UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ARQUITECTURA FUNCIONAMIENTO Y GESTIÓN EN EL PERÚ DE LA RED IP CONMUTADA

INFORME DE SUFICIENCIA
PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO
PRESENTADO POR:

DAVID RICARDO PÉREZ ROSALES

PROMOCIÓN
2000 – I
LIMA – PERÚ
2005

ARQUITECTURA FUNCIONAMIENTO Y GESTIÓN EN EL PERÚ DE LA RED IP CONMUTADA

DEDICO ESTE TRABAJO A:

MIS PADRES POR TODO EL APOYO

BRINDADO Y A MI ESPOSA POR

ESTAR A MI LADO.

SUMARIO

Este presente trabajo consta de cinco capítulos los cuales serán descritos a continuación:

En el capitulo I se menciona la teoría del protocolo IP, su datagrama y sus funciones de cada campo.El enrutamiento correcto de los paquetes desde un origen hasta un destino específico utilizando las clases de redes

En el capitulo II se menciona el modelo jerárquico de una red en general y sus diferentes capas como son la de acceso, distribución, transporte y core.

Se describe el modelo OSI con sus diferentes capas dando a conocer sus características, estándares y protocolos. El funcionamiento de equipos los cuales trabajan en diferentes capas del Modelo OSI.

En el capitulo III mencionamos la definición red con sus características, funciones y servicios brindados a los usuarios finales. Como veremos la Red se divide en 3 niveles de red, servicios y de gestión.

Se describe las funciones y características de equipos de los diferentes niveles de red, servicio y de gestión. En el nivel de red los equipos más importantes son el

MAX-TNT que es un servidor de acceso y el BSTDX que es un conmutador de paquetes. En la parte de servicios tenemos diferentes servidores entre los cuales podemos mencionar al servidor DNS el cual se utiliza para la resolución de dominios, el servidor RADIUS el cual cumple la función de autenticar, autorizar y de llevar la contabilidad de los usuarios de la red, y SOFTSWITCH que es el que procesa las llamadas y trabaja con señalización #7 conectando a la red conmutada con la RED IP.

En el capitulo IV mencionamos la topología de la red conmutada del Perú con su distribución alrededor del país. Mencionaremos que tenemos una red de servicios primaria y secundaria para los cuales tenemos servidores con esa característica de redundancia.

Veremos los diferentes métodos de acceso y autenticación de los usuarios de la red. Entre ellos cabe mencionar la autenticación delegada en la cual nuestro RADIUS delega la autenticación a un segundo RADIUS externo.

Por último mencionamos el funcionamiento de los procesos de señalización, autenticación y navegación.

En capitulo V se hace mención a los diferentes tipos de servicios que ofrece la red a los usuarios. Entre ellos tenemos el servicio de Infovía Plus Básico con modalidad delegada el cual es utilizado por mas del 50% de los usuarios.

ÍNDICE

CAPÍTULO II

CONCEPTOS DE INTERWORKING

CAPITULO III

ARQUITECTURA DE LA RED IP

CAPITULO IV

FUNCIONAMIENTO DE LA RED IP

CAPITULO V

SERVICIOS DE LA RED IP

PRÓLOGO

Desde el año 1994 las telecomunicaciones han dado un giro de 180 grados empezando con el desarrollo de la telefonía celular hasta el envío de datos a través de internet a gran escala.

Por eso es que en la actualidad tenemos una gran variedad de servicios como son el correo, juegos en línea, videoconferencias ,redes privadas virtuales, seguridad, internet, etc.

La mayoría de las redes de datos se encuentran tendidas sobre plataformas de telefonía las cuales brindan a los usuarios diferentes velocidades de acceso.

Telefónica del Perú en 2000 instaló la red IP conmutada de Lucent a nivel nacional, colocándola en servicio a partir del 2001 siendo Terra su primer proveedor.

Desde sus inicios se vendió la tarifa semi plana. Esta red tiene gran característica la de escalabilidad mediante la cual el backbone puede crecer en nodos y transporte.

Por eso mencionaremos en el contenido los diferentes servicios ofrecidos por la Red IP y sus planes futuros para el servicio.

CAPÍTULO I

INTRODUCCIÓN AL PROTOCOLO IP

1.1 INTRODUCCIÓN

El protocolo IP es el más utilizado para la interconexión entre redes y cuando se diseñó ya se tuvo en cuenta la interconexión entre redes. Su trabajo es proporcionar un medio para el transporte de datagramas del origen al destino, sin importar si estas máquinas están en la misma red, o si hay otras redes entre ellas. IP está implementado en todos los computadores y dispositivos de encaminamiento. Se preocupa de la retransmisión de los datos de un ordenador a otro ordenador, pasando por uno o varios dispositivos de encaminamiento nodo a nodo. No sabe de que aplicación son los paquetes, únicamente sabe de máquina son.

El protocolo IP cubre tres aspectos importantes:

1.- Define la unidad básica para la transferencia de datos en una red interna, especificando el formato exacto de un datagrama IP.

2.-Realiza las funciones de enrutamiento.

3.- Define las reglas para que los host y routers procesen paquetes, los descarten ó generen mensajes de error.

1.2 EL DATAGRAMA IP

El esquema de envío de IP es similar al que se emplea en la capa Acceso a red. En esta ultima se envían tramas formadas por un encabezado y los datos. En el encabezado se incluye la dirección física del origen y del destino.

En el caso de IP se envían datagramas, estos también incluyen un encabezado y datos, pero las direcciones empleadas son direcciones IP.

1.3 FORMATO DEL DATAGRAMA IP

El formato del datagrama IP consiste en una parte de cabecera y en una parte de datos cuyo tamaño es variable.

Cabecera

En la cabecera hay una parte fija de 20 bytes y una parte opcional de longitud variable. En la figura 1 se puede ver el formato de la cabecera IP.

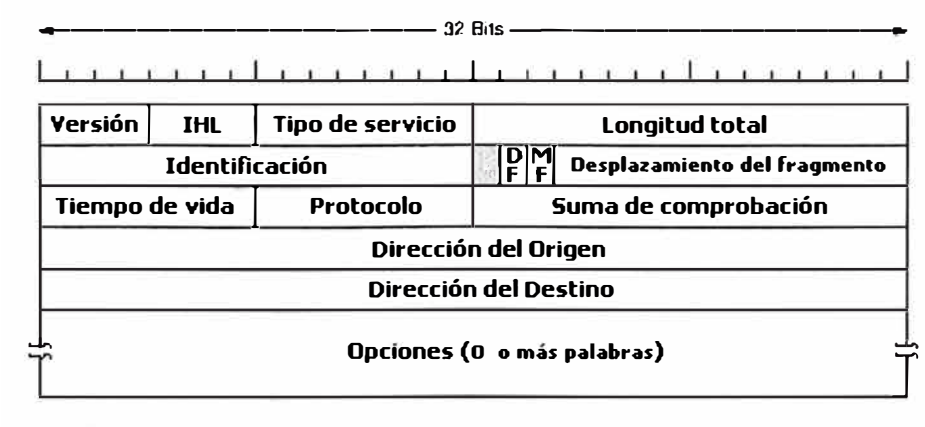

Figura.1 Cabecera del Datagrama IP

A continuación hay una descripción de cada uno de los campos que forman la cabecera del datagrama IP:

Versión (4 bits): Indica el número de versión del protocolo al que pertenece el datagrama, lo que permitirá la evolución futura del protocolo y que la transición entre las versiones se pueda hacer ejecutándose en unas máquinas la versión vieja y en otras la versión nueva.

IHL (Internet Header length) (4 bits): Indica la longitud de la cabecera en palabras de 32 bits (4 bytes). El valor mínimo es cinco (20/4=5). Este campo es necesario por no ser constante el tamaño de la cabecera como hemos comentado anteriormente. El valor máximo puede ser 15 (1111) lo que limita la cabecera a 60 bytes (15*4) y en consecuencia el campo de opciones a 40 (60-20). En el caso de que, por ejemplo, se quiera registrar la ruta de un paquete este valor puede ser insuficiente y ser totalmente inútil esta opción.

Tipo de servicio (8 bits): Permite que el host especifique que clase de servicio quiere, pudiéndose combinar confiabilidad y velocidad. Para la voz digitalizada es mas importante realizar la entrega de forma rápida que precisa, mientras que para la transferencia de ficheros no importa a que velocidad se realiza la transferencia pero si que esté libre de errores. De los 8 bits, 3 son para el campo de precedencia que en realidad es una prioridad de 0 (normal) a 7 (para los paquetes de control de red). A continuación aparecen los bits de seguridad (alta o baja), retardo (alto o bajo cuando se intenta minimizar el retardo) y rendimiento (normal o alto cuando se intenta maximizar el rendimiento durante la transmisión del datagrama).

Longitud total (16 bits) en bytes que tendrá todo el datagrama, considerando tanto la cabecera como los datos. Hay que tener en cuenta que el tamaño máximo de un datagrama es de 65535 bytes lo que puede ser insuficiente en las redes de alta velocidad.

Identificador (16 bits): es un número de secuencia que junto a la dirección origen, la dirección destino y el protocolo de usuario, sirven para que la máquina destino determine a que datagrama pertenece el fragmento que ha recibido. Todos los fragmentos de un datagrama contienen el mismo valor en el campo identificador y este número debe ser único para la dirección origen, la dirección destino y el protocolo de usuario durante el tiempo en el que el datagrama permanece en el conjunto de redes.

Indicadores (3 bits): El primer bit no se utiliza actualmente. El indicador de mas fragmentos (**MF**) cuando vale 1 indica que este datagrama tiene mas fragmentos y toma el valor 0 en el último fragmento. El indicador de no fragmentar (**DF**) prohibe la fragmentación cuando vale 1. Es una orden que se le da a los encaminadores de que no fragmenten el datagrama cuando el destino es incapaz de reensamblarlo. Si este bit vale 1, el datagrama se descartará si se excede el tamaño máximo en una subred de la ruta. Por lo tanto, cuando este bit vale 1, es aconsejable usar encaminamiento por la fuente para evitar subredes cuyo tamaño máximo de paquete sea menor que el tamaño del datagrama.

Desplazamiento del fragmento (13 bits): Indica en que posición del datagrama original, medido en unidades de 8 bytes (64 bits), va el fragmento actual. Debido a

esto, todos los fragmentos excepto el último contienen un campo de datos con una longitud múltiplo de 8 bytes. Como se proporcionan 13 bits, puede haber un máximo de 8912 (2**13) fragmentos por datagrama, y por lo tanto el tamaño máximo de un datagrama es de 65536 bytes, uno mas que el campo de longitud total.

Tiempo de vida (8 bits): Es un contador que sirve para limitar la vida de un paquete. Aunque lo lógico sería pensar que cuenta el tiempo en segundos, en realidad lo que cuenta es el número de saltos de dispositivo de encaminamiento que realiza. Cuando el contador llega a cero, el paquete se descarta y se envía de una paquete al computador origen avisándole. Con este mecanismo se consigue que los datagramas no permanezcan indefinidamente en la red si, por ejemplo, se dañan las tablas de encaminamiento.

Protocolo (8 bits): Se utiliza por la capa de red para saber a que protocolo de la capa de transporte le tiene que enviar el datagrama una vez lo ha reensamblado. Existen diferentes protocolos de transporte, entre ellos TCP y UDP. En el RFC 1700 se definen todos estos protocolos.

Suma de comprobación (16 bits): Sirve para verificar el contenido de la cabecera y es útil para la detección de errores generados durante la transmisión del datagrama. Como algunos de los campos de la cabecera pueden cambiar en alguno de los dispositivos de encaminamiento (por ejemplo, el tiempo de vida y algunos campos relacionados con la segmentación), este valor es verificado y recalculado en cada uno de los dispositivos de encaminamiento. El algoritmo empleado consiste en sumar todas las medias palabras de 16 bits a medida que van llegando, usando la

aritmética de complemento a 1, y luego obtener el complemento a 1 del resultado. Se supone que la suma de comprobación de la cabecera es cero cuando llega. Este algoritmo es algo mas robusto que una suma normal. Existen algunas técnicas para acelerar el cálculo.

Dirección origen (32 bits): Indica el número de red y el número del ordenador que envía el datagrama.

Dirección destino (32 bits): Indica el número de red y el número del ordenador al que se envía el datagrama.

Opciones (variable): Contiene las opciones solicitadas por el usuario que envía los datos y se diseñó para que las versiones posteriores del protocolo pudieran incluir información no considerada originalmente, para que los investigadores pudieran probar cosas nuevas y para que aquellas aquella información que es utilizada pocas veces no tuviera asignada unos bits determinados en la cabecera. Cada una de las opciones empieza en 1 byte que identifica la opción. Algunas de las opciones vienes seguidas de un campo de 1 byte para indicar la longitud de la opción y a continuación uno o mas bytes de datos.

Relleno (variable): El campo de opciones se rellena para que su tamaño sea múltiplo de 32 bits (4 bytes).

1.4 FRAGMENTACIÓN

Cuando tenemos un paquete IP y lo queremos pasar a la capa de enlace se le añade la cabecera y el campo de CRC. Como hemos comentado anteriormente hay redes que limitan el tamaño máximo de los paquetes que pueden transportar y por este motivo, los paquetes deben ser fragmentados como ilustra la siguiente figura 2. Recordar que al hablar de la cabecera de un paquete IP comentamos la existencia del bit de no fragmentación que cuando está activo especifica que el paquete no se puede fragmentar.

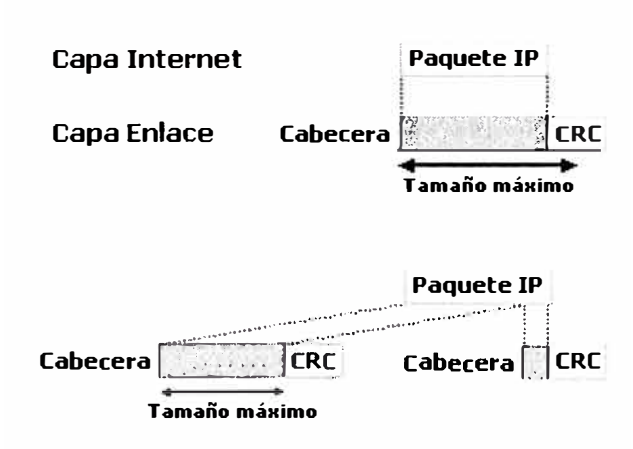

Figura.2 Fragmentación de un paquete IP

Los campos cuyo valor es modificado debido a la fragmentación son:

El campo posición o desplazamiento que indica a que byte corresponde el primer byte de datos.

El Indicador o bit de mas datos: Vale 1 en todos los fragmentos excepto en el último. Si un fragmento tiene que volver a ser fragmentado y el bit de mas datos ya

vale 1, mantendrá este valor en todos los nuevos fragmentos. Si vale 0, tomará el valor 1 excepto en el último fragmento.

El campo longitud de los datos y el campo checksum es calculado para cada fragmento.

El identificador de paquete y el resto de campos conservan el valor que tienen antes de ser fragmentado el paquete IP.

Supongamos que 1000 bytes deben ser transportados sobre una red que soporta un tamaño máximo de 256 bytes. Suponiendo que la cabecera de cada datagrama IP requiere 20 bytes, determinar el valor correspondiente que deben los tomar los diferentes campos en cada uno de los fragmentos. Suponemos que el identificador de campo vale 20.

Como el tamaño máximo es 20 para cada fragmento, podríamos usar 236 bytes (256 – 20), pero teniendo en cuenta que el desplazamiento debe ser expresado por bloques de 8 bytes, el tamaño de los datos que podemos poner es de 232 bytes (29 * 8 = 232). Por lo tanto se requieren 5 fragmentos, cuatro con 232 bytes de datos del usuario y uno con 72 bytes. En la tabla 1 se pueden ver los valores de cada uno de los campos.

IDENTIFICACION	20	20	20	20	20
LONGITUD	252	252	252	252	72
DESPLAZAMIENTO	0	29	58	87	116
MAS DATOS	1	1	1	1	0

Tabla.1 Campos de Fragmentación

Sumando la longitud de los 5 fragmentos podemos ver que la cantidad de bytes transportados es de 1100 bytes, cuando hubiera sido suficiente transportar 1020 bytes si no hubiéramos tenido la limitación del tamaño máximo que podía ser transportado por la red.

Reensamblado

Como todos los fragmentos de un paquete IP tienen el mismo identificador de paquete y en la cabecera está almacenado el tamaño del fragmento y su desplazamiento dentro del paquete es fácil realizar el reensamblado. De cualquier manera tanto la fragmentación como el reensamblado consumen bastantes recursos. Además de asignar un buffer en el que se realizará el reensamblado del paquete, también se necesita controlar que fragmentos han llegado y cuando, cual están pendientes de llegar y controlar cuando el paquete ya está completo.

Como no hay manera de saber el tamaño exacto del paquete, el tamaño del buffer tiene que ser de 65535 bytes (exactamente el tamaño máximo del paquete IP) Cuando recibe por primera vez un fragmento de un paquete se pone en marcha un temporizador (tiempo de vida de reensamblaje) y va colocando los diferentes fragmentos que le vayan llegado de ese paquete IP (todos aquellos que tienen el mismo identificador). Si transcurrido el tiempo determinado por el temporizador no se ha podido realizar el reensamblado, se para el proceso de reensamblado y los paquetes recibidos se descartan. Hay que tener en cuenta que el tiempo de vida del datagrama también se va decrementado mientras dura el reensamblado. Como IP no garantiza el servicio, el protocolo de transporte TCP será el encargado de pedir la retransmisión del paquete.

Existen dos posibilidades respecto a donde se debe realizar el reensamblado de los paquetes: en cada uno de los dispositivos de encaminamiento o solo en el destino. Realizar el ensamblado en cada uno de los dispositivos de encaminamiento tiene la ventaja de que se utilizan mejor los recursos del sistema. En cada tramo de red únicamente se transporta el número de paquetes necesario reduciéndose la carga de la red al disminuir el número de paquetes, y por consiguiente de cabeceras, que son transportados. Esta posibilidad tiene el inconveniente de que es necesario reservar memoria en cada uno de los dispositivos de encaminamiento y es necesario un tiempo en cada uno de ellos para realizar el proceso de reensamblado. Además, en este caso, es necesario que todos los fragmentos de un paquete pasen por el mismo dispositivo de encaminamiento y por lo tanto no se podrá hacer encaminamiento dinámico. El protocolo IP realiza el reensamblado en el destino.

En la tabla 2 se puede ver un pequeño resumen de las ventajas e inconvenientes de cada una de las posibilidades:

DISPOSITIVOS DE ENCAMINAMIENTO	**+4** Mejor utilización de los recursos **-8** Se necesitan grandes memorias **-8** Todos los fragmentos deben pasar por el mismo dispositivo de encaminamiento
EN EL DESTINO	**-8** Disminuye la eficiencia **+4** Es más fácil de realizar

Tabla.2 Ventajas y Desventajas del reensamblado

1.5 DIRECCIONES IP

Cada computador y cada dispositivo de encaminamiento tendrá una dirección única cuya longitud será de 32 bits, que será utilizada en los campos dirección origen y dirección destino de la cabecera. Esta dirección consta de un identificador de red y de un identificador de computador. La dirección, como puede verse en la siguiente figura, está codificada para permitir una asignación variable de los bits utilizados al especificar la red y el computador. Este formato de direcciones permite mezclar las tres clases de direcciones en el mismo conjunto de redes. La dirección IP más pequeña es la 0.0.0.0 y la mayor es 255.255.255.255.

Existen tres clases de redes que se pueden clasificar teniendo en cuenta la longitud del campo de red y del campo ordenador. La clase a la que pertenece una dirección puede ser determinada por la posición del primer 0 en los cuatro primeros bits. Las

direcciones están codificadas para permitir una asignación variable de bits para especificar la red y el ordenador.

Clase A: Pocas redes, cada una con muchos ordenadores. 7 y 24 bits (+1). Por ejemplo ARPANET.

Clase B: Un número medio de redes, cada una con un número medio de ordenadores. 14 y 16 bits (+2)

Clase C: Muchas redes, cada una con pocos ordenadores. 21 y 8 bits (+3). Por ejemplo un red de área local.

Clase D: Permite hacer multitransmisión (o multicasting) en la cual el datagrama se dirige a múltiples ordenadores. Podemos enviar un paquete IP a un grupo de máquinas que por ejemplo pueden estar cooperando de alguna manera mediante la utilización de una dirección de grupo.

Clase E: Reservado para el futuro.

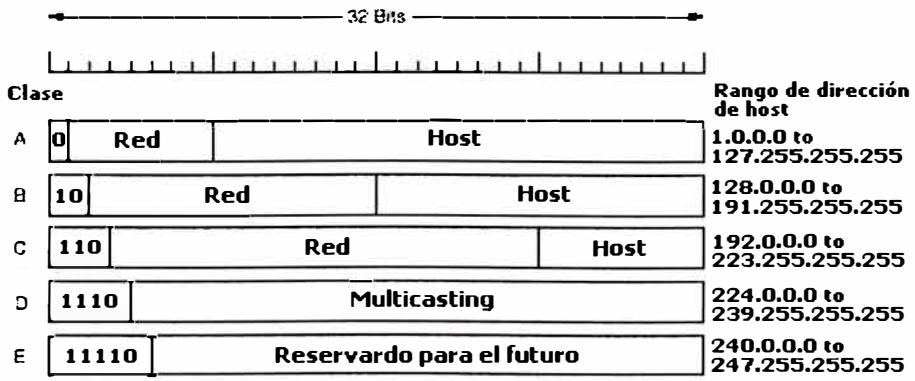

Figura.3 Clases de Redes

La siguiente tabla muestra el número de redes y de ordenadores por red en cada una de las tres clases primarias de direcciones IP:

CLASE	BITS EN EL PREFIJO	MAXIMO Nº DE REDES	BITS EN EL SUFIJO	MAXIMO Nº DE ORDENADORES POR RED
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Tabla 3 Ejemplo de clases de Direcciones IP

Normalmente las direcciones se suelen escribir en notación decimal con puntos. Por ejemplo, la dirección 82CE7C0D (1000 0010 1100 1110 0111 1100 0000 1101 que es de clase B) se escribe como 130.206.124.13.

82 = 8*16 + 2 = 128 + 2 = 130

CE = C*16 + E = 12 * 16 + 14 = 192 + 14 = 206

7C = 7 * 16 + C = 112 + 12 = 124

0D = D = 13

Observando la figura anterior puede verse que no todas las direcciones han sido asignadas a una clase en concreto. Algunas de estas direcciones se utilizan como direcciones especiales:

Este ordenador: La dirección 0.0.0.0 significa esta red o este ordenador y únicamente es usada por los ordenadores cuando son arrancados, sin que se vuelva a utilizar posteriormente. De esta forma las máquinas se pueden referir a su propia red

sin saber su número, pero tiene que saber su clase para saber cuantos ceros debe incluir.

Un ordenador de esta red: Poniendo el campo red todo a ceros (es necesario saber la clase de la red para decidir cuantos ceros se deben poner).

Difusión de red local o limitada: La dirección 255.255.255.255 (todos 1s) se usa como dirección para indicar todos los ordenadores de la red indicada y es utilizada para hacer difusión.

Difusión de una red distante o dirigida: También se puede hacer difusión a una red distante poniendo la dirección de la red y rellenando el campo ordenador con 1's.

Retrociclo: Las direcciones 127.xx.yy.zz se reservan para pruebas de realimentación. Los paquetes que tienen esta dirección no son enviados por la red sino que son procesados localmente y se tratan como si fueran paquetes de entrada. Esto permite que los paquetes se envíen a la red local sin que el transmisor conozca su número. Esta característica también se usa para la detección de fallos en el software de red.

Figura.4 Direcciones Especiales

Para estar seguros de que la dirección Internet es única, todas las direcciones de Internet son asignadas por un autoridad central. El Internet Assigned Number Authority (IANA) tiene el control sobre los números asignados. Sin embargo, cuando una organización quiere una dirección debe obtenerla de INTERNIC (Internet Network Information Center). La autoridad central solo es necesaria para asignar la porción de la dirección correspondiente a la red, cuando una organización ya tiene su prefijo, puede asignar un único sufijo a cada ordenador sin contactar con la autoridad central.

Una máquina puede estar conectada a varias redes y tener una dirección IP diferente en cada red. En este caso recibe el nombre de "multihomed". Esto se utiliza para aumentar la seguridad pues si una red falla el ordenador aún esta conectado a internet utilizando la otra red. Por otra parte, también es usado para aumentar el rendimiento de la red pues permite enviar directamente el tráfico a una red en concreto sin tener que pasar por los dispositivos de encaminamiento.

1.6 ENCAMINAMIENTO

Cuando un paquete llega a un dispositivo de encaminamiento se debe determinar cual es la dirección del siguiente dispositivo de encaminamiento teniendo en cuenta la dirección IP destino que hay almacenada en el campo correspondiente del paquete y de la información que hay almacenada en las tablas de encaminamiento. Hay que tener en cuenta que es necesario realizar una conversión entre la dirección IP y la dirección MAC (cuando el enlace entre los dos dispositivos de encaminamiento sea una LAN) que se efectúa de manera automática mediante el protocolo ARP.

Esta tabla puede ser estática o dinámica. En el primer caso puede contener rutas alternativas que serán utilizadas cuando algún dispositivo de encaminamiento no esté disponible. Las tablas dinámicas son mas flexibles cuando aparecen errores o congestión en la red. Estas tablas también pueden proporcionar servicios de seguridad y de prioridad, por ejemplo, para asegurarse que a ciertos datos no se les permita pasar por determinadas redes.

Otra técnica de encaminamiento es el encaminamiento en la fuente. En este caso, como ya comentamos anteriormente, el ordenador origen incluye en la cabecera del paquete la dirección de los dispositivos de encaminamiento que debe utilizar el paquete.

CAPÍTULO II

CONCEPTOS DE INTERWORKING

2.1 ARQUITECTURA JERÁRQUICA DE UNA RED

En el diseño de una red pueden intervenir muchos factores, sin embargo es conveniente que se tenga conocimiento de los principales esquemas se utilizan.

Es así que, el modelo jerárquico base usado es:

Capa de Acceso, Capa de Distribución o Transporte y Capa de Core

Esta jerarquía se puede apreciar en la siguiente figura:

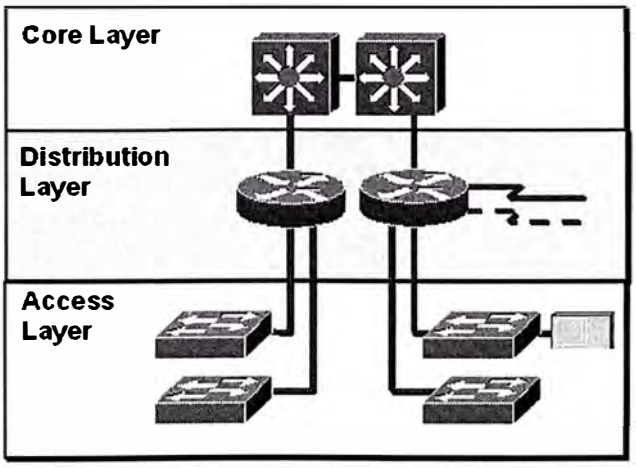

Figura.5 Arquitectura Jerárquica de un Red

2.1.1 Capa de Acceso

Se llama capa de "Acceso a la Red" al punto destinado a la conexión de los usuarios finales, para que puedan acceder a los servicios que brinda la red.

Generalmente, esta capa de la red tienen como función principal permitir a los usuarios ingresar a la red, por lo que se colocan varios puntos de acceso (dependiendo del tamaño de la red), manejando cada uno de estos puntos sólo un porcentaje de la totalidad del tráfico de los usuarios. Es por esta razón que los equipos que conforman los puntos de acceso se enfocan en una cantidad pequeña de tráfico, teniendo menor capacidad de procesamiento que el resto de equipos en la red.

2.1.2 Capa de Distribución o Transporte

La capa de "Transporte" es el punto entre la capa de acceso y la capa principal o "core".

Tiene como función principal el manejo de los paquetes en lo que respecta a enrutamiento, filtrado y acceso a WAN. Sin embargo, también es posible que se encargue de otras funciones adicionales.

Las funciones de la capa de transporte o distribución son:

- Enrutamiento de Tráfico.
- Filtrado de Tráfico.
- Acceso Remoto.
- Define el dominio de broadcast y/o multicast.
- Interconexión entre diferentes medios físicos.
- Seguridad de la Red

En resumen, la capa de distribución se encarga de la conectividad basada en políticas; ya sean de ruteo, de seguridad u otras.

2.1.3 Capa de Core

La capa de "Core" es el núcleo de toda la red y su función principal es conmutar el tráfico lo más rápido posible.

Cuando un usuario hace el requerimiento de un servicio (por ejemplo: e-mail o internet), éste ingresa por la capa de acceso hacia la capa de distribución, la cual se encarga de procesar el requerimiento para luego enviarlo hacia el core o backbone. El backbone sólo se preocupa por el transporte rápido de la información, mientras que la capa de transporte determina si es posible enrutar los paquetes y cómo debe enrutarlos.

De esta manera, las funciones de la red logran distribuirse, permitiendo una adecuada operación, gestión y administración de cada servicio.

2.2 MODELO OSI

El modelo OSI, aunque ha sido estudiado infinidad de veces y se tiene como base de las telecomunicaciones desde hace mucho tiempo, aún está completamente vigente y es muy importante que se tenga pleno conocimiento de su funcionamiento. En la figura 6 se aprecian las 7 capas del modelo OSI:

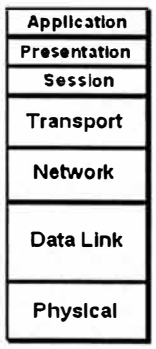

Figura.6 Modelo OSI

Seguidamente, haremos un resumen de las cuatro primeras capas del modelo OSI.

2.2.1 Capa Física

Es la primera capa del modelo OSI y especifica los requerimientos eléctricos, mecánicos, de procedimiento y funcionales para activar, mantener y desactivar un enlace físico entre sistemas.

Esta capa especifica características tales como niveles de voltaje, velocidad de transmisión, máxima distancia de transmisión y conectores físicos, todos estos definidos por normas, tales como:

- Ethernet
- IEEE 802.3
- EIA/TIA-232
- V.35

Debido a la extensiva utilización de la norma Ethernet, es que daremos un especial enfoque a este protocolo.

Ethernet/802.3

La norma Ethernet y la IEEE 802.3 definen una topología tipo bus para LAN que opera a una velocidad de 10Mbps, pudiendo utilizar cualquiera de las siguientes tres normas de cableado:

- 10Base2 o Thin Ethernet, permite segmentos de red de hasta 185 m. sobre cable coaxial.
- 10Base5 o Thick Ethernet, permite segmentos de red de hasta 500 m. sobre cable coaxial.
- 10BaseT, permite segmentos de red de hasta 500 m. sobre cable tipo UTP.

Tanto 10Base2, como 10Base5, proveen acceso a varias estaciones sobre un mismo cable físico (cable coaxial); mientras que 10BaseT sólo puede conectar una sola estación sobre el mismo cable físico, es por esto que, esta norma es utilizada conjuntamente con dispositivos como Hubs (capa física) y Switches (capa enlace).

Hub

El Hub es un dispositivo que se usa para "extender" el cable de la red y permitir la conexión de múltiples estaciones.

El Hub trabaja a nivel de capa física recibiendo la información por cualquiera de sus puertos y repitiéndola tal cual en todos los demás, sin manipularla.

Las características de una red conectada por medio de un hub son:

- Todos los dispositivos están en el mismo dominio de colisión.
- Todos los dispositivos están en el mismo dominio de broadcast.
- Los dispositivos comparten el mismo Ancho de Banda.
- Cuando varias estaciones se conectan por medio de un hub formando un segmento de red, se dice que se ha implementado una topología tipo estrella.

2.2.2 Capa de Enlace

La capa de enlace define cómo los datos deben ser transportados sobre el medio físico, es decir define:

- Direcciones físicas de origen y destino
- Tipo de protocolo usado en la capa superior (punto de acceso al servicio)
- Topología de red
- Secuencia de trama

- Control de flujo
- Tipo de comunicación: orientado a conexión o no orientado a conexión.
- Algunos protocolos de capa 2 son:
- Ethernet (dividido en MAC – 802.3 y LLC – 802.2)
- HDLC (usando la norma V.35 en la capa física)
- Frame Relay (usando la norma V.35 en la capa física)

Como ya se mencionó, entraremos más en detalle con el protocolo Ethernet.

Ethernet

En la capa de enlace se pueden observar dos subdivisiones para este protocolo:

Media Access Control (MAC) (802.3)

La capa MAC de Ethernet abarca tanto la capa física como parte de la capa de enlace del modelo OSI, y define cómo transmitir las tramas sobre el enlace físico, incluyendo lo que se conoce como direccionamiento MAC, por usar direcciones tipo MAC (expresadas en hexadecimal y únicas); topología de red, notificación de error, ordenamiento de tramas y opcionalmente control de flujo.

Logical Link Control (LLC) (802.2)

La capa LLC funciona solamente en la capa 2 del modelo OSI y es responsable de identificar los diferentes tipos de protocolos usados en la capa superior (capa de red) y encapsular la información en tramas. Para esto, hace uso del identificador de punto de acceso al servicio o service access point (SAP).

Es también su función proveer de soporte para conexiones entre aplicaciones en una LAN, control de flujo para la capa superior, así como verificar bits de control de secuencia de tramas.

Sobre los dispositivos usados en la capa de enlace tenemos a los siguientes:

Switch

Un switch es un dispositivo que trabaja a nivel de capa 2, permitiendo unir varios terminales en un mismo segmento de red. Sin embargo, no actúa como simple repetidor o hub si no que manipula la información que recibe por sus puertos, a nivel de tramas, como por ejemplo lee la dirección MAC destino (en el caso de Ethernet) y determina si dicho terminal está conectado a alguno de sus puertos según su propia tabla MAC, si fuera así entonces envía la trama solamente por dicho puerto, mientras que si no puede ubicar la dirección, entonces envía la trama por todos sus puertos.

La tabla MAC a la que se hace referencia en el párrafo anterior, es construida o aprendida por el mismo dispositivo, ya sea un bridge o switch; esta es otra ventaja del switch y bridge sobre un hub. Durante la etapa de aprendizaje del switch, éste escucha todas las tramas que atraviesan el segmento y analiza la dirección origen, de este modo puede saber la ubicación del terminal según el puerto por donde escuchó la trama. Al recopilar esta información, va construyendo su tabla MAC.

El uso de switches y bridges permite también manejar diferentes tipos de redes, como por ejemplo, tener un segmento de red de tipo Ethernet (10 Mbps) y otro de tipo Fast Ethernet (100 Mbps)

Las redes que usan switches tienen las siguientes características:

Cada puerto representa un solo dominio de colisión.

Todos los dispositivos están en el mismo dominio de broadcast.

2.2.3 Capa de Red

La capa de red define como transportar tráfico entre dispositivos que no están conectados localmente, es decir que define los siguientes parámetros:

a.- Direcciones lógicas origen y destino.

b.- El camino a seguir a través de la red

c.- Interconecta múltiples enlaces de datos.

El protocolo más usado en la capa de red es el protocolo IP, el cual utiliza direcciones conformadas por 32 bits agrupados en 4 grupos de 8 bits cada uno, éstas son las direcciones lógicas que se utilizan en la capa de red para poder identificar un terminal de otro y transportar tráfico entre ellos. Más adelante se da un resumen del protocolo IP.

Router

Este dispositivo trabaja a nivel de red del modelo OSI por lo que se puede decir que separa segmentos de red (cada segmento tiene su propia lógica, dominio de colisión y de broadcast).

Entre las principales características del router podemos mencionar las siguientes:

- Separan dominios de broadcast.
- Separan dominios de colisión.
- Determina el mejor camino a seguir por el paquete.
- Manejo de tráfico.
- Direccionamiento local.
- Permite acceso a servicios de WAN.

El router determina cual es el mejor camino a seguir para el paquete de acuerdo a lo que se llaman políticas de enrutamiento, las que pueden tomar diferentes decisiones dependiendo de las características del propio paquete como pueden ser: dirección destino, dirección origen, servicio, puerto de entrada, etc.

Adicionalmente, los routers pueden configurarse de modo que brinden seguridad y parámetros de Calidad de Servicio (QoS) para específicos tipos de tráfico de red.

Además, debido a que el router soporta múltiples protocolos de capa física, es muy utilizado para implementar WAN's, es decir permite interconectividad entre la oficina central y los lugares remotos.

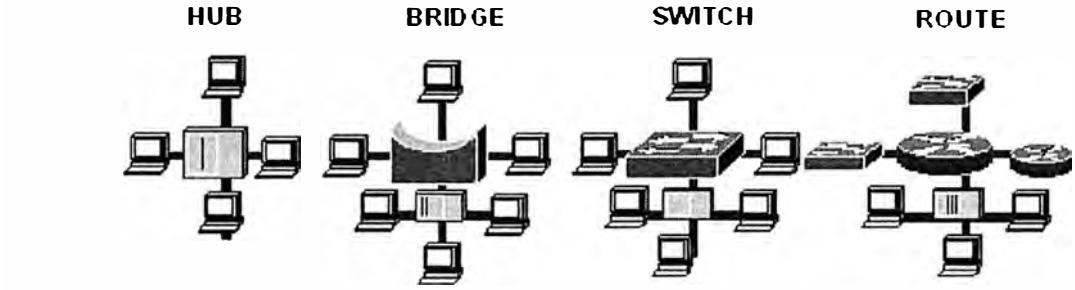

Figura.7 Equipos de Red

	Hub	Bridge	Switch	Router
Dominio de Colisión	1	4	4	4
Dominio de Broadcast	1	1	1	4

Tabla.4 Características de Equipos de Red

2.2.4 Capa de Transporte

La capa de transporte es la que define el establecimiento de la sesión de extremo a extremo. Una sesión constituye una conexión lógica entre la capa de transporte de las estaciones origen y destino.

La capa de transporte especifica las siguientes funciones:

1. Permite a las estaciones extremo ensamblar y desensamblar segmentos de diferentes protocolos de capas superiores en la misma capa de transporte, para lo cual hace uso de identificadores llamados puertos. Por ejemplo: Telnet usa el puerto 23.

2. Permite que las aplicaciones realicen requerimientos confiables de transporte de información, es decir usar un protocolo orientado a conexión, ó por el contrario elegir un servicio tipo connetion less donde lo más importante es que el retardo sea lo menor posible.

Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados a el procesamiento. Además, garantiza una entrega confiable de la información.

Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).

Este nivel define como direccionar la localidad física de los dispositivos de la red.

Asigna una dirección única de transporte a cada usuario.

Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.

Define la manera de habilitar y deshabilitar las conexiones entre losnodos.

Determina el protocolo que garantiza el envío del mensaje.

Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

CAPÍTULO III

ARQUITECTURA DE LA RED IP

3.1 DEFINICIÓN DE LA RED

La red IP es una red de transmisión de datos basada en el uso del protocolo IP (Internet Protocol), ampliamente difundida en Internet, la cual está físicamente implementada con equipos routers, nodos conmutadores, servidores y aplicaciones de software, orientada a dar conectividad a las redes y computadoras que trabajan bajo este protocolo.

La red IP está concebida como una plataforma pública orientada a brindar servicios de esta naturaleza, contando en consecuencia con los recursos y funcionalidades necesarias para permitir un manejo de direcciones IP públicas y privadas, así como proveer la asignación de estas direcciones tanto en modalidad estática como dinámica.

Entre las características de la red IP tenemos:

1. Entregar trafico IP directamente a usuarios residenciales y corporativos
2. Ofrece servicios confiables soportando calidad de servicio (QoS) para cumplir con los requisitos de las aplicaciones.
3. Proporciona comunicaciones con alta seguridad.

4. Soporta una amplia variedad de servicios que cubran las necesidades de la mayoría de usuarios.
5. Proporciona conectividad a nivel nacional para los diversos servicios prestados.
6. Maneja diversos tipos de tráfico, proporcionando capacidad de servicios multimedia.

Sobre el protocolo IP existen múltiples soluciones para las diversas necesidades de los clientes ya sean individuales o corporaciones. Como más relevantes cabe citar los servicios WEB, FTP, Correo Electrónico, Correo Multimedia, Servicios de Directorio, Servicio de Nombres de Dominio, servicios de voz sobre IP, Servicios de encapsulación/transporte de SNA, IPX, X25, y otros protocolos, Tecnología de túneles, Servicios de FireWall, etc...

Sobre estas soluciones se desarrollan los servicios que se proveerán con la red IP. Dichos servicios IP se basan en estándares internacionales desarrollados por el IETF y conocidos como RFC.

La comunicación entre si de los diversos componentes de la red IP se realiza mediante tecnología de altas prestaciones como son:

- Fast Ethernet
- ATM
- MPLS
- Frame Relay

El La red IP se puede conceptuar como dividida en tres niveles diferenciados, el nivel transporte de los paquetes IP entre los diferentes nodos de la red IP se realiza mediante una malla ATM de alto rendimiento y la utilización del protocolo MPLS

para proporcionar calidad de servicio IP y configuración de Redes Privadas Virtuales (VPN).

3.2 MODELO Y ARQUITECTURA DE LA RED

La red IP se puede conceptuar como dividida en tres niveles diferenciados, el nivel de red, el nivel de servicios y el nivel de gestión.

3.2.1 Nivel de Red

Está constituido por los elementos de red necesarios para permitir el acceso de los clientes a la red IP y el transporte de la información entre los nodos, lo cual se puede observar en el gráfico.

POP : Punto de Presencia (Nodo de Acceso)

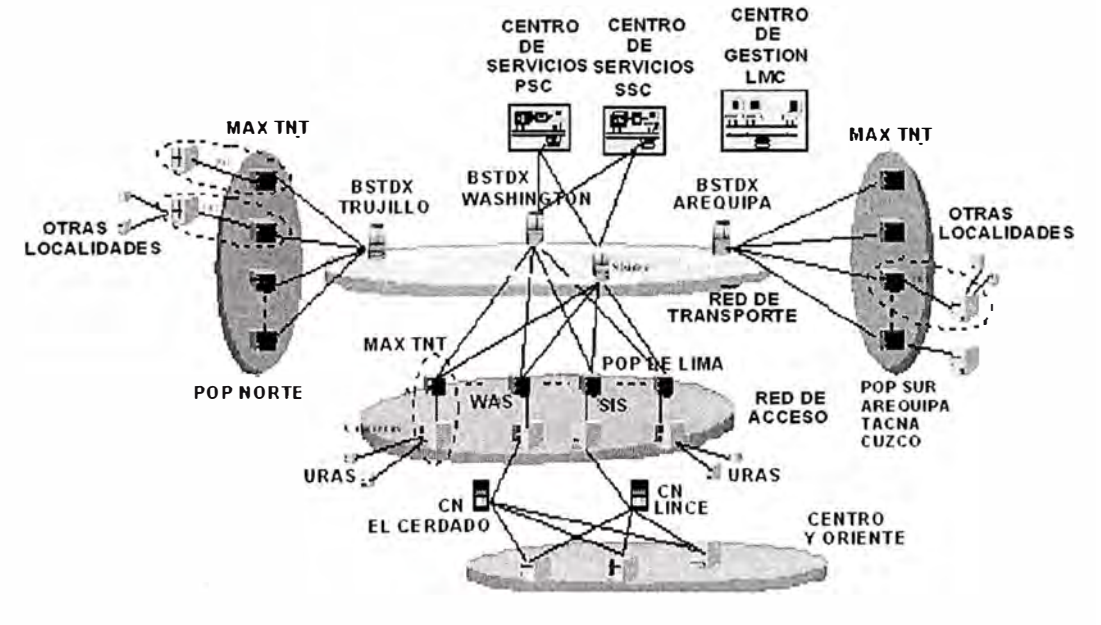

Figura.8 Nodos de la Red IP Conmutada del Perú

Arquitectura de la Red IP

Esta conformada desde los diferentes puntos de acceso hasta la parte del núcleo ó core. Tenemos 2 nodos grandes situados en Lima (Washington y San Isidro) como se puede apreciar en la figura 9.

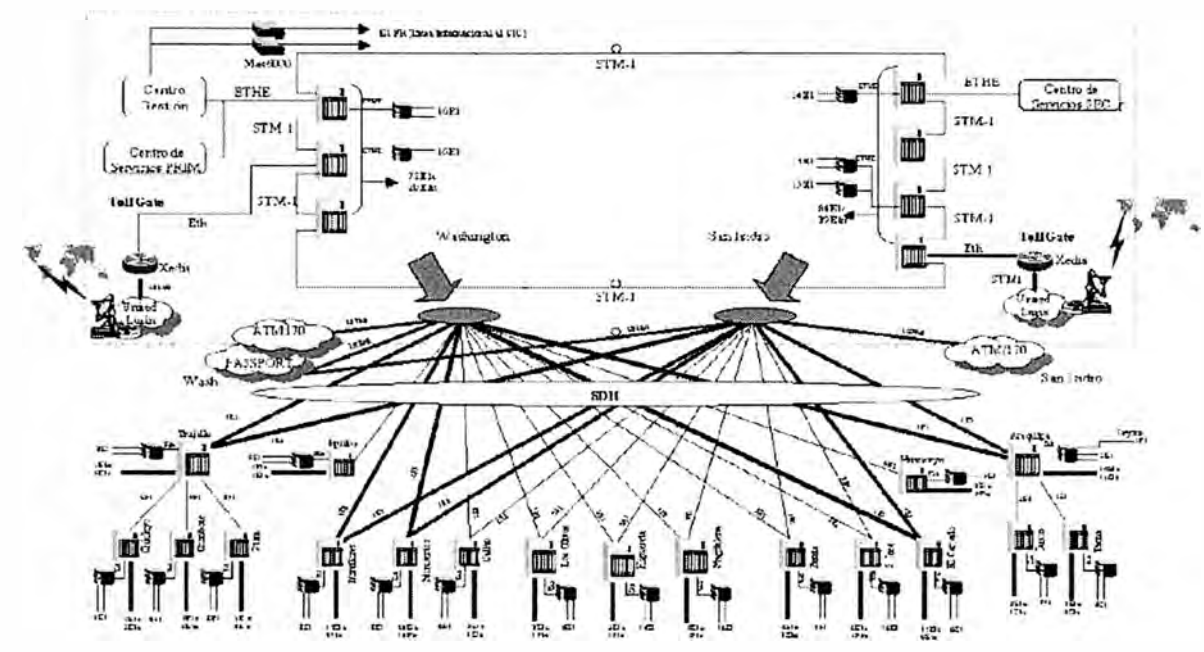

Figura.9 Arquitectura de la Red IP

El nivel de red está compuesto por:

Nivel de Acceso

Constituido por los equipos que permiten el acceso de los clientes a la red, ya sean residenciales, corporativos o CPI's. Estos equipos conforman **los nodos de acceso** de la red IP y realizan la función de interfaz con las diversas redes de acceso (datos, telefonía, celular, CATV, SDH, etc.).

Los Nodos de Acceso proporcionan la interconexión con el equipo de los clientes, ya sean mediante enlaces permanentes o enlaces conmutados. Los accesos permanentes

se realizaran mediante las tecnologías ya existentes (FR, ATM, Punto a Punto) o mediante nuevas tecnologías de acceso de cliente como son ADSL, CATV.

Los accesos no permanentes (conmutados) se realizan de la misma forma que actualmente se hace en el Servicio Infovía, es decir, mediante RTC, RDSI o celular utilizando el protocolo PPP. Este protocolo con sus capacidades avanzadas permite en el caso de RDSI la conexión mediante múltiples canales B conocida como Multilink PPP. De esta forma un usuario que se conecte con un Nodo de Acceso y que posea un acceso básico podrá utilizar sus dos canales B como un único enlace de 128Kbps para acceder a una mayor velocidad a los servicios.

Los Nodos de Acceso (NA) permiten las conexiones de los clientes mediante Frame Relay, ATM, Punto a Punto, CATV, ADSL, Conmutado (RTC, RDSI, celular), etc. con elementos caracterizados para su evolución tanto en escalabilidad, como en versatilidad. Sus routers realizan, entre otras, las funciones de filtrado de acuerdo al perfil de acceso del cliente.

Nivel de Transporte

Conformado por los equipos de red, encargados de transportar y distribuir el tráfico entre los nodos de acceso además proveen los servicios de Frame Relay y ATM.

La red de transporte se emplea para la interconexión de los nodos de acceso, Centros de Servicio y Gateway de acceso Internet. Esta conformada por conmutadores ATM de alta velocidad que permiten el transporte del tráfico IP haciendo uso de protocolos avanzados como el MPLS.

3.2.2 Nivel de Servicios

Conformado por los servidores de la red, ubicados en puntos estratégicos de la red y en los cuales se soportan los servicios ofrecidos a los clientes. Están conformados

por servidores SUN de alta capacidad de procesamiento y configurados en un esquema de alta seguridad y confiabilidad para poder ofrecer los diversos servicios brindados tales como Correo, autenticación, Web, DNS, VPNs, etc).

Contiene todos aquellos servicios que se prestan de manera centralizada y la parte de los elementos de gestión de la red que necesita estar centralizada pero que por cuestiones de ancho de banda de conexión con la red

Consta de los elementos necesarios para proporcionar los siguientes servicios básicos:

- DNS
- Directorio LDAP
- Validación de usuarios
- Tuneles
- Correo Multimedia
- Juegos en Red
- Navegadores
- Audio, Video
- Radius
- NDA
- Seguridad, etc

3.2.3 Nivel de Gestión

Constituido por los equipos que llevan a cabo la gestión y supervisión de los diversos elementos que componen la red de acceso y transporte. Efectúa también la gestión de los clientes y la recogida y preparación de datos para tarificación.

Cada servicio y elemento de la red IP debe ser gestionado, por lo que la red IP incorpora un sistema de gestión integrado, que incluye la atención de clientes, provisión y mantenimiento tanto de la red como de los servicios.

El Centro de Gestión de la Red IP se encarga de la gestión de la infraestructura de red: Nodos de Acceso, Centros de Servicio, Red de Transporte, para ello se apoya en los elementos de gestión, que residen en los elementos de red, y son los que realizan las actuaciones sobre los equipos.

Los elementos de gestion son:

- Navis Core
- Navis Access
- Gestivarios

3.3 EQUIPOS DE RED

3.3.1 MAX TNT

Figura.10 Equipo MAX TNT

Es un conmutador de acceso WAN multiprotocolo que permite construir redes de alta densidad a corporaciones y proveedores de servicios de red.

Forma parte de la red de acceso, permitiendo la conexión de las centrales con la red de transporte(BSTDX) de la red IP lucent.

Este conmutador escalable, de clase portadora, gestiona hasta 720 llamadas concurrentes efectuadas a un equipo central , a través de una mezcla de líneas de acceso analógico, ISDN, T1/E1, DS3 y Frame Relay.

Características:

- El MAX TNT tiene una arquitectura escalable, de tarjetas enchufables y placa madre que proporciona un acceso inteligente para aplicaciones en servicios de red global.
- El sistema modular de tarjeta permite a los usuarios diseñar una solución a los requerimientos específicos de aplicación de ancho de banda.
- La placa madre esta compuesta de tres barras colectoras(bus) independientes: Celdas, TDM y Paquetes(Control).
- Soporta hasta 720 sesiones simultaneas de módem digital, ISDN o Frame Relay de 56/64 kbps. Adicionalmente una placa madre puede terminar hasta 150 líneas arrendadas Frame Relay T1/E1.
- Un subbastidor soporta un máximo de 16 módulos y fuentes de alimentación redundante balanceadoras de carga.
- Un sistema MAX TNT puede ser configurado con un máximo de tres subbastidores, proporcionado redundancia y tolerancia de fallas para aplicaciones en centrales telefónicas.
- El sistema pude ser expandido agregando los siguientes módulos :
- Modulo Digital Módem: Soporte para usuarios analógicos.
- Modulo Hybrid Access: Soporte para ISDN, Switched Digital y Frame Relay canalizado Nx56/64.

- Modulo Frame Line: Soporte para líneas T1/E1 no canalizadas, T1/E1 Fraccionarias y Frame Relay E1.
- Módulos de Interfaz WAN: Conecta lineas de acceso remoto desde la red publica al MAX TNT.
- Módulos de interfaz Backbone: Permiten ruteo variado, equilibrio de carga y redundancia.
- Hace routing manejando protocolos IP.
- Realiza la función de Radius .
- Realiza Tuneles utilizando PPP (protocol point to point)
- Puede trabajar como Gateway.
- Contiene filtros lógicos para todas las conexiones.
- Soporta el protocolo IPDC.

3.3.2 BSTDX

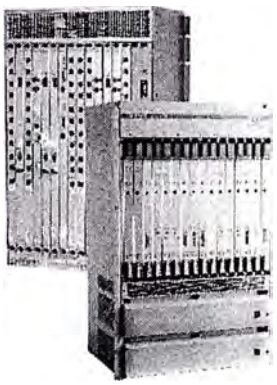

Figura.11 Equipo BSTDX

El BSTDX es un conmutador multiservicio para WAN el cual soporta interfuncionamiento Frame Relay, ATM e IP a ATM, SMDS y RDSI. Tiene una

capacidad de 1,2 Gbps y aporta una alta densidad de puertos, especialmente FR, ofreciendo hasta interfaces STM-1 ATM para acceso de alta velocidad.

El BSTDX proporciona un amplio abanico de posibles servicios generadores de beneficios para compañías suministradoras de servicios, cubriendo Frame Realy, ATM, IP/MPLS y servicios de interfuncionamiento. Los servicios son configurables por software a nivel de puerto lógico, permitiendo de esta manera que múltiples servicios coexistan en una única tarjeta, mejorando la flexibilidad de servicio conjunta, minimizando dependencias hardware y requerimientos de repuestos, y maximizando la rentabilidad del capital invertido.

Interfaces Físicos:

El BSTDX soporta los siguientes tipos de interfaces para IP/FR, IP/ATM o IP/PPP:

En IP/FR se soportan las siguientes velocidades:

- Con V.35 y X.21 se puede llegar a velocidades de hasta 8 Mbps.
- Con HSSI se puede llegar hasta 42 Mbps
- En IP/ATM se soporta:
- Accesos E1, E3 y STM-1 con encapsulado de acuerdo con el estandar RFC 1483.
- En IP/PPP se soportan las siguientes velocidades:
- Accesos E1 a 2 Mbps
- Con V.35 y X.21 a 8 Mbps
- Con HSSI se puede llegar a velocidades de hasta 40 Mbps

Es un conmutador que maneja protocolos de ruteo (RIP, OSPF, BGP) que trabaja a nivel de capa 3 en el modelo OSI.

Equipo de LUCENT que brinda una plataforma para el Frame Relay, SMDS, ATM y otros los cuales serán de vital importancia para el manejo de Redes.

Switch de 1.2 Gb/s de capacidad que realiza interworking de Frame Relay a ATM.

CARACTERISTICAS

- Maneja protocolos de ruteo (RIP, OSPF, BGP) que trabaja a nivel de capa 3 en el modelo OSI.
- Los B-STDX 8000/9000 están conformados por 16 slots (1 slot por tarjeta), y 2 fuentes de alimentación .
- Tienen 2 tarjetas de control (control processor).
- Por cada bastidor se puede colocar hasta 2 B-STDX.
- Trabaja con 48voltios, 23 amperios y 1104 watts.
- Maneja Circuitos virtuales permanentes (PVCs) y Circuitos virtuales conmutados (SVCs).
- Tiene alarmas audibles para fines de trabajo.
- Una aplicación sería trabajar como una Red de transporte, teniendo como Servidor de Acceso Remoto al Max TNT.
- Maneja entradas de :

  E1 de 2.048 Mbps (conector coaxial BNC)

  E3 de 34.368 Mbps (conector coaxial BNC)

  STM1 de 155.52 Mbps (Fibra Optica)

  Ethernet de 10/100 Mbps (RJ-45)

3.3.3 SOFTSWITCH

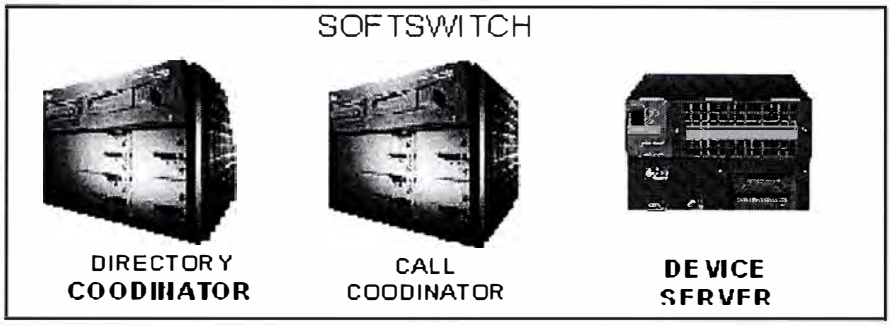

Figura.12 Equipos del SOFTSWITCH

Es un elemento de red, que provee el control de llamadas y manejo de señalización entre redes de paquetes (IP) y redes de circuitos (TDM).

Funciones típicas de manejo de llamadas son: enrutamiento de llamadas, autenticación de usuarios, control de conexiones (conexión y desconexión) y señalización.

El softswitch consta de 3 servidores el Device Server, Call Coordinator y el Directory Coordinator.

El SOFTSWITCH realiza el control de llamadas de Módem (RAS) de forma unificada usando el protocolo IPDC con el Servidor de acceso Remoto

- **DEVICE SERVER :** Es la interface para la señalización con la PSTN.

  Sirve de comunicación con otros softswitches.

  Puede trabajar como Gateway para otros devices
- **CALL COORDINATOR :** Es el que procesa toda la información de señalización intercambiada entre los elementos de red (PSTN y IP) y el Device Server.

El Call Coordinator es el responsable de conectar y desconectar las llamadas.

- **DIRECTORY COORDINATOR :** Es el que maneja el acceso a datos comunes en Bases de Datos, directorios y devices.

  El Directory Coordinator permite al Softswitch el acceso a perfiles de usuario, información de políticas, tablas de ruteo y bases de datos de proveedores de servicio específicos.

3.3.4 ERX

Figura.13 Equipo ERX

Es un router es decir decide a donde enviar cada paquete en función de las direcciones lógicas de red y de algunas variables de la red, como puede ser la densidad de ocupación de los caminos posibles, buscando agilizar al máximo el tráfico.

Puede seleccionar rutas distintas para dos paquetes que vayan al mismo destino, buscando agilizar el tráfico en la red. Esta decisión la realizará según los protocolos de decisión que se utilicen.

CARACTERISTICAS

Puede tener varias direcciones IP, una para cada una de las redes a las que esta conectado.

Se le utiliza como un equipo de borde en la Red el cual maneja diferentes protocolos de ruteo.

Maneja políticas de seguridad de entrada o salida de la red.

Realiza balanceo del tráfico de internet.

3.3.5 CAJUN

Figura.14 Equipo CAJUN

Es un switch utilizado para separar VLANs o unir redes. Físicamente se encuentran en los centro de gestión y servicio.

Puede trabajar como Hub a velocidades de 10 ó100.

3.4 EQUIPOS DE SERVICIO

Esta conformado por los siguientes equipos.

3.4.1 DNS

Figura.15 Equipo DNS

El DNS forma una parte muy importante de Internet que es la resolución de nombres (www.osmosislatina.com) a nodos IP (213.123.123.1) , para esta resolución se utiliza el software llamado BIND ("Berkeley Internet Name Domain") que esta disponible en varias versiones de Unix e inclusive en plataformas Windows.

La localización de un sitio en internet y el envío de correo electrónico dependen de esta resolución.

BIND soporta un número de métodos diferentes para proteger la actualización y zonas de transferencia, en los servidores de nombres maestro y esclavo uno de ellos es el DNSSEC.

DNSSEC: Abreviación de DNS SECurity, esta propiedad permite firmar con caracteres criptográficos zonas con una clave de zona.

De esta manera, puede verificar que la información de una zona provenga de un servidor de nombres que la ha firmado con caracteres criptográficos con una clave privada, siempre y cuando el recipiente tenga esa clave pública del servidor de nombres.

Funcionamiento

El Servidor de Nombres (name server) es un programa que forma la parte servidor del mecanismo cliente-servidor del DNS. Los Servidores de Nombres contienen información sobre un determinado segmento de la base de datos y la hace disponible para clientes (clients), denominado Resolver. Los **Resolvers** muchas veces consisten sólo en rutinas de librerías, que crean interrogaciones y las mandan a través de la red a un Servidor de Nombre.

La base de datos se muestra en figura 16. La totalidad de la base de datos se muestra como un árbol (tree) invertido con la raíz (root) en la punta. El nombre de la raíz es la etiqueta NULL, pero se escribe con un solo punto ("."). Cada nudo del árbol representa tanto una partición de la totalidad de la base de datos, como un Dominio (domain) del Sistema de Dominio de Nombre.

En adelante cada dominio puede ser dividido en particiones que se llaman Subdominios (subdomains), que son derivados como niños de sus nudos paternales.

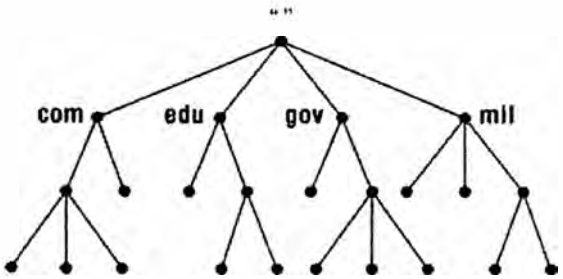

Figura.16 La base de datos del DNS

En el DNS, el nombre de dominio completo es una secuencia de etiquetas, empezando por el dominio hasta la raíz (root), separando las etiquetas por puntos "." (por ejemplo: einstein.matematicas.ac.edu).

Permitiendo que cada dominio puede ser administrado por una organización diferente. Cada organización puede dividir su dominio en varios subdominios, cuya administración puede ser realizada por otras organizaciones.

El Network Information Center p. ej. administra el dominio "edu" (educational) pero pasa la autoridad sobre el subdominio "ac.edu" (academic) a la Universidad, la cual autoriza al instituto de matemáticas para administrar el siguiente subdominio: "físicas.ac.edu" (Figura 17).

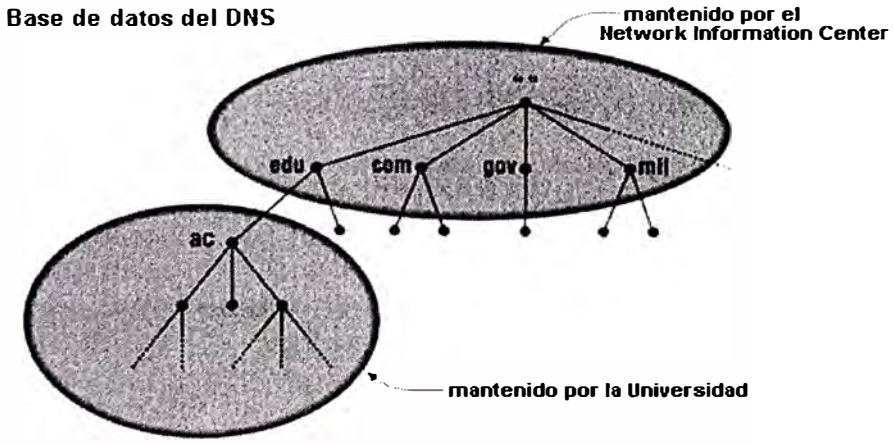

Figura.17 El mantenimiento de subdominios

Finalmente queda mencionar que un dominio puede contener tanto subdominios como hosts. Cada host en una red tiene un Nombre de Dominio que posee la información sobre el host, así como la dirección IP o como va el Routing de correo, etc.

Las organizaciones de un dominio son libres de elegir nombres dentro de su dominio. No importa cual nombre sea usado, es seguro que no causa conflicto con otro nombre, porque tiene su Nombre de Dominio único adjuntado al final. De este modo pueden existir dos hosts con el nombre Einstein en su Universidad, por ejemplo, paquetes de einstein.fisicas.ac.edu siempre van a encontrar su camino a einstein.matematicas.ac.edu, porque se trata de dominios paternales diferentes.

Importancia

Para resolver nombres de dominio y direcciones IP y para poder ubicar hosts de redes lejanas. Como fue mencionado antes, es más fácil recordar nombres en vez de cifras. Sobre todo cuando se trata de una cantidad de direcciones tan inmensa como la Internet.

Las computadoras por otro lado trabajan perfectamente con cifras como la dirección IP. Lo que sucede cuando usted entra a la Internet colocando una dirección como p. ej. http://www.altavista.com, es que su navegador dirige una petición (request) al Servidor de Dominio de su proveedor y este intenta resolver el nombre de dominio con la IP correspondiente.

(Detallamos una busqueda con la dirección "einstein.matematicas.ac.edu" en la Figura 18).

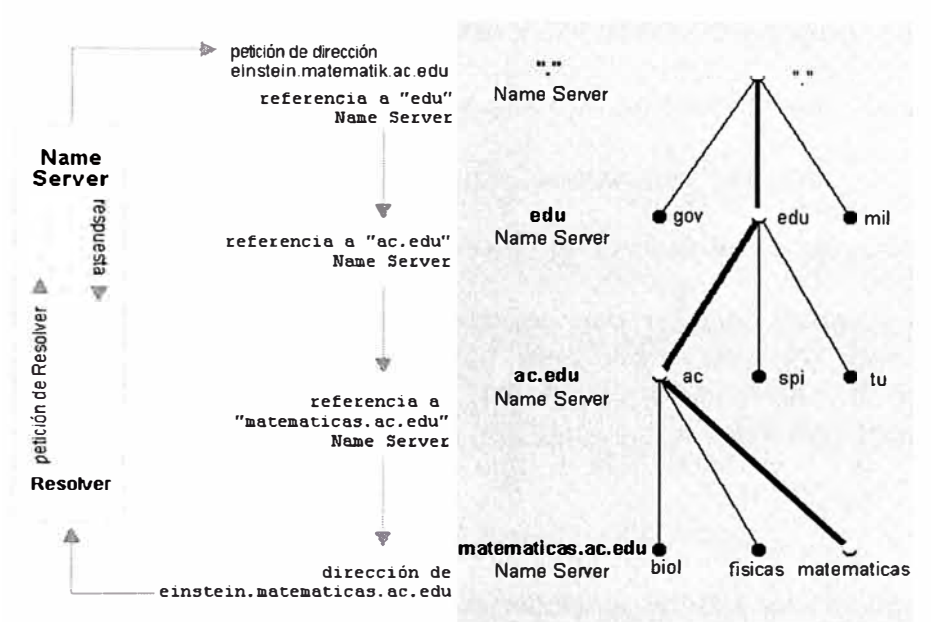

Figura.18 La resolución de einstein.matematicas.ac.edu en la Internet

Esto significa que cada servidor de dominio tiene la información completa de la zona para que esta autorizado y aparte tiene informaciones básicas sobre otras zonas. Cuando una petición (request) se dirige a una zona que esta fuera de la zona autorizada, su servidor por lo menos sabe por donde buscar. Esto puede significar que la petición (request) de una dirección tiene que pasar por varios Servidores de Dominio hasta que usted tenga contacto con el destino solicitado.

Aunque usted supiera la dirección IP del destino, es imprescindible consultar otros Servidores de Dominio si su computadora no se encuentra en la misma zona. De este modo es fácil de imaginar porque el Sistema de Dominio de Nombre no puede consistir en una sola base de datos centralizada. Primero tardaría demasiado tiempo encontrar un servidor entre millones de otros y segundo habría una cola bastante larga en el caso de miles de peticiones simultáneas de todo el mundo. Adicionalmente no tendría sentido dirigirse a un servidor lejano para comunicar con un host de la misma zona.

Hasta ahora hablamos del mapeo de nombres a direcciones. Pero, que sucede si usted de repente tiene la dirección IP y desee saber el nombre de este dominio. Para solventar este problema fue creado el dominio "in-addr.arpa". (Figura 19)

Este dominio es llamado dominio inverso y la resolución de direcciones IPs a nombres de dominio se denomina mapeo reverso (reverse mapping o reverse lookup). Un ejemplo: Nos recordamos que la IP de Einstein del instituto de matemáticas es "149.176.12.7" con el nombre de dominio "einstein.matematicas.ac.edu".

El dominio "matematicas.ac.edu" entonces tendrá el nombre de dominio inverso: "12.176.149.in-addr.arpa" y la computadora einstein.matematicas.ac.edu correspondientemente esta realizada con "7.12.176.149.in-addr.arpa".

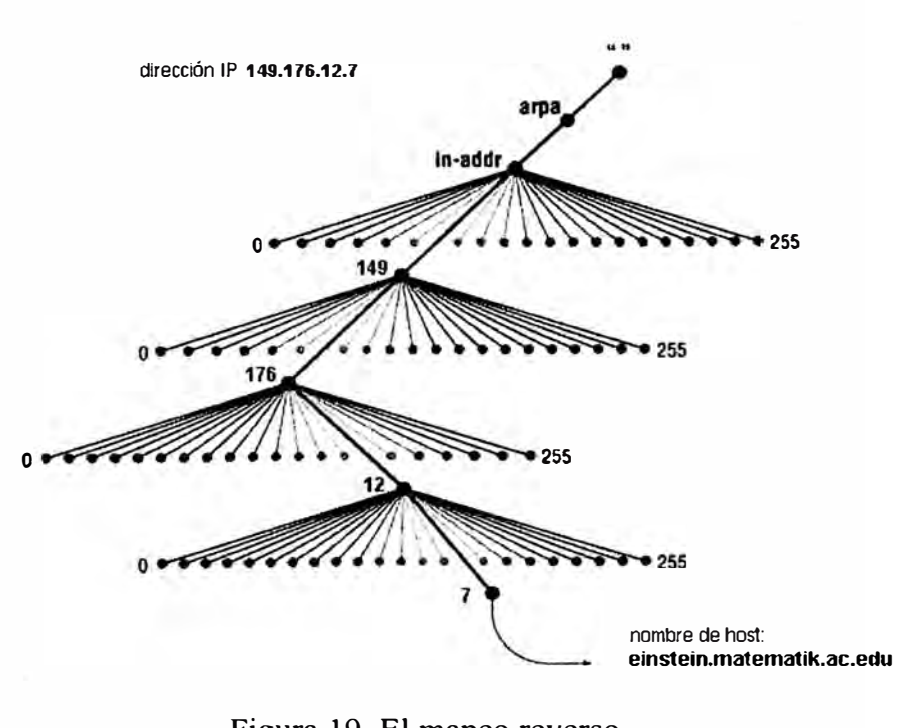

Figura.19 El mapeo reverso

3.4.2 LDAP

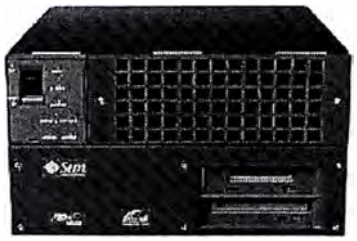

Figura.20 Equipo LDAP

LDAP (Lightweight Directory Access Protocol) es un estándar abierto para los servicios globales o locales en una red y/o en Internet. Un directorio, gestionado desde el protocolo LDAP se parece a una guía telefónica. LDAP puede gestionar mucha otra información, pero actualmente se utiliza principalmente para asociar nombres a números de teléfono con los dominios de los usuarios. Los directorios soportan un gran volumen de tráfico, pero los datos en los directorios después no cambian tan a menudo.

LDAP es un sistema cliente-servidor. Un cliente LDAP se conecta a un servidor LDAP y requiere de información o proporciona los datos necesarios para acceder a un directorio. El servidor responde a la solicitud, envía la consulta a otro servidor o acepta la información para incorporarla al directorio

La ventaja principal de usar LDAP es la consolidación de cierto tipo de información en el interior de su empresa. Por ejemplo, todas las diferentes listas de usuarios en el interior de su empresa pueden ser fusionadas en un solo directorio LDAP. Este directorio, a continuación, podrá ser consultado desde cualquier aplicación LDAP-enabled a la que le sirva la información. El directorio también podrá ser utilizado por los usuarios que necesiten información sobre el.

LDAP también es capaz de replicar su información a otros LDAPs, esto facilita la disipación de información para la redundancia:

3.4.3. RADIUS

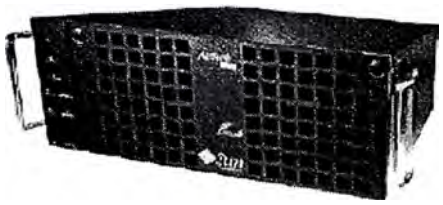

Figura.21 Equipo RADIUS

El Servidor Radius proporciona una solución AAA (Authentication, Authorization and Accounting) y se encarga de autenticar los usuarios que acceden a través de RAS así como otras funcionalidades inherentes de estos servicios tales como el control del número máximo de conexiones con los ISPs,etc. El Servidor Radius de Lucent permite integrar estructuras flexibles de AAA con entornos de red existentes. Los módulos conectables también se usan para proporcionar interfaces a datos tales como directorios de usuarios (UNIX password file, LDAP, ficheros de texto), contabilidad y bases de datos El RADIUS Accounting se encarga de llevar la contabilidad detallada de cada usuario, bases de datos de asignación de direcciones (address assignment pools), y bases de datos de configuración .

Para la gestión el Servidor Radius dispone de los siguientes sistemas de acceso:

CLI. Se implementa desde una aplicación de Java

Telnet . Permite acceso desde un centro remoto

WEB Server. Permite el acceso desde cualquier web browser.

La configuración del NavisRadius se realiza por comando.

En la modalidad de autenticación en Red las funciones de Autenticación de usuarios las realiza el Servidor Radius de la Red IP. Las funciones de asignación de direcciones IP las realiza el MAX-TNT bajo control del Servidor Radius de la Red IP.

El control del límite de sesiones, tanto por cliente como por usuario, se realiza mediante el USS. El USS es una aplicación incluida en el Servidor Radius de Lucent, corre en una aplicación independiente del Servidor Radius y se configura para un puerto TCP/IP pudiendo soportar varios Servidores Radius.

El USS se usa para limitar el número de accesos al servicio mediante restricción del número de peticiones de autenticación al servidor Radius.

3.4.4 NDA

Es un servidor que levanta un entorno grafico para dar de alta y baja a los usuarios inscritos en el LDAP. Trabaja directamente con el LDAP.

Utiliza un entorno Web para la configuración de los usuarios.

3.4.5 FIREWALL

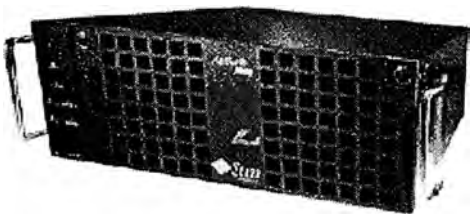

Figura.22 Equipo FIREWALL

Es un servidor que tiene la función de darle seguridad a las Redes de Gestión y Servicio.

Su labor es de proteger de ataques o ingresos no debidos a las redes de gestión y servicios mediante políticas aplicadas a la LAN.

Para esto necesitamos que todos los servidores tengan como puerta de enlace (gateway) al firewall.

3.5 EQUIPOS DE GESTION

Son aquellos que llevan a cabo la gestión y supervisión de los diversos elementos que componen la red de acceso y transporte. Efectúa también la gestión de los clientes y la recogida y preparación de datos para tarificación.

Cada servicio y elemento de la red IP debe ser gestionado, por lo que la red IP incorpora un sistema de gestión integrado, que incluye la atención de clientes, provisión y mantenimiento tanto de la red como de los servicios.

El Centro de Gestión de la Red IP se encarga de la gestión de la infraestructura de red: Nodos de Acceso, Centros de Servicio, Red de Transporte, para ello se apoya en los elementos de gestión, que residen en los elementos de red, y son los que realizan las actuaciones sobre los equipos.

El equipos de Gestión de la Red IP están basados en las plataformas Navis Core, Gestivarios, Navis Access y los restantes elementos de interconexión como conmutadores y Firewalls.

A continuación se indican las funcionalidades principales de dichas plataformas instaladas en nuestra red IP.

3.5.1 NAVIS ACCESS

Figura.23 Equipo NAVIS ACCESS

Este elemento permite gestionar los equipos de la Red IP y monitorear el rendimiento de los mismos, detectando las fallas en cualquiera de los routers, conmutadores y dispositivos de acceso. Este software es soportado sobre los siguientes sistemas operativos: Solaris y Windows .

Esta aplicación realiza funciones de gestión de elemento del MAX-TNT. El Software NavisAccess se usa para gestión de red de acceso, Puntos de Presencia (POPs) y redes de empresa. NavisAccess incluye funcionalidad de detección de elementos de red, gestión de configuración, gestión de las prestaciones (performance), y gestión de fallos desde una visión de red global hasta una visión detallada al nivel de puerto.

Realiza lo siguiente:

- Gestiona MAX-TNT
- Gestión de fallos Max-TNT
- Gestión de Rendimiento y configuraciones de Max-TNT
- Call Loging (mensajes de log de los MAX-TNT)

En el Navis Access 5.0 aparece el concepto de Call receivers encargados de recibir los paquetes de accounting "Call Loging" y reenviarlos de forma periódica a una base de datos centralizada que correla los datos y permite obtener las estadísticas.

3.5.2 NAVIS CORE

Figura.24 Equipo NAVIS CORE

Es un servidor Sun Netra 1200 el cual gestiona a los BSTDX de la Red IP.

Proporciona Provisión para cada BSTDX (crea nuevos nodos, rutas estáticas, conexiones nuevas, etc). Recepción de alarmas de BSTDX la cual la realiza vía snmp.

En el se muestra los diferentes nodos que existe a nivel nacional y sus conexiones con los 2 nodos principales en LIMA. (Figura 25)

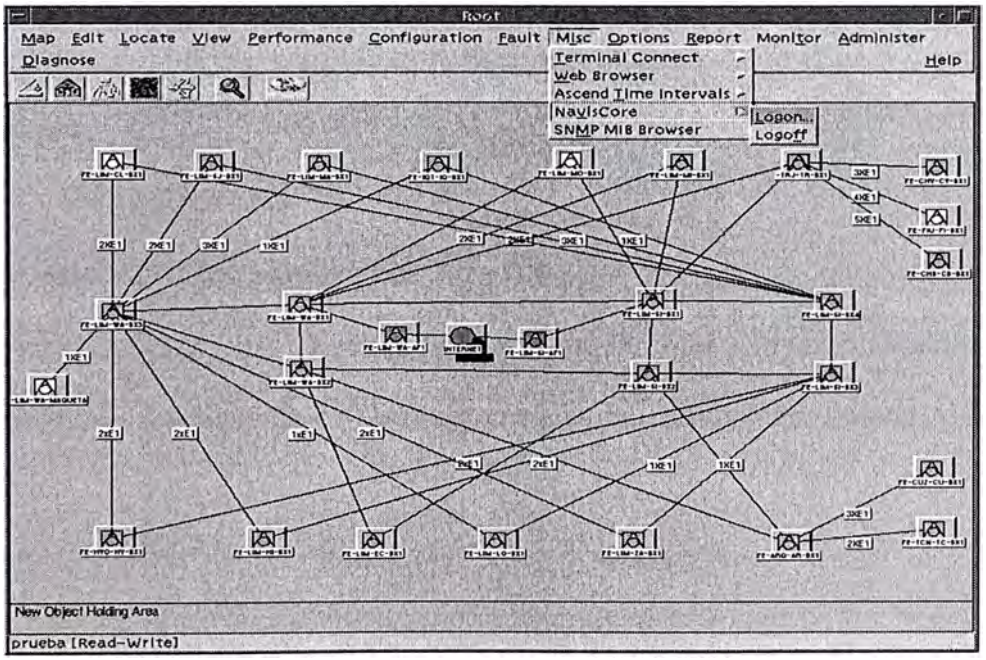

Figura.25 Entorno Gráfico del NAVIS CORE

3.5.3. GESTIVARIOS

Figura.26 Equipo Gestivarios

Es un equipo que pertenece a la gestión de la Red IP siendo su función principal recibir todos los mensajes de los equipos de la Red de Servicio incluyendo a los MAX TNT y BSTDX.

Dichos mensajes o logs de los equipos son mostrados en un entorno gráfico y se actualizan en forma inmediata.

El Gestivarios es un servidor que tiene instalado el Net BackUp, el cual permite realizar al administrador copias de respaldo y restaurar los archivos principales del sistema. Estas copias de respaldo se realizarán en forma automática a determinadas horas del día.

3.5.4. TERMINALES

Son maquinas SUN Netra con solaris 2.6 y 2.8.

Actualmente tenemos 7 maquinas para la gestión de la Red en su totalidad desde las cuales podemos displayar la s interfaces graficas del Navis Core, Navis Access y el Gestivarios.

Accedemos al resto de servidores via telnet o security shell desde el cual se le realiza mantenimiento preventivo y correctivo según sea el caso.

Adicionalmente desarrollamos aplicativos para optimizar los trabajos de rutinas.

CAPÍTULO IV

FUNCIONAMIENTO DE LA RED IP

4.1 TOPOLOGÍA DE LA RED IP

4.1.1 Descripción de la Topología de la Red IP

La topología de la Red IP se ha dividido en cuatro zonas, siendo estas: la zona norte, la zona sur, zona centro/oriente y la zona de Lima, las cuales incluyen todos los departamentos del país.

Para llevar a cabo la incorporación de cada localidad en la zona más conveniente de la red IP se consideraron los siguientes criterios:

Los actuales recursos de red con que cuenta cada localidad. (Cabeceras, URAS, etc.)

Las rutas de interconexión actuales para concentrar el tráfico telefónico.

Las proyecciones de crecimiento del volumen de tráfico hacia Internet.

El objetivo de brindar granularidad a la red IP.

Las consideraciones antes mencionadas permitieron configurar las zonas de la siguiente manera:

Zona Norte:

En esta zona se concentra el tráfico de accesos a la Red IP de : Tumbes, Cajamarca, Huaraz, Chimbote, Piura, Chiclayo y Trujillo. En cada una de estas cabeceras se

instalaron un Servidor de Acceso (MAX TNT), el cual cumple dos funciones muy importantes.

Concentra el tráfico destinado a la Red IP

Adapta (codificar, comprimir, etc) los canales de 64 Kbps recibidos de la RTC a través de los enlaces E1 entre el Servidor de Acceso y la Cabecera correspondiente.

Adicionalmente, el CN de Trujillo concentra el tráfico IP de las siguientes localidades: Huaraz, Tumbes y Cajamarca, lo que permite orientar el tráfico de accesos IP correspondiente a estas localidades hacia la Cabecera ubicada en Trujillo y lograr el acceso a la Red IP, a través del Servidor de Acceso (MAX TNT) de Trujillo.

Finalmente, los cuatro Servidores de Acceso de la Zona Norte se interconectarán a un Conmutador ATM del Core (BSTDX) de la red ubicado también en Trujillo, el cual forma parte del Backbone de la Red IP a nivel nacional, permitiendo de esta manera integrar la Zona Norte a la Red IP y por consiguiente brindar el acceso a Internet.

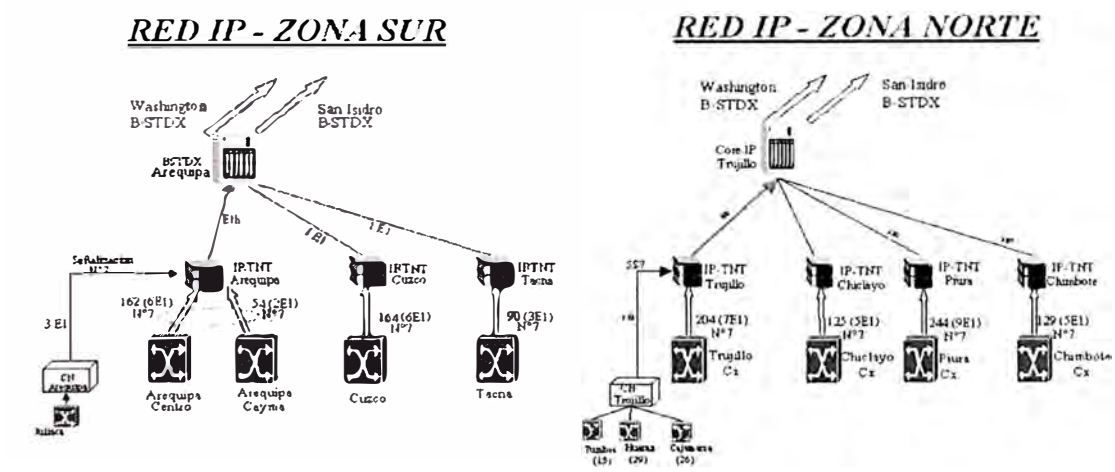

Figura.27 Accesos Zonas Norte y Sur

Zona Sur:

En esta zona se concentra el tráfico de accesos a la Red IP de Tacna, Cusco, Arequipa, Cayma, y Juliaca. En cada una de estas cabeceras se ha instalado un Servidor de Acceso (MAX TNT), que cumple las funciones descritas en el caso de la zona norte.

Es importante mencionar que el Servidor de Acceso de Arequipa concentra el tráfico de accesos IP de las Cabeceras Arequipa Centro y Cayma.

Adicionalmente, el CN de Arequipa concentra el tráfico IP de Juliaca, lo que permite orientar el tráfico de accesos IP correspondiente a esta localidad hacia la Cabecera ubicada en Arequipa y logra el acceso a la Red IP, a través del Servidor de Acceso (MAX TNT) de Arequipa.

Finalmente, los tres Servidores de Acceso de la Zona Sur se interconectan a un Conmutador ATM del Core (BSTDX) de la red ubicado también en Arequipa, el cual formará parte del Backbone de la Red IP a nivel nacional, permitiendo de esta manera integrar la Zona Sur a la Red IP y por consiguiente brindar el acceso a Internet.

Zona Centro/Oriente:

Esta zona recopila el tráfico de las siguientes localidades: Iquitos, Huancayo, Pucallpa, Tarapoto, Tarma, Ayacucho, Huanuco, Ica, Quillabamba y Puerto Maldonado. En las Cabeceras de Iquitos y Huancayo se instalaron Servidores de Acceso (Max TNT) para concentrar los accesos a la Red IP, a su vez estos dos Servidores están interconectados con el Conmutador ATM del Core de la red ubicado en Washington.

El resto de las localidades pertenecientes a esta Zona, es decir, Puerto Maldonado, Quillabamba, Huanuco, Ica, Ayacucho, Tarma, Tarapoto y Pucallpa direccionarán su tráfico IP en doblete hacia las CN de Lince y El Cercado, las que a su vez están interconectadas en doblete con las Cabeceras de Washington y Miraflores, en donde se contará con Servidores de Acceso (Max TNT) enlazados a dichas cabeceras para concentrar el tráfico de accesos IP de las localidades mencionadas e integrar la Zona Centro/Oriente al Backbone de la Red IP y por consiguiente brindar el acceso a Internet.

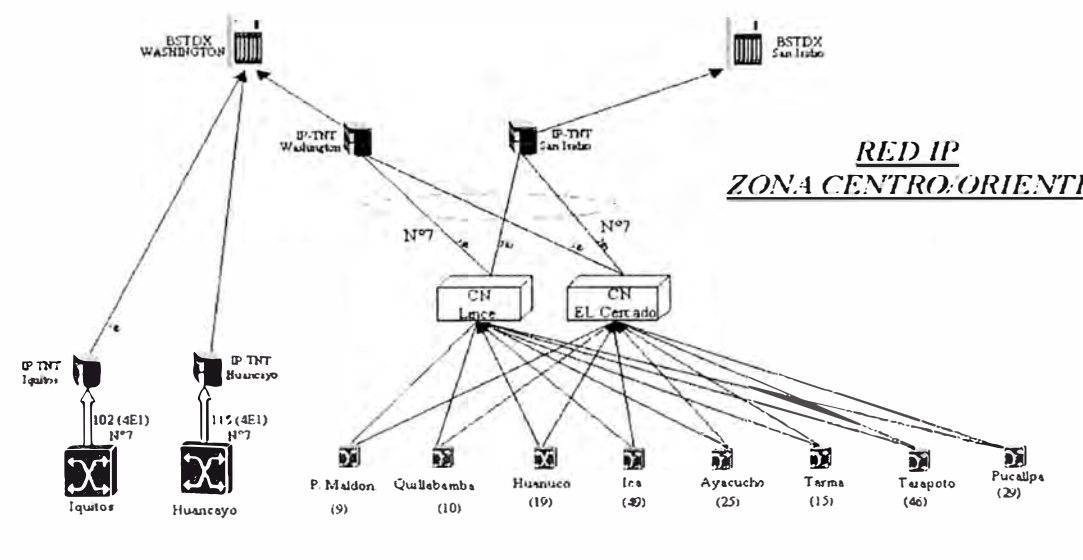

Figura.28 Acceso Zonal Centro/Oriente

Zona de Lima:

Esta zona es de gran relevancia dentro de la Topología de la Red IP, debido a que presenta el mayor volumen de tráfico IP, tanto de accesos a Internet como el funcionamiento de Redes Corporativas (Intranets) basadas en IP lo cual nos obliga a brindar un mayor despliegue de recursos de red.

Se instalaron Servidores de Acceso (MAX TNT) en cada una de las once (11) Cabeceras de Lima, para interconectarlos con la respectiva Cabecera y concentrar el tráfico de accesos IP de cada localidad.

Las Centrales NEAX de San Juan de Miraflores, San Borja, Lince y Barranco accederán a la Tandem de San Isidro la que llevará los accesos IP a la Cabecera de Miraflores; de igual manera las Centrales NEAX de La Victoria y Santa Rosa se estarían encaminando a la Tandem de Washington y de allí a la Cabecera de Washington que estará interconectada al Servidor de Acceso (MAX TNT).

Finalmente, cada uno de los Servidores de Acceso desplegados en las once Áreas de cabecera de Lima estará interconectado en doblete a los dos Conmutadores ATM del Core de la red uno ubicado en Washington y el segundo en San Isidro. Dicha interconexión permite contar con la redundancia requerida para el caso extremo de caída de uno de los nodos Conmutadores del Backbone. Es importante mencionar que los Conmutadores de Washington y San Isidro están enlazados al Centro de Servicios de Washington y al Centro de Servicios de San Isidro.

De esta manera se esta integrando todo el tráfico de Accesos IP de la Zona de Lima a la Red IP brindando el acceso a Internet.

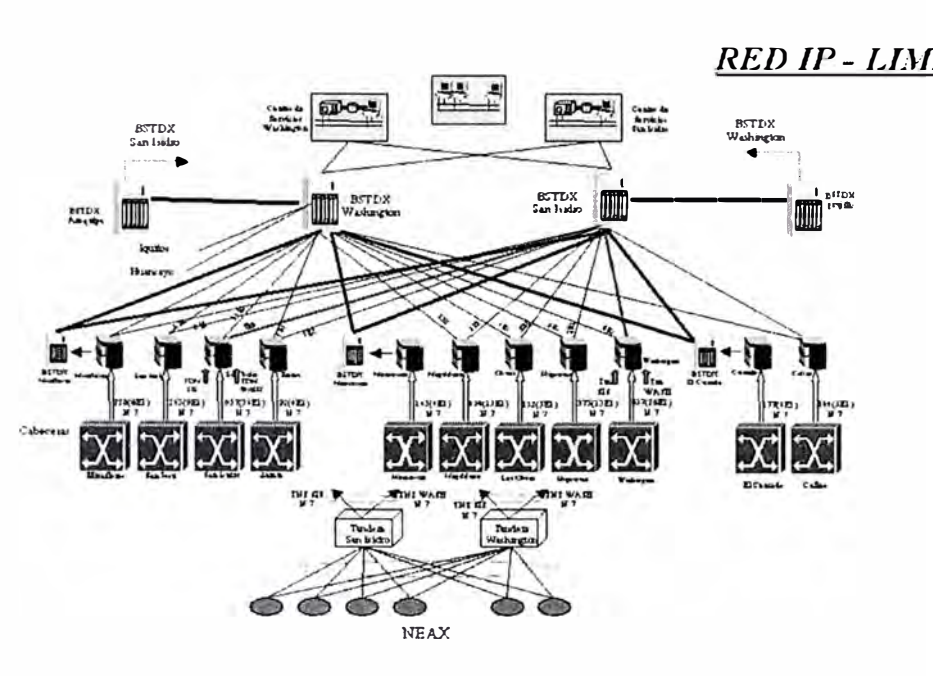

Figura.29 Acceso Zonal LIMA

4.1.2 Nodos

El despliegue de la Red IP se encuentra a nivel nacional, para lo cual se instalaron nodos de acceso en Lima y provincias, de acuerdo a los siguientes lineamientos:

En Lima : En todas las áreas de cabecera se instalaron nodos de acceso, cursándose el tráfico hacia los nodos de transporte y liberando el tráfico por los canales de voz hacia las centrales de tránsito.

En provincias : Se desplegaron nodos de acceso en las capitales de departamentos y en las principales localidades. De esta manera se eliminaron el tráfico de voz a través de los circuitos de larga distancia para el acceso a Internet y a los proveedores de información locales.

Adicionalmente al despliegue de nodos de acceso, se empezaron gradualmente a migrar los usuarios de Infovía hacia la nueva Red IP. Esto se realizará hasta desmontar completamente los centros de servicios Infovía existentes.

Esquema de numeración para acceso conmutado

- Las llamadas de acceso a la Red IP son concentradas por la red telefónica en accesos primarios RDSI atendidos por los servidores de acceso de los nodos de acceso (NA) o puntos de presencia (POP).
- En cada punto de presencia se asignó un número local para acceso al servicio, evitando de esta manera posibles problemas legales y/o económicos motivados por el uso de recursos de larga distancia.
- Para mantener el costo de la llamada local para los usuarios del servicio, se realizó un despliegue geográfico de Nodos de Accesos que cubrieron la mayoría de localidades con alta demanda del servicio a un costo razonable.
- En las localidades en que por el tráfico no se disponga de un Nodo de Acceso, se asignará un numero de la localidad y mediante la facilidad de desvío de llamada, esta se transferirá a un número de la localidad más cercana que cuente con un punto de presencia.

Velocidades de Acceso

- Las velocidades ofrecidas para este tipo de acceso son:
- Hasta 56 Kbps para acceso vía RTC.
- Para acceso vía RDSI:
- 64 Kbps bidireccional con un único canal B del acceso básico.
- 128 Kbps bidireccional agregando los dos canales B del acceso básico RDSI utilizando Multilink PPP (MPPP).

Estos accesos usan PPP como nivel de enlace y autenticación por PAP o CHAP. En cuanto a la asignación de direcciones IP al terminal de usuario, esta es siempre

dinámica y posterior a la identificación del usuario, facilitando así la asignación de direcciones dependiendo del perfil de usuario.

4.2 DIAGRAMAS

A continuación en diagrama de la Red IP compuesta por 2 centros de servicio y 1 centro de gestión.

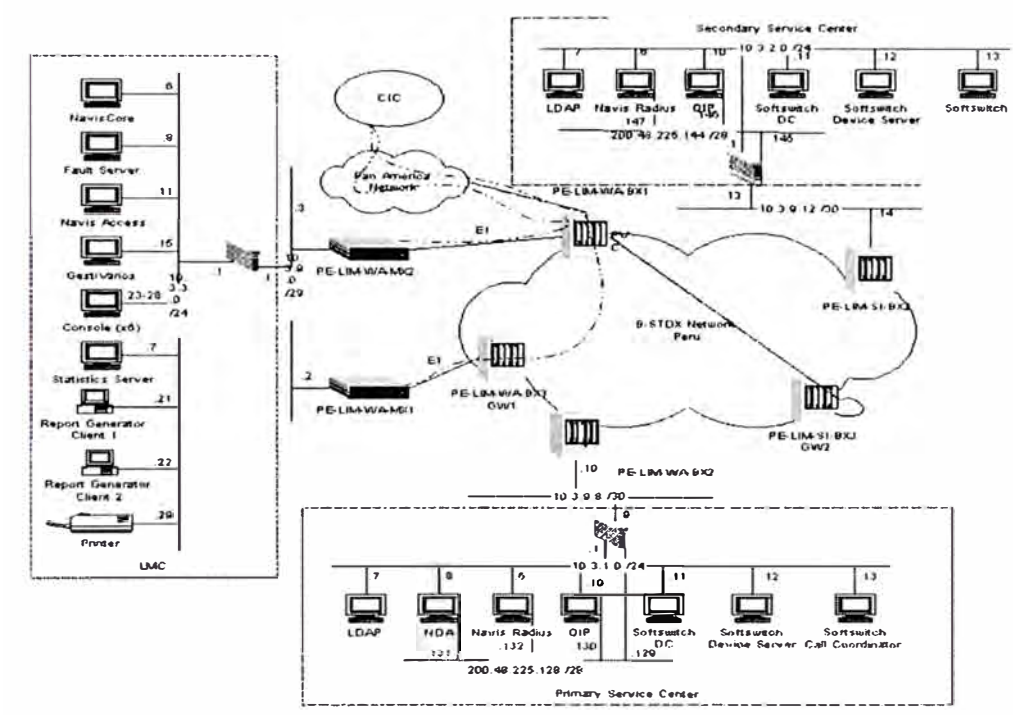

Figura.30 Diagrama de los Centros de Servicios y Gestión

4.2.1 Centro de Servicios

Este nivel es el que proveerá todo el manejo de funcionalidades para la provisión de los servicios que se brindarán con la Red IP. Esta compuesto por los Servidores SUN, el software especializado y el RADIUS que efectúe las funciones de autorización, autenticación y contabilidad.

En la Red IP tenemos 2 centros de servicios

Centro de Servicios Primario

Centro de Servicios Secundario

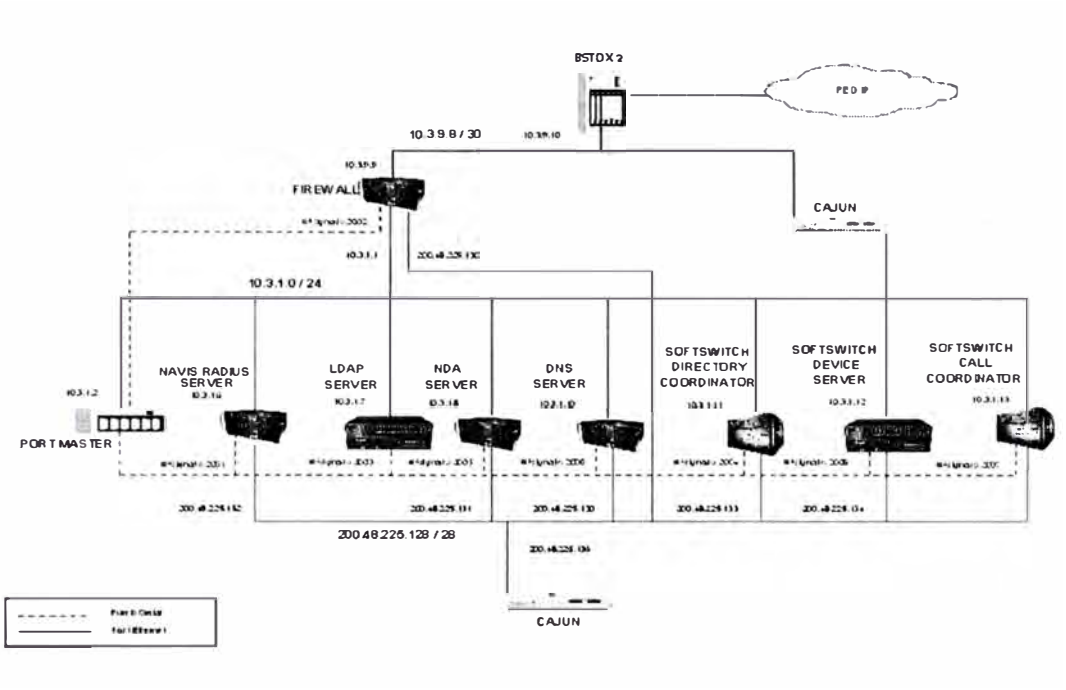

Figura.31 Diagrama del Centro de Servicio Primario

En el Centro de servicios Primario la conforman los siguientes equipos:

- 1 Port Master : para acceso a cualquier servidor por consola remotamente.
- 1 Navis Radius : para la autenticación, autorización y contabilidad.
- 1 LDAP : para almacenar la base de los usuarios de los servicios propios.
- 1 NDA : para dar de alta o baja a los usuarios del LDAP.
- 1 DNS : para realizar las resoluciones de nombres y resoluciones inversas.
- 1 SOFTSWITCH : conformado por 3 servidores para la señalización.
- 1 Firewall : para darle seguridad a la red de servicios.

Centro de Servicio Secundario

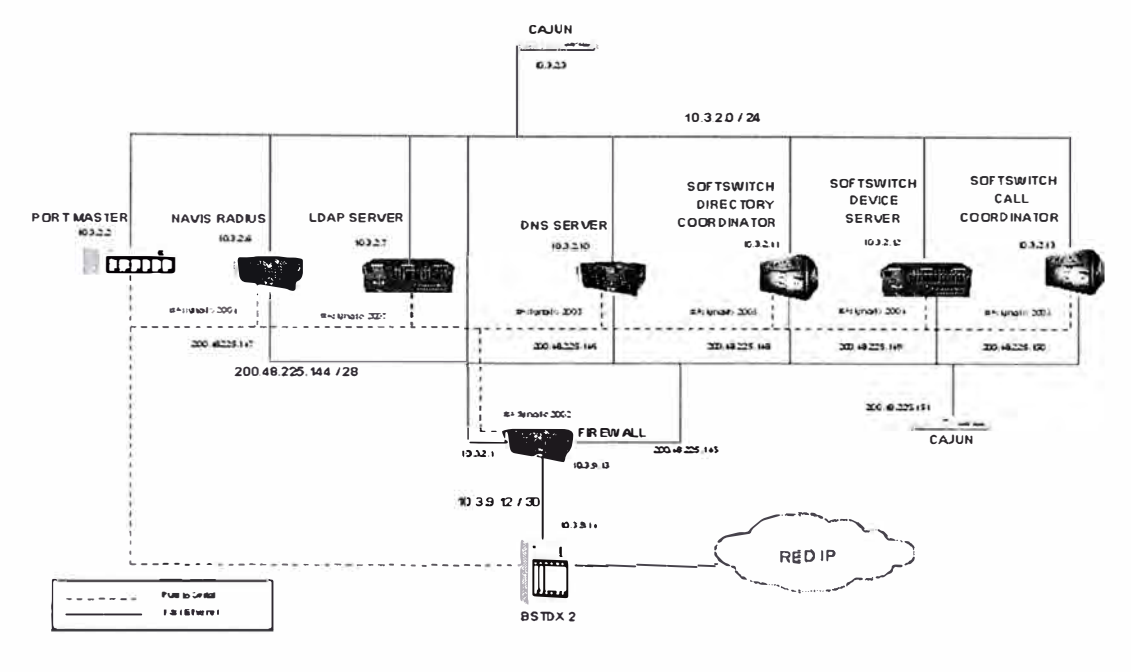

Figura.32 Diagrama del Centro de Servicio Secundario

En el Centro de servicios secundario es utilizado como un respaldo del centro de servicios primario y la conforman los siguientes equipos:

1 Port Master : para acceso a cualquier servidor por consola remotamente.

1 Navis Radius : para la autenticación, autorización y contabilidad.

1 LDAP : para almacenar la base de los usuarios de los servicios propios.

1 DNS : para realizar las resoluciones de nombres y resoluciones inversas.

1 SOFTSWITCH : conformado por 3 servidores para la señalización.

1 Firewall : para darle seguridad a la red de servicios.

4.2.2 Centros de Gestión

Este nivel requiere de los elementos de software y hardware, que soporten las herramientas que permitan efectuar las labores propias de gestión, es decir, control y supervisión de la red.

El Centro de Gestión estará ubicado en Surquillo y estará conformado por:

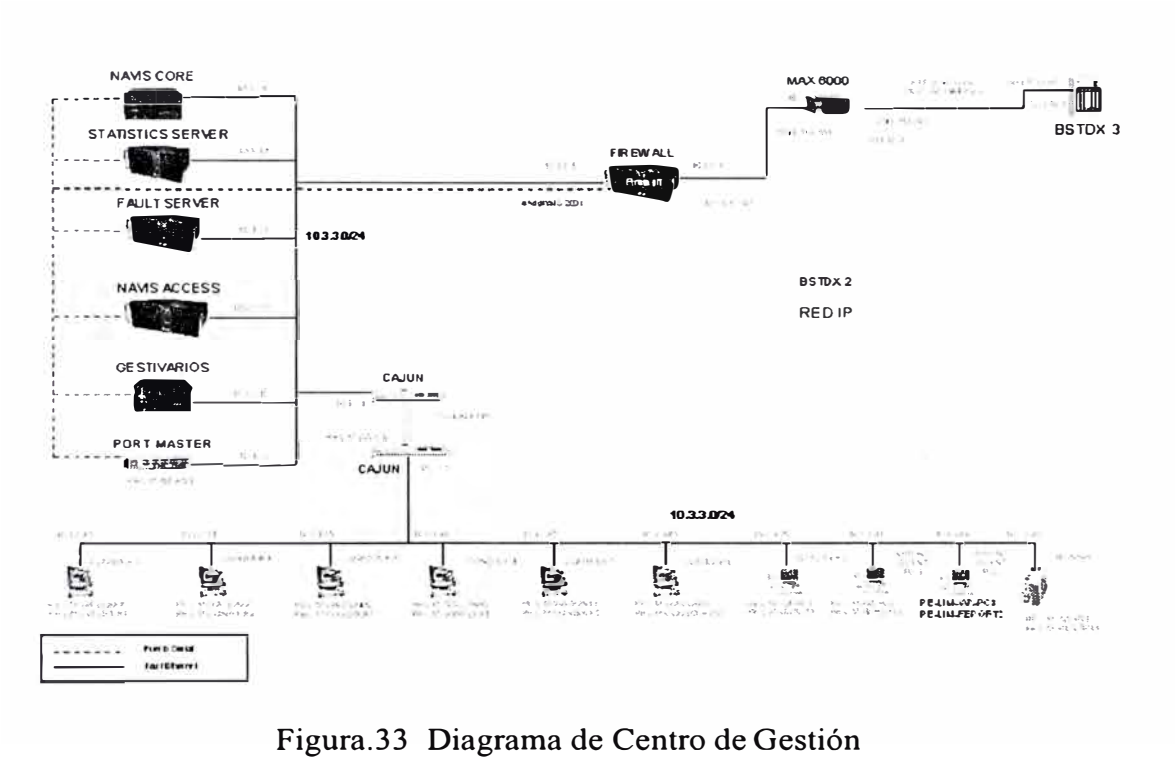

Figura.33 Diagrama de Centro de Gestión

El centro de gestión esta conformada principalmente por los siguientes equipos:

1 Navis Core : para la gestión de los BSTDXs

1 Navis Access : para la gestión de los MAX TNTs

1 Gestivarios : para la gestión de la red de acceso, transporte y servicio.

1 Firewall : para la seguridad a la red de gestión.

4.3 METODOS DE ACCESO

La Red IP deberá permitir el acceso de usuarios a través de las diferentes redes de acceso mediante la utilización de los nodos de acceso a los cuales se conectarán los usuarios.

Se tiene principalmente dos tipos de accesos:

4.3.1 Accesos conmutados

Los cuales se proveen a través de las diferentes redes de telefonía.

- Red Telefónica Conmutada (RTC).
- Red Digital de servicios Integrados (RDSI).

4.3.2 Accesos Permanentes

Brindados a través de las redes de datos existentes.

- Red de Frame Relay
- Accesos de ATM
- Accesos TDM

4.4 MODALIDADES DE AUTENTICACIÓN

La Red IP posee diversos mecanismos y facilidades que permiten realizar la autenticación de accesos conmutados a la Red IP, entendiendo como tales el acceso de un usuario de las redes RTC y RDSI a la Red IP.

Se proveen dos métodos de acceso y autenticación, Acceso anónimo y acceso autenticado.

4.4.1 Acceso anónimo a Red IP

Mediante este servicio, cualquier cliente de la Red IP con algún servicio de interconexión IP suscrito, excepto los que utilizan túneles, podrán acceder a los

servicios de carácter universal, bien prestados por la propia Red IP o por un proveedor de servicios a conectado a ella.

El usuario del servicio se le asignará una dirección IP pública identificándose con un login/password de amplia difusión. Este servicio es similar al acceso anónimo a través de las redes conmutadas de telefonía, prestado actualmente para el acceso al directorio Infovía y que permite acceder a los proveedores de información locales conectados. (ejm. login: infovia, password: infovia).

4.4.2 Acceso Autenticado a Red IP

Mediante este servicio, cualquier cliente de la Red IP con algún servicio de interconexión IP suscrito, excepto los que utilizan túneles, podrá acceder a los servicios de carácter universal, bien prestados por la propia Red IP o por un proveedor de servicios conectado a ella, y a los servicios de carácter no gratuito de la Red IP que tenga suscritos, entre ellos forzosamente el acceso a otras redes IP (Internet).

Este servicio no se ve limitado por la tecnología de la red de acceso como el anterior, si bien dicha tecnología impondrá una serie de particularidades en la autenticación que se tratarán de plasmar a lo largo de este apartado. La autenticación del acceso la realiza siempre la red IP, si bien los clientes podrán ser de cualquier proveedor o CPI.

Para llevar a cabo la identificación del usuario, este contará con un login/password que identificará unívocamente el paquete de servicios que este tiene suscrito.

4.5 FUNCIONAMIENTO DE LA RED

4.5.1 Proceso de Señalización SS7

1. El proceso de señalización se inicia cuando el usuario marca desde su PC o terminal mediante un programa de acceso telefónico a redes marca el 140100 el cual es enrutado hacia la central correspondiente.
2. La central al recibir el prefijo 140100 enruta mediante señalización SS7 hacia al Softswitch el origen de la conexión para su establecimiento.
3. Paralelamente la central le envía al MAX TNT la asignación de un canal de voz para el establecimiento de la conexión.
4. El softswitch mediante el Device Server utilizando el protocolo IPDCs le envía al TNT la asignación de recursos en el cual se encuentra (1 modem) para el establecimiento de la llamada.
5. El softswitch realiza el control de la llamada en el establecimiento, liberación y durante la conexión de la misma.

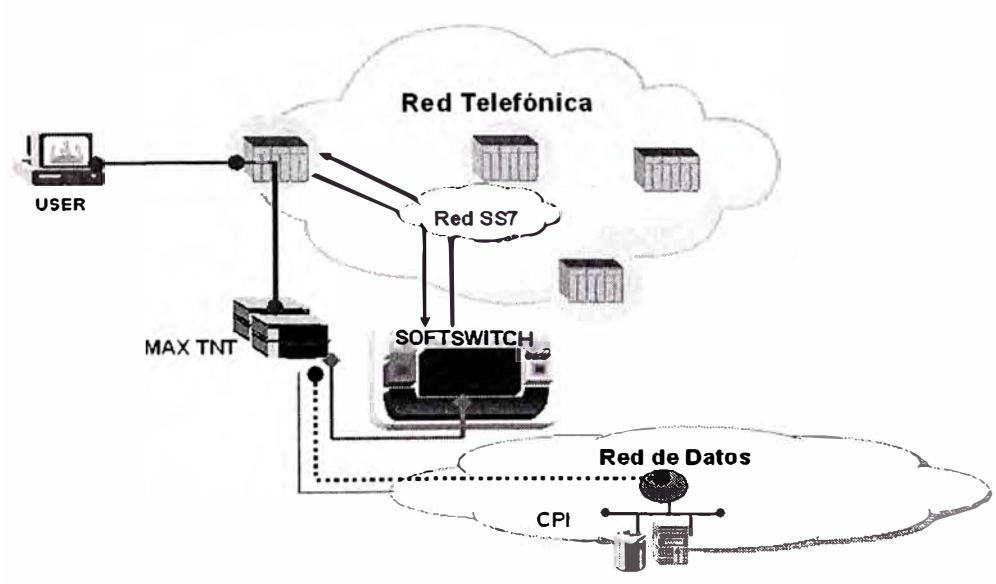

Figura.34 Proceso de Señalización

La arquitectura de la Red IP está utilizando la red de señalización SS7 basada en los nodos STP (Signalling Transfer Points) que llevan la señalización de la llamada desde la central local al SoftSwitch utilizando enlaces puros de señalización SDL (Signalling Data Link). Tanto los STPs como el SoftSwitch están duplicados para proporcionar redundancia sin embargo los STPs no llevan interconexiones cruzadas (cada STP se conecta solamente con su SS) y la redundancia se proporciona a través de la red de señalización. Tanto el Centro Primario como el Secundario llevarán los módulos (Call Directory, Call Coordinator y Device Server).

El SOFTSWITCH se comunica con los TNTs mediante IPDC sobre la red IP.

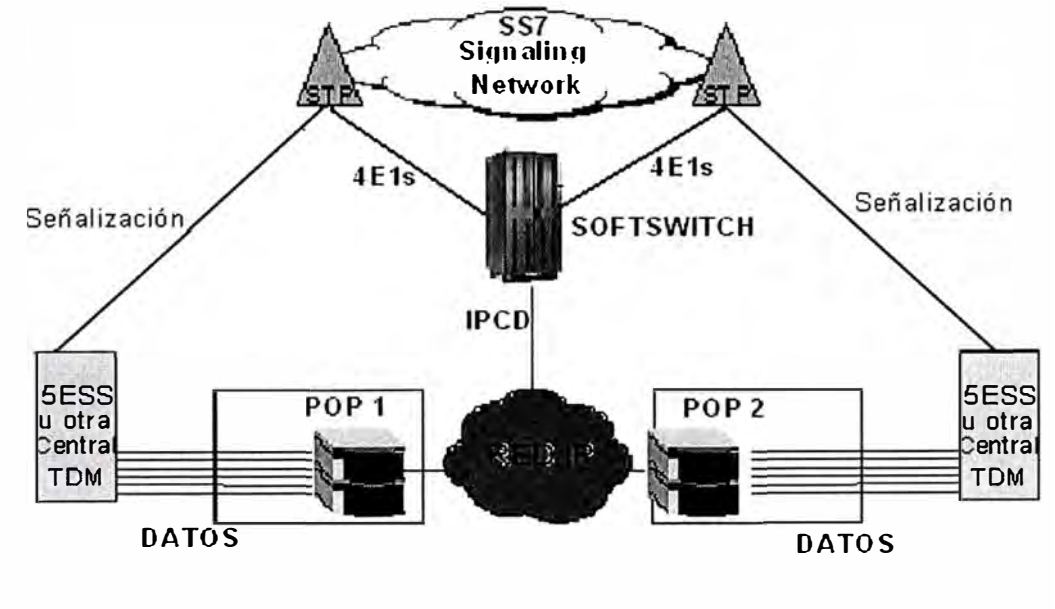

Figura.35 Diagrama SS7

4.5.2 Proceso de Autenticación

1. El cliente toma la línea y marca el 140100 solicitando acceso a la red IP.
2. La central de conmutación a través del canal CSS7 le comunica al Softswitch por intermedio del Device Server la presencia del cliente.

3. El Centro de servicios a través del canal CSS7 indica a la central de conmutación local que enrute al cliente por un E1 conectado al MAX TNT.
4. El Softswitch por intermedio del Device Server le indica al MAX TNT que le asigne un Modem al cliente.
5. Se establece una sesión PPP entre el cliente y el MAX TNT.
6. Utilizando el protocolo PPP el cliente le envía el user y password al MAX TNT.
7. El MAX TNT envía la información de user y password al Radius por el puerto UDP (1645 ó 1812).
8. El Radius verifica el dominio del cliente y si le pertenece.
9. Si el dominio le corresponde realiza la consulta del user y password del cliente al LDAP en caso contrario lo delega al Radius correspondiente.
10. El Radius le asigna una dirección IP del pool de direcciones publicas o privadas.
11. Al autenticar al usuario genera un registro de tiempo de conexión (accouting).
12. En los MAX TNTs podemos observar el tiempo de conexión de cada uno de los usuarios.

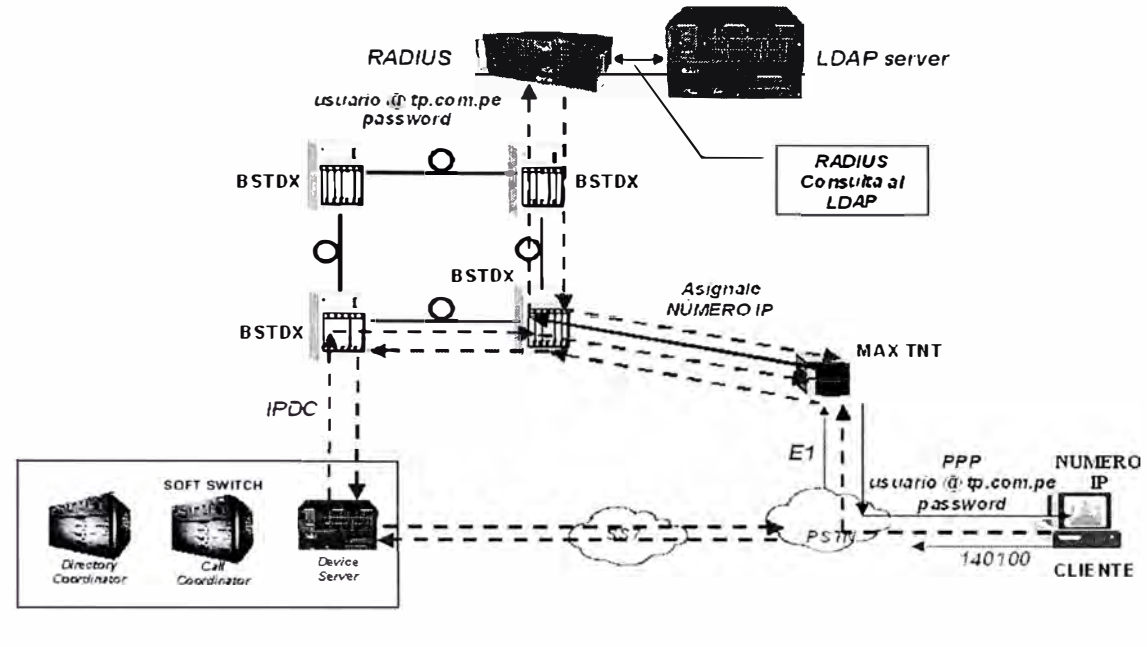

Figura.36 Proceso de Autenticación

4.5.3 Proceso de Autenticación Delegada

1. El cliente toma la línea y marca el 140100 solicitando acceso a la red IP.
2. La central de conmutación a través del canal CSS7 le comunica al Softswitch por intermedio del Device Server la presencia del cliente.
3. El Centro de servicios a través del canal CSS7 indica a la central de conmutación local que enrute al cliente por un E1 conectado al MAX TNT.
4. El Softswitch por intermedio del Device Server le indica al MAX TNT que le asigne un Modem al cliente.
5. Se establece una sesión PPP entre el cliente y el MAX TNT.
6. Utilizando el protocolo PPP el cliente le envía el user y password al MAX TNT.
7. El MAX TNT envía la información de user y password al Radius de la Red por el puerto UDP (1645 ó 1812).

8. El Radius delega la autenticación al Radius del CPI al cual pertenece dicho dominio.
9. El Radius del CPI consulta a su base de Datos de sus usuarios para verificar el usuario y el password .
10. El Radius del CPI le autentica al usuario y le baja la dirección IP en caso contrario lo asignará el Radius de la Red.
11. Los 2 Radius llevan el registro del tiempo de conexión (accouting).
12. En los MAX TNTs podemos observar el tiempo de conexión de cada uno de los usuarios.

A continuación tenemos el diagrama de la Autenticación Delegada:

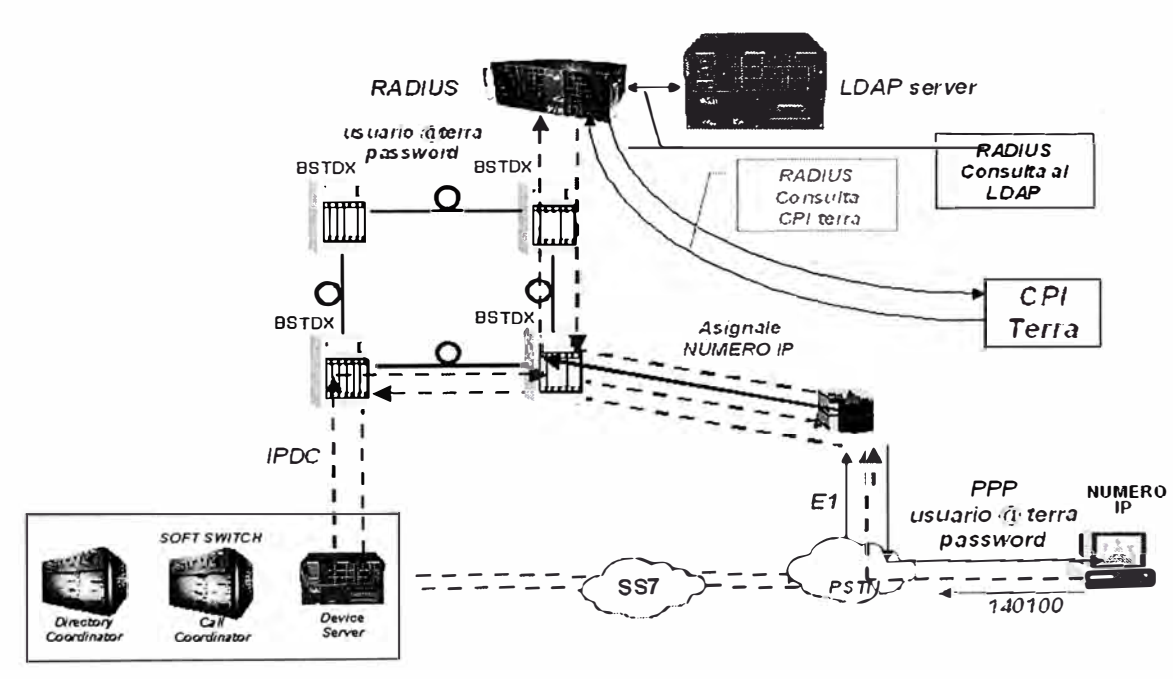

Figura.37 Proceso de Autenticación Delegada

4.5.4 Proceso de Navegación

1. El usuario después de la etapa de señalización y autenticación realizada correctamente en su explorador escribe un URL (ejm. www.cisco.com)
2. Esto es enviado hacia los DNSs inscritos en la PC del usuario.
3. El requerimiento llega hacia el MAX TNT y el lo enruta hacia el DNS primario de la Red.
4. El DNS recibe la petición del usuario y le resuelve dándole la dirección IP de la página solicitada (www.cisco.com = 198.133.219.25.
5. La dirección IP 198.133.219.25 es enviada hacia el usuario.
6. El usuario busca la dirección IP en internet por ruteo y carga la pagina.

A continuación el diagrama de Navegación :

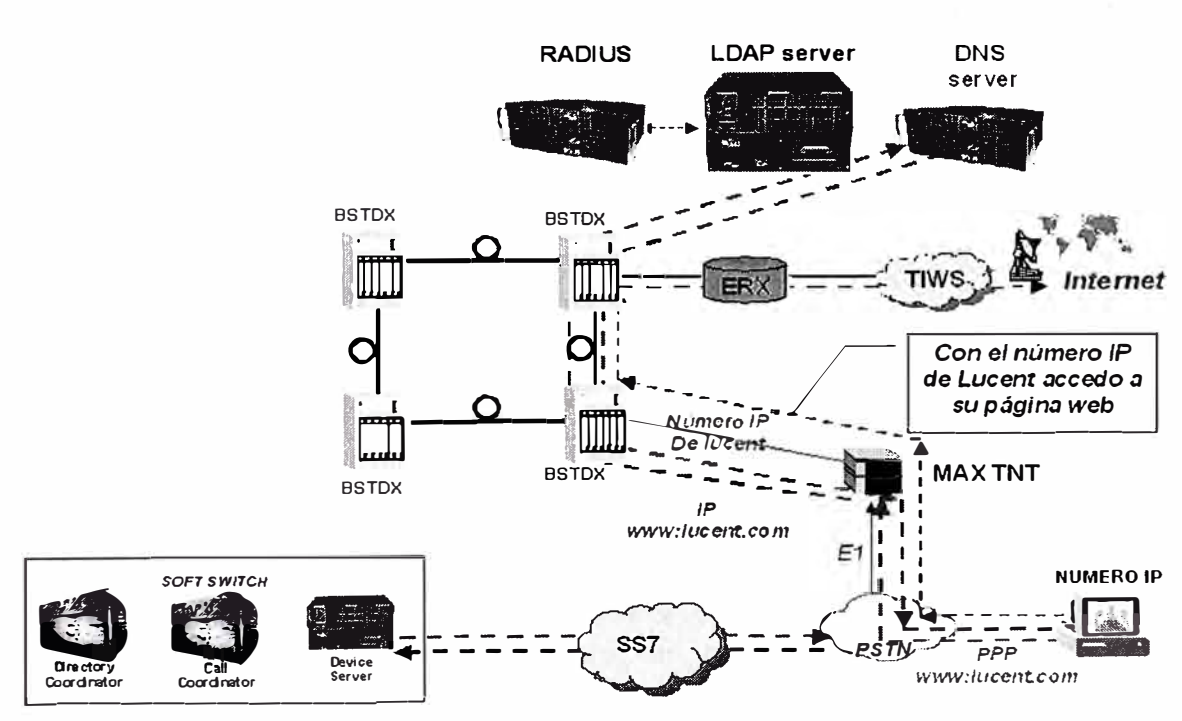

Figura.38 Proceso de Navegación

4.6 PROTOLOLOS DE RUTEO

4.6.1 OSPF (Open Shortest Path First)

OSPF es una alternativa más reciente a RIP entre los protocolos de routing internos, y que corrige todas las limitaciones que tenía éste. OSPF fue desarrollado por el IETF (Internet Engineering Task Force) como el reemplazo de RIP. Este protocolo es soportado por todos los principales vendedores de equipos de ruteo IP. OSPF es un protocolo de ruteo del tipo estado de enlace, que soporta ruteo jerárquico dentro de un sistema autónomo. OSPF provee una rápida convergencia y soporta máscaras de subred de longitud variable. OSPF se derivó del protocolo de ruteo IS-IS de la OSI, y algunas de sus características especiales incluyen ruteo de múltiples trayectorias de costo y ruteo basado en un tipo de nivel superior de solicitudes del servicio (ToS Type of Services). Por ejemplo, una aplicación puede especificar que ciertos datos son urgentes y si OSPF tiene enlaces de alta prioridad a su disposición, ellos pueden ser utilizados para transportar un paquete urgente. OSPF soporta uno o más métricas. En OSPF, un router no intercambia distancias con sus vecinos. En vez de eso, cada router chequea el status de cada uno de sus enlaces con los routers adyacentes y envía a éstos la información recogida, la que se propaga de esta forma a través del sistema autónomo. Cada router captura esta información y construye su tabla de ruteo, y todos los routers involucrados tendrán la misma tabla de ruteo. Desde un punto de vista práctico, la diferencia más importante es que un protocolo de estado del enlace converge con mayor rapidez que un protocolo de vector de distancia. Por convergencia se entiende que la estabilización después de cambios en la red, como caídas de router o de enlaces. OSPF se diferencia de RIP (y de otros muchos protocolos de ruteo) en que utiliza sólo IP, o sea, no es multiprotocolo. Además de

ser un protocolo de enlace en vez de distancia, OSPF tiene las siguientes características que lo hacen superior a RIP:

1. OSPF puede calcular un conjunto separado de rutas para cada tipo de servicio IP. Esto quiere decir que para un mismo destino puede haber varias entradas en la tabla de ruteo, una por cada tipo de servicio.
2. A cada interfaz se le asigna un costo. Este puede asignarse en función del ancho de banda de salida, seguridad, confiabilidad, etc. Pueden asignarse distintos costos para distintos servicios.
3. Cuando existen varias rutas a un mismo destino, con idénticos costos, OSPF distribuye el tráfico por ambas rutas de forma equitativa.
4. OSPF soporta subredes: una máscara de subred es asociada con cada ruta notificada. Esto permite que una única dirección IP de cualquier clase pueda ser dividida en múltiples subredes de varios tamaños. Las rutas a un host son notificadas mediante una máscara de subred con todos los bits a 1. Una ruta por defecto es notificada como una dirección IP de 0.0.0.0 con una máscara con todos los bits a 0.
5. Los enlaces punto a punto entre routers no necesitan una dirección IP a cada extremo, esto es lo que se conoce como redes no numeradas. De esta forma se ahorran direcciones IP.
6. OSPF emplea multicast en vez de broadcast, para reducir la carga en los sistemas que no emplean OSPF.

4.6.2 BGP (Border Gateway Protocol)

Un Sistema Autónomo (AS) es un grupo de redes de direcciones IP que son gestionadas por uno o más operadores de red que poseen una clara y sola política de ruteo.

Cada Sistema Autónomo tiene un número asociado el cual es usado como un identificador para el Sistema Autónomo en el intercambio de información del ruteo externo. Los protocolos de ruteo externos tales como BGP son usados para intercambiar información de ruteo entre Sistemas Autónomos.

La expresión Sistema Autónomo es con frecuencia interpretada incorrectamente como apenas una forma conveniente de agrupar redes que están bajo de una misma gestión. Sin embargo, en el caso en que hay más de una política de ruteo en el grupo, más de un AS es necesario. Por otro lado, si el grupo de redes posee la misma política que los otros grupos, estos quedan dentro del mismo AS independientemente de la estructura de la gestión. De esta manera, por definición, todas las redes que componen un AS comparten la misma política de ruteo.

BGP es un protocolo de ruteo exterior para la comunicación entre routers en diferentes ASs.

BGP es el reemplazo para el antiguo EGP que se empleaba en ARPANET. La última versión en desarrollo es la BGP Versión 4, desarrollada para soportar CIDR. Un sistema BGP intercambia información de cómo alcanzar redes con otros sistemas BGP. Esta información incluye el camino completo de los ASs que el tráfico debe recorrer para alcanzar dichas redes, y es adecuada para construir conectividades entre ASs. De esta forma, es posible eliminar loops y tomar decisiones a la hora de rutear los paquetes. En primer lugar, es necesario que el router pueda distinguir entre lo que

es el tráfico local y tráfico en tránsito. El primero se origina en el AS y termina en éste. El resto del tráfico se considera en tránsito. Uno de los objetivos de BGP es reducir el tráfico en tránsito. Un AS puede englobarse en uno de lo siguientes tipos:

Terminal.

Tiene una única conexión con otro AS y, por lo tanto, tiene tan sólo tráfico local.

Multihome.

Tiene conexión con varios ASs, pero rehusa transportar tráfico en tránsito.

De Tránsito.

Tiene conexión con más de un AS, y está destinado, bajo ciertas restricciones,a transportar tráfico tanto local como en tránsito.

La topología de Internet queda dividida entonces, en ASs terminales, multihome y de tránsito. Los dos primeros no requieren BGP, sino que pueden utilizar EGP para intercambiar información con otros ASs. BGP permite realizar un ruteo basado en políticas administrativas. Éstas son fijadas por el administrador del AS y especificadas en los archivos de configuración de BGP. Las políticas no forman parte del protocolo, pero las especificaciones de política permiten decidir entre distintos caminos cuando existen varias alternativas. También controlan la forma en la que se transmite la información. La política vendrá especificada en función de requerimientos de fiabilidad, seguridad, etc. BGP se diferencia de RIP en que emplea TCP como protocolo de transporte, no UDP como es el caso de RIP. Dos sistemas que empleen BGP establecerán una conexión TCP e intercambiarán sus tablas BGP completas. En conexiones posteriores, se enviarán actualizaciones de dichas tablas. BGP es un protocolo de vector de distancias, pero al contrario que RIP (que emplea como unidad de medida hops), BGP enumera las rutas a cada destino (la secuencia

de ASs al destino) eliminando de esta forma, algunos de los problemas asociados con RIP. Cada AS tiene asociado un número de 16 bits. BGP detecta la fallo de un enlace o un host mediante el envío de un mensaje keepalive a sus vecinos de forma regular (aproximadamente cada 30 segundos). BGP involucra tres procedimientos funcionales, que son:

Adquisición de vecino.

Dos routers son vecinos si están conectados a la misma subred y se han puesto de acuerdo en que ambos quieren intercambiar regularmente información de ruteo. Para llevar a cabo la adquisición de vecino, un router envía a otro un mensaje OPEN. Si el dispositivo destino acepta la solicitud, devuelve un mensaje KEEPALIVE como respuesta.

Detección de vecino alcanzable.

Una vez establecida la relación de vecino, para mantener la relación se realiza la detección de vecino alcanzable enviándose periódicamente mensajes KEEPALIVE.

Detección de red alcanzable.

Para la detección de red alcanzable es necesario que cada dispositivo de encaminamiento tenga una base de datos con todas las redes que puede alcanzar y la mejor ruta para alcanzarla. Cuando se realiza un cambio en la base de datos es necesario enviar un mensaje UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP para que puedan acumular y mantener la información necesaria.

CAPITULO V

SERVICIOS DE LA RED IP

5.1 INTRODUCCIÓN

Los servicios brindados por la Red IP de Lucent y desplegado por Telefónica .Dichos servicios son los siguientes:

- Infovía Plus Básico
- Infovía Plus Directo
- InfoInternet
- Uno IP

La nomenclatura utilizada para mencionar las redes IP y los servicios ha sido la siguiente:

1. Las redes IP a las que se aplican los servicios descritos en este informe estarán presentes en los distintos países con distintos nombres comerciales. Por ello, no se ha utilizado un nombre particular de red IP (red UNO IP por ejemplo) sino que nos hemos referido a ellas genéricamente con el nombre de "Red IP"
2. Los servicios soportados por la Red IP se describen en este informe utilizando los nombre con los que se comercializan es España; es decir: Infovía Plus Básico, Infovía Plus Directo, UNO IP e InfoInternet.

3. Para la descripción de los servicios se ha seguido siempre la misma metodología:
    a. Definición del servicio y descripción de las funcionalidades asociadas
    b. Implementación del servicio mediante los elementos de la arquitectura propuesta
    c. Equipo de usuario necesario para la provisión del servicio.
    d. Facilidades adicionales.

5.1.1 Características de los servicios

Como características fundamentales de estos servicios podríamos citar las siguientes:

1. **Infovía Plus Básico**: Acceso conmutado a la Red IP y Navegación por los CPIs e ISPs conectados a ella. La autenticación la realiza el Radius de la Red IP o el Radius del CPI s que se encarga de asignar direcciones públicas a los usuarios conectados a ella.
2. **Infovía Plus Directo**: Acceso a ISPs mediante túneles entre los servidores de acceso y los terminadores de túneles del ISP. La autenticación la realiza el RADIUS del ISP que puede asignar a los usuarios direcciones privadas.
3. **UNO IP**: Servicio de conexión permanente a la Red IP. Puede ser contratado por corporaciones para formar Redes Privadas Virtuales o por ISPs para conexión a la Red IP y salida a Internet.
4. **INFOINTERNET**: Servicio de acceso a Internet dentro de la Red IP. Para contratar este servicio es necesario tener acceso a Red IP mediante conexión conmutada (Infovía Plus Básico) o dedicada (UNO IP).

Cualquier tipo de servicio utiliza el backbone de la Red IP para su funcionamiento.

5.2 SERVICIO INFOVÍA PLUS BÁSICO

El servicio Infovía Plus Básico es un servicio destinado a proporcionar a las empresas e instituciones, paquetes de servicios de acceso conmutado a la Red IP para usuarios finales. El servicio, por tanto, permite la conexión de usuarios remotos a través de RTB y RDSI a los Centros Proveedores de Información y de Servicios conectados de forma abierta a la red en todo el ámbito nacional, y a los propios servicios de la Red IP contratados por el cliente.

Los usuarios acceden identificándose mediante un login **(usuario@cliente)** y un password. La autenticación del usuario y la asignación de la dirección IP es realizada por la Red IP mediante el Servidor RADIUS.

El servicio Infovía Plus Básico se define como un servicio que permite a sus clientes (proveedores, empresas o instituciones) ofrecer a los usuarios finales acceso conmutado a servicios y proveedores de servicios de la Red IP.

5.2.1 Características

La provisión del servicio **Infovía Plus Básico** ofrecido por Lucent tiene las siguientes características:

1. Proporciona acceso conmutado a usuarios finales y redes de área local (LAN) vía RTC, RDSI o GSM a la Red IP, tanto a servicios de la propia red como a centros proveedores de información y servicios conectados de forma abierta a la red.

2. El cliente del servicio (proveedores, empresas o institución) no necesita una conexión permanente a la Red IP ni disponer de infraestructura.

Puede proporcionarse calidad de servicio en tránsito (desde el RAS hasta el Toll-Gate u otro CPI o ISP), mediante la asignación de distintos Pools de direcciones para cada calidad de servicio contratada por el usuario.

3. Se soporta Multilink PPP en accesos RDSI.

Sólo se contempla el acceso conmutado utilizando los servidores de acceso de la Red IP (MAX-TNT). Los usuarios se identificarán con su nombre de usuario y password para acceder a la red a través de una URL definida por defecto en su Navegador (Lucent no proporciona la URL de acceso a la red). El usuario del servicio podrá ser un usuario residencial accediendo desde un PC con módem o bien una LAN remota.

5.2.2 Funcionamiento

Se establece la negociación LCP (Link Control Protocol) entre el usuario final y el servidor de comunicaciones (RAS). Este protocolo permite la negociación de las características lógicas de la conexión PPP tales como el tamaño máximo de trama que puede recibir cada extremo, el protocolo de autenticación utilizado etc. El usuario final envía un mensaje de "Configure-request" con las opciones de configuración deseadas al servidor de comunicaciones. Hasta que no se produce la correspondiente negociación de parámetros en los dos sentidos con el correspondiente envío de "Configure-Ack" no se da por finalizada la negociación LCP. Entre los parámetros de configuración negociados estará el protocolo de autenticación que se va a utilizar (PAP, CHAP etc). Esto indicará al RAS que después del establecimiento del LCP se iniciará una fase de autenticación.

Dependiendo de si la autenticación seleccionada es PAP o CHAP, se enviará al RAS un mensaje de "Authenticate-Request" o un "Challenge" respectivamente.

El servidor de comunicaciones recibe del usuario remoto una petición de autenticación y se la progresa al Servidor Radius de la Red IP . El mensaje de "Access-Request" enviado desde el RAS al Servidor Radius contendrá entre otros atributos el nombre de usuario y o bien un password de usuario o un password de tipo CHAP.

Una vez recibida la petición de autenticación, el Servidor Radius consultará en la base de datos de usuarios LDAP el cliente concreto, y validará el login y password enviados en el mensaje de solicitud de autenticación. Si estos datos son correctos y el usuario tiene permitido el acceso a la red, el Servidor RADIUS enviará al Servidor de Comunicaciones (RAS) un mensaje de autorización "Access_Accept". En este mensaje de aceptación, entre otros atributos se incluirán los siguientes:

1. "Filter_Id": filtros que se aplicarán al usuario en función de los servicios a los que tenga acceso asociados al usuario.

"Session-Timeout": Número máximo de segundos que podrá durar la sesión del usuario.

2. "TOS". Este campo TOS se usa para especificar si el usuario tiene contratado el servicio InfoInternet (se encuentra en fase de pruebas).
3. "IP Pool Number". Este campo contiene el número del pool de direcciones desde el que el MAX-TNT va a asignar la dirección IP de origen.

Si el usuario no tiene acceso a la red, el RADIUS contestará con un "Access_Reject", que será progresado al punto de acceso y se cerrará la conexión PPP.

Para el servicio InfoVía Plus Básico con modalidad Delegada el cliente deberá disponer de un Servidor Radius autorizado y la base de batos para dar de alta a sus clientes. Y esta última es la que se utiliza a mas del 50% de los usuarios de la red IP.

5.2.3 Funcionamiento del servicio InfoVía Plus Básico con modalidad Delegada

Este servicio como su nombre lo menciona es el del Infovía Plus Básico con la diferencia que el radius que autenticará al usuario es un radius externo a la red.

El usuario después de levantar la sesión PPP con el radius de la red le envía los siguientes parametros: user@dominio y password.

El radius de la red analiza el dominio y lo envía a un radius externo para que el lo autentica. Esto lo realiza por los puertos 1645,1646,1812 y 1813.

El radius externo valida al usuario en su base de datos; y le envía dicha información al radius de la red.

El radius de la red recibe dicha información y procede a autorizar al usuario y llevar la contabilidad.

5.3. SERVICIO INFOVÍA PLUS DIRECTO

El servicio **Infovía Plus Directo** es un servicio destinado a proporcionar a las empresas una solución global de Redes Privadas Virtuales de Acceso Conmutado (VPDN) sobre la infraestructura de la Red IP, ofreciendo como principales características la creación de redes Privadas. El servicio, por tanto, permite la conexión de usuarios remotos a una o varias sucursales del cliente, de manera segura a través del protocolo IP.

El cliente deberá tener previamente una conexión permanente a la red IP (servicio Uno-IP Básico) para facilitar la autenticación y el acceso de los usuarios remotos a sus redes. Por tanto, el cliente tendrá opción de conectarse a la Red IP a través de tecnologías como Frame-Relay, ATM o Punto a Punto. Estas tres tecnologías de acceso se encuentran soportadas en la red de Lucent mediante el equipamiento BSTDX.

El servicio Infovía Plus Directo se define como un servicio de acceso conmutado a redes privadas virtuales multiprotocolo. El servicio permite el acceso de usuarios remotos a las redes privadas del cliente a través de túneles de nivel 2 establecidos entre un servidor de comunicaciones del nodo de acceso y un servidor de túneles (ST) en la red del cliente. La utilización de estos túneles permite la encapsulación multiprotocolo, direccionamiento independiente del de la Red IP y gestión de la autenticación delegada al cliente.

5.3.1 Características

El servicio **Infovía Plus Directo** en el modelo de red ofrecido por Lucent tiene las siguientes características:

1. Acceso conmutado seguro a redes privadas virtuales a través de túneles dinámicos L2TP.
2. Autenticación de usuarios y asignación de direcciones IP mediante el servidor Radius del cliente.

Direccionamiento independiente de red. La utilización de túneles permite al cliente la utilización de direccionamiento IP, público o privado.

3. Desde el punto técnico, el servicio **Infovía Plus Directo** se apoya en el servicio Uno-IP Básico como servicio básico de conectividad a la red. Es

decir, el cliente debe al menos contratar un servicio Uno-IP Básico para que sus usuarios remotos se conecten a su red a través de este, así como para realizar la autenticación de estos. Las características del servicio Uno-IP Básico se explican en el capítulo correspondiente a este servicio.

Como elemento fundamental para la provisión de este servicio podemos mencionar el equipo Servidor de Túneles (ST), que se encarga del establecimiento de túneles dinámicos mediante protocolo L2TP que se soporta en el MAX-TNT.

5.3.2. Funcionamiento

El usuario final accederá a través de RTB, RDSI o GSM a un servidor de comunicaciones del nodo de acceso correspondiente, mediante la marcación del número destinado a tal efecto.

Se establece la negociación LCP (Link Control Protocol) entre el usuario final y el servidor de comunicaciones (MAX-TNT). Este protocolo permite la negociación de las características lógicas de la conexión PPP tales como el tamaño máximo de trama que puede recibir cada extremo, el protocolo de autenticación utilizado etc. El usuario final envía un Configure-request con las opciones de configuración deseadas al servidor de comunicaciones. Hasta que no se produce la correspondiente negociación de parámetros en los dos sentidos con el correspondiente envío de "Configure-Ack" no se da por finalizada la negociación LCP. Entre los parámetros de configuración negociados estará el protocolo de autenticación que se va a utilizar (PAP, CHAP etc). Esto indicará al RAS que después del establecimiento del LCP se iniciará una fase de autenticación.

Dependiendo de si la autenticación seleccionada es PAP o CHAP, se enviará al RAS un mensaje de "Authenticate-Request" o un "Challenge" respectivamente.

El servidor de comunicaciones recibe del usuario remoto una petición de autenticación y se la progresa al Servidor Radius de la Red IP (SR). El mensaje de "Access-Request" enviado desde el RAS al Servidor Radius contendrá entre otros atributos el nombre de usuario y un password de usuario o un password de tipo CHAP. A pesar de pasar esta información al servidor de RADIUS, en esta fase el servidor de RADIUS no realiza autenticación de usuario/password sino que sólo utilizará la parte correspondiente al dominio del nombre de usuario.

Una vez validado el atributo "Realm" enviado en el "Access-Request", el servidor de RADIUS devolverá un mensaje de "Access-Accept" con varios atributos, entre los cuales se encontrarán los siguientes:

"Tunnel-Type" : Tipo de túnel, en este caso tomará el valor correspondiente a L2TP.

- "Tunnel-Medium-Type": Indica que medio de transporte se utilizará en la creación del túnel. Tomará el valor de IP.
- "Tunnel-Server-Endpoint": Este atributo en este caso contendrá la dirección IP del servidor de túneles remoto. El valor de este atributo lo obtiene el servidor de RADIUS en función del dominio del atributo username enviado en la petición de acceso. Es decir, para el usuario user@empresa1, se obtiene la dirección IP del servidor de túneles correspondiente en función del dominio "empresa1".

La recepción de atributos relativos a un túnel por parte del RAS, obligan a que éste intente establecer un túnel L2TP (según se indique en el campo "Tunnel-Type") con el extremo indicado en el atributo "Tunnel-Server-Endpoint".

Una vez que se encuentra establecido el túnel, se reinicia la sesión PPP con el usuario final. Dicho reinicio se realiza por iniciativa del Servidor de Túneles. Este

enviará al usuario final un mensaje de "Configure_Request" ante el cual el usuario final envía al servidor de túneles otro mensaje de "Configure_Request" y se repetirán todas las fases de negociación del PPP. Tanto la negociación LCP, como la autenticación y la negociación IPCP se realizarán directamente entre el usuario final y el RAS. La autenticación se realizará contra el servidor de RADIUS del cliente y tras realizarse ésta se asignará una dirección IP o una subred al usuario remoto.

Cuando una llamada llega al MAX-TNT desde un modem V.90 se inicia la autenticación del usuario con peticiones al Servidor Radius (SR). El servidor Radius de la Red (PA) recibe la petición de autenticación del usuario del Servicio InfoVía Plus Directo. Este servidor analiza el mnemónico del cliente, verificando si este tiene contratado el servicio InfoVía Plus Directo. Si es así realiza una selección aleatoria (esta funcionalidad se soportará en la Release 3.0) entre los terminadores de túneles que se encuentran definidos por el cliente, verificando que no se excede el límite configurado para cada uno de ellos. A continuación devuelve al RAS las características del terminador de túneles en el mensaje de contestación a la petición de autenticación. El RAS entonces establece el tunel con el Terminador de Túneles. Este envía una nueva petición de autenticación al Servidor Radius de Cliente el cual realiza la autenticación y autorización del usuario.

5.4 SERVICIO UNO IP BÁSICO

El servicio UnoIP Básico está orientado a resolver los problemas de conectividad de aquellos clientes que desean ofrecer servicios de información dentro del ámbito nacional. La Red IP les ofrece la posibilidad de convertirse en un CPI y, mediante la

utilización de protocolos IP, ser accesibles desde cualquier tipo de usuario de un modo abierto.

Junto a la facilidad básica de conectividad a la Red IP, se ofrece la posibilidad de contratar otras facilidades de esta red de forma opcional. Estas facilidades están, en su mayor parte, orientadas a facilitar la accesibilidad del ISP por parte de otros usuarios de la Red IP. Entre las más importantes cabe destacar el servicio de resolución de nombres (DNS).

El CPI tendrá opción de conectarse a la Red IP a través de tecnologías de transporte como Frame-Relay, ATM o Punto a Punto. Las tres tecnologías de acceso se encuentran soportadas actualmente en los B-STDX.

El servicio UnoIP Básico es el servicio de conectividad o presencia en la Red IP que permite el acceso sin restricciones en modo no conmutado a la Red IP.

Por tanto, en este contexto, el servicio UnoIP Básico consta de los siguientes elementos:

- **Enlace físico punto a punto** de conexión a la red de acceso de la Red IP. Las velocidades soportadas son (64Kbps, 128 Kbps,192 Kbps,256 Kbps,512 Kbps,1024 Kbps y 2Mbps conectados directamente o travez de transmisiones hacia el BSTDX correspondiente. Las interfaces utilizadas son E1s canalizados los cuales soportan 31 canales de 64Kbps.

- **Equipo en domicilio de Cliente y Router de Acceso**

El router debe al menos de disponer de un interface V.35 y soportar la encapsulación de IP sobre FR standard del IETF (**RFC 1490**) o encapsulación LLC (**RFC 1483**)

para transporte ATM. Entre la Red y el cliente se utilizan los protocolos de routing BGP-4, RIP V2, OSPF.

5.4.1 Características

Todas las características de este servicio se encuentran soportadas por la plataforma B-STDX así como por su sistema de aprovisionamiento NavisCore. Los equipos B-STDX son nodos Multiservicio que proporcionan servicio FR, IP y ATM en el mismo equipo.

Mediante la solución implantada se puede además garantizar el caudal IP contratado pueden definirse distintas calidades de servicio para un mismo caudal IP contratado creando para cada uno de ellas distintos LSPs no sólo cuando el acceso es a través de FR donde se dispone de una aplicación (Priority Frame) que proporciona Calidad de Servicio similar a la proporcionada en el ámbito ATM, sino a lo largo de la Red IP mediante IP Navigator. De esta forma se dispone de Calidad de Servicio para cualquier acceso.

Basándose en la dirección IP origen (dirección del cliente), el nodo origen que recibe las tramas IP es capaz de establecer un LSP(Label Switched Path) en tiempo real con la calidad de servicio contratada.

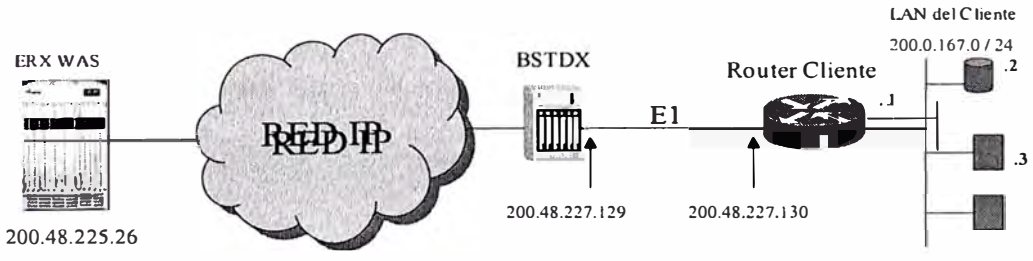

Figura.39 Diagrama del Servicio UNO IP BASICO

5.4.2 Funcionamiento

El usuario se conecta a la Red IP mediante una conexión WAN de un router contra el BSTDX utilizando el protocolo PPP.

El usuario utiliza para la conexión diferentes BWs 64,128,256,512,1024Kbps ó 2 Mbps para la conectividad a la Red IP la cual la realiza a través del BSTDX correspondiente a la zona.

El usuario tiene una Red Lan detrás del Router la cual utiliza direcciones públicas las pueden ser (1,8 ó 16 direcciones)

Es importante mencionar que el usuario no necesita autenticarse para poder levantar el protocolo PPP.

Lo único necesario es configurar:

La parte Fisica del Router hacia el BSTDX.

La parte Lógica para la Sesión PPP entre el BSTDX y el Router.

La parte IP ó de Red para que el usuario pueda navegar en internet.

Adicionalmente el usuario necesita configurar los DNSs en cada uno de las PCs.

A este servicio se le llama Servicio Speedy Plus Simétrico.

5.4.3 Calidad del Servicio

La calidad de Servicio en UNO IP Básico se consigue por medio de IP Navigator. Este es un software que corre sobre los nodos de acceso (BSTDX) a los que proporciona Calidad de Servicio respetando los acuerdos de cliente. Normalmente los routers convencionales no pueden proporcionar este nivel de calidad de servicio.

La calidad de servicio en la red se proporciona mediante IP Navigator el cual dependiendo de la dirección IP asignada en el MAX-TNT, proporciona al usuario una ruta y un canal de comunicaciones con unos determinados parámetros de calidad

de servicio, como ancho de banda garantizado, constant bit rate, rutas estáticas, etc. La versión actual de IP Navigator no soporta calidad de servicio con lo cual todas las conexiones recibirán "Best Effort".

5.4.4 IP Navigator

El empleo de IP Navigator nos permite conjugar lo mejor de dos mundos, el del routing IP y el de la conmutación de tramas o celdas. La inteligencia propia de la capa de red IP (capa 3) está soportada, ya que nuestro backbone operará con protocolos estándar como RIP, OSPF y BGP. Al mismo tiempo, gracias a IP Navigator la conmutación de tráfico se realiza con la simplicidad y altas prestaciones propias de las capas de enlace (capa 2) como Frame Relay o ATM.

Una red MPLS con IP Navigator establece un encaminamiento basado en las normas de utilización de los mapas de ruta los cuales controlan el flujo de rutas hacia y desde la tabla de encaminamiento, reflejando las decisiones administrativas sobre las rutas seleccionadas desde un protocolo que tienen que indicarse a otro protocolo. IP Navigator proporciona la plena capacidad de establecer normas de encaminamiento de forma dinámica y utiliza filtros para analizar las direcciones de origen/destino y los protocolos utilizados. Estos datos se usarán para asignar los caminos virtuales que respeten los acuerdos de cliente (Service Level Agreement).

El encaminamiento explícito o el trayecto basado en la calidad del servicio es un método en el que el primer nodo del trayecto selecciona el trayecto completo. La calidad del servicio basada en el trayecto permite a la red anticipar recursos y asignarlos como tales. Puede especificarse el trayecto al destino permitiendo la elaboración de estadísticas a lo largo del trayecto y equilibrando la carga en la red. El trayecto que la llamada va a seguir se codifica de forma explícita como parte del

establecimiento de llamada. Esto implica que los sistemas de conmutación subsiguientes del trayecto utilizan el trayecto seleccionado por el primer sistema de conmutación. La utilización de encaminamiento explícito permite a los proveedores de servicio ofrecer un nivel "absoluto" de calidad del servicio para IP. El encaminamiento explícito también permite la **ingeniería del tráfico** (también conocida como gestión de banda ancha), que es el proceso de gestionar las rutas seguidas por el tráfico de datos de usuario en una red para proporcionar una carga de los recursos de la red eficiente y relativamente equitativa.

Los objetivos de la ingeniería del tráfico MPLS del IP Navigator son optimizar la utilización de los recursos y reducir al mínimo la congestión de la red. La ingeniería del tráfico considera las capacidades de la red, la cantidad de datos de usuario que fluyen por la red en cada trayecto concreto, así como la calidad de los requisitos del servicio de los datos de usuario.

El IP Navigator hace que una agrupación de sistemas de conmutación Frame Relay o ATM parezca desde el exterior un conjunto de routers IP. Otros routers y hosts IP hacen interfaz con los sistemas de conmutación con IP Navigator como si éstos fueran routers IP, utilizando protocolos de enlace de datos estándar, tales como PPP, Frame Relay y ATM.

5.5. SERVICIO DE INFOINTERNET

El servicio InfoInternet se define como un servicio de acceso a Internet a través de la Red IP que permite la comunicación bidireccional de un usuario conectado a la Red IP con cualquier usuario conectado a Internet que no ponga restricciones adicionales a ello. Los usuarios del servicio pueden proceder de conexiones permanentes a la

Red IP (a través del Servicio UNO-IP Básico) o de accesos conmutados (a través del Servicio InfovíaPlus Básico y Infovia Plus Directo).

Para este servicio se requiere la contratación de un servicio que proporcione el acceso a la Red IP: para conexiones permanentes el servicio UNO-IP Básico, y conmutadas el servicio InfovíaPlus Básico o Infovia Plus Directo.

Por tanto, en este contexto, el servicio InfoInternet constará de los siguientes elementos, que serán detallados en mayor profundidad en los siguientes puntos :

Servicio de conectividad con la Red IP: Como ya se ha mencionado, el servicio InfoInternet es un servicio de valor añadido que permite a un servicio de conectividad con la Red IP (**Uno-IP Básico, InfovíaPlus Básico e Infovia Plus Directo**) la conectividad abierta y sin restricciones a Internet. Es decir, el servicio InfoInternet permite la comunicación con Internet de estos servicios de conectividad usando el Toll-Gate a modo de llave de acceso, permitiendo este acceso a Internet sólo a aquellos usuarios que ya posean uno de estos servicios y contraten el servicio InfoInternet.

Salida a internet: El Toll-Gate es el sistema de la Red IP que permite la comunicación con Internet. El Toll-Gate permite la comunicación bidireccional con Internet sólo de aquellos usuarios que tengan contratado el servicio InfoInternet. Para el caso de los accesos permanentes a la Red IP a través del servicio UNO IP, el Toll-Gate permite que las direcciones públicas de dicho cliente cursen tráfico a través de éste. Para el caso de los accesos conmutados a través del servicio Infovía Plus Básico, el Toll-Gate permite el tráfico de aquellos usuarios que tengan contratado el servicio InfoInternet mediante direcciones IP asignadas desde diferentes pooles de direcciones y TAG asignados a las rutas correspondientes.

5.5.1 Funcionamiento

La autenticación del servicio InfoInternet aplica solamente cuando se apoya sobre el Servicio Infovía Plus Básico y por tanto es similar a este servicio. La autenticación se realiza en el Servidor de Red (SR) el cual pasa información sobre la clase de servicio contratada. El RAS asignará posteriormente una dirección IP perteneciente a un pool en función de esta clase de servicio.

Para el caso de conectividad IP a través del acceso conmutado, el Toll-Gate distingue si el usuario tiene acceso a Internet mediante el siguiente procedimiento:

Se crean dos rutas estáticas en los BSTDX en los cuales los correspondientes MAX TNT están conectados. Estas rutas estáticas tienen dos TAG diferentes. La ruta con acceso a Internet tiene un TAG de 30 y la ruta que no tiene acceso a Internet tiene un TAG de 10.

Los IP pools con acceso a Internet se mapean a la ruta estática correspondiente.

En el caso de que el cliente tenga una conexión a la Red IP de Telefónica y una conexión a Internet con otro proveedor que no sea Telefónica, se configura el router de cliente perteneciente a Telefónica para que hable BGP con el BSTDX correspondiente. En el BSTDX se crea una ruta estática con TAG 30 o TAG 10, este BSTDX ignora toda la información de routing que provenga del router del cliente. De esta manera, el tráfico a Internet saldrá por la conexión que tenga contratada el cliente con el proveedor alternativo y el tráfico correspondiente a la Red IP de Telefónica saldrá por la conexión UNO-IP Básico contratada.

5.6 ROUTING EN LA RED IP

El BSTDX utiliza los protocolos de encaminamiento IP estándar, tales como BGP, RIPV2 o OSPF, los cuales permiten el intercambio de información de encaminamiento entre los routers IP y los sistemas de conmutación LUCENT.

Dentro de la Red IP también se emplea el protocolo de routing OSPF para reconocer la topología de la agrupación y BGP-4 para redistribuir la información de encaminamiento a otras redes. Además, se ejecuta un algoritmo de encaminamiento de VC (Virtual Network Navigator), y su señalización asociada, entre los sistemas de conmutación ofertados, permitiéndoles establecer trayectos conmutados de etiquetas punto a punto y multipunto a punto. Además se usan mapas de ruta para indicar cualquier ruta estática, Directa, BGP, RIP y VNN OSPF en el dominio de routing IP OSPF.

CONCLUSIONES

1.- En los últimos años la Red IP conmutada en el Perú ha tenido una gran evolución; brindando sólo el servicio de Internet en un inicio hasta los servicios suplementarios como correo, hosting y otros en la actualidad. Para lo cual ha tenido que ir de la mano con el desarrollo de la tecnología viéndose reflejado en los equipos cada vez de mayor capacidad y cantidad.

2.- En la actualidad la IAB (Internet Architecture Board) es el encargado de dictar algunos parámetros dentro de la comunidad de internet. La IAB se deriva a su vez en varios sub-comites llamados ITF (Internet Task Force) los cuales vienen realizando normativas para ser aplicadas en las Redes a nivel mundial. En el caso de Perú se encuentra a la espera de dichas normativas.

3.- La Red IP conmutada en el Perú es similar a la de algunos países de Sudamérica como en el caso de Chile, Brasil y Argentina de los cuales se ha tomado los diseños de topología de sus redes. Además contamos con su apoyo y experiencia de los grupos de Telefónica de dichos países.

4.- La Red IP tiene su núcleo en la Red de Telefonía Básica; la cual se encuentra desplegada a nivel nacional, brindando los recursos que permiten a los usuarios acceder a los centros proveedores de información (CPI's). Buscando así elevar el desarrollo intelectual y cultural de la población. Hoy en día la Red IP mantiene una

tarifa Semiplana y se está evaluando los recursos necesarios para poder ofrecer una tarifa plana durante todo el día.

5.- La Red IP tiene un gran característica que es la ser escalable, ya que presenta un backbone que puede crecer en nodos y transporte ofreciendo así mayor velocidad y seguridad en todos los niveles del modelo OSI. Garantizando así el pleno desarrollo de la misma.

6.- El crecimiento de la Red IP se viene dando en gran escala en Lima y provincia. Para un mayor detalle tenemos hasta el momento unas 9000 canales telefónicos utilizados en la hora pico aproximadamente entre las 20:00 y 23:00 horas.

7.- Tenemos 2 centros de servicios (Washington y San Isidro) y 1 centro de gestión (Surquillo) mediante los cuales se realiza una labor las 24 horas contando con personal de guardia para los monitoreos de alarmas y rutinas de la red. Dichas alarmas llegan al centro de gestión mediante el protocolo SNMP.

8.- Cada 4 ó 6 meses se realizan upgrade de software de los equipos que forman parte de la Red IP (ejm. MAX TNT , BSTDX, etc)

9.- Haya que tener en cuenta que el servicio brindado por la red es de internet el cual brinda un máximo ancho de banda a los usuarios conmutados de 64 Kbps (linea normal) ó 128 Kbps para líneas RDSI. En el caso de las conexiones dedicadas el ancho de banda varía entre 64 Kbps y 2 Mbps.

10.- Para la salida a internet de cada punto de presencia mantiene 2 enlaces con el core en caso de que falle un enlace, utilizará el otro enlace como ruta de backup o respaldo.

11.- La Red IP conmutada en el Perú tiene una topología estrella.

12.- Telefónica brindará adicionalmente a los Servicios IP, una nueva generación de servicios para empresas que aúnan las prestaciones que ofrecen las tecnologías desarrolladas en Internet con la seguridad propia de las redes tradicionales de transmisión de datos las cuales son ofrecidas a empresas.

ANEXO A: GLOSARIO

ADSL	Asymmetric Digital Subscriber Line. Línea de abonado asimétrica digital. Tecnología de transmisión que ofrece un gran ancho de banda a través de la línea telefónica.
AS	Sistema Autónomo (Protocolo de ruteo BGP)
ATM	Asynchronous Transfer Mode. Modo de transferencia asíncrono (MTA). Tecnología de transferencia de datos a alta velocidad, basada en el empleo de paquetes (células) de tamaño fijo y pequeño.
BGP	Border Gateway Protocol. En las redes de datos es el protocolo de enrutamiento empleado para prolongar rutas entre grandes redes independientes.
BIND	Software de los DNSs
CATV	Cable TV. Televisión por cable
CHAP	Challenge-Handshake Authentication Protocol
CPI	Centro Proveedor de servicios de Información
DNS	Domain Name System, Domain Name Service, o Domain Name Server. Sistema de nombres de dominio
DNSSEC	Es un nuevo Standard de DNS
FDDI	Fiber Distributed Data Interface. Interfaz de datos de fibra distribuida

FR	Frame Relay. Protocolo para intercambio de datos entre un "host" y una red de datos. También alude a la red que soporta el protocolo para que los usuarios puedan intercambiar datos entre sí.
FTP	File Transfer Protocol. Protocolo de transferencia de ficheros
GSM	Global System for Mobile Communications. Estándar europeo de comunicaciones móviles digitales de segunda generación.
HDLC	High level Data Link Control. Control de enlace de datos de alto nivel
IANA	Internet Assigned Number Authority
IETF	Internet Engineering Task Force. Foro de definición de los protocolos de Internet.
INTERNIC	InterNIC, en su documento RFC1591 nos dice que el sistema de servidores de nombres de dominio DNS ("Domain Name Servers") está bajo la férula de IANA
IP	Internet Protocol. Protocolo Internet. Es el protocolo estándar utilizado por los sistemas que se comunican por Internet.
IPDC	Protocolo manejado por el Softswtch.
IPX	Internetwork Packet Exchange
ISP	Internet Service Provider. Proveedor de acceso a Internet. Empresa encargada de ofrecer la infraestructura de acceso para que los clientes puedan conectarse a Internet utilizando los medios de acceso estándar.
L2TP	Level 2 Tunneling Protocol
LAN	Local Area Network. Red de área local
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios.

LLC	Logical Link Control. Control de enlace lógico. Capa del modelo lógico de protocolos donde se engloban todos los mecanismos de gestión de un enlace lógico entre un nodo de una red y la propia red.
MAC	Medium Access Control. Control de acceso al medio. Capa del modelo lógico de protocolos donde se engloban todos los mecanismos de gestión de acceso de los diferentes nodos de una red con acceso múltiple a un mismo medio (radio, cable).
MPLS	Multi-Protocol Label Switching. Conmutación mediante etiquetas multiprotocolo. Tecnología diseñada para acelerar el flujo del tráfico en la red y facilitar su gestión.
MTU	Maximum Transmission Unit
OSI	Open Systems Interconnection. Modelo de interconexión de sistemas abiertos
OSIPTEL	Organismo Supervisor de Inversión Privada en Telecomunicaciones. Entidad reguladora del mercado de telecomunicaciones en Perú.
OSPF	Domain Name System, Domain Name Service, o Domain Name Server. Sistema de nombres de dominio
PAP	Password Authentication Protocol
POP	Point of Presence. Agrupación de dispositivos de una Red de Distribución de Contenidos (RDC o CDN) donde se hospedan los contenidos y desde donde se sirven a los usuarios finales.
PPP	Point to Point Protocol. Protocolo Punto a Punto. Protocolo definido por el IETF para la conexión TCP/IP remota entre routers o entre un nodo y una red.
PVC	Permanent Virtual Circuit
QoS	Quality of Service. Calidad de Servicio. Término genérico para definir el conjunto de parámetros que definen el tipo y la calidad del servicio proporcionado.
RAS	Centro Proveedor de servicios de Información

RDSI	Red Digital de Servicios Integrados (o en inglés, ISDN, Integrated Services Digital Network).Red de comunicaciones normalizada por las recomendaciones de la serie I de ITU-T (antes CCITT), que tiene como objetivo la comunicación digital de voz, datos e imágenes a través de una sola conexión física
RFC	Request For Comments. Literalmente, petición de comentarios. Mecanismo de revisión de los borradores de documentos en el marco del IETF de cara a convertirse en un estándar de Internet
RIP	Routing Information Protocol. Protocolo de enrutamiento dinámico.
RIPV2	Routing Information Protocol version 2.
RTB	Red Telefónica Básica
SDH	Synchronous Digital Hierarchy. Jerarquía digital síncrona.Técnica de multiplexación de datos para sistemas de transmisión en los que se sincronizan transmisor y receptor.
SNMP	Simple Network Management Protocol. Protocolo de gestión y supervisión de red que permite el acceso y la modificación de objetos de una MIB (Management Information Base) dentro de un determinado elemento de red.
SS7	Sistema de Señalización número 7 (o SSN7). Conjunto de estándares y protocolos utilizados en las redes de telecomunicación para la transmisión de información de señalización.
STP	Signaling Transference Point. (Punto de Transferencia de Señalización)
TCP/IP	Es el protocolo estándar utilizado por los sistemas que se comunican por Internet.
TOS	Type of Service

URL	Es un identificador único para la localización de recursos de Internet, tales como direcciones web, páginas, ficheros, etc
USS	Universal State Server
VLAN	Virtual Local Area Network. Red de área local virtual
VNN	Protocolo propietario de Lucent Technologies
WAN	Wide Area Network. Red de área extensa. Red de datos constituida por nodos situados en emplazamientos distantes y unidos entre sí por líneas de comunicación.
WEB	Sistema basado en hipertexto que permite buscar y tener acceso a recursos de Internet, y que soporta presentaciones multimedia con audio, vídeo, texto y gráficos.
X25	Conjunto de protocolos desarrollados por la ITU para redes de transmisión de paquetes.

ANEXO B: ÍNDICE DE ILUSTRACIONES

ANEXO C: ÍNDICE DE TABLAS

BIBLIOGRAFÍA

1.- Alcócer García A. Carlos,"Redes de Computadoras", INFOLINK E.I.R.L. , Lima 2000

2.- Curso de Capacitación-Telematic, "Curso de TCP IP", Telematic, Junio 2002

3.- Cursos Lucent Technologies, "ARQUITECTURA DE LA RED IP LUCENT", Abril 2001

4.- Jordi Tarrigas, "Difusión de redes dentro de internet", Editorial Lmdata, Agosto 2000

5.- José Manuel Caballero, "REDES DE BANDA ANCHA" Marcombo Boixareus Editores, 1998

Páginas de Internet

http://www.cec.uchile.cl/nuevoSitio/atencus/conexConmutada_95.html

http://fmc.axarnet.es/redes/anexo_1.htm

http://fmc.axarnet.es/redes/indice_m.htm

http://iio.ens.uabc.mx/~jmilanez/escolar/redes/temario.html

http://www.lucent.com/products/solution/0,,CTID+2014-STID+10443-SOID+589-LOCL+1,00.html

http://www.cisco.com/global/PE/sne/cmc/glosario.shtml