UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"CAMPUS ARAGÓN"

"PROYECTO DE REESTRUCTURACIÓN DEL BACKBONE DE REDUNAM"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO

E L E C T R I C I S T A

(AREA ELECTRICA ELECTRÓNICA)

P R E S E N T A N:

HUGO MENDEZ VARA

EDGAR RIVERA BARRERA

ASESOR : ING. RAUL BARRON VERA

MÉXICO. **2003**

A

PAGINACION

DISCONTINUA

UNIVERSIDAD NACIONAL AVENTAMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN – UNAM

JEFATURA DE CARRERA DE INGENIERIA MECÁNICA ELÉCTRICA

OFICIO No. ENAR/JAME/0563/2003.

ASUNTO: Sínodo (Tesis Conjunta).

LIC. ALBERTO IBARRA ROSAS
SECRETARIO ACADÉMICO
P R E S E N T E

Por este conducto me permito relacionar los nombres de los Profesores que sugiero integren el Sínodo del Examen Profesional del alumno: **HUGO MÉNDEZ VARA**, con número de cuenta: **09333075-8**, con el tema de tesis: **"PROYECTO DE REESTRUCTURACIÓN DEL BACKBONE DE RED UNAM".**

PRESIDENTE:	**ING. RAÚL BARRÓN VERA**	**OCTUBRE**	**78**
VOCAL:	**ING. JUAN GASTALDI PÉREZ**	**OCTUBRE**	**79**
SECRETARIO:	**ING. ELEAZAR MARGARITO PINEDA DÍAZ**	**OCTUBRE**	**80**
SUPLENTE:	**ING. PABLO LUNA ESCORZA**	**ENERO**	**96**
SUPLENTE:	**ING. JOSÉ LUIS GARCÍA ESPINOSA**	**AGOSTO**	**98**

Quiero subrayar que el Director de Tesis es el Ing. Raúl Barrón Vera, quien esta incluido basándose en lo que reza el Reglamento de Exámenes Profesionales de esta Escuela.

A t e n t a m e n t e.
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Bosques de Aragón, Estado de México, 10 de junio de 2003.
EL JEFE DE CARRERA

ING. RAÚL BARRÓN VERA

C.c.p.- Lic. Ma. Teresa Luna Sánchez.- Jefa del Depto. de Servicios Escolares.
C.c.p.- Ing. Raúl Barrón Vera.- Asesor.
C.c.p.- Alumno
RBV/amce.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

SECRETARÍA ACADÉMICA

Ing. RAÚL BARRÓN VERA
Jefe de la Carrera de Ingeniería Mecánica Eléctrica,
Presente.

En atención a la solicitud de fecha 10 de junio del año en curso, por la que se comunica que los alumnos HUGO MENDEZ VARA y EDGAR RIVERA BARRERA, de la carrera de Ingeniero Mecánico Electricista, han concluido su trabajo de investigación intitulado "PROYECTO DE REESTRUCTURACIÓN DEL BACKBONE DE REDUNAM", y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 10 de junio del 2003
EL SECRETARIO

Lic. ALBERTO IBARRA ROSAS

C p Asesor de Tesis.
C p Interesado.

AIR/vr

UNIVERSIDAD NACIONAL AVENIDA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN – UNAM

JEFATURA DE CARRERA DE INGENIERIA MECÁNICA ELÉCTRICA

OFICIO No. ENAR/JAME/0564/2003.

ASUNTO: Sínodo (Tesis Conjunta).

LIC. ALBERTO IBARRA ROSAS
SECRETARIO ACADÉMICO
P R E S E N T E

Por este conducto me permito relacionar los nombres de los Profesores que sugiero integren el Sínodo del Examen Profesional del alumno: **EDGAR RIVERA BARRERA,** con número de cuenta: **09311016-7,** con el tema de tesis: **"PROYECTO DE REESTRUCTURACIÓN DEL BACKBONE DE RED UNAM".**

PRESIDENTE:	**ING. RAÚL BARRÓN VERA**	**OCTUBRE**	**78**
VOCAL:	**ING. JUAN GASTALDI PÉREZ**	**OCTUBRE**	**79**
SECRETARIO:	**ING. ELEAZAR MARGARITO PINEDA DÍAZ**	**OCTUBRE**	**80**
SUPLENTE:	**ING. PABLO LUNA ESCORZA**	**ENERO**	**96**
SUPLENTE:	**ING. JOSÉ LUIS GARCÍA ESPINOSA**	**AGOSTO**	**98**

Quiero subrayar que el Director de Tesis es el Ing. Raúl Barrón Vera, quien esta incluido basándose en lo que reza el Reglamento de Exámenes Profesionales de esta Escuela.

A t e n t a m e n t e .
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Bosques de Aragón, Estado de México, 10 de junio de 2003.
EL JEFE DE CARRERA

ING. RAÚL BARRÓN VERA

C.c.p - Lic. Ma. Teresa Luna Sánchez.- Jefa del Depto. de Servicios Escolares.
C.c.p.- Ing. Raúl Barrón Vera.- Asesor.
C.c.p.- Alumno
RBV/amce.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

SECRETARÍA ACADÉMICA

Ing. RAÚL BARRÓN VERA
Jefe de la Carrera de Ingeniería Mecánica Eléctrica,
Presente.

En atención a la solicitud de fecha 10 de junio del año en curso, por la que se comunica que los alumnos EDGAR RIVERA BARRERA y HUGO MENDEZ VARA, de la carrera de Ingeniero Mecánico Electricista, han concluido su trabajo de investigación intitulado "PROYECTO DE REESTRUCTURACIÓN DEL BACKBONE DE REDUNAM", y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 10 de junio del 2003
EL SECRETARIO

Lic. ALBERTO IBARRA ROSAS

C p Asesor de Tesis.
C p Interesado.

AIR/vr

E

Agradecimientos:

A Dios:
Por estar siempre a mi lado, darme salud y la bendición de estar con la gente que quiero y aprecio.

A mi Mamá Vicky:
Por todo el apoyo y por todos sus esfuerzos que hicieron posibles la conclusión de esta etapa de mi vida, gracias por todo tu entusiasmo y por todas tus palabras de aliento que llegaban siempre en el momento que más las necesitaba, y que sin duda hoy nos hacen juntos alcanzar esta meta.

A mi Papá Franco:
Gracias por todo tu cariño, comprensión y apoyo incondicional, a lo largo de toda la vida.

A mis hermanas Sony y Ross:
Por todos los buenos momentos que compartimos juntos, por todos esos enojos, por todas esas alegrías y por todo su interés e insistencia para que culminara este trabajo. "Las quiero Mucho"

Armando Trejo Chavez:
Gracias por tus palabras de aliento, que llegaron en el momento preciso y sin las cuales quizás hoy no estaría haciendo este trabajo de tesis.

Mamá Esther y Papá Joel:
Gracias por todo el apoyo que incondicionalmente me han brindado durante tanto tiempo, pero sobre todo gracias por su cariño y amistad.

Gibran.
Gracias Por dejarme ser parte de tu familia, por tu apoyo y amistad incondicional a lo largo de toda nuestra carrera.

Itzel Peralta Ramirez.
Gracias por lo felices que hemos sido, por estar siempre a mi lado, escucharme y apoyarme en los momentos difíciles por creer en mi y por ser no nada mas una novia sino una amiga.

Lic. Alberto Ibarra Rosas.
Gracias por todo su apoyo y comprensión a lo largo de mi estancia en la E.N.E.P.

Universidad Nacional Autónoma de México UNAM:
Gracias por la oportunidad de desarrollarme profesionalmente y alcanzar uno de los mas grandes objetivos de mi vida.

DGSCA Dirección General de Estudios de Cómputo Académico.
Por haberme dado la oportunidad de desarrollarme profesionalmente, para poder desarrollar este trabajo.

A mis amigos:
Gracias a todos mis amigos y en general a toda la gente que directamente o indirectamente me ayudaron a alcanzar este objetivo:

Alfred, Lulú, Edgar, GabyM, Felpa, Hans, Alex, Chio, Yola, Hugol, Charly Noc, Greg Lemus, Gerson, Pao, Isabel Nic, Isabel Tac, Luis, Arturo, joel, Marcov, Raypich, Ale Bombón Yesi, Romayn, Norberto, Oscar Lindoro, Gabriel, Angel.

Y a todos los que se me olvidan en este instante, pero que no por eso son menos importantes para mi.

HUGO MENDEZ VARA

AGRADECIMIENTOS

Gracias Dios por permitirme concluir este trabajo
Te doy las gracias por tener a mis padres conmigo para ver culminada su obra, ya que por ellos no desisti en la meta, por sus consejos, amor y esfuerzo
Gracias por decirme no te rindas e inspirarme para dar un paso mas

Gracias Papá y Mamá por todo el apoyo que me han brindado
A quien admiro por su paciencia y fortaleza para enfrentar los problemas y realizar lo que se proponen por su valor, ayuda y amor que siempre es de manera incondicional

Gracias Miri n y Elizabeth

Gracias UNAM por recibirme y brindarme tanta sabiduría

Gracias DGSCA, Alfred , Hugo , Hugol, Rocio, Deborah, Yolanda, Arthur, Alex, Felpa, Hans, Marco, Charly y a todos los compañeros del TAC, NOC y NIC.

Gracias a todos los que me apoyaron de alguna manera, indirecta o directamente para que concluyera este trabajo

Edgar Rivera Barrera

PROYECTO DE REESTRUCTURACIÓN DEL BACKBONE DE RedUNAM.

INDICE

INTRODUCCION.

El desarrollo acelerado de la sociedad en el mundo, principalmente en el ámbito económico y financiero, ha traído como consecuencia el desarrollo de la industria de las telecomunicaciones, ello debido a la necesidad de estar en contacto directo con las personas que nos rodean desde cualquier punto geográfico. Esta necesidad de comunicación en un principio solamente requería de aplicaciones tradicionales, como es el caso de la voz. – Sin embargo a medida que los mercados mercantiles y de servicio fueron creciendo, las aplicaciones tradicionales no fueron suficientes teniéndose la necesidad de desarrollar otros sistemas de comunicación que tuvieran el objetivo de satisfacer la demanda de dichas sociedades.

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadoras, así como a la puesta en orbita de los satélites de comunicación.

A medida que avanzamos como sociedad, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de las computadoras ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener una sola computadora para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de computadoras separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de computadoras. Estas nos dan a entender una colección interconectada de computadoras autónomas. Se dice que las PC'S están interconectadas, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones es valido además de que son también medios alternos.

Lo anteriormente expuesto trae como consecuencia que desde principios de la década de los 80 las empresas que cuentan con redes privadas, habían

tenido dificultades para resolver el problema de conectar diferentes tipos de computadoras, como máquinas basadas en UNIX, IBM compatibles y Macintosh; para compartir información. La aplicación de las tecnologías de Internet a una red privada, soluciona muchos de estos problemas de incompatibilidad de hardware y software. Y más específicamente, una red corresponde a la utilización de estas tecnologías para desarrollar aplicaciones que son empleadas dentro de una organización, las cuales han encontrado que las redes pueden ayudar a sus miembros para lograr un flujo de información más oportuno y menos costoso, aunque igualmente saben que un óptimo desarrollo de esta tecnología depende directamente de su desempeño, el cual se ve reflejado sobre toda su red, en momentos en los que la manera de trabajar en las organizaciones modernas se ha visto altamente afectada en la medida que las redes de computadoras se han tornado cada vez más extensas y poderosas, además que la actualización a nuevas versiones de software de aplicaciones que corren en ambientes cliente-servidor, ocurre más rápido que la modernización del hardware de red (routers, switches ,etc.) e incluso que la ampliación de la capacidad de los enlaces WAN, y muchas veces, esto se traduce en problemas de red relacionados principalmente con la reserva de los recursos y la administración o manejo.

Por esta razón una organización debe estar en permanente conocimiento de las condiciones en las que está trabajando su red de computadoras, para así poder determinar la forma en que podría verse afectada y tomar medidas que la hagan más eficaz.

Actualmente el desarrollo de un país, además de medirse por su componente fundamental que es el PIB, tiene una componente adicional que es su infraestructura de telecomunicaciones, esto se debe fundamentalmente al impresionante desarrollo de la tecnología y los sistemas de información y a la imperiosa necesidad de contar con la información en el preciso momento en que ésta se genera. El resultado de estos vertiginosos cambios a provocado enormes cambios en las sociedades del todo el mundo.

Hoy en día, una sociedad exitosa es aquella que cuenta con información de manera oportuna, es decir, contar con la información en el instante mismo en que ésta se genera y es aquí donde las telecomunicaciones juegan un papel fundamental para conseguir el objetivo.

El fenómeno de la globalización es el mejor de los ejemplos, ya que aquellos países que adolecen de una infraestructura de telecomunicaciones moderna y eficaz, simplemente se quedan rezagados debido a la falta de comunicación y de información

Sin lugar a dudas, el cómputo y las telecomunicaciones representan el factor de cambio más importante en el desarrollo de la tecnología y permiten que Internet sea hoy en día una herramienta fundamental para el desarrollo de las actividades de la sociedad en ámbitos tan diversos como el comercial, financiero, académico y de investigación, entretenimiento, etc.

En materia de telecomunicaciones, la UNAM inició un proceso completo de renovación y crecimiento tecnológico que da inicio en el año de 1989, siendo este uno de los seis proyectos prioritarios de aquella administración. Durante ese año se crea la Dirección de Telecomunicaciones, cuyo objetivo era crear la Red Integral de Telecomunicaciones de la UNAM. Esta red debería de ser capaz de transmitir voz, datos imágenes y posteriormente vídeo entre las dependencias universitarias, ubicadas desde Ensenada, B.C. hasta Puerto Morelos, Q. Roo.

Los objetivos principales de esta red son:

- Integrar a sus alumnos, desde el bachillerato hasta el posgrado, a la cultura informática, entendida esta como la integración del cómputo y las telecomunicaciones. Incorporar la enseñanza de la informática a los planes formales de estudio de todas las Disciplinas y actualizarla periódicamente.
- Proporcionar a su personal docente y de investigación todas las herramientas de la tecnología informática para el desarrollo de sus actividades.
- Dotar a la institución de una moderna infraestructura de telecomunicaciones y cómputo.

Durante la primera etapa, en el año de 1989, se instala una red nacional privada satelital conformada por 7 estaciones terrenas para la transmisión de voz y datos. Paralelamente se sustituye el sistema telefónico en el campus de Ciudad Universitaria por una red de conmutadores telefónicos digitales que paulatinamente se incrementa para incorporar a los siete campus de las Unidades Multidisciplinarias distribuidas en el área metropolitana.

En el campus de Ciudad Universitaria inicia un proceso acelerado de crecimiento en su Red de datos con una topología de anillo en el backbone de FDDI a 10 Mbps. En este momento la UNAM es la primera Institución latinoamericana en conectarse a Internet y es el principal protagonista del internet en México.

A finales de 1992, esta red contaba ya con 31 nodos de cómputo y telecomunicaciones enlazados a través de fibra óptica, vía satélite o vía microondas y se destaca la incorporación de la Ciudad de la Investigación Científica en Cuernavaca, Mor.

El servicio de internet es uno de los recursos más utilizados por los investigadores de la UNAM. Internet se ofrece también a universidades públicas del interior de la república, así como a universidades públicas y privadas en el D.F. y área metropolitana

A finales de 1994 se incorpora la tercera red con el propósito de llevar educación a distancia a través de videoconferencia a la comunidad universitaria.

En junio de 1997 la infraestructura de telecomunicaciones tenía más de 15,000 computadoras conectadas a la Red de datos, más de 10,000 líneas del sistema telefónico digital, 20 salas de videoconferencia y 5 enlaces internacionales con capacidad de transmisión de 10 Mbps a USA para la conexión a internet. En esta fecha, el campus de Juriquilla, Qro. se integra a esta gran Red.

En agosto de 1997 la UNAM inicia operaciones con un backbone ATM que le permite consolidar con esta tecnología las redes de voz, datos y vídeo en una plataforma multimedia. En esta fecha se coloca la Institución como una de las redes más modernas y más grandes en el ámbito académico en Latinoamérica al contar con esta moderna tecnología y comparada incluso con redes de universidades de Norteamérica

En el año de 1998 se incorpora el Campus Morelia en Michoacán. Actualmente, más del 96 % del total de las instalaciones de la Universidad están integradas a la Red con 21,500 computadoras conectadas, más de 13,000 líneas telefónicas en operación y 36 salas propias de videoconferencia que forman parte de la Red Nacional de Videoconferencia integrada por un total de 130 salas. Se tienen en operación 13 enlaces con capacidad de 25 Mbps para el tráfico de internet y 1 Mbps para el tráfico de videoconferencia del tipo H.320.

Es importante destacar que la Red Integral de Telecomunicaciones es completamente privada y propiedad de la UNAM y es operada en su totalidad por personal de la Dirección de Telecomunicaciones

RedUNAM es el proyecto desarrollado para la transmisión de datos entre las facultades, institutos, centros de difusión, coordinaciones y demás dependencias que conforman a la UNAM, y es parte integral de la Red Integral de las Telecomunicaciones.

En consecuencia y con la velocidad que salen al mercado innovaciones tecnológicas es el momento de realizar el proyecto de "REESTRUCTURACION DEL BACKBONE DE REDUNAM", con la finalidad de seguir manteniendo a RedUNAM a la vanguardia no solo en México sino a nivel internacional,

El presente trabajo consta de cinco capítulos principalmente, cada uno de ellos nos presenta aspectos fundamentales de las redes de computadoras; el primer capitulo nos menciona algunos aspectos teóricos como conceptos básicos de redes de computadoras, en el cual se trata de ver el modelo OSI, ventajas y desventajas de dos estándares como Ethernet y ATM, así como algunos otros conceptos en general. Entre los puntos importantes que definiremos esta TCP/IP, que es un punto importante para la comprensión de cómo esta estructurada la RedUNAM.

En el segundo capitulo nos habla de cómo se constituye la red Actual, de igual manera se mencionan las necesidades que surgen con el paso del tiempo y que hacen que la RedUNAM sufra una reestructuración para poder seguir brindado servicios de calidad a sus usuarios finales.

El tercer capitulo se realizará una evaluación de tecnologías, para poder finalmente recomendar lo óptimo para su funcionamiento y sus necesidades, así como su escalabilidad.

En el cuarto capitulo tocaremos la solución propuesta y el proceso de migración que se tiene que llevar a cabo para que la red opere al 100%, también en este capitulo se plantearan los alcances, el horizonte, pero sin olvidar el como repercutirá en la actual estructura de RedUNAM como es el caso de los recursos humanos.

En el quinto capitulo se abordara la manera bajo la cual se hará la adquisición de los bienes siempre apegándose a las leyes y de esta manera podremos, ver la reestructuración desde otro punto de vista.

OBJETIVO:

El objetivo de este trabajo de tesis es poder documentar y compartir la inigualable experiencia de realizar un proyecto de tal magnitud, que sin duda es uno de los proyectos mas importantes para la UNAM y para México, ya que a través de la reestructuración realizada a la RedUNAM esta podrá ofrecer mayores recursos de comunicaciones a todos sus usuarios, con base en las necesidades actuales, ya que se ha implementando un backbone Gigabit Ethernet que es capaz de soportar de forma óptima todos los servicios de datos, voz y video sobre IP, y aplicaciones emergentes que de ella se demanden; además de ser suficientemente flexible para permitir el crecimiento cuando éste se requiera.
También la UNAM podrá ofrecer a sus usuarios un nivel de estabilidad mucho mayor en comparación con el que se tenía, esto quiere decir que el tiempo fuera de operación de la red se habrá disminuido de manera considerable,
Como ultimo punto pero no menos importante es el poder haber implementado un protocolo de ruteo estándar, con el cual anteriormente no contábamos, lo cual hoy en día, nos permite trabajar con estándares y poder unir a la RedUNAM, prácticamente a equipos de cualquier fabricante que cumpla con los estándares y normas internacionales.

CAPITULO 1

CONCEPTOS BÁSICOS.

1.1 El Modelo OSI

Es un modelo abierto para la interconexión de redes desarrollado por la ISO (International Standard Organization) con la finalidad de crear un modelo únicamente de referencia sobre el cual todos los fabricantes deberían de trabajar para garantizar la interoperabilidad de redes entre marcas esto debido a que anteriormente los desarrollos se hacían de manera propietaria lo cual provocaba la falta de interoperabilidad de comunicación entre redes que ocupaban distintas especificaciones.

Este modelo se desarrollo en capas ya que si analiza esta interacción desde el punto de vista de las capas se podría entender más claramente algunos de los problemas de la comunicación (entre las personas o entre las maquinas) y cómo es posible resolver estos problemas.

Esta división de las funciones se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje

El modelo OSI define 7 capas como se muestra en la tabla 1.

Nivel	Nombre
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace
1	Fisico

Tabla No 1 Capas del Modelo OSI

A continuación se muestra una breve descripción de cada una de ellas

Nivel Físico (Phisical Layer); este nivel define las características físicas de la interfaz, como componentes mecánicos y conectores, aspectos eléctricos como niveles de voltaje que representan cada valor binario, y aspectos funcionales como establecimiento, mantenimiento y liberación de enlace físico. Interfaces de nivel físico para comunicaciones incluyen EIA RS–232.

Nivel de Enlace de Datos (Data Link Layer); este nivel define las reglas para enviar y recibir información a través de la conexión física entre dos sistemas. Este nivel codifica y descompone los datos para su transmisión, además de proporcionar detección y control de errores. Los puentes (bridges) actúan en este nivel en el grupo de protocolos. A continuación se presenta una lista de protocolos que ocupan este nivel.

- Control de enlace de datos de alto nivel (High-level Data Link Control HDLC).Manejadores y métodos de acceso de LAN, como Ethernet o Token Ring.
- ATM para redes de área extensa WAN de transmisión rápida.
- Network Driver Interface Specification (NDIS) de Microsoft.
- Open Datalink Interface (NODI) de Novell

Nivel de Red (Network Layer); este nivel define los protocolos para abrir y mantener un camino en la red entre sistemas. Está relacionado con los procedimientos de conmutación y transmisión de datos y oculta dichos procedimientos a los niveles superiores. Los "routers" actúan en este nivel. Este nivel vela por que los paquetes sean dirigidos a su destino en la red. Si está dirigido a un segmento de la red, este nivel lo envía a un dispositivo de enrutamiento el cual lo reenvía a su destino. A continuación se muestra una lista de protocolos que ocupan este nivel.

- Protocolo de Internet (IP)
- Protocolo X.25
- Internetwork Packet Exchange (IPX) de Novell.
- VINES Internet Protocol (VIP)

Nivel de Transporte (Transport Layer); este nivel proporciona un control de alto nivel para la transferencia de datos entre sistemas, incluyendo funcionalidades de manejo de errores más sofisticados, niveles de prioridad y seguridad. El nivel de transporte proporciona servicio de calidad y entrega precisa, proporcionando servicios orientados a conexión entre sistemas finales. Controla la secuencia de paquetes, regula el flujo de tráfico y reconoce paquetes duplicados. Este nivel asigna al paquete un número de secuencia el cual es comprobado en su destino. Si se pierden datos del paquete, el protocolo del nivel de transporte coordina con el nivel de trasporte de origen para la retransmisión del paquete. Este nivel asegura que se reciban los datos en el orden apropiado. Los siguientes protocolos pueden estar en este nivel:

- Internet Transport Protocol (TCP)
- Internet User Datagram Protocol (UDP)

- Sequenced Packed Exchange (SPX)
- NetBios/NetBEUI

Nivel de Sesión (Sesion Layer); este nivel coordina el intercambio de información ente sistemas utilizando técnicas conversacionales o diálogos. No siempre se requiere el diálogo, pero algunas aplicaciones pueden precisar una forma de saber dónde volver a comenzar la transmisión de datos si se pierde temporalmente la conexión o pueden necesitar un diálogo periódico para indicar el final de un conjunto de datos y el comienzo de uno nuevo.

Nivel de Presentación (Presentation Layer); los protocolos del nivel de presentación son parte del sistema operativo y de las aplicaciones utilizadas por el usuario en una estación de trabajo. Se le da formato a la información en este nivel para ser visualizada e impresa. También son interpretados los códigos dentro de los datos, como tabuladores y caracteres especiales. Asimismo es en este nivel donde se lleva a cabo la encriptación de datos y traducción desde otros juegos de caracteres.

Nivel de Aplicación (Aplication Layer); las aplicaciones acceden a los servicios de red subyacentes, utilizando procedimientos definidos en este nivel. El nivel de aplicación se utiliza para definir un rango de aplicación que manejan transferencia de archivos, e intercambio de mensajes Ej. Correo Electrónico. A continuación se listan algunos protocolos utilizados en este nivel;

- Terminal Virtual
- File Transfer Access and Management (FTAM)
- Distributed Transaction Processing (DTP)

Todas las comunicaciones de una red parten de un origen y se envían a un destino, y la información que se envía a través de una red se denomina datos o paquete de datos. Si una maquina (host A) desea enviar datos a otra (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento.

El encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información. (Nota: La palabra "encabezado" significa que se ha agregado la información correspondiente a la dirección).

Para ver cómo se produce el encapsulamiento, examinamos la forma en que los datos viajan a través de las capas como lo ilustra la figura 1.1. Una vez que se envían los datos desde el origen, como se describe en la figura, viajan a través de la capa de aplicación y recorren todas las demás capas en sentido descendiente. Como puede ver, el empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las redes ofrecen sus servicios a los usuarios finales.

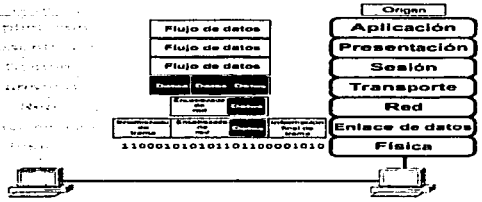


Fig. 1.1 Flujo de datos

Las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

1. **Crear los datos.**
   Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la red.

2. **Empaquetar los datos para ser transportados de extremo a extremo.**
   Los datos se empaquetan para ser transportados por la red. Al utilizar segmentos, la función de transporte asegura que los hosts del mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.

3. **Anexar (agregar) la dirección de red al encabezado.**
   Los datos se colocan en un paquete o datagrama que contiene el encabezado de red con las direcciones lógicas de origen y de destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

4. **Anexar (agregar) la dirección local al encabezado de enlace de datos.**
   Cada dispositivo de la red debe poner el paquete dentro de una trama. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

5. **Realizar la conversión a bits para su transmisión.**
   La trama debe convertirse en un patrón de unos y ceros (bits) para su

transmisión a través del medio (por lo general un cable). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio. El medio en la internetwork física puede variar a lo largo de la ruta utilizada. Por ejemplo, el mensaje de correo electrónico (ver Fig. 1.2) puede originarse en una LAN, cruzar el backbone de un campus y salir por un enlace WAN hasta llegar a su destino en otra LAN remota. Los encabezados y la información final se agregan a medida que los datos se desplazan a través de las capas del modelo OSI.

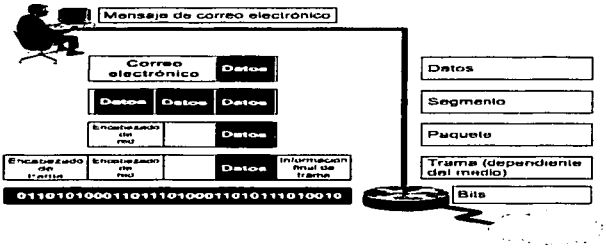


Fig. 1.2 Mensaje de correo electrónico

1.2 EL Modelo TCP/IP

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el *Protocolo de control de transmisión/Protocolo Internet (TCP/IP)*. El modelo de referencia *TCP/IP* y la *pila de protocolo TCP/IP* hacen que sea posible la comunicación entre dos maquinas, desde cualquier parte del mundo, a casi la velocidad de la luz. El modelo TCP/IP tiene importancia histórica, al igual que las normas que permitieron el desarrollo de la industria telefónica, de energía eléctrica, el ferrocarril, la televisión.

El Departamento de Defensa de EE.UU. (*DoD*) creó el modelo TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. Para brindar un ejemplo más amplio, supongamos que el mundo está en estado de guerra, atravesado en todas direcciones por distintos tipos de conexiones: cables, microondas, fibras ópticas y enlaces satelitales. Imaginemos entonces que se necesita que fluya la información o los datos (organizados en forma de paquetes), independientemente de la condición de cualquier nodo o red en particular de Internet (que en este caso podrían haber sido destruidos por la guerra). El DoD desea que sus paquetes lleguen a destino siempre, bajo cualquier condición, desde un punto determinado hasta cualquier otro. Este problema de diseño de difícil solución fue lo que llevó a la

creación del modelo TCP/IP, que desde entonces se transformó en el estándar a partir del cual se desarrolló Internet.

El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la *capa de Internet* y la capa de acceso de red (ver tabla 2). Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. No confundamos las capas de los dos modelos, porque la capa de aplicación tiene diferentes funciones en cada modelo.

Tabla 2 Capas del Modelo TCP/IP

Capa de aplicación

Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Simplemente crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y garantiza que estos datos estén correctamente empaquetados para la siguiente capa.

Capa de transporte

La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. TCP es un protocolo orientado a la conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a la conexión no significa que el circuito exista entre las maquinas que se están comunicando (esto sería una conmutación de circuito). Significa que los segmentos de Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período. Esto se conoce como conmutación de paquetes.

Capa de Internet

El propósito de la *capa de Internet* es enviar paquetes origen desde cualquier red en Internet y que estos paquetes lleguen a su destino independientemente

de la ruta y de las redes que recorrieron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Esto se puede comparar con el sistema postal. Cuando envía una carta por correo, usted no sabe cómo llega a destino (existen varias rutas posibles); lo que le interesa es que la carta llegue.

Capa de acceso de red

El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

El diagrama que aparece en la figura 1.3 se denomina *gráfico de protocolo*. Este gráfico ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP. En la capa de aplicación, aparecen distintas tareas de red que probablemente usted no reconozca, pero como usuario de la Internet, probablemente use todos los días.
Estas aplicaciones incluyen las siguientes:

- *FTP*: File Transfer Protocol (Protocolo de transferencia de archivos)
- *HTTP*: Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto)
- *SMTP*: Simple Mail Transfer Protocol (Protocolo de transferencia de correo simple)
- *DNS*: Domain Name System (Sistema de nombres de dominio)
- *TFTP*: Trivial File Transfer Protocol (Protocolo de transferencia de archivo trivial)

El modelo TCP/IP enfatiza la máxima flexibilidad, en la capa de aplicación, para los creadores de software. La capa de transporte involucra dos protocolos: el protocolo de control de transmisión (TCP) y el *protocolo de datagrama de usuario (UDP)*.

La capa inferior, la capa de acceso de red, se relaciona con la tecnología específica de LAN o WAN que se utiliza.

En el modelo TCP/IP existe solamente un protocolo de red: el protocolo Internet, o IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada. *IP* sirve como protocolo universal que permite que cualquier maquina en cualquier parte del mundo pueda comunicarse en cualquier momento.

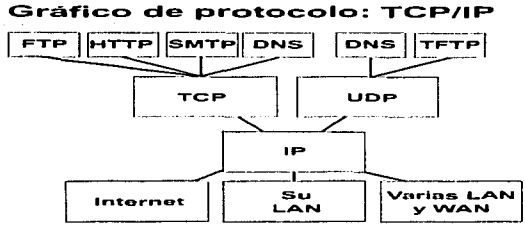


Figura 1.3

Si se compara el modelo OSI y el modelo TCP/IP, se observará que ambos presentan similitudes y diferencias (figura 1.4). Los ejemplos incluyen:

Similitudes

- Ambos se dividen en capas
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos
- Ambos tienen capas de transporte y de red similares
- Se supone que la tecnología es de conmutación por paquetes (no de conmutación por circuito)
- Los profesionales en el área de redes deben conocer ambos

Diferencias

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación
- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía

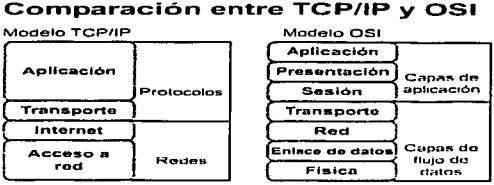


Figura 1.4

1.3 ETHERNET

Ethernet es la tecnología de red de área local (LAN) de uso más generalizado. El diseño original de Ethernet representaba un punto medio entre las redes de larga distancia y baja velocidad y las redes especializadas de las aulas de cómputo, que transportaban datos a altas velocidades y a distancias muy limitadas. Ethernet se adecua bien a las aplicaciones en las que un medio de comunicación local debe transportar tráfico esporádico y ocasionalmente pesado, a velocidades muy elevadas.

La arquitectura de red Ethernet tiene su origen en la década de los '60 en la Universidad de Hawai, donde se desarrolló el método de acceso utilizado por Ethernet, o sea, el CSMA/CD (acceso múltiple con detección de portadora y detección de colisiones. El centro de investigaciones PARC (Palo Alto Research Center) de Xerox Corporation desarrolló el primer sistema Ethernet experimental a principios de la década 1970-80. Este sistema sirvió como base de la especificación 802.3 publicada en 1980 por el Instituto de Ingeniería Eléctrica y Electrónica (Institute of Electrical and Electronic Engineers (IEEE)).

Poco después de la publicación de la especificación IEEE 802.3 en 1980, Digital Equipment Corporation, Intel Corporation y Xerox Corporation desarrollaron y publicaron conjuntamente una especificación Ethernet denominada "Versión 2.0" que era sustancialmente compatible con la IEEE 802.3. En la actualidad, Ethernet e IEEE 802.3 retienen en conjunto la mayor parte del mercado de protocolos de LAN. Hoy en día, el término Ethernet a menudo se usa para referirse a todas las LAN de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD), que generalmente cumplen con las especificaciones Ethernet, incluyendo IEEE 802.3.

Ethernet e IEEE 802.3 especifican tecnologías similares; ambas son LAN de tipo CSMA/CD. Las estaciones de una LAN de tipo CSMA/CD pueden acceder a la red en cualquier momento. Antes de enviar datos, las estaciones

CSMA/CD escuchan a la red para determinar si se encuentra en uso. Si lo está, entonces esperan. Si la red no se encuentra en uso, las estaciones comienzan a transmitir. Una colisión se produce cuando dos estaciones escuchan para saber si hay tráfico de red, no lo detectan y, acto seguido transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde. Los algoritmos de postergación determinan el momento en que las estaciones que han tenido una colisión pueden volver a transmitir. Las estaciones CSMA/CD pueden detectar colisiones, de modo que saben en qué momento pueden volver a transmitir.

Tanto las LAN Ethernet como las LAN IEEE 802.3 son redes de broadcast. Esto significa que cada estación puede ver todas las tramas, aunque una estación determinada no sea el destino propuesto para esos datos. Cada estación debe examinar las tramas que recibe para determinar si corresponden al destino. De ser así, la trama pasa a una capa de protocolo superior dentro de la estación para su adecuado procesamiento.

Existen diferencias sutiles entre las LAN Ethernet e IEEE 802.3. Ethernet proporciona servicios que corresponden a las Capas 1 y 2 del modelo de referencia OSI. IEEE 802.3 especifica la capa física, la Capa 1 y la porción de acceso al canal de la capa de enlace de datos, la Capa 2, pero no define un protocolo de Control de Enlace Lógico. Tanto Ethernet como IEEE 802.3 se implementan a través del hardware. Normalmente, el componente físico de estos protocolos es una tarjeta de interfaz en una maquina host o son circuitos de una placa de circuito impreso dentro de una maquina host.

El formato de la trama de ethernet y 802.3 consta de diversos campos los cuales se detallan a continuación (ver figura 1.5).

Los campos de trama Ethernet e IEEE 802.3 se describen en los siguientes resúmenes:

- *preámbulo*: El patrón de unos y ceros alternados les indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de trama (SOF) de la trama IEEE 802.3.

- *inicio de trama (SOF)*: El byte delimitador de IEEE 802.3 finaliza con dos bits 1 consecutivos, que sirven para sincronizar las porciones de recepción de trama de todas las estaciones de la LAN. SOF se especifica explícitamente en Ethernet.

- *direcciones destino y origen*: Los primeros 3 bytes de las direcciones son especificados por IEEE según el proveedor o fabricante. El proveedor de Ethernet o IEEE 802.3 especifica los últimos 3 bytes. La dirección origen siempre es una dirección unicast (de nodo único). La dirección destino puede ser unicast, multicast (grupo de nodos) o de broadcast (todos los nodos).

- *tipo (Ethernet)*: El tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.

- *longitud (IEEE 802.3)*: La longitud indica la cantidad de bytes de datos que sigue este campo.

- *datos (Ethernet)*: Una vez que se ha completado el procesamiento de la capa física y de la capa de enlace, los datos contenidos en la trama se envían a un protocolo de capa superior, que se identifica en el campo tipo. Aunque la versión 2 de Ethernet no especifica ningún relleno, al contrario de lo que sucede con IEEE 802.3, Ethernet espera por lo menos 46 bytes de datos.

- *datos (IEEE 802.3)*: Una vez que se ha completado el procesamiento de la capa física y de la capa de enlace, los datos se envían a un protocolo de capa superior, que debe estar definido dentro de la porción de datos de la trama. Si los datos de la trama no son suficientes para llenar la trama hasta una cantidad mínima de 64 bytes, se insertan bytes de relleno para asegurar que por lo menos haya una trama de 64 bytes.

- *secuencia de verificación de trama (FCS)*: Esta secuencia contiene un valor de verificación CRC de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

Formatos de trama Ethernet e IEEE 802.3

Ethernet						
7	1	6	6	2	46-1500	4
Preambulo	Inicio de delimitador de trama	Direccion destino	Direccion origen	Tipo	Datos	Secuencia de verificacion de trama

IEEE 802.3						
7	1	6	6	2	64-1500	4
Preambulo	Inicio de delimitador de trama	Direccion destino	Direccion origen	Longitud	Encabezado y datos 802.2	Secuencia de verificacion de trama

Figura 1.5

Ethernet es una tecnología de broadcast de medios compartidos que se resume en la figura 1.6:

Operación de Ethernet

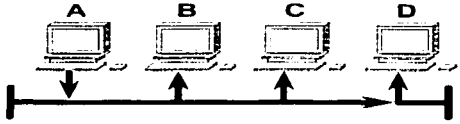


Figura 1.6

. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

1. Transmitir y recibir paquetes de datos
2. Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI
3. Detectar errores dentro de los paquetes de datos o en la red

En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir a través de los medios de la red funcionan según el modo "escuchar antes de transmitir". Esto significa que cuando un dispositivo desea enviar datos, primero debe verificar si los medios de la red están ocupados. El dispositivo debe verificar si existen señales en los medios de red. Una vez que el dispositivo determina que los medios de red no están ocupados, el dispositivo comienza a transmitir los datos. Mientras transmite los datos en forma de señales, el dispositivo también escucha. Esto lo hace para comprobar que no haya ninguna otra estación que esté transmitiendo datos a los medios de red al mismo tiempo. Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escucha.

Los dispositivos de red pueden detectar cuando se ha producido una colisión porque aumenta la amplitud de la señal en el medio de red. Cuando se produce una colisión, cada dispositivo que está realizando una transmisión continúa transmitiendo datos durante un período breve. Esto se hace para garantizar que todos los dispositivos puedan detectar la colisión. Una vez que todos los dispositivos de una red detectan que se ha producido una colisión, cada dispositivo invoca a un algoritmo. Después de que todos los dispositivos de una red han sufrido una postergación durante un período determinado de tiempo (que es distinto para cada dispositivo), cualquier dispositivo puede intentar obtener acceso a los medios de networking nuevamente. Cuando se reanuda la transmisión de datos en la red, los dispositivos involucrados en la colisión no

tienen prioridad para transmitir datos. En la figura 1.7 se presenta un resumen del proceso CSMA/CD.

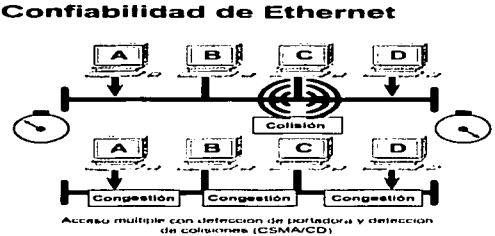


Figura 1.7

Ethernet es un medio de transmisión de broadcast. Esto significa que todos los dispositivos de una red pueden ver todos los datos que pasan a través de los medios de networking. Sin embargo, no todos los dispositivos de la red procesan los datos. Solamente el dispositivo cuya dirección MAC y cuya dirección IP concuerdan con la dirección MAC y la dirección IP destino que transportan los datos copiará los datos.

Una vez que el dispositivo ha verificado las direcciones MAC e IP destino que transportan los datos, entonces verifica el paquete de datos para ver si hay errores. Si el dispositivo detecta que hay errores, se descarta el paquete de datos. El dispositivo destino no enviará ninguna notificación al dispositivo origen, sin tener en cuenta si el paquete de datos ha llegado a su destino con éxito o no. Ethernet es una arquitectura de red no orientada a conexión considerada como un sistema de entrega de "máximo esfuerzo".

1.4 ATM

Sus siglas significan Asynchronous Transfer Mode (Modo de Transmisión Asíncrona), debido a las grandes similitudes con Frame Relay, ATM también ha sido llamado Cell Relay. ATM es la respuesta a la necesidad de redes LAN y WAN en las que se pueda transmitir Al mismo tiempo voz, video y datos. Actualmente ATM ya es reconocido como un estándar definido por la ANSI y la ITU-TSS (siendo parte de lo que se ha definido como B-ISDN, Broadband-Integrated Services Digital Network) para los cuales ATM es una tecnología de multiplexado y conmutación de celdas, orientada a conexión, y además de alta velocidad, permitiendo que esta configuración ofrezca prácticamente ancho de banda virtualmente ilimitado.

Arquitectura de ATM.

ATM es un protocolo de transporte y con respecto al modelo OSI ocupa las dos primeras capas (ver figura 1.8)

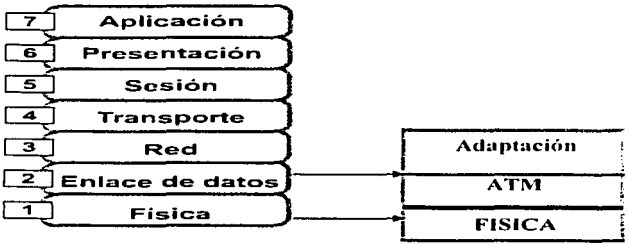


Figura 1.8

Una representación que explica de forma más clara la arquitectura de ATM es el llamado modelo tridimensional en donde obviamente se incluyen las tres capas: Capa Física, Capa ATM, Capa ATM de adaptación.

CAPA FÍSICA
La capa física se ocupa de explicar como son transportadas las celdas sobre la red. Esto incluye los tipos de interfaces, el medio físico y las tasas de información que se utilizan. En esta capa también se define el código de línea con el que se transmitirá.

Está dividida a su vez en dos subcapas: Transmission Convergence Sublayer (TC) y Physical Medium Sublayer (PM)

Subcapa Physical Medium (PM) la cual soporta funciones que son dependientes del medio de transmisión seleccionado, por ejemplo codificación de línea, temporización de bits y el medio físico.

Subcapa Transmission Convergence (TC) la cual soporta funciones que son independientes de las características del medio de transmisión, como por ejemplo la generación recuperación de la transmisión de frames, adaptación de las celdas para que viajen por el sistema de transmisión, creando los límites de la celda dentro del payload (carga) físico, generación/verificación del encabezado.

Los estándares de ATM especifican principalmente 2 tipos de interfaces:

User-to-Network Interface (UNI)
Network-to-Network Interface (NNI)

Una red ATM proporciona un servicio de transporte orientado a conexión. Esto significa que un dispositivo conectado a una red ATM requiere establecer una conexión con otro dispositivo conectado a la red antes de que la información pueda ser transmitida. Las conexiones son llamadas virtuales debido a que el ancho de banda no está permanentemente asignado a la conexión pero cuando el usuario tiene celdas que transmitir la red lo provee de ancho de banda suficiente.

Para realizar la conexión entre distintos puntos de la red, se utilizan enlaces lógicos los cuales podemos definirlos como sigue:

Virtual Channel (VC, Canal Virtual). Es una conexión lógica entre dos usuarios finales de una red, los cuales estarán conectados a una tasa de transmisión variable con una conexión full duplex. El punto en el cual una celda de ATM es pasada a o desde una capa superior es considerada el usuario

Capa ATM

La capa ATM es responsable de los mecanismos del transporte de celda. Esto incluye separar celdas de diferentes conexiones y leer e interpretar los encabezados la información de ruteo. La capa ATM provee la transmisión de las celdas usando Time-Division Multiplexing (TDM). La información multiplexada está organizada en celdas de longitud fija de 53 octetos. Cada celda contiene un encabezado de 5 octetos y un campo de información de 48 octetos. Los octetos en cada celda son transmitidos en orden creciente empezando con el octeto 1. Por lo que primero se transmite el encabezado y luego la información. Los bits dentro de cada octeto son transmitidos en orden decreciente empezando por el bit 8 (el más significativo). El uso de estas celdas pequeñas y de longitud fija reduce la tardanza en las colas a una celda de alta prioridad y por lo tanto pueden ser switcheadas eficazmente.

La capa ATM desempeña principalmente el switching de éstas el cual es realizado por hardware, lo que permite manejar altas velocidades. Excepto para el servicio de calidad (quality of service QoS), la capa ATM es totalmente independiente del tipo de información (voz, video o datos) que está transmitiendo.

Encabezado de una celda ATM

La tarea principal del encabezado es identificar las celdas que se encuentran en el mismo circuito virtual dentro del esquema del TDM asíncrono. Dentro de la red ATM las celdas son de la misma forma, sin embargo el encabezado varía ligeramente entre una UNI y una NNI.

Generic Flow Control (GFC)
Este campo de 4 bits es usado solo por la interfase UNI. El campo podría ser usado para asistir al cliente en el control del flujo del tráfico para diferentes QoS. Un candidato para el uso de este campo es un indicador de nivel de multiprioridad para controlar el flujo de información de manera dependiente del servicio. En general, el mecanismo del GFC tiene el propósito de disparar rápidamente condiciones de overload de la red.

Virtual Path Identifier (VPI)
Es el campo en la celda utilizado para el ruteo en la red: En la UNI posee 8bits soportando un máximo de 256 VP's mientras que en la NNI posee 12 bits permitiendo un mayor número de VP's (4096).

Virtual Channel Identifier (VCI)
Es el campo en la celda usada para rutear desde y hasta al usuario final. Soporta un máximo de 65536 VC's para cada VP a través de una UNI.

Payload Type Identifier (PTI)
Posee 3 bits e indica el tipo de información contenida en el campo de información distinguiendo entre celdas con información de red, o información de red. El PTI también indica cuando la celda ha encontrado congestión en su recorrido por la red.

Cell loss priority (CLP)
Este campo de 1 bit es utilizado para reajustar la red en el caso de congestión. Un valor de 0 indica una celda de prioridad relativamente alta y por lo tanto no debe ser descartada a menos que no haya alternativa. Un valor de 1 indica que la celda puede estar sujeta a eliminación dentro de la red. La capa AAL es quien se encarga de darle valor a este campo o también el proveedor de servicio.
Este campo distingue entre celdas de baja y regular prioridad dentro de un solo VC.

Header Error Control (HEC)
Los 8 bits proveen un código de redundancia cíclica (CRC) para detectar errores en el encabezado de la celda. Su función es validar el VPI y VCI para proteger que las celdas se liberen en UNI's equivocadas. Este campo en realidad es computado y usado por la capa física.

Adjunta a esta capa se encuentra AAL (ATM Adaptation Layer) la que proporciona las funciones inteligentes en la conmutación de celdas como por ejemplo las funciones de red orientada a conexión o el soporte de protocolos de capas superiores.
En esta ¿subcapa? se encuentran las diferentes clases de servicios dependiendo de lo que demanden las diferentes aplicaciones. Los tipos de clases son denominados de Clase A, B, C, D.

A su vez esta capa se encuentra subdividida en dos subcapas:

- Convergencia
- Segmentación y Reensamblaje

Debido al desarrollo de esta tecnología se han aumentado los estándares para poder definir ATM, en éstos se encuentra incluido:

- Señalización UNI
- Interim Layer Managment Interface (ILMI)
- Data Exchange Interface
- LAN Emulation

1.5 LAN Emulation (LANE).

Una vez mencionado el concepto, principios y operación de las redes ATM, toca ahora considerar el método por el cual es posible migrar esta tecnología directo al escritorio para un cierto tipo de aplicaciones.

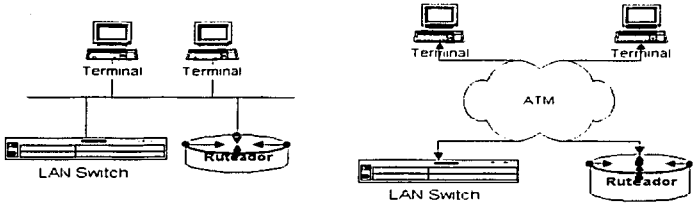
Existen diversos métodos por los cuales hacer una migración entre tecnologías LAN y WAN. Al estar hablando de RedUNAM, debemos considerar que se esta trabajando bajo la tecnología LAN Emulation que permite el entendimiento entre las redes LAN con el backbone ATM.

¿Que es LANE?

El foro ATM definió LAN Emulation como el método por el cual los usuarios de las redes de área local (LAN) pudieran migrar hacia redes ATM sin la necesidad de hacer modificaciones en software o hardware de sus sistemas terminales.

Como ya sabemos, las redes ATM son orientadas a conexión, y establecen su señalización por medio de enlaces punto a punto ó punto a multipunto, las redes LAN no son orientadas a conexión y su forma de señalización es por medio de broadcast hasta encontrar el ó los sistemas terminales destino.

LAN Emulation, como su nombre lo dice emula ó imita un ambiente de broadcast dentro de una red ATM, es decir, que los sistemas terminales como pueden ser estaciones de trabajo, ruteadores, switches, etc., imitan una red LAN a través de una red ATM sin ser requeridos cambios en los protocolos de capas superiores, ni en las aplicaciones. Esencialmente LANE puentea la información de las redes LAN transparentemente a través de ATM (Fig. 1.9)



Segmento LAN físico. **Imitación de LAN**

Fig. 1.9Función de LANE.

Los principales propósitos de LANE son:

- Proveer un estándar para llevar la mayoría de los protocolos de las redes LAN sobre ATM.
- Hacer posible una migración de los medios convencionales LAN a ATM y resolver las diferencias entre estas dos tecnologías.

LANE permite a los diversos dispositivos conectados a la red ATM comunicarse con los dispositivos conectados a las redes LAN, incluyendo conectividad entre los dispositivos LAN a través de la red ATM.

El protocolo LANE define mecanismos para imitar un ambiente IEEE 802.3 Ethernet ó un IEEE 802.5 Token Ring, es decir, que LANE hace que una red ATM parezca y se comporte como una red Ethernet o Token Ring, pero a una mayor velocidad y aprovechando las ventajas de las redes ATM, específicamente LANE emula o imita características de redes LAN como lo son:

- Servicios no orientados a conexión.
- Servicios de multicast.
- Adaptadores de servicios LAN-MAC.

Podría definirse a LANE como un conjunto de funciones que ocultan la complejidad del establecimiento de conexiones que prevalece en las redes ATM, imitando servicios similares a los ofrecidos en topologías como el BUS tales como el uso de broadcast que es un método que facilita la conexión.

¿Por que LANE?

Uno de los propósitos de las redes ATM se encuentra en mantener un nivel de interoperabilidad con las diferentes tecnologías LAN-WAN que representan la base de la tecnología de redes funcionando actualmente. Si esta interoperabilidad no fuera posible, las tecnologías LAN tendrían que ser reemplazadas totalmente ó, las redes ATM funcionarían en una forma aislada, desperdiciándose así sus ventajas y capacidades. En este caso el camino más viable es que ambas tecnologías utilicen los mismos protocolos de red como IP, IPX, etc., tanto en las redes LAN como en ATM. Debido a esto, existen diferentes caminos que llevan a cabo el entendimiento entre estas tecnologías.

Existen tres métodos entre otras diferentes tecnologías que realizan la misma función de una manera diferente dependiendo de los protocolos y las aplicaciones que estén siendo usados.

Uno de estos métodos es conocido como *operación en modo nativo*, en el cual los mecanismos de resolución de direcciones son usados para resolver las direcciones de la capa de red directamente en direcciones ATM, para entonces, enviar los paquetes a través de la red.

La operación en modo nativo esta diseñada específicamente para aprovechar las capacidades de calidad de servicio (QoS) que ofrece ATM.

Un segundo método es Classical IP, que esta limitado a redes que utilizan como protocolo base en sus aplicaciones a nivel LAN solo TCP/IP.

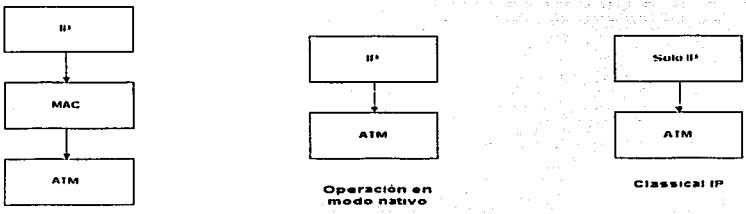


Figura 1.10 Comparación de métodos

El tercer método conocido como LAN Emulation emula una red de área local a través de una red ATM, y no limita sus aplicaciones a un solo protocolo de la capa de red en especifico.

Arquitectura del protocolo LANE.

La función básica del protocolo LANE es la de resolver las direcciones MAC en direcciones ATM con el objetivo de que los dispositivos o sistemas terminales LANE puedan establecer conexiones directamente entre ellos y así transmitir su información.

El funcionamiento del protocolo esta basado sobre dos tipos fundamentales de dispositivos que deberán estar conectados directamente a la red ATM, estos son, las tarjetas de interface de red (NIC's: Network Interface Card) y los equipos de conmutación a nivel LAN (Switch LAN).

Las NIC's son las encargadas de interconectar los sistemas terminales a la red ATM presentando una interfaz de servicios LAN a los adaptadores de las capas superiores del sistema terminal. Los protocolos de la capa de red en el sistema terminal continuarán comunicándose como si estos estuvieran en una red LAN convencional utilizando los procesos comunes y serán capaces de utilizar el ancho de banda disponible en las redes ATM.
Los equipos de conmutación de nivel LAN forman la segunda parte de los dispositivos necesarios para el funcionamiento del protocolo LANE, estos son switches a nivel LAN y ruteadores, estos dispositivos deberán contar con tarjetas de interface de red para proveer los servicios de redes de área local virtuales (Virtual LAN)[1]. A los puertos de estos switches les serán asignadas redes virtuales dependiendo de su localización física.

[1] Virtual LAN (VLAN). Red LAN establecida por medio de configuración en los switches LAN.

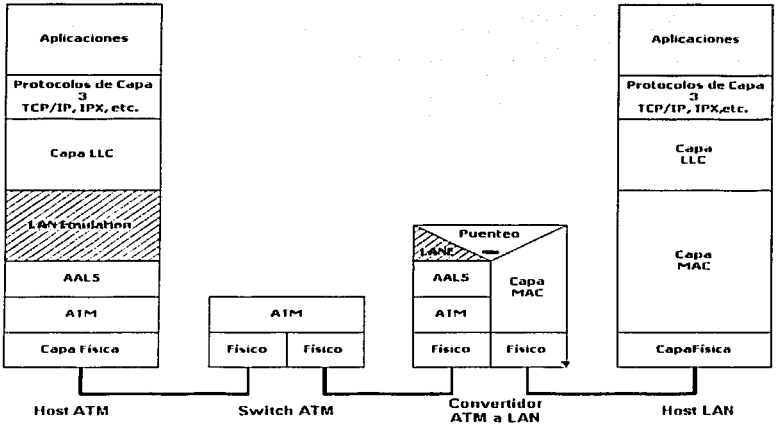


Fig. 1.11 Arquitectura del protocolo LANE.

Los protocolos de LANE operan transparentemente sobre y a través de los switches ATM utilizando solamente los procesos de señalización del estándar ATM. Los switches ATM son usados como plataformas sobre las cuales se implementan algunos de los componentes del servicio de LANE, pero este uso es independiente de la operación de los switches por si mismos (ver figura 1.11).

Componentes de LANE.

LANE define en si el funcionamiento de la emulación de una red LAN (ELAN, Emulated Local Area Network), pero a su vez, varias ELAN's pueden ser establecidas a través de la Red ATM, creando los ambientes LAN como Ethernet o Token Ring.

Cada ELAN esta formada por los siguientes componentes:

- Cliente de LAN Emulation (**LEC**, *LAN Emulation Client*).

Un LEC es la entidad en un sistema terminal que lleva a cabo las funciones de envio de datos, resolución de direcciones y registro de direcciones MAC con el servidor de LANE, también provee una interface de servicio de LAN a los protocolos y aplicaciones de las capas superiores (ver figura 1.12).

Una NIC o un switch LAN que interactué con una ELAN, tendrá un solo LEC para cada ELAN a la cual estén conectados. Un sistema terminal que conecte varias ELAN's tendrá un LEC por ELAN.

Cada LEC es identificado por una sola dirección ATM, y es asociado con una o mas direcciones MAC que sean vistas por tal dirección ATM. En el caso de una NIC el LEC podrá ser asociado con una sola dirección MAC, y en el caso de un switch LAN, el LEC será asociado con todas las direcciones MAC vistas a través de los puertos del switch, el cual, estará asociado a una ELAN.

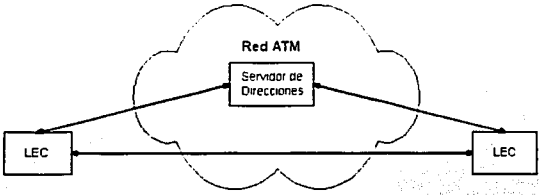


Fig. 1.12 Funcionamiento de un LEC.

- Servidor de LAN Emulation. (**LES**, *LAN Emulation Server*).

El LES es la entidad que lleva a cabo las funciones de control de una ELAN. Un LES maneja la parte de la resolución de direcciones y control de la información, su principal trabajo es el de registrar y resolver las direcciones MAC en direcciones ATM. Existe solamente un LES por cada ELAN y cada LES esta identificado por una sola dirección ATM.

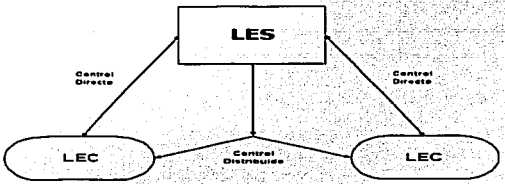


Figura 1.13 Funcionamiento de un LES

- Broadcast y Servidor Desconocido. (**BUS**, Broadcast and Unknown Server)

El BUS es el servidor de multicast de una ELAN, es usado para esparcir el tráfico que contiene direcciones de destino desconocidas y enviar el tráfico de

multicast y broadcast a los clientes dentro de la ELAN. A cada LEC le es asociado un solo BUS por ELAN, pero pueden existir varios BUS por ELAN (ver figura 1.14).

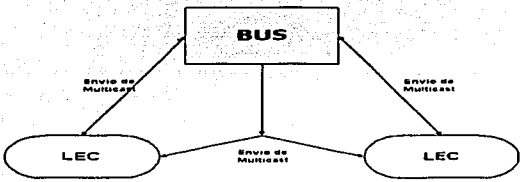


Fig. 1.14 Funcionamiento del BUS.

- Servidor de Configuración de LAN Emulation. (**LECS**, LAN Emulation Configuration Server)

El LECS es una entidad que asigna los LEC's a su ELAN correspondiente, a su vez, mantiene una base de datos de la información de configuración de cada ELAN.
Existe solo un LECS lógico por un dominio o red que sirve a todas las ELAN's dentro de la red (ver figura 1.15).

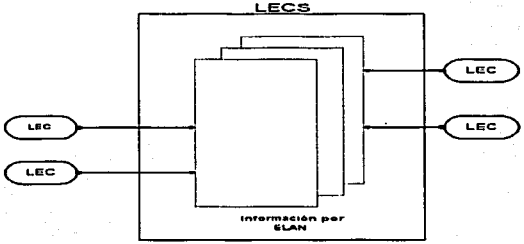


Fig. 1.15 Funcionamiento de un LECS.

Operación de LANE.

Para llevar a cabo el proceso de operación de LANE, sus componentes están comunicados por diferentes tipos de conexiones, es decir, canales virtuales (VCC's) que pueden ser unidireccionales o bidireccionales, punto a punto o punto a multipunto, cada uno de los cuales tiene un significado y función específica para manejar los procesos de comunicación.

La interfaz utilizada para la interoperabilidad entre los equipos es conocida como LUNI (LAN Emulation User to Network Interface), los protocolos de LUNI permiten a los dispositivos como sistemas terminales o equipos de conversión LAN/ATM controlar las conexiones virtuales requeridas para la transmisión.

Estas conexiones se dividen en conexiones para control y conexiones para el flujo de datos (ver figuras 1.16 y 1.17).

Para las funciones de control tenemos:

- VCC para Configuración Directa. Es una conexión de canal virtual (VCC) bidireccional punto a punto y es establecida por el LEC hacia el LECS.
- VCC para Control Directo. Es una conexión de canal virtual (VCC) bidireccional establecida por el LEC hacia el LES.
- VCC para Control Distribuido. Es una conexión de canal virtual (VCC) unidireccional punto a multipunto establecida desde el LES de regreso al LEC.

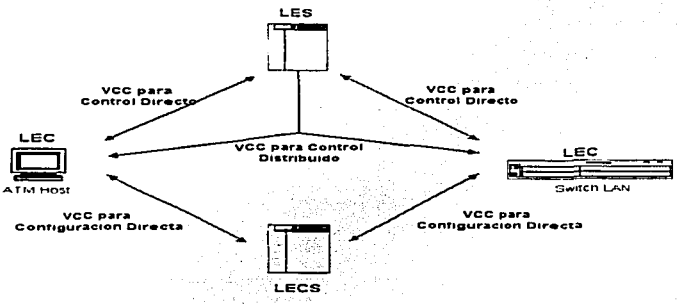


Fig. 1.16 Conexiones para mensajes de control.

Para el caso de flujo de datos tenemos:

- VCC para envío Directo de Datos. Es una conexión de canal virtual bidireccional punto a punto establecida entre dos LEC's.
- VCC para envío de Multicast. Es una conexión de canal virtual bidireccional punto a punto establecida por el LEC hacia el BUS
- VCC para re-envío de Multicast. Es una conexión de canal virtual unidireccional punto a multipunto establecida hacia el LEC desde el

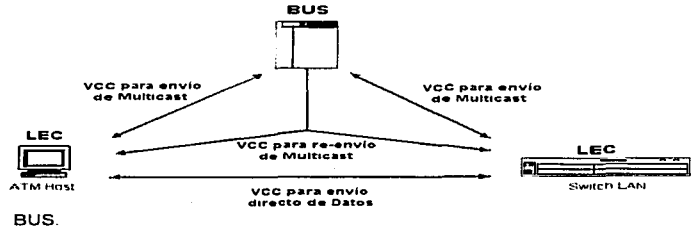


Fig. 1.17 Conexiones para el flujo de datos.

Todo el proceso de operación de LANE puede ser entendido analizando el comportamiento de los sistemas terminales cuando realizan su conexión a la red por medio de LANE.

Analizando los pasos que lleva a cabo el sistema terminal para establecer una conexión tenemos:

Inicialización y Configuración.

En el momento en el cual un sistema terminal desea establecer una conexión hacia la red, este busca a su LEC, el cual puede encontrarse dentro de su segmento de red ó puede ser el mismo sistema terminal; una vez identificado, el LEC busca al LECS con el fin de obtener información para su configuración, para encontrar al LECS el LEC puede emplear diferentes métodos, el método mas utilizado es por medio de ILMI[2], enviando mensajes hacia los switches ATM para encontrar al LECS; ya que es identificado, el LECS establece un VCC para configuración directa y utiliza un protocolo de configuración para informar al LEC sobre la información que este requiere para conectarse a la ELAN destino, esta información incluye: la dirección ATM del LES, el tipo de ELAN que esta siendo emulada, el tamaño máximo de paquetes en la ELAN, nombre de la ELAN, dirección ATM y MAC del LECS, etc. (ver figura 1.18).

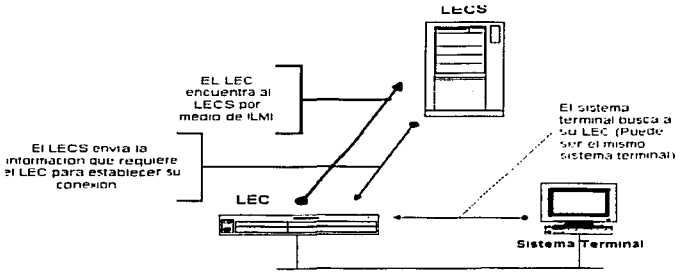


Fig. 1.18 Inicialización y configuración.

[2] ILMI: Interim Local Management Interface, interface utilizada para funciones de administración.

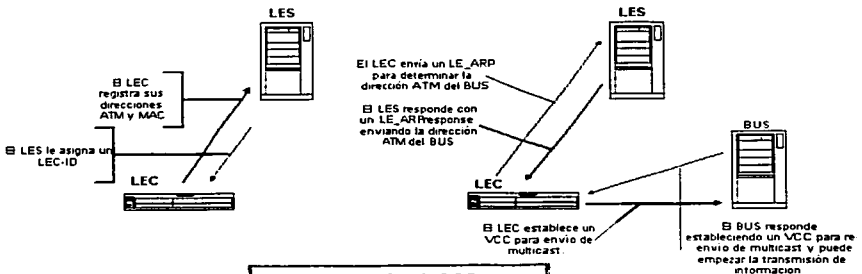
Unión y registro con el LES.

Una vez que el LEC conoce la dirección ATM del LES, el LEC establece un *VCC para control directo* con el LES, registrando su dirección MAC y su dirección ATM.
En la primera conexión con el LES, el LEC requiere ser registrado en el LES; el LES verifica el requerimiento del LEC y confirma su inscripción asignándole un identificador (LEC-ID), a partir de aquí, el LEC puede llevar a cabo la resolución de direcciones MAC a ATM.

Posteriormente el LES establece un *VCC para control distribuido* y un *VCC para control directo* que son utilizados por el LEC para realizar procesos de LAN Emulation Address Resolution Protocol (LE_ARP) para la resolución de direcciones ATM. En este proceso el LEC envía un LE_ARP *request* hacia el LES, si el LES reconoce la dirección MAC contenida en el LE_ARP *request*, este responde por medio del *VCC para control directo* con un LE_ARP *response* que contiene la dirección ATM solicitada, si no reconoce tal dirección, el LES re-envía el mensaje por medio de un *VCC para control distribuido* hacia otros LEC's que puedan conocer la dirección MAC requerida.

Para completar el proceso de inicialización el LEC envía un LE_ARP *request* para determinar la dirección ATM del BUS, una vez obtenida tal dirección, el LEC establece un *VCC para envío de multicast* hacia el BUS y el BUS responde estableciendo un *VCC para re_envio de multicast* hacia el LEC, en este punto el LEC esta listo para transmitir datos (ver figura 1.19). El BUS reconocerá al LEC como una salida en las conexiones punto a multipunto que establece para sus mensajes. Como su nombre lo indica el BUS se encargará del envío de mensajes de broadcast y multicast, el LEC por su parte, podrá utilizar su conexión hacia el BUS para enviar estos mensajes en la ELAN mientras que el LES se encargará de localizar las direcciones ATM desconocidas para establecer las conexiones requeridas.

Fig. 1.19 unión y registro con el LES

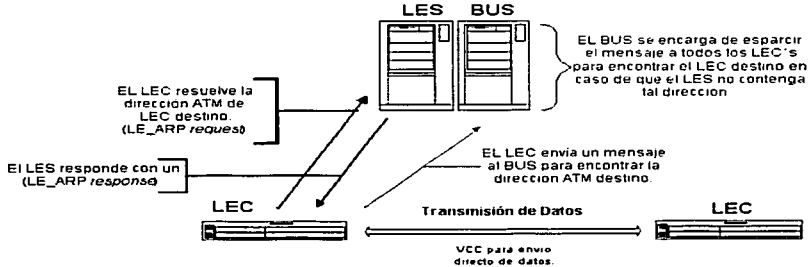


Transmisión de Datos.

Para la transmisión de datos, ahora el LEC deberá establecer la conexión con el sistema terminal destino al cual quiere transmitir su información, bajo el mismo procedimiento el LEC deberá resolver la dirección ATM del LEC destino con el LES y con el BUS, y establecer un VCC para la transmisión de sus datos (ver figura 1.20).

Durante la transmisión de los datos un LEC puede recibir paquetes de la capa de red provenientes de las NIC's, al igual que paquetes de datos a nivel MAC provenientes de los puertos LAN de un Switch. En el caso en el que los paquetes provengan de la capa de red, estos no tendrán la dirección ATM correspondiente a la dirección MAC del LEC destino, en este caso el LEC tendrá que formular una petición al LES enviando un LE_ARP *request*, y a BUS en el caso de que el LES no contenga la dirección ATM, con la finalidad de que el BUS envíe el mensaje a todos los LEC's para encontrar la dirección destino. Si el LE_ARP *response* es recibido, el LEC establece un VCC para envío directo de datos hacia el nodo destino y empieza a transmitir su información, en caso contrario el LEC continuará enviando los paquetes hacia el BUS hasta encontrar el nodo destino.

Fig. 1.20 Transmisión de datos.



De esta manera se lleva a cabo el proceso de transmisión de la información a través de las interfaces de LANE comunicando a los diferentes dispositivos LAN por medio de ATM.

1.6 Ruteo Estático y Dinámico.

Antes de hablar del protocolo de enrutamiento IGRP es necesario tocar algunos conceptos básicos de ruteo.
Existen principalmente dos clases de ruteo el Estático y el Dinámico el ruteo estático implica el conocimiento de las rutas estáticas y es administrado manualmente por el administrador de red, quien deberá de introducirlas directamente en la configuración de un router. El administrador debe actualizar manualmente cada una de estas rutas estáticas siempre que un cambio en la topología de la red requiera una actualización.

El ruteo dinámico a diferencia, trabaja de una manera distinta para este caso el administrador deberá de configurar el router para que este haga ruteo dinámico ahora bien por primera ocasión el administrador deberá configurar cada una de las redes que se pretendan anunciar después de haber concluido con esta tarea cada que exista un evento en la red que implique algún cambio los routers por default lo harán automáticamente ya que los routers hacen un proceso de actualización cada determinado tiempo dependiendo del protocolo de ruteo en cuestión.

En esta parte es necesario mencionar que ambas formas de ruteo son validas y necesarias y todo depende del tipo de red a que nos estemos refiriendo.

1.7 Protocolos Distance Vector y Link State.

Los algoritmos de enrutamiento basados en vector de distancia envían copias periódicas de una tabla de enrutamiento de un router a otro. Estas actualizaciones regulares entre routers comunican los cambios de topología.

Cada router recibe una tabla de enrutamiento de los routers vecinos directamente conectados. Por ejemplo, en la figura 1.21, el Router B recibe información del Router A.
El Router B agrega un número de vector de distancia (como, por ejemplo, el número de saltos), aumentando de esta manera el vector de distancia y luego transfiere esta nueva tabla de enrutamiento a su otro vecino, el Router C. Este mismo proceso paso a paso se produce en todas las direcciones entre los routers directamente conectados.

Conceptos del vector de distancia

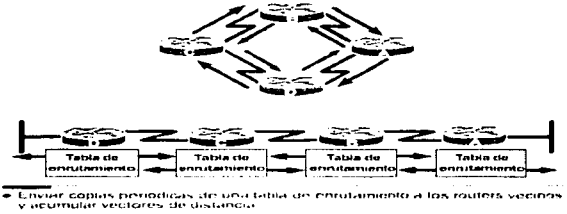


Fig. 1.21

El algoritmo eventualmente acumula distancias de red para poder mantener una base de datos de información de topología de la red. Los algoritmos por vector de distancia no permiten, sin embargo, que un router conozca la topología exacta de una red

El segundo algoritmo básico utilizado para el enrutamiento es el algoritmo de estado de enlace (Link State). Los algoritmos de enrutamiento basados en el estado de enlace, también conocidos como algoritmos SPF (primero la ruta libre más corta), mantienen una compleja base de datos de información de topología.
Mientras que el algoritmo de vector de distancia posee información no específica acerca de las redes distantes y ningún conocimiento acerca de los routers distantes, un algoritmo de enrutamiento de estado de enlace conoce perfectamente los routers distantes y cómo se interconectan. El enrutamiento de estado de enlace utiliza:

Publicaciones de estado de enlace (LSA)
Una base de datos topológica
El algoritmo SPF y el árbol SPF resultante
Una tabla de enrutamiento de rutas y puertos hacia cada red

Conceptos acerca del estado de enlace

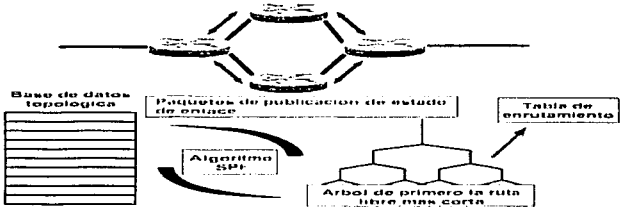


Fig. 1.22

En la figura 1.22 se muestra el proceso que generan los algoritmos de estado de enlace, donde primero se necesita que los routers envíen un paquete de publicación de estado de enlace conocido como LSA para posteriormente los demás equipos lo guarden en su base de datos topológica, posteriormente se corre el algoritmo de SPF y de allí se obtiene un árbol con la topología completa de la red desde el punto de vista de cada router.

1.8 Protocolo IGRP.

IGRP es un protocolo de enrutamiento por vector de distancia desarrollado por Cisco. IGRP envía actualizaciones de enrutamiento a intervalos de 90 segundos, publicando a las redes la existencia de un sistema autónomo en particular donde un sistema autónomo se considera al conjunto de routers administrados por una sola entidad. Algunas de las características de diseño claves de IGRP enfatizan lo siguiente:

- Versatilidad que permite manejar automáticamente topologías indefinidas y complejas
- Flexibilidad para segmentos con distintas características de ancho de banda y de retardo
- Escalabilidad para operar en redes de gran envergadura

El protocolo de enrutamiento IGRP utiliza una combinación de variables para determinar una métrica compuesta (ver figura 1.23).

Estas variables incluyen:

Ancho de banda
Retardo
Carga
Confiabilidad

En este punto es necesario considerar que la métrica hablando de protocolos de ruteo es la variable que estos emplean para elegir el mejor camino hacia cualquier punto de la red.
Algunos protocolos solos emplean el numero de saltos que tienen que dar antes de llegar a su destino en la siguiente figura podemos ver que IGRP contempla una métrica compuesta donde además de los saltos toma en cuenta el ancho de banda de los enlaces y la carga que exista en cada uno de ellos.

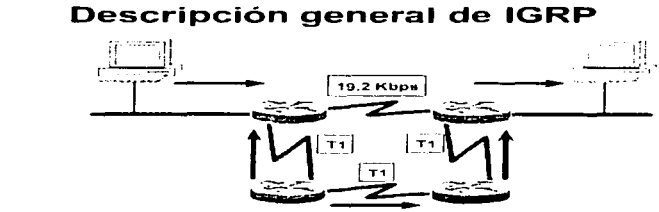


Fig. 1.23

1.9 Protocolo OSPF

Ospf es un protocolo de ruteo de estado de enlace, los cuales como ya se mencionaron anteriormente mantienen una base de datos con la topología completa de la red.
OSPF es un protocolo jerárquico basado en áreas con un esquema como el que se muestra en la figura 1.24.

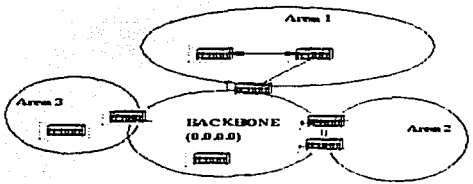


Fig. 1.24 Áreas en OSPF

De esta forma con todas estas áreas interconectadas por medio de routers se genera una red OSPF, dentro del protocolo de OSPF es necesario que exista una área 0 (cero) a la cual todas las demás áreas deberán estar conectadas directamente.
Ospf cuenta con distintos tipos de routers que son Inter-área routers, intra-área routers y es muy importante un designated router y backup designated router esto es con la finalidad de que cuando haya un evento en la red que implique un cambio el router que provoca el evento solo avisa a su designated router y este a su vez envia un LSA a toda la red para que cada equipo corra nuevamente el algoritmo de SPF y actualice su árbol de la red.
Por lo tanto esto provoca el consumo de recursos del router

1.10 Protocolos de Internet

1.10.1 Antecedentes

Los protocolos de Internet constituyen el conjunto de protocolos de sistemas abiertos (no propietario) de mayor uso mundial ya que puede servir para comunicarse a través de un conjunto de redes interconectadas y es igualmente apropiado para las comunicaciones en LANs y WANs. Los protocolos de Internet constan de un conjunto de protocolos de comunicación. Entre éstos los dos más conocidos son TCP (Protocolo de Control de transmisión e IP (Protocolo Internet). La arquitectura de protocolos de Internet no solamente incluye los protocolos de las capas inferiores (como TCP e IP), sino que también especifica aplicaciones comunes como el correo electrónico, la emulación de terminal y la transferencia de archivos. Aquí hablaremos de las especificaciones s que forman los protocolos de Internet. Se incluye el direccionamiento de IP y los protocolos de las caspas superiores clave que se utilizan en Internet. El protocolo de ruteo especifico (OSPF) analizado en este mismo capitulo se hará en el capitulo 4.

Los protocolos de ruteo fueron desarrollados por primera vez a mediados de los años 70, cuando DARPA (Agencia de Investigación de Proyectos Avanzados de la Defensa) se interesó en establecer una red de conmutación de paquetes que facilitara la comunicación entre sistemas de computadoras disímiles en instituciones de investigación. Con el objetivo de una conectividad heterogénea, DARPA financio la investigación realizada por la Universidad de Stanford y BBN (Bolt, Beranek and Newman). El resultado de este esfuerzo de desarrollo fue el conjunto de protocolos de Internet, terminado a fines de los años 70.

El protocolo TCP/IP se incluyo posteriormente en el UNIX de BSD (Berkeley Software Distribution) y, desde entonces, se convirtió en la base de Internet y World Wide Web.

La documentación de los protocolos de Internet (incluyendo los nuevos y revisados) y las políticas, se especifican en reportes técnicos llamados RFCs (Solicitud de Comentarios), que se publican y, posteriormente, son revisados y

analizados por la comunidad de Internet. Las depuraciones de protocolos se publican en los nuevos RFCs.

1.10.2 Protocolo Internet

El IP es un protocolo de la capa de red (Capa 3) que tiene información de direccionamiento e información de control que permite el ruteo de paquetes. El IP se encuentra documentado en el RFC 791 y es el protocolo principal de la capa de red en el conjunto de protocolos de Internet. Junto con el TCP, el protocolo IP representa el corazón de los protocolos de Internet. El IP tiene dos responsabilidades principales : ofrecer la entrega de datagramas basadas en el mejor esfuerzo y sin conexión a través de una red; y ofrecer la fragmentación y el reensamblado de datagramas para soportar los enlaces de datos con tamaños diferentes de las MTU (Unidades de Transmisión Máxima).

1.10.2.1 Formato de los paquetes IP

Un paquete IP contiene varios tipos de información como se muestra en la figura1.25.
El planteamiento siguiente describe los campos del paquete IP que se muestran en la figura 1.25:

- Versión – Indica la versión de IP actualmente en uso.
- IHL (Longitud de campo IP) – Indica la longitud del encabezado del datagrama en palabras de 32 bits.
- Tipo de servicio – Especifica cómo desearía un protocolo de las capas superiores que se manejara un datagrama y les asignara diferentes niveles de acuerdo a su importancia.
- Longitud total- Especifica la longitud, en bytes, del paquete IP total incluyendo los datos y el encabezado.

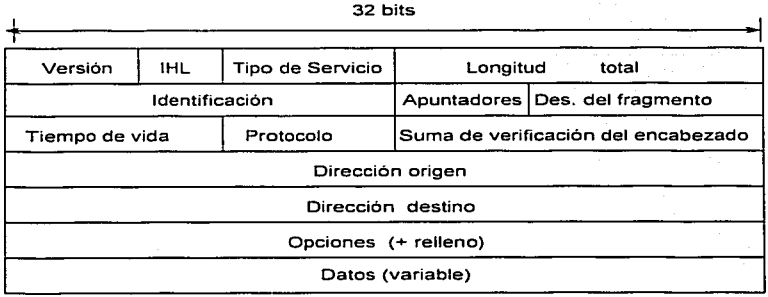


Fig. 1.25 Un paquete IP está compuesto por 14 campos

- Identificación – Consta de un número entero que identifica el datagrama actual. Este campo se utiliza para ayudar a reconstruir los fragmentos del datagrama.
- Apuntadores – Constan de un campo de 3 bits entre los cuales los 2 bits de menor orden (los menos significativos) controlan la función de fragmentación. El bit de menor orden especifica si se puede fragmentar el paquete. El bit de en medio especifica si el paquete es el último fragmento en una serie de paquetes fragmentados. El tercer bit, o el bit de mayor orden, no se usa.
- Desplazamiento del fragmento – Indica la posición de los datos del fragmento en relación con el comienzo de los datos en el datagrama original, lo cual permite que el proceso IP del destino reconstruya adecuadamente el datagrama original.
- Tiempo de vida - conserva un contador que disminuye gradualmente hasta llegar a cero, donde se elimina. Esto evita que los paquetes circulen en ciclo de manera indefinida.
- Protocolo- Indica que protocolo de las capas superiores recibe los paquetes entrantes una vez terminado el procesamiento IP.
- Suma de verificación del encabezado- Ayuda a asegurar la integridad del encabezado IP.
- Dirección origen – especifica el nodo emisor
- Dirección destino – Especifica el nodo receptor
- Opciones – Permite que el protocolo IP soporte diferentes opciones como la seguridad.
- Datos – Contiene la información de las capas superiores.

1.10.2.2 Direccionamiento IP

Igual que con cualquier otro protocolo de la capa de red, el esquema de direccionamiento de IP es fundamental en el proceso de ruteo de los datagramas IP a través de la red. Cada dirección IP tiene componentes específicos y sigue un formato básico. Estas direcciones IP pueden subdividirse y utilizarse para crear direcciones de subredes, como analizaremos más a detalle en este capítulo.

1.10.2.2.1 Formato de dirección IP

La dirección IP de 32 bits se agrupa en 8 bits a un mismo tiempo, separados por puntos y representados en formato decimal (conocidos como notación decimal de puntos). Cada bit en el octeto tiene un peso binario (128, 64, 32, 16, 8, 4, 2, 1). El valor mínimo de un octeto es de 0, y el valor máximo de un octeto es 255. La figura 1.26 muestra el formato básico de una dirección IP.

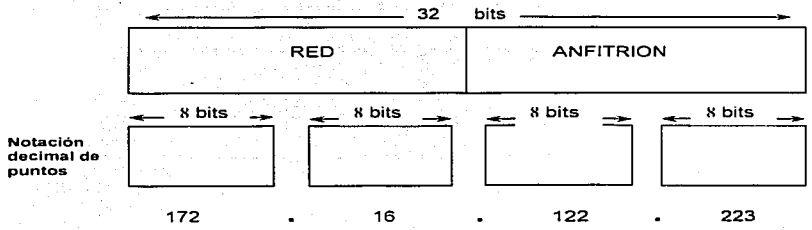


Fig. 1.26 Una dirección IP consta de 32 bits agrupados en cuatro octetos

1.10.3 Clases de direcciones en IP

El direccionamiento IP soporta cinco diferentes clases de direcciones: A, B, C, D y E. Solamente las clases A, B y C están disponibles para su uso comercial. Los bits más a la izquierda (de alto orden) indican de qué clase de red se trata. La tabla 3 ofrece información de referencia respecto a las cinco clases de direcciones IP:

La figura 1.27 muestra el formato de las clases comerciales de direcciones IP.
(Observemos los bits de alto orden en cada clase).

La clase de dirección se puede determinar fácilmente al examinar el primer octeto de la dirección y mapear ese valor con un rango de clases en la tabla 3. En una dirección IP 172.31.1.2, por ejemplo, el primer octeto es 172. Como el 172 esta entre 128 y 191, 172.31.1.2 es una dirección clase B. La figura 1.28 resume el rango de los posibles valores para el primer octeto de cada clase de direcciones.

Tabla 3

Clase de dirección de IP	Formato	Propósito	Bit(s) de orden superior	Rango de direcciones	Núm. de bits del Host/ de red	Máximo de hosts
A	N.H.H.H[1]	Para pocas organizaciones grandes	0	1.0.0.0 a 126.0.0.0	7/24	16,777,214[2] (2^24-2)
B	N.N.H.H	Para organizaciones de tamaño	1,0	128.1.0.0 a 191.254.0.0	14/16	65,543 (2^16-2)

C	N.N.H.H	mediano Para organizaciones relativamente pequeñas	1,1,0	192.0.1.0 a 223.255.254.0	22/8	245 (2^8-2)
D	N/A	Grupos de multidifusión (RFC 1112)	1,1,1,0	224.0.0.0 a 239.255.255.255	N/A (No para uso comercial	N/A
E	N/A	Experimental	1,1,1,1	240.0.0.0 a 254.255.255.255	N/A	N/A

1. N= Número de red, H= Número de host.
2. Una dirección esta reservada para la dirección de difusión y otra para la de red.

Fig 1.27 Los formatos de direcciones IP, A, B y C, estan disponibles para su uso comercial

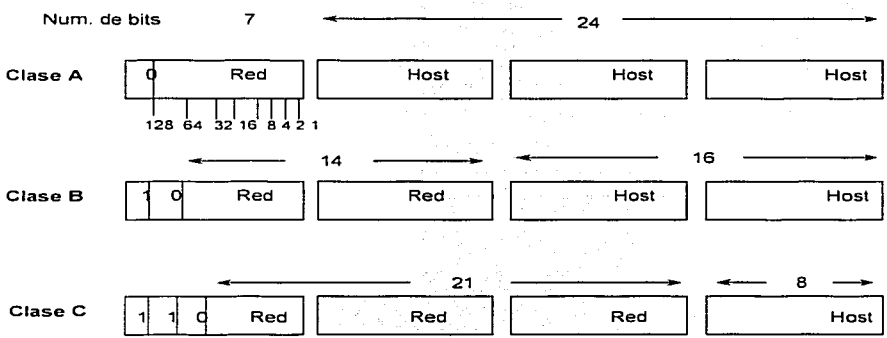


Fig. 1.28 Hay un rango de valores posibles para el primer octeto de cada clase de dirección

Clase de dirección	Primer octeto en decimal	Bits de orden superior
Clase A	1-126	0
ClaseB	128-191	10
ClaseC	192-223	110
Clase D	224-239	1110
Clase E	240-254	1111

1.10.3.1 Direccionamiento de la subred IP

Las redes IP se pueden dividir en redes pequeñas llamadas subredes. Las subredes representan varias ventajas para el administrador de red, entre ellas: una mayor flexibilidad, un uso más eficiente de ,las direcciones de red y la capacidad de manejar tráfico de difusión (una difusión no puede atravesar un ruteador).
Las redes están bajo una administración local. Como tales, el mundo exterior ve una organización como una sola red y no tiene un conocimiento detallado de la estructura interna de la organización.

Una determinada dirección de red puede subdividirse en muchas subredes. Por ejemplo, 172.16.1.0, 172.16.2.0, 172.16.3.0 y 172.16.4.0 son subredes dentro de la red 172.16.0.0 (Un valor de sólo 0s en la porción del host de una dirección, especifica toda la red.)

1.10.3.2 Máscara de subred IP

Una dirección de subred se crea "pidiendo bits prestados "del campo del host y designándolos como un campo de subred. El número de bits prestados varía y está especificado por la máscara de subred. La figura 1.29 muestra como se piden prestados los bits del campo de dirección del host para crear el campo de dirección de la subred.

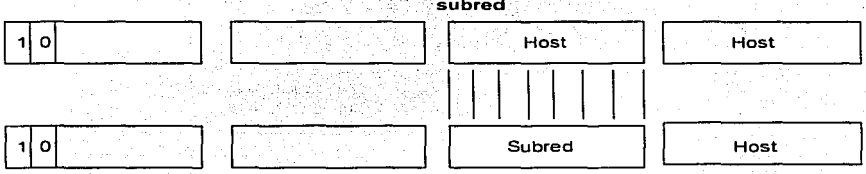


Fig. 1.29 Para crear el campo de dirección de la subred se piden prestados bits del campo de dirección del host.

Las máscaras de subred utilizan el mismo formato y técnica de representación que las direcciones IP. Sin embargo, la mascara de subred tiene 1s binarios en todos los bits, los cuales especifican los campos de red y de subred y 0s binarios en todos los bits que especifican el campo del host. La figura 1.30 muestra un ejemplo de máscara de subred.

Los bits de la máscara de subred deben provenir de los bits de orden superior (los que están más a la izquierda) del campo del host, como se muestra en la figura 1.31. A continuación presentamos los detalles de los tipos de máscaras de las subredes Clase B y Clase C. Las direcciones de Clase A las omitimos ya que generalmente forman parte de una subred en una frontera de 8 bits.

Ejemplo de una máscara de subred para una dirección Clase B

	Red	Red	Subred	Host
Representación binaria	11111111	11111111	11111111	00000000
Representación decimal de puntos	255 .	255 .	255 .	0

Fig. 1.3 Ejemplo de una máscara de subred que solo consta de 1s y 0s binarios

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	128
1	1	0	0	0	0	0	0	192
1	1	1	0	0	0	0	0	224
1	1	1	1	0	0	0	0	240
1	1	1	1	1	0	0	0	248
1	1	1	1	1	1	0	0	252
1	1	1	1	1	1	1	0	254
1	1	1	1	1	1	1	1	255

Figura 1.32 Los bits de la máscara de subred provienen de los bits de mayor orden del campo host

La máscara de subred predeterminada para la dirección Clase B que no tiene subred es 255.255.0.0, en tanto que la máscara de subred para una dirección Clase B 171.16.0.0, que especifica 8 bits de subred, es 255.255.255.0. La razón es que 8 bits de subred o 2^8-2 (1 para la dirección de red y 1 para la dirección de difusión)= 254 subredes posibles, con 2^8-2= 254 hosts por subred.

La máscara de subred para una dirección Clase C 192.168.2.0 que especifica 5 bits de subred es 255.255.255.248. Con 5 bits disponibles para la subred, 2^5-2=30 subredes posibles, con 2^3-2= 6 hosts por subred.

Los diagramas de referencia que se muestran en las tablas 4 y 5 se pueden utilizar para planear las redes Clase B y Clase C para determinar el número de subredes y de hosts que se requieren y la máscara de subred adecuada.

Número de bits	Máscara de subred	Número de subredes	Número de hosts
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

Tabla 4 Grafica de referencia de la subred Clase B

Número de bits	Máscara de subred	Número de subredes	Número de hosts
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Tabla5. Gráfica de referencia para la subred Clase C.

1.10.3.3 Uso de las máscaras de subred para determinar el número de red

El ruteador desempeña un proceso de activación para determinar la dirección de red (o más específicamente, la subred). Primero, obtiene la dirección destino de IP del paquete entrante y recupera la máscara de la subred interna. Después realiza una operación lógica AND para obtener el número de la red. Esto hace que se elimine la porción del host de la dirección destino de IP, mientras el número de la red de destino se conserva intacto. Luego, el ruteador ve el número de la red de destino y lo relaciona con una interfase de salida. Por último, direccional la trama hacia la dirección IP destino.

1.10.3.3.1 Operación AND lógica

Hay tres reglas básicas que gobiernan, desde el punto de vista lógico, la operación "AND" de dos números binarios. Primero, 1 "and" con 1 nos da 1. Segundo, 1 "and" con 0 nos da 0. Finalmente, 0 "and" con 0 nos da 0. La tabla de verdad (tabla 6) que aparece a continuación ilustra las reglas para las operaciones AND lógicas.

ENTRADA	ENTRADA	SALIDA
1	1	1
1	0	0
0	1	0
0	0	0

Tabla 6. Reglas para las operaciones AND lógicas.

Se tienen dos lineamientos simples para recordar las operaciones AND lógicas el ""AND" lógico de 1 con 1 nos da el valor original, en tanto que el "AND" de 0 con cualquier otro número nos da 0.

La figura 1.33 muestra que cuando se lleva a cabo una operación AND lógica de la dirección IP destino y la máscara de subred, se conserva el número de subred, que es utilizado por el ruteador para direccional el paquete.

		Red	Subred	Host
Dirección IP destino	171.16.1.2		00000001	00000010
Máscara de la subred	255.255.255.0		11111111	00000000
			00000001	00000000
			1	0

Fig 1.33 Al aplicar una operación AND lógica entre la dirección IP de destino y la máscara de la subred se obtiene el número de subred.

1.10.4 Visión general del protocolo ARP

Para que dos máquinas de una determinada red se puedan comunicar, cada una debe conocer la dirección física (o MAC) de la otra. Por medio de la difusión de los ARPs (Protocolos de resolución de Direcciones, un host puede, de manera dinámica, descubrir la dirección de capa MAC correspondiente a una dirección de la capa de red IP particular.

Después de recibir una dirección de la capa MAC, los dispositivos IP crean una memoria de almacenamiento ARP para guardar el mapeo de las direcciones IP-MAC adquiridas recientemente; de esta manera evitan tener que difundir ARPS cuando deseen ponerse de nuevo en contacto con el dispositivo. El parámetro se elimina si el dispositivo no responde en un periodo específico.

Además, RARP (Protocolo de Resolución Inversa de Direcciones) se utiliza para mapear direcciones de la capa MAC con direcciones IP. RARP, que es la

lógica inversa de ARP, puede ser utilizado por estaciones de trabajo sin disco que no conozcan sus direcciones IP cuando se inicializan. RARP se basa en la presencia de un servidor RARP con parámetros de la tabla correspondiente a las comparaciones de las direcciones de la capa MAC con las de IP.

1.10.5 Ruteo en Internet

Los dispositivos de ruteo en Internet tradicionalmente han sido llamados puertas de enlace. Sin embargo, en la terminología actual, el término puerta de enlace (gateway) se refiere específicamente a un dispositivo que traduce el protocolo de la capa de aplicación entre dispositivos. Las puertas de enlace interiores se refieren a dispositivos que llevan a cabo estas funciones de protocolos entre máquinas o redes bajo el mismo control administrativo o autoridad, por ejemplo una red corporativa interna. A estos sistemas se les conoce como sistemas autónomos; Red UNAM cuenta con sus propias políticas de ruteo y este hecho hace que sea un sistema autónomo el cual cuenta con un identificador. El identificador de sistema autónomo de Red es el 274.

En Internet los ruteadores están organizados jerárquicamente y los que se utilizan para intercambiar información en sistemas autónomos se llaman ruteadores interiores ; estos utilizan una gran variedad de IGPs (Protocolos de Puerta de Enlace Interior) para cumplir con este propósito. Ejemplo de un IGP es RIP (Protocolo de Información de Ruteo).

A los ruteadores que transfieren información entre sistemas autónomos se les conoce como ruteadores exteriores. Estos utilizan un protocolo de puerta de enlace exterior para intercambiar información entre sistemas autónomos. BGP (Protocolo de Enlace de Puerta de Frontera) es ejemplo de un protocolo de puerta de enlace exterior.

1.10.5.1 Ruteo de IP

Los protocolos de ruteo de IP son dinámicos. El ruteo dinámico, las rutas se calculan dinámicamente a intervalos regulares a través del software incluido en los dispositivos de ruteo. Esto contrasta con el ruteo estático, donde los ruteadores son establecidos por el administrador de red y no cambian sino hasta que el administrador de red los modifica,

Para hacer posible el ruteo dinámico, se utiliza una tabla de ruteo de I, formada por pares de direcciones destino/salto siguiente. Por ejemplo, un parámetro de esta tabla se interpretaría así: para llegar así: para llegar a la red 172.31.0., envié el paquete a la interfase Ethernet 0 (E0).

El ruteo IP especifica que los datagramas IP viajen a través de intercedes de un salto a la vez; sin embargo, al inicio del viaje no se conoce la ruta completa. Por el contrario, en cada parada se calcula el siguiente destino relacionando la dirección destino en el datagrama con un parámetro en la tabla actual de ruteo de nodos.

La participación de cada uno de los nodos involucrados en el proceso de ruteo se limita al direccionamiento de paquetes a partir de la información interna. Los nodos no supervisan si los paquetes llegan a su destino final , ni el IP presenta la función de reportar los errores de regreso al origen cuando se presentan anomalías. Esta función se deja a otro protocolote Internet, el ICMP (Protocolo de Control de Mensajes de Internet).

1.10.5.2 Protocolo ICMP

ICMP (Protocolo de Control de Mensajes de Internet) es un protocolo de Internet de la capa de red que ofrece paquetes de mensajes para reportar errores y demás información respecto al procesamiento de paquetes en IP de regreso al origen. El ICMP está documentado en el RFC 792.

1.10.5.2.1 Mensajes del ICMP

Los ICMP s generan varios tipos de mensajes útiles, entre los que se incluyen el de destino inalcanzable; solicitud y respuesta de eco; redirección; Tiempo excedido; Anuncio de ruteador y Solicitud de ruteador. Si un mensaje ICMP no puede ser entregado, no se genera un segundo mensaje. Esto es para evitar un flujo interminable de mensajes de ICMP.

Cuando un ruteador envia un mensaje de ICMP de destino inalcanzable, eso significa que el ruteador no puede enviar el paquete a su destino final. Entonces, el ruteador elimina el paquete original. Hay dos razones de por qué un destino puede ser inalcanzable. Con mucha frecuencia, el host de origen ha especificado una dirección inexistente. Es menos frecuente que el ruteador no tenga una ruta hacia el destino.

Los mensajes que no pueden llegar a su destino pueden ser de cuatro tipos básicos: los que no llegan a la red, los que no llegan al host, los que no llegan al protocolo y los que no llegan al puerto. En general, cuando los mensajes no llegan a la red significa que se ha presentado una falla en el ruteo o direccionamiento de un paquete. Los mensajes que no llegan al host indican, en general, un falla en la entrega, como puede ser una mascara errónea en la subred. En general los mensajes que no llegan al protocolo significan que el destino no soporta el protocolo de las capas superiores que especifica el paquete. Los mensajes que no llegan al puerto implican que el socket o puerto TCP no esta disponible.
Cualquier host envia un mensaje de solicitud de eco de ICMP, generado por el comando ping, host para probar la posibilidad de llegar hacia el nodo a través de la red. El mensaje de respuesta al eco del ICMP indica que es posible llegar al nodo.

El ruteador envía un mensaje de Redirección del ICMP al host de origen para estimular un ruteo más eficiente. El ruteador aún envía el paquete original hacia el destino. Los redireccionamientos del ICMP permiten que las tablas de ruteo del host conserven un tamaño pequeño ya que sólo es necesario conocer la dirección de un ruteador , incluso si ese ruteador no ofrece la mejor trayectoria. Aún después de recibir un mensaje de Redirección de ICMP, algunos dispositivos pueden seguir utilizando la ruta menos eficiente.

El ruteador envía wun mensaje de Tiempo excedido del ICMP si el campo Tiempo de vida de un paquete IP 8expresado en saltos o segundos) alcanza el valor de cero. El campo Tiempo de vida evita que los paquetes circulen de manera continua en la red si en ésta se ha presentado un ciclo de ruteo. El ruteador, entonces, elimina el paquete original.

1.10.6 Protocolo TCP

Este protocolo permite la transmisión confiable de datos en un ambiente IP. El protocolo TCP corresponde a la capa de transporte (capa 4) del modelo de referencia OSI. Entre los servicios que ofrece TCP están la transferencia de datos en ráfagas, confiabilidad, control de flujo eficiente, operación full-duplex y multiplexaje.

Con el servicio de transferencia de datos en ráfagas, el protocolo TCP entrega una ráfaga no estructurada de bytes identificada por una secuencia de números. Este servicio beneficia a las aplicaciones, que estas no tienen que fragmentar los datos en bloques antes de entregarlos a TCP. TCP agrupa los bytes en segmentos y los pasa al protocolo ip para su entrega.

El protocolo TCP ofrece la función de confiabilidad al permitir una entrega de paquetes confiable, de extremo a extremo, orientada a la conexión a través de una interred. Realiza esto colocando los bytes en secuencia con un número de confirmación de envío que indica al destino el próximo byte que el origen espera recibir. Los bytes que no se confirman en u periodo específico se transmiten de nuevo. El mecanismo de confiabilidad de TCP permite que los dispositivos puedan lidiar con paquetes mal leídos, duplicados, retrasados o perdidos. Un mecanismo de expiración de tiempo permite a los dispositivos detectar paquetes perdidos y solicitar su retransmisión

El protocolo TCP ofrece un control de flujo eficiente, lo cual significa que cuando se envían confirmaciones de regreso de origen, el proceso TCP de recepción indica el número de secuencia más grande que puede recibir sin saturar sus dispositivos de almacenamientos internos.

La operación duplex total significa que los procesos de TCP se pueden enviar y recibir al mismo tiempo.

Por último el multiplexaje de TCP significa que es posible multiplexar varias conversaciones de las capas superiores de manera simultanea a través de una sola conexión.

1.10.6.1 Establecimiento de la conexión TCP

Para utilizar un servicio de transporte confiable, los hosts TCP deben establecer una sesión orientada a la conexión entre sí. La conexión se establece por medio de un mecanismo de "saludo en tres direcciones".

Un saludo en tres direcciones sincroniza ambos extremos de una conexión permitiendo que ambos lados convenga en cuanto a los números de secuencia iniciales. Este mecanismo también garantiza que ambos lados estén listos para transmitir. Esto es necesario para que los paquetes no se transmitan o retransmitan durante el establecimiento de la sesión o después de que la sesión haya terminado.

Cada host selecciona de manera aleatoria un número de secuencia que se utiliza para rastrear los bytes dentro de la ráfaga que esta enviando y recibiendo. Posteriormente, el saludo en tres direcciones procede de la manera siguiente:

El primer host (Host A) inicia una conexión enviando un paquete con el número de secuencia inicial (X) y el bit SYN activado para indicar una solicitud de conexión. El segundo host (Host B) recibe el SYN, graba el número de secuencia X, y responde confirmando el SYN (con un ACK= X+1). El Host B incluye su propio número de secuencia inicial (SEQ=Y). Un ACK=20 significa que le host ha recibido los bytes 0al 19 y espera el 20 a continuación. A esta técnica se le llama confirmación hacia delante. El host A, posteriormente, confirma todos los bytes que el Host B envió con una confirmación hacia delante que indica el siguiente byte que el host A espera recibir (ACK=Y+1).

Sólo en este momento puede comenzar la transferencia de datos.

1.10.6.2 Técnica PAR

Un simple protocolo de transporte puede implementar una técnica para el control de confiabilidad y del flujo donde el origen envíe un paquete , inicialice un temporizador y espere duna confirmación antes de enviar un paquete nuevo.
Si la confirmación no se recibe antes de que el temporizador expire, el origen retransmite el paquete. A dicha técnica se le conoce con el nombre de PAR (Confirmación y Retransmisión Positivas).

Al asignar un número de secuencias a cada paquete, PAR permite que el host rastree los paquetes perdidos o duplicados que surgieron como resultado de los retardos en la red y provocaron la retransmisión prematura. Los números de secuencia se envían de regreso en las confirmaciones de modo que puedan ser rastreados.

Sin embargo, PAR implica un uso deficiente del ancho de banda, ya que un host debe esperar la confirmación antes de enviar un paquete nuevo y solamente se puede enviar un paquete a la vez.

1.10.6.3 Ventana deslizante de TCP.

Con la ventana deslizante de TCP se puede dar un uso más eficiente al ancho de banda de la red que con PAR ya que permite que los host envíen múltiples bytes o paquetes antes de esperar una confirmación.

EN TCP, el receptor especifica el tamaño real de la ventana de cada paquete. Como TCP ofrece una conexión de ráfagas de bytes, el tamaño de las ventanas se expresa en bytes. Esto significa que una ventana es el número de bytes de datos que el emisor puede enviar antes de esperar una confirmación. Los tamaños iniciales de las ventanas se indican en el periodo de establecimiento de la conexión, sin embargo, pueden modificarse en el transcurso de la transferencia de datos para ofrecer un control de flujo. Un tamaño de ventana igual a cero, por ejemplo, significa "No enviar datos".

La operación de ventana deslizante de TCP, el emisor puede tener una secuencia de bytes (numerados del 1 al 10) para enviarla a un receptor cuyo tamaño de ventana sea cinco. El emisor, entonces, colocará una ventana alrededor de los cinco primeros bytes y los transmitirá juntos. Después de esto esperará la confirmación.

El receptor podría responder con un ACK=6, lo que indicaría que ha recibido los bytes 1 al5 y qye esta esperando el 6. El receptor podría indicar en el mismo paquete que su tamaño de ventana es 5. El emisor, entonces, podría mover la ventana deslizante cinco bytes hacia la derecha y transmitir los bytes 6 al 10. El receptor podría contestar con un ACK= 11, lo que indicaría que espera a continuación el byte 11 en la secuencia. En este paquete, el receptor podría indicar que su tamaño de ventana es 0 (pues por ejemplo, sus buferes internos están saturados). En esta etapa del proceso, el emisor no puede enviar ningún byte más sino hasta que el receptor envíe otro paquete con un tamaño de ventana mayor a 0.

1.10.6.4 Formato del paquete TCP

La figura 1.34 muestra los campos y el formato general de un paquete TCP.

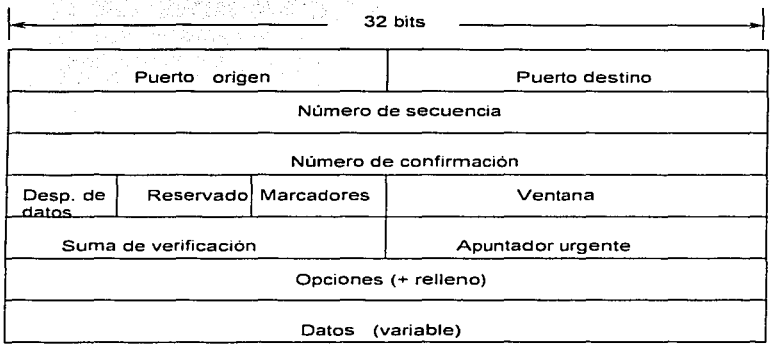


Fig 1.34 Un paquete TCP esta compuesto por doce campos.

Describimos los campos del paquete TCP que se ilustran en la figura 1.34:

- Puerto origen y Puerto destino- Identifican los puntos en que los procesos de origen y destino de las capas superiores reciben los servicios TCP.
- Número de secuencia – En general, especifica el número que se le asigna al primer byte de datos en el mensaje actual. En la fase del establecimiento de la conexión, este campo también puede utilizarse para identificar un número de secuencia inicial que será utilizado en una transmisión futura.
- Número de confirmación – Contienen el número de secuencia del siguiente byte de datos que el emisor del paquete espera recibir.
- Desplazamiento de datos – indica el número de palabras de 32 bits en el encabezado de TCP.
- Reservado- Permanece reservado para su uso en un futuro.

- Apuntadores - Transportan una gran variedad de información de control, incluyendo los bits de SYN y ACK utilizados para el establecimiento de la conexión y el bit FIN que se utiliza para la terminación de la conexión.
- Ventana – Especifica el tamaño de la ventana del receptor del emisor 8esto es, el espacio de almacenamiento disponible para los datos entrantes).
- Suma de verificación - Indica si el encabezado se daño durante su viaje.
- Apuntador urgente - Apunta hacia el primer byte de datos urgente en el paquete.
- Opciones – Especifica las diferentes opciones de TCP.
- Datos - Contiene información de las capas superiores.

1.10.7 Protocolo UDP

UDP (Protocolo de Datagrama de Usuario) Es un protocolo de la capa de transporte (Capa 4) no orientado a la conexión, que pertenece a la familia de protocolos de Internet. El UDP es, basicamente, una interfase entre IP y los procesos de las capas superiores. Los puertos del protocolo UDP distinguen entre las diversas aplicaciones que corren en un solo dispositivo.
A diferencia de TCP, UDP no agrega a IP funciones de confiabilidad, control del flujo y recuperación de errores. Debido a la simplicidad de los UDPs, los encabezados de los encabezados de los UDPs contienen menos bytes y generan un menor gasto indirecto en la red que el TCP.
UDP es útil en situaciones donde no se requieren mecanismos de confiabilidad de TCP, como cuando un protocolo de las capas superiores ofrezca las funciones de recuperación de errores y control de flujo.

UDP es el protocolo de transporte de varios protocolos bien conocidos de la capa de aplicación, entre los cuales se incluye n NFS (Sistema de Archivos de Red),SNMP(Protocolo Simple de Administración de la Red), DNS (Sistema de Nombres de Dominio) y TFTP (Protocolo Trivial de Transferencia de Archivos).

El Formato del paquete UDP tienen cuatro campos, como se muestra en la figura 1.35. Entre estos se cuentan los campos de los puertos de origen y destino, el de longitud y el de la suma de verificación.

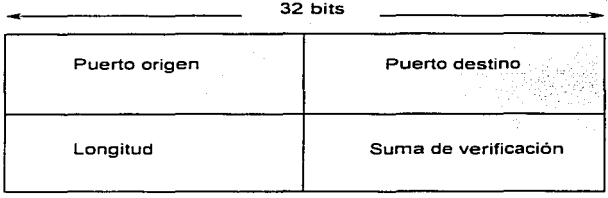


Fig 1.35 Un paquete UDP consta de cuatro campos

Los puertos origen y destino constan de números de puerto de protocolo UDP de 16 bits que se utilizan para demultiplexar datagramas para los procesos de recepción de la capa de aplicación. Un campo de longitud especifica la longitud del encabezado y de los datos del UDP. La suma de verificación ofrece una verificación de la integridad (opcional) del encabezado y los datos del UDP.

CAPITULO 2

DESCRIPCION DE LA ESTRUCTURA ACTUAL DE RED UNAM.

En el transcurso de este capítulo se verá la historia y evolución de RedUNAM, así como la estructura actual de la red de datos de manera modular con la finalidad de dar un enfoque más detallado de su funcionamiento y los problemas que presenta por lo que éste capitulo se encuentra dividido en cinco partes:

- Historia y Descripción general de RedUNAM
- Nivel de Transporte: Ethernet, Fast Ethernet, ATM y LANE
- Nivel de Red: switches capa 3, backbone de routers
- Problemática
- Desventajas de la estructura de enrutamiento actual.

2.1 Historia de RedUNAM

En el año del 1987, la UNAM establece la primera conexión de la Red Académica de cómputo de aquel entonces con la Red BITENET mediante enlaces telefónicos desde Ciudad Universitaria hasta el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) en Monterrey y de ahí hasta San Antonio, Texas en los EUA. Dicha conexión consistia en una computadora IBM 4381 para manejo de correo electrónico.

Para 1989, a través del Instituto de Astronomía se establece un convenio para enlazar a la red académica de la UNAM con la red de la NFS en EUA. El enlace se realizó mediante el satélite mexicano Morelos II que conectaba el Instituto de Astronomía en la UNAM y el UCAR-NCAR con residencia en Boulder Colorado. La finalidad del proyecto estaba enfocada a la investigación de fenómenos astrales. A la par se llevó a cabo el primer enlace para conectar las redes de área local, del Instituto de Astronomía y la Dirección General de Servicios de Cómputo Académico (DGSCA) utilizando enlaces de fibra óptica. A partir de ese momento se inició dentro de la UNAM una revolución en las comunicaciones.

Acciones como la adquisición masiva de computadoras personales, su conexión a red y la intercomunicación de redes de área local (principalmente en las dependencias de investigación científica) permitió desarrollar la infraestructura de comunicaciones de fibra óptica actual de RedUNAM, establecer más enlaces satelitales hacia Cuernavaca, Morelos, y San Pedro Mártir en Ensenada, Baja California Norte, también el primer enlace de microondas de alta velocidad sobre la Ciudad de México entre la Torre II de Humanidades y la Dirección General de Servicios de Cómputo Académico, DGSCA.

Para el año de 1990 la UNAM, fue la primera institución en Latinoamérica que se incorpora a la red mundial Internet, que enlaza a millones de máquinas y

decenas de millones de usuarios en todo el mundo. Su ininterrumpido desarrollo contempla como elemento fundamental el diseño de una arquitectura que permita la comunicación de redes de diferentes arquitecturas trabajando bajo el protocolo TCP/IP mismo que se mantiene como estándar en la actualidad dado su funcionalidad y posibilidad de adaptación a los requerimientos que se van presentando.

La operación de la Red Integral de Telecomunicaciones con una plataforma de backbone basada en la tecnología ATM dio inicio en la primera semana del mes de agosto de 1997. En esa fecha solo se enviaba tráfico de datos. Para la segunda quincena del mes de octubre se incorpora el tráfico de voz y videoconferencia. Este mismo esquema basado en ATM se encuentra en funcionamiento hoy en día y es el que se explica a lo largo de este capítulo.

Uno de los aspectos relevantes de la Red Integral de Telecomunicaciones de la UNAM es la interoperabilidad, ya que la plataforma de RedUNAM esta formada por equipos de diferentes fabricantes, sin embargo, aunque los productos cumplen con los estándares, se tuvieron en un principio algunas incompatibilidades entre ellos, éstas incompatibilidades fueron resueltas con actualizaciones en las versiones del software y que a la fecha están interoperando adecuadamente. Desde entonces a la fecha, se han hecho muchas mejoras a las versiones de software lo que permite optimizar el funcionamiento de los equipos entre las que destaca mejorar el esquema de enrutamiento estático.

2.2 Descripción general de RedUNAM

RedUNAM es el proyecto que se desarrolló para la transmisión de información entre las facultades, institutos, centros de difusión, coordinaciones y demás dependencias que conforman a la UNAM. Actualmente RedUNAM cuenta con más de 25,000 computadoras conectadas a la red de datos, más de 424 líneas del sistema telefónico digital que atienden a cerca de 12,000 cuentas de Dial-Up y 11 enlaces internacionales sumando una capacidad de transmisión de más de 21 Mbps a EE.UU. para la conexión a Internet.

RedUNAM es una red de computadoras LAN dentro de las dependencias e institutos; MAN con las conexiones a las ENEPs, FESes, Preparatorias, CCHs y demás centros dentro del área metropolitana; WAN en las conexiones con instituciones externas (instituciones públicas y privadas) y enlaces internacionales. Utiliza tecnología Ethernet, Fast Ethernet, ATM y TDM que sirven como infraestructura para comunicarse principalmente por medio de la suite de protocolos TCP/IP.

Debido a la complejidad y tamaño de la red, se describe únicamente la parte que concierne a la tesis, es decir, las conexiones de los equipos que conforman el backbone y la forma en como interactúan para posteriormente poder entender el comportamiento que presentan en el enrutamiento de datos. El objetivo que se pretende alcanzar en éste capítulo está más enfocado a la

parte del enrutamiento de datos, por lo que la parte referente a enlace de datos se mencionará de manera somera.

2.3 Nivel de transporte

A grandes rasgos, la capa encargada del transporte de información de la red de la UNAM cuenta con un core, una capa de distribución y una de acceso.

Core

Se maneja un backbone de ATM debido a que posee las siguientes ventajas: integración de servicios (voz, datos y video), mayor ancho de banda (155 Mbps), posibilidades de escalabilidad, redundancia en enlaces, etc. Sin embargo, la tecnología ATM no es completamente compatible con las tecnologías de redes LAN, por lo que se hace necesario usar un mecanismo que permita la interacción de ambas, es decir, emular redes LAN o LANEmulation. LANE es el método para permitir a los dispositivos de redes locales comunicarse sobre ATM sin realizar cambios en protocolos de capas superiores y software de aplicación (LANE se explica más a detalle en capítulo anterior).

Distribución

Debido a que la tecnología ATM es muy costosa para hacerla llegar a las dependencias, y además de que las dependencias de la UNAM en su mayoría cuenta con redes Ethernet, se optó por seleccionar la tecnología Fast Ethernet como medio para conectar las dependencias hacia el core (capa de distribución). Fast Ethernet ofrece las ventajas de costos aceptables, compatibilidad con las redes LAN y debido a que es una tecnología switcheada, nos permite mejorar el manejo de tráfico de broadcast.

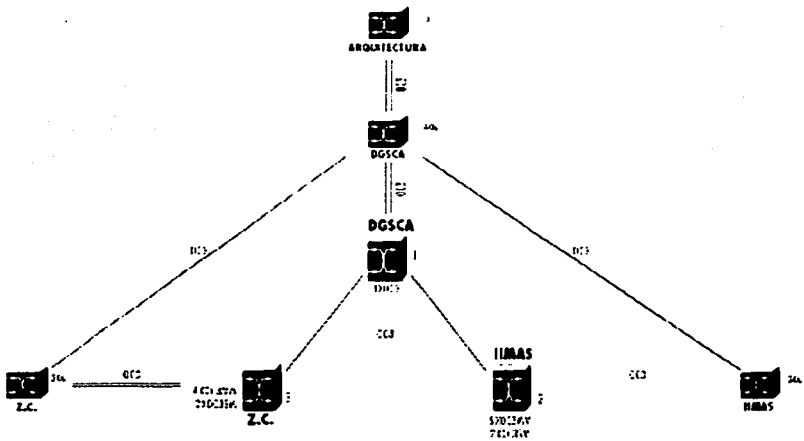
Acceso

Casi todos los equipos de cómputo de las dependencias de la UNAM poseen tarjetas de red con tecnología Ethernet, de modo que éstos al conectarse a RedUNAM hacen uso de ésta tecnología (capa de acceso). La capa de acceso se refiere a la interfaz final hacia el usuario.

De lo anterior, la estructura global de RedUNAM se observa en la figura 2.1

Esquema del funcionamiento global en capa 2 de RedUNAM
Fig. 2.1

Ahora que se ha dado la idea general de la estructura de transporte, se procede a describir el funcionamiento de RedUNAM de acuerdo a los equipos que la integran y a las funciones que realizan dentro de cada una de las capas (core, distribución, acceso). Los principales equipos que son: Passport 160 (core), CELLplex 7000 (core, distribución, acceso), LANplex (distribución y acceso).



Backbone ATM de RedUNAM
Fig 2.2

Switches ATM Passport 160

Los equipos 1, 2, 3 son switches ATM del modelo Passport 160 marca Nortel con interfaces de OC-3 ATM para datos, E1s para voz y video, y Frame Relay para la interfaz de administración del equipo. Este equipo conforma el backbone o core de servicios integrados de RedUNAM. Como únicamente nos concierne la parte de datos, sólo se tomarán a los equipos Passport como equipos de transporte de celdas ATM y no se profundizará en ellos.

Switches ATM/LAN CELLplex 7000

Por el contrario, los equipos 10, 20, 30, 40 de la figura 2.2 dedicados a datos, son switches ATM/LAN CELLplex 7000 de la marca 3Com que provee servicios de las tres capas por medio de las interfaces:

- OC-3 de ATM que proveen el transporte de información en celdas ATM (core).
- Fast Ethernet para la conexión hacia los switches LANplex 2500 (capa de distribución).
- Ethernet para 22 redes LAN de las diferentes facultades, dependencias e institutos internos de la UNAM (capa de acceso).

Las características de los equipos LANplex se explicaran más adelante.

Como se observa el CELLplex 7000 tiene funciones en el core, en la distribución y en el acceso. Por lo anterior, también provee los servicios de LANE ya que provee la interacción de las redes LAN de la UNAM con el core ATM.

Funcionamiento de LANE en el CELLplex 7000

En RedUNAM, la emulación de redes LAN (LANE) funciona de la siguiente manera:

- Dentro de la nube ATM existen dispositivos con interfaces tanto de ATM como Ethernet o Fast Ethernet (CELLplex 7000), que implementan los servicios de LANE (LECS, LES, BUS, LEC vistos en el capítulo I).
- Estos equipos permiten crear redes virtuales dispersas geográficamente llamadas ELANs.
- Cada ELAN actúa de manera análoga a un dominio de broadcast[1].
- Todo equipo conectado a una interfaz Ethernet o Fast Ethernet del CELLplex tiene configurado una ELAN.
- RedUNAM soporta 64 ELANs, cada uno de los cuatro CELLplex aloja 16 ELANs.
- De las 64 ELANs, actualmente sólo operan 23 de ellas.
- 22 de ellas están asignadas a 22 dependencias internas de RedUNAM.
- La restante, es la ELAN de administración.
- La ELAN de administración funge como backbone o core para todas las redes de las dependencias de la UNAM, ya que conecta a todos los equipos LAN (switches LAN, switches capa 3 y enrutadores) necesarios para brindar el funcionamiento sobre TCP/IP de RedUNAM.
- Dicha ELAN es el punto donde toda la información de los diferentes segmentos debe de circular para alcanzar algún segmento diferente e inclusive la salida hacia Internet (a excepción de las dependencias que

[1] Un dominio de broadcast es un conjunto de máquinas que reciben un paquete tipo broadcast enviado por cualquiera de las máquinas. Un dominio de broadcast generalmente corresponde a una subred.

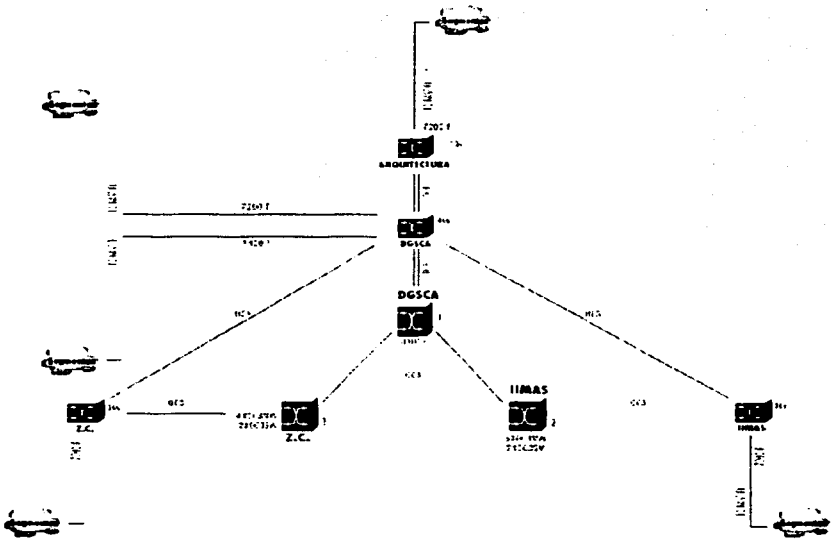
se conectan dentro de un mismo LANplex). Estos equipos se explican más adelante.

Las ventajas que provee esta configuración a través de LANE dentro de la UNAM son:

- Mayor velocidad de transmisión (155 Mbps).
- Reducción en los costos debidos a cambios y movimientos de dependencias, ya que con la creación de redes emuladas, si alguna dependencia se cambia de edificio o crece su red a un nuevo edificio, los cambios sólo se llevan a cabo en la configuración de los CELLplex 7000 sin realizar ningún cambio físico.
- Mayor rapidez en el caso de tener la red de determinada dependencia segmentada y separada geográficamente ya que se elimina el uso de equipos de capa 3: enrutadores "switchear es más rápido y barato que enrutar".
- Creación de grupos de trabajo dispersos, tal es el caso de la ELAN de administración ya que tiene configurados equipos en diferentes partes geográficas del campus universitario.
- De lo anterior tenemos una operación y administración centralizada de todos los equipos de backbone en una sola ELAN.
- Capacidad de escalamiento en la velocidad de transmisión, ya que ATM nos provee la característica de incrementar en ancho de banda a diferencia de las redes LAN.

Como se ha venido explicando, la ELAN de administración permite la interconexión de todos los equipos que intervienen en el enrutamiento en un solo segmento de broadcast, lo que permite que la comunicación entre todos ellos sea una comunicación de punto a punto para ofrecer un mejor servicio de distribución y por consiguiente un mejor enrutamiento.

Como se mencionó anteriormente, existen 22 dependencias, representadas por las nubes en la figura 2.3, conectadas a uno de los puertos del CELLplex 7000 y configuradas a una ELAN diferente de la de administración. Estas dependencias representan la capa de acceso dentro del CELLplex.



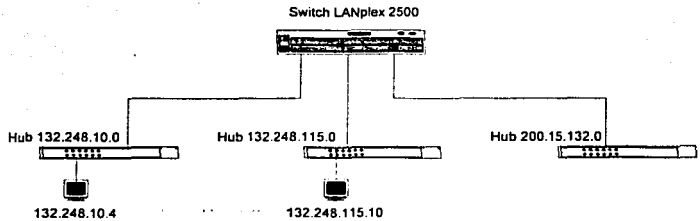
Dependencias internas en el CELLplex 7000
Fig. 2.3

Switches LAN LANplex 2500.

En la capa de acceso a RedUNAM, la mayor parte de los institutos, facultades y dependencias de la UNAM se conectan a través de uno o varios segmentos de red Ethernet, dependiendo del número de equipos DTEs que posea dicha dependencia. Estos segmentos de red se encuentran conectados a través de un switch LAN con capacidades de enrutamiento modelo LANplex 2500 de la marca 3Com. Dicho equipo cuenta con una interfaz de Fast Ethernet para llevar a cabo la capa de distribución de las dependencias y comunicarlas hacia el core.

Para dar un ejemplo de la capa de acceso, en la siguiente figura se observa que toda dependencia se conecta a través de un hub o switch a un puerto Ethernet en el LANplex 2500. Éste puerto puede ser de fibra óptica o UTP

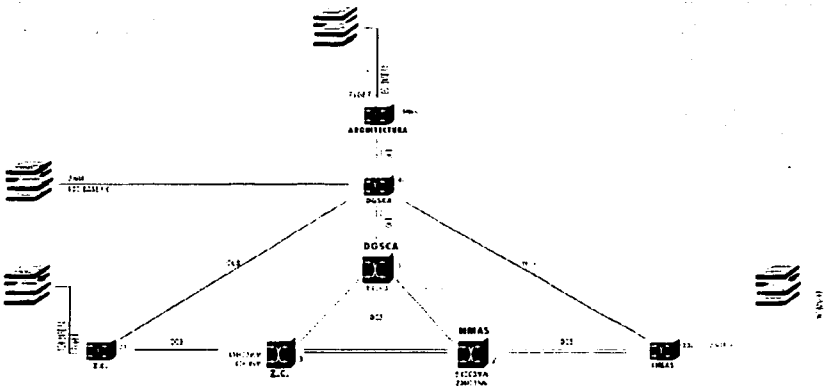
dependiendo de la distancia geográfica entre el LANplex y la dependencia. Por otra parte, la capa de distribución al core se realiza a través de un puerto Fast Ethernet configurado en la ELAN de administración.



Dependencias dentro del LANplex 2500
Fig. 2.4

En conjunto, los 26 LANplex con que cuenta la Universidad (conectados de los equipos 10, 20, 30, y 40), cada uno de ellos cuenta en promedio con 5 segmentos de red Ethernet (5 dependencias) para dar servicio a un total de 99 dependencias. Estos equipos están repartidos dentro de los cuatro nodos de telecomunicaciones de la UNAM como sigue:

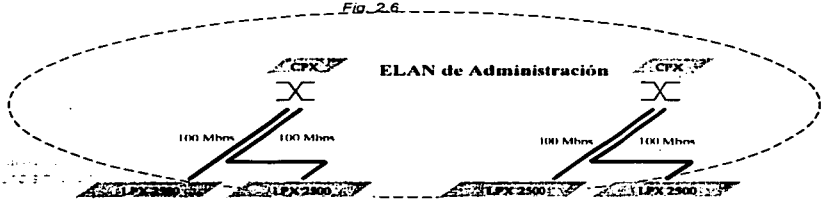
- Nodo DGSCA con 7 LANplex.
- Nodo Zona Cultural con 4 LANplex.
- Nodo IIMAS con 8 LANplex.
- Nodo Arquitectura con 6 LANplex.



LANplex 2500 en el Backbone
Fig. 2.5

Las interfaces de conexión entre los LANplex y los CELLplex son a través de tecnología Fast Ethernet con la finalidad de brindar una distribución de la información de todas las dependencias conectadas al LANplex con un ancho de banda adecuado. La interfaz Fast Ethernet que conecta al LANplex 2500 con el CELLplex se configura a la ELAN de administración (ver figura 2.6) por lo que todos los LANplex pertenecen a la misma red emulada o lo que es lo mismo, la comunicación que establecen entre ellos es de punto a punto con la finalidad de establecer un óptimo enrutamiento de información entre las dependencias.

Fig. 2.6



Sin embargo, todas estas dependencias requieren establecer comunicación con las demás e inclusive con el resto de Internet, por lo que es necesario implantar servicios de enrutamiento de datos a través de TCP/IP.

2.4 Nivel de enrutamiento

En el ámbito de enrutamiento, la RedUNAM cuenta con un conjunto de redes de instituciones externas e internas[2], además de las conexiones a Internet. Actualmente la UNAM cuenta con 84 enlaces hacia instituciones externas, 71 enlaces a instituciones internas, además de 11 enlaces internacionales (9 enlaces E1s y 2 T1s) para brindar un ancho de banda de 21 Mbps aproximadamente de salida a Internet. Todo esto se explica con mayor detalle a lo largo de ésta capítulo.

Pero antes de profundizar en el tema de enrutamiento, y recordando que RedUNAM trabaja con protocolos de enrutamiento que hacen uso de la tecnología TCP/IP, es necesario hablar acerca de la asignación de las subredes IP dentro de la UNAM.

Todas las ELANs y las redes Ethernet de las diferentes dependencias tienen asignado un segmento de red para proveer el enrutamiento de información de TCP/IP entre ellas. La RedUNAM cuenta con dos redes clase B la 132.248.0.0 y la 132.247.0.0, además del bloque de direcciones clase C de la 200.15.1.0 a la 200.15.254.0 asignada por la Universidad de Rice para ser administrada por la UNAM, es decir, en calidad de préstamo.

La red 200.15.0.0 está asignada a redes de dependencias externas, cuando hablamos de instituciones externas nos referimos a las redes de instituciones ajenas a la UNAM como pueden ser hospitales, escuelas particulares, instituciones gubernamentales, etc. La red 132.247.0.0 no está asignada actualmente y para el caso de la red 132.248.0.0, para hacer mejor uso de ésta red clase B, se hace necesario subnetearla, para lo cual se utiliza la mascara de red; en RedUNAM se utiliza la mascara de red 255.255.255.0 o mascara de 24 bits. La mascara de 24 bits nos genera 255 subredes (ver capítulo I para mayor detalle) de la 132.248.0.0 a la 132.248.2555.255. Con excepción de la 132.248.0.0 usada como identificador de la red clase B y la 132.248.255.255 dirección de broadcast de la red clase B, las demás subredes están asignadas a dependencias internas de la UNAM, por dependencias internas nos referimos a todas las redes de instituciones que dependen directamente de la UNAM como lo son facultades, institutos de investigación, CCHs, preparatorias, FESs.

Sin embargo el subnetear la red implica separar la red en segmentos completamente independientes en el nivel de enrutamiento. Así, aunque se mejoró el direccionamiento IP para la red clase B 132.248.0.0 ahora se tiene el problema de comunicar diferentes subredes. Para resolver lo anterior, se hace

[2] Para mayor información de las dependencias conectadas a RedUNAM consultar los URLs http://www.dgsca.unam.mx/REDUNAM/inst-externas.html y http://www.dgsca.unam.mx/REDUNAM/nodos.html.

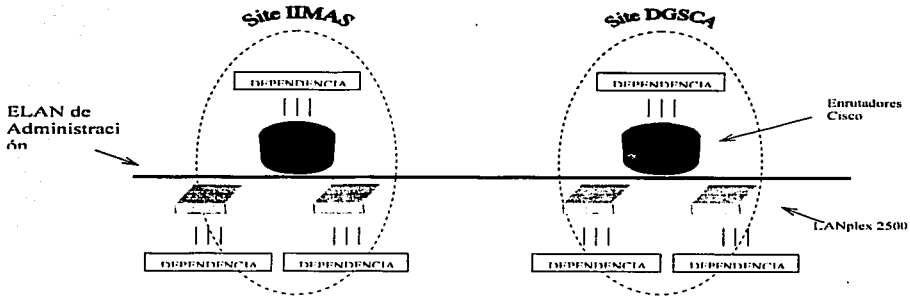
necesario implantar enrutamiento entre los diferentes segmentos de dependencias a través de equipos enrutadores. A éstos equipos se les asigna la última dirección de cada subred, la 254 (ejemplo 132.248.*.254, donde * puede ser de la 1 a la 254). Dentro de las redes Internet (redes que hacen uso del protocolo TCP/IP), a éste equipo se le conoce como Default Gateway ya que permite la comunicación entre varias subredes independientes.

Por lo anterior hay tres cosas importantes que recordar en el enrutamiento de información en IP para todos los equipos:

Dirección de Subred:
Cualquier dirección que termine en cero, 132.248.[1-254].**0**.
Dirección IP:
Puede ir de la 132.248. **[1-254].[1-253]**.
Default Gateway:
Dirección asignada a un enrutador con terminación 254, 132.248.[1-254].**254**.
Mascara de red:
Para subnetear la clase B en RedUNAM se utiliza **255.255.255.0** o mascara de 24 bits.

La RedUNAM para fines de administración y de enrutamiento tiene asignada toda la subred 132.248.254.0 a la ELAN de administración y dentro de ella se encuentran todos los equipos encargados del enrutamiento.

La estructura general de enrutamiento de la RedUNAM es un sistema plano o lineal. Como se menciono en el capitulo anterior, en éste enrutamiento todos los equipos con función de enrutamiento son peers o vecinos, es decir, se encuentran en un mismo dominio de broadcast como se muestra en la figura 2.7.



Esquema del funcionamiento global de enrutamiento de RedUNAM
Fig. 2.7

Como se puede observar, las dependencias internas se encuentran conectadas en los puertos de los equipos LANplex 2500; las dependencias conectadas al CELLplex y configuradas a una ELAN diferente a la de administración se representan conectadas a los Cisco (que es la forma en como se comportan a nivel de enrutamiento como se verá más adelante). La ELAN de administración está representada por el segmento de red que interconecta a los equipos que poseen capacidades de enrutamiento (Ciscos y LANplex). El enrutamiento de información entre las diferentes dependencias puede ser de distintos tipos:

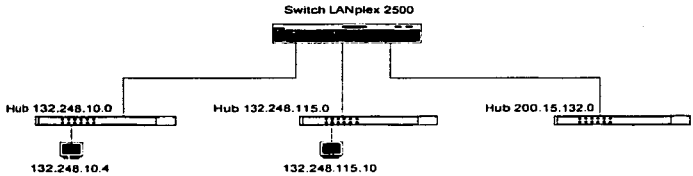
- Dependencias conectadas en un mismo LANplex.
- Dependencias conectadas en los CELLplex.
- Dependencias conectadas en los Cisco.

Dependencias conectadas dentro del mismo LANplex.

Los LANplex 2500 no llevan a cabo el proceso de enrutamiento de información ya que actualmente no poseen la configuración necesaria (aunque es capaz de hacerlo); por el contrario, cuentan con una configuración de ruta estática hacia un equipo que sí esté ejecutando un proceso de enrutamiento (cualquier equipo Cisco).

A pesar de esto, los equipos de computo (PC's, workstation, etc.) de 99 dependencias de la UNAM poseen configurado como Default Gateway a un LANplex por poseer características de enrutamiento. Este equipo es capaz de identificar únicamente el tráfico que tenga como destino un segmento de subred dentro del mismo switch y lo enruta por el puerto adecuado.

Por ejemplo, como se observa en la figura 2.8, si la máquina 132.248.10.4 desea comunicarse con la máquina 132.248.115.10, el switch será capaz de encaminar los paquetes por el puerto correspondiente.



Dependencias dentro del LANplex 2500

Fig. 2.8

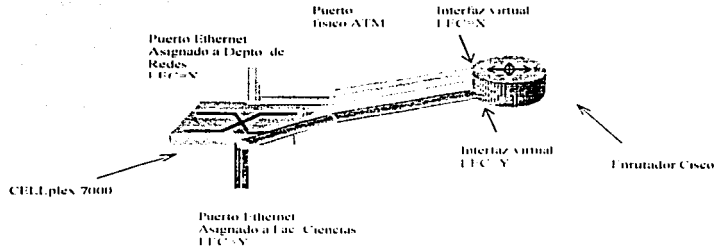
La forma en como el LANplex 2500 decide hacia donde enviar la información es a través de una tabla de enrutamiento. Esta tabla contiene las redes o subredes que tiene directamente conectadas (para este caso las subredes 132.248.10.0, 132.248.115.0 y la 200.15.132.0), adicionalmente posee una ruta estática hacia su salida o ruta por default (el Cisco) utilizada para enviar la información cuando no tiene directamente conectada la red destino. Por lo tanto todo el enrutamiento de las dependencias que se conectan a un LANplex y tiene como destino una red fuera del mismo depende totalmente del Cisco, éste el que se encarga de enrutarlas a cualquier parte de RedUNAM e inclusive de Internet. Un ejemplo de la tabla de enrutamiento dentro de un LANplex es la siguiente:

Destination	***Subnet mask***	***Metric***	***Gateway***	***Status***
Default Route	--	--	*132.248.254.25 4*	*Static*
132.248.10.0	*255.255.255.0*	--	--	*Direct*
132.248.115.0	*255.255.255.0*	--	--	*Direct*
132.248.254.0	*255.255.255.0*	--	--	*Direct*
200.15.132.0	*255.255.255.248*	--	--	*Direct*

Tabla de enrutamiento

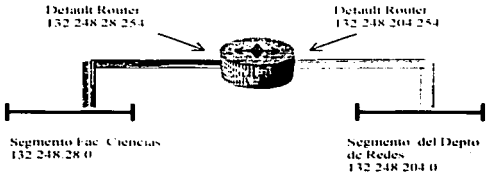
Dependencias conectadas dentro de los CELLplex

Existen 22 dependencias internas de RedUNAM que se encuentran directamente conectadas a los puertos Ethernet/Fast Ethernet de los equipos CELLplex. Cada uno de los puertos del CELLplex es un Cliente de LANEmmulation (LEC). El Cisco por su parte posee una interfaz ATM, lo que permite crear múltiples LECs (conocidos como interfaces virtuales ATM). Todos LEC deben ser configurados a una ELAN.



Vista física de las diferentes ELANs
Fig. 2.9

Una vez que el/los puertos del CELLplex y una interfaz virtual del Cisco se asocian a una misma ELAN, a ésta se le asigna una subred IP dentro del rango 132.248.1.0 — 132.248.253.0. De lo anterior, la conexión a través de LANE emulando una red 802.3 antes explicada nos permite una topología lógica muy parecida a la de un segmento físico Ethernet como se muestra en la Fig. 2.10:



Vista lógica de las diferentes ELANs
Fig. 2.10

En la figura 2.10, se muestra que todas las subredes de las dependencias conectadas al CELLplex poseen su Default Gateway en un puerto virtual ATM dentro del Cisco.

Por lo tanto, la forma en como trabajan el enrutamiento en las dependencias conectadas a los CELLplex es muy similar a la que se presenta en un segmento Ethernet, si un equipo que se conecta en un puerto del CELLplex quiere comunicarse con cualquier equipo en algún otro segmento, a través de LANE buscará el puerto de su Default Router en el Cisco para que este lo

encamine a algún otro puerto virtual ATM, un puerto físico Ethernet, FDDI e inclusive a través de un puerto serial hacia alguna red externa a RedUNAM. Para mayor detalle, como su funcionamiento es el mismo que presenta cualquier red conectada al Cisco se describe más adelante.

Cabe destacar que cuando se forma una ELAN, los clientes de LANE (LEC) pueden estar distribuidos geográficamente, lo que significa que el(los) puerto(s) del CELLplex asignado(s) a la dependencia y la interfaz virtual dentro del puerto ATM del Cisco pueden estar geográficamente separados. Tal es el caso de la ELAN de administración.

La topología lógica y física explicada anteriormente se presenta también en los equipos de la ELAN de administración. Todos los equipos que se conectan a los CELLplex —LANplex 2500, equipos de monitoreo y los equipos de acceso remoto— y algunas interfaces virtuales dentro de los Cisco se configuran a la ELAN de administración. A ésta ELAN se le asigna el segmento de red 132.248.254.0 de forma que todos los equipos dentro de la ELAN deben poseer una dirección dentro de dicho segmento como se muestra a continuación:

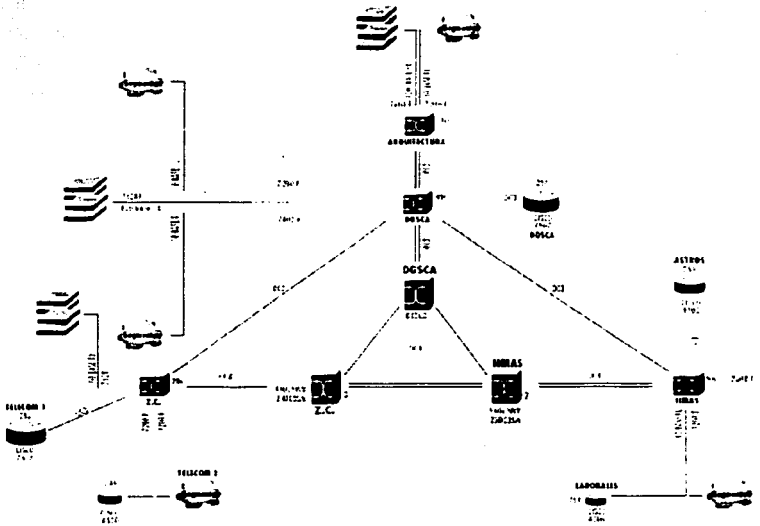
EQUIPOS	DGSCA	IIMAS	Zona Cultural	Arquitectura
CELLplex	132.248.254.40	132.248.254.30	132.248.254.20	132.248.254.10
LANplex	132.248.254.240 a 132.248.254.246 (7 LANplex)	132.248.254.230 a 132.248.254.237 (8 LANplex)	132.248.254.220 a 132.248.254.223 (4 LANplex)	132.248.254.210 a 132.248.254.215 (6 LANplex)
Cisco	132.248.254.254	132.248.254.253	132.248.254.252	132.248.254.251

La clasificación anterior es importante por que permite entender el esquema de enrutamiento dentro de RedUNAM. Todos los equipos que se conectan dentro de un CELLplex deben mantener el patrón de direcciones IP de acuerdo a ese CELLplex. Por ejemplo si el CELLplex tiene la dirección 132.248.254.**40**, todos los LANplex que se conecten a él deben conservar un direccionamiento del 132.248.254.**240** al 132.248.254.**246** y como se mencionó anteriormente los LANplex cuentan con una configuración de ruta estática hacia un equipo de enrutamiento, un equipo Cisco, éste tiene la dirección132.248.254.**254.** Como se observa todas las direcciones de los equipos dentro de un CELLplex (DGSCA en este caso) conservan el patrón de: 40, 240's, 254. Para el caso de Zona Cultural el patrón será: 20, 220's, 252.

Las interfaces virtuales ATM dentro del Cisco configuradas para las dependencias dentro de un CELLplex se configuran dentro del equipo de enrutamiento más cercano. Por ejemplo si la red de la Subdirección de Redes y Comunicaciones (segmento 132.248.204.0) se encuentra conectado en el CELLplex de DGSCA, la interfaz virtual se debe configurar dentro del Cisco conectado en DGSCA, el 132.248.254.254. De esta forma la interfaz virtual dentro del Cisco DGSCA tendrá asignada la dirección 132.248.204.254.

De manera análoga, los LANplex tendrán configurado como Default Gateway al Cisco que tengan más cercano, así, todos los LANplex de DGSCA tendrán configurado al 132.248.254.254, para los LANplex de Zona Cultural su Default Gateway será el 132.248.254.252.

En la figura 2.11 enfatizamos la topología lógica de enrutamiento para los equipos LANplex 2500 y de los CELLplex



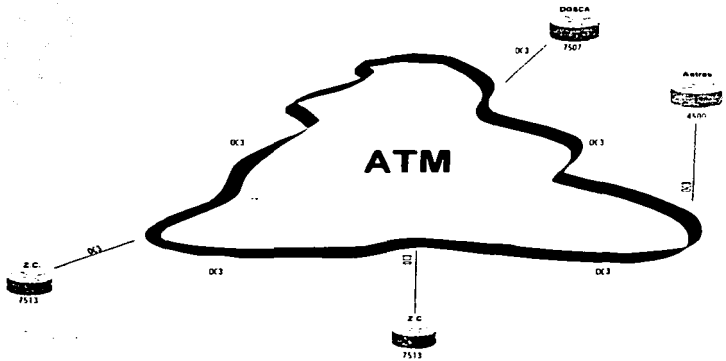
Topología lógica de enrutamiento
Fig. 2.11

Dependencias conectadas dentro de los Cisco

Dentro de ésta categoría entran las dependencias conectadas al CELLplex y las físicamente conectadas por un puerto Ethernet o serial al Cisco. Todos estos casos presentan el mismo comportamiento.

Ya que los equipos ATM CELLplex, puertos Ethernet y puertos seriales sólo brindan el transporte de la información para las dependencias conectadas a

ellos, se hace necesario contar con equipo que brinden la capacidad de enrutamiento de paquetes a través de TCP/IP —éste mismo equipo funge como Default Gateway para los switches LANplex que como se mencionó anteriormente no tienen configurado el proceso de enrutamiento—. Estos son los enrutadores marca Cisco que integran el backbone de enrutamiento de RedUNAM y que se muestra en la siguiente figura.



Backbone de enrutamiento
Fig. 2.12

Los enrutadores de RedUNAM permiten comunicar a los segmentos de diferentes dependencias internas y externas e institutos a la UNAM entre sí— es decir, segmentos que se encuentran conectados a los diferentes equipos CELLplex, LANplex y Cisco— y a su vez con el resto del mundo con conexiones internacionales a Internet. La forma en que estos equipos llevan a cabo el enrutamiento de información es a través del intercambio de información de enrutamiento con el fin de que todos los enrutadores pertenecientes al Sistema Autónomo de la UNAM tengan las rutas para poder llegar a cualquier otra red, sea dentro o fuera de la UNAM.

Los enrutadores Cisco tienen configurado dos tipos de enrutamiento: estático y dinámico. Esta configuración se debe a las diversas necesidades que se presentan en RedUNAM debido a la gran extensión geográfica, complejidad y diversidad de equipos que existen dentro de ésta.

2.4.1 Enrutamiento estático

El enrutamiento estático dentro de RedUNAM se tiene configurado entre los Cisco y los LANplex 2500, ya que estos últimos no están configurados para mantener una sesión de enrutamiento con los Cisco dado que no hablan el mismo lenguaje o protocolo de enrutamiento. Para que se lleve a cabo éste tipo de enrutamiento es necesario configurar rutas estáticas en ambos equipos de todas y cada una de las redes configuradas en un LANplex.

Hay que recordar que un enrutador con rutas estáticas reenvía la información a un equipo predeterminado, esto se lleva a cabo gracias a que se configura en el cisco una relación entre la red destino y el puerto o equipo por el cual puede llegar a esa red. Un ejemplo de ésta configuración estática en RedUNAM es la siguiente:

ip route 132.248.10.0 255.255.255.0 132.248.254.243
ip route 132.248.11.0 255.255.255.0 132.248.254.237

Dicha configuración se ve reflejada en la tabla de enrutamiento de la siguiente manera:

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
*i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default*
U - per-user static route, o - ODR

Gateway of last resort is 200.33.209.9 to network 200.33.208.0

B 170.170.37.0 [200/0] via 207.248.130.142, 10:44:02
S 132.248.10.0/24 [1/0] via 132.248.254.243
S 132.248.11.0/24 [1/0] via 132.248.254.237

Donde:

S = Indica que es una ruta estática.

Como se puede observar, la dirección 132.248.254.243 pertenece a un equipo LANplex en DGSCA y 132.248.254.237 a uno en IIMAS. Debajo de ellos se encuentran la red 132.248.10.0 y la 132.248.11.0 respectivamente, cuando cualquier paquete que sea procesado por un Cisco y tenga como destino cualquier red perteneciente al segmento 10 o al segmento 11, el enrutador ya sabe a que LANplex reenviarlo.

Este tipo de enrutamiento presenta muchas desventajas como son:

- Actualización constante por parte del administrador de las tablas de enrutamiento estático.

- Subutilización de las capacidades de enrutamiento de los equipos LANplex.
- Sobrecarga en el procesamiento de los enrutadores principales en horas pico lo que puede hacer que éstos fallen.
- Si uno de los Cisco falla, los LANplex que dependen de cada uno de ellos quedan sin servicio de red.
- En el caso de que falle un Cisco con salida a Internet, gran parte del ancho de banda internacional se pierde.

Sin embargo existen beneficios en el uso de éstas:

- Por ejemplo, las rutas programadas estáticamente te ayudan a tener una red más segura, ya que existe una ruta única tanto para entrar como para salir de dicha red o subred.

La configuración que se presenta para rutas estáticas en los equipos LANplex, donde todos y cada uno de ellos posee una ruta hacia un Cisco dentro del mismo site, se menciono anteriormente.

2.4.2 Enrutamiento dinámico

El proceso de enrutamiento dinámico se presenta con las instituciones externas a la UNAM y en los enlaces hacia Internet. El protocolo que se está utilizando para llevar a cabo el enrutamiento de paquetes dentro del backbone de enrutadores de RedUNAM es el protocolo propietario de CISCO: IGRP. *En las dependencias internas no se esta trabajando con este proceso de enrutamiento debido a que IGRP es propietario y ningún equipo 3COM puede entenderlo.*

Este proceso de enrutamiento se encuentra trabajando en todos los enrutadores administrados por la UNAM, como se menciono anteriormente los algoritmos de enrutamiento dinámico van ajustando las rutas en tiempo real, gracias a que analizan los mensajes de actualización de rutas. Una ventaja de éste tipo de algoritmos es que permite la implantación de rutas estáticas cuando estas sean necesarias como es el caso presentado anteriormente.

Un ejemplo de enrutamiento dinámico en los equipos Cisco se presenta en la siguiente tabla de enrutamiento:

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
*i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default*
U - per-user static route, o - ODR

Gateway of last resort is 200.33.209.9 to network 200.33.208.0

S 132.248.11.0/24 [1/0] via 132.248.254.237

I 200.15.55.0/24 [100/160358] via 132.248.254.249, 00:00:32, ATM0/0.1
I 200.15.80.0/24 [100/158358] via 200.15.3.108, 00:00:34, ATM0/0.1
[100/158358] via 192.100.199.28, 00:00:34, ATM0/0.1
[100/158358] via 192.100.200.76, 00:00:34, ATM0/0.1
[100/158358] via 132.247.254.252, 00:00:34, ATM0/0.1
I 200.15.20.0/24 [100/158550] via 192.100.199.99, 00:00:00, Ethernet4/3
I 192.100.164.0/24 [100/41162] via 192.100.199.34, 00:00:00, Serial6/3

Donde:

S = Indica que es una ruta estática.
I = Indica que es una ruta aprendida por el algoritmo de enrutamiento IGRP.

Como podemos observar en la tabla anterior, para poder llegar a una máquina perteneciente a la red 200.15.55.0 es necesario reenviar la información a un siguiente enrutador con dirección IP 132.248.254.249 a través de la interfaz virtual ATM0/0.1[3] y el segundo enrutador puede o no tener directamente conectada dicha red, en caso de tenerla conectada directamente lo envía por el puerto adecuado, en caso contrario realiza el mismo proceso de reenvío hacia otro enrutador, para de ésta manera llegar al destino.

En el caso de querer llegar a la red 200.15.80.0 como se puede observar existen cuatro opciones en la tabla de enrutamiento por la cual podemos llegar a dicha red, estas son a través de los siguientes enrutadores: 200.15.3.108, 192.100.199.28, 192.100.200.76 y el 132.247.254.252, todas a través de la interfaz virtual ATM0/0.1. Este tipo de configuración se debe gracias a que IGRP es un protocolo de enrutamiento muy sofisticado que acepta múltiples rutas para un mismo destino, a éste tipo de algoritmos se les llama Multipath

RedUNAM brinda a muchas instituciones externas la salida hacia Internet, por lo que RedUNAM es un ISP (Internet Service Provider), es decir, provee por medio de convenios a universidades, escuelas, dependencias gubernamentales externas a la UNAM que requieran conectarse a RedUNAM para poder tener conexión con Internet; también provee la asesoría técnica para la adquisición de equipo, medios de enlace, software.

Dos requisitos técnicos que las dependencias deben cubrir son: Contratar con un carrier (Telmex, Avantel, etc.) un enlace TDM dedicado que puede ser desde un DS0 hasta un E1 completo y contar con un equipo que provea los servicios de enrutamiento.

La conexión es muy sencilla, se colocan dos enrutadores en ambos extremos del enlace, por lo general la UNAM provee uno de los puertos dentro de los enrutadores de backbone. Existen algunos casos en los cuales las dependencias externas no cuentan con enrutadores marca Cisco, por lo que es necesario configurar el protocolo de enrutamiento estándar RIP en el enrutador

[3] Notación que se refiere a la tarjeta en el slot ATM cero, al puerto ATM cero e interfaz virtual 1.

de la dependencia externa así como en el enrutador de la UNAM que reciba la conexión. Sin embargo se requiere de una redistribución de rutas entre protocolos con el fin de anunciar las redes tanto de las dependencias externas hacia RedUNAM como las redes de RedUNAM e Internet hacia las dependencias. Todo este procedimiento tiene como objetivo que las redes de las dependencias sean alcanzables por todo equipo de cómputo en cualquier parte de la Internet y viceversa.

Aunque tenemos configurado lo necesario para llegar a cualquier red conectada directamente a RedUNAM a través de enrutamiento estático y los protocolos RIP e IGRP, se hace necesario configurar en los enrutadores un protocolo de compuerta externa que permita comunicar el Sistema Autónomo de la UNAM con otros para que todas las redes de RedUNAM y las redes de las instituciones que dependen de ella sean anunciadas al resto del mundo. Este se hace a través del protocolo estándar BGP (Border Gateway Protocolo).

Existen dos tipos de BGP: iBGP y eBGP. Enrutadores que pertenecen al mismo Sistema Autónomo de la UNAM e intercambian información de BGP, están hablando BGP interno (iBGP). Enrutadores que pertenecen a un diferente Sistema Autónomo de la UNAM e intercambian información de BGP, la hacen a través de BGP externo (eBGP).

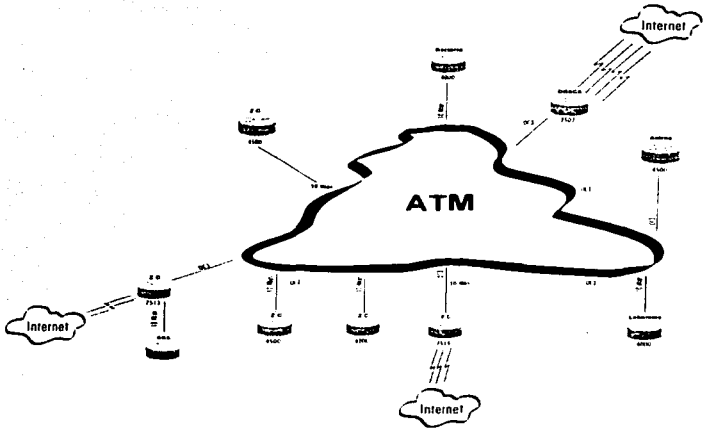
Antes de intercambiar información de enrutamiento con un Sistema Autónomo externo, BGP se asegura que todas las redes dentro de su Sistema Autónomo sean alcanzables, por lo que se hace necesario:

- Tener una configuración full-mesh (conexión en malla de todos contra todos) entre los enrutadores que hablan iBGP dentro del Sistema Autónomo a través de IGPs.
- Redistribuir rutas de IGP a BGP (y viceversa) del Sistema Autónomo, es decir, RIP e IGRP a BGP para el caso de RedUNAM.

Una vez que todas las redes internas de RedUNAM son conocidas por los enrutadores que tienen configurado el proceso de iBGP, se utiliza eBGP para anunciarlas a su(s) vecino(s) externo(s). De esta forma todas las redes que dependen de RedUNAM son anunciadas al resto del mundo. Un proceso similar realizan los demás Sistemas Autónomos de toda Internet.

Es por lo anterior que BGP solamente esta configurado en aquellos enrutadores que tienen enlaces con instituciones externas que pertenezcan a un Sistema Autónomo diferente al de la UNAM.

En la siguiente figura observamos que tres de los enrutadores de backbone tienen conexión hacia Internet, por lo tanto, cada uno de ellos tienen configurado eBGP para con sus vecinos de otros Sistemas Autónomos fuera de la UNAM e iBGP para con sus vecinos internos. En RedUNAM los enrutadores configurados con iBGP y eBGP son tres: dos enrutadores de ZC y uno más en DGSCA.



Salidas a Internet
Fig. 2.13

Los enrutadores que tienen conectadas las salidas internacionales de RedUNAM poseen una configuración más robusta, es por ello que éstos equipos necesitan ser mayores capacidades de hardware con respecto a los otros enrutadores del backbone debido a que manejan información de enrutamiento tanto de protocolos IGPs y EGPs y la redistribución que implica.

2.5 Desventajas de la estructura de enrutamiento actual

Enrutamiento estático:

En el caso de que la información dentro de un LANplex tenga como destino un segmento de red conectado fuera de éste equipo, el LANplex 2500 no está configurado para enrutarla debido a que cuenta con una configuración de enrutamiento estático a un gateway por default y aunque es capaz de hacerlo y originalmente estaba pensado de esa forma, no se implantó por lo incompatibilidad de RIP y el protocolo de enrutamiento del backbone, IGRP.

Esta configuración trae como consecuencia:

- Trabajo excesivo para los gateway por default de los LANplex (enrutadores Cisco) en horas pico.
- Subutilización de la capacidad de enrutamiento de los equipos LANplex.
- Actualización constante por parte del administrador de las tablas de enrutamiento estático.
- Si alguno de los Cisco falla, los LANplex que dependen de cada uno de ellos quedan sin servicios de capa 3 de OSI.

Los beneficios de OSPF si se implanta en RedUNAM son:

El objetivo principal de la tesis es proponer que se habiliten los servicios de enrutamiento de OSPF en los equipos LANplex para:

- Aligerar la carga de trabajo en los enrutadores Cisco.
- Aprovechar la capacidad de enrutamiento de los equipos LANplex.
- Dado que OSPF es un protocolo de enrutamiento estándar es el único que permite mantener compatibilidad entre equipos de enrutamiento de diferentes marcas, lo que permite no depender de un fabricante en particular.
- Implantación de un esquema de enrutamiento jerárquico que permite la segmentación de la red en áreas
- La asignación de áreas permite ocultar la información de enrutamiento entre enrutadores de diferentes áreas lo que elimina el tráfico en la red y proporciona un mejor aprovechamiento del ancho de banda.
- Se optimiza el tiempo de convergencia.
- Soporta esquemas de seguridad
- Se tienen mejores esquemas de administración.

CAPITULO 3

EVALUACIÓN DE TECNOLOGÍAS.

Tráfico inconstante, aplicaciones que consumen un gran ancho de banda están haciendo que las necesidades de los campus crezcan y que sus backbones cambien su infraestructura , hoy en día hay dos elecciones para que los backbones de los campus corran a una alta velocidad : ATM o Gigabit Ethernet. Esto es debido a varias razones, de negocios y técnicas.

Gigabit ethernet es seleccionada como una tecnología de posibilidades Una alta capacidad, un alto performance, y un backbone muy flexible tan escalable como las estaciones terminales crecen en número o exigen más ancho de banda. También se necesita la habilidad de apoyar niveles de servicio diferenciado (Calidad de Servicio o QoS), para que la alta prioridad, las aplicaciones sensibles al tiempo, y las de misión crítica puedan compartir la misma infraestructura de red como aquellos que requieren el servicio de best-effort

En el pasado, la mayoría de los campus usaban backbones de medio compartido (tales como redes token ring a 16/32 Mbps y redes FDDI a 100Mbps) que eran ligeramente más rápidas que las LAN's y que las estaciones terminales que interconectaban. Esto ha causado congestiones severas en los backbones de los campus cuando estos interconectan un número considerable de accesos a LAN.

Hasta hace poco tiempo. ATM (Modo de transferencia asincrona), era la única tecnología de switcheo para entregar alta capacidad y escalable ancho de banda, con la promesa de calidad de servicio de punto a punto. ATM ofreció integración transparente desde el escritorio, a través del campus, y sobre la MAN o WAN. Esto fue pensado, para los usuarios que quisieran desplegar masivamente recursos orientados a conexión, ATM basado en células, desde el escritorio para habilitar nuevas aplicaciones nativas de ATM y para influir en sus ricas funcionalidades (tales como Calidad de Servicio, QoS). Sin embargo esto no llego a pasar. El protocolo de Internet (IP), ayudado y alentado, por el explosivo crecimiento de Internet, montado sobre ATM, desplegándose y marchando implacable hacia la dominación.

Cuando no existía otra tecnología de velocidad en giga, ATM proporciono alivio a muchas necesidades, como altos anchos de banda para interconectar varias LAN. Pero con la masiva proliferación de aplicaciones IP, nuevas aplicaciones de ATM nativas no aparecieron. Incluso 25Mbps y 155 Mbps de ATM no llegaron a la mayoría de los usuarios debido a que era mucha su complejidad, solo se incrementaba el ancho de banda en muy poco y el costo era alto cuando se comparaba con el muy sencillo y no muy caro 100Mbps Fast Ethernet.

Por otro lado, Fast Ethernet, con su auto detección, sus capacidades de auto negociación, integración con los millones de clientes y servidores que corren a 10Mbps. Aunque relativamente simple y elegante en concepto , la

implementación actual de ATM es complicada por una multitud de protocolos estándar y especificaciones (por ejemplo, LAN Emulation, Private Network Node Interface, y Multiprotocolo sobre ATM). Esta complejidad adicional es requerida en orden para adaptar ATM al mundo basado en tramas sin conexión a los campus LAN (to the connectionless, frame – based world of the campus LAN) Mientras tanto , la experiencia tan exitosa de Fast Ethernet incito el desarrollo del estándar de Gigabit Ethernet. Desde su concepción (Junio 1996), Gigabit Ethernet sobre fibra (1000BASE-X) y cobre (1000BASE-T), estos estándares fueron aprobados, desarrollados y puestos en operación. Gigabit Ethernet no solo provee una escalabilidad masiva de ancho de banda a 1000 Mbps (1 Gbps), pero la ventaja es que también comparte una natural afinidad con las redes que son mucho muy vastas de base Ethernet y Fast Ethernet en los campus corriendo aplicaciones IP

Mejorado por protocolos adicionales ahora comunes en Ethernet (tales como IEEE 802.1Q Virtual LAN tagging, IEEE 802.1p priorización, IETF Differentiated Services, y Common Open Policy Services). Gigabit Ethernet es ahora capaz de proveer las diferentes calidades de servicio que previamente solo ATM podría dar. Una diferencia clave con Gigabit Ethernet es que adicionalmente a la funcionalidad puede ser incrementado en una forma no perjudicial como se vaya requiriendo, comparado con el mejor y revolucionado método de ATM. Desarrollos futuros en ancho de banda y escalabilidad en distancias verán 10Gbps Ethernet sobre redes locales (10G-BASE-T) y en WAN's (10G-BASE-WX). De esta manera, la promesa de integraciones punto a punto, que alguna vez solo se podía realizar con ATM, será posible con Ethernet y todas sus derivaciones.

Hoy en dia hay dos tecnologías a elegir para los backbones de los campus de alta velocidad: ATM y Gigabit Ethernet. Mientras ambos están tratando de proveer alto ancho de banda y calidad de servicio dentro de las diferentes LAN's, hay diferentes soluciones para esto.

Gigabit Ethernet es una apropiada elección para la mayoría de los backbones de los campus. Varios usuarios adentrados en diferentes negocios han escogido Gigabit Ethernet como la tecnología para las redes de sus campus, esto lo argumentamos basados en una investigación realizada por infonetics, estos estudios arrojaron como resultado que el 91 % de los encuestados cree que Gigabit Ethernet es una tecnología adecuada para conexiones de backbone hacia LAN, comparado con 66 % para ATM . ATM continúa siendo una buena opción donde su única, rica y compleja funcionalidad pueden ser exploradas por su despliegue, comúnmente en redes de área metropolitana y amplia (MAN'S y WAN'S).

Si Gigabit Ethernet o ATM es desplegado como la tecnología que se debe elegir para un campus, la última decisión es la económica y el sentido de negocio, mejor que puras consideraciones técnicas.

En los dos siguientes apartados describiremos brevemente a estas dos tecnologías: ATM y Gigabit Ethernet.

3.1 Modo de Transferencia Asíncrona (ATM)

ATM (Asynchronous Transfer Mode), que traducido es Modo de Transferencia Asíncrona, esta tecnología ha sido usada en los campus desde su introducción en el inicio de los 90's. ATM es específicamente diseñada para transportar múltiple tipo de tráfico –datos, voz y video, en tiempo real y en no real – con su inherente QoS para cada tipo de servicio .

Para habilitar este y otro tipo de capacidades, funciones adicionales y protocolos son agregados a la tecnología ATM básica. PNNI Private Network Node Interface (Interfaces de Nodo de Red Privadas) proporciona anuncios de OSPF, como funciones para señalar y rutear peticiones de QoS a través de una red jerárquica de ATM. Multiprotocolo sobre ATM (MPOA) permite el establecimiento de rutas de acceso directo entre sistemas finales de comunicación sobre diferentes subredes, saltándose los cuellos de botella que se llegan a formar en los routers, esto ha aumentado en conectividad de áreas físicas, escalabilidad en ancho de banda, señalización, ruteo y direccionamiento, seguridad y administración. Mientras es rico en características, estas funcionalidades han venido con una etiqueta con el precio muy alto en complejidad y costo. Para proveer a los backbone conectividad y para acceder a las redes actuales, ATM – una tecnología orientada a conexión- tiene que emular características que son inherentemente disponibles en las redes Ethernet LAN , incluyendo transmisiones broadcast, multicast y unicast.
ATM debe también que manipular el tráfico predominante basado en tramas sobre esas LAN'S, segmentando todas las tramas en celdas antes de la entrega final. Muchos de los asuntos de complejidad e interoperabilidad son resultado de esta emulación de LAN (LAN Emulation), también como de la necesidad de proveer elasticidad en estas LAN emuladas. Son muchos los componentes que se requieren para hacer esto práctico o factible , la configuración de servidores que emulen la LAN, servidores de : Broadcast , de multicast selectivo , de protocolo de sincronización de cache, interface de red para usuarios de LAN emulada y una multitud de protocolos adicionales , controles de señalización y conexiones (punto a punto , punto a multipunto, multipunto a punto y multipunto a multipunto).

Hasta hace poco, ATM fue la única tecnología capaz de prometer los beneficios de QoS desde el escritorio, cruzando la LAN y el campus, y alrededor del mundo. Sin embargo, el despliegue de ATM hacia el escritorio, al igual que en las LAN'S del backbone de algún campus, no ha sido difundido como se predijo. Tampoco no ha habido aplicaciones nativas disponibles o capaces de beneficiarse del las características inherentes de QoS proporcionadas por una solución ATM end to end. De esta manera, los beneficios de las conexiones end-to-end con QoS han sido más imaginados que realizados.
Gigabit Ethernet como la tecnología de elección para los backbones de los campus esta ahora sobrepasando a ATM. Este punto lo argumentamos debido a que la complejidad y el precio muchísimo mas alto de los componentes de ATM tales como tarjetas de red, switches, software para los diferentes

sistemas tales como de administración, herramientas de diagnóstico y personal con conocimientos especificos, a esto se le agregan cuestiones de interoperabilidad y una falta de "explotadores" calificados en la tecnología ATM.

3.1.1Gigabit Ethernet

Ahora en nuestros dias, Gigabit Ethernet es una solución muy atractiva y viable como para la infraestructura Lan de un backbone en un campus. Aunque relativamente nuevo, Gigabit Ethernet es derivado de una tecnología simple, y una base muy larga y bien probada como Ethernet y Fast Ethernet. Desde su introducción, Gigabit Ethernet ha sido adoptada vigorosamente como una tecnología para los backbone de los campus, con usos posibles como una alta capacidad de conexión para un alto performance en servidores y estaciones de trabajo hacia los switches de distribución del backbone. La razón principal para que esto tenga éxito es que Gigabit Ethernet provee la funcionalidad que reconoce hoy en día la necesidad inmediata con un precio costeable, sin una complejidad y un costo impropios. Gigabit Ethernet es complementado por un súper conjunto de funciones y capacidades que pueden ser agregadas como se necesite, con la promesa de mejoramiento en sus funcionalidades y escalabilidad en ancho de banda (por ejemplo, IEEE 802.3ad Link Agregation, y 10 Gbps Ethernet) en un futuro cercano , debido a que Gibabit Ethernet provee una escalabilidad de ancho de banda simple desde LANs que corren a 10/100 Mbps Ethernet y Fast Ethernet y que son empleadas masivamente, solo se pone , es decir que Gigabit Ethernet es Ethernet pero 100 veces más rápido

Desde que Gigabit Ethernet utiliza el mismo formato de trama, no se necesita la segmentación y la función de reensamble que ATM requiere para proveer transiciones de celdas a tramas y de tramas a celdas. Como una tecnología connection-less Gigabit Ethernet no requiere que se le agregue complejidad de señalización y protocolos de control y conexiones que ATM requiere. Finalmente, porque todas las capacidades de escritorio que QoS provee no son tan fácilmente disponibles, Gigabit Ethernet no es menos deficiente en proveer QoS. Nuevos métodos han sido desarrollados para incrementar la entrega de QoS y otras necesidades ademas de capacidades que prestan a estos mismos mucho más pragmáticos y adopción de costos efectivos y despliegue.

Para complementar la capacidad de ancho de banda de Gigabit Ethernet como una tecnología para un backbone de un campus, funciones de capas mas altas y protocolos son disponibles, o están siendo definidos por cuerpos de estándares tales como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) y el Internet Enginereering Task Force (IETF, Grupo de trabajo para el desarrollo de Internet). Muchas de estas capacidades reconocen el deseo de converger por encima del omnipresente protocolo de Internet (IP). Las aplicaciones IP y protocolos de transporte están siendo mejorados o desarrollados para direccionar las necesidades de alta velocidad, interconexión de multimedia que beneficia Gigabit Ethernet. Los estándares de servicios diferenciados (DiffServ) proveen a QoS diferencias que pueden

ser desplegadas desde escritorios con Ethernet y Fast Ethernet a través de un backbone en un campus con Gigabit Ethernet . El uso del estándar IEEE 802.1Q que se refiere al taggeo de VLANs y 802.1p. La configuración de usuarios con prioridad permite diferenciar tipos de tráfico, esto para acordar el apropiado avance de prioridades y servicios. Cuando se combina con "policy-enabled networks", DiffServ adquiere características muy poderosas como seguridad y flexibilidad en el aspecto de QoS , esto se da en Gigabit Ethernet usando protocolos tales como " Common Open Policy Services (COPS),Lightweight Directory Access Protocol (LDAP), Dynamic Host Configuration Protocol(DHCP), y Domain Name System (DNS), además desarrollos, tales como Resource Reservation Protocol, multicasting, real time multimedia, transporte audio y video, y telefonia IP, adicionaran funcionalidad a los campus con Gigabit Ethernet , usando un gradual y manejable acercamiento cuando los usuarios necesiten estas funciones. Hay diferencias técnicas importantes entre Gigabit Ethernet y ATM. Un consorcio de "White Papers", escribió "***Gigabit Ethernet and ATM: A Bussiness Perspective,*** provee una vista comparativa de dos tecnologias desde una perspectiva administrativa.

3.2 Aspectos Tecnológicos.

Los aspectos tecnológicos son muy importantes porque estos deben de tener en cuenta algunos mínimos requerimientos para que sean aceptables a los usuarios. Capacidades de valor agregado serán implementadas en donde se desee o en donde sea costeable. Si estas capacidades adicionales no son usadas, sea por razones de complejidad o por falta de gente que pueda explotar los beneficios de estas capacidades, entonces los usuarios están pagando por caracteristicas que no tienen sentido o razón (un ejemplo típico es que varias de las caracteristicas avanzadas de las VCR video Casete recorder son raramente utilizadas por la mayoria de los usuarios). Si las caracteristicas son muy caras, relativas a los beneficios que pueden ser derivados, entonces la tecnologia no encontraria una aceptación. Las elecciones de tecnologia son finalmente decisiones de negocios

Los requerimientos fundamentales para redes LAN de algún campus son mucho muy diferentes a los de una WAN. Esto de debe a que es necesario identificar los minimos requerimientos de una red, también como las capacidades de valor agregado que son "agradables" como para implementar.

En las secciones que siguen, varios términos son usados con los siguientes significados:

- "Ethernet ": es usado para referirse a todas variaciones actuales de la tecnologia Ethernet: tradicional 10 Mbps Ethernet, 100 Mbps Fast Ethernet, y 1000 Mbps Gigabit Ethernet.
- "Trama " y "Paquete" son usados de forma intercambiable, aunque esto no es absolutamente correcto desde un punto de vista técnico

3.3 Calidad de servicio (QoS)

Hasta hacer poco, Quality of Service (QoS) la llave diferenciadora entre ATM y Gigabit Ethernet. ATM fue la única tecnología que prometió QoS para voz, video y datos. El IETF (Grupo de trabajo para el desarrollo de Internet) y varios vendedores han estado desarrollando especificaciones de protocolos y estándares que enriquecen el mundo de "frame-switched" con capacidades de QoS y QoS-like. Estos esfuerzos se están acelerando, y en ciertos casos, se han desarrollado para usarse en ambos: en ATM y mundos basados en tramas.

La diferencia entre ATM y Gigabit Ethernet en la entrega de QoS es que ATM es orientado a conexión, mientras que Ethernet es no orientado a conexión. Con ATM, QoS es solicitado vía señalización antes de que la comunicación de comienzo. La conexión es solamente aceptada si esta no esta corrompida (especialmente para aplicaciones de anchos de banda reservados).
Recursos de red son entonces reservados como se requiere, y el aceptado servicio de QoS es garantizado para ser entregado a una conexion "end-to-end". En contraste, QoS para Ethernet es principalmente entregado "hop-by-hop" es decir salto por salto, con estándares en progreso para señalización, conexión, control de admisión, y reservación de recursos.

3.3.1 ATM QoS

Desde su nacimiento, ATM ha sido diseñado con QoS para voz, video y aplicaciones de datos. Cada uno de estos tiene sus diferentes tiempos de salto, retardo, sensibilidad a la variación y retardo (jitter), y requerimiento de ancho de banda.

En ATM, QoS tiene muchos y específicos significados que son materia del Forum ATM y otras especificaciones de estándares. Definido en la capa de ATM (OSI capa 2), el manejar esta arquitectura provee cinco categorías de servicios que relacionan características de tráfico y requerimientos de QoS para requerimientos de red.

*CBR Constant Bit Rate (Tasa o porcentaje de bit constante), para aplicaciones que son sensibles al retardo y variaciones de retardo, y necesitan un ajuste pero continuamente disponen de un porcentaje de ancho de banda para la duración de una conexión. El porcentaje de ancho de banda requerido es caracterizado por el "Peak Cell Rate". Un ejemplo de esto es un circuito de emulación
* rt-VBR Real –time Variable Bit Rate, tasa de bit variable en tiempo real, para aplicaciones que necesitan porcentajes variantes de ancho de banda con una regulación muy justa del delay (retardo) y del delay variation (variación del retardo) y cuyo tráfico es naturalmente a ráfagas. El porcentaje de ancho de banda es caracterizado por el "Peak Cell Rate" y el "Sustentable Cell Rate", las rafagas están definidas por el tamaño máximo de despliegues violentos.

Aplicaciones que pueden funcionar como ejemplo incluimos a la voz en tiempo real y videoconferencias.

- nrt-VBR: Non-real-time Variable Bit Rate, para aplicaciones con necesidades similares como rt- VBR, requiriendo baja perdida de celdas, porcentajes variantes de ancho de banda , y retardo no critico además de requerimientos de variación de retardo. Aplicaciones de ejemplo incluye voz y video en tiempo no real.
- ABR Available Bit rate, para aplicaciones que requieren baja pérdidas de celdas , mínimo y máximo ancho de banda garantizado, y con retardos no criticos o requerimientos de variaciones de retardo. El ancho de banda mínimo y máximo son caracterizados por el "Minimum Cell Rate "y el "Peak Cell Rate" respectivamente.
- UBR: unspecified Bit Rate, para aplicaciones que pueden usar la red sobre una base de mejor esfuerzo, que no garantiza el servicio de pérdida de celdas, delay(retardo) y delay variations (variaciones de retardo)aplicaciones que podemos ejemplificar para UBR son el e-mail y el FTP

Dependiendo de la petición de QoS, ATM provee un especifico nivel de servicio. En un extremo, ATM provee un mejor servicio para el más bajo QoS (UBR), sin ancho de banda reservado para el tráfico. En el otro extremo, ATM provee un nivel de servicio garantizado para el más alto QoS(que son ,CBR y VBR)el tráfico entre estos dos extremos, ABR esta disponible para usar cualquier ancho de banda, es disponible también para manejar tráfico adecuado y controlarlo.

Como ATM es orientado a conexión, las peticiones para un particular QoS, control de acceso, y localización de recursos es una parte integral de el "call signaling" y el proceso de establecimiento de la conexión. La llamada es admitida y la conexión establecida entre los sistemas terminales de comunicación, solo si los recursos existen como para hacer petición de QoS, sin arriesgar servicios que ya habían establecido conexiones. Una vez establecido, el tráfico de los sistemas terminales son vigilados y formados de acuerdo a un contrato de tráfico. Flujo y congestión son manejados en orden para asegurar la apropiada entrega de QoS

3.3.2 Gigabit Ethernet con QoS

Una simple estrategia para resolver el problema de congestión de backbone es dar una sobre dosis de ancho de banda en este mismo. Esto es especialmente atractivo si la inversión inicial es relativamente barata y el mantenimiento continuo es virtualmente "sin costo" durante su vida operacional. Gigabit Ethernet habilita esta estrategia. Gigabit Ethernet y prontamente 10Gigabit Ethernet proveerán todo el ancho de banda que es necesitado por varios tipos de aplicaciones, eliminando la necesidad de complejos esquemas de QoS en varios ambientes. Sin embargo algunas aplicaciones son a ráfagas por naturaleza y consumirán todo el ancho de banda disponible, en detrimento de otras aplicaciones que pueden tener requerimientos de tiempo-crítico. La solución es proporcionar un mecanismo de prioridad que asegure el ancho de banda, el espacio en el buffer, y que el poder del procesador sea asignado ha diferentes tipos de tráficos. Con Gigabit

sencillamente posible –aunque con diferentes mecanismos – para reunir los requisitos de voz, video y aplicaciones de datos.

En general, QoS en Ethernet es entregado a una capa alta del modelo OSI. Tramas son típicamente clasificadas individualmente por un esquema de filtro. Diferentes prioridades son asignadas a cada clase de tráfico, o explícitamente tratando de decir configuraciones de bits de prioridad en la cabecera de la trama, o implícitamente en el nivel de prioridad de la cola de espera (queue) o VLAN a la cual son asignados. Los recursos entonces son abastecidos en una forma preferentemente prioritizada (desigual o injusta) para que actúen las colas de espera. De esta manera, QoS es entregado al proporcionar diferente servicio a tráfico diferenciado a través de sus mecanismos de clasificación, ajustes de prioridad, la asignación de la cola priorizada, y servicio de prioritización de cola.

3.3.3 Servicios Diferenciados (DiffServ)

Uno de los principales mecanismos disponible para QoS en Ethernet es Servicios diferenciados (DiffServ). El grupo de trabajo del IETF para DiffServ lo propuso como un simple término para proporcionar servicios diferenciados escalables en redes IP. DiffServ redefine el precedente de IP/ El campo de tipo de servicio en el encabezado de IPv4 y el campo de Clase de tráfico en el encabezado de IPv6 como el nuevo campo DS (Ver Fig. 3.1). El campo DS de un paquete IP es entonces marcado con un patrón de bit específico, entonces el paquete recibirá el servicio diferenciado deseado (es decir, la prioridad deseada de envió),

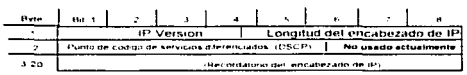


Fig. 3.1 Campo de diferenciación de servicios.

también conocida como el funcionamiento de por brinco (PHB per-hop behavior), en cada nodo de la red a lo largo del camino de la fuente al destino.

Para proporcionar un uso común de los posibles patrones de bit del DSCP, RFC 2474 y RFC 2475 definen la arquitectura, formato y uso general de estos bits dentro del campo DSCP.

Estas definiciones son requeridas en el orden de garantizar la consistencia de servicio esperado cuando un paquete cruza de un dominio administrativo de red a otro, o para interoperabilidad de multi-vendor. El grupo de trabajo también regularizó los funcionamientos de por-brinco específicos y siguientes, además patrones de bits recomendados (también conocidos como puntos de código o DSCPs) del campo del DS para cada PHB:

- Expedited Forwarding (envió acelerado) (EF-PHB), algunas veces descrito como servicio Premium, usa un DSCP de bit "101110". El EF-

- Expedited Forwarding (envió acelerado) (EF-PHB), algunas veces descrito como servicio Premium, usa un DSCP de bit "101110". El EF-PHB proporciona el servicio equivalente de una perdida baja, latencia baja, jitter bajo, ancho de banda asegurado para conexiones punto a punto (una línea arrendada virtual). Las tramas EF-PHB son asignadas a una cola de espera con prioridad alta donde la proporción de la llegada de tramas a un nodo se forma para siempre ser menos que la proporción de la salida configurada en ese nodo.
- Assured Forwarding (AF-PHB) -envió asegurado- utiliza 12 DSCPs para identificar cuatro clases de envío, cada uno con tres niveles de drop precedence (12 PHBs). Las tramas son asignadas por el usuario a diferentes clases y "drop precedence" dependiendo del grado deseado de entrega –pero no garantizada- asegurada. Cuando se asignan recursos (buffers y ancho de banda) son insuficientes para la demanda, tramas con alto drop precedence son descartadas primero. Si los recursos son aun restringidos, tramas con medio "precedence" son las proximas a descartar, y las tramas con bajo "precedence" son tiradas solo en las condiciones más extremas de falta de recursos.
- Un Valor por defecto recomendado de PHB con un DSCP de b"000000" (seis ceros) que iguala a los mejores servicios de hoy en día cuando ningún DS marcando explicito existe.

En esencia, DiffServ opera como sigue:

- Cada trama que entra a una red es analizada y clasificada para determinar el apropiado servicio deseado por la aplicación.
- Una vez clasificadas las tramas, son marcadas en el campo DS asignándoles un valor de DSCP para indicar el apropiado PHB. Dentro del core de la red, las tramas son enviadas de acuerdo a el PHB indicado.
- Análisis, clasificación, marcado, monitoreo, y operaciones de modelado necesitan llevarse a cabo solo por el host o por el nodo de límite de red. Los nodos que intervienen solo necesitan examinar la corta longitud del campo DS para determinar el apropiado PHB que se le dará a la trama. Esta arquitectura es la llave para la escalabilidad de DiffServ. En contraste, otros modelos tales como RSVP/Integrated Services son severamente limitados por la señalización, flujo de aplicación, y enviando el mantenimiento del estado a cada uno y cada uno de los nodos a lo largo del camino.
- Las políticas gobiernan como las tramas son marcadas y el tráfico condiciona la entrada a la red; estas también gobiernan la asignación de recursos al flujo de tráfico y como el tráfico es enviado dentro esas redes.

DiffServ permite nodos que no tienen la capacidad DS o incluso que si tienen DS para continuar usando la red en la misma forma y previo a esto usando el valor por defecto de PHB, el cual es el mejor para realizar envíos. Así, sin requerir el empleo de sistemas end-to-end. DiffServ proporciona un gran poder

a Gigabit Ethernet, aun simple y escalable, es decir que proporciona diferentes servicios de QoS para soportar varios tipos de tráfico de aplicaciones.

3.3.4 Servicios comunes de politica abierta (COPS Common Open Policy Services)

Para habilitar una política basada la capacidad de la gestión de redes, el protocolo de servicios comunes de política abierta (COPS) puede ser usado para complementar a los dispositivos que están habilitados para manejar a DiffServ. COPS proporciona una arquitectura y un protocolo de petición-respuesta para peticiones de control de admisión de comunicaciones, decisiones basadas, e información de la política entre un servidor de política de red y el conjunto de clientes a los que les da servicio. Los switches al ingresar a la red pueden actuar como clientes de COPS. Los clientes de COPS examinan las tramas cuando ellos entran a la red, se comunican con un servidor central de COPS para decidir si el tráfico debe admitirse a la red, y reforzar las políticas. Estas políticas incluyen cualquier trato a los envíos de QoS para que se apliquen durante el transporte. Una vez determinado, los switches Gigabit Ethernet que tienen habilitado DiffServ pueden marcar las tramas utilizando el patrón bit seleccionado por DSCP, aplicando el apropiado PHB, y enviando tramas al próximo nodo. EL próximo nodo necesita solamente examinar las marcas de DiffServ para aplicar el apropiado PHB. Así, las tramas son enviadas salto-por-salto a través del campus de Gigabit Ethernet con el QoS deseado.

3.4 Orientado a conexión versus No orientado a conexión

ATM es un protocolo orientado a conexión. Muchas de las empresas que cuentan con LANs son redes Ethernet no orientados a conexión, si son Ethernet estas pueden ser Fast Ethernet y Gigabit Ethernet.
Nota: Debido a la predominancia de Ethernet, simplifica grandemente la discusión a no referirse a la ficha comparativa de la Tecnología de Token-Ring; esto evita complicadas comparaciones con calificaciones para LANs Token-Ring y ELANs

Una red ATM puede ser usada como un backbone de alta velocidad para conectar LAN Switches Ethernet y estaciones terminales juntos. Sin embargo, una conexión-orientada ATM en un backbone requiere los protocolos del Forum ATM: LAN Emulation (LANE), esto para emular la operación de sin conexión que es legado de las LANs. En contraste con simples backbone Gigabit Ethernet, mucha de la complejidad de los backbones de ATM se debe de la necesidad de LANE.

3.4.1 ATM LAN Emulation v1

LANE versión 1 fue aprobado en Enero de 1995. Considerando que un backbone de Gigabit Ethernet es muy simple de implementar, cada LAN ATM emulada (ELAN) necesita varios componentes lógicos y protocolos que se agregan a la complejidad de ATM. Estos componentes son:

- Servidor(es) de configuración de LAN Emulation (LECS) para, entre otras cosas, proporcionar configuración de datos a un sistema terminal, y asignar estos a una ELAN (Aunque el mismo LECS puede servir a más de una ELAN).
- Solo un servidor de LAN Emulation (LES) por ELAN para resolver direcciones MAC de 6-byte en una LAN a direcciones de 20-byte en ATM y viceversa.
- Solamente un Broadcast y Unknown Server o Servidor de Difusión y desconocido (BUS) por ELAN para enviar tramas de Broadcast, tramas de Multicast y tramas de destino ya sea dirección LAN o ATM que aun es desconocida.
- Uno o más Clientes de LAN Emulation (LEC) para representar los sistemas terminales. Esto es más complicado si el sistema terminal es un LAN switch y se encuentra conectado a otro sistema terminal Ethernet, o si es ATM y esta conectado directamente a un sistema terminal. Un switch LAN requiere un proxy LEC, considerando que un sistema terminal conectado a ATM requiere un non-proxy LEC.

Colectivamente, el LECS, LES, y BUS son conocidos como servicios de LAN Emulation. Cada LEC (proxy o non-proxy) se comunica con los servicios de LAN Emulation utilizando diferentes conexiones de canales virtuales (VCCs) y protocolos LUNI (LAN Emulation User Network Interface). La figura 2 muestra los VCCs utilizados en LANE v1

Connection Name	Uni- or Bi-directional	Point-to-point or Point-to-multipoint	Used for communication between
Configuration Direct VCC	Bi-directional	Point-to-point	Between an LECS and an LEC
Control Direct VCC	Bi-directional	Point-to-point	Between an LEC and its LECS
Control Distribute VCC	Uni-directional	Point-to-multipoint	From an LEC to its LECS
Multicast Send VCC	Bi-directional	Point-to-point	Between a BUS and an LEC
Multicast Forward VCC	Uni-directional	Point-to-multipoint	From a BUS to its LECs
Data Direct VCC	Bi-directional	Point-to-point	Between an LEC and another LEC

Fig. 3.2 VCCs Utilizados en LANE V1

Algunos VCCs son obligatorios una vez establecidos, estos deben mantenerse si el LEC esta participando en la ELAN. Otros VCCs son opcionales- pueden o no establecerse y, si están establecidos, pueden o no soltarse o dejarse libres.

La desconexión imprevista de un VCC requerido puede activar el proceso del arreglo. En ciertas circunstancias, esto puede llevar a la inestabilidad en la red.

Los componentes más críticos de el servicio de LAN Emulation son el LES y el BUS, sin el cual una ELAN no puede funcionar. Porque cada ELAN puede solo servirse por un solo LES y un BUS, estos componentes necesitan ser apoyados o respaldados por otro LES y BUS para prevenir cualquier un punto de falla de comunicación entre posiblemente cientos o incluso miles de estaciones terminales "conectados" a una ELAN. Además, el solo LES o BUS representa un cuello de botella para el performance de la red.
Así, se ha vuelto necesario para los componentes de Servicio de Emulación de LAN que sean dobles por cuestiones de redundancia y para eliminar un punto de falla y tener un performance distribuido de la red.

3.4.2 ATM LAN Emulation v2

Para habilitar la comunicación entre los componentes redundantes y distribuidos del Servicio de Emulación LAN, también como otros perfeccionamientos funcionales, LANE v1 fue re-especificado como LANE v2; ahora comprende dos protocolos separados:

- LUNI: LAN Emulation User Network Interface, aprobado en julio de1997
- LNNI: LAN Emulation Network-Network Interface, aprobado en febrero de 1999.

LUNI, entre otros perfeccionamientos, agrego el Servidor Selectivo de Multicast (Selective Multicast Server, SMS), para proporcionar un medio mas eficaz de envió de tráfico de multicast, el cual fue previamente realizado por el BUS. SMS así descarga mucho del procesamiento de multicast al BUS, permitiendo que el BUS se enfoque más en el envió de tráfico de broadcast y también con el tráfico LAN con destino todavía a ser resuelto.
LNNI proporciona para el intercambio de configuración, estados, coordinación de control, y sincronización de bases de datos entre componentes redundantes y distribuidos del Servicio de LAN Emulation.

Sin embargo, cada mejora agrega nueva complejidad. Protocolos adicionales son requeridos y VCCs adicionales necesitan ser establecidos, mantenidos, y monitoreados para que exista comunicación entre los nuevos componentes del servicio de LAN Emulation y los LECs Por ejemplo, todos los LESs que sirven a una ELAN comunican los mensajes de control a nosotros a través de una malla (full mesh) de VCCs de control coordinado. Estos LESs deben también sincronizar sus bases de datos de direcciones LAN-ATM, usando el protocolo de sincronización de servidor de cache (Server Cache Synchronization Protocol, SCSP-RFC 2334), a través del VCC de sincronización de cache. Similarmente todos los BUS que sirven a una ELAN deben conectarse totalmente por una malla de VCCs de envió de Multicast utilizada para enviar datos.

El tráfico de Unicast de un LEC transmisor es inicialmente enviado a un LEC receptor vía el BUS. Cuando un Data Direct VCC (ver figura 2) ha sido establecido entre dos LECs, el tráfico de Unicast es enviado por el camino

directo. Durante la transición desde el inicio hasta el camino directo, es posible que las tramas sean entregadas fuera de orden. Para prevenir esta posibilidad LANE requiere un LEC para implementar el protocolo Flush, o para el LEC enviante retrasar la transmisión a un costo de latencia.

El envió de tráfico de multicast desde un LEC depende de la disponibilidad de un SMS:

- Si un SMS no esta disponible, el LEC establece el "Default Multicast Send VCC" hacia el BUS que, a su vez, agregará al LEC como una hoja a su "Default Multicast Forward VCC". El Bus es entonces usado para el envio de tráfico de Multicast.
- Si un SMS esta disponible, el LEC puede establecer, en adición al "Default Multicast Send VCC" hacia el BUS, un "Selective Multicast Send VCC" hacia el SMS. En este caso, el BUS agregará al LEC como una hoja a su "Default Multicast Forward VCC" y el SMS agregará al LEC como una hoja a su "Selective Multicast Forward VCC". El BUS entonces es usado inicialmente para enviar tráfico de multicast hasta que el destinatario de multicast es resuelta a una dirección ATM, y también al mismo tiempo se esta utilizando el SMS. El SMS también sincroniza su base de datos de direcciones multicast LAN-ATM con su LES utilizando SCSP a través de "Cache Synchronization VCCs".

La figura 3.3 muestra las conexiones adicionales requeridas por LANE v2.

LECS Synchronization VCC	Bi-directional	Point-to-point	Between LE
Configuration Direct VCC	Bi-directional	Point-to-point	Between an LEC and an LECS
Control Coordinate VCC	Bi-directional	Point-to-point	Between LE
Cache Synchronization VCC	Bi-directional	Point-to-point	Between an LE
Default Multicast Send VCC	Bi-directional	Point-to-point	Between a BUS and an LE
Default Multicast Forward VCC	Uni-directional	Point-to-multipoint	From a BUS to its LECs and other BUS
Selective Multicast Send VCC	Bi-directional	Point-to-point	Between an SMS and an LEC
Selective Multicast Forward VCC	Uni-directional	Point-to-multipoint	From an SMS to its LEC

Fig. 3.3 Conexiones adicionales utilizadas por LANE V2

Esta multitud de controles y conexiones coordinadas, también como el intercambio de tramas de control, consume memoria, poder de procesamiento y ancho de banda, simplemente para que un "Data Direct VCC" pueda finalmente establecerse por comunicaciones persistentes entre dos sistemas terminales. La complejidad puede verse en la figura 3.4.

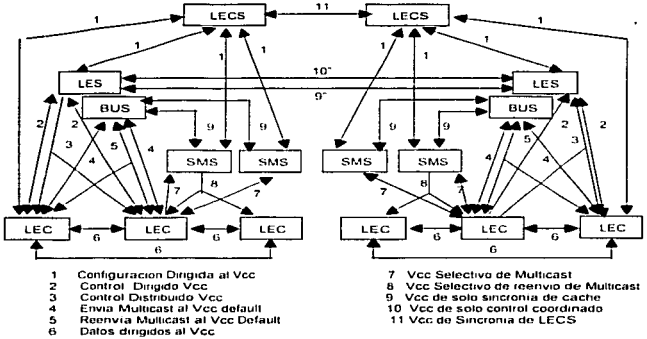


Fig. 3.4 Complejidad de ATM LANE

3.4.3 Encapsulamiento AAL-5

Además de la complejidad de conexiones y protocolos, los datos llevados sobre LANE utilizan un encapsulamiento llamado AAL-5(ATM Adaptation Layer-5) el cual agrega overhead a las tramas de Ethernet. La trama de Ethernet es despojada de su Secuencia de chequeo de trama (FCS Frame Check Sequence); los campos restantes son copiados a la porción de payload o carga útil del CPCS-PDU (CPCS: subcapa de convergencia de la parte común, PDU: Unidad de Datos de Protocolo), y un encabezado de 2-bytes de LANE (LEH, LANE header) se agrega en el frente, y con 8-bytes de trailer al final. Arriba de 47 bytes de almohadilla se pueden agregar, para producir un CPCS-PDU que es múltiplo de 48, el tamaño de una celda de ATM de carga útil.

El CPCS-PDU también tiene que ser segmentado en células de ATM de 53-bytes antes de ser transmitidas hacia la red. En el extremo que recibe, las células de ATM de 53-bytes tienen que ser desencapsuladas y reensambladas en la trama de Ethernet original.

La figura 3.5 nos muestra el CPCS-PDU que se utiliza para transportar tramas de Ethernet sobre LANE

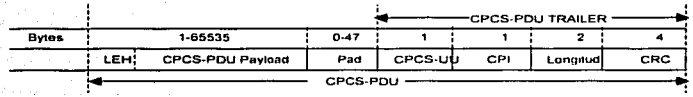


Fig. 3.5 CPCS-PDU para transportar tramas de Ethernet sobre LANE

3.4.4 Gigabit Ethernet LAN

En contraste, un backbone LAN Gigabit Ethernet no tiene la complejidad y el overhead de funciones de control, encapsulamineto de datos y desencapsulamiento, segmentación y reensamble, además del control y conexiones de datos requeridos por un backbone ATM.

Como originalmente se intento, al menos en un despliegue inicial en un ambiente LAN, Gigabit Ethernet utiliza transmisiones full-duplex entre switches, o entre un switch y un servidor en una "granja" de servidores- en otras palabras en el backbone. El full-duplex en Gigabit Ethernet es mucho más simple y no sufre de las complejidades y deficiencias de utilizar half duplex en Gigabit Ethernet, el cual utiliza el protocolo CSMA/CD, extensión de portadora y bursting de trama o estallido de trama.

3.4.5 Formato de Trama (Full-Duplex)

Full-Duplex Gigabit Ethernet utiliza el mismo formato de trama de Ethernet y de Fast Ethernet, con una minima longitud de trama de 64 bytes y un máximo de 1518 bytes (incluyendo el FCS pero excluyendo el preámbulo /SFD. Si la porción de datos es menos de 46 bytes, bytes de almohadilla son agregados para producir una trama de tamaño mínimo de 64 bytes.

La figura 3.6 muestra el mismo formato para Ethernet, Fast Ethernet y full-duplex Gigabit Ethernet que habilita la integración transparente de backbones Gigabit Ethernet en Campus con escritorios Ethernet y Fast Ethernet además de los servidores que se interconectan.

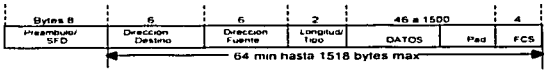


Fig. 3.6 Formato de trama Gigabit Ethernet Full Duplex.

3.4.6 Formato de trama (Half-Duplex)

Debido al gran aumento de velocidad de propagación y la necesidad de soportar distancias de red prácticas, half- duplex en Gigabit Ethernet requiere el uso de portadores de extensión. El portador de extensión proporciona una longitud de transmisión mínima de 512 bytes. Esto permite que las colisiones sean detectadas sin incrementar la mínima longitud de trama que es de 64bytes; así, no se requieren de cambios en capas más altas de software, tales como controladores de tarjetas de red y stacks de protocolos.

Con la transmisión half-duplex, si la porción de datos es menos de 46 bytes, se agregan bytes de almohadilla en el campo exclusivo para esto; esta acción se realiza para incrementar el mínimo de trama a 64 bytes (no-extendido). Además, se agregan bytes en el campo de extensión de portadora (Carrier Extensión field) para que exista un mínimo de 512 bytes para que la transmisión sea generada. Por ejemplo, con 46 bytes de datos, no se necesitan bytes en el campo de almohadilla (pad field), y 448 bytes son agregados al campo de extensión de portadora. Por otro lado con 494 o más (arriba de1500) bytes de datos, no se necesita poner bytes en los campos de almohadilla o en el de extensión de portadora.

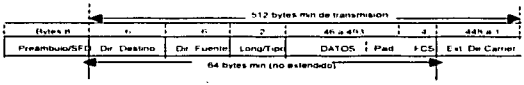


Figura 3.7 Formato de trama Gigabit Ethernet Half Duplex.

3.4.7 Eficiencia "Goodput"

Con Gigabit Ethernet en full-duplex el buen rendimiento ("goodput" derivado de good throughput") en un ambiente predominante de tramas con 64-bytes de tamaño, donde ninguna portadora de extensión se necesita, se calcula como sigue (donde SFD=comienzo del delimitador de trama, y IFG=espacio entre tramas)

$$\frac{\text{64 bytes (frame)}}{\text{(64 bytes (frame) + 8 bytes (SFD)+ 12 bytes (IFG))}} = \text{76 \% approx.}$$

Esta eficiencia o "goodput" se traduce a una proporción de envío de 1.488 millones de paquetes por segundo (Mpps), conocido como la proporción de "wire speed" o velocidad de alambre

Con extensión de portadora, el resultado del goodput es mucho muy reducido (donde CE es Extensión de portadora):

$$\frac{\text{64 bytes (frame)}}{\text{(512 bytes (frame con CE) + 8 bytes (SFD)+ 12 bytes (IFG))}} = \text{12 \% approx.}$$

Comparando ATM y Gigabit Ethernet, este 12 % es a veces citado como evidencia de ineficiencia de Gigabit Ethernet. Sin Embargo este cálculo solo es aplicable a Gigabit Ethernet en half-duplex (como opuesto a full-duplex). En el backbone, en las conexiones de "granjas" de servidores, y en la vasta mayoría (si no es que en todas) de Gigabit Ethernet que esta instalado, es en modo full-duplex.

3.4.8 Conversión de tramas Ethernet a Células de ATM LANE

Como se menciono previamente, al utilizar ATM LAN Emulation como el backbone de un campus y con escritorios Ethernet, se requiere encapsulamiento AAL-5, una subsecuente segmentación, y un reensamble

La figura 3.8 nos muestra una trama de Ethernet de su máximo tamaño, 1518 bytes, convertida en CPCS-PDU y segmentado en 32 células ATM de 53 bytes, utilizando AAL-5; este se traduce a una eficiencia "goodput" de:

$$\frac{\text{1514 bytes (frame sin FCS)}}{\text{(32 Celdas ATM X 53 bytes por celda ATM)}} = \text{89 \% approx}$$

Para una trama de Ethernet de tamaño mínimo de 64 bytes, se requerirán dos células de ATM, esto se traduce en una eficiencia "goodput" de:

$$\frac{\text{60 bytes (frame sin FCS)}}{\text{(2 Celdas ATM X 53 bytes por celda ATM)}} = \text{57 \% approx}$$

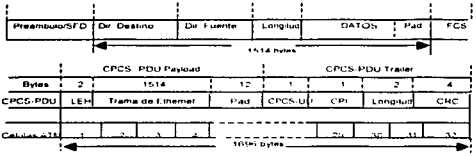


Fig. 3.8 Conversión de tramas a celdas.

3.4.9 Estallido de Trama "Frame Bursting"

La extensión de portadora es un encabezado, especialmente si el tamaño del tráfico predominante son tramas cortas. Para mejorar la eficiencia "goodput", Gigabit Ethernet en su modalidad de half-duplex permite estallido de trama (frame bursting). Este estallido de trama permite a una estación terminal enviar múltiples tramas en un solo acceso (es decir, sin competir por canal de acceso por cada trama) arriba del parámetro "burstLength" (longitud del estallido). Si una trama se esta transmitiendo cuando el umbral del "Burst length "se esta excediendo, el transmisor esta permitido para completar la transmisión. Así, la máxima duración de estallido de trama es de 9710 bytes, esto es que el "Burst length" tiene 8192 bytes, y si le sumamos el tamaño máximo de trama, que es de 1518 bytes nos resulta los 9710 bytes arriba mencionados. Solamente la primera trama se puede extender si se requiere. Cada trama esta separada por un campo de intertrama previo de 96 bits. Ambos el transmisor y el receptor deben de ser capaces de procesar el estallido de trama.

Fig 3.9 Estallido de trama

3.4.10 Protocolo CSMA/CD

Gigabit Ethernet en su modalidad full-duplex no utiliza o no usa el protocolo CSMA/CD. Puesto que es dedicado, simultáneo, además de que separa y recibe canales, esto es mucho más simple sin la necesidad de utilizar detección de portadora, detección de colisión, backoff (Backoff en una red 802.3 es el retardo entre una colisión y cuando la estación retransmite. Si intentos subsecuentes también resultan en colisiones la estación retransmitirá poniendo en marcha este algoritmo de backoff, el cual intentará transmitir

nuevamente, pero en otro tiempo escogido al azar y el cual se incrementa exponencialmente) y retry, extensión de portadora, y estallido de portadora.

3.5 Control de flujo y administración de congestión

En ambos ATM o Gigabit Ethernet, el control de flujo y la administración de congestión son necesarios para asegurar que los elementos de la red, individualmente y colectivamente, pueda resolver los objetivos de QoS requeridos por aplicaciones que utilizan esa red.

Una congestión continua en un switch, tanto ATM o Gigabit Ethernet, eventualmente e resultado en tramas será que sean descartadas. Varias técnicas son empleadas para minimizar o prevenir sobre flujos en buffer, especialmente bajo condiciones de sobrecarga transitorias. La diferencia entre Gigabit Ethernet y ATM esta e la disponibilidad, alcance y complejidad (funcionalidad y granularidad) de esas técnicas.

3.5.1 Administración de congestión y tráfico de ATM

En una red ATM, los medios empleados para administrar el flujo tráfico y congestión están basados en el contrato de tráfico: el servicio de categoría de ATM y la unificación de parámetros en listas de datos de tráfico para que se pueda establecer una conexión.

Estos medios pueden incluir:

Control de Admisión de conexión (CAC)
Aceptando o rechazando conexiones siendo solicitada en la etapa de la disponibilidad de los recursos de la red (este es el primer punto del control y considera las conexiones ya establecidas).

Monitoreo de tráfico: El control y monitoreo de la afluencia de células de células que entran a la red con conexiones ya establecidas, y marcando el tráfico hacia afuera del perfil para posibles descartes utilizando "Usage Parameter Control" (UCP, Control de parámetros de uso) y el "Generic Cell Rate Algorithm (GCRA, Algoritmo de tasa de célula genérica).
Backpressure: aplicándose sobre la fuente para disminuir la tasa de transmisión de células cuando la congestión aparece muy probable o cuando es inminente.
Notificación de congestión: Notificando el origen y los nodos que intervienen de la congestión actual o inminente fijando el bit de indicación de congestión de envió explicito (EFCI) en el header de la célula (Indicador de tipo de carga) o utilizando los bits de tasa relativa (RR, relative rate) o el de tasa explicita (ER, Explicit Rate) en las células de Administración de Recurso (RM, Resource Management) para proporcionarla regeneración en las direcciones de envió y de regreso. Para poder tomar la acción remediadora.
Descarte de célula: empleando varias estrategias de descarte para evitar o desahogar congestiones:
-Descarte de células selectivas: tirando células que no son dóciles con el contrato del tráfico o tienen su prioridad de pérdidas de células (CLP Cell

Loss Priority) implementado por un bit de marca para posibles descarte si se necesita.
- Descarte de paquetes temprana (EDP, Early Packet Discard): Tirando todas las células pertenecientes a una trama que esta en estado de espera, pero por el cual la transmisión no ha comenzado.
- Descarte Parcial de Paquete (PPD, Partial Packet Discard): tirando todas las células pertenecientes a una trama que esta siendo transmitida (una acción más drástica que EDP)
-Detección Aleatoria Temprana (RED, Random Early Detection): tirando todas las células de tramas que han sido seleccionadas aleatoriamente (de diferentes fuentes) cuando el algoritmo de llegada de tráfico indica una inminente congestión (asi evitando la congestión), y previniendo ondas de re-transmisión sincronizada que precipitan al colapso de la congestión. Un futuro perfeccionamiento es ofrecido al utilizar WRED (Weighted RED).
- Perfilado de tráfico: modificando el flujo de las células que salen de un switch (para entrar o transitar una red) para asegurar conformidad con los perfiles contratados y servicios. El perfilado puede incluir la reducción del "Peak Cell Rate", limitando la duración del estallido de tráfico, y separando células más uniformemente para reducir la variación de retraso de célula (Cell Delay Variation).

3.5.2 Control de flujo en Gigabit Ethernet.

Para operar en half-duplex, Gigabit Ethernet utiliza el protocolo CSMA/CD para proporcionar control de flujo implícito por "backpressuring", el remitente puede transmitir en dos simples formas:
Forzando colisiones con el tráfico entrante, el cual obliga al remitente que retroceda y reintente transmitir como un resultado de la colisión, esto de acuerdo al protocolo CSMA/CD.
Sosteniendo la detección de portadora para proporcionar una señal de "canal ocupado" el cual previene al transmisor del acceso al medio para poder transmitir, una vez más de acuerdo al protocolo CSMA/CD.
Con la operación en full-duplex, Gigabit Ethernet utiliza control flujo explicito para contener al transmisor. El grupo de trabajo del IEEE 802.3x definió una arquitectura de control de MAC, el cual agrega una sub-capa de control de MAC a la sub-capa de MAC arriba mencionada, y utiliza tramas de control MAC para poder realizar el flujo de control. Hasta la fecha, solamente un control de trama MAC has sido definido; esto es para la operación de la PAUSA.

Un switch o una estación terminal pueden enviar una trama de PAUSA para detener al remitente de una transmisión de trama de datos por una duración de tiempo especifico, el remitente puede empezar de nuevo la transmisión. El remitente también puede continuar con la transmisión cuando recibe una trama de PAUSA con un tiempo especificado de cero, indicando que el periodo de espera ha sido cancelado. Por otro lado, el periodo de espera puede extenderse si el remitente recibe una trama de PAUSA con un periodo más largo que el que recibió previamente.

Utilizando este simple mecanismo de "inicio-parada", Gigabit Ethernet previene descarte de tramas cuando los buffer (buffer: espacio de memoria para

almacenamiento temporal de datos) de entrada están temporalmente agotados por sobrecargas pasajeras. Esto es efectivo solamente cuando se usa un enlace sencillo de full-duplex entre dos switches, o entre un switch y una estación terminal (servidor).
Debido a su simplicidad, la función de PAUSA no proporciona control de flujo a través de múltiples enlaces, de "end-to-end" o a través de de los switches que intervienen. Esto también requiere que ambos extremos de un enlace (el transmisor y el receptor) sean capaces de manejar control de MAC.

3.6 Escalabilidad de ancho de banda.

Avances en la tecnología de cómputo ha impulsado la explosión de aplicaciones visualmente y auricularmente para el comercio electrónico, tanto en Internet como en Intranet o extranet. Estas aplicaciones requieren de incrementos exponenciales en anchos de banda. Como un negocio crece, incrementos en le ancho de banda son también requeridos para satisfacer el mayor número de usuarios sin degradar el rendimiento. Por consiguiente, la escalabilidad en el ancho de banda en la infraestructura de red es crítica para soportar el incremento o cuanto se incrementa la capacidad del ancho de banda, el cual es frecuentemente requerido por varios negocios.
ATM y Gigabit Ethernet ambos proporcionan escalabilidad en ancho de banda. Mientras que la escalabilidad en el ancho de banda de ATM es más granular y se extiende desde los escritorios y sobre la MAN/WAN. Gigabit Ethernet ha enfocado su escalabilidad en el establecimiento de una red del campus desde el escritorio hacia el lado de la MAN/WAN.
De esta manera, Gigabit Ethernet proporciona saltos fijos en un ancho de banda de 10Mbpsa través de 100Mbps, 1000Mbps (1Gbps), y hasta 10000 Mbps (10Gbps) sin un salto correspondiente fijo en costo.

3.6.1 Ancho de banda en ATM

ATM es escalable desde 1.544Mbps hasta 2.4 Gbps y mas altas velocidades. Aprobado por el Forum de ATM las especificaciones para la capa física incluye los siguientes anchos de banda:
1.544 Mbps DS1
2.048 Mbps E1
25.6 Mbps sobre cable de par trenzado blindado y no blindado (el ancho de banda que fue conceptualizado originalmente para los escritorios de ATM)
34.368 Mbps E3
44.736 Mbps DS3
100 Mbps sobre cableado de fibra multimodo
155.52 Mbps SONET/SDH sobre cableado de fibra multimodo y monomodo
622.08 Mbps SONETH/SHH sobre cableado de fibra multimodo y monomodo
622.08 Mbps y 2.4 Gbps basados en células en capa física (sin cualquier estructura de trama)

3.6.2 Multiplexaje Inverso sobre ATM.

Además, el estándar del Forum de Multiplexaje Inverso sobre ATM (IMA, Inverse Multiplexing) ATM permite varias velocidades bajas como DS1/E1 de enlaces físicos para ser agrupados junto con un enlace lógico de una velocidad mayor, sobre la cual las células de ATM son individualmente multiplexadas. El flujo original de células es recuperado en una secuencia correcta de múltiples enlaces físicos al recibir el final. Pérdida y recuperación de enlaces individuales en un grupo IMA son transparentes para los usuarios. Esta característica permite a los usuarios a:
Interconectar redes de campus ATM sobre la WAN, donde las facilidades de la WAN ATM no están disponibles por utilizar las facilidades existentes de los DS1/E1
Subscripciones incrementales a mas enlaces físicos DS1/E1 como se necesite.
Protección contra fallas de enlaces simples cuando se interconectan redes de campus ATM a través de una WAN
Utilización de enlaces múltiples DS1/E1 que son típicamente de costo más bajo que un solo enlace ATM para WAN como un DS3/E3 (o de velocidad más alta) para una operación normal o como enlaces de respaldo.

3.6.3 Ancho de banda en Gigabit Ethernet

Ethernet es escalable desde el tradicional Ethernet a 10Mbps, pasando por Fast Ethernet a 100 Mbps, y Gigabit Ethernet a 1000 Mbps. Ahora que los estándares de Gigabit Ethernet han sido terminados, el próximo paso evolucionario es 10 Gbps Ethernet. El grupo de estudio del IEEE para altas velocidades (IEEE P802.3) ha sido creado para trabajar sobre 10Gbps Ethernet, con la petición de la autorización de proyecto y la formación de un grupo de trabajo apuntado en noviembre de 1999.

Escalabilidad en el ancho de banda es posible también a través de "link aggregation" (Esto es agrupando múltiples enlaces de Gigabit Ethernet para proporcionar un mayor ancho de banda y elasticidad. El trabajo en esta área de estandarización esta siendo desarrollado por la fuerza de trabajo del IEEE 802.3ad de "link aggregation"

3.7 Escalabilidad de Distancia

La escalabilidad de distancia es importante debido a la necesidad de extender redes a través de campuses dispersos, dentro de largos edificios, mientras se pueda utilizar el existente cable de cobre UTP-5 y cableado común de fibra multimodo y monomodo, y sin la necesidad de equipo adicional tales como repetidores, "extenders", y amplificadores.

Ambos ATM y Gigabit Ethernet (IEEE 802.3ab) pueden operar fácilmente dentro del límite de 100 metros desde algún armario de telecomunicaciones donde se desprende de algún switch hasta algún escritorio utilizando cableado de cobre UTP-5. Distancias más largas son típicamente cubiertas utilizando cableado fibra multimodo (50/125 o 62.5/125 µm) o monomodo (9-10/125 µm).

3.7.1 Distancias en Ethernet.

La figura 3.10 muestra el máximo de distancia soportado por Ethernet y Fast Ethernet utilizando varios medios.

	Ethernet 10Base-T	Ethernet 10Base-FL	Ethernet 100Base-TX	Ethernet 100Base-FX
IEEE Standard	802.3	802.3	802.3u	802.3u
Data Rate	10Mbps	10Mbps	100Mbps	100Mbps
Distancia en Fibra Multimodo	N/A	2km	N/A	412 m (half duplex) 2 km (full duplex)
Distancia en fibra Monomodo	N/A	25 km	N/A	20 km
Distancia cable UTP CAT 5	100m	N/A	100 m	N/A
Distancia coaxial/STP	500 m	N/A	100 m	N/A

Fig. 3.10 Distancias en ethernet.

3.7.1.1Gigabit Ethernet IEEE 802.3z

-Cableado de fibra

El estándar del IEEE 802.3u-1995 (Fast Ethernet) expandió la velocidad de operación de las redes CSMA/CD a 100 Mbps sobre ambos medios, ya sea cableado de cobre o de fibra.

El grupo de trabajo para el estándar del IEEE P802.3z Gigabit Ethernet fue formado en Julio de1996 para desarrollar el estándar de Gigabit Ethernet. Este trabajo fue completado en julio de 1998 cuando la barra de estándares del IEEE aprobó el estándar IEEE 802.z-1998.

El estándar IEEE 802.3z especifica la operación de Gigabit Ethernet sobre cableado de fibra multimodo monomodo existente. Este soporta también puentes cortos de cobre (hasta 25 metros) para interconectar switches, routers, u otros equipos (servidores) en un cuarto sencillo de cómputo, o armario de cableado. Colectivamente, las tres designaciones -1000BASE-SX, 1000BASE-LX y 1000BASE-CX- se refieren como 1000BASE-X.

La figura 3.11 muestra las máximas distancias soportadas por Gigabit Ethernet, utilizando varios medios.
1000BASE-X Gigabit Ethernet tiene la capacidad de auto-negociación para operar en half- y full- duplex. Para operar en full-duplex, la auto-negociación del flujo de control incluye la dirección y la simetría de la operación – simétrica y asimétrica.

	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T
IEEE Standard	802.3z	802.3z	802.3z	802.3ab
Data Rate	1000 Mbps	1000 Mbps	1000 Mbps	1000 Mbps
Longitud de onda (Nominal)	850 nm (shortwave)	1300 nm (longwave)	N/A	N/A
Distancia Fibra Multimodo (50 (m))	525 m	550 m	N/A	N/A
Distancia en fibra multimodo (62.5 (m))	260 m	550 m	N/A	N/A
Distancia en fibra monomodo (10(m))	N/A	3 km	N/A	N/A
Distancia UTP-5 100 ohms	N/A	N/A	N/A	100 m
Distancia STP 150 ohms	N/A	N/A	25 m	N/A
Número de pares de Alambre/Fibra	2 fibras	2 fibras	2 pares	4 pares
Tipo de Conector	Duplex SC	Duplex SC	2 canales de Fibra o DB-9	RJ-45

Fig. 3.11 Distancias soportadas por GigabitEthernet

3.7.1.2 IEEE 802.3ab Gigabit Ethernet

Cableado de cobre

Para Gigabit Ethernet sobre cableado de cobre, un grupo de trabajo del IEEE, empezó a desarrollar una especificación en 1997. Una especificación de diseño preliminar muy estable, con cambios no muy significativos, ha estado disponible desde julio de 1998. Esta especificación, conocida como IEEE 802.3ab, fue aprobada (en Junio de 1999) como un estándar del IEEE por la barra de estándares del IEEE.
El estándar IEEE 802.3ab especifica la operación de Gigabit Ethernet sobre distancias arriba de 100 metros utilizando cableado de par trenzado de cobre no blindado balanceado categoría 5 de 4 pares de 100 ohms. Este estándar es también conocido como la especificación 1000BASE-T: la cual

permite el despliegue de Gigabit Ethernet en los armarios de cableado, al igual que si es necesitado en los escritorios, sin ningún cambio en el cableado de cobre UTP-5 que esta instalado en varios edificios de hoy en día.

3.8 "Trunking" y "Link Aggregation"

El "trunking" proporciona conectividad de switch a switch para ATM y Gigabit Ethernet. "Link Aggregation" permite múltiples enlaces paralelos entre switches, o entre un switch y un servidor, para proporcionar mayor elasticidad y ancho de banda. Mientras la conectividad de switch a switch en ATM esta bien definida a través de las especificaciones NNI y el PNNI, varios protocolos específicos de vendedores son usados para Gigabit Ethernet, con estándares basados en conectividad para ser proporcionados por el estándar IEEE 802.3ad Link aggregation.

3.8.1 ATM PNNI

El trunking en ATM es proporcionado a través de NNI (Network Node Interface o Network to NEtwork Interface) utilizando protocolos Private NNI v1.0 (PNNI), una especificación del Forum ATM aprobada en Marzo de 1996.

Para proporcionar elasticidad, distribución de carga y balanceo, escalabilidad en ancho de banda, múltiples enlaces PNNI pueden ser instalados entre un par de switches ATM. Dependiendo de la implementación, estos enlaces paralelos pueden ser tratados por los procedimientos del CAC (Connection Admisión Control) como un solo enlace lógico agregado. Los enlaces individuales dentro de un conjunto de enlaces paralelos pueden ser cualquier combinación de velocidades soportadas por ATM. Cuando más ancho de banda se necesita, más enlaces PNNI pueden ser agregados entre switches como requisito sin la preocupación de que se puedan formar "loops" en el camino del tráfico.

Al utilizar una fuente de ruteo para establecer un camino (VCC) entre cualquier sistema terminal fuente y uno de destino, PNNI automáticamente elimina la formación de "loops". El camino end-to-end, es computado al ingresar al switch ATM usando los procedimientos de control de admisión de conexión genérica (GCAC, Generic Connection Admisión Control), esto esta especificado en una lista de nodos de ATM conocida como lista de tránsito designado (DTL, Designated Transit List).

El cómputo o el cálculo basado en los parámetros predeterminados tendrá como resultado el camino más corto que reúne los requisitos, aunque la preferencia puede ser dada a ciertos caminos al asignar pesos administrativos bajos hacia enlaces preferidos. Esta DTL es entonces validada por procedimientos de CAC locales a cada uno de los nodos ATM que se encuentran en la lista. Si un nodo intermedio encuentra que el camino es inválido, puede ser como un resultado de la topología o que un estado de enlace haya cambiado en ese preciso momento, ese nodo es capaz entonces

de automáticamente moverse a la lista de regreso para ingresar nuevamente al switch y recalcular un nuevo camino. Un switch ATM puede ejecutar cálculos de caminos como una tarea en segundo plano después de que las llamadas son recibidas (para reducir la latencia durante las llamadas son establecidas), o cuando una petición de llamada a sido recibida (para un camino de tiempo real optimizado al costo de algún retraso de establecimiento de llamada), o par ambos (para ciertas categorías de QoS), dependiendo de la configuración del usuario.

PNNI también proporciona cumplimiento de escalabilidad cuando se rutea el tráfico a través de una red ATM, utilizando la estructura jerárquica de las direcciones de ATM. Un sistema terminal individual ATM en un grupo par PNNI puede ser alcanzado utilizando la dirección sumariada para ese grupo par, siendo similar a utilizar la porción del identificador de la red y de la subred de una dirección IP. Un nodo cuya dirección no corresponde a la dirección sumariada (la dirección que no corresponde se conoce como dirección extraña o como foreign address) puede ser fijada explícitamente para que sea alcanzada y anunciada.

Un grupo líder par (PGL) puede representar los nodos en el grupo par en una capa más alta. Estos PGLs son grupos de nodos lógicos (LGNs) que forman grupos pares de más alto nivel, el cual permite incluso direcciones sumariadas más cartas. Estos grupos pares de mayor nivel pueden ser representados en grupos incluso mayores, así formando una jerarquía. Al utilizar esta jerarquía multi-nivel de ruteo, menos direcciones, topología, e información de estado de enlace necesita ser anunciada a través de una red ATM, permitiendo escalabilidad así como crezca el número de nodos.

Sin embargo, estas ricas funcionalidades vienen con un precio. PNNI requiere memoria, recursos de procesamiento, y ancho de banda proveniente de los switches ATM para mantener el estado de la información, intercambio del estado de los enlaces y de topología, además del cálculo de caminos para la información, PNNI también resulta en una mayor complejidad en diseño de hardware, algoritmos de software, configuración de switches, despliegue y soporte operacional, y finalmente costos mucho más altos.

3.8.2 Enlaces de subida "uplinks" UNI ATM versus tubos de subida "risers" NNI

PNNI proporciona varios beneficios con atención hacia la escalabilidad y elasticidad cuando se conectan switches ATM en el backbone del campus. Si embargo, estas ventajas no están disponibles en la mayoría de las instalaciones de ATM donde los switches LAN en los clset's de cableado están conectados a los switches del backbone utilizando "uplinks" UNI de ATM. En tales conexiones, las estaciones terminales adjuntas a los switches LAN están asociadas, directa o indirectamente (a través de VLANs), con proxys de LECs específicos localizados en los "uplinks". Una estación terminal no puede ser asociada con más de un proxy LEC activo en "uplinks" separados a cualquier hora. Sin embargo caminos no redundantes están disponibles si el proxy LEC (refiriéndonos al uplink o el camino del uplink) que

representa a la estación terminal debe fallar. Mientras es posible el tener un uplink activo y otro en "standby", conectado al backbone por una vía diferente y listo para tomar el control en caso de falla, muy pocas instalaciones de ATM han implementado este diseño por razones de costo, complejidad, y falta de esta capacidad desde el proveedor del equipo.

3.8.3 Link aggregation en Gigabit Ethernet

Con Gigabit Ethernet, enlaces múltiples físicos pueden estar instalados entre dos switches, o entre un switch y un servidor, para proporcionar mayor ancho de banda y elasticidad. Típicamente, el Protocolo Spanning Tree (STP, IEEE 802.1d) es utilizado para prevenir loops o bucles que se puedan formar entre enlaces paralelos, al bloquear ciertos puertos y reenviar sobre otros que solo tienen un camino entre cualquier de fuente destino y estación terminal. De esta forma, STP incurre en alguna pena de ejecución cuando converge una nueva estructura de spanning tree después que una topología de red cambia.

Aunque la mayoría de los switches son plug-and-play con parámetros predeterminados para el STP, configuraciones erróneas de estos parámetros pueden conducir a que se formen bucles, lo cual es difícil de resolver. Además, al bloquear ciertos puertos, STP permitirá que un solo enlace de varios en paralelo entre un par de switches para llevar el tráfico. Por lo tanto, escalabilidad de ancho de banda entre switches no puede ser incrementada al agregar mas enlaces paralelos aun cuando se requiera, aunque la elasticidad se mejora así.

Para superar las deficiencias de STP, varias características provenientes de especificaciones de vendedores son ofrecidas para incrementar la elasticidad, distribución de carga y balanceo, además de escalabilidad en ancho de banda, esto para enlaces paralelos entre switches Gigabit Ethernet.

3.8.4 Multi-Link Trunking

Permite agrupar varias conexiones físicas entre switches y que sean vistas o agrupadas como un solo enlace lógico, el cual tiene mayor elasticidad y ancho de banda que varias conexiones individuales.

Cada grupo Multi- Link Trunking (MLT) puede estar compuesto ya sea de interfaces físicas Ethernet, Fast Ethernet o Gigabit Ethernet, todos los enlaces dentro de un grupo deben estar en el mismo tipo de medio (cobre o fibra), tener la misma velocidad y estar configurado en half o full-duplex, además de pertenecer al mismo grupo de spanning tree, aunque no necesitan estar en la mismo módulo interface dentro de un switch. La carga es automáticamente balanceada a través de enlaces MLT, basados en una dirección MAC fuente y un destino (tráfico puenteado), una dirección IP fuente y una destino (tráfico ruteado).

3.8.5 Link Aggregation IEEE P802.3ad

IEEE P802.3ad Link Aggregation es una importante tecnología full-duplex, punto a punto para infraestructura de core LAN y proporciona varios beneficios:

- Capacidad para mayor ancho de banda, permitiendo enlaces paralelos entre dos switches, o entre un servidor y un switch, para que sean agregados juntos como una solo conexión lógica con capacidad de multi-Gigabit Ethernet (si es necesario); el tráfico es automáticamente distribuido y balanceado sobre esta conexión para un alto rendimiento.
- Incrementa la escalabilidad de ancho de banda, permitiendo más enlaces para ser agregados entre dos switches, o un switch y un servidor, solamente cuando se necesita un mayo rendimiento, desde una inversión mínima de de hardware , y con una mínima interrupción de la red.
- Mayor elasticidad y tolerancia de fallo, donde el tráfico es automáticamente reasignado para mantener enlaces operativos, así se mantiene la comunicación si enlaces individuales entre dos switches, o un switch y un servidor, falla.
- Medio de simple y flexible migración, donde switches Ethernet y Fast Ethernet en el borde de una LAN pueden tener enlaces adicionales múltiples de baja velocidad para proporcionar transporte con un mayor ancho de banda dentro del core en Gigabit Ethernet.

Describimos en pocas palabras como sigue al estándar IEEE P802.3ad Link aggregation (el cual puede cambiar todavía) Una conexión física entre dos switches, o un switch y un servidor, es conocido como un segmento de enlace. Enlaces individuales de segmento de mismo tipo de medio y velocidad pueden formar un LAG (Link Aggregation Group), con un segmento de enlace perteneciente unicamente a un solo LAG en cualquier momento. Cada LAG esta asociada con una sola dirección MAC. Tramas que permanecen lógicamente juntos (por ejemplo, para una aplicación que es usada en una instancia dada fluyendo en secuencia entre un par de estaciones terminales) son tratadas como una conversación (similar al concepto de un "flujo"). Conversaciones individuales se agrupan para formar una "Conversación Agregada", de acuerdo a reglas de conversación agregadas de usuario específico. El cual puede especificar acumulacion, por ejemplo, en base a la dirección de pares ya sea fuente o destino, VLAN ID, subred IP, o tipo de protocolo. Tramas que pertenecen a una conversación dada son transmitidas en un solo enlace de segmento dentro de un LAG para asegurar la entrega en secuencia.

Un protocolo de control de "Link Aggregation" es utilizado para intercambiar configuraciones de enlace, capacidad, y estado de información entre switches adyacentes, con el objetivo de formar LAGs dinámicamente. Un protocolo "flush" (que limpia una parte de la memoria), similar al de LAN

Entre los objetivos del estándar IEEE P802.3ad están las configuraciones automáticas, protocolos de encabezado pequeño convergencia rápida y determinista cuando los estados de enlace cambian, y alojamiento de enlaces agregados desapercibidos.

3.9 Tecnología, Complejidad y Costo.

Dos de los criterios más severos en la decisión de tecnología son la complejidad y costo de la tecnología. En ambos aspectos, simple y de precio razonable Gigabit Ethernet gana en comparación a ATM, a la menos n redes de empresas.

ATM es bastante complejo debido a que es una tecnología orientada a conexión que tiene que emular la operación de LANs no orientada a conexión. Como un resultado, componentes físicos y lógicos, conexiones, y protocolos han sido agregados, con la necesidad acompañante de entender, configuración, y soporte operacional.

No como Gigabit Ethernet (el cual es ampliamente plug-and-play) hay una curva de aprendizaje escarpada asociada con ATM, en desarrollo del producto también como utilización del producto. ATM también sufre de un mayor número de interoperabilidad y compatibilidad que Gigabit Ethernet, debido a sus diferentes opciones que implementan los vendedores que presentan en sus productos. Aunque las pruebas de interoperabilidad mejoran la situación, esto también agrega tiempo y costo para el desarrollo de productos ATM.
Debido a la gran complejidad, el resultado es también mayor costo en:

- Educación y capacitación
- Implementación y despliegue
- Determinación y resolución de problemas
- Soporte operacional continuo
- Equipo de análisis y prueba, y otras herramientas de administración.

3.10 Integración de capa 3 y sus funciones.

Ambos ATM y Gigabit Ethernet proporcionan la base de una red interna sobre la cual paquetes IP son transportados. Aunque inicialmente una tecnología de capa 2, la funcionalidad de ATM se mueve hacia arriba en el modelo de referencia OSI. La interface de nodo de red privada de ATM (PNNI) proporciona señalización y OSPF- como la mejor determinación de ruta cuando se esta configurando el camino de un sistema terminal de fuente a destino. Multiprotocol sobre ATM (MPOA , Multiprotocol over ATM) permite rutas de acceso rápido para ser establecidas entre dos sistemas terminales ATM que se comunican localizados en diferentes subredes IP, completamente saltándose los routers que intervienen a lo largo del camino.

En contraste, Gigabit Ethernet es estrictamente una tecnología de capa 2; con mucha de las otras funcionalidades necesarias y agregadas arriba mencionadas. A un mayor grado, esta separación de funciones es una ventaja

debido a los cambios de una función no interrumpen otra si hay modularidad clara de funciones.

Este desacoplamiento fue una motivación clave en el desarrollo original de la capa 7 del modelo de referencia OSI. De hecho, la complejidad de ATM puede ser debido a todas las ricas funcionalidades proporcionadas "en un bit" no como la relativa simplicidad de Gigabit Ethernet, donde capas más altas operacionales es mantenida de forma separada desde, y agregada "una a la vez" hacia, las funciones básicas de la física y de enlace de datos.

3.10.1 Protocolos MPOA y NHRP

Un router tradicional proporciona 2 funciones básicas de capa 3: determinar el mejor camino posible hacia el destino utilizando protocolos de control de ruteo tales como RIP y OSPF(esto es conocido como la función de ruteo), y entonces se envían las tramas sobre ese camino (esto es conocido como la función de reenvió).
Multi protocolo sobre ATM (MPOA) mejora la funcionalidad de la capa 3 sobre ATM en tres formas:

- MPOA utiliza un modelo de router virtual para proporcionar un rendimiento mayor en cuanto a escalabilidad permitiendo la típica función de control de ruteo centralizada, para separar de la función de envió de tramas de datos y distribuyendo la función de envió de trama de datos a los switches de acceso en la periferia de la red. Esta "separación de mando permite a la capacidad de ruteo y la de envió a ser distribuidos hacia donde cada uno es más efectivo, y permita a cada uno ser escalados cuando se necesite sin la interferencia de otro.
- MPOA habilita caminos (conocidos como atajos de VCCs) para ser directamente establecidos entre una fuente y su destino, sin el salto-por-salto, procesamiento trama-por-trama y envió que es necesario en las tradicionales redes de routers. Routers intermedios, los cuales son potencialmente embotellamientos para el funcionamiento, son completamente puenteados, de tal modo realzar el funcionamiento del envió.
- MPOA utiliza menos recursos en el formato de VCCs. Cuando los routers tradicionales son utilizados en una red ATM, un Data Direct VCC (DDVCC) debe ser establecido entre un sistema terminal fuente y su gateway router, un DDVCC entre un sistema terminal destino y su gateway router, y varios DDVCCs entre routers intermedios a lo largo del camino o la ruta. Con MPOA, solamente un DDVCC se necesita entre el sistema terminal fuente y el destino.

Gigabit Ethernet también puede impulsar una característica similar para el tráfico IP utilizando el protocolo de resolución en el próximo salto (NHRP, Next Hop Resolution Protocol). De hecho, MPOA utiliza NHRP como parte de su proceso para resolver las direcciones destino MPOA. Las peticiones de resolución MPOA son convertidos a peticiones de resolución NHRP al ingresar al servidor MPOA antes de ser enviadas hacia la fuente solicitante.

Solo como un atajo MPOA puede establecerse para redes ATM, atajos en NHRP pueden también establecerse para proporcionar una mejora en el funcionamiento en una red switcheada de tramas.

3.10.2 Compuerta de redundancia.

Para rutear entre subredes en una red ATM o Gigabit Ethernet, los sistemas terminales típicamente están configurados con una dirección estática de un gateway router de capa 3. Siendo un solo punto de falla, algunas veces con consecuencias catastróficas, varias técnicas han sido desplegadas para asegurar que un cuando exista una falla de este estilo otro equipo entre para suplantar al que fallo.

Con ATM, los gateways capa 3 redundantes y distribuidos son actualmente las especificaciones de los vendedores. Incluso si emerge un estándar es probable que más componentes lógicos, protocolos y conexiones necesiten ser puestos en ejecución para proporcionar funcionalidad redundante y/o distribuida en el gateway.

3.10.3 Protocolo redundante de router virtual.

Para Gigabit Ethernet, un IETF RFC 2338 Virtual Router Redundancy Protocolo (VRRP) esta disponible para el despliegue de interoperabilidad y que gateway routers cuenten con alta elasticidad. VRRP permite a un grupo de routers proporcionar redundancia y funciones de gateway distribuidas para los sistemas terminales a través del mecanismo de una dirección IP virtual – la dirección que es configurada en sistema terminal como el gateway router predeterminado.

A cualquier hora, la dirección IP virtual es trazada hacia un router físico, conocido como el maestro o el dominante. Si este router maestro falla, otro router dentro del grupo es elegid como el nuevo router Maestro con la misma dirección IP virtual. El nuevo router maestro automáticamente asume el control como el nuevo gateway predeterminado, sin requerir cambios de configuración en los sistemas terminales. Además, cada router puede ser el router maestro para un conjunto de sistemas terminales en una subred mientras se proporcionan funciones de respaldo para otros, así distribuyendo la carga a través de múltiples routers.

3.11 Integración de LAN

Los requerimientos de las LAN son muy diferentes de los de una WAN. En la LAN, el ancho de banda es prácticamente"libre" una vez instalado, mientras no hay ningún costo por uso. Tanto como la suficiente capacidad de ancho de banda es proporcionado(o incluso sobre abastecido) para reunir la demanda, puede no haber una necesidad de técnicas complejas de controlar el uso del ancho de banda. Si suficiente ancho de banda existe para reunir toda la demanda, entonces la administración compleja de tráfico y esquemas de control de congestión no pueden ser necesarios para todos. Para el usuario,

otros asuntos suponen mayor importancia; estos incluyen facilidad de integración, manejabilidad, flexibilidad (movimiento, agregaciones y cambios), simplicidad, escalabilidad, y rendimiento.

3.11.1 Integración transparente.

ATM ha sido a menudo importunado como la tecnología que proporciona integración transparente desde el escritorio, sobre algún campus o empresa, a través de la WAN y alrededor del mundo. Los mismos protocolos y la misma tecnología son usados en todas partes. Desplegando soporte operacional en curso es mucho más fácil debido a la oportunidad para "aprender una vez y así realizar mucho." Una conjetura importante en este escenario es que ATM será ampliamente desplegada hacia los escritorios. Esta suposición no va de acuerdo con la realidad.

El despliegue de ATM hacia los escritorios es poco menos que insignificante, mientras que Ethernet y Fast Ethernet están instalado muy extensamente en millones de estaciones de trabaja de escritorio y servidores. De hecho, varios vendedores de PCs incluyen tarjetas de red Ethernet, Fast Ethernet, y (cada vez más) Gigabit Ethernet en las tarjetas madre de sus estaciones de trabajo o servidores que ofrecen. Dada esta base instalada y la tecnología común de la cual se desarrollo, Gigabit Ethernet proporciona integración transparente desde el escritorio a través de los backbones de campus o empresas.

Si ATM se despliegara como tecnología para el backbone en un campus para todos los escritorios Ethernet, entonces existiría la necesidad de convertir de trama a celda y de celda a trama (Esto es el encabezado SAR: Segmentation and Reassembly)
Con Gigabit Ethernet como tecnología de backbone en un campus y Ethernet en los escritorios, no existe la necesidad de conversión de célula a trama o de trama a célula. Ni siquiera la conversión de trama a trama se requiere desde una forma de Ethernet a otra, por lo tanto, Gigabit Ethernet proporciona una mayor integración transparente en un ambiente LAN.

3.11.2 Broadcast y Multicast

Broadcasts y Multicasts son medios para enviar información muy naturales desde una fuente a múltiples receptores en una LAN no orientada a conexión. Gigabit Ethernet esta diseñado precisamente para ese estilo de ambiente. La capa alta de direcciones IP Multicast es fácilmente mapeada hacia la dirección MAC del hardware. Utilizando IGMP (Internet Group Management Protocol), se recibe el reporte de estaciones terminales pertenecientes a un grupo (y responde a las preguntas de este) un ruteador que maneje multicast para recibir tráfico de multicast desde redes mas allá de las que localmente están anexadas. Los sistemas terminales fuente necesitan no pertenecer a un grupo de multicast en orden para poder enviar a miembros de ese grupo.
En contraste, broadcast y multicast en una LAN ATM presentan pocos retos debido a la naturaleza de que ATM es orientado a conexión.

En cada LAN emulada (ELAN), ATM necesita de un servidor de LAN Emulation (LES) y un Broadcast y un Unknown Server (BUS) para traducir de direcciones MAC hacia direcciones ATM. Estos componentes adicionales requieren de recursos adicionales y complejidad necesaria para señalar, instalar, mantener, y liberar el control directo, control distribuido, enviar multicast, y enviar VCCs de Multicast. La complejidad se incrementa porque una ELAN puede solamente tener un solo LES/BUS, el cual debe ser apoyado o respaldado por otro LES/BUS para eliminar cualquier punto de falla. Comunicación entre nodos LES/BUS activos y de respaldo requieren más conexiones virtuales y protocolos para sincronización, detección de falla, y apoderamiento (SCSP y LNNI).

Con todo el tráfico de broadcast que pasa a través del BUS, el BUS presenta un potencial cuello de botella.

Para realizar una multidifusión o multicasting de IP en una red LANE, ATM necesita los servicios del BUS y, si esta disponible (con LUNI v2), un SMS. Para realizar multidifusión o multicasting en una red ATM clasica de IP, ATM necesita los servicios de un MARS (Multicast Address Resolution Server o Servidor de Resolución de Direcciones Multicast), un MCS (Multicast Connection Server o Servidor de Conexión de Multicast), y el Control de Cluster de VCCs. Estos componentes requieren recursos adicionales y complejidad para señalización de conexión, instalación, mantenimiento y desinstalación.

Con UNI 3.0/3.1, la fuente debe primero resolver la dirección destino hacia los miembros del grupo de direcciones ATM, y entonces construir un árbol punto-multipunto, con la misma fuente como raíz hacia los múltiples destinos antes de que el tráfico de multicast sea distribuido. Con UNI 4.0, las estaciones terminales pueden entrar tanto como salir de un árbol de distribución de punto a multipunto, con o sin intervención de la raíz. Asuntos de interoperabilidad entre las diferentes versiones de UNI son realzadas en cada caso.

3.11.3 Multi-Integración LAN

Como una tecnología de backbone, ATM puede interconectar segmentos de LAN físicos utilizando Ethernet, Fast Ethernet, Gigabit Ethernet y Token Ring. Utilizando ATM como tecnología de enlace de subida común y con funcionalidades de puenteo, Ethernet y Token Ring pueden inter operar relativamente fácil.

Con Gigabit Ethernet, la interoperación entre Ethernet y Token Ring las LAN requieren puentes que transformen el formato de trama de un tipo al otro.

3.12 Integración MAN/WAN

Es relativamente fácil interconectar backbones de campus ATM a través de una MAN o una WAN. La mayoría de los switches ATM cuentan con interfaces DS1/E1, DS3/E3, SONET OC-3c/SDH STM-1 y SONET OC-12c/SDH STM-4 ATM que pueden ser conectadas directamente a la MAN ATM o las facilidades de una WAN. Algunos switches son ofrecidos con circuitos que emulan DS1/E1, DS1/E1 con multiplexaje inverso sobre ATM, y redes Frame Relay y características de servicio de inter conectividad que conectan hacia la existente MAN que no es ATM o a las facilidades de la WAN. Todas estas interfaces permiten que ATM tenga conexiones directas en sus switches hacia las MAN o WAN, sin la necesidad de equipos adicionales en el borde LAN-WAN.

En este momento, varios switches Gigabit Ethernet no ofrecen interfaces MAN/WAN. Conectar redes Gigabit Ethernet de campus a través de MAN o WAN típicamente requiere el uso de equipos adicionales para acceder a las facilidades de la MAN/WAN, tales como Frame Relay, líneas rentadas, y aun las redes ATM. Estos equipos de interconexión son típicamente routers u otros switches multiservicio y eso se agrega a la complejidad y costo. Con la rápida aceptación de Gigabit Ethernet como el backbone del campus de opción, sin embargo, en el mercado ya se encuentran ofertas de interfaces tales como ATM SONET OC-3c/SDH STM-1, SONET OC12-c/SHD STM-4, y Packet-over-SONET/SDH en switches Gigabit Ethernet.

Mientras una LAN ATM ofrezca integración transparente con la MAN ATM o WAN a través de su inter conectividad directa, la MAN/WAN para la mayoría continuará siendo heterogénea y no homogénea. Esto se debe al equipo instalado que no es ATM, a cuestiones geográficas, y el tiempo que se necesita para cambiar. Esta situación persistirá más en las LAN donde existe un mayor control por las empresas y, por consiguiente, mayor facilidad de convergencia. Incluso en las LAN, la convergencia es hacia Ethernet y no hacia ATM. Otras tecnologías que no son ATM se necesitarán para interconectar localidades e incluso regiones enteras, debido al terreno geográfico difícil o alcance económico. Así seguirá existiendo la necesidad de una tecnología de conversión de LAN a WAN, excepto donde ATM ha sido implementado.

Otro desarrollo (el difundido empleo de fibra óptica) puede permitir que las LAN puedan ser extendidas sobre las WAN utilizando el aparentemente ilimitado ancho de banda óptico para el tráfico de LAN. Esto significa que los campuses con Gigabit Ethernet pueden extenderse a través de una WAN tan fácil, quizás aun más fácil y más barato, que ATM sobre WAN.

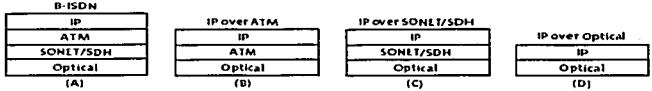
Entre las posibilidades esta el acceso a la "fibra obscura" ("Dark fiber o fibra obscura" es la fibra de alta velocidad. Esta es la fibra de red en la cual otros conectan sus equipos. El proveedor de servicio conecta sus equipos en un extremo y el cliente pone el suyo al otro extremo. Una compañía de telecomunicaciones es la propietaria del medio entre estos dos) con largo

alcance para distancias extendidas para Gigabit Ethernet (50km o más), paquetes-sobre-SONET/SDH e IP sobre "Optical Dense Wave Division Multiplexing".

Una simple y aun poderosa forma para tener un desempeño alto en redes de campus Gigabit Ethernet a través de WAN, especialmente en áreas metropolitanas, es el uso de Packet-over-SONET/SDH (POS, también conocido como IP sobre SONET/SDH). SONET esta emergiendo como un servicio competitivo para ATM sobre la MAN/WAN. Con POS, los paquetes IP son directamente encapsulados en tramas SONET, así eliminando el encabezado adicional de la capa (ver columna "C" en la figura 12)

Para extender esto a un paso más, los paquetes de IP pueden ser transportados sobre fibra al natural sin el encabezado de tramas SONET/SDH; esto es llamado IP sobre Optical(ver columna "D" en la figura 12) "Opical Networking" puede transportar muy altos volúmenes de tráfico datos, voz y video sobre diferentes longitudes de onda de luz.

Fig. 12 Interconexión de tecnologías sobre la MAN/WAN



El patrón de tráfico también ha cambiado rápidamente, con más de 80 por ciento de tráfico de red esperado en atravesar la MAN/WAN, contra solamente el 20 por ciento restante en el campus local. Dado el patrón cambiante de tráfico, y el surgimiento de IP como el protocolo de red dominante, la total eliminación de capas de comunicación para IP sobre la MAN/WAN significa reducir el costo de uso de ancho de banda y mayor rendimiento para las aplicaciones de otros usuarios. Mientras todas estas tecnologías se están desarrollando, los negocios intentan reducir al mínimo los riesgos invirtiendo en Gigabit Ethernet por su bajo costo, al contrario del alto costo de ATM.

3.13 Aspectos de administración

Debido a que los negocios necesitan ser incrementados dinámicamente para responder a las oportunidades y retos, el ambiente de las redes de los campus está en un constante estado de flujo. Hay movimientos continuos, agregados, y cambios; usuarios y estaciones de trabajo forman y reforman grupos de trabajos; y los usuarios altamente móviles trabajan desde sus casas y hoteles para incrementar la productividad.

Con todos estos constantes cambios, la capacidad de dirección de las redes de los campus es un criterio de selección muy importante. El más homogéneo y simple de los elementos de la red son, los más fáciles de manejar. Dada la omnipresencia de Ethernet y Fast Ethernet, Gigabit Ethernet presenta una integración más transparente con los elementos existentes de la red que con

los de ATM. Así, Gigabit Ethernet es más fácil de manejar. Gigabit Ethernet también es fácil de manejar debido a su simplicidad innata y el acervo de experiencia y herramientas disponibles con sus tecnologías predecesoras.

En contraste, ATM es significativamente diferente de los predominantes escritorios que utilizan Ethernet que los interconectan. Debido de sus diferencias y su relativa novedad, existen pocas herramientas y experiencia disponible para manejar los elementos de redes ATM. ATM es también más difícil para manejar por su complejidad de componentes lógicos y conexiones, y la multitud de protocolos que se necesitan para hacer a ATM utilizable. Arriba de la topología de red física descansan un número de capas lógicas, tales como PNNI, LUNI, LNNI, MPOA, QoS, señalización, SVCs, PVCs, y "sofá PVCs. Los componentes lógicos son más difíciles de arreglar que los elementos físicos cuando los problemas ocurren.

3.14 Estándares e Interoperabilidad

Como todas las tecnologías, los estándares de ATM y Gigabit Ethernet y sus funciones maduran y se estabilizan con el tiempo. Evolucionando de una tecnología común, backbones Gigabit Ethernet basados en tramas interoperan transparentemente con millones de escritorios no orientados a conexión, Ethernet y Fast Ethernet basados en tramas y servidores que se encuentran en los campuses y las empresas de hoy. En contraste, los backbones basados en células, orientados a conexión, necesitan funciones adicionales y capacidades que requieren estandarización, y puedan fácilmente dirigirse hacia temas de interoperabilidad.

3.14.1Estandares ATM

Aunque relativamente nuevos, los estándares ATM han sido desarrollados desde 1984 como parte de B-ISDN, diseñados para soportar redes privadas y públicas. Desde la formación del Forum ATM en 1991, varias especificaciones ATM fueron completadas, especialmente entre 1993 y 1996.

Debido al rápido ritmo de los esfuerzos de desarrollo durante este periodo, un ambiente estable se tuvo que sentir para que se diera la consolidación, implementación e interoperabilidad. En Abril de 1996, el acuerdo de fondo se convino en una colección de 60 especificaciones del Forum ATM que proporciono las bases para una estable implementación. Además diseñando un conjunto de fundacionales y especificaciones características expandidas, el acuerdo también estableció criterios para asegurar la interoperabilidad de los productos ATM y servicios entre las actuales y futuras especificaciones. Este acuerdo proporciono la confianza requerida para la adopción de ATM y un punto de referencia para desarrollo de futuros estándares. En julio de 1999, hubo más de 40 especificaciones del Forum ATM en varios escenarios de desarrollo.

Para promover la interoperabilidad, el consorcio de ATM fue formado en Octubre de 1993, uno de los varios consorcios del Laboratorio de Interoperabilidad de la Universidad de New Hampshire. El consorcio de ATM

es una agrupación de vendedores de productos de ATM interesados en probar la interoperabilidad y conformidad de sus productos de ATM en una atmósfera de cooperación, sin ninguna publicidad competitiva perjudicial.

3.14.2 Estándares de Gigabit Ethernet

Por el contrario, Gigabit Ethernet ha evolucionado del esfuerzo y el crédito que se le da a las tecnologías de Ethernet y Fast Ethernet, el cual ha estado en uso por más de 20 años. Siendo relativamente simple comparado con ATM, mucho del desarrollo fue completado dentro de un relativo corto tiempo. La alianza de Gigabit Ethernet, un grupo de vendedores de sistemas de redes promovió el desarrollo, demostración e interoperabilidad de los estándares de Gigabit Ethernet. Desde su formación en 1996, la Alianza ha tenido mucho éxito ayudando a introducir los estándares de Gigabit Ethernet IEEE 802.3z 1000BASE-X, y el IEEE 802.3ab 1000BASE-T.

Similar al consorcio de ATM, el consorcio de Gigabit Ethernet fue formado en Abril de 1997 en la Universidad de New Hampshire en el Laboratorio de Interoperabilidad como un esfuerzo cooperativo entre los vendedores de productos de Gigabit Ethernet. El objetivo del consorcio de Gigabit Ethernet es la comprobación continua de los productos de Gigabit Ethernet y software para que exista una interoperabilidad y una perspectiva de conformidad.

Por último de este capítulo lo que nos resta decir es que en redes empresariales, ya sea ATM o Gigabit Ethernet cualquiera puede emplearse como tecnología de un backbone. La clave esta en la complejidad y mucho más alto costo de ATM, contra la simplicidad y el mucho más bajo costo de Gigabit Ethernet. Mientras que se puede argumentar que ATM es mucho más rico en funcionalidades, la consideración puramente técnica es solamente uno de los criterios de decisión, a pesar de ser uno de los más importantes.
De importancia extrema es la funcionalidad la cual resuelve las necesidades de hoy en día a un precio que sea realista. No tiene caso el pagar por mayor funcionalidad y complejidad que es innecesaria, que puede o no ser necesitada, y que de igual manera puede ser obsoleta en el futuro. El índice de cambio de la tecnología y las presiones competitivas demandan que la solución sea disponible ahora, antes de próximo paradigma de cambio, y antes que nuevas soluciones introduzcan otro conjunto de retos completamente nuevos.

Gigabit Ethernet proporciona una solución de backbone pragmática, viable, y relativamente barata (y así, bajos riesgos) que reúne los requerimientos de hoy e integra transparencia con la omnipresencia de lo no orientado a conexión, y las LANs Ethernet y Fast Ethernet basados en tramas.

En contraste, ATM proporciona una solución de backbone que tiene las desventajas de una inmerecida complejidad, inaprovechada funcionalidad, y el mucho más alto costo de pertenencia. Mucha de la complejidad resulta de la multitud de componentes adicionales, protocolos, control, y conexiones de datos requeridos por ser orientado a conexión, ATM basado en celdas para emular broadcast, orientado a no conexión, LANs basadas en tramas. Mientras

que la Calidad de Servicio (QoS) es un requerimiento cada ve más importante en las redes empresariales o de los campus universitarios que requieran un proyecto de estas magnitudes, así existen otras soluciones para el problema que son más simples, crecientes, y menos caras.

CAPITULO 4

PROCESO DE MIGRACION DEL BACKBONE DE REDUNAM.

En este capitulo abordaremos la manera en la que se deberá migrar el backbone de RedUNAM para al final poder tener en buen termino nuestro proyecto de reestructuración, es importante tomar en cuenta que se describirá todo el proceso en base a equipos de marca Foundry modelo BIGIRON 8000 y NETIRON 800 por haber sido estos los equipos que se adquirieron, mediante un proceso de licitación que tocaremos en el siguiente capitulo.

4.1 Habilitación del protocolo OSPF en los routers del Backbone.

El protocolo OSPF V2 es un protocolo de compuerta interior definido en el RFC 2328. OSPF es importante debido a que tiene un número de características no encontradas en otros protocolos de compuerta interior. El soporte para estas características adicionales hace a OSPF la elección preferida para las nuevas implementaciones de IP sobre redes, especialmente en redes largas. Algunas de las características más distintivas son las siguientes:

- OSPF no tiene una limitante máxima de 15 saltos. Debido a que OSPF es un protocolo link state, cada ruteador tiene un completo entendimiento de todas las redes en su área. Por consiguiente, el peligro de loops de ruteo no se presentaran más, haciendo que la limitante de hop-count no exista más
- El uso del ancho de banda es más eficiente, debido a que OSPF es un protocolo de link state y por lo tanto manda solo los cambios de actualización en lugar de actualizaciones completas
- Debido a las relaciones con sus vecinos, combinado con el envió de solamente los cambios, OSPF propaga los cambios de redes mucho más rápido.
- OSPF soporta VLSM totalmente, sumarización de ruteo y redes no contiguas.
- Un número de opciones de seguridad pueden ser configuradas para habilitar las actualizaciones de ruteo para ser enviadas utilizando encripción.
- La determinación de la ruta es mejorada debido a que el valor de la métrica pueden ser configuradas manualmente.
- OSPF es muy flexible con respecto al direccionamiento y en cambios de diseño.

Estas características hacen a OSPF muy apropiado para redes de escala larga y más sensible a los cambios de la topología.
El diseño abierto del estándar de OSPF ofrece soluciones flexibles en varias situaciones. Su característica de flexibilidad asegura la interoperabilidad con otros protocolos de ruteo mientras se mantiene sus opciones de escalabilidad

Listamos algunos atributos clave del protocolo OSPF:

- Los enrutadores que corren OSPF mantienen una relación orientada a conexión con otros enrutadores en el mismo segmento físico en el cual residen. En términos de OSPF, estos enrutadores en particular son llamados vecinos adyacentes.
- OSPF no esta limitado en la segmentación solamente por direcciones IP o subred; este utiliza "áreas" para designar grupos de redes.
- Aunque OSPF puede ser implementado como un protocolo de ruteo que interconecta varias áreas, este sigue siendo un protocolo de ruteo interno

4.1.1 Jerarquía de OSPF

Existen tres tareas básicas que un router en una red con OSPF puede realizar: operación en una área, conexión inter-área, y conectar un sistema autónomo entero, por ejemplo un ISP; Red UNAM es considerado como un ISP (Proveedor de Servicio de Internet). Como hemos mencionado previamente una de las características claves de OSPF para lograr esto es su capacidad de asignar funcionalidades especificas a un router en particular. Esta funcionalidad esta definida por un conjunto de tareas y responsabilidades que dependen de la posición del router en la jerarquía del diseño de la red de OSPF. Los ruteadores que desempeñan estas funciones tienen nombres distintivos en la terminología de OSPF:

- *Router interno* (IR) Un IR funciona solamente dentro de una área. Su tarea primordial es mantener una base de datos correcta y arriba que contenga todas las subredes del área. Este reenvía datos a otras redes en el área, y ruteando o inundando a otras áreas siempre que se requiera la intervención de un ruteador de límite de área (ABR).
- *Router de backbone* (BR) Una de las reglas de diseño de OSPF es que cada área en la red tiene que ser interconectada a través de una sola área, la cual generalmente es llamada "área 0" o el "área de backbone". La mayoría de los routers del backbone tienen una interfase hacia el área del backbone y una o más a otras áreas. Sin embargo, un router que tiene una o más interfases que solamente lo conectan al backbone es también llamado Router de backbone. Una cosa importante a recordar aquí es que un router de backbone no se requiere que tenga un ABR. La figura 4.1 muestra la funcionalidad y el lugar de un BR en una red OSPF
- *Router de límite de área* (ABR) Un ABR conecta 2 o más áreas OSPF, y por consiguiente, múltiples ABRs pueden existir en una red OSPF. Para desempeñar este papel, un ABR tiene múltiples copias de una base de datos de estado de enlace. Cada base de datos contiene la topología completa de cada área que esta conectada a este tipo de router y de esta manera puede ser sumarizado. Esta información es entonces reenviada hacia la red del backbone para que sea

distribuida. El asunto clave aquí es que un ABR es el lugar para configurar la sumarización, debido a que este es el lugar donde el algoritmo de estado de enlace puede maximizar su capacidad para poner las actualizaciones de ruteo reducidas para ser usadas. Cuando hablamos de la capacidad de los ABR para minimizar las actualizaciones de ruteo.

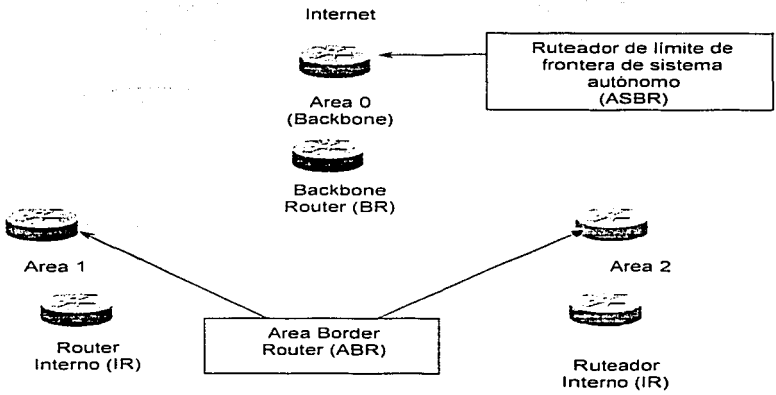


Fig. 4.1Tipos de routers en OSPF

- *Ruteador de frontera de sistema autónomo* (ASBR) Recordemos que al tener conectado el mundo afuera de nuestro sistema autónomo que maneja OSPF, se necesita un router que pueda actuar como una clase de compuerta entre los dos sistemas autónomos. Es aquí donde el ABSR entra en función. Intercambiando información de ruteo con los ASBRs de otros sistemas autónomos es el principal propósito de un ASBR. Esta información consecuentemente es distribuida dentro del Sistema Autónomo por el ASBR.

4.1.2 Pasos que sigue OSPF para aprender acerca de otras áreas

Aquí hablaremos del mecanismo que utiliza OSPF para saber en que área está un router y de como construye la tabla de la topología y la tabla de ruteo.

Existen tres pasos que un router que correo OSPF necesita completar para estar disponible al paso del tráfico.

1. El ruteador debe encontrar sus routers vecinos. Para hacer esto, el ruteador utiliza paquetes Hello. Usualmente, existen 2 tipos especiales de vecinos: el *ruteador designado* (DR) y el *ruteador designado de respaldo (BDR)*.
2. Este aprende acerca de todas las rutas hacia otros ruteadores en el área e inserta estas en la tabla de la topología.
3. OSPF utiliza el algoritmo de "primero el camino más corto" (SPF) para encontrar la mejor ruta e insertar estas dentro de la tabla de ruteo.

4.1.2.1 Secuencia que sigue OSPF para encontrar router vecinos

Los ruteadores vecinos son el primer paso cuando se esta descubriendo la red con el protocolo de OSPF. Desde estos vecinos la adyacencia puede ser construida, permitiendo a los ruteadores el intercambio de información del estado del enlace y construir sus bases de datos de estado de enlace.
Como ya mencionado OSPF utiliza mensajes Hello para encontrar a los vecinos y ver si existe algún cambio en la red. Los paquetes Hello son del tipo multicast, el cual es muy parecido a un broadcast, pero solamente los equipos que están corriendo OSPF aceptaran tales paquetes.

Un paquete Hello de OSPF contiene la siguiente información:

- *Router ID* Este número indica que puede ser una dirección IP o un número que fue configurado manualmente y que identifica como único al router. Es cuestión del diseñador de red la elección entre un número o una dirección IP, es decir que depende de los ingenieros que diseñamos la red la decisión de utilizar números o direcciones IP. El router ID tiene una función especial: se utiliza como desempate entre dos routers que están compitiendo por ser el ruteador designado.
- *Hello interval* Este número indica que tan frecuente un ruteador mandará un paquete Hello. Los paquetes Hello son enviados para ver si los routers vecinos están aun vivos y para informar a ellos que aun el está vivo. El valor por defecto de este contador es de 10 segundos y debe ser el mismo en todos los routers de la misma área; de otra forma, los routers no aceptaran al vecino.

- *Dead interval* Este intervalo es la cantidad de tiempo que un router esperara sin recibir paquetes Hello antes de que considere que su router vecino a muerto. El valor por defecto es cuatro veces el *Hello interval*, y este también debe ser el mismo para todos los routers en el área.
- *Área ID* Este es un identificador que le dice a otros routers a cual área pertenece. Los routers solamente se comunicarán si ellos están en la misma área. Este número puede ser representado como un número decimal o ya sea como una dirección IP.
- *Router priority* Este número influye en la decisión de la cual router va a ser el "ruteador designado (DR)". El valor por defecto es 1, y este valor puede configurado por uno mayor en orden para que algún router siempre sea el DR. Si dos routers tienen el mismo número, el protocolo desempata utilizando el número del " router ID"
- *DR y BDR* Si el ruteador conoce la dirección IP del DR y BDR, este campo se llena con esa información.
- *Authentication password* Esta es una característica opcional para asegurar que routers extraños o no pertenecientes, estén anexándose al área
- *Bandera de Stub y Area* Esta bandera indica que si esta área tiene solamente un ruteador que conecta el área a otras áreas. Esto se utiliza para simplificar el proceso de ruteo.
- *Neighbors* Si el ruteador sabe de algún vecino que descubrió a través del proceso neighbor-discovery, esto se incluye al propio router en ese campo.

Cuando se manda un paquete Hello sucede lo siguiente, el router tiene una tabla que tiene todos los routers vecinos que el conoce. El router pasa a través de ciertos estados que indica como la comunicación esta progresando:

1. Cuando un ruteador A comienza a descubrir la red, este se encuentra en el estado down (abajo). Este no conoce a ningún vecino y envía hacia afuera un paquete Hello para anunciarse a otros routers. Obviamente, bastantes campos en el paquete Hello estarán vacios, debido a que se esta comenzando a conocer la red, este no tiene ninguna información acerca de su entorno. ver figura 4.2
2. Todos los ruteadores que han visto el paquete Hello crean una nueva entrada en la tabla de adyacencia. Entonces ellos mandan un paquete Hello directamente de regreso hacia el router A utilizando un unicast. Este paquete Hello incluye toda la información que el router conoce de el. El router A pasa al estado "init". Ver figura 4.3.
3. Después de que el router A recibe todos los paquetes Hello de los routers cercanos, este construye su propia tabla de adyacencia. esta adyacencia son configuradas en dos sentidos para indicar que la comunicación esta arriba y corriendo, Ver figura 4.4

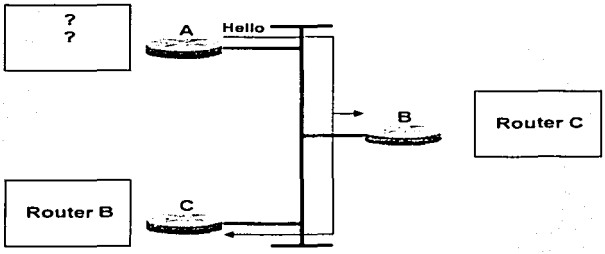


Fig. 4.2 El router A manda un paquete Hello

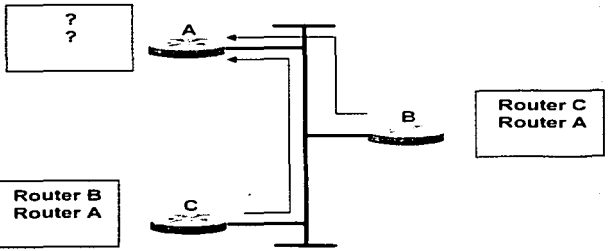


Figura 4.3 El router A obtiene una contestación de los routers B y C

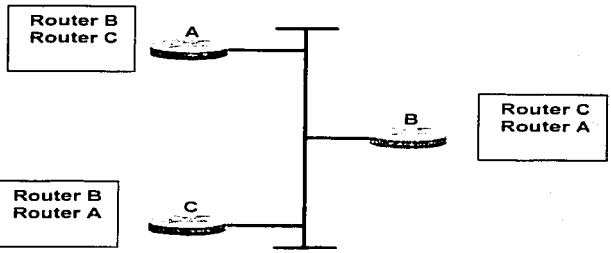


Figura 4.4 El router A ha aprendido acerca de sus routers vecinos, y el estado en los dos sentidos han sido llevada a cabo

4. Si no ha habido información de regreso acerca de los DRs y BDRs cuando los paquetes Hello han retornado (por ejemplo, si todos los routers son encendidos al mismo tiempo), estos comenzaran a discutir quien debe de ser el DR y quien debe de ser el BDR.
5. Los vecinos envían paquetes Hello con un intervalo de unos pocos segundos, como se indica en el campo del Hello Interval en el paquete Hello.

4.1.2.2 Elección de DR y BDR

Ahora que ya vimos como los routers pueden hablarse uno al otro para encontrar si estos están funcionando adecuadamente, se tiene que elegir un DR y un BDR.

Examinaremos primero las funciones de un DR y del BDR. El DR actúa como la base de datos central para toda la información de estado de enlace para la red en la cual fue elegido para ser DR. Todos los ruteadores en la red entonces solo envían información de estado de enlace hacia los DRs y BDRs, y solamente reciben información proveniente del DR.

Puesto que todos los ruteadores OSPF necesitan recibir todas las actualizaciones de estado de enlace proveniente de todos los otros routers , lo óptimo es tener un router que actúe como un punto central desde el cual información confiable pueda ser recibida y enviada. Esto reduce la cantidad de tráfico necesario para mantener todos los routers actualizados y hacer mucho más fácil esto y asegurar que todos los routers tienen información idéntica acerca de la topología de la red.

EL BDR obtiene todas las actualizaciones al igual que el DR, pero este deja las actualizaciones y la sincronización de la información de estado de enlace al DR hasta que llega a ser inaccesible en la red.

- Cuando no hay DRs o BDRs en una red, los routers examinan el campo "Priority" en el paquete Hello, y el router con el más alto número en este campo llega a ser el DR. Y el próximo más alto llega a ser el BDR. Si el número en el campo "Priority" es igual a cero, entonces el router no puede llegar a ser un DR o BDR.
- Si existen 2 routers con el mismo número más alto, el número de "Router ID "es verificado, y el valor más alto en ese campo decide cual router llega a ser el DR.
- Si existe un router con un valor más alto en prioridad que el existente DR y este es insertado en la red, nada cambia. El nuevo router puede solamente ser asignado como el BDR si el existente DR o BDR llega a ser inalcanzable.
- El DR es asumido que es inalcanzable por el BDR si este no ve las actualizaciones enviadas hacia los routers desde el DR en términos regulares.

La figura 4.5 muestra el resultado de una elección de DR/BDR.

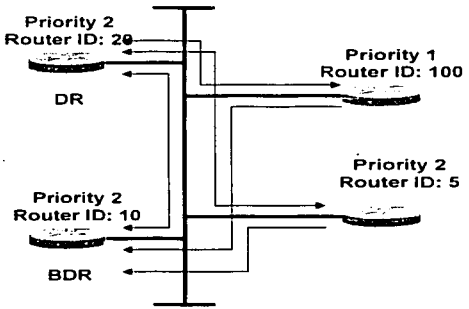


Fig. 4.5 El resultado de la elección de DR/BDR. Las flechas indican los enlaces lógicos formados a través de las adyacencias.

4.1.2.3 Proceso que se sigue cuando se descubre la topología por primera vez

Como hemos comentado en los puntos anteriores los routers han alcanzado una etapa importante. Han aprendido lo siguiente:

- Los routers saben acerca de todos los otros routers (vecinos) en su red local (tabla de adyacencia).
- Los routers saben cual es el que manda las actualizaciones de la topología, y desde cual router ellos recibirán las actualizaciones (DR).

Los routers entonces ahora comienzan a construir una topología, es decir una base de datos de estados de enlace de toda el área completa y aprenden acerca de los enlaces de otras áreas.

En primera instancia, cuando un router no tiene base de datos de estado de enlace, el protocolo de intercambio es utilizado para obtener, digámoslo así, una foto del DR.

Este estado es llamado "exstart". Cuando el router ha recibido la base completa de los estados de enlaces proveniente del DR y enviado sus propios números de redes conectadas al DR, se dice que el DR se encuentra en estado "full", y este tiene toda la información necesaria para construir su tabla de ruteo.

Los pasos que se siguen para transferir esta información son los siguientes.

1. Un router que decide recibir información de link state proveniente de otro router establece una adyacencia. El router envía un paquete de descripción de base de datos (DDP, también llamado DBD), informando a el router que se tiene como objetivo, que es el dominante y necesita enviar su base de datos de estado de enlace hacia el router que se tiene como objetivo.
2. El router receptor realiza un chequeo para ver si su propio "router ID" tiene un valor más alto que el router remitente. Si este es el caso, el router receptor rechaza la transferencia, se apunta a el mismo como router dominante, e inicia una transferencia de su propia base de datos de estado de enlace hacia el router remitente. Si este router receptor tiene un valor más bajo en su "router ID", este router acepta la información. Este método de utilizar un sistema de maestro y esclavo es necesario para asegurar que los paquetes que contienen la base de datos puedan ser secuenciados para tener una entrega correcta.
3. El router principal (maestro) envía información de estado de enlace hacia el router que en este caso estaría como esclavo en DDPs e incluye una secuencia numerada. Cada vez que el esclavo recibe un

DDP, este reconoce el paquete retornando una aceptación (Paquete LSAck) con la secuencia numerada del DDP que esta siendo reconocida. Esto continúa hasta que la base de datos es transferida completamente.

4. Como las bases de datos están siendo actualizadas, el router podría encontrar que en cierto router hace falta información, o que tiene mejor información acerca de una ruta. Este recuerda las rutas, y después de los intercambios que se han dado, este envía los paquetes de link-state que se le han pedido para obtener la información exacta que necesita.
5. Cuando todo esto ha sido hecho, el router esta"completo", y la creación de la adyacencia esta completa.

La figura 4.6 muestra la secuencia de transferencia de la base de datos de la topología.

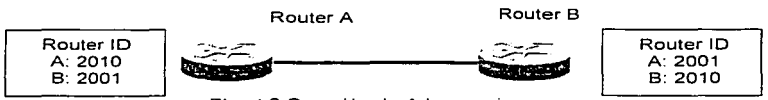
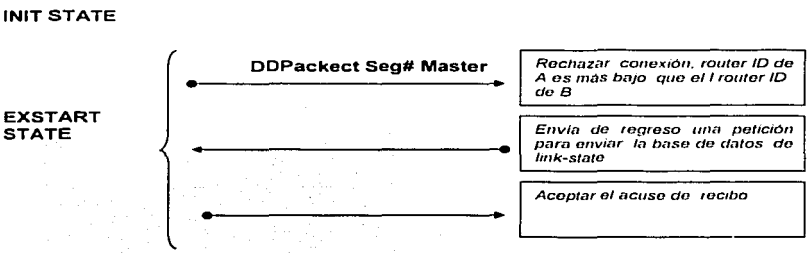
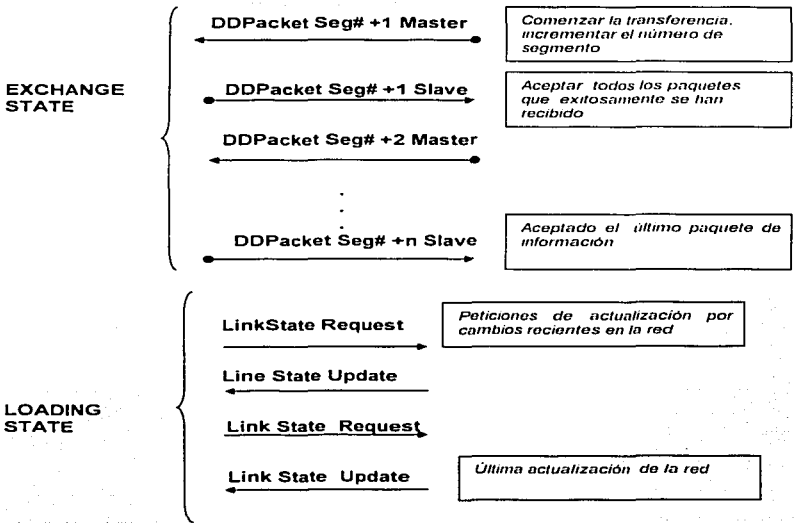


Fig. 4.6 Creación de Adyacencia.





4.1.2.4 Llenado de la tabla de ruteo

Después de que todos los routers en la red tienen completa sus bases de datos de link-state, incluyendo todas las posibles rutas de todos los routers en el área, los routers necesitan todavía resolver cuales son las mejores rutas de todos los routers. Solamente esa información es insertada en la tabla de ruteo y utilizada para rutear paquetes.

Los protocolos link-state utilizan el algoritmo SPF (primero el camino más corto) para calcular la mejor ruta en cada red. Esto se realiza mediante la construcción de una imagen de la red utilizando la información que existe en la base de datos de link-state. La imagen final es muy parecida a un árbol, en el cual el router es la raíz. Esto asegura que no existe ningún bucle de ruteo posible.

Como cada "ramificación" es calculada, el ruteador realiza un chequeo para ver si este es el camino más corto.

Para determinar el camino más corto, el router utiliza una métrica llamada "cost".
La métrica total de todos los enlaces que crea un dominio forma la métrica utilizada para el "costo total" para una ruta particular.
Cada vez que la base de datos de estado de enlace cambia debido a un suceso en la red, el algoritmo SPF es corrido nuevamente para rehacer otra tabla de ruteo.

4.1.2.5 Anuncios "Link-State"

La información en una actualización "link-state" (LSU's) es dividida en seis tipos y son llamadas "anuncios de link-state" (LSA's). Cada LSA envía cierto tipo de información:

1. Router LSA
2. Network LSA
3. Summary LSA (ABR's)
4. Summary LSA (ASBR's)
5. Autonomous System (AS) external LSA
6. No utilizado
7. Not-so-stubby area (NSSA)

1. *Router LSA* Los Router LSA le dicen al resto del área acerca del router. Un Router LSA contiene información acerca de todas las interfases conectadas de un router en particular. También tiene una bandera que informa que tipo de router es en los términos de OSPF. Estos tipos son los siguientes:
a. Punto terminal hacia una adyacencia de enlace virtual (V type)
b. router delimitador de sistema autónomo (AS) (E type)
c. router de frontera de área (B type)

2. *Network LSA* Si un DR se encuentra en una red, este comienza a enviar LSA's, este describe todos los routers en una red que tienen adyacencia con el DR (usualmente, todos ellos). Este también contiene la dirección de red y la dirección IP que es propiedad del DR.

3. *Area Border Router (ABR) summary LSA* Los ruteadores de frontera de área inundan con estos LSA's para decir a los routers en el área acerca de las redes en otras áreas a las cuales ellos están conectadas.

4. *Autonomous System border router (ASBR) summary LSA* Es muy parecido a los LSA tipo 3, estos son mandados por los ABRs para informar a las áreas acerca de las rutas externas.

5.Autonomous System external LSA Estos LSAs son mandados a través del área y contienen un resumen de los enlaces externos. El ASBR es el responsable de mandar estos LSAs a través del área. Las redes contenidas en el LSA son reenviadas hacia otras áreas como LSA tipo 4 por los ABRs.

6. No utilizado.

7. No so stubby area (NSSA) *LSA* Este es generado por un ASBR en una NSSA y describe las rutas externas hacia el área NSSA. Si el ASBR habilita un bit especial en el paquete tipo 7, puede ser transformado en un LSA external AS (Tipo 5) por el ABR para mandarse a través de otras áreas.

La figura 4.7 muestra algunos ejemplos de LSAs.

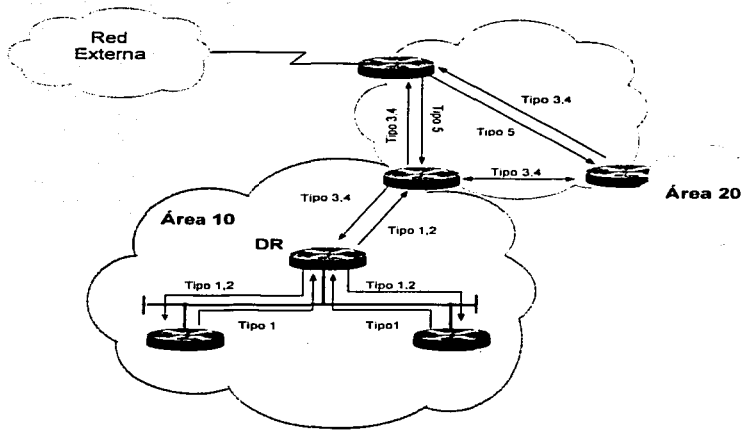


Figura 4.7 varios tipos de LSAs y en donde pueden ser encontrados

4.1.3 Configuración del protocolo OSPF para una sola área en los routers de Backbone.

El siguiente ejemplo de configuración involucra a un solo router interno (IR) dentro de una sola área OSPF. Mostramos los pasos básicos y necesarios para hacer un router que no se encuentra configurado tome parte en una red OSPF:
NOTA: Los comandos manejados en este ejemplo corresponden a equipos marca CISCO.

1. Habilitar el protocolo de ruteo OSPF
2. Asignar un número de proceso de OSPF que se requiere para que de comienzo OSPF.
3. Identificar las área(s) del router o las interfaces específicas del router que están conectadas a el.
4. Identificar las interfaces en las cuales la operación de OSPF se requiere.
5. Asignar un router ID para identificación del router en la red.

Paso1
Suponiendo que el protocolo OSPF no fue seleccionado cuando el SETUP del router fue corrido. Este tiene que ser configurado utilizando el siguiente comando:
router (config) #router ospf "número de proceso"

Paso2
El número de proceso que tiene que ser ingresado es para uso interno del router, solamente para identificar cada proceso de ruteo que esta corriendo en OSPF. Aunque es perfectamente posible correr múltiples instancias de OSPF en un router, esta no es una situación muy recomendada debido a que esto podría causar que se incremente el uso de recursos. Aunque el número de procesos no tiene que ser el mismo en todos los routers en la red, este usualmente es el método escogido por razones de claridad.

Pasos 3 y 4
Ahora que el protocolo esta habilitado en el router, debe ser configurado para que este sepa en cuales áreas tiene que tomar parte. Este es un paso obligatorio, y el comando que se utiliza es el siguiente:
router (config-router) # network "número de red" wildcard mask area "número de área"

Este comando configura el proceso de OSPF para que tome parte en el envío y recibimiento de actualizaciones de ruteo. La principal diferencia entre otros protocolos de ruteo y OSPF es que OSPF se puede especificar que interfaces pueden correr ese protocolo, con otros protocolos al configurarlo en un equipo significa que todas las interfaces tomaran parte en el proceso de ruteo. Retomando que con OSPF, se puede especificar que dirección IP tenga lugar en el proceso de OSPF y que área debe estar conectada. Como las interfases que participan en el proceso de OSPF están identificadas por OSPF utilizando el "wildcard mask". La interfase de la dirección IP es comparada con la dirección especificada en el comando "network". Esta granularidad hace posible que se pueda especificar la parte de las direcciones que utilizará OSPF. La clase entera de direcciones podría utilizarse, por ejemplo, o una dirección de una interfase específica podría ser ingresada. Cada interfase que corresponde con el número de red configurado toma parte en el área (aquí nos referimos al último parámetro editado en el comando de network)

Paso 5

Un router ID es requerido para cada router para participar en una red OSPF. Una dirección IP es utilizada como un router ID, ya sea definida manualmente o automáticamente configurada por el router. Se recomienda que el router ID sea ingresado manualmente por razones de claridad en la documentación de red y en situaciones en las cuales exista un desperfecto. Cuando no se configura un router ID, el router selecciona la dirección IP más alta que esté configurada en una de sus interfases. En esta etapa, esta dirección IP puede ser cambiada, quizá debido a un

cambio de diseño, aunque esto podría causar un comportamiento raro y difícil de localizar en la red. Puesto que no existe un comando específico para configurar el router ID manualmente, el siguiente procedimiento es el que se utiliza generalmente.

En lugar de utilizar la dirección IP de una interfase existente, una interfase de loopback se puede utilizar para este propósito. Puesto que esta no es una interfase física, sino que es una interfase virtual, esta nunca estará fuera de servicio.

En el caso de Cisco, el proceso de OSPF escoge la dirección IP con el valor numérico más alto asignado a una interfase en el router. Si el proceso de OSPF encuentra una interfase de loopback , no obstante , OSPF da a la dirección de la interfase de loopback preferencia ante cualquier otra dirección IP que encuentre. Esto se debe a que la interfase de loopback no puede ser influenciada por problemas físicos (diferente situación en una interfase ya sea Ethernet o Serial, porque estas si se ven afectadas por problemas físicos) y de esta manera se asegura mayor estabilidad en el proceso de ruteo. Cuando ninguna de estas opciones es utilizada y ningún router ID es configurado, el router selecciona la dirección IP más alta configurada en el router como su router ID.
Para configurar una interfase loopback, se utiliza los siguientes comandos:

router (config) #interfase loopback "número de interfase"
router (config-if) # ip address "dirección ip" "máscara de subred"

4.1.4 Configuración de OSPF en múltiples áreas

En el punto pasado tratamos acerca de la configuración de un router en OSPF dentro de una sola área. En este punto explicaremos algunos términos de OSPF dentro de una red de varias áreas.

Cuando el número de routers en un área de OSPF crece, llega a ser necesario limitar la cantidad de LSAs producidos por los routers para mantener la convergencia y estabilidad razonable dentro de las fronteras. Esto se logra dividiendo un área grande en múltiples áreas, además de, restringir los LSA a su propia área.
Las razones principales para crear áreas son las siguientes:

1. Reducir el número de LSAs que se envías entre los routers.
2. Reducir el tamaño de la base de datos de link-state.
3. Reducir el numero de repeticiones del algoritmo SPF
4. Reducir el tamaño de las tablas de ruteo a través del uso de rutas resumidas entre áreas.

4.1.4.1 Múltiples áreas

Cuando se crean múltiples áreas en OSPF, una red jerárquica se crea, en la cual diferentes áreas forman límites con otras áreas (ver figura 4.8). Dentro de cada límite, los routers comparten la misma base de datos de

link-state. Routers especiales en los límites reciben información acerca del mundo exterior del área y la pasan dentro del área y por lo tanto los routers pueden aprender acerca de rutas fuera del área. La forma en que estos datos son pasados a través y el tipo de datos reenviados depende del tipo de área en que se encuentre el router.

A cada área se le asigna un número único, que se le llama área ID, que sirve como identificador para las otras áreas. Los números pueden ser arbitrariamente números o direcciones IP. Puesto que las áreas usualmente son diseñadas junto con el diseño de espacios de direcciones IP, esto puede ser muy favorable el utilizar las direcciones IP de una red asignadas al área como su "área ID". El área más alta en la jerarquía es un caso especial y debe siempre tener el número 0. Esto es porque el área 0 debe estar conectada directamente a todas las demás áreas (ver figura 4.9)

Fig. 4.8 Una red básica de OSPF con áreas

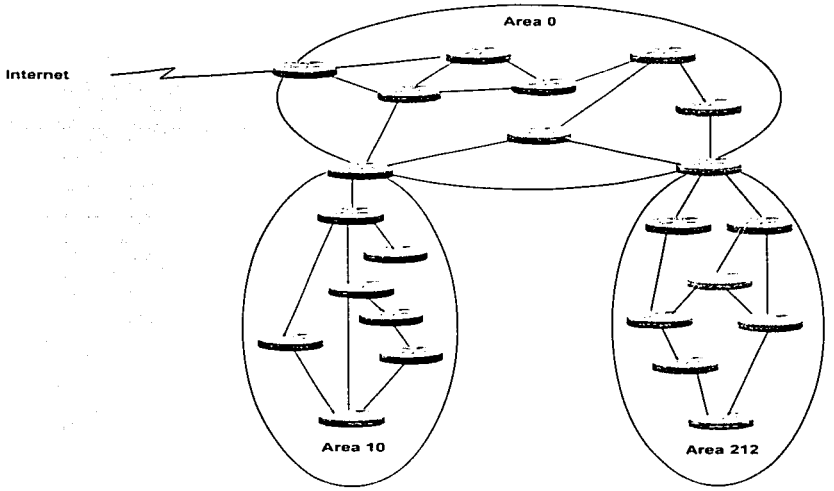
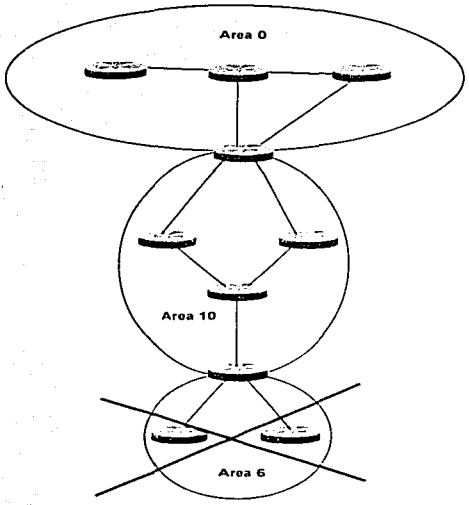


Fig. 4.9 Todas las áreas deben estar conectadas al área central



Esto también debe "sumarizar" toda la información de ruteo de todas las áreas y pasarla a las otras áreas. Por esta razón el área 0, no debe ser dividida en múltiples partes (ver figura 4.10). Las áreas no pueden tener enlaces directos entre una y otra, llamadas puertas traseras, ya que la jerarquía puede ser rota (ver figura 4.11)

Tres principales tipos de información de tráfico son tratados dentro del AS (Sistema Autónomo):

- *Intra-área* Es el tráfico que permanece dentro de un área y describe la información de un área.
- *Inter-área* Es el tráfico que se mueve a través de las áreas y tiene información acerca de otras áreas para el área en cuestión.

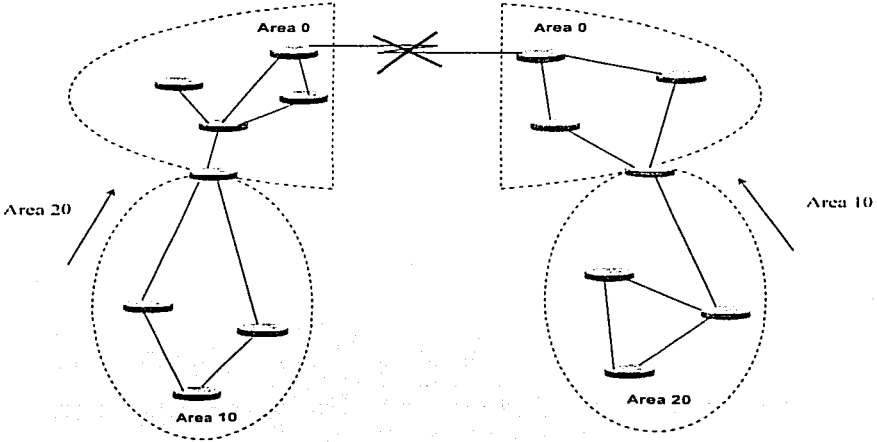
Existe una información especial del tipo Inter-área:

"*Virtual links*" Para evitar que se divida el área 0, un "virtual link" puede ser hecho a través de otra área (ver figura 4.12). El virtual link es terminado en ambas partes del área 0 y atraviesa la otra área sin interactuar con los routers en el área que no es la cero. De esta forma el área 0 aun puede actuar como una sola área contigua.

- *Externo* Es el tráfico que se mueve entre el AS (Sistema Autónomo) bajo el protocolo OSPF y un AS diferente

Para ser capaz de formar esta red jerárquica y diferenciar entre los tres tipos de tráfico, OSPF ofrece tipos de paquetes y routers, los cuales trabajan juntos para formar el AS.

Fig. 4.10 El área 0 no debe estar dividida



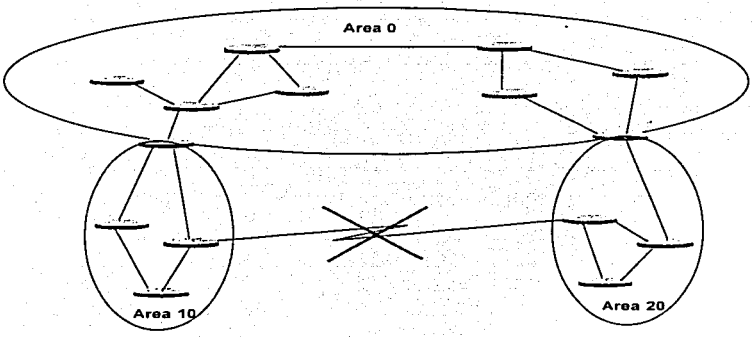


Fig. 4.11 No pueden existir puertas traseras entre áreas

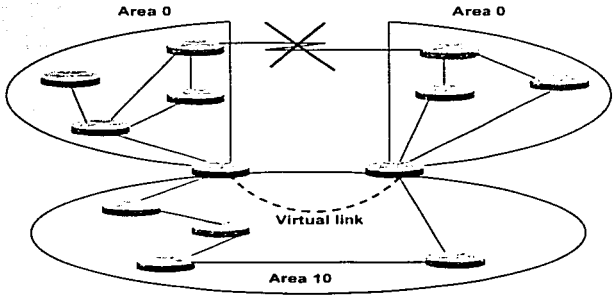


Fig. 4.12 Un virtual link conectando un área 0 particionada

4.1.4.1.1 Tipo de áreas en OSPF

La tabla 4.1da una visión general de los tipos de área de OSPF.

Tipo de área OSPF	Descripción
Area estándar	Esta área es la que se describe al principio del capitulo. Todas las otras áreas están basadas en un área por defecto de OSPF, pero restringen cierto tipo de tráfico u ofrecen servicios extra.
Area 0 (Area de backbone)	Esta área enlaza todas las otras áreas, e intercambia resúmenes de rutas y de datos de un área a otra.
Area "Stub"	Esta es un área que recibe actualizaciones acerca de todas las redes en el AS, pero no recibe las de los enlaces externos que el AS podría tener (LSAs tipo 4 y 5). Los routers utilizan una ruta por defecto de 0.0.0.0 para llegar a las redes externas. ABR. Para llegar a ser un área "stub" se debe tener el siguiente criterio: • Los routers deben de programarse para llegar a ser un router "stub", anunciar esto en los paquetes "Hello", y solamente crear adyacencias con otros routers "stub" • Los "virtual link" no pueden existir en áreas "stub", ya que estas tienen conexiones en otras áreas. • No pueden existir routers ASBR en un área "stub". Esto se debe a que los LSAs tipo 4 y 5 que los ASBR necesitan no son propagados dentro del área. • Puesto que en este tipo de áreas solo puede ser configurada una ruta por default, las áreas "stubby" solamente pueden utilizar uno de los ABRs para conectar hacia los enlaces externos. El área "stub" es creada para reducir el tamaño de la base de datos de "link-state" al remplazar las rutas externas con una sola ruta por default de 0.0.0.0 hacia el ABR. El ABR en turno sabe a cual ASBR reenviar los datos.
Area "Totally Stubby"	Esta también es un área "stub", además con la excepción de que tampoco acepta rutas hacia otras redes en otras áreas, (LSAs tipo 3, 4 y 5). Se debe tener el mismo criterio que se sigue en las áreas "stub". En otras palabras, los routers que se encuentran en un área "totally stubby" solamente saben de las redes

Tipo de área OSPF	Descripción
	que se encuentran en su propia área, y se confía en el ABR para reenviar los datos a otras áreas, y redes externas. Este método impulsa a reducir la carga en los routers.
Area "No-So-Stubby" (NSSA)	Este tipo de área es como un área "stub", pero este tipo de área soluciona el asunto de no ser capaz de conectarse a redes remotas desde un área "stub". El área "stub" utiliza una ruta por defecto para conectar todos los sitios externos. Este tipo de área no permite un ASBR, ya que los LSAs del tipo 4 y 5 no son permitidos en estas áreas. Para solucionar esto, un ASBR puede ser programado para enviar LSAs del tipo 7, los cuales si son aceptados en esta área especial del tipo "stub". Los LSA tipo 7 son anunciados a través del área NSSA, así que todos los routers saben acerca de las conexiones externas. El NSSA ASBR tiene la opción de permitir al ABR el propagar los LSAs tipo 7 dentro del resto de las redes como LSAs tipo 5, pero esto en los router viene deshabilitado por default. Las alternativas para utilizar una NSSA son: • Permitir LSAs tipo 5, y esto trae como consecuencia que esta área se convierta en un área estándar, pero con el requerimiento de routers más potentes. • Utilizar otro protocolo de ruteo a través de lo que será la NSSA, y recordando que es un enlace externo, desde el punto de vista del área cero.

En las figuras 4.13, 4.14, 4.15 y 4.16 podemos observar los diferentes tipos de áreas que pueden existir en una red bajo el protocolo OSPF.

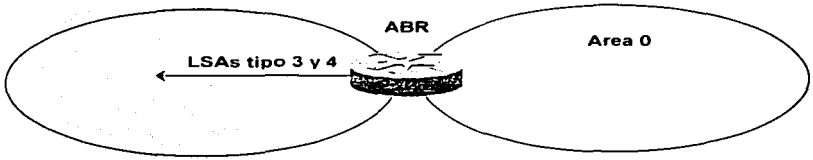


Figura 4.13 Area de OSPF estándar

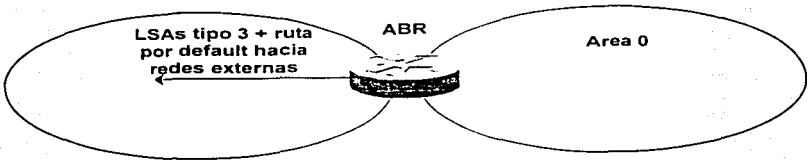


Figura 4.14 Area de OSPF "stubby"

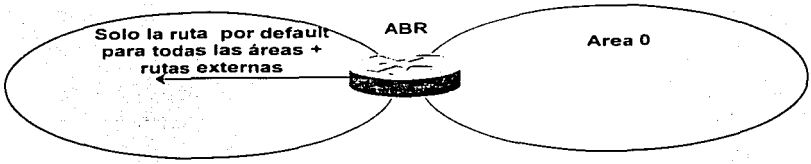


Fig. 4.15 Area de OSPF "Totally Stubby"

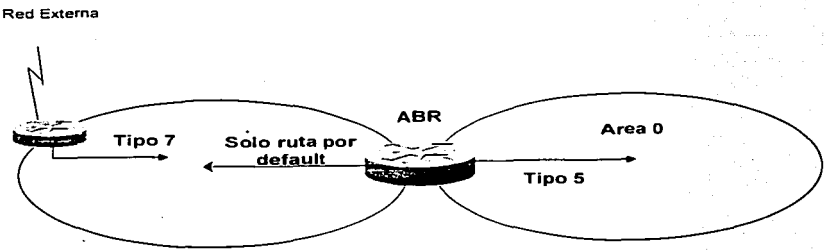


Figura 4.16 Area de OSPF "No so stubby"

4.1.5 Sumarización de rutas

En contraste con otros protocolos (como IGRP y RIP), OSPF fue diseñado con VLSM y CIDR: Cuando es combinado con áreas "stubby", "totally stubby", y "NSSA", OSPF puede reducir el porcentaje de tráfico de actualizaciones de ruteo y el tamaño de la base de datos de"link-state" considerablemente (ver figura 4.17). Si una red ha sido diseñada bien, es posible asignarle un rango continuo de direcciones IP a un área y dejar que el ABR anuncie este rango solamente a el área 0 en un solo anuncio (y viceversa).

La sumarización también puede incrementar la estabilidad del proceso de ruteo, puesto que los routers en un área no necesitan saber todo lo que existe en otra área. Si una red falla en un área sumariada, el resumen de rutas permanece igual y los routers en las otras áreas no tienen que correr el algoritmo SPF.

Si dos áreas están conectadas a través de dos o más ABRs, se debe de tener cuidado cuando se sumariza. Puesto que los ABR no anuncian la métrica exacta a cada red, es imposible, bajo esta condición, que los routers encuentren el camino óptimo hacia una de las redes en la sumarización.

¿Qué pasa si existen múltiples rutas de un área hacia otra? ¿Cómo el router determina la mejor ruta?

Esto se hace al utilizar el "costo" de la ruta, el cual es determinado de la siguiente manera:

Rutas "Inter-area" sumariadas:
Un costo total de una ruta "Inter-area" es la suma del "costo" de la ruta sumariada, más el "costo" de la ruta hacia el ABR que anuncia la ruta.

Rutas externas:
Las rutas externas vienen en dos tipos, E1 y E2. Estas rutas son anunciadas por el ASBR, y pueden ser configurados para enviar ya sea el tipo E1 o el tipo E2.

- Las rutas E1 tienen un "costo" que es la suma del "costo" de las rutas externas, y el "costo" de las áreas cruzadas dentro de la red. Este es un método muy útil para aplicar si existen múltiples routers ASBR, como el router tratara de encontrar la mejor ruta externa también tomará en consideración el "costo" de la red que esta cruzando.
- Las rutas E2 no contienen el "costo" de la red que están cruzando. Simplemente expresan el "costo" externo. Esto se puede utilizar cuando solamente existe un solo ASBR. Este tipo de ruta externa esta por defecto en los equipos, y preferida por un router que trata de encontrar una ruta con el mejor "costo" si existen múltiples áreas.

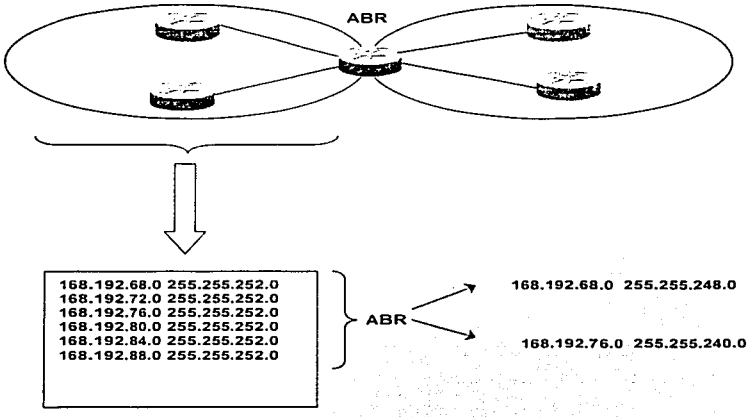


Fig. 4.17 Sumarización entre áreas

4.1.6 Configuración de ABRs y ASBRs en OSPF

Hacer a un router ABR o ASBR no requiere el uso de algún comando en especial, el router toma este rol por las virtudes del área a la cual esta conectado (ver figura 4.18). Los pasos básicos para configurar OSPF en un router son los siguientes (estos pasos también se mencionan en el punto 4.1.3):

1. Habilitar OSPF como sigue:
   router (config) #router OSPF "process-ID"
2. Configurar cada red IP en el router que toma parte en la red OSPF:
   Identificar en el área cada una de las redes que le pertenecen. Cuando se t tiene que configurar múltiples áreas de OSPF, se tiene que estar bien seguro que se asocian las direcciones de las redes correctas con el "area ID" del área de la cual serán parte.

Router (config-router) **#network** *address wildcard-mask area "area-ID"*

3. Si el router tiene una o más interfases conectadas a una red no OSPF, se tiene que realizar configuración adicional, puesto que el router ahora ha tomado el rol de un ASBR. Esta configuración adicional se refiere a que el router tendrá configurado la redistribución de información de rutas no OSPF.

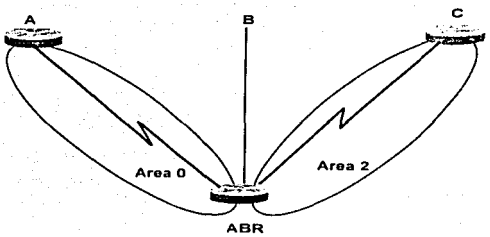


Fig. 4.18 Dos áreas conectadas por un ABR

4.1.7 Configuración de la sumarización de rutas

Con OSPF, la sumarización esta apagada por default. Para configurar la sumarización de rutas en un ABR, se tienen estos pasos:

1. Configurar el protocolo OSPF como se muestra en los puntos 4.1.3 o 4.1.6
2. Tener las rutas sumariadas en el ABR para un área específica antes de inyectar estas dentro de otra área, esto se realiza mediante el siguiente comando :
   Router (config-router) ·**area** "area-ID" **range** "address mask"

donde: "area-ID" es el identificador de el área y nos indica cuales rutas serán sumariadas, "address" es el resumen de direcciones asignado para un rango de direcciones , y "mask" representa la máscara de subred IP utilizada para el resumen de ruta.

Para configurar la "sumarización" de rutas externas en un router ASBR (ver figura 4.19) se utilizan los siguientes pasos:

1. Configurar el protocolo OSPF como se indica en los puntos 4.1.3. o 4.16
2. Configurar el ASBR con los siguientes comandos para sumariar rutas externas antes e inyectarlas dentro del dominio de OSPF:
   router (config-router) **#summary-address** "address" "mask "

donde: "address" es el resumen de direcciones que está designado para un rango de direcciones, y "mask" es la máscara de subred IP utilizado para la "sumarización" de rutas.

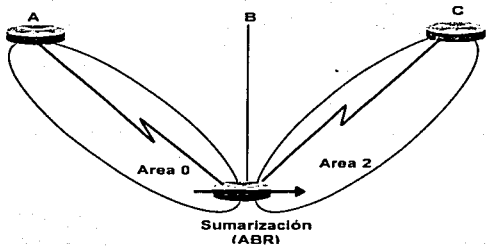


Fig. 4.19 un ejemplo de configuración de sumarización de rutas entre dos áreas

4.1.8 Configuración de áreas "Stub" y "Totally Stubby"

Un área puede ser configurado como área "stub" o "totally stub" (ver figura 4.20) con los siguientes pasos:

1. Configurar el protocolo como se menciona en el punto 4.1.6.
2. Definir un área como "stub"/"totally stubby" al agregar el siguiente comando a cada router dentro del área:

router (config-router) **#area** "area-ID" **stub [no summary]**

donde: "area-ID" es el identificador para el área "stub"/"totally stubby" el cual puede ser un valor decimal o una dirección IP, y **no-summary** es una opción para crear un área "totally stub". Al agregar **no-summary** previene a un ABR de enviar cualquier anuncio "summary-link" hacia un área "stub". Esto se puede configurar solamente sobre los ABRs que están conectados a áreas "totally stub".

3. Este paso es opcional para los ABRs solamente y define el costo del "default route" que es inyectado en las áreas "stub/totally stubby". Se utiliza el siguiente comando:

Router (config-router) **#area** "area-ID" **default-cost** cost

donde: "area-ID" es el identificador para el área "stub", el cual puede ser un valor decimal o una dirección IP, y "cost" es el costo para la síntesis de rutas de default. Utilizadas en las áreas "stub"/"totally stubby". El valor puede ser un número de 24 bits, con un valor como costo de 1 por defecto.

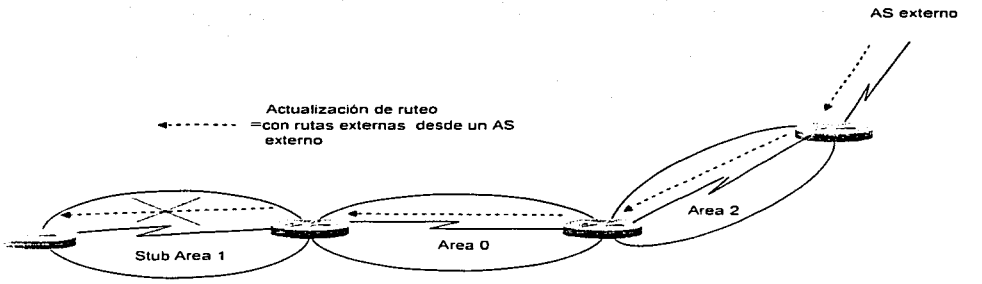


Fig. 4.20 un ejemplo de la configuración de un área "stub" en OSPF

4.1.9 Configuración de un área "Not So Stubby" (NSSA)

Los pasos siguientes son los que se utilizan para configurar un área NSSA en OSPF (ver figura 4.21):

1. Configurar OSPF (como se describe en el punto 4.1.6) en el ABR conectado al NSSA.
2. Configurar el área como NSSA utilizando el siguiente comando:

router (config-router) **#area** "area-ID" nssa

Esto trabaja solamente si cada router en la misma área esta de acuerdo que el área es del tipo NSSA ; Esto es necesario en orden para que los routers sean capaces de comunicarse uno con otro.

3. Existe una opción que habilita el control sobre la "sumarización"o filtrado durante la traducción. Las siguientes líneas muestran como un router "X" sumariza rutas utilizando este comando:

router (config-router) **#summary-address** address *mask prefix mask* ***(not-advertise)***

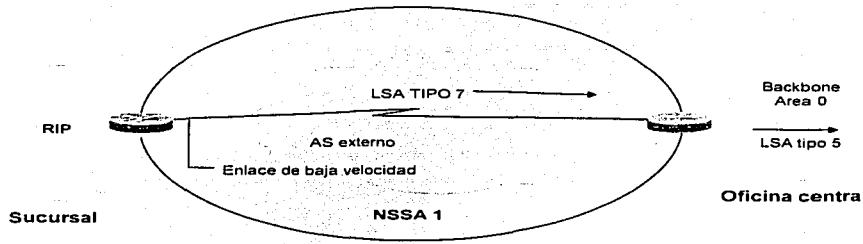


Fig. 4.21 Visión general de una NSSA

4.1.10 Configuración de "virtual-links"

Un enlace virtual (virtual-link) puede ser configurado (ver figura 4.22) utilizando los siguientes pasos:

1. Configurar el protocolo OSPF como se indica en el punto 4.1.3
2. Crear el "virtual-link" en cada router que será parte de este.

Estos routers siguen:

- Al ABR que conecta el área remota a el área de transito
- Al ABR que conecta el área de tránsito a el área de backbone

Se utiliza este comando:
router (config-router) **#area** "area-ID" **virtual-link** "router-ID"

Donde "area-ID" es el identificador del área del área de transito para el "virtual-link" (el formato puede ser decimal o punto y decimal, el cual no tiene un valor de default) y "router-ID" es el identificador del router del "virtual-link" vecino.

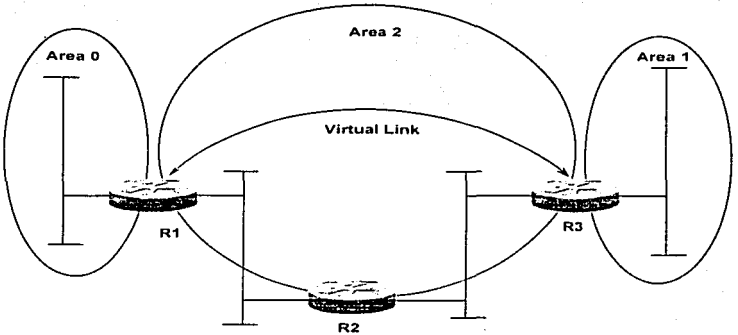


Fig. 4.22 Un Virtual-link conectando el Area 1 a el Area 0 a través del Area 2

4.2 Set de pruebas

Para la implementación del proyecto de re-estructuración se instaló una maqueta simulando un ambiente real de producción. En esta maqueta se probaron los siguientes puntos:

1.- Inspección física de los equipos Foundry modelos NetIron 800 y BigIron 8000 (fuentes redundantes, tarjetas de administración redundantes, capacidad hot-swap de las tarjetas de puertos, actualización de las versiones de software a las versiones de producción).
2.- Conexión de los equipos de acuerdo al diseño de la maqueta. Esta maqueta representa el diseño final del backbone propuesto.
3.- Diseño e integración de las redes de rectoría y los ruteadores principales de Red UNAM al dominio de OSPF en un escenario de alta disponibilidad.
4.- Redistribución de rutas estáticas e IGRP de los ruteadores Cisco a los switches Foundry.
5.- Redistribución de rutas estáticas y RIP de los switches Foundry a los ruteadores Cisco.
6.- Diseño y definición de las áreas de OSPF e interoperabilidad entre ruteadores Cisco y switches Foundry
7.- Diseño de la configuración de BGP4 e interoperabilidad entre ruteadores Cisco y switches Foundry en un ambiente "full mesh" de IBGP.

8.- Diseño de la configuración de IP Multicast e interoperabilidad entre ruteadores Cisco y switches Foundry con los protocolos de PIM DM y SM.
9.- Diseño de la configuración de IP Multicast e interoperabilidad entre ruteadores Cisco y swtiches Foundry entre distintos sistemas autónomos con los protocolos de MSDP y MBGP.
10.- Ruteo de redes IPX a través del backbone probando la interoperabilidad entre ruteadores Cisco y switches Foundry.
11.- Escenario de alta disponibilidad para la red de San Pedro Mártir.

4.2.1Escenarios de pruebas y resultados.

1.- Inspección física de los equipos Foundry modelos NetIron 800 y BigIron 8000 (fuentes redundantes, tarjetas de administración redundantes, capacidad hot-swap de las tarjetas de puertos, actualización de las versiones de software a las versiones de producción).

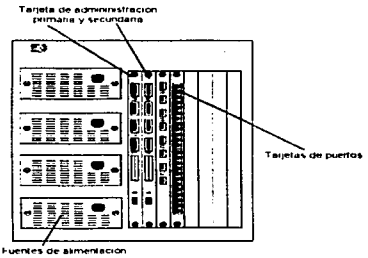


Fig. 4.23 Vista frontal de un Foundry Netiron 8000.

Los resultados de las pruebas físicas de los equipos fueron satisfactorios. Se removió la tarjeta de administración principal en dos equipos simulando una falla de la misma. En cada caso el equipo detectó que la tarjeta principal había fallado y procedió a la activación de la tarjeta secundaria. En los otros dos equipos, la simulación del fallo se realizó por software deshabilitando la tarjeta principal. De la misma manera, el equipo detectó la falla y procedió a la activación de la tarjeta secundaria.
El tiempo de recuperación del servicio para todos los casos fue menor a 30 segundos.
Las fuentes de los equipos fueron conectadas y probadas para verificar la funcionalidad de balanceo de carga y redundancia, observando en todos los casos un funcionamiento correcto.

El funcionamiento de cada uno de los puertos fue revisado a nivel físico sin observarse ninguna eventualidad.
Se instaló y revisó la memoria de los cuatro switches de CORE BigIron 8000 y NetIron 800, verificando que cada uno de ellos reconociera los 512 MB de DRAM.
De estas pruebas resultó el cambio por garantía de una tarjeta de administración que presentaba fallas intermitentes en el proceso de failover ya que en algunas ocasiones lo realizaba correctamente y otras no, así como en el cambio de un chassis cuyo ventilador realizaba mucho ruido.

2.- Conexión de los equipos de acuerdo al diseño de la maqueta. Esta maqueta representa el diseño final del backbone propuesto.

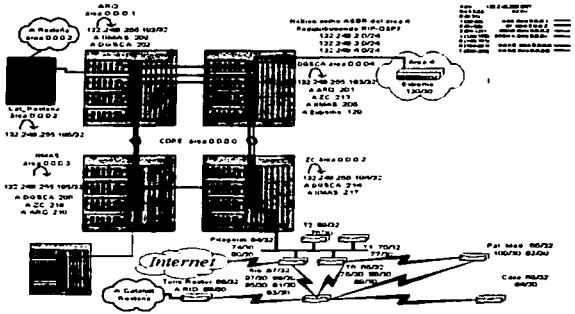


Fig. 4.24 Maqueta de pruebas.

El diagrama de la maqueta del backbone propuesto está integrado por los cuatro switches Foundry de CORE (2 NetIron 800 y 2 BigIron 8000) interconectados a través de un área 0 de backbone por medio de enlaces troncales de Gigabit Ethernet en las trayectorias ARQUITECTURA-IIMAS, IIMAS-DGSCA y DGSCA-ZC. Estos enlaces troncales fueron probados para verificar su capacidad de balanceo de carga y redundancia. El fallo de alguno de los enlaces miembros de la troncal ocasionaba una suspensión en el servicio menor a 3 segundos.
La interconexión inicial de los switches Foundry a través de OSPF resultó satisfactoria.
3.- Diseño e integración de las redes de rectoría y los ruteadores principales de Red UNAM al dominio de OSPF en un escenario de alta disponibilidad.

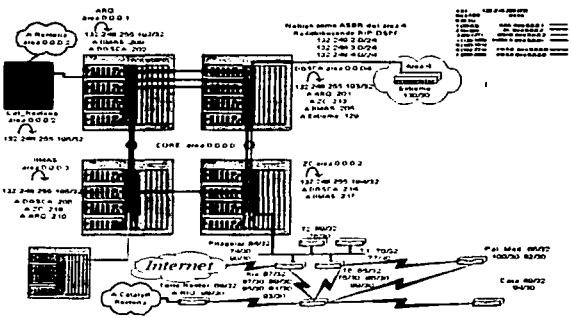


Fig. 4.25 Integración de OSPF

La integración de las redes de rectoría a un esquema de alta disponibilidad representaba un problema de diseño. Dado que las redes de rectoría tiene dos conexiones físicas al backbone en diferentes nodos fue necesario incluir al switch Catalyst de Torre como un segundo ABR entre el área 0 y el área 5 definida para estas redes. De esta manera se evitó el uso de Virtual-links para el área 5. Con este diseño, las redes de rectoría tienen dos maneras de salir al backbone, una a través del switch de Torre y la otra a través del switch Foundry de ZC. La falla de cualquier enlace WAN en el área 5, a excepción del enlace a la casa del rector, no suspende el servicio hacia ninguna de las redes LAN de rectoría.
Para la inclusión de los equipos que brindan servicio en esta área al dominio de OSPF se configuraron interfaces de loopback que proveen una mayor estabilidad y se numeraron todos los enlaces WAN sin afectar el direccionamiento actual que utilizan las redes LAN. El tiempo de convergencia de la topología en caso de la falla de algún equipo o enlace WAN no fue nunca superior a los 10 segundos.

4.- Redistribución de rutas estáticas e IGRP de los ruteadores Cisco a los switches Foundry.

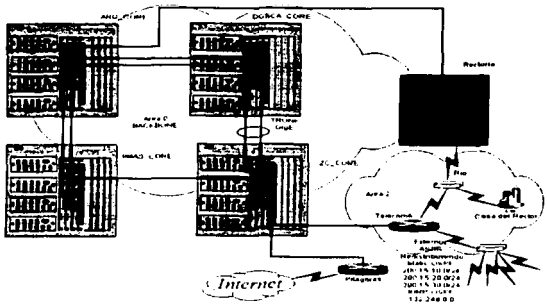


Fig. 4.26 Redistribución de ruteo.

De acuerdo al diagrama anterior, se configuraron a los ruteadores Cisco para que redistribuyeran rutas estáticas e IGRP a los switches Foundry por medio de OSPF. La prueba se realizó satisfactoriamente inyectándolas como tipo External Type 1 y External Type 2. Al mismo tiempo se probó exitosamente. que el resto de los switches del backbone vieran estas redes a través de los dos ruteadores ABR configurados para el área alternando fallas en cada uno para probar la redundancia. Con esta configuración quedó validado que el área de rectoría tuviera conexiones duales al backbone para proveer redundancia en caso de falla.

5.- Redistribución de rutas estáticas y RIP de los switches Foundry a los ruteadores Cisco.

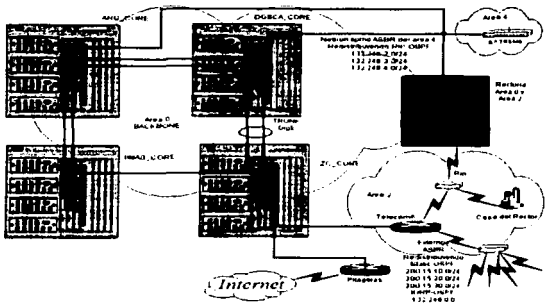
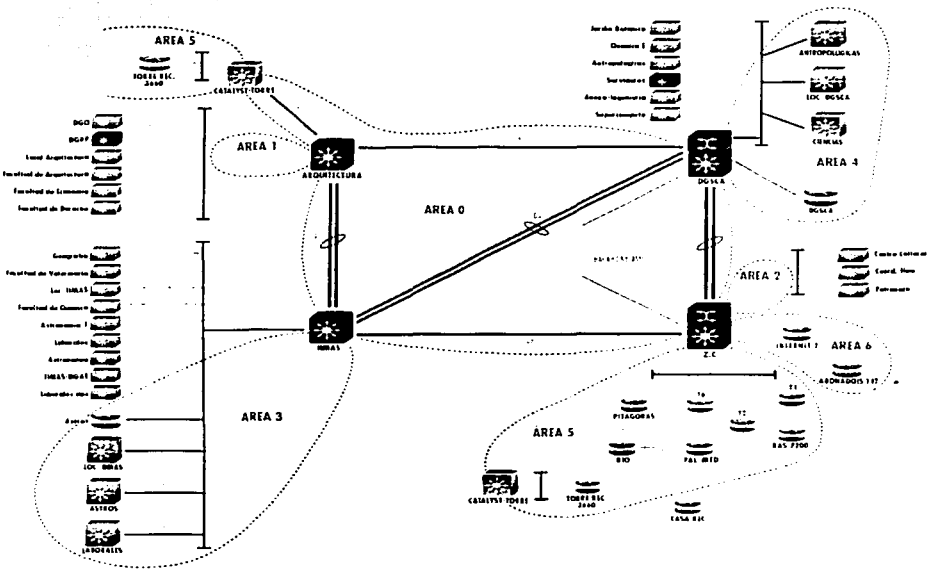


Fig. 4.27 Redistribución de ruteo incluyendo RIP.

De acuerdo al diagrama anterior, se configuraron los switches Foundry para que redistribuyeran rutas estáticas y RIP a los ruteadores Cisco por medio de OSPF. LA prueba se realizó satisfactoriamente inyectándolas como tipo External Type 1 y External Type 2. Al mismo tiempo se probó exitosamente que el resto de los switches de la maqueta vieran estas redes redistribuidas en su tabla de ruteo con la métrica adecuada.

6.- Diseño y definición de las áreas de OSPF e interoperabilidad entre ruteadores Cisco y switches Foundry

Fig. 4.28 Diseño del esquema de OSPF.



De las pruebas realizadas anteriormente surgió el diseño de las áreas propuestas. El diseño está compuesto por un área principal que es el área 0 o

backbone a la que los cuatro switches Foundry de CORE y el switch Cisco Catalyst de Rectoría van conectados. Cada uno de estos equipos cumplen las funciones de ABR´s y en algunos casos de ASBR's para las distintas áreas a las que pertenecen. Hay 6 áreas que se conectan al área 0 distribuidas de la siguiente manera:

El Área 0 está asignada para los equipos del Backbone en GigabitEthernet.

El Área 1 está reservada para los equipos del nodo principal Arquitectura.

El Área 2 está reservada para los equipos del nodo principal Zona Cultural.

El Área 3 está asignada a los equipos del nodo principal IIMAS.

El Área 4 está asignada a los equipos del nodo principal DGSCA.

El Área 5 está asignada a los Routers con enlaces WAN hacia los ISP's de la UNAM, dependencias fuera del campus, instituciones externas y la red de Rectoría

El Área 6 está asignada a los routers que conforman la red de Internet2 de la UNAM así como de los routers que se conectan a Internet2 a través de la UNAM.

Todas estas áreas están configuradas como áreas normales. La definición inicial incluía áreas del tipo NSSA y STUB para limitar la cantidad de LSA's que recibieran del backbone, y sumarización tanto para limitar el impacto fuera de su propia área de redes que estuvieran oscilando como para disminuir el tamaño de la tabla de ruteo. Sin embargo, en la práctica, dado el esquema de direccionamiento actual de Red UNAM, resulta prácticamente imposible realizar una sumarización eficiente. Igualmente se encontró que la mayor parte de los equipos de distribución actuales marca 3COM, de Red UNAM no tienen la capacidad de hablar el protocolo de OSPF y algunos de los que sí tienen esta capacidad, no soportan la configuración de áreas NSSA. El área 5, que cuenta con equipos que soportan áreas NSSA, no fue definida así dado que por definición las áreas NSSA bloquean los LSA's tipo 4 y 5 evitando que las redes redistribuidas a OSPF provenientes de otras áreas sean aprendidas en los ruteadores internos del área 5. Es la recomendación de este documento reordenar el direccionamiento en Red UNAM para permitir la sumarización de redes inter-areas como una buena práctica a futuro que permita la optimización de los recursos de la red así como el minimizar el impacto de redes inestables en Red UNAM. Por último, la interoperabilidad entre los ruteadores Cisco y los switches Foundry fue probada exitosamente, habiéndose probado distintos tipos de configuraciones que incluían áreas de tipo normales, STUB y NSSA.

7.- Diseño de la configuración de BGP4 e interoperabilidad entre ruteadores Cisco y switches Foundry en un ambiente "full mesh" de IBGP.

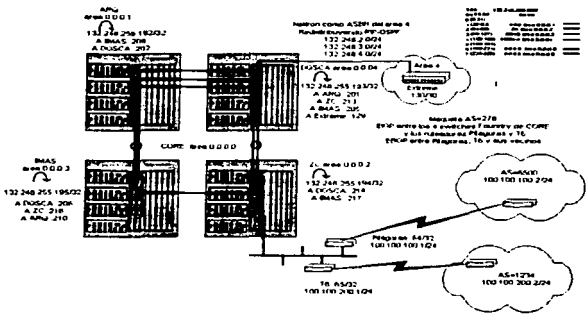


Fig. 4.29 configuración de BGP4

La configuración de BGP4 fue realizada en un ambiente "full mesh" de IBGP descrito en el diagrama anterior. Se simularon tres sistemas autónomos. Los cuatros switches Foundry de CORE fueron configurados en uno de ellos estableciendo relaciones de IBGP entre si y contra dos ruteadores Cisco de orilla que a la vez tenían relaciones de EBGP con los dos sistemas autónomos restantes. Cada uno de los equipos corriendo BGP fueron configurados para inyectar NLRI's a sus vecinos. En las tablas de BGP se verificaron que todos los NLRI's fueran insertados de manera adecuada, revisando los valores de métricas, AS_PATH, weight, local preference, NEXT HOP, etc.. La tabla de ruteo IP también fue verificada para que incluyera la información relevante al protocolo de BGP. Este documento recomienda la utilización de Route Reflectors en el futuro para disminuir la cantidad de sesiones de IBGP que corren en el sistema autónomo de la UNAM. Con un total de 8 equipos corriendo IBGP se necesitan, sin Route Reflectors, 28 sesiones para establecer el "full mesh". Cabe mencionar que el uso de Route Reflectors no se incluye en el diseño inicial para no introducir un nivel de complejidad extra al proceso de implementación.

8.- Diseño de la configuración de IP Multicast e interoperabilidad entre ruteadores Cisco y switches Foundry con los protocolos de PIM DM y SM.

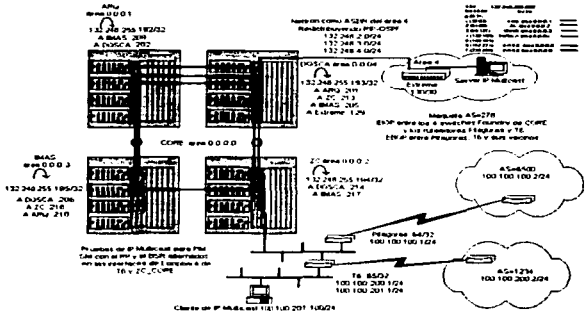


Fig. 4.30 Pruebas de multicast.

La primera prueba que se realizó fue con PIM DM. En esta prueba se ubicaron los clientes y el servidor de multicast de acuerdo al diagrama anterior. El resultado de esta prueba fue satisfactorio permitiendo a los clientes acceder a los flujos del servidor. La segunda prueba fue con el protocolo de PIM SM. En esta prueba el Bootstrap Router y el RP fueron alternados entre el ruteador cisco y un switch Foundry pudiéndose conectar en ambas ocasiones. Cabe destacar que la redistribución de DVMRP, único protocolo de multicast soportado por los actuales switches de acceso marca 3COM, a PIM no está soportada en los switches Foundry, por lo que las dependencias que deseen conectarse a las redes de multicast tendrán que hacerlo por medio del protocolo PIM SM seleccionado por la UNAM.

9.- Diseño de la configuración de IP Multicast e interoperabilidad entre ruteadores Cisco y swtiches Foundry entre distintos sistemas autónomos con los protocolos de MSDP y MBGP.

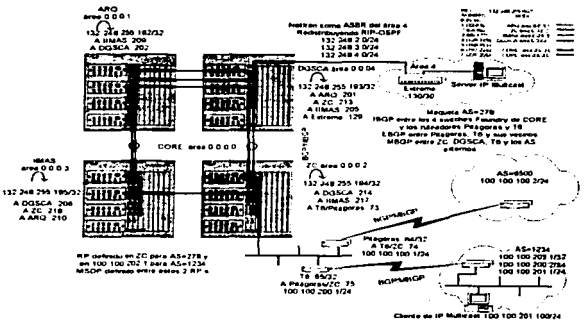


Fig. 4.31 Integración de multicast.

Esta configuración utilizó una variante del diagrama del punto número 8. Se crearon dos sistemas autónomos cuyos ruteadores de borde eran Foundry y Cisco. En cada sistema autónomo se configuró PIM SM y se estableció una relación de peers entre los RP's de cada sistema vía MSDP. Una vez hecha esta configuración se prendió MBGP entre los sistemas y se conectaron servidores y clientes en cada uno de ellos. Los clientes fueron capaces de acceder a los flujos de multicast de servidores en el otro sistema autónomo sin ningún contratiempo. Las versiones de software utilizadas fueron: 7.5.2 en los equipos Foundry y 12.2.8 en los ruteadores Cisco. Previamente se habían probado versiones 12.1 y 12.0 en los ruteadores Cisco sin éxito.

10.- Ruteo de redes IPX a través del backbone probando la interoperabilidad entre ruteadores Cisco y switches Foundry.

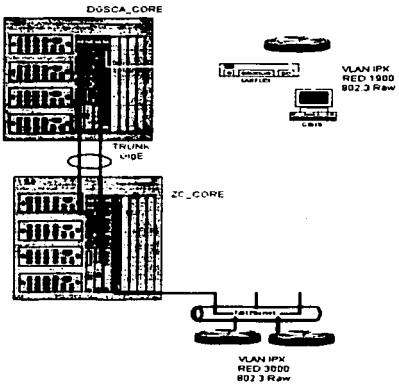


Fig. 4.32 Ruteo de protocolos diversos no IP

El objetivo de esta prueba era rutear redes IPX probando la interoperabilidad entre los switches de distribución 3COM, los switches de CORE Foundry y los ruteadores Cisco.
Se simuló el escenario actual de Red UNAM configurando un equipo 3COM 2500 para que originara una red IPX al switch Foundry de CORE Arquitectura. Este equipo, a su vez, propagaba el anuncio de la red a través del CORE al switch Foundry de ZC. El switch Foundry de ZC tenía un equipo Cisco conectado que veía la red de IPX originada por el 3COM 2500. La conectividad y el ruteo de redes IPX de extremo a extremo, se probó ejecutando PINGs de IPX entre ruteadores Cisco conectados en las distintas puntas.

11.- Escenario de alta disponibilidad para la red de San Pedro Mártir.

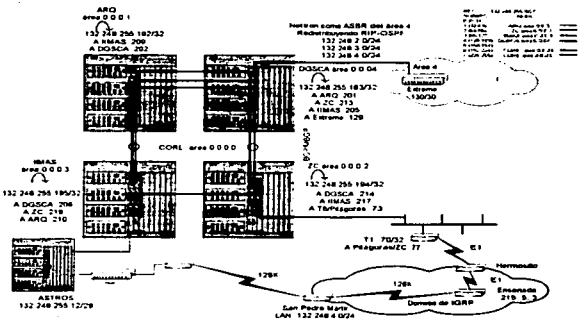


Fig. 4.33 Esquema de alta disponibilidad para redes WAN.

El diagrama anterior muestra la red de San Pedro Mártir. Esta red tiene conexiones duales que van a distintas áreas de OSFP (5 y 3). Al área 5 a través de los equipos de Ensenada, Hermosillo y Telecom1 y al área 3 a través del ruteador Astros1. El objetivo de esta prueba fue encontrar la configuración adecuada que mantuviera la alta disponibilidad y redundancia de esta red. Para este propósito, se configuró un dominio de IGRP entre Hermosillo, Ensenada y San Pedro Mártir con rutas estáticas por default en Hermosillo hacia Telecom1 y en San Pedro Mártir hacia Astros, además de una ruta estática con distancia de 254 de San Pedro Mártir hacia Ensenada. De esta manera, San Pedro Mártir siempre toma Astros como su DG salvo en el caso que el enlace serial entre ellos esté fuera de servicio, donde buscaría a Ensenada como una segunda opción. Para completar el esquema de redundancia, el ruteador de Astros y Telecom1 están redistribuyendo la red de San Pedro Mártir con métrica tipo External Type 1 al dominio de OSPF. Como las redes LAN de Hermosillo y Ensenada no requieren de este tipo de redundancia, únicamente Telecom1 cuenta con rutas estáticas a dichas redes.

4.3 Pasos para la migración del Backbone de RedUNAM

4.3.1. Configuración y puesta a punto del protocolo de ruteo OSPF

El proyecto de reestructuracion del Backbone de RedUNAM contempla la utilización del protocolo OSPF como IGP en un ambiente multiarea mismo que se detalla en los apartados siguientes.

4.3.1.1 Definición y delimitación de las áreas

Inicialmente se propone configurar cuatro áreas y dejar reservados dos identificadores para un futuro. Las cuatro primeras áreas están destinadas para agrupar a los equipos que brindan servicio para redes LAN dentro del campus universitario y las dos restantes para los equipos que brinden servicio a dependencias de la UNAM fuera del campus Universitario, así como instituciones externas. Las áreas estarán delimitadas como se muestra en el siguiente diagrama.

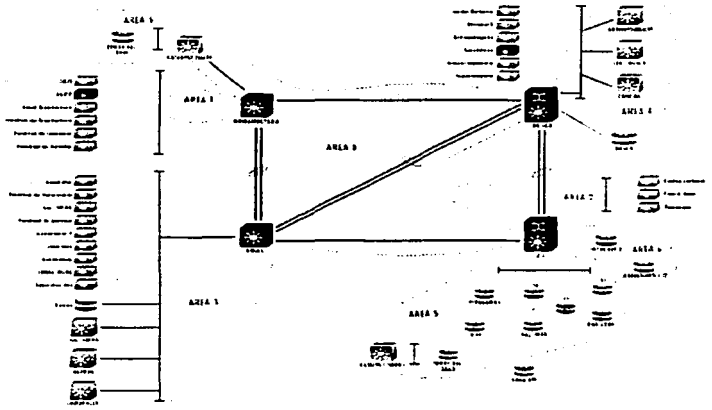


Fig. 4.34 Delimitación de Áreas de OSPF.

Donde:
El Área 0 está asignada para los equipos del Backbone en GigabitEthernet.
El Área 1 está reservada para los equipos del nodo principal Arquitectura.
El Área 2 está reservada para los equipos del nodo principal Zona Cultural.
El Área 3 está asignada a los equipos del nodo principal IIMAS.
El Área 4 está asignada a los equipos del nodo principal DGSCA.
El Área 5 está asignada a los Routers con enlaces WAN hacia los ISP's de la UNAM, dependencias fuera del campus, instituciones externas y la red de Rectoría
El Área 6 está asignada a los routers que conforman la red de Internet2 de la UNAM así como de los routers que se conectan a Internet2 a través de la UNAM.

4.3.1.2 Definición y asignación del direccionamiento para cada área.

Para numerar las redes de los equipos del backbone se ha considerado utilizar la subred 132.248.255.0/24, y aplicarle una nueva máscara de 27 bits, para dividirla a su vez en 8 subredes, cada una se asignará a un área excepto al área 6 ya que esta cuenta actualmente con su propio direccionamiento.
Las subredes resultantes y el área asignada a cada una de ellas se muestra en la siguiente tabla.

Subred	Rango	Área OSPF	Nombre del Área
0	132.248.255.0 - 132.248.255.31	1	Arquitectura
1	132.248.255.32 - 132.248.255.63	2	Z.C.
2	132.248.255.64 - 132.248.255.95	3	IIMAS
3	132.248.255.96 - 132.248.255.127	4	DGSCA
4	132.248.255.128 - 132.248.255.159	5	Routers
5	132.248.255.160 - 132.248.255.191	5	Routers
6	132.248.255.192 - 132.248.255.223	0	Backbone
7	132.248.255.224 - 132.248.255.255	0	Backbone

Tabla 4.2

En la implementación inicial del backbone ninguno de los equipos 3Com (Lanplex 2500 y CoreBuilder 3500) serán incluidos al dominio de OSPF debido a que no soportan o no son lo suficientemente robustos para ello, sin embargo dichos equipos serán configurados en una misma LAN junto con los equipos Foundry de distribución y/o core de su respectivo nodo como se muestra en el diagrama del Backbone, esto con el fin de facilitar su inclusión al domino de OSPF en sus respectivas áreas cuando dichos equipos (Switches 3Com 2500 y 3500) se cambien por otros que si cumplan con los requerimientos para ello.
Para simplificar la administración y brindar mayor estabilidad al proceso de ruteo OSPF, en cada área se tomarán la cantidad necesaria de direcciones comenzando por la IP más alta de la subred asignada, para configurarse en la primer interfaz de loopback de cada equipo, con una máscara de 32 bits, forzando así a que dicha IP se tome como el RouterID. A continuación se detalla la asignación de las ocho subredes creadas.

Subred 0 132.248.255.0/27 -- AREA 1 Arquitectura
La red LAN para los equipos de distribución 3Com y el switch de core Foundry BigIron8000 utilizará la subred 132.248.255.0/28, la siguiente tabla indica a detalle la asignación de las direcciones IP a lo equipos.

Dirección IP	Equipo	Máscara de Red	Configurable
132.248.255.0	NET ID	255.255.255.240	--
132.248.255.1	Lanplex 2500 DGO	255.255.255.240	Actualmente
132.248.255.2	CoreBuilder 3500 DGPP	255.255.255.240	Actualmente
132.248.255.3	Lanplex 2500 Local Arquitectura	255.255.255.240	Actualmente
132.248.255.4	Lanplex 2500 Fac. Arquitectura	255.255.255.240	Actualmente
132.248.255.5	Lanplex 2500 Fac. Economía	255.255.255.240	Actualmente
132.248.255.6	Lanplex 2500 Fac. Derecho	255.255.255.240	Actualmente
132.248.255.7	Libre	255.255.255.240 A futuro	
132.248.255.8	Libre	255.255.255.240 A futuro	
132.248.255.9	Libre	255.255.255.240 A futuro	
132.248.255.10	Libre	255.255.255.240 A futuro	
132.248.255.11	Libre	255.255.255.240 A futuro	
132.248.255.12	Libre	255.255.255.240 A futuro	
132.248.255.13	Libre	255.255.255.240 A futuro	
132.248.255.14	BigIron 8000 Arquitectura (core)	255.255.255.240	Actualmente
132.248.255.15	BROADCAST	255.255.255.240 --	

Tabla 4.3

Todos los equipos 3Com tendrán configurado su *default gateway a* la dirección del BigIron8000 132.248.255.14 y en este último habrá rutas estáticas redistribuyéndose al dominio de OSPF para las subredes 132.248.X.0/24 que se encuentran configuradas en los equipos 3Com.
Se deja libre la siguiente subred para numerar enlaces punto a punto que se creen en un futuro, para numerar una nueva LAN o para asignar más interfaces loopback en caso de ser necesario
- 132.248.255.16/29
Las direcciones de Loopback a configurar cuando algún equipo se integre al dominio de OSPF en el área 1 son:

Dirección loopback	Equipo	Máscara de Red	Configurable
132.248.255.24	Libre	255.255.255.255 A futuro	
132.248.255.25	Libre	255.255.255.255 A futuro	
132.248.255.26	Libre	255.255.255.255 A futuro	
132.248.255.27	Libre	255.255.255.255 A futuro	
132.248.255.28	Libre	255.255.255.255 A futuro	
132.248.255.29	Libre	255.255.255.255 A futuro	
132.248.255.30	Libre	255.255.255.255 A futuro	
132.248.255.31	Libre	255.255.255.255 A futuro	

Tabla 4.4

Subred 1 132.248.255.32/27 – ÁREA 2 ZONA CULTURAL
La red LAN para los equipos de distribución 3Com y el switch de core Foundry NetIron 800 utilizará la subred 132.248.255.32/29, la siguiente tabla indica a detalle la asignación de las direcciones IP a lo equipos.

Dirección IP	Equipo	Máscara de Red	Configurable
132.248.255.32	NET ID	255.255.255.248	--
132.248.255.33	Lanplex 2500 Centro Cultural	255.255.255.248	Actualmente
132.248.255.34	Lanplex 2500 Coord. Humanidades	255.255.255.248 Actualmente	
132.248.255.35	Lanplex 2500 Patronato	255.255.255.248 Actualmente	
132.248.255.36	Libre	255.255.255.248 A futuro	
132.248.255.37	Libre	255.255.255.248 A futuro	

132.248.255.38	NetIron 800 Z.C. (core)	255.255.255.248 Actualmente	
132.248.255.39	BROADCAST	255.255.255.248 --	

Tabla 4.5

Todos los Lanplex tendrán configurado su *default gateway a* la dirección IP del NetIron800 132.248.255.38 y en este último habrá rutas estáticas redistribuyéndose al dominio de OSPF para las subredes 132.248.X.0/24 que se encuentran configuradas en los 3Com.
Se dejan libres las siguientes subredes para numerar enlaces punto a punto que se creen en un futuro, para numerar una nueva LAN (o extender la ya existente) o para asignar más interfaces loopback en caso de ser necesario
- 132.248.255.40/29
- 132.248.255.48/29
Las direcciones de Loopback a configurar cuando algún equipo se integre al dominio de OSPF en el área 1 son:

Dirección loopback	Equipo	Máscara de Red	Configurable
132.248.255.56	Libre	255.255.255.255 A futuro	
132.248.255.57	Libre	255.255.255.255 A futuro	
132.248.255.58	Libre	255.255.255.255 A futuro	
132.248.255.59	Libre	255.255.255.255 A futuro	
132.248.255.60	Libre	255.255.255.255 A futuro	
132.248.255.61	Libre	255.255.255.255 A futuro	
132.248.255.62	Libre	255.255.255.255 A futuro	
132.248.255.63	Libre	255.255.255.255 A futuro	

Tabla 4.6

Subred 2 132.248.255.64/27 -- ÁREA 3 IIMAS
La red LAN para los equipos de distribución 3Com y los switches de distribución y core Foundry BigIron8000 utilizará la subred 132.248.255.64/28, la siguiente tabla indica a detalle la asignación de las direcciones IP a lo equipos.

Dirección IP	Equipo	Máscara de Red	Configurable
132.248.255.64	NET ID	255.255.255.240	--
132.248.255.65	Lanplex 2500 Geografía	255.255.255.240	Actualmente

132.248.255.66	Lanplex 2500 Fac. Veterinaria	255.255.255.240	Actualmente
132.248.255.67	Lanplex 2500 Local IIMAS	255.255.255.240	Actualmente
132.248.255.68	Lanplex 2500 Fac. de Química	255.255.255.240	Actualmente
132.248.255.69	Lanplex 2500 Astronomía1	255.255.255.240	Actualmente
132.248.255.70	Lanplex 2500 Laborales	255.255.255.240	Actualmente
132.248.255.71	Lanplex 2500 Astronomía	255.255.255.240	Actualmente
132.248.255.72	Lanplex 2500 IIMAS-DGAE	255.255.255.240	Actualmente
132.248.255.73	Lanplex 2500 Laborales-dos	255.255.255.240	Actualmente
132.248.255.74	Router Astros1	255.255.255.240	Actualmente
132.248.255.75	BigIron 8000 Local IIMAS (dist.)	255.255.255.240	Actualmente
132.248.255.76	BigIron 8000 Astronomía (dist.)	255.255.255.240	Actualmente
132.248.255.77	BigIron 8000 Laborales (dist.)	255.255.255.240	Actualmente
132.248.255.78	BigIron 8000 IIMAS (core)	255.255.255.240 Actualmente	
132.248.255.79	BROADCAST	255.255.255.240 --	

Tabla 4.7

Todos los Lanplex tendrán configurado su *default gateway* a la dirección IP del BigIron8000 IIMAS de core 132.248.255.78 y en este último habrá rutas estáticas redistribuyéndose al dominio de OSPF para las subredes 132.248.X.0/24 que se encuentran configuradas en los 3Com.
El área 3 cuenta actualmente con cuatro routers internos, por lo que en un principio se necesitan sólo tres IP's para las direcciones de loopback, sin embargo, se van a considerar las direcciones de loopback necesarias para estar listo en el caso de que todos los demás equipos de distribución (Lanplex 2500) sean sustituidos por equipos que si puedan ser incluidos en el dominio de OSPF. Como se menciono al inicio, se tomarán las direcciones IP más altas de cada subred para configurarse en las interfaces de loopback, esto brinda mayor flexibilidad para tomar los boques de IP's que no se requieran como loopback, para utilizarlas en la numeración de enlaces punto a punto o nuevas LAN.

Las direcciones IP de loopback serán configuradas de la siguiente forma:

Dirección loopback	Equipo	Máscara de Red	Configurable
132.248.255.80	Libre	255.255.255.255 A futuro	
132.248.255.81	Libre	255.255.255.255 A futuro	

132.248.255.82	Libre	255.255.255.255 A futuro	
132.248.255.83	Libre	255.255.255.255 A futuro	
132.248.255.84	Libre	255.255.255.255 A futuro	
132.248.255.85	Libre	255.255.255.255 A futuro	
132.248.255.86	Libre	255.255.255.255 A futuro	
132.248.255.87	Libre	255.255.255.255 A futuro	
132.248.255.88	Libre	255.255.255.255 A futuro	
132.248.255.89	Libre	255.255.255.255 A futuro	
132.248.255.90	Libre	255.255.255.255 A futuro	
132.248.255.91	Libre	255.255.255.255 A futuro	
132.248.255.92	Router Astros1	255.255.255.255	A futuro
132.248.255.93	BigIron 8000 Laborales (dist.)	255.255.255.255	Actualmente
132.248.255.94	BigIron 8000 Astronomía (dist.)	255.255.255.255	Actualmente
132.248.255.95	BigIron 8000 Local IIMAS (dist.)	255.255.255.255	Actualmente

Tabla 4.8

Subred 3 132.248.255.96 /27 – ÁREA 4 DGSCA

La red LAN para los equipos de distribución 3Com, los switches de distribución Foundry BigIron8000 y core Foundry NetIron800 así como el swtich Cisco Catalyst de la Fac. de Ciencias utilizarán la subred 132.248.255.96/28, la siguiente tabla indica a detalle la asignación de las direcciones IP para cada equipo.

Dirección IP	Equipo	Máscara de Red	**Configurable**
132.248.255.96	NET ID	255.255.255.240	--
132.248.255.97	Lanplex 2500 Jardín Botánico	255.255.255.240	**Actualmente**
132.248.255.98	Lanplex 2500 Química E	255.255.255.240	**Actualmente**
132.248.255.99	Lanplex 2500 Antropológicas	255.255.255.240	**Actualmente**
132.248.255.100	CoreBuilder 3500 Servidores	255.255.255.240 Actualmente	
132.248.255.101	Lanplex 2500 Anexo Ingeniería	255.255.255.240	Actualmente
132.248.255.102	Lanplex 2500 Supercómputo	255.255.255.240	Actualmente

132.248.255.103	Cisco Catalyst 6509 Ciencias	255.255.255.240 Actualmente	
132.248.255.104	Libre	255.255.255.240 A futuro	
132.248.255.105	Libre	255.255.255.240 A futuro	
132.248.255.106	Libre	255.255.255.240 A futuro	
132.248.255.107	Libre	255.255.255.240 A futuro	
132.248.255.108	BigIron 8000 Antropológicas (dist.)	255.255.255.240	Actualmente
132.248.255.109	BigIron 8000 Local DGSCA (dist.)	255.255.255.240	Actualmente
132.248.255.110	NetIron 800 DGSCA (core)	255.255.255.240 Actualmente	
132.248.255.111	BROADCAST	255.255.255.240 --	

Tabla 4.9

Todos los Lanplex tendrán configurado su default gateway a la dirección IP del switch NetIron800 de core 132.248.255.110 y en este último habrá rutas estáticas redistribuyéndose al dominio de OSPF para las subredes 132.248.X.0/24 que se encuentran configuradas en los 3Com.
Para la numeración del enlaces OC-3 ATM punto a punto entre el Router Cisco dgsca1 y el switch NetIron 800 se utilizará una subred la subred 132.248.255.112/30 asignada de la siguiente forma:
Enlace ATM Router dgsca1 – NetIron 800 DGSCA (core)

Subred	IP Cisco dgsca1	IP NetIron DGSCA	Máscara de Red
132.248.255.112	132.248.255.113	132.248.255.114	255.255.255.252

Para ello se debe crear una subinterfaz ATM con 0/112 como los valores de VPI/VCI
El área 4 cuenta actualmente con tres routers internos, por lo que en un principio se necesitan sólo tres IP's para las direcciones de loopback, sin embargo, se van a considerar las direcciones de loopback necesarias para estar listo en el caso de que todos los demás equipos de distribución (Lanplex 2500) sean sustituidos por equipos que si puedan ser incluidos en el dominio de OSPF. Como se menciono al inicio, se tomarán las direcciones IP más altas de cada subred para configurarse en las interfaces de loopback, esto brinda mayor flexibilidad para tomar los boques de IP's que no se requieran como loopback, para utilizarlas en la numeración de enlaces punto a punto o nuevas LAN.
Las direcciones IP de loopback serán configuradas de la siguiente forma:

Dirección loopback	Equipo	Máscara de Red	Configurable
132.248.255.116	Libre	255.255.255.255	

		Actualmente	
132.248.255.117	Libre	255.255.255.255 Actualmente	
132.248.255.118	Libre	255.255.255.255 A futuro	
132.248.255.119	Libre	255.255.255.255 A futuro	
132.248.255.120	Libre	255.255.255.255 A futuro	
132.248.255.121	Libre	255.255.255.255 A futuro	
132.248.255.122	Libre	255.255.255.255 A futuro	
132.248.255.123	Libre	255.255.255.255 A futuro	
132.248.255.124	Router Cisco 7000 DGSCA1	255.255.255.255	A futuro
132.248.255.125	Cisco Catalyst 6509 Ciencias	255.255.255.255	A futuro
132.248.255.126	BigIron 8000 Antropológicas (dist.)	255.255.255.255	A futuro
132.248.255.127	BigIron 8000 Local DGSCA (dist.)	255.255.255.255	A futuro

Tabla 4.10

Subred 4 132.248.255.128/27 y subred 5 132.248.255.160/27 -- ÁREA 5 Routers

Esta es el área con más equipos dentro del dominio de OSPF, razón por la cual fue necesario asignarle dos subredes /27 contiguas para así sumarizarlas en un solo anuncio /26.

Para la numeración de la red LAN donde se encuentran los routers principales de RedUNAM se utilizará la subred 132.248.255.128/28 asignando las IP's como lo muestra la siguiente tabla:

Dirección IP	Equipo	Máscara de Red	Configurable
132.248.255.128	NET ID	255.255.255.240	--
132.248.255.129	Router 4500 Telecom2	255.255.255.240	Actualmente
132.248.255.130	Router 7200 RAS	255.255.255.240	Actualmente
132.248.255.131	Router 7500 Telecom6	255.255.255.240	Actualmente
132.248.255.132	Router 7500 Pitágoras	255.255.255.240 Actualmente	
132.248.255.133	Router 7500 Telecom1	255.255.255.240	Actualmente
132.248.255.134	Libre	255.255.255.240 A futuro	
132.248.255.135	Libre	255.255.255.240 A futuro	
132.248.255.136	Libre	255.255.255.240 A	

		futuro	
132.248.255.137	Libre	255.255.255.240 A futuro	
132.248.255.138	Libre	255.255.255.240 A futuro	
132.248.255.139	Libre	255.255.255.240 A futuro	
132.248.255.140	Libre	255.255.255.240 A futuro	
132.248.255.141	Switch 3900 Routers y DNS	255.255.255.240	A futuro
132.248.255.142	NetIron 800 Z.C. (core)	255.255.255.240 Actualmente	
132.248.255.143	BROADCAST	255.255.255.240 --	

Tabla 4.11

Para la numeración de los enlaces WAN punto a punto entre los routers de ésta área se utilizarán subredes con máscara de 30 bits asignadas de la siguiente forma:

Enlace Telecom6 – Palacio de Medicina

Subred	IP Telecom6	IP P. Medicina	Máscara de Red
132.248.255.144	132.248.255.145	132.248.255.146	255.255.255.252

Enlace Río Magdalena – Pitágoras

Subred	IP Río Magdalena	IP Pitágoras	Máscara de Red
132.248.255.148	132.248.255.149	132.248.255.150	255.255.255.252

Enlace Río Magdalena – Telecom6

Subred	IP Río Magdalena	IP Telecom6	Máscara de Red
132.248.255.152	132.248.255.153	132.248.255.154	255.255.255.252

Enlace Río Magdalena – Palacio de Medicina

Subred	IP Río Magdalena	IP P. Medicina	Máscara de Red
132.248.255.156	132.248.255.157	132.248.255.158	255.255.255.252

Enlace Río Magdalena – Torre de Rectoría

Subred	IP Río Magdalena	IP Torre Rectoría	Máscara de Red
132.248.255.160	132.248.255.161	132.248.255.162	255.255.255.252

Enlace Río Magdalena – Casa del Rector

Subred	IP Río Magdalena	IP Casa Rector	Máscara de Red
132.248.255.164	132.248.255.165	132.248.255.166	255.255.255.252

Se dejan libres las siguientes subredes para numerar enlaces punto a punto que se creen en un futuro o para asignar más interfaces loopback
- 132.248.255.168/30
- 132.248.255.172/30
- 132.248.255.176/30

Dirección loopback	Equipo	Máscara de Red	Configurable
132.248.255.184	Router 2620 Palacio de Medicina	255.255.255.255 Actualmente	
132.248.255.185	Router 3640 Torre de Rectoría	255.255.255.255 Actualmente	
132.248.255.186	Router 2620 Río Magdalena	255.255.255.255	Actualmente
132.248.255.187	Router 4500 Telecom2	255.255.255.255	Actualmente
132.248.255.188	Router 7200 RAS	255.255.255.255	Actualmente
132.248.255.189	Router 7500 Telecom6	255.255.255.255	Actualmente
132.248.255.190	Router 7500 Pitágoras	255.255.255.255 Actualmente	
132.248.255.191	Router 7500 Telecom1	255.255.255.255	Actualmente

Tabla 4.12

- 132.248.255.180/30
Las direcciones IP de las interfaces de loopback serán las siguientes:

Subred 6 132.248.255.192/27 y subred 7 132.248.255.224/27 – ÁREA0 BACKBONE
Para la numeración de los enlaces en GigabitEthernet entre los switches Foundry de ésta área se utilizarán subredes con máscara de 30 bits asignadas de la siguiente forma:
Enlace DGSCA Core – ZONA CULTURAL Core

Subred	IP DGSCA Core	IP Z.C. Core	Máscara de Red
132.248.255.192	132.248.255.193	132.248.255.194	255.255.255.252

Enlace DGSCA Core – IIMAS Core

Subred	IP DGSCA Core	IP IIMASCore	Máscara de Red
132.248.255.196	132.248.255.197	132.248.255.198	255.255.255.252

Enlace DGSCA Core – ARQUITECTURA Core

Subred	IP DGSCA Core	IP ARQ Core	Máscara de Red
132.248.255.200	132.248.255.201	132.248.255.202	255.255.255.252

Enlace IIMAS Core – ARQUITECTURA Core

Subred	IP IIMAS Core	IP ARQ Core	Máscara de Red
132.248.255.204	132.248.255.205	132.248.255.206	255.255.255.252

Enlace CATALYST TORRE DE RECTORÍA – ARQUITECTURA Core

Subred	IP TORRE RECT.	IP ARQ Core	Máscara de Red
132.248.255.208	132.248.255.209	132.248.255.210	255.255.255.252

Los siguientes enlaces no estarán presentes en el backbone inicial, pero se tiene planeado agregarlos para tener un backbone en full-mesh en cuanto se cuente con las trayectorias de fibra óptica monomodo necesarias.
Enlace IIMAS Core – ZONA CULTURAL Core

Subred	IP IIMASCore	IP Z.C. Core	Máscara de Red
132.248.255.212	132.248.255.213	132.248.255.214	255.255.255.252

Enlace ARQUITECTURA Core – ZONA CULTURAL Core

Subred	IP ARQ. Core	IP Z.C. Core	Máscara de Red
132.248.255.216	132.248.255.217	132.248.255.218	255.255.255.252

Para el enlace ATM OC-3 entre el NetIron DGSCA core y el NetIron Z.C. core se utilizará red
Enlace de Backup en ATM DGSCA Core – ZONA CULTURAL Core

Subred	IP DGSCA Core	IP Z.C. Core	Máscara de Red
132.248.255.220	132.248.255.221	132.248.255.222	255.255.255.252

Para ello se debe crear una subinterfaz ATM con 0/220 como los valores de VPI/VCI.
De la subred 7 132.248.255.224/27 que también se asignó al área 0, se tomarán las IP's más altas para configurarse en las interfaces loopback, por lo que se podrá tener libres las siguientes subredes:
- 132.248.255.224/28
- 132.248.255.240/29

Las direcciones IP de las interfaces de loopback para los switches de core son las siguientes:

Dirección loopback	Equipo	Máscara de Red	Configurable
132.248.255.248	Libre	255.255.255.255 A futuro	
132.248.255.249	Libre	255.255.255.255 A futuro	

132.248.255.250	Cisco Catalyst 6509 Ciencias	255.255.255.255	A futuro *
132.248.255.251	BigIron 8000 ARQ. (core)	255.255.255.255 Actualmente	
132.248.255.252	NetIron 800 Z.C. (core)	255.255.255.255 Actualmente	
132.248.255.253	BigIron 8000 IIMAS (core)	255.255.255.255 Actualmente	
132.248.255.254	NetIron 800 DGSCA (core)	255.255.255.255 Actualmente	
132.248.255.255	R E S E R V A D A	255.255.255.255	--

Tabla 4.13

4.3.1.3 Sumarización de las subredes 132.248.255.0/27 en los ABR's

Con el esquema de direccionamiento para las redes y enlaces punto a punto del Backbone planteado anteriormente, se puede realizar la sumarización de las redes /27 en las áreas 1, 2, 3 y 4.

4.3.1.4 Definición del DR y BDR para cada LAN

Con el objetivo de llevar un mejor control, así como de distribuir la carga de los routers en cada LAN, se propone asignar manualmente el *Designated Router* y *Backup Designated Router* para cada LAN dentro del dominio de OSPF con el comando a nivel de interface (la Ethernet o FastEthernet hacia la LAN) ip ospf priority <0-255>, donde al equipo que se defina como DR se le configurará una prioridad de 255 y BDR una prioridad de 250. A continuación se especifican los equipos que cumplirán con dichas funciones en las diferentes LAN's de cada área.
En el ÁREA 1 – ARQUITECTURA
En caso de que se configure el proceso de OSPF para esta área el único equipo de dicha LAN seria el switch BigIron8000 de ARQUITECURA por lo que no habria necesidad de definir el DR.
En el ÁREA 2 – ZONA CULTURAL
En caso de que se configure el proceso de OSPF para esta área el único equipo de dicha LAN seria el switch NetIron800 de Z.C., por lo que no habría necesidad de definir el DR.
En el ÁREA 3 – IIMAS
Para la LAN ésta área el DR será el switch de distribución BigIron8000 Local IIMAS y el BDR será el switch de distribución Astronomía.
En el ÁREA 4 – DGSCA
Para la LAN de esta área el DR será el switch de distribución BigIron8000 Local DGSCA y el BDR será el switch de distribución Antropológicas.
En el ÁREA 5 – Routers
En ésta área existen dos LAN's, la primera es donde se encuentran los Routers principales de RedUNAM y la segunda es la LAN formada por los equipos en la Torre de Rectoría.
- LAN Routers

Para ésta LAN el DR será el switch de core NetIron800 de Z.C. y el BDR será el Router 7500 Pitágoras.

- LAN Torre de Rectoría

Para ésta LAN el DR será el Router Cisco 3660 de Torre de Rectoría y el BDR será el switch de capa 3 Catalyst Torre.

En el ÁREA 6 – Internet2

Para la LAN de ésta área el DR será el Router Cisco 7500 Telecom7-I2 y el BDR será el switch de core NetIron800 de Z.C.

CAPITULO 5

PROCESO DE ADQUISICION.

5.1 Pasos de Adquisición.

En base y con apego a la ley general de adquisiciones vigente al 28 de Agosto del año 2001, se definió que la adquisición del equipo de telecomunicaciones (Switches L2 y L3) para el nuevo backbone de RedUNAM debería ser a través de una licitación publica internacional, donde es permitido que participen todos los proveedores que así lo deseen y que cumplan con los requisitos solicitados en la misma.

Articulo 28.- Las licitaciones públicas podrán ser:
Nacionales, cuando únicamente puedan participar personas de nacionalidad mexicana y los bienes a adquirir sean producidos en el país y cuenten por lo menos con un cincuenta por ciento de contenido nacional, el que será determinado tomando en cuenta el costo de producción del bien, que significa todos los costos menos la promoción de ventas, comercialización, regalías y embarque, así como los costos financieros. La Secretaría de Comercio y Fomento Industrial, mediante reglas de carácter general, establecerá los casos de excepción correspondientes a dichos requisitos, así como un procedimiento expedito para determinar el grado de contenido nacional de los bienes que se oferten, para lo cual tomará en cuenta la opinión de la Secretaría y de la Contraloría.

La Secretaría de Comercio y Fomento Industrial, de oficio o a solicitud de la Contraloría, podrá realizar visitas para verificar que los bienes cumplen con los requisitos señalados en el párrafo anterior, o Internacionales, cuando puedan participar tanto personas de nacionalidad mexicana como extranjera y los bienes a adquirir sean de origen nacional o extranjero.
Solamente se deberán llevar a cabo licitaciones internacionales, en los siguientes casos:

Cuando resulte obligatorio conforme a lo establecido en los tratados;
Cuando, previa investigación de mercado que realice la dependencia o entidad convocante, no exista oferta de proveedores nacionales respecto a bienes o servicios en cantidad o calidad requeridas, o sea conveniente en términos de precio;
Cuando habiéndose realizado una de carácter nacional, no se presente alguna propuesta o ninguna cumpla con los requisitos a que se refiere la fracción I de este artículo, y cuando así se estipule para las contrataciones financiadas con créditos externos otorgados al gobierno federal o con su aval.

En este tipo de licitaciones la Secretaría de Comercio y Fomento Industrial, mediante publicación en el Diario Oficial de la Federación, determinará los casos en que los participantes deban manifestar ante la convocante que los precios que presentan en su propuesta económica no se cotizan en condiciones de prácticas desleales de comercio internacional en su modalidad de discriminación de precios o subsidios.

Podrá negarse la participación a extranjeros en licitaciones internacionales, cuando con el país del cual sean nacionales no se tenga celebrado un tratado y ese país no conceda un trato recíproco a los licitantes, proveedores, bienes o servicios mexicanos.

Artículo 29.- Las convocatorias podrán referirse a uno o más bienes o servicios, y contendrán:

I. El nombre, denominación o razón social de la dependencia o entidad convocante;
II. La indicación de los lugares, fechas y horarios en que los interesados podrán obtener las bases de la licitación y, en su caso, el costo y forma de pago de las mismas. Cuando las bases impliquen un costo, éste será fijado sólo en razón de la recuperación de las erogaciones por publicación de la convocatoria y de la reproducción de los documentos que se entreguen; los interesados podrán revisarlas previamente a su pago, el cual será requisito para participar en la licitación. Igualmente, los interesados podrán consultar y adquirir las bases de las licitaciones por los medios de difusión electrónica que establezca la Contraloría;
III. La fecha, hora y lugar de celebración de las dos etapas del acto de presentación y apertura de proposiciones;
IV. La indicación de si la licitación es nacional o internacional; y en caso de ser internacional, si se realizará o no bajo la cobertura del capítulo de compras del sector público de algún tratado, y el idioma o idiomas, además del español, en que podrán presentarse las proposiciones;
V. La indicación que ninguna de las condiciones contenidas en las bases de la licitación, así como en las proposiciones presentadas por los licitantes, podrán ser negociadas;
VI. La descripción general, cantidad y unidad de medida de los bienes o servicios que sean objeto de la licitación, así como la correspondiente, por lo menos, a cinco de las partidas o conceptos de mayor monto;
VII. Lugar y plazo de entrega;
VIII. Condiciones de pago, señalando el momento en que se haga exigible el mismo;
IX. Los porcentajes de los anticipos que, en su caso, se otorgarían;
X. La indicación de que no podrán participar las personas que se encuentren en los supuestos del artículo 50 de esta Ley, y
XI. En el caso de arrendamiento, la indicación de si éste es con o sin opción a compra

Artículo 31.- Las bases que emitan las dependencias y entidades para las licitaciones públicas se pondrán a disposición de los interesados, tanto en el domicilio señalado por la convocante como en los medios de difusión electrónica que establezca la Contraloría, a partir del día en que se publique la convocatoria y hasta, inclusive, el sexto día natural previo al acto de presentación y apertura de proposiciones, siendo responsabilidad exclusiva de los interesados adquirirlas oportunamente durante este periodo. Las bases contendrán en lo aplicable como mínimo lo siguiente:

I. Nombre, denominación o razón social de la dependencia o entidad convocante;
II. Forma en que deberá acreditar la existencia y personalidad jurídica el licitante;
III. Fecha, hora y lugar de la junta de aclaraciones a las bases de la licitación, siendo optativa la asistencia a las reuniones que, en su caso, se realicen; fecha, hora y lugar de celebración de las dos etapas del acto de presentación y apertura de proposiciones; comunicación del fallo y firma del contrato;
IV. Señalamiento de que será causa de descalificación el incumplimiento de alguno de los requisitos establecidos en las bases de la licitación, así como la comprobación de que algún licitante ha acordado con otro u otros elevar los precios de los bienes o servicios, o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás licitantes;
V. Idioma o idiomas, además del español, en que podrán presentarse las proposiciones. Los anexos técnicos y folletos podrán presentarse en el idioma del país de origen de los bienes o servicios, acompañados de una traducción simple al español;
VI. Moneda en que se cotizará y efectuará el pago respectivo. En los casos de licitación internacional, en que la convocante determine efectuar los pagos a proveedores extranjeros en moneda extranjera, los licitantes nacionales podrán presentar sus proposiciones en la misma moneda extranjera que determine la convocante. No obstante, el pago que se realice en el territorio nacional deberá hacerse en moneda nacional y al tipo de cambio vigente en la fecha en que se haga dicho pago;
VII. La indicación de que ninguna de las condiciones contenidas en las bases de la licitación, así como en las proposiciones presentadas por los licitantes podrán ser negociadas;
VIII. Criterios claros y detallados para la adjudicación de los contratos de conformidad a lo establecido por el artículo 36 de esta Ley;

IX. Descripción completa de los bienes o servicios, o indicación de los sistemas empleados para identificación de los mismos; información específica que requieran respecto a mantenimiento, asistencia técnica y capacitación; relación de refacciones que deberán cotizarse cuando sean parte integrante del contrato; aplicación de normas a que se refiere la fracción VII del artículo 20 de esta Ley; dibujos; cantidades; muestras, y pruebas que se realizarán, así como método para ejecutarlas;

X. Plazo y condiciones de entrega; así como la indicación del lugar, dentro del territorio nacional, donde deberán efectuarse las entregas;

XI. Requisitos que deberán cumplir quienes deseen participar, los cuales no deberán limitar la libre participación de los interesados;

XII. Condiciones de precio y pago, señalando el momento en que se haga exigible el mismo. Tratándose de adquisiciones de bienes muebles, podrá establecerse que el pago se cubra parte en dinero y parte en especie, siempre y cuando el numerario sea mayor, sin perjuicio de las disposiciones relativas de la Ley General de Bienes Nacionales;

XIII. Datos sobre las garantías; así como la indicación de si se otorgará anticipo, en cuyo caso deberá señalarse el porcentaje respectivo y el momento en que se entregará, el que no podrá exceder del cincuenta por ciento del monto total del contrato;

XIV. La indicación de si la totalidad de los bienes o servicios objeto de la licitación, o bien, de cada partida o concepto de los mismos, serán adjudicados a un solo proveedor, o si la adjudicación se hará mediante el procedimiento de abastecimiento simultáneo a que se refiere el artículo 39 de esta Ley, en cuyo caso deberá precisarse el número de fuentes de abastecimiento requeridas, los porcentajes que se asignarán a cada una y el porcentaje diferencial en precio que se considerará;

XV. En el caso de contratos abiertos, la información a que alude del artículo 47 de este ordenamiento;

XVI. Penas convencionales por atraso en la entrega de los bienes o en la prestación de los servicios;

XVII. La indicación de que el licitante que no firme el contrato por causas imputables al mismo será sancionado en los términos del artículo 60 de esta Ley, y

XVIII. En su caso, términos y condiciones a que deberá ajustarse la participación de los licitantes cuando las proposiciones sean enviadas a través del servicio postal o de mensajería, o por medios remotos de comunicación electrónica. El que los licitantes opten por utilizar alguno de estos medios para enviar sus proposiciones no limita, en ningún caso, que asistan a los diferentes actos derivados de una licitación.

Para la participación, contratación o adjudicación en adquisiciones, arrendamientos o servicios no se le podrá exigir al particular requisitos distintos a los señalados por esta Ley.

5.1.1 Lanzamiento y publicación de las bases de la licitación.

En base a lo anterior se lanzo la convocatoria para la Licitación Publica Internacional No. 01-DGP-LPIS-0059 con fecha de abril de 2001, en la cual se detallan todos los requisitos que debieran cumplir todos los concursantes, de igual forma se detallan las cantidades y características técnicas que deberían cumplir los equipos ofertados, mismos que se dividieron en 2 partidas separadas una para equipos de core y la otra para los equipos de distribución esto a razón de que sus características técnicas son distintas. nosotros en este trabajo de tesis nos abocaremos únicamente a la parte técnica de dicha licitación por el enfoque de la misma, y la confidencialidad de cierta información.

En las bases emitidas para dicha licitación se pidió que con la finalidad de garantizar, el óptimo desempeño de la operación de la RedUNAM, los equipos propuestos se sometieran a un set de pruebas, para evaluar su desempeño y verificar que cumplieran con todas las funcionalidades antes descritas

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
DIRECCIÓN GENERAL DE PROVEEDURÍA

COORDINACIÓN DE ADQUISICIONES
"PROGRAMA UNAM – BID"

INSTITUCIÓN: UNAM
CLASE DE EQUIPO: REDES. SWITCHES DE CORE, PARTIDA 18

CANTIDAD:	4
UNIDAD DE MEDIDA:	PIEZAS
MARCA:	
MODELO:	
CATÁLOGO:	

DESCRIPCIÓN DEL EQUIPO:

PARTIDA 18. Switches de Core
Se trata de switches capa 2 y 3.
Las funcionalidades y especificaciones deberán ser cubiertas al 100% en una sola caja. No se aceptarán cajas externas.

Especificaciones Técnicas

HARDWARE

Característica	Especificación
Chasis	Modular para montaje en bastidor de 19" Mínimo 6 ranuras (slots) para puertos y 2 para tarjetas controladoras Indicadores visibles de estado: Operación en línea, Standby, fuera de servicio y falla en módulos. Módulos Hot Swap
Condiciones de Operación	Alimentación: Corriente alterna 220 o 110 Volts Temperatura: 0 a 40 grados centrígrados Humedad Relativa: 10% a 85% o 5% a 95% . Sin condensación en operación
Backplane	Capacidad mínima 64 Gigabits y escalable
Memoria en tarjeta Controladora	Mínimo 64 Mbps DRAM
Interfases Soportadas	ATM en OC-3c en fibra multimodo y monomodo. Gigabit Ethernet. 1000BaseSX/LX (Preferentemente en Gbic´s) 100Base FX, 10/100 Base TX Hot-swap en todos los módulos y componentes (PCMCIA, Gbic´s etc.) No se aceptarán transceivers ni adaptadores externos.
Redundancias	En procesador central. Deberá ser Hot-swap En fuente de poder. Deberá ser Hot-swap En enlaces troncales, mínimo en 4 enlaces.
Crecimiento	Capacidad de crecimiento del 30%, con respecto a la capacidad mínima de puertos mencionados. Ver tabla de cantidades.

Tabla 5.1

Bajo la siguiente estructura y cantidades

4 switches L2/L3, bajo la siguiente estructura:

Equipo	Nodo	# Puertos Gigabit Ethernet (Uplink)	# Puertos Gigabit Ethernet	# Puertos ATM OC-3	# Puertos Fast Ethenet 100BaseFX
1	DGSCA	3 1000Base LX	12 1000BaseLX 4 1000BaseSX	1	16
2	**ARQUITECTURA**	3 1000Base LX	10 1000BaseLX 2 1000BaseSX		12

3	IIMAS	3 1000Base LX	9 1000BaseLX 4 1000BaseSX		14
4	ZONA CULTURAL	3 1000Base LX	8 1000BaseLX 4 1000BaseSX	1	12

Tabla 5.2

De esta forma se les detallo a todos los concursantes que la configuración requerida en los equipos con la finalidad de que pudieran configurar y cotizar cada una de los partes para dichos equipos que generalmente son modulares.

Ahora bien una vez que se contaba con la configuración física de los equipos se deberían contemplar las funcionalidades requeridas para los mismos, dichas funcionalidades se detallan a continuación.

SOFTWARE

Característica	Especificación
Protocolos en Capa 2	IEEE 802.1Q IEEE 802.1P IGMP STP (Grupos) Port Mirror IEEE 802.1d Tamaño de tabla de direcciones: 8,000 como mínimo
Protocolos en Capa 3	Protocolos de ruteo: OSPF, RIPv1, RIPv2 y BGP4 (mínimo 20,000 prefijos) DiffServ PIM DVMRP Capacidad de limpiar las tablas de Ruteo y MAC Bootp/DHCP relay (RFC 2131)
Estándares ATM	RFC 1483 (ATM-Routing)
Switcheo ATM	Soporte PVC/SVC. Manejo de congestión vía: EFCI y CLP.
Priorización de tráfico	Soporte QoS
Protocolos de redes de datos soportados	Suite TCP/IP e IPX
Seguridad	Listas de acceso ACL´s: Por IP Por MAC Por puertos TCP/UDP
Administración	Accesos: Vía Telnet (RS-232) Vía puerto auxiliar (Outband) o Ethernet

	Vía Consola (RS-232) Del software de administración Basado en plataforma Unix SNMP RMON (manejo mínimo de 4 grupos) Respaldo de configuración Vía TFTP o FTP o SCP Actualizaciones de Software vía FTP o TFTP o SCP
Documentación	Manuales de Operación, Programación y Mantenimiento.
Tipos de VLAN's	Por Puerto
Especificaciones futuras (a corto plazo)	DHCP Server NAT IPv6 MPLS TACACS RADIUS Web Cache Redirect IS-IS SSH versión 1 o 2 Vlans por MAC MBGP MSDP IGMP Snooping Vlans por Subred de IP, por protocolo y MAC Vlans Autenticadas (por login y password) Si durante el período de garantía del equipo, el fabricante saca al mercado la(s versión(es) de software o módulos (en hardware o software) que cubran las funcionalidades anteriores, el licitante se compromete por escrito a proporcionárselas a la UNAM sin costo alguno.

Tabla 5.3

De igual forma se emitieron las bases para los equipos de distribución que habrían de cumplir con lo siguiente.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
DIRECCIÓN GENERAL DE PROVEEDURÍA

COORDINACIÓN DE ADQUISICIONES
"PROGRAMA UNAM – BID"

INSTITUCIÓN: UNAM
CLASE DE EQUIPO: REDES. SWITCHES DE DISTRIBUCIÓN . PARTIDA 19

CANTIDAD:	5
UNIDAD DE MEDIDA:	PIEZAS
MARCA:	
MODELO:	
CATÁLOGO:	

DESCRIPCIÓN DEL EQUIPO:

PARTIDA 19. Switches de Distribución
Se trata de switches capa 2 y 3.
Las funcionalidades y especificaciones deberán ser cubiertas al 100% en una sola caja. No se aceptarán cajas externas.
Especificaciones Técnicas

HARDWARE

Característica	**Especificación**
Chasis	Modular para montaje en bastidor de 19" Mínimo 6 ranuras (slots) Indicadores visibles de estado: Operación en línea, Standby, fuera de servicio y falla en módulos. Módulos Hot Swap
Condiciones de Operación	Alimentación: Corriente alterna 220 o 110 Volts Temperatura: 0 a 45 grados centrigrados Humedad Relativa: 10% a 85% o 5% a 95% . Sin condensación.
Backplane	Capacidad mínima 64 Gigabits
Memoria	Mínimo 32 Mbps DRAM
Interfases Soportadas	Gigabit Ethernet. 1000BaseSX/LX (Preferentemente en Gbic´s) 100 BaseFX. 10/100 Base Tx **Hot-swap en los módulos.** No se aceptarán transceivers ni adaptadores externos.

Redundancias	En fuente de poder. Deberá ser Hot swap En enlaces troncales, mínimo en 4 enlaces
No de Puertos	Capacida minima de 16 puertos Gigabit LX o SX con conectores SC o MT-RJ
Crecimiento	Capacidad de crecimiento del 30%, con respecto a la capacidad mínima de puertos mencionados.

Tabla 5.4

Ahora bien una vez que se contaba con la configuración física de los equipos se deberían contemplar las funcionalidades requeridas para los mismos, dichas funcionalidades se detallan a continuación.

SOFTWARE

Caracteristica	**Especificación**
Protocolos en Capa 2	IEEE 802.1Q IEEE 802.1P IEEE 802.1 D IGMP, IGMP Snooping (RFC 1112, RFC 2236) Port Mirror BOOTP / DHCP Relay (RFC 2131)
Protocolos en Capa 3	Protocolos de ruteo: OSPF, RIPv1, RIPv2 DiffServ PIM (RFC 2362) DVMRP V3
Protocolos de redes de datos soportados	Suite TCP/IP, IPX
Switcheo Ethernet-Ethernet	Switcheo Ethernet: Transparente para todos los protocolos a nivel MAC. Tamaño de tabla de direcciones: 8,000 como mínimo.
Seguridad	Listas de acceso ACL´s: Por IP Por MAC Por puertos TCP/UDP
Administración	Accesos: Vía Telnet Vía Consola Del software de administración Basado en plataforma Unix o Windows SNMPv1. RMON1 (Mínimo 4 Grupos) Respaldo de configuración vía TFTP o FTP o SCP Actualizaciones de Software vía FTP o TFTP o SCP SSH
Documentación	Manuales de Operación, Programación y Mantenimiento.
Especificaciones futuras (a corto plazo)	-WEB Cache Redirect -NAT -BGP4 (mínimo 20,000 prefijos) Si durante el período de garantía del equipo, el fabricante

	saca al mercado la(s) versión(es) de software o módulos (en hardware o software) que cubran las funcionalidades anteriores, el licitante se compromete por escrito a proporcionárselas a la UNAM sin costo alguno.

Tabla 5.5

Estos equipos beberán venir físicamente configurados con el detalle de puerto que se muestra a continuación.

Estructura y Cantidades
5 switches L2/L3, bajo la siguiente estructura:

Equipo	Nodo	# Puertos Gigabit Ethernet (Uplink)	# Puertos Gigabit Ethernet	# Puertos Fast Ethenet 10/100 BaseTx
	DGSCA			
1	DGSCA	1 1000BaseSX	6 1000BaseSX	24
2	Antropológicas	1 1000BaseLX	9 1000BaseLX 2 1000BaseSX	
	ARQUITECTURA			
3	Arquitectura	1 1000BaseSX	13 1000BaseLX 2 1000BaseSX	
	IIMAS			
4	Laborales	1 1000BaseLX	12 1000BaseLX 2 1000BaseSX	
5	Astros	1 1000BaseLX	8 1000BaseLX 5 1000BaseSX	

Tabla 5.6

Todos los concursantes que adquirieron las bases en tiempo y forma deberán proponer equipos que cumplan fielmente con las características antes mencionadas, y de no ser así serían descalificados.

5.2 Junta de aclaraciones.

Posteriormente a la adquisición de las bases se realizo el acto denominado como junta de aclaraciones, con la finalidad de aclarar, cualquier duda o controversia que tuvieran los licitantes ara poder elaborar sus propuestas técnicas y cotizar, sus productos, de igual forma en este acto se respondieron las discrepancias que pudieran existir en cuanto a marcas, o funcionalidades de los equipos, para que todo se lleve con apego a la ley y se verifique en presencia de todos los licitantes, la legalidad del evento y que no se incurra en favorecer a alguno de ellos.

5.3 Acto de presentación de propuestas.

En este punto se todos los licitantes que hayan comprado las bases de la licitación en tiempo y forma, y que cumplan con todos los requisitos legales, administrativos y técnicos, y que hayan elaborado una propuesta técnica y una oferta económica se presentan a entregar las mismas en sobres cerrados cada una por separado, este acto consta de una junta publica donde se encuentran todos los proveedores que deseen concursar y las autoridades de la UNAM, destinadas para este proceso.
Posteriormente a la recepción de las propuestas se abre el sobre que contiene la documentación legal y las propuestas técnicas, con la finalidad de revisar que cumpla con toda la documentación administrativa y técnica, ya que de faltar algún documento dicha propuesta habría de ser desechada. Una vez que se reviso dicha documentación se entregan las propuestas técnicas al área encargada de su minuciosa revisión y evaluación, ya que de haberse omitido alguna característica técnica la propuesta debería de ser desechada.

En dicho acto se recibieron de igual forma todas las ofertas económicas mismas que quedaron perfectamente selladas y sobre los sellos las firmas todos los participantes de la reunión con la finalidad de poder garantizar la legalidad de dicho acto.

5.4 Realización de pruebas.

Posteriormente a la entrega de las propuestas técnicas y con estricto apego a las bases se requirió, el equipo que habría de someterse al set de pruebas correspondiente, cabe aclarar que dicho set de pruebas fue publicado en las bases con la finalidad de que todos los licitantes lo conocieran y lo dominaran al dia de las pruebas.

para este punto existían 3 proveedores con distintas soluciones a evaluar, como se muestra a continuación:

1) INTERSYS	CORE DISTRIBUCION	CISCO EXTREME
2) AMYCO	CORE DISTRIBUCION	RIVERSTONE RIVERSTONE
3) TECHTEL INTERNATIONAL	CORE DISTRIBUCION	FOUNDRY FOUNDRY

Los proveedores participantes deberían cumplir las siguientes condiciones de la metodología de pruebas:

5.4.1 Metodología de pruebas

Las pruebas se llevarán a cabo un solo día por proveedor. El día que le corresponda a cada proveedor será asignado a través de sorteo e informado el mismo día de entrega de ofertas.

La recepción de los equipos para las pruebas será 5 días hábiles después de la fecha límite de entrega de las propuestas, en horario de 10:00 a las 19:00, en la Subdirección de Redes de la DGSCA (Circuito Ext. S/n Frente a Fac. De Contaduría).

El fabricante deberá entregar sus equipos en cajas cerradas y plenamente identificadas. Se entregará documento de recibo por parte de la Subdirección de Redes.

El horario de pruebas será de 10:00 a 19:00 por ninguna razón se podrá modificar el horario de pruebas.

Al inicio de las pruebas todos los equipos deberán de estar en valores por default, la configuración inicial debe de programarse mediante línea de comando (CLI), las configuraciones necesarias deberán de ser realizadas exclusivamente por el proveedor, ya que se estará evaluando su experiencia en el manejo de los equipos que proponen.

El proveedor deberá traer todo el equipo necesario para realizar las maquetas incluyendo los switches ofertados en su propuesta (partida 18 y 19), es necesario 2 equipos por partida), cables de red, consola, transceivers, estación de monitoreo con el software de administración necesario para las pruebas, y/o equipo adicional que se requiera para cubrir las funcionalidades solicitadas en la licitación y marcadas en este esquema de pruebas, es necesario que etiqueten todos los equipos y cables con el fin de evitar retrasos en la entrega de los mismos.

Será responsabilidad de RedUNAM proporcionar el generador de tráfico (SmartBits), server de multicast, clientes de multicast (los fabricantes pueden usar como clientes adicionales de multicast sus laptops y/o server) y los equipos de terceros (switches o routers), en caso de ser necesario, otorgar un punto de red y una dirección IP para que sea utilizada por el proveedor durante el intervalo de pruebas.

Las personas que participen deberán portar una identificación que los acredite como miembros del proveedor participante, y es indispensable que se entregue una lista del personal que estará en las pruebas, no se aceptarán observadores y/o alguna otra persona que no hubiera sido confirmada.

El proveedor podrá contar con la documentación de sus productos ya sea por medios electrónicos o impresos.

El software de monitoreo deberá venir previa y completamente instalado para cubrir las pruebas de monitoreo de la maqueta de la red, con el fin de agilizar éstas.

El set de pruebas que se correría para cada participante de los equipos de CORE seria el siguiente:

5.4.2 Virtual Lans

Puntos a evaluar:
Mostrar la facilidad de configuración de las redes virtuales y asignaciones de puertos vía consola y/o sesión remota (Comand Line Interface).

Mostrar el soporte de configuración de redes virtuales en base a dirección MAC, por puerto físico de switch, por protocolo y por VLAN autenticada (Documentada) .

Configuración de 802.1Q para el manejo de redes virtuales entre los switches de Core a través de los puertos de Gigabit y FastEthernet, mismo fabricante

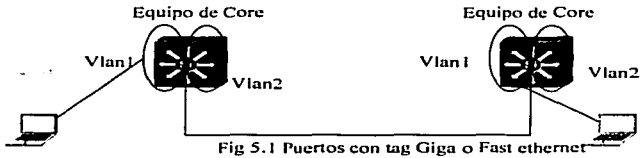


Fig 5.1 Puertos con tag Giga o Fast ethernet

Configuración de 802.1Q para el manejo de redes virtuales entre los switches de Core a través de los puertos de Gigabit y FastEthernet, equipos de terceros

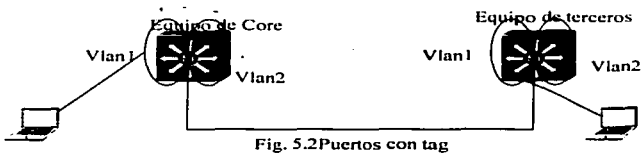


Fig. 5.2Puertos con tag

5.4.3 Prueba de 802.1p (CoS)

Comprobación de las funcionalidades de 802.1p a través de la medición de los siguientes parámetros:

Throughput,
Pérdida de paquetes,
Latencia,
Distribución de latencia,
Jitter.

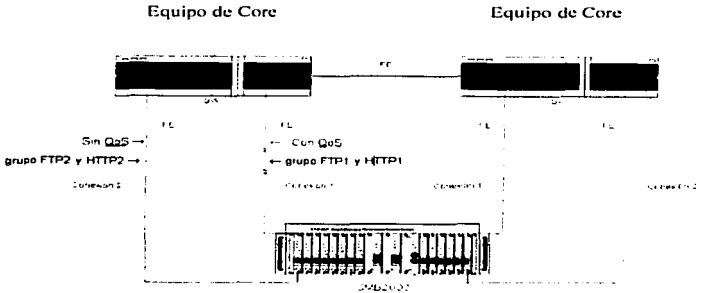


Fig 5.3 Prueba de 802.1P

5.4.4 Troncales

Comprobación de la operación de troncales de gigabit Ethernet (utilizando 2 puertos de gigabit) características a evaluar:

Redundancia
Balanceo
Tiempo de recuperación de la troncal

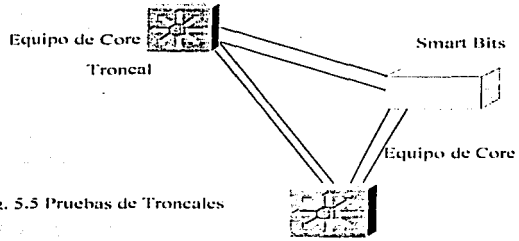


Fig. 5.5 Pruebas de Troncales

5.4.5 Spanning Tree Protocol.

Comprobación del estándar 802.1d

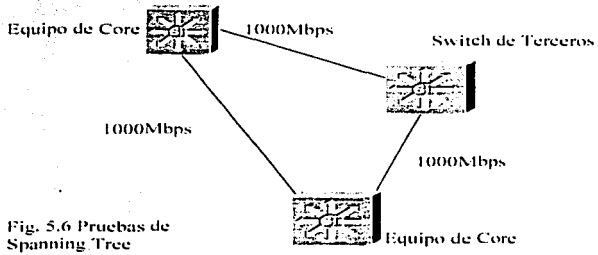


Fig. 5.6 Pruebas de Spanning Tree

5.4.6 ATM
Comprobación de los estándares a evaluar

ATM RFC-1483
Configuración de PVC'S

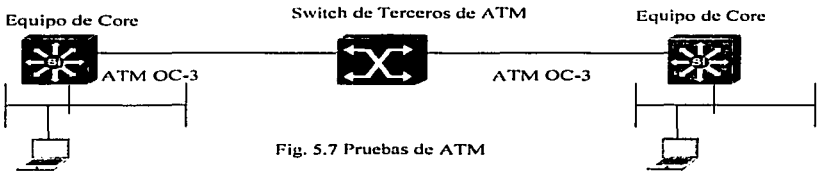


Fig. 5.7 Pruebas de ATM

5.4.7 Autenticación

Verificar el funcionamiento de AAA en los equipos, así mismo la creación de listas de acceso para restringir la administración a ciertos usuarios y/o nodos, es necesario que el proveedor cuente con su servidor de autenticación (TACACS y/o Radius) instalado bajo cualquier sistema operativo.

5.4.8 Rip V1/V2

Evaluar el correcto funcionamiento del protocolo RIP versión 1 y versión 2 en todas sus especificaciones.

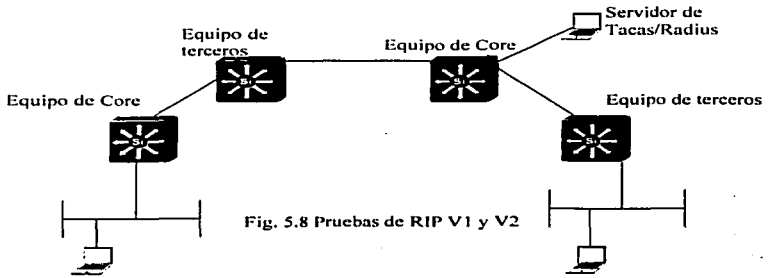


Fig. 5.8 Pruebas de RIP V1 y V2

5.4.9 OSPF

Verificar la correcta operación de OSPF con los equipos existente del backbone de RedUNAM utilizando varias áreas.

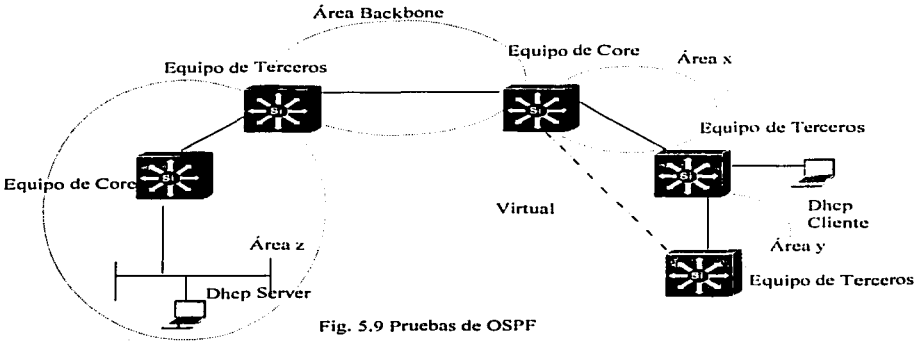


Fig. 5.9 Pruebas de OSPF

5.4.10 Multicast

Comprobar la operación de los siguientes protocolo de multicast, para ello se utilizar un server de real audio de dominio publico.

DVMRP
PIM-DM
PIM-SM

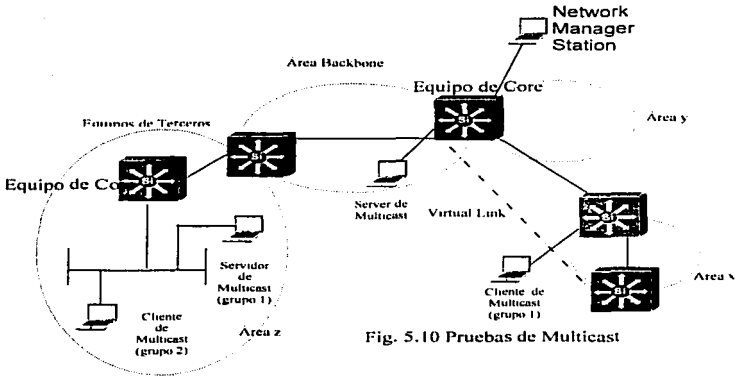


Fig. 5.10 Pruebas de Multicast

5.4.11 Herramienta de Administración

La herramienta de administración deberá de ser instalada en plataforma UNIX y se evaluara lo siguiente:

SNMP
RMON (manejo mínimo de 4 grupos)
Respaldo de configuración Vía TFTP, FTP o SCP
Actualizaciones de Software vía FTP, TFTP o SCP
Rastreo de usuarios por dirección IP, MAC
Envió de alarmas por medio de Pagers, correo electrónico, etc.

5.4.12 BGP4/MBGP,MSDP

Comprobar la correcta operación del protocolo BGP4 y su extensión para soportar de multicast y el protocolo MSDP.
Se evaluaran filtros y políticas de ruteo

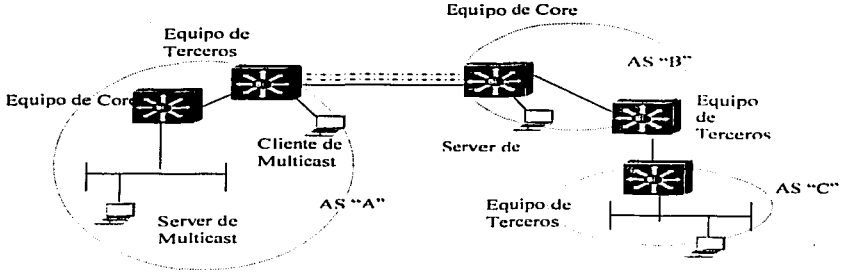


Fig. 5.11 Pruebas de BGP4/MBGP,MSDP

5.4.13 PRUEBAS PARA LA PARTIDA EQUIPO DE DISTRIBUCION

5.4.14 Virtual Lans

Puntos a evaluar:
Mostrar la facilidad de configuración de las redes virtuales y asignaciones de puertos vía consola y/o sesión remota (Comand Line Interface).

Mostrar el soporte de configuración de redes virtuales en base a dirección MAC, por puerto físico de switch, por protocolo y por VLAN autenticada (Documentada) .

Configuración de 802.1Q para el manejo de redes virtuales entre los switches de Core a través de los puertos de Gigabit y FastEthernet, mismo fabricante

Fig. 5.12

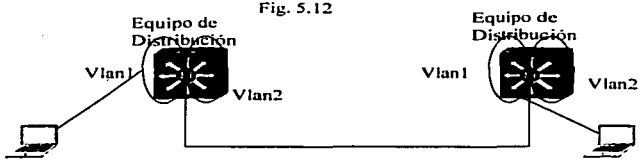


Fig. 5.12 Puertos con tag Giga o Fast ethernet

Configuración de 802.1Q para el manejo de redes virtuales entre los switches de Core a través de los puertos de Gigabit y FastEthernet, equipos de terceros

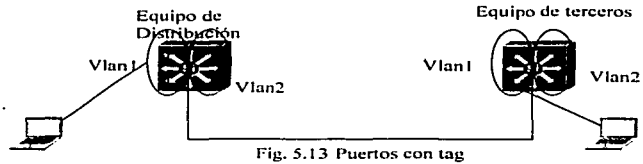


Fig. 5.13 Puertos con tag

5.4.15 Prueba de 802.1p (CoS)

Comprobación de la funcionalidades de 802.1p a través de la medición de los siguientes parámetros:

Throughput,
Pérdida de paquetes,
Latencia,
Distribución de latencia,
Jitter.

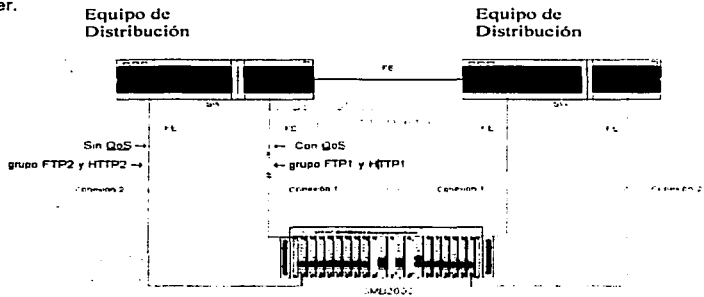


Fig 5.14 Prueba de 802.1P

5.4.16 Troncales

Comprobación de la operación de troncales de gigabit Ethernet (utilizando 2 puertos de gigabit) características a evaluar:

Redundancia
Balanceo
Tiempo de recuperación de la troncal

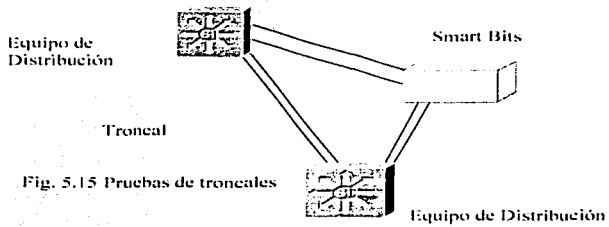


Fig. 5.15 Pruebas de troncales

5.4.17 Spanning Tree Protocol.

Comprobación del estándar 802.1d

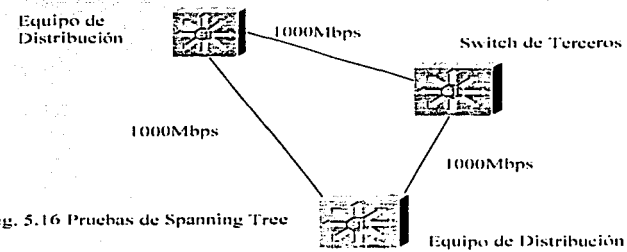


Fig. 5.16 Pruebas de Spanning Tree

5.4.18 Autenticación

Verificar el funcionamiento de AAA en los equipos, así mismo la creación de listas de acceso para restringir la administración a ciertos usuarios y/o nodos, es necesario que el proveedor cuente con su servidor de autenticación (TACACS y/o Radius) instalado bajo cualquier sistema operativo.

5.4.19 Rip V1/V2

Evaluar el correcto funcionamiento del protocolo RIP versión 1 y versión 2 en todas sus especificaciones.

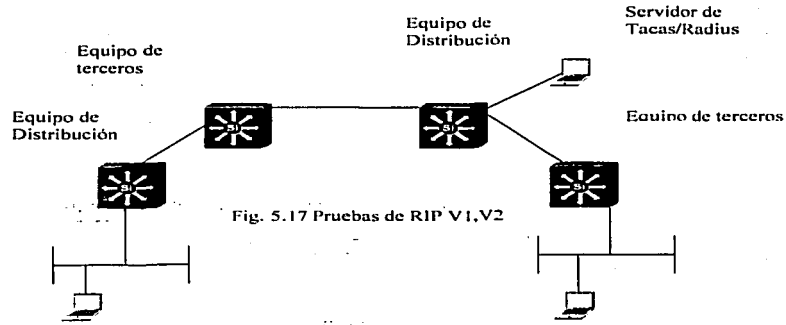


Fig. 5.17 Pruebas de RIP V1,V2

5.4.20 OSPF

Verificar la correcta operación de OSPF con los equipos existente del backbone de RedUNAM utilizando varias áreas.

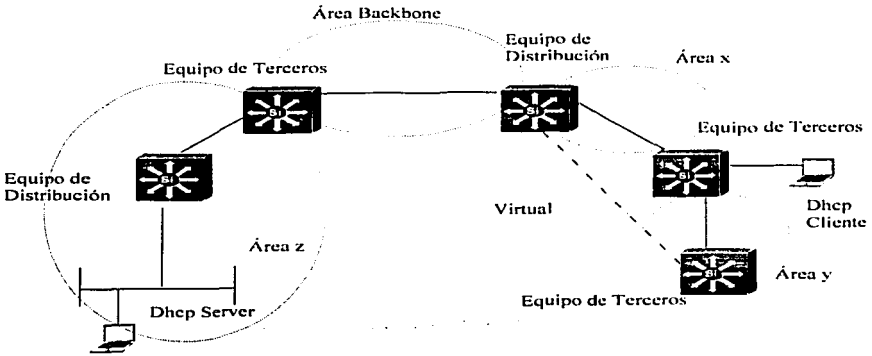


Fig. 5.18 Pruebas de OSPF

5.4.21 Multicast

Comprobar la operación de los siguientes protocolo de multicast, para ello se utilizar un server de real audio de dominio publico.

DVMRP
PIM-DM
PIM-SM

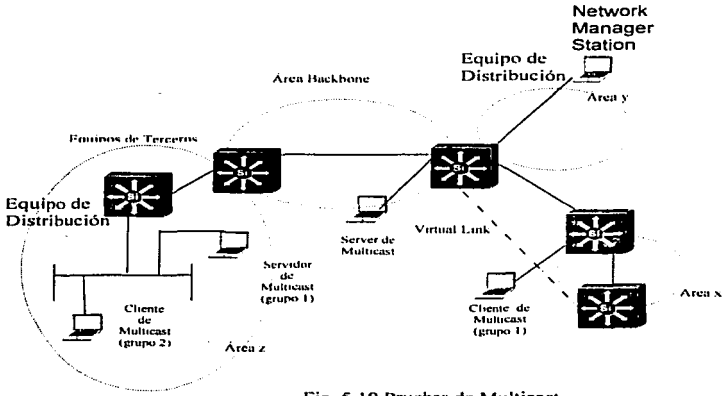


Fig. 5.19 Pruebas de Multicast

5.4.22 Herramienta de Administración

La herramienta de administración deberá de ser instalada en plataforma UNIX y se evaluara lo siguiente:

SNMP
RMON (manejo mínimo de 4 grupos)
Respaldo de configuración Vía TFTP, FTP o SCP
Actualizaciones de Software vía FTP, TFTP o SCP
Rastreo de usuarios por dirección IP, MAC
Envió de alarmas por medio de Pagers, correo electrónico, etc.

5.4.23 Formato de pruebas.

Los resultados de las pruebas fueron plasmados en el documento que a continuación se presenta por cada uno de los participantes que se presentaron, los datos de la evaluación técnica de las pruebas se omiten por razones de confidencialidad de la información.
Ofertas Técnicas que Cumplen con las Especificaciones Solicitadas

Licitante :	
Lote:	

Pruebas UNAM		Evaluación Observaciones
VLAN'S		
Configuración de Vlans con 802.1		
Configuración de Vlans con 802.1 con terceros		
Facilidad de configuración de Vlans y asignación		
Diversidad de Vlans(Mac,puerto,Protocolo,autenticada)		
Relay de DHCP		
Comunicación entre diferentes tipos de Vlans		
Spanning Tree		
Gigabit Ethernet		
Interoperabilidad con equipos de cómputo y switches de terceros		
Comportamiento del switch con carga		
Soporte de interfases SX y LX		
Non-Blocking		
Link Agregation (Trunking)		
Capacidad de trunking		
Redundancia en el trunking		
Balanceo en el trunking		
Servicios de capa 3		
Soporte OSPF		

Soporte RIP/RIP II		
Soporte de BGP		
Soporte de IP, IPX, APPLETALK		
Seguridad		
Soporte de servicios AAA		
Soporte de NAT		
Listas de Acceso(por IP,MAC,Puerto de TCP/UDP		
Creación listas Via consola		
Creación listas Via plataforma de Administración		
Redundancia		
Hotswap		
Redundancia en servicios L2/L3		
Redundancia fuentes de poder		
Tiempo en levantar todos los servicios (Segundos)		
Monitoreo		
Grupos de RMON		
Soporte para NTP		
Configuración de Vlans y asignaciones de puertos		
Funcionalidades de inventario		
Rastreo de usuarios		

Observaciones Generales

X No cumple
√ Cumple

Tabla 5.7 Formato de pruebas.

Posteriormente a la realización del set de pruebas se entregaron, los resultados aprobatorios a la propuesta de INTERSYS y a la propuesta de TTI, siendo descalificada la propuesta de AMYCO por no haberse presentado a la realización de dichas pruebas .Posteriormente a la entrega de dichos resultados, solo habria que esperar el acto de apertura de propuestas económicas en donde habria de definirse el ganador en base al precio mas bajo de su cotización.

5.5 Apertura de propuestas económicas.

Este acto se lleva a cabo en una junta publica en la que participan los licitantes que aprobaron las pruebas y cumplieron con todas la documentación legal solicitada, de no ser así en dicho acto se plantea el por que de la descalificación, ahora bien se procede a la revisión de que los sellos previamente puestos a las propuestas económicas no hallan sido violados, una vez verificado esto se procede a abrir dichos sobres para poder saber quien es el ganador, al que se le adjudicara la compra de dichos bienes, resultando ganadora la empresa licitante TECHTEL INTERNATIONAL S.A. DE C.V.

Ofertando el total de los bienes para la partida de switches de CORE en un monto total de: **$ 520986 USD.**
Ofertando equipos NETIRON 800

De igual forma la empresa TECHTEL INTERNATIONAL S.A. DE C.V. se adjudico, la partida de los switches de DISTRIBUCION con un monto total de:
$ 520986 USD
Ofertando equipos BIGIRON8000

Seguido a este acto se procede a realizar la entrega del fallo y la firma del contrato, que de dicha licitación se derive para por ultimo poder hacer la entrega de los bienes licitados a la UNAM.
Concluyendo de esta manera con el proceso de adquisición de los bienes.

CONCLUSIONES

Red UNAM mediante el proyecto de reestructuración, a traves de una migración y actualización del backbone ha alcanzado la capacidad de soportar óptimamente todos los servicios de datos, voz y video sobre IP y aplicaciones emergentes que de ella se demanden; además de ser suficientemente flexible para permitir su crecimiento.

Posteriormente a la culminación del proyecto de reestructuración del backbone de RedUNAM se ha generado un muy amplio panorama de posibilidades como son el poder integrar la red de datos con las de voz y video, gracias a que el backbone de Gigabit Ethernet goza de una velocidad de transmisión bastante grande, un direccionamiento y un diseño de red que satisface los requerimientos de las aplicaciones actuales. Esto nos trae como resultado el poder poner en práctica nuevas aplicaciones y tecnologías como voz sobre IP bajo los estándares H.323 y SIP, video sobre IP también con el estándar H.323, que sin duda lo mas importante es que Red UNAM esta dimensionada para poder alojar, nuevas aplicaciones que demanden un gran ancho de banda.

Más sin embargo aun quedan muchas cosas por hacer, y la realización de este proyecto marcara sin duda el inicio de la convergencia de nuevas tecnologías y protocolos dentro de RedUNAM.

Realizando una comparación entre el backbone ATM y el de Gigabit Ethernet a nivel de enrutamiento podemos decir lo siguiente:

Con el backbone de ATM la carga de trabajo para los enrutadores en hora pico era excesivo debido a su enrutamiento estático, con el backbone de Gigabit Ethernet al estar utilizando el protocolo OSPF aligera la carga de trabajo en los enrutadores. Dado que OSPF es un protocolo de enrutamiento estándar es el único que permite mantener compatibilidad entre equipos de enrutamiento de diferentes marcas, lo que permite no depender de un fabricante en particular, esto lo podemos visualizar en el backbone de Gigabit Ethernet de la siguiente forma: los enrutadores marca Cisco que se utilizaban con el backbone de ATM se pudieron interconectar con los Foundry gracias a que las dos marcas manejan protocolos de ruteo estándar y para el caso de Red UNAM el de OSPF.

Con el backbone de Gigabit Ethernet se logro implantar un esquema de enrutamiento jerárquico que permite la segmentación de la red en áreas. La asignación de estas áreas nos permite ocultar la información de enrutamiento entre enrutadores de diferentes áreas lo que elimina el tráfico en la red y proporciona un mejor aprovechamiento del ancho de banda; con el backbone de ATM como se emulaba una LAN y recordando que este tipo de red es un medio compartido el ancho de banda no se aprovechaba de forma correcta.

Teniendo en mente que pueden existir fallas eléctricas y dejar fuera de funcionamiento a un router poniendo nuevamente a la balanza al backbone de ATM y el de Gigabit Ethernet con respecto a la convergencia el backbone de Gigabit Ethernet optimiza el tiempo de convergencia debido al protocolo de ruteo utilizado que como ya sabemos es OSPF

GLOSARIO.

Fibra local de 8 bytes/10 bytes :
Ver fibra local 8B/10B.

100BaseFX :
Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos hebras de cable de fibra óptica multimodo por enlace. Para garantizar una correcta temporización de la señal, un enlace 100BaseFX no puede superar los 400 metros de longitud. Se basa en el estándar IEEE 802.3. Ver también 100BaseX, Fast Ethernet e IEEE 802.3.

100BaseT :
Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cableado UTP. Al igual que la tecnología 10BaseT en la que se basa, 100BaseT envía impulsos de enlace a través del segmento de la red cuando no se detecta tráfico. Sin embargo, estos impulsos de enlace contienen más información que los utilizados en 10BaseT. Se basa en el estándar IEEE 802.3. Ver también 10BaseT, Fast Ethernet e IEEE 802.3.

100BaseT4 :
Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cuatro pares de cableado UTP de Categoría 3, 4 ó 5. Para garantizar una correcta temporización de la señal, un segmento 100 BaseT4 no puede superar los 100 metros de longitud. Se basa en el estándar IEEE 802.3. Ver también Fast Ethernet e IEEE 802.3.

100BaseTX :
Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos pares de cableado UTP o STP. El primer par de cables se utiliza para recibir datos y el segundo para transmitir. Para garantizar una correcta temporización de las señales, un segmento 100 BaseTX no puede superar los 100 metros de longitud. Se basa en el estándar IEEE 802.3. Ver también 100BaseX, Fast Ethernet e IEEE 802.3.

100BaseX :
Especificación Fast Ethernet de banda base de 100 Mbps que se refiere a los estándares 100BaseFX y 100BaseTX para Fast Ethernet sobre cableado de fibra óptica. Se basa en el estándar IEEE 802.3. Ver también 100BaseFX, 100BaseTX, Fast Ethernet e IEEE 802.3.

100VG-AnyLAN :
Tecnología de medios Fast Ethernet y Token Ring de 100 Mbps que utiliza cuatro pares de cableado UTP de Categoría 3, 4 ó 5. Esta tecnología de transporte de alta velocidad, desarrollada por Hewlett-Packard, puede operar en redes Ethernet 10BaseT existentes. Se basa en el estándar IEEE 802.12. Ver también IEEE 802.12.

10Base2 :
Especificación Ethernet de banda base de 10 Mbps que utiliza un cable coaxial delgado de 50 ohmios. 10Base2, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia de 185 metros por segmento. Ver también Ethernet e IEEE 802.3.

10Base5 :
Especificación Ethernet de banda base de 10 Mbps que utiliza un cable coaxial de banda base estándar (grueso) de 50 ohmios. 10Base5 forma parte de la especificación de capa física de banda base IEEE 802.3 y tiene un límite de distancia de 500 metros por segmento. Ver también Ethernet e IEEE 802.3.

10BaseF :
Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BaseFB, 10BaseFL y 10BaseFP para Ethernet a través de cableado de fibra óptica. Ver también 10BaseFB, 10BaseFL, 10BaseFP y Ethernet.

10BaseFB :
Especificación Ethernet de banda base de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFB forma parte de la especificación 10BaseF de IEEE. No se utiliza para conectar estaciones de usuario, sino para establecer un backbone de señalización síncrona que permite que se conecten segmentos y repetidores adicionales a la red. Los segmentos 10BaseFB pueden tener hasta 2000 metros de largo. Ver también 10BaseF y Ethernet.

10BaseFL :
Especificación Ethernet de banda base de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFL forma parte de la especificación 10BaseF de IEEE y, aunque puede interoperar con FOIRL, se encuentra diseñada para reemplazar a la especificación FOIRL. Los segmentos 10BaseFL pueden tener una longitud de hasta 1000 metros si se los utiliza con FOIRL y de hasta 2000 metros si se utiliza exclusivamente 10BaseFL. Ver también 10BaseF y Ethernet.

10BaseFP :
Especificación Ethernet de banda base de fibra pasiva de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFP forma parte de la especificación 10BaseF de IEEE. Organiza varios computadores en una topología en estrella sin el uso de repetidores. Los segmentos 10BaseFP pueden tener una longitud de hasta 500 metros. Ver también 10BaseF y Ethernet.

10BaseT :
Especificación Ethernet de banda base de 10 Mbps que utiliza dos pares de cableado de par trenzado (Categoría 3, 4 ó 5): un par para transmitir datos y otro para recibirlos. 10BaseT, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia aproximado de 100 metros por segmento. Ver también Ethernet y IEEE 802.3.

10Broad36 :
Especificación Ethernet de banda ancha de 10 Mbps que utiliza cable coaxial de banda ancha. 10Broad36 forma parte de la especificación IEEE 802.3 y tiene un límite de distancia de 3600 metros por segmento. Ver también Ethernet e IEEE 802.3.

fibra local 8B/10B :
fibra local de 8 bytes/10 bytes. Medio físico de canal de fibra que admite velocidades de hasta 149,76 Mbps en fibra multimodo.

ABM :
Modo de Compensación Asíncrono. Modo de comunicación HDLC (y protocolo derivativo) que admite comunicaciones punto a punto orientadas a iguales entre dos estaciones, en el cual cualquiera de las estaciones puede iniciar la transmisión.

ACK :
Ver Acuse de recibo

ACL (*lista de control de acceso*) **:**
Lista mantenida por un router de Cisco para controlar el acceso desde o hacia un router para varios servicios (por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interfaz en particular del router). Ver también ACL extendida y ACL estándar.

ACL estándar (*lista de control de acceso estándar*) **:**
ACL que filtra basándose en la máscara y dirección origen. Las listas de acceso estándares autorizan o deniegan todo el conjunto de protocolos TCP/IP. Ver también ACL, ACL extendida.

ACL extendida (*lista de control de acceso extendida*) **:**
ACL que verifica las direcciones origen y destino. Comparar con ACL estándar. Ver también ACL.

actualización del enrutamiento :
Mensaje que se envía desde el router para indicar si la red es accesible y la información de costo asociada. Normalmente, las actualizaciones del enrutamiento se envían a intervalos regulares y luego de que se produce un cambio en la topología de la red. Comparar con actualización relámpago.

actualización del horizonte dividido :
Técnica de enrutamiento en la cual se impide que la información acerca de los routers salga de la interfaz del router a través de la cual se recibió la información. Las actualizaciones del horizonte dividido son útiles para evitar los bucles de enrutamiento.

actualización inversa :
Función de IGRP destinada a evitar grandes bucles de enrutamiento. Las actualizaciones inversas indican explícitamente que una red o subred no se puede alcanzar, en lugar de implicar que una red no se puede alcanzar al no incluirla en las actualizaciones.

actualización relámpago :
Proceso mediante el cual se envía una actualización antes de que transcurra el intervalo de actualización periódica para notificar a otros routers acerca de un cambio en la métrica.

adaptador :
Ver NIC

administración de errores :
Una de cinco categorías de administración de red (administración de costos, de la configuración, de rendimiento y de seguridad)
definidas por ISO para la administración de redes OSI. La administración de errores intenta asegurar que las fallas de la red se detecten y controlen.

administración de red :
Uso de sistemas o acciones para mantener, caracterizar o realizar el diagnóstico de fallas de una red.

administrador de red :
Persona a cargo de la operación, mantenimiento y administración de una red.

ADSL (*asymmetric digital subscriber line*) **:**
Línea Digital del Suscriptor Asimétrica. Una de las cuatro tecnologías DSL. ADSL entrega mayor ancho de banda hacia abajo (desde la oficina central al lugar del cliente) que hacia arriba (desde el lugar del cliente a la oficina central). Las tasas hacia abajo oscilan entre 1.5 a 9 Mbps, mientras que el ancho de banda hacia arriba oscila entre 16 a 640 kbps. Las transmisiones a través de ADSL funcionan a distancias de hasta 5,488 metros sobre un único par de cobre trenzado. Vea también DSL, HDSL, SDSL y VDSL.

AFP (*Protocolo de archivo AppleTalk*) **:**
Protocolo de capa de presentación que permite que los usuarios compartan archivos de datos y programas de aplicación que residen en un servidor de archivos. AFP reconoce archivos compartidos de AppleShare y Mac OS.

alcance de cable :
Intervalo de números de red válidos para su uso por parte de nodos en una red extendida AppleTalk. El valor del alcance de cable puede ser un solo número de red o una secuencia contigua de varios números de red. Las direcciones de los nodos se asignan con base en el valor de alcance de cable.

algoritmo :
Ver protocolo.

algoritmo de árbol de extensión :
Algoritmo utilizado por el Protocolo de árbol de Extensión para crear un árbol de extensión. A veces abreviado como STA.

almacenamiento en caché :
Forma de réplica en la cual la información obtenida durante una transacción anterior se utiliza para procesar transacciones posteriores.

almacenamiento y envío :
Técnica de conmutación de paquetes en la que las tramas se procesan completamente antes de enviarse al puerto apropiado. Este procesamiento incluye calcular el CRC y verificar la dirección destino. Además, las tramas se deben almacenar temporalmente hasta que los recursos de la red (como un enlace no utilizado) estén disponibles para enviar el mensaje.

analizador de protocolo :
Ver analizador de red.

analizador de red :
Dispositivo de hardware o software que le brinda diversas funciones de diagnóstico de fallas de la red, incluyendo decodificadores de paquete específicos del protocolo, pruebas de diagnóstico de fallas específicas preprogramadas, filtrado de paquetes y transmisión de paquetes.

ancho de banda :
Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Asimismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

anillo :
Conexión de dos o más estaciones en una topología circular lógica. La información se pasa de forma secuencial entre estaciones activas. Token Ring, FDDI y CDDI se basan en esta topología.

anillos dobles contrarrotantes :
Topología de red en la que dos rutas de señales, cuyas direcciones son opuestas, existen en una red de transmisión de tokens. FDDI y CDDI se basan en este concepto.

ANSI (*Instituto Nacional Americano de Normalizacion*) **:**
Organización voluntaria compuesta por corporativas, organismos del gobierno y otros miembros que coordinan las actividades relacionadas con estándares, aprueban los estándares nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante organizaciones internacionales de estándares. ANSI ayuda a desarrollar estándares de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional), y la Organización Internacional para la Normalización.

aplicación :
Programa que ejecuta una función directamente para un usuario. Los clientes FTP y Telnet son ejemplos de aplicaciones de red.

aplicación cliente/servidor :
Aplicación que se almacena en una posición central en un servidor y a la que tienen acceso las estaciones de trabajo, lo que hace que sean fáciles de mantener y proteger.

APPN (*Internetwork avanzada de par a par*) **:**
Mejoramiento de la arquitectura original SNA de IBM. APPN maneja el establecimiento de una sesión entre nodos de iguales, cálculos de ruta transparentes y dinámicos, y priorización del tráfico APPC.

aprendizaje de la dirección MAC :
Servicio que caracteriza a un switch de aprendizaje en el que se guarda la dirección MAC origen de cada paquete recibido, de modo que los paquetes que se envían en el futuro a esa dirección se pueden enviar solamente a la interfaz de switch en la que está ubicada esa dirección. Los paquetes cuyo destino son direcciones de broadcast o multicast no reconocidas se envían desde cada interfaz de switch salvo la de origen. Este esquema ayuda a reducir el tráfico en las LAN conectadas. El aprendizaje de las direcciones MAC se define en el estándar IEEE 802.1.

ARA (*Acceso Remoto AppleTalk*) **:**
Protocolo que brinda a los usuarios de Macintosh acceso directo a la información y recursos de un sitio remoto AppleTalk.

ARP (*Protocolo de Resolucion de Direcciones*) **:**
Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826. Comparar con RARP.

ARP proxy (*ARP proxy (protocolo proxy de resolución de direcciones)*) :
Variación del protocolo ARP en el cual un dispositivo intermedio (por ejemplo, un router) envía una respuesta ARP en nombre de un nodo final al host solicitante. ARP proxy puede reducir el uso del ancho de banda en enlaces WAN de baja velocidad.

ARPANET :
Red de la Agencia de proyectos de Investigación Avanzada. Una red de conmutación de paquetes de gran importancia establecida en 1969. ARPANET fue desarrollada durante los años 70 por BBN y financiada por ARPA (y luego DARPA). Con el tiempo dio origen a la Internet. El término ARPANET se declaró oficialmente en desuso en 1990.

AS (*sistema autonomo*) :
Conjunto de redes bajo una administración común que comparte una estrategia de enrutamiento en común. También denominado dominio de enrutamiento. La Agencia de Asignación de Números Internet le asigna al AS un número de 16 bits.

ASBR (*Router límite de sistema autonomo*) :
ABR ubicado entre un sistema autónomo OSPF y una red no OSPF. Los ASBR ejecutan OSPF y otro protocolo de enrutamiento, como RIP. Los ASBR deben residir en un área OSPF no sustitutiva.

ASCII (*Código americano normalizado para el intercambio de la información*) :
Código de 8 bits (7 bits más paridad) para la representación de caracteres.

asignación de direcciones :
Técnica que permite que diferentes protocolos interoperen convirtiendo direcciones de un formato a otro. Por ejemplo, al enrutar IP en X.25, las direcciones IP deben asignarse a las direcciones X.25 para que la red X.25 pueda transmitir los paquetes IP

atenuación :
Pérdida de energía de la señal de comunicación

ATM (*modo de transferencia asíncrona*) :
Estándar internacional para relay de celdas en el que varios tipos de servicios (por ejemplo, transmisión de voz, vídeo o datos) se transmiten en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de las celdas se produzca en el hardware, reduciendo así los retardos de tránsito. ATM se encuentra diseñado para aprovechar los medios de transmisión de alta velocidad como E3, SONET y T3.

ATP (*Protocolo de Transaccion AppleTalk*) :
Protocolo a nivel de transporte que brinda un servicio de transacción libre de pérdidas entre sockets. El servicio permite intercambios entre dos clientes de sockets, donde uno de los clientes solicita al otro que realice una tarea en particular y que informe los resultados. ATP enlaza la solicitud y la respuesta juntas para asegurar un intercambio confiable de pares de solicitud/respuesta.

AUI (*interfaz de unidad de conexion*) :
Interfaz IEEE 802.3 entre una MAU y una tarjeta de interfaz de red. El término AUI también puede hacer referencia al puerto del panel posterior al que se puede conectar un cable AUI, como los que pueden encontrarse en la tarjeta de acceso Ethernet del LightStream de Cisco. También denominado cable transceptor.

AURP (*Protocolo de enrutamiento AppleTalk basado en actualización*) :
Método para encapsular tráfico AppleTalk en el encabezado de un protocolo ajeno, permitiendo la conexión de dos o más internetworks de redes AppleTalk no contiguas a través de una red ajena (como TCP/IP) para formar una WAN AppleTalk. Esta conexión se denomina túnel AURP. Además de su función de encapsulamiento, AURP mantiene tablas de enrutamiento para toda la WAN AppleTalk intercambiando información de enrutamiento entre routers exteriores.

autenticación :
Con respecto a la seguridad, la verificación de la identidad de una persona o proceso.

backbone :
Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

balanceo de la carga :
En el enrutamiento, la capacidad de un router para distribuir el tráfico a lo largo de todos sus puertos de red que están a la misma distancia desde la dirección destino. Los buenos algoritmos de balanceo de carga usan velocidad de
línea e información de confiabilidad. El balanceo de carga aumenta el uso de segmentos de red, aumentando así el ancho de banda efectivo de la red.

banda ancha :
Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etcétera).

Banyan VINES :
Ver VINES.

base de información de administración. :
Ver MIB.

BECN (*notificacion de la congestion retrospectiva*) :
Bit colocado por una red Frame Relay en las tramas que viajan en sentido opuesto al de las tramas que encuentran una ruta congestionada. Los dispositivos DTE que reciben tramas con el bit BECN pueden solicitar que los niveles de protocolos más elevados tomen las medidas de control de flujo que consideren adecuadas. Ver también FECN.

BGP (*protocolo de gateway frontenzo*) :
Protocolo de enrutamiento interdominios que reemplaza a EGP. BGP intercambia información de accesibilidad con otros sistemas BGP y se define en RFC 1163.

binario :
Sistema numérico compuesto por unos y ceros (1 = encendido; 0 = apagado).

bit :
Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno. Ver también byte.

BOOTP (*Protocolo Bootstrap*) :
Protocolo usado por un nodo de red para determinar la dirección IP de sus interfaces Ethernet para afectar al inicio de la red.

bootstrap :
Operación simple predeterminada para cargar instrucciones que a su vez hacen que se carguen otras instrucciones en la memoria o que hacen entrar a otros modos de configuración.

BPDU (*unidad de datos de protocolo de puente*) **:**
Paquete Hello del protocolo Spanning-Tree (árbol de extensión) que se envía a intervalos configurables para intercambiar información entre los puentes de la red.

BRI (*Interfaz de Acceso Básico*) **:**
Interfaz RDSI compuesta por dos canales B y un canal D para la comunicación por un circuito conmutado de voz, vídeo y datos. Comparar con PRI.

broadcast :
Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast. Ver también dirección broadcast, dominio de broadcast y tormenta de broadcast.

bucle :
Ruta donde los paquetes nunca alcanzan su destino, sino que pasan por ciclos repetidamente a través de una serie constante de nodos de red.

bucle local :
Cableado (normalmente de cables de cobre) que se extiende desde la demarcación a la oficina central del proveedor de la WAN.

búfer de memoria :
área de la memoria donde el switch almacena los datos destino y de transmisión.

buffer (*aprox. colchon*) **:**
Memoria intermedia que se utiliza como memoria de datos temporal durante una sesión de trabajo.

bug (*aprox. bicho error*) **:**
Error en el hardware o en el software que, si bien no impide la ejecución de un programa, perjudica el rendimiento del mismo al no permitir la realización de determinadas tareas o al complicar su normal funcionamiento. Esta palabra también se utiliza para referirse a un intruso.

búsqueda de direcciones de internet :
Ver ping.

byte :
Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits). Ver también bit.

cable coaxial :
Cable que consta de un conductor cilíndrico externo hueco, que reviste a un conductor con un solo cable interno. Actualmente se usan dos tipos de cable coaxial en las LAN: el cable de 50 ohmios, utilizado para la señalización digital, y el cable de 75 ohmios, utilizado para señales analógicas y señalización digital de alta velocidad.

cable de fibra óptica :
Medio físico que puede conducir una transmisión de luz modulada. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otra parte no es susceptible a la interferencia electromagnética, y permite obtener velocidades de datos más elevadas. A veces se denomina fibra óptica.

cableado backbone :
Cableado que brinda interconexiones entre los armarios de cableado, entre los armarios de cableado y el POP, y entre edificios que forman parte de la misma LAN

cableado de categoria 1 :
Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 1 se utiliza para comunicaciones telefónicas y no es adecuado para la transmisión de datos. Ver también UTP.

cableado de categoria 2 :
Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 2 puede transmitir datos a velocidades de hasta 4 Mbps. Ver también UTP.

cableado de categoria 3 :
Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps. Ver también UTP.

cableado de categoria 4 :
Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 4 se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Ver también UTP.

cableado de categoria 5 :
Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps. Ver también UTP.

cableado vertical :
cableado del backbone

caching :
La tecnología caching permite que las páginas web solicitadas con mayor frecuencia por los usuarios puedan ser almacenadas en múltiples locaciones geográficas. De esta manera, cuando un cibernauta requiere una página determinada, ésta puede bajarse desde el servidor más cercano, en lugar de hacerse desde una única computadora centralizada, localizada en algún lugar lejano del mundo. Esta tecnología permite mayores velocidades de navegación para el usuario final y ahorros en tiempos y costos.

CAM (*memoria de contenido direccionable*) **:**
Memoria que mantiene una base de datos precisa y funcional

canal B (*canal principal*) :
En RDSI, canal de dúplex completo de 64 kbps usado para enviar datos del usuario. Ver también 2B+D, canal D, canal E y canal H.

canal D (*canal de datos*) :
Canal RDSI, de 16 kbps (BRI) o 64 kbps (PRI), dúplex completo. Ver también canal B, canal D, canal E, y canal H.

canal de eco :
Ver canal E.

canal E (*canal de eco*) :
Canal de control de conmutación de circuito RDSI de 64 kbps. El canal E se definió en la especificación RDSI de la UIT-T de 1984, pero se abandonó en la especificación de 1988. Comparar con canal B, canal D y canal E.

canal H (*canal de alta velocidad*) :
Canal de velocidad primaria RDSI de dúplex completo que opera a 384 kbps. Comparar con canal B, canal D y canal E.

CAP, Competitive Access Provider (*Empresa proveedora de acceso que busca competir con las empresas ya establecidas*) :

capa de acceso :
Capa en la cual una LAN o grupo de LAN, normalmente Ethernet o Token Ring, le ofrecen a los usuarios acceso frontal a los servicios de la red.

capa de aplicación :
Capa 7 del modelo de referencia OSI. Esta capa brinda servicios de red para aplicaciones del usuario. Por ejemplo, una aplicación de procesamiento de textos recibe servicios de transferencia de archivos en esta capa. Ver también modelo de referencia OSI.

capa de control de enlace de datos :
Capa 2 del modelo arquitectónico SNA. Es responsable por la transmisión de datos a través de un enlace físico en particular. Corresponde aproximadamente a la capa de enlace de datos del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

capa de control de flujo de datos :
Capa 5 del modelo arquitectónico SNA. Esta capa determina y maneja las interacciones entre socios de sesión, especialmente el flujo de datos. Corresponde a la capa de sesión del modelo de referencia OSI. Ver también capa de control de enlace de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión

capa de control de ruta :
Capa 3 del modelo arquitectónico SNA. Esta capa ejecuta servicios de control secuencial relacionados con el reensamblaje adecuado de datos. La capa de control de ruta también es responsable por el enrutamiento. Equivale aproximadamente a la capa de red del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control físico, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

capa de control de transmisión :
Capa 4 en el modelo arquitectural SNA. Esta capa tiene la responsabilidad de establecer, mantener y finalizar las sesiones SNA, secuenciar mensajes de datos y controlar el flujo de nivel de sesión. Equivale a la capa de transporte del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación y capa de servicios de transacción.

capa de control físico :
Capa 1 del modelo arquitectónico SNA. Esta capa es responsable por las especificaciones físicas de los enlaces físicos entre sistemas finales. Corresponde a la capa física del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

capa de distribución :
Capa en la que la distribución de los servicios de red se produce en múltiples LAN en un entorno de WAN. Esta es la capa en la que se encuentra la red backbone de la WAN, normalmente basada en Fast Ethernet.

capa de enlace :
Ver capa de enlace de datos.

capa de enlace de datos :
Capa 2 del modelo de referencia . Esta capa proporciona un tránsito de datos confiable a través de un enlace físico. La capa de enlace de datos se ocupa del direccionamiento físico, topología de red, disciplina de línea, notificación de errores, entrega ordenada de las tramas y control de flujo. IEEE dividió esta capa en dos subcapas: la subcapa MAC y la subcapa LLC. A veces se denomina simplemente capa de enlace. Corresponde aproximadamente a la capa de control de enlace de datos del modelo SNA. Ver también modelo de referencia OSI.

capa de presentacion :
Capa 6 del modelo de referencia OSI. Esta capa suministra representación de datos y formateo de códigos, junto con la negociación de la sintaxis de transferencia de datos. Asegura que los datos que llegan de la red puedan ser utilizados por la aplicación y garantiza que la información enviada por la aplicación pueda transmitirse a través de la red. Ver también modelo de referencia OSI.

capa de red :
Capa 3 delmodelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales. La capa de red es la capa en la que se produce el enrutamiento. Equivale aproximadamente a la capa de control de ruta del modelo SNA. Ver también modelo de referencia OSI.

capa de servicios de presentación :
Capa 6 del modelo arquitectónico SNA. Esta capa proporciona administración de recursos de red, servicios de presentación de sesión y algo de administración de aplicaciones. Equivale aproximadamente a la capa de presentación del modelo de referencia OSI.

capa de servicios de transacción :
Capa 7 en el modelo de arquitectura SNA. Representa las funciones de aplicación del usuario, por ejemplo, hojas de cálculo, procesamiento de texto o correo electrónico, mediante los cuales los usuarios interactúan con la red. Equivale aproximadamente a la capa de aplicación del modelo de referencia OSI. Ver también capa de control de flujo de datos, capa de control de enlace
de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación y capa de control de transmisión.

capa de sesión :
Capa 5 del modelo de referencia OSI. Esta capa establece, mantiene y administra las sesiones entre las aplicaciones. Ver también modelo de referencia OSI.

capa de transporte :
Capa 4 del modelo de referencia OSI. Esta capa segmenta y reensambla los datos dentro de una corriente de datos. La capa de transporte tiene el potencial de garantizar una conexión y ofrecer transporte confiable. Ver también modelo de referencia OSI.

capa física :
Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Corresponde a la capa de control físico del modelo SNA. Ver también modelo de referencia OSI.

capa núcleo :
Capa que suministra conexiones rápidas de área amplia entre sitios geográficamente remotos, uniendo una serie de redes de campus en una WAN de empresa o corporativa.

carga :
Parte de una celda, trama o paquete que contiene información de capa superior (datos).

carga :
Cantidad de actividad de un recurso de la red, como por ejemplo un router o un enlace.

carrier común :
Compañía de servicios privada, que opera bajo licencia, a cargo del suministro de servicios de comunicación al público, con tarifas reguladas.

CCITT (*Comité de Consultoría Internacional para Telefonía y Telegrafía*) **:**
Organización internacional responsable por el desarrollo de estándares de comunicación. Actualmente ha pasado a llamarse UIT-T..

CDDI (*Interfaz de datos distribuidos por cobre*) :
Implementación de protocolos FDDI en cableado STP y UTP. CDDI transmite a distancias relativamente cortas (unos 100 metros), con velocidades de datos de 100 Mbps mediante una arquitectura
de doble anillo para brindar redundancia. Se basa en el estándar dependiente del medio físico de par trenzado (TPPMD) de ANSI. Comparar con FDDI.

CHAP (*Protocolo de autenticacion de intercambio de señales*) :
Función de seguridad utilizada en líneas que usan el encapsulamiento PPP para evitar el acceso no autorizado. CHAP no impide por sí mismo el acceso no autorizado, pero sí identifica el extremo remoto; el router o servidor de acceso determina entonces si se permite el acceso a ese usuario.

CIDR (*enrutamiento sin clase entre dominios*) :
Técnica reconocida por BGP y basada en el agregado de rutas. CIDR permite que los routers agrupen rutas para reducir la cantidad de información de enrutamiento transportada por los routers principales. Con CIDR, un conjunto de redes IP aparece ante las redes ajenas al grupo como una entidad única de mayor tamaño.

cifrado, codificado (*encryption*) :
Método para proteger los datos de un acceso no autorizado a los mismos. Se utiliza normalmente en Internet para sustraer el correo electrónico.

CIR (*velocidad de informacion suscrita*) :
Velocidad en bits por segundo, a la que el switch Frame Relay acepta transferir datos.

circuito :
Ruta de comunicaciones entre dos o más puntos.

circuito asíncrono :
Señal que se transmite sin sincronización precisa. Estas señales normalmente tienen diferentes frecuencias y relaciones de fases. Las transmisiones asíncronas habitualmente encapsulan caracteres individuales en bits de control (denominados bits de inicio y detención) que designan el principio y el final de cada carácter. Ver también circuito síncrono.

circuito síncrono :
Señal transmitida con sincronización precisa. Estas señales tienen la misma frecuencia, y los caracteres individuales están encapsulados en bits de control (denominados bits de arranque y bits de parada) que designan el comienzo y el fin de cada carácter.

circuito virtual :
Circuito creado para garantizar la comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por un par VPI/VCI y puede ser permanente (PVC) o conmutado (SVC). Los circuitos virtuales se usan en Frame Relay y X.25. En ATM, un circuito virtual se denomina canal virtual. A veces se abrevia VC.

circuito virtual permanente :
Ver PVC.

cliente :
Nodo o programa de software (dispositivo front-end) que requiere servicios de un servidor. Ver también servidor.

cliente :
Nodo o programa de software (dispositivo front-end) que requiere servicios de un servidor. Ver también servidor.

cliente/servidor :
Arquitectura de la relación entre una estación de trabajo y un servidor en una red.

CMIP (*Protocolo de informacion de administracion comun*) **:**
Protocolo de administración de red de OSI, creado y estandarizado por ISO para el control de redes heterogéneas. Ver también CMIS.

CMIS (*Servicios de informacion de administracion comun*) **:**
Interfaz de servicio de administración de red de OSI creada y estandarizada por ISO para el control de redes heterogéneas. Ver también CMIP.

CO (*oficina central*) **:**
Oficina local de la compañía telefónica en la cual todos los pares locales en un área determinada se conectan y donde ocurre la conmutación de circuito de las líneas del subscriptor.

codificación :
Técnicas eléctricas utilizadas para transmitir señales binarias.

codificación :
Proceso a través del cual los bits son representados por voltajes.

cola :
En general, una lista ordenada de elementos a la espera de ser procesados. 2. En enrutamientos, una reserva de paquetes que esperan ser enviados por una interfaz de router.

cola de prioridad :
Función de enrutamiento en la cual se da prioridad a las tramas de una cola de salida de interfaz basándose en diversas características, tales como el protocolo, el tamaño de paquete y el tipo de interfaz.

colisión :
En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

colocación en cola :
Proceso en el que las ACL pueden designar ciertos paquetes para que los procese un router antes que cualquier otro tráfico, con base en el protocolo.

compañía telefónica regional en EE.UU. :
Ver RBOC.

compartir la carga :
Uso de dos o más rutas para enrutar paquetes al mismo destino de forma igualitaria entre múltiples routers para equilibrar el trabajo y mejorar el desempeño de la red

concentrador :
Ver hub.

conexión a tierra de referencia de señal :
Punto de referencia que usan los dispositivos informáticos para medir y comparar las señales digitales entrantes. Punto de referencia que usan los dispositivos informáticos para medir y comparar las señales digitales entrantes.

conexión doble :
Topología de red en la que un dispositivo se encuentra conectado a la red a través de dos puntos de acceso independientes (puntos de conexión). Un punto de acceso es la conexión primaria, y el otro es una conexión de reserva que se activa en caso de falla de la conexión primaria.

conexión punto a multipunto :
Uno de dos tipos fundamentales de conexión. En ATM, una conexión punto a multipunto es una conexión unidireccional en la cual un solo sistema final de origen (denominado nodo raíz) se conecta a múltiples sistemas finales de destino (denominados hojas). Comparar con conexión punto a punto.

conexión punto a punto :
Uno de dos tipos fundamentales de conexión. En ATM, una conexión punto a punto puede ser una conexión unidireccional o bidireccional entre dos sistemas finales ATM. Comparar con conexión punto a multipunto.

confiabilidad :
Proporción entre los mensajes de actividad esperados y recibidos de un enlace. Si la relación es alta, la línea es confiable. Utilizado como métrica de enrutamiento.

congestión :
Tráfico que supera la capacidad de la red.

conmutación :
Proceso de tomar una trama entrante de una interfaz y enviarla a través de otra interfaz.

conmutación asimétrica :
Tipo de conmutación que brinda conexiones conmutadas entre puertos de ancho de banda diferente, como una combinación de puertos de 10 Mbps y 100 Mbps.

conmutación de circuito :
Sistema de conmutación en el que un circuito físico dedicado debe existir entre el emisor y el receptor durante la "llamada". Se usa ampliamente en la red de la compañía telefónica. La conmutación de circuito se puede comparar con la contención y la transmisión de tokens como método de acceso de canal y con la conmutación de mensajes y la conmutación de paquetes como técnica de conmutación.

conmutación de paquetes :
Método de networking en el cual los nodos comparten el ancho de banda entre sí enviando paquetes

conmutación rápida :
Conmutación que ofrece el nivel más bajo de latencia, enviando inmediatamente un paquete después de recibir la dirección destino.

conmutación sin fragmentos :
Técnica de conmutación que filtra, antes de que comience el envío, los fragmentos de colisión que constituyen la mayoría de los paquetes de errores..

consola :
Equipo terminal de datos a través del cual se introducen los comandos en un host.

contención :
Método de acceso en el que los dispositivos de la red compiten para obtener permiso para acceder a un medio físico.

Control de Acceso al Medio :
Ver MAC.

control de enlace de datos síncrono :
Ver SDLC.

control de enlace lógico :
Ver LLC.

control de flujo :
Técnica para garantizar que una entidad transmisora no supere la capacidad de recepción de datos de una entidad receptora. Cuando los búferes del dispositivo receptor están llenos, se envía un mensaje al dispositivo transmisor para que suspenda la transmisión hasta que se hayan procesado los datos en los búferes. En las redes IBM, esta técnica se llama pacing.

control del flujo de ventana deslizante :
Método de control de flujo en el que un receptor le da a un transmisor permiso para transmitir datos hasta que una ventana esté llena. Cuando la ventana está llena, el emisor debe dejar de transmitir hasta que el receptor publique una ventana de mayor tamaño. TCP, otros protocolos de transporte, y varios otros protocolos de la capa de enlace de datos usan este método de control de flujo.

convergencia :
Velocidad y capacidad de un grupo de dispositivos de internetwork que ejecutan un protocolo de enrutamiento específico para concordar sobre la topología de una internetwork de redes luego de un cambio en esa topología.

cookie ***(galleta)*** **:**
Pequeño archivo que se genera en el disco duro del usuario desde una página web. Un archivo de esta clase puede registrar las actividades del usuario en la página visitada. Su uso es controvertido, puesto que implica un registro de datos en la computadora del usuario.

costo :
Valor arbitrario, basado normalmente en el número de saltos, ancho de banda del medio, u otras medidas, que es asignado por un administrador de red y utilizado para comparar diversas rutas a través de un entorno de internetwork de redes. Los valores de costo utilizados por los protocolos de enrutamiento determinan la ruta más favorable hacia un destino en particular: cuanto menor el costo, mejor es la ruta

CPE (*equipo terminal del abonado*) :
Equipo de terminación (por ejemplo: terminales, teléfonos y módems) proporcionados por la compañía telefónica, instalados en el sitio del cliente y conectados a la red de la compañía telefónica.

CSMA/CD (*Acceso multiple con deteccion de portadora y deteccion de colisiones*) :
Mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que colisionan. Esta colisión subsecuentemente demora las retransmisiones desde esos dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

CSU/DSU (*unidad de servicio de canal/unidad de servicio de datos*) :
Dispositivo de interfaz digital que conecta el equipamiento del usuario final al par telefónico digital local.

cuenta al infinito :
Problema que puede ocurrir al enrutar algoritmos que son lentos para converger, en los cuales los routers incrementan continuamente el número de saltos a redes particulares. Normalmente se impone algún número arbitrario de saltos para evitar este problema.

DARPA (*Agencia de Proyectos de Investigacion Avanzada para la Defensa*) :
Agencia gubernamental de los EE.UU. que financió la investigación y la experimentación con la Internet. Antiguamente denominada ARPA, volvió a utilizar ese nombre a partir de 1994. Ver también ARPA.

DAS (*estacion de doble conexion*) :
Dispositivo conectado a los anillos FDDI primario y secundario. La doble conexión brinda redundancia para el anillo FDDI. Si falla el anillo primario, la estación puede reiniciar el anillo primario al anillo secundario, aislando la falla y recuperando la integridad del anillo. También denominada estación Clase A. Comparar con SAS.

datagrama :
Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de la Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

datagrama IP :
Unidad fundamental de información transmitida a través de la Internet. Contiene direcciones origen y destino junto con datos y una serie de campos que definen cosas tales como la longitud del datagrama, la suma de verificación de el encabezado y señaladores para indicar si el datagrama se puede fragmentar o ha sido fragmentado.

datos :
Datos de protocolo de capa superior.

DCE (*equipo de transmisión de datos*) :
Dispositivo usado para convertir los datos del usuario del DTE en una forma aceptable para la instalación de servicios de WAN. Comparar con DTE

DDN (*Red de Defensa de los Datos*) :
Red militar de los EE.UU. compuesta por una red no clasificada (MILNET) y varias redes secretas y de secreto máximo. DDN es operada y mantenida por DISA.

DDP (*Protocolo de entrega de datagramas*) :
Protocolo de capa de red AppleTalk responsable por la entrega socket-a-socket de datagramas en una internetwork AppleTalk.

DDR (*enrutamiento por llamada telefónica bajo demanda*) :
Técnica utilizada para que un router inicie y cierre dinámicamente sesiones conmutadas por circuito a medida que las estaciones transmisoras finales las necesiten.

DECnet :
Grupo de productos de comunicaciones (incluyendo un conjunto de protocolos) desarrollado y soportado por Digital Equipment Corporation. DECnet/ OSI (también denominado DECnet Fase V) es la iteración más reciente y es compatible con los protocolos OSI y protocolos Digital propietarios. Fase IV Prime brinda soporte para direcciones inherentes MAC que permiten que los nodos DECnet coexistan con sistemas que ejecutan otros protocolos que tengan restricciones de dirección MAC.

demarcación :
Punto donde termina CPE y comienza la parte del bucle local del servicio. A menudo se produce en el POP de un edificio

demultiplexión :
Separación en múltiples corrientes de entrada que han sido multiplexadas en una señal física común en múltiples corrientes de salida. Ver también multiplexión

determinación de ruta :
Decisión de cuál es la ruta que debe recorrer el tráfico en la nube de red. La determinación de ruta se produce en la capa de red del modelo de referencia OSI.

DHCP :
Protocolo de configuración dinámica del Host. Protocolo que proporciona un mecanismo para asignar direcciones IP de forma dinámica, de modo que las direcciones se pueden reutilizar automáticamente cuando los hosts ya no las necesitan.

dial up (*marcar*) :
Establecer comunicación entre dos computadoras.

Dial up Access (*Acceso por marcación telefónica*) :

dirección :
Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso o dispositivo de red en particular

dirección broadcast :
Dirección especial reservada para enviar un mensaje para todas las estaciones. Por lo general, una dirección broadcast es una dirección destino MAC compuesta exclusivamente por números uno. Comparar con dirección multicast y dirección unicast. Ver también broadcast.

dirección de capa MAC :
Verdirección MAC

dirección de enlace de datos :
Ver dirección MAC.

dirección de hardware :
Ver dirección MAC

dirección de host :
Ver número de host

dirección de presentación OSI :
Dirección utilizada para ubicar una entidad de aplicación de OSI. Está compuesta por una dirección de red OSI y hasta tres selectores, uno para cada entidad de transporte, sesión y presentación.

dirección de protocolo :
Ver dirección de red

dirección de punto decimal :
Anotación común para direcciones IP con el formato a.b.c.d, donde cada número representa, en decimales, 1 byte de la dirección IP de 4 bytes. También denominada dirección de punto o anotación punteada en cuatro partes.

dirección de red :
Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada dirección de protocolo

dirección de subred :
Parte de una dirección IP especificada como la subred por la máscara de subred.

dirección de zona de multicast :
Dirección multicast dependiente de enlace de datos en el que un nodo recibe los broadcasts NBP dirigidos a esta zona.

dirección del salto siguiente :
Dirección IP del siguiente router en una ruta hacia determinado destino.

dirección destino :
Dirección de un dispositivo de red que recibe datos. Ver también dirección origen

dirección física :
Ver dirección MAC.

dirección IP :
Dirección de 32 bits asignada a los hosts mediante TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D o E) y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred, y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet (dirección IP)

dirección MAC (*Control de Acceso al Medio*) :
Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

dirección multicast :
Dirección única que se refiere a múltiples dispositivos de red. Sinónimo de dirección de grupo. Comparar con dirección broadcast y dirección unicast. Ver también multicast.

dirección origen :
Dirección de un dispositivo de red que envía datos.

dirección unicast :
Dirección que especifica un solo dispositivo de red. Comparar con dirección broadcast y dirección multicast.

direccionamiento plano :
Esquema de direccionamiento que no utiliza una jerarquía lógica para determinar una ubicación.

división en capas :
Separación de funciones de networking utilizadas por el modelo de referencia OSI, que simplifica las tareas requeridas para que dos computadores se comuniquen entre sí.

DLCI (*identificador de conexión de enlace de datos*) :
Valor que especifica un PVC o un SVC en una red Frame Relay. En la especificación Frame Relay básica, los DLCI son significativos localmente (es decir, dispositivos conectados que usan diferentes valores para especificar la misma conexión). En la especificación extendida LMI, los DLCI son significativos globalmente (es decir, los DLCI especifican dispositivos de extremos individuales).

DNS (*Sistema de denominación de dominio*) :
Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

DoD (*Departamento de Defensa*) :
Organización gubernamental de los EE.UU. responsable por la defensa nacional. El Departamento de Defensa ha financiado con frecuencia el desarrollo de protocolos de comunicación.

dominio (*domain*) :
Nombre empleado para referirse a una máquina o a un servidor determinado en Internet. El nombre de dominio comprende varias partes; la última parte, o sufijo, designa el nivel de estructura superior. Ejemplos de dominios:
.com (organizaciones comerciales)
.edu (organizaciones educativas)
.gov (organizaciones gubernamentales)

dominio de broadcast :
Conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo dentro de ese conjunto. Los dominios de broadcast normalmente se encuentran limitados por routers porque los routers no envían tramas de broadcast. Ver también broadcast.

dominio de colisión :
En Ethernet, el área de la red en la que las tramas que colisionan se propagan. Los repetidores y los hubs propagan las colisiones, mientras que los switches de LAN, puentes y routers no lo hacen..

DRP (*Protocolo de Enrutamiento DECnet*) :
Esquema de enrutamiento propietario introducido por Digital Equipment Corporation en DECnet Fase III. En DECnet Fase V, DECnet completó su transición a los protocolos de enrutamiento OSI (ES-IS e IS-IS).

DSAP (*punto de acceso al servicio destino*) :
SAP del nodo de red designado en el campo Destino de un paquete. Comparar con SSAP. Ver también SAP (punto de acceso al servicio).

DSL (*digital subscriber line*) :
Línea Digital del Suscriptor. Tecnología de red que permite conexiones de ancho de banda ancha sobre el cable de cobre a distancias limitadas. Hay cuatro tipos o sabores de DSL: ADSL, HDSL, SDSL y VDSL. Todas estas tecnologías funcionan a través de pares de módems, con un módem localizado en la oficina central y el otro en el lugar del cliente. Debido a que la mayoría de tecnologías DSL no utilizan todo el ancho de banda del par trenzado, queda espacio disponible para un canal de voz.

DTE (*equipo terminal de datos*) :
Dispositivo en el extremo del usuario de una interfaz usuario a red que sirve como origen de datos, destino, o ambos. DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y utiliza normalmente señales de sincronización generadas por el DCE. DTE incluye dispositivos tales como computadores, traductores de protocolo y multiplexores. Comparar con DCE

E1 :
Esquema de transmisión digital de área amplia utilizado especialmente en Europa, que lleva datos a una velocidad de 2,048 Mbps. Las líneas E1 pueden ser dedicadas para el uso privado de carriers comunes. Comparar con T1.

E3 :
Esquema de transmisión digital de área amplia utilizado especialmente en Europa, que lleva datos a una velocidad de 34,368 Mbps. Las líneas E3 pueden ser dedicadas para el uso privado de carriers comunes. Comparar con T3.

EEPROM (*memoria programable de solo lectura borrable electricamente*) :
EPROM que se puede borrar utilizando señales eléctricas aplicadas a contactos (pins) específicos.

EIA (*Asociacion de Industrias Electronicas*) :
Grupo que especifica los estándares de transmisiones eléctricas. EIA y TIA han desarrollado en conjunto numerosos estándares de comunicación de amplia difusión, como EIA/TIA-232 y EIA/TIA-449.

EIA/TIA568 :
Estándar que describe las características y aplicaciones para diversos grados de cableado UTP.

encabezado :
Información de control colocada antes de los datos al encapsularlos para la transmisión en red.

encapsulamiento :
Colocación en los datos de un encabezado de protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes
que no son similares, toda la trama de una red se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red. Ver también tunneling.

encapsular :
Colocar un encabezado de protocolo en particular a los datos. Por ejemplo, a los datos de Ethernet se les agrega un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red simplemente se coloca en el encabezado utilizado por el protocolo de enlace de datos de la otra red.

enlace :
Canal de comunicaciones de red que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor. Se utiliza con mayor frecuencia para referirse a una conexión de WAN. A veces se denomina línea o enlace de transmisión.

enlace dedicado :
Enlace de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse según lo requiera la transmisión. Ver también línea arrendada.

enlace punto a punto :
Enlace que proporciona una sola ruta preestablecida de comunicaciones de WAN desde las instalaciones del cliente a través de una red de carrier, como, por ejemplo, la de una compañía telefónica, a una red remota. También denominado enlace dedicado o línea arrendada.

enlace WAN :
Canal de comunicaciones de WAN que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

enrutador :
Vea router.

enrutamiento :
Proceso de descubrimiento de una ruta hacia el host destino. El enrutamiento es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

enrutamiento del camino más corto :
Enrutamiento que reduce al mínimo la distancia o costo de la ruta a través de una aplicación de un algoritmo.

enrutamiento dinámico :
Enrutamiento que se ajusta automáticamente a la topología de la red o a los cambios de tráfico. También denominado enrutamiento adaptable. Comparar con enrutamiento estático.

enrutamiento estático :
Ruta que se ha configurado e introducido explícitamente en la tabla de enrutamiento Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico. Comparar con enrutamiento dinámico.

enrutamiento multiprotocolo :
Enrutamiento en el que un router entrega paquetes desde distintos protocolos enrutados, como TCP/IP e IPX, en los mismos enlaces de datos.

enrutamiento por llamada telefónica bajo demanda :
Ver DDR.

envío :
Proceso para enviar una trama hacia su destino final mediante un dispositivo de internetwork.

envío de tramas :
Mecanismo a través del cual el tráfico basado en tramas, como HDLC y SDLC, atraviesa una red ATM.

EPROM :
memoria programable de sólo lectura borrable

EPROM (*memoria programable de solo lectura borrable*) **:**
Chips de memoria no volátil programados después de su fabricación y que, de ser necesario, pueden ser borrados por ciertos medios y reprogramados. Comparar con EEPROM y PROM

ES-IS (*Sistema Final a Sistema Intermedio*) **:**
Protocolo OSI que define el modo en que los sistemas finales (hosts) se anuncian a los sistemas intermedios (routers). Ver también IS-IS.

escalabilidad :
Capacidad de una red para aumentar de tamaño sin que sea necesario realizar cambios importantes en el diseño general.

Especificación de convenciones de función-llamada que define una interfaz a un servicio. :
Serie de protocolos de comunicaciones diseñados por Apple Computer que consta de dos fases. La Fase 1, la versión más antigua, admite una sola red física que puede tener un solo número de red y estar en una sola zona. La Fase 2 admite varias redes lógicas en una sola red física y permite que las redes se encuentren en más de una zona. Ver también zona.

espera :
Función de IGRP que rechaza nuevas rutas para el mismo destino durante un período determinado de tiempo.

estación con doble conexión :
Ver DAS.

estación local doble :
Dispositivo conectado a múltiples concentradores FDDI para lograr redundancia.

estación secundaria :
En protocolos síncronos de bit de la capa de enlace de datos (por ejemplo, HDLC), una estación que responde a los comandos desde una estación primaria. A veces se le denomina simplemente secundaria.

estándar :
Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

Ethernet :
Especificación de LAN de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y funcionan con una variedad de tipos de cable a 10 Mbps. Ethernet se asemeja a la serie de estándares IEEE 802.3. Ver también Fast Ethernet.

Ethernet de dúplex completo :
Capacidad de transmisión simultánea de datos entre una estación emisora y una estación receptora. Comparar con Ethernet semidúplex.

Ethernet semidúplex :
Capacidad de transmisión de datos en una sola dirección a la vez entre una estación transmisora y otra receptora. Comparar con Ethernet de dúplex completo.

evaluación loopback :
Prueba en la que se envían las señales y luego se dirigen de vuelta hacia su origen desde un punto a lo largo de la ruta de comunicaciones. La evaluación loopback a menudo se usa para probar la capacidad de uso de la interfaz de la red.

Fast Ethernet :
Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de trama, mecanismos MAC, y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3. Ver también Ethernet.

FDDI (*Interfaz de datos distribuida por fibra*) :
Estándar de LAN, definido por ANSI X3T9.5, que especifica una red de transmisión de tokens de 100 Mbps que utiliza cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI usa una arquitectura de anillo doble para brindar redundancia. Comparar con CDDI y FDDI II.

FDDI II :
Estándar ANSI que mejora FDDI. FDDI II brinda transmisión isócrona para circuitos de datos no orientado a conexión y circuitos de voz y vídeo orientados a conexión. Comparar con FDDI.

FECN (*notificacion explicita de la congestion*) :
Bit colocado por una red Frame Relay para informar a los dispositivos DTE que reciben las tramas que se produjo congestión en la ruta del origen hacia el destino. Los dispositivos DTE que reciben las tramas con el bit FECN pueden solicitar que los protocolos de más alto nivel tomen las medidas de control de flujo correspondientes. Ver también BECN.

fibra local 4B/5B :
fibra local de 4 bytes/5 bytes. Medio físico de canal de fibra utilizado para FDDI y ATM. Admite velocidades de hasta 100 Mbps en fibra multimodo.

fibra local 8B/10B :
fibra local de 8 bytes/10 bytes. Medio físico de canal de fibra que admite velocidades de hasta 149,76 Mbps en fibra multimodo.

fibra local de 4 bytes/5 bytes :
Verfibra local 4B/5B

fibra multimodo :
Fibra óptica que soporta la propagación de múltiples frecuencias de luz.

fibra óptica :
Fibra basada en el vidrio, que sustituye a los clásicos cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a gran distancia. La información no se transmite mediante impulsos eléctricos, sino que se modula en una onda electromagnética generada por un láser.

filtrado de tráfico local :
Proceso por el cual un puente filtra (descarta) tramas cuyas direcciones MAC origen y destino se ubican en la misma interfaz en el puente, lo que evita que se envíe tráfico innecesario a través del puente. Definido en el estándar IEEE 802.1.

filtro :
En general, se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, por ejemplo, una dirección origen, dirección destino o protocolo y determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

firewall :
Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

firmware :
Instrucciones de software establecidas de forma permanente o semipermanente en la ROM.

flooding :
Técnica de transmisión de tráfico utilizada por switches y puentes, en la cual el tráfico recibido por una interfaz se envía a todas las interfaces de ese dispositivo, salvo a la interfaz desde la cual se recibió originalmente la información.

flujo :
Corriente de datos que viajan de un punto a otro a través de una red (por ejemplo, desde una estación de la LAN a otra). Se pueden transmitir varios flujos en un solo circuito.

Foro ATM :
Organización internacional fundada en 1991 de forma conjunta por Cisco Systems, NET/ADAPTIVE, Northern Telecom y Sprint, con el fin de desarrollar y promover acuerdos de implementación basados en estándares para tecnología de ATM. El Foro ATM expande los estándares oficiales desarrollados por ANSI y UIT-T, y desarrolla acuerdos de implementación antes de los estándares oficiales.

fragmentación :
Proceso de dividir un paquete en unidades más pequeñas al transmitir a través de un medio de red que no puede acomodar el tamaño original del paquete.

fragmento :
Parte de un paquete mayor que se ha dividido en unidades más pequeñas. En las redes Ethernet, también se hace referencia a esto como una trama con un límite inferior al límite permitido de 64 bytes.

Frame Relay :
Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25, el protocolo para el cual se considera por lo general un reemplazo.

FTP (*Protocolo de Transferencia de Archivos*) :
Protocolo de aplicación, parte de la pila de protocolo TCP/IP, utilizado para transferir archivos entre nodos de red. FTP se define en la RFC 959.

full dúplex :
Capacidad para la transmisión simultánea de datos entre la estación emisora y la estación receptora. Comparar con semidúplex y unidireccional.

gateway :
En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término router se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro. Comparar con router.

gateway de último recurso :
Router al cual se envían todos los paquetes no enrutables.

Gb (*gigabit*) :
Aproximadamente 1.000.000.000 de bits.

Gbps (*gigabytes por segundo*) :
Medida de velocidad de transferencia

gigabit :
Ver Gb

GNS (*Obtener Servidor Mas Cercano*) :
Paquete de solicitud enviado por un cliente en una red IPX para ubicar el servidor activo más cercano de un tipo en particular. Un cliente de red IPX emite una solicitud GNS para pedir una respuesta directa de un servidor conectado o una respuesta de un router que le indique en qué parte de la internetwork de redes se puede ubicar el servicio. GNS es parte de IPX SAP.

GPRS (*Servicio general de paquetes por radio*) :
General Package Radio Service. Servicio general de paquetes por radio que permite manejar datos sobre redes celulares de una manera más eficiente.

grupo de circuito :
Agrupación de líneas seriales asociadas que unen dos puentes. Si uno de los enlaces seriales en un grupo de circuito se encuentra en el árbol de extensión para una red, cualquiera de los enlaces seriales en el grupo de circuito se puede usar para blanceo de carga. Esta estrategia de balanceo de carga evita los problemas de ordenamiento de los datos, asignando cada dirección destino a un enlace serial en particular.

GUI (*interfaz grafica del usuario*) :
Entorno del usuario que utiliza representaciones gráficas y textuales de las aplicaciones de entrada y salida y de la estructura jerárquica (o de otro tipo) en la que se almacena la información. Las convenciones como botones, iconos y ventanas son típicas, y varias acciones se realizan mediante un apuntador (como un ratón). Microsoft Windows y Apple Macintosh son ejemplos importantes de plataformas que usan GUI.

HCC (*interconexion horizontal*) :
Armario de cableado donde el cableado horizontal se conecta a un panel de conmutación conectado mediante cableado backbone al MDF.

HCC (*interconexion horizontal*) :
Armario de cableado donde el cableado horizontal se conecta a un panel de conmutación conectado mediante cableado backbone al MDF.

HDLC (*Control de Enlace de Datos de Alto Nivel*) :
Protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO. HDLC especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación.

HDLC (*Control de Enlace de Datos de Alto Nivel*) :
Protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO. HDLC especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación

HDSL (*high-data-rate digital subscriber line*) :
Línea Digital del Suscriptor de alta velocidad. Una de las cuatro tecnologías DSL. HDSL entrega 1.544 Mbps de ancho de banda hacia arriba (desde el lugar del cliente a la oficina central) y hacia abajo (desde la oficina central al lugar del cliente), sobre dos pares de cobre trenzados. Debido a que HDSL ofrece velocidad T1, las compañías telefónicas han estado utilizando HDSL para entregar acceso local para servicios T1 en la medida de lo posible. El funcionamiento de HDSL está limitado a un rango de distancia de hasta 3658.5 metros. Se utilizan repetidoras de señal para ampliar el servicio. HDSL requiere dos pares trenzados. Por esta razón es utilizado principalmente para conexiones de red PBX, sistemas de circuito de carrier digitales, POPs de intercambio, servidores de Internet y redes de datos privadas. Vea también DSL, ADSL, SDSL y VDSL.

header (*cabecera*) :
Parte inicial de un paquete de datos a transmitir, que contiene la información sobre los puntos de origen y de destino de un envío y sobre el control de errores. Esta expresión se aplica con frecuencia, y de manera errónea, sólo a envío de correo electrónico, por lo que recibe el nombre de "mailheader", pero normalmente cualquier paquete de datos que se transmite de computadora a computadora contiene una "header".

herramienta de punción :
Herramienta accionada por resorte que se usa para cortar y conectar cables en un jack o en un panel de conmutación.

herramienta de punción :
Herramienta accionada por resorte que se usa para cortar y conectar cables en un jack o en un panel de conmutación.

hexadecimal (*base 16*) :
Representación numérica que usa los dígitos del 0 al 9, con su significado habitual, y las letras de la A a la F, para representar dígitos hexadecimales con valores del 10 al 15. El dígito ubicado más a la derecha cuenta por uno, el siguiente por múltiplos de 16, el siguiente por 16^2=256, etc.

host :
Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers. Ver también nodo.

HTML (*Lenguaje de Etiquetas por Hipertexto*) :
Formato simple de documentos en hipertexto que usa etiquetas para indicar cómo una aplicación de visualización,
como por ejemplo un navegador de la Web, debe interpretar una parte determinada de un documento.

HTTP (*Protocolo de Transferencia de Hipertexto*) :
Protocolo utilizado por los navegadores y servidores de la Web para transferir archivos, como archivos de texto y de gráficos.

hub :
1. En general, dispositivo que sirve como centro de una topología en estrella. También denominado repetidor multipuerto.
2. Dispositivo de hardware o software que contiene múltiples módulos de red y equipos de red independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen las señales enviadas a través de ellos).

IAB (*Comite de Arquitectura de Internet*) :
Comité de investigadores de internetwork de redes que discute temas relativos a la arquitectura de Internet. Responsables por designar una serie de grupos relacionados con Internet, como IANA, IESG e IRSG. El IAB es nombrado por los síndicos de la ISOC. Ver también IANA, IESG, IRSG e ISOC.

IANA (*Agencia de Asignacion de Numeros Internet*) :
Organización que funciona bajo el auspicio de la ISOC como parte del IAB. La IANA delega la autoridad de asignar espacios de direcciones IP y nombres de dominio al InterNIC y otras organizaciones. La IANA mantiene también una base de datos de identificadores de protocolo asignados que se utilizan en la pila TCP/IP, incluyendo los números de sistemas autónomos.

ICMP (*Protocolo de mensajes de control en Internet*) :
Protocolo Internet de capa de red que informa errores y brinda información relativa al procesamiento de paquetes IP. Documentado en RFC 792.

IDF (*Servicio de distribucion intermedia*) :
Sala de comunicaciones secundaria para un edificio donde funciona una topología de networking en estrella. El IDF depende del MDF.

IEC (*Comision Electrotecnica Internacional*) :
Grupo industrial que escribe y distribuye estándares para productos y componentes eléctricos.

IEEE (*Instituto de Ingeniería Electrica y Electronica*) :
Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares de mayor importancia para las LAN de la actualidad.

IEEE 802.2 :
Protocolo de LAN de IEEE que especifica una implementación del la subcapa LLC de la capa de enlace de datos. IEEE 802.2 maneja errores, entramados, control del flujo y la interfaz de servicio de la capa de red (Capa 3). Se utiliza en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

IEEE 802.3 :
Protocolo IEEE para LAN que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a varias velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT y 10Broad36. Las variaciones físicas para Fast Ethernet incluyen 100BaseTX y 100BaseFX.

IEEE 802.5 :
Protocolo de LAN de IEEE que especifica la implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.5 usa acceso de transmisión de tokens a 4 ó 16 Mbps en cableado STP o UTP y desde el punto de vista funcional y operacional es equivalente a Token Ring de IBM. Ver también Token Ring.

IETF (*Fuerza de Tareas de Ingeniería de Internet*) :
Fuerza de tareas compuesta por más de 80 grupos de trabajo responsables por el desarrollo de estándares de Internet. IETF opera bajo el auspicio de ISOC.

IGRP (*Protocolo de enrutamiento de gateway interior*) :
Protocolo desarrollado por Cisco para tratar los problemas asociados con el enrutamiento en redes heterogéneas de gran envergadura

IGRP extendido (Protocolo de enrutamiento de gateway interior extendido) :
Versión avanzada de IGRP desarrollada por Cisco. Ofrece propiedades de convergencia y eficacia operativa superiores, y combina las ventajas de los protocolos del estado de enlace con las de los protocolos por vector distancia. Comparar con IGRP. Ver también OSPF y RIP.

Impedimento de congestión :
Mecanismo mediante el cual una red ATM controla el tráfico que entra en la red para minimizar las demoras. A fin de usar los recursos de manera más eficiente, el tráfico de baja prioridad se descarta en el límite de la red si las condiciones indican que no se podrá entregar

Información final :
Información de control añadida a los datos cuando se encapsulan para una transmisión de red. Comparar con encabezado.

informática cliente/servidor :
Sistemas de red de computación distribuida (procesamiento) en los que las responsabilidades de transacción se dividen en dos partes: el cliente (front-end) y el servidor (back-end). Ambos términos (cliente y servidor) se pueden aplicar a los programas de software o a los dispositivos informáticos en sí. También se denomina informática distribuida. Comparar con informática de par a par.

informática de par a par :
La informática de par a par requiere que cada dispositivo de red cumpla las partes de cliente y servidor en una aplicación. También describe la comunicación entre implementaciones de la misma capa del modelo de referencia OSI en dos dispositivos de red distintos. Comparar con arquitectura cliente/servidor.

Instituto de Ingenieros Eléctricos y Electrónicos :
Ver IEEE.

Intercambio de paquetes de internetwork :
Ver IPX

Intercambio de Paquetes Secuenciado :
Ver SPX

intercambio de señales :
Secuencia de mensajes intercambiados entre dos o más dispositivos de red para garantizar la sincronización de transmisión antes de enviar datos del usuario.

interconexión horizontal :
Ver HCC.

interconexión vertical :
Ver VCC.

interfaz :
1. Conexión entre dos sistemas o dispositivos. 2. En terminología de enrutamiento, una conexión de red. 3. En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas. 4. Límite entre capas adyacentes del modelo de referencia OSI.

Interfaz de Acceso Básico :
Ver BRI

interfaz de administración local :
Ver LMI.

Interfaz de datos distribuida por fibra :
Ver FDDI.

interfaz de red :
Límite entre una red de carrier y una instalación de propiedad privada

Interfaz de Red a Usuario :
Ver UNI

Internet :
La internetwork de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la llamó Internet DARPA, y no debe confundirse con el término general internet.

internet :
Abreviatura de internetwork de redes. No debe confundirse con la Internet. Ver internetwork de redes.

internetwork :
Industria dedicada a la conexión de redes entre sí. Este término se refiere a productos, procedimientos y tecnologías.

internetwork de redes :
Agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (de modo general) como una sola red.

internetwork de sistemas abiertos :
Ver OSI.

InterNIC :
Organización que brinda asistencia al usuario, documentación, capacitación, servicios de registro para nombres de dominio de Internet, direcciones de red y otros servicios a la comunidad de Internet. Antiguamente denominada NIC.

interoperabilidad :
Capacidad de los equipos de informática de diferentes fabricantes para comunicarse entre sí en una red.

interrupción :
Mensaje que envía un agente SNMP al NMS, a una consola, o a una terminal para indicar que se ha producido un evento importante, por ejemplo, que se ha alcanzado una condición o umbral definido específicamente.

intervalo de mensajes de actividad :
Período de tiempo transcurrido entre cada mensaje de actividad enviado por un dispositivo de red.

IOS (*Sistema Operativo de Internetwork*) **:**
Ver software Cisco IOS.

IP (*Protocolo Internet*) **:**
Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientado a conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Se define en RFC 791. IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación no orientado a conexión de máximo esfuerzo. Ver también IPv6.

IPv6 (*IP version 6*) :
Reemplazo de la versión actual de IP (versión 4). IPv6 brinda soporte para identificación de flujo en el encabezado del paquete, que se puede usar para identificar flujos. Anteriormente denominado IPng (IP de próxima generación).

IPX (*Intercambio de Paquetes de Internetwork*) :
Protocolo de capa de red de NetWare utilizado para transferir datos desde los servidores a las estaciones de trabajo. IPX es similar a IP y XNS.

IPX de Novell :
Ver IPX.

IPXWAN (*red de área amplia IPX*) :
Protocolo que negocia opciones de extremo a extremo para nuevos enlaces. Cuando aparece un enlace, los primeros paquetes IPX enviados son paquetes IPXWAN que negocian las opciones para el enlace. Cuando las opciones IPXWAN se determinan con éxito, comienza la transmisión IPX normal. Definido por RFC 1362.

IS-IS (*Sistema Intermedio a Sistema Intermedio*) :
Protocolo de enrutamiento jerárquico de estado de enlace OSI basado en el enrutamiento DECnet Fase V, en el que los IS (routers) intercambian información de enrutamiento con base en una métrica única para determinar la topología de la red. Ver también ES-IS y OSPF.

ISO (*Organizacion Internacional para la Normalizacion*) :
Organización internacional que tiene a su cargo una amplia gama de estándares, incluyendo aquellos referidos al networking. ISO desarrolló el modelo de referencia OSI, un modelo popular de referencia de networking.

ISOC (*Sociedad Internet*) :
Organización internacional sin fines de lucro fundada en 1992, que coordina la evolución y el uso de la Internet. Además la ISOC delega facultades a otros grupos relacionados con la Internet, por ejemplo el IAB. La ISOC tiene su sede en Reston, Virginia, EE.UU. Ver también IAB

kb (*kilobit*) :
Aproximadamente 1.000 bits.

kB (*kilobyte*) :
Aproximadamente 1.000 bytes.

kbps (*kilobits por segundo*) :
Medida de velocidad de transferencia.

kBps (*kilobytes por segundo*) :
Medida de velocidad de transferencia.

Kilobit :
Ver kb.

kilobits por segundo :
Ver kbps

Kilobyte :
Ver kB.

Kilobytes por segundo :
Ver kBps.

LAN (*red de área local*) :
Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas. Comparar con MAN y WAN. Ver también VLAN.

LAPB (*Procedimiento de Acceso al Enlace Balanceado*) :
Protocolo de capa de enlace de datos en la pila de protocolo X.25. LAPB es un protocolo orientado a bit derivado de HDLC. Ver también HDLC y X.25.

LAPD (*Procedimiento de Acceso al Enlace en el Canal D*) :
Protocolo de capa de enlace de datos RDSI para el canal D. LAPD deriva del protocolo LAPB y se diseñó primariamente para satisfacer los requisitos de señalización del acceso básico de RDSI. Definido por las Recomendaciones de UIT-T Q.920 y Q.921.

LAT (*Transporte de area Local*) :
Protocolo de terminal virtual de red desarrollado por Digital Equipment Corporation.

Latencia :
Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede el permiso para transmitir. Intervalo de tiempo que toma el procesamiento de una tarea.

LCP (*Protocolo de Control de Enlace*) :
Protocolo que proporciona un método para establecer, configurar, mantener y terminar una conexión punto a punto.

LEC, Local Exchange Carrier (*Empresa Telefónica Local*) :

Lenguaje de Etiquetas por Hipertexto :
Ver HTML

límite de tiempo :
Evento que se produce cuando un dispositivo de red espera saber lo que sucede con otro dispositivo de red dentro de un período de tiempo especificado, pero nada de esto sucede. El agotamiento del límite de tiempo resultante generalmente hace que se deba volver a transmitir la información o que se termine la sesión entre los dos dispositivos.

línea arrendada :
Línea de transmisión reservada para una portadora de comunicaciones para uso privado de un cliente. Una línea arrendada es un tipo de línea dedicada. Ver también enlace dedicado.

línea de acceso telefónico :
Circuito de comunicaciones establecido por una conexión conmutada por circuito que usa la red de la compañía telefónica

LLC (*control de enlace lógico*) **:**
La más alta de las dos subcapas de enlace de datos definidas por el IEEE. La subcapa LLC maneja el control de errores, control del flujo, entramado y direccionamiento de subcapa MAC. El protocolo LLC más generalizado es IEEE 802.2, que incluye variantes no orientado a conexión y orientadas a conexión.

LMI (*Interfaz de Administracion Local*) **:**
Conjunto de mejoras a la especificación básica Frame Relay. LMI incluye soporte para un mecanismo de actividad, que verifica que los datos estén fluyendo; un mecanismo de multicast, que le ofrece al servidor de red su DLCI local y DLCI de multicast; direccionamiento global, que le ofrece a los DLCI significado global en lugar de local en las redes Frame Relay; y un mecanismo de estado, que proporciona un informe de estado constante sobre los DLCI que el switch conozca.

localizador de recursos uniforme :
Ver URL

LSA (*publicación del estado de enlace*) **:**
Paquete de broadcast utilizado por los protocolos del estado de enlace que contiene información acerca de vecinos y costos de ruta. Los LSA son utilizados por los routers receptores para mantener sus tablas de enrutamiento. A veces se denomina paquete de estado de enlace (LSP).

MAC (*Control de Acceso al Medio*) **:**
Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir. Ver también capa de enlace de datos y LLC.

malla :
Topología de red en la cual los dispositivos se organizan de manera administrable, segmentada, con varias interconexiones, a menudo redundantes, colocadas de forma estratégica entre los nodos de la red. Ver también malla completa y malla parcial.

mapa de ruta :
Método para controlar la redistribución de rutas entre dominios de enrutamiento.

máscara :
Ver máscara de dirección y máscara de subred.

máscara de dirección :
Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host. A veces se llama simplemente máscara

máscara de subred :
Máscara utilizada para extraer información de red y subred de la dirección IP.

máscara wildcard :
Cantidad de 32 bits que se utiliza junto con una dirección IP para determinar qué bits en una dirección IP deben ser ignorados cuando se compara dicha dirección con otra dirección IP. Una máscara wildcard se especifica al configurar una ACL.

MAU (unidad de conexión al medio) :
Dispositivo utilizado en redes Ethernet e IEEE 802.3 que proporciona una interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que puede ser incorporada a una estación, o puede ser un dispositivo separado, lleva a cabo funciones de la capa física, incluyendo la conversión de datos digitales de la interfaz Ethernet, la detección de colisiones, y la inyección de bits en la red. Denominada a veces unidad de acceso al medio, también abreviada como MAU , o transceptor

máximo esfuerzo de entrega :
Entrega que se produce cuando un sistema de red no usa un sistema sofisticado de acuse de recibo para garantizar la entrega confiable de la información.

Mb (megabit) :
Aproximadamente 1.000.000 de bits.

megabits por segundo :
Ver Mbps.

megabyte :
Ver MB.

memoria de acceso aleatorio :
Ver RAM.

memoria flash :
Almacenamiento no volátil que se puede borrar eléctricamente y reprogramar, de manera que las imágenes de software se pueden almacenar, iniciar y reescribir según sea necesario. La memoria flash fue desarrollada por Intel y se otorga bajo licencia a otras empresas de semiconductores.

mensaje :
Agrupación lógica de información de la capa de aplicación, a menudo compuesta por una cantidad de agrupaciones lógicas de las capas inferiores, por ejemplo, paquetes. Los términos datagrama, trama, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

mensaje de actividad :
Mensaje enviado por un dispositivo de red para informar a otro dispositivo de red que el circuito virtual entre ellos se mantiene activo.

método de acceso :
1. En general, la manera en que los dispositivos de red acceden al medio de red. 2. Software dentro de un procesador SNA que controla el flujo de información a través de una red.

método de corte :
Técnica de conmutación de paquetes que hace pasar los datos por un switch de manera tal que la parte frontal de un paquete salga del switch en el puerto de salida antes de que el paquete termine de entrar al puerto de entrada. Un dispositivo que usa conmutación de paquetes por método de corte lee, procesa y envía los paquetes inmediatamente después de que se verifica la dirección destino y se determina el puerto saliente. También denominado conmutación de paquete al vuelo.

métrica de enrutamiento :
Método mediante el cual un protocolo de enrutamiento determina que una ruta es mejor que otra. Esta información se almacena en tablas de enrutamiento. Las métricas incluyen ancho de banda, costo de la comunicación, retardo, número de saltos, carga, MTU, costo de ruta, y confiabilidad. A menudo denominada simplemente métrica.

MIB (*Base de Información de Administración*) **:**
Base de datos de información de administración de la red utilizada y mantenida por un protocolo de administración de la red, por ejemplo SNMP. El valor de un objeto MIB se puede modificar o recuperar mediante los comandos SNMP, generalmente a través del sistema de administración de red GUI. Los objetos MIB se organizan en una estructura de árbol que incluye las ramas pública (estándar) y privada (propietaria).

modelo cliente/servidor :
Descripción común de los servicios de red y los procesos del usuario modelos (programas) de estos servicios. Los ejemplos incluyen el paradigma servidor de nombres/resolución de nombres del DNS y las relaciones entre servidor de archivos/archivo-cliente como NFS y hosts sin disco.

Modelo de referencia de Internetwork de Sistemas Abiertos. :
Ver modelo de referencia OSI.

Modelo de referencia OSI (*Modelo de referencia de internetwork de sistemas abiertos*) **:**
Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, tales como el direccionamiento, el control de flujo, el control de errores, el encapsulamiento y la transferencia confiable de mensajes. La capa inferior (la capa física) es la más cercana a la tecnología de los medios. Las dos capas inferiores se implementan en el hardware y en el software, y las cinco capas superiores se implementan sólo en el software. La capa superior (la capa de aplicación) es la más cercana al usuario. El modelo de referencia OSI se usa a nivel mundial como método para la enseñanza y la comprensión de la funcionalidad de la red. Similar en algunos aspectos a SNA. Ver capa de aplicación, capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

módem :
Contracción de modulador y demodulador. Puesto que la computadora y la red telefónica tradicional utilizan diferentes técnicas para la transmisión de datos – la computadora utiliza la técnica digital, y la línea telefónica tradicional emplea la analógica - , entre ambos se debe conectar un módem, que convierte la señal de la computadora en señal acústica, y que en el punto de destino la convierte de nuevo en señal digital.

modo de compensación asíncrono :
Ver ABM.

modo de transferencia asincrona :
Ver ATM.

modo de transferencia asincrona :
Ver ATM.

modo de transferencia asincrona :
Ver ATM.

Módulo Cargable de NetWare :
Ver NLM.

monitor activo :
Dispositivo a cargo de las funciones de mantenimiento de una red Token Ring. Se selecciona un nodo de red para ser el monitor activo si tiene la dirección MAC más alta del anillo. El monitor activo se encarga de las tareas de mantenimiento de anillo; por ejemplo, garantiza que no se pierdan los tokens y que las tramas no circulen indefinidamente.

MPLS, Multiprotocol Label Switching (*Switching de etiquetas multiprotocolo*) **:**
MPLS es un estándar de la industria sobre el cual se basa la conmutación (switching) de etiquetas, las cuales identifican los diferentes tipos de información sobre la red. La tecnología MPLS le permite a un proveedor de servicio montar sobre su red servicios diferenciados a los cuales se tiene acceso a través del protocolo IP. MPLS permite que los usuarios tengan acceso a la red y se "matriculen" a algunos servicios específicos, sin que esto implique tener acceso a toda la red, es decir que se garantiza la privacidad y seguridad de la Información mediante la creación de redes virtuales privadas, VPNs.

MPLS ofrece tanto a los operadores como a los usuarios gran flexibilidad en la implementación de servicios basados en IP así como también facilidad en la implementación de múltiples esquemas de acceso y una alta disponibilidad.

MSAU (*unidad de acceso de estacion multiple*) **:**
Concentrador de cableado al que se conectan todas las estaciones finales de una red Token Ring. La MSAU suministra una interfaz entre estos dispositivos y la interfaz Token Ring de un router. A veces abreviada MAU.

MSAU (*unidad de acceso de estacion multiple*) **:**
Concentrador de cableado al que se conectan todas las estaciones finales de una red Token Ring. La MSAU suministra una interfaz entre estos dispositivos y la interfaz Token Ring de un router. A veces abreviada MAU.

MTU (*unidad maxima de transmision*) **:**
Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

multicast :
Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

multiplexión :
Esquema que permite que varias señales lógicas se transmitan de forma simultánea a través de un canal físico exclusivo. Comparar con demultiplexión.

NAK (*acuse de recibo negativo*) :
Respuesta que se envía desde un dispositivo receptor a un dispositivo transmisor que indica que la información recibida contiene errores. Comparar con acuse de recibo.

NAT (*traduccion de direcciones de red*) :
Mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. NAT permite que las organizaciones cuyas direcciones no son globalmente exclusivas se conecten a la Internet transformando esas direcciones en espacio de direccionamiento enrutable global. También denominado traductor de dirección de red.

NAUN (*vecino corriente arriba activo mas cercano*) :
En las redes Token Ring o IEEE 802.5, el dispositivo de red corriente arriba más cercano a cualquier dispositivo que aún esté activo

NCP (*Programa de control de red*) :
Programa que enruta y controla el flujo de datos entre un controlador de comunicaciones y otros recursos de red.

NetBEUI (*Interfaz de Usuario NetBIOS Extendida*) :
Versión mejorada del protocolo NetBIOS que usan los sistemas operativos de red (por ejemplo: LAN Manager, LAN Server, Windows for Workgroups y Windows NT). NetBEUI formaliza la trama de transporte y agrega funciones adicionales. NetBEUI implementa el protocolo OSI LLC2.

NetBIOS (*Sistema Basico de Entrada/Salida de Red*) :
Interfaz de programación de aplicación que usan las aplicaciones de una LAN IBM para solicitar servicios a los procesos de red de nivel inferior. Estos servicios incluyen establecimiento y finalización de sesión, así como transferencia de información.

NetWare :
Popular sistema operativo de red distribuido desarrollado por Novell. Proporciona acceso remoto transparente a archivos y varios otros servicios de red distribuidos.

networking :
Interconexión de estaciones de trabajo, dispositivos periféricos (por ejemplo, impresoras, unidades de disco duro, escáneres y CD-ROM) y otros dispositivos.

NFS (*Sistema de Archivos de Red*) :
Se utiliza comúnmente para designar un conjunto de protocolos de sistema de archivos distribuido, desarrollado por Sun Microsystems, que permite el acceso remoto a archivos a través de una red. En realidad, NFS es simplemente un protocolo del conjunto. Los protocolos NFS incluyen RPC y XDR. Estos protocolos son parte de una arquitectura mayor que Sun denomina ONC.

NIC (*Centro de Información de Red*) :
Organización cuyas funciones ha asumido InterNIC. Ver InterNIC.

NIC (*tarjeta de interfaz de red*) :
Tarjeta que brinda capacidades de comunicación de red hacia y desde un computador. También denominada adaptador

NLM (*Módulo Cargable NetWare*) :
Programa individual que se puede cargar en la memoria y que funciona como parte del sistema operativo de red NetWare.

NLSP (*Protocolo de Servicios de Enlace de NetWare*) :
Protocolo de enrutamiento de estado de enlace basado en IS-IS. La implementación de Cisco de NLSP también incluye variables y herramientas MIB para redistribuir el enrutamiento y la información SAP entre NLSP y otros protocolos de enrutamiento IPX.

NMS (*sistema de administracion de red*) :
Sistema que tiene la responsabilidad de administrar por lo menos parte de una red. Por regla general, un NMS es un computador bastante potente y bien equipado, como, por ejemplo, una estación de trabajo de ingeniería. Los NMS se comunican con los agentes para ayudar a realizar un seguimiento de las estadísticas y los recursos de la red.

no orientado a conexión :
Transferencia de datos sin un circuito virtual. Comparar con orientado a conexión. Ver también circuito virtual.

nodo :
Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo. Los nodos, que varían en cuanto al enrutamiento y a otras aptitudes funcionales; pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra dispositivo.

NOS (*sistema operativo de red*) :
Sistema operativo utilizado para hacer funcionar una red, como, por ejemplo, NetWare de Novell y Windows NT.

NT1 (*terminacion de red de tipo 1*) :
Dispositivo que conecta el cableado RDSI del suscriptor de cuatro alambres a la instalación de bucle convencional local de dos alambres.

NT2 (*terminacion de red de tipo 2*) :
Dispositivo que dirige el tráfico hacia y desde distintos dispositivos del suscriptor y el NT1. El NT2 es un dispositivo inteligente que realiza conmutación y concentración.

NTP (*Protocolo de Tiempo de Red*) :
Protocolo desarrollado sobre el TCP que garantiza la precisión de la hora local, con referencia a los relojes de radio y atómicos ubicados en la Internet. Este protocolo puede sincronizar los relojes distribuidos en milisegundos durante períodos de tiempo prolongados.

número de host :
Parte de una dirección IP que designa a qué nodo de la subred se realiza el direccionamiento. También denominada dirección de host.

número de la red :
Parte de una dirección IP que especifica la red a la que pertenece el host.

número de saltos :
Métrica de enrutamiento utilizada para medir la distancia entre un origen y un destino. RIP utiliza el número de saltos como su métrica exclusiva.

número de socket :
Número de 8 bits que identifica a un socket. Se pueden asignar como máximo 254 números de socket en un nodo AppleTalk.

NVRAM (*RAM no volátil*) **:**
Memoria RAM que conserva su contenido cuando se apaga una unidad.

obtener servidor más cercano :
Ver GNS.

octeto :
8 bits. En networking, el término octeto se utiliza a menudo (en lugar de byte) porque algunas arquitecturas de máquina utilizan bytes que no son de 8 bits de largo.

ODI (*Interfaz Abierta de Enlace de Datos*) **:**
Especificación de Novell que suministra una interfaz estandarizada para tarjetas de interfaz de red (NIC) que permite que múltiples protocolos usen una sola NIC.

oficina pequeña/oficina hogareña :
Ver SOHO.

orden de bytes de la red :
Ordenamiento estándar de la Internet de los bytes correspondientes a valores numéricos.

Organización internacional para la normalización :
Ver ISO.

orientado a conexión :
Transferencia de datos que requiere que se establezca un circuito virtual. Ver también no orientado a conexión y circuito virtual.

OSI (*Internetwork de sistemas abiertos*) **:**
Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

OSPF (*Primero la ruta libre mas corta*) **:**
Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet. Entre las características de OSPF se incluyen el enrutamiento de menor costo, el enrutamiento de múltiples rutas, y el balanceo de carga.

OUI (*identificador exclusivo de organización*) **:**
Tres octetos asignados por el IEEE en un bloque de direcciones de LAN de 48 bits.

panel de conmutación :
Conjunto de ubicaciones de pins y puertos que se pueden montar en un bastidor o en una consola en el armario de cableado. Los paneles de conmutación actúan como tableros de conmutación que conectan los cables de las estaciones de trabajo entre sí y con el exterior.

PAP (*Protocolo de Autenticación de Contraseña*) **:**
Protocolo de autenticación que permite que los PPP iguales se autentiquen entre sí. El router remoto que intenta conectarse al router local debe enviar una petición de autenticación A diferencia de CHAP, PAP pasa la contraseña y el nombre de host o nombre de usuario sin cifrar. PAP no evita el acceso no autorizado, sino que identifica el extremo remoto, el router o el servidor de acceso y determina si a ese usuario se le permite el acceso. PAP es compatible sólo con las líneas PPP. Comparar con CHAP.

papelera de bits :
Destino de los bits descartados, según lo determine el router.

paquete :
Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

paquete de temporizador :
Método utilizado para asegurarse de que un cliente todavía está conectado a un servidor NetWare. Si el servidor no ha recibido un paquete de parte de un cliente durante un período de tiempo determinado, envía a dicho cliente una serie de paquetes de temporizador. Si la estación no envía ninguna respuesta a una cantidad predefinida de paquetes de temporizador, el servidor deduce que la estación ya no está conectada y cierra la conexión para dicha estación.

paquete hello :
Paquete multicast utilizado por routers que utilizan ciertos protocolos de enrutamiento para el descubrimiento y recuperación de vecinos. Los paquetes hello también indican que un cliente se encuentra aún operando y que la red está lista.

PBX (*central telefónica privada*) **:**
Conmutador de un teléfono analógico o digital ubicado en las instalaciones del suscriptor y que se usa para conectar redes telefónicas privadas y públicas.

PDN (*red de datos públicos*) **:**
Red operada por el gobierno (como en el caso de Europa) o por entidades privadas para suministrar comunicaciones computacionales al público, generalmente cobrando una tarifa. Las PDN permiten que las pequeñas organizaciones creen una WAN sin los costos de equipamiento de los circuitos de larga distancia.

PDU (*unidad de datos de protocolo*) **:**
Término OSI equivalente a paquete.

petición de comentarios :
Ver RFC.

PHY :
1. Subcapa física. Una de las dos subcapas de la capa física de FDDI. 2. Capa física En ATM, la capa física se encarga de la transmisión de celdas a través de un medio físico que conecta dos dispositivos ATM. La PHY está compuesta por dos subcapas: PMD y TC.

pico de tensión :
Cualquier aumento de voltaje por sobre el 110% del voltaje normal transportado por una línea de alimentación eléctrica.

pila de protocolo :
Conjunto de protocolos de comunicación relacionados entre sí que operan de forma conjunta y, como grupo, dirigen la comunicación a alguna o a todas las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo, y a menudo un solo protocolo de la pila se refiere a varias capas a la vez. TCP/IP es una pila de protocolo típico.

ping *(búsqueda de direcciones de internet)* **:**
Mensaje de eco ICMP y su respuesta. A menudo se usa en redes IP para probar el alcance de un dispositivo de red.

plan de distribución :
Diagrama simple que indica la ubicación de los tendidos de cables y los números de las habitaciones a los que se dirigen.

PLP *(protocolo a nivel de paquete)* **:**
Protocolo de capa de red en la pila de protocolo X.25. Algunas veces denominado X.25 Nivel 3 y protocolo X.25 Ver también X.25.

POP *(punto de presencia)* **:**
Punto de interconexión entre las instalaciones de comunicación suministradas por la compañía telefónica y el servicio de distribución principal del edificio.

portadora :
Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos.

POST *(pruebas al inicio)* **:**
Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando se enciende.

postergación :
Retardo en la retransmisión que se produce cuando tiene lugar una colisión

PPP *(Protocolo Punto a Punto)* **:**
Sucesor del SLIP, un protocolo que suministra conexiones router a router y host a red a través de circuitos síncronos y asíncronos.

PRI *(Interfaz de Acceso Principal)* **:**
Interfaz RDSI al acceso principal. El acceso principal consta de un canal D único de 64 Kbps más 23 canales B (T1) o 30 canales B (E1) para voz o datos. Comparar con BRI.

Primero la ruta libre más corta :
Ver OSPF.

Procedimiento de acceso al enlace balanceado :
Ver LAPB.

Procedimiento de acceso al enlace en el canal D :
Ver LAPD.

Programa de Control de Red :
Ver NCP.

PROM (*memoria programable de sólo lectura*) **:**
ROM que puede programarse utilizando equipo especial. Las PROM pueden ser programadas solamente una vez. Comparar con EPROM.

protocolo :
Descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.

Protocolo Bootstrap :
Ver BOOTP

protocolo de árbol de extensión :
Protocolo puente que utiliza el algoritmo de árbol de extensión, lo que habilita un puente de aprendizaje para funcionar dinámicamente en torno de bucles en una topología de red creando un árbol de extensión. Los puentes intercambian mensajes BPDU con otros puentes para detectar bucles y luego eliminarlos al desactivar las interfaces de puente seleccionadas. Se refiere tanto al estándar IEEE 802.1 de Protocolo de árbol de extensión, como al Protocolo de árbol de extensión más antiguo, de Digital Equipment Corporation, en el cual se basa. La versión de IEEE admite dominios de puente y permite que el puente desarrolle una topología sin bucles a través de una LAN extendida. Generalmente, se prefiere la versión de IEEE en lugar de la de Digital.

Protocolo de Autenticación de Contraseña :
Ver PAP.

Protocolo de autenticación de intercambio de señales :
Ver CHAP.

Protocolo de Control de Enlace :
Ver LCP.

protocolo de control de transmisión :
Ver TCP.

protocolo de datagrama de usuario :
Ver UDP.

protocolo de enrutamiento :
Protocolo que logra el enrutamiento mediante la implementación de un protocolo de enrutamiento específico. Entre los ejemplos de protocolo de enrutamiento se incluyen IGRP, OSPF y RIP. Comparar con protocolo enrutado.

Protocolo de enrutamiento DECnet :
Ver DRP.

protocolo de enrutamiento híbrido balanceado :
Protocolo que combina aspectos de los protocolos de estado de enlace y por vector distancia. Ver también protocolo de enrutamiento de estado de enlace y protocolo de enrutamiento por vector distancia.

protocolo de enrutamiento por estado de enlace :
Protocolo de enrutamiento en el cual cada router realiza un broadcast o multicast de información referente al costo de alcanzar cada uno de sus vecinos a todos los nodos de la internetwork de redes. Los protocolos de estado de enlace crean una vista coherente de la red y por lo tanto no son propensos a bucles de enrutamiento, pero por otro lado para lograr esto deben sufrir dificultades informáticas relativamente mayores y un tráfico más diseminado (comparado con los protocolos de enrutamiento por vector distancia). Comparar con protocolo de enrutamiento híbrido balanceado y protocolo de enrutamiento por vector de distancia

protocolo de enrutamiento por vector distancia :
Protocolo que itera en el número de saltos en una ruta para encontrar el árbol de extensión de ruta más corta. Los protocolos de enrutamiento por vector distancia piden a cada router que envíe su tabla de enrutamiento completa en cada actualización, pero solamente a sus vecinos. Los algoritmos de enrutamiento por vector distancia pueden ser propensos a los bucles de enrutamiento, pero desde el punto de vista informático son más simples que los algoritmos de enrutamiento de estado de enlace. También denominado algoritmo de enrutamiento Bellman-Ford. Comparar con el protocolo de enrutamiento híbrido balanceado y el protocolo de enrutamiento del estado de enlace.

Protocolo de Mantenimiento de la Tabla de Enrutamiento :
Ver RTMP.

Protocolo de mensajes de control en Internet :
Ver ICMP.

protocolo de publicación de servicio :
Ver SAP.

protocolo de resolución de direcciones :
Ver ARP.

Protocolo de Resolución Inversa de Dirección :
Ver RARP.

Protocolo de Servicios de Enlace NetWare :
Ver NLSP.

protocolo de transferencia de archivos :
Ver FTP.

Protocolo de Transferencia de Hipertexto :
Ver HTTP.

protocolo enrutado :
Protocolo que puede ser enrutado por el router. Un router debe ser capaz de interpretar la internetwork de redes lógica según lo que especifique dicho protocolo enrutado. AppleTalk, DECnet e IP son ejemplos de protocolos enrutados. Comparar con protocolo de enrutamiento.

protocolo exterior :
Protocolo utilizado para intercambiar información de enrutamiento entre redes que no comparten una administración común. Comparar con protocolo interior.

Programa de Control de Red :
Ver NCP.

PROM (*memoria programable de sólo lectura*) **:**
ROM que puede programarse utilizando equipo especial. Las PROM pueden ser programadas solamente una vez. Comparar con EPROM.

protocolo :
Descripción formal de un conjunto de normas y convenciones que establecen la forma en que los dispositivos de una red intercambian información.

Protocolo Bootstrap :
Ver BOOTP

protocolo de árbol de extensión :
Protocolo puente que utiliza el algoritmo de árbol de extensión, lo que habilita un puente de aprendizaje para funcionar dinámicamente en torno de bucles en una topología de red creando un árbol de extensión. Los puentes intercambian mensajes BPDU con otros puentes para detectar bucles y luego eliminarlos al desactivar las interfaces de puente seleccionadas. Se refiere tanto al estándar IEEE 802.1 de Protocolo de árbol de extensión, como al Protocolo de árbol de extensión más antiguo, de Digital Equipment Corporation, en el cual se basa. La versión de IEEE admite dominios de puente y permite que el puente desarrolle una topología sin bucles a través de una LAN extendida. Generalmente, se prefiere la versión de IEEE en lugar de la de Digital.

Protocolo de Autenticación de Contraseña :
Ver PAP.

Protocolo de autenticación de intercambio de señales :
Ver CHAP.

Protocolo de Control de Enlace :
Ver LCP.

protocolo de control de transmisión :
Ver TCP.

protocolo de datagrama de usuario :
Ver UDP.

protocolo de enrutamiento :
Protocolo que logra el enrutamiento mediante la implementación de un protocolo de enrutamiento específico. Entre los ejemplos de protocolo de enrutamiento se incluyen IGRP, OSPF y RIP. Comparar con protocolo enrutado.

Protocolo de enrutamiento DECnet :
Ver DRP.

protocolo de enrutamiento híbrido balanceado :
Protocolo que combina aspectos de los protocolos de estado de enlace y por vector distancia. Ver también protocolo de enrutamiento de estado de enlace y protocolo de enrutamiento por vector distancia.

protocolo de enrutamiento por estado de enlace :
Protocolo de enrutamiento en el cual cada router realiza un broadcast o multicast de información referente al costo de alcanzar cada uno de sus vecinos a todos los nodos de la internetwork de redes. Los protocolos de estado de enlace crean una vista coherente de la red y por lo tanto no son propensos a bucles de enrutamiento, pero por otro lado para lograr esto deben sufrir dificultades informáticas relativamente mayores y un tráfico más diseminado (comparado con los protocolos de enrutamiento por vector distancia). Comparar con protocolo de enrutamiento híbrido balanceado y protocolo de enrutamiento por vector de distancia

protocolo de enrutamiento por vector distancia :
Protocolo que itera en el número de saltos en una ruta para encontrar el árbol de extensión de ruta más corta. Los protocolos de enrutamiento por vector distancia piden a cada router que envíe su tabla de enrutamiento completa en cada actualización, pero solamente a sus vecinos. Los algoritmos de enrutamiento por vector distancia pueden ser propensos a los bucles de enrutamiento, pero desde el punto de vista informático son más simples que los algoritmos de enrutamiento de estado de enlace. También denominado algoritmo de enrutamiento Bellman-Ford. Comparar con el protocolo de enrutamiento híbrido balanceado y el protocolo de enrutamiento del estado de enlace.

Protocolo de Mantenimiento de la Tabla de Enrutamiento :
Ver RTMP.

Protocolo de mensajes de control en Internet :
Ver ICMP.

protocolo de publicación de servicio :
Ver SAP.

protocolo de resolución de direcciones :
Ver ARP.

Protocolo de Resolución Inversa de Dirección :
Ver RARP.

Protocolo de Servicios de Enlace NetWare :
Ver NLSP.

protocolo de transferencia de archivos :
Ver FTP.

Protocolo de Transferencia de Hipertexto :
Ver HTTP.

protocolo enrutado :
Protocolo que puede ser enrutado por el router. Un router debe ser capaz de interpretar la internetwork de redes lógica según lo que especifique dicho protocolo enrutado. AppleTalk, DECnet e IP son ejemplos de protocolos enrutados. Comparar con protocolo de enrutamiento.

protocolo exterior :
Protocolo utilizado para intercambiar información de enrutamiento entre redes que no comparten una administración común. Comparar con protocolo interior.

protocolo interior :
Protocolo utilizado para enrutar redes que se encuentran bajo una administración de red común.

protocolo Internet :
Cualquier protocolo que forme parte de la pila de protocolo TCP/IP. Ver IP. Ver también TCP/IP.

Protocolo Internet :
Ver IP.

protocolo proxy de resolución de direcciones :
Ver ARP proxy.

protocolo punto a punto :
Ver PPP.

protocolo SPF (*primero la ruta mas corta*) **:**
Algoritmo de enrutamiento que itera sobre la longitud de la ruta para determinar el árbol de extensión de la ruta más corta. Comúnmente empleado en los algoritmos de enrutamiento de estado de enlace. A veces denominado algoritmo de Dijkstra.

proveedor de acceso (*access provider*) **:**
Cualquier organización comercial o privada que ofrece acceso a Internet o a un servicio de esta red, por ejemplo, al correo electrónico (e-mail).

proxy :
Entidad que, para aumentar la eficiencia, esencialmente reemplaza a otra entidad.

PTT (*administracion postal, de telegrafos y de telefonos*) **:**
Agencia gubernamental que brinda servicios telefónicos. Las PTT existen en la mayoría de las áreas fuera de América del Norte y brinda servicios telefónicos tanto locales como de larga distancia.

publicación :
Proceso de router en el que las actualizaciones de servicio o enrutamiento se envían de tal manera que otros routers de la red puedan mantener listas de rutas utilizables.

puente :
Dispositivo que conecta y transmite paquetes entre dos segmentos de red que usan el mismo protocolo de comunicaciones. Los puentes operan en la capa de enlace de datos (Capa 2) del modelo de referencia OSI. En general, un puente filtra, envía o realiza un flooding de una trama entrante con base en la dirección MAC de esa trama.

puenteado :
Tecnología en la que un puente conecta dos o más segmentos de LAN.

puerto :
Interfaz en un dispositivo de internetwork (por ejemplo, un router). 2. Enchufe hembra en un panel de conmutación que acepta un enchufe macho del mismo tamaño, como un jack RJ--45. En estos puertos se usan los cables de conmutación para interconectar computadores conectados al panel de conmutación. Esta interconexión permite que la LAN funcione. 3. En la terminología IP, un proceso de capa superior que recibe información de las capas inferiores. Los puertos tienen un número, y muchos de ellos están asociados a un proceso específico. Por ejemplo, SMTP está asociado con el puerto 25. Un número de puerto de este tipo se denomina dirección conocida. 4. Volver a escribir el software o el microcódigo para que se ejecute en una plataforma de hardware o en un entorno de software distintos de aquellos para los que fueron diseñados originalmente.

punto de acceso al servicio :
Campo definido por la especificación IEEE 802.2 que forma parte de una especificación de dirección.

punto de acceso al servicio destino :
Ver DSAP.

punto de referencia :
Especificación que define la conexión entre dispositivos específicos, según su función en la conexión de extremo a extremo.

PVC *(circuito virtual permanente)* **:**
Circuito virtual que se establece de forma permanente. Los PVC ahorran el ancho de banda relacionado con el establecimiento y el desmantelamiento del circuito en situaciones en las que ciertos circuitos virtuales deben existir de forma permanente. Comparar con SVC.

Q.931 :
Protocolo que recomienda una capa de red entre el extremo final de la terminal y el switch RDSI local. Q.931 no impone una recomendación de extremo a extremo. Los diversos proveedores y tipos de switch de RDSI pueden usar varias implementaciones de Q.931.

QoS *(calidad de servicio)* **:**
Medida de desempeño de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

RAM *(memoria de acceso aleatorio)* **:**
Memoria volátil que puede ser leída y escrita por un microprocesador

RARP *(Protocolo de Resolución Inversa de Dirección)* **:**
Protocolo en la pila TCP/ IP que brinda un método para encontrar direcciones IP con base en las direcciones MAC. Comparar con ARP.

RBOC *(compañía telefónica regional en EE.UU)* **:**
Compañía telefónica local o regional que posee y opera líneas telefónicas y switches en una de siete regiones de Estados Unidos. Las RBOC fueron creadas a partir de la división de AT&T

RDSI (*Red digital de servicios integrados*) :
Protocolo de comunicaciones que ofrecen las compañías telefónicas y que permite que las redes telefónicas transmitan datos, voz y tráfico de otros orígenes.

red :
Agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

red con productos de varios fabricantes :
Red que usa equipamiento de más de un fabricante. Las redes con productos de varios fabricantes presentan muchos más problemas de compatibilidad que las redes con productos de un solo fabricante. Comparar con red de un único fabricante.

red de área local :
Ver LAN.

red de área local en bus con paso de token :
Arquitectura de LAN que usa la transmisión de tokens en una topología de bus. Esta arquitectura de LAN es la base de la especificación de LAN IEEE 802.4.

red de conexión única :
Red con una sola conexión a un router.

red de portadora :
Red de un proveedor de servicios.

red de un único fabricante :
Red que usa equipamientos de un solo fabricante. Las redes de único fabricante rara vez experimentan problemas de compatibilidad. Ver también red con productos de varios fabricantes.

red digital de servicios integrados. :
Ver RDSI

red empresaria :
La red de una asociación comercial, agencia, escuela u otra organización que une sus datos, comunicaciones, informática y servidores de archivo.

red híbrida :
Internetwork de redes compuesta por más de un tipo de tecnología de red, incluyendo LAN y WAN.

red interna :
Red interna a la que tienen acceso los usuarios con acceso a la LAN interna de una organización.

red no extendida :
Red AppleTalk Fase 2 que soporta direccionamiento de hasta 253 nodos y sólo 1 zona.

red plana :
Red en la cual no hay routers ubicados entre los switches, los broadcasts y las transmisiones de Capa 2 se envían a todos los puertos conmutados, y hay un dominio de broadcast que ocupa toda la red.

red suministrada :
El conjunto de switches e instalaciones (denominadas enlaces troncales) dentro de la nube del proveedor de WAN.

redirigido :
Parte de los protocolos ICMP y ES-IS que permiten que el router le indique al host que sería más efectivo usar otro router.

redundancia :
1. En internetwork, duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla. 2. En telefonía, la porción de la información total contenida en un mensaje que se puede eliminar sin sufrir pérdidas de información o significado esencial.

reensamblaje :
Colocación en su formato original de un datagrama IP en el destino después de su fragmentación en el origen o en un nodo intermedio.

rendimiento :
Velocidad de la información que llega a, y posiblemente pase a través de, un punto determinado del sistema de red.

repetidor :
Dispositivo que regenera y propaga las señales eléctricas entre dos segmentos de red.

reserva de ancho de banda :
Proceso de asignar ancho de banda a usuarios y aplicaciones que reciben servicios de una red. Involucra asignar una prioridad a diferentes flujos de tráfico según su importancia y grado de sensibilidad al retardo. Utiliza de la mejor manera posible el ancho de banda disponible y, si la red se congestiona, el tráfico de baja prioridad se descarta. A veces se denomina asignación de ancho de banda.

resolución de direcciones :
En general, un método para resolver diferencias entre esquemas de direccionamiento del computador. La resolución de direcciones habitualmente especifica un método para asignar las direcciones de capa de red (Capa 3) a las direcciones de capa de enlace de datos (Capa 2) .

resolución de nombre :
En general, el proceso de asociación de un nombre con una dirección de red.

resumen de ruta :
La consolidación de números de red publicados en OSPF e IS-IS. En OSPF, esto hace que un resumen de ruta único se publique a otras áreas a través de un router fronterizo.

retardo :
Tiempo entre la iniciación de una transacción por parte del emisor y la primera respuesta recibida por éste. Asimismo, el tiempo requerido para mover un paquete desde el origen hasta el destino en una ruta dada.

retardo de cola :
Cantidad de tiempo que los datos deben esperar antes de poder ser transmitidos a un circuito físico multiplexado estadísticamente.

retardo de propagación :
Tiempo requerido para que los datos recorran una red, desde el origen hasta el destino final. También denominado latencia.

RFC (*petición de comentarios*) :
Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de la Internet. Algunas RFC son designadas por el IAB como estándares de Internet. La mayoría de las RFC documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. Las RFC pueden encontrarse en línea en distintas fuentes.

RIP (*Protocolo de información de enrutamiento*) :
Protocolo suministrado con los sistemas BSD de UNIX. El Protocolo de Gateway Interior (IGP) más común de la Internet. RIP utiliza el número de saltos como métrica de enrutamiento.

RMON (*monitoreo remoto*) :
Especificación del agente MIB descrita en RFC 1271 que define las funciones del monitoreo remoto de dispositivos de la red. La especificación RMON suministra varias capacidades de monitoreo, detección de problemas e informes.

ROM (*memoria de sólo lectura*) :
Memoria no volátil que puede ser leída, pero no escrita, por el microprocesador.

router :
Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

router de generación :
Router de una red AppleTalk que tiene el número de red o rango de cable incorporado en el descriptor de puerto. El router de generación define el número de red o el alcance de cable para otros routers de ese segmento de la red y responde a las consultas de configuración de los routers no generadores en la red AppleTalk conectada, permitiendo que esos routers confirmen o modifiquen sus configuraciones en consecuencia. Cada red AppleTalk debe tener al menos un router de generación.

router designado :
Router OSPF que genera LSA para una red multiacceso y tiene otras responsabilidades especiales al ejecutar OSPF. Cada OSPF multiacceso que tiene por lo menos dos routers conectados tiene un router designado elegido por el protocolo Hello OSPF. El router designado permite una reducción en la cantidad de adyacencias requeridas en una red multiacceso, que a su vez reduce la cantidad de tráfico de protocolo de enrutamiento y el tamaño de la base de datos topológica.

router fronterizo :
Router ubicado en los bordes, o al final, de la frontera de la red, que brinda protección

básica contra las redes externas, o contra un área menos controlada de la red para un área más privada de la red.

router no generador :
En AppleTalk, un router que primero debe obtener, y luego verificar, su configuración con un router de generación antes de poder comenzar a operar. Ver también router de generación.

routers vecinos :
En OSPF, dos routers que tienen interfaces a una red común. En redes multiacceso, el protocolo Hello OSPF detecta a los vecinos de forma dinámica.

RPC (*llamada de procedimiento remoto*) :
Base tecnológica de la arquitectura cliente/servidor. Las RPC son llamadas de procedimiento que los clientes crean o especifican y que se ejecutan en los servidores. Los resultados se devuelven a los clientes a través de la red.

RPF (*Envío del camino inverso*) :
Técnica multicast en la cual un datagrama multicast se envía a todas las interfaces salvo la interfaz receptora si ésta es la que se utiliza para enviar datagramas unicast hacia el origen del datagrama multicast.

RSVP (*Protocolo de reserva de recursos*) :
Protocolo que hace posible la reserva de recursos a través de una red IP. Las aplicaciones que se ejecutan en los sistemas
finales IP pueden usar RSVP para indicarle a los otros nodos la naturaleza (ancho de banda, fluctuación de fase, ráfaga máxima, etc.) de las corrientes de paquetes que desean recibir. RSVP depende de IPv6. También denominado Protocolo de configuración de reserva de recursos.

RTMP (*Protocolo de Mantenimiento de Tabla de Enrutamiento*) :
Protocolo de enrutamiento propietario de Apple Computer. RTMP establece y mantiene la información de enrutamiento que se necesita para enrutar datagramas desde cualquier socket origen hacia cualquier socket destino en una red AppleTalk. Al usar RTMP, los routers mantienen las tablas de enrutamiento de forma dinámica para reflejar los cambios en la topología. RTMP deriva de RIP.

RTP (*Protocolo de Tabla de Enrutamiento*) :
Protocolo de enrutamiento VINES basado en RIP. Distribuye la información de la topología de red y ayuda a los servidores VINES a detectar a los clientes, servidores y routers vecinos. Usa el retardo como medida de enrutamiento.

RTP (*Protocolo de Transporte Rápido*) :
Protocolo que suministra control de flujo y recuperación de errores para datos APPN a medida que atraviesa la red APPN. Con RTP, la recuperación de errores y el control de flujo se realizan de extremo a extremo en lugar de en cada nodo. RTP previene la congestión, en lugar de reaccionar ante ella.

RTP (*Protocolo de Transporte en Tiempo Real*) :
Uno de los protocolos IPv6. RTP está diseñado para suministrar funciones de transporte de red de extremo a extremo para aplicaciones que transmiten datos de tiempo real, como, por ejemplo, datos de audio, vídeo o simulación, a través de servicios de red de multicast o de unicast. RTP suministra diversos servicios, tales como la identificación de tipo de carga, la numeración de secuencias, el uso de marca horaria y el monitoreo de entrega para aplicaciones de tiempo real.

ruta por defecto :
Una entrada de la tabla de enrutamiento que se utiliza para dirigir las tramas para las cuales el próximo salto no está explícitamente mencionado en la tabla de enrutamiento.

ruteador
Ver router.

SAI (*sistemas de alimentacion ininterrumpida*) :
Dispositivo de seguridad diseñado para suministrar una fuente de alimentación ininterrumpida en caso de que se produzca una interrupción del suministro de energía. Los SAI habitualmente se instalan en servidores de archivos y hubs de cableado.

salto :
Pasaje de un paquete de datos entre dos nodos de red (por ejemplo, entre dos routers).

SAP (*Protocolo de Publicación de Servicio*) :
Protocolo IPX que suministra un medio para informar a los clientes, a través de routers y servidores, acerca de los recursos y los servicios de red disponibles.

SAS (*estacion de una conexion*) :
Dispositivo conectado sólo al anillo primario de un anillo FDDI. También denominada estación de Clase B. Comparar con DAS. Ver también FDDI.

SDLC (*Control Sincrono del Enlace de Datos*) :
Protocolo de comunicaciones de capa de enlace de datos de SNA. SDLC es un protocolo serial de dúplex completo orientado a bit que ha dado origen a numerosos protocolos similares, entre ellos HDLC y LAPB.

SDSL (*very-high-data-rate digital subscriber line*) :
Línea Digital del Subscriptor de altísima velocidad. Una de las cuatro tecnologías DSL. VDSL entrega entre 13 y 52 Mbps hacia abajo (desde la oficina central al lugar del cliente) y entre 1.5 y 2.3 hacia arriba (desde el lugar del cliente a la oficina central) sobre un único par de cobre trenzado. El funcionamiento de VDSL está limitado a un rango de entre 304.8 y 1.372 metros. Vea también DSL, ADSL, HDSL y VDSL.

segmentación :
Proceso de división de un solo dominio de colisión en dos o más dominios de colisión para reducir las colisiones y la congestión de la red.

segmento :
Sección de una red que está rodeada de puentes, routers o switches 2. En una LAN que usa topología de bus, un circuito eléctrico continuo que a menudo está conectado a otros segmentos similares a través de repetidores. 3. En la especificación TCP, una unidad única de información de capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

semidúplex :
Capacidad de transmisión de datos en una sola dirección a la vez entre una estación transmisora y otra receptora. Comparar con full dúplex y unidireccional.

señalización :
En el contexto RDSI, el proceso de configuración de llamada utilizado, como establecimiento de la llamada, terminación de la llamada, información y mensajes varios, incluyendo configuración, conexión, liberación, información del usuario, cancelación, estado y desconexión.

Señalización de bit A&B :
Procedimiento utilizado en las instalaciones de transmisión de T1, en el que cada uno de los 24 subcanales T1 dedica 1 bit de cada seis tramas a la información de señalización supervisora.

servicio de distribución intermedia :
Ver IDF.

servidor :
Nodo o programa de software que suministra servicios a los clientes. Ver también cliente.

servidor de empresa :
Servidor que soporta a todos los usuarios en una red, ofreciendo servicios como correo electrónico o Sistema de Denominación de Dominio (DNS). Comparar con servidor de grupo de trabajo.

servidor de grupo de trabajo :
Servidor que soporta un conjunto específico de usuarios y ofrece servicios tales como procesamiento de texto y compartir archivos, que son servicios que sólo algunos grupos de personas necesitan. Comparar con servidor de empresa.

servidor de nombre :
Servidor conectado a una red que resuelve nombres de red en direcciones de red.

sesión :
Conjunto relacionado de transacciones de comunicaciones orientadas a conexión entre dos o más dispositivos de red. 2. En SNA, una conexión lógica que permite que dos unidades de red direccionables se comuniquen.

Sistema Básico de Entrada/Salida de Red :
Ver NetBIOS.

sistema de administración de red :
Ver NMS.

sistema de archivos de red :
Ver NFS.

sistema operativo de red :
Ver NOS.

SLIP (*Protocolo Internet de Enlace Serial*) :
Protocolo estándar para las conexiones seriales punto a punto que utiliza una variación de TCP/IP. El antecesor del PPP.

SMI (*Estructura de Administración de la Información*) :
Documento (RFC 1155) que especifica normas que se usan para definir objetos administrados en la MIB.

SNA (*Arquitectura de Sistemas de Red*) :
Arquitectura de red grande, compleja, con gran cantidad de funciones, desarrollada en 1970 por IBM. Similar en algunos aspectos al modelo de referencia OSI, pero con varias diferencias. SNA está compuesto esencialmente por siete capas. Ver capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control físico, capa de servicios de presentación, capa de servicios de transacción y capa de control de transmisión.

SNMP (*Protocolo simple de administración de redes*) :
Protocolo de administración de redes utilizado casi con exclusividad en redes TCP/IP. El SNMP brinda una forma de monitorear y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

socket :
Estructura de software que funciona como un punto final de las comunicaciones dentro de un dispositivo de red (similar a un puerto). 2. Entidad direccionable dentro de un nodo conectado a una red AppleTalk; los sockets son propiedad de procesos de software denominados clientes de socket. Los sockets AppleTalk se dividen en dos grupos: las SAS, que están reservadas para clientes como, por ejemplo, los protocolos principales AppleTalk, y las DAS, que son asignadas de forma dinámica por DDP a pedido de los clientes del nodo. Un socket AppleTalk es conceptualmente similar a un puerto TCP/IP.

software Cisco IOS (*Sistema Operativo de Internetwork*) :
Software de sistema de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes a todos los productos bajo la arquitectura CiscoFusion. El software Cisco IOS permite la instalación y administración centralizada, integrada y automatizada de internetwork, garantizando al mismo tiempo la compatibilidad con una amplia variedad de protocolos, medios, servicios y plataformas.

SOHO (*oficina pequeña/oficina hogareña*) :
Oficina pequeña u hogareña que incluye pocos usuarios que requieren una conexión que brinde conectividad más rápida y confiable que una conexión de marcado analógico.

spanning tree :
Subconjunto sin bucles de una topología de red de Capa 2 (conmutada).

SPID (*identificador del perfil de servicio*) :
Número que algunos proveedores de servicios usan para definir los servicios a los cuales se suscribe un dispositivo RDSI. El dispositivo RDSI usa el SPID al acceder al switch que inicializa la conexión a un proveedor de servicio.

split horizon :
Función de IGRP destinada a evitar que los routers tomen rutas erróneas. El horizonte dividido evita que se produzcan bucles entre routers adyacentes y mantiene reducido el tamaño de los mensajes de actualización.

spoofing :
1. Esquema que usan los routers para hacer que un host trate a una interfaz como si estuviera funcionando y soportando una sesión. El router hace spoofing de respuestas a mensajes de actividad del host para convencer a ese host de que la sesión continúa. El spoofing resulta útil en entornos de enrutamiento como DDR, en el cual un enlace de conmutación de circuito se desconecta cuando no existe tráfico que se deba enviar a través del enlace, a fin de ahorrar gastos por
llamadas pagas.
2. La acción de un paquete que ilegalmente dice provenir de una dirección desde la cual en realidad no se lo ha enviado. El spoofing está diseñado para contrarrestar los mecanismos de seguridad de la red, tales como los filtros y las listas de acceso.

spoofing de temporizador :
Subconjunto de spoofing que se refiere específicamente al router que actúa especialmente para un cliente NetWare enviando paquetes de temporizador a un servidor NetWare para mantener activa la sesión entre el cliente y el servidor. Es de utilidad cuando el cliente y el servidor están separados por un enlace de WAN DDR.

SPP (*Protocolo de Paquete Secuenciado*) :
Protocolo que brinda transmisión de paquetes con control de flujo, basada en conexión a nombre de procesos del cliente. Parte del conjunto de protocolos XNS.

SPX (*Intercambio de Paquete Secuenciado*) :
Protocolo confiable, orientado a conexión, que complementa el servicio de datagramas suministrado por los protocolos de capa de red. Novell derivó este protocolo de transporte NetWare de uso común del SPP del conjunto de protocolos XNS.

SQE (*error de calidad de señal*) :
En Ethernet, una transmisión enviada por un transceptor de vuelta al controlador para hacer saber al controlador si el circuito de colisión es funcional. También denominado heartbeat.

SS7 (*Sistema de Señalización Número 7*) :
Sistema de canal de señalización común desarrollado por Bellcore, utilizado en RDSI, que usa mensajes y señales de control telefónico entre los puntos de transferencia en el camino al destino llamado.

SSAP (*punto de acceso al servicio origen*) :
SAP del nodo de red designado en el campo Origen de un paquete. Comparar con DSAP. Ver también SAP.

STP *(par trenzado blindado)* :
Medio de cableado de dos pares que se usa en diversas implementaciones de red. El cableado STP posee una capa de aislamiento blindada para reducir la interferencia electromagnética. Comparar con UTP. Ver también par trenzado.

subinterfaz :
Una de una serie de interfaces virtuales en una sola interfaz física

subnetwork :
Ver subred.

subred :
1. Red segmentada en una serie de redes más pequeñas.
2. En redes IP, una red que comparte una dirección de subred individual. Las subredes son redes segmentadas de forma arbitraria por el administrador de la red para suministrar una estructura de enrutamiento jerárquica, de varios niveles mientras protege a la subred de la complejidad de direccionamiento de las redes conectadas. A veces se denomina subnetwork. 3. En redes OSI, un conjunto de sistemas finales y sistemas intermedios bajo el control de un dominio administrativo exclusivo y que utiliza un protocolo de acceso de red exclusivo.

SVC *(circuito virtual conmutado)* :
Circuito virtual que se establece de forma dinámica a pedido y que se desconecta cuando la transmisión se completa. Los SVC
se usan en situaciones en las que la transmisión de datos es esporádica. Comparar con PVC.

switch :
Dispositivo que conecta computadoras. El switch actúa de manera inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera.

Los switches son más "inteligentes" que los "Hubs" y ofrecen un ancho de banda más dedicado para los usuarios o grupos de usuarios. Un switch envía los paquetes de datos solamente a la computadora correspondiente, con base en la información que cada paquete contiene. Para aislar la transmisión de una computadora a otra, los switches establecen una conexión temporal entre la fuente y el destino, y la conexión termina una vez que la conversación se termina.

switch de LAN :
Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches de LAN envían tráfico basándose en las direcciones MAC. Los switches de LAN a menudo se clasifican según el método utilizado para enviar tráfico: conmutación de paquetes por método de corte o conmutación de paquetes por almacenamiento y envío. Un ejemplo de switch de LAN es el Cisco Catalyst 5000.

T1 :
Servicio de portadora WAN digital que transmite datos formateados DS-1 a 1.544 Mbps a través de la red de conmutación telefónica, usando la codificación AMI o B8ZS. Comparar con E1.

T3 :
Servicio de portadora WAN digital que transmite datos formateados DS-3 a 44.736 Mbps a través de la red de conmutación telefónica. Comparar con E3.

TA *(adaptador de terminal)* **:**
Dispositivo usado para conectar conexiones BRI de RDSI a interfaces existentes como EIA/TIA-232. Esencialmente es un módem RDSI.

tabla de enrutamiento :
Tabla almacenada en un router o en algún otro dispositivo de internetwork que realiza un seguimiento de las rutas hacia destinos de red específicos y, en algunos casos, las métricas asociadas con esas rutas.

TACACS *(Sistema de Control de Acceso al Controlador de Acceso a la Terminal)* **:**
Protocolo de autenticación, desarrollado por la comunidad DDN, que suministra autenticación de acceso remoto y servicios relacionados, como, por ejemplo, el registro de eventos. Las contraseñas de usuario se administran en una base de datos central en lugar de administrarse en routers individuales, suministrando una solución de seguridad de red fácilmente escalable.

tamaño de ventana :
Cantidad de mensajes que se pueden transmitir mientras se espera recibir un acuse de recibo

tarjeta de interfaz de red :
Ver NIC.

TCP *(Protocolo de Control de Transmisión)* **:**
Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP *(Protocolo de Control de Transmisión /Protocolo Internet)* **:**
Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los
años '70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

TDM *(multiplexado por división de tiempo)* **:**
Señal de conmutación de circuito utilizada para determinar la ruta de llamada, que es una ruta dedicada entre el emisor y el receptor.

TE1 *(equipo terminal tipo 1)* **:**
Dispositivo compatible con la red RDSI. TE1 se conecta a una terminación de red de Tipo 1 o Tipo 2.

TE2 *(equipo terminal tipo 2)* **:**
Dispositivo no compatible con la red RDSI que requiere un adaptador de terminal.

Telnet :
Protocolo de emulación de terminal estándar de la pila de protocolo TCP/IP. Telnet se usa para la conexión de terminales remotas, permitiendo que los usuarios se registren en sistemas remotos y utilicen los recursos como si estuvieran conectados a un sistema local. Telnet se define en RFC 854.

temporizador maestro :
Mecanismo de hardware o software utilizado para disparar un evento o un escape de un proceso a menos que el temporizador se reajuste periódicamente. 2. En NetWare, un temporizador que indica el período máximo de tiempo durante el cual un servidor esperará que un cliente responda a un paquete de temporizador. Si el temporizador expira, el servidor envía otro paquete de temporizador (hasta una cantidad máxima establecida).

TFTP (*Protocolo de Transferencia de Archivos Trivial*) **:**
Versión simplificada de FTP que permite la transferencia de archivos de un computador a otro a través de una red.

TIA (*Asociación de la Industria de las Telecomunicaciones*) **:**
Organización que desarrolla estándares relacionados con las tecnologías de telecomunicaciones. En conjunto, TIA y EIA han formalizado estándares, como EIA/TIA-232, para las características eléctricas de la transmisión de datos.

tictac :
Retardo en un enlace de datos que utiliza tictacs de reloj de PC IBM (aproximadamente 55 milisegundos). Un tictac equivale a un segundo.

tiempo de conexión de llamada :
Tiempo requerido para establecer una llamada conmutada entre dispositivos DTE.

tiempo de existencia :
Ver TTL.

token :
Trama que contiene información de control. La posesión del token permite que un dispositivo de red transmita datos a la red.

Token Ring :
LAN de transmisión de tokens desarrollada y soportada por IBM. Token Ring se ejecuta a 4 ó 16 Mbps a través de una topología de anillo. Similar a IEEE 802.5.

TokenTalk :
Producto de enlace de datos de Apple Computer que permite que una red AppleTalk se conecte mediante cables Token Ring.

topología :
Disposición física de los nodos y medios de red en una estructura de networking a nivel empresarial.

topología de anillo :
Topología de red compuesta por una serie de repetidores conectados entre sí por enlaces de transmisión unidireccionales para formar un bucle cerrado único. Cada estación de la red se conecta a la red a través de un repetidor. Aunque son anillos lógicos, las topologías de anillo a menudo se organizan en una estrella de bucle cerrado. Comparar con topología de bus, topología en estrella y topología en árbol.

topología de bus :
Topología de LAN en la que las transmisiones desde las estaciones de la red se propagan a lo largo del medio y son recibidas por todas las demás estaciones Comparar con topología de anillo, topología en estrella y topología en árbol.

topología de malla completa :
Topología en la que todos los dispositivos Frame Relay tienen un PVC hacia todos los demás dispositivos en una WAN multipunto.

topología de malla parcial :
Topología en la cual no todos los dispositivos en la nube Frame Relay tienen un PVC hacia cada uno de los demás dispositivos.

topología en árbol :
Topología de LAN similar a una topología de bus, salvo que las redes en árbol pueden tener ramas con varios nodos. Las transmisiones desde una estación se propagan a lo largo del medio y todas las demás estaciones las reciben. Comparar con topología de bus, topología de anillo y topología en estrella.

topología en estrella :
Topología de LAN en la que los puntos finales de una red se encuentran conectados a un switch central común mediante enlaces punto a punto Una topología de anillo que se organiza en forma de estrella implementa una estrella de bucle cerrado unidireccional, en lugar de enlaces punto a punto. Comparar con topología de bus, topología de anillo y topología en árbol.

tormenta de broadcast :
Suceso de red no deseado, en el que se envían varios broadcasts simultáneamente a todos los segmentos de red. Una tormenta de broadcast usa una parte considerable del ancho de banda de la red y normalmente hace que se agoten los tiempos de espera de la red. Ver también broadcast.

traceroute :
Programa disponible en varios sistemas que rastrea la ruta que recorre un paquete hacia un destino. Se utiliza a menudo para depurar los problemas de enrutamiento entre hosts. Existe también un protocolo traceroute definido en RFC 1393.

traducción de dirección de red :
Ver NAT.

trama :
Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

transmisión de tokens :
Método de acceso mediante el cual los dispositivos de red acceden al medio físico de forma ordenada basándose en la posesión de una pequeña trama denominada token. Comparar con switching y contención de circuitos.

transmisión en paralelo :
Método de transmisión de datos en el que los bits de un carácter de datos se transmiten de forma simultánea a través de una serie de canales. Comparar con transmisión serial.

transmisión serial :
Método de transmisión de datos en el cual los bits de un carácter de datos se transmiten de forma secuencial a través de un solo canal. Comparar con transmisión en paralelo.

TTL (*Tiempo de Existencia*) :
Campo en un encabezado IP que indica el tiempo durante el cual se considera válido un paquete.

tunneling :
Arquitectura diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estánd

UDP (*Protocolo de Datagrama de Usuario*) :
Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768

UIT-T (*Sector de normalizacion de las Telecomunicaciones de la Union de Telecomunicaciones Internacional*) :
Antiguamente denominado Comité Consultivo Internacional Telegráfico y Telefónico (CCITT), una organización internacional que desarrolla estándares de comunicación. Ver también CCITT.

UNI (*Interfaz de Red a Usuario*) :
Especificación que define un estándar de interoperabilidad para la interfaz entre productos (un router o un switch) ubicados en una red privada y los switches ubicados dentro de las redes de carriers públicas. También utilizado para describir conexiones similares en redes Frame Relay.

unicast :
Mensaje que se envía a un solo destino de red.

unidad de acceso a varias estaciones (*Ver MSAU*) :

unidad de acceso al medio :
Ver MAU.

unidad de conexión al medio :
Ver MAU.

unidireccional :
Capacidad de transmisión en una sola dirección entre una estación emisora y una estación receptora. La televisión es un ejemplo de tecnología unidireccional. Comparar con full dúplex y semidúplex.

URL (*localizador de recursos uniforme*) :
Esquema de direccionamiento estandarizado para acceder a documentos de hipertexto y otros servicios utilizando un explorador de Web.

UTP (*par trenzado no blindado*) :
Medio de cable de cuatro pares que se emplea en varias redes. UTP no requiere el espacio fijo entre conexiones que es necesario para las conexiones de tipo coaxial. Hay cinco tipos de cableado UTP de uso común: cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Comparar con STP.

VCC (*interconexión vertical*) :
Conexión utilizada para interconectar los diversos IDF al MDF central

VDSL (*very-high-data-rate digital subscriber line*) :
Línea Digital del Suscriptor de altísima velocidad. Una de las cuatro tecnologías DSL. VDSL entrega entre 13 y 52 Mbps hacia abajo (desde la oficina central al lugar del cliente) y entre 1.5 y 2.3 hacia arriba (desde el lugar del cliente a la oficina central) sobre un único par de cobre trenzado. El funcionamiento de VDSL está limitado a un rango de entre 304.8 y 1,372 metros. Vea también DSL, ADSL, HDSL y SDSL.

velocidad asegurada :
Rendimiento de datos a largo plazo, en bits o celdas por segundo, que una red ATM puede proporcionar bajo condiciones normales de la red. La velocidad asegurada se encuentra asignada en un 100 por ciento. Se deduce en su totalidad del ancho de banda troncal a lo largo de la ruta del circuito. Comparar con velocidad excesiva y velocidad máxima.

velocidad de acceso local :
Velocidad de reloj (velocidad de puerto) de la conexión (bucle local) a la nube Frame Relay. Es la velocidad a la que se desplazan los datos hacia o desde la red.

velocidad excesiva :
Tráfico que supera la velocidad asegurada de una conexión en particular. Específicamente, la velocidad excesiva es igual a la velocidad máxima menos la velocidad asegurada. El tráfico excesivo se entrega solamente si los recursos de red están disponibles y se pueden descartar durante los períodos de congestión. Comparar con velocidad asegurada y velocidad máxima.

velocidad máxima :
Rendimiento total máximo de datos que se permite en un circuito virtual determinado, que es igual a la suma del tráfico asegurado y del tráfico no asegurado desde el origen del tráfico. Los datos del tráfico no asegurado pueden descartarse si la red se congestiona. La velocidad máxima, que no puede superar la velocidad del medio, representa el rendimiento de datos más elevado que el circuito virtual puede enviar, medida en bits o en celdas por segundo. Comparar con velocidad excesiva y velocidad asegurada.

ventana :
Cantidad de octetos que el remitente desea aceptar

ventana deslizante :
Ventana cuyo tamaño se negocia dinámicamente durante la sesión TCP

VINES (*Servicio de Red Integrado Virtual*) :
Sistema operativo de red desarrollado y comercializado por Banyan Systems

VLAN (*LAN virtual*) :
Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

VLAN de puerto central :
VLAN en la que todos los nodos en la misma VLAN se conectan al mismo puerto de switch.

VLAN dinámica (*VLAN basada en las direcciones MAC, las direcciones lógicas o el tipo de protocolo de los paquetes de datos Comparar con VLAN estática Ver también LAN y VLAN*) :
VLAN basada en las direcciones MAC, las direcciones lógicas o el tipo de protocolo de los paquetes de datos. Comparar con VLAN estática. Ver también LAN y VLAN.

VLAN estática :
VLAN en la que los puertos de un switch se asignan estáticamente. Comparar con VLAN dinámica. Ver también LAN y VLAN.

VoIP (*voice over IP*) :
Voz sobre Protocolo de Internet. La habilidad para transportar voz telefónica normal sobre una red basada en Internet con la misma funcionalidad, confiabilidad y calidad de voz que ofrecen las empresas telefónicas tradicionales.

voz sobre IP (*voice over IP*) :
La Voz sobre protocolo Internet le permite a un router llevar tráfico de voz (por ejemplo llamadas telefónicas y faxes) sobre una red IP. En Voz sobre IP, la parte de dominio específica (DSP), segmenta la señal de voz en tramas, las cuales son luego agrupadas en parejas y guardadas en paquetes de voz. Estos paquetes de voz son transportados utilizando IP, de acuerdo con la especificación ITU-T H.323.

WAN (*Red de area amplia*) :
Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por carriers comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

X.25 :
Estándar UIT-T que define la manera en que las conexiones entre los DTE y DCE se mantienen para el acceso a la terminal remota y las comunicaciones en computadores en las redes de datos públicas. Frame Relay ha reemplazado en cierta medida a X.25.

XNS (*Sistema de red de Xerox*) :
Conjunto de protocolo originalmente diseñado por PARC. Muchas empresas de networking para PC tales como 3Com, Banyan, Novell y UB Networks utilizaron o actualmente utilizan una variante de XNS como protocolo de transporte primario.

ZIP (*Protocolo de Información de Zona*) :
Protocolo de capa de sesión AppleTalk que asigna números de red a nombres de zona. NBP usa ZIP para determinar cuáles de las redes contienen nodos que pertenecen a una zona.

zona :
En AppleTalk, un grupo lógico de dispositivos de red.

BIBLIOGRAFÍA

BSCN, Building Scalable Cisco Networks Course Companion
Thomas M. Thomas II, Arjan Aelmans, Floris Houniet & Tan Nam-Kee
Mc. Graw Hill

Cisco Router Internetworking
Paul T. Ammann, CCNA
Mc. Graw Hill

Electronic Communications
D. Roddy, J. Coolen
Prentice Hall

Óptica
Hecht-Zajac
Addison Wesley

Tecnologías de Interconectividad de Redes
Merilee Ford, H. Kim Lew, Steve Spanier & Tim Stevenson
PEARSON, CISCO PRESS

TCP/IP Network Administration
Craig Hunt
O'REILLY

Sistemas de Comunicaciones Electrónicas
Wayne Tomasi
Prentice Hall

Telecommunications Engineering
J. Dunlop, D. G. Smith
Editorial Gutavo Gili
Direcciones Electrónicas

http://www.cisco.com

http://www.nortel.com

http://www.3com.com

http://148.204..219.113/cnap/index.html

http://www.lvr.com

http://www.dtd.unam.mx

ANEXO A

"Configuraciones finales de los equipos Foundry NetIron 800 y BigIron 8000 del nuevo Backbone GigabitEthernet de RedUNAM"

```
 Equipos de la capa de core
 DGSCA-CORE NetIron 800
ver 07.5.04T53
!
module 1 bi-4-port-gig-m4-management-module
module 2 bi-4-port-gig-m4-management-module
module 3 bi-8-port-gig-module
module 4 bi-8-port-gig-module
module 5 bi-24-port-100fx-module
module 6 bi-atm-2-port-155m-module
!
global-protocol-vlan
!
trunk switch ethe 3/1 to 3/2
port-name "A IIMAS" ethernet 3/1
trunk switch ethe 4/1 to 4/2
port-name "A ARQ" ethernet 4/1
trunk switch ethe 4/3 to 4/4
port-name "A DGSCA DIST" ethernet 4/3
trunk switch ethe 4/7 to 4/8
port-name "a ZC" ethernet 4/7
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 96 name AREA4 by port
untagged ethe 2/1 ethe 4/3 to 4/4 ethe 5/1 to 5/6
router-interface ve 96
!
vlan 192 name DGSCA-ZC by port
untagged ethe 4/7 to 4/8
router-interface ve 192
!
vlan 196 name DGSCA-IIMAS by port
untagged ethe 3/1 to 3/2
router-interface ve 196
!
vlan 200 name DGSCA-ARQ by port
untagged ethe 4/1 to 4/2
router-interface ve 200
!
vlan 336 name C.INTRUMENTOS by port
```

```
untagged ethe 5/9
!
vlan 3168 name DOCENCIA by port
untagged ethe 5/7
!
vlan 329 name C.NUCLEARES by port
untagged ethe 5/8
!
vlan 3213 name T.SOCIAL by port
untagged ethe 5/10
!
vlan 328 name F.CIENCIAS by port
untagged ethe 5/11
!
vlan 3124 name CLUSTER.IBM by port
untagged ethe 5/14
!
vlan 3221 name SUPER_221 by port
untagged ethe 5/13
!
vlan 1234 name BPX-TELEFONIA by port
untagged ethe 5/23
!
!
router ipx
router appletalk
appletalk rtmp-update-interval 50
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
aaa accounting commands 0 default start-stop tacacs+
aaa accounting exec default start-stop tacacs+
boot sys fl sec
atm boot sec
enable telnet authentication
enable super-user-password .....
hostname DGSCA_CORE
!
ip as-path access-list NO-CUDI-NETWORKS seq 5 deny ^18592_
ip as-path access-list NO-CUDI-NETWORKS seq 10 permit .*
ip dns domain-name core-gigabit.unam.mx
ip dns server-address 132.248.204.1
ip route 0.0.0.0 0.0.0.0 132.248.255.194
ip route 132.248.13.0 255.255.255.0 132.248.255.97
ip route 132.248.49.0 255.255.255.0 132.248.255.97
ip route 132.248.86.0 255.255.255.0 132.248.255.97
ip route 132.248.126.0 255.255.255.0 132.248.255.97
ip route 132.248.208.0 255.255.255.0 132.248.255.97
```

```
ip route 132.248.10.0 255.255.255.0 132.248.255.100
ip route 132.248.115.0 255.255.255.0 132.248.255.100
ip route 132.248.61.0 255.255.255.0 132.248.255.98
ip route 132.248.125.0 255.255.255.0 132.248.255.98
ip route 132.248.194.0 255.255.255.0 132.248.255.99
ip route 132.248.69.0 255.255.255.0 132.248.255.99
ip route 132.248.83.0 255.255.255.0 132.248.255.99
ip route 132.248.236.0 255.255.255.0 132.248.255.99
ip route 132.248.110.0 255.255.255.0 132.248.255.99
ip route 132.248.132.0 255.255.255.0 132.248.255.99
ip route 132.248.139.0 255.255.255.0 132.248.255.101
ip route 132.248.159.0 255.255.255.0 132.248.255.102
ip route 132.248.160.0 255.255.255.0 132.248.255.102
ip route 132.248.161.0 255.255.255.0 132.248.255.102
ip route 132.248.201.0 255.255.255.0 132.248.255.102
ip route 132.248.205.0 255.255.255.0 132.248.255.102
!
telnet access-group 1
tacacs-server host 200.15.3.14
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
snmp-server community ..... ro 40
snmp-server community ..... ro 41
snmp-server community ..... rw 40
snmp-server community ..... rw 41
snmp-server contact Depto. de Operacion de la Red Tel. 5622 8509
snmp-server location Nodo DGSCA
ssh access-group 1
router ospf
area 0.0.0.0
area 0.0.0.4
auto-cost reference-bandwidth 1000
metric-type type1
redistribution static
!
router pim
!
interface loopback 1
port-name ROUTER-ID
ip address 132.248.255.254 255.255.255.255
ip ospf area 0.0.0.0
!
interface ethernet 2/1
port-name A ANTROPOLOGICAS
!
interface ethernet 3/1
port-name A IIMAS
```

```
!
interface ethernet 3/3
port-name A ARQUITECTURA
!
interface ethernet 4/1
port-name A ARQ
!
interface ethernet 4/3
port-name A DGSCA DIST
!
interface ethernet 4/7
port-name a ZC
!
interface ethernet 5/1
port-name A JARDIN BOTANICO
!
interface ethernet 5/2
port-name A QUIMICA E
!
interface ethernet 5/3
port-name A ANTROPOLOGICAS
!
interface ethernet 5/4
port-name A SERVIDORES
!
interface ethernet 5/5
port-name A ANEXO DE INGENIERIA
!
interface ethernet 5/6
port-name A SUPERCOMPUTO
!
interface ethernet 5/7
port-name A DOCENCIA
appletalk cable-range 1200 - 1200
appletalk address 1200.161
appletalk zone-name dgsca-225
appletalk routing
ip address 132.248.168.254 255.255.255.0 ospf-passive
ip address 132.248.225.254 255.255.255.0 ospf-passive
ip helper-address 1 132.248.204.50 unicast
ip ospf area 0.0.0.4
!
interface ethernet 5/8
port-name A NUCLEARES
ip address 132.248.29.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.4
!
```

```
interface ethernet 5/9
port-name C.INSTRUMENTOS
ip address 132.248.36.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.4
!
interface ethernet 5/10
port-name A T.SOCIAL
ip address 132.248.213.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.4
!
interface ethernet 5/11
port-name A F.CIENCIAS
ip address 132.247.16.254 255.255.255.0 ospf-passive
ip address 132.248.28.254 255.255.255.0 ospf-passive
ip address 132.248.109.254 255.255.255.0 ospf-passive
ip address 132.248.129.254 255.255.255.0 ospf-passive
ip address 132.248.133.254 255.255.255.0 ospf-passive
ip address 132.248.195.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.4
!
interface ethernet 5/13
port-name SUPER_221
ip address 132.248.221.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.4
!
!
interface ethernet 5/14
port-name CLUSTER.IBM
ip address 132.248.124.94 255.255.255.240 ospf-passive
ip ospf area 0.0.0.4
!
interface ethernet 5/23
port-name A BPX-TELEFONIA
ip address 192.100.200.233 255.255.255.252 ospf-passive
ip ospf area 0.0.0.4
!
interface atm 6/1
port-name A ROUTER DGSCA1
!
interface atm 6/1.1 point-to-point
atm pvc 0 112 ubr
ip address 132.248.255.114 255.255.255.252
ip ospf area 0.0.0.4
!
interface ve 96
port-name AREA4
appletalk cable-range 96 - 96
```

```
appletalk address 96.110
appletalk zone-name Apple.DGSCA.CORE-DIST
appletalk routing
ip address 132.248.255.110 255.255.255.240
ip ospf area 0.0.0.4
ipx net 00025596 ethernet_802.3 netbios-disallow
!
interface ve 192
port-name DGSCA-ZC
ip address 132.248.255.193 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255192 ethernet_802.3 netbios-disallow
!
interface ve 196
port-name DGSCA-IIMAS
ip address 132.248.255.197 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255196 ethernet_802.3 netbios-disallow
!
interface ve 200
port-name DGSCA-ARQ
ip address 132.248.255.201 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255200 ethernet_802.3 netbios-disallow
!
!
router bgp
cluster-id 2
local-as 278
neighbor CLIENTES-SWITCHES-REDUNAM peer-group
neighbor CLIENTES-SWITCHES-REDUNAM remote-as 278
neighbor CLIENTES-SWITCHES-REDUNAM update-source loopback 1
neighbor CLIENTES-SWITCHES-REDUNAM route-reflector-client
neighbor CLIENTES-SWITCHES-REDUNAM soft-reconfiguration inbound
neighbor CLIENTES-ROUTERS-REDUNAM peer-group
neighbor CLIENTES-ROUTERS-REDUNAM remote-as 278
neighbor CLIENTES-ROUTERS-REDUNAM update-source loopback 1
neighbor CLIENTES-ROUTERS-REDUNAM filter-list NO-CUDI-NETWORKS out
neighbor CLIENTES-ROUTERS-REDUNAM route-reflector-client
neighbor 132.248.255.253 peer-group CLIENTES-SWITCHES-REDUNAM
neighbor 132.248.255.253 description IIMAS_CORE
neighbor 132.248.255.251 peer-group CLIENTES-SWITCHES-REDUNAM
neighbor 132.248.255.251 description ARQ_CORE
neighbor 132.248.255.252 peer-group CLIENTES-SWITCHES-REDUNAM
neighbor 132.248.255.252 description ZC_CORE
neighbor 132.248.255.124 peer-group CLIENTES-ROUTERS-REDUNAM
neighbor 132.248.255.124 description dgsca1
```

```
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.248.204.100
access-list 1 permit host 132.248.204.101
access-list 1 permit host 132.248.204.102
access-list 1 permit host 132.248.204.104
access-list 1 permit host 132.248.204.37
access-list 1 permit host 132.248.204.38
access-list 1 permit host 132.248.204.48
access-list 1 permit host 132.248.204.49
access-list 1 permit host 132.248.204.50
access-list 1 permit host 132.248.204.105
access-list 1 permit host 132.247.253.1
access-list 1 permit host 132.248.204.27
access-list 1 deny any
!
access-list 40 permit host 132.248.204.27
access-list 40 permit host 132.247.253.1
access-list 40 permit host 200.15.3.86
access-list 40 permit host 200.15.3.14
access-list 40 permit host 132.248.204.37
access-list 40 deny any
!
access-list 41 permit host 200.15.3.14
access-list 41 deny any
!
ip ssh pub-key-file tftp 200.15.3.82 pubkeys.txt
!
ip ssh source-interface loopback 1
!
end

 !IMAS-CORE BigIron 8000
Current configuration:
!
ver 07.5.04T53
!
module 1 bi-8-port-gig-m4-management-module
module 2 bi-8-port-gig-m4-management-module
module 3 bi-24-port-100fx-module
!
global-protocol-vlan
!
trunk switch ethe 1/1 to 1/2
```

```
port-name "A DGSCA" ethernet 1/1
trunk switch ethe 2/1 to 2/2
port-name "A ARQ" ethernet 2/1
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 64 name AREA3 by port
tagged ethe 3/9
untagged ethe 2/3 to 2/5 ethe 3/1 to 3/8
router-interface ve 64
!
vlan 196 name IIMAS-DGSCA by port
untagged ethe 1/1 to 1/2
router-interface ve 196
!
vlan 204 name IIMAS-ARQ by port
untagged ethe 2/1 to 2/2
router-interface ve 204
!
vlan 353 name I.INGENIERIA by port
untagged ethe 3/11
!
vlan 315 name ICMYL by port
untagged ethe 3/12
!
vlan 3192 name ROUTER-GOBIERNO_D.F. by port
tagged ethe 3/9
router-interface ve 168
!
vlan 3134 name AS5300 by port
tagged ethe 3/9
router-interface ve 134
!
!
router ipx
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
boot sys fl sec
enable telnet authentication
enable super-user-password .....
hostname IIMAS_CORE
ip dns server-address 132.248.10.2 132.248.204.1
ip route 0.0.0.0 0.0.0.0 132.248.255.197
ip route 0.0.0.0 0.0.0.0 132.248.255.206 distance 2
ip route 132.248.6.0 255.255.255.0 132.248.255.65
ip route 132.248.14.0 255.255.255.0 132.248.255.65
ip route 132.248.20.0 255.255.255.0 132.248.255.65
```

```
ip route 132.248.46.0 255.255.255.0 132.248.255.65
ip route 132.248.182.0 255.255.255.0 132.248.255.65
ip route 132.248.211.0 255.255.255.0 132.248.255.65
ip route 192.100.200.96 255.255.255.240 132.248.255.65
ip route 192.100.200.128 255.255.255.240 132.248.255.65
ip route 132.248.62.0 255.255.255.0 132.248.255.66
ip route 132.248.105.0 255.255.255.0 132.248.255.66
ip route 132.248.119.0 255.255.255.0 132.248.255.66
ip route 132.248.56.0 255.255.255.0 132.248.255.68
ip route 132.248.131.0 255.255.255.0 132.248.255.68
ip route 132.248.175.0 255.255.255.0 132.248.255.68
ip route 132.248.55.0 255.255.255.0 132.248.255.70
ip route 132.248.72.0 255.255.255.0 132.248.255.70
ip route 132.248.73.0 255.255.255.0 132.248.255.70
ip route 132.248.183.0 255.255.255.0 132.248.255.70
ip route 132.248.233.0 255.255.255.0 132.248.255.70
ip route 132.248.250.0 255.255.255.0 132.248.255.70
ip route 132.248.252.0 255.255.255.0 132.248.255.70
ip route 132.248.7.0 255.255.255.0 132.248.255.71
ip route 132.248.8.0 255.255.255.0 132.248.255.71
ip route 132.248.9.0 255 255.255.0 132.248.255.71
ip route 132.248.12.0 255.255.255.0 132.248.255.71
ip route 132.248.163.0 255.255.255.0 132.248.255.71
ip route 132.248.11.0 255.255.255.0 132.248.255.72
ip route 132.248.16.0 255.255.255.0 132.248.255.72
ip route 132.248.27.0 255.255.255.0 132.248.255.72
ip route 132.248.51.0 255.255.255.0 132.248.255.72
ip route 132.248.52.0 255.255.255.0 132.248.255.72
ip route 132.248.57.0 255.255.255.0 132.248.255.72
ip route 132.248.59.0 255.255.255.0 132.248.255.72
ip route 132.248.63.0 255.255.255.0 132.248.255.72
ip route 132.248.64.0 255.255.255.0 132.248.255.72
ip route 132.248.212.0 255.255.255.0 132.248.255.72
ip route 132.248.17.0 255.255.255.0 132.248.255.67
ip route 132.248.54.0 255.255.255.0 132.248.255.67
ip route 132.248.78.0 255.255.255.0 132.248.255.67
ip route 132.248.107.0 255.255.255.0 132.248.255.67
ip route 132.248.1.0 255.255.255.0 132.248.255.69
ip route 132.248.230.0 255.255.255.0 132.248.255.69
ip route 132.248.31.0 255.255.255.0 132.248.255.73
ip route 132.248.85.0 255.255.255.0 132.248.255.73
ip route 132.248.50.0 255.255.255.0 132.248.255.73
ip route 132.248.76.0 255.255.255.0 132.248.255.73
ip route 200.15.162.0 255.255.255.0 192.168.1.93
ip route 200.15.163.0 255.255.255.0 192.168.1.93
ip route 132.248.4.0 255.255.255.0 132.248.255.74
!
```

```
telnet access-group 1
route-only
tacacs-server host 200.15.3.14
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
snmp-server community ..... ro 40
snmp-server community ..... rw 40
ssh access-group 1
router ospf
area 0.0.0.0
area 0.0.0.3 stub 3 no-summary
auto-cost reference-bandwidth 1000
metric-type type1
redistribution static
!
router pim
!
interface loopback 1
port-name ROUTER-ID
ip address 132.248.255.253 255.255.255.255
ip ospf area 0.0.0.0
!
interface ethernet 1/1
port-name A DGSCA
!
interface ethernet 2/1
port-name A ARQ
!
interface ethernet 2/3
port-name A LABORALES
!
interface ethernet 2/4
port-name A ASTRONOMIA
!
interface ethernet 2/5
port-name A LOC_IIMAS
!
interface ethernet 3/1
port-name A GEOGRAFIA
!
interface ethernet 3/2
port-name A FAC.VETERINARIA
!
interface ethernet 3/3
port-name A LOC.IIMAS
!
interface ethernet 3/4
```

```
port-name A FAC.QUIMICA
!
interface ethernet 3/5
port-name A ASTRONOMIA1
!
interface ethernet 3/6
port-name A LABORALES
!
interface ethernet 3/7
port-name A ASTRONOMIA
!
interface ethernet 3/8
port-name A IIMAS-DGAE
!
interface ethernet 3/9
port-name A LABORALES2
!
interface ethernet 3/11
port-name A I.INGENIERIA
ip address 132.248.53.254 255.255.255.0 ospf-passive
ip address 132.248.153.254 255.255.255.0 ospf-passive
ip address 132.248.154.254 255.255.255.0 ospf-passive
ip address 132.248.155.254 255.255.255.0 ospf-passive
ip address 132.248.156.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.3
!
interface ethernet 3/12
port-name A ICMYL
ip address 132.248.15.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.3
!
interface ve 64
port-name AREA3
ip address 132.248.255.78 255.255.255.240
ip ospf area 0.0.0.3
ipx net 00025564 ethernet_802.3 netbios-disallow
!
interface ve 134
port-name AS5300-LABORALES
ip address 132.248.134.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.3
!
interface ve 168
port-name ROUTER-GOB-D.F.
ip address 192.168.1.94 255.255.255.0 ospf-passive
!
interface ve 196
```

```
port-name IIMAS-DGSCA
ip address 132.248.255.198 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255196 ethernet_802.3 netbios-disallow
!
interface ve 204
port-name IIMAS-ARQ
ip address 132.248.255.205 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255204 ethernet_802.3 netbios-disallow
!
!
!
router bgp
local-as 278
neighbor 132.248.255.252 remote-as 278
neighbor 132.248.255.252 update-source loopback 1
neighbor 132.248.255.252 soft-reconfiguration inbound
neighbor 132.248.255.254 remote-as 278
neighbor 132.248.255.254 update-source loopback 1
neighbor 132.248.255.254 soft-reconfiguration inbound
network 132.248.0.0 255.255.0.0
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.248.204.100
access-list 1 permit host 132.248.204.101
access-list 1 permit host 132.248.204.102
access-list 1 permit host 132.248.204.104
access-list 1 permit host 132.248.204.37
access-list 1 permit host 132.248.204.38
access-list 1 permit host 132.248.204.48
access-list 1 permit host 132.248.204.49
access-list 1 permit host 132.248.204.50
access-list 1 permit host 132.248.204.105
access-list 1 permit host 132.247.253.1
access-list 1 permit host 132.248.204.27
!
access-list 40 permit host 132.248.204.27
access-list 40 permit host 132.247.253.1
access-list 40 permit host 200.15.3.86
access-list 40 permit host 200.15.3.14
access-list 40 permit host 132.248.204.37
access-list 40 deny any
!
```

```
!
!
!
!
end

 ZC-CORE NetIron 800
Current configuration:
!
ver 07.5.04T53
!
module 1 bi-4-port-gig-m4-management-module
module 2 bi-4-port-gig-m4-management-module
module 3 bi-24-port-100fx-module
module 4 bi-8-port-gig-module
module 5 bi-atm-2-port-155m-module
!
global-protocol-vlan
!
trunk switch ethe 4/1 to 4/2
port-name "A DGSCA" ethernet 4/1
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 128 name AREA5 by port
tagged ethe 4/3
untagged ethe 3/1 to 3/3
router-interface ve 128
!
vlan 32 name AREA2 by port
untagged ethe 3/4 to 3/6
router-interface ve 32
!
vlan 192 name ZC-DGSCA by port
untagged ethe 4/1 to 4/2
router-interface ve 192
!
vlan 212 name ZC-IIMAS by port
untagged ethe 4/5
router-interface ve 212
!
vlan 338 name DGIRE by port
untagged ethe 3/7
!
vlan 339 name PLANEACION-DGEDI by port
untagged ethe 3/8
!
```

```
vlan 368 name PROTECCION-DGSG by port
untagged ethe 3/9
!
vlan 366 name UNIVERSUM by port
untagged ethe 3/10
!
vlan 3253 name DNS-MX by port
tagged ethe 4/3
router-interface ve 253
!
vlan 3237 name ASCEND by port
tagged ethe 4/3
router-interface ve 237
!
vlan 2220 name INTERNET2 by port
tagged ethe 4/3
router-interface ve 220
!
vlan 3165 name DGSQUITA by port
tagged ethe 4/3
router-interface ve 165
!
!
router ipx
router appletalk
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
boot sys fl sec
atm boot sec
enable telnet authentication
enable super-user-password .....
hostname ZC_CORE
!
ip as-path access-list NO-CUDI-NETWORKS seq 5 deny ^18592_
ip as-path access-list NO-CUDI-NETWORKS seq 10 permit .*
ip dns domain-name core-gigabit.unam.mx
ip dns server-address 132.248.10.2 132.248.204.1
ip route 0.0.0.0 0.0.0.0 132.248.255.133 distance 2
ip route 0.0.0.0 0.0.0.0 132.248.255.131 distance 3
ip route 132.248.77.0 255.255.255.0 132.248.255.33
ip route 132.248.117.0 255.255.255.0 132.248.255.33
ip route 132.248.192.0 255.255.255.0 132.248.255.33
ip route 132.248.37.0 255.255.255.0 132.248.255.35
ip route 132.248.40.0 255.255.255.0 132.248.255.35
ip route 132.248.101.0 255.255.255.0 132.248.255.35
ip route 132.248.177.0 255.255.255.0 132.248.255.35
ip route 132.248.2.0 255.255.255.0 132.248.255.34
```

```
ip route 132.248.65.0 255.255.255.0 132.248.255.34
ip route 132.248.82.0 255.255.255.0 132.248.255.34
ip route 132.248.150.0 255.255.255.0 132.248.255.34
ip route 132.248.174.0 255.255.255.0 132.248.255.34
ip route 132.247.27.0 255.255.255.0 132.248.255.34
ip route 132.248.42.0 255.255.255.0 132.248.255.34
ip route 0.0.0.0 0.0.0.0 132.248.255.132 distance 2
ip route 148.237.220.0 255.255.255.0 132.247.255.253
!
telnet access-group 1
tacacs-server host 200.15.3.14
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
snmp-server community ..... ro 40
snmp-server community ..... ro 41
snmp-server community ..... rw 40
snmp-server community ..... rw 41
ssh access-group 1
router ospf
area 0.0.0.0
area 0.0.0.2
area 0.0.0.5
area 0.0.0.6
auto-cost reference-bandwidth 1000
metric-type type1
redistribution static
!
interface loopback 1
port-name ROUTER-ID
ip address 132.248.255.252 255.255.255.255
ip ospf area 0.0.0.0
!
interface ethernet 3/1
port-name A TELECOM 6
!
interface ethernet 3/2
port-name A TELECOM 1
!
interface ethernet 3/3
port-name A PITAGORAS
!
interface ethernet 3/4
port-name A C.CULTURAL
!
interface ethernet 3/5
port-name A C.HUMANIDADES
!
```

```
interface ethernet 3/6
port-name A PATRONATO
!
interface ethernet 3/7
port-name A DGIRE
ip address 132.248.38.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.2
!
interface ethernet 3/8
port-name A PLANEACION-DGEDI
ip address 132.248.39.254 255.255.255.0 ospf-passive
ip address 132.248.105.46 255.255.255.240 ospf-passive
ip ospf area 0.0.0.2
!
interface ethernet 3/9
port-name A PROTECCION-DGSG
ip address 132.248.68.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.2
!
interface ethernet 3/10
port-name A UNIVERSUM
ip address 132.248.66.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.2
!
interface ethernet 3/24
port-name PRUEBAS CON PEDIATRIA
!
interface ethernet 4/1
port-name A DGSCA
!
interface ethernet 4/3
port-name A SWITCH 3900 CON TAG
!
interface ethernet 4/5
port-name A IIMAS
!
interface atm 5/1
port-name ATM A TELECOM7-I2
!
interface atm 5/1.1 point-to-point
atm pvc 0 67 ubr
ip address 132.247.255.254 255.255.255.252
ip ospf area 0.0.0.6
!
!
interface ve 32
port-name AREA2
```

```
ip address 132.248.255.38 255.255.255.248
ip ospf area 0.0.0.2
ipx net 00025532 ethernet_802.3 netbios-disallow
!
interface ve 128
port-name AREA5
ip address 132.248.255.142 255.255.255.240
ip ospf area 0.0.0.5
ip ospf priority 255
ipx net 00255128 ethernet_802.3 netbios-disallow
!
interface ve 165
port-name A DGSQUITA
ip address 132.248.165.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.2
!
interface ve 192
port-name ZC-DGSCA
ip address 132.248.255.194 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255192 ethernet_802.3 netbios-disallow
!
interface ve 212
port-name ZC-IIMAS
ip address 132.248.255.214 255.255.255.252
ip ospf area 0.0.0.0
!
interface ve 220
ip address 132.247.255.222 255.255.255.252 ospf-passive
!
interface ve 237
port-name ASCEND
ip address 132.248.237.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.2
!
interface ve 253
port-name DNS-MX
ip address 132.248.253.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.2
!
ip tacacs source-interface loopback 1
!
!
router bgp
cluster-id 1
local-as 278
neighbor CLIENTES-ROUTERS-REDUNAM peer-group
```

```
neighbor CLIENTES-ROUTERS-REDUNAM remote-as 278
neighbor CLIENTES-ROUTERS-REDUNAM update-source loopback 1
neighbor CLIENTES-ROUTERS-REDUNAM filter-list NO-CUDI-NETWORKS out
neighbor CLIENTES-ROUTERS-REDUNAM route-reflector-client
neighbor CLIENTES-ROUTERS-REDUNAM soft-reconfiguration inbound
neighbor CLIENTES-SWITCHES-REDUNAM peer-group
neighbor CLIENTES-SWITCHES-REDUNAM remote-as 278
neighbor CLIENTES-SWITCHES-REDUNAM update-source loopback 1
neighbor CLIENTES-SWITCHES-REDUNAM route-reflector-client
neighbor CLIENTES-SWITCHES-REDUNAM soft-reconfiguration inbound
neighbor 132.248.255.189 peer-group CLIENTES-ROUTERS-REDUNAM
neighbor 132.248.255.189 description Telecom6
neighbor 132.248.255.253 peer-group CLIENTES-SWITCHES-REDUNAM
neighbor 132.248.255.253 description IIMAS_CORE
neighbor 132.248.255.251 peer-group CLIENTES-SWITCHES-REDUNAM
neighbor 132.248.255.251 description ARQ_CORE
neighbor 132.248.255.254 peer-group CLIENTES-SWITCHES-REDUNAM
neighbor 132.248.255.254 description DGSCA_CORE
neighbor 132.248.255.191 peer-group CLIENTES-ROUTERS-REDUNAM
neighbor 132.248.255.191 description Telecom1
neighbor 132.248.255.190 peer-group CLIENTES-ROUTERS-REDUNAM
neighbor 132.248.255.190 description Pitagoras
neighbor 132.247.255.4 peer-group CLIENTES-ROUTERS-REDUNAM
neighbor 132.247.255.4 description Telecom7-I2
network 132.248.0.0 255.255.0.0
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.248.204.100
access-list 1 permit host 132.248.204.101
access-list 1 permit host 132.248.204.102
access-list 1 permit host 132.248.204.104
access-list 1 permit host 132.248.204.37
access-list 1 permit host 132.248.204.38
access-list 1 permit host 132.248.204.48
access-list 1 permit host 132.248.204.49
access-list 1 permit host 132.248.204.50
access-list 1 permit host 132.248.204.105
access-list 1 permit host 132.247.253.1
access-list 1 permit host 132.248.204.27
!
access-list 40 permit host 132.248.204.27
access-list 40 permit host 132.247.253.1
access-list 40 permit host 200.15.3.86
access-list 40 permit host 132.248.204.37
```

```
access-list 40 deny any
!
access-list 41 permit host 200.15.3.14
access-list 41 deny any
!
!
!
!
!
end

 ARQUITECTURA-CORE BigIron 8000
Current configuration:
!
ver 07.5.04T53
!
module 1 bi-8-port-gig-m4-management-module
module 2 bi-8-port-gig-m4-management-module
module 3 bi-24-port-100fx-module
!
global-protocol-vlan
!
trunk switch ethe 1/1 to 1/2
port-name "A IIMAS " ethernet 1/1
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 204 name ARQ-IIMAS by port
untagged ethe 1/1 to 1/2
router-interface ve 204
!
vlan 200 name ARQ-DGSCA by port
untagged ethe 2/1
router-interface ve 200
!
vlan 208 name ARQ-RECTORIA by port
untagged ethe 2/7
router-interface ve 208
!
vlan 3247 name DGI by port
untagged ethe 3/7
!
vlan 323 name DGP by port
untagged ethe 3/8
!
vlan 325 name PSICOLOGIA by port
untagged ethe 3/9
```

```
!
vlan 3137 name PATRONATO by port
untagged ethe 3/10
!
vlan 4095 name AREA1 by port
untagged ethe 3/1 to 3/6
router-interface ve 255
!
!
router ipx
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
boot sys fl sec
enable telnet authentication
enable super-user-password .....
hostname ARQ_CORE
ip route 0.0.0.0 0.0.0.0 132.248.255.201
ip route 0.0.0.0 0.0.0.0 132.248.255.205 distance 2
ip route 132.248.21.0 255.255.255.0 132.248.255.1
ip route 132.248.22.0 255.255.255.0 132.248.255.1
ip route 132.248.185.0 255.255.255.0 132.248.255.1
ip route 132.248.112.0 255.255.255.0 132.248.255.2
ip route 132.248.122.0 255.255.255.0 132.248.255.3
ip route 132.248.178.0 255.255.255.0 132.248.255.3
ip route 132.248.144.0 255.255.255.0 132.248.255.3
ip route 132.248.123.0 255.255.255.0 132.248.255.3
ip route 132.248.67.0 255.255.255.0 132.248.255.3
ip route 132.248.70.0 255.255.255.0 132.248.255.3
ip route 132.248.197.0 255.255.255.0 132.248.255.3
ip route 132.248.130.0 255.255.255.0 132.248.255.3
ip route 132.248.47.0 255.255.255.0 132.248.255.3
ip route 132.248.116.0 255.255.255.0 132.248.255.3
ip route 132.248.214.0 255.255.255.0 132.248.255.3
ip route 132.248.43.0 255.255.255.0 132.248.255.4
ip route 132.248.45.0 255.255.255.0 132.248.255.5
ip route 132.248.167.0 255.255.255.0 132.248.255.5
ip route 132.248.84.0 255.255.255.0 132.248.255.6
ip route 132.248.74.0 255.255.255.0 132.248.255.3
!
telnet access-group 1
tacacs-server host 200.15.3.14
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
snmp-server community ..... ro 40
snmp-server community ..... rw 40
snmp-server contact Depto. de Operacion de la Red Tel. 5622 8509
snmp-server location Nodo ARQUITECTURA
```

```
ssh access-group 1
router ospf
area 0.0.0.0
area 0.0.0.1
auto-cost reference-bandwidth 1000
metric-type type1
redistribution static
!
router pim
!
interface loopback 1
port-name ROUTER-ID
ip address 132.248.255.251 255.255.255.255
ip ospf area 0.0.0.0
!
interface ethernet 1/1
port-name A IIMAS
!
interface ethernet 2/1
port-name A DGSCA
!
interface ethernet 2/7
port-name A RECTORIA
!
interface ethernet 3/1
port-name A DGO
!
interface ethernet 3/2
port-name A DGPP
!
interface ethernet 3/3
port-name A LOC.ARQ
!
interface ethernet 3/4
port-name A FAC.ARQ
!
interface ethernet 3/5
port-name A FAC.ECONOMIA
!
interface ethernet 3/6
port-name A FAC.DERECHO
!
interface ethernet 3/7
port-name A DGI
ip address 132.248.247.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.1
!
```

```
interface ethernet 3/8
port-name A DGP
ip address 132.248.23.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.1
!
interface ethernet 3/9
port-name A PSICOLOGIA
ip address 132.248.25.254 255.255.255.0 ospf-passive
ip address 132.248.104.254 255.255.255.0 ospf-passive
ip address 132.248.228.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.1
!
interface ethernet 3/10
port-name A PATRONATO
ip address 132.248.137.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.1
!
interface ve 200
port-name ARQ-DGSCA
ip address 132.248.255.202 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255200 ethernet_802.3 netbios-disallow
!
interface ve 204
port-name ARQ-IIMAS
ip address 132.248.255.206 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255204 ethernet_802.3 netbios-disallow
!
interface ve 208
port-name ARQ-RECTORIA
ip address 132.248.255.210 255.255.255.252
ip ospf area 0.0.0.0
ipx net 00255208 ethernet_802.3 netbios-disallow
!
interface ve 255
ip address 132.248.255.14 255.255.255.240
ip ospf area 0.0.0.1
ipx net 02554095 ethernet_802.3 netbios-disallow
!
!
!
router bgp
local-as 278
neighbor 132.248.255.252 remote-as 278
neighbor 132.248.255.252 update-source loopback 1
neighbor 132.248.255.252 soft-reconfiguration inbound
```

```
neighbor 132.248.255.254 remote-as 278
neighbor 132.248.255.254 update-source loopback 1
neighbor 132.248.255.254 soft-reconfiguration inbound
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.248.204.100
access-list 1 permit host 132.248.204.101
access-list 1 permit host 132.248.204.102
access-list 1 permit host 132.248.204.104
access-list 1 permit host 132.248.204.37
access-list 1 permit host 132.248.204.38
access-list 1 permit host 132.248.204.48
access-list 1 permit host 132.248.204.49
access-list 1 permit host 132.248.204.50
access-list 1 permit host 132.248.204.105
access-list 1 permit host 132.247.253.1
access-list 1 permit host 132.248.204.27
!
access-list 2 permit host 132.248.106.0
access-list 2 permit host 132.248.19.0
access-list 2 permit host 132.247.28.0
access-list 2 permit host 132.248.255.250
access-list 2 permit host 132.248.244.0
access-list 2 permit host 132.248.186.0
access-list 2 permit host 132.248.171.0
access-list 2 permit host 132.248.151.0
access-list 2 permit host 132.248.136.0
!
access-list 40 permit host 132.248.204.27
access-list 40 permit host 132.247.253.1
access-list 40 permit host 200.15.3.86
access-list 40 permit host 200.15.3.14
access-list 40 permit host 132.248.204.37
access-list 40 deny any
!
!
!
!
!
end
 Equipos de la capa de distribuci¶on
 DGSCA-DIST BigIron 8000
Current configuration:
!
```

```
ver 07.5.04T53
!
module 1 bi-8-port-gig-m4-management-module
module 2 bi-24-port-copper-module
!
global-protocol-vlan
!
trunk switch ethe 1/1 to 1/2
port-name "A DGSCA CORE" ethernet 1/1
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 96 name AREA4 by port
untagged ethe 1/1 to 1/2
router-interface ve 96
!
vlan 348 name CUAED-DGDI by port
untagged ethe 2/1
!
vlan 1317 name CONECTIVIDAD by port
untagged ethe 2/2
!
vlan 3170 name DGSCA-170 by port
untagged ethe 2/3 ethe 2/12
router-interface ve 170
!
vlan 371 name COORD-DE-SERVICIOS by port
untagged ethe 2/4
!
vlan 3204 name REDES by port
untagged ethe 2/8
!
vlan 21 name SERVIDORE-EXT by port
untagged ethe 2/13
!
vlan 2 name ROUTER-IPV6 by port
untagged ethe 2/9
!
vlan 3202 name VIDEOCONFERENCIA by port
untagged ethe 2/24
!
vlan 3200 name DGSCA-200 by port
untagged ethe 2/23
!
vlan 3190 name DGSCA-190 by port
untagged ethe 2/17 to 2/22
router-interface ve 190
```

```
!
vlan 16 name AS5100-DGSCA by port
untagged ethe 2/5
!
!
router ipx
router appletalk
appletalk rtmp-update-interval 50
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
boot sys fl sec
enable telnet authentication
enable super-user-password .....
hostname DGSCA_DIST
ip dns domain-name dist-gigabit.unam.mx
ip dns server-address 132.248.204.1
ip route 0.0.0.0 0.0.0.0 132.248.255.110
ip route 132.248.108.0 255.255.255.0 192.100.200.226
!
telnet access-group 1
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
snmp-server community ..... ro 1
snmp-server community ..... ro 41
snmp-server community ..... rw 41
ssh access-group 1
router ospf
area 0.0.0.4
auto-cost reference-bandwidth 1000
metric-type type1
redistribution static
!
router pim
!
interface loopback 1
port-name ROUTER-ID
ip address 132.248.255.127 255.255.255.255
ip ospf area 0.0.0.4
!
interface ethernet 1/1
port-name A DGSCA CORE
!
interface ethernet 2/1
port-name A CUAED-DGDI
ip address 132.248.48.254 255.255.255.0 ospf-passive
ip address 132.248.184.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.4
```

```
!
interface ethernet 2/2
port-name CONECTIVIDAD
ip address 200.15.3.17 255.255.255.248 ospf-passive
ip address 200.15.3.97 255.255.255.248 ospf-passive
ip ospf area 0.0.0.4
!
interface ethernet 2/3
port-name DGSCA-170
!
interface ethernet 2/4
port-name COORD-DE-SERVICIOS
ip address 132.248.71.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.4
!
interface ethernet 2/5
port-name AS5100-DGSCA
ip address 132.248.120.30 255.255.255.240 ospf-passive
ip ospf area 0.0.0.4
!
interface ethernet 2/8
port-name REDES
ip address 132.248.204.254 255.255.255.0 ospf-passive
ip helper-address 1 132.248.10.50 unicast
ip helper-address 2 132.248.204.50 unicast
ip ospf area 0.0.0.4
!
interface ethernet 2/9
port-name ROUTER-IPV6
appletalk routing
ip address 192.100.200.225 255.255.255.252 ospf-passive
ip ospf area 0.0.0.4
speed-duplex 10-full
!
interface ethernet 2/12
port-name DGSCA-170
!
interface ethernet 2/13
port-name SERVIDORES-EXTERNOS
ip address 132.247.1.254 255.255.255.0 ospf-passive
ip ospf area 0.0.0.4
!
interface ethernet 2/17
port-name DGSCA-190
!
interface ethernet 2/18
port-name DGSCA-190
```

```
!
interface ethernet 2/19
port-name DGSCA-190
!
interface ethernet 2/20
port-name DGSCA-190
!
interface ethernet 2/21
port-name DGSCA-190
!
interface ethernet 2/22
port-name DGSCA-190
!
interface ethernet 2/23
port-name DGSCA-200
ip address 132.248.200.254 255.255.255.0 ospf-passive
ip helper-address 1 132.248.204.50 unicast
ip ospf area 0.0.0.4
!
interface ethernet 2/24
port-name A VIDECONFERENCIA
ip address 132.248.202.254 255.255.255.0 ospf-passive
ip helper-address 1 132.248.204.50 unicast
ip ospf area 0.0.0.4
!
interface ve 96
port-name AREA4
appletalk routing
ip address 132.248.255.109 255.255.255.240
ip ospf area 0.0.0.4
!
interface ve 170
port-name DGSCA-170
ip address 132.248.170.254 255.255.255.0 ospf-passive
ip helper-address 1 132.248.204.50 unicast
ip ospf area 0.0.0.4
!
interface ve 190
port-name DGSCA-190
ip address 132.248.190.254 255.255.255.0 ospf-passive
ip helper-address 1 132.248.204.50 unicast
ip ospf area 0.0.0.4
!
!
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
```

```
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.247.253.14
access-list 1 permit host 132.248.204.100
access-list 1 permit host 132.248.204.101
access-list 1 permit host 132.248.204.102
access-list 1 permit host 132.248.204.104
access-list 1 permit host 132.248.204.37
access-list 1 permit host 132.248.204.38
access-list 1 permit host 132.248.204.48
access-list 1 permit host 132.248.204.49
access-list 1 permit host 132.248.204.50
access-list 1 permit host 132.248.204.105
!
access-list 41 permit host 200.15.3.14
access-list 41 deny any
!
access-list 111 deny tcp any any eq 8888
access-list 111 deny tcp any any eq 6699
access-list 111 deny tcp any any eq 7777
access-list 111 deny tcp any any eq 8875
access-list 111 deny tcp any any eq 6688
access-list 111 deny tcp any any eq 1214
access-list 111 deny tcp any any eq 5634
access-list 111 deny tcp any any range 41000 50000
access-list 111 deny tcp any any range 1117 5719
access-list 111 deny tcp any any range 5500 5503
access-list 111 deny tcp any any eq 4814
access-list 111 deny tcp any any eq 60683
access-list 111 deny tcp any any eq 1603
access-list 111 deny tcp any any range 6346 6347
access-list 111 permit ip any any
access-list 111 remark FILTRO NAPSTER KAZAA HOLINE AUDIOGALAXY
GNUTELLA MORPHEUS;OA;230702
!
!
!
ip ssh pub-key-file tftp 200.15.3.82 pubkeys.txt
!
ip ssh source-interface loopback 1
!
end

 ANTROPOLOGICAS BigIron 8000
Current configuration:
!
ver 07.2.09T53
```

```
module 1 bi-8-port-gig-m4-management-module
module 2 bi-8-port-gig-module
!
global-protocol-vlan
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 96 name AREA4 by port
untagged ethe 1/1
router-interface ve 96
!
!
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
enable telnet authentication
enable super-user-password .....
hostname ANTROPOLOGICAS
ip dns server-address 132.248.204.1
ip route 0.0.0.0 0.0.0.0 132.248.255.110
!
telnet access-group 1
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
router ospf
area 0.0.0.4
auto-cost reference-bandwidth 1000
!
interface loopback 1
port-name ROUTER_ID
ip address 132.248.255.126 255.255.255.255
ip ospf area 0.0.0.4
!
interface ve 96
port-name AREA4
ip address 132.248.255.108 255.255.255.240
ip ospf area 0.0.0.4
!
!
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.247.253.14
access-list 1 permit host 132.248.204.100
access-list 1 permit host 132.248.204.101
```

```
access-list 1 permit host 132.248.204.102
access-list 1 permit host 132.248.204.104
access-list 1 permit host 132.248.204.37
access-list 1 permit host 132.248.204.27
access-list 1 permit host 132.248.204.38
access-list 1 permit host 132.248.204.48
access-list 1 permit host 132.248.204.49
access-list 1 permit host 132.248.204.50
access-list 1 permit host 132.248.204.105
!
!
!
end
```

```
 LOCAL IIMAS BigIron 8000
Current configuration:
!
ver 07.5.04T53
!
module 1 bi-8-port-gig-m4-management-module
module 2 bi-8-port-gig-module
!
global-protocol-vlan
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 64 name AREA3 by port
untagged ethe 1/1
router-interface ve 64
!
!
router ipx
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
boot sys fl sec
enable telnet authentication
enable super-user-password .....
hostname LOC_IIMAS
ip route 0.0.0.0 0.0.0.0 132.248.255.78
!
telnet access-group 1
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
ssh access-group 1
router ospf
area 0.0.0.3 stub 1
```

```
auto-cost reference-bandwidth 1000
!
interface loopback 1
port-name ROUTER-ID
ip address 132.248.255.95 255.255.255.255
ip ospf area 0.0.0.3
!
interface ethernet 1/1
port-name A IIMAS
!
interface ve 64
port-name AREA3
ip address 132.248.255.75 255.255.255.240
ip ospf area 0.0.0.3
ip ospf priority 255
!
!
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.248.204.105
!
!
!
!
!
end

 LABORALES BigIron 8000
Current configuration:
!
ver 07.5.04T53
!
module 1 bi-8-port-gig-m4-management-module
module 2 bi-8-port-gig-module
!
global-protocol-vlan
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 64 name AREA3 by port
untagged ethe 1/1
router-interface ve 64
!
```

```
!
router ipx
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
boot sys fl sec
enable telnet authentication
enable super-user-password .....
hostname LABORALES
ip route 0.0.0.0 0.0.0.0 132.248.255.78
!
telnet access-group 1
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
ssh access-group 1
router ospf
area 0.0.0.3 stub 1
auto-cost reference-bandwidth 1000
!
interface loopback 1
port-name ROUTER-ID
ip address 132.248.255.93 255.255.255.255
ip ospf area 0.0.0.3
!
interface ethernet 1/1
port-name A IIMAS
!
interface ve 64
port-name AREA3
ip address 132.248.255.77 255.255.255.240
ip ospf area 0.0.0.3
ip ospf priority 250
!
!
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.248.204.105
!
!
!
!
!
end
```

ASTRONOMIA BigIron 8000

```
Current configuration:
!
ver 07.5.04T53
!
module 1 bi-8-port-gig-m4-management-module
module 2 bi-8-port-gig-module
!
global-protocol-vlan
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 64 name AREA3 by port
untagged ethe 1/1
router-interface ve 64
!
!
router ipx
aaa authentication enable default tacacs+ enable
aaa authentication login default tacacs+ enable
boot sys fl sec
enable telnet authentication
enable super-user-password .....
hostname ASTRONOMIA
ip route 0.0.0.0 0.0.0.0 132.248.255.78
!
telnet access-group 1
tacacs-server host 200.15.3.82
tacacs-server key 1 .....
ssh access-group 1
router ospf
area 0.0 0.3 stub 1
auto-cost reference-bandwidth 1000
!
interface loopback 1
port-name ROUTER-ID
ip address 132.248.255.94 255.255.255.255
ip ospf area 0.0.0.3
!
interface ethernet 1/1
port-name A IIMAS
!
interface ve 64
port-name AREA3
ip address 132.248.255.76 255.255.255.240
ip ospf area 0.0.0.3
!
```

```
!
!
access-list 1 permit 132.248.254.0 0.0.0.255
access-list 1 permit 132.248.255.0 0.0.0.255
access-list 1 permit 200.15.3.80 0.0.0.7
access-list 1 permit 200.15.3.8 0.0.0.7
access-list 1 permit host 132.248.204.105
!
!
!
!
!
end
```