

TRABAJO ESPECIAL DE GRADO

**PASE A PRODUCCIÓN DE LA FACILIDAD DE “VIRTUAL
PRIVATE NETWORKS” Y “VIRTUAL ROUTING” SOBRE LA
RED DE GESTIÓN DE DATOS (DCN) DE CANTV**

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Tovar F., Julián R.
para optar al Título de
Ingeniero Electricista

Caracas, 2005

TRABAJO ESPECIAL DE GRADO

PASE A PRODUCCIÓN DE LA FACILIDAD DE “VIRTUAL PRIVATE NETWORKS” Y “VIRTUAL ROUTING” SOBRE LA RED DE GESTIÓN DE DATOS (DCN) DE CANTV

TUTOR ACADÉMICO: Prof. Paolo Maragno
TUTOR INDUSTRIAL: Ing. Aymara Gámez

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Tovar F., Julián R.
para optar al Título de
Ingeniero Electricista

Caracas, 2005

CONSTANCIA DE APROBACIÓN

Caracas, 01 de junio de 2005

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por la Bachiller Julián R. Tovar F, titulado:

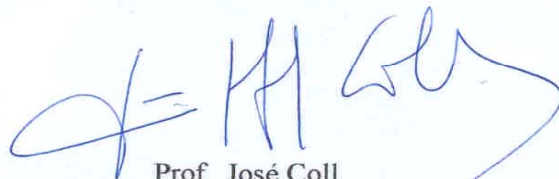
“PASE A PRODUCCIÓN DE LA FACILIDAD DE “VIRTUAL PRIVATE NETWORKS” Y “VIRTUAL ROUTING” SOBRE LA RED DE GESTIÓN DE DATOS (DCN) DE CANTV”

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.



Prof. Bartolomé Cusati

Jurado



Prof. José Coll

Jurado



Prof. Paolo Maragno
Prof. Guía

DEDICATORIA

A mis padres Julián y Margarita.

A mis hermanos July, Julián Enrique y Cora.

A Rafael y Rafael Aníbal.

A Amarelys.

AGRADECIMIENTOS

Un especial agradecimiento a mi tutora industrial la Ing. Ayamara Gaméz por su orientación y aporte en la realización de esta investigación.

Al Prof. Paolo Maragno, tutor académico de está investigación, por sus consejos y aportes.

A Luciano Gomes de Nortel Networks, por su ayuda en la realización de las pruebas sobre la maqueta e importante contribución con el desarrollo de la investigación..

Al Ing. Juan Figueira por darme la oportunidad de formar parte de CANTV.

A la Universidad Central de Venezuela, en especial la escuela de Ingeniería Eléctrica, por permitir desarrollarme como profesional.

A mis padres, mis hermanos y toda mi familia por su apoyo y comprensión durante toda la carrera. ¡Muchas Gracias!

A Amarelys por apoyarme en los momentos más difíciles y formar parte de este logro (Mi corazón TAMt)

A la familia Cobos Díaz por todo su cariño.

A Pedro por ser compañero y amigo durante toda la carrera.

A Nela y Salvador por creer en mi y darme esta oportunidad.

A todo el personal del piso 3 del NEA (CANTV) por hacerme sentir como uno más del ustedes.

ÍNDICE GENERAL

PAGINAS PRELIMINARES

CONSTANCIA DE APROBACIÓN.....	ii
DEDICATORIA.....	iii
AGRADECIMIENTOS.....	iv
ÍNDICE GENERAL.....	v
ÍNDICE DE FIGURAS.....	ix
ACRONIMOS.....	x
RESUMEN.....	xii

CUERPO DEL TRABAJO

INTRODUCCIÓN	1
CAPITULO I.....	4
EL PROBLEMA.....	4
1.1 PLANTEAMIENTO DEL PROBLEMA	4
1.2 JUSTIFICACIÓN DEL PROBLEMA.....	4
1.3 OBJETIVOS DEL PROYECTO	5
1.3.1 OBJETIVO GENERAL.....	5
1.3.2 OBJETIVOS ESPECIFICOS.....	5
1.4 METODOLOGÍA DE TRABAJO Y ALCANCE DE LA INVESTIGACIÓN. 5	
1.5 LIMITACIONES DE LA INVESTIGACIÓN.....	6
1.6 DESCRIPCIÓN DE LA EMPRESA DONDE SE REALIZÓ LA INVESTIGACIÓN.....	7
1.6.1 NOMBRE DE LA EMPRESA	7
1.6.2 DESCRIPCIÓN DE LA EMPRESA	7
1.6.3 MISIÓN DE LA EMPRESA	7
1.6.4 OBJETIVOS DE LA CORPORACIÓN	7
1.6.5 ESTRUCTURA ORGANIZATIVA DE CANTV	8
CAPITULO II	9

MARCO TEÓRICO.....	9
2.1 GESTIÓN DE REDES.....	9
2.1.1 FUNCIÓN DE LOS SISTEMAS GESTORES DE RED	9
1. Supervisión de la Red	9
2. Control de los dispositivos de la Red.....	9
3. Administración de la Red.....	9
2.1.2 COMPONENTES DE UN SISTEMA DE GESTIÓN.....	11
2.2 PROCESO DE PASE A PRODUCCIÓN (PAP).....	12
2.2.1 PARTES INTEGRANTES DEL PROCESO DE PAP.....	12
2.2.3 METODOLOGÍA PARA EL DESARROLLO DE PROYECTOS	13
2.3 FRAME RELAY.....	15
2.3.1 TRAMA FRAME RELAY	17
2.4 ASYNCHRONOUS TRANSFER MODE – ATM.....	18
2.4.1 CAPAS ATM.....	18
2.4.1.1 CAPA FÍSICA	19
2.4.1.2 CAPA ATM	19
2.4.1.3 CAPA DE ADAPTACIÓN ATM.....	21
2.4.1.3.1 AAL Tipo 1	21
2.4.1.3.2 AAL Tipo 2.....	22
2.4.1.3.3 AAL Tipo 3 / 4.....	22
2.4.1.3.4 AAL Tipo 5.....	22
2.4.2 CONEXIONES VIRTUALES ATM.....	22
2.4.2.1 CONEXIÓN VIRTUAL PERMANENTE – PERMANENT VIRTUAL CONNECTION (PVC).....	23
2.4.2.2 CONEXIÓN VIRTUAL CONMUTADA – SWITCHED VIRTUAL CONNECTION.....	23
2.4.2.3 CONEXIÓN VIRTUAL PERMANENTE SUAVE – SOFT PERMANENT VIRTUAL CONNECTION (SPVC).....	23
2.4.3 USER-TO-NETWORK INTERFACE (UNI) Y NETWORK – TO – NETWORK INTERFACE (NNI).....	24

2.5 OSPF – <i>OPEN SHORTEST PATH FIRST</i>	24
2.5.1 ALGORITMO DE LA RUTA MÁS CORTA (SHORTEST PATH).....	25
2.5.1.1 METRICA OSPF	26
2.5.1.2 ÁREAS Y ROUTERS DE BORDE.....	26
2.6 EQUIPOS PASSPORT NORTEL 7000	28
2.6.1 PROCESADORES DE CONTROL (CP).....	30
2.6.2 PROCESADORES DE FUNCIÓN (FP)	31
2.7 VIRTUAL PRIVATE NETWORK (VPN).....	31
2.8 FACILIDAD VPN DE PASSPORT	31
2.8.1 VPN EXTENDER CARD	32
2.8.2 OPCIONES PARA DESPLEGAR EL SERVICIO IP VPN	33
2.8.2.1 SERVICIO PREMIUM.....	33
2.8.2.2 SERVICIO AGREGADO.....	34
2.8.2.3 SERVICIO HÍBRIDO.....	35
2.9 IP SOBRE ATM	35
2.9.1 ATM MPE sobre PVC	36
2.9.2 ATM MPE SOBRE SOFT PVC	36
2.10 IP SOBRE FRAME RELAY	36
CAPITULO III.....	38
PROPUESTA DE OPTIMIZACIÓN DE LA RED DCN.....	38
3.1 RED ATM / FR DE CANTV	38
3.1.1 TOPOLOGÍA.....	38
3.1.2 TOPOLOGÍA.....	38
3.2 RED DCN DE CANTV	40
3.2.1 TOPOLOGÍA.....	40
3.3 PROPUESTA DE OPTIMIZACIÓN DE LA RED DCN	42
3.3.1 CREACIÓN DE LA CAPA DE DISTRIBUCIÓN	42
3.3.2 IMPLEMENTACIÓN DE LA FACILIDAD DE VPN Y VR SOBRE LA NUEVA PLATAFORMA.....	44
3.3.3 ARQUITECTURA OSPF	44
CAPITULO IV	47

4.1 AMBIENTE DE PRUEBA.....	47
4.2 TOPOLOGÍA DE LA RED DE GESTIÓN DE LA MAQUETA.....	49
4.3 DIGRAMA DE CONEXIÓN PARA LA REALIZACIÓN DE LAS PRUEBAS	50
4.4 VERIFICACIÓN DE LA FUNCIONALIDAD DE LA PLATAFORMA	52

ELEMENTOS FINALES

CONCLUSIONES.....	56
RECOMENDACIONES.....	58
BIBLIOGRAFÍA.....	59
ANEXOS.....	60

ÍNDICE DE FIGURAS

Figura 1 - 1 Esquema Organizativo de CANTV.....	8
Figura 2 - 1 Componentes de un Sistema de Gestión	11
Figura 2 - 2 Fases para el desarrollo de proyectos	14
Figura 2 - 3 Trama Frame Relay	17
Figura 2 - 4 Formato de la Celda ATM	19
Figura 2 - 5 Interfaces ATM	24
Figura 2 - 6 Áreas y Routers de Borde.....	27
Figura 2 - 7 Passport 7480	28
Figura 2 - 8 Placa Frontal de la VPN Xc	33
Figura 2 - 9 IP - VPN Servicio Premium	34
Figura 2 - 10 Servicio Agregado.....	35
Figura 3 - 1 Esquema general de la red ATM / Frame Relay de CANTV.....	39
Figura 3 - 2 Topología de la Red DCN actual	41
Figura 3 - 3 Capas jerárquicas de la nueva plataforma	43
Figura 3 - 4 Arquitectura OSPF de la nueva plataforma.....	45
Figura 3 - 5 Topología general de la plataforma propuesta.	46
Figura 4 - 1 Maqueta de Pruebas CET - CANTV	48
Figura 4 - 2 Red de Gestión Maqueta de Pruebas CET - CANTV	49
Figura 4 - 3 Configuración ambiente de pruebas	50
Figura 4 - 4 Configuración ambiente de pruebas (2)	51
Figura 4 - 5 Software de Gestión de los equipos Passport.....	60
Figura 4 - 6 Estatus del enlace entre el router 2610 XM y el Passport 7k.....	52
Figura 4 - 7 Verificación de tráfico desde el router hasta el Passport.....	53
Figura 4 - 8 Tabla de enrutamiento del Router Cisco 2610 XM.....	54

ACRÓNIMOS

AAL:	ATM Adaptation Layer
ATM:	Asynchronous Transfer Mode
CCITT:	Comite Consultatif International de Telegraphique et Telephonique (Icomite Consultivo Internacional de Telegrafia y Telefonía) [Ahora ITU-T]
CET:	Centro de Estudios de Telecomunicaciones
CP:	Control Processor
CVR:	Customer Virtual Router
DCN:	Data Communication Network
DLCI:	Data Link Connection Identifier
FP:	Function Processor
FR:	Frame Relay
FRAD:	Frame Relay Assembler / Disassembler (Ensamblador / Desensamblador Frame Relay)
FRND:	Frame Relay Network Device
HDLC:	High - Level Data Link Control
IP:	Internet Protocol
ITU:	International Telecommunication Union
LP:	Logical Processor
NNI:	Network to Network Interface
OSI:	Open System Interconnections
OSPF:	Open Shortest Path First
PAP:	Pase a Producción
PVC:	Permanent Virtual Circuit
RDSI:	Red Digital de Servicios Integrados
SP:	Service Provider
S-PVC:	Soft Permanent Virtual Circuit
SVC:	Switched Virtual Connection

TMN:	Telecommunications Management Network
UNI:	User to Network Interface
VC:	Virtual Connection
VCG:	Virtual Connection Gateway
VCI:	Virtual Circuit Identifier
VPI:	Virtual Path Identifier
VPN:	Virtual Private Network
VPN Xc:	Virtual Private Network Extender Card
VR:	Virtual Router
WAN:	Wide Area Network
X.25:	Protocolo de conmutación de paquetes.

Tovar F., Julián R.

PASE A PRODUCCIÓN DE LA FACILIDAD DE “VIRTUAL PRIVATE NETWORKS” Y “VIRTUAL ROUTING” SOBRE LA RED DE GESTIÓN DE DATOS (DCN) DE CANTV

Tutor Académico: Prof. Paolo Maragno. Tutor Industrial: Ing. Ayamara Gámez
Tesis. Caracas, U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica.
Ingeniero Electricista. Opción: Comunicaciones. Institución: CANTV. 2005. Año
2005. 59 h. + anexos

Palabras Claves: Virtual Private Networks, Virtual Routing, Enrutamiento, Gestión.

Resumen. El objetivo de esta investigación es el de elaborar una propuesta de optimización de la red de gestión de datos ó DCN (Data Communication Network) de la empresa CANTV y en paralelo llevar a cabo el proceso de pase a producción (PAP) cuya finalidad es la de realizar la transferencia tecnológica a la unidad encargada del mantenimiento y operación de la nueva plataforma cuando esta sea implementada. La finalidad de la red DCN es la de servir como medio para el monitoreo y administración en forma remota de los elementos de: conmutación (Cx), transmisión (Tx), datos (Dx), elementos de infraestructura, sensores, etc., que prestan servicio a clientes tanto internos como externos. La topología de la red actual no ofrece un medio seguro para la gestión de los elementos de red, ya que se basa en el establecimiento de enlaces únicos entre los dispositivos de gestión local y los dispositivos de gestión remota. Por ello la propuesta de la nueva plataforma está orientada a ofrecer una estructura jerárquica, altamente escalable y mucho más segura. Se aprovecharon las soluciones de Virtual Private Networks y Virtual Routing soportadas por los equipos Passport de la compañía Nortel, los cuales conforman la red ATM / Frame Relay de CANTV. En la propuesta de diseño se contempla el establecimiento de varias rutas para la conexión entre los dispositivos remotos y locales de gestión, al igual que se considera que la elección de la ruta de conexión se realice de forma automática por medio de la implementación del protocolo de enrutamiento dinámico llamado OSPF (*Open Shortest Path First* – Primera ruta abierta más corta). Se realizaron pruebas funcionales de la propuesta de optimización sobre una maqueta, las cuales nos permitieron comprobar el correcto funcionamiento del sistema.

INTRODUCCIÓN

En los últimos años las redes de comunicaciones se han convertido en parte silente de nuestra vida cotidiana. Conforme éstas han ido evolucionando y creciendo en importancia y complejidad tecnológica, los sistemas de gestión se han hecho de vital importancia. Una red que preste servicios de telecomunicaciones debe contar con un sistema de administración y gestión que asegure a los usuarios su utilización. El monitoreo de los dispositivos y elementos pertenecientes a la red se debe manejar proactivamente, y si se llegara a presentar algún problema, poder llegar a una solución rápida y eficiente.

El monitoreo de redes de cierto tamaño no se puede realizar manualmente debido a que las redes se hacen más heterogéneas, por tanto se requieren herramientas automatizadas de: gestión de fallas, de configuración y de seguridad, basadas sobre estándares que funcionen sobre la gran variedad de dispositivos de diferentes fabricantes, con interfaces de operador únicas y con capacidad de responder a las ordenes de un centro de control, donde se concentra todo lo relacionado con el monitoreo de la red. Así pues, se ha hecho muy común escuchar el término VPN (Virtual Private Network), debido a la gran demanda de redes privadas por parte de empresas, y dada su fuerte inserción en el mercado de los “Service Providers” (SPs). Las “Virtual Private Networks” (VPN) son una alternativa a la conexión WAN (Wide Area Network), bajando los costos de éstas y brindando los mismos servicios.

Una VPN es una red (corporativa, educativa, etc.) en que los distintos componentes que la conforman son conectados utilizando una infraestructura compartida, pero quedando lógicamente independiente y aislada de otras redes. La infraestructura compartida normalmente es provista por un proveedor de servicio (SP), quien administra los recursos y mantiene las políticas de acceso y seguridad dentro de su red.

Como parte integral de las VPN se encuentran los VR (“Virtual Router”); un “Virtual Router” es definido como la emulación de un router físico desde el punto de vista de software, tiene exactamente los mismos componentes que su contraparte física, por tanto, hereda todo los mecanismos y herramientas para su configuración, despliegue, operación y monitoreo, siendo su ventaja principal la consolidación de múltiples routers físicos en un solo sistema de software, logrando con esto la reducción de costos, energía, aspectos gerenciales y espacio físico.

Actualmente la red DCN (Data Communications Network), como se le conoce a la red de gestión de datos de CANTV, presenta una topología basada en enlaces estáticos, siendo esto contraproducente debido a que si algunos de estos enlaces llegara a fallar se perdería comunicación con el dispositivo de red, imposibilitando su gestión y pudiendo con esto generar problemas mayores hasta el punto de afectar al usuario final. Por medio de la red DCN de CANTV se puede realizar el monitoreo de los elementos de red como lo son: conmutación (Cx), Transmisión (Tx), Datos (Dx), incluyendo elementos de infraestructura como aires acondicionados, generadores, sensores de seguridad, etc.

Aprovechando la facilidad de “Virtual Routing” de los switches Passport Nortel, se busca optimizar la red de gestión de CANTV existente, creando para ello una topología redundante basada sobre una estructura jerárquica.

Esta investigación comprende el diseño y evaluación en maqueta de una propuesta de optimización de la red DCN, basándose en la facilidad de VR y VPN de los equipos Passport 7k de la Red ATM / FR de CANTV. La estructura de este informe está dividida en cinco (5) capítulos abarcando todo el desarrollo de la investigación. Cada uno de los capítulos trata de los siguientes puntos:

Capítulo I: El Problema

En este capítulo se estudia todo lo relacionado con el planteamiento del problema. Se justificará y se expondrán los objetivos, tanto generales como específicos, además del alcance y metodología empleada para el desarrollo de la investigación. Se incluye una descripción de la empresa donde se desarrolló la investigación.

Capítulo II: Marco Teórico

Corresponde a todas aquellas bases teóricas sobre las cuales se soporta el desarrollo de la investigación. En este capítulo se tratan los temas concernientes a: conceptos básicos de la gestión de redes, los estándares ATM y Frame Relay, OSPF, equipos Passport serie 7000 de Nortel y las distintas opciones para la implementación de VPN.

Capítulo III: Propuesta de Optimización de la Red DCN

Este capítulo presenta la estructura de la red ATM / FR de CANTV sobre la cual funciona la red DCN. Se estudia la topología actual de la red DCN, para luego presentar el diseño de la propuesta de optimización de la red de gestión de datos.

Capítulo IV: Pruebas Funcionales

En este capítulo se muestra la implementación de la propuesta de diseño sobre una maqueta de equipos Passport 7k / 15K que se encuentra en el Centro de Estudios de Telecomunicaciones (CET) de CANTV. También se describen una serie de pruebas que se realizaron sobre el diseño implementado en la maqueta, con sus respectivos resultados.

Por último, las conclusiones y recomendaciones producto de la investigación, se presenta la bibliografía consultada, y los anexos.

CAPITULO I

EL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La red de comunicación de datos (DCN por sus siglas en inglés) de la empresa CANTV, es una red diseñada específicamente para la gestión de los dispositivos de red interconectados a nivel nacional. Estos dispositivos generan señales de alarma que permiten su monitoreo en tiempo real. Los elementos a monitorear pueden ser: transmisión (Tx), Conmutación (Cx) o Datos (Dx), incluyendo elementos de acceso (radios, fibra óptica, etc.) y elementos de infraestructura (aires acondicionados, generadores, sensores de seguridad etc.), para de esta manera, si llegara a existir alguna degradación en uno de ellos, poderlo detectar proactivamente antes de que se generen problemas mayores.

Debido a la importancia que representa la gestión de estos equipos, la topología actual de la red DCN no se presenta como la más adecuada, por lo tanto, se plantea la necesidad de crear una plataforma que sea lo suficientemente flexible para aceptar la incorporación de nuevos elementos, ya que esta es una red en constante crecimiento. Además debe poder ofrecer seguridad y confiabilidad en el manejo de la gestión y administración de los dispositivos y elementos interconectados a ella.

1.2 JUSTIFICACIÓN DEL PROBLEMA

El motivo fundamental que impulsa el desarrollo de este proyecto de optimización de la red DCN de la empresa CANTV, se basa en el aprovechamiento de la facilidad de “Virtual Routers” (VR) y “Virtual Private Networks” (VPN), que

ofrecen los equipos Passport 7000, permitiendo con esto la creación de una plataforma jerárquica y segura para el manejo de las señales de gestión.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Presentar una propuesta de optimización de la red DCN mediante el diseño e implementación de la facilidad de “Virtual Routing” y “Virtual Private Networks” sobre los switches multiservicios Passport marca Nortel, actualmente usados en la red ATM / FR de CANTV a nivel nacional.

1.3.2 OBJETIVOS ESPECIFICOS

1. Proponer un diseño jerarquizado de la red de gestión o DCN.
2. Determinar los protocolos y dispositivos de interconexión entre las diferentes partes integrantes de la red de gestión.
3. Desarrollar el proceso de “Pase a Producción” de la facilidad de “Virtual Routing” y “Virtual Private Network”.
4. Validación de la propuesta de diseño mediante su implementación a nivel de maqueta, esto aplicado a los switches Passport para el funcionamiento de los mismos como enrutadores virtuales.

1.4 METODOLOGÍA DE TRABAJO Y ALCANCE DE LA INVESTIGACIÓN.

En función del objetivo general, los objetivos específicos y el planteamiento del problema de este proyecto, el desarrollo del mismo, en su primera fase, está orientado a un estudio detallado de la estructura y topología actual de la red de gestión DCN de CANTV, logrando con esto establecer las deficiencias y fallas que se quieren corregir.

En tal sentido, la segunda y tercera fase del proyecto consisten en una exhaustiva revisión y análisis bibliográfico de documentos, libros de texto, páginas web especializadas y manuales de los equipos Passport, con el objetivo de estudiar y comprender las alternativas que ofrece el proveedor de tecnología, y cuales de estas aplican en forma más conveniente al proyecto, generando así la propuesta de optimización.

La cuarta fase tiene por objetivo determinar los dispositivos de interconexión necesarios para el desarrollo del proyecto, en esta fase se desarrolla la matriz de requerimientos del proceso de “Pase a Producción”, requerimientos que son necesarios para la explicación con el mayor detalle de la nueva plataforma. Estos requerimientos se entregan a la unidad encargada de la operación y mantenimiento de la plataforma, garantizando con ello que se efectúe el proceso de transferencia tecnológica necesaria para la correcta operación de la nueva plataforma y bajo los parámetros de calidad establecidos.

En la quinta fase se valida la propuesta de optimización de la red de gestión, mediante su implementación en la maqueta de CANTV de equipos Passport 7000 y 15000, y la aplicación, sobre esta, de ciertas pruebas para comprobar su correcto funcionamiento.

En la sexta y última fase del proyecto, se realiza la entrega de los requerimientos desarrollados en la cuarta fase, en una reunión de cierre, a la unidad encargada de la operación y mantenimiento de la nueva plataforma.

1.5 LIMITACIONES DE LA INVESTIGACIÓN.

La propuesta de optimización de la red DCN estará limitada a las soluciones que ofrezca el fabricante y además deben compatibles con los elementos de red actualmente instalados.

Otra limitación encontrada durante el desarrollo de la investigación, corresponde a las pruebas funcionales de la propuesta de diseño. Debido a la poca distancia de los equipos que simulan la red en la maqueta de pruebas, los retardos en la propagación de la información no son comparables con los retardos que se presentarían en la red real.

1.6 DESCRIPCIÓN DE LA EMPRESA DONDE SE REALIZÓ LA INVESTIGACIÓN

1.6.1 NOMBRE DE LA EMPRESA

CANTV

1.6.2 DESCRIPCIÓN DE LA EMPRESA

Cantv fue la primera empresa que funcionó en Venezuela para proveer servicios de telecomunicaciones. En sus inicios, la telefonía básica fue uno de los servicios privilegiados. Hoy en día, la gama de productos y servicios abarcan desde interconexión, comunicaciones de larga distancia nacional e internacional en toda Venezuela. Desde su privatización en 1991, la compañía ha experimentado una constante transformación para convertirse en una empresa competitiva, con altos niveles de calidad en la oferta de sus productos y servicios, entre ellos: telefonía pública, telefonía celular, buscapersonas, centros de comunicación comunitaria, redes privadas, servicios de telefonía rural, hosting, servicios inalámbricos, transmisión de datos, servicios de directorios de información y distintos servicios de valor agregado.

1.6.3 MISIÓN DE LA EMPRESA

Mejorar la calidad de vida de la gente en Venezuela al proveer soluciones de comunicaciones que excedan las expectativas de los clientes.

1.6.4 OBJETIVOS DE LA CORPORACIÓN

- Ser el proveedor dominante de soluciones integrales de telecomunicaciones en el mercado, defendiendo la marca y el cliente.

- Aplicar la tecnología para responder oportunamente a las necesidades y requerimientos del mercado. Crear y mantener ventajas competitivas mediante el manejo de la información de la base de clientes.
- Crear y mantener ventajas competitivas basadas en la calidad de los recursos humanos y servicios.

1.6.5 ESTRUCTURA ORGANIZATIVA DE CANTV

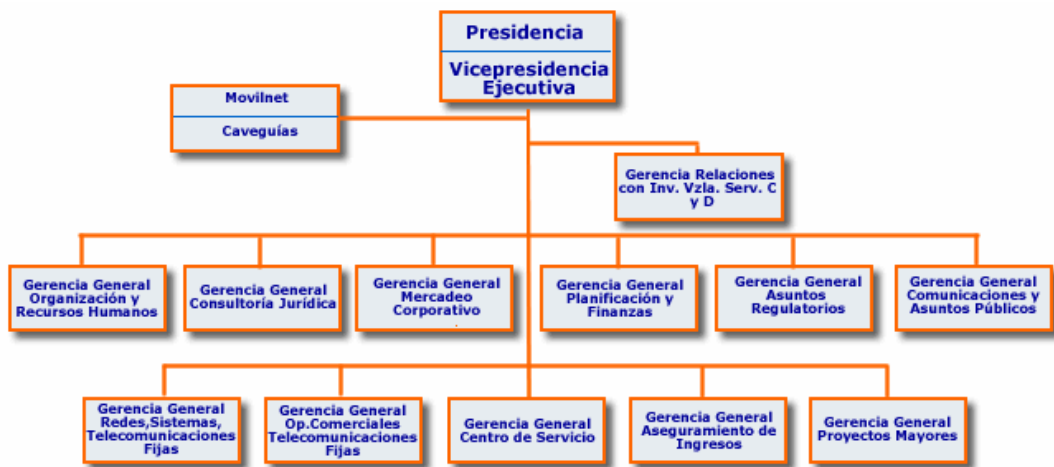


Figura 1 - 1 Esquema Organizativo de CANTV

Este trabajo especial de grado se llevo a cabo bajo la Gerencia General Redes, Sistemas, Telecomunicaciones Fijas, específicamente en la Coordinación de Reingeniería de Datos, a cargo de la Gerencia de Planificación e Ingeniería.

CAPITULO II

MARCO TEÓRICO

2.1 GESTIÓN DE REDES

La ISO (International Organization for Standardization) define a la gestión de red como: “El conjunto de elementos de control y supervisión de los recursos que permiten que la comunicación tenga lugar sobre la red”

2.1.1 FUNCIÓN DE LOS SISTEMAS GESTORES DE RED

1. Supervisión de la Red

Se suele Realizar de dos formas: mediante una estación de gestión (ordenador personal o estación de trabajo) que reciba mensajes de los dispositivos de la red (puentes o *bridges*, routers, servidores de terminales,etc.) o mediante una estación que pregunte regularmente el estado de los dispositivos.

2. Control de los dispositivos de la Red

Se realiza enviando comandos por la red, desde la estación de gestión hasta los dispositivos de red para cambiar su configuración o estado.

3. Administración de la Red

Además de la gestión operativa (Atender usuarios, resolver fallas en el menor tiempo posible, monitoreo, etc.) existen otros aspectos involucrados que permiten definir el análisis y optimización de la red:

- a) Descripción funcional de tareas que serán objetos de gestión.

- b) Adecuación organizativa de las entidades u organismos.
- c) Especificación de procedimientos que faciliten la tramitación de sucesos de interés.
- d) Adquisición y adaptación de medios técnicos y humanos.

A continuación se presentan las ventajas tanto técnicas como funcionales de los Sistemas de Gestión de redes, cumpliendo con el estándar TMN para la gestión de redes propuesto por la ITU (ITU-T M.3400) el cual comprende 5 áreas funcionales:

- Gestión de fallas
- Gestión de configuración
- Gestión de facturación
- Gestión de desempeño
- Gestión de seguridad

Ventajas Técnicas:

- Administración de entornos heterogéneos desde una misma plataforma.
- Administración de elementos de interconexión.
- Interfaces con grandes sistemas.
- Evolución según las necesidades del cliente.

Ventajas Funcionales:

- Gestión del nivel de servicio, para garantizar la disponibilidad, la atención a los usuarios, el tiempo de respuesta, etc.
- Gestión de problemas, para facilitar la segmentación de los mismos resolviéndolos en etapas o niveles.
- Gestión de cambios, para minimizar el impacto asociado habitualmente con los procesos de modificación de las configuraciones existentes.

2.1.2 COMPONENTES DE UN SISTEMA DE GESTIÓN

Los componentes de un sistema de gestión de red y las relaciones entre ellos se representa en el siguiente diagrama:

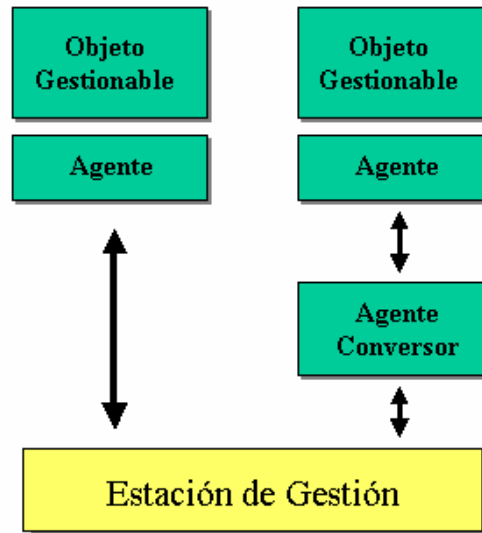


Figura 2 - 1 Componentes de un Sistema de Gestión

1. Objeto gestionable (Elemento de red):

Representa cualquier dispositivo físico o lógico de la red y el equipamiento lógico relacionado con él, que permita su gestión.

2. Agente:

Es el equipamiento lógico de gestión que reside en el objeto gestionable.

3. Protocolo:

Utilizado por el agente para pasar información entre el objeto gestionable y la estación de gestión.

4. Objeto Ajeno:

Se define como un objeto gestionable que utiliza un protocolo ajeno, es decir, un protocolo distinto al de la estación de gestión.

5. Agente conversor:

Actúa de conversor entre el protocolo ajeno y el protocolo utilizado por la estación de gestión.

6. Estación de gestión:

Esta formada por varios módulos o programas. Es una estación de trabajo u ordenador personal

2.2 PROCESO DE PASE A PRODUCCIÓN (PAP)

Son las actividades que deben ser realizadas por cada una de las Unidades encargadas del desarrollo e implantación de una Plataforma o Servicio, así como en su posterior puesta en producción, para que finalmente la Gerencia General de Redes y Sistemas Telecomunicaciones Fijas asuma la responsabilidad de la Operación, Mantenimiento, Administración, Soporte y Monitoreo de la nueva Plataforma o Servicio.

Este proceso se hace con el objetivo de que el proyecto se desenvuelva de una manera estructurada y organizada, garantizando que se efectúe el proceso de transferencia tecnológica necesaria para la correcta operación de la nueva plataforma bajo los parámetros de calidad establecidos.

2.2.1 PARTES INTEGRANTES DEL PROCESO DE PAP

CLIENTES: Son todas aquellas Unidades, internas o externas, que requieren de un servicio de alguna unidad Operativa, en cuanto a Operación, Mantenimiento, Administración, Soporte y Monitoreo de una Plataforma o Servicio.

SOLICITANTE DEL PASE A PRODUCCIÓN: Corresponde a cualquier Unidad o empleado adscrito a la Gerencia General de Redes y Sistemas Telecomunicaciones Fijas o no, que genera una solicitud de Pase a Producción, siendo de este modo el responsable de cumplir con todas las actividades y documentación para la aceptación en Producción de una Plataforma o Servicio.

PLATAFORMAS Y SERVICIO: Se definen como cualquier Producto, Componente, Aplicación, u otro elemento que se encuentre dentro de alguna Plataforma y requiere ser Operado, Administrado, Monitoreado o Soportado por las unidades de Gerencia General de Redes y Sistemas Telecomunicaciones Fijas.

OPERACIONES: Al usar este término se hace referencia a la Unidad Operativa que pertenece a la Gerencia General de Redes y Sistemas Telecomunicaciones Fijas que realiza actividades de operación, mantenimiento, administración, soporte y monitoreo.

LIDER DE PROYECTO: Es la persona responsable del desarrollo de la nueva Plataforma o Servicio, independientemente de la descripción del cargo que tenga y Unidad a la que pertenezca, y será la persona designada para canalizar y gestionar el proceso de pase a producción ante la Gerencia de Gestión de la Calidad.

2.2.3 METODOLOGÍA PARA EL DESARROLLO DE PROYECTOS¹

A continuación se hará mención a la metodología para el desarrollo de proyectos, con el fin de definir los aspectos involucrados en el proceso de Pase a Producción, así como la relación de cada uno de ellos con las fases establecidas en dicha metodología. En cada una de estas fases se desarrollan una serie de documentos y controles asociados con la elaboración de un proyecto.

¹ La metodología adoptada por CANTV para el desarrollo de proyectos corresponde a la propuesta por el PMI (Project Management Institute).



Figura 2 - 2 Fases para el desarrollo de proyectos

Fase I: Inicio

Esta fase corresponde a la conceptualización y diseño del proyecto. En este momento se deben identificar las necesidades del cliente, para ello el Gerente de Cuenta debe convocar a reunión al personal perteneciente a la Gerencia General de Redes y Sistemas Telecomunicaciones Fijas y a todas las áreas que se involucrarán en el desarrollo del Servicio, el propósito de la reunión es identificar en forma mancomunada las oportunidades del proyecto, definir sus objetivos, alcance, marco de tiempo, asignar el líder, evaluar las posibles soluciones al problema planteado, seleccionar la mejor y obtener la aprobación de la Empresa.

Fase II: Planificación

En esta Fase es donde se realiza la reunión de arranque del proyecto a fin de informar el objetivo y el alcance. La información recibida en esta fase servirá de base para la planificación de las actividades en la futura responsabilidad como administrador del nuevo servicio, así como para generar el Plan de Proyecto.

Fase III: Ejecución

En esta fase se ejecutan las actividades identificadas en el Plan de Proyecto, se asegura que sea completado de acuerdo al programa y a los requerimientos, se coordinan los equipos de trabajo, se efectúan reuniones periódicas de seguimiento, se preparan informes periódicos, se elaboran reportes, minutas sobre asuntos pendientes y se distribuye la información dentro de los integrantes del proyecto.

Una de las actividades de esta fase es la elaboración de la documentación para el Pase a Producción. Esta documentación debe iniciarse en esta fase para que una vez que el proyecto esté listo, no se retrase su Pase a Producción y la entrega a la unidad de operación sea de forma gradual, por esto se recomienda contacto permanente con el personal de la Gerencia General de Redes y Sistemas Telecomunicaciones Fijas para la revisión periódica de la documentación.

Igualmente durante esta Fase se deben ir desarrollando las Pruebas de Aceptación, en donde los responsables de la ejecución del proyecto deberán realizar y documentar pruebas de la Plataforma o Servicio en sus diferentes versiones, basándose en constatar que se cumplan cada una de las especificaciones del Servicio y su funcionalidad. Durante esta etapa se deben hacer las correcciones que sean necesarias a fin de cumplir con la Calidad del Servicio.

Fase IV: Control

Esta es la fase de seguimiento continuo al Plan de Proyecto, en donde se mide el avance físico de las actividades, se controlan las horas de ejecución, los cambios de alcance, y se recomiendan soluciones para resolver asuntos críticos. Como actividad puntual dentro de esta fase es el control de la documentación para el Pase a Producción y la transferencia de conocimientos.

Fase V: Cierre

Esta Fase incluye el informe de cierre asociado al progreso del proyecto en términos de costo, programación y desempeño, se prepara la documentación histórica, se revisa la documentación para el Pase a Producción y se procede a la firma del acta de aceptación por parte de las unidades involucradas en el servicio.

2.3 FRAME RELAY

Frame Relay comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25 y RDSI (Red Digital de Servicios Integrados): La

UIT (Unión Internacional de Telecomunicaciones - entonces CCITT). Sus especificaciones fueron definidas por ANSI (American National Standard Institute), fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los conmutadores, en cada "salto" (hop) de la red. X.25 tiene el grave inconveniente de su importante "overhead" producido por los mecanismos de control de errores y de flujo.

Frame Relay, por el contrario, maximiza la eficiencia, aprovechándose para ello de las modernas infraestructuras, de mucha mayor calidad y con muy bajos índices de error, y además permite mayores flujos de información.

Frame Relay es un protocolo de red basado en una versión sincronizada de HDLC (High – Level Data Link Control). La data es enviada como paquetes HDLC, llamados “frames”, por tanto se puede definir como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 45 Mbps. Cabe destacar que la corrección de errores en este protocolo es “end – to – end”, es decir, se delega la corrección de errores a los equipos terminales, dejándole únicamente a los switches Frame Relay la función de conmutar.

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red. Este equipo se denomina FRAD o "Ensamblador / Desensamblador Frame Relay" (Frame Relay Assembler / Disassembler) y el nodo de red se denomina FRND o "Dispositivo de Red Frame Relay" (Frame Relay Network Device).

2.3.1 TRAMA FRAME RELAY

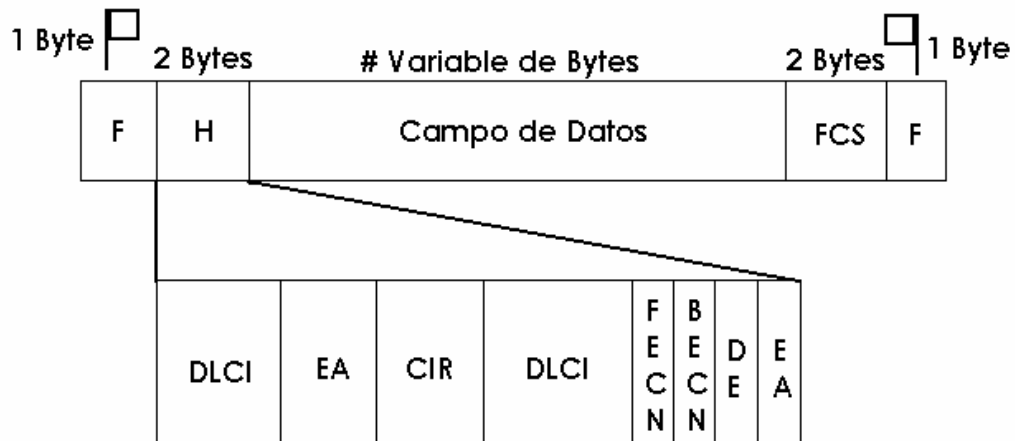


Figura 2 - 3 Trama Frame Relay

F	Flag (Bandera de Inicio / Finalización)
H	Header (Encabezado)
FCS	Frame Check Sequence (Secuencia de revisión de trama)
DLCI	Data Link Connection Identifier (Identificador de Conexión de enlace de Datos).
EA	Extended Adress (Dirección extendida)
CIR	Committed Information Rate (Tasa de Información Comprometida).
FECN	Forward Explicit Congestion Notification. (Notificación de Congestión Explicita hacia delante)
BECN	Backward Explicit Congestion Notification. (Notificación de Congestión Explicita hacia atrás).
DE	Elección de descargo.

Tabla 2-1 Acrónimos de la Trama Frame Relay

Una trama Frame Relay, puede ser enviada sobre cualquier enlace serial. Cada trama está delimitada por dos secuencias de bits llamadas banderas (“flags”), cuya

unicidad en el caudal de bits está garantizada. Solo puede existir una bandera entre tramas. Aparte de los datos del usuario, existen sólo dos campos de datos en una trama: el encabezado y la cola. El encabezado viene después de la bandera de inicio y contiene el DLCI, además de algunos bits de señalización.

2.4 ASYNCHRONOUS TRANSFER MODE – ATM

ATM es un estándar para transporte de paquetes, diseñado con la idea de soportar tráfico de naturaleza diversa, tal como el de redes *B-ISDN* (Red Digital de Servicios Integrados) que incluyen voz, datos y video.

El protocolo ATM se basa en la tecnología de conmutación de celdas. ATM crea rutas entre los nodos llamadas circuitos virtuales (*VC – Virtual Circuits*). Estas celdas provienen de diferentes fuentes representadas como generadores de bits a tasas de transferencia constantes como la voz y a tasas variables tipo ráfagas (*burst traffic*) como los datos. Cada celda es compuesta por 53 bytes, de los cuales 48 son para transferencia de información y los restantes para uso de campos de control (Cabecera ó Header en inglés) con información de “quién soy” y “donde voy”; esta información es suministrada por un “Virtual Circuit Identifier” (VCI) y un “Virtual Path Identifier” (VPI) dentro de esos campos de control, que incluyen tanto el enrutamiento de celdas como el tipo de conexión. La organización de la cabecera (header) variará levemente dependiendo de si la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local, ya que pueden ser cambiados de interface a interface.

2.4.1 CAPAS ATM

La arquitectura ATM utiliza un modelo lógico para describir las funciones que soporta. La funcionalidad ATM corresponde a las capas Físicas y de Enlace del modelo de referencia OSI (Open System Interconnections). Específicamente el

modelo ATM posee tres capas principales: la capa física, la capa ATM y la capa de adaptación ATM o AAL (ATM Adaptation Layer).

2.4.1.1 CAPA FÍSICA

Define las interfases físicas con los medios de transmisión y el protocolo de trama para la red ATM, es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado. ATM es independiente del transporte físico. Las celdas ATM pueden ser transportadas en redes SONET (Synchronous Optical Network), SDH (Synchronous Digital Hierarchy), STM – 1, STM – 4, STM – 16, T3/E3, TI/EI o aún en modems de 9600 bps.

2.4.1.2 CAPA ATM

Define la estructura de la celda y cómo las celdas fluyen sobre las conexiones lógicas en una red ATM, esta capa es independiente del servicio. En la siguiente figura se presenta el formato de una celda ATM.

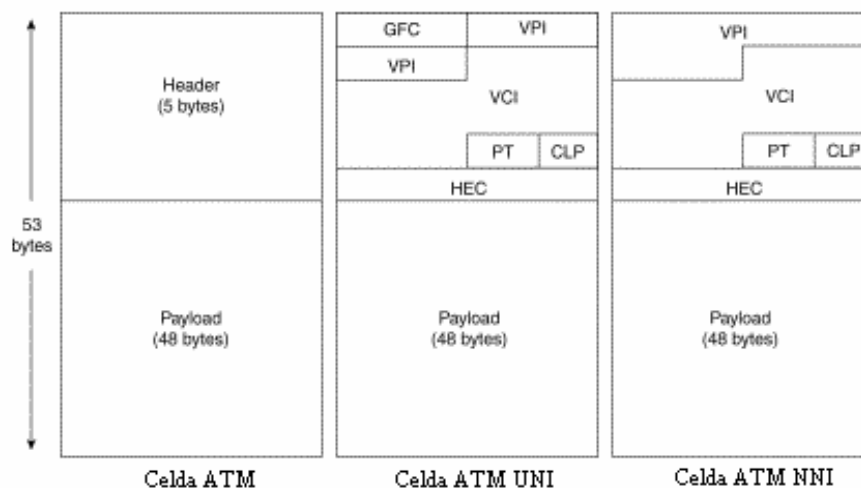


Figura 2 - 4 Formato de la Celda ATM

A continuación se describen los campos de las celdas ATM,

- 1) GFC – Generic Flow Control: Provee funciones locales, tales como identificar las múltiples estaciones que comparten una única interface ATM. Este campo no es utilizado generalmente, por lo tanto su valor típico es cero (0).
- 2) VPI – Virtual Path Identifier: En conjunto con el VCI, identifica el próximo destino de una celda que pasa a través de una serie de switches ATM.
- 3) VCI – Virtual Channel Identifier: Trabaja en conjunto con el VPI para identificar el próximo destino de una celda ATM.
- 4) PT – Payload Type: Su primer bit indica si la celda contiene datos de control o datos de usuario. Si la celda contiene datos de usuario, el bit se configura en cero (0), si contiene datos de control el bit se configura en uno (1). El segundo bit indica congestión (0 = no congestión, 1 = congestión). El tercer bit indica si la celda es la última de una serie de celdas que representan una trama AAL 5, si su valor es uno (1) indica que es la última celda de la trama.
- 5) CLP – Cell Loss Priority: Indica si la celda debería ser descartada si se encuentra en una situación de extrema congestión. Si el bit CLP es igual a uno (1), la celda debería ser descartada, dándole prioridad a las celdas cuyo valor del bit CLP es igual a cero (0).
- 6) HEC – Header Error Control: Revisa si hay errores en los primeros 4 bytes de la cabecera. HEC solo puede corregir un solo bit de los bytes revisados, permitiendo con esto que la trama no sea descartada.

2.4.1.3 CAPA DE ADAPTACIÓN ATM

La tercera capa es la ATM Adaptation Layer (AAL). La AAL juega un rol clave en el manejo de múltiples tipos de tráfico para usar la red ATM, y es dependiente del servicio. Específicamente, su trabajo es adaptar los servicios dados por la capa ATM a aquellos servicios que son requeridos por las capas más altas, tales como emulación de circuitos (circuit emulation), vídeo, audio, etc. La AAL recibe los datos de varias fuentes o aplicaciones y los convierte en los segmentos de 48 bytes.

La capa de adaptación se divide en dos subcapas:

1) Capa de convergencia (Convergence Sublayer - CS) :

En esta capa se calculan los valores que deben llevar la cabecera y los payloads del mensaje. La información en la cabecera y en el “payload” depende de la clase de información que va a ser transportada.

2) Capa de Segmentación y reensamblaje (Segmentation And Reassembly - SAR):

Esta capa recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes ATM. Agrega la cabecera que llevara la información necesaria para el reensamblaje en el destino.

Cinco tipos de servicio AAL están definidos actualmente:

2.4.1.3.1 AAL Tipo 1

La capa de adaptación ATM Tipo 1 esta diseñada para transferir tasas de bits constantes que dependen del tiempo. Por tanto, la información de sincronismo debe enviarse con los datos. AAL-1 provee recuperación de errores e indica la información con errores que no podrá ser recuperada. Un buen ejemplo del tipo de tráfico que maneja este tipo de capa de adaptación es el de transmisión de video sin comprimir.

2.4.1.3.2 AAL Tipo 2

AAL-2 se usa para transferir datos con tasa de bits variable que dependen del tiempo. Envía la información de sincronismo conjuntamente con los datos para que esta pueda recuperarse en el destino. AAL-2 provee recuperación de errores e indica la información que no puede recuperarse. Un ejemplo del tráfico que puede manejar este tipo de capa de adaptación es el de voz sobre DSL (VoDSL).

2.4.1.3.3 AAL Tipo 3 / 4

Estos dos tipos (3 y 4) son combinados dentro de un solo protocolo (AAL 3 / 4), el cual es diseñado para transmitir tasas de bits variables como: tráfico asíncrono (tipo 3) ó paquetes de datos no orientados a la conexión (tipo 4). AAL 3 / 4 provee tanto control de errores como mecanismos para recuperación.

2.4.1.3.4 AAL Tipo 5

AAL 5 esta diseñado para transmitir la misma tasa variables de bits suportada por AAL 3 / 4 (tráfico asíncrono, paquetes de datos no orientados a conexión), pero sin los requerimientos de mecanismos de recuperación y control de errores. Un ejemplo de este servicio es “Classical IP over ATM”, “LAN Emulation” (LANE) y RFC 1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5). AAL 5 asume que los mecanismos de recuperación y control de errores son ejecutados por las capas superiores, por tanto, los 48 bytes destinados para carga útil, efectivamente pueden ser utilizados en su totalidad para la transmisión de datos. También asume que un único mensaje es transmitido sobre el UNI (User – to – Network Interface) a la vez, si existe más de un usuario al mismo tiempo, los mensajes entran en cola para una transmisión secuencial. Este servicio también es conocido como Capa de Adaptación Simple y Eficiente ó SEAL (Simple and Efficient Adaptation Layer) por sus siglas en ingles.

2.4.2 CONEXIONES VIRTUALES ATM

Debido a que ATM es orientado a la conexión, obliga a establecimiento de una conexión desde el usuario origen al usuario destino antes de que se inicie la

transmisión de información. Existen dos (2) tipos de conexiones virtuales: permanentes y conmutadas.

2.4.2.1 CONEXIÓN VIRTUAL PERMANENTE – PERMANENT VIRTUAL CONNECTION (PVC)

Una conexión virtual permanente es una conexión lógica dentro de la red que se establece entre dos puntos y es perdurable en el tiempo. Usualmente múltiples PVC comparten el mismo medio físico.

2.4.2.2 CONEXIÓN VIRTUAL CONMUTADA – SWITCHED VIRTUAL CONNECTION

A diferencia de las conexiones permanentes, las conexiones conmutadas se establecen por medio de señalización a raíz de una solicitud de llamada en el punto de origen, por lo que no se hace necesario la configuración de los nodos a lo largo de la trayectoria. Sin embargo, la red debe tener la capacidad de poder enrutar la conexión automáticamente.

En este tipo de conexiones el tiempo de duración es relativamente corto, tanto así que se les conoce como conexiones temporales, y esto se debe que la conexión se libera al terminar la transmisión de información.

2.4.2.3 CONEXIÓN VIRTUAL PERMANENTE SUAVE – SOFT PERMANENT VIRTUAL CONNECTION (SPVC).

Las Soft PVC establecen una conexión lógica entre dos puntos, esta conexión es invariable en el tiempo hasta que una de los switches ATM presenta una falla, en este caso, la soft PVC será reenrutada sobre la red ATM.

2.4.3 USER-TO-NETWORK INTERFACE (UNI) Y NETWORK – TO – NETWORK INTERFACE (NNI)

Es la interfaz que conecta los equipos de usuario ATM CPE (ATM Customer Premises Equipment) con los elementos de una red ATM pública o privada. NNI se refiere a la interface que conecta dos nodos dentro de la red.

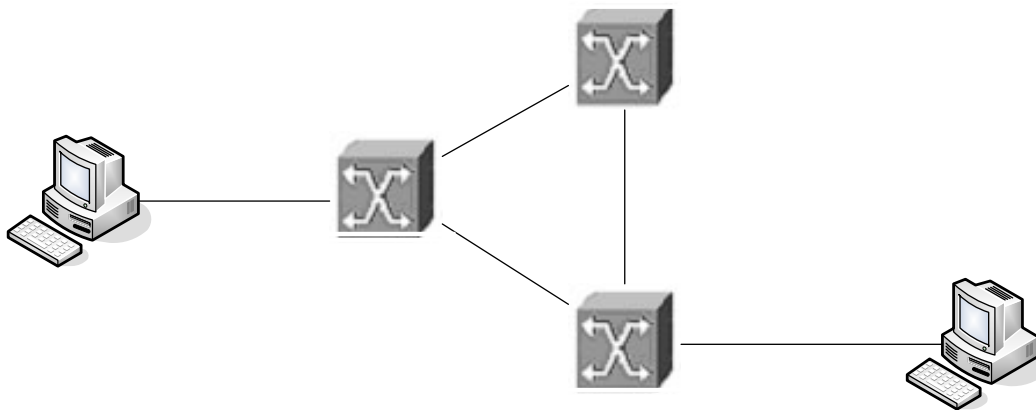


Figura 2 - 5 Interfaces ATM

2.5 OSPF – OPEN SHORTEST PATH FIRST

OSPF es el nombre de uno de los protocolos de enrutamiento dinámico IP. El enrutamiento dinámico ocurre cuando los routers informan a los routers adyacentes, a que red están actualmente conectados. Los routers se comunican usando un protocolo de enrutamiento que es manejado por el “Routing Daemon”². En contraste con los protocolos estáticos, donde la información yace dentro de tablas de enrutamiento, en los protocolos dinámicos las rutas son añadidas y borradas dinámicamente por el “Routing Daemon”. El “Routing Daemon” añade y borra rutas de enrutamiento al

² Routing Daemon: Proceso del router que se encarga de manejar todo lo referente al protocolo de enrutamiento.

sistema, eligiendo que rutas insertar en la tabla de enrutamiento. En el caso de múltiples rutas con el mismo destino, el “Routing Daemon” elige que ruta es la mejor, por el otro lado, si un enlace se cae, el “Routing Daemon” borra las rutas conectadas a ese enlace, y encuentra rutas alternas para ese destino (si existen).

Diferentes protocolos de enrutamiento son utilizados en las grandes redes, Internet, por ejemplo, esta dividido en una colección de sistemas autónomos (Autonomous Systems – AS’s), los cuales normalmente son manejados por una única entidad. Cada sistema autónomo utiliza su protocolo de enrutamiento para la comunicación entre sus routers. Estos protocolos son llamados IGP (Internal Gateway Protocol).

OSPF fue desarrollado debido a la necesidad dentro de la comunidad de Internet de introducir un IGP altamente funcional y no – propietario, para la familia de protocolos TCP / IP. La discusión para la creación de un IGP común para Internet comenzó en 1988 y no se formalizó sino hasta 1991, para ese entonces el grupo de trabajo OSPF, solicitó que OSPF fuese considerado como un estándar para Internet. El protocolo OSPF es basado en la tecnología de “Estado de Enlace” (link – state). El “Estado de Enlace” es una descripción de la interfase y su relación con los routers vecinos, la descripción de la interfase puede incluir, por ejemplo, la dirección IP de la interfase, la mascara, el tipo de red a la cual esta conectado, los routers conectados a la red, etc. (Cisco Systems, OSPF)

2.5.1 ALGORITMO DE LA RUTA MÁS CORTA (SHORTEST PATH)

La ruta más corta es calculada utilizando el algoritmo Diskjtra. El algoritmo coloca cada router en la raíz de un árbol y calcula la ruta más corta para cada destino, basado en la métrica acumulada para alcanzar dicho destino. La ruta que tenga la métrica menor será la ruta más corta. Cada router tendrá su propia visión de la topología de la red.

2.5.1.1 METRICA OSPF

La métrica de una interfase OSPF es una indicación del costo de operación requerido para enviar paquetes a través de dicha interfase, entendiéndose como costo de operación factores como: (1) retardo, (2) capacidad del canal y (3) conectividad. Si el retardo es excesivo la capacidad del canal es muy pequeña generando una métrica elevada, respecto al factor de conectividad es obvio que cada router debe estar en la capacidad de establecer enlaces que permitan alcanzar el destino final, si esto no se logra el valor de la métrica es irrelevante. (RFC 1245)

Después que el router construye el árbol de la ruta más corta (Shortest Path Tree), empezará a construir la tabla de enrutamiento acorde a la topología aprendida. Las redes directamente conectadas tendrán una métrica de cero (0), y las otras redes tendrán una métrica acorde a la topología del árbol.

2.5.1.2 ÁREAS Y ROUTERS DE BORDE

Las áreas son introducidas para colocar límites en el intercambio de información de actualización de los estados de enlace. El cálculo del algoritmo Dijkstra de un router es limitado a los cambios dentro de un área. Todos los routers dentro de un área tienen la misma base de datos de los estados de enlace. Los routers que pertenecen a múltiples áreas, llamados Routers de Borde ó *Area Border Routers* en inglés, tienen la tarea de discriminar la información de enrutamiento entre áreas.

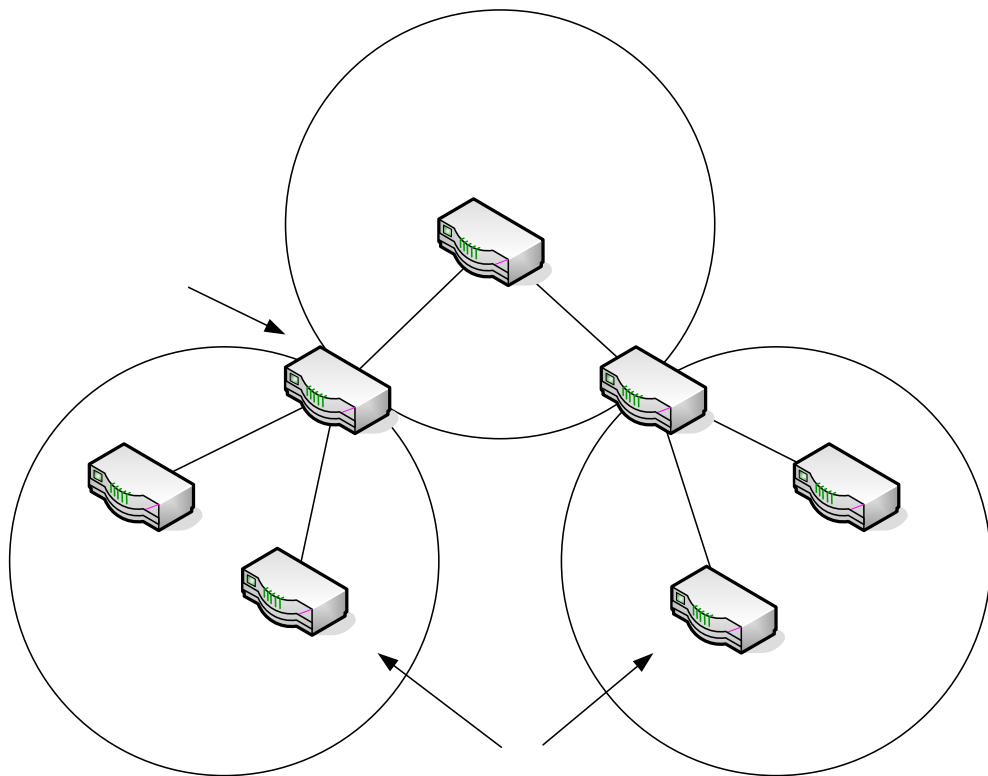


Figura 2 - 6 Áreas y Routers de Borde

Área 0

Router de Borde

2.6 EQUIPOS PASSPORT NORTEL 7000



Figura 2 - 7 Passport 7480

Estos equipos se definen como switches multiservicios o nodos integrados dentro de la categoría *Carrier Backbone – Edge* pertenecientes al núcleo y borde de una red pública de servicios ATM, que pueden interactuar con voz y otras tecnologías de datos, como Frame Relay e IP.

Los passport 7000 ó 7k, como se les conoce, soportan una gran variedad de servicios e interfaces, a continuación se muestra un listado de las más importantes para este proyecto:

- **Servicios ATM**
 - SVCs, SPVPs, SPVCs, PVPs, y PVCs
 - UNI 3.0, 3.1, 4.0 con *interworking* ILMI 4.0, AINI
 - Punto a Multipunto (Point-to-multipoint - lógico y espacial)

- **Servicios IP**
 - IP VPN's (soporta 1000 VPN's por nodo)
 - Gestión IP VPN
 - Filtrado IP
 - Tuneles IP
 - Protocolos de Enrutamiento: OSPF, RIPv1, RIPv2, ISIS, BGP-4, MPBGP-4

- **Servicios Frame Relay**
 - FR UNI y NNI (FRF.1, FRF. 2)
 - Forum UIT-T, ANSI, Frame Relay y Vendor
 - PVCs y SVCs
 - Señalización por DLCI y por Puerto

- **Interfaces ATM (ATM UNI/NNI y MPLS)**
 - DS1/E1, IMA (nxDS-1/nxE1), DS-3/E3, DS-3/E3ch, OC-3c/STM-1c.

- **Interfaces y Transporte IP**
 - 10/100 Base T
 - VPN Extender Card
 - FR (RFC1490), PPP (RFC1661), ATM (RFC1483R/RFC1483B Termination)

- **Interfaces Frame Relay**
 - V.11, V.35, HSSI, DS-0, DS-1, DS-3, DS-3 y STM-1.

Físicamente los equipos Passport poseen ranuras para la inserción de tarjetas, que son las que se encargan de ejecutar las distintas funciones que realizan estos dispositivos, permitiendo transportar y proporcionar el gran rango de servicios e interfaces que mencionamos anteriormente. En especial nos estaremos enfocando en el modelo Passport 7480, debido a que este es el modelo utilizado en el borde de la red ATM / FR de la empresa CANTV, es decir, en la red de transporte. Los equipos Passport no tienen conexión directa con los equipos de usuario, de esto se encargan los equipos de red de acceso, este modelo específicamente posee 16 *slots* disponibles para la inserción de tarjetas (15 FP's con su respectiva CP o 14 FP's y su respectiva CP en redundancia).

Las tarjetas procesadoras que se insertan en las ranuras de los nodos Passport se clasifican en dos tipos: Procesadores de Control ó *CP* (Control Processor) y Procesadores de Función ó *FP* (Function Processor), a continuación se presentan las definiciones y características más importantes de estas tarjetas.

2.6.1 PROCESADORES DE CONTROL (CP)

Los CP son las tarjetas procesadoras más importantes, ya que son las encargadas de dirigir a los FP insertados en el nodo, además de proporcionar la capacidad básica del sistema, entre las que se tienen: reinicio del nodo, monitoreo del armario ó *shelf*, así como también, mantener las tablas de enrutamiento. Adicionalmente se encargan del procesamiento de comandos, interfaces para la gestión de dispositivos, incluyendo un puerto *Ethernet* para conexión a un sistema de gestión de red.

2.6.2 PROCESADORES DE FUNCIÓN (FP)

Los Procesadores de Función o FP, al igual que los CP, son tarjetas que se insertan en los *slots* del *switch*, y tienen la responsabilidad de proporcionar los puertos e interfaces que conectan los elementos de la red de comunicaciones con los propios equipos Passport. Soportan y ejecutan procesos en tiempo real que son esenciales para proporcionar los servicios.

2.7 VIRTUAL PRIVATE NETWORK (VPN)

Una VPN se puede definir como la emulación de una red privada utilizando una infraestructura compartida. El proveedor de servicio de la VPN es el responsable por el aprovisionamiento y mantenimiento de la infraestructura compartida. El usuario final de una VPN es usualmente una empresa (pequeña, mediana o grande).

Una VPN puede ser basada en capa 2 o basada en capa 3 (modelo de referencia OSI), dependiendo del mecanismo utilizado por los dispositivos de borde de la red del proveedor de servicio para enrutar los paquetes recibidos. Por ejemplo, si la decisión de enrutamiento es basada en el puerto de entrada, identificador de circuito (DLCI o VCC) o una dirección MAC, estamos hablando de un servicio basado en capa 2, por otro lado, si la decisión de enrutamiento es en la dirección IP destino del paquete entonces nos referimos a un servicio VPN basado en capa 3.

2.8 FACILIDAD VPN DE PASSPORT

Los equipos Passport 7k soportan servicios de VPN basados en Virtual Routers (VR's). Un Virtual Router provee una emulación a nivel de software de un Router Físico. Por definición, un router enruta datagramas IP, esto lo realiza seleccionando la dirección e interface correspondiente al proximo router de salto (hop router) o *host* de destino. La decisión de enrutamiento depende de una base de datos dentro del router, llamada tabla de enrutamiento o tabla de direccionamiento, la cual es construida por medio de configuración local e información aprendida de otros routers (utilizando protocolos de enrutamiento).

Un dispositivo que provea VPN's basada en *Virtual Routers*, tiene un virtual router para cada VPN que soporta. Cada VR tiene sus propias tablas de enrutamiento y direccionamiento IP.

Existen tres tipos de *Virtual Routers*: (a) Management Virtual Router, (b) Customer Virtual Router (cVR's) y (c) Virtual Connection Gateway (VCG's). El primer VR que es provisionado en el switch Passport es siempre el *Management Virtual Router*, que provee acceso de gestión al nodo utilizando protocolos como Telnet. Un cVR es provisionado y dedicado para cada cliente de la VPN, que va a ser atendido por el equipo Passport al borde de la red. El cVR determina las conexiones de acceso (frame relay, PVC's, ATM PVC's, enlaces PPP, etc.) desde los sitios pertenecientes al cliente. El VCG es un VR común a donde se conectan todos los cVR's, el VCG provee una única conexión de salida hacia el backbone, para el tráfico de cada cliente en el nodo. La función principal de los VCG's es la de enlazar todos los nodos Passport que proveen la funcionalidad IP VPN, a través de túneles punto – multipunto (PTMP en inglés).

Para el provisionamiento de los Virtual Routers en los equipos Passport, se puede utilizar una tarjeta procesadora de función (FP), llamada VPN Extender Card (VPN Xc), la cual tiene la responsabilidad de absorber todos los Virtual Routers del equipo Passport, y con ello todos los procesos que los VR's realizan liberando a la tarjeta CP del procesamiento IP. A continuación se explican las características más importantes de la VPN Xc.

2.8.1 VPN EXTENDER CARD

La *VPN Extender Card* es una tarjeta procesadora para servicios IP. Los servicios IP utilizan la VPN Xc para ofrecer escalabilidad IP – VPN sin impactar el desempeño de los multiservicios prestados por el equipo Passport 7000. La VPN Xc es utilizada para alojar todos los routers virtuales (VR's) que soportan los servicios IP – VPN.

La VPN Extender Card consiste en una tarjeta madre, que se conecta al armario o *shelf* de la placa madre. La VPN Xc posee las siguientes características:

- 8 Mbytes de memoria FLASH
- 256 Mbytes de memoria SDRAM

La VPN Xc no tiene conexiones externas o puertos que requieran configuración, este tipo de tarjeta acepta la configuración en redundancia (dos tarjetas por nodo).

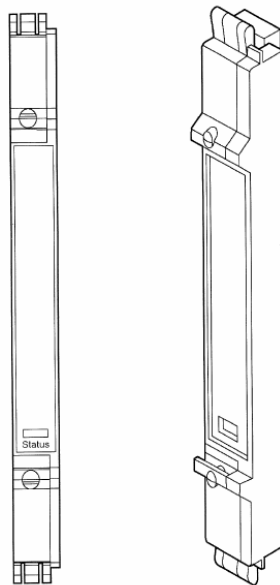


Figura 2 - 8 Placa Frontal de la VPN Xc

2.8.2 OPCIONES PARA DESPLEGAR EL SERVICIO IP VPN

La solución IP VPN de los equipos Passport puede ser desplegada para ofrecer servicios: Premium, Agregados, o Híbridos.

2.8.2.1 SERVICIO PREMIUM

En este tipo de servicio cada VR es dedicado para cada cliente situado dentro de la VPN, los VR's están conectados con circuitos virtuales dedicados en la red de

transporte. El ancho de banda entre cada sitio puede ser dedicado y garantizado por la red. Los VR's pueden estar conectados usando ATM VCC's o Frame Relay DLCI's. Un ejemplo del servicio IP – VPN Premium es mostrado en la siguiente figura.

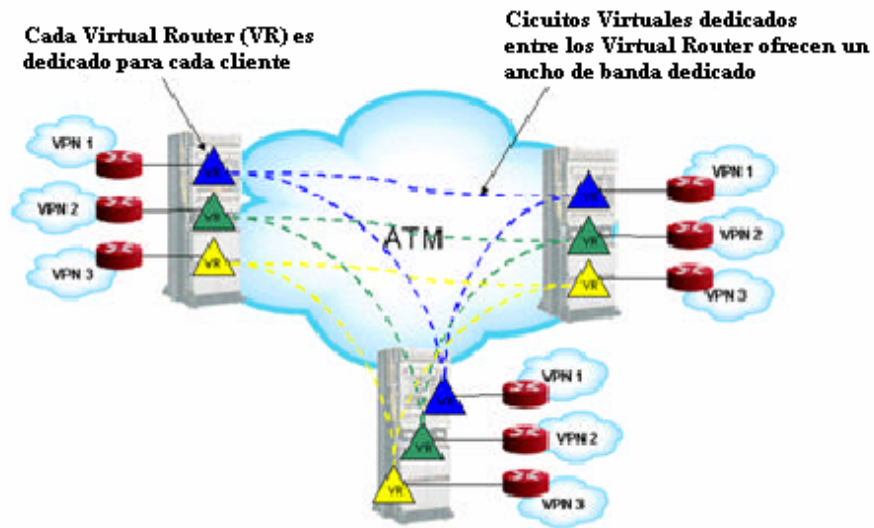


Figura 2 - 9 IP - VPN Servicio Premium

2.8.2.2 SERVICIO AGREGADO

El modelo de servicio IP – VPN Agregado hace uso de los Virtual Connections Gateways (VCG's). Los VCG's están total o parcialmente mallados dentro de la red para proveer conectividad. Cada Virtual Router es conectado al VCG por medio de una conexión interna. El medio capa 2 soportado entre VCG's es ATM. La principal ventaja del uso de los VCG's es la reducción del numero de conexiones capa 2 a través del backbone ATM. En la siguiente figura se presenta un ejemplo de este servicio.

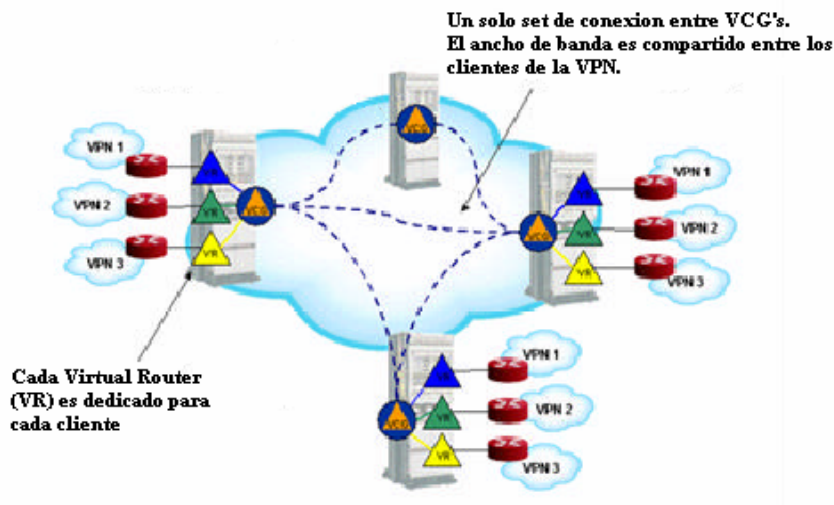


Figura 2 - 10 Servicio Agregado

2.8.2.3 SERVICIO HÍBRIDO

La versión híbrida del servicio de IP – VPN se refiere cuando los servicios Premium y Agregado son ofrecidos en el mismo nodo. (Nortel Networks Basic VPN Fundamentals)

2.9 IP SOBRE ATM

El multiprotocolo de encapsulación ATM ó (ATM MPE – ATM Multiprotocol Encapsulation) es un servicio ofrecido por los equipos Passport que permite la encapsulación IP sobre ATM en concordancia con RFC 1483. Se puede utilizar el servicio ATM MPE para transmitir tráfico IP hacia routers externos interconectados a los equipos Passport ó hacia otros Virtual Routers sobre una red ATM.

ATM MPE utiliza los siguientes medios para transmitir tráfico IP sobre redes ATM.

- Circuitos virtuales permanentes (PVC)

- Circuitos virtuales permanentes suaves (Soft PVC)

2.9.1 ATM MPE sobre PVC

En un PVC, todos los puntos de conexión a través de la red están definidos. Con la utilización de la encapsulación estándar utilizando RFC 1483 permite al sistema interactuar con cualquier otra implementación RFC 1483 (Nortel u otro fabricante).

El servicio ATM MPE de Passport sigue las especificaciones detalladas en RFC 1483, la cual describe dos (2) métodos para transportar tráfico de redes no orientadas a la conexión sobre la capa de adaptación ATM 5 (AAL 5). El primer método es llamado *Logical Link Control* (LLC), donde multiples protocolos de capas superiores (ULP's – Upper Layer Protocols), son transportados sobre un único canal de conexión virtual (VCC – Virtual Channel Connection) ATM. El segundo método es llamado encapsulación VC (Virtual Circuit encapsulation), donde solo el protocolo IP es permitido por cada ATM VCC.

2.9.2 ATM MPE SOBRE SOFT PVC

El servicio ATM MPE de Passport solo permite transportar tráfico IP sobre Soft PVC dentro de redes ATM PNNI (Private network – to –network interface). En un soft PVC solo los extremos del PVC estan definidos. El enrutamiento PNNI provee la selección de la ruta a través de la red entre los dos extremos definidos. Este servicio ATM MPE sobre soft PVC solo interactúa con redes Passport.(RFC 1483)

2.10 IP SOBRE FRAME RELAY

El servicio de encapsulación de tráfico IP sobre redes Frame Relay en los equipos Passport se realiza por medio de un componente de software llamado Frame Relay DTE. La encapsulación se realiza acorde a lo especificado en RFC 2427, que especifica el uso de NLPID (Network Level Protocol ID) para el protocolo IP y

SNAP para otros protocolos. Los equipos Passport solo soportan encapsulamiento IP sobre redes Frame Relay.

El Frame Relay user – to – network interface (FrUni) es la interfaz estándar entre el dispositivo usuario y la red. Por lo tanto se tiene que configurar una conexión lógica entre el componente FrDTE y el componente FrUni, para así lograr transportar tráfico IP sobre una red Frame Relay. (RFC 2427)

CAPITULO III

PROPUESTA DE OPTIMIZACIÓN DE LA RED DCN

3.1 RED ATM / FR DE CANTV

La red ATM / Frame Relay de CANTV, es la encargada de ofrecer de una manera integral y flexible voz, video y datos con velocidades desde E1 hasta STM – 1, con miras a satisfacer la demanda de clientes internos y externos, siendo capaz de ofrecer ancho de banda bajo demanda y una arquitectura escalable.

3.1.2 TOPOLOGÍA

La arquitectura que presenta la red ATM / FR esta conformada por: una sub-red de transporte o backbone, una sub-red de acceso y elementos de red.

1) backbone

El backbone de la red ATM / FR de CANTV esta constituido por equipos Passport 15k de Nortel, configurados para trabajar con ATM. Actualmente existen once (11) nodos configurados y operativos, distribuidos a lo largo del territorio nacional. Estos equipos se interconectan por enlaces STM – 4 (622 Mbps) y STM – 16 (2.5 Gbps).

2) Sub-Red de Acceso

Esta conformada por los equipos Passport 7k de Nortel, configurados para trabajar en Frame Relay. La sub-red de acceso esta integrada por ochenta y nueve (89) nodos a nivel nacional. Entre sus funciones se encuentran: proveer respaldo al protocolo de acceso, concentración de datos, conmutación local,

control de los circuitos virtuales, entre otras. Estos equipos se interconectan por enlaces STM – 1 (155 Mbps), E3 (140 Mbps) y E1 (2 Mbps).

3) *Elementos de Red (NE - Networks Elements)*

Lo conforman todos aquellos elementos conectados a la sub-red de acceso, incluyendo los equipos previos al usuario. Entre los elementos de Red encontramos: cable modems, modems, routers, DLC, etc.

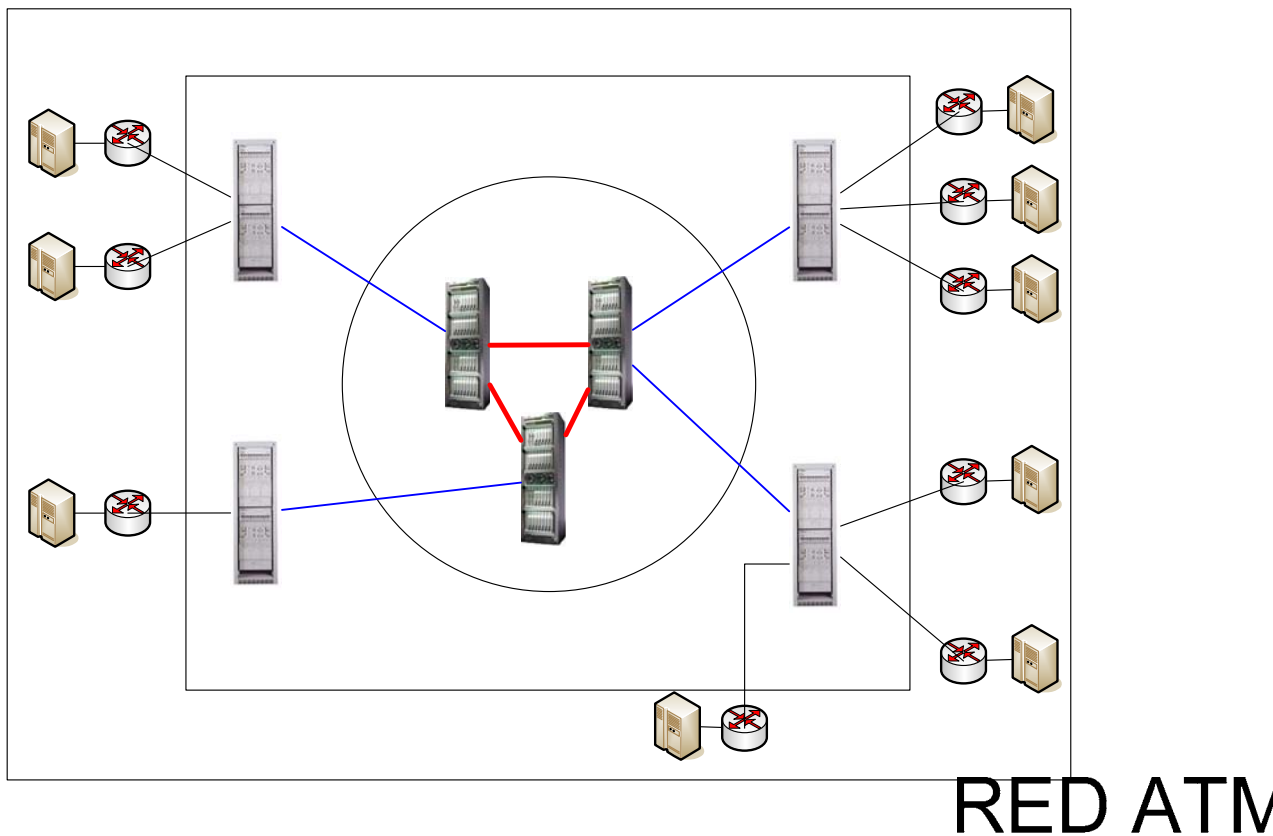


Figura 3 - 1 Esquema general de la red ATM / Frame Relay de CANTV

3.2 RED DCN DE CANTV

La red DCN de CANTV se soporta sobre la red ATM / FR explicada anteriormente, su función es la de concentrar aquellos dispositivos y / o elementos de red (NE – Networks Elements) que deban ser gestionados, esta gestión se realiza por medio de un sistema de gestión independiente de la tecnología de cada dispositivo de la red.

3.2.1 TOPOLOGÍA

A continuación se presenta una descripción de la topología actual de la red DCN de CANTV.

En la actualidad los elementos de red o *NE* (Network Elements) son conectados físicamente a los router marca CISCO modelo 2610 XM, llamados router de gestión local, cuya función es la de enrutar solamente la información concerniente a la gestión de los *NE*. Los router CISCO 2610 XM son conectados por medio de una interfase serial al equipo Passport 7k perteneciente a la sub-red de acceso de la red ATM / FR.

Otro de los dispositivos de la red DCN son los routers Cisco modelo 7500, llamados routers de gestión remota, que al igual que los routers de gestión local, se conectan por medio de una interfase serial a un equipo Passport 7k de la red de acceso. Entre los equipos Passport 7k del borde de la red se configura un DLCI (circuito virtual en una red Frame Relay). Del router de gestión remoto se enruta la información proveniente del router de gestión local, hacia el Centro de Control y Monitoreo de CANTV, ente encargado de la gestión de los *NE* de forma remota.

En la actualidad existe tres (3) router de gestión remoto que son: Los Palos Grandes (LPG), Chacao (CHA) y Centro Nacional de Comunicaciones (CNT), todos ubicados en la ciudad de Caracas. Debido a que los router CHA y CNT son relativamente nuevos, la mayor cantidad de enlaces se concentra en el router LPG.

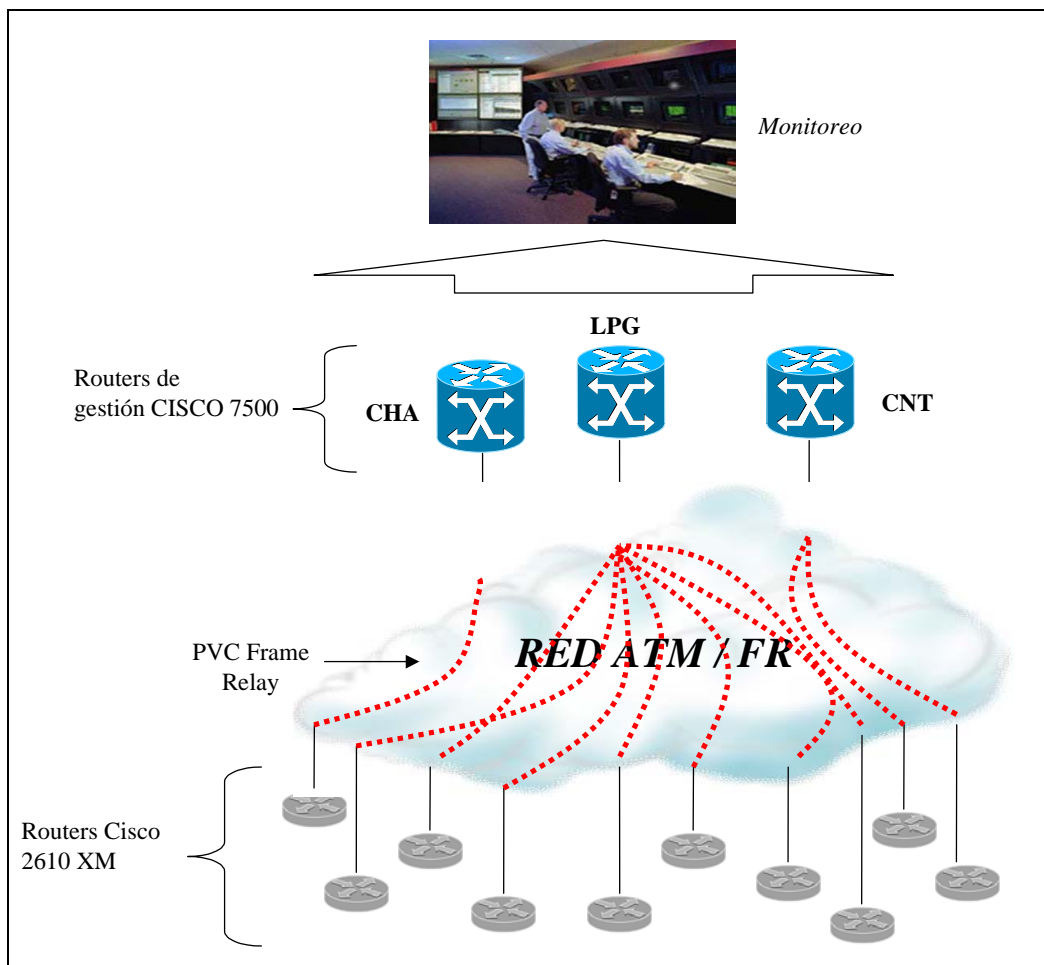


Figura 3 - 2 Topología de la Red DCN actual

3.3 PROPUESTA DE OPTIMIZACIÓN DE LA RED DCN

El objetivo principal de la nueva plataforma, es la de ofrecer mayor seguridad en el manejo de la información de gestión de todos los router de gestión local a nivel nacional. Debido a que en la actualidad el manejo de la gestión de los elementos de red se realiza a través de un único enlace DLCI para cada router de gestión local, queriendo decir con esto que al presentarse una falla en el enlace, se pierde comunicación con los elementos de red, y por lo tanto se hace imposible su gestión de forma remota hasta que el enlace vuelva a estar operativo.

Por lo expuesto anteriormente se proyectó una red que ofreciera múltiples rutas para la gestión de dichos elementos de red, es decir, ofreciera una plataforma redundante para el manejo de la información de gestión, y así al presentarse algún tipo de falla en el enlace, la información sea re-enrutada por un medio alternativo y así la duración de la falta de comunicación con el router de gestión local, y por lo tanto, con los elementos de red conectados a él sea del menor tiempo posible.

3.3.1 CREACIÓN DE LA CAPA DE DISTRIBUCIÓN

Otros de los objetivos de la nueva plataforma es la de conformar una arquitectura jerárquica, para ello se aprovechó la facilidad de VPN y VR que ofrecen los equipos Passport 7k que conforman la sub-red de acceso de la red ATM / FR. Con la adición de los equipos Passport 7k a la topología de la nueva plataforma se crea una capa de distribución entre los routers de gestión local y los routers de gestión remota, cuya función es la de concentrar los enlaces provenientes de los router de gestión local y enrutarlos, aplicando redundancia, hacia los routers de gestión remota. Al final la nueva plataforma ofrecerá una doble redundancia en los enlaces, ofreciendo cuatro (4) rutas diferentes para el intercambio de información de gestión entre los elementos de red y los router de gestión remota.

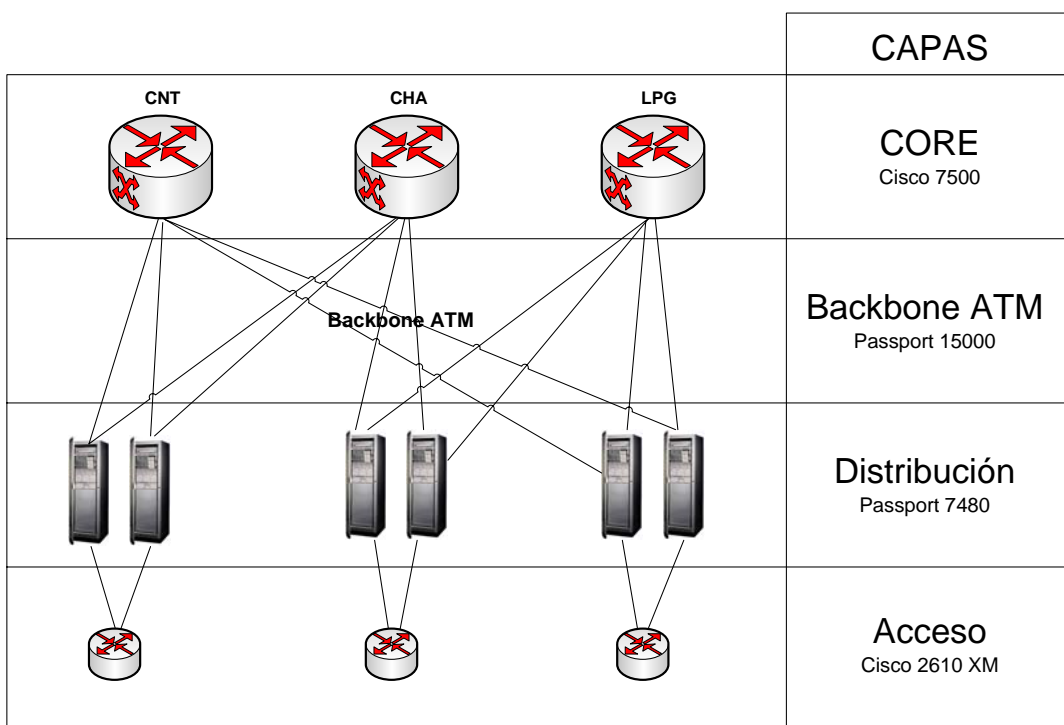


Figura 3 - 3 Capas jerárquicas de la nueva plataforma

3.3.2 IMPLEMENTACIÓN DE LA FACILIDAD DE VPN Y VR SOBRE LA NUEVA PLATAFORMA

Debido a que la nueva plataforma se soporta sobre la red ATM / FR de la empresa, lo que significa que es una plataforma compartida, por ello la implementación de la nueva red DCN esta orienta a la creación de una VPN, en donde se contará solamente con un solo tipo de cliente, los router de gestión local. Por lo tanto se implementa la opción de VPN Premium, servicio ofrecido por los equipos Passport 7k, en donde cada virtual router servirá exclusivamente a un tipo de cliente.

3.3.3 ARQUITECTURA OSPF

Al conformar una plataforma redundante es necesario la implementación de un protocolo de enrutamiento dinámico. La literatura ofrece dos (2) opciones que son las utilizadas con mayor frecuencia, RIP y OSPF. OSPF se seleccionó por sus ventajas sobre RIP, las cuales se mencionan a continuación.

- La convergencia para los cambios de topología de red es más rápida.
- La información de enrutamiento para redes estables genera menos tráfico.
- Como cada área OSPF está aislada, la infraestructura de enrutamiento es más robusta.
- OSPF no se ve afectado por los loops de la red.

Acorde a lo topología OSPF de dividir la red por áreas adyacentes al *backbone*, también llamado área 0, se agruparan los routers de gestión local de acuerdo a su ubicación geográfica. Estas áreas serán: (1) capital, (2) central, (3) centro occidente, (4) occidental, (5) oriente, y (6) los andes.

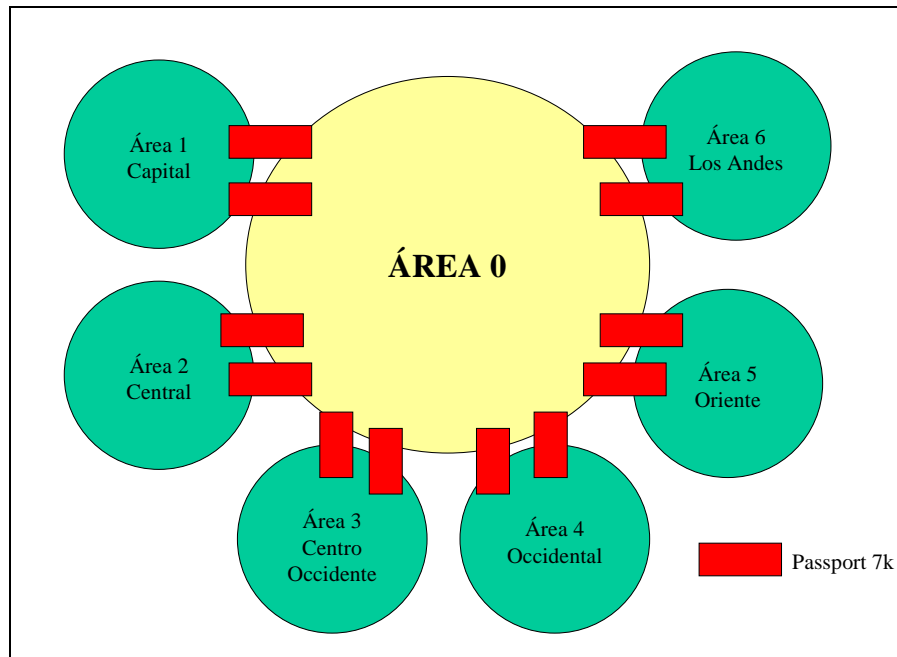


Figura 3 - 4 Arquitectura OSPF de la nueva plataforma

Cabe destacar que debido a que la red DCN se soporta sobre una plataforma compartida como lo es la red ATM / FR de CANTV, los enlaces entre los router de gestión local y los router de gestión remoto se crearan con PVC, debido a que es necesario especificar, reservar y garantizar el ancho de banda para cada ruta.

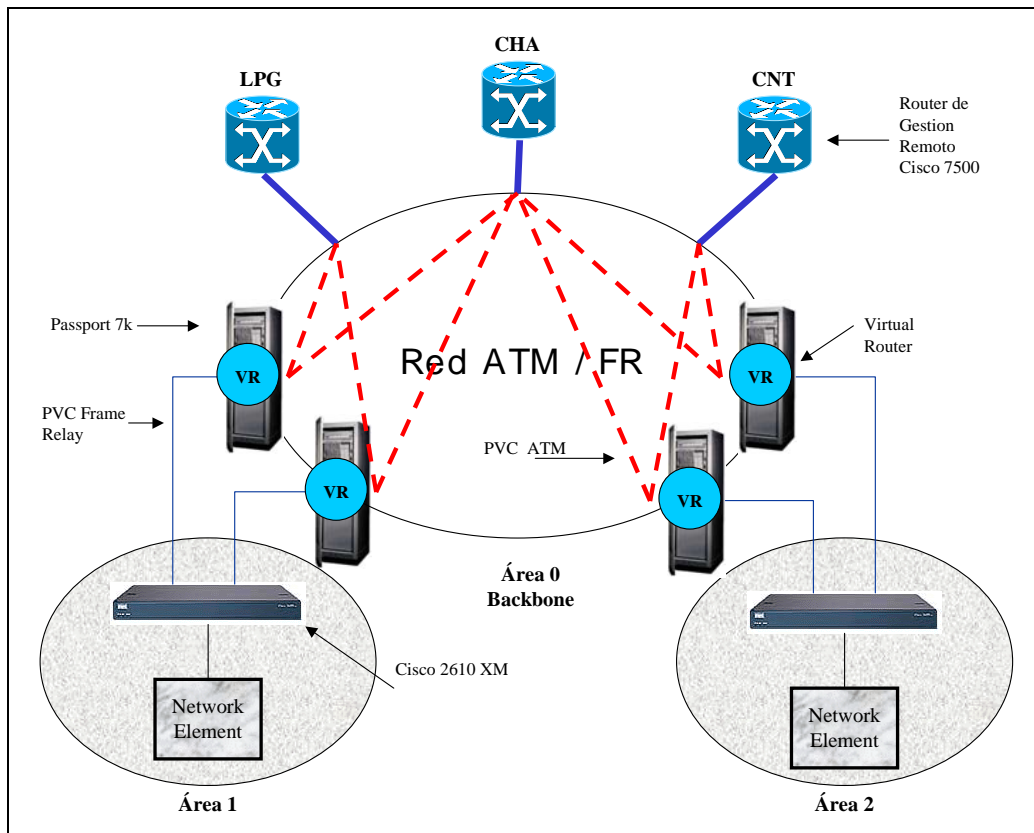


Figura 3 - 5 Topología general de la plataforma propuesta.

CAPITULO IV

PRUEBAS FUNCIONALES

4.1 AMBIENTE DE PRUEBA

Las pruebas en maqueta se refieren a ensayos o experimentos en un laboratorio con equipos conectados punto a punto, a muy corta distancia un terminal del otro, y cuyo principal propósito es el de simular el comportamiento de un sistema real. En este capítulo se muestran las pruebas realizadas para simular la implementación de la facilidad de VPN y VR, con el fin de estimar su comportamiento al momento de su ejecución en la red real.

A continuación se describe el ambiente de prueba, el cual está basado en la maqueta de Passport existente en el CET (Centro de Estudios en Telecomunicaciones) de CANTV.

Esta maqueta está constituida por:

- 3 Passports 15k (Release de software PCR 4.2), equipados con tarjetas STM-1, STM-4 y E3 ATM
- 3 Passports 7480 (Release de software PCR 4.2), equipados con tarjetas V.35 (FR/PPP), ethernet (100Mbps), E3 ATM, STM-1 ATM, E1 y MSA.

Los Passports 15k simulan el *core* (backbone) de la red, y los Passports 7480 simulan el edge (acceso) de la red.

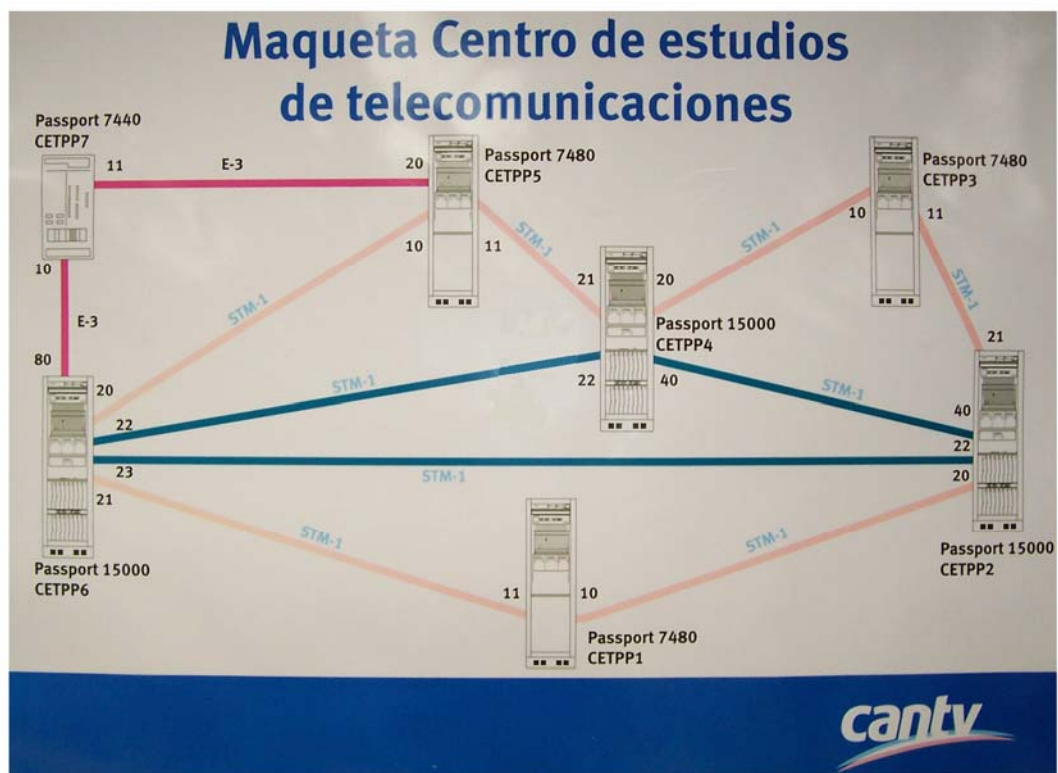


Figura 4 - 1 Maqueta de Pruebas CET - CANTV

4.2 TOPOLOGÍA DE LA RED DE GESTIÓN DE LA MAQUETA

Esta red tiene la finalidad de transportar las señales de administración por la gestión de los elementos de red que conforman la maqueta de pruebas. Para la gestión del router CISCO 2600 XM se configuró una interface Ethernet sobre el router, con la finalidad de hacer pertenecer al router a la red de gestión.

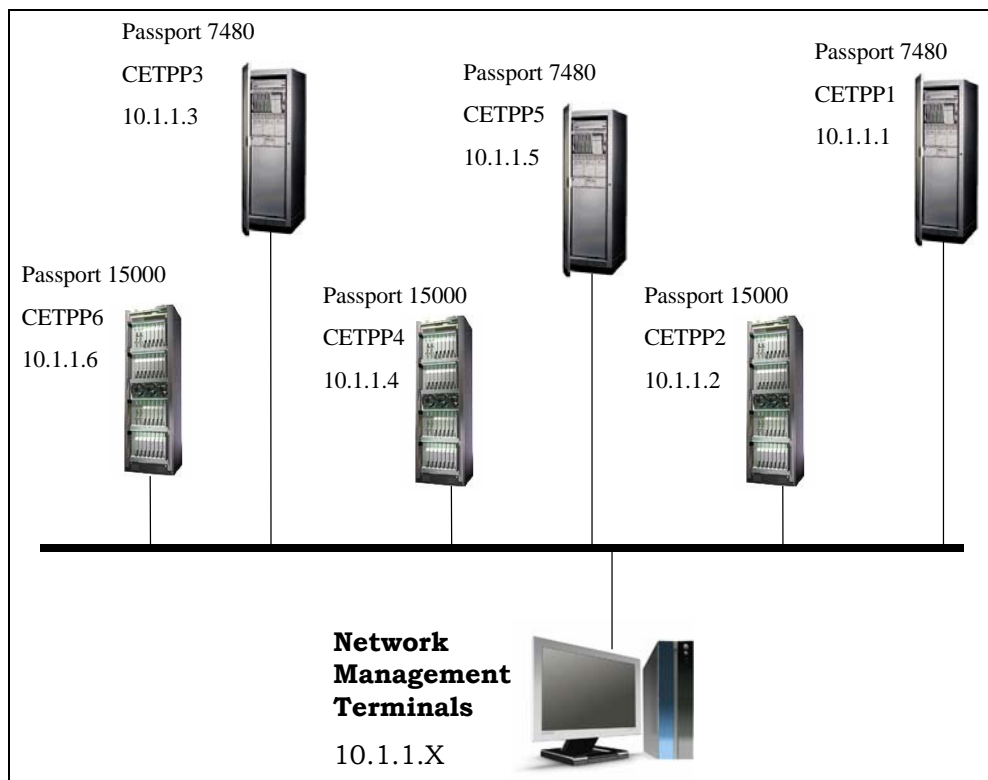


Figura 4 - 2 Red de Gestión Maqueta de Pruebas CET - CANTV

4.3 DIGRAMA DE CONEXIÓN PARA LA REALIZACIÓN DE LAS PRUEBAS

El router de gestión remota (CORE) se emuló configurando un VR en uno de los equipos Passport de la maqueta de pruebas, esto debido a que no se disponía de un router de esas características al momento de realizar las pruebas. A continuación se presenta la conexión de la plataforma bajo prueba sobre la maqueta de Passports:

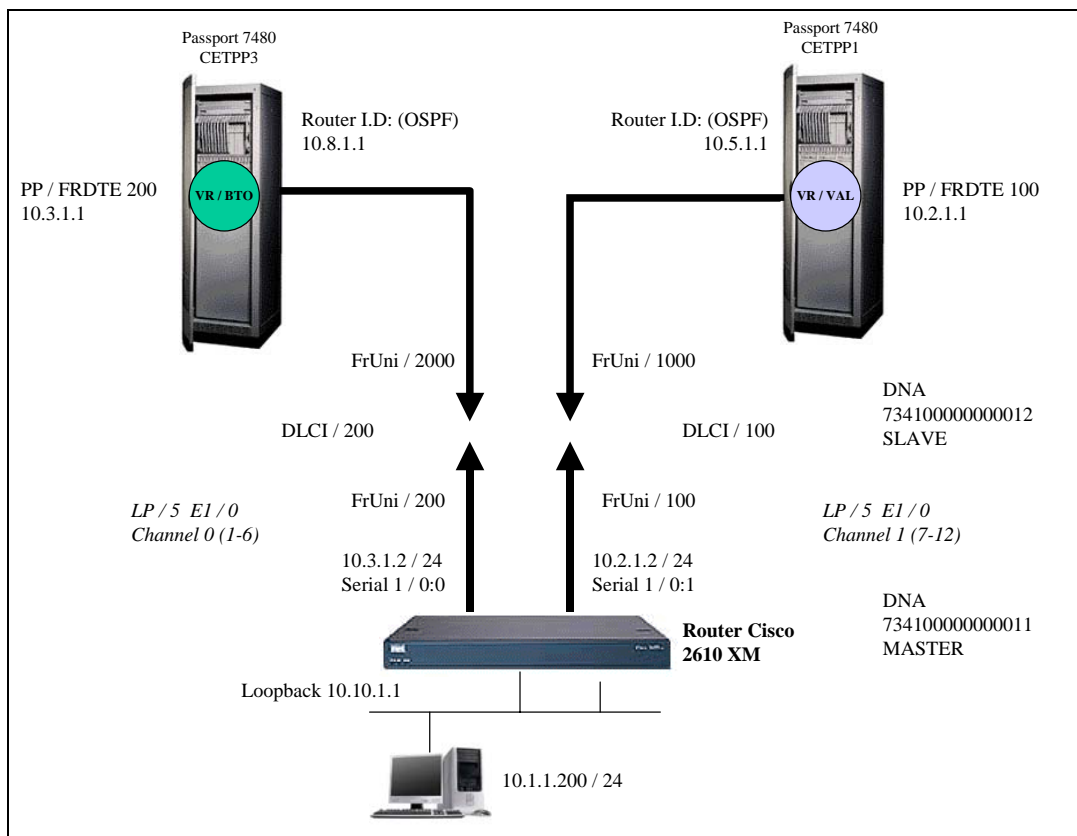


Figura 4 - 3 Configuración ambiente de pruebas

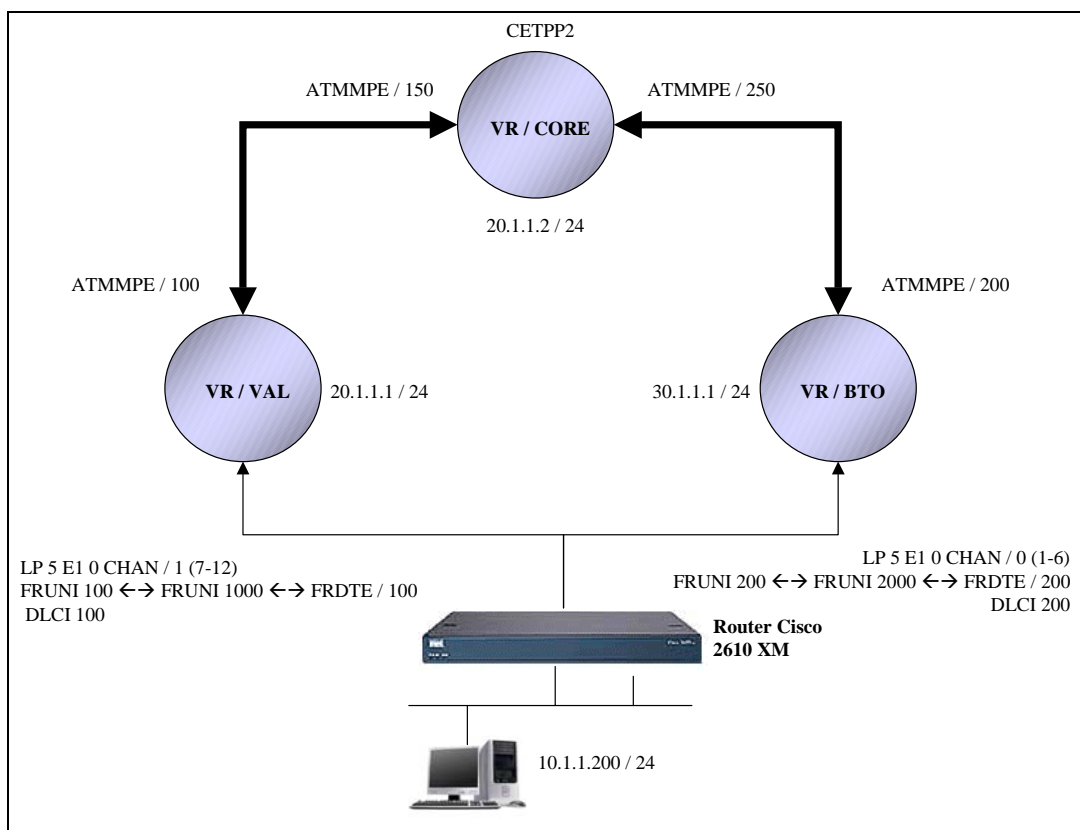


Figura 4 - 4 Configuración ambiente de pruebas (2)

4.4 VERIFICACIÓN DE LA FUNCIONALIDAD DE LA PLATAFORMA

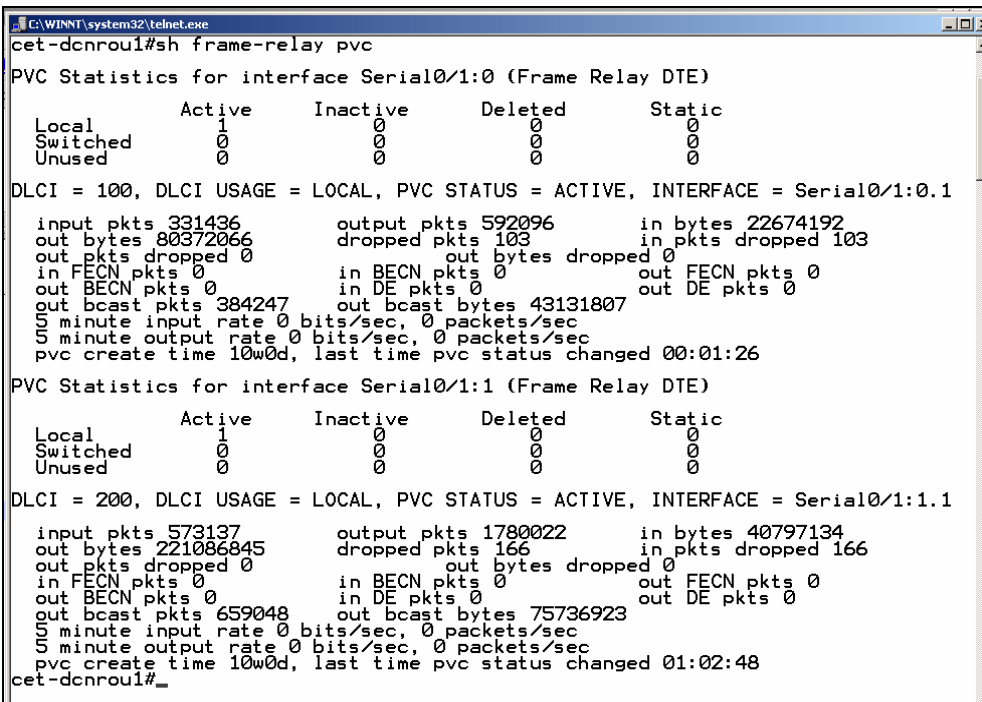
A continuación se describen las pruebas y resultados obtenidos para la verificación del protocolo de enrutamiento OSPF configurado sobre la plataforma, así como de los enlaces ya establecidos.

1. Verificación de los enlaces Frame Relay y ATM configurados.

Se realizó un PING desde el Router Cisco 2610 XM (Router de Gestión Local) hasta cada uno de los Passport 7k configurados anteriormente

El Procedimiento utilizado fue el siguiente:

- Telnet desde la estación de trabajo al 10.1.1.200 (Router Cisco 2610 XM)
- Ping a la dirección 10.2.1.1 (VR / VAL)
- Ping a la dirección 10.3.1.1 (VR / BTO)



```

C:\WINNT\system32\telnet.exe
cet-dcnrou1#sh frame-relay pvc
PVC Statistics for interface Serial0/1:0 (Frame Relay DTE)
Local      Active    Inactive  Deleted   Static
Switched   1        0        0        0
Unused    0        0        0        0
DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/1:0.1
input pkts 331436      output pkts 592096      in bytes 22674192
out bytes 80372066  dropped pkts 103      in pkts dropped 103
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0      in BECN pkts 0      out FECN pkts 0
out BECN pkts 0      in DE pkts 0      out DE pkts 0
out bcast pkts 384247  out bcast bytes 43131807
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 10w0d, last time pvc status changed 00:01:26
PVC Statistics for interface Serial0/1:1 (Frame Relay DTE)
Local      Active    Inactive  Deleted   Static
Switched   0        0        0        0
Unused    0        0        0        0
DLCI = 200, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/1:1.1
input pkts 573137      output pkts 1780022    in bytes 40797134
out bytes 221086845  dropped pkts 166      in pkts dropped 166
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0      in BECN pkts 0      out FECN pkts 0
out BECN pkts 0      in DE pkts 0      out DE pkts 0
out bcast pkts 659048  out bcast bytes 75736923
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 10w0d, last time pvc status changed 01:02:48
cet-dcnrou1#_

```

Figura 4 - 5 Estatus del enlace entre el router 2610 XM y el Passport 7k

Desde el Passport 7000:

- CETPP1 > ping -ip(10.2.1.2) vr/val ip icmp
- CETPP3 > ping -ip(10.3.1.2) vr/bto ip icmp

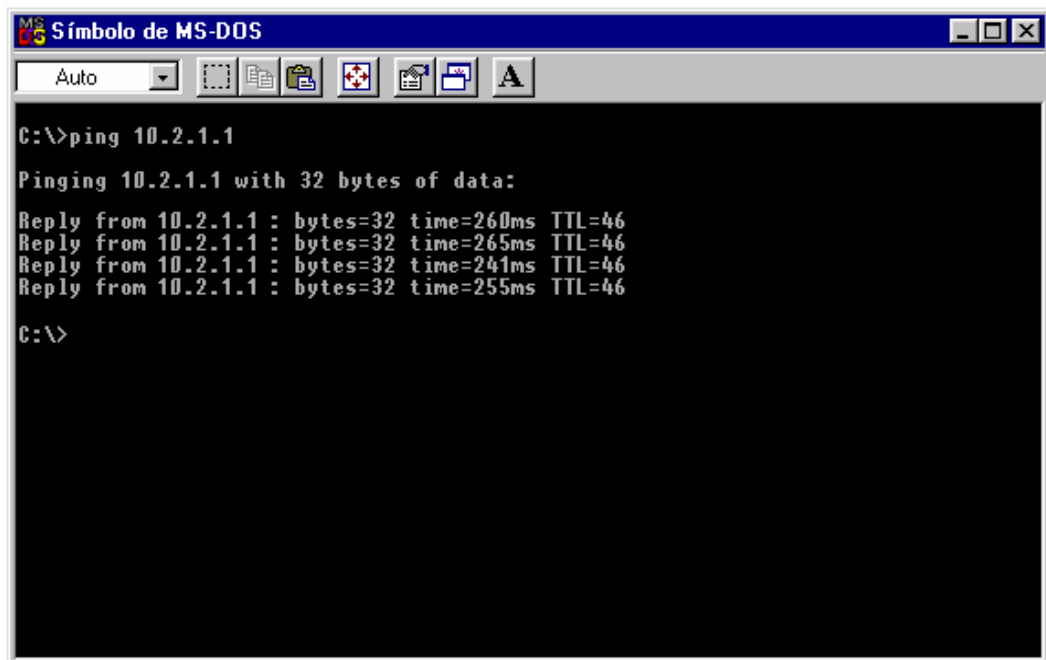
En todos los casos se observó un 0% de paquetes perdidos.

Se realizó un PING desde el Router CISCO hasta el VR llamado Router COR utilizado como emulación del Router de Gestión Cisco 7200.

El procedimiento utilizado fue el siguiente:

- Telnet desde la estación de trabajo al 10.1.1.200 (Router Cisco 2610 XM)
- Ping a la dirección 20.1.1.2

Se observó 0% de paquetes perdidos. Se verificó el tráfico entre el router de gestión local y el VR Router COR emulación del router de gestión remoto.



```
MS-DOS Símbolo de MS-DOS
Auto
C:\>ping 10.2.1.1
Pinging 10.2.1.1 with 32 bytes of data:
Reply from 10.2.1.1 : bytes=32 time=260ms TTL=46
Reply from 10.2.1.1 : bytes=32 time=265ms TTL=46
Reply from 10.2.1.1 : bytes=32 time=241ms TTL=46
Reply from 10.2.1.1 : bytes=32 time=255ms TTL=46
C:\>
```

Figura 4 - 6 Verificación de tráfico desde el router hasta el Passport

2. Comprobación de la tabla de enrutamiento de los dispositivos configurados.

El procedimiento utilizado fue el siguiente:

Sobre los VR's:

- CETPP1 > d vr/val ip fwd/*
- CETPP3 > d vr/bto ip fwd/*

Sobre el router Cisco 2610 XM:

- cet-dcnrou1# show ip route

Se comprobó que la plataforma “aprendió” por OSPF, las direcciones IP no locales.

```

C:\WINNT\system32\telnet.exe
cet-dcnrou1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.3.1.1 to network 0.0.0.0

O 10.0.0.0/24 is subnetted, 1 subnets
  O 20.1.1.2 [110/1825] via 10.3.1.1, 00:03:48, Serial0/1:1.1
  O [110/1825] via 10.2.1.1, 00:03:48, Serial0/1:0.1
C 10.0.0.0/24 is subnetted, 5 subnets
  C 10.10.1.0 is directly connected, Loopback0
  C 10.9.0.0 is directly connected, Loopback2
  C 10.3.1.0 is directly connected, Serial0/1:1.1
  C 10.2.1.0 is directly connected, Serial0/1:0.1
  C 10.1.1.0 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 10.3.1.1
  [1/0] via 10.2.1.2
  
```

Enrutamiento por OSPF del Router CORE
(Emulación del router de gestión remoto Cisco 7500)

Figura 4 - 7 Tabla de enrutamiento del Router Cisco 2610 XM

3. Comprobación de re-enrutamiento por OSPF.

Debido a la métrica arrojada por la tabla de enrutamiento del Virtual Router COR, se establece que el “camino” desde el router cisco hasta el Virtual Router COR es por el Virtual Router Valencia (VR/VAL). Sabiendo esto, se le hizo un PING Indefinido desde el Router Cisco 2600 hasta el Virtual Router COR. Sabiendo que el trafico se

enrutaba a través del VR Valencia, este VR se bloqueó, obligando al tráfico a re-enrutarse a través del Virtual Router Barquisimeto.

El procedimiento utilizado fue el siguiente:

Router Cisco 2610 XM:

- Desde la estación de trabajo se realizó un telnet al router Cisco 2610 XM
- Ping -T 20.1.1.2

Luego, desde el Passport 7k CETPP1:

- CETPP1 > lock VR/VAL

Antes de bloquear el Virtual Router Valencia, se observó que el Router COR respondía normalmente al comando PING desde el Router Cisco 2600, al aplicar el bloqueo, este dejó de responder por aproximadamente 2 segundos, para luego responder nuevamente, verificándose así que el tráfico fue re-enrutado por OSPF a través del VR Barquisimeto.

CONCLUSIONES

La propuesta de optimización presentada en este proyecto cumple con los objetivos planteados, ya que ofrece una topología jerárquica y segura para la gestión en forma remota de todos los elementos de red interconectados a la red de gestión de datos (DCN) de la empresa. Esto se logró mediante la facilidad de VPN y VR que ofrecen los equipos Passport 7k del fabricante Nortel, los cuales junto con los equipos Passport 15k, integran la red ATM / Frame Relay de CANTV.

Los resultados altamente satisfactorios obtenidos de las pruebas funcionales de la propuesta de optimización, realizadas sobre la maqueta de pruebas de la empresa CANTV, permite asegurar el buen desempeño de estas tecnologías cuando sean implementadas en la red ATM / FR real, ofreciendo las siguientes ventajas:

- 1) Debido a que es requisito el uso de circuitos virtuales permanentes para así garantizar el ancho de banda en las transmisiones, se establecen enlaces redundantes entre los dispositivos de red locales y remotos, ofreciendo múltiples rutas para el establecimiento de las conexiones logrando disminuir considerablemente las probabilidades de que algún elemento integrante de la red quede sin gestión.
- 2) La red DCN funciona sobre la red ATM / FR que es una plataforma compartida, por ello es necesario el aislamiento de la red DCN de todas aquellas redes que funcionan sobre la misma plataforma, esto se logra con la implementación de una VPN donde los únicos clientes son los routers de gestión local.
- 3) Con la implementación del protocolo de enrutamiento OSPF, al fallar unos de los enlaces establecidos, el envío de información se reenruta automáticamente

por otro de las rutas configuradas anteriormente, lo que significa que la pérdida de comunicación con los elementos gestionables es relativamente corta, además que al implementar OSPF, la red se robustece, ya que al dividir la red en áreas alrededor del *backbone*, el impacto de agregar algún elemento nuevo a la red es mínimo.

- 4) Con la instalación de las tarjetas VPN Xc en los nodos de borde de las áreas OSPF, el desempeño de los equipos Passport no se ve afectado, ya que las tarjetas VPN Xc absorben todos los procesos relacionados a enrutamiento y procesamiento IP. Otra de las ventajas que ofrece esta propuesta es la instalación de dos (2) tarjetas VPN Xc por nodo, dejando una de ellas en *Hot Stand By* aumentando aun más la seguridad de la plataforma.

RECOMENDACIONES

En base a las pruebas realizadas, alcance de la investigación y a la investigación en general se presentan las siguientes recomendaciones:

- a) Realizar pruebas de re-enrutamiento sobre la red ATM / FR, para así establecer los retardos que se puedan presentar en la realidad, ya que, debido a la poca distancia entre los elementos en la maqueta de pruebas, los retardos allí generados no son comparables a los retardos que se puedan presentar en un nodo real de la red.
- b) Debido a que el característica principal de la propuesta de optimización es la de presentar una plataforma redundante, es conveniente establecer un redundancia en los routers cisco 2610 XM (router de gestión local), es decir, colocar un segundo router en estancia pasiva que a la hora que el router principal sufra alguna falla, el router pasivo entre en actividad para así no interrumpir la gestión de los elementos conectados a él.
- c) Implementar normas de cableado estructurado para la conexión de los elementos de red a los routers de gestión (Cisco 2610 XM). En la actualidad los elementos de red están directamente conectados a los routers de gestión local Cisco 2610 XM, los cuales solo poseen dieciséis (16) puertos para conexión. Las normas de cableado establecen la utilización de paneles de distribución (Patch panel) para la conexión entre los elementos de red y el router, esto es para facilitar las labores de mantenimiento, también se sugiere la instalación de switches Cisco Catalyst como elemento concentrador de los enlaces debido a la limitante de dieciséis puertos que posee el router.

BIBLIOGRAFÍA

- (1) Ibe, Oliver. **Essentials of ATM Networks and Services**. Addison-Wesley Professional. 1997
- (2) Mendillo, Vincenzo. **Curso de Extensión de Conocimientos Gestión de Redes**. 2002.
- (3) NERI – VELA, Rodolfo. **Lineas de Transmisión** McGraw Hill. 1999.
- (4) Nortel Networks. **Basic VPN Fundamentals**. 2001
- (5) Nortel Networks. **Passport 7400, 15000, 20000 Configuring IP**.
- (6) Nortel Networks. **Passport 7400, 15000, 20000 Component VR**.
- (7) Nortel Networks. **Passport 7400 Hardware Description**. 2001
- (8) Nortel Networks. **Passport 7400, 15000, 20000 Overview**. 2001.
- (9) Nortel Networks. **VPN Configuration Management**.
- (10) CANTV. **Proceso de Pase a Producción**
- (11) RFC 1245 - **OSPF Protocol Analysis**
- (12) RFC 1483 - **Multiprotocol Encapsulation over ATM Adaptation Layer 5**.
- (13) RFC 2427 - **Multiprotocol Interconnect over Frame Relay**.
- (14) Rodriguez, Daniel. **Trabajo de Grado “Diseño de un plan de optimización del enrutamiento PNNI de la red de datos ATM Nortel Passport 7000 y 15000 instalada en CANTV”**. 2003

REFERENCIAS ELECTRÓNICAS

www.atmforum.com

www.cisco.com

www.monografias.com

www.nortel.com

<http://www2.rad.com/networks/1995/ospf/ospf.htm>

[ANEXO N° 1]

[CONFIGURACIÓN DE LOS DISPOSITIVOS DE RED]

Para la configuración y aprovisionamiento de los equipos Passport de Nortel, se hizo uso del software de configuración denominado “CLI Manager” propio de la compañía Nortel. Para la configuración del router de gestión local marca CISCO modelo 2610 XM, se realizó una conexión telnet al router desde la estación de trabajo. A continuación se muestran los comandos con su respectiva descripción para la configuración de los dispositivos de red.

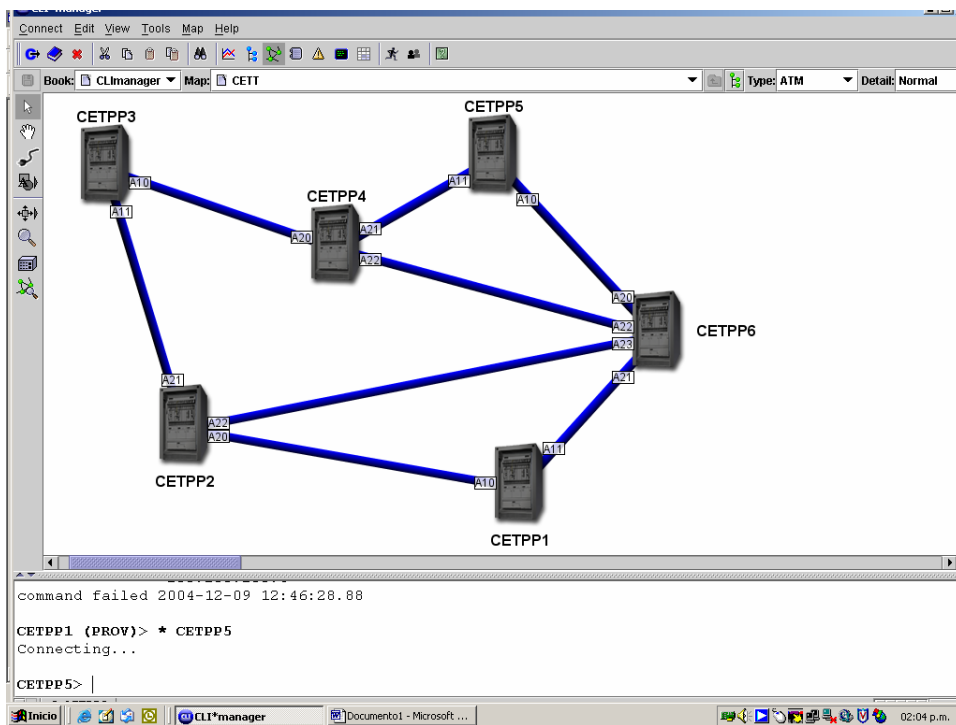


Figura 4 - 8 Software de Gestión de los equipos Passport

Prueba No.	1	Resultado: <i>Satisfactorio</i>
Título	Aprovisionamiento de los VR's (Virtual Routers)	
Propósito	Mostrar el proceso de aprovisionamiento de los VR's sobre los equipos Passport 7000. Procedimiento para Frame Relay. Mostrar la configuración en los VR's del Protocolo de Enrutamiento OSPF.	

Acción Comando	<p>Se repiten los comandos para los diferentes Nodos</p> <p>Añadir un VR <i>Add -s vr / <nombre></i></p> <p>CETPP1 (PROV) > add Vr/VAL</p> <p><i>Definir en que LP corre el VR</i> Set vr/<nombre> virtualRouterProcessor lp/<numero></p> <p>CETPP1 (PROV) > set vr/val virtualRouterProcessor lp/0</p>	
Nota:	<p>Por defecto coloca lp/0 pero puede cambiarlo a la Lp donde este la tarjeta VPN XC.</p> <p>Añadir un Protocol Port</p> <p><i>Add vr/<nombre> pp/<nombre del pp> iport logicalif/<direccion IP del la interfaz></i></p> <p>CETPP1 (PROV) > add Vr/VAL Pp/FRDTE100 IpPort LogicalIf/10.2.1.1</p> <p>Colocar mascara, dirección de broadcast y next hop.</p> <p><i>s vr/<nombre> pp/<nombre del pp> iport logicalif/<direccion IP del la interfaz> netmask < mascara de subred></i></p>	
Pruebas Realizadas por Nortel Networks CANTV	<p>Nombre: Luciano Gomes Julián Tovar</p>	

<p>Acción</p> <p>Comando</p>	<p><i>s vr/<nombre> pp/<nombre del pp> iport logicalif/<direccion IP del la interfaz> broadcastAddress <direccion IP de broadcast></i></p> <p><i>s vr/<nombre> pp/<nombre del pp> iport logicalif/<direccion IP del la interfaz> linkDestinationAddress <direccion ip al otro lado del circuito></i></p> <p>CETPP1 (PROV) > set Vr/VAL Pp/FR IpPort LogicalIf/10.2.1.1 netMask 255.255.255.0</p> <p>CETPP1 (PROV) > set Vr/VAL Pp/FR IpPort LogicalIf/10.2.1.1 broadcastAddress 10.2.1.255</p> <p>CETPP1 (PROV) > set Vr/VAL Pp/FR IpPort LogicalIf/10.2.1.1 linkDestinationAddress 10.2.1.2</p> <p>Hacer que la interfaz del Protocol Port participe en el proceso de OSPF</p> <p><i>Add vr/<nombre> pp/<nombre del pp> iport logicalif/<direccion IP del la interfaz> ospfif</i></p> <p>CETPP1 (PROV) > Vr/VAL Pp/FRDTE100 IpPort LogicalIf/10.2.1.1 OspfIf</p> <p>Agregar a que área pertenece</p> <p><i>set vr/<nombre> pp/<nombre del pp> iport logicalif/<direccion IP del la interfaz> areaid <area x.x.x.x></i></p> <p>CETPP1 (PROV) > set Vr/VAL Pp/FRDTE100 IpPort LogicalIf/10.2.1.1 OspfIf areaId 0.0.0.0</p>
<p>Pruebas Realizadas por: Nortel Networks CANTV</p>	<p>Nombre: Luciano Gomes Julián Tovar</p>

Prueba No.	2	Resultado: <i>Satisfactorio</i>
Título	Aprovisionamiento de los VR's (Virtual Routers)	
Propósito	Mostrar el proceso de aprovisionamiento de los VR's sobre los equipos Passport 7000. Procedimiento para ATM	

Acción	Para conectar un circuito ATM a un Protocol Port se requiere el uso del componente ATMMPE.	
Comando	Agregar Componente ATMMPE <i>add atmmpe/<numero></i> CETPP1 (PROV) > add AtmMpe/100 Asociar el ATMMPE al Protocol Port <i>Set atmmpe/<numero> linktoprotocolport vr/<nombre> pp/<nombre del protocol port></i> CETPP1 (PROV) > set AtmMpe/100 linkToProtocolPort Vr/VAL Pp/ATMMPE100 Asociar el atmmpe con un PVC <i>s atmmpe/<numero> ac/1 atmconnection <atmif numero> vcc/<vpi>.<vci> nep</i> CETPP1 (PROV) >set AtmMpe/100 Ac/1 atmConnection AtmIf/100 Vcc/0.100 Nep	
Pruebas Realizadas por Nortel Networks CANTV	Nombre: Luciano Gomes Julián Tovar	

Prueba No.	3	Resultado: <i>Satisfactorio</i>
Título	Aprovisionamiento de los PVC's	
Propósito	Mostrar el proceso de aprovisionamiento de los PVC's sobre los equipos Passport 7000.	

Acción	Programación de PVC's	
Comando	Agregar la interfaz ATM y PVC	
	<i>add -s atmif/<numero de atmif> vcc/<vpi>.<vci></i>	
	CETPP1 (PROV) > add -s AtmIf/100 Vcc/0.100	
	Asignar en que Lp y puerto esta asociado el AtmIf	
	<i>add -s atmif/<numero de atmif> interfacename lp/<numero> sdh/<numero del puerto> path/0</i>	
Nota:	Este es el procedimiento para una interfaz STM-1, si es E3 o STM-4 varia ligeramente.	
	Ajuste del parámetro txTrafficDescType	
	<i>set atmif/<numero> vcc/<vpi>.<vci> vcd tm txTrafficDescType 1</i>	
	CETPP1 (PROV) > set AtmIf/100 Vcc/0.100 Vcd Tm txTrafficDescType 1	
Pruebas Realizadas por Nortel Networks CANTV	Nombre: Luciano Gomes Julián Tovar	

Prueba No.	4	Resultado: <i>Satisfactorio</i>
Título	Aprovisionamiento del componente FRDTE	
Propósito	Mostrar el proceso de aprovisionamiento del componente FRDTE, necesario para la conexión de un circuito Frame Relay al Protocol Port del equipo Passport 7000.	

Acción	Programación del componente FRDTE	
Comando	Agregar componente FRDTE <i>Add frdte/<numero del frdte></i> <i>Set frdte/<numero del frdte> logicalprocessor lp/<numero de lp></i> CETPP1 (PROV) > add FrDte/100 CETPP1 (PROV) > logicalProcessor Lp/14 Se requiere borrar el componente Framer que se crea automáticamente y agregar un Virtual Framer para conexión lógica al Protocol Port. <i>Del frdte/<numero> framer</i> <i>Add frdte/<numero> vframer</i> CETPP1 (PROV) > del frdte/100 framer CETPP1 (PROV) > add FrDte/100 Vframer Asociación del FRDTE al Protocol Port. <i>Set frdte/<numero> rg/1 linktoprotocolport vr/<nombre del vr></i> <i>pp/<nombre del protocol port></i> CETPP1 (PROV) > set FrDte/100 Rg/1 linkToProtocolPort Vr/VAL Pp/FRDTE100	
Pruebas Realizadas por Nortel Networks CANTV	Nombre: Luciano Gomes Julián Tovar	

	<p>Procedimiento para la asociación del FRDTE al circuito Frame Relay (un circuito Frame Relay tiene dos extremos llamados FRUNI's).</p> <p>Agregar DLCI</p> <p>Add frdte/<numero> stdlci/<numero de dlci></p> <p>CETPP1 (PROV) > add FrDte/100 StDlci/100</p> <p>Configuración del Ancho de Banda (BW)</p> <p>Set frdte/<numero> stdlci/<nuemro de dlci> committedinformationrate <CIR></p> <p>Set frdte/<numero> stdlci/<nuemro de dlci> committedBurst <BC></p> <p>Set frdte/<numero> stdlci/<nuemro de dlci> linktoremotegroup FRDTE/<NUMERO> RG/1</p> <p>CETPP1 (PROV) > set FrDte/100 StDlci/100 committedInformationRate 384000</p> <p>CETPP1 (PROV) > set FrDte/100 StDlci/100 committedBurst 384000</p> <p>CETPP1 (PROV) > set FrDte/100 StDlci/100 linkToRemoteGroup FrDte/100 Rg/1</p> <p>Ajuste del LMI</p> <p>Set frdte/<numero> stdlci/<numero de dlci> lmi procedures <ansi o ccitt></p> <p>CETPP1 (PROV) > set FrDte/100 Lmi procedures ccitt</p> <p>Asociación del FRDTE con el FRUNI</p> <p>Set frdte/<numero> vframer othervirtualframer fruni/<numero del fruni> vframer</p>
Pruebas Realizadas por Nortel Networks CANTV	Nombre: Luciano Gomes Julián Tovar

<p>Nota:</p>	<p>CETPP1 (PROV) > Set FrDte/100 VFramer otherVirtualFramer FrUni/1000 Vframer</p> <p>Hay que tomar en cuenta la creación de un Vframer en la punta del circuito Frame Relay que se conecta al FrDTE.</p> <p>Creación del FRUNI</p> <p><i>Add -s fruni/<numero> dlci/<numero del dlci></i></p> <p><i>Set fruni/<numero> dlci/<numero del dlci> dc remoteDNA <direccion X121 del puerto remoto></i></p> <p><i>Set fruni/<numero> dlci/<numero del dlci> dc remotedlci <numero del dlci del otro fruni></i></p> <p><i>Set fruni/<numero> dlci/<numero del dlci> DNA datanetworkaddress <direccion X121 del puerto></i></p> <p><i>Set fruni/<numero> dlci/<numero del dlci> dc type slave</i></p> <p><i>Set fruni/<numero> dlci/<numero del dlci> sp commitedinformationrate <CIR></i></p> <p><i>Set fruni/<numero> dlci/<numero del dlci> sp commitedBurstSize<bc></i></p> <p>CETPP1 (PROV) > add -s FrUni/1000 Dlci/100</p> <p>CETPP1 (PROV) > set FrUni/1000 Dlci/100 Dc remoteDna 73410000000011</p> <p>CETPP1 (PROV) > set FrUni/1000 Dlci/100 Dc remoteDlci 100</p> <p>CETPP1 (PROV) > set FrUni/1000 Dlci/100 Dna dataNetworkAddress 73410000000012</p>
<p>Pruebas Realizadas por Nortel Networks CANTV</p>	<p>Nombre: Luciano Gomes Julián Tovar</p>

	<p>CETPP1 (PROV) > set FrUni/1000 Dlci/100 dc type slave</p> <p>CETPP1 (PROV) > set FrUni/1000 Dlci/100 Sp committedInformationRate 384000</p> <p>CETPP1 (PROV) > set FrUni/1000 Dlci/100 Sp committedBurstSize 384000</p> <p>Ajuste del LMI</p> <p><i>Set fruni/<numero> stdlci/<numero de dlci> lmi procedures <ansi o ccitt></i></p> <p>CETPP1 (PROV) > Set FrUni/1000 stdlci/100 lmi procedures ANSI</p> <p>Creación del Vframer</p> <p><i>Del fruni/<numero> framer</i></p> <p><i>add fruni/<numero> vframer</i></p> <p>CETPP1 (PROV) > del fruni/1000 framer</p> <p>CETPP1 (PROV) > add fruni/1000 vframer</p> <p>Asociación del FRUNI con el FRDTE</p> <p><i>set fruni/<numero> vframer othervirtualframer frdte/<numero> vframer</i></p> <p>CETPP1 (PROV) > set FrUni/1000 VFramer otherVirtualFramer FrDte/100 Vframer</p> <p>Especificación del LP donde corre el FrUni</p> <p><i>Set fruni/<numero> vframer logicalprocessor lp/<numeo de lp></i></p> <p>CETPP1 (PROV) > add FrUni/1000 Vframer logicalProcessor Lp/14</p>
Pruebas Realizadas por Nortel Networks CANTV	Nombre: Luciano Gomes Julián Tovar

	<p>Configuración del otro extremo del FRUNI</p> <pre> Add -s fruni/<numero> dlci/<numero del dlci> set fruni/<numero> dlci/<numero del dlci> dc remoteDNA <direccion X121 del puerto remoto> set fruni/<numero> dlci/<numero del dlci> DNA datanetworkaddress <direccion X121 del puerto> set fruni/<numero> dlci/<numero del dlci> dc remotedlci <nuero del dlci del otro fruni> set fruni/<numero> dlci/<numero del dlci> dc type master set fruni/<numero> dlci/<numero del dlci> sp committedinformationrate <CIR> set fruni/<numero> dlci/<numero del dlci> sp committedBurstSize <bc> Set fruni/<numero> stdlci/<nuemro de dlci> lmi procedures <ansi o ccitt> set fruni/<numero> framer logicalprocessor lp/<numeo de lp> set fruni/<numero> framer interfacename lp/<numero> El/<numero de puerto> chan/<canalizacion, numero> CETPP1 (PROV) > add -s FrUni/100 Dlci/100 CETPP1 (PROV) > set FrUni/100 Dlci/100 Dc remoteDna 73410000000012 CETPP1 (PROV) > set FrUni/100 Dlci/100 Dna dataNetworkAddress 73410000000011 </pre>
Pruebas Realizadas por Nortel Networks CANTV	Nombre: Luciano Gomes Julián Tovar

	<p>CETPP1 (PROV) > set FrUni/100 Dlci/100 Dc remoteDlci 100</p> <p>CETPP1 (PROV) > set FrUni/100 Dlci/100 Dc type master</p> <p>CETPP1 (PROV) > set FrUni/100 Dlci/100 Sp committedInformationRate 384000</p> <p>CETPP1 (PROV) > set FrUni/100 Dlci/100 Sp committedBurstSize 384000</p> <p>CETPP1 (PROV) > Set fruni/100 stdlci/100 lmi procedures ansi</p> <p>CETPP1 (PROV) > set fruni/100 framer logicalprocessor lp/5</p> <p>CETPP1 (PROV) > set FrUni/100 Framer interfaceName Lp/5 E1/0 Chan/0</p>
Pruebas Realizadas por Nortel Networks CANTV	Nombre: Luciano Gomes Julián Tovar


[ANEXO N° 2]

[PROCESO DE PASE A PRODUCCIÓN]

A continuación se muestra una lista y parte de los documentos entregados a la unidad Soporte a las Redes, misma encargada del mantenimiento y operación de la nueva plataforma.

	INFORMACIÓN GENERAL DEL SERVICIO	Fecha: 07 / 01 / 2005
NOMBRE DEL SERVICIO		
IMPLEMENTACION DE LA FACILIDAD "VIRTUAL ROUTING" Y VPN SOBRE LOS EQUIPOS PASSPORT		
EMPRESA SOLICITANTE		UNIDAD SOLICITANTE
CANTV		REINGENIERÍA DE DATOS
PERSONA CONTACTO (Líder del Proyecto)		DIRECCIÓN PERSONA CONTACTO
GÁMEZ AYMARA		PISO 3 ALA SUR, EDIF. NEA. CNT AV. LIBERTADOR
TELÉFONO /OFICINA/ CELULAR /OTRO		CORREO ELECTRONICO
(0212) 500 ****		****@cantv.com.ve
RESPONSABLE FUNCIONAL		DIRECCIÓN USUARIO FINAL
GERENCIA CENTRO DE OPERACIONES DE LA RED ANA C. RODRÍGUEZ		SALA CORTIJOS
TELEFONO / OFICINA / CELULAR / OTRO		CORREO ELECTRONICO
(0212) 273 ****		****@cantv.com.ve
RESPONSABLE TÉCNICO POR PARTE DEL CLIENTE		DIRECCIÓN USUARIO FINAL
COORDINADOR DE SOPORTE A LAS REDES DE DATOS RAMÓN A. CABELLO		LOS PALOS GRANDES, PISO 1.
TELEFONO / OFICINA / CELULAR / OTRO		CORREO ELECTRONICO
(0212) 209 ****		****@cantv.com.ve
BREVE DESCRIPCIÓN DEL PRODUCTO, Haciendo referencia al tipo de usuario al cual va dirigido, plataforma involucrada (Hardware, Software) y la funciones que desempeña.		
<p>Implementación de la facilidad "Virtual Routing" y "Virtual Private Networks" sobre los equipos Passport 7k, mediante la instalación de VPN's Xc (Extender Cards) en los Passport elegidos como cabeceras de región a nivel nacional. Con la implementación de esta plataforma se busca jerarquizar la Red DCN, ofreciendo seguridad para los usuarios de la misma, debido a que ofrece redundancia en su configuración y mejora el desempeño de los equipos Passport involucrados en el diseño. Otro de los objetivos de la puesta en marcha de esta plataforma es la de distribuir equitativamente la carga de los routers de gestión, la cual en la actualidad es absorbida casi en su totalidad por el router de gestion Palos Grandes.</p>		
FOR-0042		

		Aseguramiento Calidad Pase a Producción		Fecha: 07 / 01 / 2005	
INFORMACIÓN DE LAS CONDICIONES DE REDUNDANCIA DE LA PLATAFORMA					
Software					
Alta Disponibilidad		Si tiene Alta Disponibilidad Indique			
Si <input type="checkbox"/> No <input type="checkbox"/>	Replicación de Aplicación <input type="checkbox"/>	Manual <input type="checkbox"/>	Automática <input type="checkbox"/>	Explique:	
	Replicación de Base de Datos <input type="checkbox"/>	Manual <input type="checkbox"/>	Automática <input type="checkbox"/>		
Redundancia		Si <input type="checkbox"/> No <input type="checkbox"/>		Explique:	
Hardware					
Alta Disponibilidad		Si tiene Alta Disponibilidad Indique el esquema			
Si <input type="checkbox"/> No <input type="checkbox"/>	Cluster <input type="checkbox"/>	Indique Tecnología (NLB, CLB, Nodos, etc)		Metodo Fail Over	
	Tipo: Activo-Activo <input type="checkbox"/> Activo- Pasivo <input checked="" type="checkbox"/>			Manual <input type="checkbox"/> Automática <input checked="" type="checkbox"/>	
Redundancia		Si <input checked="" type="checkbox"/> No <input type="checkbox"/>		Explique: Se instalaran dos (2) tarjetas VPN Xc en los equipos Passport 7k cabeceras de región, aprovechando la configuración de Spare.	
Comunicación					
Energía		Suministrada por el equipo Passport, debido que las tarjetas es un elemento agregado a los mismos.			
FOR-0049					

		INFORMACIÓN INVENTARIO FÍSICO Y DE PROCESOS		Fecha: 14/01/2005	
INFORMACIÓN DE INVENTARIO FÍSICO					
Nombre del Componente/Parte/Equipo			Cantidad		
VPN Extender Card Serial: NNTM*****			1		
VPN Extender Card Serial: NNTM*****			1		
INFORMACIÓN DE INVENTARIO DE PROCESOS					
Nombre Del Proceso/Script/ Servicio/Programa		Fuente	Frecuencia	Función	Destinatario
INFORMACIÓN DE APLICACIONES INSTALADAS POR EL PROVEEDOR Y QUE NO LE PERTENECEN					
Aplicaciones		Soportados		Argumento	
N/A					

NORTEL



Caracas, 9 de Marzo de 2.005

Señores
CANTV
Caracas.-

Para: Gerencia General de Redes, Sistemas, Telecomunicaciones Fijas
Gerencia de Planificación e Ingeniería
Coordinación Reingeniería de Datos

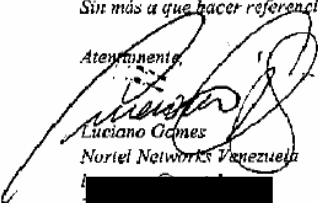
Asunto: Consulta sobre reportes abiertos referentes a la funcionalidad Virtual Routing o IP VPN
en la Plataforma Passport 7k/15k

Estimados señores,

Basado en el requerimiento expresado por ustedes, les informamos que al día de hoy no tenemos abierto reporte alguno por parte de CANTV asociado a fallas o consultas técnicas referentes a la funcionalidad Virtual Router o IP VPN. Asimismo les comentamos que al día de hoy únicamente existen abiertos dos ticket por fallas, en los cuales se esta trabujando con CANTV de acuerdo a la metodología ya establecida, no teniéndose afectación del servicio a los clientes internos o externos. La cantidad de reportes abiertos se considera normal (de hecho muy bajo) para una red con 100 nodos Passport y cerca de 100 nodos DPN 100.

Estamos a sus gratas ordenes para cualquier consulta o aclaratoria adicional.

Sin más a que hacer referencia.

Ateentamente

Luciano Gómez
Nortel Networks Venezuela

[Redacted contact information]

[ANEXO N° 3]

[MAQUETA DE PRUEBAS DE CANTV]

A continuación se muestran los equipos Passport 7480 y 15000 de Nortel pertenecientes a la maqueta de pruebas de CANTV ubicada en el sector San Martín (Caracas), específicamente en el CET (Centro de Estudio de Telecomunicaciones), también se muestran los equipos utilizados para la realización de las pruebas funcionales de la propuesta de optimización de la red DCN de CANTV.



Figura C - 1 Centro de Estudios de Telecomunicaciones

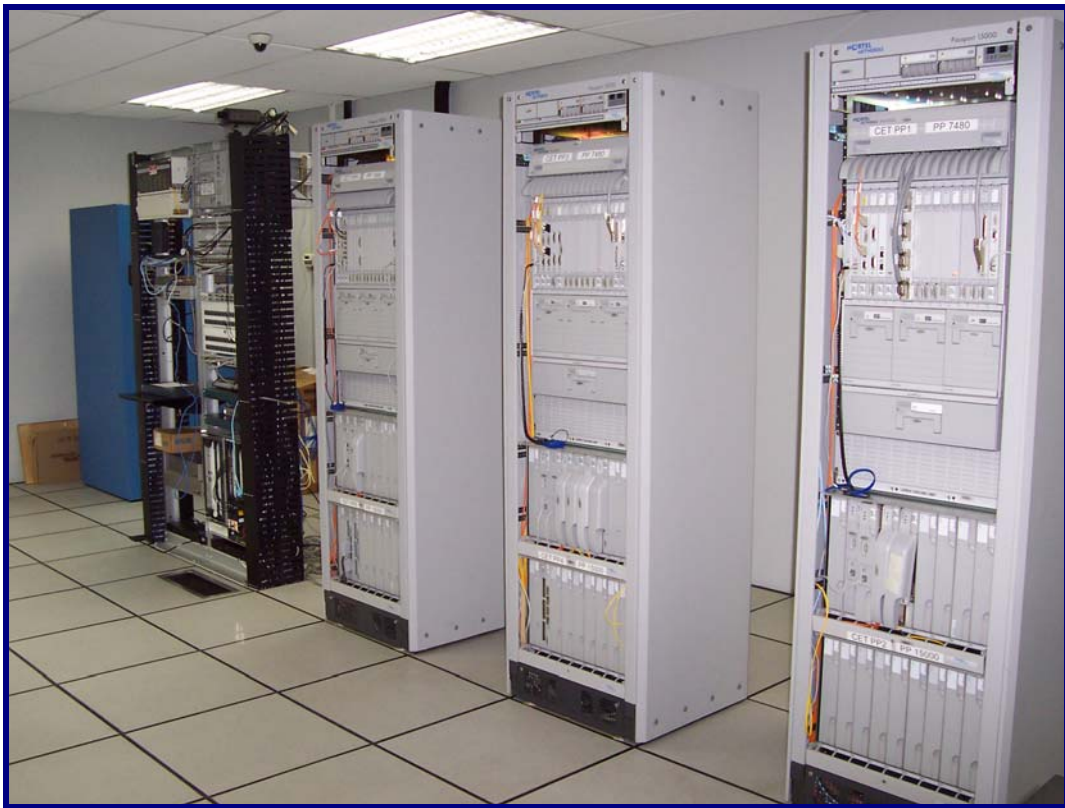


Figura C - 2 Equipos Passport 7k y 15k pertenecientes a la maqueta de pruebas.

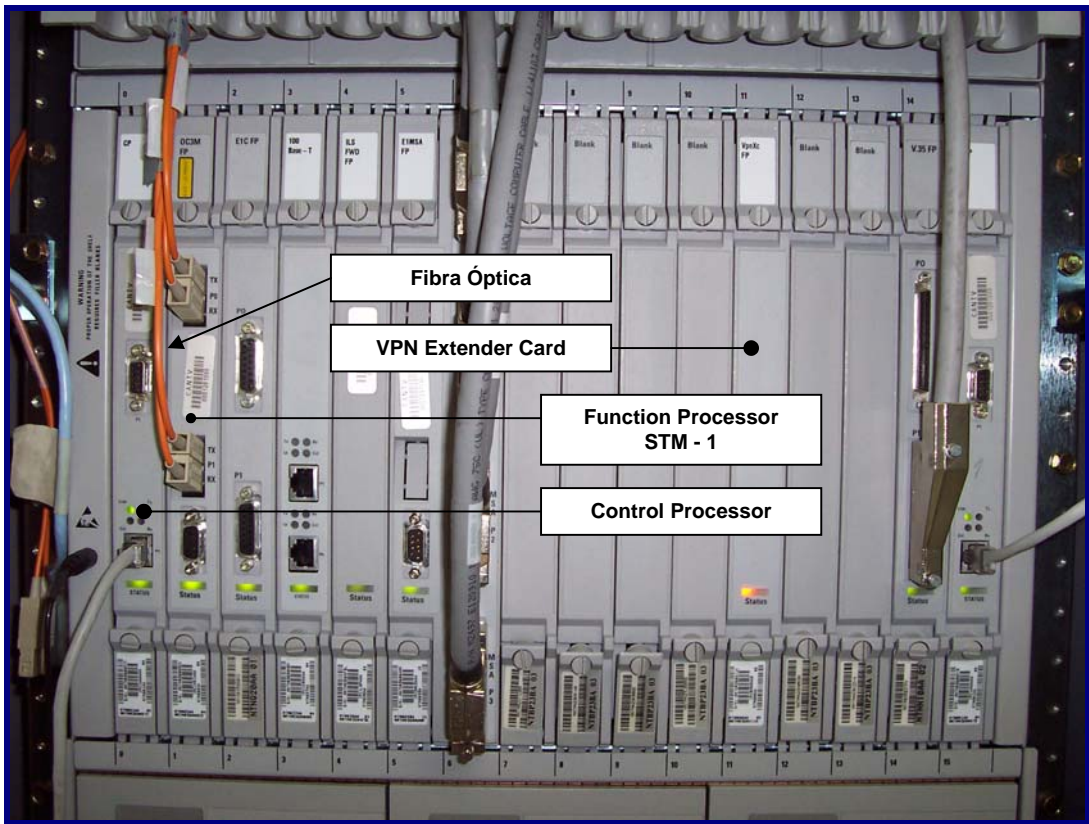


Figura C - 3 Passport 7480

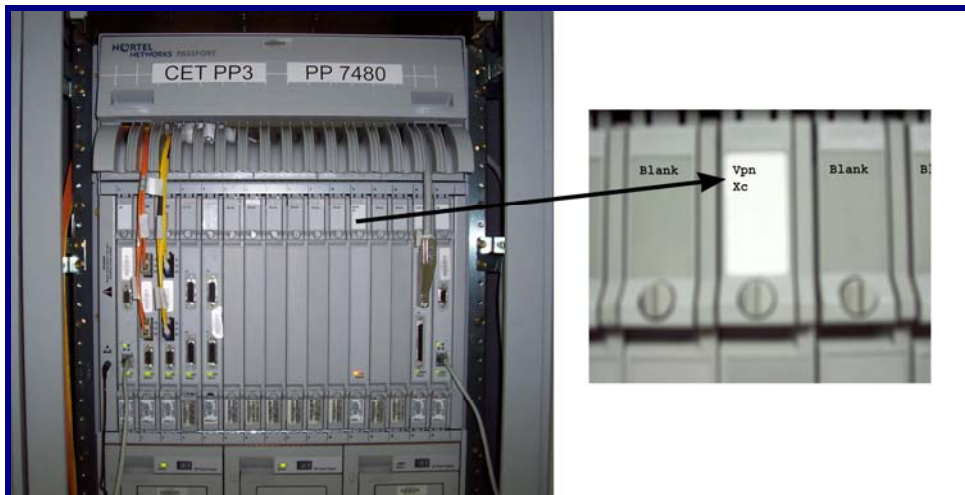


Figura C - 4 Instalación de la VPN Xc en el Passport

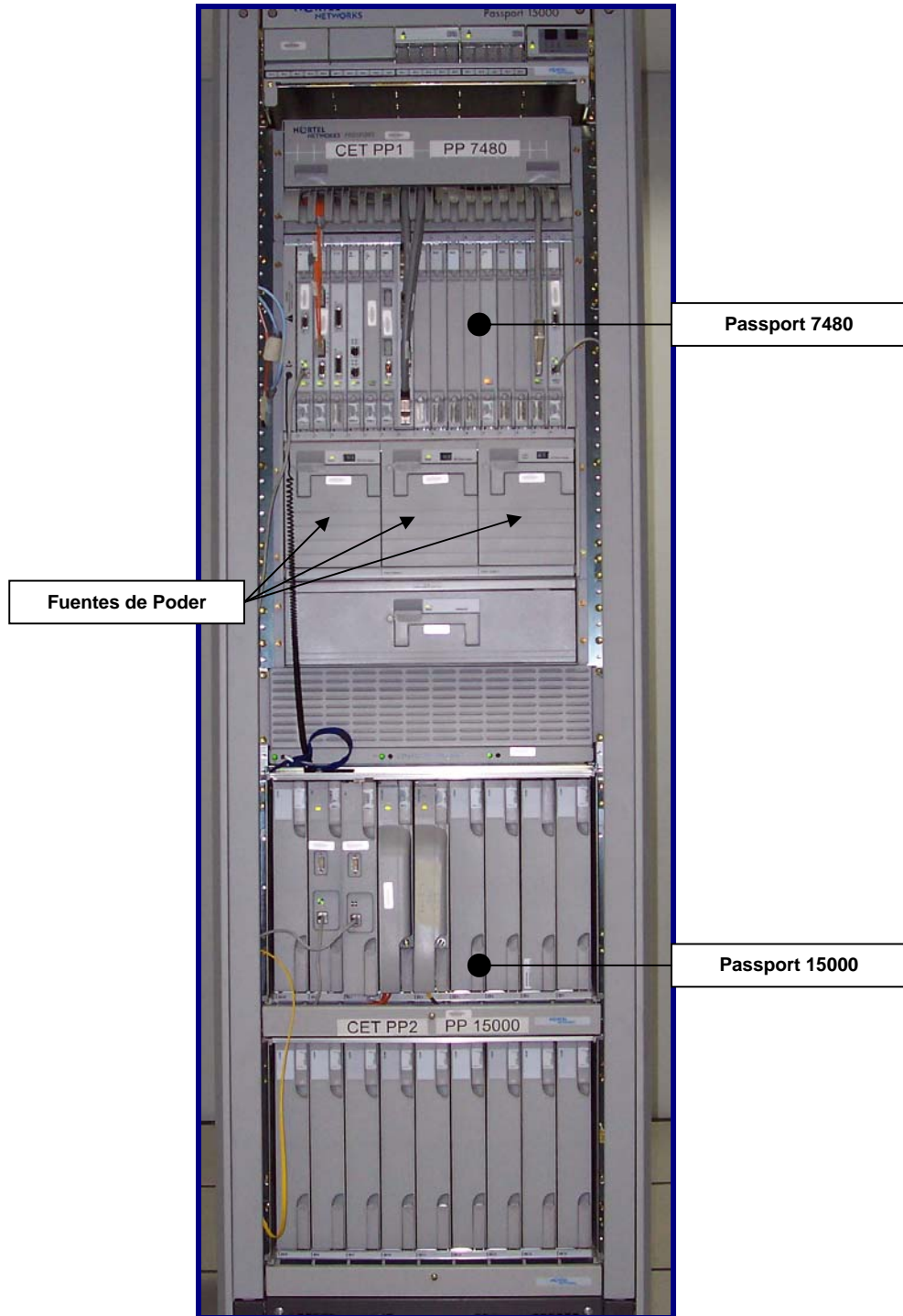


Figura C - 5 Passport 7k y 15k



Figura C - 6 Router Cisco 2610 XM (Vista Frontal)

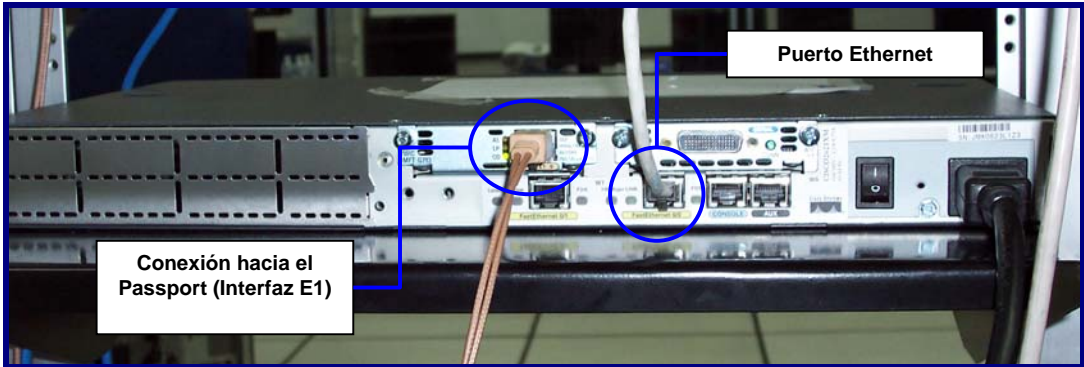


Figura C - 7 Router Cisco 2610 XM (Vista Trasera)

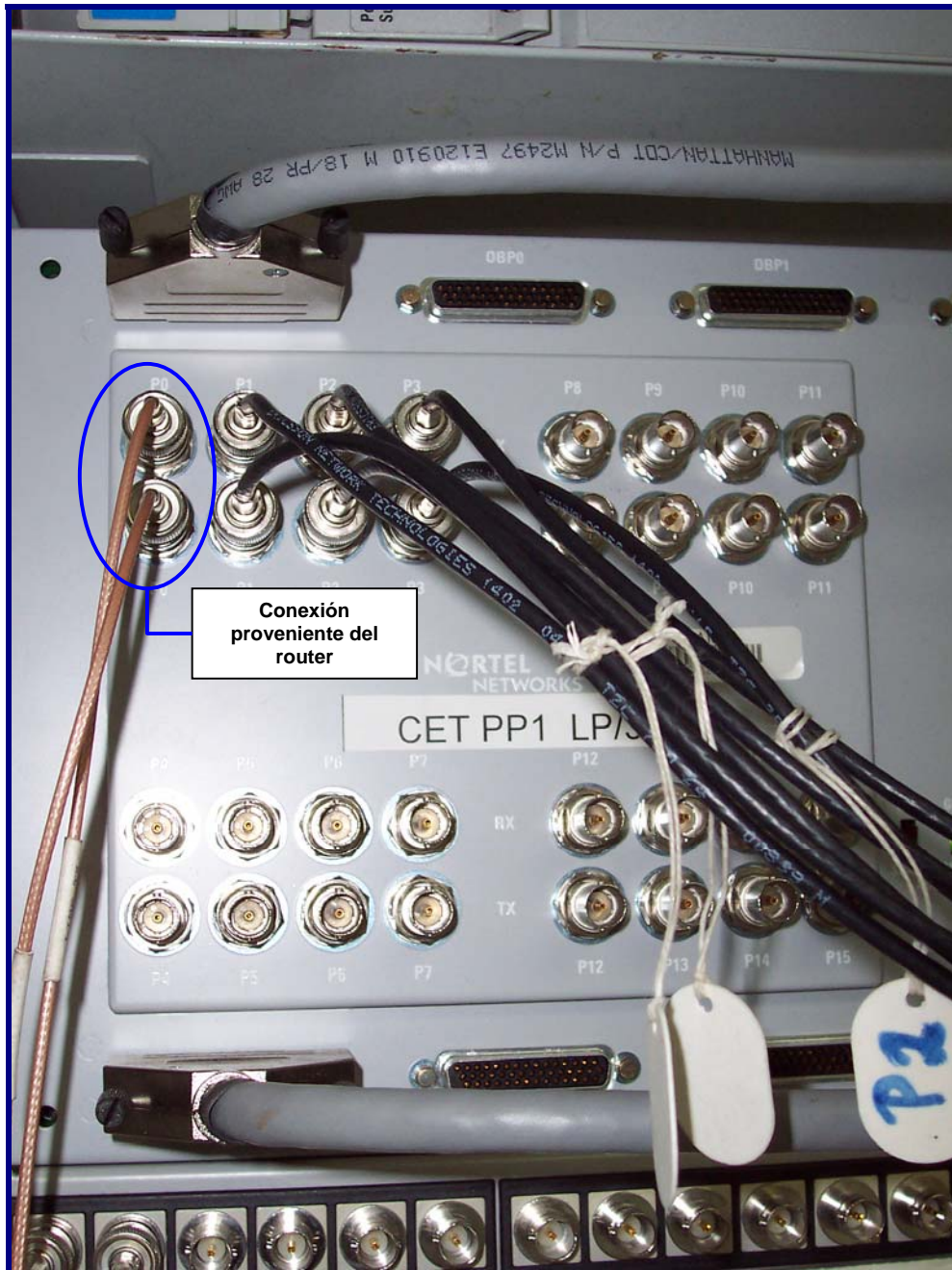


Figura C - 8 Panel de conexión del Passport 7480 CETPP1

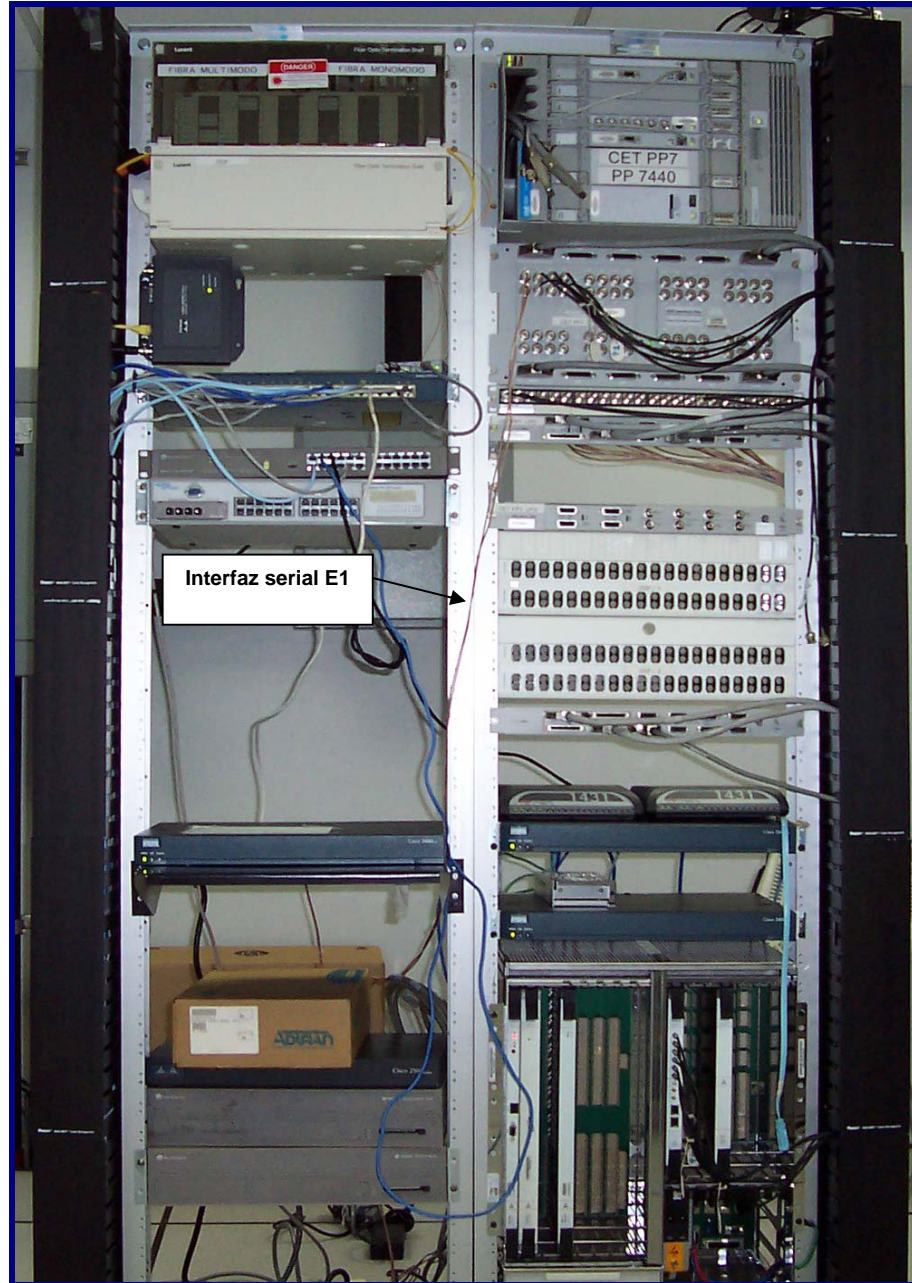


Figura C - 9 Conexión entre el Router y el Passport

[ANEXO N° 4]
[ESPECIFICACIONES TECNICAS DE LOS ROUTER CISCO
SERIE 2600 Y 7500]



DATA SHEET

CISCO 2600 SERIES MODULAR ACCESS ROUTERS, INCLUDING THE CISCO 2600XM MODELS AND THE CISCO 2691

The Cisco® 2600 Series is an award-winning series of modular multiservice access routers, providing flexible LAN and WAN configurations, multiple security options, voice and data integration, and a range of high-performance processors. The wide range of features and interfaces and the flexibility of adding more than 50 modules makes the Cisco 2600 Series the ideal branch-office router for today's and tomorrow's customer requirements.

The Cisco 2600 Series of modular routers includes the Cisco 2612, Cisco 2600XM models, and the Cisco 2691 (see Figure 1). These models deliver extended performance, high density, enhanced security performance, and concurrent application support to meet the growing demands of branch offices. In addition, numerous Cisco 2600 Series product bundles have been introduced (Refer to Table 9). These bundles offer an additional cost savings and provide easy ordering to meet branch-office requirements.

Figure 1. Cisco 2600 Series Modular Access Routers



PRODUCT OVERVIEW

Cisco 2600 Series Modular Access Routers: Introduction

As companies grow, the diversity of protocols, increased performance, LAN media, WAN services, and networking equipment required to support mission-critical network services expand dramatically. With extensive support for multiprotocol data routing, voice and data integration, DSL access, ATM, dial access services, and integrated switching, the Cisco 2600 Series provides a flexible, scalable, integrated solution that simplifies the process of deploying and managing the branch-office network solutions.

The Cisco 2600 Series offers a comprehensive feature set ideal for solutions requiring the following support:

- Multiservice voice and data integration
- VPN access with firewall and encryption options
- Analog dial access services
- Routing with bandwidth management
- Inter-VLAN routing

- Delivery of high-speed business-class DSL access
- Cost-effective ATM access
- Integration of flexible routing and low-density switching
- Integration of content networking
- Integration of intrusion detection systems (IDSs)
- Integration of network analysis systems

The foundations of these solutions are the Cisco IOS[®] Software elements of security, availability, quality of service (QoS), manageability, and integration. Combined, these features support the delivery of distributed intelligence that extends to the branch office. By delivering powerful business tools and applications to the branch, enterprises can realize the business benefits of increased productivity, cost reductions, and scalable exchange of information.

The modular architecture of the Cisco 2600 Series allows interfaces to be upgraded to accommodate network expansion or changes in technology as new services and applications are deployed. Modular interfaces are shared with the Cisco 1700 and Cisco 3700 series, providing unrivaled investment protection and reducing the complexity of managing the remote network solution by integrating the functions of multiple, separate devices into a single, compact unit. Network modules available for the Cisco 2600 and Cisco 3700 series support a broad range of applications, including multiservice voice and data integration, integrated switching, analog and ISDN dial access, and serial device concentration.

The integration of field-installable advanced integration modules (AIMs) enhances the performance of the Cisco 2600 Series by offloading processor-intensive functions onto a dedicated coprocessor while preserving external interface slots for other applications. A variety of AIMs are currently supported on all Cisco 2600 and Cisco 3700 series routers, providing high-performance, hardware-assisted data compression, data encryption, ATM, and digital-signal-processor (DSP) functions for up to 30 digital voice channels.

Cisco Systems[®] delivers enterprise- and provider-class versatility, integration, and power to branch offices with the Cisco 2600 Series of modular access routers. The Cisco 2600XM models and the Cisco 2691, they provide a high degree of performance, service density, and flexibility to address evolving branch-office requirements.

Cisco 2600 Series Modular Access Routers: Overview

Driven by a powerful CPU processor along with high-performance DSPs and auxiliary processors on various interfaces, the Cisco 2600 Series supports the advanced QoS, security, and network integration features required in today's evolving branch offices (see Table 1).

Each of the Cisco 2610XM through Cisco 2651XM releases supports one network module slot, two WAN interface card (WIC) slots, and one AIM slot. One network module slot is provided on the Cisco 2691, offering the same format as the Cisco 2600XM Series of routers, but the Cisco 2691 also includes one additional WIC and AIM slot for applications that require increased service requirements. These slots share more than 50 different modules across three Cisco product lines—the Cisco 1700 Series, the Cisco 2600 Series, and the Cisco 3700 Series.

Table 1. Platform Overview

Platform	Network Modules	AIMs	WICs	Fixed LAN Ports	Performance (up to kpps)	DRAM (default MB/maximum MB)	Flash Memory (default MB/maximum MB)	Included Cisco IOS Software Feature Set
Cisco 2610XM and Cisco 2611XM	1	1	2	1 Fast Ethernet/2 Fast Ethernet	20	128/256	32/48	Cisco IOS Software IP Base
Cisco 2612	1	1	2	1 Token Ring/1 Ethernet	15	32/64	8/16	Cisco IOS Software IP Base
Cisco 2620XM and Cisco 2621XM	1	1	2	1 Fast Ethernet/2 Fast Ethernet	30	128/256	32/48	Cisco IOS Software IP Base
Cisco 2650XM and Cisco 2651XM	1	1	2	1 Fast Ethernet/2 Fast Ethernet	40	256/256	32/48	Cisco IOS Software IP Base
Cisco 2691	1	2	3	2 Fast Ethernet	70	256/256	32/128	Cisco IOS Software IP Base

KEY FEATURES AND BENEFITS

The Cisco 2600 Series supports a wide range of performance and scalability for branch-office networking solutions, allowing businesses to extend a cost-effective, transparent network infrastructure to the branch office with the following benefits:

- *Investment protection*—Support for field-upgradable, modular components on the Cisco 2600 Series allows customers to easily change network interfaces without a complete system upgrade of the entire branch-office network. The AIM slot(s) further protects investments by offering the expandability to support advanced services such as hardware-assisted data compression, data encryption, ATM data and voice access, or DSP digital voice applications.
- *Lower cost of ownership*—By integrating the functions of switches, channel service units (CSUs), data service units (DSUs), ISDN Network Termination 1 (NT1) devices, firewalls, modems, compression or encryption devices, and other equipment found in branch-office wiring closets in a single, compact unit, the Cisco 2600 Series provides a space-saving solution that is more manageable.
- *Integrated flexible routing and low-density switching*—With support of an optional 16-port 10/100 Cisco EtherSwitch® Network Module, branch offices can take advantage of the flexibility of integrated routing and switching functions in one unit for low port densities. This offers high-speed connections between individual desktops, servers, and other network resources in a single unit for Layer 2 and allows WAN connection at Layer 3 through the router. An optional external power chassis provides in-line power to IP phones and to Cisco Aironet® 802.11 base stations.

- *Integration of content networking and branch-office routing*—With the integration of an optional content-engine network module with branch-office routing, Cisco offers the industry’s first and only router-integrated content-delivery system. Combining intelligent caching, content routing, and management with robust branch-office routing, WAN bandwidth is conserved for important branch IP services such as voice over IP (VoIP), while simplifying configuration, deployment, and operations.
- *Voice and data integration*—Cisco offers the industry’s broadest, most scalable multiservice voice and data integration solution set. The Cisco 2600 Series allows network managers to provide scalable analog and digital telephony without investing in a one-time solution, giving enterprises greater control of their converged telephony needs. Using the voice and fax modules, the Cisco 2600 Series may be deployed in both VoIP and voice-over-Frame Relay (VoFR) networks. The packet voice trunk network module supports up to 60 simultaneous voice calls as well as supporting routing and other services. When used with the ATM AIM, voice over ATM (VoATM) using ATM Adaption Layer 2 (AAL2) or AAL5 can be deployed.
- *Enterprise and provider-class solution*—This solution meets the requirements of multiservice enterprises and their managed service customer-premises-equipment (CPE) providers with high-reliability features, multiple WAN connections, and the ability to migrate from data-only to time-division multiplexing (TDM) voice and from data to packetized voice and data infrastructure.
- *Security*—With the integration of optional VPN modules, Cisco IOS Software-based firewalls and Intrusion Prevention System (IPS), content-engine network modules, or intrusion detection network modules, Cisco offers the industry’s most robust and adaptable security solution for branch-office routers. VPN modules can be used to provide up to 10 times the performance over software-only encryption. Additionally, the new Cisco Intrusion Detection System Network Module allows decryption, tunnel termination, and traffic inspection at the first point of entry into the network while freeing the router CPU from process-intensive IDS tasks.
- *Business-class DSL connectivity*—With the WIC-ADSL, WIC-1ADSL-I-DG, WIC-1ADSL-DG, WIC-1SHDSL, and WIC-1SHDSL-V2 modules added to the Cisco 2600 Series offers a broad range of business-class broadband options with scalable performance, flexibility, and security for branch and regional offices. The Cisco 2600 Series provides an ideal solution for a variety of businesses requiring high-speed business-class DSL connectivity on a secure, high-performance modular platform.
- *Increased memory capacity on Cisco 2600XMs*—The memory capacity of the Cisco 2600XM platforms can now be increased to 256 MB of synchronous dynamic RAM (SDRAM) using a new 128-MB SDRAM dual in-line memory module (DIMM). This new 128-MB DIMM offers higher-density memory, providing the ability to support memory increases to 256 MB of DRAM (with the correct ROMmon).

The Cisco 2600 Series brings a cost-effective combination of versatility, integration, and increased performance to remote branch offices with the key features listed in Table 2.

Table 2. Cisco 2600 Series Benefits

Feature	Benefit
Versatility and Investment Protection	
<i>Modular Architecture that Shares Interfaces with Cisco 1700 and Cisco 3700 Series Routers</i>	<ul style="list-style-type: none"> • Network interfaces are field-upgradeable to accommodate future technologies. • Additional services can be added on an “integrate as you grow” basis. • This architecture takes advantage of the large existing portfolio of WICs, virtual interface cards (VICs), network modules, and AAIMs shared across platforms to reduce sparring, training, configuration and installation, and maintenance costs.

Feature	Benefit
<i>LAN and WAN Connectivity Integrated into Chassis</i>	<ul style="list-style-type: none"> • Voice and WIC support can be used for WAN (data-only) connectivity and then redeployed to support channelized voice and data or packet voice applications. • The Cisco 2600 Series offers integrated 10/100 Ethernet ports on most platforms. • A combination of AIMs and WICs along with network modules provides greater flexibility to create new configurations as requirements change.
<i>Flexible IP Telephony and Voice Gateway Configurations</i>	<ul style="list-style-type: none"> • The Cisco 2600 Series helps enable incremental migration from TDM infrastructure to IP telephony. • Support for optional embedded call processing using Cisco CME for up to 72 IP Phones. • Support for up to a 100 mailboxes using the Cisco Unity[®] Express voice messaging system is possible with the integration of an optional voice-mail AIM or network module. • The Cisco 2600 Series is compatible with over 90 percent of the world's TDM private branch exchanges (PBXs). • The Cisco 2600 Series offers configuration options for higher density and mixed analog and digital gateway configurations. • New voice gateway bundles include the features needed for immediate integration of voice and data.
<i>AIM Slot</i>	<ul style="list-style-type: none"> • The architecture is expandable for integration of advanced services such as hardware-assisted data compression, encryption, voice, and ATM. • The Cisco 2600 Series maximizes performance by offloading processor-intensive applications to a coprocessor. • The AIM slot provides expanded services, freeing the network module slot for other applications.
<i>DC Power Supply Option Platforms</i>	<ul style="list-style-type: none"> • This platform allows deployment in DC power environments such as telecommunications carrier central offices.
Enterprise and Managed Service CPE-Class Performance	
<i>High-Performance Architecture</i>	<ul style="list-style-type: none"> • The Cisco 2600 Series offers support for advanced QoS features such as the Resource Reservation Protocol (RSVP), Weighted Fair Queuing (WFQ), and IP Precedence to reduce recurring WAN costs. • The Cisco 2600 Series offers support for cost-effective, software-based data compression and data encryption. • Integration of traditional networks is accomplished with data-link switching plus (DLSW+) and Advanced Peer-to-Peer Networking (APPN). • High-speed routing performance of up to 70,000 packets per second offers maximum scalability to support more concurrent functions (Cisco 2691).

Feature	Benefit
<i>Security</i>	<ul style="list-style-type: none"> • Cisco IOS Firewall feature sets provide support for advanced security features such as Context-Based Access Control (CBAC), Java blocking, denial-of-service protection, intrusion prevention, and audit trails. • Network Admission Control (NAC) support provides Anti-virus protection and is available with an optional upgrade to a Cisco IOS Security image. • The high-performance architecture helps enable security features such as data encryption, tunneling, and user authentication and authorization for VPN access. • The Cisco 2600 Series supports the Advanced Encryption Standard (AES). • The Cisco 2600 Series offers optional encryption AIMs, providing up to 80 Mbps of encryption performance. • URL filtering is available onboard with an optional content-engine network module or externally with a PC server running URL filtering software working in conjunction with IOS. • Support for the Cisco Router and Security Device Manager (SDM) provides support faster and easier deployment of security and WAN access features. • An optional IDS network module is available that is capable of monitoring up to 45 Mbps of traffic and has support for over 1000 intrusion prevention signatures.
<i>Cisco IOS Software</i>	<ul style="list-style-type: none"> • The Cisco 2600 Series supports common Cisco IOS Software feature sets as used on the Cisco 2600 and Cisco 3700 routers. • New releases of Cisco IOS Software add support for new services and applications. • The Cisco 2600 Series helps enable end-to-end solution support for Cisco IOS Software-based QoS and security mechanisms. • A full range of VoIP and security and routing features is available.
Reliability	
<i>Support for Optional Redundant Power</i>	<ul style="list-style-type: none"> • The Cisco 2600 Series accommodates an optional redundant power supply and minimizes network downtime. • The redundant power supply can be shared with other network components such as the Cisco Catalyst® 2950 Series to protect the network from downtime due to power failures.
<i>Survivable Remote Site Telephony</i>	<ul style="list-style-type: none"> • The Cisco 2600 Series helps enable branch offices to take advantage of centralized voice applications while cost-effectively providing backup redundancy.
<i>Dial-on-Demand Routing</i>	<ul style="list-style-type: none"> • The Cisco 2600 Series allows automatic backup of WAN connection in case of a primary link failure.
QoS	
<i>Full Support for Cisco IOS Software-Based QoS Mechanisms</i>	<ul style="list-style-type: none"> • The Cisco 2600 Series allows enhanced use of network resources and guarantees quality, reliability, and efficiency in voice and data service delivery.

Feature	Benefit
Simplified Management	
<i>Cisco Router and Security Device Manager (SDM)</i>	<ul style="list-style-type: none"> The Cisco SDM is an intuitive, easy-to-use, Web-based device management tool embedded within the Cisco IOS Software access routers. The Cisco SDM helps enable resellers and customers to quickly and easily deploy, configure, and monitor a Cisco access router without requiring knowledge of the Cisco IOS Command-Line Interface (CLI).
<i>Integrated CSU and DSU, Add/Drop Multiplexers, Analog Modems, and NT1 Options</i>	<ul style="list-style-type: none"> This integration helps enable remote management of all CPE elements for higher network availability and lower operational costs.
<i>Enhanced Setup Feature</i>	<ul style="list-style-type: none"> Context-sensitive questions guide the user through the router configuration process, allowing faster deployment.
<i>Support for Cisco AutoInstall</i>	<ul style="list-style-type: none"> Remote routers are configured automatically across a WAN connection to save the cost of sending technical staff to the remote site.
<i>VLAN Support</i>	<ul style="list-style-type: none"> VLAN support enables inter-VLAN routing with the Cisco Inter-Switch Link (ISL) protocol and 802.1Q.

Cisco 2600 Series Hardware and Software Options

Cisco 2600 Series routers offer a choice of Ethernet, Token Ring, and autosensing 10/100 Ethernet LAN interfaces. In addition, depending on the model, one network module slot, two or three WIC slots, and one or two AIM slots as well as one 115.2-kbps console port and one 115.2-kbps auxiliary asynchronous port are offered.

Network Module Options

Network modules help enable the Cisco 2600 Series to be customized to meet the needs of virtually any branch office. These modules support a broad range of applications, including multiservice voice and data integration, analog and ISDN dial access, ATM access, integration of low-density switching, IDSs, content networking, and serial device concentration (refer to Table 5 for the complete list of supported network modules for the Cisco 2600 Series). Other advantages of the network module are to provide integrated services onto one platform for greater management of services and ease of operations. By offering network modules such as the Cisco EtherSwitch Network Module, content engine, network analysis, and intrusion detection network modules, more services are integrated onto a single platform. These modules provide the advantage of integrating switching, content networking, or intrusion detection with routing onto one platform for greater management and ease of operation.

The Cisco 16-Port 10/100 EtherSwitch Network Module combines robust Layer 3 flexible WAN routing with low-density line-rate Layer 2 switching, providing straightforward configuration, easy deployment, and integrated management in a single platform (see Figure 2). The Cisco EtherSwitch modules use the powerful features available in both Cisco IOS Software and Cisco Catalyst switching, with hardware supporting 802.1p Layer 2 prioritization, while Cisco IOS Software supports Layer 3 Differentiated Services (DiffServ) and class-of-service (CoS) markings for critical

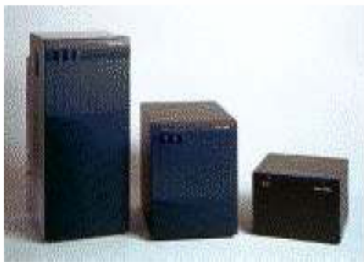


DATA SHEET

CISCO 7500 SERIES ROUTER

High-density, highly available aggregation and intelligent distributed network services at the edge for service providers and enterprises.

Figure 1. Cisco 7500 Series Router



The Cisco® 7500 Series router is the premier Cisco distributed services, multiprotocol platform, now with twice the performance and enhanced high-availability (HA) features. The Cisco 7500 Series combines proven Cisco software technology with exceptional reliability, availability, serviceability, and performance features to meet the requirements of today's most mission-critical networks. The Cisco 7500 Series router provides service provider and enterprise networks with the flexibility they need to meet the constantly changing requirements of their networks. The three models of the Cisco 7500 Series allow users to choose the exact configuration needed to optimize installations and network designs for cost and functionality.

KEY FEATURES

- *High-performance distributed switching* - This feature delivers high performance for mission-critical applications by supporting high-speed media and high-density configurations. Using the processing capabilities of the Versatile Interface Processors (VIP) and distributed Cisco Express Forwarding (dCEF), the Cisco 7500 Series router system capacity can exceed two million packets per second (pps).
- *Full support for Cisco IOS® Software and enhancements for high-performance, feature-rich IP network services* - The Cisco 7500 Series router performs network services such as quality of service (QoS) at high speed. VIP technology extends the performance of these features through distributed IP services.
- *High port density and unmatched interface flexibility* - The Cisco 7500 Series router provides high port density and an extensive range of LAN and WAN interfaces (port adapters). These features dramatically reduce the cost per port and allow for a flexible configuration.
- *High availability* - Enhanced features and capabilities include redundant route processors and power supplies, software fault isolation, and failover capabilities.

Table 1. Feature and Benefits Overview

Features	Benefits
Chart_subhead Style Sheet	Scales the performance linearly with a number of VIPs
Doubled switching and forwarding performance	Provides high-performance switching up to 2.2 Mpps
LAN/WAN interfaces	Lowers cost of ownership by consolidating interfaces in one platform
Most complete port adapter family	Increases customer's flexibility for various media access
Common port adapters with Cisco 7200 Router, Cisco 7400 Router, and FlexWAN	Protects customer's investment
High port density (two port adapters per VIP)	Reduces the cost per port and allows flexible configuration
Enhanced high-availability features	Reduces customer's downtime and increases customer loyalty
Advanced IP network services	Brings customer new revenue stream by value-added services
Broad customer base	Provides market-proven performance, stability, reliability, and serviceability

APPLICATIONS

- Content networking-Network-Based Application Recognition (NBAR) and QoS services, such as Distributed Weighted Random Early Detection (dWRED), Distributed Class-Based Weighted Fair Queuing (dCBWFQ), and distributed traffic shaping (dTS)
- Multiservice-Real-Time Transport Protocol (RTP) header compression, Multilink PPP (MLPPP) with link fragmentation and interleaving (LFI), Frame Relay Forum (FRF) 11 and 12 support for optimal digital voice transmission
- DS0 to DS1, DS3 and STM-1 WAN aggregation
- IBM mainframe connectivity

Table 2. Maximum Physical Ports/Slots

	Cisco 7505	Cisco 7507	Cisco 7513
Configurable interface slots	4	5	11
Ethernet (10BASE-T) ports	64	80	176
Ethernet (10BASE-FL) ports	40	50	110
Fast Ethernet (TX) ports	16	20	44
Fast Ethernet (FX) ports	16	20	44
Gigabit Ethernet ports	1	2	2
FDDI (FDX, HDX) ports	8	10	22
ATM ports	8	10	22
Packet over SONET OC3	8	10	22
Token Ring (FDX, HDX) ports	32	40	88
Synchronous serial ports	64	80	176
ISDN PRI, multichannel T1/E1 ports	64	80	176

Multichannel T3 ports	16	20	44
HSSI ports	8	10	22
IBM channel interface ports	8	10	22

Table 3. Chassis, Route Switch Processors (RSPs), and VIPs

Feature	Cisco 7505	Cisco 7507	Cisco 7513
Chassis/rack	5	3	2
IP/VIP slots	4	5	11
Bandwidth	1 Gbps	2 Gbps	2 Gbps
Maximum RSPs	1	2	2
Maximum power supplies	1	2	2

Table 4. Route Switch Processor (RSP) Specifications

Product	Cisco Express Forwarding Switching (pps)	Packet Memory (SRAM)	Program Memory (DRAM)	Boot Flash	PCMCIA Flash Card	Flash Disk Support	Support for Error Correction Code (ECC)
RSP16	530k	8 MB	128 MB (default)	16 MB	N/A	48 MB (default)	Yes
			256 MB			64 MB	
			512 MB			128 MB	
			1 GB (post FCS)				
RSP8	470+ k	8 MB	64 MB (default)	16 MB	16 MB	48 MB	Yes
			128 MB		20 MB (default)	64 MB	
			256 MB		32 MB	128 MB	
RSP4+	345k	2 MB	64 MB (default)	8 MB	16 MB (default)	64 MB	Yes
			128 MB		20 MB	128 MB	
			256 MB		32 MB		
RSP4	345k	2 MB	64 MB (default)	8 MB	16 MB (default)	No	No
			128 MB		32 MB		
			256 MB		20 MB		
RSP2	220k	2 MB	32 MB (default)	8 MB	16 MB (default)	No	No
			64 MB		20 MB		
			128 MB		32 MB		

Table 5. Versatile Interface Processor (VIP) Specifications

Product	Packet Forwarding (pps)	Bandwidth	Packet Memory	Program Memory
VIP6-80	140,000 to 220,000	750+ MB	64 MB (default)	64 MB (default) 128 MB 256 MB
VIP4-80	140,000 to 220,000	750+ MB	64 MB (default)	64 MB (default) 128 MB 256 MB
VIP4-50	90,000 to 140,000	750+ MB	64 MB (default)	64 MB (default) 128 MB 256 MB
VIP2-50	90,000 to 140,000	400 MB	4 MB (default) 8 MB	32 MB (default) 64 MB 128 MB
VIP2-40	60,000 to 95,000	400 MB	2 MB (default)	32 MB (default) 64 MB

*Values in bold are options

With support for up to two port adapters, the VIP supports the following:

- *High port density* - Provides a high level of network consolidation; reduces overall inventory, logistics, and maintenance costs.
- *Mixed media* - Allows users to obtain better utilization of the slots available in the Cisco 7500. Mixed-media boards (for example, Fast Ethernet and serial) enable users to tailor the VIPs to specific media and density requirements.
- *Packet memory* - Each VIP ships with onboard packet memory, augmenting the total available system memory. This is particularly useful for applications where a large amount of buffering is required, such as in the presence of bursty traffic conditions, long round-trip propagation delays, or where there might be many high-bandwidth media vying for access to a smaller number of slower media.
- *Offload processing* - By operating a subset of the Cisco IOS Software, a VIP in a Cisco 7500 can offload some of the interface-specific functions that run in the central processor. This feature increases overall system performance.
- *Distributed switching* - Routing information is distributed from the RSP in the Cisco 7500 to one or more interfaces, enabling the VIP to make its own multilayer switching decisions. This feature enables an architecture that can gracefully scale to meet increasingly higher levels of system performance.

PRODUCT SPECIFICATIONS

Interfaces

The Cisco 7500 Series offers scalable density with a wide range of interfaces. These interfaces include:

- Ethernet, Fast Ethernet, Gigabit Ethernet
- Fiber Distributed Data Interface (FDDI), Token Ring
- ISDN Primary Rate Interface (PRI)

- High-Speed Serial Interface (HSSI)
- Packet over T3/E3
- Multichannel T1/E1/T3
- ATM
- Packet over SONET (POS)
- Spatial Reuse Protocol (SRP) [also known as Dynamic Packet Transport (DPT)]
- IBM
- Voice

High-Availability Features

- *High System Availability* - The RSP supports the HSA feature, which allows two RSPs to be used simultaneously with the HSA feature enabled and configured. With the HSA feature, one RSP operates as the active processor and the other RSP operates as the standby processor, which takes over and reboots the system if the active RSP fails. In addition, the Cisco 7500 supports redundancy of power supplies.
- *Cisco 7500 Single Line Card Reload* - The Single Line Card Reload (SLCR) feature isolates a fault in one VIP from the rest of the system. It allows the system to reload only the line card that has failed, without affecting the work of the other line cards. This feature dramatically reduces total outage time and impact.
- *Cisco 7500 Route Processor Redundancy+* - The RPR+ feature is an enhancement to the RPR feature. RPR+ further accelerates RSP switchover (down to only 30–40 seconds) compared to RPR. Also, it keeps the line cards from being reset and reloaded when an RSP switchover occurs.
- *Cisco 7500 Fast Software Upgrade* - The Fast Software Upgrade (FSU) feature reduces planned downtime; this feature is based on the same mechanism as RPR. It allows users to configure the system to switch over to a standby RSP, which is preloaded with a different image from that running on the active RSP.
- *Cisco 7500 stateful switchover* - This feature, which is based on RPR+, allows the active RSP to pass the necessary state information of key routing and interface protocols to the standby RSP upon switchover, thereby reducing the time for the standby RSP to learn and converge routes.
- *Cisco 7500 Non-stop forwarding* - Also based on RPR+, Non-Stop Forwarding allows routers with redundant RSPs to continue forwarding data to the standby RSP during a switchover. This feature uses the Forwarding Information Base (FIB) that was current at the time of the switchover. Once the routing protocols have converged, the FIB table is updated and stale route entries are deleted. This feature eliminates downtime during the switchover.

PHYSICAL SPECIFICATIONS

Table 6. Environmental Conditions

	Cisco 7505	Cisco 7507	Cisco 7513
Operating temperature	32° to 104°F (0° to 40°C)	32° to 104°F (0° to 40°C)	32° to 104°F (0° to 40°C)
Storage temperature	–4° to 149°F (–20° to 65°C)	–4° to 149°F (–20° to 65°C)	–4° to 149°F (–20° to 65°C)
Operating humidity	10 to 90% (noncondensing)	10 to 90% (noncondensing)	10 to 90% (noncondensing)

Table 7. Physical Specifications

	Cisco 7505	Cisco 7507	Cisco 7513
Height	10.5 in. (26.67 cm)	19.3 in. (48.9 cm)	33.75 in. (85.73 cm)
Width	17.5 in. (44.45 cm)	17.5 in. (44.6 cm)	17.5 in. (44.45 cm)
Depth	17.0 in. (43.18 cm)	25.1 in. (63.8 cm)	22.0 in. (55.88 cm)
Weight (max)	70 lb (31.75 kg)	145 lb (65.90 kg)	160 lb (72.58 kg)
Weight (installation/minimum)	46 lb (20.87 kg)	76 lb (34.60 kg)	62 lb (28.13 kg)

Table 8. Power

	Cisco 7505	Cisco 7507	Cisco 7513
Input VA	780 max	945 max	1600 max
Output watts	600 max	700 max	1200 max
	540 typical	650 typical	1050 typical
Heat dissipation	780W (2661 Btus/hr)	945W (3224 Btus/hr)	1600W (5461 Btus/hr)
AC input voltage	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
Frequency	50–60 Hz	50–60 Hz	50–60 Hz
AC input current	9A max @ 100 VAC	12A max @ 100 VAC	16A max @ 100 VAC
	4A max @ 240 VAC	6A max @ 240 VAC	7A max @ 240 VAC
DC input voltage	–48 to –60 VDC	–48 to –60 VDC	–48 to –60 VDC
DC input current	20A max @ –48 VDC		35A max @ –48 VDC
	16A max @ –60 VDC		28A max @ –60 VDC

Protocols

The Cisco 7500 Series supports the following standard Internet protocols:

- *Layer 2 and Layer 3 protocols* - ARP, IPCP, IP forwarding, IP host, IP multicast, PPP-over-ATM, TCP, Telnet, TFTP, UDP, HDLC, frame relay, IPX, AppleTalk, DecNet, transparent bridging, VLAN, MPLS, and IPv6
- *Layer 3 routing protocols* - EIGRP, IGRP, IS-IS, OSPF, BGP, PIM, and RIP
- *Network management and security* - AAA, CHAP, FTP, RADIUS, SNMP, PAP, and TACACS
- RFC 1483: Multiprotocol Encapsulation over ATM AAL 5
- RFC 1577: Classical IP and ARP over ATM AAL 5
- *Address Resolution Protocol (ARP)* - Determines the destination MAC address of a host using its known IP address
- *BOOTP* - Uses connectionless transport layer User Datagram Protocol (UDP); allows the switch (BOOTP client) to get its IP address from a BOOTP server
- *Internet Control Message Protocol (ICMP)* - Allows hosts to send error or control messages to other hosts; is a required part of IP; for example, the ping command uses ICMP echo requests to test if a destination is alive and reachable

- *IP or IP over ATM* - Suite used to send IP datagram packets between nodes on the Internet
- *TCP* - A reliable, full-duplex, connection-oriented end-to-end transport protocol running on top of IP; for example, the Telnet protocol uses the TCP/IP protocol suite
- *Packet Internet groper (ping)* - Tests the accessibility of a remote site by sending it an ICMP echo request and waiting for a reply
- *Trivial File Transfer Protocol (TFTP)* - Downloads network software updates and configuration files (Flashcode) to workgroup switch products
- *Reverse Address Resolution Protocol (RARP)* - Determines an IP address knowing only a MAC address; for example, BOOTP and RARP broadcast requests are used to get IP addresses from a BOOTP or RARPD server
- *Serial Line Internet Protocol (SLIP)* - A version of IP that runs over serial links, allowing IP communications over the administrative interface
- *Point-to-Point Protocol (PPP)* - Provides host-to-network and switch-to-switch connections over synchronous and asynchronous circuits
- *Simple Network Management Protocol (SNMP)* - Agents that process requests for network management stations and report exception conditions when they occur; requires access to information stored in a MIB
- *Telnet* - A terminal emulation protocol that allows remote access to the administrative interface of a switch over the network (in-band)
- *User Datagram Protocol (UDP)* - Enables an application (such as an SNMP agent) on one system to send a datagram to an application (a network management station using SNMP) on another system; uses IP to deliver datagrams; TFTP uses UDP/IP protocol suites
- *Dynamic Host Connection Protocol (DHCP)* - Lets a host automatically obtain their IP address, subnet mask, and default route from a pre-configured DHCP server on the network

PRODUCT REGULATORY APPROVALS AND COMPLIANCE

The Cisco 7500 Series router conforms to a number of different safety, EMI, immunity, and network homologation standards. Details of the regulatory specifications are available at: <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/4194pc75.htm>

SOFTWARE REQUIREMENTS

The minimum supported Cisco IOS Software release(s) by train for all Cisco 7500 Series router products can be found by using the Hardware/Software Compatibility Matrix available at: <http://www.cisco.com/pcgi-bin/front.x/Support/HWSWmatrix/hwswwmatrix.cgi>

Please visit: http://www.cisco.com/public/ordering_info.shtml to place an order.

Product Part Numbers

Table 9. Cisco 7500 Series Router Port Adapters, Interface Processors, and Service Adapters

Part Number	Description
LAN Port Adapters	
PA-4E	Four-port Ethernet 10BASE-T port adapter
PA-8E	Eight-port Ethernet 10BASE-T port adapter
PA-FE-FX	One-port Fast Ethernet 100BASE-FX port adapter
PA-FE-TX	One-port Fast Ethernet 100BASE-TX port adapter
PA-2FE-TX	Two-port Fast Ethernet 100BASE-FX port adapter
PA-2FE-FX	Two-port Fast Ethernet 100BASE-TX port adapter

Part Number	Description
PA-5EFL	Five-port Ethernet 10BASE-FL port adapter
PA-4R-DTR	Four-port dedicated Token Ring, 4/16 Mbps, HDX/FDX port adapter
PA-F/FD-MM	One-port FDDI full-duplex multimode port adapter
PA-F/FD-SM	One-port FDDI full-duplex single-mode port adapter
Serial Port Adapters	
PA-4T+	Four-port serial port adapter, enhanced
PA-8T-V35	Eight-port serial, V.35 port adapter
PA-8T-232	Eight-port serial, 232 port adapter
PA-8T-X21	Eight-port serial, X.21 port adapter
PA-4E1G/75	Four-port E1 G.703 serial port adapter (75ohm/unbalanced)
PA-4E1G/120	Four-port E1 G.703 serial port adapter (120ohm/balanced)
PA-T3	One-port T3 serial port adapter with T3 DSUs
PA-T3+	One-port T3 serial port adapter enhanced
PA-2T3	Two-port T3 serial port adapter with T3 DSUs
PA-2T3+	Two-port T3 serial port adapter enhanced
PA-E3	One-port E3 serial port adapter with E3 DSU
PA-2E3	Two-port E3 serial port adapter with E3 DSUs
HSSI Port Adapters	
PA-H	One-port HSSI port adapter
PA-2H	Two-port HSSI port adapter
Multichannel and ISDN Port Adapters	
PA-MC-2T1	Two-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-4T1	Four-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-8T1	Eight-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2E1/120	Two-port multichannel E1 port adapter with G.703 120ohm interface
PA-MC-8E1/120	Eight-port multichannel E1 port adapter with G.703 120ohm interface
PA-MC-8TE1+	Eight-port multichannel T1/E1 8PRI port adapter
PA-MC-STM-1SMI	One-port multichannel STM-1 single-mode port adapter
PA-MC-STM-1MM	One-port multichannel STM-1 multimode port adapter
PA-MC-T3	One-port multichannel T3 port adapter
PA-MC-2T3+	Two-port multichannel T3 port adapter, enhanced
PA-MC-E3	One-port multichannel E3 port adapter
ATM Port Adapters	
PA-A3-8E1IMA	Eight-port ATM inverse multiplexer E1 (120 ohm) port adapter
PA-A3-8T1IMA	Eight-port ATM inverse multiplexer T1 port adapter
PA-A3-E3	One-port ATM enhanced E3 port adapter
PA-A3-T3	One-port ATM enhanced DS3 port adapter
PA-A3-OC3MM	One-port ATM enhanced OC-3c/STM1 multimode port adapter
PA-A3-OC3SMI	One-port ATM enhanced OC-3c/STM1 single-mode (IR) port adapter

Part Number	Description
PA-A3-OC3SML	One-port ATM enhanced OC-3c/STM1 single-mode (LR) port adapter
PA-A3-OC12MM	One-port ATM enhanced OC12/STM4 multimode
PA-A3-OC12SMI	One-port ATM enhanced OC12/STM4 single-mode intermediate reach
SONET Port Adapters	
PA-POS-OC3MM	One-port Packet/SONET OC-3c/STM1 multimode port adapter
PA-POS-OC3SMI	One-port Packet/SONET OC-3c/STM1 single-mode (IR) port adapter
PA-POS-OC3SML	One-port Packet/SONET OC-3c/STM1 single-mode (LR) port adapter
Digital Voice Trunk Port Adapters	
PA-VXB-2TE1+	Two-port T1/E1 moderate capacity enhanced voice port adapter
PA-VXC-2TE1+	Two-port T1/E1 high-capacity enhanced voice port adapter
PA-VXA-1TE1-30+	One-port T1/E1 Digital Voice Port Adapter with 30 channels
PA-VXA-1TE1-24+	One-port T1/E1 Digital Voice Port Adapter with 24 channels
DPT Interface Processors	
SRPIP-OC12MM	Dynamic Packet Transport Interface Processor, multimode
SRPIP-OC12SMI	Dynamic Packet Transport Interface Processor, single-mode, intermediate reach
SRPIP-OC12SML	Dynamic Packet Transport Interface Processor, single-mode, long reach
SRPIP-OC12SMX	Dynamic Packet Transport Interface Processor, single-mode, extended reach
GEIP Interface Processor	
GEIP	Gigabit Ethernet Interface Processor
GEIP+	Gigabit Ethernet Interface Processor, enhanced
Service Adapter	
SA-ENCRYPT	Encryption Service Adapter
IBM Interface Processors	
CX-CIP2-ECA1	Channel IP2 with single ESCON channel interface
CX-CIP2-ECA2	Channel IP2 with dual ESCON channel interface

Migration Program

A Technology Migration Plan has been established for this product.

The Technology Migration Plan is an innovative, industry first, sales program that allows customers to trade in Cisco products to receive a trade-in credit towards the purchase of any new Cisco product. The program underscores Cisco's commitment to its customers for end-to-end product solutions and emphasizes Cisco's commitment to provide effective migration options in the face of ever-changing network requirements.

More specifics about this program are available at: http://www.cisco.com/offer/tic/TMP_PA.html

SERVICE AND SUPPORT

Cisco Systems® offers a wide range of service and support options for its customers. More information on Cisco service and support programs and benefits is available at: http://www.cisco.com/public/Support_root.shtml