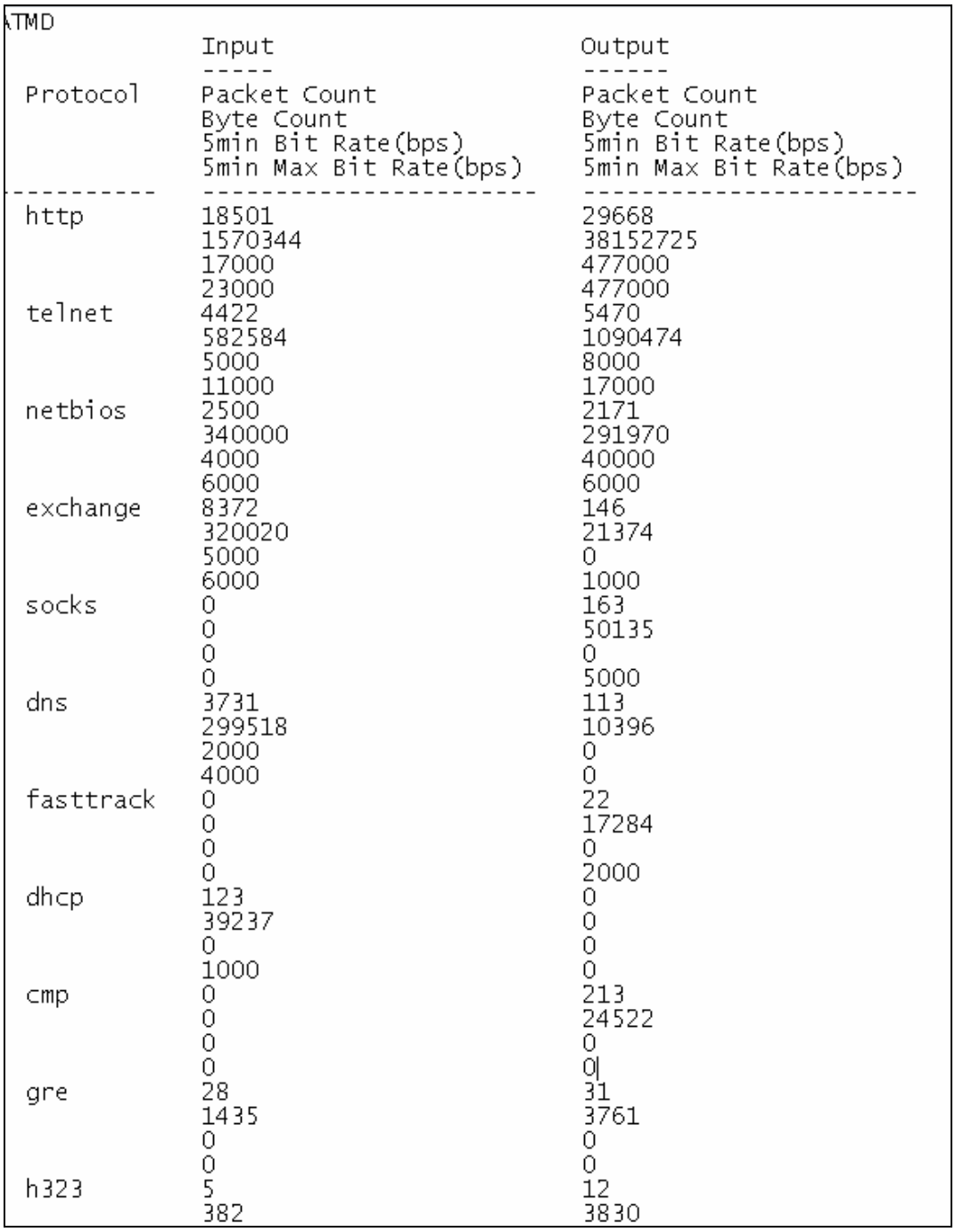
Además por los datos recopilados durante un intervalo de tiempo de 3 días, se puede determinar el porcentaje que utiliza cada aplicación del total de

ancho de banda, este análisis se lo realizará tanto para tráfico de entrada como de salida.

3.2.3.2. Tráfico de Entrada a la Red de Datos del Municipio

Este tráfico es el que ingresa en la red de datos del Municipio de Quito, este proviene de los sitios remotos, en la figura 3.4 se pueden identificar diferentes tipos de tráfico de red que circulan a través del router que conecta a varias dependencias municipales con la red del Municipio a través del proveedor Andinadatos. El tráfico principalmente corresponde a tramas del protocolo Netbios correspondiente a los puertos: 137,138,139, Microsoft-ds que comparten archivos en Windows 2000(445), Exchange; y representan un consumo del 72% del ancho de banda disponible, adicionalmente tenemos el tráfico de red de la aplicación crítica la cual reside en el servidor IBM 390, esta comunicación se la realiza a través de un software emulador de terminales 390 que trabaja en el puerto 23, por ello la herramienta MRTG la reconoce como tráfico de la aplicación telnet.

A continuación se presenta un gráfico que muestra el Tráfico de Aplicaciones Red de Entrada.



```
ATMD
                Input                       Output
                -----                       ------
 Protocol       Packet Count                Packet Count
                Byte Count                  Byte Count
                5min Bit Rate(bps)          5min Bit Rate(bps)
                5min Max Bit Rate(bps)      5min Max Bit Rate(bps)
-----------     --------------------------  --------------------------
 http           18501                       29668
                1570344                     38152725
                17000                       477000
                23000                       477000
 telnet         4422                        5470
                582584                      1090474
                5000                        8000
                11000                       17000
 netbios        2500                        2171
                340000                      291970
                4000                        40000
                6000                        6000
 exchange       8372                        146
                320020                      21374
                5000                        0
                6000                        1000
 socks          0                           163
                0                           50135
                0                           0
                0                           5000
 dns            3731                        113
                299518                      10396
                2000                        0
                4000                        0
 fasttrack      0                           22
                0                           17284
                0                           0
                0                           2000
 dhcp           123                         0
                39237                       0
                0                           0
                1000                        0
 cmp            0                           213
                0                           24522
                0                           0
                0                           0
 gre            28                          31
                1435                        3761
                0                           0
                0                           0
 h323           5                           12
                382                         3830
```

Figura 3.4: Tráfico de Aplicaciones Red de Entrada

También se puede apreciar que existe un alto consumo de tráfico de Internet representado principamente por el HTTP y MSN-Messenger, este tipo de aplicaciones tienen un mayor uso que las consideradas aplicaciones críticas

las cuales utilizan el puerto 23, estas son identificadas por la herramienta MRTG como aplicación telnet.

El router es un dispositivo que básicamente se encarga de encaminar los paquetes que ingresan por una interfaz de entrada, hacia la interfaz de salida requerida, también es utilizado para separar segmentos de red, por lo que generalmente se cierran puertos que no sirven para cumplir este objetivo, pero en este router existen puertos TCP/UDP abiertos que normalmente deben mantenerse cerrados, como son:

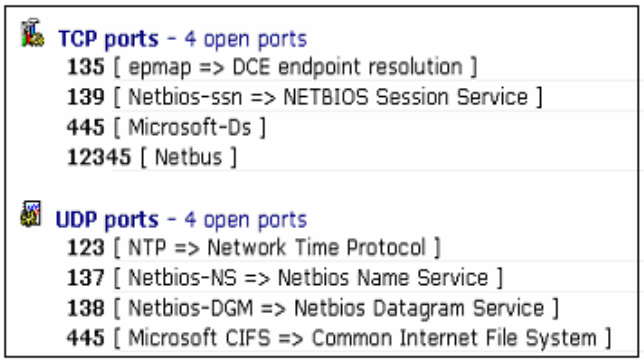


Figura 3.5: Puertos Abiertos

Como se puede apreciar existe tráfico en los puertos 445 Microsoft-ds, el cual comparte archivos en Windows 2000 y el puerto 137 Netbios que atraviesan el router, este tráfico necesita ser revisado por la Dirección Metropolitana de Informática, a fin de determinar la legalidad del mismo, es decir, establecer si alguna aplicación crítica la utiliza.

A continuación se presenta un reporte de tráfico de paquetes de entrada que circulan a través del router, en este se detallan las direcciones IP origen y destino involucrados, en esta muestra podemos observar que existen

retransmisiones constantes de paquetes de 48 bytes, paquetes que causan que la red de datos no mantenga niveles de eficiencia adecuados, este tipo de retransmisiones son respuesta a peticiones de envío de cookies o información requerida por servidores web del Internet.

Source	Destination	Packets	Bytes
172.20.8.117	31.119.44.147	1	48
172.20.8.117	212.25.152.130	1	48
172.20.8.117	31.119.44.146	1	48
172.20.8.117	212.25.152.131	1	48
172.19.12.15	172.20.24.8	77	7983
172.20.8.117	31.119.44.149	1	48
172.20.8.117	212.25.152.132	1	48
172.20.8.117	31.119.44.148	1	48
172.20.31.26	172.20.24.8	97	7566
172.20.8.117	212.25.152.133	1	48
172.20.8.117	31.119.44.151	1	48
172.20.8.117	212.25.152.134	1	48
172.20.7.1	172.20.24.8	105	12716
172.20.31.27	172.20.24.3	1514	219036
172.20.7.187	172.20.11.121	82093	18528156
172.20.7.153	172.20.24.93	7856	763028
172.20.7.192	172.20.24.3	34366	6052138
172.20.7.200	172.20.24.8	10083	786834
172.20.7.162	172.20.24.93	11926	1387435
172.20.7.163	172.20.24.93	4304	407504
172.20.19.71	10.0.0.1	1266	96216
172.20.7.165	172.20.24.93	24608	2223834

Figura 3.6: Tráfico de Paquetes

En este segmento de acceso de redes remotas, el dispositivo que realiza funciones de encaminamiento es el Router, marca Cisco, este dispositivo llega a tener un procesamiento de hasta un 90%, cabe recordar que el máximo nivel de utilización de recursos permitido de cualquier dispositivo es del 75%, sobre ese nivel es necesario ampliar recursos de hardware, pero en este caso este efecto es causado por las constantes retransmisiones de paquetes de 48 bytes y el exceso de tráfico generado por las máquinas.

3.2.3.3. Tráfico de Salida de la Red de Datos del Municipio

En cuanto al tráfico que se envía desde la matriz hacia los sitios remotos, la figura 3.7 muestra la existencia de un trafico de salida que ocupa el 80 % del canal, este tráfico es mayor que el tráfico de Entrada a la red del Municipio, lo cual es comprensible debido básicamente a la descarga de información proveniente del Internet y de los sistemas centrales ubicados en la Dirección Metropolitana de Informática, a continuación se presenta un reporte detallado en donde se puede identificar las horas de mayor afluencia de tráfico tanto entrante como saliente.

Graph | Table: 24 Hours | Table: 30 Days | Table: 365 Days

Table: Port 1 (ATM0) on ROUTER PRUEBA (172.20.24.239) (24 Hours, 5 min A

	Port 1 (ATM0) on ROUTER PRUEBA (172.20.24.239)				
	Bandwidth Traffic IN		Bandwidth Traffic OUT		
	kbyte	kbit/second	kbyte	kbit/second	kb
21/12/2006 8:45 - 8:50	451,469	20,657	418,930	19,168	8
21/12/2006 8:40 - 8:45	796,153	21,750	1.862,932	50,893	2.6
21/12/2006 8:35 - 8:40	880,423	24,052	1.293,309	35,331	2.1
21/12/2006 8:30 - 8:35	811,478	22,168	730,493	19,956	1.5
21/12/2006 8:25 - 8:30	719,261	19,649	637,654	17,420	1.3
21/12/2006 8:20 - 8:25	1.034,232	28,254	1.076,877	29,419	2.1
21/12/2006 8:15 - 8:20	1.050,592	28,701	1.918,087	52,399	2.9
21/12/2006 8:10 - 8:15	959,817	26,222	573,731	15,674	1.5
21/12/2006 8:05 - 8:10	754,663	20,616	428,453	11,705	1.1
21/12/2006 8:00 - 8:05	821,646	22,446	1.025,834	28,024	1.8
21/12/2006 7:55 - 8:00	256,632	7,011	1.359,743	37,146	1.6
21/12/2006 7:50 - 7:55	69,371	1,895	486,623	13,294	5
21/12/2006 7:45 - 7:50	117,465	3,209	945,766	25,837	1.0
21/12/2006 7:40 - 7:45	118,111	3,227	1.454,389	39,732	1.5
21/12/2006 7:35 - 7:40	16,843	0,460	129,230	3,530	1
21/12/2006 7:30 - 7:35	10,756	0,294	2,311	0,063	
21/12/2006 7:25 - 7:30	71,478	1,953	622,515	17,006	6
21/12/2006 7:20 - 7:25	68,009	1,858	191,694	5,237	2
21/12/2006 7:15 - 7:20	6,715	0,183	0,626	0,017	
21/12/2006 7:10 - 7:15	14,027	0,383	6,220	0,170	
21/12/2006 7:05 - 7:10	14,339	0,392	0,815	0,022	
21/12/2006 7:00 - 7:05	77,332	2,113	63,968	1,748	1
21/12/2006 6:55 - 7:00	7,297	0,199	2,396	0,065	

Figura 3.7: Tráfico de Salida de la Red de Datos del Municipio

3.2.3.4. Eficiencia del Segmento de Red Entrante

El siguiente parámetro a ser analizado es el uso del ancho de banda en comparación con el CIR[4] y la velocidad del puerto WAN. Aquí el número de retransmisiones nos da una idea de la pérdida de paquetes en la red, los cuales pueden ser un indicativo de congestión o sobredemanda. En términos generales esto es Eficiencia de Red y representa el porcentaje del tráfico efectivamente transferido por el enlace, descontando las retransmisiones de paquetes.

En la figura 3.8 se puede apreciar que existe un alto porcentaje de retransmisión de paquetes, lo cual muestra que la red no tiene una eficiencia aceptable. Además esta deficiencia es más notoria en horarios fuera de oficina, entre las 22:h00 y 6:h00, en este lapso de tiempo existen aplicaciones que están generando tráfico y que influye en la ineficiencia de la red y de acuerdo al reporte de utilización representado en la figura 3.8 corresponde al puerto 445 Microsoft-ds, el cual comparte archivos en Windows 2000; esta aplicación es responsable de que el 20% de los paquetes estén siendo retransmitidos. Esto refleja claramente la presencia de un Virus que ataca a todo el segmento de red.

[4] Commited Information Rate: Indica el ancho de banda mínimo garantizado.

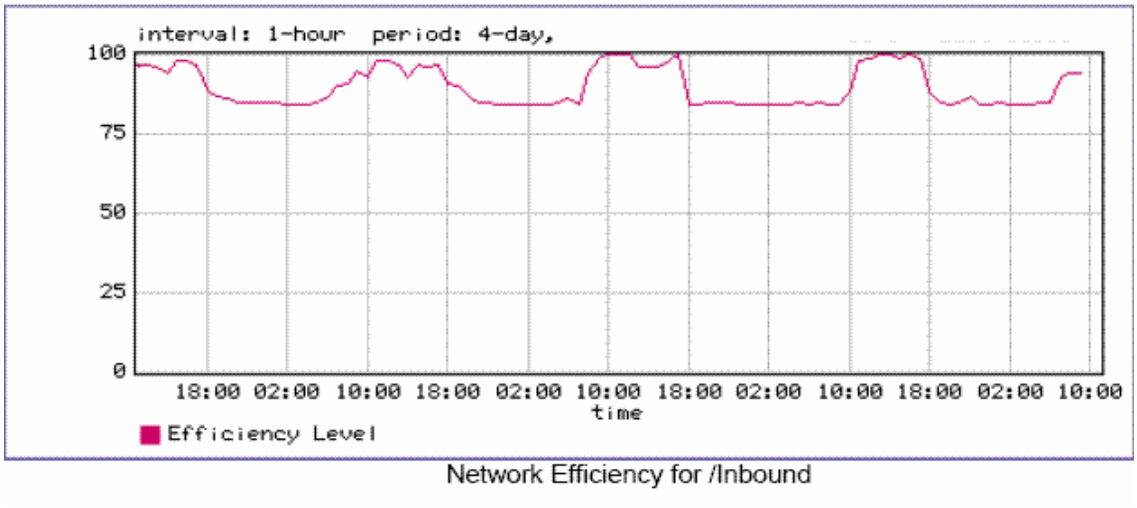


Figura 3.8: Eficiencia de la Red

3.2.4. Proveedor PuntoNet

Para cubrir el enlace de todos los sitios remotos encargados al proveedor PuntoNet, se dispone de una red multipunto IP, por lo que el análisis se realizará sobre la interfaz Ethernet del router, esta red puede ser representada de la siguiente manera:

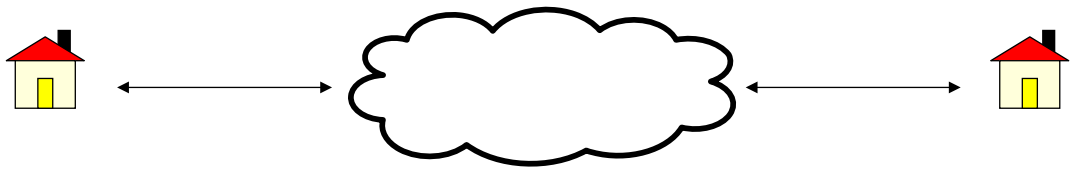


Figura 3.9: Diagrama Lógico del Proveedor PuntoNet

La vista física de la red de datos que maneja el proveedor PuntoNet se la puede representar de la siguiente forma:

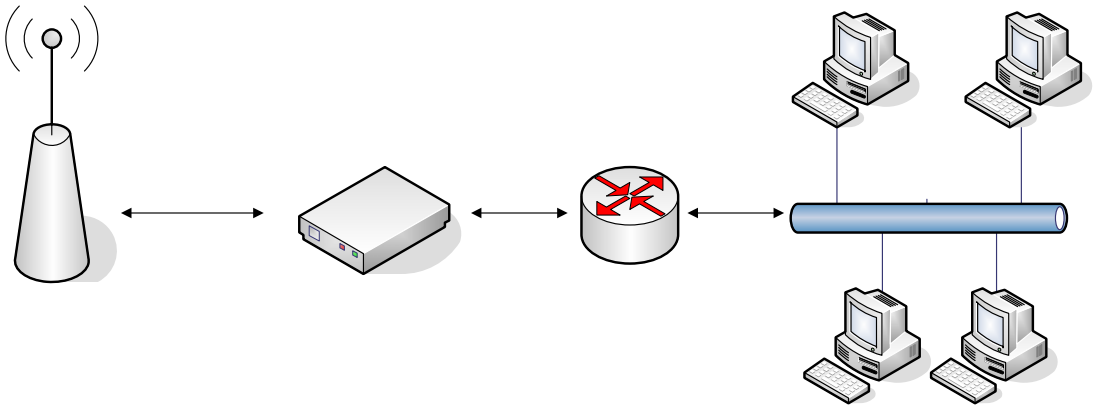


Figura 3.10: Diagrama Físico del Proveedor PuntoNet

El dispositivo Cisco 871 que utiliza PuntoNet para interconectar las redes remotas con la red principal del Municipio, están equipadas con dos interfaces Ethernet cuyas direcciones IP son:

Antena IP Multipunto Wipll Marconi SPR Antena: 0.3 mts

Modem IP Multipunto

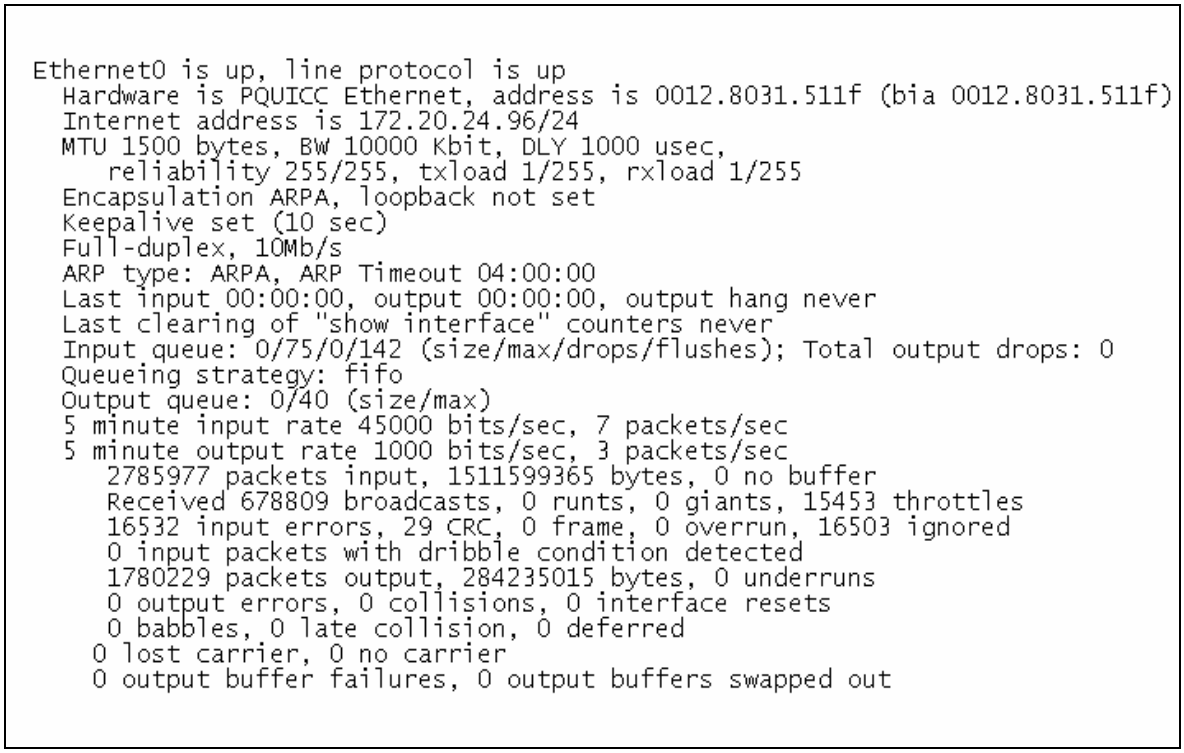
Ethernet0	172.20.24.96
Ethernet1	172.16.12.10

En la red que mantiene PuntoNet al tratarse de una red IP, se realizará la verificación del performance observando el comportamiento en la interfaz Ethernet que mira hacia la red del proveedor, así como en la interfaz Ethernet que lo hace hacia la red LAN del Municipio de Quito.

De esta manera en la Figura 3.11, se presenta información relativa a la interfaz que conecta hacia la red LAN principal del Municipio, aquí se observa que no hay errores de transmisión sobre esta interfaz, pero si existe el control

de redundancia cíclica (CRC[5]), que básicamente se generan porque la interfaz Ethernet del router es full duplex de 10Mbps está conectada en el switch de 100 Mbps full dúplex, además encontramos tráfico de broadcast, esto se debe a que en las redes se corre el protocolo 802.11, es decir difusión.

A continuación se presenta un gráfico que muestra la Interfaz Ethernet LAN.



```
Ethernet0 is up, line protocol is up
  Hardware is PQUICC Ethernet, address is 0012.8031.511f (bia 0012.8031.511f)
  Internet address is 172.20.24.96/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 10Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/142 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 45000 bits/sec, 7 packets/sec
  5 minute output rate 1000 bits/sec, 3 packets/sec
     2785977 packets input, 1511599365 bytes, 0 no buffer
     Received 678809 broadcasts, 0 runts, 0 giants, 15453 throttles
     16532 input errors, 29 CRC, 0 frame, 0 overrun, 16503 ignored
     0 input packets with dribble condition detected
     1780229 packets output, 284235015 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Figura 3.11: Interfaz Ethernet LAN

La interfaz que conecta a la red del proveedor PuntoNet, registra un gran tráfico Broadcast esto puede ser normal, pero hay que recordar que el protocolo ARP basa su funcionamiento en este tipo de tráfico, por otro lado la presencia de este tráfico puede deberse a virus o troyanos en la red de datos, esto puede provenir de algún sitio remoto que utiliza este enlace.

[5] Mecanismo de detección de errores en sistemas digitales

A continuación se presenta un gráfico que muestra la Interfaz de la Red del Proveedor PuntoNet.

```
Ethernet1 is up, line protocol is up
  Hardware is PQUICC_FEC, address is 0012.8031.5120 (bia 0012.8031.5120)
  Internet address is 172.16.12.10/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, 10Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:11, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 3 packets/sec
  5 minute output rate 41000 bits/sec, 3 packets/sec
     1730268 packets input, 278503440 bytes, 0 no buffer
     Received 25156 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     2243180 packets output, 1394951265 bytes, 0 underruns
     8087 output errors, 13220 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```

Figura 3.12: Interfaz de la Red del Proveedor PuntoNet

3.2.4.1. Resultados del Servicio de Internet

La red de acceso hacia el Internet puede ser representada en la siguiente figura:

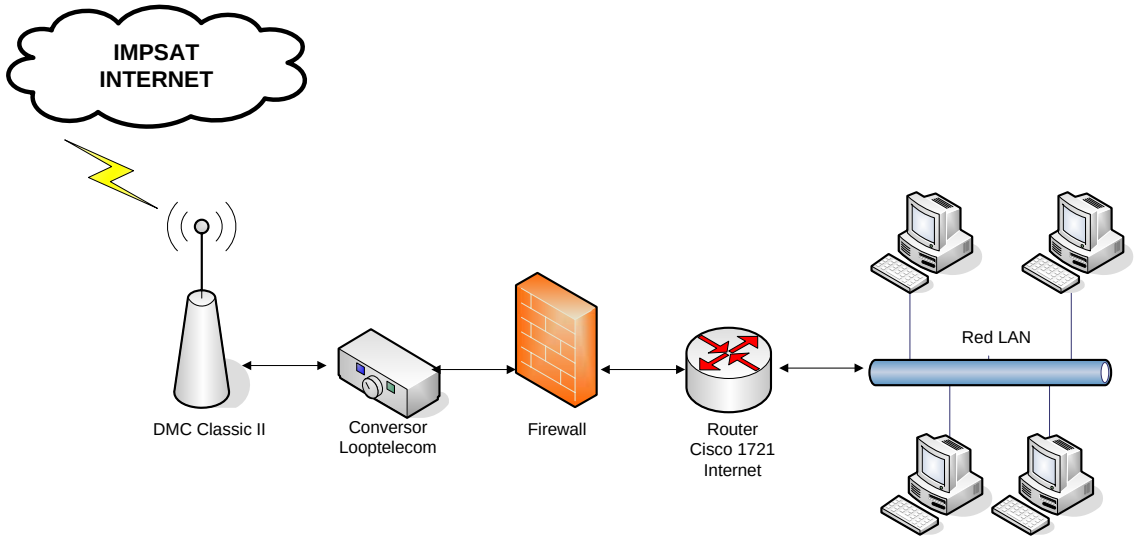
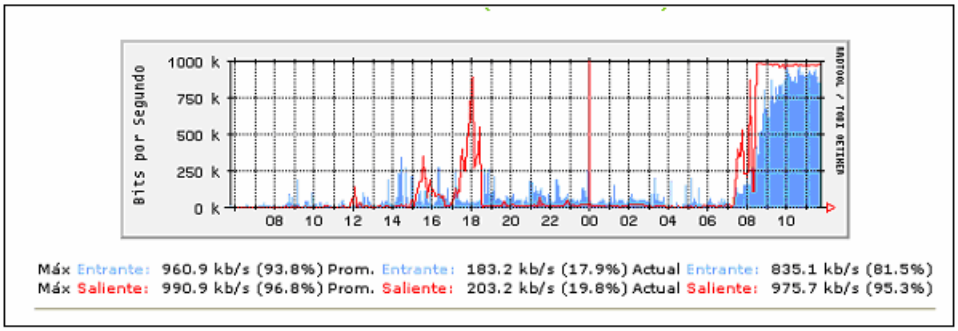


Figura 3.13: Acceso a Internet

El análisis se lo realizará tanto en la interfaz serial como en la interfaz Ethernet del ruteador Cisco 1721, en primera instancia se muestra la utilización promedio del canal:



Referencias	
Celeste	Tráfico Entrante desde el Cliente hacia Internet, en Bits por Segundo
Rojo	Tráfico Saliente desde Internet hacia el Cliente, en Bits por Segundo
Azul	Tráfico entrante máximo en 5 minutos
Verde	Tráfico saliente máximo en 5 minutos

Figura 3.14: Utilización Promedio del Canal

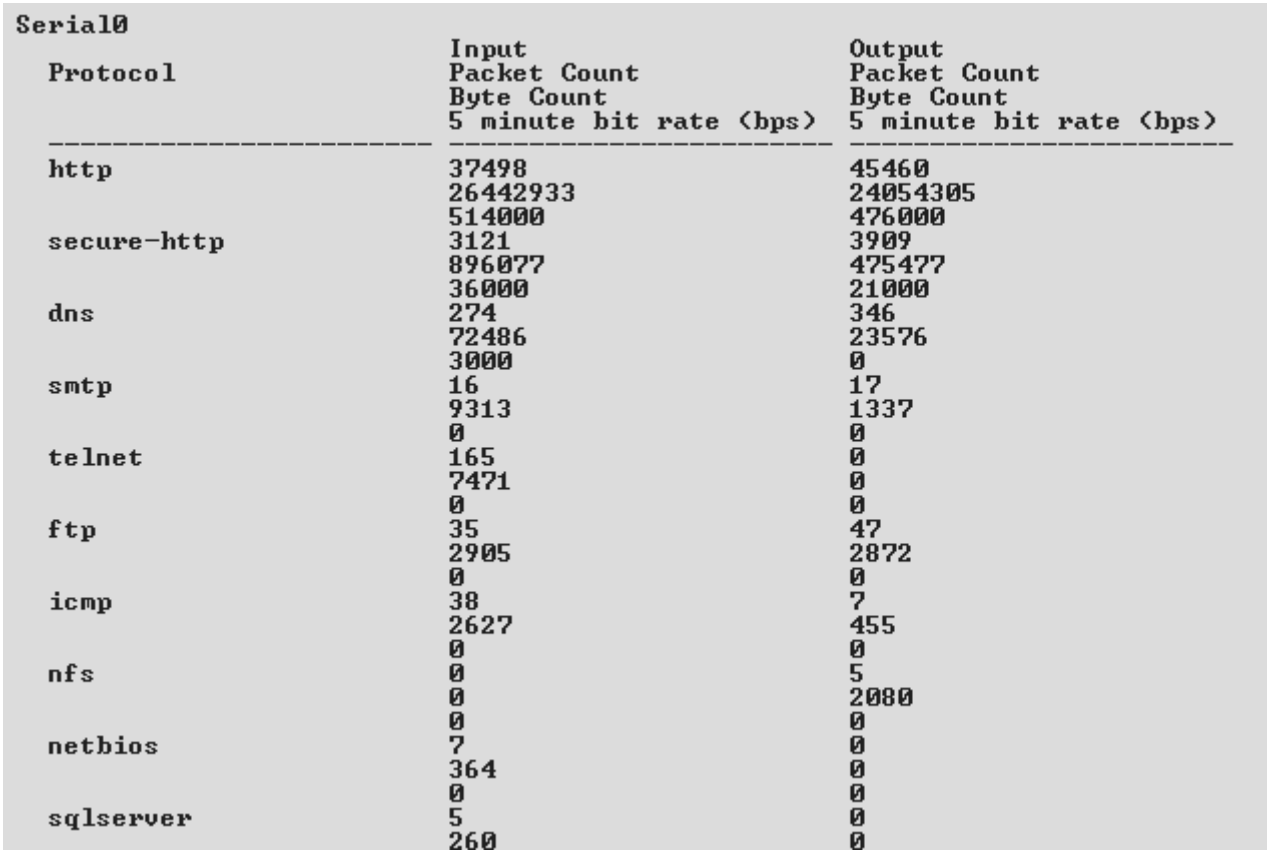
Podemos apreciar que el trafico de descarga download utiliza un máximo del 98 % de la capacidad del canal y el trafico de subida upload llega a un máximo de ocupación del 74% del canal, además este enlace no presenta degradación del nivel en la señal, así como tampoco se observan errores en el canal.

A diferencia de los ruteadores de las redes MAN, aquí no se identifican problemas de procesamiento en el router, el nivel de procesamiento es bajo.

El Internet es una herramienta de trabajo muy amplia, por lo que es importante detallar todos los protocolos utilizados en este enlace, a su vez esto será una guía para determinar las aplicaciones más utilizadas por los usuarios

en la red de datos del Municipio de Quito, que en un futuro servirán como referencia para establecer políticas de navegación en Internet.

A continuación se presenta un gráfico que muestra el Tráfico de Internet.



Serial0

Protocol	Input Packet Count Byte Count 5 minute bit rate (bps)	Output Packet Count Byte Count 5 minute bit rate (bps)
http	37498 26442933 514000	45460 24054305 476000
secure-http	3121 896077 36000	3909 475477 21000
dns	274 72486 3000	346 23576 0
smtp	16 9313 0	17 1337 0
telnet	165 7471 0	0 0 0
ftp	35 2905 0	47 2872 0
icmp	38 2627 0	7 455 0
nfs	0 0 0	5 2080 0
netbios	7 364 0	0 0 0
sqlserver	5 260	0 0

Figura 3.15: Tráfico de Internet

3.3. DISEÑO PROPUESTO PARA LA RED LAN – WAN

Se observa que las redes LAN de las dependencias municipales no se rigen a ningún modelo en cuanto a su diseño, más bien su crecimiento ha sido desordenado, por ello se propone el modelo SAFE de Cisco como referencia de diseño, este modelo agrupa componentes y funcionalidades de la red de datos en una estructura modular, por lo que cada módulo puede ser tratado de

forma independiente, en cuanto a seguridad, escalabilidad, calidad de servicio y soporte para nuevas tecnologías, respondiendo a estrategias generales de la organización que son controladas de manera centralizada, esto no implica para nada que se deba utilizar equipos de red de esta marca en su implementación.

A continuación se presenta un gráfico que muestra el Modelo SAFE de Cisco.

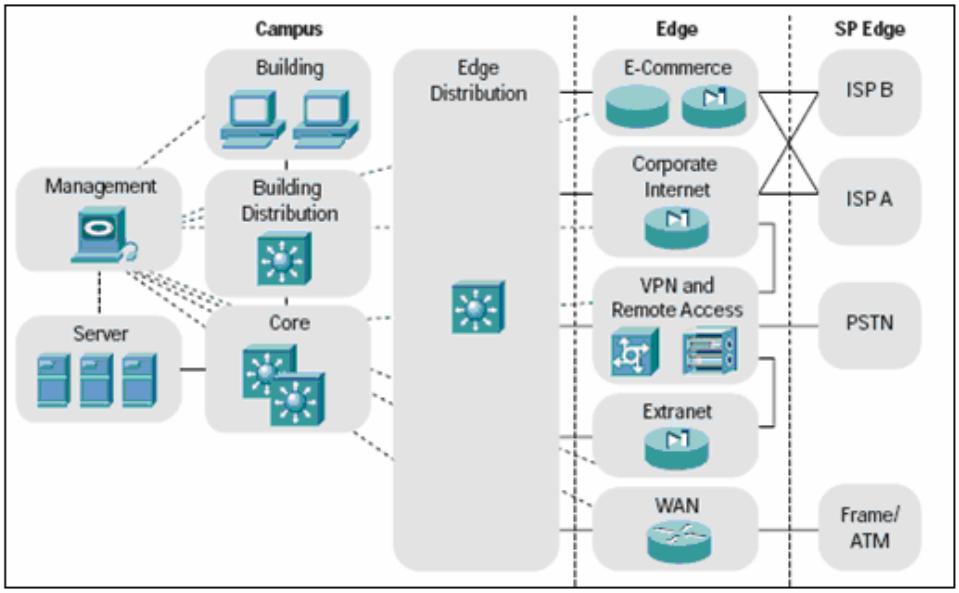


Figura 3.16: Modelo SAFE de Cisco

Para el caso de la red principal del Municipio de Quito, el diseño basado en Safe de Cisco sería:

En este diseño se pueden notar los módulos que se deben implementar en una red de datos de una organización:

3.3.1. Módulo de Administración

Está compuesto por un switch de capa 3, que conecta hacia el switch de core[6] y además recoge todas las conexiones de los equipos que no poseen puerto de consola para su administración, como es el caso de Firewall y Servidores, los cuales serán administrados mediante una tarjeta de red independiente, formando una red fuera de banda, esta red también puede ser aprovechada para obtener respaldo de la información de los servidores y las configuraciones de los dispositivos en un solo servidor encargado de esta función, sin interferir en la red de datos de producción. Los dispositivos que disponen de puerto de consola se unirán hacia un Terminal Server (múltiples puertos seriales) y de allí al servidor de administración que finalmente mediante el software adecuado gestionará toda la red de comunicaciones, garantizando que este tráfico con fines administrativos no sea interceptado desde cualquier punto de la red.

Para completar este módulo de administración se debe disponer de un servidor que gestione el tráfico del protocolo SNMP en la red fuera de banda, recopile la información almacenada en los diferentes archivos ó registro de accesos fallidos o exitosos, tráfico de ingreso y salida, etc. propios de cada

[6] Concentran el transporte de datos y voz formando backbones robustos y modulares.

dispositivo de la red de datos, además debe existir un servidor que cumpla las funciones de Servidor de Backup.

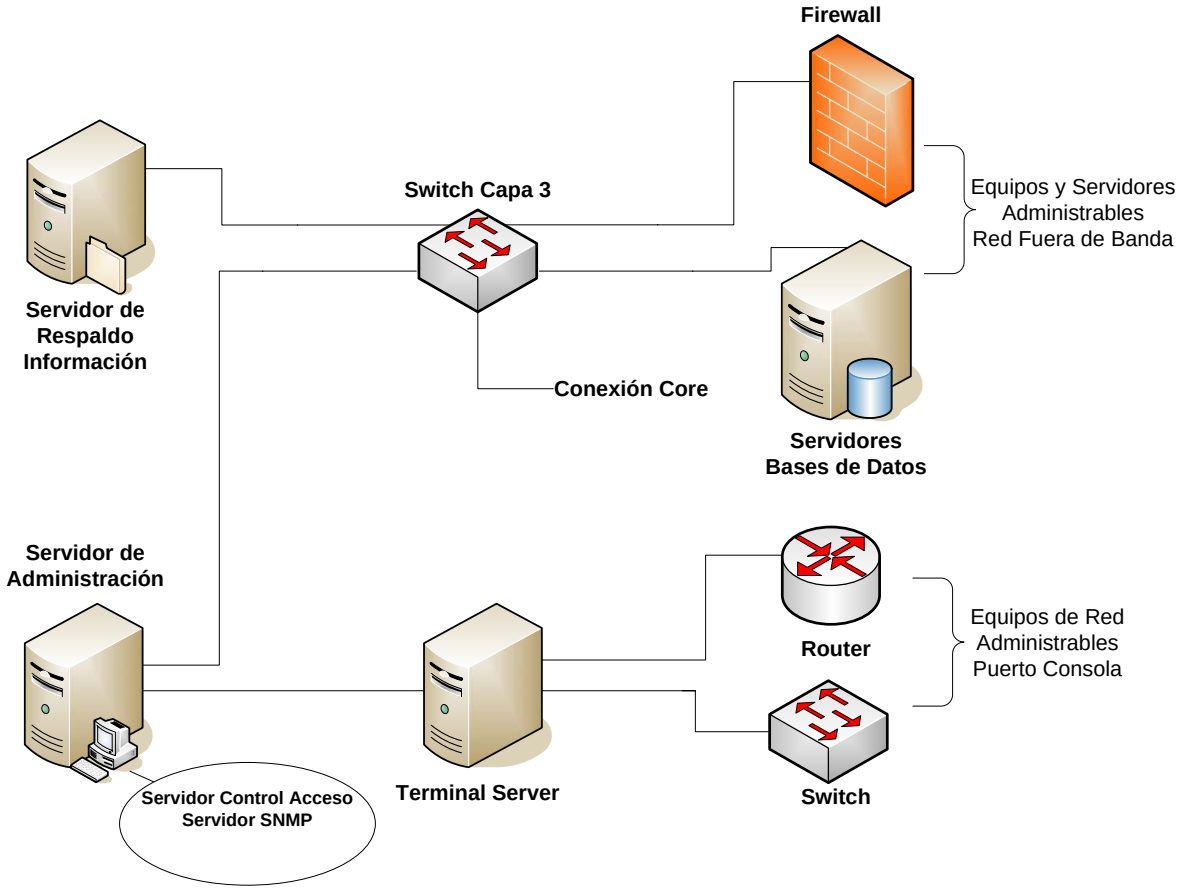


Figura 3.18: Módulo de Administración

3.3.2. Módulo de Building

Está compuesto por las estaciones de trabajo con sus debidos concentradores de señal, su objetivo principal es proporcionar servicios a los usuarios finales, en el caso de la red de datos del Municipio está compuesta por las redes LAN aledañas hacia la Dirección Metropolitana de Informática y que están unidas a la misma a través de enlaces mediante cable UTP o fibra óptica.

3.3.3. Módulo de Building Distribution

Su objetivo es agrupar todos las conexiones provenientes de las redes de Building, normalmente está compuesto por un equipo switch de capa 3 o por un router que realice funciones de encaminamiento, calidad de servicio QoS y control de acceso. En el caso del Municipio este equipo recibirá todo el tráfico proveniente de las redes Building aledañas a la Dirección Metropolitana de Informática.

3.3.4. Módulo de Core

Su principal función es la de filtrar y conmutar el tráfico tan pronto como sea posible de una red hacia la otra, está conformado por un switch de capa 3 con velocidad de conmutación elevada.

3.3.5. Módulo Edge

Uno de los equipos que tiene mucha importancia en este diseño para el caso de la red de datos del Municipio de Quito constituye el Switch Edge (extremo) que es el encargado de concentrar y gestionar todas las señales provenientes de los sitios remotos hacia la red central, está compuesto por un equipo switch de capa 3 o por un router que realice funciones de encaminamiento, calidad de servicio QoS y control de acceso.

3.3.6. Módulo Server

Está compuesto por los servidores que posee el Municipio de Quito, así como el switch de capa 3 de gran velocidad de conmutación.

3.3.7. Módulo Internet Corporativo

Proporciona conectividad hacia los servicios de Internet a los usuarios internos, y a los usuarios de Internet acceso a los servidores públicos de manera rápida y confiable, está conformado por el Firewall, los servidores de comunicaciones y el router de conexión hacia la red del Proveedor ISP. En el caso del Municipio este módulo está implementado en su totalidad.

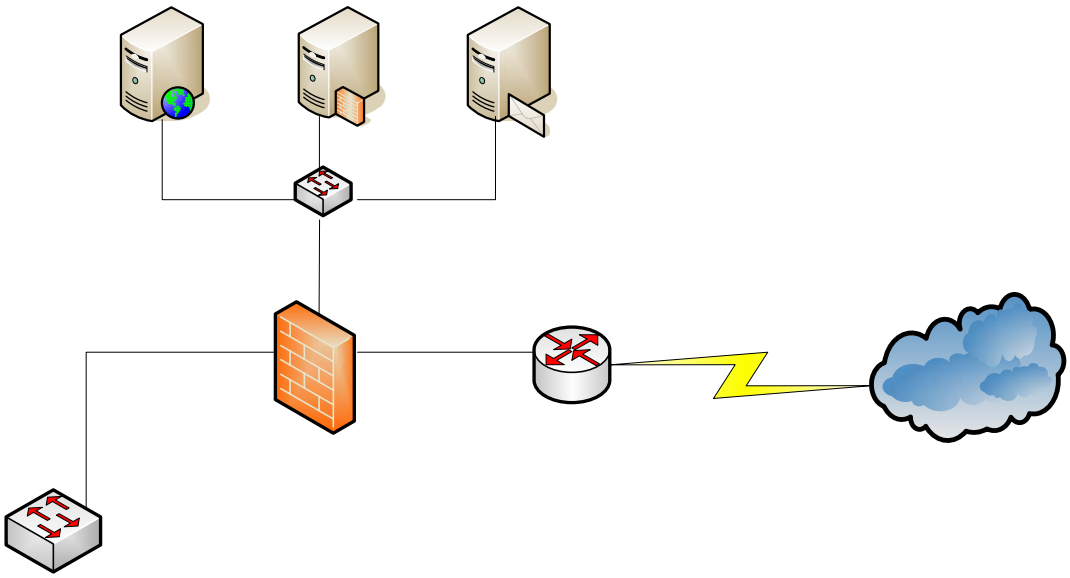


Figura 3.19: Módulo Internet Corporativo

3.3.8. Módulo WAN

Su finalidad es permitir la interconectividad entre las oficinas remotas y la oficina matriz, la red de datos del Municipio de Quito dispone de proveedores Andinatel y PuntoNet que proporcionan este servicio a las distintas dependencias municipales, está compuesto básicamente por los routers instalados por estos proveedores.

Para el caso de las redes LAN de las dependencias municipales, este diseño también puede ser implementado, lo único que se haría es concentrar las funciones de varios módulos en un solo equipo, lo importante es no quitar funciones sino asumirlas.