



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

FACULTAD DE INGENIERÍA

**Diseño e implementación del Sistema de Control y
Operación de la Red Internet 2 de México:
NOC-CUDI**

TESIS

Que para obtener el título de:

INGENIERO EN COMPUTACIÓN

Presenta:

NORMA GABRIELA MEDINA GALINDO

Director de tesis:

Ing. Armando Vega Alvarado

Codirector:

Ing. Alberto González Guízar

México, D.F.

Febrero del 2007





Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Agradecimientos:

A Dios, en cualesquiera de sus formas, por haberme dado el maravilloso regalo de la vida. Dios, espero no desperdiciarlo y disfrutarlo cada día más.

La vida me dio la oportunidad de conocer a otro ser maravilloso: mi madre, la cual le agradezco su amor, su protección, sus enseñanzas y sabiduría.

Mamá, te agradezco con toda mi existencia el habérmela dado y todo ese hermoso sueño que significó mi crecimiento a tu lado y que tu colmaste de amor. Gracias infinitas porque a ti te debo lo que soy ahora.

A un ser particularmente especial para mí: Ángel, mi bebé. Hijo, gracias por existir porque eres mi razón de vivir y de querer ser cada vez mejor ser humano y mi compromiso es formarte como un gran hombre, pondré todo mi esfuerzo porque así sea. Eres lo que más amo en este mundo y mi preparación es para ofrecerte un ejemplo de vida.

A los cuatro de los cinco mosqueteros que somos, "uno para todos y todos para uno": Adry, Carlos, Ericka, Sergio (y yo). Los amo entrañablemente. Su compañía en este mundo ha sido mi mejor regalo. De cada uno de ustedes aprender ha significado divertirse y fortalecerse juntos. Son parte de mí.

A todo el gran equipo que somos ahora con los agregados fruto del amor: mis cuñados Gabriel, Miguel, Gabriela que me han apoyado siempre y propagado la semilla de familia y proporcionado su grano de arena para las semillitas maravillosas: Carlitos, Miguelito, Gabrielito, Emiliano, Marianita, Marifer, Valeria, Eduardito y Gabrielita. Son y serán mis pequeños amores.

A mis amigos, valiosos compañeros de mi vida que gracias a Dios son varios, de los cuales conocí los valores de la amistad, la lealtad, la compañía, la charla amable, a veces trascendental y a veces frívola pero igual de rica en filosofía y cariño. Siempre los tengo a mi lado. Los quiero.

A mis maestros de la Facultad de Ingeniería, por sus enseñanzas, guías y formación.

A mi adorada UNAM, vislumbrada como un sueño desde pequeña y que tuve la gran oportunidad de pertenecer y formarme en ella. Eres mi sueño alcanzado que me cobijaste para formarme como una profesional.

Pero toda mi vida guardo un agradecimiento muy especial...a mi padre. Desde mi juventud no está conmigo, está en el cielo, pero dejó un enorme legado en mí, un legado de amor, fortaleza y sabiduría... Me enseñó a soñar! Y a luchar por cumplir los sueños...te extraño...te amo....gracias por abrir mis alas...gracias por enseñarme a volar...gracias por creer en mi vuelo...AHORA VUELO!!!

Mi vida es y será un eterno disfrute...

"...te digo que no mires atrás...y que nos comeremos el mundo poco a poco..."

"...lo haremos, pero en el camino de eso, vamos divirtiéndonos..." (agregación propia)

Índice Temático

PREFACIO	i
Capítulo 1 ANTECEDENTES	1
1.1 Internet y sus limitantes	1
1.2 El desarrollo de la nueva generación	5
1.3 La nueva red: Internet 2	6
1.4 Descriptivo de las Aplicaciones Internet 2	15
1.5 Nuevas Capacidades de la Red	17
1.6 El reto en la Operación de Internet 2	19
Capítulo 2 INTERNET 2 EN MÉXICO: CUDI	23
2.1 Desarrollo de Internet 2 en México	23
2.2 CUDI	25
2.3 Descripción de la Red CUDI	27
2.4 Aplicaciones	33
Capítulo 3 DESARROLLO DE LA PROPUESTA PARA EL CENTRO DE CONTROL Y OPERACIÓN DE LA RED INTERNET 2 DE MÉXICO "NOC-CUDI"	
3.1 Objetivo del Centro de Operación	35
3.2 Desarrollo de la Propuesta	39
Capítulo 4 PROPUESTA DEL NOC-CUDI: DEFINICIÓN, ESTRUCTURA DE OPERACIÓN Y CONTROL	85
4.1 Objetivo del NOC-CUDI	85
4.2 Metas del NOC-CUDI	85
4.3 Descripción de funciones	86
4.4 Identificación y definición de elementos de la red a operar	90

4.5	Descripción del Esquema de Operación	93
4.6	Responsabilidades de las Entidades	101
4.7	Contacto al NOC-CUDI	104
4.8	Administración de Fallas	108
4.9	Administración de Cambios	113
4.10	Procedimientos	116
Capítulo 5	CONFIGURACIÓN BASE DE OPERACIÓN DEL BACKBONE DE LA RED (DORSAL PRINCIPAL)	121
5.1	Esquema inicial de ruteo para la dorsal	121
5.2	Esquema de direccionamiento IPv6 de la red	128
5.3	Esquema de multicast	137
Capítulo 6	CONCLUSIONES	139
ANEXOS	143
ANEXO 1. INSTITUCIONES DE CUDI		144
ANEXO 2. APLICACIONES		149
GLOSARIO	154
BIBLIOGRAFÍA	158

PREFACIO

Sin duda que las redes de datos de todos los tipos y tamaños han cambiado sustancialmente de acuerdo a los cambios de tecnología que estamos viviendo. Estos cambios tecnológicos han propiciado la evolución de las redes de comunicaciones posicionándolas como un elemento crítico para la operación de cualquier compañía, universidad, escuela, centro de investigación, del gobierno, salud, etc.

La aparición del Internet fue una pieza clave para impulsar la explosión de los requerimientos y demandas de conexión de todas estas entidades usándola ya como parte de la operación diaria de sus actividades. Hoy en día no se conciben la realización de las actividades o de la productividad de estas entidades sin las redes de datos.

Por supuesto mientras mas grande sea la organización, complejas sus actividades y crítica la ejecución de sus procesos, más esencial se vuelve el mantener sus redes funcionando en buen estado; cada caída del sistema o cada corte de conexión de los usuarios con este, puede significar grandes pérdidas económicas o productivas en cualquier sentido.

Todavía hace unos años se tenían divididas las redes de voz y datos por ejemplo, pero hoy en día, las redes están apuntando cada vez mas hacia la integración de las aplicaciones de tal forma que se mantenga una sola infraestructura para el soporte de todas las necesidades de comunicación, en este momento las redes de voz y datos ya viajan por el mismo clave lo que conlleva a un compromiso de mantener estas aplicaciones en operación continua y con buena calidad.

Estas nuevas necesidades han impulsado a tener sistemas de operación y control de las redes eficientes y de ubicar la posición del administrador o del operador de la red de una forma más relevante dentro de las organizaciones. Sin embargo, la operación de una red no es trivial y debe darse la importancia y enfoque adecuado para cumplir los objetivos. Esta puede ser tan sencilla o tan compleja como se requiera para cubrir las expectativas de calidad de funcionamiento de las aplicaciones

Cuando se trata de redes de alto desempeño para cubrir necesidades de aplicaciones de alta demanda el diseño del esquema de operación se hace más crítico y elemental la definición de una entidad de responsabilidad específica en ello y de la definición de sus actividades y herramientas a ser utilizadas.

Internet 2 es una red de alto desempeño con características particulares de las aplicaciones a las que va orientado y no es trivial la definición de su operación ya que a pesar de que es un proyecto académico e investigación particularmente, son miembros de la conexión entidades independientes, con objetivos diversos y compromisos diferentes, adicionalmente de que trabajan con procedimientos independientes en un proyecto conjunto.

Objetivo

Diseñar y presentar un esquema de control y operación de la red nacional de Internet 2 de México definiendo una identidad operativa central, como Centro de Operación de la Red (NOC-CUDI), sus alcances, esquemas técnicos, funciones operativas, herramientas tecnológicas y procedimientos que conformen el control, monitoreo y operación de la infraestructura física y lógica de la red de Internet 2 de México (CUDI), que garantice en el país, el soporte de las aplicaciones académicas e investigación de alto desempeño, apoye el desarrollo de Internet y las nuevas tecnologías del Internet Protocol (IP).

Contenido

El presente trabajo no es una descripción propiamente de tecnologías sino un análisis para una propuesta de solución y esta dividido en 5 capítulos sustanciales y un capítulo de Conclusiones, de acuerdo a:

Capítulo 1. Se proporciona un histórico del desarrollo de Internet, sus problemáticas existentes, sus desventajas de uso para las aplicaciones de alto desempeño y la respuesta de la comunidad internacional a esto con la iniciativa de desarrollo de la nueva generación de Internet 2.

Capítulo 2. Se expone el desarrollo de Internet 2 en México, los esfuerzos conjuntos del ámbito académico y la creación de la corporación de respaldo para el desarrollo del proyecto, se explican el panorama de las aplicaciones a las que se debe dar soporte, el diseño y las necesidades operativas de la nueva red a implantar.

Capítulo 3. Se definen las necesidades del proyecto de Internet 2 y de sus aplicaciones, las expectativas que se sostienen de la operación de la nueva red, se describe el análisis desarrollado para atacar cada una de las necesidades de la operación de la nueva red en base al modelo OSI y a la operación de TCP/IP, las iniciativas de los esquemas a implementar, la conjunción de herramientas tecnológicas para cada nivel de operación. En este capítulo se da una breve descripción de estas tecnologías enfocándonos principalmente en los análisis de las diferentes recomendaciones y estándares de administración de redes existentes para hacer una recapitulación y diseño del esquema propio para las necesidades de la red de CUDI

Capítulo 4. En este capítulo se definen puntualmente los alcances, se describen las actividades, herramientas, desarrollos y procedimientos establecidos para la propuesta de operación de la red de CUDI. Se describe el diseño de la estructura funcional del NOC-CUDI y sus iteraciones recomendadas con otras áreas de apoyo en el desarrollo de sus funciones.

Capítulo 5. Se plantean las configuraciones básicas de inicio de operación de la dorsal de CUDI con las configuraciones recomendadas por el NOC-CUDI de una forma general pero puntual para el tránsito adecuado del tráfico de las aplicaciones críticas de la red.

Capítulo 6. Conclusiones de los alcances cumplidos en el presente trabajo y la experiencia y conocimientos obtenidos durante su desarrollo.

Capítulo 1

ANTECEDENTES

1.1 INTERNET Y SUS LIMITANTES

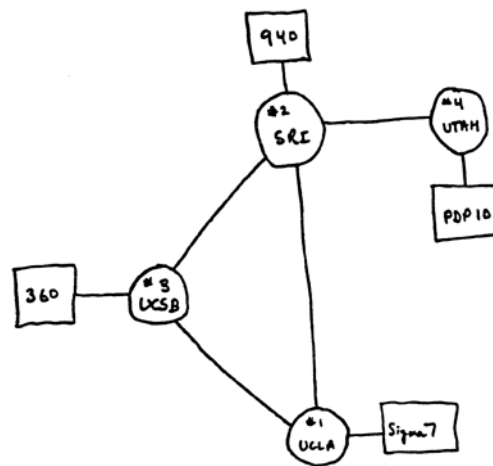
1.1.1 Historia y Evolución de Internet

Definitivamente Internet es uno de los proyectos más importantes en la historia de la humanidad que ha revolucionado el cómputo y las comunicaciones a nivel mundial y ha sido punto clave en la evolución tecnológica de la sociedad entera.

Desde sus inicios, en el periodo final de los 60s, Internet surge como una red experimental, como una colaboración entre entidades de gobierno y educación, orientada como una herramienta de apoyo al sector de investigación y de acercamiento entre proyectos académicos; subsecuentemente son varios sus aspectos de desarrollo: tecnológicos, administrativos, de operación, sociales y comerciales, sin mencionar el aspecto jurídico. Cada uno de ellos con partícipes y velocidades diferentes, pero todos encaminados en el crecimiento y desarrollo vertiginoso de la Internet.

En este periodo de los 60s justamente se desarrollaban por diferentes grupos –entre ellos el MIT- proyectos en paralelo sobre la comunicación de computadoras usando paquetes en lugar de circuitos, esto significó un paso importantísimo para las comunicaciones ya que implicaba mejores comportamientos y velocidades en las conexiones punto a punto a mayores distancias, mecanismos que fueron rápidamente adoptados en diferentes proyectos de comunicaciones contemporáneos gracias a sus excelentes resultados, como lo hizo la DARPA (Defense Advanced Research Projects Agency) en 1966 quien estaba a cargo del desarrollo de una red experimental denominada ARPANET.

El reto de DARPA era la interconexión de sistemas remotos de una forma transparente y ágil investigando técnicas y tecnologías que lo permitieran independientemente al tipo de sistema. DARPA instaló el primer nodo de ARPANET en 1969 (en la UCLA), conformando mas tarde la red experimental por 4 nodos unidos a 56 kbps basada en la comunicación por paquetes. Rápidamente se fueron uniendo otros nodos a la ARPANET.



Red ARPANET. Dibujo original. Fuente: www.isoc.org/cerf

A partir de 1973, DARPA enfatizó sus esfuerzos en el desarrollo de estas técnicas de comunicación conjuntados en protocolos que se describían como sistemas abiertos ya que se lograba la comunicación cualesquiera que fuera el tipo de sistema, impulsando fuertemente el crecimiento de ARPANET.

La visión entonces con los protocolos abiertos era la de conformar estos ambientes de interconexión también de forma local, entre equipos pertenecientes a una misma área, lo que dio espacio a las redes locales, conectadas en topologías diversas e independientes pero todas ellas tendientes a interconectarse a redes mas amplias como ARPANET, y formar una gran, “red de redes” entonces llamada Internet. El protocolo usado para Internet fue el conocido como TCP/IP (Transmission Control Protocol/Internet Protocol).

La propagación de redes locales, estaciones personales de trabajo, topologías como ethernet, el sistema operativo Unix y protocolos abiertos como TCP/IP impulsaron el

uso de Internet entre la comunidad académica y la red militar MILNET se unió a ella. Ya para 1985, ARPANET era ampliamente usada, provocando que la NSF (National Science Foundation) tomara mayor interés en el desarrollo de una red de mayores capacidades, instalando en 1986 la NSFNET, exclusivamente para fines académicos. En Europa surgieron otras iniciativas más.

Para 1989, ARPANET fue declinada y la red MILNET separó sus conexiones en una red privada. La NSFNET creció en extensión y en capacidades, concesionada en 1989 a Merit Networks para su administración, con alianzas de MCI, IBM y el estado de Michigan. Debido al gran crecimiento y demanda de servicios de la NSFNET, estos grupos crearon la ANS (Advanced Networks Services) dividiendo las tareas de manejo de la red, encargándose Merit de la administración y políticas de enrutamiento de ésta y la ANS de la operación propia de los equipos.

En el periodo de finales de los 80s y principios de los 90, diversas inquietudes de otras partes del mundo y de otros sectores diferentes al académico empezaron visualizar la Internet como una gran herramienta y solicitaban conexiones a ella para enlazar sus propias redes, creándose una demanda internacional y diversificada; cubierta a través de proveedores locales de servicios de Internet, ISP (Internet Service Provider) que se conectaban hacia la dorsal de la red de la NSFNET creciendo en una arquitectura ampliamente distribuida y operada de la misma forma e integrándose a otros esfuerzos a través de puntos de intercambio.

La incursión del sector comercial en 1988 fue crucial para el paradigma de Internet, dando paso a un “boom” de nuevas herramientas y servicios implementados sobre esta, como el uso del correo electrónico y por supuesto el desarrollo del WWW (World Wide Web), una aplicación de visualización gráfica de la información que permitió acceder de forma mas rápida, cómoda, amigable y atractiva a la información y que hoy en día representa el 75% del uso de la Internet. Sus potencialidades están basadas en la gran variedad de servicios tecnológicos interactuando, diferentes protocolos de comunicación, de ruteo, servicios de nombres, aplicaciones técnicas, etc., conjuntas pero siempre delimitadas y enfocadas a arquitecturas abiertas.

No sabemos el número de redes que actualmente conforman Internet, ni el número exacto de computadoras conectadas, pero podemos hablar de muchos millones de equipos y personas; de acuerdo a las estadísticas, se visualiza que para el 2006 habrá unas 900 millones de cosas conectadas y distancias imprevistas de alcance.

1.1.2 Limitantes y Problemáticas de Internet

Después de este vertiginoso desarrollo, es innegable la importancia que Internet tiene hoy en día en todos los aspectos de nuestras vidas; el desarrollo de las tareas profesionales, académicas, de investigación o simplemente tareas cotidianas se hacen imposibles de pensar sin el uso de las tecnologías de comunicación que utilizan la Internet como herramienta de enlace a nivel mundial. Sin embargo, el uso del Internet por diferentes sectores principalmente el sector comercial ha empujado fuertemente a algunas saturaciones del servicio y limitantes en su desarrollo y calidades de respuesta. Sus grandes ventajas que ayudaron su crecimiento y evolución también han marcado limitantes en algunos aspectos de su desarrollo, sobretodo el tecnológico y el principio tan abierto de sus tecnologías, que por un lado le da flexibilidad y homogeneidad a su implantación y uso, por otro, ha marcado lentitud de innovaciones y delimitaciones en su utilización, sobretodo para algunas aplicaciones que demandan respuestas aseguradas, de buena calidad y con exigencias muy por encima de las aportadas por el Internet actual. El sector educativo y de investigación es el ambiente que principalmente se vio afectado por esto.

Las aplicaciones académicas y de investigación tienen características particulares de comportamiento y requerimientos de red diferentes al de otros sectores como es la seguridad de la conexión y los retardos en la respuesta de las aplicaciones si es un factor importante. La calidad de la transmisión también es un factor crítico para algunas aplicaciones.

Debido a que Internet es una red pública, basada en el mejor esfuerzo de servicio pero no garantizado, abierta y masiva que no permite la particularidad tecnológica para cada una y diferentes tipos de aplicaciones, se convierte en una red que no cumple las expectativas para muchas de las aplicaciones de la academia e investigación.

De la misma forma, a nivel regulatorio, administrativo, de seguridad y operativo queda extremadamente coartada ya que Internet esta conformada por diferentes grupos sectoriales que funcionan por acuerdos y cooperaciones limitadas por jurisdicciones comerciales y legales estrictas y muchas veces por restricciones económicas, características que repartidas entre diferentes sectores de usuarios, deja poco espacio para la alta demanda de las aplicaciones científicas.

El aspecto de seguridad y de reservas de derechos sin un control real en Internet también es un factor crítico para la abertura de uso de algunas aplicaciones con

derechos que reservar o resultados que garantizar y cuidar, de esta forma podemos concluir que Internet es grande y útil, con grandes potenciales de usos comerciales pero limitada para las aplicaciones de alta demanda científica o académica.

Entonces retomamos la famosa frase y la reubicamos ante un paradigma: Internet para todos pero para las aplicaciones de alta demanda, venga una nueva Internet de mayores capacidades.

1.2 EL DESARROLLO DE LA NUEVA GENERACIÓN DE INTERNET

El uso de Internet como herramienta educativa y de investigación científica ha crecido aceleradamente debido a la ventaja que representa el poder acceder a grandes bases de datos, la capacidad de compartir información entre colegas y facilitar la coordinación de grupos de trabajo.

Debido a la gran importancia que ha tenido Internet en las actividades, docente y de investigación, han surgido nuevas necesidades y aplicaciones que están demandado mayor rapidez en la transmisión de la información, calidades de servicio, soporte de voz y video sobre IP, consultas a bases de datos muy grandes y educación a distancia entre otras y previendo la importancia de las necesidades futuras para correr aplicaciones cada vez mas complejas bajo Internet, estamos observando que la red actual esta siendo ya sobrepasada a las necesidades actuales de nuestros usuarios.

Bajo este panorama, en E.U., la comunidad académica no paró de impulsar iniciativas de mejoras para el Internet y proyectos colaborativos apuntados a su evolución como el proyecto de NGI (Next Generation Internet) conducido por el gobierno federal.

No solo Internet estaba evolucionando, de la misma forma, las aplicaciones crecían en funciones, alcances, demandas y características tecnológicas. Surgían camas de prueba y aplicaciones que involucraban voz, video y almacenamiento masivo sobre las redes paquetizadas.

En paralelo a esta y otras iniciativa comunes de desarrollo de redes de alto desempeño, en 1996, la gestión del presidente William Clinton creó el proyecto de

implantar una red de alta velocidad y grandes capacidades que enlazara universidades y laboratorios con el objeto de impulsar el desarrollo de las nuevas aplicaciones y la investigación, bajo velocidades 1000 veces mas rápidas que el Internet. En este proyecto participaron la NASA, la NSF y los Departamentos de Defensa y Energía, el costo de este proyecto se calculó en 1998 fue de 100 millones de dólares y promovió el desarrollo de las nuevas tecnologías de redes.

Por su parte y en este mismo año, un conjunto de universidades se reunieron en Chicago para discutir y visionar una red que satisficiera las necesidades de sus propias aplicaciones científicas y crearon el proyecto de Internet2, que conjuntaba infraestructura de alta velocidad, tecnologías de vanguardia, laboratorios de prueba para crear nuevas herramientas tecnológicas, pero sobretudo, el desarrollo de aplicaciones que marquen la evolución en el aprendizaje, enseñanza e investigación de las universidades.

1.3 LA NUEVA RED: INTERNET 2

Con este impulso de la NGI, el sector académico es uno de los principales demandantes de respuestas y se presenta una reunión entre algunas universidades de Estados Unidos que buscan encontrar soluciones de comunicación de sus aplicaciones científicas, tanto las actuales como la fuerte evolución a corto tiempo de ellas.

Así, este grupo conformado de 34 universidades se comprometen con el objetivo de formar una nueva infraestructura de alto desempeño y se asocian conformando la University Corporation for Advanced Internet Development (UCAID) que inicia el proyecto no lucrativo denominado genéricamente Internet2. Rápidamente se unen a este proyecto grandes consorcios privados y gubernamentales, todos ellos tratando de construir la Internet del futuro siguiendo la estrategia de implantar un backbone de nacional de altas capacidades llamado Red Abilene.

Por supuesto que la iniciativa de Internet2 esta avalada además por el gran beneficio económico de retorno y las visiones financieras para el mercado privado y militar. Se tiene una gran red de desarrollo donde probar y avalar las nuevas tecnologías para después ser exportada al resto de las redes incluyendo la Internet comercial.

La Misión de Internet 2:

- Proporcionar un marco tecnológico para el desarrollo y uso de aplicaciones de vanguardia que apoyen la misión educativa y de investigación.
- Implantar infraestructura de redes avanzadas de alta capacidad, control y calidad que cubran las necesidades de estas nuevas aplicaciones.

Los alcances:

- Investigar, probar, instalar y explotar una red avanzada que brinde un desempeño y funciones que no tiene el Internet actual.
- Su desarrollo abrirá las puertas a aplicaciones que usen transferencia masiva de datos, video en tiempo real, investigación y colaboración remota, etc.

Estas metas anteriores son llevadas a cabo y se han visto posibles siguiendo esfuerzos en base de grupos de trabajo conformados para lograr metas específicas y complementarias:

- El grupo de ingeniería que esta en proceso de construir conexiones de gran ancho de banda entre las instituciones educativas y de investigación participantes en el proyecto.
- El grupo de aplicaciones, él cual esta desarrollando aplicaciones específicas que utilicen y aprovechen en su totalidad las capacidades de una red de gran ancho de banda.
- El grupo de Middleware que se encarga del software entre la red y las aplicaciones, arquitecturas que acoplen el funcionamiento robusto entre ellos y que hoy en día tienen que ser proporcionados de forma aislada e independiente.

Cada área tiene un coordinador responsable y a su vez consta de subgrupos de trabajo que llevan a cabo tareas más específicas de su especialidad.

Ahora, el gran acierto de Internet2 ha sido usar las mismas fortalezas y ventajas de la Internet -gracias que ha sido impulsado por los mismos participantes- ,sistemas abiertos, TCP/IP como protocolo de comunicación, complementándolas con características específicas, particulares y refuerzos como conexiones garantizadas punto a punto, seguridad, calidades de servicio, tecnologías emergentes, etc. con la

gran ventaja de contar con un gran marco de pruebas tecnológicas, teniendo un gran laboratorio internacional dispuesto a estas pruebas.

Es tal el resultado de esta iniciativa que el proyecto es retomado por otros países y se replican los esfuerzos por crear redes similares, conformando diferentes iniciativas y consorcios para implantar estas redes de altas capacidades y creando convenios de colaboración entre corporaciones.

En una de las últimas reuniones entre las corporaciones nacionales de redes académicas avanzadas se determinaron por regiones (por país) estas redes y se han identificado como Redes Nacionales Avanzadas de Investigación denominan las NRENs (National Research E Networks) buscando la organización técnica, administrativa y normativa en el desarrollo y colaboración de estas redes.

Conocimos el término de Internet2 como nombre genérico pero recientemente se registró oficialmente este nombre al proyecto que representa la red de Abilene, pero podemos seguir usando la nomenclatura Internet 2 (con espacio) como término genérico y NRENs para ubicar e identificar cada uno de los esfuerzos regionales a nivel mundial: NREN de México, NREN de Chile, NREN de Brasil, etc.

1.3.1 Internet 2 en Estados Unidos

Como ya hemos introducido, en Estados Unidos surgen fuertes iniciativas en Internet 2 diversificado en diferentes proyectos regionales pero hay principalmente 2 fuertes iniciativas nacionales: la red Abilene y la red vBNS, que si bien siguen visiones similares y conformadas por tecnologías de punta, sus misiones e integrantes son complementarios ambas reforzadas con proyectos de interconexión nacional e internacional que remarcan proyectos colaborativos.

Una visión estratégica de los proyectos de las redes académicas avanzadas radica en el estudio detallado de los diseños de conexión y se delinea la importancia de las estructuras jerárquicas de la red enfatizando esquemas operativos analíticos física y lógicamente de la red. Este cuidado radica principalmente en el control que se quiere tener del tráfico y el desempeño de las aplicaciones.

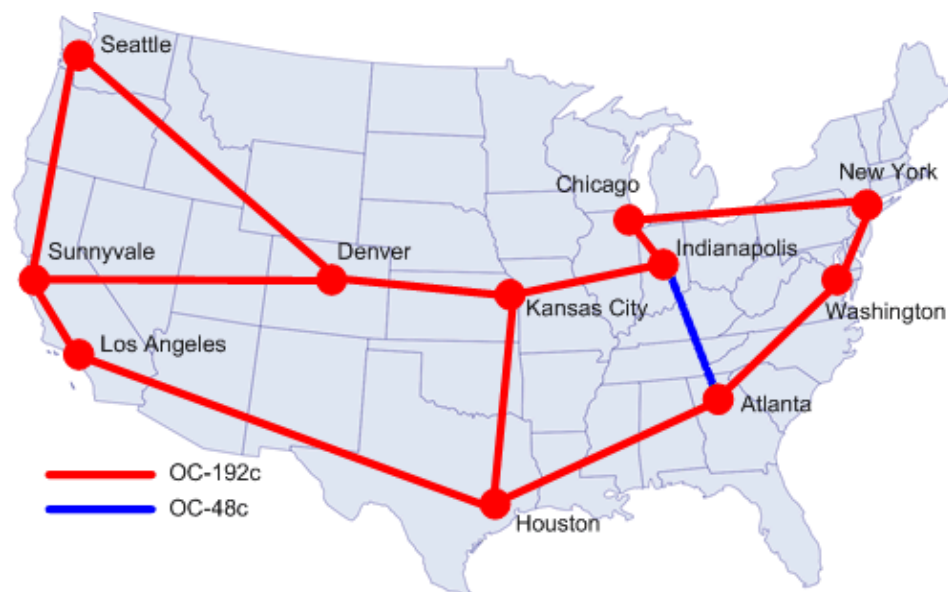
Es importante describir la estructura de la red Abilene porque ha sido un marco de referencia para otras redes incluyendo la red CUDI, materia de esta tesis y servirá para comprender su estructura.

a) ABILENE

Hoy en día en el proyecto de UCAID participan mas de 200 universidades, entidades privadas y gubernamentales y la dorsal nacional de la red Abilene está constituida por mas de 13,000 millas de enlaces de alta velocidad sobre tecnología de 10 Gigabit Ethernet enlazando nodos de acceso en los 50 estados y Puerto Rico.

Backbone

Esta red es patrocinada por Qwest Communications para los enlaces, Nortel Networks para equipo de transmisión SONET, Juniper en equipo de ruteo, Cisco Systems en la parte de equipos switches, ruteadores y equipos de acceso y la Universidad de Indiana en el Centro de Operación de la red. Esta infraestructura permite sostener aplicaciones avanzadas como grids de supercómputo y teragrids, laboratorios virtuales, acervos digitales, telemedicina, televisión de alta definición, etc.



Backbone Red Abilene. Obtenida de www.internet2.edu

La red sigue una estructura jerárquica de acuerdo a:

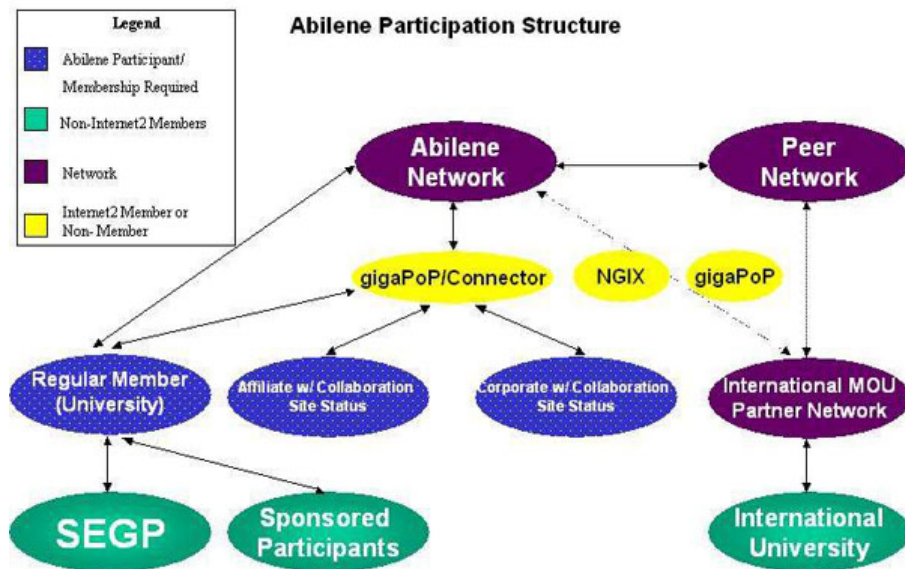


Figura obtenidas de www.internet2.edu

Los nodos de integración regionales de Abilene son principalmente Centros de Investigación o Instituciones Académicas conectadas directamente a la dorsal de la red, estos nodos se denominan **Gigapops** y cuentan con equipamiento robusto que permite recibir los diferentes redes que conjunta la conexión de los asociados a la dorsal a través de diferentes tipos de acceso.

Puntos de Intercambio

Los nodos de intercambio son aquellos donde se entrelazan diferentes redes nacionales e internacionales compartiendo información de rutas de tráfico para proporcionar el acceso a cada uno de sus abonados. La tarea de estos puntos de intercambio es muy importante porque es donde se extenderán las colaboraciones a nivel mundial de esta red.

Abilene International Network Peers

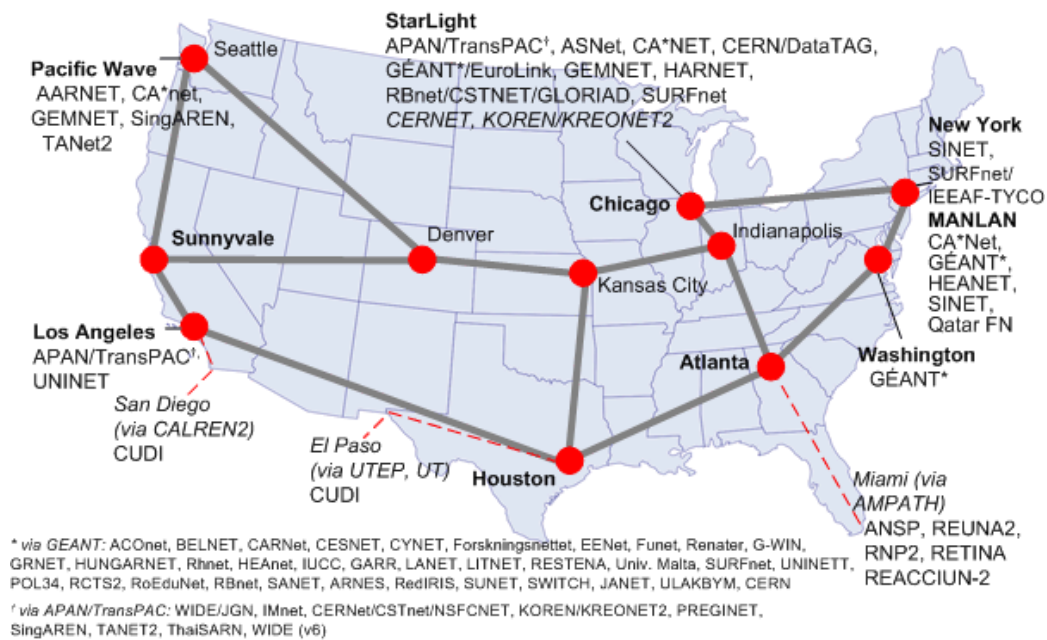


Figura obtenida de www.internet2.edu

A través de estos puntos se comunican otros proyectos de otras regiones del mundo a la red Abilene, mas adelante identificaremos específicamente la interconexión a la red de CUDI.

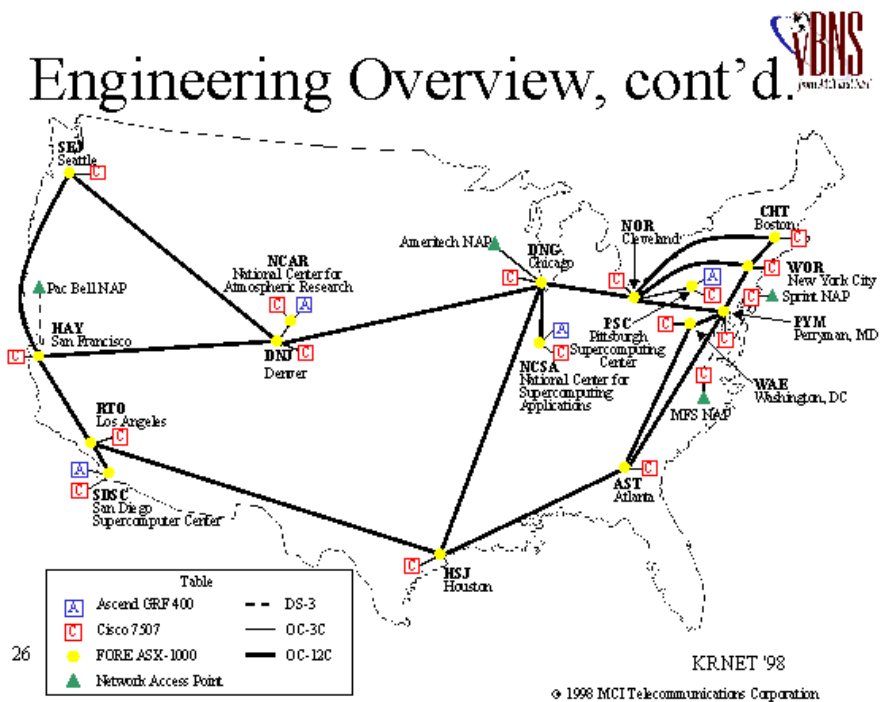
Operación

El compromiso de operación de esta red esta bajo responsabilidad de la Universidad de Indiana quien patrocina el Centro de Operación (NOC-Abilene) con un soporte de 7x24. Sus actividades reflejan las responsabilidades de mantener esta infraestructura en adecuado funcionamiento e intercambiar esfuerzos de operación con otros centros de operación de las otras redes avanzadas como CUDI.

b) *vBNS*

La “very High Performance Backbone Network Service” (*vBNS*) es una red transnacional originada en 1995 como una red dorsal de muy alto desempeño bajo el trabajo cooperativo entre MCI Worldcom y la NSF (National Science Foundation), cambiando su nombre por *vBNS+* en abril del 2000 como una extensión del convenio entre MCI y NSF para ofrecer servicios comerciales. *vBNS+* emplea una topología Backbone dual, utilizando paquetes sobre SONET (POS) y dorsales ATM. Todas las troncales son OC-12 ó mayores. A finales de este año se espera que todas las troncales sean OC-48.

Figura obtenida de www.internet2.edu

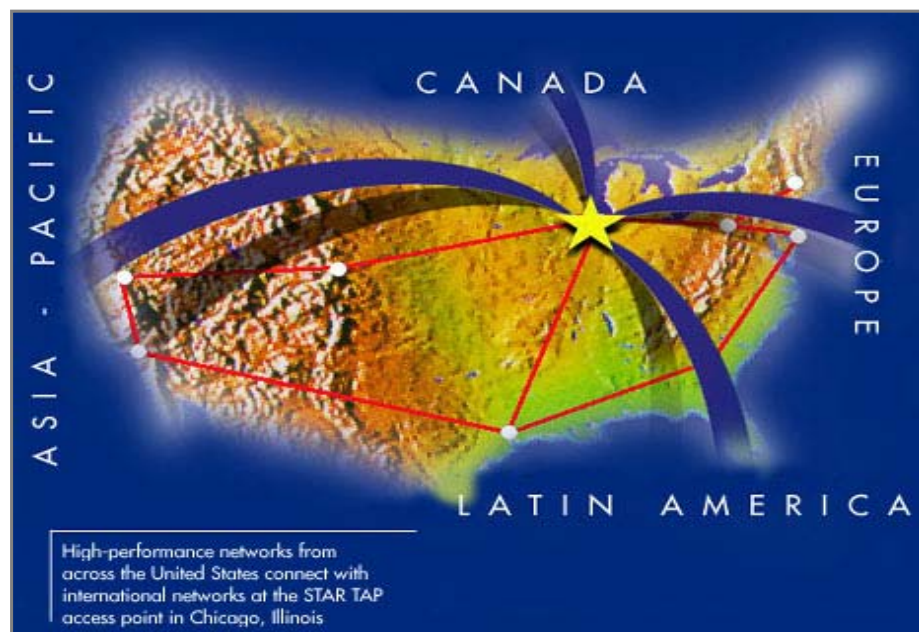


c) *STARTAP/STAR LIGTH*

El crecimiento de la colaboración científica alrededor del mundo trae consigo la necesidad de una infraestructura global para la comunicación de datos.

STARTAP (Science, Technology And Research Transit Access Point) es la infraestructura creada por la NSF para facilitar la interconexión e interoperabilidad de redes y aplicaciones avanzadas internacionales. STARTAP apunta al programa abreviado como HPIIS (High-Performance Research & Education Networking).

La arquitectura original STARTAP con una sola conexión en Chicago ha ido evolucionando hacia un modelo distribuido, el cual soporta múltiples puntos de conexión distribuidos.



STAR TAP en Chicago. Figura obtenida de www.internet2.edu

A la par, a partir de 2001, se ha ido desarrollando el proyecto STARLIGTH que se visualizó bajo la instalación de una red de interconexión de muy alta capacidad con

infraestructura óptica de 1 a 10 Gb y sus requisitos de interconexiones de redes exigen sean también a través de enlaces de muy alta velocidad.

En abril del 2004 se concluye el proyecto de STARTAP y se impulsa continuar estos objetivos a través de STARLIGHT.

1.3.2 Iniciativas Internet 2 en el mundo

Estas iniciativas se han extendido rápidamente teniendo presencia en prácticamente todas las regiones, a continuación una tabla general de identificación de estas redes avanzadas listadas por región, aunque nos centraremos en el proyecto en México y sus interconexiones:

Américas – Norteamérica	
<ul style="list-style-type: none"> ▪ Abilene (USA) ▪ CANet4 (Canadá) ▪ DREN (USA) ▪ ESNnet (USA) ▪ FASTnet ▪ NISN (USA) ▪ NREN (USA) ▪ Red-CUDI (México) ▪ vBNS (USA) 	<ul style="list-style-type: none"> ▪ SURFnet (Netherlands)
Américas - Sudamérica	Asia y Oceanía
<ul style="list-style-type: none"> ▪ AMPATH ▪ ANSP (Sao Paulo, Brasil) ▪ RETINA (Argentina) ▪ REUNA2 (Chile) ▪ RNP2 (Brasil) 	<ul style="list-style-type: none"> ▪ AARNeT (Australia) ▪ APAN (Japón) ▪ CERNET (China) ▪ GEMnet (Japón) ▪ IMnet (Japón) ▪ KOREN (Corea) ▪ KreoNet2 (Corea) ▪ SINET (Japón) ▪ SingAREN (Singapur) ▪ TANet2 (Taiwan) ▪ TransPAC ▪ UNINET (Tailandia) ▪ WIDE (Japón)
Europe	
<ul style="list-style-type: none"> ▪ DFN (Alemania) ▪ GÉANT (Europa) ▪ HEAnet (Irlanda) ▪ IUCC (Israel) ▪ JANET (Inglaterra) ▪ NORDUnet (Escandinava) ▪ RBnet (Rusia) ▪ RENATER2 (Francia) 	

1.4 DESCRIPTIVO DE LAS APLICACIONES INTERNET 2

Si queremos hablar de las redes de Internet 2 tenemos que entender la importancia de las aplicaciones que correrán sobre estas redes.

Las aplicaciones de Internet 2 se definen como aplicaciones de alta demanda que marcan diferencias en la enseñanza, investigación y aprendizaje de sus aplicaciones. Dado que requieren capacidades y características técnicas específicas de red, estas aplicaciones no operan adecuadamente en la Internet comercial ya que el factor de calidad y capacidad si es importante en su funcionamiento.

Estas aplicaciones siguen el impulso evolutivo de los esfuerzos de las comunicaciones e Internet, respaldadas por el apoyo del gobierno y algunas instituciones privadas, compartiendo esfuerzos por desarrollar y mejorar redes que le den soporte.

Las aplicaciones de Internet 2 difieren en su procesamiento y distribución de la información y se han englobado en áreas de aplicación:

- Tecnología de Redes de Telecomunicaciones
- Educación a Distancia
- Bibliotecas Digitales
- Telemedicina y Salud
- Ciencias de la tierra
- Astronomía
- Supercómputo compartido
- Laboratorios Remotos
- Ciencias de la Vida
- Visualización

Los atributos de estas aplicaciones se perfilan en colaboraciones interactivas, accesos en tiempo real a los recursos, procesamientos distribuidos y realidad virtual, se distinguen por su definitivo uso de tecnologías como multicast, video sobre IP, mayor ancho de banda, calidad de servicio, etc., describiremos mas de estas características técnicas en la siguiente sección.

Actualmente existen más de 2000 proyectos registrados a nivel mundial de aplicaciones de Internet 2 y son coordinados y llevados a cabo a través de grupos de trabajo, grupos de interés y laboratorios:

- Ciencias de la Salud
- Medicina Veterinaria
- Artes y Humanidades
- Desempeño de Arte
- Física Nuclear y Energía
- Aplicaciones Geoespacial
- Ortopedia
- Voz sobre IP
- Video Digital
- Videoconferencia
- Almacenamiento en red
- Telecomunicaciones

Estas aplicaciones tienen mucho en común y, a diferencia del Internet comercial, se requiere una calidad garantizada punto a punto o dicho de otro modo, entre puntos finales de la aplicación.

Pero el objetivo principal de Internet 2 es la colaboración y compartición de esfuerzos entre investigadores y el factor de difusión y acercamiento toma un papel muy importante por lo que se abren espacios y esfuerzos en ello como lo son la definición de comunidades, reuniones informativas y de seguimiento anuales, reuniones

específicas por grupos de trabajo eventuales, videoconferencias, días de conferencias, etc.

Si bien las aplicaciones se definen por sus características particulares de demanda de la red, exigen que sean tratadas de forma puntual y particular, entendiendo su comportamiento y sus necesidades por lo que el conocimiento, manejo y control de la red es crítico. Estas aplicaciones demandan mayor rapidez en la transmisión de la información, calidades de servicio, soportes integrados, controles de retardo, bajas pérdidas, etc.

Para cumplir con el entorno operacional acorde a estas aplicaciones, se han implementado tecnologías emergentes y capacidades técnicas y lógicas de punta, respaldadas por laboratorios de prueba, implementaciones beta para ser acopladas, etc. La operación de la red cambia su enfoque y se vuelve analítico a nivel aplicación.

1.5 NUEVAS CAPACIDADES DE LA RED

Como hemos ido recalado en el transcurso del presente capítulo, el proyecto de Internet 2 busca implantar redes de altas capacidades para cubrir las necesidades específicas y altas demandas de las aplicaciones académicas y de investigación, que buscan soluciones más certeras en el objetivo de la enseñanza-aprendizaje-investigación, buscando mayores alcances y respuestas en su meta de calidad y eficiencia de sus proyectos. Pensando precisamente en estas demandas se diseñan redes nuevas, evolucionadas en capacidad y funcionalidad.

Las bondades técnicas que se disponen en estas redes son:

Mayor ancho de Banda: Una característica clara en las redes de Internet 2 es su infraestructura robusta, enlaces de mayores capacidades que el Internet, sobre los gigabits incluso, proporcionados a las aplicaciones. Estos amplios canales permiten poder reservar o controlar el tráfico con mayor eficiencia.

Multicast: Esta tecnología permite a las redes de Internet 2 optimizar altamente los recursos de la red debido a que permite controlar el envío de información solicitada sin que se duplique, esto es el caso por ejemplo de las aplicaciones de video, transmisiones en vivo, etc., con Multicast se evita enviar los paquetes a cada usuario que lo solicita; se envían los paquetes a todos de forma íntegra y confiable en una sola transmisión.

Calidad de Servicio: Se proporcionan al tráfico de las aplicaciones características que definen su óptimo desempeño, dándoles prioridad a los servicios, reservaciones de ancho de banda, control de los retardos, etc., de forma que se garanticen ampliamente el funcionamiento de las aplicaciones en la red.

Ingeniería de Tráfico: Este es un concepto muy importante en las redes avanzadas ya que permiten dar un trato inteligente a la operación del tráfico dentro de la red, se incluyen conceptos avanzados de control y orientación del ruteo, el beneficio obtenido es muy resaltante ya que los tiempos de respuesta se reducen, el ruteo se eficientiza, los procesos se minimizan, lo que permite una respuesta en la operación de la red más eficaz.

Bajo retardo: Algunas aplicaciones son altamente dependientes del tiempo, lo cual en Internet 2 pueden ser disminuidos los tiempos de respuesta y transmisión para dichas aplicaciones, como control a distancia.

Esto por mencionar algunas características.

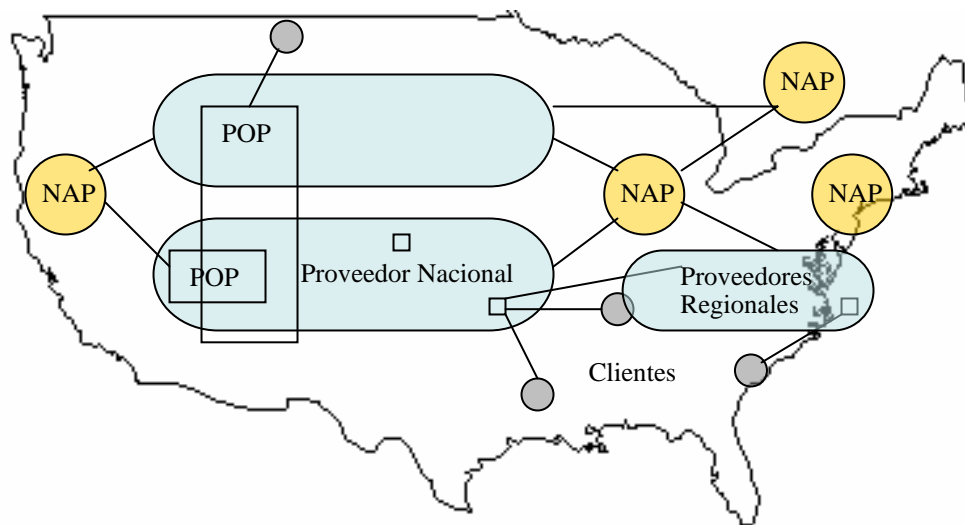
La importancia real no radica en proporcionar estos servicios sino en controlarlos sobre la red y proporcionarlos de forma específica y adecuada a las aplicaciones que correrán sobre ella, así que adentrándonos más ya a la parte operativa podemos ir mencionando la importancia de la operación de la red que proporcionará el control de estas características técnicas y la tecnología necesaria para que la funcionalidad de las aplicaciones sean las esperadas. No es un trabajo sencillo, hay que tener pleno conocimiento de la red, de sus elementos, de la tecnología y sobretodo saberlos aplicar en el día a día de su funcionalidad.

1.6 EL RETO EN LA OPERACIÓN DE INTERNET 2

Pues ya para irnos introduciendo a la parte sustancial de la presente tesis, debemos hablar de la importancia del control y operación de la infraestructura física y lógica de Internet 2.

Si hacemos una sencilla comparación entre la Internet comercial e Internet 2, podemos comentar que ambas redes están basadas en el mismo esfuerzo de comunicaciones, protocolos abiertos y sobre estándares. Internet 2 usa las mismas mejores ventajas que el Internet comercial, pero además se le suman esas nuevas y robustas capacidades de las que ya hablamos, por lo que la operación necesaria de esta varía sustancialmente. No es que el compromiso sea mayor, solo se hace más puntual para el tipo de tráfico de un sector: el académico.

En la infraestructura de la Internet comercial encontramos un esquema parecido al siguiente:



Estructura general del Internet actual. Figura obtenida de www.internet2.edu

Las conexiones a la red son proporcionadas por los ISPs y la operación de la Internet comercial se basa en jerárquicas de cobertura y se le denominan “Tier”, el nivel de mayor cobertura es el 1 y el de menor puede llegar a 4, así:

Tier 1, es el ISP de mayor cobertura, básicamente nacional o internacional basado en redes de alta velocidad que sirven de tránsito al resto de los ISPs.

Tier 2-3, son los ISPs regionales que se conectan a los ISPs Tiers 1, tienen menor infraestructura que estos

Tiers 4 son ISPs locales y con infraestructura limitada, en algunos países no hay este nivel de ISPs.

En este esquema, la operación está orientada por áreas locales proporcionada por los carriers locales que proporcionan el servicio al usuario, en este caso una entidad, este compromiso no se extiende a mas allá de la red del proveedor y si algo funciona mal fuera de su infraestructura ya no es su responsabilidad corregirla y queda a cargo del siguiente proveedor. En algunas ocasiones no es fácil detectar la fuente o punto de falla así que esto se convierte en un posible punto débil de la operación, al quedarse sin un verdadero seguimiento de la falla o en el mejor de los casos solo se ve reflejado en períodos más largos de atención y la solución llega en tiempos no adecuados.

Otro punto crítico y común en la operación de Internet comercial es la generalidad de trato que se le da al tráfico; es decir, todas las aplicaciones que circulan por Internet comercial son tratadas de la misma forma, sin recursos extras, sin calidades particulares, ni siquiera se verifica su seguridad o su conexión asegurada. La tarea operativa en Internet 2 difiere precisamente por la operación dedicada a las aplicaciones.

El reto de la operación en Internet 2 es proporcionar en lo más posible a las aplicaciones su óptima funcionalidad cuidando los resultados esperados, esto conlleva a una característica fundamental que es sensibilizar mucho a las personas encargadas de la operación del comportamiento de las aplicaciones, se enfatiza en su análisis y conocimiento de sus características, no se trata de la misma forma las visualizaciones astronómicas que las bibliotecas digitales por ejemplo, por un lado las primeras requieren mayor precisión y garantía de la conexión, bajo retardo y bajo uso de ancho de banda y la segunda, de alta seguridad, ráfagas de tráfico, etc., cada una de estas particularidades deben ser entendidas, analizadas y proporcionadas de forma específica .

De la misma forma la operación en Internet 2 se exterioriza mundialmente a través de colaboraciones muy cercanas entre centros encargados, así si se presenta algún evento dentro de una red regional, este es visto desde el punto de vista de un segmento de la red mundial y se conjugan esfuerzos entre cada centro implícito en la conexión de la aplicación para analizarlo y resolverlo.

Un esquema plenamente identificador y diferencial de la operación de Internet 2 es que todos y cada una de las experiencias, conocimientos, estudios, laboratorios, etc., manejados y adquiridos son ampliamente difundidos entre todos los participantes de los diferentes proyectos Internet 2 a nivel mundial a través de eventos técnicos periódicos que difunden y comparten conocimientos entre la comunidad de operadores de las redes académicas.

Así, podemos resumir las características diferenciales de operación de Internet 2 de la red comercial remarcando el reto a cubrir por el personal encargado a ello:

- **El control del tráfico en base a las aplicaciones**
- **Trato específico por tipo de aplicación**
- **El cuidado de la operación a nivel punto a punto de la aplicación**
- **La garantía del servicio**
- **El uso de tecnologías emergentes**
- **La integración de servicios**
- **Aplicación de pruebas preliminares de operación sobre la red real**
- **Uso de maquetas internacionales de pruebas**
- **Actualizaciones constantes a versiones recientes e innovadoras de los equipos de red activos**
- **Basada en la cooperación**
- **Externada a otras regiones fuera de la Infraestructura de una sola red**
- **Personal sensibilizado de las aplicaciones**
- **Difusión y compartición de recursos y conocimientos**

Detectamos la importancia de estas tareas, entonces se entiende la importancia que recae en tener un adecuado esquema operativo de la red que es el objetivo de esta tesis, plantear una solución para su instalación y funcionamiento con todos los puntos fundamentales para el sustento robusto de la red, integrando cada uno de sus entornos de responsabilidad que hemos comentado en el Capítulo de Introducción. Con esto se pretenden cumplir los retos de Internet 2.

Capítulo 2

INTERNET 2 EN MÉXICO: CUDI

2.1 DESARROLLO DE INTERNET 2 EN MÉXICO

En nuestro país también surge un fuerte interés de impulsar el proyecto de Internet 2 dado las necesidades reales del sector académico y el panorama tan limitado presente de Internet, así que a partir de mediados de 1998 se inician varias reuniones entre las Universidades mas grandes del país para visualizar y dar forma al proyecto, la idea era instalar una red de alto desempeño con infraestructura de vanguardia que facilitara y fomentara las aplicaciones científicas actuales y emergentes y buscar la colaboración estrecha entre proyectos interinstitucionales. Además también buscaban un ambiente que fomentara el desarrollo tecnológico para las propias universidades, así como dar un marco de formación a la nueva generación de profesionales de tecnologías de la información y técnicos expertos en redes y operación de las mismas.

El reto del proyecto era diversificar los caminos y apoyos para la enseñanza y la investigación, en un país donde solo el 18% de la población en edad universitaria es atendida esto era un verdadero impulso, sobretodo porque los recursos y caminos tradicionales representaban cada vez mas una limitante en vez de apoyo, no se podía crecer en edificios, laboratorios, etc., al mismo nivel de la demanda, asimismo la evolución de la forma de hacer negocios, el desarrollo de la vida cotidiana misma exigían un punto de atención en la preparación de los nuevos profesionistas e invertir en tecnología significaría tangiblemente grandes beneficios para cada uno de estos puntos que redundarían en reducir costos en corto plazo al aumentar la capacidad y calidad de la enseñanza.

Así que, los representantes de estas universidades comenzaron sus acercamientos con proyectos afines en USA iniciando una investigación exhaustiva, recabando información y puntos de colaboración, amarrando intercambios de esfuerzos, con el fin de preparar un proyecto sólido basado en experiencias y análisis que permitiera

preparar un proyecto robusto acoplado a nuestro país. De la misma forma, de manera interna, se buscaron los acercamientos necesarios con los organismos gubernamentales de nuestro país que apoyara su implementación.

Fue un largo año de trabajo y el 8 de abril de 1999 se vieron consolidados estos esfuerzos al constituirse oficialmente el grupo de desarrollo de Internet en México nombrado “Corporación Universitaria para el Desarrollo de Internet” (CUDI), constituida como una corporación privada y no lucrativa y respaldada por las entidades académicas, gubernamentales y privadas, con el fin de desarrollar una red de alta velocidad y unirse a la red internacional Internet2.

Las universidades fundadoras de CUDI fueron: Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE), Instituto Politécnico Nacional (IPN), Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM), Universidad Autónoma Metropolitana (UAM), Universidad de Guadalajara (UDG), Universidad de las Américas (UDLA), Universidad Nacional Autónoma de México (UNAM).

Posterior a este magno logro, el 20 de Mayo de 1999 se firman alianzas y colaboraciones inicialmente con 2 entidades internacionales de Internet 2, UCAID (University Corporation for Advanced Internet Development) y CENIC (Education Network Initiatives in California), posteriormente se firma otro memorándum de entendimiento con CANARIE (Organización Canadiense para el Desarrollo del Internet Avanzado), todos ellos en la línea de llevar el proyecto a una base robusta en la colaboración de aplicaciones científicas.

Esto fue el inicio de todo un gran reto para CUDI. Posterior a la conformación del grupo, se dio inicio al diseño de la red. No fue nada fácil conformar la infraestructura, tecnología y protocolos ha implantar en la dorsal (backbone), sobretodo considerando la interconexión de las redes de cada institución a la dorsal con la visión de la interoperabilidad entre todas ellas: un gran reto definitivamente.

En ese mismo periodo, CUDI logró un avance importante al firmar un convenio con la empresa Telmex para su participación en el proyecto. Con este convenio, Telmex patrocinó la infraestructura de los medios de red: enlaces y equipos

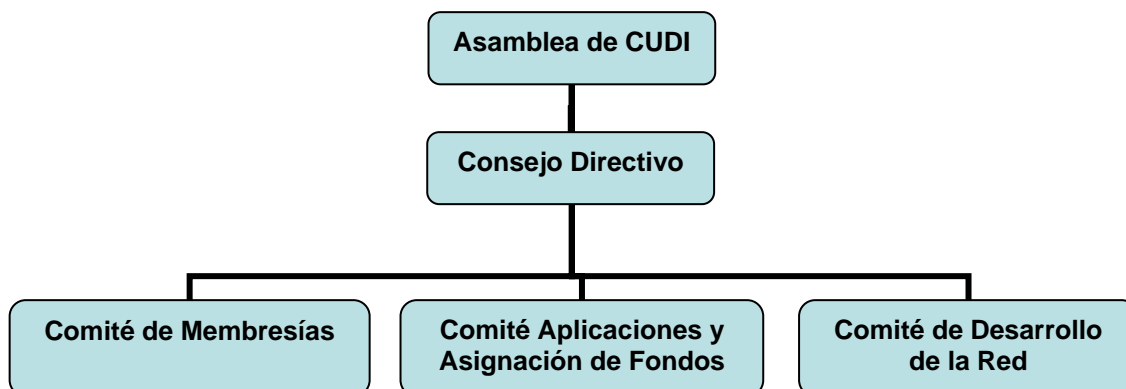
A este convenio se unieron otras compañías interesadas en formar parte del proyecto Internet 2 de México firmando su asociación y patrocinando en especie otros conceptos del proyecto: Nortel Networks, Marconi, Enterasys, VCON, Cisco.

La compañía Avantel se unió posteriormente al patrocinar una parte complementaria de la red, con enlaces y equipos, permitiendo con esto dar una cobertura nacional.

Para la parte de aplicaciones, se logró ubicar las principales e iniciales aplicaciones de CUDI por parte de cada Universidad, buscando crear alianzas y colaboraciones entre colegas nacionales inicialmente y posteriormente con colegas de otros países.

2.2 CUDI

Para cumplir sus tareas, la estructura de CUDI se formó de la siguiente manera:



La integración a CUDI conlleva a las instituciones participantes a requisitos, responsabilidades y derechos, técnicos y administrativos, de acuerdo a niveles de asociación:

Asociaciones académicas:

Son aquellas instituciones académicas o de investigación que aportan una cuota por asociación participando en el pago a prorrata el costo parcial del proyecto. Su conexión a la red es directamente a la dorsal nacional a través de puntos de presencia de esta con requisitos técnicos de enlaces de alta capacidad (mínimamente de 34 Mbps) y responsabilidades de puntos de interconexión o paso para los afiliados académicos. Regularmente son las instituciones con mayor desarrollo en sus redes internas.

Afiliados Académicos:

Son aquellas instituciones académicas o de investigación que aportan una cuota menor a las asociadas. Un afiliado académico solo puede ser conectado a la red a través de un asociado académico, es decir, se conectan a un nodo receptor de enlace Internet 2 del asociado académico y este es responsable de su comunicación a CUDI. Las redes de los afiliados académicos son regularmente de menor tamaño.

Asociados Institucionales

Son aquellas entidades fuera del sector académico, como gubernamentales, privadas, etc., que se integran a CUDI realizando aportaciones económicas y en especie para el proyecto. Su nivel les permite participar activamente en el Consejo Directivo y el resto de los comités.

Afiliados Institucionales

De la misma forma que los asociados institucionales pero en menor medida de aportación, no participan en la toma de decisiones del Consejo Directivo.

La comunidad CUDI la integran actualmente, a través de sus diferentes tipos de asociaciones, más de 70 instituciones, véase Anexo 1 para listado de ellas y todas ellas pueden participar en diferentes medidas en los diferentes Comités de trabajo, donde

en cada uno de ellos se llevan a cabo tareas específicas para el seguimiento y crecimiento del proyecto de acuerdo a:

El Comité de Membresías se encarga de buscar y fomentar nuevas asociaciones en las instituciones del país, manejando mecanismos informativos para su integración, es parte fundamental en el análisis de los prospectos de acuerdo a las aplicaciones y nivel de participación.

El Comité de Aplicaciones y Asignación de Fondos, es el encargado del análisis y difusión de las aplicaciones, impulsando la colaboración interinstitucional y convenios de colaboración e identificando aplicativos potenciales para usar la red y compartirlas.

El Comité de Desarrollo de la Red es el responsable del diseño, instalación desarrollo, crecimiento, operación y prospección de la red.

Se estima que un muy alto porcentaje, arriba de las 2/3 partes de la matrícula escolar están integradas a las Instituciones miembros de CUDI con lo que se da un soporte importante a la cobertura de Internet 2 en México.

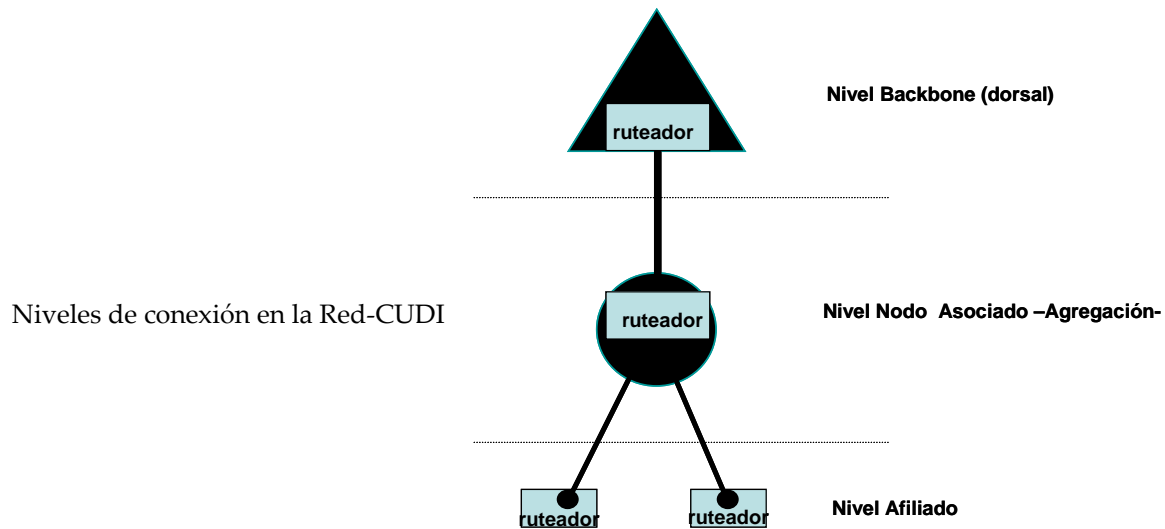
2.3 DESCRIPCIÓN DE LA RED CUDI

El Diseño, implementación, puesta en marcha y operación de la red de CUDI esta a cargo de su Comité de Desarrollo de la Red, quien además se encarga de revisiones tecnológicas que mantengan a la red a la vanguardia, proporcionando continuamente herramientas útiles y actuales para las aplicaciones.

El diseño de la red se llevo varios meses en completarse, desde definir la topología de la red hasta la selección de protocolos a utilizar en sus diferentes niveles de comunicación (de capa 1 a capa6 del modelo OSI). Fue un reto interesante debido a que la dorsal de la red debería acoplarse e interconectarse a las redes internas de cada

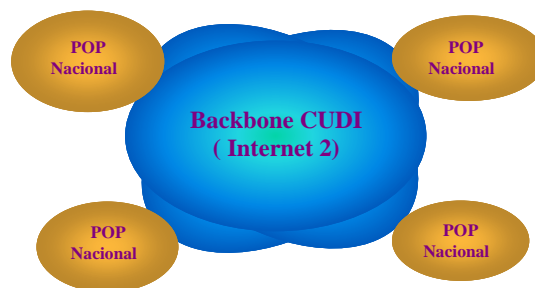
institución asociada intercambiando información transparente y ágilmente, eso implicaba *interoperabilidad* entre todas las redes.

En el diseño se definió un esquema jerárquico de operación de la red:



a) ESQUEMA DE CONEXIÓN

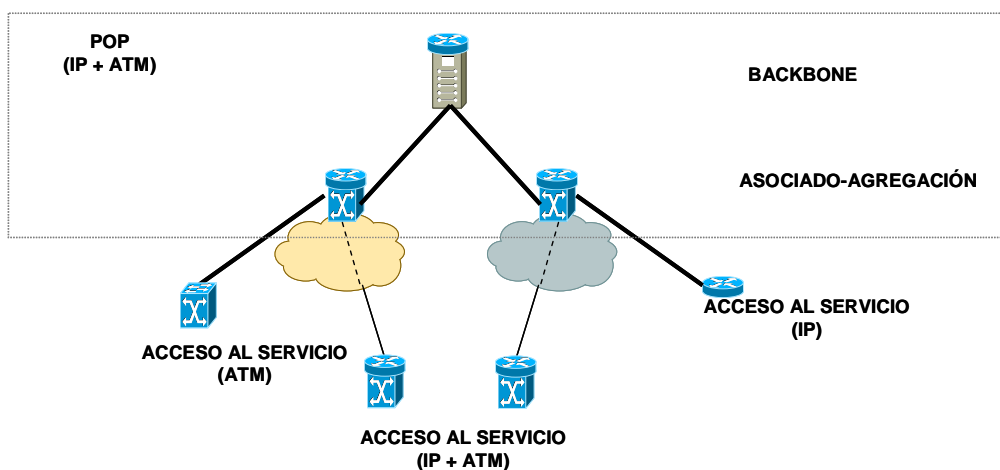
La dorsal o backbone se define como la infraestructura principal, global y de alcance nacional que conecta los nodos o puntos de presencia e interoperabilidad nominados *POPs*, este es un esquema muy común en las redes de Internet 2 y en CUDI se adoptó esta misma estructura:



Esquema de la dorsal de la Red-Internet 2

Las instituciones asociadas a CUDI se conectan directamente a un POP a través de enlaces mínimamente E3 (34 Mbps) e incluso pueden conformar parte de este. Las instituciones afiliadas se conectan a los nodos asociados a través de enlaces mínimos de E1 (2 Mbps). Para estas conexiones se pueden realizar a través de IP, ATM o IP+ATM. El esquema de acceso se puede resumir en la siguiente figura:

Topología de acceso



b) BACKBONE

El backbone consistente de 8000 kms. de fibra óptica, lo conforman 6 POPs aportados por Telmex y Avantel y ubicados actualmente en Tijuana, Cd. Juárez, Monterrey, Guadalajara, Cd. De México y Cancún conectados a través de enlaces STM1 (155 Mbps) trabajando con el protocolo IPv4 e IPv6 sobre una arquitectura tecnológica basada en conmutación de celdas ATM y algunos en POS, utilizando equipos tipo carrier switch-ruteador o ruteador exclusivamente.

Conexiones internacionales:

Se cuenta actualmente con 3 conexiones físicas internacionales:

- **Conexión Tijuana-San Diego (California), enlace de 155 Mbps con ATM interconectando CUDI con la red Abilene a través de la red CENIC,**
- **Conexión Cd. Juárez-UTEP (Texas), enlace de 100 Mbps con ATM interconectando CUDI con Abilene a través de la red de la Universidad de Texas,**
- **Conexión Reynosa-VBNS (Houston), enlace de 155 Mbps con POS, interconectando a CUDI con la red de alta velocidad vBNs.**
- **En el caso de las conexiones con Abilene se tienen configurados túneles de conexiones lógicas hacia la red Abilene.**
- **Próximamente conexión a la Red CLARA, conexión en Tijuana que permitirá tener acceso a más de 700 instituciones de la región de Latinoamérica y Europa**

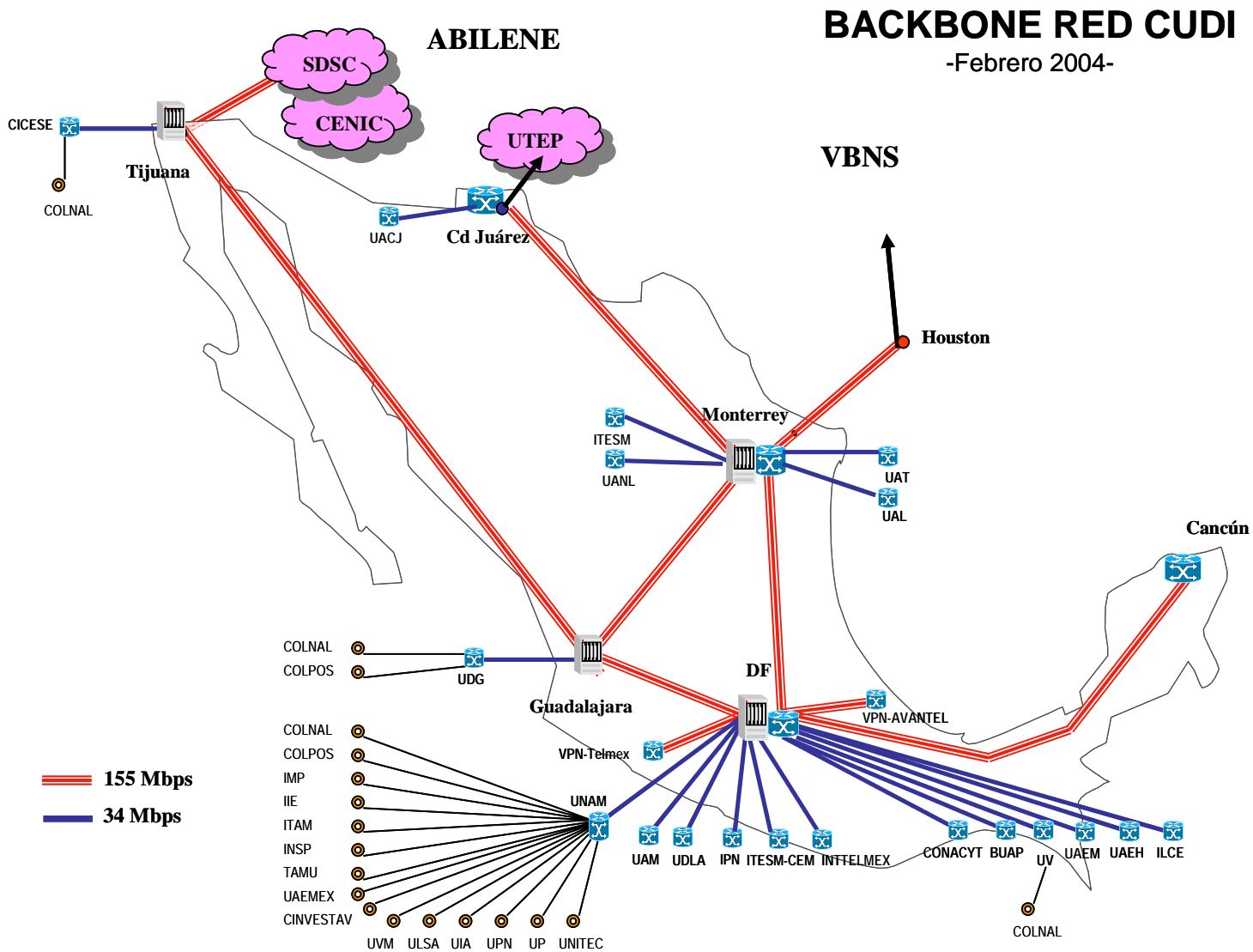
c) OPERACIÓN

La responsabilidad de la operación global de la red recae en CUDI a través del Comité de Desarrollo de la Red. Los carriers apoyan a CUDI exclusivamente en la operación física de los medios y equipos aportados y ubicados físicamente en sus instalaciones y por solicitud expresa de CUDI, pero ambas entidades trabajan muy de cerca.

Se ha consolidado una red que mantiene en su dorsal: Multicast, IPv6, H323, VoIP, enrutamiento inteligente y seguridad.

Para la realización y cumplimiento de las tareas y objetivos técnicos de la red de CUDI, se han conjuntado actividades específicas en grupos de trabajo:

- Grupo de Enrutamiento
- Grupo de Topología
- Grupo de Operación
- Grupo de H.323
- Grupo de VoIP
- Grupo de QoS
- Grupo de IPv6
- Grupo de Seguridad
- Grupo de Middleware
- Grupo de HDTV
- Grupo de operación de videoconferencia
- Grupo de Multicast
- Grupo de End-to-End
- Grupo de MPLS



2.4 APLICACIONES

Una infraestructura de red tan robusta es pensada para dar precisamente soporte a las aplicaciones académicas avanzadas existentes e impulsar el desarrollo de proyectos. La red deberá refrendar la colaboración entre académicos e investigadores que se verán beneficiados con una red de vanguardia para sus trabajos.

El Comité de Aplicaciones de CUDI es justamente el grupo encargado del seguimiento de esta meta, identificando y fomentando las aplicaciones avanzadas dentro del proyecto, determinando responsabilidades y alcances de cada una de ellas y por supuesto promoviendo fondos de apoyo para su puesta en marcha.

Para cumplir con estos objetivos, en CUDI se han identificado las aplicaciones y definido en grupos temáticos:

- Bibliotecas Digitales
- Astronomía
- Ciencias de la Tierra
- Telemedicina y Salud
- Cómputo Distribuido y Compartido
- Tecnología de Redes
- Educación a Distancia
- Laboratorios y colaboratorios remotos
- Artes

En la comunidad internacional de Internet 2 existen más de 2500 proyectos de aplicaciones registradas¹

¹ Puede referirse para su consulta a www.nlanr.net

Estas aplicaciones tienen diferentes demandas de la red y difieren en su comportamiento dentro de ella, por lo que a nivel operación deben ser tratadas de forma específica a sus demandas y desempeños, ese es el valor de las redes de Internet 2 y lo que marca la diferencia con la red Internet convencional.

Para tener una referencia de las aplicaciones registradas en CUDI puede revisar el Anexo 2 de esta tesis.²

En este tipo de aplicaciones se manejan diversos tipos de tráfico y características de procesos en su funcionamiento, pueden utilizar una sola aplicación tecnológica o conjuntar en su desempeño varios aplicativos; por ejemplo, hablando de las aplicaciones de Educación a Distancia se presenta el uso de la videoconferencia como tecnología nativa, combinada en algún nivel con acervos digitales, procesamiento distribuido o control a distancia, lo que define una aplicativo robusto y de trato puntual en lo que a red se refiere; el caso de Telemedicina es aún mas amplio en cuanto a aplicativos inmersos.

Definiendo por ejemplo algunos campos aplicativos tenemos a las **Bibliotecas Digitales**, donde nos referimos a materiales multimedia de todos los aspectos y niveles que se encuentran almacenados en formato digital, estructurados para accesos a través de la red utilizando herramientas de navegación sencillas. Los contenidos se mantienen en línea a través de diferentes recursos y ambientes para compartir la información. Las Bibliotecas Digitales son definidas como una aplicación nativa de Internet 2 pero también es una aplicación inmersa y utilizada como soporte para otras aplicaciones dentro de este proyecto.

Otro campo es la **Telemedicina** que se encarga de la aplicación de los campos de la distancia, principalmente la medicina clínica y asistencial donde existen varios campos en desarrollo como la telerehabilitación, la imagenología, segunda opinión, etc.

Educación a Distancia, donde se entiende la instrucción distribuida en ambientes diferentes y distantes, utilizando la red como herramienta de alcances y distribución de diversos mecanismos utilizados en una sesión de capacitación.

² También puede consultar en www.cudi.edu.mx

Capítulo 3

DESARROLLO DE LA PROPUESTA PARA EL CENTRO DE CONTROL Y OPERACIÓN DE LA RED INTERNET 2 DE MÉXICO "NOC-CUDI"

3.1 OBJETIVO DEL CENTRO DE OPERACIÓN

Las redes de comunicaciones globales están cada día expandiéndose y actualizándose, sus tecnologías, coberturas y complejidades de interoperabilidad se ven cada vez más agresivas en sus alcances y posibilidades; los retos de su control crecen con ellas en paralelo a la demanda de mantener su operación eficiente y constante. Este reto empuja a buscar e implementar sistemas de operación adecuados que sirvan de apoyo a los encargados de su funcionamiento para mantener en línea la comunicación de las instituciones.

Los sistemas de operación apuntan a proporcionar al personal de una red a tener la posibilidad de monitorear y manipular los elementos o parámetros de una red con la finalidad de:

- Incremento de la confiabilidad del estado y respuesta de un elemento de la red
- Incremento de eficiencia en corrección de errores
- Incremento de seguridad
- Incremento en la optimización de recursos
- Incremento de conocimiento de la red
- Apoyo de las estrategias en el desarrollo del proyecto
- Decremento en los costos
- Aumento en la calidad del servicio

Todos estos puntos son esenciales a considerar en el desarrollo del proyecto de la red Internet 2 mexicana. El diseñador, administrador, y el técnico deben estar en perfecta sincronía para conformar una red bajo control, permitiendo la toma de decisiones de

acuerdo a su tiempo de respuesta: operacionales, que son las decisiones inmediatas durante la misma operación diaria, las decisiones tácticas, es decir a corto plazo y las decisiones estratégicas que son la toma de decisiones a largo plazo encausadas hacia la visión futura del proyecto de comunicaciones.

También es importante diferenciar entre la operación de una red LAN y una red WAN, la diferencia entre ambas es el tipo de conexiones, medios de transmisión y equipamiento por lo que su control y operación también debe ser de acuerdo a esto.

3.1.1 Análisis y expectativas

Un punto crítico e importante para el planteamiento del Centro de Operación de la Red CUDI es primero darse cuenta del panorama funcional que las redes de Internet 2 persiguen, la forma en que operan y los lineamientos que respetan; ya hemos mencionado que no es el mismo nivel de esfuerzos, tecnologías y recursos que demandan que la red Internet convencional. Para la funcionalidad de una aplicación en Internet 2, hay una calidad punta a punta exigida y perseguida a través de todo el camino de conexión recorrido y donde para cumplir este propósito participan todas las entidades académicas necesarias que de ello dependa. En cada parte del camino se inyecta a la red de las tecnologías necesarias para mantener su nivel esperado de operación. Es una cooperación de operaciones locales. Los recursos mismos son un punto restrictivo en el compromiso de mantener una red, se requieren grandes cantidades de tecnologías, equipos, personas, tiempo, etc., para un adecuado control de la red Internet 2, muchas veces de esfuerzos ilimitados de ellos de acuerdo al nivel de demanda y calidad exigida, la cual casi siempre ha resultado sacrificada en Internet por este motivo. Internet 2 también puede verse como el gran impulsor de la colaboración misma de operación y de recursos. Queda muy por encima de la descripción de un área física porque se plantea más virtual y cooperativo.

En este trabajo se plantea una visión más ilimitada de operación, un esquema de administración y operación que deba ser más abierto y que permita la distribución de esfuerzos, la colaboración de recursos dispersos y la aportación de experiencias entre las diferentes entidades que conforman este magno proyecto.

Bajo esta premisa y justo para dar cumplimiento a los objetivos planteados, dentro del proyecto Internet 2 se han creado múltiples grupos técnicos a nivel mundial dedicados

al estudio y desarrollo de las tecnologías de punta y su aplicación dentro de la red, grupos dedicados especialmente en cuidar el comportamiento de la infraestructura física y lógica compaginada con las aplicaciones.

En CUDI se sigue el mismo impulso, se crean estos grupos de trabajo técnicos, que ya hemos descrito en el capítulo anterior, dedicados a, inicialmente a analizar las tecnologías mas adecuadas a implantar en la red, a cuidar el uso de los medios físicos y lógicos y sobretodo a intercambiar experiencias y estudios que permitan optimizar los recursos e integrar de la mejor forma posible las infraestructuras que hagan en un todo una red altamente robusta y suficientemente lista para su conexión al proyecto global mundial.

Entre todos estos grupos técnicos de CUDI se intenta dar un soporte y operación completa a la red mexicana.

Así pues plantearemos el esquema lógico y virtual como se debe trabajar el centro de control y operación de la red de CUDI bajo la óptica anterior pero vislumbrando los puntos clave de operación.

3.1.2 Necesidades

Los tiempos en que se requería una gran área física con instalaciones especiales para el funcionamiento de un centro de operación han pasado a la historia. Con la evolución de los sistemas de cómputo, de las redes y de la tecnología, los requerimientos de un centro de operaciones se han minimizado en cuanto a espacios y necesitan de menos especificaciones técnicas especiales en su instalación, realmente se demanda más sistemas, equipo de cómputo de propósito específico, procedimientos bien diseñados y recursos humanos con niveles de conocimientos dependiente del nivel y tipo de la red a operar. La operación se vuelve más a distancia, con menos requerimientos especiales pero más específicos.

En el caso de este trabajo, se considera el diseño del centro de operación en base al tipo de red, las características del proyecto de Internet 2, de las entidades de quienes lo conforman, de los equipos que lo conforman y la operación de cada uno de ellos.

De acuerdo a lo anterior, se define cada uno de los puntos de operación para una red tipo WAN con especificaciones basadas en capa 3 a 6 del modelo OSI orientado a un

diseño de operación virtual, más cooperativa, distribuida y abierta, donde se deben cubrir las necesidades y características existentes y esenciales en la operación de la Red CUDI.

Inicialmente debemos considerar que la red CUDI esta conformada por cada red académica nacional, cada una con sus propios mecanismos e infraestructuras, con la autonomía de operación mas variada y diversa que podemos imaginar. Al llegar a cada “puerta” de estas redes se cede el control a los operadores de propios de cada universidad, por tal razón, la operación de la dorsal de la red deberá ser transparente e integral dado la gran variedad de topologías, protocolos, aplicaciones y normatividades de estas redes internas. En forma general se identifican las siguientes necesidades a cubrir:

En el aspecto físico:

- o Control de la dorsal de la red de CUDI, cuidando su adecuado funcionamiento y evitando en lo mas mínimo sus tiempos muertos o de fuera de servicio
- o La disponibilidad efectiva de los medios de transmisión
- o El comportamiento óptimo de los equipos
- o La calidad punta a punta de los equipos de dorsal garantizada
- o El diseño del comportamiento que deberá cumplir la red y sus aplicaciones
- o La interoperabilidad física de los elementos

En el aspecto lógico:

- o El uso adecuado de los recursos
 - o La aplicación de tecnologías de vanguardia
 - o La participación activa de todas las entidades
 - o El balanceo de funciones
 - o La interoperabilidad lógica de la red y de las funciones
- o En el aspecto administrativo:
- o La acotación de funciones

- o La definición de fronteras operativas y de responsabilidad
- o La definición de interacciones y cooperaciones
- o Descripción de procesos y procedimientos
- o Información y Difusión

3.2 DESARROLLO DE LA PROPUESTA

Para la operación de redes y en base a la experiencia obtenida en el ramo de operación es muy importante demarcar los niveles de actuación en una red para obtener los mejores resultados en su control.

En este trabajo se propone la identificación de cuatro niveles a converger:

- a) Los dispositivos que generan información
- b) Los equipos o instrumentos de medición o análisis de datos
- c) Las herramientas de predicción
- d) Las tecnologías de apoyo para eficientar la operación

En el primer caso, **los dispositivos que generan información**, se trata de los equipos como ruteadores, switches, módems, radios, enlaces, etc.; **los equipos de medición** nos hablan de monitores, software de monitoreo, bases de datos, sistemas de información y herramientas de administración; mientras que las **herramientas de predicción** se define en técnicas estadísticas y simulación, teoría de colas, entre otras.

Para el panorama planteado de operación y control completo y eficiente de la red Internet 2 de México se determina el uso necesario de **tecnologías de vanguardia** que apoyen en el cumplimiento los alcances expuestos y que no son cubiertas por las herramientas propias de operación.

Se le denominan tecnologías de vanguardia porque son protocolos relativamente jóvenes que hasta la fecha están en constante desarrollo, perfilándose y adecuándose a satisfacer el comportamiento de las aplicaciones actuales sobre la red, especialmente

dedicadas a definir un comportamiento específico del tráfico haciendo controlables las altas demandas. Son tecnologías que responden a los nuevos medios físicos y demandas actuales de las nuevas aplicaciones.

Cada tecnología es aplicada en diferente momento y en diferente nivel de la operación de la red, a lo largo o dentro de alguno de los siete niveles del modelo OSI, en el punto justo de aprovechamiento.

Describiremos algunas de las tecnologías de vanguardia previstas a utilizar sin considerar su ubicación o nivel de integración, esto lo iremos describiendo a lo largo del Capítulo 4 siguiente.

3.2.1 La red a operar

En el Capítulo 2 se describió a detalle el diseño de la red CUDI pero la analizaremos en este inciso en forma general.

Como hemos descrito anteriormente, la red CUDI esta integrada físicamente por los dos *carriers* más grandes de México: Avantel y Telmex, por lo que además lograr la interoperabilidad entre medios, equipos, protocolos y tecnologías de la dorsal nacional, es también necesario integrar a nivel lógico y procesal ambas infraestructuras, siendo quizá esto lo mas complejo de lograr.

Los Nodos de Presencia (*POP*) se encuentran distribuidos a lo largo y ancho de toda la república, que al proporcionarlos diferentes carriers, mantienen esquemas tecnológicos diferentes y tipos de acceso particulares.

Otro aspecto a considerar son los nodos a conectar a la dorsal o nodos de acceso, que conectan y pertenecen a las instituciones académicas. Estos nodos también son de diferentes marcas, modelos, tecnologías, etc., y que suman las redes académicas nacionales a la dorsal de la red CUDI. Cada red académica difiere en diseño, topología, operación, procesos, administración, etc., a las otras.

El panorama a considerar entonces, es una integración de ambientes diversos y operar una red multifuncional y *multi-todo*. En el capítulo siguiente se describe a detalle los elementos de la dorsal de la red.

3.2.2 Estrategias y tecnologías a utilizar

Una de las iniciativas del proyecto CUDI es que la operación de la red mantuviera el mismo espíritu de academia, propositivo y de colaboración que el resto del proyecto. Se lanzó una convocatoria abierta para el concurso de propuestas del esquema de operación de la red CUDI. El capítulo siguiente, describe en su totalidad la propuesta definida por la UNAM para participar en el concurso de definición y ubicación del Centro de Operación de la Red Internet 2 de México, desde la definición de los objetivos y alcances, hasta los procedimientos a implementar.

El tópico de gestión de redes es un concepto anterior a los 90's, sin embargo es relativamente joven lo relacionado con redes de datos de área amplia, basadas en tecnología SDH, con características abiertas de operación y en constante crecimiento y actualización. Cualquiera de estos modelos existentes no se encuentra completamente desarrollado, no existe en sí ningún patrón o sistema de gestión estándar aún que se pueda tomar e implementar como un saco a medida por lo que cada propuesta de operación de una red, es desarrollada e implementada de acuerdo a cada necesidad, haciendo uso de los conocimientos de gestión de redes, manipulando protocolos y estándares de operación hasta conformar un ambiente favorable a una adecuada manipulación de los elementos de la red a administrar.

La perspectiva a seguir en la propuesta se apoyó en diferentes esquemas recomendados de gestión de redes tipo, tal cual basado en SNMP (Simple Network Management Protocol), en el modelo "TMN" (Telecommunication Management Network) que plantea soluciones de administración de la red que satisfagan los estándares de la ITU-T basada en una arquitectura de capas administrativas y de control de la red y el esquema aportado por el CMIP (OSI).

Tomando este marco de visión, la propuesta desarrollada mantiene el compromiso de presentar un sistema de operación **aplicable** para una red **real, en crecimiento y para gestionar distintos tipos de redes.**

Para el desarrollo de la propuesta se consideran conceptos globales a tomar y conjuntar en la propuesta:

-Modelo de operación

-Funciones de operación

- Protocolos estándares
- Interconexión de redes
- Sistemas e interfases de operación

Se considera que el alcance de los compromisos de la operación de la red de CUDI debe ser compartido por quienes participan activamente en este proyecto:

- Usuarios
- Operadores locales de red
- Proveedores de servicio
- Fabricantes de equipamiento

Sin embargo un punto importante a subrayar es que la propuesta aquí presentada es respetuosa de la topología actual de conexión, las tecnologías que emplea y de los sistemas de operación propios de cada Universidad participante de CUDI, sacando el mejor partido a esto mismo. De este hecho se basan las tecnologías analizadas y su empleo en la operación.

- Implementación del Protocolo de Internet versión 6 (IPv6)

IPv6 surge como una respuesta a la preocupación del agotamiento de las direcciones de la actual versión 4 del Protocolo de Internet 4 (Internet Protocol -IPv4-) y como un desafío a cubrir sus debilidades proporcionando en el nuevo protocolo funcionalidades adicionales para los dispositivos actuales y emergentes. Este protocolo inicia su desarrollo en el Grupo de trabajo de ingeniería de Internet (IETF, Internet Engineering Task Force).

IPv6 cubre problemas de diseño de IPv4 aunque es importante mencionar que IPv4 ha logrado superar estas debilidades a través de herramientas adicionales en cuanto la madurez de IPv6 se da.

Los conceptos que fundamentalmente cubre IPv6 para las nuevas redes y necesidades del Siglo XXI y en adelante en materia de comunicaciones son:

- a) Contar con un espacio de direcciones prácticamente inagotable (cuenta con mayor capacidad que estrellas conocidas). Las direcciones en Ipv6 son de 128 bits (16 bytes) obteniéndose con esto $3,4 \times 10^{38}$ posibilidades y adicionalmente con el manejo de subniveles.
- b) Nuevo formato de encabezado que permite que la carga de trabajo basada en el encabezado sea mínima.
- c) El tener suficiente capacidad de direcciones nos evita utilizar herramientas adicionales como traductores de direcciones (NAT, Network Address Translator) para asignar múltiples direcciones privadas a una sola dirección IP pública y poder salir a Internet 2.
- d) Robustece la seguridad basada en estándares desde la capa de red con servicios de cifrado incluidos que protejan la información desde su origen, durante su tránsito y hasta su destino. En IPv4 la seguridad es optativa y puede apoyarse en el protocolo IPSec (Internet Protocol Security) por ejemplo. En IPv6 ya es inmersa en el propio protocolo.
- e) Con el nuevo formato del encabezado de IPv6 se ayuda a optimizar el manejo de las tablas de ruteo en los ruteadores de dorsal. En IPv4 el anuncio de ruteo es plano y jerárquico y con el nuevo formato de encabezado de IPv6 se hace más eficiente y ágil.
- f) Configuraciones más sencillas basadas en procesos automáticos que apoyen la administración de un cada vez mayor número de equipos en red. Con IPv4 se realizan manual o a través del protocolo de configuración de direcciones con estado como el DHCP (Dynamic Host Configuration Protocol).
- g) Parte del paquete de IPv6 ya considera dentro de este la calidad del servicio (Quality of Service –QoS-) facilitando la entrega de datos en tiempo real y con garantía de servicio. Esto basado en el nuevo encabezado de IPv6 donde incluyen campos como el campo de “etiqueta de flujo” (flow label) donde se identifica y controla el tráfico y donde los enrutadores identifican y proporcionan un trato especial al paquete que pertenece a cierto flujo.
- h) Protocolo de “Interacción con Vecinos” (Neighbor Discovery) integrada que permite descubrir a los vecinos del equipo a través de mensajes tipo ICMPv6 (Internet Control Message Protocol for IPv6) identificando a los nodos que se encuentran en el mismo vínculo.

i) Capacidad de extender las características agregando encabezados de extensión.

o Descripción del encabezado IPv6.

Los campos del encabezado son los siguientes:

Version (Versión): se utilizan 4 bits para indicar la versión de IP, que se establece en el valor 6.

Traffic Class (Clase de tráfico): indica la clase o la prioridad del paquete IPv6. El tamaño de este campo es de 8 bits. El campo Traffic Class proporciona una funcionalidad similar a la del campo Type of Service (Tipo de servicio) de IPv4.

Flow Label (Etiqueta de flujo): indica que este paquete pertenece a una secuencia específica de paquetes entre un origen y un destino, lo que requiere un control especial por parte de los enrutadores IPv6 intermedios. El tamaño de este campo es de 20 bits. El campo Flow Label se utiliza para conexiones de calidad de servicio que no son predeterminadas, como las que se necesitan para los datos en tiempo real (voz y vídeo). Para el control del enrutador predeterminado, el campo Flow Label se establece en el valor 0.

Payload Length (Longitud de carga): Campo de 16 bits que indica la longitud de la carga IP. En este campo se incluye los encabezados de extensión y la unidad PDU de nivel superior.

Next Header (Encabezado siguiente): Campo de 8 bits que indica el primer encabezado de extensión (si existe) o el protocolo de la unidad PDU de nivel superior (como TCP, UDP o ICMPv6).

Hop Limit (Límite de saltos): Campo de 8 bits que indica el número máximo de vínculos por los que puede viajar el paquete IPv6 antes de que se descarte. Este campo es similar al TTL en IPv4.

Source Address (Dirección de origen): Campo de 128 bits que almacena la dirección IPv6 del host de origen.

Destination Address (Dirección de destino): Campo de 128 bits que almacena la dirección IPv6 del host de destino actual.

o Descripción del Direccionamiento IPv6.

El esquema de direccionamiento de IPv6 se define en el RFC 2373 y su tamaño es de 128 bits; cuatro veces mayor que el de una dirección de IPv4.

El direccionamiento de IPv4 de 32 bits (4 octetos) conforman 4.294.967.296 direcciones mientras que en IPv6 con 128 bits (16 bytes) se tiene un espacio de direcciones disponibles de 340.282.266.920.938.463.463.374.607.431.768.211.465 (o $3,4 \times 10^{38}$) direcciones con lo que se cuenta aproximadamente con 655.570.793.348.866.943.898.599 ($6,5 \times 10^{23}$) direcciones por metro cuadrado de la superficie terrestre.

Para IPv6, la dirección de 128 bits se divide en límites de 16 bits y cada bloque de 16 bits se convierte en un número hexadecimal de 4 dígitos y se separa con signos de dos puntos (:). La representación resultante se denomina hexadecimal con dos puntos.

Ejemplo de dirección IPv6:

```
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
```

Para simplificar, se ha convenido la omisión de los ceros a la izquierda de cada bloque de 16 bits con lo que se tendría para el mismo ejemplo anterior la dirección siguiente:

```
21DA:D3:0:2F3B:2AA:FF:FE28:9C5A
```

La única consideración es que cada bloque tenga un dígito como mínimo. Sin embargo algunos bloques pueden ser secuencias de ceros por lo que se pueden representar estos como “:”

Ejemplo:

La dirección:

```
FE80:0:0:0:2AA:FF:FE9A:4CA2
```

Se puede comprimir en:

```
FE80::2AA:FF:FE9A:4CA2.
```

La compresión de ceros sólo se puede utilizar una vez en una dirección dada. De lo contrario, no se podría determinar el número de bits 0 representados por cada instancia de “::”.

La particularidad del direccionamiento IPv6 es que se pueda subdividir en dominios de enrutamiento jerárquico que definan la topología de la red desde la local hasta la Internet 2, incluyendo la conocida Internet. Esta división se realiza según el valor de los bits de orden superior.

Los bits de orden superior y su valor fijo se conocen como prefijo de formato (FP, Format Prefix). El prefijo es la parte de la dirección que indica los bits con valores fijos o los bits del identificador de red. Los prefijos para IPv6 se expresan con la notación dirección/longitud de prefijo.

Por ejemplo:

FE80::2AA:FF:FE9A:4CA2/64

Indica que los primeros 64 bits de la dirección corresponden al prefijo de red.

La notación de prefijo también se utiliza para expresar los identificadores de red o de subred.

Por ejemplo:

21DA:D3::/48 es una subred.

En IPv6 no se utiliza la máscara de subred, sólo se admite la notación de longitud de prefijo.

Hay tres tipos de direcciones IPv6:

- a). Unidifusión. Identifica una sola interfaz, los paquetes se entregan a una sola interfaz. El RFC 2373 permite que varias interfases tengan la misma dirección pero deben aparecer como una sola interfaz.
- b) Multidifusión. Identifica varias interfases, los paquetes se entregan a todas las interfases identificadas en esta dirección.
- c) Cualquier difusión. Identifica a varias interfases, los paquetes dirigidos a una dirección se entregan a la interfaz mas próxima que se identifica de acuerdo a enrutamiento.

Un punto a recordar es que en IPv6 las direcciones identifican internos NO NODOS.

Se debe considerar que para que trabajen en conjunto IPv4 e IPv6 en los ruteadores, estos deben tener implementado ambos protocolos simultáneamente.

3.2.3 Modelo de operación

Jerárquico

Inicialmente identificaremos a la dorsal a la red de CUDI en un sistema basado en jerarquías de operación de acuerdo a TCP/IP. Desde el punto de vista operacional existen tres categorías de sistemas en una red de datos IP, el primer nivel son los sistemas o nodos finales (computadoras, hosts, etc.), estos dispositivos generan o reciben datos de la aplicación; otro nivel son los sistemas intermedios (ruteadores, switches, etc.), los cuales direccionan y pasan los datos del nivel de red y los dispositivos de transmisión son aquellos que transportan los datos entre el medio físico y el nivel de enlace. Todos estos sistemas cuentan con una o más interfaz de datos y utilizan varios tipos de tecnologías de transmisión y protocolos de comunicación.

En una siguiente categorización identificamos los sistemas como locales y externos. Los sistemas locales son aquellos en los cuales tenemos control total de su operación y los externos aquellos dependen de otra entidad y tenemos nulo o control parcial de su operación.

La red CUDI es una red tipo “enterprise” o corporativa por lo que la operación deberá dividirse en dominios de acción o responsabilidades de operación. El segmentar las responsabilidades de operación permite manejar independientemente los detalles de operación de un dominio local al de la WAN y controlar mejor las actividades y resultados de esto, aun cuando la red se vea como una sola entidad. De esta manera mantendremos una jerarquización. La definición inicial es granular la red conforme queremos enfocar la operación; esto dependerá del tipo de equipos en que consiste la dorsal de CUDI ya que estos definirán la capacidad de exportar información al operador. Un esquema de niveles de estos es el siguiente:



Tratándose de la red de CUDI, los equipos se enfocan a los tres últimos niveles.

Arquitectura de Gestión

- Basado en ISO

Para el esquema de operación se debe definir los componentes y su estructura de interacción, esto conllevará a su implementación. Existen diferentes tipos de arquitecturas de operación tanto propietarios como abiertos. Basaremos nuestra propuesta en precepto del modelo ISO de dividir la operación de la red dentro de áreas funcionales, donde la operación esta contribuida desde la capa 1 a la 6 del modelo OSI.

El modelo ISO particiona la administración de redes en cinco áreas funcionales:

Administración de Configuración

Es el proceso de iniciar la red, definiendo configuraciones iniciales y cambios o modificaciones de estas configuraciones en respuesta a los cambios de la red. Es una de las tareas más importantes ya que de esta depende el buen comportamiento de cada elemento y de la red en general.

Administración de Fallas.

Se refiere a detectar, aislar y reparar una falla dentro de algún elemento de la red. El apropiado manejo de una falla puede ayudar a resolver los problemas de la red y prevenir algunos más.

Administración de Desempeños.

Se establecen las métricas de desempeño de la red, desde los tiempos de respuesta punto a punto de cada elemento de la red y la utilización de la misma. La utilización de la red es la fracción usada de un elemento de la red para transmitir la información y el tiempo de respuesta es la cantidad de tiempo que se toma un paquete de datos en ir desde un equipo de la red a otro.

Administración de Seguridad

Se refiere a definir los niveles y tipos de seguridad a tu red y a cada elemento de esta, dependiendo de su actividad y de su tipo de operación dentro de la red.

Administración de Contabilidad

Se registran y controlan los recursos de la red, desde los accesos y tiempos hasta prioridades en la operación del tráfico, con esta actividad se puede optimizar y garantizar en gran medida la operación efectiva de las aplicaciones críticas de la red.

Adicionalmente de estos, para nuestra propuesta analizaremos los siguientes componentes:

Interfase unificada de usuario: Integración entre el operador y el sistema, un punto unificado de observación para todos los elementos de la red, usando símbolos genéricos e identificados con textos relacionados al objeto asociado, con capacidad de examinar cada uno de estos objetos de forma detallada y con capacidad de multitarea

Manejo integral de elementos de la red: control de todos los elementos de la red sea cual sea su fabricante, tipo o modelo, en un solo esquema de operación de tal forma que esto y la presentación de servicios conforme un esquema integral de toda la propuesta de operación de la red de CUDI.

Presentación de servicios: debe permitir la organización, visualización y almacenaje de la información de una manera ordena y asimismo que se tenga la capacidad de recuperar la información de una forma ágil y precisa a lo que requerimos. Este punto es vital tratándose de una red compleja como la red de CUDI.

Operación: en general describe como se crean, borran, modifican y relacionan los objetos dentro del repositorio de información; se tienen reglas diseñadas para esta interrelación y como afectar la operación de otro objeto dentro de sistemas abiertos.

Base de datos: un punto crítico es definir el conjunto de objetos que identificarán los elementos de la red y su interrelación. Este aspecto es sumamente importante debido a que un buen manejo de los objetos significará información oportuna y confiable. Dentro del repositorio de objetos, cada uno de ellos debe ser único dentro de la red que describen. Estos pueden ser objetos reales, los cuales definen el elemento de un fabricante específico u objetos genéricos, los cuales pueden describir de forma general varios elementos.

-Sistema de análisis y reporte: permite realizar pruebas a los objetos administrados para saber la calidad de los servicios y diagnosticar fallas, consecuentemente se debe establecer una base de registros de eventos y resultados para que la información sea reportada indicando tipos de error, causas probables, severidad de la afectación, etc. El método del reporte o de plasmar esta información dependerá del gusto del operador o del tipo de la información a plasmar pudiendo tratarse de un reporte gráfico y visual o impreso en diferentes modelos.

- TMN (Telecommunication Management Network)

Algunas de los lineamientos que marca el modelo TMN son:

Administración remota de los componentes de un sistema, así como del hardware y software involucrado en la transmisión de voz, video y datos.

Proporcionar una interfaz sencilla y de fácil iteración por parte de los clientes para la solicitud de servicios.

Proporcionar una automatización en la resolución de problemas concernientes a los recursos involucrados y sus usuarios.

Lograr la integración de la administración y nuevo equipamiento con la infraestructura actualmente instalada y en operación con un bajo costo.

La arquitectura funcional de TMN define cinco clases de bloques funcionales. No necesariamente todos los bloques están o deben estar presentes en cada configuración de un esquema basado en TMN, en algunos casos se pueden incluso repetir bloques.

Para delimitar los bloques funcionales se definen los puntos de referencia TMN. Los tipos de bloques funcionales son:

NEF: Network Element Functions, funciones de elementos de red. Corresponden a las funciones llevadas a cabo por dichos elementos.

OSF: Operations System Functions, que se encargan de iniciar las operaciones de gestión y recibir las notificaciones.

WSF: Work Station Functions, que se encargan de mostrar la información de gestión al operador humano, y por tanto no se consideran parte del modelo propiamente dicho.

QAF: Q Adaptor Functions, conjunto de funciones que se encargan de conectar a TMN a aquellas entidades que no soporten los puntos de referencia estándar definidos por TMN.

MF: Mediation Functions, que se encargan de filtrar, almacenar, y adaptar informaciones de gestión entre NEF y OSF o entre QAF y OSF.

La arquitectura física se encuentra en un nivel más bajo de abstracción que la arquitectura funcional, y muestra cómo los bloques funcionales se asocian con bloques de construcción (equipos físicos) y los puntos de referencia con interfaces.

- Bloques de construcción
- Interfaces

Parte de generar una jerarquía de responsabilidades de gestión que puede ser descrita en términos de capas de gestión. Las capas de gestión en el modelo TMN son:

- Elementos de red

- Gestión de elementos de red
- Gestión de red
- Gestión de servicios
- Gestión de negocio

Sistemas de operación

Los sistemas de operación se basan en hardware, software y uso de protocolos de facto para la recolección, evaluación, manipulación, control, registro y almacenaje de los datos de operación de los elementos de la red. Utilizan ambientes gráficos para su utilización.

Existe una amplia gama de sistemas de gestión en el mercado; ninguna estándar, algunos son propietarios como los ofrecidos por fabricantes de equipamiento y algunos de facto, que utilizan los protocolos abiertos y estándar. Los hay desde sistemas básicos u orientados a una línea de producto; hasta los orientados a redes multifabricante y multiproveedor.

No existen sistemas de gestión que cumplan todas las expectativas operacionales de todas las redes. Debemos considerar que lo más importante es seleccionar un sistema de gestión que cubra en su totalidad las expectativas globales para la red que tenemos y un amplio rango de opciones específicas y particulares de las necesidades a operar; pero el sistema deberá ser suficientemente abierto para complementarlo con otras herramientas.

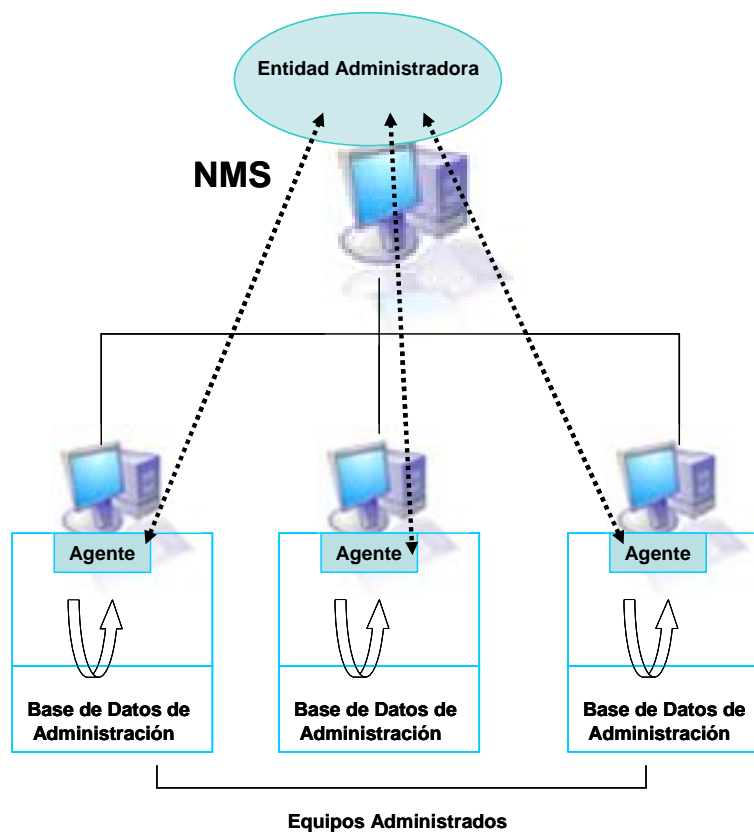
Los más usados son los basados en SNMP y CMIP

- SNMP(Simple Network Management Protocol)

Es un sistema de facto, desarrollado por la Comunidad de Internet para la gestión de redes que implementan la suite de TCP/IP, como las LANs Ethernet, Internet, etc. Se encuentra en actualización de su versión 2 y 3.

SNMP es un conjunto de estándares de protocolos que definen el intercambio de información entre el elemento de red a operar y las entidades del software de

administración. Estas entidades que radican en la máquina administradora son: el gestor (NMS), los agentes y la base de información de gestión (MIB).



El RFC 1157 define el SNMP usado entre las estaciones gestoras y los agentes, este protocolo facilita el poleo para verificar el estado de los equipos y otras características de su comportamiento en la red de acuerdo al objeto solicitado y es a través de este que se reciben los avisos de algún evento ocurrido en alguno de los equipos conectados en la red. La expectativa de SNMP es que sea un protocolo sencillo en su operación y manejo con la finalidad de que no genere tráfico pesado en la red y trabaja por lo tanto sobre el nivel UDP/IP. SNMP trabaja enviando paquetes para básicamente 5 operaciones:

SET – le da atributos a un dispositivo de la red

GET- solicita los atributos de un dispositivo

GETNEXT- proporciona una secuencia de atributos del dispositivo

SET O GET RESPONSE - para dar respuesta a las peticiones de *SET*, *GET* o *GETNEXT*

TRAP – para enviar información de cambio de estado del dispositivo

Actualmente existe la versión SNMPv1, SNMPv2 y se está desarrollando SNMPv3.

CMIP es el protocolo de información de administración común y es un protocolo de administración de redes creado según el modelo de comunicación de interconexión de sistemas abiertos (OSI). Es uno de los elementos de apoyo de las aplicaciones tipo TMN. Está diseñado de una forma más completa como un verdadero sistema de gestión orientado a objetos y ofrece una plataforma de software completa para integrar productos y tecnologías diferentes a través de interfases comunes utilizando de marco el dominio OSI. Esto nos permitirá hacer converger la operación de los diferentes tipos de fabricantes en la red CUDI aprovechando la gestión abierta de CMIP, así como hacer convivir diferentes herramientas de administración de la red que podamos utilizar.

- MIB (Management Information Base)

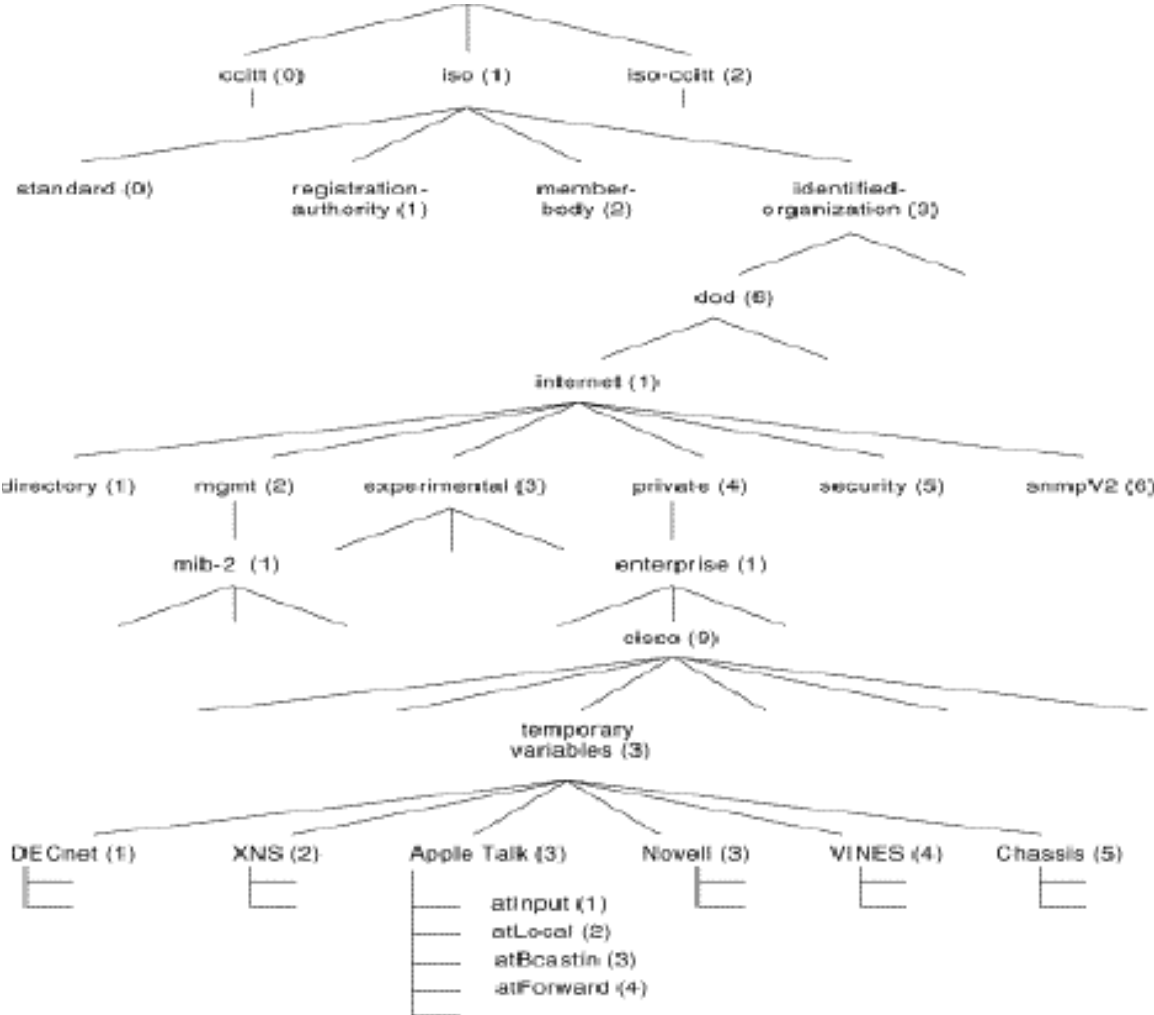
La MIB es la base de datos de información que define los aspectos funcionales y operacionales de un dispositivo en red. Específicamente la MIB es la base de información para gestión de redes y es a través de su funcionalidad que SNMP o CMIP la utilizan para identificar a los dispositivos que deben manejarse, asociando cada uno de estos a información particular, esta información asociada se denomina objeto. Por ejemplo una MIB puede contener la información de la cantidad de paquetes ATM que un equipo ha transmitido por su interfaz. Estos objetos son definidos con un lenguaje especial llamado Notación de Sintaxis Abstracta Uno (ANSI, Abstract Syntax Notation One).

Un MIB define (a) a los dispositivos que se administran, (b) la forma en que el usuario accede a ellos y (c) la forma en que se pueden informar.

Los sistemas de gestión operan sobre el conjunto de la MIB completa por lo que si las MIB no son implementadas adecuadamente la operación de SNMP o CMIP se complica sobremedida.

Hay una diversidad existente de objetos MIB, algunos específicos a ciertas marcas y definidos por los propios fabricantes del equipo y otros son mas abiertos y generales, los cuales son mucho más manejables desde cualquier manejador de gestión. Este es el caso de el conjunto MIB-2, RMON y RMON2.

El RFC 1213 define el grupo de MIB-2 para SNMP que es orientada a las redes de alta velocidad. El árbol MIB es el siguiente:



Enseguida algunos ejemplos de objetos de cada grupo. Se puede consultar el RFC 1213 para la lista completa:

- Grupo de sistema
 - sysDescr - Descripción completa del sistema(version, HW, OS)
 - sysObjectID - Identificación que da el distribuidor al objeto
 - sysUpTime - Tiempo desde la última reinicialización
 - sysContact - Nombre de la persona que hace de contacto
 - sysServices - Servicios que ofrece el dispositivo
- Grupo de interfaces
 - ifIndex - Número de interfaz
 - ifDescr - Descripción de la interfaz
 - ifType - Tipo de la interfaz
 - ifMtu - Tamaño máximo del datagrama IP
 - ifAdminisStatus - Status de la interfaz
 - ifLastChange - Tiempo que lleva la interfaz en el estado actual
 - ifInErrors - Número de paquetes recibidos que contenían errores
 - ifOutDiscards - Número de paquetes enviados y desechados
- Grupo de traducción de direcciones
 - atTable - Tabla de traducción de direcciones
 - atEntry - Cada entrada que contiene una correspondencia de dirección de red a dirección física
 - atPhysAddress - La dirección física dependiente del medio
 - atNetAddress - La dirección de red correspondiente a la dirección física
- Grupo IP
 - ipForwarding - Indicación de si la entidad es una pasarela IP
 - ipInHdrErrors - Número de datagramas de entrada desechados debido a errores en sus cabeceras IP
 - ipInAddrErrors - Número de datagramas de entrada desechados debido a errores en sus direcciones IP
 - ipInUnknownProtos - Número de datagramas de entrada desechados debido a protocolos desconocidos o no soportados
 - ipReasmOKs - Número de datagramas IP reensamblados con éxito
 - ipRouteMask - Máscara de subred para el encaminamiento
- Grupo ICMP
 - icmpInMsgs - Número de mensajes ICMP recibidos

- icmpInDestUnreachs - Número de mensajes ICMP "destino inalcanzable"(destination unreachable) recibidos
- icmpInTimeExcds - Número de mensajes ICMP "time exceeded"(tiempo excedido) recibidos
- icmpInSrcQuenchs - Número de mensajes ICMP "source quench(desbordamiento del emisor) recibidos
- icmpOutErrors - Número de mensajes ICMP no enviados debido a problemas en ICMP
- Grupo TCP
 - tcpRtoAlgorithm - Algoritmo que determina el timeout para retransmitir octetos para los que no se ha recibido reconocimiento
 - tcpMaxConn - Límite en el número de conexiones TCP que puede soportar la entidad
 - tcpActiveOpens - Número de veces que las conexiones TCP han efectuado una transición directa del estado SYN-SENT al estado CLOSED
 - tcpInSegs - Número de segmentos recibidos, incluyendo aquellos con error
 - tcpConnRemAddress - La dirección IP remota para esta conexión TCP
 - tcpInErrs - Número de segmentos desechados debido a errores de formato
 - tcpOutRsts - Número de resets generados
- Grupo UDP
 - udpInDatagrams - Número de datagramas UDP entregados a usuarios UDP
 - udpNoPorts - Número de datagramas UDP recibidos para los que no existía aplicación en el puerto de destino
 - udpInErrors - Número de datagramas UDP recibidos que no se pudieron entregar por razones otras que la ausencia de la aplicación en el puerto de destino
 - udpOutDatagrams - Número de datagramas UDP enviados por la entidad
- Grupo EGP
 - egpInMsgs - Número de mensajes EGP recibidos sin error
 - egpInErrors - Número de mensajes EGP con error
 - egpOutMsgs - Número de mensajes EGP generados localmente
 - egpNeighAddr - La dirección IP del vecino de esta entrada EGP

La dorsal de CUDI esta conformada por dos tipos de tecnologías de transmisión cada una de ellas proporcionada a través de sus dos proveedores, a través de Telmex es tecnología ATM (Asynchronous Transfer Mode) y a través de Avantel es tecnología POS (Packet Over Sonet) por lo que la operación debe ser orientada a este tipo de tecnologías de transmisión. Mas adelante se describe lo propio a la dorsal por cada fabricante y a continuación analizaremos a nivel de tecnología las implicaciones propias a la operación.

- Administración de ATM. Asynchronous Transfer Mode.

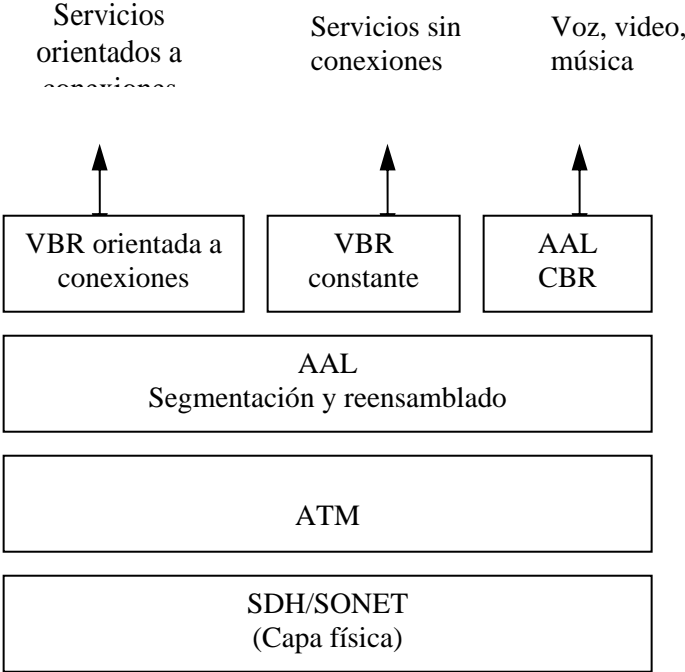
Provee un medio de comunicación de alta velocidad y bajo retardo (de hecho ese es su propósito), que transporta simultáneamente diferentes tipos de datos, tales como texto, video, voz a través de unidades pequeñas de longitud fija de 53 octetos, denominadas “celdas”; pero no es un medio compartido como ethernet por lo que el desempeño no se degrada con el incremento de usuarios como en ethernet porque es un medio orientado a conexión y se garantiza la conexión a través de un conjunto de parámetros de negociación.

Cada celda se identifica con identificadores de circuito virtual y de trayecto virtual contenidos en el encabezado y una red ATM utiliza estos identificadores para enrutar el tráfico entre los switches de alta velocidad de la dorsal de la red. Sus principales medios de transmisión se basan en velocidades de 25, 155 y 622 Mbps; en el caso de la red de CUDI, esta trabaja en 155 Mbps.

ATM utiliza los conceptos de circuitos virtuales permanentes (PVCs) y Switcheados (SVCs) para definir los caminos de comunicación entre equipos. Los circuitos permanentes son configurados manualmente por el administrador de la red y son estáticos. Los circuitos switcheados son dinámicos de acuerdo a las necesidades del tráfico y son configurados de forma dinámica de acuerdo a un protocolo inteligente de señalización y de demanda de calidad de servicio requerido por el usuario. Hay limitaciones respecto al proveedor en la capacidad de PVCs o SVCs que soportan los equipos.

Las capas de operación de ATM son similares a otras tecnologías y ofrece capacidad de convergencia en su capa de adaptación para aplicaciones de tasa de bits variable orientadas a conexión y sin conexiones apoyando por ejemplo a aplicaciones como voz y video.

Capas de ATM



AAL = Capa De adaptación de ATM
CBR = Tasa de bits constante
VBR = Tasa de bits variable

Asimismo, ATM trabaja con un protocolo denominado LAN Emulation (LANE) quien provee los servicios no orientados a conexión y de multicast ya que emula el protocolo de acceso al medio usado comúnmente por las tecnologías no orientados a conexión de las redes tipo LAN.

Por su propia tecnología de transporte, en una red tipo WAN como la de CUDI, el uso de ATM demanda en su topología física el uso de LAN Emulation Server (LES) y LAN Emulation Client (LEC) y LAN Emulation Configuration Servers (LECS). El LEC se refiere al software que apoya la conexión de nodos finales a la red ATM, el LES proporciona la translación de las direcciones MAC de 48 bits a las direcciones tipo ATM.

De esta manera convenimos que ATM es un protocolo que garantiza un nivel de calidad en la conexión de acuerdo a los requerimientos, siendo útil para las aplicaciones sensibles al tiempo de respuesta tales como la voz, siendo esto su principal ventaja. Otra de las ventajas de ATM es su operación está basada en la conmutación de alta velocidad de las interconexiones físicas de la tarjeta de procesamiento del switch mismo, llamado tecnología ASIC.

La configuración del camino permanente que deberá seguir una transmisión de datos entre dos puntos en ATM se denomina "trunk" y se requiere definir el camino y el puerto de conexión entre los equipos ATM, solo hay un trunk por conexión.

En cuestión de operación, ATM ofrece operaciones de detección de errores limitada. Con excepción del tráfico de señalización, no ofrece servicio de retransmisión. Las tasas de errores de las redes en general se miden a la tasa de errores de bits (BER, bit error rate), la cual se calcula:

$$\text{BER} = \frac{\text{bits con error recibidos}}{\text{total de bits enviados}}$$

Otra métrica útil es la tasa de errores de bloque (BLER), que se define como el número de bloques recibidos con errores contra el número de bloques enviados, tomando el concepto de bloques como en este caso la celda.

Otra estadística es la tasa de pérdidas y se refiere a la cantidad de celdas pérdidas de acuerdo al total de celdas enviadas, ya sea por daño de la celda y no puedan corregirse, las celdas que llegan demasiado tarde y ya no sirven y aquellas que la misma red desecha. Esta métrica es de suma utilidad para el diseño de la red que administramos, a medida que aumentan los errores en ella se hace necesario la retransmisión de información y eso aumenta la cantidad de tráfico en la red y se hace necesario los reajustes en su operación incluso de cambios de trayectorias o cambios físicos de algún elemento que sea la causa de los errores.

Cada enlace físico de la UNI tiene una entrada de MIB que se define en la atmPortTable, donde se contiene: un valor único para cada puerto, una dirección, el tipo de puerto, el tipo de medio, la situación del puerto y otra información.

La tabla atmfAtmLayerTable contiene información de la interfaz física como el identificador, del puerto, el número máximo de VCC, los VPC que se configuran, los bits de VCI/VPI activos, y una descripción pública o privada de la UNI.

La tabla atmfAtmStatsTable contiene estadísticas de tráfico de la capa ATM, la tabla contiene los datos del identificador de puerto, el número de celdas recibidas y no desechadas y el número de celdas transmitidas.

Hablando de desempeño, el cálculo de la utilización en ATM es basado en los objetos de la MIB-2:

Utilización total en Interfase ATM=

$$((\Delta \text{ifInOctets} + \Delta \text{ifOutOctets}) * 8 \text{ bits por octetos}) / ((\text{Tiempo final} - \text{Tiempo inicial}) * \text{IfSpeed})$$

Δ Significa los cambios de valor sobre el intervalo del tiempo

Los objetos MIB-2 valiosos en el monitoreo de ATM son:

ifOperStatus	ifOutNUcastPkts
ifAdminStatus	ifOutDiscards
ifInErrors	ifOutNUcastPkts
ifInUcastPkts	ifOutOctets
ifInNUcastPkts	ifInMulticastPkts
ifInDiscards	ifInBroadcastPkts
ifInOctets	ifOutMulticastPkts
ifOutErrors	ifOutBroadcastPkts
ifOutUcastPkts	ifHighSpeed

• Manejo de Redes Virtuales VLAN (Virtual Local Network)

Esta tecnología te permite crear grupos lógicos de los dispositivos físicos a través de toda la red. Hay diferentes técnicas para la creación de estas VLAN:

VLAN basadas en direcciones MAC. Los miembros de la VLAN son determinados por la dirección MAC de los dispositivos.

VLAN basada en Puerto. La VLAN se define por una colección de puertos de uno o varios switches y los equipos conectados a esos puertos son miembros de la VLAN.

VLAN basada en protocolo. El grupo esta basado en un tipo de protocolo o en una dirección de red

Técnica de VLAN	Ventaja	Desventaja
Por puerto	<ul style="list-style-type: none"> • Es fácil de comprender y administrar • Es soportada por diferentes fabricantes de equipos 	<ul style="list-style-type: none"> • Deberá ser reconfigurada manualmente cada vez que se mueva un equipo de puerto • No puede asociarse un puerto a mas de una VLAN
Por dirección MAC	<ul style="list-style-type: none"> • No es necesario reconfigurar ya que el dispositivo detecta la MAC 	<ul style="list-style-type: none"> • Se tiene degradación en el desempeño en puertos con varias MACs en diferentes VLANs • Todos los usuarios deberán asociarse por lo menos a una VLAN
Por protocolo	<ul style="list-style-type: none"> • Se puede particionar por tipo de protocolo • Un mismo puerto puede ser asociado en múltiples VLANs • Puede usarse en conjunto con máscaras de subred para evitar la excesiva granularidad 	<ul style="list-style-type: none"> • Le puede ocasionar degradación al desempeño de los equipos • Se requieren equipos capa 3 • Se requiere que los equipos ruteen.

El concepto de Redes Virtuales es utilizado en la red de CUDI para parametrizar áreas de operación dentro de la dorsal de CUDI y con esto controlar efectivamente el tráfico y las tormentas de broadcast

3.2.4 Base Inicial de Operación: Monitoreo

La operación de redes puede contemplar la realización de diversas tareas, pudiendo ser estas tan específicas, detalladas o complejas como se requiera o simplemente básicas y globales o una combinación de ambos estilos dependiendo de lo que se necesite. En nuestra propuesta definiremos una combinación que englobe los puntos necesarios, incluyendo: *monitoreo, atención de fallas, operación, ingeniería y administración de software.*

Quizá el punto mas crítico dentro de la operación de la red es el monitoreo ya que contar con la información adecuada en el momento y lugar preciso es la base del manejo adecuado del desempeño de la red, la atención de fallas, la seguridad y el resto de las actividades subsecuentes en el control de la misma. Asimismo, tener la información del comportamiento en tiempo real servirá para una planeación y diseño de la red con mejores resultados.

La toma de decisiones depende en gran medida de esta información. Por lo que definiremos claramente este concepto.

Monitoreo

El monitoreo es el efecto de extraer, interpretar y condensar los datos del comportamiento de un elemento de la red cerca de su origen y transferirlo a la entidad administradora. El monitoreo de la red nos permitirá conocer el desempeño de un elemento de la red en particular y sus puntos de enlaces, así para todos los elementos y agrupados saber el comportamiento completo de la red.

El extraer la información desde diferentes tipos de elemento puede resultar complejo debido a que los elementos de la red son diversos y cada uno tiene su propio formato de almacenamiento de datos. Esto puede ser simplificado si los datos son convertidos a un formato común.

Regularmente los monitores trabajan con la interpretación de cambios de estado de un elemento de la red, el cual el conjunto de estos cambios de estado lo conceptualiza como un evento. Así, el formato que ellos reciben son diferentes tipos de cambios de estado representados por valores binarios los cuales conformaran un evento y ese evento es enviado al sistema de administración de la red. Ya ahí, el sistema administrador de la red se encargará de conjuntarlo con el resto de los eventos de ese elemento de la red para conformar el estudio de su comportamiento. El comportamiento de cada uno de los elementos de la red nos permitirá elaborar reportes del comportamiento de un conjunto de puntos de a red que pueden conformar un enlace y así representar el comportamiento de toda la red.

Existen múltiples tipos de instrumentos, tanto en hardware como en software, que sirven para coleccionar esta información a diferentes niveles de los dispositivos tanto físicos como lógicos de la red, cada uno de estos instrumentos son caracterizados por costo, complejidad, desempeño, utilidad y tipo de extracción. Los instrumentos de extracción y colección de esta información residen en los mismos elementos de la red o en algún otro sistema alrededor de ellos y son manipulados por los sistemas llamados de monitoreo o por una entidad conjuntiva de ellos. Muchas veces los mismos elementos de la red participan de cierta manera en esta tarea de monitoreo pero hay que diferenciar entre un objeto monitoreado y un sistema de monitoreo.

Las redes están conformadas por múltiples elementos y cada uno de ellos debe tener un método de monitorearlo diferente de acuerdo a la parte de la red que pertenece, así, hay que contemplar el monitoreo para las líneas seriales, enlaces de banda ancha, servidores, ruteadores, etc.

Dentro del monitoreo se contempla una entidad que esquematizará, estudiará y administrará la información, la cual es el sistema de administración de la red. Por lo tanto, el monitoreo es un elemento de todo el esquema de Administración de la Red.

Niveles de Monitoreo

Los instrumentos de monitoreo se desempeñan en alguno de los 3 tipos de monitoreo siguientes:

- a) Monitoreo de la red física o monitoreo físico
- b) Monitoreo lógico de la red, o monitoreo lógico

c) Monitoreo de servidores-LAN's

a) Monitoreo de la red física o monitoreo físico

Se monitorean los elementos físicos de la red y su comportamiento, tales como interfases de comunicación, puertos, canales, interfases internas de equipos y en casos especiales elementos de software que reportan estados físicos.

Los instrumentos para el monitoreo físico permitirán:

1. Monitoreo y pruebas en forma automática y remota del sistema. El objetivo es evitar un servicio en sitio para realizar esto.
2. Recobrar una falla en el sistema en tiempo real, así como realizar reconfiguraciones necesarias.
3. Proveer estadísticas del comportamiento de la red y todos sus elementos para facilitar una mejor planeación y administración de la misma.

Categorías en el monitoreo de la red física:

1. Control técnico de los elementos de la red
3. Monitoreo y control equipo de CSU/DSU
4. Monitoreo de Multiplexores y bancos de canales
5. Monitoreo de PBX's
6. Monitores de red
7. Monitores de Hardware

Para nuestro proyecto solo nos interesan las categorías 1, 2, 3, 6 y 7.

1. Control técnico de los elementos de la red. En esta categoría de monitoreo de la red física, se pretende la observación del comportamiento de cada uno de los componentes de la red, su desempeño de acuerdo al tipo de componente que se trata y de acuerdo a sus parámetros de funcionamiento.

Entre los principales instrumentos que se encargan de ésta tarea están los monitores de línea, que son los instrumentos más simples para probar equipo, pero debido a esto

también uno de los instrumentos más básicos e importantes. Estos son equipos de diagnóstico usados para observar y analizar los datos que pasan a través de la red, concentrando la información de los elementos, los analiza y envía al administrador central desplegándolos en una pantalla ó los almacena para que sean analizados posteriormente. Existen algunos monitores de línea que incorporan analizadores de protocolos e inclusive pueden realizar tareas de simulación. Los monitores de línea son considerados genéricos debido a que algunos de ellos pueden abarcar monitoreo y pruebas en LAN y WAN de acuerdo a sus capacidades. Existen analógicos y digitales.

Para probar las líneas analógicas existe un panel de conexión analógico, llamado panel de parcheo, que permite un punto de conexión entre las líneas analógicas y los módems y además el monitoreo de éstas. Este panel de parcheo cuenta con herramientas de audio como son un speaker y un amplificador para que el personal encargado haga pruebas y prácticas en las líneas y pueda reconocer líneas deterioradas, variaciones en respuestas, etc.

Regularmente se conectan otros instrumentos de monitoreo a través de éste panel de parcheo, como puede ser el metro decibel (dB) el cual mide los niveles de audio transmitidos y recibidos en la línea. Los niveles de audio son regidos por el proveedor nacional (su nombre estándar en inglés es "carrier"), estos niveles de audio los proporciona de acuerdo a parámetros de acondicionamiento para una línea y son ajustados por el proveedor.

Otro instrumento es el monitor de la calidad de la línea que mide los imperfectos en la línea como puede ser: atenuación, desfasamiento, alteración en la amplitud de la señal, movimientos en la frecuencia, picos de ganancia, ruido, interrupciones cortas, distorsión en la frecuencia, etc.

Todo este conjunto de pruebas analógicas alineadas a los valores proporcionados por los comités nacionales oficiales, nos sirven para complementar todo el monitoreo de las líneas, determinando las condiciones de ellas y evitar alguna falla posterior de mayor importancia.

Para detectar imperfecciones en las señales digitales, debido a su naturaleza de codificación por pulsos, se requieren patrones para medir el control del código y el valor del bit-error (error por bit) siendo cubierto ampliamente por los monitores de línea. Estos, se encargaran de desplegar la información que circula por la red en ambos sentidos de la línea puntualizando los caracteres de control que pasan por la línea

activando ciertas señales (leds o sonidos) cuando ocurre algún evento que sea importante en la transmisión o recepción de las señales de información. Estos monitores de línea son equipos portátiles para mayor facilidad de llevar por el personal de campo al lugar de las pruebas, pero también pueden estar conectados permanentemente o por periodos largos a ciertas interfases de algunos equipos como parte de un control técnico de ellos enviando información al monitor central, ya sea a través de una línea de la red o de una línea telefónica; el usar una u otra dependerá de decisiones del administrador de la red ya que es un punto que puede influir en el tráfico que circule por la red y del control en tiempo real que se requiera.

Algunos criterios de lecturas son: señales de las interfases, estado de entrada y salida, interrupciones del servicio, etc.

Existen monitores pasivos, los cuales solo albergan datos de la red y son comúnmente usados en redes pequeñas y sencillas. De acuerdo a la complejidad y tamaño de la red, también existen otros monitores que incluyen tareas mas sofisticadas como el conteo de bits y bloques con errores en intervalos de tiempo y considerando la velocidad de la línea (el bit-error, BER y el block-error, BLER); temporizador, timeout, jitter, etc., e inclusive algunos que traen unidades de simulación, los cuales pueden emular varios componentes de red como módems, CPU's y realizar pruebas interactivas; así también sirven para probar protocolos de comunicación, estos monitores son llamados analizadores de protocolo.

Los sistemas de control técnico de la red pueden ser sistemas manuales o automatizados, su principal característica es que llevan a cabo un monitoreo centralizado y son capaces de restaurar una conexión de red en caso de que hayan sufrido alguna falla gracias a que cuentan con equipo de conmutación y conexión de líneas entre canales alternos o secundarios que les permiten esta tarea. Están conectados a través de líneas dedicadas o telefónicas a los equipos remotos que deben monitorear y así no es necesario que el personal se desplace hasta el origen de la falla. Por este tipo de características, son útiles en puntos de conexión importantes de la red, donde se mantenga algún nodo grande o esencial en su funcionamiento.

Estos dispositivos también cuentan con una base de datos, la cual es útil para llevar mejor control de los eventos, estadísticas e incluso el manejo de un inventario, el cual es de mucha ayuda para llevar el control de los dispositivos de la red, entre otras cosas. Como su módulo de administración de red está basado en software, esto lo hace muy versátil y manejable, ya que se le puede amoldar a las necesidades de la red y

suprimir tareas innecesarias o adicionarle paquetes, módulos o aplicaciones para robustecer la administración de la red, como pueden ser sistemas de reportes de falla, software de encapsulamiento o seguridad. Entre otras cosas también puede contar con un sistema reporteador con un formato sencillo de manejar y un registro histórico de eventos que permita llevar a cabo estadísticas desde las más sencillas hasta alguna sofisticadas de esta manera son una herramienta fundamental para el administrador para su análisis y planeación de su red.

Estos equipos resultan más caros que los monitores de línea pero mas económicos que otros monitores de control de red que además de las características antes mencionadas ofrecen herramientas y facilidades más sofisticadas, que más adelante trataremos.

2. *Monitoreo y Control CSU/DSU.* Es uno de los sistemas más importantes del monitoreo y control de los enlaces punto a punto es el CSU. El CSU es una interfase protectora diseñada para conectar el equipo de de datos a la línea de transmisión del carrier, ya sea un servicio digital de datos o un DS1/T1/E1 o sus múltiplos. Cuenta con características internas capaces de monitorear y probar las señales enviadas y recibidas por el DTE. Sus desplegados de diagnóstico se componen de pantallas de LED's y switches para crear loopbacks, que son las pruebas básicas útiles tanto para las líneas de transmisión como para los equipos conectados. Algunos CSU's pueden comunicarse con un sistema central de monitoreo.

Los CSU's permiten realizar diagnósticos locales o remotos de acuerdo al tipo de señalización de prueba que se maneje. Su panel frontal contiene LEDS de diagnóstico que determinan fallas menores en las líneas de transmisión como despolarización, desincronización, estados de loopback, etc. Este tipo de pruebas son útiles de ejecutar para una detección rápida de problemas de comunicación en el enlace. Algunos CSU's inteligentes pueden trabajar en conjunto con el sistema de administración para cubrir el monitoreo de varios equipos como son los multiplexores, PBX's, puentes y enrutadores.

3. *Monitoreo de Multiplexores-T1 y bancos de canales* Las funciones básicas del monitoreo de multiplexores incluyen detección de fallas, alarmas y reportes. La administración del multiplexor puede ser realizada en el mismo puerto, en el nodo, en la red o en la conexión punto a punto.

La elección de adecuados multiplexores para las necesidades de la red debe contemplar, además de sus características de descanalización, etc., capacidades de monitoreo. Mientras más capacidades de monitoreo tenga el equipo mejor control se tendrá de él. Esto habla bien de estos equipos ya que se entiende que son equipos sofisticados en donde no se ha descuidado ningún detalle. Así, como comentamos anteriormente, se debe contar con los diferentes niveles de monitoreo en un multiplexor, definidos como:

Monitoreo a nivel del puerto: Nos permite monitorear, controlar y hacer las pruebas necesarias en la interfase del multiplexor hacia el equipo terminal (DTE); por lo tanto las interfases deberán ser flexibles ante pruebas de capacidades, para lo cual se requiere que se puedan obtener los valores de sus niveles, estado de la conexión, estadísticas del uso del puerto; que se puedan hacer pruebas de loopback en cada una de ellas, que cuenten con software de control que nos evite tener que abrir el equipo para deshabilitar una tarjeta sino que trabaje con a través de switches.

Monitoreo a nivel del nodo: Nos permite monitorear y controlar el multiplexor en sí y su enlace WAN (T1, E1 o múltiplos), incluyendo por supuesto el puerto físico de conexión del enlace, Este nivel es muy importante ya que la disponibilidad y optimización del ancho de banda es esencial en el desempeño de la conexión y el sistema de administración debe garantizar esto, apoyándose de un manejo dinámico del ancho de banda. Además de esto, el equipo debe soportar una consola local amigable que controle su desempeño, que despliegue alarmas y debe proporcionar la capacidad de realizar pruebas asimismo y deducir reportes de sus eventos.

Monitoreo a nivel de red: Este nivel trabaja con el control y monitoreo en el nivel de aplicación, por lo tanto se encargará de la correcta ejecución de las aplicaciones y la calidad del servicio de conexión. Este monitoreo debe contemplar el paso a través de diversos medios (carriers) hasta llegar al multiplexor final por lo que los puntos de falla que atraviesa son varios. Algunas características que deben ser cubiertas son circuitos de conexión sencillos y respaldos de conexión en caso de alguna falla. Los respaldos de conexión al ocurrir alguna falla puede ser sustituyendo algún equipo dañado, lo cual tomará bastante tiempo, ó re-enrutando el circuito por alguna otra conexión existente y disponible que puede llevar pocos segundos. Algunos multiplexores sofisticados proveen estas facilidades de reenrutamiento automático con lapsos de tiempo dependiendo del tipo de multiplexor del que se trate (de manejo de paquetes o basados en circuitos). Después de la recuperación del enlace se realiza el reajuste de los parámetros de éste que contempla varios factores, rutas, tiempos, etc.

Monitoreo a nivel de Control de red: En este nivel se contempla todos los componentes de la red que están vinculados con los multiplexores en algún punto de la conexión. Está apoyado por una base de datos y por un generador de reportes. La base de datos debe tener capacidad para guardar una gran cantidad de datos, que incluyen descripciones de equipos, enlaces, softwares, procedimientos, relaciones, etc., y para una manejar una diversidad de topologías. Algunos multiplexores requieren de equipo y software anexo para que puedan ser monitoreados a estos niveles, como son los analizadores de protocolos, monitores de red, etc. y deben abarcar

El monitoreo del enlace WAN es tanto en voz como en datos e incluye las señales analógicas y las digitales.

La diferencia entre en el monitoreo del enlace analógico de voz y el digital radica en los parámetros que se observan; en el analógico se observan los niveles y violaciones bipolares mientras que en el digital se observa la sincronización de reloj, bits de señalización, etc. Las pruebas en los canales requieren de la habilidad del personal que va a realizar las pruebas para que, primero, al probar las líneas no interrumpan el servicio, segundo, realizar las pruebas apropiadas (loops, etc.), tercero, realizar en forma apropiada las simulaciones de señalización y por último detectar el punto de falla rápidamente.

Las fallas analógicas incluyen voz, atenuación, distorsión, pérdidas de señal, retardos, interferencias en la frecuencia.

El monitoreo diario de la línea estando ésta en servicio se realiza ejecutando pruebas y reportes periódicos de su funcionamiento y es útil para darnos cuenta de degradaciones en el servicio y darle soporte antes de que ocurra una falla real en él. Así también se lleva a cabo debido a que el tráfico que circula por la línea no puede ser desviado por otro canal. Algunas veces el tráfico si puede ser desviado por otro canal y realizarse pruebas con la línea fuera de servicio, este tipo de pruebas son menos periódicas y solo se realizan cuando se da un mantenimiento exhaustivo a la línea o cuando ocurre alguna falla en ella ya que implica costos altos monetarios y de personal, además el mantenerla fuera de servicio también acarreo consecuencias en el servicio debido a que el canal que la sustituye no se de abasto con el tráfico o requiera de cambios sofisticados en la red que se reflejen en lentitud, loops, traslapes de rutas, etc. El monitoreo fuera de servicio es precedido por un monitoreo en línea que ha

detectado la necesidad de él. Un monitoreo en línea adecuado y el soporte por tramos de la línea pueden evitar la suspensión total del servicio para realizar el monitoreo de prueba o por lo menos reducir el tiempo necesario de reparación.

Las pruebas en servicio son divididas en dos clases:

-Las mediciones ejecutadas en el enlace WAN propiamente, que analizan violaciones en la codificación, detección de excesos de ceros, nivel de la señal, determinación de la frecuencia de la señal, condiciones de todos unos, alteración de tiempos, etc.

-Las mediciones ejecutadas en el contenido del canal, cuales analizan errores en el formato de envío, chequeo de redundancia cíclica (CRC) y detección de alarmas amarillas.

Algunas de las pruebas básicas en las salidas del enlace WAN es colocar en algún slot determinado un canal VF digitalizado y pasar bits de señalización tipo A y B, así probamos algún canal específico y no afectamos el resto de los slots.

Otra prueba tradicional es la del "bit error rate", el cual requiere de la inserción de un patrón aleatorio definido dentro de cada uno de los canales o en el canal completo, no trabaja muy bien debido a los procedimientos de bit-robbing usados en el fraccionamiento de la canalización y señalización del enlace.

4. Monitores de red. Los monitores de red son de las herramientas más importantes y completas en el monitoreo de la red. Además, son de los monitores mas completos ya que algunos tienen capacidad de monitorear la gran mayoría de los elementos de la red, ya sea en forma individual, sus enlaces o su desempeño en conjunto. Son bastante manejables y pueden ser desde muy sencillos hasta bastante sofisticados apoyados por otros módulos externos que pueden ser acoplados por medio de hardware y software. Por tales razones son los monitores que se encargan de monitorear la red, analizar y controlar los eventos en todo momento, Su robustez les permite monitorear cientos de dispositivos a la vez.

Este sistema puede realizar en banda o fuera de banda, es decir, para llegar a los elementos a monitorear puede usar la misma línea de la red operativa o en conexiones alternas o superpuestas. La decisión de esto radica en el administrador de la red.

Como comentamos anteriormente, estos sistemas se apoyan en módulos externos que llegan a formar parte de él, uno de estos módulos es el help desk o grupo que se encarga de recibir y dar atención a los reportes de fallas de la red, contando con características poderosas y sofisticadas de alertas que indican cuando a ocurrido un problema, en que parte de la red y cuales son las posibles causas. En el help desk, comienza el verdadero trabajo del administrador de la red, pero de éste hablaremos más adelante.

El módulo de colección de datos son computadoras cuyo objetivo es monitorear múltiples canales de comunicación simultáneamente, tantos como el ancho de banda del módulo soporte, para determinar su estado por medio de interpretar el tráfico que circula por los canales. Los programas para interpretar el tráfico son almacenadas en PROM's y dependen del protocolo de comunicación que trabajen ya sea para interpretar a nivel de paquete, de bit, caracter, etc. En el nivel de paquete, por ejemplo, los eventos significativos incluyen llamadas de reset, limpieza y reenvío de paquetes. Estos módulos son generalmente conectados al CPU a través de puertos de comunicación asíncronos y realizan su función de colección de datos reconociendo eventos significativos en el estado y desempeño de la línea de comunicación; cuando ha detectado estos eventos se envían al CPU mensajes de alerta.

Los monitores más sofisticados cuentan con diferentes protocolos y varios puertos.

Algunas veces se requiere de módulos remotos de colección de la información de los elementos de la red, donde éstos pueden ser conectados en cualquier interfase digital y comunicándose al CPU en forma asíncrona usando los canales productivos de la red, canales secundarios o servicios de circuitos switcheados. El tipo throughput (comportamiento) de éstos módulos es muy importante para las mediciones de las conexiones principales. Regularmente la colección remota es muy útil, los casos típicos incluyen:

- Usar procesadores remotos front-end y conexiones principales entre el lugar remoto y el local
- Colectar información en el lugar remoto pero sin sacrificar el control central
- Colectar figuras relacionadas con tráfico para tráfico terminal a terminal sin que se tenga procesadores front-end.

Estos módulos pueden extenderse para que incluyan funciones de pruebas, reinicialización, medición y desplegado de estado, etc., dependiendo de la capacidad de la computadora donde se encuentra. El CPU de la computadora llevará el control de las operaciones de todos los sistemas, es por ello que mientras el sistema de monitoreo sea más sofisticado y extendido, se debe encontrar en una computadora bastante sofisticada, con características propias robustas, como son la capacidad de memoria, de disco duro para almacenar la información, de procesamiento, de multitareas, multiproceso, etc., y algunas características de manejabilidad como:

- Técnicas de manejo por menú
- Teclas de funciones principales
- Procesador de palabras
- Capacidad de acercamientos del desplegado
- Capacidades de reportes gráficos
- Interfases de desarrollo de aplicaciones para lenguajes de alto nivel
- Menú de ayuda
- Técnicas de Ventaneo
- Características de modelado
- Monitor de alta resolución
- Correo electrónico

Otra característica importante en estos sistemas es el manejo de datos históricos. Estos pueden ser almacenados en una base de datos recabando todo el comportamiento de la red y sacando de ahí los datos necesitados para ser procesados posteriormente. Esta es una herramienta bastante útil para sacar mayor provecho cuando se necesita rediseñar la red u optimizar alguna conexión, utilizando datos de diferentes tipos de mediciones del desempeño, ya sean mediciones orientadas al servicio, tales como disponibilidad, tiempo de repuesta y precisión y medidas orientadas a la eficiencia, tales como la utilización y el comportamiento del canal.

Todo depende del elemento que se desea investigar, los parámetros son coleccionados, analizados y comprimidos a niveles diferentes de detalle, el último minuto, hoy, ayer, un día específico, por semana, por mes, etc.

Existen otras bases de datos que mantienen otros conceptos de la administración de la red, como son el inventario, manejo de reportes, etc., y todas deben ser acopladas entre sí para un manejo de la administración. El tamaño de una base de datos

dependerá del número de elementos y enlaces que se manejan en la red. Eventualmente, los datos almacenados deberán ser respaldados en algún dispositivo externo, ya sea por concepto de seguridad, por limpiar la base de datos para nuevos datos, cuando la capacidad del equipo de almacenamiento ha llegado a su límite o inclusive por llevar una secuencia ordenada de respaldos cada cierto tiempo. Estos pueden ser almacenados en cintas, en otro disco duro, en discos ópticos, etc., y ser consultados posteriormente si es necesario.

Otro factor muy importante son los indicadores que maneja el monitor. Los monitores de red soportan varios tipos de indicadores. Estos indicadores están relacionados con el tipo de elemento de red que observan y los eventos que queremos que nos señalen. El habilitar los adecuados dependerá del uso que queremos hacer de su reporte posteriormente. Algunos indicadores básicos son:

o Para parámetros de servicio:

-Disponibilidad

- Disponibilidad de la red completa
- Disponibilidad de la línea
- Nivel de disponibilidad del usuario

-Tiempo de respuesta

- Retardo de la red
- Retardo del nodo
- Tiempo de respuesta Promedio
- Tiempo de respuesta máximo
- Tiempo de respuesta mínimo
- Alternativas en el nivel del usuario
 - Sobre el primer caracter
 - Sobre la llegada de la información completa
 - Sobre el acceso a la terminal
- Lista de tiempos de poleo

-Seguridad e integridad

- Números de reportes por elemento de red
- Lista de reportes más frecuentes
 - Número de mensajes perdidos
 - Número de mensajes duplicados
 - Número de mensajes llegados pero no deliberados

	Números de retransmisiones
	Números de timeouts
	Número de transmisiones incompletas
Parámetros de eficiencia:	
-Throughput (Comportamiento)	
Transmisión	Número de transacciones
	Número de mensajes
	Número de caracteres
	El mensaje más largo
	Longitud promedio de mensajes
	Número de paquetes
Recepción	Número de transacciones
	Número de mensajes
	Número de caracteres
	El mensaje más largo
	Longitud promedio de mensajes
	Número de paquetes
Poleo	Número de poleos positivos y negativos
	Retardo de poleo
Utilización	Controlador de comunicación
	Dispositivo terminal
Líneas desocupadas	
Utilización de Líneas	
Utilización de software	
Contención	

o Módulo de alertas.

Estos dispositivos de alerta asociados con el monitor de red usualmente son manipulados a través de una pantalla grande (a veces gigante) con gráficas a color de

alta resolución. En sistemas sofisticados se tiene una pantalla gigante en el centro de control de la red, donde el desempeño de la red es visible a más de un administrador y los sistemas receptores están alertas, como impresoras. Estas alertas pueden ser programadas o filtradas y pueden hacerse presentes de diversas maneras como: cambios de colores de los elementos, sonidos diferentes, envío de mensajes, parpadeos de íconos, etc.

Las alertas pueden ser optimizadas preprogramando umbrales de valores cuidadosamente. El establecimiento de los umbrales es realmente muy importante en el monitoreo de la red ya que el establecimiento de ellos en forma inadecuada puede traer consecuencias malas en el mantenimiento de la operación de la red. La programación de umbrales rígidos o desplegados frecuentemente de excepciones, es decir umbrales muy modificables por el propio sistema pueden permitir sobrerreacciones por parte del centro de control ó si no se tienen los chequeos por parte del sistema puede ocasionar un gran impacto en el soporte en caso necesario. La atención de estas alertas se lleva a cabo en varios niveles, la determinación de la falla, la localización, acciones recomendadas, etc., y los primeros niveles ayudan en mucho los subsecuentes niveles hasta la resolución de la falla. El manejo de múltiples niveles de la alerta, sin llegar a la exageración, ayudará a simplificar el problema y resolverlo e incluso definir un reporte mas detallado de la falla.

Así, el desempeño de la red es almacenado, procesado, analizado, interpretado y reportado usando sistemas estadísticos y gráficos. El análisis es muy útil para determinar orígenes de fallas y dependencias de parámetros entre sí y dentro del él se utilizan técnicas completas de estadística y correlación. Los monitores de red analizan todo en correspondencia con la dirección física aunque muchas veces esto puede ser programado para que se comporte como si se monitoreará por grupo de aplicaciones.

Es importante mencionar que no todo viene programado por el vendedor del sistema y muchas veces hay que reestructurar las aplicaciones a la medida de las necesidades de la red, integrándole software externo para robustecer sus aplicaciones e inclusive compilarle módulos dentro de la programación misma. Los administradores mas experimentados pueden pedir acceso al código fuente del sistema, aunque esto no debe ser realizado por los inexpertos ya que pueden alterar el sistema y no poderlo componer después significándole esfuerzo, dinero y tiempo perdido innecesario.

o Algunos criterios para la selección de los monitores de red son:

- Disponibilidad de un control central
- Protocolos soportados
- Soporte de manejo de base de datos
- Soporte de sistema de reportes de fallas
- Soporte de indicadores de desempeño
- Disponibilidad de múltiples niveles de alarmas
- Disponibilidad de múltiples niveles de generación de reportes
- Soporte de análisis de desempeño
- Difusión de mensajes
- Soporte de manejo de funciones
- Programabilidad
- Interfase del usuario
- Expansibilidad
- Seguridad
- Control por software de inhabilitación de líneas
- Flexibilidad adecuada para cambios de configuración
- Corrección de errores.

5. *Monitores de Hardware.* En los sistemas electrónicos se pueden detectar la mayoría de las características de comportamiento de los circuitos de su hardware a través de cambios de voltaje de señal en él. De este factor se sirven los monitores de hardware y cualquier hardware de cualquier marca puede ser medido, por ejemplo: líneas, dispositivos de almacenamiento, concentradores, puentes, switch, computadoras, etc.

De alguna manera es el monitor de bajo nivel y básico para los dispositivos individuales de la red. Las señales observadas en el equipo son modificadas a través de técnicas especiales para que puedan ser almacenadas en forma comprimida y son llevados al sistema central o son procesados en el mismo monitor de hardware donde se elaboran reportes.

Los monitores de hardware están equipadas con minicomputadoras que les permiten llevar a cabo procesamiento de los datos, poderosas bases de datos con técnicas de acceso directo y generador de reportes sofisticados. Fundamentalmente se tienen

contemplados dos tipos de medición con estos equipos: los eventuales y los temporizados.

-Eventuales. Acumulación de ocurrencias de un evento específico.

-Temporizado. Temporización de la duración de una señal específica por frecuencia de pulsos de reloj fijos desde el comienzo de la señal hasta que ésta termina.

El contacto directo entre el equipo a ser medido y el monitor es a través de sensores de monitoreo. Estas interfaces de medición deben ser estándar para poder medir todo tipo de equipo, aunque no todos los fabricantes los elaboran así, a veces los hacen propietarios para equipos del mismo fabricante. Estos sensores son capaces de detectar todo tipo de señales en el equipo; así, lo que realizan es sensar un voltaje diferencial en un punto de prueba, amplificar la señal detectada y transmitirla al un módulo especial del monitor para un procesamiento posterior, almacenando la información en la base de datos, pero antes puede ser filtrada para seleccionar algún tipo especial de datos. Esta información puede ser desplegada para atender algún tipo de soporte técnico en ese momento o elaborarse en forma de reporte posteriormente para un estudio de desempeño y quizá para apoyo de la planeación de la red.

b) Monitoreo de la red lógica

En esta fase del monitoreo se observan los estados lógicos de los elementos de la red. El desempeño de la red y la respuesta a el usuario también puede estar influenciado por el estado lógico de los elementos, la memoria, el procesador, la memoria caché, etc. Estos elementos son controlados por los sistemas operativos, control de colas, administración de recursos, temporización, prioridades, ejecución de programas y aplicaciones, etc. Por ejemplo, el retardo en el tiempo de respuesta del nodo puede determinar arriba de 70% o 80% del tiempo de respuesta al usuario. Los monitores de software son utilizados para observar el desempeño de estas características lógicas; aunque estos no son usados continuamente, ya que se supone que el desempeño lógico de la red no tiene comportamientos tan variantes ni tan seguidos como el físico. Los monitores de software constituyen la clase de programas para medir hardware, sistemas y aplicaciones. Están residentes en el sistema de almacenamiento y pueden ser activados y desactivados por el administrador en el momento que lo requiera,

incluso pueden ser activados o desactivados por la marcación de algún evento o por un reloj.

Como los demás monitores, los datos medidos son colectados, resumidos, procesados y reportados; así, a través de alguna base de datos pueden ser accesados en cualquier momento. En los monitores de software es más usual la programación de umbrales de mediciones para la sofisticación de los reportes, pudiendo generar alarmas, excepciones en avisos y automatización de procesos; además, algunos de estos monitores cuentan con módulos de medición de variables del estado del sistema del propio elemento de la red, con lo cual se puede tener un control más completo de los recursos del elemento.

Según el monitor de software, algunas veces pueden llevar a cabo una interpretación de las lecturas y tomar algunas medidas básicas y enviar el un mensaje de aviso al administrador de la red o desplegarlo en una pantalla especial para esto para que se le pueda dar al evento el soporte técnico completo, o inclusive conformar un reporte para un análisis posterior.

Algunas de las mediciones realizadas son las siguientes:

Perfil del sistema: Muy útil para evaluar el desempeño del sistema completo. En muchos casos son incluidos parámetros relacionados con el CPU y con los dispositivos de I/O. Toda la información del perfil del sistema es generada como una función de aplicación.

Utilización de la memoria: Nos da información con respecto al uso del espacio de direcciones para las aplicaciones, la cual ayuda a distribuir los programas residentes de una forma más efectiva.

Arreglo de datos: Provee información física sobre la localización física de los datos, lo cual puede ocasionar demasiados movimientos del brazo del disco, innecesarios o extremadamente largos. Analizando esto pueden ser optimizados.

Utilización de los canales lógicos: Provee información básica para el mejoramiento de todas las configuraciones de I/O.

Distribución de la longitud de colas: Puede ser usado para afinar al sistema operativo cuando los recursos están trabajando en forma lenta y cuando la longitud de las colas es excesiva.

Mapas de los programas de aplicación: Nos da una alineación para optimizar los programas de aplicación. Los monitores insertan contadores y dan información concerniente al desempeño del programa durante la ejecución, como frecuencia de ejecución de módulos específicos, tiempo promedio de ejecución de algún módulo en particular, etc.

Monitoreo Básico que debemos considerar:

Contabilidad de paquetes: La mayoría de los sistemas tienen por lo menos un contador de paquetes, esto es muy común ya que es una de las mediciones básicas en cualquier sistema, que sepan que entra y que sale de ellos, es decir, del consumo de sus recursos por ciertas aplicaciones. Regularmente esto se da en bytes, aunque también se manejan mucho las unidades de paquete. Mientras mantengamos un estándar dentro de nuestra red de esta unidad puede ser una u otra. La elección de la unidad de lectura también depende del enfoque que queremos tener de la medida y del dispositivo que estamos leyendo.

Monitores de aplicación: Ayudan a dar el estado de los subsistemas de aplicación, particiones o de las aplicaciones en sí. Este monitoreo es muy útil para la administración de la red de punto a punto. Estos monitores también pueden utilizarse para controlar el consumo de los recursos en tiempo real.

Monitores de comunicación: Esta categoría es muy cerrada ya que solo monitorean lo respectivo a las actividades de la comunicación en sí de los elementos de la red. La información fluye hacia y desde la instancia de control y es regulada por las reglas de la arquitectura bajo consideración. Cada arquitectura tiene especificadas sus propias reglas para coleccionar, comprimir, consolidar y transferir los datos.

Monitores de seguridad: Los monitores de seguridad se encargan de supervisar continuamente los indicadores de seguridad principal. Estos indicadores deben ser manejados por niveles jerárquicos:

-nivel de dispositivo del usuario final

- nivel del medio de transmisión
- nivel del procesador

Trabajan en forma parecida al resto de los monitores y su trabajo básico está dividido en la administración del acceso a los elementos de la red o por lo menos a los más importantes y el monitoreo de la seguridad de las aplicaciones. Con el monitoreo del acceso a los elementos se puede llevar un control de los accesos autorizados a cada elemento.

c) Monitoreo de LANs

Como comentamos anteriormente, no se le da la importancia adecuada a l monitoreo de las LAN's; se ha concentrado más la atención en los elementos de conectividad en forma individual o las aplicaciones en forma individual, pero el monitoreo en la LAN no se contempla en forma conjunta. A lo largo de la experiencia se ha visto que este tipo de monitoreo ya es básico dependiendo el tamaño de la red, muchos de los problemas que surgen se pueden resolver en la mitad del tiempo si se lleva un buen monitoreo del segmento de la red local a analizar. Debemos ver a la red local como segmentos de la totalidad de nuestra red.

Existen varios problemas comunes en las LANs:

- Gran número de componentes: Que en una LAN se tenga un gran número de equipos, entre ellos, computadoras, concentradores, multiplexores, repetidores, puentes, etc., que originará que los puntos de falla de una red sean múltiples y muy diversos, entre otras fallas físicas debido al propio límite físico de la topología de la red, donde esto no es muy enfatizado y claro de definir siempre. El hecho de monitorear todos los diferentes dispositivos en la red lo convierte en inmanejable ya que saturaría aún más la red y afectaría su desempeño.

- Monitoreo estático: Dada la naturaleza pasiva de las LAN's, en comparación con las WAN's, si un dispositivo dentro de ellas falla, puede ser independiente de la actividad del resto de los dispositivos dentro de ella y puede que no se detecte el tipo de falla que ocurrió ni se distinga su importancia. Tampoco se puede monitorear todos los dispositivos por la razón anteriormente explicada. Así, el administrador de la red no se entera si la red local ha fallado o se entera hasta que ya ha transcurrido bastante tiempo o el usuario final le avisa.

- Saturación de supervisión: Dado el hecho de tener muchos componentes en la red y tengan que ser monitoreados, muchas veces han tendido a descentralizar el monitoreo pero el exceso de supervisión puede ocasionar múltiples traslapes de información y tráfico innecesario en la red.

- Difusión inherente de las operaciones de la LAN: La difusión inherente de la operación de la red hace sencillo de registrar algunos parámetros de manera sencilla por casi cualquier elemento de la red, esto puede ser una ventaja pero cuando no es controlado resulta desventajoso ya que la velocidad y nivel de trabajo de muchas LAN's tienen un alto requerimiento de CPU y el nivel de monitoreo que se obtiene no es muy alto; así el activar esta característica en los dispositivos degrada el desempeño de los dispositivos y de la red misma y no se obtiene un gran provecho. Por lo tanto es mejor dedicar dispositivos especiales para este propósito.

-Diversidad de tecnologías: Una LAN con una gran variedad de equipos, marcas, protocolos, entre otras entidades, es muy difícil de manejar y monitorear. Mientras más diferentes tecnologías se tengan en la LAN se necesitan más diferentes sistemas de monitoreo ya que cada tecnología tiene su propio esquema de monitoreo y éstas trabajan con protocolos de monitoreo diferentes, como SNMP, CMIP, NETBIOS, etc. Es intuible la saturación de tráfico en la red y la complicación de manejarla.

-Falta de estándares: Los primeros sistemas de monitoreo se caracterizaban por ser propietarios, dado que no se tenía un estudio detallado de las necesidades de la red general y la cobertura de los dispositivos en su totalidad por saber su estado. Existen aún algunos sistemas propietarios y se caracterizan por no abarcar en su monitoreo más que los dispositivos de su misma tecnología, esto los hace incosteables e inmanejable ya que no se puede tener para cada elemento un sistema de monitoreo o por lo contrario no se puede monitorear solo algunos elementos y otros de igual o mayor importancia no hacerlo. Se tiene un monitoreo incompleto de la red, nada sofisticado y por lo tanto no es un buen trabajo.

-Mezcla de administración de red y sistemas: Las últimas arquitecturas de monitoreo son una combinación de monitoreo de red y de sistemas, debido al desarrollo que han tenido los elementos de la red donde ya cuentan con módulos de software bastante sofisticados reemplazando la complejidad del hardware. Además a nivel local, son muy usados servidores poderosos de administración de cuentas de usuarios, espacio en

disco, procesos, etc., que deben ser monitoreados. Todo esto hace del monitoreo local un esquema complejo.

-Mal control de configuración: El no tener un buen control de las configuraciones de cada uno de los elementos de la red conlleva a cambios innecesarios en estas configuraciones, repetición de parámetros en ellos que dan como resultado problemas de desempeño de la red. Además, si las configuraciones son elaboradas por diversas personas y no se lleva un control, se presta a que se traslapen configuraciones, o se realice trabajo repetitivo, o no se realice una adecuada configuración del dispositivo.

-Descoordinación con los responsables locales: El desconocimiento por parte de los responsables del monitoreo local da como resultado que ejecuten el monitoreo en forma inadecuada y que ellos mismos se traslapen funciones, o que se pierdan en el control de su red.

El monitoreo de las LAN's es soportada por 3 tipos de instrumentos:

- Analizadores de protocolos
- Herramientas de diagnóstico de software
- Reflectómetros de dominio-tiempo

En el siguiente Capitulo 4 se describirán el resto de las actividades implementadas de el modelo de gestión y que van directamente como resultado del monitoreo.

Capítulo 4

PROPUESTA DEL NOC-CUDI: DEFINICIÓN, ESTRUCTURA DE OPERACIÓN Y CONTROL

4.1 OBJETIVO DEL NOC-CUDI

El NOC-CUDI, es el grupo de trabajo encargado de la administración, control, monitoreo y operación de toda la infraestructura física y lógica que conforma la dorsal (*backbone*) de la red CUDI manteniendo la disponibilidad, los niveles de desempeño y el óptimo funcionamiento de la red y sus interconexiones.

4.2 METAS DEL NOC-CUDI

- Mantener día a día en óptimo funcionamiento la red de CUDI
- Implantación de estándares y nuevas tecnologías en los equipos del Backbone para mantener a la vanguardia tecnológica la red de CUDI.
- Proporcionar en el backbone el esquema operativo adecuado para el alto desempeño de las aplicaciones académicas de las instituciones miembros de CUDI
- Resolución de fallas en el mínimo de tiempo posible
- Proporcionar el apoyo necesario a las instituciones miembros de CUDI para pruebas técnicas punto-a-punto
- Mantener una base de conocimientos
- Difundir conocimientos adquiridos a la comunidad de CUDI
- Difundir el estado de operación de la red

- Participación en la definición de estándares y normatividades de la operación de la red de CUDI
- En conjunto con el Comité de Desarrollo de la Red y sus grupos de trabajo desarrollar e implementar herramientas que auxilien a la correcta operación de la red

4.3 DESCRIPCIÓN DE FUNCIONES

Sus actividades aseguran una alta disponibilidad del servicio, un rápido reconocimiento de fallas y detección de niveles de degradación del servicio. Entre sus tareas se abarcan actividades de control proactivas y correctivas, así como la coordinación y apoyo en la implantación de pruebas tecnológicas con otros grupos de trabajo¹ inherentes al desarrollo de la red.

El NOC-CUDI divide sus funciones de acuerdo a recomendaciones del modelo TMN (Telecommunications Management Network) de la ITU² pero orientado y adecuándolo a las necesidades, topología, esquemas de interconexión, protocolos, tipos de redes inmersas, integración multi-vendor, multi-carrier, etc., de la red CUDI:



Fig. 1. Funciones del NOC

¹ Grupos de Trabajo de CUDI: QoS, Multicast, Seguridad, H323, VNOC, HDTV, Topología, IPv6, UPL, etc.

² International Telecommunications Union . TMN se refiere a las soluciones de administración de la red que satisfagan los estándares de la ITU-T, serie M.3000.

Despachador.- Es el punto de entrada para la recepción de solicitudes y reportes, tanto de los administradores de red como de los grupos de trabajo de CUDI. Esta área recibe la información y redirecciona las peticiones o reportes al área de operación correspondiente para su seguimiento y resolución. De esta área depende en gran medida una rápida respuesta a las fallas en virtud de la adecuada asignación del reporte.

Monitoreo.- Es el área encargada de verificar continuamente el estado operacional de la red, su funcionamiento, niveles de desempeños y detección de fallas. El área de monitoreo verifica las alarmas procedentes de la funcionalidad de los equipos, enlaces y software que conforman la infraestructura de la red, identifica mediante ellas, los posibles puntos de falla, realiza pruebas preliminares y básicas para un seguimiento necesario, oportuno y certero del área de Operación e Ingeniería de la Red.

La información extraída del monitoreo, sirve de materia prima para el desarrollo de tareas de las áreas de Administración de Software y Análisis Avanzado y Administración de Configuración; así como para otros grupos de trabajo de CUDI.

Operación/Soporte.- Se encarga directamente de realizar las configuraciones a los equipos, revisar fallas en ellos, revisar desempeños en línea, hacer cambios o revisiones de las versiones, configuraciones y se encarga de realizar los cambios requeridos por otros grupo de trabajo que soliciten para la implantación de las diferentes tecnologías. Se encarga de que el nivel de funcionamiento de la red sea el adecuado y esperado. Apoya fuertemente al grupo de monitoreo para garantizar una rápida resolución de problemas detectadas.

Administrador de Software.- Es el grupo encargado de revisar los sistemas operativos, programas y software en general de la base lógica instalada del NOC-CUDI. Controla las actualizaciones, versiones, configuraciones de los sistemas ubicados físicamente en instalaciones del NOC-CUDI y de uso exclusivo de este para la realización de sus tareas diarias.

Ingeniería de Red.- Dentro del NOC-CUDI se deben llevar a cabo algunas tareas de revisión de protocolos y adecuación de configuraciones muy específicas al funcionamiento diario de cada equipo que conforma el backbone para obtener el rendimiento y comportamiento esperado de cada uno de ellos. De la misma forma, cuando una prueba o configuración particular es solicitada por alguno de los grupos de trabajo del CDR, se coordinan con el grupo de ingeniería de la red del NOC-CUDI, se revisa y afinan los detalles técnicos por ambas partes hasta dejar a punto las configuraciones necesarias para la funcionalidad requerida. Lo mismo sucede para implantar una nueva tecnología o funcionalidad en la red.

Análisis /Configuración.- Este grupo se encarga de revisar a detalle los desempeños de los equipos del backbone; apoya al 100% al grupo de ingeniería de la red y a otros grupos del CDR; mayormente al grupo global de análisis existente. Su trabajo es buscar posibles deficiencias y mejorías en la operación tanto de los equipos como de las configuraciones, saca estadísticas básicas y gráficas de funcionamiento de la red, información que aporta a grupos responsables de la normatividad. Deduce y modela posibles afectaciones, así como trabaja en visionar comportamientos a corto y largo plazo del backbone de acuerdo a la información actual registrada, realiza maquetas de estrés y posibles nuevas configuraciones. Define e implanta en conjunto con el grupo de Ingeniería, las configuraciones apropiadas y adecuadas para los equipos del backbone.

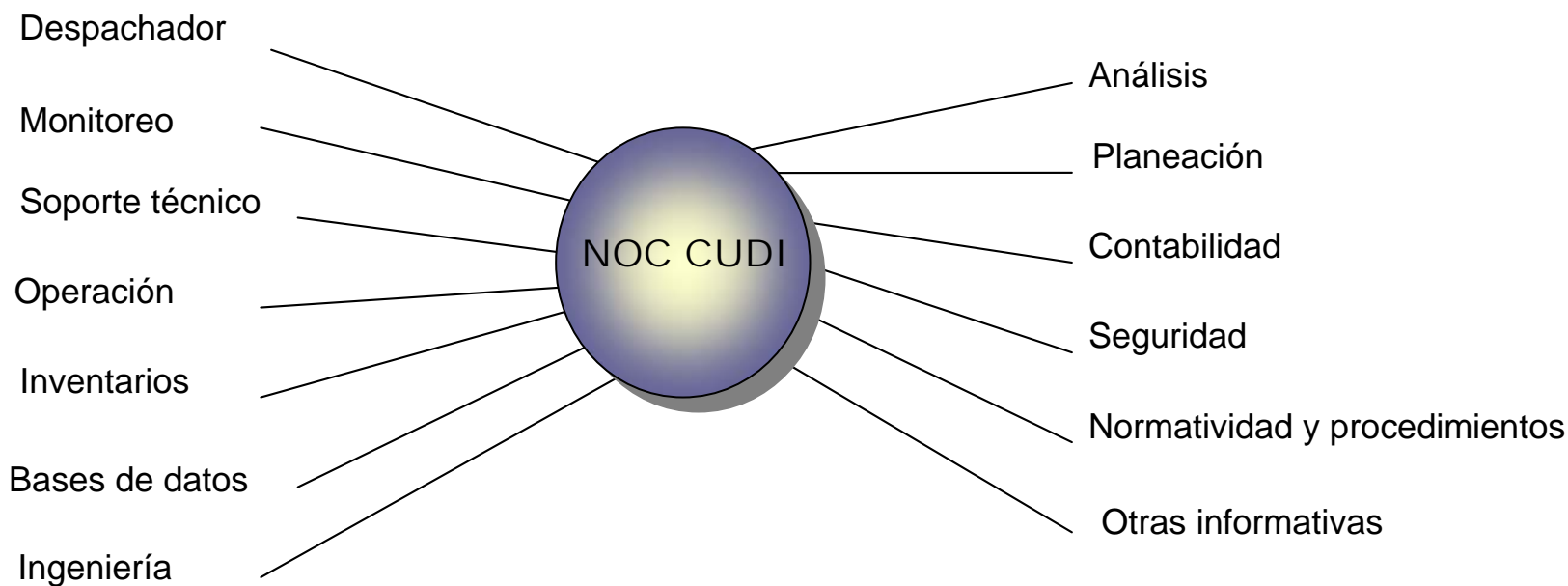
Con estas funciones se pretende; además de cubrir amplia y conjuntamente las actividades técnicas de la red, propiciar un adecuado flujo de soporte operativo hacia y desde otros NOCs inherentes a las interconexiones -de las instituciones académicas u otras NRENs (National Regional Education Networks)- ; cumpliendo el papel de apoyo para los administradores de red de cada institución asociada al proyecto.

Aunado a sus responsabilidades directas, el NOC deberá también contribuir directo, parcial o eventualmente con el resto de los grupos del Consejo y Comité de Redes de CUDI encargados de análisis, planeación, seguridad, procedimientos y pruebas de tecnologías emergentes, normatividad, aplicaciones, topología, etc.

Fig. 2. Actividades contributivas

ACTIVIDADES DIRECTAMENTE
INMERSAS

ACTIVIDADES DE SOPORTE A OTROS
GRUPOS DE TRABAJO



4.4 IDENTIFICACIÓN Y DEFINICIÓN DE LOS ELEMENTOS A OPERAR

Los elementos que se identifican como parte del alcance y compromisos de su cuidado y operación por parte del NOC-CUDI, son aquellos que conforman la dorsal de la red; dispositivos físicos y lógicos que permiten la integración y comunicación de las instituciones nodos asociados miembros de CUDI entre sí; así como su interconexión hacia otras redes. Esta definición contempla los elementos actuales, y aquellos que existan a futuro, debido a cambios o crecimientos en la red.

De acuerdo a esta definición, los elementos actuales (en el tiempo de desarrollo de esta tesis) bajo administración y operación del NOC-CUDI que correspondería se dividen en:

Infraestructura

Todos aquellos equipos, en hardware y software que reciben algún tipo de conexión

Enlaces

Todos los medios de transmisión que interconectan la infraestructura y servicios

Servicios

Actividades y funciones que proporcionan la operación de la red

Podemos identificar cada elemento a considerar resumido en la Tabla a continuación:

INFRAESTRUCTURA	<ul style="list-style-type: none"> ◆ 4 Carrier-Switches Cisco BPX 8600 ◆ 4 Backbone-Routers Cisco 7200 ◆ Conectan 4000 kms de fibra que conectan 6 enlaces de Backbone STM1´s y 11 enlaces asociados E3´s. ◆ 1 conexión a nodo Cisco 7200 para enlaces VPN 	TELMEX
	<ul style="list-style-type: none"> ◆ 2 Ruteadores Carrier-Class Cisco GSR10K ◆ 1 Ruteador Cisco 7200 NP4 ◆ Conectan 4000 kms de fibra que conecta 5 enlaces de Backbone STM1´s y 9 enlaces asociados E3´s 	AVANTEL
ENLACES	<ul style="list-style-type: none"> ◆ Enlace de Interconexión Avantel-Telmex ◆ Enlace Internacional Tijuana-San Diego (enlace físico) ◆ Enlace Internacional Cd. Juárez-El Paso (enlace físico) ◆ Enlace Internacional Monterrey-Houston (enlace físico) ◆ Enlace Tijuana-San Diego Supercomputer Center (enlace lógico) ◆ Enlace Tijuana-CENIC (enlace lógico) ◆ Enlace Tijuana-Abilene nodo Los Ángeles (enlace lógico) ◆ Enlace Internacional Cd. Juárez-Abilene, nodo Houston (enlace lógico) ◆ Enlace Internacional Monterrey-vBNs nodo Houston (enlace lógico) ◆ 22 Enlaces asociados E3´s de nodos de agregación ◆ Administración de 22 conexiones lógicas de tránsito a redes I2 internacionales. ◆ Monitoreo de enlaces afiliados 	
	<ul style="list-style-type: none"> ◆ Nodo de interconexión a red CLARA (Red regional I2 latinoamericana) ◆ Nodo de interconexión de CLARA a red Europa POR EL PROYECTO @LIS 	PROXIMAMENTE
SERVICIOS	<ul style="list-style-type: none"> ◆ Administración de la pagina NOC-CUDI de soporte técnico www.noc-internet2.unam.mx 	

Tabla 1. Elementos actuales bajo la responsabilidad del NOC-CUDI:

Podemos identificar en forma general en la dorsal de la red la ubicación e interconexión de estos elementos:

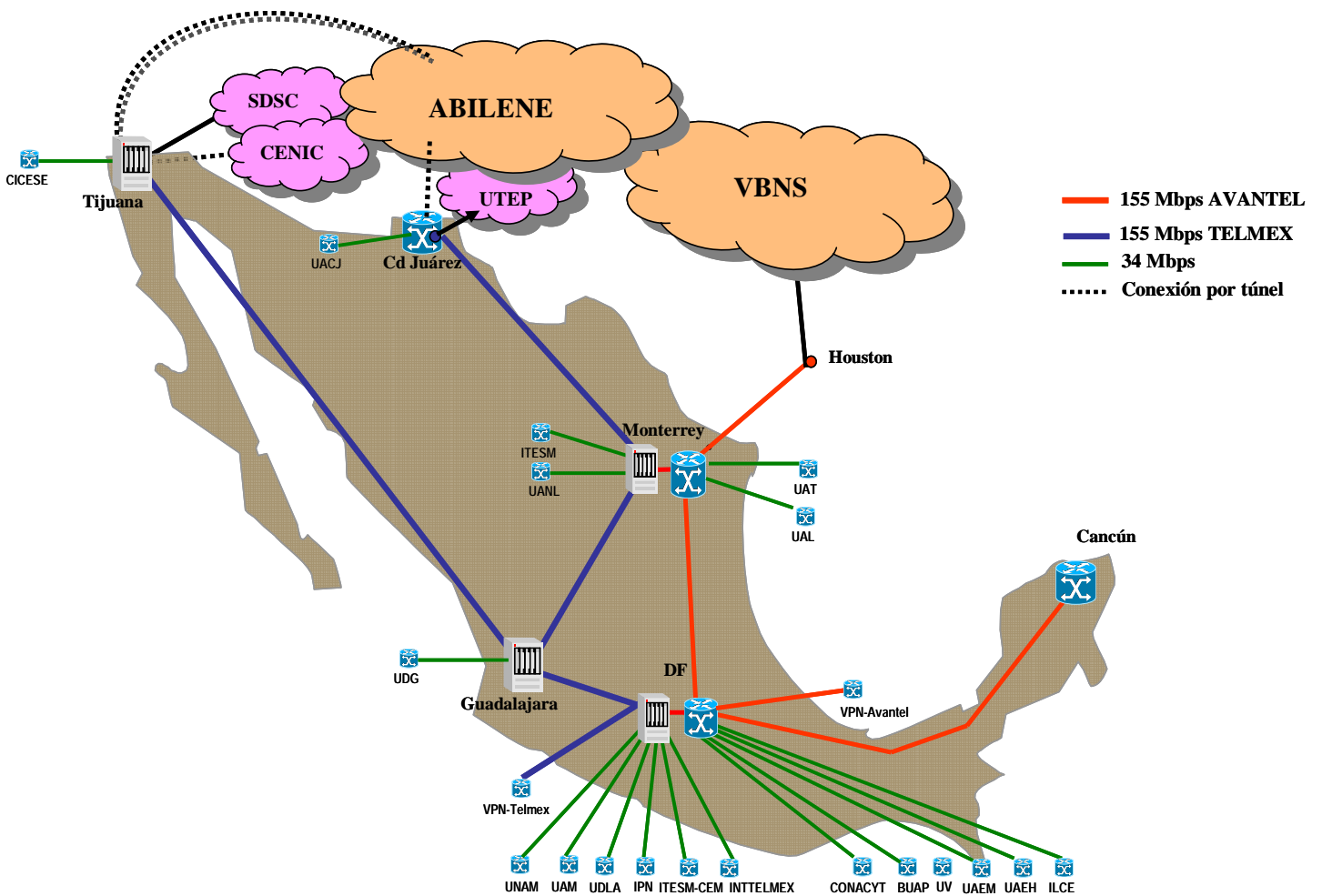


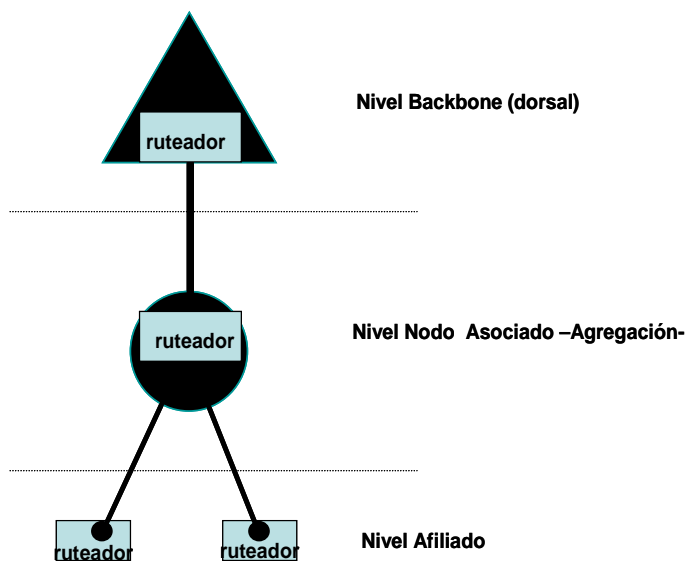
Fig. 3. Backbone CUDI

4.5 DESCRIPCIÓN DEL ESQUEMA DE OPERACIÓN DEL NOC-CUDI

El rol del Centro de Operación es fungir como el punto central y coordinador de las actividades de operación la red, distribuir y repartir, a su vez desde un solo punto el tratamiento de problemas. El usuario deberá dirigirse a una sola ventanilla de servicio, tener un punto único de contacto hace más fluida y amable su visualización de la operación de CUDI.

La operación global de la red CUDI esta basada en servicios IP y respeta su topología jerárquica:

- Nivel de Dorsal
- Nivel de Asociación o agregación (a través de nodo asociado o vía VPN)
- Nivel de Afiliado



Cada nivel de la red, especifica un tipo de conexión con características físicas propias pero todas las conexiones mantienen un punto de acceso a la red cuyo punto terminal es un ruteador.

Definir y dividir los alcances de la operación en estos niveles permite sumar esfuerzos y compartir las responsabilidades entre el NOC-CUDI y los grupos

de operación de las otras instituciones miembros de la red, logrando su inclusión directa en las tareas operativas y de esta forma verse beneficiados, creciendo todos en experiencia en la ingeniería de redes.

4.5.1 Alcances

Desde el panorama físico de los niveles de conexión, están bajo los alcances del NOC-CUDI:

La administración, control, configuración y operación del nivel de dorsal y cubre todos aquellos elementos que conforman el backbone de la red, sus enlaces y conexiones directas nacionales e internacionales y todas aquellas circunstancias inherentes a su operación.

La operación y monitoreo del nivel asociado, desde la interfase del ruteador hasta el enlace que conecta a la institución asociada al backbone de CUDI.

El monitoreo y revisión del estado global (visto como elemento global) de los ruteadores intermedios que conectan servicios hacia el Backbone de CUDI: el ruteador de la institución asociada, de la NREN internacional, del servicio VPN del carrier.

El monitoreo y revisión del estado funcional del ruteador del nivel afiliado

El servicio de red Internet 2 completo de CUDI

4.5.2 Estructura funcional Interna Y Actividades

Siguiendo la practicidad del esquema TMN, la división de tareas en el NOC-CUDI facilita el manejo de la red y establece una operación eficiente e integridad de todos los dispositivos que conforman el Backbone de CUDI; dando un marco definitorio a las actividades inmersas a su operación. Los grupos que conforman el NOC-CUDI son:

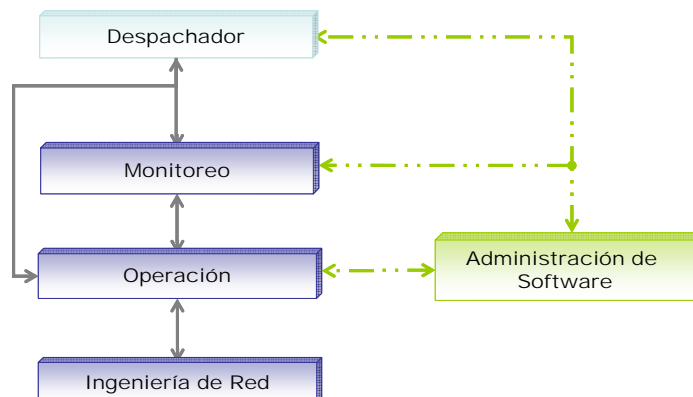


Fig. 4. Esquema funcional interno

Definición de actividades

- Monitoreo:

El monitoreo es una de las partes fundamentales de la administración de las redes. Sus tareas comprenden, entre otras cosas, la extracción e interpretación de datos relacionados con el estado y el desempeño de los dispositivos conectados a la red. Mediante su correcta interpretación, y llevando un registro histórico de los acontecimientos que se van dando a lo largo del tiempo, el administrador de red podrá determinar de manera más rápida el comportamiento de ciertos equipos e incluso, adelantarse y predecir el deterioro del nivel de servicio en alguna parte de la red.

Para poder realizar esta tarea, el NOC-CUDI cuenta con sistemas de monitoreo que trabajan las 24 hrs. del día bajo el ambiente cliente-servidor, permitiéndonos manejar de manera distribuida el tráfico generado, de manera natural, por los sistemas de monitoreo tradicionales y basados en SNMPv1, SNMPv2, SNMPv3 y RMON, (MIB, MIBII).

El monitoreo de la red alcanza:

- o Los equipos y elementos del backbone, descritos en la sección 4.1 y la Tabla 1,

o los equipos, procesos y servicios de interconexión I2 (de acceso a CUDI) de cada nodo asociado (universidades, institutos, etc.) descritos en la sección 4.1.

o los procesos o actividades de los elementos de la Tabla 1

- Tarificación:

Otra tarea importante que se lleva a cabo en el NOC-CUDI, se refiere a contabilizar el tráfico y otros datos generados por los elementos y enlaces que conforman el backbone de Internet 2. Los sistemas de monitoreo recolectan esta información diariamente para ser almacenada en una base de datos que será accesada por los diversos programas y sistemas de los grupos de trabajo de CUDI con la finalidad de generar información útil y manejable para diferentes objetivos analíticos o de difusión.

- Generación de estadísticas:

En base a los datos monitoreados y coleccionados se proporcionarán estadísticos de primera fuente en tiempos reales e históricos del comportamiento de la red. Estos informes se ubican en dos niveles: las estadísticas abiertas al público y las estadísticas de aspecto restringido y con información confidencial para los administradores de cada red que pertenece al proyecto.

Para apoyo a los administradores de cada red de CUDI que así lo soliciten, se generarán estadísticas de desempeño de enlaces, desempeño de equipos y capacidades.

- Administración y Configuración de equipos de backbone:

Se administran y realizan las configuraciones de operación para cada equipo mencionado en la Tabla 1. Dado que estos equipos son los encargados de conformar los pops, enlazar e interconectar a los nodos de las diferentes universidades que participan en este proyecto, es importante también configurar las interoperabilidades necesarias para permitir la comunicación entre estos, así como su comunicación hacia las redes Internet 2 internacionales.

El NOC-CUDI se encargará de cuidar bajo recomendación que cada nodo conectado al backbone respete en su configuración y funcionalidad los esquemas topológicos, de operación, de configuración y de estándares aceptados para la red CUDI a través del Comité de Red de esta organización, de no cumplir con las especificaciones demandadas por el CDR, el NOC-CUDI notificará inicialmente a la institución en cuestión y en paralelo al CDR para que se tomen las medidas pertinentes.

- Seguridad

Otra actividad es la de mantener la seguridad fundamental de los equipos de la dorsal, proporcionar las configuraciones de seguridad que garanticen la confiabilidad de estos equipos. Dentro de esta actividad se contempla el trabajo en conjunto con el grupo de seguridad de CUDI y pruebas tecnológicas de hardware y software de seguridad para el backbone, como son *firewalls* y listas de acceso. No se refiere a la seguridad de los equipos de los asociados, ni de las aplicaciones ya que éstas son revisadas por otros grupos de trabajo del CDR.

En el NOC-CUDI se manejan registros de todos los cambios que realiza cada ingeniero de soporte dentro de los equipos de backbone.

- Recepción y seguimiento de reportes (Troubleshooting):

El NOC-CUDI realiza la atención de reportes de acuerdo a una división tipográfica: de fallas, de pruebas, de implantación o de información.

Tipos de reportes

Reporte de Falla. Una falla en la red, significa que su servicio se está viendo afectado en cualquiera de sus elementos por alguna circunstancia interna o externa a la misma y no cumple las expectativas y niveles de efectividad que se demandan; considerando que cualquiera de sus elementos y dispositivos no se desempeña como se espera y que por lo tanto se le debe poner atención hasta que se normalice su funcionamiento. El NOC-CUDI se encarga de minimizar el número de fallas y reducir el tiempo de resolución de las mismas.

Solicitudes de pruebas y de implantación. Éstas deberán ser solicitadas con el respaldo de un preestudio y diseño de la misma y serán revisadas por el NOC-CUDI y el (los) grupos de trabajo inmersos para su mejor desarrollo.

Reportes informativos. Son aquellos que requieren datos particulares y pueden ser atendidos por el NOC-CUDI o redireccionados al área adecuada para su seguimiento.

Cada uno de estos tipos de reportes maneja relevancias, prioridades y escalaciones diferentes.

Las actividades básicas a desarrollar durante el seguimiento de reportes son:

- o Detección o recepción
- o Diagnóstico
- o Determinación
- o Resolución

Para la primera parte, que es la **detección**, se cuenta con sistemas que despliegan en monitores, de manera gráfica o textual, los problemas existentes en la red. O bien, para cuando el staff del NOC-CUDI no se encuentra atendiendo a sus consolas, se utiliza un sistema que "redirecciona" estos mensajes de alarma a los correos electrónicos o inclusive a los localizadores de los operadores.

El NOC-CUDI garantiza la disponibilidad del servicio de atención de fallas, de acuerdo a su prioridad, a través de diferentes tipos de herramientas las 24 Hrs. del día, los 365 días del año.

El **diagnóstico** de un reporte se realiza de manera un poco más compleja. Aquí intervienen una serie de herramientas –basadas en hardware y software- de apoyo que inicialmente proporcionan información necesaria para su seguimiento y determinar la causa de su efecto. Para tener la idea precisa de lo que se trata **-determinación de la falla-** cuenta mucho la experiencia del staff del NOC-CUDI y de la ayuda de los sistemas de manejo de reportes, que llevan la historia de los casos resueltos con anterioridad. Estos sistemas cuentan con bases de conocimiento que se van

enriqueciendo con las experiencias de los operadores que constantemente resuelven problemas en la red, y nos pueden proporcionar información relativa a la *resolución* de problemas recurrentes.

Con esto, se garantiza la rápida solución de los problemas que se presentan comúnmente en las redes de datos.

- Documentación y difusión:

Esta actividad representa una de las principales actividades ya que se completa el compromiso del NOC-CUDI al dar una continuidad e históricos para una base de conocimientos que sirvan de apoyo a las tareas diarias del NOC-CUDI y a todos los grupos del CDR sirviendo incluso de complemento en el crecimiento profesional y de la formación de recursos humanos. De la misma forma está el difundir el estado de la red, experiencias obtenidas y conocimientos técnicos especializados que a las personas relacionadas con el manejo de redes de datos puede interesar.

El NOC-CUDI elaborará y proporcionará documentación que pueda apoyar a cada institución conectada a la red de CUDI de operaciones, configuraciones, desempeños, etc. De enlaces, estándares, equipos y configuraciones previamente probadas en el NOC-CUDI.

Algunos de los reportes emitidos son:

- Reporte Técnico Semanal de Eventos

- Reporte Ejecutivo Mensual del estado de la red

- Anuncios preliminares de cambios, pruebas, mantenimientos e instalaciones agendadas

4.5.3 Esquema Funcional Externo (Flujo Operativo Externo)

Se refiere al esquema funcional y de interacción hacia y desde el NOC-CUDI de los grupos externos de operación, es decir, quienes y como interactúan con éste:

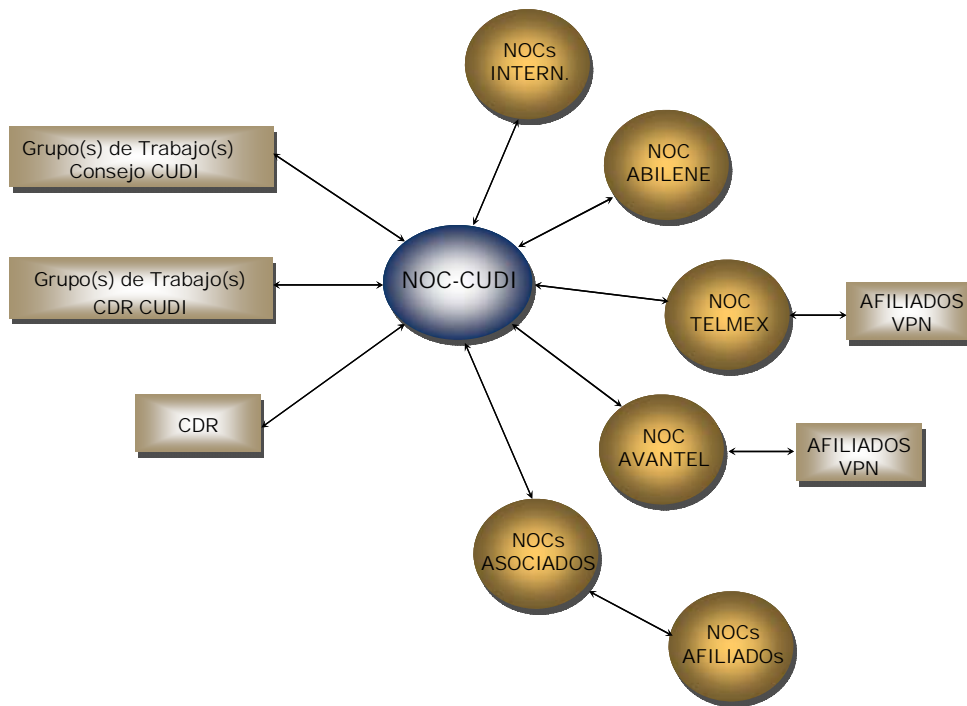


Fig. 5. Esquema funcional externo

Las entidades que interactúan directamente y en primer nivel con el NOC-CUDI son:

El Consejo de CUDI

EL Comité de Redes de CUDI

los centro de operación de las instituciones de nodos asociados,

los centros de operación de NRENs (National Regional Education Networks)

los centros de operación de interconexiones internacionales

los grupos de trabajo del CDR de CUDI

los grupos de trabajo de Comité de Aplicaciones de CUDI

los centros de operación de carriers proveedores

El NOC-CUDI fungirá como directriz entre estos centros de operación para el desarrollo de la operación de la red y apoyará a otros centros o agrupamientos que lo soliciten. De la misma forma difundirá información del estado de la red hacia entidades como el Consejo de CUDI, el CDR, los grupos s de trabajo, etc.

De esta forma se fomenta un flujo adecuado de información y seguimiento de actividades entre entidades involucradas.

Los nodos afiliados contactarán a los centros de operación de su nodo asociado y los enlaces vía VPN al centro de operación del carrier proveedor del servicio. Sin embargo, podrán solicitar el apoyo del NOC-CUDI en el momento que lo requieran.

4.6 RESPONSABILIDADES DE LAS ENTIDADES

Basándonos en las descripciones de los puntos desarrollados en el presente documento, se definen las siguientes responsabilidades:

4.6.1 Del NOC-CUDI

Conformar y mantener una planta de personal eficiente, profesional, robusta y de altos conocimientos para la realización de las tareas del NOC

Diseñar e implantar la estructura de trabajo del Centro de Operación de CUDI robusto que cumpla con cada uno de los objetivos y metas

Proporcionar un esquema de recepción, seguimiento y resolución de problemas en el servicio de la red de CUDI eficiente y a satisfacción del usuario

Configuración y administración de los equipos del backbone

Administración de cambios y crecimientos en la red

Monitoreo y operación de los equipos y enlaces del backbone

Seguridad en los equipos del backbone

Proporcionar los niveles adecuados de operación y desempeño de la red

Mantener la prospección tecnológica en el backbone de CUDI

Difundir los estados operacionales de la red

Proporcionar herramientas de prueba y difusión a los usuarios

Establecer los procedimientos para sus actividades

Apoyar al usuario en las dudas e inquietudes de su propia conexión al backbone

Apoyar al usuario en dudas e inquietudes de su conexión a Internet 2 internacional y en caso necesario coordinar actividades entre puntas finales de dicha comunicación

Probar nuevas herramientas operativas para implementarlas en el ambiente real de operación

Gestionar y coordinar las actividades de pruebas, operación, falla, etc. en que participen diferentes entidades

Participar en los diferentes foros de discusión y desarrollo que involucren la tecnología y operación de la red CUDI

Participar en la definición y elaboración de Políticas de Uso Aceptable, Acuerdos o Diseños Técnicos de colaboración, conexión e intercambio que involucren en algún aspecto la tecnología y operación de la red CUDI

Mantener el acercamiento continuo con los encargados de los diferentes NOCs de las instituciones asociadas.

4.6.2 De los centros de operación de los nodos asociados

Contar con personal destinado a la operación de I2 de su institución, proporcionar datos completos (Nombre, teléfono, dirección postal, correo electrónico. Estos contactos son los contactos para el NOC-CUDI.

Proporcionar información actualizada de su red: esquema de ruteo externo, direccionamientos asignados, direccionamiento anunciado a Internet 2, información básica del esquema de ruteo interno

Mecanismos y procedimientos de operación, reporte de fallas, contactación y escalación

Proporcionar apoyo, soporte y asesoría técnica a sus nodos afiliados

En caso de alguna eventualidad en uno de sus nodos afiliados, el asociado deberá establecer contacto con el NOC-CUDI para reportar el problema y fungir como punto de enlace

El nodo asociado se compromete a mantenerse informado y participativo en todas y cada una de las actividades realizadas entre sus nodos afiliados y el NOC-CUDI

Proporcionar apoyo al NOC-CUDI para la detección, seguimiento y resolución de reportes que se refieran a su conexión o al servicio de otra entidad donde el se vea implícito.

Proporcionarle al personal del NOC-CUDI una cuenta de acceso a su equipo (ruteador) de conexión a CUDI con permisos de lectura y aplicación de comandos de prueba, con la finalidad de que éste pueda contar con un apoyo en la resolución de las fallas del nodo. No se requiere permisos mayores en ningún momento. Si el nodo asociado no proporciona este acceso, deberá entonces instalar una herramienta tipo *“proxy-router”* que cumpla con los mismos objetivos.

Implantar herramientas de pruebas básicas (ping, traceroute, mrtg, etc) para su equipo I2 y permitirle al NOC-CUDI su utilización de manera que apoye las actividades de operación de la red CUDI.

Proporcionar apoyo al NOC-CUDI para la realización de pruebas de desempeño punto-a-punto

Proporcionarle al NOC-CUDI la información técnica necesaria que se le solicite y que sirva para apoyar el seguimiento y realización de las tareas de operación de la red CUDI.

Respetar las Políticas de Uso Aceptable del NOC-CUDI

Proporcionar información de retroalimentación al NOC-CUDI que permita mejorar y robustecer sus sistemas de operación

Dar seguimiento a sus reportes con el NOC-CUDI, hasta su conclusión, no deberá dejar ningún reporte resuelto abierto.

Dar aviso al NOC-CUDI a través del mecanismo definido por éste, de cambios, mantenimientos, pruebas, fallas, y cualquier actividad que afecte su conexión o la de sus afiliados a la red Internet 2.

4.7 CONTACTO AL NOC-CUDI

4.7.1 Quienes pueden contactar al NOC-CUDI

Para información general, cualquier persona puede tener acceso o contactar al NOC-CUDI. Pueden tener acceso a la información pública de la red Internet 2 proporcionada a través de la página del NOC-CUDI o contactarlo para solicitar información general de la red, de sus miembros o de Internet 2 o incluso para solicitar el apoyo del NOC-CUDI como intermediario en la resolución de algún problema.

Para aspectos relacionados con la administración y operación de la red, atención de fallas, atención de cambios, atención de pruebas, mantenimientos y reportes, solo tendrán acceso los consejeros, administradores y responsables de operación de cada institución miembro de CUDI **plenamente registrados y reconocidos** ante el NOC-CUDI:

Miembros del consejo de CUDI,

Miembros del Comité de Redes de CUDI (CDR),

Administradores y operadores de las redes de las instituciones asociadas,

Administradores y operadores de las redes de las instituciones afiliadas

Administradores y operadores de las redes de interconexión internacional de CUDI (NRENs)

Coordinadores de los grupos de trabajo del CDR de CUDI

Coordinadores de los grupos de trabajo de Comité de Aplicaciones de CUDI

Personal de los centros de operación de carriers proveedores de CUDI

Los accesos a la información o al nivel de contacto de CUDI están definidos de acuerdo al perfil del usuario.

Para más información puede referirse a las secciones 4.3 y 5.2.

Para información de cómo registrarse en el NOC-CUDI, referirse a la sección 7.4. **“Procedimiento de Registro de Contactos en el NOC-CUDI”**

4.7.2 Medios de Contacto.

El NOC-CUDI cuenta con alternativas de contacto bajo diferentes perspectivas de prioridad para los diversos tipos de eventos de la red. Dependiendo del tipo de evento, se atenderán con la cobertura y herramientas necesarias que el NOC-CUDI proporciona.

Telefónico: Número telefónico único

TELÉFONO 56228869

Página WEB: El medio de contacto mas completo para abertura de reportes, información o contactar al Despachador es a través de la página del NOC-CUDI:

www.noc-cudi.unam.mx

A través de esta página se puede abrir un reporte, solicitar un servicio, todos los reportes son registrados e identificados con un número.

Además, en esta página se puede acceder a las herramientas de pruebas y apoyo para los administradores de red, cuenta con herramientas como *proxy router*, *ping*, *traceroute*, *show ip route*, gráficas de desempeño, anuncios de eventos, escalaciones, etc. Los reportes abiertos a través de la página se apoyan en mecanismos automatizados para manejo de prioridades, urgencias, escalaciones, notificaciones grupales, etc.,

Correo de Voz: Para mayor apoyo en el contacto vía telefónica se cuenta con un sistema de correo de voz. De estar ocupado el teléfono, no contesten, etc., el usuario podrá dejar un mensaje en el buzón. En una pantalla aparecerá la notificación de que se ha recibido una llamada y también se enviará de manera automática una notificación al Despachador y/o radiolocalizadores de los ingenieros de soporte.

Correo Electrónico: Se puede reportar o contactar al NOC-CUDI vía correo electrónico enviando un mensaje a:

noc@internet2.unam.mx

Se da la opción al usuario de que se le notifique automáticamente del envío de su correo a su radiolocalizador.

Mensaje a radiolocalizador: El usuario puede enviar su reporte al Despachador vía mensajes a radiolocalizador. Este medio también puede ser usado para un ingeniero de soporte específico o al grupo completo del NOC-CUDI.

Dentro de cada herramienta de contacto se puede especificar el nivel de urgencia del mensaje.

Todos los contactos al NOC-CUDI son registrados en bitácora.

4.7.3 Horario

El conjunto de estos mecanismos y herramientas ofrecen una disponibilidad del NOC-CUDI de 7x24 los 365 días del año. Véase en las descripciones de las actividades específicas mas detalle de las variables de los horarios.

- Horario Normal

De 10:00 a 20:00 hrs. (Hora Central-GMT-) De Lunes a Viernes. Se opera en el sitio del centro de operación con todas las herramientas habituales: página WEB, correo electrónico, teléfono, pager, etc., como medios de contacto.

Horario agendado. Cualquier institución puede agendar, bajo previa solicitud, la cobertura del personal del NOC-CUDI en el centro de operaciones en cualquier horario que esta lo necesite para cubrir algún evento o darle seguimiento a un reporte o prueba. Véase sección 7.6 **“Procedimiento para que el usuario agende eventos en el NOC-CUDI”**

- Horario Extendido

Es el horario que no cubre el horario normal, sábados, domingos, días festivos, vacaciones, etc. En este horario se atenderá a través de guardias del personal y herramientas de apoyo vía red: correo electrónico, WEB, pager y teléfono celular, de acuerdo al tipo, nivel y prioridad del problema.

Cualquier prioridad que amerite la cobertura en sitio fuera del horario normal, será atendido a la brevedad por personal del NOC-CUDI quien(es) se desplazarán al centro de operación.

4.8 ADMINISTRACIÓN DE FALLAS

4.8.1 Objetivo

Las actividades del NOC-CUDI son variadas y una de ellas está la de atender y resolver los problemas de comunicación y problemas que puedan resultar dentro del funcionamiento entre:

Instituciones asociadas o afiliadas conectadas a la red CUDI

Instituciones asociadas o afiliadas de CUDI hacia cualquier red de interconexión internacional de Internet 2 (Abilene, Canarie, GEANT, etc)

Instituciones asociadas o afiliadas de CUDI hacia cualquier otra institución conectada a una red Internet 2 internacional

El backbone de CUDI hacia redes de interconexión internacional de Internet 2

El backbone de CUDI hacia cualquier otra institución conectada a una red Internet 2 internacional

4.8.2 Sistema de Detección de Fallas

Dentro del NOC existen herramientas para poder detectar en forma reactiva o proactiva problemas en la red.

La *detección proactiva* es aquella que mediante el monitoreo, revisiones y análisis cotidianos nos permite visualizar, comportamientos que hagan predecible alguna necesidad o problema, a corto o largo plazo, en el servicio de la red o en cualquiera de sus elementos y permita trabajar anticipadamente sobre estas necesidades.

La *detección reactiva* es aquella que reacciona ante alguna fluctuación en la operación del servicio de la red o cualquiera de sus elementos y que afecta los niveles de operación necesarios para el funcionamiento de los servicios.

Entre las herramientas actuales de apoyo para detectar fallas en la red se encuentran: Cisco View, Cisco WAN Manager, MRTG, CGI's, etc.

También el usuario puede detectar alguna anomalía en la red desde sus propios centros de control o a través de la notificación de algunos de sus usuarios internos y deberá reportarla al staff del NOC-CUDI.

Ya sea por parte NOC-CUDI o por parte del usuario, cualquier eventualidad en la red deberá ser reportada al NOC-CUDI.

Detección por parte del NOC-CUDI:

- a) Se levanta un reporte del evento
- b) Se da aviso interno

Por parte del usuario:

- a) Se levanta reporte en el NOC-CUDI

Para la atención de reportes y fallas se describe en la sección **“Procedimiento de Atención y Seguimiento de Reportes”** y se atenderá de acuerdo a su nivel de gravedad (Tabla 4 “Manejo de escalación”).

4.8.3 Inventario de Problemas

Se deben establecer un inventario de problemas inicial e ir alimentando esta base de conocimientos conforme la operación diaria de la red vaya comportándose, podemos iniciar con los siguientes ejemplos:

4.8.4 Sistema de Atención y Seguimiento de Reportes.

Existe un sistema de seguimiento de cada uno de los problemas que puedan estar afectando a la red y todos los eventos llevan un seguimiento, registrando todas y cada

una de las actividades que se están realizando para resolver el problema. Este procedimiento inicia a partir de la recepción del reporte.

El sistema permite el registro del reporte, priorizarlo, notificar, atenderlo, revisar su seguimiento, escalarlo y almacenarlo para su uso en estadísticas o reportes de operación y está programado para poder realizar acciones o tareas automatizadas según sea el tipo o gravedad del reporte.

Todas y cada una de las instituciones miembro de la red de CUDI tendrá un identificador único en el Sistema de Atención y Seguimiento de Reportes –ID-RED-.

A los contactos técnicos oficiales ante el NOC-CUDI, se le proporcionará un identificador de usuario -ID-USUARIO- que servirá de cuenta de acceso (*login*) y una contraseña (*password*) para poder realizar reportes, consultas, etc. Este es un área restrictiva y se les solicitará al usuario que siempre tenga a la mano su contraseña. Si la olvidó o requiere cambiarla puede hacerlo a través de la página o contactando directamente al NOC-CUDI (esta acción es considerado como un reporte y se le enviará al usuario su nueva contraseña vía correo electrónico).

Cualquier otra consulta general del sistema de reportes podrá ser consultado sin restricción.

Una vez introducido un reporte en el sistema, este no puede ser borrado y será almacenado en la base de datos para su tratamiento.

Un problema particular en el servicio de la red sólo podrá ser reportado una sola vez por el mismo usuario.

Cualquiera que sea el método de contacto que se use para reportar un problema, se ejecuta de manera automática un proceso que suministra este reporte al sistema de reportes, de esta manera:

si se realiza un reporte vía telefónica, el despachador interrogará al usuario para llenar el formato del reporte y suministra este al sistema y se inicia el seguimiento.

Si reporta a través de la página del NOC-CUDI, el propio usuario deberá llenar el formato y suministrar el reporte, se inicia el seguimiento.

Si se reporta a través de correo electrónico, al recibirlo el sistema, automáticamente abre un reporte, regresa por la misma vía un número de reporte al usuario, lanza una

notificación al personal del NOC-CUDI, quien se contactará con el usuario para pedirle los datos completos del problema.

Si se reporta vía radiolocalizador, el mensaje es recibido por el sistema, automáticamente abre un reporte, regresa vía correo electrónico (de ser posible) un número de reporte al usuario, lanza una notificación al personal del NOC-CUDI, quien se contactará con el usuario para pedirle los datos completos del problema. Si no fuera posible notificar al usuario su número de reporte vía correo electrónico, el personal del NOC-CUDI se lo proporcionará directamente.

El usuario puede consultar el estado de los reportes a través de la página del NOC-CUDI (www.noc-internet2.unam.mx) o el mismo NOC-CUDI estará notificando periódicamente al usuario el estado de su reporte hasta que este sea resuelto.

- Reporte del usuario

El usuario tiene varios caminos para poder reportar un problema en el servicio de la red, ya sea vía telefónica, página WEB o correo, descritos el horario y los métodos de contacto en la sección 6. En todos los casos, al momento de reportar el problema, el usuario recibirá un número de identificación del reporte (NR) y con este deberá consultar su seguimiento en el transcurso de la solución.

Es importante mencionar que el contacto válido ante el NOC-CUDI para reportar alguna falla en la operación de la red CUDI es el administrador o contacto técnico registrado ante este de acuerdo a la sección 6.1 y este contacto deberá proporcionar su identificador y el de su institución.

- Número de Reporte

El formato completo del NR o número de reporte es:

aammdd - ####

donde:

IDENTIFICADOR	CONCEPTO	USO
Aammdd	Es la fecha (últimos 2 dígitos de año, mes, día).	Solo es necesaria y utilizada por el NOC-CUDI para almacenamientos y procesamientos de la información, históricos, estadísticas, etc.
####	Es un número secuencial, creciente que se le da al usuario para identificar su número de reporte ante el NOC-CUDI. Se reinicializa anualmente.	Es el número de reporte que se le da al usuario.

Tabla 2. Identificador de Número de Reporte

Ejemplo de NR:

031117-184 Se le indica al usuario que su número de reporte es el 184 y se registra en la base de datos como un reporte del 17 de Noviembre de 2003.

La asignación de los reportes para ser atendidos por el personal del NOC-CUDI es bajo un proceso de *round-robin*³ por lo que son repartidos y atendidos de una forma mas eficiente y tratando de que todos los miembros del NOC-CUDI tenga la misma carga de trabajo.

Todos los reportes son registrados y almacenados en las bases de datos para cualquier cómputo, análisis y tratamiento necesario de los datos para ser usados en la misma operación o reingeniería de la red y además para emitir información de interés de CUDI en sus diferentes niveles.

Todas las llamadas generan la asignación de un número de reporte y este solo podrá ser cerrado por el usuario cuando esté satisfecho con la resolución de su problema o duda.

³ El proceso round-robin significa que los reportes se asignan de forma cíclica,.

Todos los reportes pueden ser consultados por el usuario a través de la página del NOC-CUDI.

● Formato del Reporte (Vista inicial)

ID RED:	<input type="text"/>	ID-USUARIO	<input type="text"/>
Datos de la Institución		Datos del Responsable Técnico	
Institución:	<input type="text"/>	Apellido Paterno:	<input type="text"/>
		Apellido Materno:	<input type="text"/>
Tipo de conexión:	<input type="text"/>	Nombre(s):	<input type="text"/>
Red(es) Anunciada(s):	<input type="text"/>	Teléfono:	<input type="text"/>
		Teléfono celular:	<input type="text"/>
Equipo conectado:	<input type="text"/>	e-mail:	<input type="text"/>
DATOS DEL PROBLEMA		Radiolocalizador:	<input type="text"/>
		Puesto:	<input type="text"/>
		Escalación siguiente:	<input type="text"/>
Tipo de Problema:		<input type="text"/>	
Prioridad:	<input type="text"/>	NR	<i>aammdd-XXXXX</i>
Descripción del Problema:	<input type="text"/>	Fecha de Reporte: DD-MM-AA	Hora de Reporte: HH:MM (GMT)
SEGUIMIENTO (Bitácora):	<input type="text"/>	Estado:	<input type="text"/>

Fig. 6. Formato del Reporte

4.9 ADMINISTRACIÓN DE CAMBIOS

4.9.1 Objetivo

Apoyar y coordinar las actividades necesarias para llevar a cabo la adecuada implementación de cualquier tipo de cambio en la red que garantice acotar, en tiempo y forma, las afectaciones en la operación de la red, apoyando a los responsables de los cambios en llegar a los resultados esperados.

4.9.2 Responsabilidades

El NOC es responsable de apoyar las actividades de cambios proporcionando los mecanismos necesarios para llevar a cabo estas actividades:

- Formatos de solicitud
- Calendarización
- Revisión y aprobación del cambio
- Preparación de ambiente
- Avisos a las áreas implícitas
- Monitoreo y seguimiento de las actividades en los cambios
- Pruebas
- Notificación de resultados
- Robustecer la documentación proporcionada por el solicitante y poner en línea

El solicitante del cambio es responsable de llevar a cabo la actividad de acuerdo a:

- Preparar sus cambios con anticipación
- Conocer plenamente la actividad que desea realizar
- Contar con los elementos necesarios para realizarla
- Solicitar el cambio al NOC a través del mecanismo provisto por este
- Notificar inicio y cierre de su actividad
- La realización y seguimiento completo de la actividad
- Notificar resultados obtenidos
- Documentar la actividad en el Sistema de Control de Cambios del NOC

El responsable de la red afectada deberá dar su visto bueno para la realización del cambio.

4.9.3 Quienes pueden solicitar cambios

- NOC Universidad –Responsable(s) de la red
- Encargad –Responsable(s) de aplicación
- Universidad - Responsable(s) de equipo(s)
- Ingeniería
- Instalaciones
- Personal del NOC-CUDI

4.9.4 Quienes deben avalar las solicitudes

- En primer nivel el NOC de la Universidad miembro de CUDI
- En segundo nivel el NOC-CUDI

4.9.5 Ventanas de cambios

- Establecidas: Cambios programados cotidianos, rutinarios o no emergentes; Lunes y Jueves de 18:00 a 20:00 hrs.
- Solicitud programada: Actividad específica que requiere llevarse a cabo en algún momento en particular debido a requerimientos específicos y que percibe una mejoría necesaria para el adecuado desempeño de la red. Se deberá solicitar por lo menos con 24 hrs. de anticipación.
- Emergentes: Todos aquellos cambios solicitados para corregir una degradación o falla presente en la operación de la red. Se revisará caso por caso y se dará respuesta particular.

Se recomienda establecer el formato tal cual un reporte de fallas a través de un esquema Web a través de la página del NOC CUDI (noc.cudi.edu.mx por ejemplo) con por lo menos 24 horas de anticipación.

Es necesario que se proporcione la información requerida en cada campo del formato.

En el momento de la entrada de la solicitud, el Sistema abrirá un reporte y le proporcionará inmediata y automáticamente un número de solicitud para que el solicitante pueda revisar el estado de su solicitud posteriormente.

El Sistema deberá emitir en ese momento un aviso al NOC-CUDI de llegada de una solicitud de cambio y asimismo al encargado del NOC o encargado de la red de la Universidad miembro de CUDI que solicita el cambio con los datos incluidos.

El NOC CUDI contará por lo menos con 24 hrs. para revisar el cambio solicitado, las actividades inmersas, nivel de afectación y grupos de trabajo implícitos y proporciona al solicitante el estado de factibilidad de su petición. Solicita o retroalimenta mayor información al solicitante si es necesaria.

El NOC CUDI siempre debe pedir visto bueno del encargado de red de la Universidad solicitante para llevar a cabo esta actividad. Si el visto bueno es obtenido, es entonces que el NOC CUDI notifica al solicitante la aceptación de su cambio proporcionando los datos: calendarización, tiempo de inicio, tiempo de terminación, prepara el ambiente de la actividad y emite los avisos correspondientes a los grupos y personas implícitas sobre esta solicitud de cambio documentando todas las actividades inmersas en la actividad.

4.10 PROCEDIMIENTOS

4.10.1 Procedimiento de Avisos

El NOC CUDI emitirá notificaciones para:

- Aviso de entrada de solicitud vía un número de identificación
- Aviso de aceptación o no-aceptación del cambio solicitado a través de un correo electrónico

- Aviso a las personas o grupos de trabajo implícitos en la actividad
- Aviso de recordatorio de las actividades programadas al solicitante, grupos implícitos y al encargado de la red de la Universidad solicitante
- Aviso al solicitante de inicio y final de su cambio programado

4.10.2 Procedimiento de Registro de Contactos en el NOC-CUDI

- 1.- Contactar al NOC-CUDI vía telefónica o vía correo electrónico y solicitar su registro, deberá acreditar su representatividad ante el Comité de Redes.
- 2.- El NOC-CUDI verificará los datos con el Comité de Redes, en este caso con el Presidente del Comité y en caso aprobatorio, devolverá al usuario vía correo electrónico sus identificadores correspondientes.
- 3.- El usuario deberá corroborar la información recibida conectándose a la página www.noc-internet2.unam.mx

4.10.3 Procedimiento de Atención y Seguimiento de Reportes

Este procedimiento deberá ser conocido y seguido por el usuario.

- 1.- El usuario abre un reporte en el NOC-CUDI, anunciando un problema en el servicio de la red, a través de alguno de los siguientes medios:

MEDIO DE CONTACTO	
A través de la página	www.noc-internet2.unam.mx
A través de vía telefónica	(01) (55) (5XXXX)
A través de correo electrónico	noc@internet2.unam.mx
A través de radiolocalizador	XXXXXX
Dependiendo del método de acceso que utilice el usuario para reportar su problema, será atendido por el despachador, ya sea el sistema o una personal a cargo de este.	

Tabla 3. Medios de contacto

- 2.- Deberá proporcionar su login y password para suministrar un reporte, si abre el reporte vía telefónica, deberá tener su identificador de red.
- 3.- Validado su acceso, deberá llenar o dar los datos completos descriptivos de su problema siguiendo el formato establecido (Véase Fig. 6 Formato de Reporte).
- 4.- Al suministrar el reporte en el sistema, el despachador (personal o automáticamente) entregará al usuario un número de reporte, que identificará su reporte a lo largo de su seguimiento y hasta su resolución.
- 5.- El reporte será asignado a un miembro del personal del NOC-CUDI de acuerdo a sus características y prioridades para darle seguimiento y resolución.
- 6.- Si el reporte tiene prioridad distinta de 0, se notificará tanto al personal del NOC-CUDI como a los responsables del nivel de prioridad para su conocimiento y atención del mismo. De acuerdo al nivel de prioridad se levantarán procesos distintos de acuerdo a lo descrito en la Tabla 3 y 4.
- 7.- El usuario podrá consultar el estado de su reporte a través de la página del NOC-CUDI o vía telefónica.
- 8.- Cada eventualidad modificada o actualizada en el reporte del usuario, será notificada automáticamente vía correo electrónico a este.
- 9.- Una vez resuelto su problema, el usuario deberá cerrar el reporte a través de la página del NOC-CUDI o vía telefónica.

4.10.4 Procedimiento para control de cambios y ventanas de mantenimiento

- 1.- El usuario deberá contactar al NOC-CUDI vía telefónica o vía correo electrónico para solicitar programar un evento.
- 2.- El NOC-CUDI solicitará los datos precisos del evento a realizar por parte del usuario, de acuerdo al tipo de evento se calendarizará de común acuerdo de las partes implícitas.

3.- En dado caso que se llegará a afectar directa o indirectamente algún elemento de la red, el NOC-CUDI realizará las notificaciones pertinentes al resto de los usuarios de CUDI.

4.-De la misma forma si se requiere la intervención de algún grupo de trabajo del CDR o del Comité de Aplicaciones, el NOC-CUDI se encargará de integrar y coordinar las tareas entre los participantes.

4.10.5 Procedimiento de Escalación

Ante cualquier problemática en el desarrollo y realización de las diferentes actividades del NOC-CUDI, en que el usuario no se encuentre satisfecho o se vea afectado, éste podrá escalar sus reportes de acuerdo al siguiente diagrama de escalación:

NIVEL DE ESCALACIÓN	PRIORIDAD
Director General de CUDI	Nivel 5
Presidente de Consejo	Nivel 4
Representante ante Consejo de la Institución que alberga el NOC-CUDI	Nivel 3
Presidente del CDR	Nivel 2
Coordinador del NOC-CUDI	Nivel 1
NOC-CUDI	Nivel 0

Tabla 4. Manejo de Prioridades

Capítulo 5

CONFIGURACIÓN BASE DE OPERACIÓN DEL BACKBONE DE LA RED (DORSAL PRINCIPAL)

Es muy importante señalar que este capítulo solo resume los trabajos que se han realizado o realizados en la configuración base sin describir tecnologías o protocolos, esto debido a que no es correspondiente a esta tesis estas definiciones ya que requiere un documento más extenso y preciso por lo que se recomienda que para cualquier duda sobre las tecnologías, protocolos o definiciones se atiendan las fuentes de referencia adecuadas y que al final de este trabajo se señalen algunas.

5.1 ESQUEMA INICIAL DE RUTEO PARA LA DORSAL

El esquema de ruteo es sin duda un punto en la operación que requiere su definición analítica. De acuerdo al Capítulo 4 donde revisamos los niveles de conexión de los miembros de la red CUDI tanto afiliados como asociados, se debe establecer un esquema de ruteo adecuado que permita transacciones de datos efectivas, desempeños adecuados, optimizando los recursos de la infraestructura y también que permita una operación ordenada de la red; esto dado que cada vez se interconectan más miembros a la red y el no establecer un orden en el ruteo podría repercutir en todo el funcionamiento de esta.

La función del backbone es servir de tránsito desde la conexión de las redes de los miembros de CUDI y la red internacional de Internet 2.

Existe un grupo de trabajo de ruteo de CUDI que se encarga del análisis e implementación de los esquemas y políticas de ruteo adecuadas a la red de CUDI de cuyos trabajos mencionaremos:

Los protocolos de ruteo elegidos para la red de CUDI son:

- a) Protocolo de enrutamiento intradominio OSPF (Open Shortest Path First).
- b) Protocolo de enrutamiento interdominio BGP

Esta selección se basa en que se trata de protocolos estándar y de recomendación de la IETF para redes de gran desempeño y tamaño.

a) Protocolo de enrutamiento intradominio OSPF. Este protocolo fue desarrollado por la IETF como reemplazo del protocolo RIP y se trata de un protocolo de computación abierta estándar. Su versión más reciente es la recomendación descrita en el RFC 2328. Su mayor ventaja es su rápida convergencia y soporte de redes de gran tamaño.

Para que el protocolo fuera verdaderamente eficiente se debe establecer un esquema jerárquico basado en definición de áreas de dominio y realizar sumarización de rutas entre estas áreas. Con la sumarización se evita anunciar rutas o información de ruteo innecesarias en la dorsal. Si se logra que las áreas sean continuas se puede realizar el anuncio a un grupo de redes simultáneamente.

Todos los equipos de la dorsal pertenecen a la misma área dado que no son muchos y no se prevé un crecimiento en número de gran magnitud pero si deberá permitir un crecimiento gradual posible. Esta área es definida el *área 0*

Ligada al área 0 deben estar el resto de las áreas definidas y se deben evitar el uso de virtual-links, es decir de aquellas áreas que no tienen conexión física al área 0.

OSPF solo debe transportar las rutas de la infraestructura de la red y en el caso de utilizar redistribuciones hacia OSPF se deben realizar a través de rutas externas tipo 1.

Posteriormente al diseño de áreas se define el direccionamiento donde se deben mantener la base de datos topológica (link-state database) donde se define por completo la red: ruteadores, segmentos y la forma de sus interconexiones.

Trabajos a realizar:

- Habilitar el proceso OSPF
- Habilitar el log del proceso de OSPF
- Modificar la referencia del costo para el enlace de mayor ancho de banda
- Poner en modo pasivo los enlaces a los vecinos de otros AS

- Agregar las redes de la infraestructura al proceso OSPF
- Definir el identificador del ruteador (router ID)

b) Protocolo de enrutamiento interdominio BGP. La versión actual de BGP es la versión 4 definida en 1995 en el RFC 1771. BGP realiza una comunicación basada en Unicast con cada uno de sus vecinos de BGP los cuales se denominan *peers*. BGP es un protocolo basado en vector distancia en el cual cada nodo confía en sus vecinos enviando sus rutas desde sus tablas de enrutamiento

El principal atributo de BGP es que dado que no trabaja basado en métricas, si es rico en atributos que pueden ser configurables para determinar el camino de un paquete hacia su destino.

Al momento de la implementación de BGP se debe considerar:

- Utilizarlo para transportar los prefijos de Internet a través del backbone
- Utilizar interfases de loopback en los ruteadores para establecer las sesiones de iBGP
- Usar peer-groups
- Usar contraseñas en cada sesión de iBGP

Se debe definir la forma en que el tráfico fluye por la red, delimitando los sistemas autónomos de tránsito. En BGP las políticas de tránsito se pueden crear basándose en prefijos, comunidades y sistemas autónomos. Se empleará:

- Route flap dampening
- Communities
- Route reflectors

Asimismo se considera el uso de la reconfiguración dinámica (soft reconfiguration) que servirá para forzar las actualizaciones de anuncios sin que se tenga que reiniciar la sesión de BGP. Esto ahorra mucho tiempo de reinicio de sesión no solo en los ruteadores vecinos sino en los que repropaga los cambios.

Que se debe evitar:

- Los anuncios de prefijos de las redes del RFC 1918
- La ruta por default
- El anuncio de bloque de direcciones que tienen como origen el AS local

-El anuncio de prefijos con una máscara de longitud demasiado grande, en el caso de Internet 2 esto es mayores a 27 bits.

Trabajos a realizar:

BGP

- Habilitar dampening
- Habilitar el log del cambio de estado de los vecinos
- Habilitar MED en modo determinístico
- Deshabilitar la sincronización
- Deshabilitar la sumarización automática de rutas
- Definir el router ID
- Agregar al proceso de BGP el bloque de direcciones del AS
- Agregar al proceso los bloques de direcciones propias de los clientes que no “hablan” BGP

iBGP

- Habilitar el proceso BGP
- Definir los peer-groups
- Agregar descripción
- Definir el vecino como interno
- Establecer las sesiones utilizando interfases de loopback
- Utilizar el comando “next-hop-self”
- Enviar las comunidades a todos los vecinos
- Especificar la versión 4 de BGP
- Usar contraseñas en cada sesión de iBGP
- Habilitar el uso de “soft-reconfiguration inbound”

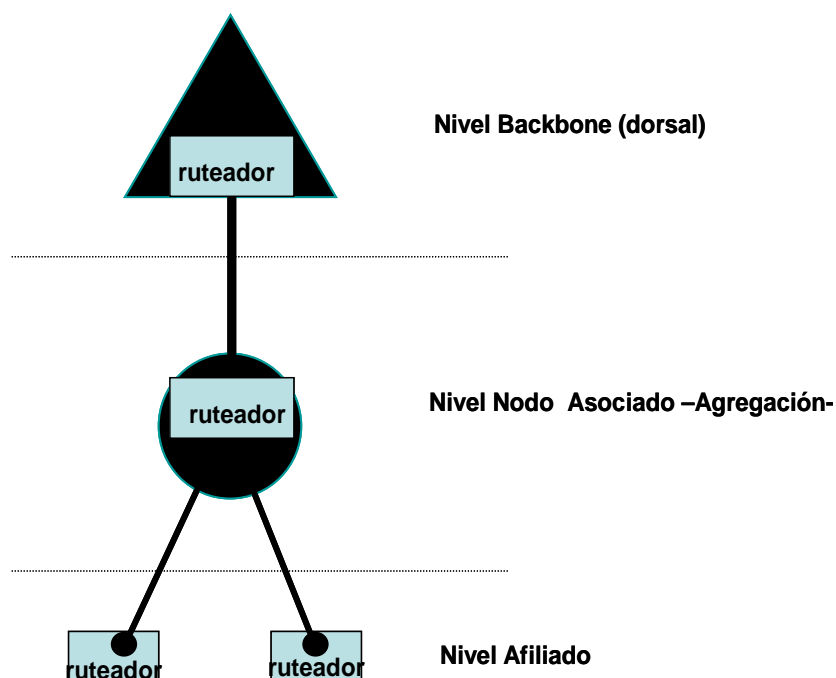
EBGP

- Definir el vecino con su AS
- Agregar descripción del vecino
- Borrar los sistemas autónomos privados
- Definir los filtros
- Asignar contraseña a la sesión de EBGP
- Limitar el número máximo de anuncios recibidos en cada sesión
- Habilitar el uso de “soft-reconfiguration inbound”

Políticas de Ruteo

Adicional al esquema de ruteo se deben esclarecer políticas de ruteo que promueven la buena operación de los anuncios de rutas provenientes de los asociados y afiliados hacia la dorsal de CUDI y delimitando aquellos anuncios innecesarios hacia el backbone y que restan desempeños a la red.

De acuerdo al esquema de conexión tenemos:



Con cada miembro de CUDI que se interconecta se hacen anuncios de sus propias rutas desde su punto origen de conexión y propagándose hacia los ruteadores de la dorsal de la red, reflejándose esto en el crecimiento de tamaño de las tablas de ruteo tanto internas como externas y anunciando esto a su vez a las redes internacionales con las que tenemos interconexión.

Por los mismos motivos de desempeños de la red CUDI pero adicionalmente por políticas de buen vecino se debe cuidar el esquema de ruteo que se establezca. En estas políticas de ruteo se establece que no debe anunciarse entonces hacia la dorsal de CUDI.

De esta forma se recomienda realizar los anuncios necesarios hacia el interior de cada nivel de asociado y solo los necesarios hacia la dorsal de CUDI.

En los RFC's 3330 y 2439, se describen recomendaciones basadas en la identificación de niveles de anuncio de ruteo y de penalizaciones hacia los anuncios inadecuados de las administraciones de red, de tal forma que se encuentre el punto adecuado de operación y sus principales niveles se identifican como:

- *Bogus Routes*: Son los anuncios de redes que se deben quedar al interior de los equipos de cada miembro asociado y no anunciarse a la dorsal.
- *Route Flapping*: son la frecuencia de los anuncios enviados a la dorsal de la red.

En este último concepto se maneja el término *Import Routing Policy*, que es el tamaño de las redes recibidas y que a través de este se da atención a no tener tablas excesivas en los ruteadores de dorsal.

Dentro de CUDI existe un grupo de trabajo destinado a la definición y análisis de la red denominado "Grupo de Enrutamiento"

De acuerdo a la recomendación del RFC 3330 y a este grupo de trabajo de CUDI, en el primer nivel, el nivel de Bogus Routes los asociados deben enviar sus rutas de acuerdo al nivel mas alto de globalidad que tengan, es decir, las rutas válidas relacionadas o que afectan operativamente a todo el grupo de conexiones tanto del asociado como del afiliado.

De acuerdo a lo anterior, por ejemplo, la siguiente tabla muestra aquellas redes que son Bogus routes:

Red	Uso
0.0.0.0/8	Esta red identifica a la red local.
10.0.0.0/8	Red privada.
14.0.0.0/8	Redes públicas de datos
24.0.0.0/8	Redes de televisión por cable.
39.0.0.0/8	Reservado para uso futuro
127.0.0.0/8	Loopback
128.0.0.0/16	Reservado para uso futuro
169.254.0.0/16	Reservado para auto-configuración
172.16.0.0/12	Red privada
191.255.0.0/16	Reservado para uso futuro
192.0.0.0/24	Reservado para uso futuro
192.0.2.0/24	Reservado para documentación
192.88.99.0/24	Direcciones 6to4 Relay Anycast
192.168.0.0/16	Red privadas
198.18.0.0/15	Reservado para pruebas de interconexión
223.255.255.0/24	Reservado para uso futuro.
224.0.0.0/4	Redes multicast
240.0.0.0/4	Reservadas para uso futuro.

Asimismo, para aquellas redes locales de los afiliados o asociados que no mantengan una estabilidad en su operación se establecen “penalizaciones” que conllevan a especie de periodos de aislamiento o cuarentena de dicha red de forma global con la finalidad de obligar a su revisión y adecuación del ruteo por parte de sus administradores.

Estas premisas son reflejadas en el RFC 2439 y son aceptadas por comunidades globales de Internet e Internet 2.

En el aspecto de Import Routing Policy se recomienda implementar sumarización en los prefijos anunciados a la red CUDI

Cualquier operación incorrecta del ruteo de la red de los asociados deberá reportarla de inmediato en NOC-CUDI.

5.2 ESQUEMA DE DIRECCIONAMIENTO IPv6 DE LA RED

La UNAM inició investigaciones en la materia desde el mes de diciembre de 1998, fecha en la que se constituye el proyecto IPv6 en nuestra Máxima Casa de Estudios. Dentro del Proyecto IPv6 de la UNAM se estableció un amplio programa de pruebas y trabajos con temas como: implementaciones, stacks IPv4/IPv6, túneles, software de conexión, aplicaciones multimedia, servidores para Web y DNS, autoconfiguración, calidad de servicio, IPv6 sobre ATM, conexión con redes internacionales de IPv6 (6Bone, 6REN), IPv6 en Internet2, etc.

Dentro de las primeras pruebas realizadas, destaca la de conexión a 6Bone, la cual es una red mundial experimental utilizada para probar los conceptos y la puesta en operación de IPv6. Posteriormente en septiembre de 1999 la UNAM fue aceptada como uno de los 68 nodos de Backbone que a la fecha operan en 6Bone, obteniendo un rango de direcciones tipo pTLA: 3ffe:8070::/28.

Para contar con una red de pruebas en una primera etapa, y posteriormente con una red de producción, se instaló la Red IPv6 de la UNAM, la primera red IPv6 instalada en México y que inició operaciones en agosto de 1999. Esta red cuenta con varios túneles hacia otros nodos de Backbone de 6Bone: SPRINT, FIBERTEL, MERIT, BAY NETWORKS, JANET e ISI-LAP, y hacia los hosts que tiene la UNAM corriendo con sistemas operativos como Win NT, Solaris y Linux.

Actualmente se está trabajando con instituciones mexicanas para realizar su conexión IPv6 hacia la UNAM, entre estas instituciones destacan: Instituto Politécnico Nacional, Universidad Autónoma Metropolitana, Instituto Tecnológico de Estudios Superiores de Monterrey, Universidad Autónoma de Chiapas, Universidad Autónoma de Guerrero, Universidad Autónoma del Estado de Hidalgo, Universidad Autónoma de Nuevo León, Instituto Tecnológico de Oaxaca, Instituto Tecnológico de Mérida, PEMEX, STYX, ASTER, etc.

Esta experiencia permitió trabajar y extender la cobertura de IPv6 a la red de CUDI proporcionándole las capacidades y funcionalidades que el nuevo protocolo ofrece.

Objetivos.

- Instalar IPv6 en los equipos del backbone de la red CUDI.
- Instalar IPv6 en los equipos de los asociados académicos de la red CUDI.

- Investigar y ensayar mecanismos de transición de IPv4 a IPv6 para los equipos y las redes de Internet2 en México.
- Preparar la red de CUDI para correr aplicaciones que se beneficien con las nuevas características de IPv6.
- Fortalecer la colaboración con grupos de trabajo de IPv6 en Internet2 que existen en el mundo.

Equipos considerados a integrar en el direccionamiento IPv6:

El backbone de la red de CUDI tiene cuatro GigaPoPs, para habilitarlos para IPv6 es necesario:

Cambiar el IOS de los ruteadores Cisco 7200 por la versión 12.2(0.5)T (c7200-p-mz.122-0.5.T IPv6 beta).

No es necesario cambiar nada en los Switches ATM Cisco BPX 8620.

GIGAPoP	EQUIPO	ACCION REQUERIDA	COMENTARIOS
Tijuana	Router Cisco 7200	Cambiar IOS	Instalar versión c7200-p-mz.122-0.5.T
	Switch ATM Cisco BPX 8620	Ninguno	
Monterrey	Router Cisco 7200	Cambiar IOS	Instalar versión c7200-p-mz.122-0.5.T
	Switch ATM Cisco BPX 8620	Ninguno	
Guadalajara	Router Cisco 7200	Cambiar IOS	Instalar versión c7200-p-mz.122-0.5.T
	Switch ATM Cisco BPX 8620	Ninguno	
México D.F.	Router Cisco 7200	Cambiar IOS	Instalar versión c7200-p-mz.122-0.5.T
	Switch ATM Cisco BPX 8620	Ninguno	

En los nodos de los asociados académicos es necesario:

- Cambiar el IOS de los ruteadores Cisco por la versión que soporta IPv6.
- Los ruteadores Cabletron soportan IPv6 desde la versión 3.0 de su software, así hay que revisar que versión tiene instalada y entonces cambiarla si se requiere.
- Hay que revisar la información para los equipos Fore para conocer su soporte para IPv6.
- El ruteador Nortel de la UNAM ya soporta IPv6. Los ruteadores Nortel soportan IPv6 desde la versión 12.0 de su software.
- No es necesario cambiar nada en los Switches ATM.

GIGAPoP	NODO	EQUIPO	CAMBIO REQUERIDO	COMENTARIOS
Tijuana	CICESE	Router Cabletron SSR 2000	Verificar versión primero	Soporta IPv6 desde la versión 3.0 de su software
		Switch ATM Cabletron SS 9000	Ninguno	
Monterrey	ITESM	Router Cisco 7500	Cambiar IOS	Verificar información de soporte para IPv6
		Switch ATM	Ninguno	
	UANL	Router Cabletron SSR 2000	Verificar versión primero	Soporta IPv6 desde la versión 3.0 de su software
		Switch ATM Cabletron SS 9000	Ninguno	
	UAT	Router Cisco 7200	Cambiar IOS	Instalar versión c7200-p-mz.122-0.5.T
Guadalajara	UDG	Router Cabletron SSR 2000	Verificar versión primero	Soporta IPv6 desde la versión 3.0 de su software
		Switch ATM Cabletron SS 9000	Ninguno	
México D.F.	IPN	Router Fore	Verificar información de soporte para IPv6	
		Switch ATM Fore	Ninguno	
	UAM	Router Cabletron SSR 2000	Verificar versión primero	Soporta IPv6 desde la versión 3.0 de su software
		Switch ATM Cabletron SS 9000		
	UDLA	Router Cabletron SSR 2000	Verificar versión primero	Soporta IPv6 desde la versión 3.0 de su software
		Switch ATM Cabletron SS 9000	Ninguno	
	UNAM	Router Nortel BLN	Ninguno	Ya soporta IPv6 desde la versión 12.0 de su software
		Switch ATM Nortel Passport 6800	Ninguno	

Plan de trabajo desarrollado.

Se proponen los siguientes pasos y fechas para la instalación y uso de IPv6 en la red CUDI:

Nº	ACCION
1	Cambiar el IOS de los cuatro ruteadores del backbone por la versión requerida.
2	Verificar las versiones de los ruteadores de los asociados académicos.
3	Cambiar en los equipos que se requiera el IOS de los ruteadores de los asociados académicos.
4	Configurar túneles de IPv4 sobre IPv6 y conexiones nativas de IPv6 sobre ATM para comunicación entre los participantes en México.
5	Ya se cuenta con un túnel de IPv6 sobre Internet2 desde la UNAM a Abilene, así resta aumentar las conexiones con IPv6 entre los nodos de México, E. U., Canadá, Chile, etc.
6	Trabajar con aplicaciones de IPv6

Para el uso de aplicaciones con IPv6, es necesario que los asociados académicos instalen y configuren uno o varios host que soporten IPv6. Existen varias opciones, siendo las más recomendables: Windows NT y 2000, XP, Solaris y RedHat, etc.

Sobre los pasos necesarios para la instalación y configuración, el NOC-CUDI puede asesorar a los encargados en cada institución.

Direccionamiento IPv6.

Las direcciones IPv6 que se usarán en las conexiones, ya sean por túneles o enlaces nativos, son las siguientes:

La UNAM tiene el bloque de direcciones IPv6 para usos de producción, llamado sTLA: 2001:0448::/35

designando el sNLA para CUDI: 2001:0448:0003::/48

entonces, se usará el sSLA para los nodos: 2001:0448:0003:XYZZ::/64

donde:

X identificará las regiones (16 regiones posibles)

- X = 0 -> Backbone
- X = 1 -> Internacional
- X = 2 -> Internacional
- X = 3 -> Tijuana
- X = 4 -> Monterrey
- X = 5 -> México D. F.
- X = 6 -> Guadalajara

YY identificará las redes de los asociados académicos (256 redes posibles).

NOTA: inicialmente se le asignarán dos redes a cada asociado académico, pudiendo asignar más si así lo requieren.

X = 3 -> Tijuana

YY = 00 CICESE > 2001:0448:0003:300Z::/64

YY = 01 CICESE > 2001:0448:0003:301Z::/64

X = 4 -> Monterrey

YY = 00 ITESM > 2001:0448:0003:400Z::/64

YY = 01 ITESM > 2001:0448:0003:401Z::/64

YY = 02 UANL > 2001:0448:0003:402Z::/64

YY = 03 UANL > 2001:0448:0003:403Z::/64

YY = 04 UAT > 2001:0448:0003:404Z::/64

YY = 05 UAT > 2001:0448:0003:405Z::/64

X = 5 -> México D. F.

YY = 00 IPN > 2001:0448:0003:500Z::/64

YY = 01 IPN > 2001:0448:0003:501Z::/64

YY = 02 UAM > 2001:0448:0003:502Z::/64

YY = 03 UAM > 2001:0448:0003:503Z::/64

YY = 04 UDLA > 2001:0448:0003:504Z::/64

YY = 05 UDLA > 2001:0448:0003:505Z::/64

YY = 04 UNAM > 2001:0448:0003:506Z::/64

YY = 05 UNAM > 2001:0448:0003:507Z::/64

X = 6 -> Guadalajara

YY = 00 UDG > 2001:0448:0003:600Z::/64

YY = 01 UDG > 2001:0448:0003:601Z::/64

Finalmente, Z identificará las subredes para los asociados académicos (16 subredes posibles).

Estas subredes las delegará cada asociado académico, ya sea para su propio uso y para el uso de los afiliados que se conecten con ellos. Agradeceremos que nos informen de estas delegaciones en cuanto se realicen, con el fin de tener una base de datos de las direcciones usadas.

IMPORTANTE:

- Las redes delegadas tiene un prefijo de /64, que es lo definido para la porción de red, quedando 64 bits para la porción de host (así, cada institución tendrá 2 redes con 16 subredes con ¡ 2^{64} hosts cada una!). De manera regular no se deben hacer subredes con estos 64 bits, esto es para preservar la agregación de las redes y además serán útiles para autoconfiguración, reenumeración y multihoming.
- Para hacer la delegación oficial necesitamos que nos contacte el responsable de cada asociado académico, para ir recopilando información para nuestra base de datos, para acordar las conexiones y ayudarlos en las configuraciones.
- Estas direcciones son para las conexiones sobre Internet2. Si desean direcciones para pruebas en Internet les podemos proporcionar otras direcciones.



	Tijuana	Monterrey	México D.F.	Guadalajara
Tijuana	2001:0448:0003:0033::1/64	2001:0448:0003:0043::1/64 2001:0448:0003:0043::2/64	2001:0448:0003:0053::1/64 2001:0448:0003:0053::2/64	2001:0448:0003:0063::1/64 2001:0448:0003:0063::2/64
Monterrey		2001:0448:0003:0044::1/64	2001:0448:0003:0054::1/64 2001:0448:0003:0054::2/64	2001:0448:0003:0064::1/64 2001:0448:0003:0064::2/64
México D.F.			2001:0448:0003:0055::1/64	2001:0448:0003:0065::1/64 2001:0448:0003:0065::2/64
Guadalajara				2001:0448:0003:0066::1/64

Las direcciones de la tabla anterior tienen el siguiente formato:

2001:0448:0003:XTRS::/64

donde:

X=0 identifica a una dirección de Backbone

T identifica el tipo de conexión

T=0 ->Backbone-Backbone

T=1 -> Backbone-Asociado Académico

R identifica la región origen

S identifica la región destino

R, S = 1 -> Internacional

R, S = 2 -> Internacional

R, S = 3 -> Tijuana

R, S = 4 -> Monterrey

R, S = 5 -> México D. F.

R, S = 6 -> Guadalajara

	Tijuana	Monterrey	México D.F.	Guadalajara
CICESE	2001:0448:0003:0130::1/64 2001:0448:0003:0130::2/64			
ITESM		2001:0448:0003:0140::1/64 2001:0448:0003:0140::2/64		
UANL		2001:0448:0003:0141::1/64 2001:0448:0003:0141::2/64		
UAT		2001:0448:0003:0142::1/64 2001:0448:0003:0142::2/64		
IPN			2001:0448:0003:0150::1/64 2001:0448:0003:0150::2/64	
UAM			2001:0448:0003:0151::1/64 2001:0448:0003:0151::2/64	
UDLA			2001:0448:0003:0152::1/64 2001:0448:0003:0152::2/64	
UNAM			2001:0448:0003:0153::1/64 2001:0448:0003:0153::2/64	
UDG				2001:0448:0003:0160::1/64 2001:0448:0003:0160::2/64

Las direcciones de la tabla anterior tienen el siguiente formato:

2001:0448:0003:XTRS::/64

donde:

X=0 identifica a una dirección de Backbone

T identifica el tipo de conexión

T=0 ->Backbone-Backbone

T=1 -> Backbone-Asociado Académico

R identifica la región de origen

R = 1 -> Internacional

R = 2 -> Internacional

R = 3 -> Tijuana

R = 4 -> Monterrey

R = 5 -> México D. F.

R = 6 -> Guadalajara

S identifica el nodo destino (Asociados Académicos)

R = 3 -> Tijuana

S = 0 -> CICESE

R = 4 -> Monterrey

S = 0 -> ITESM

S = 1 ->UANL

S = 2 ->UAT

R = 5 -> México D. F.

S = 0 ->IPN

S = 1 ->UAM

S = 2 ->UDLA

S = 3 ->UNAM

R = 6 -> Guadalajara

S = 0 ->UDG

5.3 ESQUEMA DE MULTICAST

En el caso de la red de CUDI donde se tienen diferentes sistemas autónomos se define el uso del protocolo PIM-SM en la dorsal para el registro de las fuentes de multicast.

El protocolo PIM-SM es muy eficiente ya que trabaja a través de un modelo de solicitud explícito que permite el ingreso de los hosts a los grupos de multicast y el tráfico de multicast solo fluye a los puntos donde es demandado dentro de la red. Asimismo es un protocolo escalable y trabaja igualmente eficientemente en redes densas o de poca densidad, esto lo hace muy eficiente.

Las dos únicas deficiencias para utilizar en la dorsal de CUDI el protocolo PIM-SM es que este protocolo demanda el uso de enrutamiento unicast compatible con el protocolo de enrutamiento que se tenga en los otros sistemas autónomos y que el RP local debe conocer la existencia de las fuentes de multicast en los otros sistemas autónomos, para solucionar estos problemas se emplea el MBGP y MSDP

MSDP permitirá que cada sistema autónomo pueda tener su propio RP y permitirá que cada sistema autónomo pueda tener sus propias políticas sobre las fuentes y grupos en donde se desea intercambiar tráfico multicast.

Para definir el RP se utiliza el auto-RP utilizando direcciones anycast para ganar redundancia de otros RP. La razón de esto es para hacer creer a los ruteadores que solo existe un RP, de esta forma si uno de los RP falla, los ruteadores se comunican con el otro RP, además teniendo varios RP se puede balancear la carga de trabajo al distribuir la cantidad de ruteadores que atiende cada RP.

Los asociados y afiliados deberán definir su propio RP si quieren recibir o enviar tráfico multicast y establecer una sesión de MSDP de manera jerárquica. Todas las sesiones deberán contener los filtros recomendados de frontera.

- Habilitar globalmente el enrutamiento multicast
- Habilitar PIM-SM en las interfases definiendo el filtro de frontera
- Definir el RP del AS
- Habilitar la sesión de MBGP para soportar prefijos multicast
- Habilitar la sesión de MSDP

*Capítulo 6***CONCLUSIONES**

Con el trabajo desarrollado de la presente tesis se llegó al cumplimiento de los objetivos planteados al proporcionar una propuesta de implementar un esquema de control y operación de la red nacional de Internet 2 de México definiendo una entidad denominada NOC-CUDI con alcances y compromisos claramente especificados.

El NOC-CUDI no es la definición de un espacio físico que anteriormente concebíamos como medular en el control de una red. Con los cambios en la tecnología, la visión y el ambiente de operación de Internet 2 en México y en el mundo, las bases de operación de los elementos de esta red, sus definiciones de funcionalidad y de los procedimientos críticos del comportamiento del tráfico son material esencial en la descripción de un centro de operación de siguiente evolución, donde el control y la operación van mas allá de espacios físicos y propagándose responsabilidades de operación hacia puntos de apoyo dispersos pero apoyados en las nuevas potencialidades de la tecnología. Una red que tiene bien diseñado su esquema de operación y comportamiento de cada uno de sus elementos permite una operación exitosa que da como resultado excelentes desempeños con la optimización de los recursos, esto es de gran beneficio para CUDI ya que se trata de una red cuyos miembros son entidades académicas y los presupuestos deben ser parte del compromiso cuidar y utilizar inteligentemente.

En la presente propuesta NOC-CUDI se plantea el esquema global de operación, se plantean las actividades específicas en cada entidad, las herramientas a utilizar en cada concepto, los procedimientos a llevar a cabo, los alcances que deberán ser cubiertos para dar el soporte a las aplicaciones de CUDI y las propuestas de inicio de operación. Los problemas de red no pueden ser categorizados y rara vez se utiliza solo una tecnología para resolverlos por lo que la recomendación mas extensa es la operación de la red se debe dividir el nivel del problema a ser resuelto, se debe dividir los niveles de operación, siguiendo el precepto de “divide y vencerás”; tenemos 7 niveles en el modelo OSI que podemos usar de marco de referencia para dividir y acotar los alcances de cada nivel de operación con la finalidad de ir cubriendo cada

uno de estos haciendo uso de las múltiples tecnologías que existen para cubrir cada uno de estos, si se trata de un equipo o de un comportamiento o de un procedimiento. También es importante seguir estándares establecidos en cada nivel de operación para lograr una administración mas abierta, transparente y controlada.

Actualmente esta propuesta ya ha sido implementada y se tienen excelentes resultados en la operación de la red de CUDI, pero aun más, gracias al trabajo desarrollado en ejercicio de la operación global de CUDI, ya existe dentro de la Corporación CUDI la definición de grupos de trabajo que desarrollen específicamente cada concepto de operación de la red, como el grupo de trabajo de enrutamiento, el de topología, el de IPv6, el de Multicast, el de Calidad de Servicio, hasta el de video de alta definición entre otros. Esto permitirá llevar a cabo análisis mas precisos de cada concepto y sacar aun mas inteligencia de la red.

El campo de operación de redes es todavía un campo de desarrollo muy joven y más aún el de operación de redes de alto desempeño; no existen manuales ni libros para los administradores de red que indiquen estrictamente el ABC de la operación de la red, existen múltiples libros y apoyos sobre las tecnologías y recomendaciones de administración diversas, así como existen grupos de trabajo internacionales que producen como resultado sus recomendaciones para impulsar los estándares en este campo, pero no hay ninguna implementación estipulada de únicamente cambiar parámetros en configuraciones, no; la operación de redes es un campo donde el administrador o coordinador de la red debe primero estrictamente conocer su red que tiene que operar, segundo debe tener un amplio conocimiento de las tecnologías en materia de redes existentes, tercero conocer el comportamiento de las aplicaciones de alta demanda o de demanda de alto desempeño de la red, el administrador de la red debe ser analítico y creativo para trabajar con estos elementos y diseñar el esquema adecuado de operación, seleccionando las plataformas y herramientas informáticas y de redes de datos acorde a las necesidades de su red, que lo lleven a mantenerla en los adecuados niveles de desempeños.

Es por esto que sumado a los objetivos, el presente trabajo también representó un reto personal, un reto como Universidad y un reto como México con éxitos alcanzados, ya que el presente trabajo sirvió en paralelo para participar en la selección de la ubicación del Centro de Operación de la red CUDI y la UNAM fue seleccionada para coordinar y realizar estos compromisos. Asimismo el NOC-CUDI ubicado en la UNAM se postuló para ser el Centro de Operación de la red regional Internet 2 de Latinoamérica

(Red CLARA) y se obtuvo también la coordinación del NOC-CLARA gracias a la experiencia, conocimientos y trabajos demostrados desde el inicio de los estudios en materia de operación de redes de alto desempeño.

A N E X O S

ANEXO 1. Listado de las Instituciones miembros de CUDI

Fuente: www.cudi.edu.mx

• Asociados Institucionales

- Benemérita Universidad Autónoma de Puebla
2. Centro de Investigación Científica y de Educación Superior de Ensenada
3. Centros Públicos de Investigación Conacyt**
4. Dirección General de Educación Superior Tecnológica ****
5. Dirección General de Televisión Educativa
6. Instituto Latinoamericano de la Comunicación Educativa
7. Instituto Politécnico Nacional
8. Instituto Tecnológico y de Estudios Superiores de Monterrey
9. Institutos Nacionales de Salud*
10. Subsistema de Universidades Politécnicas***
11. Universidad Anáhuac de Xalapa
12. Universidad Autónoma de Ciudad Juárez
13. Universidad Autónoma de la Laguna
14. Universidad Autónoma de Nuevo León
15. Universidad Autónoma de Tamaulipas
16. Universidad Autónoma del Estado de Hidalgo
17. Universidad Autónoma del Estado de Morelos
18. Universidad Autónoma Metropolitana
19. Universidad de Guadalajara
20. Universidad de las Américas Puebla
21. Universidad Nacional Autónoma de México
22. Universidad Veracruzana

Institutos Nacionales de Salud*

1. Centro Nacional de Transfusión Sanguínea
2. Centro Nacional de Trasplantes
3. Hospital Infantil de México
4. Instituto Nacional de Cancerología
5. Instituto Nacional de Cardiología
6. Instituto Nacional de Ciencias Médicas y Nutrición
7. Instituto Nacional de Enfermedades Respiratorias
8. Instituto Nacional de Medicina Genómica
9. Instituto Nacional de Neurología y Neurocirugía
10. Instituto Nacional de Pediatría
11. Instituto Nacional de Perinatología
12. Instituto Nacional de Psiquiatría
13. Instituto Nacional de Rehabilitación
14. Instituto Nacional de Salud Pública

Centros Conacyt**

1. Centro de Ingeniería y Desarrollo Industrial
2. Centro de Investigación Científica de Yucatán
3. Centro de Investigación en Alimentación y Desarrollo
4. Centro de Investigación en Geografía y Geomática "Ing. Jorge L. Tamayo"
5. Centro de Investigación en Matemáticas
6. Centro de Investigación en Materiales Avanzados
7. Centro de Investigación en Química Aplicada
8. Centro de Investigación y Asistencia en Tecnología y Diseño del Estado de Jalisco, A.C.
9. Centro de Tecnología Avanzada
10. Centro de Innovación Aplicada en Tecnologías Competitivas
11. Centro de Investigación y Desarrollo Tecnológico en Electroquímica
12. Centro de Investigación y Docencia Económicas
13. Centro de Investigaciones Biológicas del Noroeste
14. Centro de Investigaciones en Óptica
15. Centro de Investigaciones y Estudios Superiores en Antropología Social
16. Corporación Mexicana de Investigación en Materiales
17. El Colegio de la Frontera Norte
18. El Colegio de la Frontera Sur
19. El Colegio de México
20. El Colegio de Michoacán
21. El Colegio de San Luis
22. Facultad Latinoamericana de Ciencias Sociales
23. Fondo de Información y Documentación para la Industria
24. Instituto de Ecología
25. Instituto de Investigaciones "Dr. José María Luis Mora"
26. Instituto Nacional de Astrofísica, Óptica y Electrónica
27. Instituto Potosino de Investigación Científica y Tecnológica

Subsistema de Universidades Politécnicas ***

1. Universidad Politécnica de Aguascalientes
2. Universidad Politécnica de Baja California
3. Universidad Politécnica de Chiapas
4. Universidad Politécnica de Durango
5. Universidad Politécnica de Francisco I. Madero
6. Universidad Politécnica de Gómez Palacio Durango
7. Universidad Politécnica de Guanajuato
8. Universidad Politécnica de Morelos
9. Universidad Politécnica de Pachuca
10. Universidad Politécnica de Puebla
11. Universidad Politécnica de Querétaro
12. Universidad Politécnica de San Luis Potosí
13. Universidad Politécnica de Sinaloa
14. Universidad Politécnica de Tlaxcala
15. Universidad Politécnica de Tulancingo
16. Universidad Politécnica de Valle de México
17. Universidad Politécnica de Zacatecas
18. Zona Metropolitana de Guadalajara

Institutos Tecnológicos****

- | | |
|---|---|
| 1. Centro de Investigación y Desarrollo Tecnológico | 31. Instituto Tecnológico de Chetumal |
| 2. Instituto Tecnológico Cd. Madero | 32. Instituto Tecnológico de Chihuahua II |
| 3. Instituto Tecnológico Celaya | 33. Instituto Tecnológico de Chilpancingo |
| 4. Instituto Tecnológico de Aguascalientes | 34. Instituto Tecnológico de CIIDET |
| 5. Instituto Tecnológico de Chihuahua | 35. Instituto Tecnológico de Colima |
| 6. Instituto Tecnológico de Conkal | 36. Instituto Tecnológico de Comitán |
| 7. Instituto Tecnológico de Durango | 37. Instituto Tecnológico de Comitancillo |
| 8. Instituto Tecnológico de Laguna | 38. Instituto Tecnológico de Culiacán |
| 9. Instituto Tecnológico de León | 39. Instituto Tecnológico de Delicias |
| 10. Instituto Tecnológico de Mérida | 40. Instituto Tecnológico de Hermosillo |
| 11. Instituto Tecnológico de Minatitlán | 41. Instituto Tecnológico de Istmo |
| 12. Instituto Tecnológico de Morelia | 42. Instituto Tecnológico de Jiquilpan |
| 13. Instituto Tecnológico de Oaxaca | 43. Instituto Tecnológico de La Cuenca del Papaloapan |
| 14. Instituto Tecnológico de Orizaba | 44. Instituto Tecnológico de La Paz |
| 15. Instituto Tecnológico de Puebla | 45. Instituto Tecnológico de Lázaro Cárdenas |
| 16. Instituto Tecnológico de Querétaro | 46. Instituto Tecnológico de Los Mochis |
| 17. Instituto Tecnológico de Saltillo | 47. Instituto Tecnológico de Matamoros |
| 18. Instituto Tecnológico de Tepic | 48. Instituto Tecnológico de Mexicali |
| 19. Instituto Tecnológico de Tijuana | 49. Instituto Tecnológico de Nogales |
| 20. Instituto Tecnológico de Veracruz | 50. Instituto Tecnológico de Nuevo Laredo |
| 21. Instituto Tecnológico de Acapulco | 51. Instituto Tecnológico de Pachuca |
| 22. Instituto Tecnológico de Apizaco | 52. Instituto Tecnológico de Parral |
| 23. Instituto Tecnológico de Boca del Río | 53. Instituto Tecnológico de San Luis Potosí |
| 24. Instituto Tecnológico de Campeche | 54. Instituto Tecnológico de Tlajomulco |
| 25. Instituto Tecnológico de Cancún | 55. Instituto Tecnológico de Toluca |
| 26. Instituto Tecnológico de Cd. Cuauhtémoc | 56. Instituto Tecnológico de Tuxtepec |
| 27. Instituto Tecnológico de Cd. Guzmán | 57. Instituto Tecnológico de Valle de Oaxaca |
| 28. Instituto Tecnológico de Cd. Juárez | 58. Instituto Tecnológico de Villahermosa |
| 29. Instituto Tecnológico de Cd. Valles | 59. Instituto Tecnológico de Zacatecas |
| 30. Instituto Tecnológico de Cerro Azul | 60. Instituto Tecnológico de Zacatepec |
| | 61. Instituto Tecnológico de Zitácuaro |

- **Afiliados Académicos**

1. Banco Interamericano de Desarrollo
2. Centro de Articulación Productiva Médico, A.C.
3. Centro de Investigación y de Estudios Avanzados del IPN
4. Centro Internacional de Mejoramiento de Maíz y Trigo
5. Colegio de Postgraduados
6. Colegio Nacional
7. Comisión Nacional para el Conocimiento y Uso de la Biodiversidad
8. Comité Regional Norte de Cooperación con la UNESCO
9. Fundación Clínica Medica Sur
10. Instituto de Investigaciones Eléctricas
11. Instituto Mexicano del Petróleo
12. Instituto Nacional de Estadística, Geográfica e Informática
13. Instituto Tecnológico Autónomo de México
14. Instituto Tecnológico de Estudios Superiores de Irapuato

15. Instituto Tecnológico de Sonora
16. Laboratorio Nacional de Informática Avanzada
17. La Casa de la Universidad de California en México A.C.
18. Tecnológico de Estudios Superiores de Ecatepec
19. Texas A&M University Center México
20. Universidad Autónoma Benito Juárez de Oaxaca
21. Universidad Autónoma Chapingo
22. Universidad Autónoma de Aguascalientes
23. Universidad Autónoma de Baja California
24. Universidad Autónoma de Chiapas
25. Universidad Autónoma de Chihuahua
26. Universidad Autónoma de Coahuila
27. Universidad Autónoma de Guadalajara
28. Universidad Autónoma de Guerrero
29. Universidad Autónoma de Nayarit
30. Universidad Autónoma de Querétaro
31. Universidad Autónoma de San Luis Potosí
32. Universidad Autónoma de Tlaxcala
33. Universidad Autónoma de Yucatán
34. Universidad Autónoma del Estado de México
35. Universidad de Colima
36. Universidad de Guanajuato
37. Universidad de Quintana Roo
38. Universidad de Sonora
39. Universidad del Valle de México
40. Universidad Iberoamericana
41. Universidad Juárez Autónoma de Tabasco
42. Universidad Juárez del Estado de Durango
43. Universidad La Salle
44. Universidad Michoacana de San Nicolás de Hidalgo
45. Universidad Montemorelos
46. Universidad Pedagógica Nacional
47. Universidad Popular Autónoma del Estado de Puebla
48. Universidad Regiomontana
49. Universidad Tecnológica de México

• **Asociados Institucionales**

1. Avantel, S.A.
2. Cisco Systems de México S.A. de C.V.
3. Consejo Nacional de Ciencia y Tecnología
4. Teléfonos de México S. A. de C.V.

• **Afiliados Empresariales**

1. Centro NETEC
2. VITECH

• **Convenios Internacionales**

1. Canadian Network for Advanced Research Industrie and Education (CANARIE, Canadá)
2. Cooperación Latinoamericana de Redes Avanzadas (CLARA,)
3. Corporation of Education Network Initiatives in California (CENIC, Estados Unidos)
4. Red Iris (IRIS, España)
5. Red Teleinformática Académica de Argentina (RETINA, Argentina)
6. Red Universitaria Nacional de Chile (REUNA, Chile)
7. University Corporation for Advanced Internet Development (UCAID, Estados Unidos)

ANEXO 2. Aplicaciones de CUDI

Fuente: www.cudi.edu.mx

Institución	Tipo de Aplicaciones	Aplicaciones	Beneficios
Benemérita Universidad Autónoma de Puebla	Salud	El programa de "telemedicina", "sesiones hospitalarias interactivas" y próximamente "La red latinoamericana para educación y salud"	Educación, salud e investigación
Benemérita Universidad Autónoma de Puebla	Bibliotecas Digitales	-	Acceso a contenidos desde cualquier punto de la red o fuera de ella
Benemérita Universidad Autónoma de Puebla	Educación	Educación a distancia, Programa para el uso de la tecnología en la docencia, transmisión de cursos y programas producidas de audio y video por TV-RED	Fácil acceso, audio y video en tiempo real e interacciones desarrolladas y semidesarrolladas
Benemérita Universidad Autónoma de Puebla	Cómputo de Alto Rendimiento	Modelado computacional	-
Centro Investigación y de Estudios Avanzados del IPN	Salud	Existe una aplicación sobre Telediagnóstico y sobre Telecirugía	-
Centro Investigación y de Estudios Avanzados del IPN	Bibliotecas Digitales	sistema de transferencia de documentos mediante ARIEL	Se utiliza para la transferencia electrónica de documentos
Centro Investigación y de Estudios Avanzados del IPN	Educación	Curso sobre Matemáticas a nivel medio	-
Centro Investigación y de Estudios Avanzados del IPN	Cómputo de Alto Rendimiento	Química Molecular	Modelación de reacciones químicas a nivel molecular
Centro Investigación y de Estudios Avanzados del IPN	Robótica	Laboratorio virtual de Robotica	Manipulación a distancia de un robot de 3 grados de libertad para propósitos educativos
Centro Investigación y de Estudios Avanzados del IPN	Otras Aplicaciones	Proyecto Mazarón	Base de datos genómica sobre las diversas variedades de plantas de

Institución	Tipo de Aplicaciones	Aplicaciones	Beneficios
IPN			maiz
Instituto de Investigaciones Eléctricas	Educación	VIBORA: Capacitación Inteligente basada en objetos de aprendizaje	La aplicación todavía no esta
Instituto Politécnico Nacional	Educación	Biología Humana	los elementos pueden ser tratados como objetos de aprendizaje en sus diversos niveles, pueden separarse como capítulos, temas específicos o unidades atomizadas. Existen muchos proyectos de bibliotecas digitales en el mundo, sin embargo, Phronesis se distingue de otros debido a que contempla los siguientes aspectos: -Indexamiento y búsquedas en texto completo y/o en metadatos - Control de acceso de los usuarios que pueden contribuir material a la biblioteca -Soporte para búsquedas de documentos escritos en el idioma español e inglés - Interfaz de usuario basada en WWW en español e inglés - Búsquedas simultáneas en varias instancias de Phronesis -Soporte de búsquedas en documentos completos en varios formatos como lo son texto, -PostScript, html, pdf y rtf -Soporte para almacenar cualquier tipo de documento y realizar búsquedas con base en sus metadatos -El software que constituye Phronesis es 100% del dominio público - Compresión eficiente de los documentos digitales. Phronesis se basa en el sistema MG (Managing Gigabytes) el cual es un proyecto de investigación diseñado para
Instituto Tecnológico de Estudios Superiores de Monterrey	Bibliotecas Digitales	Phronesis	

Institución	Tipo de Aplicaciones	Aplicaciones	Beneficios
Instituto Tecnológico de Estudios Superiores de Monterrey	Bibliotecas Digitales	Personal Digital Library (PDLib)	<p>crear y manejar una biblioteca digital de documentos.</p> <p>Mediante este proyecto se creará una infraestructura de bibliotecas digitales distribuidas que permitirá el acceso a colecciones multimediales heterogéneas a través de dispositivos móviles. Las bibliotecas digitales a integrar incluirán servicios de recuperación de información basados en agentes, los cuales extienden los mecanismos tradicionales de consulta, utilizando componentes de software con características de modularidad, escalabilidad y autonomía, y aprovechando el alto rendimiento de la red Internet 2. Se establecerán y se fortalecerán lazos de colaboración entre los proyectos de bibliotecas digitales en la Universidad de las Américas, Puebla (UDLA), y el Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Monterrey (ITESM). La infraestructura resultante podrá extenderse a otros miembros de CUDI que cuenten con colecciones digitales para hacerlas disponibles ampliamente.</p>
Instituto Tecnológico de Estudios Superiores de Monterrey	Educación	Videoconferencias	Colaboración e intercambio de conocimientos entre diferentes instituciones educativas.
Instituto Tecnológico de Estudios Superiores de Monterrey	Visualización	12 Inmersivo Realidad Virtual proyectada colaborativa	Realidad Virtual proyectada colaborativa de bajo costo
Texas A&M University	Educación	New York-Mexico City Language	Thanks to the increasing

Institución	Tipo de Aplicaciones	Aplicaciones	Beneficios
Center Mexico		Exchange	development of the > Telecommunications (Internet2) and the close relationship between Mexico > and USA, a group of leaders in the field of education joined forces in > order to bring together an English class in Mexico City and a Spanish > class in New York City
Universidad Autónoma de Ciudad Juárez	Ciencias de la Tierra	Estudio hidrogeológico y de calidad del agua en el bolsón del Hueco	Conocer Integralmente la hidrología de aguas subterráneas y superficiales, así como conocer las causas del deterioro de la calidad química del agua en la región transfronteriza Cd. Juárez, Chih.-El Paso, TX.
Universidad Autónoma de La Laguna	Ciencias de la Tierra	Análisis de multiescalas de la Climatología Urbana de la zona conurbada de la comarca lagunera	Velocidad en la transmisión de datos e imágenes entre México y Francia
Universidad Autónoma de Nuevo León	Salud	educación a distancia	ofrecer cursos de educación a distancia por parte de nuestro departamento de medicina preventiva y salud pública.
Universidad Autónoma de San Luis Potosí	Educación	Videoconferencia	Participar en cursos virtuales, Menores Costos
Universidad Autónoma del Estado de Hidalgo	Salud	Portal de Telesalud UAEH	El Portal de Telesalud de la UAEH integra cursos e información relacionada con las Ciencias de la Salud
Universidad Autónoma del Estado de Hidalgo	Bibliotecas Digitales	Biblioteca Digital UAEH	Tener acceso ilimitado de información sin límites de tiempo y espacio.
Universidad Autónoma del Estado de Hidalgo	Educación	Campus Virtual	El Campus Virtual está soportado por una plataforma que permite ofrecer cursos en línea
Universidad de Colima	Bibliotecas Digitales	Biblioteca Virtual Iberoamericana y Caribeña	Permite instalar una biblioteca digital, incluye metodología con estándares internacionales,

Institución	Tipo de Aplicaciones	Aplicaciones	Beneficios
			intercambio de información entre servidores y acceso a los usuarios al texto completo libre de derechos de autor
Universidad de Guadalajara	Bibliotecas Digitales	Acervos digitales	Revista de difusión científica y tecnológica
Universidad de Las Américas-Puebla	Ciencias de la Tierra	Servicios Geograficos (Aplicacion Volcan Popocatepetl)	Difusión de Información del volcán para prevención y planeación en caso de contingencias
Universidad de Las Américas-Puebla	Bibliotecas Digitales	Digitalización y divulgación digital de acervos antiguos	La preservación y difusión del patrimonio cultural universal, se construirá un acervo digital que concentrará las obras más importantes que se encuentran en las bibliotecas con libros antiguos pertenecientes a las instituciones miembros de CUDI.
Universidad de Las Américas-Puebla	Educación	BIDACI: Bib. Dig. Para aprendizaje colaborativo en Informática.CASSIEL: Ambiente p/generar comunidades de aprendizaje.	Distribución y construcción social de conocimientos vinculación de la academia con el sector público y productivo orientado al aprendizaje durante toda la vida
Universidad de Las Américas-Puebla	Laboratorios Virtuales	Experimentos asistidos vía Internet para la enseñanza de Ing en Alimentos	Apoya a la enseñanza y prácticas de Ing en Alimentos
Universidad de Las Américas-Puebla	Visualización	Las descritas en 615 y bibliotecas digitales	-
Universidad Popular Autónoma del Estado de Puebla	Salud		

GLOSARIO

ABR. (Area Border Router). Ruteador de área fronteriza de una o mas áreas de OSPF que las conecta al backbone de la red.

Acknowledgment. Notificación codificada enviada desde un dispositivo de red a otro para confirmar que ha ocurrido un evento.

Actualización de Enrutamiento (routing update). Mensaje enviado desde un ruteador para dar aviso de las rutas alcanzables de la red e información asociada con los costos.

Adyacencia. Es la relación que se establece entre ruteadores vecinos seleccionados y nodos terminales con el objetivo de intercambiar información de rutas.

Algoritmo de enrutamiento. Mecanismo que determina la mejor ruta para enviar tráfico desde un nodo origen hasta un destino específico.

Ancho de Banda (bandwidth). Es la tasa máxima de transmisión en un medio físico o en un protocolo determinado.

ANSI (American National Standards Institute). Instituto Nacional Americano de Estándares. Conformado por voluntarios de Estados Unidos, corporaciones, gobierno y otras dependencias.

Área. Es un conjunto lógico de segmentos de red y sus dispositivos conectados.

Área non-stub. Es un área de OSPF con grandes recursos que transporta una ruta predeterminada, rutas estáticas, rutas entre áreas, rutas intra-áreas y rutas externas.

Área stub. Área de OSPF que transporta una ruta predeterminada, rutas intra-área y rutas inter-área, pero no transportan rutas externas.

ARPANET (Advanced Research Projects Agency NET). Red de la Agencia de Proyectos de Investigación Avanzada. Importante red de conmutación de paquetes establecida en 1969.

ASBR (Autonomous System Border Router). Ruteador fronterizo de sistema autónomo que ejecutan tanto el protocolo de enrutamiento OSPF y una red que no emplea OSPF.

ATM (Asynchronous Transfer Mode). Modo de Transferencia Asíncrono. Estándar internacional para la conmutación de celdas en el cual se transporta varios tipos de tráfico (voz, video y datos).

Backbone. Dorsal principal de una red, la cual es responsable de conectar a todos los nodos y segmentos de red en una organización.

BGP (Border Gateway Protocol). Protocolo de puerta de enlace fronteriza. Protocolo de enrutamiento entre dominios que reemplaza a EGP.

Broadcast. Paquetes de datos que se envía a todos los nodos de la red en forma indistinta.

CISCO. Compañía fabricante de equipos de comunicaciones.

Core. Parte de la red donde cruza la mayor parte del tráfico, también es denominado backbone.

CUDI (Corporación Universitaria de Desarrollo de Internet).. Es la Corporación que desarrolla e impulsa Internet 2 en México.

DARPA. Defense Advanced Research Projects Agency.

Dirección IPv4. Es una dirección de 32 bits asignada a los hosts que utilizan TCP/IP como protocolo de comunicación.

Dirección IPv6. Evolución de IPv4 para dar mayor servicios en una red TCP/IP. Utiliza 128 bits.

Dirección MAC. Es la dirección estándar de 6 bytes de la capa de enlace de datos que se requiere para cada dispositivo que se conecta a una LAN. Es un estándar de la IEEE.

DNS. Sistema de Nombres de Dominio. Es usado en Internet para traducir los nombres de los nodos de la red hacia direcciones IP.

DVMRP (Distance Vector Multicast Routing Protocol). Protocolo de Enrutamiento Multicast basado en vector distancia y en gran parte de RIP.

E1. Esquema de transmisión digital de área amplia utilizado principalmente en Europa para transportar datos a una velocidad de 2.048 Mbps.

E3. Esquema de transmisión digital de área amplia utilizado principalmente en Europa para transportar datos a una velocidad de 34.368 Mbps.

BIBLIOGRAFIA

Tecnologías Emergentes para Redes de Computadoras. Uyles Black. Prentice Hall.

CCITT X.710. Redes de comunicación de datos: Interconexión de sistemas abiertos (ISA); gestión. Definición del servicio común de información de gestión para aplicaciones del CCITT.

CCITT X.711. Redes de comunicación de datos: Interconexión de sistemas abiertos (ISA); gestión. Especificación del protocolo común de información de gestión para aplicaciones del CCITT.

SNMP, SNMPv2, and RMON Practical Network Management. Stallings Williams. Addison-Wesley Publishing Company, Inc. Second edition. Massachusetts. 479 pp. 1996.

Simple Network Management Protocol (SNMP) -Current standards and Status-. Cekro Z. University Libre de Bruxelles. Paper. Bruxelles 40 pp. 1998

An Effective Bit Rate/Table Lookup Based Admission Control Strategy for the ATM B-ISDN. DuBose, Ken. Carnegie Mellon University, Thesis submitted for the degree Master of Science in Information Networking. 1991

Draft Definitions of Supplemental Managed Objects for ATM Management. Ly Faye, Noto Michael, Smith Andrew, Spiegel Ethan Mickey, Tesink Kaj, IETF. 1999.

SNMP A guide to network management. Feit Sidnie. Mc Graw Hill. New York. 674 pp. 1995

Tesis "Propuesta de implementación de los protocolos de enrutamiento de la red de alto desempeño del Backbone de CUDI". Hans Ludwing Reyes Chavéz. Ciudad Universitaria. Junio 2003.

Tesis "Propuesta de implementación de los protocolos de enrutamiento de la red de alto desempeño del Backbone de CUDI". Hans Ludwing Reyes Chavéz. Ciudad Universitaria. Junio 2003.

Documentación "Backbone Gigabitethernet de RedUNAM". Gabriela Medina Galindo. DGSCA. Ciudad Universitaria. Agosto 2001.

A brief History of the Internet and Related Networks. V.G. Cerf, ISOC Document. November 2001.

A Brief History of Internet. Barry M Leiner, Vinton G. Cerf, David D.Clark, Robert E Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, ISOC Document. April 2003.

Presentación "Situación Actual de Internet 2 en México". Carlos Casasús LópezHermosa. Abril 2004

RFC 1933: Transition Mechanisms for IPv6 Hosts and Routers, R. Gilligan, E. Nordmark, <http://www.ietf.org/rfc/rfc1933.txt>. April 1996

RFC 2450: Proposed TLA and NLA Assignment Rules, R. Hinden, December 1998. <http://www.ietf.org/rfc/rfc2450.txt>

RFC 2772: 6Bone Backbone Routing Guidelines, R. Rockell, B. Fink, February 2000. <http://www.ietf.org/rfc/rfc2772.txt>

RFC 2921: 6Bone pTLA and pNLA Formats (pTLA), B. Fink, September 2000. <http://www.ietf.org/rfc/rfc2921.txt>

IPv6 la nueva generación de Internet, Comunicaciones World N° 146, J. Palet, Junio 2000. <http://www.idg.es/comunicaciones/mainart.asp?artid=110687>

Recomendaciones M.3010 y M.3400. The Series of TMN-Related recommendations

Recomendaciones Recommendations For Comments RFC 1155, 1212, 1157, 1213, 3330, 2439

Ligas:

Página del Grupo de trabajo de Enrutamiento de CUDI.

<http://www.abilene.iu.edu/abilene/documentation/policy-statements/prefix-length-routing-policy.html>

<http://apps.internet2.edu/>

<http://www.vbns.net>

<http://www.internet2.edu>

<http://www.isoc.org>

Pagina Web del Grupo de Trabajo de IPv6 de CUDI:

<http://www.ipv6.unam.mx/internet2.html>