UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

MODELO DE GESTIÓN DE CALIDAD QUE GARANTICE EL QoS EN LAS REDES QUE INTERVIENEN EN EL TRANSPORTE DE IPTV

CASO DE ESTUDIO: CORPORACIÓN CANTV

TRABAJO ESPECIAL DE GRADO

presentado ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

como parte de los requisitos para optar al titulo de

INGENIERO EN TELECOMUNICACIONES

REALIZADO POR *López García, Laura B.*
Rosario Castillo, María Elena

PROFESOR GUÍA *Ing. Encinoza, Jenny*

FECHA *Caracas, 6 de julio de 2007*

APÉNDICE A.- Plataformas que soportan el servicio IPTV

Se reseñará a continuación la infraestructura técnica de las plataformas que permiten soportar los servicios de IPTV, esta información es la base para el modelo de gestión propuesto en el presente trabajo.

La Red de Banda Ancha IP soporta servicios basados en el protocolo IP (*Internet Protocol*), principalmente el acceso a la Internet. Está conformada básicamente por tres niveles: red de Acceso de Banda Ancha, red ME y el *Backbone* IP. En la Ilustración A.1, se muestran los elementos que conforman la red de Banda Ancha IP, basados en el servicio de IPTV, cada uno de los cuales serán desarrollados en profundidad en esta sección del documento.

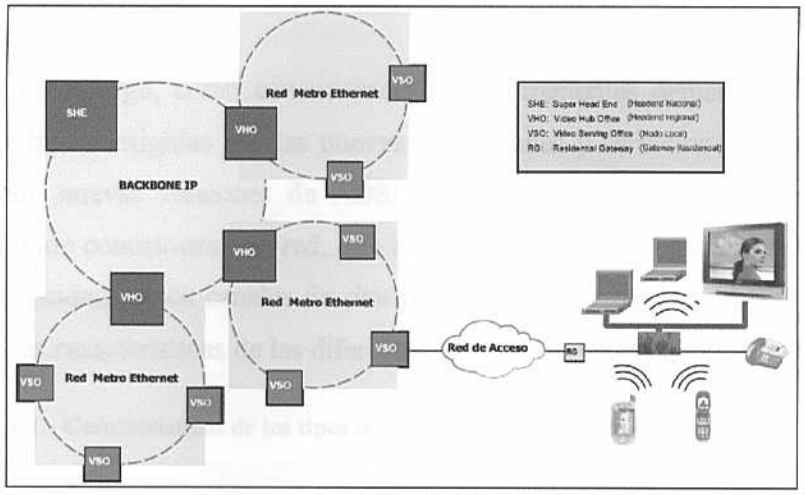


Ilustración A.1.- Red de banda ancha IP que soporta el servicio de IPTV
Tomado de *IPDR IPTV Kick-off Event*

Red de acceso de banda ancha

La Red de Acceso comprende los elementos tecnológicos que soportan los enlaces de telecomunicaciones entre los usuarios finales y el último nodo de la red, también conocido como la *última milla*. Sus principales componentes son: los medios de comunicación (par de cobre, cable coaxial, fibra óptica, canal radioeléctrico) y los elementos que realizan la adecuación de la señal a los mismos. La necesidad de ancho de banda ha hecho nacer varias tecnologías de

acceso de banda ancha. Específicamente, la tecnología xDSL, surge por la necesidad de aumentar la capacidad de transmisión del par de cobre, y utiliza técnicas de modulación modernas soportadas por los avances en el procesamiento digital de señales, para lograr transmitir a altas velocidades sobre la última milla.

La tecnología ADSL (*Asymmetric Digital Suscriber Line*) es actualmente la más utilizada, y consiste en una línea digital de alta velocidad, apoyada en el par trenzado de cobre, que soporta la línea telefónica convencional, por la cual se transmiten tres canales de información mediante la división del espectro de frecuencia en tres secciones. Es una tecnología de carácter asimétrico dado que la velocidad de bajada y de subida de datos no coincide. La velocidad de bajada es por lo general mayor debido a que el usuario exige más información de la red que la que aporta a la misma.

Sin embargo, como consecuencia de las crecientes demandas de mayor ancho de banda exigidas por las nuevas aplicaciones y servicios multimedia, se han creado nuevas versiones de ADSL. ADSL2 y ADSL2+ son una nueva generación de conexiones a la red, que aumenta el ancho de banda y permite una mayor velocidad de los canales de *downstream* y *upstream*. En la tabla A.1, se resumen las características de las diferentes tecnologías ADSL mencionadas.

Tabla A.1.- Características de los tipos de ADSL. Tomado de White Paper: ADSL2 and ADSL2+

Parámetro	ADSL	ADSL2	ADSL2+
Ancho de banda de bajada	0,5 MHz	1,1 MHz	2,2 MHz
Velocidad máx. de subida	1 Mbps	1 Mbps	1,2 Mbps
Velocidad máx. de bajada	8 Mbps	12 Mbps	24 Mbps
Distancia	2 Km.	2.5 Km.	2,5 Km.
Corrección de errores	no	si	si

Los DSLAM, son dispositivos multiplexores localizados en las centrales telefónicas, que proporcionan a los abonados acceso a los servicios DSL sobre cable de par trenzado de cobre. El dispositivo separa la voz y los datos de las

líneas de abonado. En la ilustración A.2, se muestra una red típica para IPTV, servicio que demanda gran ancho de banda, sobre la tecnología ADSL.

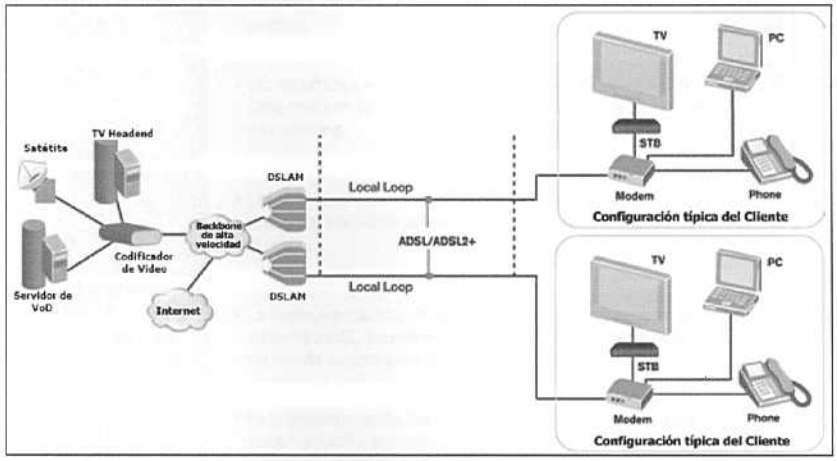


Ilustración A.2.- Red típica de IPTV sobre la tecnología DSL
Tomado de *IPTV testing over DSL*

Por otro lado, la tecnología de fibra óptica ofrece capacidades extremadamente altas a la última milla, capaces de llevar millares de flujos de audio y video simultáneos. En algunos casos, los proveedores de servicio están instalando conexiones de fibra óptica al Hub más cercano o al extremo de la calle, conocido como FTTN (*Fiber-to-the-Node*), o FTTC (*Fiber-to-the-Curb*), o incluso directamente hasta el hogar (FTTH, *Fiber-to-the-Home*). Estas tecnologías son generalmente conocidas como FTTx.

Red Metro Ethernet

La red Metro Ethernet (ME), es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, basadas en tecnología Ethernet sobre fibra óptica, con lo cual se elimina la capa ATM/SDH de las redes metropolitanas tradicionales. Estas redes soportan una amplia gama de servicios, aplicaciones y mecanismos que implican la transmisión en tiempo real, *streaming*, y flujo de datos continuo, como es el caso del audio y video. Los beneficios de la implementación de una red ME, se resumen en la siguiente tabla:

Tabla A.2.- Ventajas de la red ME

Fácil uso	• Interconectando las distintas redes que conforman un sistema ADSL mediante ME, se simplifican las operaciones de red, administración, manejo y actualización de las mismas.
Amplio uso	• Las interfaces empleadas para la operación de Metro Ethernet son las más difundidas en las instalaciones de networking.
Bajo costo	• Los servicios que ofrece Metro Ethernet ofrecen un bajo costo para la administración, operación y funcionamiento de la red.
Ancho de banda	• La implementación de una ME como red de acceso de un sistema ADSL, permiten a los usuarios acceder a conexiones de banda ancha a menor costo.
Flexibilidad	• La implementación de una ME como red de acceso de un sistema ADSL, permite modificar y manipular de forma más dinámica, versátil y eficiente, anchos de banda y cantidad de usuarios en corto tiempo.

Los nodos ME son *switches* Ethernet que se interconectan utilizando directamente fibra óptica en topologías de anillo o bus, garantizando calidad, escalabilidad y protección de los servicios.

El modelo básico de los servicios ME (véase Ilustración A.3), está compuesto por una red "switcheada" ofrecida por el proveedor de servicios (MEN, *Metro Ethernet Network*); los usuarios acceden a la red mediante los equipos del cliente (CEs, *Customer Equipment*) que se conectan a través de las interfaces de red del usuario (UNIs, *User Network Interface*) a velocidades de 10Mbps, 100Mbps, 1Gbps o 10Gbps.

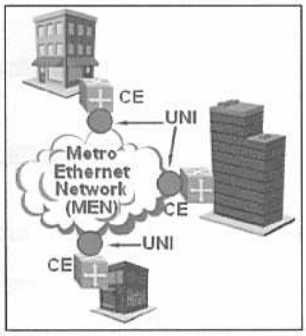


Ilustración A.3.- Modelo básico de una red ME
Tomado de Metro Ethernet Services- A technical overview

Santitoro (2003), ha definido dos tipos de conexiones virtuales Ethernet (EVC, *Ethernet Virtual Connection*), las cuales permiten la conexión entre uno o más UNIs y es creada por el ISP para un cliente específico. Éstas son:

- Tipo de Servicio Ethernet Line (E-Line): Punto a Punto.
- Tipo de Servicio Ethernet LAN (E-LAN): Multipunto a Multipunto.

La conexión E-Line, provee ancho de banda simétrico, para el envío de datos en ambas direcciones, sin asegurar desempeño.

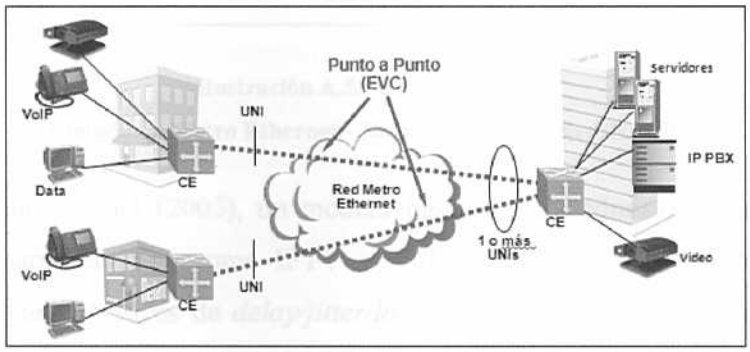


Ilustración A.4.- Conexión E-Line
Tomado de Metro Ethernet - Jornadas técnicas RedIRIS 2005

Por otra parte, una conexión E-LAN provee conectividad multipunto, conectando dos o más UNIs (véase Ilustración A.5). Cada interfaz (UNI) es conectada a un EVC multipunto, simplificando el aprovisionamiento y la activación del servicio. Sobre este tipo de conexiones serán enviados los flujos de datos de servicios como IPTV.

En la tabla A.3 se reseñan los atributos principales de los EVC y las UNI.

Servicios Triple Play en la red ME

Cada tipo de servicio *Ethernet* presenta un conjunto de atributos de servicio y sus correspondientes parámetros que definen las capacidades del servicio, y que son gestionados mediante la implementación de Políticas de

Calidad que determinan los requerimientos de la red. En la tabla A.3, se resumen los atributos en un UNI y un EVC.

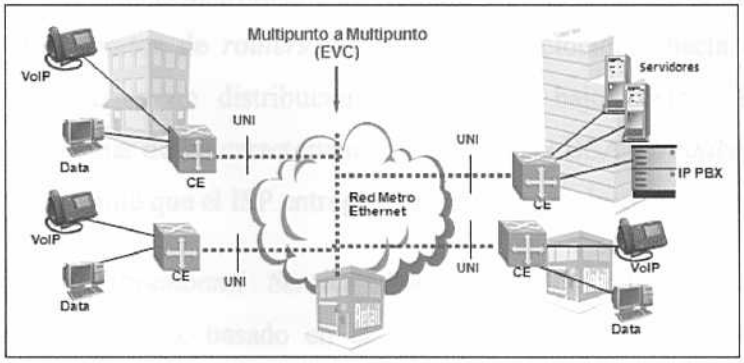


Ilustración A.5.- Conexión E-Lan
Tomado de Metro Ethernet - Jornadas técnicas RedIRIS 2005

Según Alcatel (2005), un modelo basado en la admisión de sesiones o llamadas para servicios como IPTV o VoIP, permite cubrir la necesidad de garantizar características de *delay/jitter/loss*, una vez que se acepte la conexión del servicio, definiendo controles de QoS para el ancho de banda por suscriptor, incluyendo funciones de *shaping* y políticas de servicio. Conjuntamente con la arquitectura de soporte para la diferenciación del contenido, esto permite un servicio diferenciado dentro del HSI (*High Speed Internet*).

Tabla A.3.- Atributos de servicio en UNIs y EVCs

Atributos de UNI
• Identificador, tipo de medio, velocidad, duplex, etc.)
• Atributo de soporte de VLAN tag
• Atributo de multiplexación de servicio
• Atributos de "Bundling": Más de una VLAN de cliente está asociada al EVC en una UNI.
• Atributo para el filtraje de seguridad
• Entre otros

Atributos de EVC
• Parámetros de tráfico (CIR, PIR, in, out, etc)
• Parámetros de prestaciones (delay, jitter, etc)
• Parámetros de Clase de Servicio (VLAN-ID, valor de .1p, etc.)
• Atributo de entrega de trama de servicio
• Entrega de tráfico Unicast
• Entrega de tráfico Multicast
• Entre otros

La distribución y aplicación de la política QoS, permite al ISP implementar controles significativos para el nivel del servicio por suscriptor. Esto es alcanzado mediante la distribución de carga de cientos de millares de interfaces lógicas, en los puertos de *routers* locales de alta velocidad, hacia cientos de interfaces en puertos de distribución Ethernet de bajo costo. El soporte sofisticado y granular de las características de QoS en el BSA (*Broadband Service Aggregation*), permite que el ISP entregue los servicios realmente diferenciados.

El BSR (*Broadband Service Router*), realiza el enrutamiento de distribución del servicio, basado en las garantías requeridas para su entrega. Según lo mostrado en la ilustración A.6, el BSR necesita clasificar solamente el contenido basado en las clases de envío requeridas por un BSA dado, de forma de asegurar que el tráfico de cada servicio se trate apropiadamente hacia el BSA.

En la dirección BSR-BSA, los servicios IP confían en la clasificación de del tráfico en la capa IP, para encolarlo apropiadamente hacia el BSA. Bajo condiciones de carga extrema, las cuales generalmente ocurren bajo condiciones de fallas o de congestión, los servicios de datos de baja prioridad o el tráfico del HSI, serán comprometidos para proteger el tráfico de vídeo y de voz. La clasificación del tráfico HSI, basada en la dirección IP de origen o en la marca de IEEE 802.1p (priorización de tráfico a nivel 2), permite que la información de QoS sea propagada a los nodos *upstream* o *downstream*, por los elementos de la red.

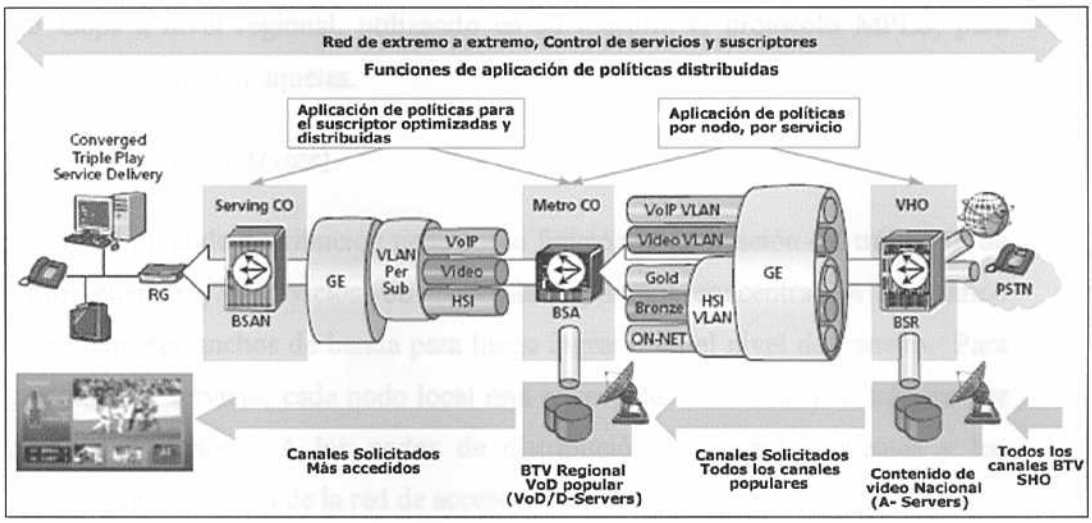


Ilustración A.6.- Arquitectura de entrega de servicios Triple Play según Alcatel-Lucent

Tomado de *the broadband aggregation networks for triple play services*

***Backbone* IP**

La palabra *backbone* se refiere a las principales conexiones troncales de una red IP, en donde las decisiones de encaminamiento IP se hacen y actualizan durante el uso en tiempo real. Está compuesta de un gran número de *routers* comerciales de gran capacidad interconectados, que llevan los datos entre puntos muy distantes. El *Backbone* IP es una red especializada en el envío de paquetes que posibilita la definición de diferentes VPN's lógicas permitiendo que diferentes subredes compartan la misma estructura física sin afectar la seguridad de la red. Posee un elevada velocidad de transmisión o *throughput*, utilizando generalmente el protocolo MPLS en el core para. Básicamente, es una red de dos niveles, uno denominado Tránsito (*Core*) y otro denominado Distribución (*Edge*).

Nivel de Tránsito (*Core*)

El nivel de tránsito está compuesto por nodos de alta capacidad cuya función es el envío de paquetes IP. Generalmente, cada nodo *core* se interconecta, por medio de fibra óptica, con por lo menos otros dos nodos *core* por caminos disjuntos, generalmente en configuración de anillo. La capacidad de transporte soportada entre nodos, es aproximadamente de 10 Gbps a nivel metropolitano y

2.5 Gbps a nivel regional, utilizando en su mayoría el protocolo MPLS, para mejorar el ruteo de paquetes.

Nivel Local (*Edge*)

El nivel de distribución tiene como función la agregación del tráfico IP de varios clientes y/o servicios, de modo de lograr una concentración del tráfico sobre mayores anchos de banda para luego ingresar en el nivel de tránsito. Para garantizar el servicio, cada nodo local está conectado a dos nodos de tránsito por caminos disjuntos. A los nodos de distribución se conectan clientes y los servicios provenientes de la red de acceso y/o otras redes.

Plataformas de servicios de CANTV

Según Gerencia Arquitectura de Redes y Sistemas (2006), en CANTV, las redes fijas soportan los servicios de voz y datos a nivel nacional, e incluyen: voz, telefonía pública, datos de baja y alta velocidad, Internet y video. Las diferentes redes que soportan estos servicios son: la Red Pública de Voz (PSTN), la Red ATM/FR, la Red de Datos Dedicada (RDCD), las Redes ME , el *Backbone* IP y las Redes de Transporte Urbanas e Interurbanas.

Específicamente hablando del transporte de los servicios de datos, actualmente, se soportan en tres plataformas diferentes: la red RDCD (Red Digital de Circuitos Dedicados), la red ATM/FR y la red IP de banda ancha, siendo transmitidos, sobre esta última, los flujos de datos de tiempo real (IPTV), por lo cual será descrita a profundidad a continuación.

Red IP de banda ancha

La Red de Banda Ancha IP de CANTV, está conformada principalmente por tres niveles: Red de Acceso de Banda Ancha, Red ME y el Backbone IP, en base a distintos proveedores, tal como se muestra en la Ilustración A.7.

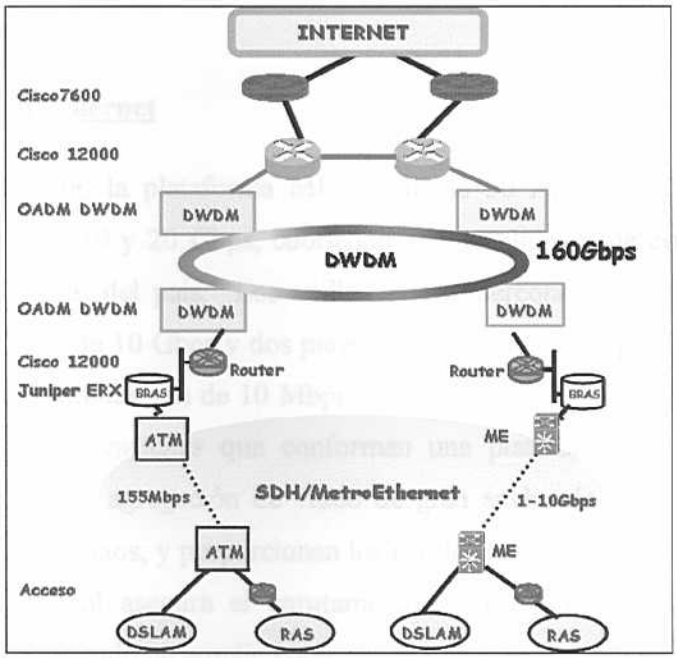


Ilustración A.7.- Arquitectura de Red Banda Ancha IP
Tomado de Arquitectura de Redes y Plataformas de Servicios de CANTV

Red de Acceso de Banda Ancha

La Red de Acceso de Banda Ancha IP está basada en la tecnología ADSL y actualmente utiliza dos tipos de DSLAM (*Digital Suscriber Line Access Multiplexer*), tanto ATM como IP, como nodos de acceso que concentran y agregan las conexiones de los suscriptores ADSL.

Los DSLAM están distribuidos en las centrales a nivel nacional, existiendo actualmente alrededor de 400 DSLAM instalados en 290 localidades, lo cual totaliza unos 520.089 puertos ADSL y ADSL2+. Una sola línea en el DSLAM implantado por CANTV, es capaz del envió de audio, video y datos para un total de 10.000 usuarios simultáneos. Presenta una interfaz de Ethernet de 1Gb, que esta acorde con la evolución de los servicios de red asociados con redes metropolitanas Ethernet. También posee un procesador de 5Gbit/seg, y soporta 1.4 Gbit/seg de ancho de banda por slot, así como un bus de 622 Mbit/seg y 155 Mbit/seg para broadcast de video y datos respectivamente. El bus de video permite a los usuarios acceder a 250 canales.

Red Metro Ethernet

Actualmente, la plataforma ME consta de 30 Anillos y 24 Buses con capacidad de 1, 2, 10 y 20 Gbps, cubriendo 157 localidades de centrales de las principales ciudades del país. Los anillos están interconectados con un par de fibras para el caso de 10 Gbps y dos pares de fibra para 20 Gbps. Las interfaces de acceso a los *switches* son de 10 Mbps, 100 Mbps, 1 GE y 10 GE. Los nodos ME utilizados, son *switches* que conforman una plataforma de enrutamiento Ethernet/MPLS para agregación de vídeo de gran ancho de banda en redes de proveedores de servicios; y proporcionan los niveles más altos de disponibilidad y redundancia, lo cual asegura el enrutamiento y distribución del servicio sin interrupción, soportando un amplio conjunto de servicios.

Los switches ME implantados por CANTV, tienen y soportan las siguientes características y protocolos:

- 802.1p: Ethernet QoS/Priority
- DSCP: Differentiated Services Code Point (DiffServ)-IP QoS
- IP Precedence: IP QoS
- EXP Bits: MPLS QoS

En la ilustración A.8, se muestra la arquitectura general de los anillos a nivel nacional y su interconexión a través del backbone IP/DWDM.

A nivel de la red ME, todo el tráfico de los usuarios que proviene desde o se dirige hacia los DSLAM, es concentrado y distribuido por los switches ME, y transportado a través de la red ME utilizando MPLS.

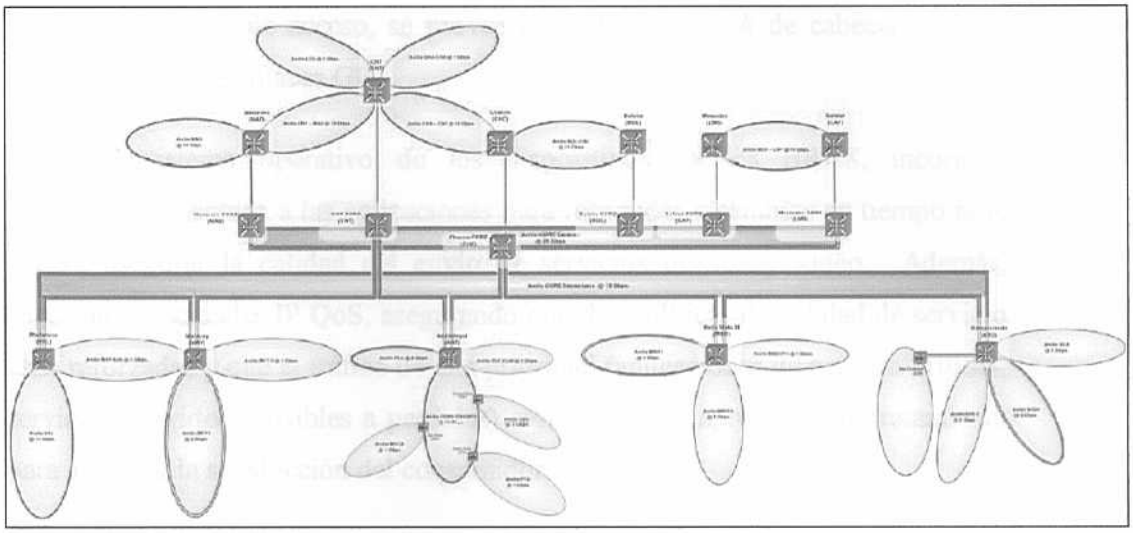


Ilustración A.8.- Arquitectura de Anillos ME a nivel nacional

Tomado de Arquitectura de Redes y Plataformas de Servicios de CANTV

En términos generales, todos los servicios de usuarios finales son transportados por la ME como servicios MPLS, con las siguientes ventajas intrínsecas:

- Aseguramiento de QoS sobre toda la ME
- Alta confiabilidad tanto para la red como para los servicios transportados, con tiempos de restauración del orden de los milisegundos.
- Escalabilidad basada en MPLS
- Gestión de red y servicios extremo a extremo.

Por otro lado, los equipos Agregadores (BRAS) utilizados en la red de CANTV, proveen acceso a Internet basado en DHCP, así como conectividad VPN L3 para usuarios residenciales y empresariales respectivamente. Estos agregadores se comunican con los *routers* de distribución a través de conexiones LAN y reciben el tráfico proveniente de los DSLAMs a través de la red ATM, para el caso de los DSLAM ATM y a través de las redes ME, para el caso de los DSLAM IP. En la cabecera de cada uno de los anillos de acceso existe uno o más BRAS conectados a través del *switch* ME vía la GE. La conectividad entre el

BRAS y el *router* de acceso, se provee a través del *switch* de cabecera vía un grupo separado de enlaces GE.

El sistema operativo de los dispositivos de los BRAS, incorpora inteligencia orientada a las aplicaciones para responder a cambios en tiempo real, y para asegurar la calidad del envío de servicios de voz y video. Además, soportan capacidades IP QoS, asegurando que las políticas de calidad de servicio sean reforzadas y que el tráfico de alta prioridad (aplicaciones de negocio críticas, servicios de video sensibles a perdidas) reciba el nivel apropiado de tratamiento para asegurar la satisfacción del consumidor.

Backbone IP

El Backbone IP/MPLS de CANTV, consiste de cuatro niveles jerárquicos: Borde, Core, Distribución y Agregación (véase Ilustración A.9). Todas estas capas están soportadas por routers que pueden escalar velocidades desde 2.5 Gbps por slot a 40 Gbps por slot, para permitir el establecimiento de servicios en las redes IP/MPLS de núcleo y cabecera de los proveedores de servicio.

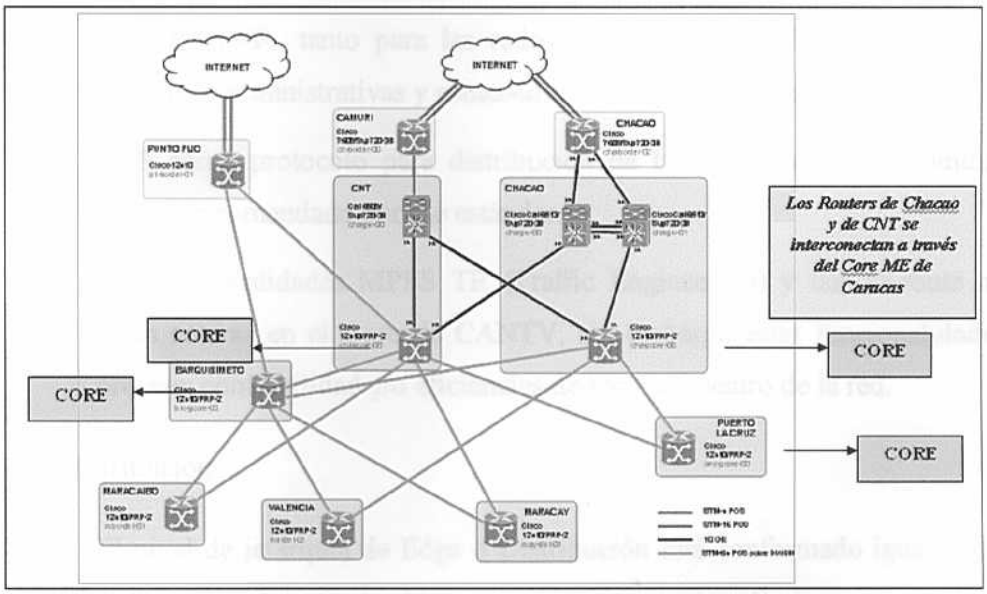


Ilustración A.9.-Arquitectura del *Backbone* IP/MPLS

Tomado de Arquitectura de Redes y Plataformas de Servicios de CANTV

Borde/ISP

Este nivel está constituido por los 3 puntos de acceso internacional para conexión hacia la Internet. Estos puntos están ubicados en tres localidades del país con enlaces STM-16 POS.

Core

El *Core* está conformado por cuatro (4) routers de *Core*. Para aumentar la disponibilidad de la red, cada router tiene dos enlaces, cada uno hacia un nodo de *Core* diferente, conformando una topología parcialmente mallada.

Cada nodo de *Core* se interconecta con la red ME de Acceso y la red de agregación local a través de dos interfaces 10GE con conectores ópticos. Entre las funcionalidades para los routers de *Core* están:

- Implementación de la funcionalidad de *Provider* ("P") para el enrutamiento usando etiquetas de conmutación.
- Conectividad MPLS hacia las diversas redes de agregación de CANTV.
- Se usa OSPF tanto para las redes internas de CANTV (loopbacks o interfaces administrativas y router-id, como para las redes de clientes).
- LDP como protocolo para distribución de las etiquetas en el dominio MPLS, recomendado por ese estándar.
- Las funcionalidades MPLS TE (Traffic Engineering) y fast re-route no están activas en el Core de CANTV, sin embargo estas funcionalidades proveen confiabilidad y/o eficiencias de recursos dentro de la red.

Distribución

El nivel de jerarquía de Edge o Distribución está conformado igualmente por *routers* con tarjetas procesadoras de nueva generación. En la región Capital, existen 6 *routers* que se interconectan al *Core* a través del anillo ME *Core* de Caracas, con una interfaz 10GE, como se ilustra en la ilustración A.10.

Los servicios IP/MPLS, QoS, Enrutamiento, *Traffic Shaping*, Filtros, etc. están configurados en los *routers* de Distribución. En el interior del país, existen 5 *routers* de distribución que se conectan al *Core* a través de enlaces DWDM (cada enlace usa una longitud de onda) para alta disponibilidad de enlace.

Entre las funcionalidades que proveen los *routers* de Distribución están las siguientes:

- Funcionalidades de Provider Edge ("PE") para L3 VPNs y L2 VPNs.
- Funcionalidades de QoS: Low-Latency Queueing / Priority Queueing, Marcaje, Mapeo de L2 CoS a MPLS EXP / DiffServ DSCP, Class-Based Weighted Fair Queueing, WRED, etc.
- Terminación Capa-2 en los enlaces de acceso a los clientes, a través de diversas tecnologías que incluyen: ATM, ME, Frame Relay, TDM y L2TP/PPP.
- Implementación de servicios IP y MPLS: Acceso Internet, L3-VPN, L2-VPN, VoIP y Video (IP Multicast).
- Seguridad: Control-Plane Policing, Traffic Shaping, uRPF, Received ACLs, etc.

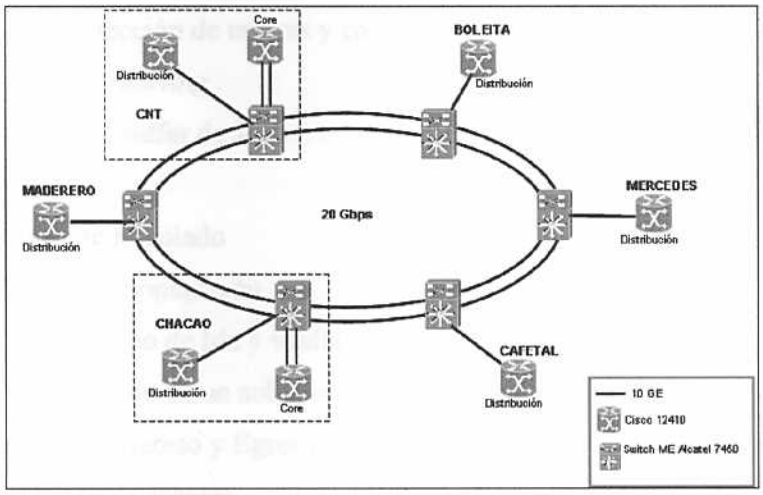


Ilustración A.10.- Arquitectura de Distribución IP en Región Capital

Tomado de Arquitectura de Redes y Plataformas de Servicios de CANTV

APENDICE B.- Inconvenientes de red y efectos negativos en la percepción de la imagen

Inconvenientes de red

Retardo

Según el VoIP Foro (2006), el retardo se define técnicamente como el tiempo que tarda un paquete en llegar desde la fuente hasta el destino. Las comunicaciones en tiempo real (como IPTV) son sensibles a este efecto. Al igual que el *jitter*, es un problema frecuente en enlaces lentos o congestionados. No hay una solución que se pueda implementar de manera sencilla ante este problema de transporte, muchas veces depende de los equipos por los que pasan los paquetes, es decir, de la red misma. Según Kun (2006), entre las fuentes de retardo en las redes se pueden mencionar las siguientes:

1. Codificación
    a. Retardo debido a conversores AD y DA
    b. Retardo de Trama
2. Retardo de Paquetización (*framing*)
3. Codificación de Canal
    a. Detección de errores y corrección
    b. Interleaving
4. Retardo de Buffer de Jitter

Relacionados a los códec a nivel de usuario final.

5. Retardo de Encolado
6. Retardo de Propagación
    a. Retardo de Ida y vuelta
    b. Retardo en un solo sentido
7. Retardo de Ingreso y Egreso
8. Retardo entre canales

Relacionados a problemas de transmisión a nivel de red.

Jitter

Según el VoIP Foro (2006), el *jitter* se define como la variación en el tiempo de llegada de los paquetes, causada por congestión de red, pérdida de sincronización, o por las diferentes rutas seguidas por los paquetes para llegar al destino.

La solución más ampliamente adoptada ante este inconveniente de transmisión es la utilización del *Jitter Buffer*. El *Jitter Buffer* consiste básicamente en asignar una pequeña cola o almacén en el receptor, para ir recibiendo los paquetes y sirviéndolos con un pequeño retraso. Un aumento del *buffer* implica menos pérdida de paquetes, pero más retraso y viceversa.

Pérdida de Paquetes

Las comunicaciones en tiempo real utilizan UDP (siglas en inglés del término *User Datagram Protocol*) como protocolo de transporte. Este protocolo no está orientado a conexión, y si se produce una pérdida de paquetes, no se encarga de su retransmisión. Si los *buffer* de los equipos de red se congestionan porque no pueden transmitir los paquetes lo suficientemente rápido, o porque los circuitos de salida son muy lentos, los paquetes pueden ser descartados por la falta de espacio.

Según VoIP Foro (2006), éste parámetro se define como la desaparición en la red de un paquete que ha sido transmitido. Existen algunos mecanismos para recuperar los paquetes perdidos, aunque generalmente con un retardo adicional.

Según Azcárate (2006), varias condiciones son causantes de la presencia de pérdida de paquetes a nivel de red:

- Errores de transmisión: Modifican bits aleatorios de los paquetes. Los niveles que hacen detección de errores se ven obligados a descartar el paquete al no estar seguros de entregarlo correctamente. Esta situación es independiente del tráfico.

- Desbordamiento de *buffer*: Un *router* que debe reenviar un paquete se encuentra con que todos sus recursos de memoria (por ejemplo en la cola de paquetes esperando la salida están ocupados). Debe descartar el paquete por falta de recursos.

Esta falta de recursos, es originada por la congestión de red, o dicho en otras palabras, cuando demasiadas fuentes envían excesivo tráfico para que la red pueda soportarlo. En la siguiente tabla, se reseñan las causas a nivel de red que pueden originar los inconvenientes de transmisión mencionados, según Adams (2006).

Tabla B.1.- Causas de los inconvenientes de Red. Tomado de: End to end QoS and Triple Play – Quality of experience for residential voice, data and video services.

Pérdida de paquetes	Retardo	Jitter
•Ruido de línea. •Cables y conectores en mal estado. •Colisiones en medios compartidos. •Interrupciones en los enlaces de telecomunicaciones, inestabilidad de reloj. •Buffers de entrada o salida inadecuados. •Fallas de Hardware •ARP cache *timeouts* •Fallas e inestabilidad de enrutamiento. •Errores de configuración. •Fallas y errores de software. •Firewalls. •Túneles de datos con MTU no adecuados. Causando descarte de paquetes.	•Distancia (Tiempo de propagación de la señal) •Enlaces de poco ancho de banda. •Largas colas en equipos de red. •Switches con retardos de serialización. •Modelado de tráfico para QoS. Procesamiento del firewall.	•Retardos de acceso al medio (ej. CSMA) •Cambios de topología de capa 2. •Cambios de enrutamiento. •Ciclos de enrutamiento. •Procesamiento basado en opción de paquetes. •Mensajes ICMP originados como resultado de la recepción de paquetes. •ARP cache *timeouts* •Congestión en los equipos de red. •Paquetes de alta prioridad ocupando colas y enlaces de telecomunicaciones. •Congestión del tráfico de la misma prioridad. •Múltiples enlaces paralelos, particularmente cuando son establecidos junto a cualquier mecanismo de QoS. •Fragmentación IP (el receptor no puede procesar los paquetes hasta que el ultimo paquete no haya llegado) •Procesamiento QoS y modelado de tráfico. •Procesamiento del firewall. •Túneles de datos con MTU no adecuados, causando así fragmentación. •Intercepción de paquetes (causas legales).

Problemas relativos a QoE que afectan la calidad de video

Se presenta a continuación, según Telchemy Incorporated[1] (2006), los problemas que pueden causar degradación en la percepción del video.

Problemas de transmisión

Esta situación se presenta cuando limitaciones en el ancho de banda, falta de estabilidad en la red, o fallas en los equipos ocasionan pérdida o corrupción el los paquetes de video, haciendo que los decodificadores de video no funcionen correctamente.

La pérdida de paquetes durante la transmisión del flujo de video origina bloques faltantes en la imagen decodificada en el receptor, este fenómeno en inglés se conoce como "*blockiness*". Si existe una gran cantidad de bloques faltantes la imagen se percibe como "congelada". En la siguiente ilustración, se observa una imagen con cierto porcentaje de bloques ausentes:

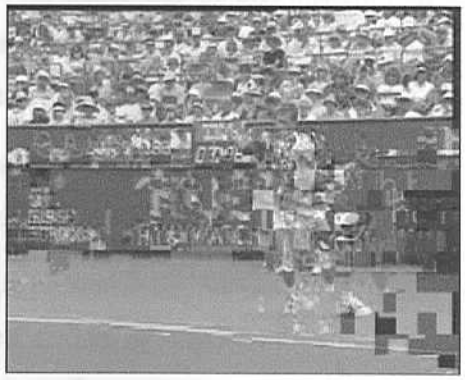


Ilustración B.1.- Imagen con bloques ausentes. Tomado de: IPTV Troubleshooter –Telchemy Incorporated.

Problemas debido al "suavizado" insuficiente del ancho de banda de video

Si los paquetes de video son enviados inmediatamente a medida que son recibidos, los picos de ancho de banda pueden originar sobrecarga en los *buffers* de los *routers*. Existen mecanismos de "suavizado" del ancho de banda para que la tasa de transmisión sea constante, ello puede originar un mayor nivel de *jitter* en los enlaces. Esta situación origina que una gran cantidad de tramas de video sean descartadas, haciendo que la calidad del video recibido se vea degradada.

Problemas debido al proceso de codificación

El proceso de codificación produce cierta distorsión, que puede variar considerablemente con la cantidad de movimiento que presenta la imagen. Algunos problemas son los siguientes:

- Distorsión de Bloques: puede ser ocasionado por una cuantificación inexacta de los componentes espaciales de la imagen durante el proceso de codificación, y ocurre debido a la estructura de bloques que caracteriza a una imagen MPEG.
- *Blurring*: se conoce como *blurring* a la reducción de la agudeza en las orillas de la imagen, puede ser observado de una manera más fácil en algoritmos de compresión de baja tasa de transmisión o pocas tramas, o en secuencias de video con mucho movimiento.
- Ruido de Cuantificación: típicamente se reconoce como "nieve" en la mayor parte de la imagen percibida.
- *Color Pixellation*: la presencia de bloques de píxeles de colores en la imagen se debe típicamente a errores que ocurren durante el proceso de conversión de una imagen digital de un formato a otro.

Ilustración B.2.- Ejemplo de una imagen pixelada debido a problemas de compresión. Fuente: IPTV Troubleshooter – Telchemy Incorporated.

APÉNDICE C.- Modelos de evaluación de calidad de video

Principios básicos de la transmisión de video

Según Telchemy Incorporated (2006), el video es transmitido como una serie de tramas o imágenes, generalmente a una tasa entre 25 y 60 *frames* por segundo. Algunos sistemas de video (como por ejemplo la TV tradicional), transmiten tramas que se relacionan unas con otras (*interlacing*), en donde la información enviada sólo indica las variaciones entre la imagen anterior y la siguiente (necesaria para modificar la imagen en el receptor). De esta forma se evita el envío de información redundante, lo que permite ahorrar considerablemente el ancho de banda.

A continuación, se muestra una tabla que contiene diferentes tipos de resolución de video junto con sus correspondientes características, necesarias para la correcta transmisión. Se puede apreciar como a mayor resolución y tasa de tramas se obtienen mayores tasas de bits transmitidos; por ejemplo una imagen de 1080p tiene aproximadamente diez veces más números de píxeles que los que tiene una imagen de 480i.

Tabla C.1.- Tramas e Imágenes. Tomado de *IP Video Basics*

Resolution	Type	Horizontal	Vertical	Frame/sec	Interlaced
480i	SDTV	720 pixels	480 pixels	25-30 fps	Yes
480p	EDTV	640-852 pixels	480 pixels	50-60 fps	No
720i	HDTV	1024 pixels	720 pixels	25-30 fps	Yes
720p	HDTV	1024 pixels	720 pixels	50-60 fps	No
1080i	HDTV	1920 pixels	1080 pixels	25-30 fps	Yes
1080p	HDTV	1920 pixels	1080 pixels	50-60 fps	No

Streams de Video IP

Cada trama es comprimida y dividida en pequeños fragmentos para ser posteriormente transmitida sobre las redes IP. Las tramas pueden ser comprimidas independientemente de otras tramas (tramas "I", las cuales corresponden a codificaciones *intra-frame*) o comprimidas basadas en las

diferencias con respecto a las tramas anteriores (tramas "P" o "B", las cuales corresponden a codificaciones *inter-frame*).

Un grupo típico de imágenes (GoP) consta de una trama "I" y un conjunto de tramas tipo "P" y potencialmente de tipo "B", tal como se muestra en la ilustración C.1. Por ejemplo, un GoP puede estar constituido por I, B ,B ,P ,B ,B ,B ,P enviadas a 30 *frames* por segundo. La trama "I" esta independientemente comprimida y de ella resultan un gran número de paquetes IP correspondientes a tramas tipo "P" o "B", las cuales sólo codifican los cambios que presenta la trama anterior.

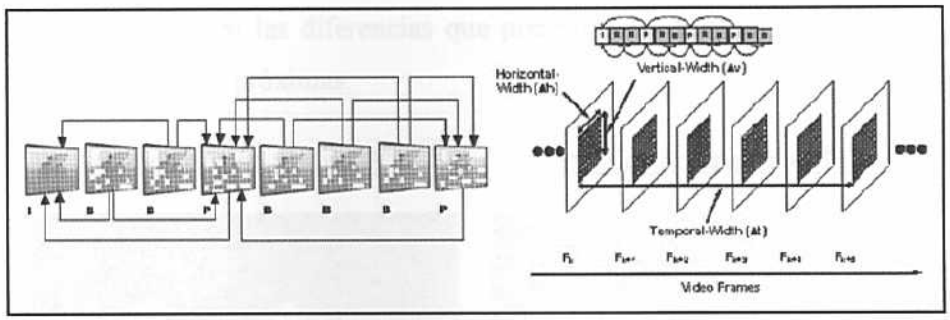


Ilustración C.1.- Tramas I-B-P comprimidas digitalmente
Tomado de MPQM versus *Media Delivery Index*

Cada trama comprimida es dividida en un número de unidades de transporte y cada unidad de transporte es primero encapsulada en un paquete de transporte (RTP, *Real Time Protocol*- o transporte MPEG-x), luego en un paquete UDP o TCP, y por último, en un paquete IP. De ahí, un paquete de video IP es enviado sobre la red IP, presentando la siguiente forma:

[Cabecera IP] [Cabecera UDP o TCP] [Cabecera RTP o transporte MPEG-x] [Carga útil de Video]

En algunos casos el transporte de MPEG-x es llevado por RTP. Los paquetes IP pueden presentar errores o perderse, lo que puede ocasionar la degradación de la calidad del video. Algunos sistemas de video utilizan *Forward Error Correction*, lo que agrega redundancia al paquete y permite que algunos de los paquetes perdidos puedan ser reemplazados en el receptor. Otro común

enfoque es utilizar una retransmisión basada en un protocolo que reemplace los paquetes perdidos, por ejemplo UDP, TCP o *multicast* con retransmisión *unicast*.

Codificación

Las tramas "I" son codificadas independientemente de cualquier trama anterior. Para este tipo de tramas, cada una es dividida en bloques, generalmente de un tamaño de 16 x 16 píxeles, los cuales serán transformados usando la transformada discreta Coseno (DCT). Los coeficientes de la DCT son cuantificados y luego comprimidos al máximo. Las tramas "P" están basadas en las diferencias que presentan las tramas previas tipo "I" o tipo "P". Las tramas "B" están basadas en las diferencias que presentan las tramas previas "I" o las tramas "P" previas o próximas.

Pérdida de una trama "B" Pérdida de una trama "I"

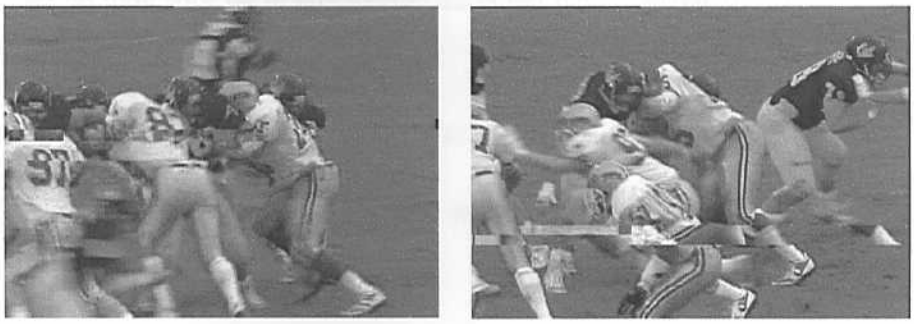


Ilustración C.2.- Impacto de una sóla pérdida de un paquete IP (Tramas "I" y "B")
Tomado de DSL Forum: Triple-Play services Quality of Experience Requirement

En la ilustración C.2, se muestra el impacto de las pérdidas de las diferentes tramas sobre la imagen. Los codificadores comunes de video usados en *video Broadcast* son MPEG-2, MPEG-4/H.264 y VC1 de Microsoft. En aplicaciones de video conferencia se utilizan H.261, H.263 y principalmente H.264.

***Media Delivery Index* (MDI)**

Las soluciones para proveer la transmisión confiable de tramas de datos, están diseñadas para controlar las ráfagas y los retardos de los paquetes a través de la red. Desafortunadamente, las métricas relacionadas a protocolos como RTP, sólo proporcionan valores promedios de *jitter* y *packet loss*, debido a que su alcance no incluye un estudio profundo de dónde y cómo los ocurren problemas.

Para satisfacer esta necesidad de mayor profundidad en las pruebas, *Cisco Systems* e *IneoQuest Technologies* han propuesto a la IETF (*Internet Engineering Task Force*) el conjunto de métricas MDI.

Según se encuentra definido en IETF (2006), el MDI esta formado por dos componentes: DF (*Delay Factor*) y MLR (*Media Loss Rate*). Estas mediciones pueden realizarse para cada trama de video, en cualquier punto de la red, y proveen un indicador de la efectividad de la red para manejar *streaming* a tiempo real.

El MDI es típicamente representado de la siguiente manera:

DF: MLR

Delay Factor (DF)

Para poder entender con facilidad el componente DF del MDI es útil señalar la relación entre el *jitter* y el encolado. El *Jitter* es un cambio con respecto al tiempo de latencia de los paquetes en la red, por ejemplo, los paquetes que se reciben a una tasa constante tiene un *jitter*= 0. La siguiente ilustración muestra la diferencia entre la presencia y la ausencia del *jitter,* en relación a la llegada de los paquetes recibidos. En la gráfica de la izquierda, se observa como a medida que pasa el tiempo, el crecimiento de los paquetes recibidos se comporta de forma lineal, a diferencia de la gráfica con presencia de *jitter*, la cual se comporta de forma irregular.

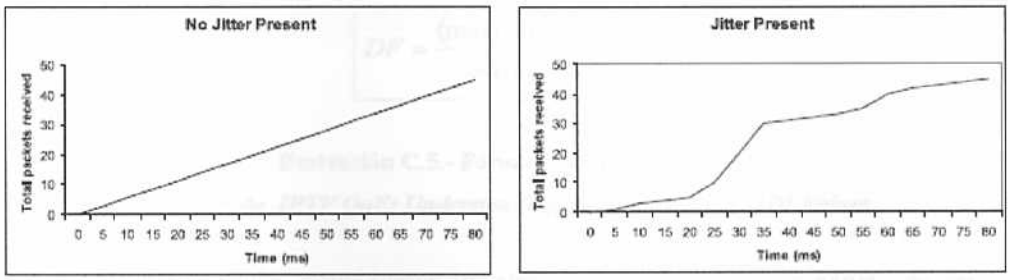


Ilustración C.3.- Presencia y ausencia de jitter
Tomado de *IPTV QoE: Understanding and Interpreting MDI Values*

Como se ha comentado anteriormente, mientras más severo es el *jitter* en el *stream* de video, mayor longitud deben presentar los *buffers* en los dispositivos de red para compensar esta situación y prevenir la pérdida de paquetes. Sin embargo, el costo de *buffers* más largos se ve reflejado en mayores tasas de retardo del *stream*. El DF cuantifica este retardo mediante la especificación del tamaño en los *buffers* (en milisegundos de datos, requerido para el envió de video a la tasa de transmisión deseada, ante la presencia de *jitter*; es procesado mientras los paquetes ingresan y es mostrado al usuario en intervalos regulares de tiempo. El DF es calculado de la siguiente manera:

- Para cada paquete de llegada, es calculada la diferencia entre los *bytes* recibidos y los retransmitidos. Este valor es la profundidad virtual del *buffer* (Δ) y se expresa como se muestra en la siguiente fórmula:

$$\Delta = |bytes\_received - bytes\_drained|$$

Ilustración C.4.- Fórmula de Profundidad del Buffer
Tomado de *IPTV QoE: Understanding and Interpreting MDI Values*

- En un intervalo de tiempo, se debe tomar la diferencia entre los valores máximos y mínimos de Δ y dividirla entre la tasa media de transmisión, como se muestra en la siguiente ilustración:

$$DF = \frac{(\max(\Delta) - \min(\Delta))}{media\_rate}$$

Ilustración C.5.- Fórmula del Delay Factor
Tomado de *IPTV QoE: Understanding and Interpreting MDI Values*

Como ejemplo, considérese un *stream* de video de 3.75 Mb/s. Si en el transcurso de un intervalo de un segundo, la máxima cantidad de datos en el buffer virtual es de 3.75 Mb y la mínima cantidad es de 3.74 Mb, el DF va a ser calculado de la siguiente manera:

$$DF = \frac{3.755Mb - 3.740Mb}{3.75Mb/s} = \frac{15kb}{3.75Mb/s} = 4ms$$

Ilustración C.6.- DF calculado bajo ciertas condiciones
Tomado de *IPTV QoE: Understanding and Interpreting MDI Values*

De esta manera, ese valor de DF igual a 4ms indica que el buffer de recepción del dispositivo en cuestión debe soportar 15Kb a fin de impedir la pérdida de paquetes originado por la presencia de *jitter*, el cual introduce un retardo de 4 ms.

El valor DF puede ser utilizado en el receptor de los *streams* de video, para avaluar la calidad de video desde la perspectiva del usuario, a fin de inferir la QoE. También, puede ser utilizado para determinar el impacto de cada elemento de la red a través del camino de envío de *streams*. Mediante la comparación del DF en la interfaz de ingreso y egreso del dispositivo, es posible determinar la "huella" del mismo, es decir, mientras mas pequeño sea el valor de dicha huella menor es el *jitter* que el dispositivo introduce en la red, y mejor es para el envío de video.

Delay Factor Aceptable

Un alto valor de DF indica directamente que una latencia creciente capaz de degradar la calidad de video ha sido inducida por un dispositivo o por el sistema. También alarma la posibilidad inminente de pérdida de paquetes, debido

al estado de *overflow* o *underflow* que los *buffers* de los dispositivos de red deben estar presentando.

El valor de DF que es aceptable para cada red en particular, varía ampliamente debido a la gran variedad de tamaños de *buffers* disponibles. La mayoría de los STBs (*Set Top Boxes*) utilizan sólo un modulo RAM, siendo sólo una parte de esta memoria utilizada como *buffer* para eliminar el *jitter* de los *streams* de video entrantes, esta es la razón por la cual la mayoría de las especificaciones de STB no especifican el tamaño del *buffer*.

Tabla C.1.- Valores aceptables de DF. Tomado de *IPTV QoE: Understanding and Interpreting MDI Values*

Maximum Acceptable DF
9-50 ms

Los estándares que están siendo desarrollados en el ADSL Forum, como parte de WT-126, para garantizar la QoE en los servicios Triple Play, recomiendan que el *jitter* introducido por la red debe permanecer debajo de los 50 ms, según se muestra en la tabla C.1, sin embargo, esto es mucho menos de lo que pueden soportar los STB en la mayoría de los receptores. Pruebas realizadas en los laboratorios de *Agilent Technologies* han determinado que el mínimo valor aceptable de DF para un STB en particular debe ser de 9 ms. Esta discrepancia entre los dos valores (50 ms y 9 ms) es atribuida a la gran variedad de calidad en los STB disponibles, así esta recomendación es útil para distintos tamaños de *buffer*. El número exacto aceptable para el máximo valor de DF, debe especificarse según el tamaño del buffer de los STB a utilizar, para lograr esto es necesario determinar el máximo valor de *jitter* que el STB puede soportar antes de afectar la calidad de la imagen, es decir, cero pérdidas de paquetes.

Media Loss Rate (MLR)

El término *Media Loss Rate* (MLR) es definido como el número de paquetes *media* perdidos o fuera de secuencia por segundo. Estos paquetes fuera de secuencia son importantes, debido a que muchos dispositivos no hacen el

intento de reordenar los paquetes antes de presentárselos al decodificador. Cualquier pérdida de paquetes, representado con un MLR diferente de cero, va a afectar de manera adversa a la calidad de video y puede introducir distorsiones visuales. El MLR es un formato conveniente para especificar el SLA (*Service Level Agreement*) en términos de tasas de pérdidas de paquetes. Así, tomando el contexto del componente explicado anteriormente, un dispositivo con un MDI de 4:0.001 va a indicar que este presenta un factor de retardo de 4 ms y una tasa de pérdidas de paquetes *media* de 0.001 por segundo.

Imagen sin ningún inconveniente $MLR = 0$	Imagen con perdidas de paquetes $MLR > 0$

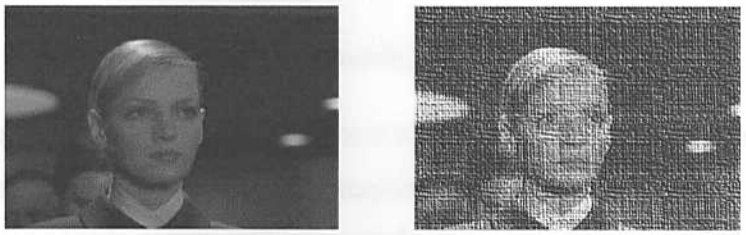


Ilustración C.7.- Impacto del MLR sobre la imágen
Tomado de *White Paper: Scalable IPTV Quality Testing*

La ilustración C.7, muestra el mismo cuadro de video enviado por dos proveedores de servicio distintos, ¿Cuál escogerá el usuario?, la respuesta a esta pregunta determinará el futuro de cada proveedor y sus suplidores de equipos. Esta es la razón por la cual los equipos deben probarse bajo condiciones reales, para determinar si pueden soportar en envío de video de calidad para sus suscriptores. La ilustración también permite observar que el MLR se puede utilizar como predictor de la calidad de video ofrecida.

Media Loss Rate (MLR) Aceptable

Debido a que MLR es un valor que representa una tasa, alguna información importante no es tomada en cuenta, como por ejemplo que los paquetes IP perdidos sean consecutivos o no. Un estudio realizado por el ADSL Forum, indica que casi cualquier pérdida de paquetes IP produce un error visible

en la imagen, así como que un usuario típico prefiere errores importantes poco frecuentes a errores sin importancia con una frecuencia considerable. Los estándares en QoE recomiendan una pérdida máxima de 5 paquetes IP consecutivos cada 30 minutos para un formato SDTV, y cada 4 horas para uno HDTV. Trasladando ésto a términos MLR (y asumiendo que 7 paquetes media es un paquete IP), se obtiene un valor de 0.019 paquetes media por segundo, como se puede observar a continuación:

$$\frac{5 \text{ IP Packets}}{30 \text{ minute}} \times \frac{1 \text{ minute}}{60 \text{ second}} \times \frac{7 \text{ Media Packets}}{1 \text{ IP Packet}} = \frac{0.019 \text{ Media Packets}}{\text{second}}$$

Ilustración C.1.- Cálculo de MLR bajo distintas unidades

Tomado de *IPTV QoE: Understanding and Interpreting MDI Values*

Esa tasa implica que un valor de 0.019 paquetes media por segundo puede ser interpretado también como aceptable para 5 eventos de pérdidas inconsecutivos (cada evento está relacionado con un solo paquete IP) por cada 30 minutos, lo cual no sería necesariamente el caso. Esta es la causa de porque el escenario de pérdidas considerado es para un único paquete IP o evento.

El máximo valor aceptable de MLR depende de su implementación. En el caso del *channel zapping*, un canal es generalmente visto por un periodo breve, por ende es de interés si cualquier pérdida de paquetes ocurre al cambiar de un canal a otro. En este caso, el máximo valor aceptable de MLR es 0, tal como se expresa en la tabla C.2, debido a que cualquier valor mayor implica la pérdida de uno o mas paquetes en un tiempo pequeño, mucho mayor de lo que es recomendado por los estándares en QoE.

Tabla C.2.- Channel Zapping MLR recomendado para todos los codecs. Tomado de *IPTV QoE: Understanding and Interpreting MDI Values*

Maximum Acceptable Channel Zapping MLR
0

La segunda implementación esta relacionada al monitoreo de red, donde el periodo de muestreo es generalmente largo. Esto significa que el número de paquetes perdidos está mejor expresado en términos de promedios por segundo en vez de un total, como esta ilustrado en la tabla C.3.

Tabla C.-3.- MLR promedio recomendado para distintos tipos de formatos. Tomado de *IPTV QoE: Understanding and Interpreting MDI Values*

Service (All Codecs)	MaxAcceptable Average MLR
SDTV	0.004
VOD	0.004
HDTV	0.0005

De esta manera, y tomando el contexto del componente explicado anteriormente, un dispositivo con un MDI de 40:0.003 va a indicar que este presenta un factor de retardo de 40 ms y una tasa de pérdidas de paquetes *media* de 0.003 por segundo.

La calidad de video que el usuario percibe bajo estos valores en los componentes no es satisfactoria, debido a que tanto el DF como el MLR están cercanos a los valores umbral presentados por los estándares internacionales de calidad (50 ms para DF y 0.004 para MLR). Esta situación puede ser evitada mediante la correcta implementación de los componentes MDI mostrados.

Moving Picture Quality Metrics (MPQM)

Moving Picture Quality Metrics (MPQM) ha sido propuesto como un modelo que permite la entrega de video manteniendo la calidad del servicio.

Según *Spirent Communications*[1] *(2006)*, es un sistema de medición objetivo que afirma reproducir la experiencia subjetiva del observador humano, por lo que se considera que está basado en un modelo de visión básico. La entrada de la métrica es una secuencia original de video y una versión distorsionada de ésta. La distorsión es calculada, en primer lugar, mediante la diferencia entre las secuencias originales y las distorsionadas. Luego, ambas son

descompuestas en canales de percepción, mediante etapas de transformación lineal. Este modelo consta de 17 filtros espaciales, 2 filtros temporales y un total de 34 componentes de percepción, por cada secuencia que debe ser computada. La siguiente etapa, modela patrones de sensibilidad, utilizando una función de estimación de contraste y una sumatoria lineal modelo de enmascaramiento. Deben ser computarizadas por cada píxel, de cada componente de percepción, de la secuencia de error.

Los valores umbrales de contraste, son entonces utilizados para dividir el componente de percepción de la secuencia de error (en una base píxel por píxel). Los datos son recogidos para producir una sola figura y para determinar niveles de percepción más altos, lo que se denomina asociación. Este paso es computarizado de la siguiente manera:

Primero, la asociación es calculada sobre bloques de secuencia, los cuales son tridimensionales (uno para considerar la información temporal y los otros dos para considerar la información espacial). La dimensión espacial es escogida para considerar el foco de atención, por ejemplo, el tamaño se calcula para cubrir dos grados de ángulo visual. Por otro lado, la medición de distorsión es calculada para cada bloque mediante la asociación del error en los canales, mediante la siguiente fórmula, donde E es la distorsión para un bloque dado:

$$E = \left(\frac{1}{N} \sum_{c=1}^{N} \left(\frac{1}{N_x N_y N_t} \sum_{t=1}^{N_t} \sum_{y=1}^{N_y} \sum_{x=1}^{N_x} |e(x,y,y,c)| \right)^{\beta} \right)^{\frac{1}{\beta}}$$

Ilustración C.2.- Fórmula del modelo computacional de E
Tomado de MPQM versus *Media Delivery Index*

Siendo $e(x, y, t, c)$, la señal de error enmascarada en la posición (x, y) y tiempo t, en el bloque en cuestión y en el canal c; N_x, N_y y N_t son las dimensiones verticales y horizontales de los bloques; N es el numero de canales; y β es una constante que presenta el valor 4. La medición final de calidad puede

ser expresada bien sea utilizando, como se muestra a continuación, el llamado PSNR enmascarado:

$$MPSNR = 10 \log \frac{255^2}{E^2}$$

Ilustración C.3.- PSNR enmascarado
Tomado de MPQM versus *Media Delivery Index*

También, puede ser mapeado en la escala de 5 valores de calidad, recomendada por la ITU, utilizando la ecuación:

$$Q = \frac{5}{1 + \gamma E}$$

Ilustración C.4.- Fórmula de escala de calidad
Tomado de MPQM versus *Media Delivery Index*

Donde γ, es una constante a ser obtenida experimentalmente. Esto puede lograrse, si la evaluación de calidad subjetiva Q es conocida para una secuencia dada.

Comparación entre MDI y MPQM

Las métricas MPQM han sido introducidas como un método de evaluación de la codificación de video y han sido analizadas en relación a las métricas PSNR (*Peak Signal-to-Noise Ratio*), ampliamente utilizadas de manera subjetiva en pruebas de laboratorio. En contraste, el MDI ha sido desarrollado como una herramienta evaluadora de la capacidad de la red, para la emisión de paquetes a tiempo real.

Cuando la salida de video es el resultado de una transmisión de red, existe una considerable probabilidad de pérdida de información, bien sea debido a congestión o retardo. Según *Spirent Communications (2006)*, la métrica MDI, por ser una herramienta basada en la red, no esta al tanto de la importancia de cada paquete para el envío de contenido de video, por lo que no puede ofrecer

descompuestas en canales de percepción, mediante etapas de transformación lineal. Este modelo consta de 17 filtros espaciales, 2 filtros temporales y un total de 34 componentes de percepción, por cada secuencia que debe ser computada. La siguiente etapa, modela patrones de sensibilidad, utilizando una función de estimación de contraste y una sumatoria lineal modelo de enmascaramiento. Deben ser computarizadas por cada píxel, de cada componente de percepción, de la secuencia de error.

Los valores umbrales de contraste, son entonces utilizados para dividir el componente de percepción de la secuencia de error (en una base píxel por píxel). Los datos son recogidos para producir una sola figura y para determinar niveles de percepción más altos, lo que se denomina asociación. Este paso es computarizado de la siguiente manera:

Primero, la asociación es calculada sobre bloques de secuencia, los cuales son tridimensionales (uno para considerar la información temporal y los otros dos para considerar la información espacial). La dimensión espacial es escogida para considerar el foco de atención, por ejemplo, el tamaño se calcula para cubrir dos grados de ángulo visual. Por otro lado, la medición de distorsión es calculada para cada bloque mediante la asociación del error en los canales, mediante la siguiente fórmula, donde E es la distorsión para un bloque dado:

$$E = \left(\frac{1}{N} \sum_{c=1}^{N} \left(\frac{1}{N_x N_y N_t} \sum_{t=1}^{N_t} \sum_{y=1}^{N_y} \sum_{x=1}^{N_x} |e(x,y,y,c)| \right)^{\beta} \right)^{\frac{1}{\beta}}$$

Ilustración C.2.- Fórmula del modelo computacional de E
Tomado de MPQM versus *Media Delivery Index*

Siendo $e(x, y, t, c)$, la señal de error enmascarada en la posición (x, y) y tiempo t, en el bloque en cuestión y en el canal c; N_x, N_y y N_t son las dimensiones verticales y horizontales de los bloques; N es el numero de canales; y β es una constante que presenta el valor 4. La medición final de calidad puede

indicación de la calidad de compresión de un *stream* de video. Si el proceso de envió, ha sido mejorado con un transporte robusto (por ejemplo, estrategias de corrección de errores – FEC), el MDI reportará una calidad de video no mejorada, mientras que MPQM reportará la calidad de la manera adecuada.

Sin embargo, aunque MPQM ha sido diseñado básicamente para evaluar la calidad de video que puede ser afectada por distorsiones en codificación, no es capaz de evaluar la calidad ante la modificación de la variable más básica de codificación, la tasa de bits. Por otro lado, la complejidad de procesamiento que implica y los requerimientos de acceso tanto a las señales originadas como a las procesadas, trae como consecuencia que este modelo no sea aplicable a aplicaciones de tiempo real, tal como es el caso de servicios como IPTV o VoIP, debido a que limita su uso en la evaluación multimedia de tiempo real en Internet.

Las métricas MDI se presentan de esta forma, como un modelo de evaluación de video eficiente, para detectar y distinguir el envío normal de video de problemas relacionados con la transmisión en la red, para servicios en tiempo real como IPTV, en relación con el envió de video seriamente degradado.

APÉNDICE D.- Parámetros de medición de estándares internacionales

En el presente apéndice se reseñan los parámetros de evaluación de calidad de servicio recomendados por distintas organizaciones internacionales. En primer lugar, se reseñan los parámetros de evaluación de funcionamiento de las redes basadas en el protocolo IP, según la recomendación de la ITU-T Y-1540 (2006) y ITU- T M.2301 (2006), seguido por los parámetros adicionales recomendados por el Foro ADSL en relación a servicios *triple play*, específicamente de video. Por último, se reseñan parámetros desarrollados internamente por centros tecnológicos y universidades del área.

Recomendación ITU-T - Y.1540

Esta recomendación define parámetros que se pueden utilizar para especificar y evaluar la calidad de funcionamiento en cuanto a velocidad, exactitud, seguridad de funcionamiento y disponibilidad de la transferencia de paquetes IP del servicio de comunicación de datos con protocolo Internet (IP, *Internet protocol*).

Los parámetros de calidad de funcionamiento de la transferencia de **Paquetes IP,** que define la ITU-T Y.1540 (2006) son los siguientes:

- **Retardo de transferencia de paquetes IP (IPTD, siglas en inglés de *IP packet transfer delay*):** Este parámetro se define para todos los paquetes, satisfactorios y con errores, a través de una sección básica. El IPTD es el tiempo (t2 – t1) que transcurre entre la ocurrencia de dos eventos de paquetes IP correspondientes, evento de ingreso en el momento t1 y evento de egreso en el momento t2, siendo (t2 > t1) y (t2 – t1) ≤ Tmáx.

  Según Paucar (2003), una de las formas de calcular este parámetro es mediante mediciones de los retardos experimentados por los mensajes de prueba del tipo *ping* que utiliza el protocolo ICMP, enviados a intervalos de 5 minutos. El número de mensajes ICMP enviados a través del comando *ping*

es de cuatro (4) con un tamaño de 32 bytes, del cual se obtiene el tiempo promedio de ida y vuelta que equivale al retardo durante su recorrido. La ecuación que define el retardo promedio es la siguiente:

$$RetardoMedia = \frac{\sum_{i=1}^{n} Retardo\_muestreado}{n}$$

Ilustración D.1.- Fórmula para el retardo promedio

donde n es el número total de muestras realizadas.

- **Retardo medio de transferencia de paquetes de protocolo Internet:** El retardo medio de la transferencia de paquetes IP es la media aritmética de los retardos de la transferencia de paquetes IP de una población de interés.

- **Variación del retardo de la transferencia de paquetes IP (IPDV, siglas en inglés de *IP packet delay variation*):** La variación del retardo de paquetes entre dos puntos (vk) para un paquete IP k entre el origen y el destino es la diferencia entre el retardo de transferencia de paquetes IP absoluto (xk) del paquete y un retardo de transferencia de paquetes IP de referencia definido, d1,2, entre esos mismos puntos de medición.

$$vk = xk - d1,2$$

Ilustración D.2.- Fórmula para la variación del retardo

- **Tasa de errores en los paquetes IP (IPER, siglas en inglés *IP packet error ratio*)**: La tasa de errores en los paquetes IP es la relación entre el total de paquetes IP con errores y el total de paquetes IP de transferencia satisfactoria, más los paquetes IP no reconocidos, en una población de interés.

$$IPER = \frac{Paquetes\ IP\ con\ errores + Paquetes\ IP\ no\ reconocidos}{Paquetes\ IP\ Entrantes\ Totales}$$

Ilustración D.3.- Fórmula para la tasa de errores en los paquetes IP

- **Tasa de pérdida de paquetes IP (IPLR, *IP packet loss ratio*)**: La tasa de pérdida de paquetes IP es la relación entre el total de paquetes IP perdidos y la cantidad de paquetes IP enviados para transmisión, en una población de interés. En otras palabras, es la relación de los paquetes recibidos y entregados a la capa superior y la cantidad de paquetes enviados para transmisión. Los paquetes perdidos pueden concebirse como la sumatoria de los paquetes descartados, con errores y espurios.

$$IPLR = \frac{Total\ de\ paquetes\ IP\ perdidos}{Total\ de\ paquetes\ IP\ enviados\ para\ transmisión}$$

Ilustración D.4.- Fórmula para la tase de pérdida de paquetes

- **Tasa de paquetes de protocolo Internet espurios**: La tasa de paquetes IP espurios (paquetes de naturaleza desconocida) en un punto de medición de egreso, es el número total de paquetes IP espurios observados en ese punto durante un intervalo de tiempo especificado dividido por la duración del intervalo de tiempo.

$$P.E = \frac{Total\ de\ paquetes\ IP\ espurios}{Duración\ de\ intervalo\ de\ tiempo}$$

Ilustración D.5.- Fórmula para la tasa de paquetes IP espurios

Recomendación ITU-T M.2301

Esta recomendación define los objetivos de rendimiento y procedimientos para establecer y mantener redes basadas en el protocolo Internet. Dentro del contexto de los procedimientos reseñados, se incluye un parámetro referente a los paquetes IP descartados:

- **Tasa de paquetes IP descartados (IPDR)**: La tasa de descarte de paquetes IP es la relación del total de paquetes IP descartados y total de paquetes IP transmitidos de una población de interés. Los paquetes descartados son los perdidos en forma deliberada, aunque no tengan error. En general, los paquetes se descartan porque no hay espacio suficiente en la memoria para

almacenar los paquetes que esperan su procesamiento. **Entonces, la tasa de descarte de paquetes IP es una medida de la congestión de la red.** Este parámetro no es reseñado explícitamente en la recomendación Y.1540, aunque en la recomendación M.2301 se especifica su metodología de obtención vía SNMP.

$$IPDR = \frac{Paquetes\ IP\ Descartados}{Paquetes\ IP\ Transmitidos}$$

Ilustración D.6.- Fórmula para la tasa de paquetes IP descartados

Reporte Técnico 126 – ADSL Forum

El reporte técnico 126 del ADSL Forum presenta las directrices mínimas recomendadas para garantizar la QoE del usuario final, en términos de mediciones objetivas para aplicaciones *tiple play* ofrecidas a través de una infraestructura de banda ancha.

- **Paquetes IP perdidos en un evento de pérdida (Loss period):** Permite medir la duración de un evento de pérdida, y cuantos paquetes se han perdido en ese intervalo.
- **Número máximo de eventos de errores por hora (Loss Distance):** Permite medir el espacio en tiempo entre eventos de errores o pérdida de paquetes.

Otros Parámetros

Los siguientes parámetros son recomendados por distintas investigaciones desarrolladas de manera interna en universidades y centros tecnológicos:

- **Porcentaje de utilización:** Permite medir la congestión de un enlace determinado, mediante la relación de la tasa de paquetes transmitidos en dicho enlace y el ancho de banda disponible en el mismo. La siguiente ecuación representa el porcentaje de utilización:

$$\% \, utilización = \frac{\frac{\text{Paquetes Tx}_n - \text{Paquetes Tx}_{n-1}}{\Delta t}}{\text{Ancho de Banda del canal}} x100$$

Ilustración D.7.- Fórmula para el porcentaje de utilización

- **Porcentaje de pérdida de paquetes:** Este parámetro define los paquetes o datagramas de información descartados, paquetes con errores o paquetes de protocolos desconocidos que son eliminados por los dispositivos de red. A diferencia del parámetro Tasa de pérdida de paquetes, recomendado por la UIT, los valores obtenidos son representados en forma de porcentaje. La fórmula que representa este parámetro es la siguiente:

$$\%pérdidas = \frac{Paquetes\ Perdidos_n - Paquetes\ Perdidos_{n-1}}{Paquetes\ Procesados_n - Paquetes\ Procesados_{n-1}} x100$$

Ilustración D.8.- Fórmula para el porcentaje de pérdida de paquetes

- **Disponibilidad:** La disponibilidad de la red se entiende como la situación en la cual se pueden recibir/enviar paquetes de datos desde/hacia Internet. También se define como el estado de operación activo del enlace. Para el cálculo de este parámetro se debe detectar si el enlace de interconexión al proveedor de servicios está en estado operativo. Para ello, se utilizan las variables MIBs de calidad de servicio, a través del protocolo SNMP.

Relación entre los parámetros de QoS básicos

Con la finalidad de analizar y comprender cómo los parámetros en conjunto afectan el servicio de IPTV, para un monitoreo preventivo y eficaz, fue necesario definir la interrelación entre los parámetros de QoS básicos en la transmisión de servicios en tiempo real.

En investigaciones realizadas a documentos publicados por el *ADSL Forum*, se concretó que los valores razonables de *jitter* y retardo de extremo a extremo, no son problemáticos en la calidad de la imagen percibida, debido a la existencia de un *buffer*, denominado en inglés como *de-jitter buffer* a nivel del

STB, cuyo tamaño es establecido para mantener el flujo correcto (*drain*) de los paquetes de video en los terminales del suscriptor. Sin embargo, si el retardo o el *jitter* producido por la red es mayor al que soporta el *de-jitter buffer*, los errores en la imagen comenzarían a apreciarse, a raíz de la situación de descarte de paquetes que se originaría, por lo que sigue siendo necesario su monitoreo y control.

Este conjunto de ideas reflejan la relación de los parámetros QoS que debe ser tomada en cuenta durante el monitoreo del tráfico de video, y confirman la importancia del efecto del descarte de paquetes en la recepción de una imagen de calidad, debido a que la dinámica de transmisión de video se basa en la *prevención de pérdida y descartes de paquetes* a nivel de equipos de red, originado por la presencia de *jitter*, y que a su vez puede ocasionar retardos de transmisión.

APÉNDICE E.- Medición de Tráfico de Red

Adams (2006), reseña que la garantía de la calidad de los nuevos servicios *triple play* se basa en los siguientes requerimientos:

- Los proveedores de servicio deben monitorear toda su red.
- Las empresas manufactureras de equipos terminales deben agregar funcionalidades de monitoreo a sus productos.
- Los dispositivos de acceso, así como los *gateways*, deben proveer a los administradores de red capacidades de reporte y monitoreo.

Williamson (2001), permite complementar el primer requerimiento al afirmar que las mediciones de tráfico a nivel de red proveen un mecanismo para conocer y entender cuáles dispositivos están funcionando correctamente y cuáles no. Mediante el uso de hardware o software especializado, el administrador de red puede colectar información detallada acerca de la transmisión de los paquetes y situaciones de congestión en los enlaces de transmisión. Existen 4 razones principales por las cuales la medición de tráfico de red es una técnica de utilidad:

- **Resolución de problemas de red:** Las redes no son infalibles. Constantemente, un equipo o pieza que no esté funcionando correctamente puede interrumpir la operación de toda la red, o al menos, degradar significativamente su calidad de servicio. Estos problemas están dados, entre otros factores, por ataques de seguridad, direcciones incorrectas, tamaños de paquetes ilegales, tormentas de *broadcast*. En dichos escenarios, mediciones detalladas en la red pueden proveer al administrador la información requerida para localizar y solventar los problemas.
- **Depuramiento de protocolos (*Protocol Debugging*):** Desarrolladores generalmente desean probar el funcionamiento de una nueva o mejorada versión de aplicaciones o protocolos. Las mediciones en el tráfico de red proveen la vía para asegurarse del funcionamiento correcto de dichos protocolos o aplicaciones.

- **Caracterización de carga:** Mediciones de tráfico de red pueden ser utilizadas como entrada de un proceso de caracterización de carga de trabajo (*workload*), el cual analiza muestras estadísticas para obtener propiedades representativas que puedan describir una aplicación o protocolo de red. El conocimiento de estas características pueden guiar el diseño de nuevos protocolos y redes para el soporte de las aplicaciones.

- **Evaluación de funcionamiento:** Finalmente, las mediciones de tráfico de red pueden ser utilizadas para determinar el correcto funcionamiento de un protocolo o servicio de red dado, como por ejemplo IPTV. Un análisis detallado de las mediciones de tráfico de red permite identificar los puntos de congestión.

Como se ha reseñado en secciones anteriores, existen distintos valores de interés a la hora de evaluar la calidad de funcionamiento de la red: retardo de paquetes, ancho de banda, pérdidas de paquetes, etc. También tiene importancia en qué punto o puntos de la red se mide. Para un determinado tráfico, se puede medir el retardo que se produce extremo a extremo entre origen y destino, o el retardo en uno de los trayectos por los que atraviesa el tráfico. Se pueden efectuar mediciones en cada enlace de la red o en enlaces específicos, dichos enlaces, seleccionados para una medición particular, se denominan "población de interés".

La siguiente ilustración, permite concretar todas las etapas que forman parte del proceso de monitoreo de tráfico, como se puede observar, uno de los propósitos del proceso de medición de trafico es integrar la información recolectada al monitoreo preventivo y reactivo de los parámetros de funcionamiento de red relacionados a los distintos servicios que los proveedores ofrecen a sus clientes, garantizando así el correcto funcionamiento de sus sistemas.

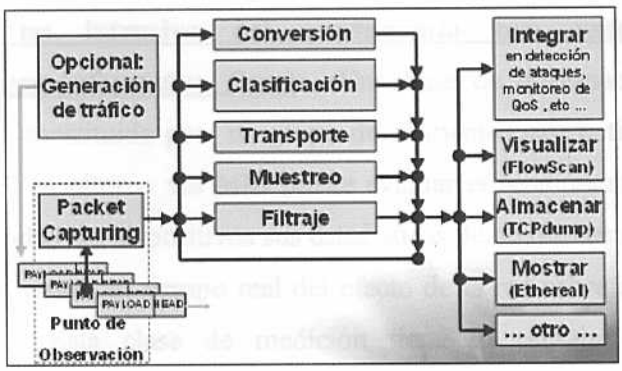


Ilustración E.1.- El proceso de medición de tráfico.

Tomado de *IP traffic measurement technologies, tools, and protocols*

Métodos de Medición de Tráfico de Red

Según la Unión Internacional de Telecomunicaciones en su recomendación M.2301 (2006), los dos métodos básicos para medir el rendimiento de las redes se definen como métodos "intrusivo" y "no intrusivo", que corresponden a los términos "activo" y "pasivo" utilizados por el IETF.

- **Medición intrusiva del rendimiento (con paquetes de prueba):** Las mediciones intrusivas del rendimiento consisten en insertar paquetes de prueba intercalados con los flujos de tráfico normal entre dos puntos. Esta clase de medición permite un estudio más detallado de ciertos parámetros de rendimiento específicos, por ejemplo el retardo en un sentido mediante paquetes con sellos de tiempo, y el efecto del tamaño y de la cantidad de paquetes en el rendimiento.

  Las técnicas de medición intrusiva se utilizan cuando es difícil o imposible utilizar la medición no intrusiva, como por ejemplo la medición del retardo de transferencia de paquetes en un sentido y de la variación del retardo de paquetes. Cabe señalar que la medición intrusiva del rendimiento crea tráfico adicional en la red, por lo que hay que ser cuidadosos para que esta prueba no cause congestión y la pérdida consiguiente de paquetes de cliente.

- **Medición no intrusiva del rendimiento con supervisión MIB (*Management Information Base*):** Una base de información de gestión (MIB), está constituida por un grupo de elementos que entiende un agente SNMP. El monitoreo vía MIB puede evaluar el rendimiento de la red al solicitar a todos los dispositivos sus estadísticas de rendimiento, con lo que se obtiene una visión en tiempo real del efecto de la red sobre el tráfico que la atraviesa. Esta clase de medición tiene la ventaja de reducir las repercusiones en el tráfico del cliente y prueba cada ruta a través de la red. Además, permite identificar rápidamente los problemas en los enlaces o en los dispositivos.

Algunos parámetros de rendimiento se pueden medir solamente de forma intrusiva, mientras que otros, sólo de forma no intrusiva, y algunos se pueden medir de ambas maneras como se ilustra en la siguiente tabla:

Tabla E.1.- Medición Intrusiva y no intrusiva de los parámetros de rendimiento
Tomado de Recomendación Y.1540, Unión Internacional de Telecomunicaciones

Parámetro	Intrusiva	No Intrusiva
IPTD	√	
IPDV	√	
IPER	√	√
IPLR	√	√
IPDR		√

APÉNDICE F.- Aspectos relacionados al monitoreo de las colas de diferenciación de servicio en los dispositivos Alcatel

A continuación, se reseña la información referente al acceso vía MIB a las colas de los *switches* Metro, obtenida en reuniones con proveedores de equipos Alcatel:

Distribución de Colas

La distribución de colas en los *switches* Alcatel, de una forma general, esta diseñada de la siguiente manera:

Tabla F.1.- Tipos de colas de prioridad "1" definidas en la red de CANTV

Cola	Especificación
Real Time	Relacionada a tráfico con requerimientos de tiempo real.
Critical	Relacionada a tráfico interno de gestión.
Bussiness	Relacionada a tráfico proveniente de clientes específicos de la empresa. Ej: bancos, instituciones publicas.
Best Effort	Relacionada a tráfico con pocos requerimientos de transmisión.

De la misma forma, el marcado del tráfico puede establecerse según el tipo de direccionamiento del tráfico circulante:

Tabla F. 2.- Tipos de cola de prioridad "2" definidas en la red ME de CANTV

Colas	Especificación
Multicast	Relacionada al tráfico de aplicaciones cuya naturaleza requiere direccionamiento *multicast*, por ejemplo: *broadcast* TV (IPTV)
Unicast	Relacionada al tráfico proveniente de aplicaciones cuya naturaleza requiere de direccionamiento *unicast*, por ejemplo: Video en Demanda. (IPTV)

La aplicación de una cola u otra dentro del diseño de diferenciación de tráfico de la red, depende considerablemente de las políticas de calidad establecidas para cada tipo de servicio. Para el caso de IPTV, y según conversaciones con representantes de la gerencia de planificación de la empresa, se ha establecido el uso del enfoque de diferenciación de tráfico según el tipo de direccionamiento del flujo de video, de esta forma, se concretó que son dos colas las que van a ser incluidas dentro del MGC, la cola *unicast* y la *multicast*.

IPTV, está constituido por distintos tipos de aplicaciones, de éstas, las de mayor despliegue son la televisión digital por suscripción (BTV), y video en demanda (VoD). Ambas aplicaciones presentan distintos tipos de requerimientos que dependen de su naturaleza.

En reuniones con el director de los laboratorio de prueba de la empresa, Ing. Miguel Zambrano, se obtuvo información referente a los requerimientos de transmisión que diferencian a ambas aplicaciones: la televisión digital por suscripción, busca emular el tipo de transmisión *broadcast* de las redes de televisión terrestre, debido a esto, utilizan un tipo de direccionamiento *multicast*, donde todos los canales ofrecidos están fluyendo en la red y están siendo direccionados a los terminales que pertenezcan a un grupo de suscripción determinado. En las fases de diseño del servicio, el ancho de banda requerido para el funcionamiento de BTV es asegurado, convirtiéndolo en una constante de tráfico.

Por su parte, el video bajo demanda requiere de un flujo *unicast* por cada usuario que esté disfrutando del mismo, independientemente del tipo de información que se esté transmitiendo, esto quiere decir, que dos usuarios pueden estar disfrutando la misma película al mismo tiempo, pero los datos al STB van a ser transmitidos por dos flujos de video independientes, consumiendo un ancho de banda determinado por cada uno de ellos. Por esta razón, a diferencia del servicio BTV, el comportamiento del tráfico no es constante, y aunque existen mecanismos de control de ancho de banda, como VAD (*Video Admission Control*), que permiten establecer un número máximo de clientes VoD en un

tiempo determinado, la naturaleza del servicio es propensa a originar mayores situaciones de congestión y de porcentaje de utilización en las colas de prioridad que la televisión digital por suscripción.

En base a las razones expuestas, las operaciones reseñadas como parte del MGC propuesto estuvieron enfocadas en primer lugar a la evaluación del funcionamiento de la cola de prioridad que soporta las aplicaciones *unicast*, al ser aquella la encargada de procesar el flujo del servicio VoD, y en segundo plano a la cola de prioridad que soporta las aplicaciones *multicast*, al ser aquella la encargada de procesar el flujo de servicios de televisión digital por difusión.

Perfiles de Tráfico

Como parte del diseño de las políticas de QoS en los dispositivos Alcatel, es posible delimitar distintos perfiles de tráfico. Este diseño previo, orientará los mecanismos de medición a nivel de las colas, debido a que las mediciones pertinentes van a verse diferenciadas en relación a los paquetes que están dentro o fuera del perfil. Los paquetes dentro del perfil, conocidos también como *In Profile,* son aquellos que satisfacen el CIR (*Commited Informatio Rate*). Por su parte, los paquetes fuera del perfil, conocidos también como *Out Profile*, son aquellos que exceden el CIR, y pertenecientes al grupo EIR (*Excesses Information Rate*), que pueden ser transmitidos dada una condición de congestión que lo permita, estos paquetes son marcados de una manera específica permitiendo indicar al dispositivo que en caso de una situación de congestión, los paquetes *Out Profile* deben ser descartados primero.

El diseño de aprovisionamiento de ancho de banda para las aplicaciones de IPTV está orientado a garantizar que todo el tráfico del servicio que fluya a través de la red esté *dentro* del perfil, debido a que no se asegura un ancho de banda estático para el funcionamiento del servicio, si no más bien se utiliza la tendencia de disminuir el rendimiento de los servicios de menor prioridad cuando hay una situación de demanda excesiva de las aplicaciones del servicio, garantizando de esta forma su correcto funcionamiento, esto aplica mayormente a

VoD, debido a que el flujo de tráfico para BTV es una constante, al ser de tipo *multicast*. Es por esta razón que el monitoreo y análisis de los parámetros que requieren contadores en las colas de los *switches* va a estar orientado a los paquetes que estén *dentro* del perfil, de todas maneras, se propone el monitoreo en la OID de los paquetes fuera de perfil, ya una actividad en esos contadores puede indicar alguna falla en la política de aprovisionamiento de tráfico de video, que pueden originar problemas innecesarios en la percepción de la imagen, al momento de una mínima situación de congestión.

Atributos de OID de las colas

Según Cisco Systems (2004), todos los objetos administrados en el entorno SNMP se encuentran dispuestos en una estructura jerárquica también conocida como de árbol. Los identificadores de los objetos, ubicados en la parte superior del árbol, pertenecen a diferentes organizaciones estándares, mientras los identificadores de los objetos, ubicados en la parte inferior del árbol, son colocados por los proveedores. El objeto administrado es identificado por el descriptor de objeto equivalente (OID), y constituye la forma de identificar a una variable dentro de la MIB, permitiendo obtener la trayectoria que hay que seguir hasta alcanzar dicha variable.

Es importante mencionar, que por requisitos de confidencialidad, la trayectoria concreta que permite alcanzar las variables de las colas dentro de las MIBs de los *switches* no pueden ser reseñadas en el presente trabajo. Para brindar una idea de la constitución y los atributos de la OID que permiten lograr la gestión de las colas, se presenta el siguiente ejemplo:

In .1.3.6.1.4.1.6527.3.1.2.4.3.7.1.12.XXX.38043648.0.1

Out .1.3.6.1.4.1.6527.3.1.2.4.3.8.1.6.XXX.38043648.0.1

Existen dos tipos de contadores en las colas, uno (In) que permite obtener información acerca del tráfico y paquetes descartados a la entrada de la misma durante el intervalo de muestreo, y uno (out) que permite obtener información

acerca del tráfico y los paquetes descartados a la salida de la cola durante el intervalo de muestreo. Es importante mencionar, que como parte de los atributos requeridos para obtener las variables en la gestión de colas, es necesario indicar los parámetros como el SAP (*Service Access Port*), *Service ID*, y número de cola a acceder, en la tabla F.3 se reseña una descripción de cada uno de estos parámetros.

Por otro lado, también fue otorgada información relacionada al tipo de variables que pueden ser obtenidas mediante el acceso vía MIB a las colas de prioridad: a través de las rutas OID pertinentes, se pueden obtener valores de contadores de paquetes descartados y procesados, así como de un tipo de variable, conocida como *gauge*, que permite obtener un valor análogo a un porcentaje, en relación a una situación determinada (descarte de paquetes, porcentaje de utilización de la cola) que crece o decrece hasta un valor máximo. Esta información fue de gran importancia al momento de establecer los mecanismos de obtención de los distintos parámetros QoS seleccionados.

Tabla F.3.- Atributos necesarios para el acceso de las colas vía MIB.

Atributo OID	Descripción
SAP	ID del puerto físico (pueden pasar varios servicios por él). Este atributo está reseñado en la OID ejemplo con el número 38043648, correspondiente al SAP 2/2/9.
Service ID	Es el ID del servicio, por un SAP pueden pasar varios Service ID, por ejemplo: Servicios EPIPE, o VPLS. Este atributo está reseñado en la OID ejemplo como XXX. IPTV es un servicio VPLS.
Número de Cola	Indica el número de cola a la cual se quiere acceder dentro de un servicio determinado. Este atributo está reseñado en la OID ejemplo como 1.

APÉNDICE G.- Descripción técnica de los mecanismos de obtención de los parámetros QoS incluidos en el MGC

Retardo y Jitter – Módulo de Pruebas OAM

El módulo de pruebas OAM soporta dos tipos de funciones:

- La función SDP Ping, provee verificación de conectividad entre dos dispositivos de red.
- La función CPE Ping, provee verificación de conectividad entre un dispositivo de red y un CPE (*Customer Premises Equipment*).

La siguiente ilustración permite ilustrar la diferencia entre las dos funciones que presenta este módulo de pruebas:

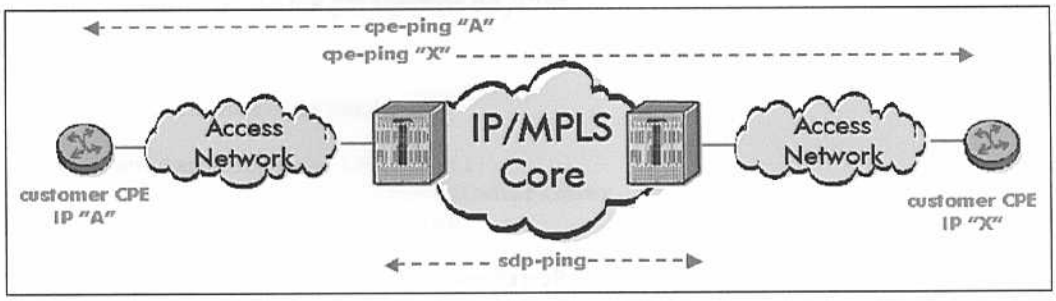


Ilustración G.1.- Tipos de pruebas OAM. Tomado de: proveedores ALCATEL.

El módulo de pruebas OAM, es gestionado vía SNMP mediante la siguiente rama MIB:

iso.org.dod.internet.private.enterprises.timetra.timetraProducts.tmnxSRMIB .tmnxSRObjs.tmnxOamTestObjs

A partir de esta rama MIB es posible obtener las siguientes tablas:

Tabla G.1.- Tablas obtenidas por el módulo OAM.

Tabla de la rama MIB	Características
tmnxOamPingCtlTable	Define la tabla de control del módulo OAM, para poder proveer, vía SNMP, la capacidad de ejecutar pruebas de conectividad.
tmnxOamPingResultsTable	Define la tabla de resultados de las pruebas realizadas, de la misma forma, esa información es almacenada por la tabla tmnxOamPingHistoryTable.
tmnxOamCpePingCtlTable	Define la tabla de control para proveer la capacidad de realizar pruebas de conectividad con la función CPE Ping.

A continuación, se presenta una demostración de una tabla de resultados, proveniente de una prueba realizada por los proveedores. El fin de esta demostración es indicar los campos de dicha tabla que deben ser utilizados para el cálculo y medición de los parámetros de *jitter* y retardo:

```
+--tmnxOamPingResultsTable(4)
   |
   +--tmnxOamPingResultsEntry(1)
      |  Index: tmnxOamPingCtlOwnerIndex, tmnxOamPingCtlTestIndex,
tmnxOamPingResultsTestRunIndex
      |
      +-- -R-- EnumVal   tmnxOamPingResultsOperStatus(1)
      |        Values: enabled(1), disabled(2)
      +-- -R-- Unsigned  tmnxOamPingResultsMinRtt(4)
      +-- -R-- Unsigned  tmnxOamPingResultsMaxRtt(5)
      +-- -R-- Unsigned  tmnxOamPingResultsAverageRtt(6)
      +-- -R-- Unsigned  tmnxOamPingResultsRttSumOfSquares(7)
      +-- -R-- Unsigned  tmnxOamPingResultsMtuResponseSize(8)
      +-- -R-- EnumVal   tmnxOamPingResultsSvcPing(9)
      |        Values: undetermined(0), failed(1), success(2)
      +-- -R-- Unsigned  tmnxOamPingResultsProbeResponses(10)
      +-- -R-- Unsigned  tmnxOamPingResultsSentProbes(11)
      +-- -R-- String    tmnxOamPingResultsLastGoodProbe(12)
      |        Textual Convention: DateAndTime
      |        Size: 8 | 11
      +-- -R-- String    tmnxOamPingResultsLastRespHeader(13)
      |        Size: 100
      +-- -R-- Integer32 tmnxOamPingResultsMinTt(14)
      +-- -R-- Integer32 tmnxOamPingResultsMaxTt(15)
      +-- -R-- Integer32 tmnxOamPingResultsAverageTt(16)
      +-- -R-- Integer32 tmnxOamPingResultsTtSumOfSquares(17)
      +-- -R-- Integer32 tmnxOamPingResultsMinInTt(18)
      +-- -R-- Integer32 tmnxOamPingResultsMaxInTt(19)
      +-- -R-- Integer32 tmnxOamPingResultsAverageInTt(20)
```

```
+-- -R-- Integer32 tmnxOamPingResultsInTtSumOfSqrs(21)
+-- -R-- Integer32 tmnxOamPingResultsOutJitter(22)
+-- -R-- Integer32 tmnxOamPingResultsInJitter(23)
+-- -R-- Integer32 tmnxOamPingResultsRtJitter(24)
+-- -R-- Unsigned  tmnxOamPingResultsProbeTimeouts(25)
+-- -R-- Unsigned  tmnxOamPingResultsProbeFailures(26)
+-- ---- Unsigned  tmnxOamPingResultsTestRunIndex(27)
         Range: 1..2147483647
```

Mediante la implementación de las siguientes fórmulas, y a partir de los campos señalados en la tabla de resultados, se pudo establecer un mecanismo de medición de los parámetros de retardo y *jitter*:

$$\text{Re}\,tardo\,(OneWay) = \frac{AverageRTT}{2}$$

Ilustración G.2.- Fórmula para el cálculo del retardo

$$Jitter(OneWay) = \frac{\sqrt{\frac{(RttSumOfSq\,uares - AverageRtt)^2}{\text{Pr}\,obe\,\text{Re}\,sponses}}}{2}$$

Ilustración G.3.- Fórmula para el cálculo del Jitter.

Porcentaje de Utilización de las colas

El cálculo basado en el uso de contadores obtenidos en las colas, se basa en la relación matemática siguiente relación matemática:

$$\%utilizacio\,n = \frac{\frac{PaquetesTr\,áficoOut - PaquetesTr\,áficoIn}{\Delta t}}{Anchodeban\,dadelacola} x100$$

Ilustración G.4.- Porcentaje de utilización en las colas

Donde, Δt es 300 segundos (correspondiente a 5 minutos de espaciado entre mediciones), y el *anchodebandadelacola* corresponde al ancho de banda configurado en la política de calidad de servicio para las colas por las cuales fluirán las aplicaciones de IPTV. Es importante mencionar que el diseño de la política de QoS para IPTV se encuentra en estudio por la empresa. Los valores de paquetes procesados son obtenidos a partir de las OID de las colas mencionadas anteriormente.

Diferencia entre DF de saltos consecutivos – Ajuste del mecanismo propuesto por el MDI:

- En vez de para cada paquete de llegada, es calculada la diferencia entre los *bytes* recibidos y los transmitidos cada 5 minutos, de la misma forma. Este valor es la profundidad virtual del buffer (Δ) y se expresa como se muestra en la siguiente fórmula:

$$\Delta = |bytes\_received - bytes\_drained|$$

Ilustración G.5.- Fórmula de Profundidad del Buffer

Los *bytes_received* son los correspondientes a los contadores de tráfico entrante de la cola (In). Para obtener el número en *bytes*, debe multiplicarse el valor obtenido en el contador por 1316 bytes, correspondiente al tamaño promedio en bytes de un paquete de video, según lo expuesto en la sección III.4.2. Es importante mencionar, que el valor *bytes_drained* es una constante para el MDI, y corresponde a la tasa a la cual deben ser drenados los paquetes en las premisas del cliente para garantizar correcta decodificación de los paquetes en el STB, esta tasa depende del tipo de codificación empleada y es el factor que caracteriza el carácter "virtual" del cálculo de la profundidad del *buffer*.

- En un intervalo de tiempo, se debe tomar la diferencia entre los valores máximos y mínimos de Δ y dividirla entre la tasa media de transmisión, como se muestra en la siguiente ilustración. Para la personalización al MGC, este intervalo de tiempo fue establecido inicialmente como una hora, es importante recalcar que estos valores corresponden un punto de partida, y con el concepto de mejora continua pueden ser ajustados una vez ofrecido el servicio de IPTV.

$$DF = \frac{(\max(\Delta) - \min(\Delta))}{media\_rate}$$

Ilustración G.6.- Fórmula del Delay Factor

APÉNDICE H.- Gráficas de reportes de tráfico utilizadas en el MGC

Reporte Diario: se proyectan diariamente las mediciones obtenidas cada 5 minutos, para cada uno de los equipos que conforman la red ME, sobre una gráfica de tiempo versus parámetro ligado a la medición, donde se encuentran los umbrales de alarma de referencia según el caso. Se genera de tipo automático.

Es importante reseñar, que debido a la naturaleza de la Diferencia entre DF de saltos consecutivos, así como para los parámetros de retardo y *jitter*, las gráficas no se van a generar por cada uno de los dispositivos, sino para cada uno de los enlaces objetivo de cada parámetro.

Para delimitar mejor las posibles alarmas, que ponen en riesgo la calidad del servicio, y sea más sencillo el monitoreo preventivo de los puntos críticos, además se genera un reporte diario que contenga los equipos y enlaces que presentaron mayor actividad, durante esas 24 horas y que superaron algún umbral preventivo o de congestión.

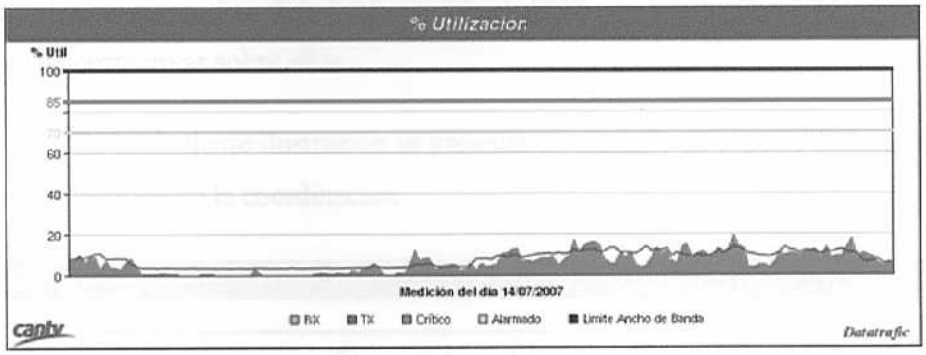


Ilustración H.1.- Ejemplo de Reporte diario. Tomado de Datatrafic

Reporte HCM (Hora Cargada Media): se proyecta un promedio lineal por hora, de las mediciones más críticas durante el día, sobre una gráfica semanal de tiempo versus parámetro ligado a la medición, donde se encuentran los umbrales de alarma de referencia según el caso. De esta forma se puede ver de forma

resumida el estado por parámetro de cada enlace de estudio y *switch* ME, pero en base a su hora más crítica, durante la semana.

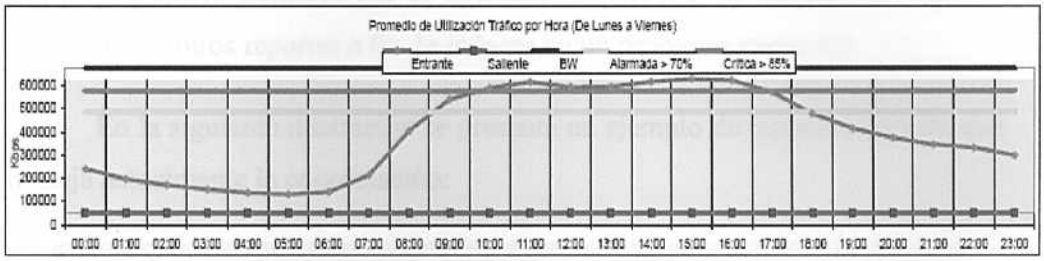


Ilustración H.2.- HCM Semanal (Lunes a Viernes). Tomado de Datatrafic

Reporte Semanal: se proyecta sobre una gráfica, de tiempo versus parámetro ligado a la medición, las mediciones semanales obtenidas mediante un cruce con los reportes diarios, con el fin de determinar cuáles dispositivos y enlaces presentaron problemas durante 5 días consecutivos (tiempo máximo definido en base a las buenas prácticas de la CGPRD para enviar una alarma), para un parámetro y servicio determinado. De esta forma se pueden, marcar aquellos dispositivos cuyas mediciones consecutivamente excedieron los umbrales críticos que ponen en riesgo la calidad del servicio de IPTV, ya sea VoD o BTV, y tomar acciones correctivas sobre ellos.

En la siguiente ilustración se presenta un ejemplo de reporte semanal que maneja actualmente la coordinación:

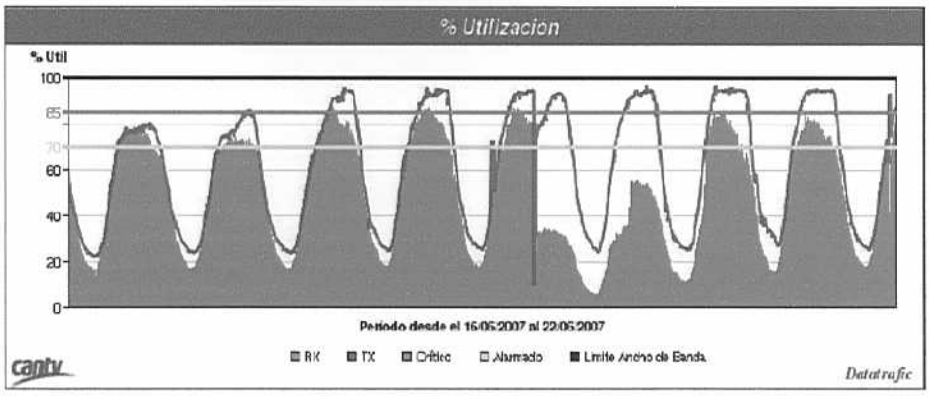


Ilustración H.3.- Ejemplo Reporte Semanal. Tomado de Datatrafic

Reporte Detallado: se proyecta sobre una gráfica de tiempo versus parámetro ligado a la medición, las mediciones tomadas cada 5 minutos, para un intervalo de tiempo específico definido por el operador, en base a los indicios de alarmas mostrados en otros reportes a fin de indagar en un problema particular.

En la siguiente ilustración se presenta un ejemplo de reporte detallado que maneja actualmente la coordinación:

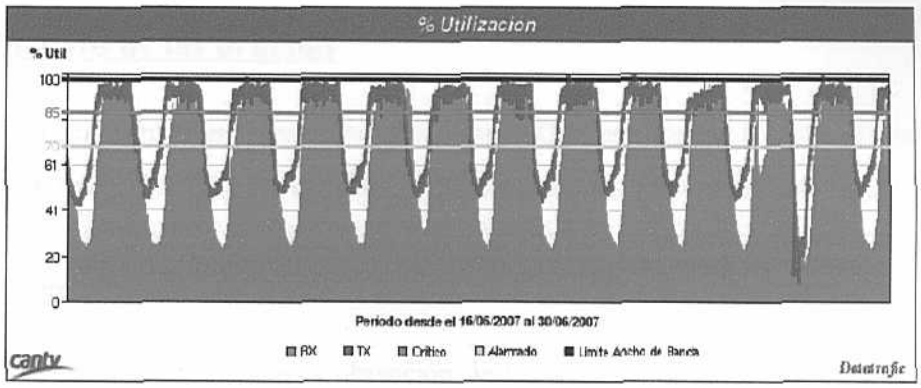


Ilustración H.4.- Reporte Detallado en base a dos semanas. Tomado de Datatrafic.

APÉNDICE I.- Diseño de Pruebas bajo ambiente controlado para el ajuste de umbrales

En el presente apéndice, se sugiere un diseño de pruebas sobre una maqueta que simule la arquitectura de IPTV, con el fin de ajustar los umbrales propuestos como resultado de la investigación, debido a que éstos sólo ofrecen un punto de partida, que debe ser optimizado en base a la práctica.

Objetivos de las pruebas

- Ajustar umbrales, para cada parámetro de QoS establecido durante el proceso de selección, descrito en la sección III.3, definiendo y/o ajustando los límites de los valores que alcanzan los parámetros, cuando se ve afectada la percepción de la imagen.

- Evaluar la eficacia de la obtención de los valores, en las colas de prioridad destinadas para el video (para BTV y VoD), necesarios para el cálculo de los parámetros de QoS, vía SNMP. De esta forma, se puede corroborar los resultados obtenidos en la práctica con la teoría de las MIBs utilizadas dentro de los *switches* ME.

- Validar los parámetros de QoS seleccionados, mediante el estudio del comportamiento de los mismos, sobre la calidad de la imagen, cuando la red manejaba condiciones críticas de congestión en un ambiente *triple play*.

Requerimientos para las pruebas

- Una configuración a pequeña escala que simule las redes que intervienen el transporte de IPTV, basándose en la plataforma actual de CANTV. La maqueta de IPTV, debe simular la sección de red señalada en la ilustración I.1, donde se utiliza de ejemplo la plataforma de CANTV.

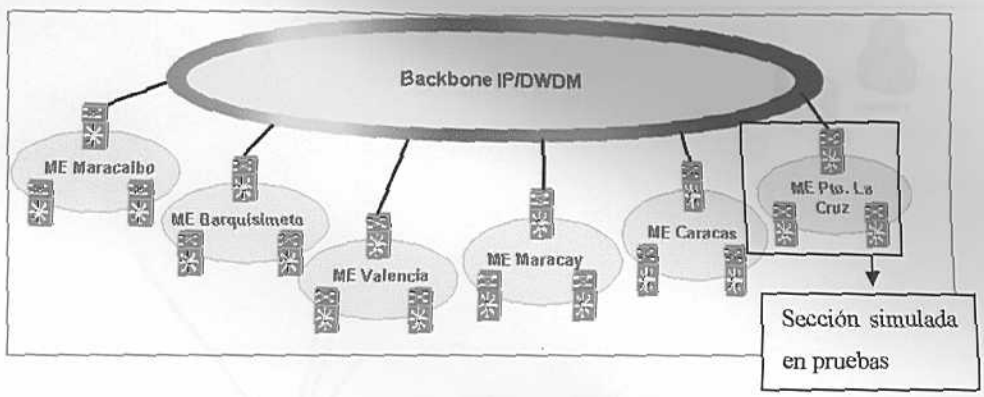


Ilustración I.1.- Arquitectura de Anillos Metro Ethernet
Tomado de Arquitectura de Redes y Plataformas de Servicios de CANTV

- Generación de tráfico de voz, video y datos que permitan estresar la red a los niveles reales que pasan por la red ME. Capacidad de indicar porcentajes de generación de cada uno (Por ejemplo, del 100 % del tráfico, tanto % para voz, tanto % para video y tanto % para datos).
- Capacidad de monitoreo de colas de prioridad, para obtener valores de retardo o *jitter* que pueda afectar la calidad del video.
- Capacidad de medición de parámetros de QoS básicos (*Jitter*, Pérdida de Paquetes y Retardo), tanto en un sentido como de ida y vuelta.
- Capacidad de medición de parámetros objetivos de calidad de video.
- Capacidad de marcar el tráfico de tal manera que los switches ME
- Capacidad de realizar las tareas de priorización y encolado.

Diseño de las Pruebas

La arquitectura de prueba diseñada se muestra a continuación:

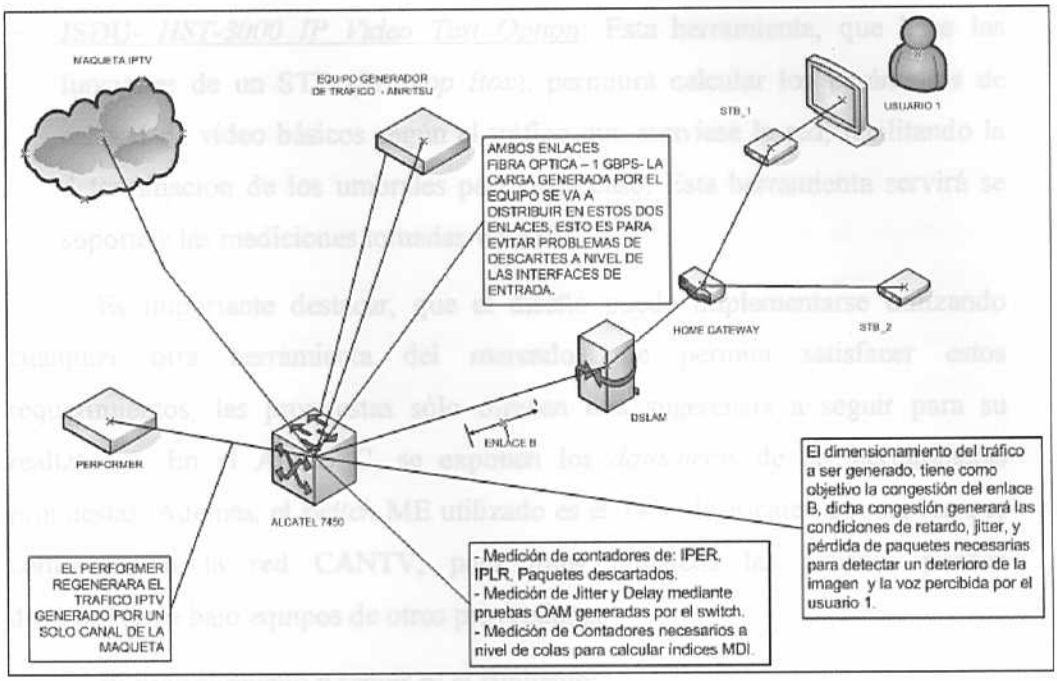


Ilustración I.2.- Diseño de la arquitectura de prueba

Para el caso específico de las pruebas a realizarse, sobre la maqueta de IPTV, perteneciente a la Corporación CANTV, las herramientas bajo las cuales se desarrolló el diseño y que permitieron alcanzar los objetivos planteados, fueron las siguientes:

- *Performer VoIP* de RadCom: Esta herramienta permitirá introducir tráfico de video exclusivamente, simulando condiciones reales de congestión sobre las colas de prioridad de video.
- *Anritsu MX123001A:* Permitirá introducir tráfico exclusivo de voz y datos, de forma controlada, simulando un tráfico de *background* de servicios *triple play*, característico de las red ME.
- SNMP (*Simple Network Management Protocol*): Esta herramienta permitirá extraer de los equipos las mediciones de la cola de video tomadas durante el desarrollo de las pruebas, con la finalidad de procesar esos datos y obtener los parámetros de video. A partir de aquí podrán ajustarse los umbrales del servicio, midiendo la calidad que se proyecta en la televisión del suscriptor (usuario 1).

- JSDU- *HST-3000 IP Video Test Option*: Esta herramienta, que hace las funciones de un STB (*Set Top Box*), permitirá calcular los parámetros de calidad de video básicos según el tráfico que atraviese la red, facilitando la determinación de los umbrales para cada caso. Esta herramienta servirá se soporte a las mediciones tomadas vía MIB.

Es importante destacar, que el diseño puede implementarse utilizando cualquier otra herramienta del mercado que permita satisfacer estos requerimientos, las propuestas sólo ofrecen una sugerencia a seguir para su realización. En el Anexo C, se exponen los *datasheets* de las herramientas propuestas. Además, el *switch* ME utilizado es el 7450 de Alcatel, por ser los que conforman a la red CANTV, para fines prácticos las pruebas pueden desenvolverse bajo equipos de otros proveedores.

El procedimiento a seguir es el siguiente:

- Previo a las pruebas, es necesario tener el acceso a los equipos de la maqueta IPTV, para poder obtener los valores requeridos vía SNMP.
- Se alimentará la herramienta *Performer* con flujo videos (ej. película de DVD). Con este flujo introducido, se configurará la herramienta para generarlo N veces, simulando de esta forma las condiciones reales de tráfico de video presentes en la red ME.
- Por otro lado se configurará la herramienta *Anritsu*, para que genere N veces tráfico de voz y datos. Con la finalidad de completar el *background triple play* característico de la ME.
- N se va a configurar de forma tal que genere tráfico de la siguiente manera: 80% datos, 10% voz y 10% de video. Este porcentaje inicial se estimó en base a los valores que maneja actualmente la coordinación, de tráfico de la ME.
- Una vez que se genere el tráfico deseado, se debe analizar el comportamiento de las colas y el trato que la red le da el video. Vía SNMP, se accederán a las MIB de los *switches* y se monitorearan los valores en bruto registrados en la cola de video.

- La herramienta JDSU se utilizará como complemento en la medición de parámetros de QoS del tráfico de video, la cuál se conectará al tubo del otro extremo de la maqueta, justo antes del STB1.
- Para video, si con el tráfico generado la señal recibida se aprecia sin errores, se procederá a cambiar los porcentajes de cada tráfico y se repetirá el procedimiento nuevamente para un caso más critico (provocando mayor congestión en la cola de video). En caso contrario, se podrá determinar el umbral en el cual la calidad de servicio del video disminuye la calidad de experiencia del usuario.

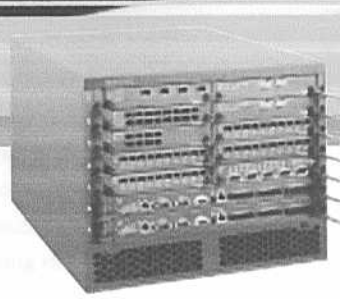
Limitaciones

- Las pruebas se realizarán en pequeña escala y bajo ambiente controlado, por lo que pueden producirse imprecisiones a la hora de extrapolar los resultados a escala real.
- Es necesario que todos los equipos cuenten con las MIBs apropiadas para el monitoreo de las colas destinadas para IPTV, lo cual depende del proveedor, así como con una política de QoS que acepte priorización y encolado del tráfico.

Anexo A.- Hoja Técnica del *switch* Alcatel 7450.

Alcatel 7450 ESS

Ethernet Service Switch | Release 2.0



The Alcatel 7450 Ethernet Service Switch (ESS) sets a new market standard for enabling the delivery of profitable metro Ethernet, Ethernet WAN services and high-density, service-aware Ethernet aggregation over networks based on Internet protocol/multiprotocol label switching (IP/MPSL). The 7450 ESS overcomes the limitations of traditional Ethernet switches that were developed to provide best-effort connectivity and therefore lack the scalability, reliability and service orientation required in the service provider environment. The Alcatel 7450 ESS was designed to excel in all these areas. The deterministic service orientation of the Alcatel 7450 ESS and the advanced service management tools provided by the Alcatel 5620 Service Aware Manager (SAM) enable a whole new stream of revenue opportunities, while minimizing operating expenses to reduce the total cost of ownership. The Alcatel 5620 SAM is composed of the Alcatel 5620 SAM Element Manager (SAM-E), Alcatel 5620 SAM Provisioning (SAM-P) and Alcatel 5620 SAM Assurance (SAM-A).

The Alcatel 7450 ESS delivers scalable performance and port density in two NEBS-compliant chassis configurations, the seven-slot ESS-7 and the single-slot ESS-1. The chassis are equipped with robust carrier-class features such as a service-oriented architecture, a wide range of interfaces with unmatched density and performance, and enough capacity to handle multigigabit and 10 Gigabit Ethernet — all at wire speed.

The Alcatel 7450 ESS can simultaneously deliver tens of thousands of metro Ethernet services with no performance penalties. Examples of revenue-generating Ethernet services for the metropolitan area and beyond are:

- Layer 2 Ethernet VPNs
- Ethernet virtual leased line (VLL) services
- Ethernet virtual private LAN services (VPLS)
- High-density, service-aware Ethernet aggregation

An Ethernet service switc
with unmatched density
performance that suppor
scalable, reliable and pr
dictable SLA-based Ether
services, flexible MPLS a
IP tunneling, programma
10 Gb/s fast path, STP,
802.1P/Q, H-QoS, Ethe
OA&M and stackable V

The Alcatel 7450 ESS is unique in two ways: it offers predictable and scalable user-centric services with per-application service guarantees and it can generate detailed and accurate billing records for tiered service offerings. These features enable the service provider to tailor service definitions that directly align with their customers business objectives and thereby create real value.

Market-Leading Programmable Fast Path

The Alcatel 7450 ESS includes a fully programmable, flexible fast path based on the latest network processor array (NPA) chip technology. The flexible fast path performs deep packet inspections and manipulations at 10 Gb/s line rates. A programmable fast path offers significant advantages over ASICs or off-the-shelf network processors that lack feature depth and programmability, or cannot perform at 10 Gb/s rates.

The programmable fast path eliminates the need for expensive and disruptive hardware upgrades. New features and releases can be remotely downloaded to installed systems. Features implemented in the programmable fast path include: access control lists (ACLs), quality of service (QoS), queues, filters, forwarding, accounting, and operations, administration and maintenance (OA&M) features.

Hierarchical Service-Based QoS

The Alcatel 7450 ESS enables service providers to deliver Ethernet services with the most stringent SLAs. The Alcatel 7450 ESS delimits an Ethernet service by an 802.1Q tag, a Q-in-Q tag, MPLS label or the Ethernet port itself. Each Ethernet service is buffered on the ingress side of the Alcatel 7450 ESS and shaped to a service level agreement (SLA) with service guarantees of committed information rate (CIR) and peak information rate (PIR). The buffers can accommodate different maximum burst sizes (MBS) due to per-service programmability, implemented in the flexible fast path. Each service can use multiple queues to enable shaping, policing and marking of different flows. Each service has counters to measure service-based statistics and enable enhanced billing on a per-customer basis. The QoS implementation of the Alcatel 7450 ESS scales to tens of thousands of services, supporting an aggregate of 8,000 ingress queues and 8,000 egress queues per MDA.

The Alcatel 7450 ESS, through its extensive QoS implementation, enables the delivery of intelligent Ethernet WAN service with guaranteed application SLAs, which the service providers have been used to delivering over frame relay and ATM networks. For example, the 7450 ESS:

- Enables the ability to run different applications within a single VPLS with distinct SLAs, as well as an aggregate SLA for each customer.
- Provides each service with its reserved bandwidth, but allows lower priority service burst to use all available bandwidth.

With this greater degree of control for service level differentiation, the 7450 ESS provides the freedom for the service provider to guarantee critical application performance without resorting to over-provisioning of bandwidth.

SLA features supported include service-based queuing, policing, and shaping. QoS and hierarchical QoS (H-QoS) are implemented in the flexible and programmable fast path.

Service Assurance and Rapid Troubleshooting

The 7450 ESS offers a full suite of integrated Ethernet OA&M tools enabling service providers to operate and manage their carrier metro, national and international Ethernet service networks, reducing truck rolls and operational expenses. No other Ethernet switch provides service providers such an extensive and easy-to-use set of tools to deploy and troubleshoot their Ethernet services. The Alcatel 7450 ESS hosts service-centric assurance tools specifically designed for rapid troubleshooting, and diagnosing service transport and service provisioning problems. The Ethernet Service OA&M tool kit aligns with the service provider's operational model.

Service-Aware Accounting and Billing

The Alcatel 7450 ESS comes with per-service or per-flow accounting and billing through an extensive set of statistics and counters implemented in the programmable fast path. The collection statistics are designed and sized to reduce the burden on the system CPUs, enabling statistics for thousands of simultaneous services. In addition, local data storage allows historical statistics to be maintained for several days. The advantage of a forward-planned architecture truly enables detailed and accurate billing records for tiered service offerings.

Features

Reliability and Redundancy

- Passive backplane
- 1:1 rapid failover between redundant switch fabric/control plane modules in seven-slot chassis
- 1:1 redundancy on common system elements, power supply (AC or DC), cooling fan
- Switch fabric graceful degradation
- Hot-swappable system components and physical interfaces
- ECC memory protection
- IEEE 802.3ad link aggregation and IEEE 802.1w Rapid Spanning Tree
- Equal cost multi-path
- MPLS path protection
- MPLS fast reroute (FRR) — sub 50 ms failover
- H-VPLS spoke redundancy with media access control (MAC) flush capability

Density and Flexibility

Seven-slot chassis:

- 100 Gb/s or 200 Gb/s switch fabric option (redundant, full duplex)
- 5 input/output modules (IOMs)
- 20 Gb/s or 40 Gb/s IOM slot capacity (full duplex)
- Five ESS-7 chassis can be mounted in a 7-ft. rack

One-slot chassis:

- 20 Gb/s (full duplex) fabric/system capacity in 1.5 RUs
- 1 IOM
- 20 Gb/s IOM slot capacity

On both chassis:

- On both systems each IOM accepts two hot-pluggable media dependent adapters (MDAs). IOMs and MDAs can be spared across two chassis.
- Optical interfaces use small form factor pluggable (SFP) optics that can be populated on a per-port basis
- 10 Gigabit Ethernet MDA
- Multirate PoS/SDH OC-3/STM-1, OC-12/STM-4 MDAs provide soft-selectable interface speeds on a per-port basis

Quality of Service

- Per-service QoS/H-QoS
- Per-service queuing, shaping and policing
- Ingress and egress buffering (up to 200 ms at 10 Gb/s in each direction)
- CIR, PIR, MBS queue parameters
- Thousands of ingress and egress operations
- Programmable queues, CIR/PIR enforcement
- Premium, assured and best-effort forwarding classes
- IEEE 802.1p filtering/marking/re-marking
- IETF DiffServ Code Point (DSCP) filtering/marking/re-marking
- Weighted random early detection (WRED) on ingress and egress
- Packet marking (DiffServ)
- Traffic shaping and policing (ingress and egress)
- Packet and byte counter statistics (ingress and egress)

Services

- Service-aware Ethernet aggregation
- VLL – point-to-point Layer 2 VPNs
- VPLS/H-VPLS – multipoint Layer 2 VPNs
- Generic routing encapsulation (GRE)

Alcatel's Broadband Services Aggregation Architecture

- Dynamic host configuation protocol (DHCP) relay with support for option 82 and DHCP snooping
- Local proxy address resolution protocol (ARP)
- IEEE 802.1x port-based authentication
- Internet group management procotol (IGMP) support for multicast and video services
- Split horizon groups to control unauthorized peer-to-peer communication

Service Assurance and Troubleshooting

- Integrated Ethernet OA&M utilities and diagnostics for VPN services
- Ethernet service, label switched path (LSP) and MAC pings, following the actual provisioned path of the service through the network

> Port and service mirroring, which goes far beyond the basic port mirroring, available on both ingress and egress flows. Can be set up locally or remotely.
> VPLS MAC trace route displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address

Service-Aware Accounting and Billing

> Per-service, per-flow accounting and billing statistics — all at wire speed
> Maintains statistics for thousands of services simultaneously
> Local data storage allows historical statistics to be maintained for several days
> Accounting data stored in XML format

Physical Interfaces

Copper Ethernet Cards

> 60-port 10/100Base-T Ethernet
> 20-port 10/100/1000Base-T Ethernet

Optical Ethernet Cards

> 20-port 100-FX Ethernet
> 10-port Gigabit Ethernet
> 20-port Gigabit Ethernet
> 1-port 10 Gigabit Ethernet
> 2-port 10 Gigabit Ethernet

POS cards (SONET and SDH)

> 16-port OC-3c/STM-1 POS
> 8-port OC-12c/STM-4 and OC-3c/STM-1 multirate POS
> 16-port OC-12c/STM-4 and OC-3c/STM-1 multirate POS
> 2-port OC-48c/STM-16 POS
> 4-port OC-48c/STM-16 POS

Certification

Safety

> UL60950-1
> CAN60950-1
> EN60950-1
> CE Mark

EMC

> AS/NZS 3548:1995 (Australia/New Zealand)
> EN55022 (Europe)
> VCCI Class A (Japan)
> FCC Part 15 Class A (United States)

Environmental Conditions

> Operating temperature: 0 C to 40 C (32 F to 104 F)
> Relative humidity: 0 to 90% (non-condensing)
> Operating altitude: Sea level to 3,048 m (10,000 ft.)

Software Specifications

Layer 2 features

> 802.1d Bridging, 802.1w Rapid Spanning Tree
> PVST Interoperability
> 802.1p/Q
> Q-in-Q VLAN stacking support
> 802.3x Flow Control
> 802.3ad Link Aggregation

Routing

> IS-IS, OSPF, RIPv1 and 2
> OSPF-TE and IS-IS-TE
> Equal cost multipath routing (up to 16 paths)
> Line rate Layer 2, Layer 3 and Layer 4 ACL filtering at 10 Gb/s
> Static and default routing
> Generic routing encapsulation (GRE)
> IGMP v1, v2, v3 and IGMP snooping

MPLS

> Static and dynamic LSPs
> Traffic engineering
> Signaling protocols: LDP and RSVP-TE
> LSR and LER
> LSP redundancy
> RSVP-TE: Primary/secondary paths and explicit routing
> Fast reroute (FRR) with sub 50 ms failover

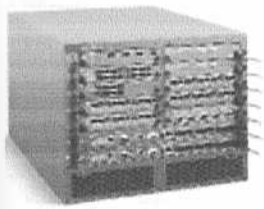
Security

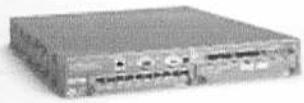
> Denial of service (DoS) attack prevention
> Wire-speed access control lists (ACLs)
> MD5 password encryption and authentication for routing protocols
> Classification and prioritization of control traffic
> SSH/SCP
> 802.1x port-based authentication
> Prevention of unauthorized communication between DSL subscribers
> DHCP-based automatic IP filter and static ARP cache population for DSL subscribers

Network Management

> Alcatel 5620 SAM provides extensive fault, configuration, accounting performance and security
> Fully featured industry command line interface (CLI), including service CLI
> SSH and Telnet
> FTP, TFTP and SCP
> RADIUS (AAA)
> TACACS+
> SNMP v1, v2c and v3
> Local and remote port/service/flow mirroring
> Service assurance tools including: service ping, SDP ping, LSP ping, MAC ping and MAC trace route
> Path MTU size measurement
> Round-trip delay measurement

Techinal Summary





ESS-7

Bandwidth
> 100 Gb/s or 200 Gb/s full duplex switch fabric options
> 20 Gb/s or 40 Gb/s IOM slot capacity (full duplex)
> Optional switch fabric/CPU redundancy

IOM Slots/MDAs
> 5/10

Redundancy
> Power, CPU, fabric, fans

Dimensions
> Height: 35.56 cm (14 in./8 rack units)
> Width: 44.4 cm (17.5 in.)
> Depth: 59.69 cm (23.5 in.)

Weight
> 27.22 kg (60 lb.) chassis weight (with 2 fan trays and air filters)
> Power supplies:
- DC PEM: 2.27 kg (5 lb.)
- AC PEM: 0.68 kg (1.5 lb.)
- AC power supply module (PSM): 4.76 kg (10.5 lb.)

Power
> 220 vAC (requires external shelf)
> 48 vDC
> 1+1 redundancy

Cooling
> Side-to-back air flow

ESS-1

Bandwidth
> 20 Gb/s fabric/system capacity (full duplex)
> 20 Gb/s IOM slot capacity (full duplex)

IOM Slots/MDAs
> 1/2

Redundancy
> Power, fans

Dimensions
> Height: 6.6 cm (2.6 in./1.5 rack units)
> Width: 44.4 cm (17.5 in.)
> Depth: 56.4 cm (22.2 in.)

Weight
> 12.25 kg (27 lb.) chassis weight

Power
> 110 vAC or 220 vAC
> -48 vDC
> 1+1 redundancy (requires external shelf)

Cooling
> Side-to-side air flow

Standards Compliance

Spec	Number	Description
Ethernet		
EEE	802.1D	Bridging
IEEE	802.1P/Q	VLAN Tagging and Priority
IEEE	802.1w	Rapid STP
IEEE	802.1x	Port based Authentication
IEEE	802.3	10Base-T
IEEE	802.3u	100Base-TX
IEEE	802.3x	Flow Control
IEEE	802.3z	1000Base-SX/LX
IEEE	802.3ad	Link Aggregation
IEEE	802.3ae	10 Gb/s Ethernet
TCP/IP		
RFC	768	UDP - User Datagram Protocol
RFC	1350	TFTP - Trivial File Transfer Protocol
RFC	791	IP – Internet Protocol
RFC	792	ICMP - Internet Control Message Protocol
RFC	793	TCP – Transmission Control Protocol
RFC	826	ARP – Address Resolution Protocol
RFC	854	Telnet
RFC	1542	BootP
RFC	1519	CIDR - Classless Inter-Domain Routing
RFC	1812	Requirements for IPv4 Routers
VRRP		
RFC	3768	Virtual Router Redundancy Protocol
RIP		
RFC	1058	RIP Version 1
RFC	2082	RIP Version 2
RFC	2453	RIP-2 MD5 Authentication
OSPF		
RFC	1765	OSPF Database Overflow
RFC	2370	Opaque LSA Support
RFC	2328	OSPF Version 2
RFC	3101	OSPF NSSA Option
RFC	3630	Traffic Engineering Extensions OSPFv2
RFC	1321	The MD5 Message-Digest Algorithm

>>>

IS-IS		
RFC	1142	OSI IS-IS Intra-domain Routing Protocol
RFC	1195	Use of OSI IS-IS for routing in TCP/IP and dual environments
RFC	2763	Dynamic Hostname Exchange for IS-IS
RFC	2966	Domain-wide Prefix Distribution with Two-Level IS-IS
RFC	2973	IS-IS Mesh Group
RFC	3373	3-way handshake for IS-IS point-to-point adjacencies
draft-ietf-isis-traffic-02.txt		Traffic Engineering Extensions ISIS
RFC 3567		IS-IS Cryptographic Authentication (MD5)
ISO/IEC	10589	IS to IS intra-domain routing information exchange protocol
IGMP		
RFC	1112	Host Extensions for IP Multicasting
RFC	2236	Internet Group Management Protocol, Version 2
RFC	3376	Internet Group Management Protocol, Version 3
PPP		
RFC	1332	PPP IPCP
RFC	1377	PPP OSINLCP
RFC	3518	PPP BCP
RFC	1661	PPP
RFC	1662	PPP in HDLC-like Framing
RFC	1989	PPP Link Quality Monitoring
RFC	2615	PPP over SONET/SDH
DHCP		
1542		Clarifications and Extensions for the Bootstrap Protocol
RFC	2131	Dynamic Host Configuration Protocol
RFC	3046	DHCP Relay Agent Information Option (Option 82)
RFC	1534	Interoperation between DHCP and BOOTP
GRE		
RFC	1701	Generic Routing Encapsulation (GRE)
RFC	1702	Generic Routing Encapsulation over IPv4 networks
RFC	2784	Generic Routing Encapsulation (GRE)
MPLS		
RFC	2702	Requirements for Traffic Engineering over MPLS
RFC	3031	MPLS Architecture
RFC	3032	MPLS Label Stack Encoding
RFC	3063	MPLS Loop Prevention Mechanism
draft-ietf-mpls-lsp-ping-02.txt		LSP Ping

>>>

LDP		
RFC	3036	LDP Specification
RFC	3037	LDP Applicability
RSVP-TE		
RFC	2430	A Provider Architecture for DiffServ and TE
RFC	3209	Extensions to RSVP for LSP Tunnels
RFC	3210	Applicability Statement for Extensions to RSVP for LSP Tunnels
RFC	2961	RSVP Refresh Overhead Reduction Extensions
RFC	3175	Aggregation of RSVP for IPv4 and IPv6 Reservations
RFC	3181	Signaled Pre-emption Priority Policy Element
draft-ietf-mpls-lsp-fastreroute-03.txt		Fast Reroute (FRR)
Differentiated Services		
RFC	2474	Definition of the DS Field in the IPv4 and IPv6 Headers
RFC	3246	Assured Forwarding PHB Group
RFC	2598	An Expedited Forwarding PHB
RFC	3140	Per-Hop Behavior Identification Codes
RADIUS		
RFC	2865	Remote Authentication Dial In User Service
RFC	2866	RADIUS Accounting
VPLS		
draft-ietf-l2vpn-vpls-ldp-xx.txt (previously know as "lasserre-vkompella")		
draft-stokes-vkompella-ppvpn-hvplsoam-xx.txt or "stokes-vkompella"		
draft-augustyn-vpls-requirements-xx.txt		
TACACS+		
IETF	draft-grant-tacacs-02.txt	
SSH		
IETF	draft-ietf-secsh-userauth-18.txt	SSH Authentication Protocol
IETF	draft-ietf-secsh-connect-18.txt	SSH Connection Protocol
IETF	draft-ietf-secsh-transport-17.txt	SSH Transport Protocol
Ethernet Pseudowire		
draft-ietf-pwe3-ethernet-encap-xx.txt		
draft-ieft-pwe3-control-protocol-xx.txt		
draft-so-pwe3-ethernet-xx.txt		
draft-martini-l2circuit-trans-mpls-xx.txt		
draft-martini-l2circuit-encap-mpls-xx.txt		
SONET/SDH		
Telcordia	GR-253-CORE	Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria
ITU-T	G.783	Characteristics of Synchronous Digital Hierarchy (SDH) equipment functional blocks
ITU-T	G.957	Optical interfaces for equipment and systems relating to the synchronous digital hierarchy
ITU-T	G.707	Synchronous Digital Hierarchy Bit Rates >>>

Network Management		
RFC	1724	RIPv2 MIB Extensions
RFC	1850	OSPF-MIB
RFC	1907	SNMPv2-MIB
RFC	2011	IP-MIB
RFC	2012	TCP-MIB
RFC	2013	UDP-MIB
RFC	2096	IP-Forward-MIB
RFC	2206	RSVP-MIB
RFC	2558	SONET-MIB
RFC	2571	SNMP-FRAMEWORK-MIB
RFC	2572	SNMP-MPD-MIB
RFC	2573	SNMP-TARGET-&-NOTIFICATION-MIB
RFC	2574	SNMP-USER-BASED-SM-MIB
RFC	2575	SNMP-VIEW-BASED-ACM-MIB
RFC	2576	SNMP-COMMUNITY-MIB
RFC	2665	EtherLike-MIB
RFC	2819	RMON-MIB
RFC	2863	IF-MIB
RFC	2864	Inverted-Stack-MIB
RFC	2987	VRRP-MIB
RFC	3014	Notification-LOG-MIB
RFC	3273	HCRMON-MIB
IETF	draft-ietf-ospf-mib-update-04.txt	OSPF Version 2 Management Information Base
IETF	draft-ietf-mpls-lsr-mib-06.txt	MPLS Label Switch Router Management Information Base Using SMIv2
IETF	draft-ietf-mpls-te-mib-04.txt	MPLS Traffic Engineering Management Information Base Using SMIv2
IETF	draft-ietf-mpls-ldp-mib-07.txt	Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)
IETF	draft-ietf-isis-wg-mib-05.txt	Management Information Base for IS-IS
IANA	ifType-MIB	Textual Convention
IEEE	8023-LAG-MIB	Link Aggregation module for managing IEEE Std 802.3ad
An extensive array of private enterprise MIBs are also supported.		

Anexo B.- Hoja Técnica de la solución de monitoreo OMNI-Q de RADCOM

Omni-Q Probes

VoIP Quality and Performance Probes

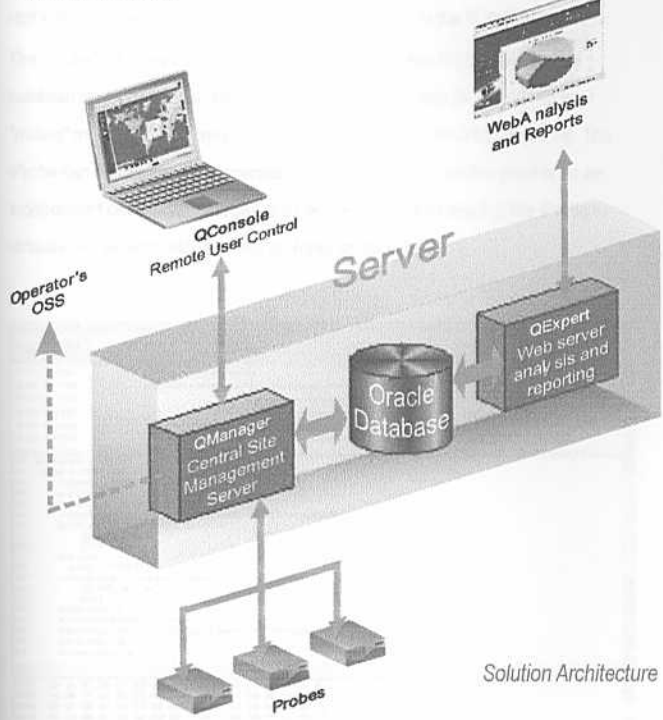
Omni-Q - Quality online

Is VoIP quality an issue for you?
Do you need to trace signaling across your network?
Do you need to continuously collect, monitor and analyze voice traffic performance parameters?

Omni-Q is a VoIP quality monitoring solution designed to continuously collect, monitor and analyze voice traffic performance parameters and voice quality. Omni-Q consists of a comprehensive array of voice performance and quality measurement methodologies, all under one unified offering. These include a broad range of intrusive (active) and non-intrusive (passive) hardware and software probes covering both the PSTN and the IP environments. A powerful user-friendly management layer offers many features that allow you to set up and monitor value-added voice related offering such as Service Level Agreements and Partner Verification Services.

Omni-Q - Probe-based Solution

The Omni-Q probes are centrally managed by the Management Server, the QManager. They are remotely accessed by the QConsole Software, installable on any PC/laptop. All collected parameters are stored in an Oracle database for use by the QExpert Web-based analysis and reporting tool. Both active and passive probes are available.



Solution Architecture

Active Probe Operations

Active probes provide link quality and performance measurements by creating te calls between probes. Users can define a flexible automated scheduling regime, execute ad-hoc test calls. Creating automated test schedules is an important component of real pro-active monitoring/testing, as it enables operators to benchmark VoIP service quality and detect service degradation before their customers. The probes provide availability (signaling), performance and voice quality (PESQ) measurements on the test call session.

Passive Probe Operations

Passive monitoring probes provide single point quality and performance measurements on all live user-traffic and on detected test calls generated by oth Omni-Q probe. The vPobe's operational concept is based on user configurable definitions of the target traffic and of the actions to be performed on the detecte target traffic. Once actions are defined, the vProbe continuously monitors those targets 24 hours a day, 7 days a week. The targeting mechanism is direction aware and is based on the probes sophisticated run-time signaling and packet- packet analysis capabilities, where 'wild characters such as * and ? can be appl to the extracted E164 and Alias, and where masks and ranges can be applied t IP addresses.

The action options include:

- Enhanced detail record (eDR) of the session, providing measurements on both RTP directions and on the signaling plane
- Saving of a full detailed, hardware time stamped call flow signaling decode the session (this can be limited to abnormal calls only)
- Saving the WAV of the call
- Calculating the ITU T P862 (PESQ) voice quality on detected test calls generated by active Omni-Q probes
- Calculating passive mean opinion scores for each live (user traffic) stream

RAD COM

TEST-OF-THE-AR

vProbe - Live Traffic Visibility

The vProbe provides multiple parameters and measurements on VoIP signaling, user media, and availability indicators. Supporting a three-layered operational approach, it enables operators to easily shift between monitoring, drill down and trouble shooting, all-in-one probe. In the first level enhanced call-detail-record of performance measurements are collected for each call (both RTP directions). RTP streams and their associated signaling procedures are correlated. In the second level signaling storage is offered. In signaling storage, abnormal calls can be specifically targeted and their detailed call-flow decodes collected and stored for on-line, real-time operations and customer support.

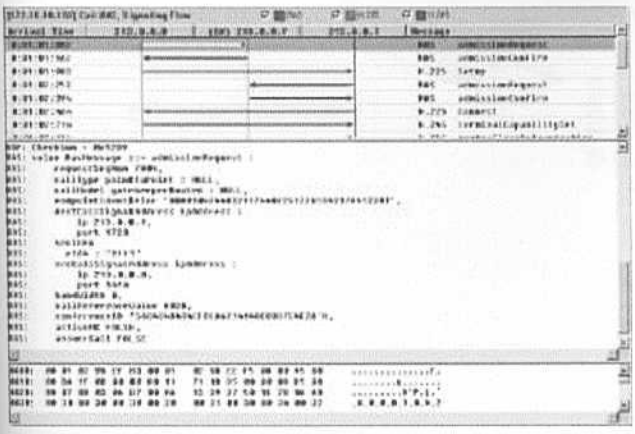
The signaling flow decode is provided for each call, and is displayed together with all the other quality detail records of the call. These provide a more comprehensive view that could be further utilized for assessing and correcting degradation on the network.

The graphic flow display is based on accurately time stamped frames collected from probe hardware (The arrival times are accurate to within 200 nano seconds). In the third level, run time and more in-depth real-time trouble shooting capabilities are offered. In this manner, the probe server unit can be used for remote testing capabilities, saving on operations cost by eliminating the need for a field engineer.

cProbe/iProbe - End-to-end User Perspective

The cProbe-server supports multiple types of PSTN interfaces including analogue, BRI, PRI (E1/T1), CAS (E1/T1), SS7 and cellular handsets and is used to establish real voice test calls to other Omni-Q entities deployed in the IP or PSTN clouds.

The iProbe probe-server comes in two variants, SIP and H323. It is used to establish up to 15 simultaneous real voice test calls, either in "direct" mode or "routed" mode, to other Omni-Q entities deployed in the IP or PSTN clouds. The iProbe can be configured to operate either as a VoIP termination point or as an independent closed-box gateway, thus enabling the attachment of the iProbe to virtually any network element with an Ethernet interface.



Signaling Flow Report

Active Probe Deployment Applications

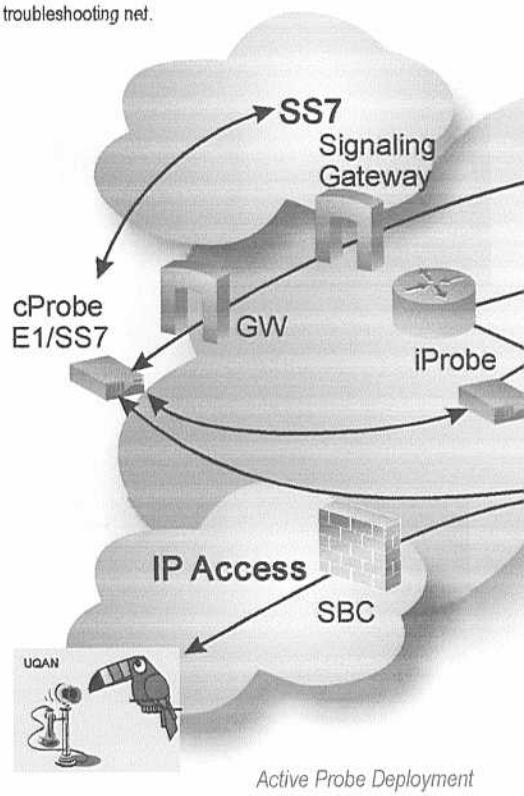
The active probes can be deployed with other Omni-Q probes to fulfill the demanding needs of VoIP monitoring in core and access applications. Active probes provide link quality and performance measurements by creating test calls between probes. Some example scenarios aimed at demonstrating the Probes unique deployment flexibility and operational advantages follow.

PoP-to-PoP/edge-to-edge - Probes at the edges of the IP cloud, configured to make real test calls, obtain benchmarks of various VoIP routes.

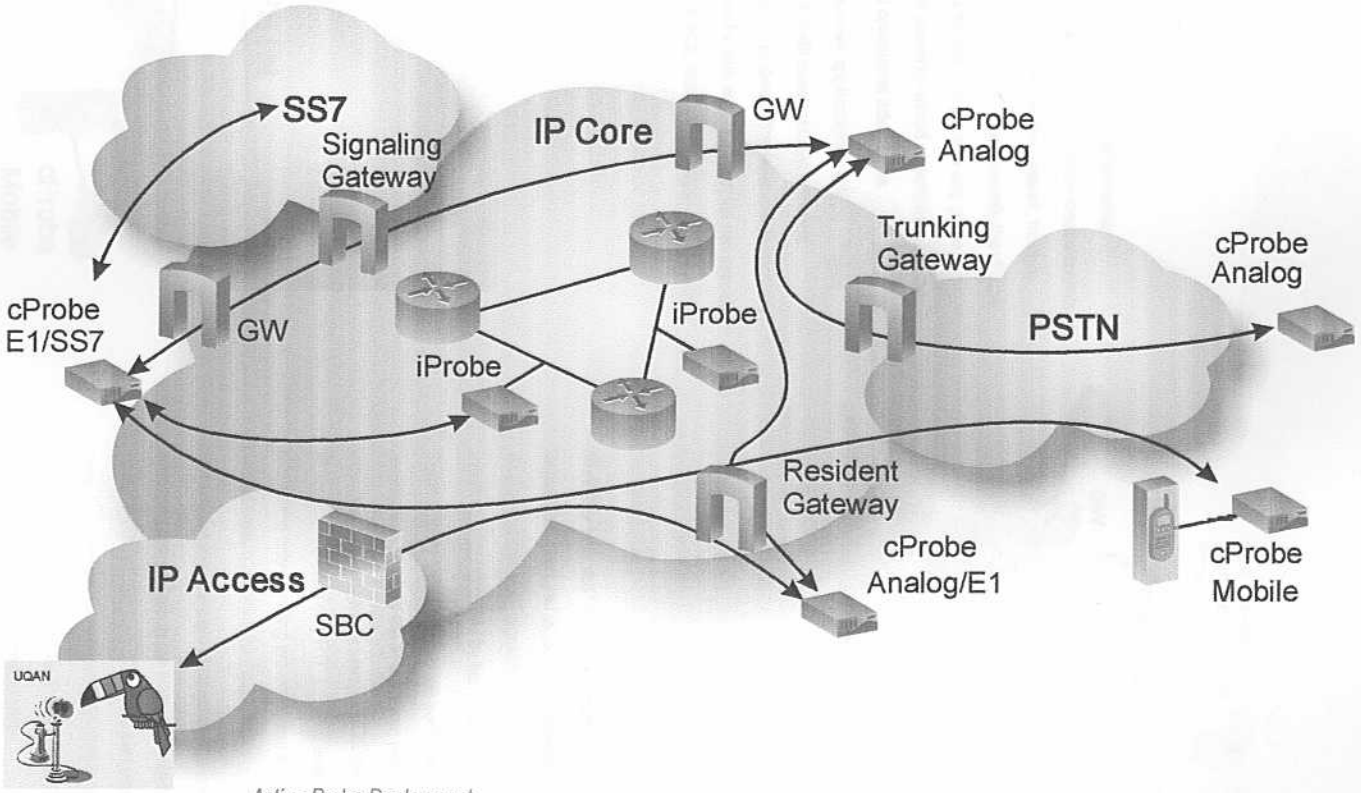
PoP-to-end user - Probes located at central points in the network scheduled to make automated test calls to the Omni-Q's UQAN probes deployed at end-users, perform pro-active monitoring and troubleshooting of end-user perception of voice quality and quality of service.

PSTN-to-IP crossover - Probes located at central points in the network (iProbes) or at edge PoPs (cProbes) scheduled to make automated test calls to Omni-Q's IP or PSTN probes; provide pro-active monitoring and troubleshooting capabilities across the IP or PSTN network for calls originating in the PSTN and terminating in VoIP, or vice versa.

Segmenting the IP cloud - iProbes deployed in multiple locations across the IP cloud, scheduled to set up automated test calls, create a fully meshed pro-active monitoring and troubleshooting net.



Active Probe Deployment



Active Probe Deployment

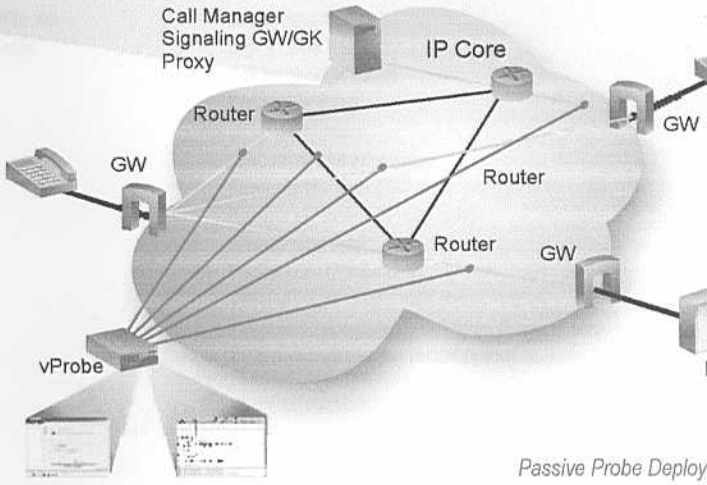
cProbe iProbe vProbe

Passive Probe Applications

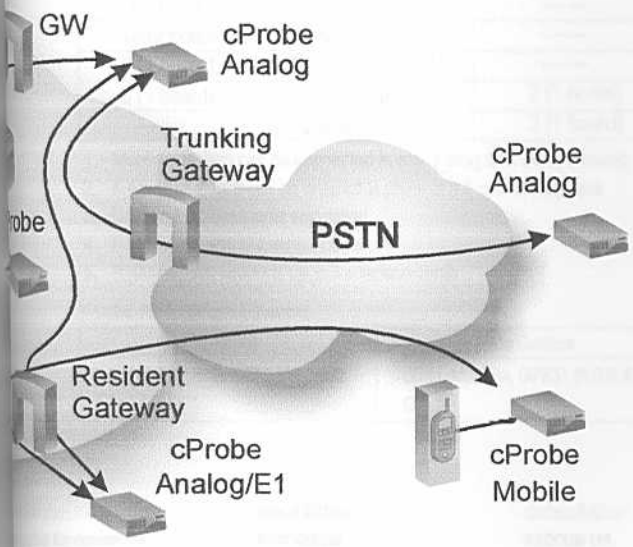
vProbe Deployment Applications

Passive monitoring probes provide single point quality and performance measurements. However, since the Omni-Q solution can correlate measurements made by different probes of same session as it traverses the network, multiple vProbes can be used to provide end-to-end link quality. Consequently the vProbe can be deployed with other active Omni-Q probes or in passive only probe deployment. Following are some example scenarios aimed at demonstrating the vProbes unique deployment flexibility and operational advantages.

Enhance any of the active probe deployment applications - adding vProbes provides the user with additional detailed in-path quality and performance measurements. eDR's collected from different probes of the same call session are correlated together. This provides the operator with unified view of the call session and information on degradations across the path, enabling for better understanding and troubleshooting of the service.



Passive Probe Deploy



Visibility into VoIP networks - multi technology vProbes with signaling storage capabilities deployed at signaling gateways are able to measure, decode and display multiple VoIP signaling protocols. Via the QManager, the different signaling sessions/legs measured by the vProbe are correlated into a single call session.

Voice quality monitoring - high performance vProbes located at central aggregation points in the IP cloud can provide live user media with performance measurements as well as passive MOS per RTP stream. Results collected from vProbes monitoring only RTP streams, and results collected from vProbes monitoring only signaling are correlated to present the operator with a single unified view.

Edge point monitoring - vProbes can be used for edge point monitoring by deploying probes both at the core and deeper towards the edge. This provides the operator with a fuller view of network performance behavior at the edge and at the core. Furthermore, by supporting RFC 3611 the vProbe can intercept, collect and analyze reports generated by IP Phones and gateways and use them to provide end-to-end voice quality assessments.

cProbe iProbe vProbe

Measurements

The dedicated hardware used for generating test calls and monitoring voice calls ensures accurate hardware time-stamped measurements. The probes provide a wide variety of measurements

vProbe Measurements

vProbe measurements include:

- Call Setup Time
- ASR & NER
- ITU T P862 PESQ Voice Quality on identified test traffic generated by the Omni-Q active probes (cProbe/iProbe) to provide in-path voice quality measurements
- Call termination cause
- Round trip delay
- Passive MOS
- Jitter (RTP)
- Packet loss, packet loss burst (RTP)
- Answer delay
- Source/destination number/IP address/ endpoint/ termination ID
- RFC3611 analysis(future option)
- RTCP analysis application add-on (future option)
- Video quality monitoring (future option)

Active Probe Measurements

- Call Setup Time
- ASR & NER
- ITU T P.862 PESQ Voice Quality
- Background Noise
- Signal Level & insertion loss
- Call termination cause
- Round Trip delay
- DTMF verification
- Echo delay and attenuation
- Facsimile test calls (T30 compliant) (cProbe only)
- Number of Packets (iProbe only)
- Jitter (iProbe only)
- Packet Loss (iProbe only)
- Variable length quality calls (future option)
- Advanced voice analysis drill down (future option)
- T105 responder testing (future option)

Specifications

Probe Specifications

	Width	Depth	Height	
R1000	440mm (17.5in)	470mm (18.7in)	89mm (3.5in)	Rack Mount
P1000	360mm (14.1in)	480mm (18.9in)	130mm (5.1in)	Portable
R4000	430mm (17in)	680mm (27in)	220mm (8.7in)	High-density Rack Mount

Available in 110-230 Volt AC or -48 Volt DC

cProbe port densities (based on R1000 probe server)[5]

Analog [1,2]	Digital [3,4]	SS7 (E1/T1)
24 (3 boards)	——	——
16 (2 boards)	1 to 4 (1 board)	——
8 (1 board)	2 to 8 (2 boards)	——
8 (1 board)	1 to 4 (1 board)	2 (1 board)
——	2 to 8 (2 boards)	2 (1 board)

1. Mobile adapters can be connected to any analog interface (optional).
2. A 4 port BRI card can be ordered in place of a 8 port analog card.
3. CAS and CCS variants supported
4. PCM A-Law and U-Law supported
5. P1000 server supports up to 3 interface cards

iProbe 10/100Mbps Ethernet

Signalling	Voice Codecs
H.323, SIP	G711 A/u-Law, G7231 (5.3/6.4), G729

vProbe

Signalling	Voice Codecs
H.323, SIP, MGCP, NCS, H.248, SCCP (future option)	G711 A/u Law, G723.1 (5.3/6.4,) G729, G726 (32)

vProbe port densities (based on R1000 probe server)

Port mirror [1]	In-line [2]
Up to 2 GBE ports (2-port board)	1 GBE link (2-port board)
Up to 4 GBE ports (4-port board)	Up to 2 GBE links (4-port board)
Up to 4 FE ports (4-port board)	Up to 2 FE links (4-port board)

1. In port mirror connection the vProbe is connected to the network a mirrored port (spanned port) in a switch or router.
2. In in-line connection (bump-on-the-wire) the vProbe is connected on the traffic, from and to the switch/router/gateway.

S Office:
ADCOM Equipment Inc.
Forest Avenue
ramus NJ 07652 USA
: (201) 518-0033
x: (201) 556-9030
00-RADCOM-4
mail: info@radcomusa.com

Israel Office:
RADCOM Ltd.
24 Raoul Wallenberg Street
Tel-Aviv 69719 Israel
Tel: +972-3-6455055
Fax:+972-3-6474681
e-mail: info@radcom.com

China Office:
RADCOM Ltd.
Handerson Center, Office 506, Tower 3
18 Jianguomennei Avenue,
Beijing 1000005, P.R. China
Tel: +86-10-65187723
Fax:+86-10-65187721
e-mail: china@radcom.com

United Kingdom Office:
RADCOM UK
2440 The Quadrant
Aztec West, Almondsbury
Bristol, BS32 4AQ England
Tel: +44-145- 487 8827
Fax: +44-145-487 8788
e-mail: uk@radcom.com

RADCOM
TEST-OF-THE-ART

ecifications subject to change without notice. MS-Windows is a trademark of Microsoft Corporation.
and and product names are trademarks of the respective companies.

Anexo C.- Hoja Técnica de las herramientas propuestas en el diseño de pruebas.

HST-3000

VDSL2 Service Interface Module (SIM)

Highlights

- Test the technology, test the service, improve the process
- Thoroughly qualifies VDSL2 access service: Attenuation, Noise Margin, Bits per Tone, Actual bit rate, Maximum bit rate, % Capacity, and Estimated Loop Length
- Data layer test options: PPPoE, PPPoA, IPoA, FTP throughput, and Web Browser
- Test interfaces: VDSL2-wire and Ethernet 10/100
- Option copper test capability up to 30Mhz
- Test modes: Terminate, Through, and TE (Terminal Equipment)
- Flexible, modular design allows you to buy what you need now and easily upgrade later in the field

In one lightweight, robust, battery operated tester, the JDSU HST-3000 offers more testing power than any other handheld tester on the market. Its scalable, modular design cost-effectively addresses today's needs. Upgrade later in the field to meet emerging requirements through plug-in hardware modules and software options.

JDSU's HST-3000 VDSL2 SIM delivers comprehensive VDSL2 test support including VDSL2 physical layer, Data layer, and Services (Web, VoIP, and IPVideo) in one module. Optional data service test support includes: PPPoE, PPPoA, IPoA, Bridged Ethernet, DNS client, DHCP client and server, as well as FTP throughput, Web Browser, IP PING, and IP Trace Route. Test modes include: Terminate Mode (VDSL2 modem emulation), Through mode (VDSL2 to Ethernet), and TE mode (Ethernet). With a simple to use GUI, the ability to store multiple configurations and auto test routines, VDSL2 service provisioning and troubleshooting becomes efficient and thorough. Using scripting features of the HST, specific test scenarios can be consistently performed. Using the results storage and export features of the HST-3000, key VDSL2 line parameters can be captured for benchmarking and later used in trouble resolution.

Test the Technology

- Max bit rate
- Actual bit rate
- Loop attenuation
- Noise Margin
- Percent (%) capacity
- Bits per tone
- Estimated loop length
- VDSL chipset support dependent on SIM part number
  - *Ikanos*
  - *Connexant*
  - *Infineon Aware*

Test the Service

- Data PPPoE, PPPoA, IPoA, Bridged Ethernet
- DNS, DHCP Client/Server, IP PING, IP Trace Route
- FTP throughput
- Web browser

Improve the Process

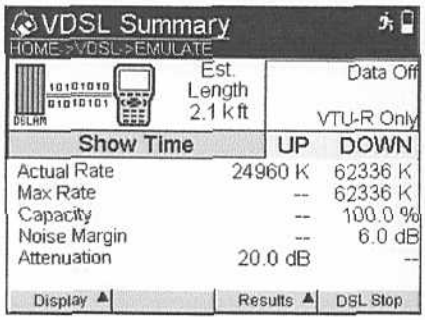
- Multiple configuration storage
- Test results export, serial, USB, Ethernet
- FTP throughput
- Web browser

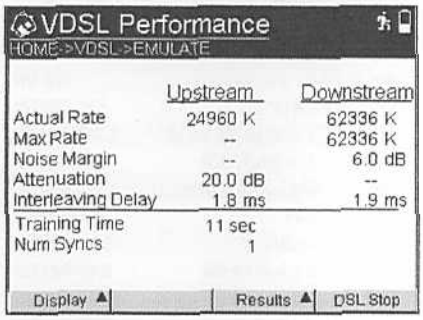
Added benefits

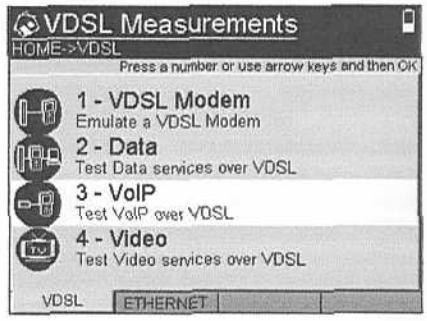
- VoIP and IP video testing over VDSL2 support
- Three modes of operation: Terminate, Through, and TE

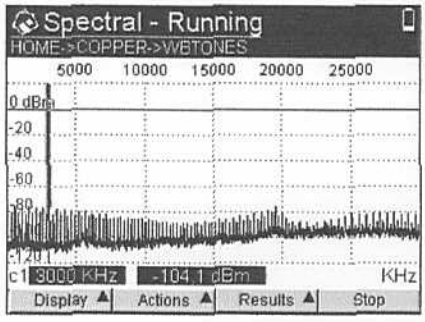
The HST-3000 boasts advanced scripting features to improve compliance with operator Methods and Procedures, through interactive, one-button auto-tests. These tests are fully customizable on a per-customer basis, to include pass-fail thresholds.

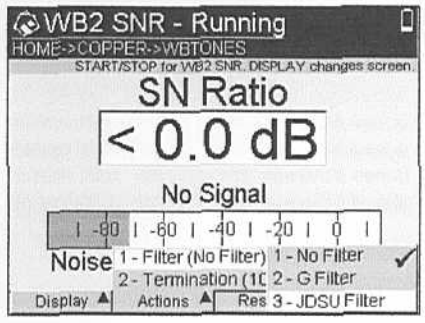
Use the HST-3000 everywhere you need to quickly isolate your troubles: the network "IN," the loop "OUT" or the CPE. The handheld, rugged and easy-to-use HST-3000 is ideal for field use. It is compact, rugged and can be used in almost all conditions, from inside the CO/Exchange to outside in moderate rain.

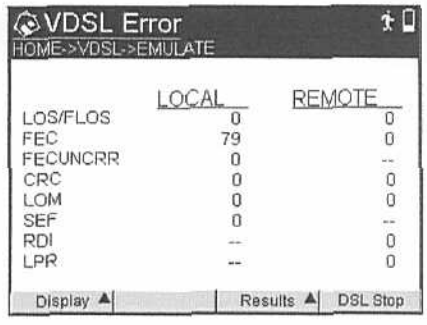












Ordering information

WBII Only SIMs (Modules)

HST3000-WBII (CHST-M34)	Wideband Copper II SIM

Combination WBII and VDSL/VDSL2 SIMs (Modules)

HST3000-VDSL-CNXT	VDSL with Connexant Chipset SIM
HST3000-CUVDSL-CNXT	VDSL and copper with Connexant Chipset SIM
HST-3000-VDSL-CNXT-WB2	VDSL and copper (up to 30 MHz) with Connexant Chipset SIM
HST3000-VDSL-IK	VDSL with Ikanos Chipset SIM
HST3000-CUVDSL-IK	VDSL and copper with Ikanos Chipset SIM
HST-3000-VDSL-IK-WB2	VDSL and copper (up to 30 MHz) with Ikanos Chipset SIM
HST3000-VDSL-INF	VDSL with Infineon Aware Chipset SIM
HST3000-CUVDSL-INF	VDSL and copper with Infineon Aware Chipset SIM
HST-3000-VDSL-INF-WB2	VDSL and copper (up to 30 MHz) with Infineon Aware Chipset SIM

Available SIMS (Modules)

HST3000-DC	Datacom SIM
HST3000-4WLL	4 wire local loop
HST3000-T1	Dual TX/RX bantam T1 interface and T1 software option
HST3000-CT1	Dual T/R/G interface for copper testing and dual TX/RX bantam T1
HST3000-T3	Dual TX/RX bantam T1 interface, and dual RX/single TX BNC DS3 interface and DS3 software option
HST3000-BRI	ISDN BRI option
HST3000-ARCE	ADSL (ATU-R) option
HST3000-CAR	Copper (ATU-R) option
HST3000-CU	Dual T/R/G interface to copper test option
HST-GSH	G.SHDSL option
HST3000-CuCE	Cu only SIM, CE mark
HST3000-CARCE	Cu and ATU-R (Annex A) SIM, CE mark
HST3000-ARCA	ATU-R/C dual mode SIM, AoPOTS
HST3000-CARCA	Cu and ATU-R/C dual mode SIM, AoPOTS
HST3000-ARB	Annex B ATU-R SIM
HST3000-CARB	Annex B Cu/ATU-R SIM
HST3000-ARCB	ATU-R/C dual mode SIM, AoISDN
HST3000-CARCB	Cu and ATU-R/C dual mode SIM, AoISDN
HST3000-CSHCE	G.SHDSL and Cu SIM
HST3000-BLK	Blank SIM
HST-BRA ETSI (Euro)	ISDN BRA SIM
HST-BRA ETSI	(Euro) ISDN BRA SIM
HST3000-ETH	10/100/1000 Ethernet SIM
HST3000-WB2	Wide Band 2 (up to 30 MHz) copper test SIM
HST3000-AR2A	ADSL1/2/2+ (ATU-R, Annex A)
HST3000-AR2B	ADSL1/2/2+ (ATU-R, Annex B)
HST3000-CAR2A	ADSL1/2/2+ with copper (ATU-R, Annex A)
HST3000-CAR2B	ADSL1/2/2+ with copper (ATU-R, Annex B)

Software options

HST3000-AR2A	ADSL2+ (ATU-R, Annex A)
HST3000-AR2AB	ADSL2+ (ATU-R, Annex A/B)
HST3000-AR2B	ADSL2+ (ATU-R, Annex A)
HST3000-OPTETH	Optical Ethernet
HST3000-MSTR	Multiple Streams
HST3000S-IP-Video	IP Video Analysis
HST3000S-VoIP	VoIP Analysis
HST3000S-MOS	VoIP Mean Opinion Score
HST3000S-H.323	H.323 VoIP Signaling
HST3000S-SCCP	SCCP VoIP Signaling
HST3000S-SIP	SIP VoIP Signaling
HST3000S-MGCP	SCCP MGCP VoIP Signaling
HST3000-PS	Pulse Shape software option
HST3000-FR	Frame Relay software option
HST3000S-IP	Advanced IP suite – PING and Through mode support
HST3000S-WEB	Web browser option
HST3000-WBTONES	WB TIMS option
HST3000-RFP	RFL option
HST3000S-VOIP	VoIP software analysis option
HST3000-FTP	FTP software option
HST3000-SCRIPT	Scripted test option
HST3000S-H.323	VoIP Signalling call controls for H.323
HST300S-SCCP	n for Cisco SCCP
HST3000S-SIP	VoIP Signalling option for SIP call control
HST3000-PCMSIG	Signalling (PCM) software option
HST3000-PCMTIMS	TIMS (PCM) software option
HST3000-T1DDS	DDS-T1 software option
HST3000-PRI	ISDN PRI software option (NC Standard)
HST3000-SPE	Spectral Noise software option
HST3000S-MOS	MOS (Mean Opinion Score) Analysis option
HST3000S-UNISTIM	VoIP signaling option for Nortel Unistim
HST3000S-VMOS	Video MOS analysis option
HST3000S-VIDEO	Video analysis option

Wideband Copper SIM Cables

CB-WBII-PKG1	North America centric cable package includes CB00688,CB00686, and (2) C70901
CB-WBII-PKG2	International centric cable package includes CB00688, CB00686, and S1505
CB00688	Tip(A) - Ring(B) - Ground 4MM connectors
CB00686	Tip1(A1) - Ring1(B1) -Ground 4MM connectors
C70901	4MM Telco Lineman Clips
S1505	4MM Clip Package

Test & Measurement Regional Sales

NORTH AMERICA
TEL: 1 866 228 3762
FAX: +1 301 353 9216

LATIN AMERICA
TEL: +55 11 5503 3800
FAX: +55 11 5505 1598

ASIA PACIFIC
TEL: +852 2892 0990
FAX: +852 2892 0770

EMEA
TEL: +49 7121 86 2222
FAX: +49 7121 86 1222

WEBSITE: www.jdsu.com

1014223 503 1206 HSTADSL2.SS.ACC.TM.AE

Anritsu

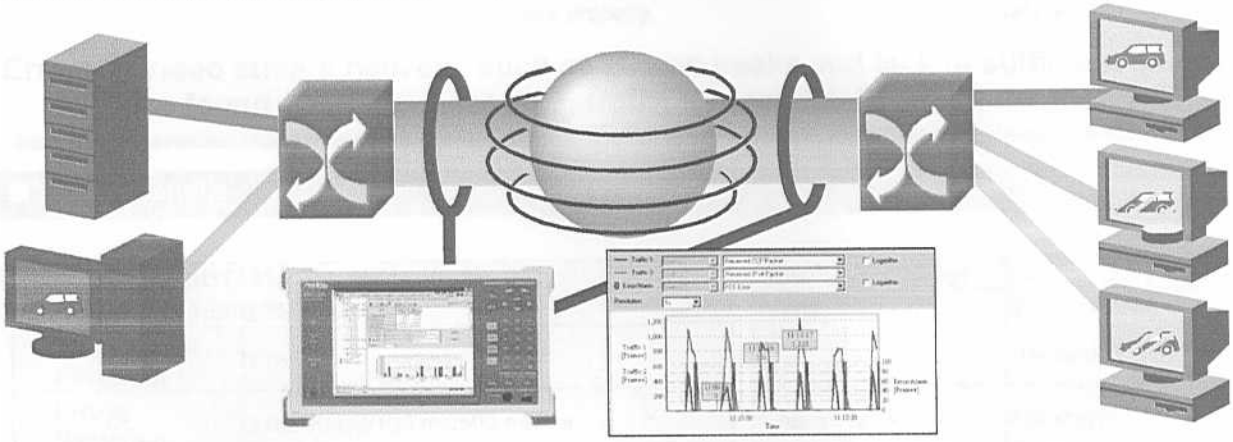
Application Traffic Monitor

MD1230A-20/MD1231A-20 and MX123001A-20

Monitoring Video Streaming with 1 ms Resolution

■ Broadband Trends in Network Services

New network services are continuously impacted by technology advancement. One area of rapid progress is in streaming transmission service, used in applications such as video transport. Streaming transmission has critical latency time requirements, so real-time performance is much more important there than in traditional data transmission. Streaming networks are designed by calculating bandwidth utilizations, so it is necessary to measure the bandwidth of each traffic stream to design these networks and to investigate the causes of problems.
This MD1230A Family option allows for high-resolution analysis though high-resolution time-series monitoring that cannot be implemented by using existing measurement techniques



Errors in stream delivery cannot be found by traditional monitoring at one second intervals

■ MD1230A-20/MD1231A-20 and MX123001A-20 Application Traffic Monitor

The High Resolution Traffic Monitor enables precise network traffic measurements with **1 ms resolution**.

■ Monitoring 4 Flows Simultaneously

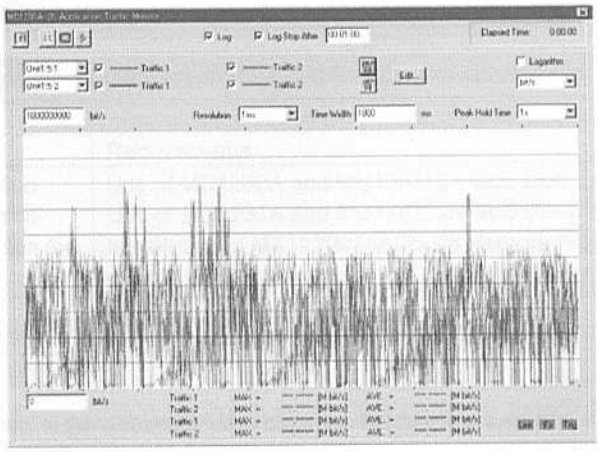
This application can monitor 2 flows per port on each of 2 GbE ports, thereby handling up to 4 flows simultaneously. (Note: normal test applications do not operate during high resolution traffic monitoring.)

■ Real-Time Disk Logging

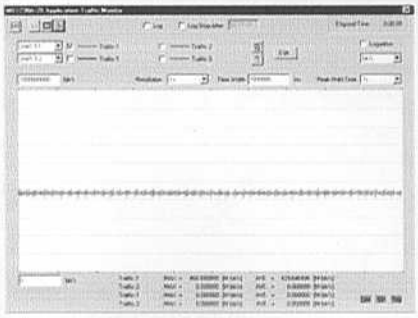
Monitored 1 ms traffic counts are logged to the hard drive in real time. The log results are exported in CSV format, and graphics can be displayed with regeneration software.

■ Robust Trigger Function

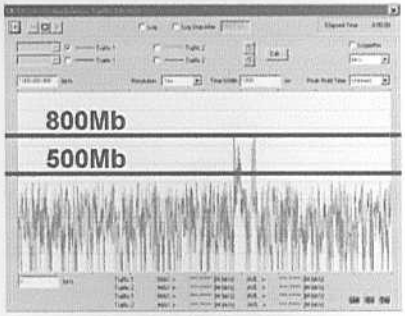
With the High Resolution Traffic Monitor, the trigger for data capture is traffic exceeding a specified level. 1 ms resolution captures sudden peaks that are ignored when the monitoring resolution is only 1 second.



Application Examples



Case 1 (No Problem)
500 Mb data is sent on a 500 Mb bandwidth link. Traffic monitoring at one second intervals is sufficient.



Case 2 (Bandwidth Problem)
Video data with 800 Mb peaks is sent on a 500 Mb link, leading to occasional traffic loss. The network manager has to ascertain the cause of the problem and configure the network properly.

Case 3 (Bandwidth Problem)
1 ms monitoring on this link shows that there is alternating 20 Mb and 600 Mb data, although the average bandwidth is 500 Mb. The solution will require a with 600 Mb bandwidth link or the use of data smoothing.

Errors in video stream delivery, such as stream peaks and lack of sufficient bandwidth, can be found easily by measuring traffic stream details with 1 ms monitoring.

Specifications

MD1230A-20/MD1231A-20, MX123001A-20 Application Traffic Monitor	
Measurement Resolution	1 ms
Display Resolution	1 ms/10 ms/100 ms/500 ms/1 s
IP Packets	IPv4, IPv6 (including L2 tag)
Log Storage	Depends on file system and HDD space File System: Theoretical/Guaranteed values FAT16: 15.6 hours / 15 hours FAT32: 19 hours / 30 hours NTFS: 1193 hours / 400 hours
Graph	Vertical: Monitored value Horizontal: Time
Operation	MD1230A Mainframe External PC (via Ethernet/IP)

Modules Supported	MU120112A 2-Port GbE
Ports	MAC Address, IP Address Netmask, Gateway
Duplex Mode	Full duplex
Flow Control	On/off, Direct Address, Multicast, Port Address

External PC Minimum Requirements for MX123001A-20	
Architecture	Compatible with IBM-PC/AT
CPU	Intel Pentium II 400MHz
OS	Windows 98/2000 (Japanese/English)
Memory	64 MB (128 MB recommended)
Disk Space	50 MB (plus log file capacity)

Ordering Information

Model/Order No.	Item	Requirements
MD1230A-20	High Resolution Application Traffic Monitor Option	Use of MD1230A and MU120112A GbE Module
MD1231A-20	High Resolution Application Traffic Monitor Option	Use of MD1231A and MU120112A GbE Module
MX123001A-20	High Resolution Application Traffic Monitor Option for MX123001A Remote PC Control Software	Installation of MX123001A/-05/-08 Remote PC Control Software
Optional Accessories		
W2134AW	Traffic Monitor Operation Manual	

Microsoft and Windows are trademarks or registered trademarks of Microsoft Corp. in the U.S. and/or other countries. Pentium is a registered trademark of Intel Corp. Other company and product names in this document are trademarks or registered trademarks of their respective owners.