ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

TESINA DE SEMINARIO

"Diseño de seguridad en una Red GEPON orientada a servicios X-Play"

Previa a la obtención del Título de:

INGENIERO EN COMPUTACIÓN
ESPECIALIZACIÓN SISTEMAS MULTIMEDIA

INGENIERO EN COMPUTACIÓN
ESPECIALIZACIÓN SISTEMAS INFORMACIÓN

INGENIERO EN COMPUTACIÓN
ESPECIALIZACIÓN SISTEMAS MULTIMEDIA

Autoras:

MARGIE DENISSE CERVANTES VALENCIA
DOLORES MARGARITA PESANTEZ PESANTEZ
GIOMAYRA OFELIA ROSALES BASANTES

Guayaquil – Ecuador

2011

AGRADECIMIENTO

A Dios por brindarnos salud, vida, esperanza, sabiduría y por permanecer siempre a nuestro lado en cada paso dado para cumplir esta meta.

A nuestras familias por ser el pilar fundamental en nuestras vidas, que siempre nos apoyan con su incondicional amor, consejos y paciencia.

Al Ingeniero Alfonso Aranda e Ingeniera Patricia Chávez por su constante colaboración en la realización, revisión y culminación del Proyecto.

Las Autoras

DEDICATORIA

A Dios, mis padres, mi abuelita, y hermanos, quienes siempre han estado a mi lado durante toda mi etapa estudiantil, brindándome los consejos y el apoyo necesarios para culminar con éxito mi carrera profesional.

MARGIE

A Dios que me ha dado la oportunidad de llegar a culminar esta etapa de mi vida, a mis padres, hermanos y tíos quienes siempre han estado a mi lado y han sido un pilar fundamental en mi vida y mi carrera estudiantil, por su constante apoyo les agradeceré siempre.

DOLORES

A mis padres y hermanos quienes con su apoyo incondicional me han ayudado y brindado sus sabios consejos, a mis amigas de proyecto por su gran Amistad y colaboración.

GIOMAYRA

TRIBUNAL DE SUSTENTACIÓN

Ing. Alfonso Aranda

PROFESOR DEL SEMINARIO DE GRADUACIÓN

Ing. Patricia Chávez

PROFESORA DELEGADA POR EL DECANO

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesina de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de exámenes y títulos profesionales de la ESPOL)

MARGIE DENISSE CERVANTES VALENCIA

DOLORES MARGARITA PESANTEZ PESANTEZ

GIOMAYRA OFELIA ROSALES BASANTES

RESUMEN

El desarrollo de este proyecto se lo ha dividido en seis capítulos que se detallan a continuación:

En el primer capítulo, se redacta la definición de los problemas que se presentan en una red GEPON, los objetivos generales y específicos, la justificación, alcances y limitaciones que se presentan en la red.

En el segundo capítulo, se ha realizado una introducción teórica de los componentes, protocolos y características de los servicios cuádruple-play los cuales son internet, IPTV, telefonía IP y video vigilancia; así como también una descripción del funcionamiento de cada uno de estos servicios.

En el tercer capítulo, se presenta un estudio de las tecnologías GEPON, se mencionan las características técnicas, arquitectura, elementos que incluyen en una red GEPON, protocolos que utilizan estas tecnologías, la forma en la que trabajan como tecnología de última milla, los beneficios que presentan como reemplazo de las formas de comunicación actuales y el futuro que tienen estas tecnologías como tecnologías de última milla.

En el cuarto capítulo, se menciona las vulnerabilidades, consecuencias y soluciones que se pueden presentar en los servicios cuádruple-play con

relación a cada una de las capas del modelo TCP/IP, así como también los diseños de posibles ataques con sus respectivas soluciones que se pueden presentar en cada una de las capas de una red GEPON; las cuales son: Red Núcleo, Red Metro y Red Acceso en donde se encuentran alojados cada uno de los equipos que administran los servicios cuádruple-play.

En el quinto capítulo, se presentan los diferentes sistemas de gestión con sus respectivas características y requerimientos necesarios para su uso, que pueden utilizarse para administrar una red GEPON.

En el sexto y último capítulo, se ha realizado el diseño respectivo de la red describiendo el posible dimensionamiento, ubicación y distribución de cada uno de los equipos en la red GEPON.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

ÍNDICE DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 6

ABREVIATURAS

-A-

ACL: Access Control List – Lista de Control de Acceso

ADSL: Asymmetric Digital Subscriber Line – Línea de Abonado Digital Asimétrica

AES: Advanced Encryption Standard – Estándar de Cifrado Avanzado

APON: ATM Passive Optical Network – Red Óptica Pasiva ATM

ATM: Asynchronous Transfer Mode – Modo de transferencia Asíncrono

-B-

BPON: Broadband Passive Optical Network – Red Óptica Pasiva Banda Ancha

-C-

CLI: Command Line Interface – Interfaz de Línea de Comando

CMIP: Common Management Information Protocol – Protocolo de administración de información común

CO: Central Office – Oficina Central

CORBA: Common Object Request Broker Architecture – Arquitectura Común de Intermediarios en Peticiones a Objetos

CWDM: Coarse Wavelength Division Multiplexing – Multiplexación por División en Longitudes de Onda Ligeras

-D-

DBA: Dynamic Bandwith Allocation – Asignación dinámica de ancho de banda

DES: Data Encryption Standard – Estándar de cifrado de datos

DSL: Digital Subscriber Line – Línea de Abonado Digital

DVR: Digital Video Recorder – Grabadora Digital de Video

DWDM: Dense Wavelength Division Multiplex – Multiplexión por división de Longitud de Onda Densa

-E-

EFM: Ethernet in the First Mile – Ethernet en la Primera Milla

EMS: Element Management System – Elemento de Administración del Sistema

EPON: Ethernet Passive Optical Network – Ethernet de Red Optica Pasiva

-F-

FCS: Frame Check Sequence – Verificación de Secuencia de Frame

FSAN: Full Service Access Network – Servicio Completo de Acceso a Redes.

FTTA: Fiber To The Apartament – Fibra hasta el Apartamento

FTTB: Fiber To The Building – Fibra hasta el Edificio

FTTB/C: Fibra al edificio/a la acometida

FTTH: Fiber To The House – Fibra hasta la Casa

FTTP: Fiber To The Premises – Fibra Hacia los Nodos

-G-

GEM: GPON Encapsulation Method – Método de Encapsulamiento

GEPON: Gigabit Ethernet Passive Optical Network – Gigabit Ethernet de Red Óptica Pasiva

GUI: Graphical User Interface – Interfaz de Usuario Gráfica

GTC: GPON Transmission Convergence – convergencia de transmisión GPON

-H-

HOTV: High Definition Television – Televisión de Alta Definición

-I-

IGMP: Internet Group Management Protocol – Grupo de Gestión del Protocolo de Internet

IP: Internet Protocol – Protocolo de Internet

IPTV: Televisión sobre protocolo IP

-J-

JMX: Java Management Extensions – Extensiones de Gestión Java

-M-

MAC: Media Access Control Address – Control de Acceso al Medio.

MITM: Man In The Middle – Hombre en el Medio

MPCP: Protocolo de Control Multipunto

-N-

NETCONF: Network Configuration Protocol – Protocolo de configuración de red

NMS: Network Management System – Sistema de Gestión de Red

NTSC: Comité Nacional de Sistemas de Televisión

-O-

OAM: Operación y Administración

OAN: Red Óptica de Acceso

ODN: Red de Distribución Óptica

OLA: Operating Level Agreements – Acuerdo del Nivel de Operación

OLT: Optical Line Terminal – Terminal de Línea Óptica

ONT: Red Terminal Óptica

ONU: Optical Network Unit – Unidad Óptica de Red

-P-

P2MP: Topología Punto Multipunto

PAL: Línea de Alternancia de Fase

PC: Computador Personal

PLC: Planar Lightwave Circuits - Circuitos de Onda de Luz Plana

PLOAM: Physical Layer Operations, Administration and Maintenance – Capa física de Operación de Administración y Mantenimiento

PON: Passive Optical Network – Red Óptica Pasiva.

POS: Passive Optical Splitter – Splitter Óptica Pasiva

POTS: Plain Old Telephone Service – Servicio telefónico Ordinario Antiguo

PtP: Point to Point – Punto a Punto

PtPE: Point-to-Point Emulation – Emulación punto a punto

PTZ: Pan, Tilt, Zoom – Inclinación, acercamiento

-Q-

QAM: Quadrature Amplitude Modulation – Modulación de Amplitud en Cuadratura

QoE: Quality of Experience – Calidad de Experiencia

QoS: Quality of Service – Calidad de Servicio.

-S-

SLA: Service Level Agreements – Acuerdos del Nivel de Servicio

SNMP: Simple Network Management Protocol – Protocolo Simple de Administración de Red

SOTV: Standard Definition Television – Televisión de Definición Estándar

SSL: Secure Sockets Layer – Seguridad en capa de conexión

-T-

TDM: Time Division Multiplexation – Tiempo de División y Multiplexación

TL1: Transaction Language 1 – Transacción Idioma 1

TMN: Telecommunications Management Network – Gestión de redes de telecomunicaciones

TCP: Transmission Control Protocol – Protocolo de Control de Transmisiones

TLS: Transport Layer Security – Seguridad en Capa de Transporte

-U-

UDP: User Datagrama Protocol – Protocolo de Datagrama de Usuario

UTP: Cable de Par Trenzado

-V-

VoIP: Voice over IP – Voz sobre IP

-W-

WBEM: Web-Based Enterprise Management – Empresa de Gestión basada en Web

WiMAX: Interoperabilidad Mundial del Acceso por Microondas – World Wide Interoperability For Microwave Access

WMI: Windows Management Instrumentation – Instrumental de Administración de Windows

-X-

XML: Extensible Markup Language – Lenguaje de Marcas Extensible

INTRODUCCIÓN

Empresas de telecomunicaciones en el mundo están en continua competencia en cuanto a brindar un mejor servicio de ancho de banda se refiere, por lo que muchas empresas optan por innovar servicios, inclinándose por redes que utilizan banda ancha basadas en IP, lo que ofrece servicios bajo una misma infraestructura y a precios cada vez más competitivos, y con una considerable reducción de inversión en el equipamiento de red.

Entre las tecnologías más interesantes del momento, tenemos a GEPON, que es una tecnología de acceso mediante fibra óptica con arquitectura punto a multipunto más avanzada en la actualidad.

La tecnología GEPON es nueva para nuestro país, admite servicios X-Play como voz, TV digital, Video Seguridad, Video bajo Demanda, Datos e Internet por medio de fibra óptica con una conectividad de alta velocidad y costos mínimos de instalación, para esta tesis nos enfocaremos en servicios Cuádruple-Play.

La implementación de una red GEPON permitirá a los proveedores de internet maximizar el valor de sus activos, atraer nuevos clientes y mantener a sus actuales clientes, ofreciéndoles más servicios y de mejor calidad a

precios competitivos, con una inversión reducida en el equipamiento y mantenimiento de la red.

Sin embargo en el mundo real encontramos factores económicos, legales y tecnológicos que provocan ciertos escenarios como: Obligaciones regulatorias con sus respectivas consecuencias: Necesidad de interoperabilidad entre terminales de distintos operadores, el diagnóstico del buen funcionamiento de los tramos y entre otros factores que hacen que una red GEPON no sea segura.

Por tal motivo se propone como Proyecto el Diseño y Seguridad de una Red GEPON para servicios Cuádruple-Play, partiendo del análisis de los diferentes servicios Cuádruple-Play, los Tipos de Redes, Protocolos, la Arquitectura, Diseño y Seguridad de una Red GEPON aplicando el Ciclo de Deming.

CAPÍTULO 1

1. PLANTEAMIENTO DEL PROYECTO

1.1 DEFINICIÓN DEL PROBLEMA

Debido a que la tecnología GEPON es nueva en nuestro país, aun está sujeta a muchas vulnerabilidades, y antes de considerar montar una red GEPON en nuestra ciudad, debe realizarse un análisis de todos los posibles ataques de los que podría ser víctima y a su vez proponer posibles soluciones a cada uno de estos; con esa finalidad se propuso este tema de tesis.

Una vez llevado a cabo este estudio, se podría dar paso a montar la red con el fin de prestar un mejor servicio a los usuarios en términos de velocidad, seguridad, variedad de servicios, costos y tiempo.

1.2 OBJETIVOS GENERALES

Analizar todas las vulnerabilidades que materializan los posibles ataques y violaciones a la información y los recursos presentes en una red GEPON, con el fin de obtener una red segura que conserve

y proteja la alta Disponibilidad, Confidencialidad e Integridad de los servicios Cuádruple play hasta el usuario final o usuario home.

Proporcionar información oportuna, precisa y concisa, que pueda ser bien interpretada por los administradores de la red para que apliquen la mejor solución o contramedida antes y después de cualquier intento de ataque, evitando numerosas pérdidas para las empresas que proveen y utilizan los servicios cuádruple play.

1.3 OBJETIVOS ESPECÍFICOS

Para llegar al objetivo general se definieron los siguientes objetivos específicos:

- Estudiar el ambiente actual de seguridad (disponibilidad, integridad, confidencialidad) de la red GEPON.

- Definir el mejor diseño y plataforma de una red GEPON.

- Comprensión y manejo de las tecnologías de acceso multimedia, altamente utilizadas en la actualidad.

- Analizar todos los posibles puntos frágiles de ataque en una red GEPON proponiendo respectivas soluciones.

- Mantener los sistemas generando resultados.

- Conocer los diferentes tipos de amenazas que puedan presentarse en todos los activos de la empresa, para reconocer su importancia y permitirnos minimizar el impacto que provocan.

- Identificar los diferentes tipos de puntos débiles de los activos y conocer como éstos pueden permitir que las amenazas alteren la disponibilidad, confidencialidad o integridad de la información.

- Impedir que las amenazas exploten los puntos débiles de la red.

1.4 JUSTIFICACIÓN

Es necesario realizar un estudio profundo basado en todos los posibles ataques a los que la red GEPON es susceptible, esto lo lograremos analizando cada una de las posibles vulnerabilidades que podrían presentarse en los equipos de la red, en las configuraciones, en los protocolos que emplea, en los servicios que presta ya sea internet, IPTV, telefonía IP y video vigilancia, provocando de esta

manera que la red se comporte de una forma débil a los diferentes ataques.

Una vez analizados todos los posibles puntos recomendaremos soluciones a dichas vulnerabilidades que logren que la red GEPON sea robusta y finalmente, esta tesis quedará a disposición para que puedan considerarse todos los requisitos necesarios para armar una red GEPON sólida.

1.5 ALCANCES Y LIMITACIONES

Esta tesis esta básicamente enfocada al análisis de todas las posibles vulnerabilidades que pueda presentar la red GEPON con servicios cuádruple-play y proporcionar soluciones a cada una de las mismas. Nuestra finalidad al término de esta tesis es proveer un estudio que garantice una Red GEPON Segura.

Todo este estudio lo vamos a llevar a cabo a través de investigaciones, consultas y análisis. Tenemos el factor económico como una limitación en esta tesis; debido al costo que implica montar una red GEPON, aproximadamente $169000, en el capítulo de pruebas no se harán pruebas sino un esquema de análisis.

CAPÍTULO 2

2. SERVICIOS X-PLAY

2.1 INTRODUCCIÓN

A lo largo de esta tesis nos vamos a enfocar en los servicios "Cuádruple-play", de los cuales se va a detallar las principales características que engloban estos cuatro servicios.

El concepto de Cuádruple-play identifica la presencia de los servicios de internet, IPTV, telefonía IP y Video vigilancia IP, sobre una infraestructura común de transmisión de datos o IP.

El servicio Cuádruple-play es el futuro cercano para el desarrollo integral de comunicación entre hogares. Propone una solución única para varios problemas, todo en un mismo servicio.

2.2 ¿QUÉ SON LOS SERVICIOS CUÁDRUPLE-PLAY?

El cuádruple-play se define como el empaquetamiento de servicios y contenidos audiovisuales. Lo que diferencia a esta nueva tecnología

de las anteriores radica en que todos los servicios están contenidos por un único soporte físico, ya sea cable coaxial, fibra óptica, cable de par trenzado, red eléctrica, o bien microonda (1).

Una red única reduce gastos de operación, mantenimiento y gestión de la red. Permite que se sumen de una forma rápida y eficiente de nuevos servicios, arrastrando más ventajas competitivas (2).

2.3 DESCRIPCIÓN DE LOS SERVICIOS

Los servicios de datos, video y voz tienen requisitos de calidad y características distintas entre todos ellos, que podemos resumir en:

2.3.1 TELEFONÍA IP

En este apartado apreciaremos el funcionamiento técnico de la tecnología de voz sobre IP, la formación de la trama de VolP que transporta los paquetes de voz y como efectuar el cálculo del ancho de banda necesario para soportar una aplicación de telefonía IP (1).

2.3.1.1 FUNCIONAMIENTO TELEFONÍA IP

La tecnología de voz sobre el protocolo de Internet conocida como telefonía IP (voice over IP), se fundamenta en transportar la voz mediante las redes de comunicaciones encapsuladas en paquetes IP (1).

La voz humana se traslada mediante una señal analógica, por ende para poder enviarla a través de un medio digital basado en la conmutación de paquetes como es Internet, se requiere un proceso previo para convertirla en una señal digital.

El proceso de digitalización de la señal se realiza mediante un códec de audio. El códec sirve para comprimir el tamaño del paquete de voz digitalizado y conseguir mayor eficiencia en el transporte de datos (stream). Existen diferentes tipos de códecs de audio, cada uno con sus características específicas. En la tabla 2.1 podemos ver algunos de los códecs de voz:

Códec	Tasa de Bits	Tasa de Muestreo	Retardo Paquetización
G.711	64 Kbps	0,125 ms	20 ms
G.723	64 Kbps	0,30 ms	30 ms
G.726	32 Kbps	125 ms	20 ms
G.728	16 Kbps	625 ms	20 ms

Tabla 2.1.Descripción códecs de voz (1)

Después de tener el códec de voz procesado, se ha de encapsular con las cabeceras correspondientes de todos los protocolos, que se usan para la transmisión del paquete.

El primer nivel de encapsulamiento que se realiza es el del Protocolo de Transporte en Tiempo real (Real-time Transport Protocol). Este protocolo, se utiliza en sistemas de comunicación, entretenimiento y aplicaciones que requieren parámetros de funcionamiento en tiempo real, con lo cual encaja perfectamente con el servicio de telefonía, su función principal es implementar los números de secuencia de paquetes IP para reconstruir la información de voz o video en el destino incluso si la red cambia el orden de los paquetes.

El siguiente nivel de encapsulamiento es el de Protocolo de Datagrama de Usuario (UDP, User Datagrama Protocol), este protocolo ofrece un mecanismo para enviar datagramas IP a través de la red sin que haya establecido una conexión y con relación a TCP tiene un mayor ancho de banda y es mejor para el envío de paquetes pequeños, como el caso de la voz.

Posteriormente se encapsula con el protocolo de Internet (IP) y finalmente se realiza lo mismo con el nivel de enlace de datos, que en este caso será Ethernet. La trama final de VoIP quedaría como se muestra en la figura 2.1:

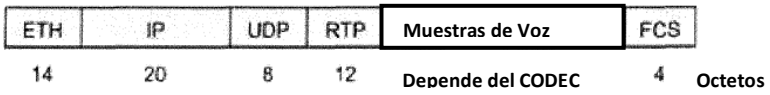

Figura 2.1. Formato trama VoIP (1)

En el libro de Análisis y Evaluación Comparada de redes de acceso GPON Y EP2P (1), Arquitectura de Computadores, José Torres expresa cabalmente los beneficios de este tipo de redes: “En el lado del receptor se desencapsula el paquete con los protocolos aplicados en orden inverso al del envío, y posteriormente se descomprime y se hace la conversión digital-analógica del paquete resultante para obtener la voz que se envió” (1).

2.3.1.2 CÁLCULO ANCHO BANDA REQUERIDO PARA TELEFONÍA IP

El ancho de banda que se requiere para una aplicación de Telefonía IP, depende de dos factores principales (1):

a) El códec de voz utilizado.

b) Número de paquetes de audio enviados dentro de una misma trama de telefonía IP.

Los paquetes de voz se caracterizan por utilizar un ancho de banda limitado. Si se usa el códec básico G.711, la tasa de bits será de 64 kbps, pero a medida que se van usando códecs más avanzados, esta tasa se puede reducir hasta los 4 kbps; se recomienda utilizar concretamente G.723 ya que su alta comprensión ofrece una mejor calidad. La fórmula que aplicaremos para el cálculo del ancho de banda de cada canal de voz será la siguiente (1):

Ancho Banda (kbps) = paquetes enviados por segundo x número bytes de trama VolP

Los factores que pueden afectar de manera más significativa la calidad del servicio son el retraso y el jitter. Es recomendable para el servicio telefónico retardos inferiores a 400 ms (3).

2.3.2 TELEVISIÓN IP (IPTV)

La Televisión por Protocolo de Internet conocida como Televisión IP (IPTV, Internet Protocol Television), detalla los servicios por los cuales se puede recibir la señal de televisión o vídeo a través de la conexión de banda ancha a Internet (1).

En este servicio se transmiten grandes volúmenes de datos y, puede llegar a presentar conflictos con el jitter y los retardos. Comúnmente este servicio suele ir de la mano del audio, por lo que se necesita sincronización entre el audio y el vídeo (3).

Dentro de lo que comprende el servicio de IPTV, hay dos tipos de datos a transmitir:

- Datos para un cliente a la vez, este tipo de tráfico se llama unicast IP, es más común en la red ya que es el que se usa para navegar, leer el correo, etc. Por ejemplo un programa a la carta, un usuario decide comprar y ver en un momento dado una película o un programa ya pasado (3). En la figura 2.2 podemos observar un ejemplo de transmisión Unicast.

- Datos vistos por múltiples usuarios simultáneamente, este tipo de tráfico se llama multicast IP. Este tráfico se caracteriza por tener un único flujo entrante por el cual puede transmitir varias interfaces de salida a la vez, permitiendo así ahorrar tráfico en los enlaces troncales. Por ejemplo la televisión actualmente, sería la emulación de un sistema broadcast (3). En la figura 2.3 podemos observar un ejemplo de transmisión Multicast.

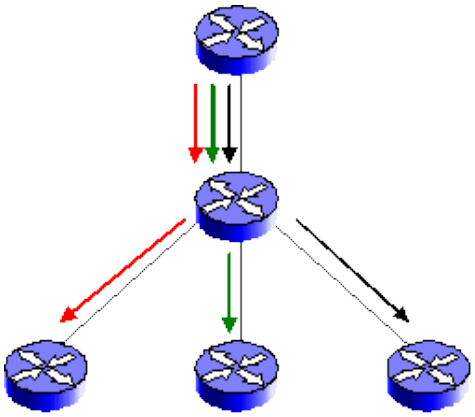

Figura 2.2. Transmisión Unicast (3)

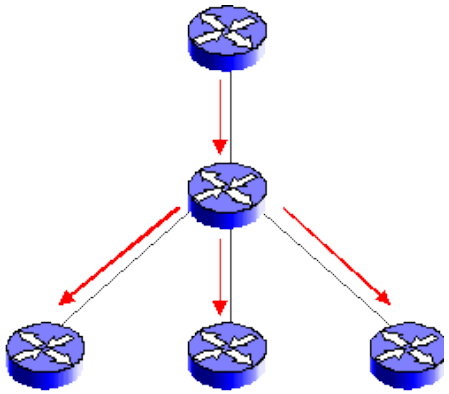

Figura 2.3. Transmisión Multicast (3)

2.3.2.1 TIPOLOGÍA DE CANALES

La tecnología IPTV requiere alta velocidad para poder cumplir con los requerimientos técnicos que demanda y poder garantizar la calidad en el servicio. Por lo que es aconsejable el uso de la fibra óptica para el desarrollo de este servicio.

La televisión IP se ha desarrollado en base al denominado video-streaming, del cual se diferencian dos tipos de canales (1):

a) **Canal de definición estándar SOTV:** señales de televisión con una resolución de 720x576 pixeles en PAL. Para su transmisión por Internet con MPEG4 se necesita un ancho de banda de 1.5Mbbps

b) **Canales de alta definición HOTV:** señales de televisión con resoluciones de 1280x720 o 1920x1080 pixeles. Para su transmisión por internet con MPEG4 se necesita un ancho de banda de 8Mbps.

2.3.3 INTERNET BANDA ANCHA

El funcionamiento principal del Internet, es transportar varios canales de información por un mismo medio de transmisión, esta técnica se la denomina multiplexación, de la cual existen varios tipos, según como se haga la distinción de los canales de comunicación (1):

a) **Distinción en Tiempo:** cada usuario recibe el ancho de banda total por una fracción o intervalo de tiempo.

b) **Distinción por frecuencia:** cada usuario recibe un rango de frecuencia para las transmisiones (comunicaciones inalámbricas).

c) **Distinción de la longitud de onda:** cada usuario recibe una longitud de onda para las transmisiones (transmisiones ópticas).

d) **Distinción de código:** cada usuario recibe un código que utiliza para filtrar la información que le transmiten y quedarse solamente con la destinada a él.

2.3.4 VIDEOVIGILANCIA IP

Video Vigilancia IP o IP Video Surveillance es una de las más recientes tecnologías de seguridad que se ofrece a través del Protocolo de Internet; gracias a los avances informáticos y el aumento de velocidad de ancho de banda en las redes se ha permitido transmitir videos digitalizados en tiempo real con el fin de brindar una mejor seguridad a personas, comunidades, pymes y organizaciones como centros comerciales, supermercados, hoteles y hasta los hogares.

Los sistemas de Video Vigilancia IP permiten administrar las cámaras IP con un software de gestión de video, visualizar el área vigilada, almacenar las grabaciones, detectar movimiento, activar alarma contra robo, incendios y otros eventos desde cualquier lugar y a toda hora con solo tener acceso a un ordenador conectado a internet.

Las cámaras IP compatibles a este sistema de seguridad pueden ser de diversos tipos: cableadas, inalámbricas, fijas, móviles además de poseer micrófono incorporado, para uso interior y exterior.

2.3.4.1 CARACTERÍSTICAS DE VIDEOVIGILANCIA IP

La demanda por los sistemas de Video Vigilancia IP ha aumentado por los beneficios que se mencionan a continuación:

- Permite acceder a los videos desde cualquier lugar de la red, como un Centro de Seguridad o sitios remotos a través de Internet.

- Los videos pueden ser transmitidos en redes privadas y por internet mediante el Protocolo de Internet (IP, Internet Protocol).

- Se puede ajustar el video a diferentes tasas de datos para adaptarse al ancho de banda disponible para cada abonado.

- Se puede emplear cámaras IP inalámbricas para áreas en las que resulta difícil o costoso instalar cables.

- Procesamiento inteligente de eventos mediante el software de administración de video, como detección de movimiento hasta algoritmos avanzados de seguimiento de objetos.

- Se adapta a la infraestructura tecnológica para reducir costes y mejorar la escalabilidad y la confiabilidad de las grabadoras de video digitales cerradas.

- Posee aplicaciones de software de Administración integradas que incluyen control de accesos, y sistemas anti-intrusión, anti-incendios, video y negocio con las aplicaciones de transacciones, como el punto de ventas y la lectura de barras.

- Mejora la calidad de video con respecto al video analógico, las cámaras digitales son compatibles con resoluciones en varios megapíxeles.

- La búsqueda de las imágenes se realiza de forma rápida, directa y eficiente.

- La transferencia de video por las redes IP puede ser cifrado para evitar que sean interpretados por terceros.

- Alimentación eléctrica a través de Ethernet

- Acceso a múltiples usuarios autorizados quienes pueden observar simultáneamente en cualquier momento, desde cualquier lugar la misma cámara IP.

- Los costos de instalación y mantenimiento son más eficientes en costo que los sistemas análogos.

- La conexión con teléfonos celulares 3G permite un sistema móvil de vigilancia en la palma de la mano.

2.3.4.2 COMPARACIÓN DE TECNOLOGÍAS VIDEO IP Y DVR

En esta sección se realiza una comparativa entre las características de los sistemas de vigilancia analógico que incluye cámaras análogas, grabaciones basadas en servidores y Grabadores de Video Digital (DVR, Digital Video Recorder) y los sistemas de video vigilancia basado en IP que incluyen cámaras IP o de red, infraestructura IP, servidores, software de gestión de video y almacenamiento. (4)

Escaneo de imagen: En un sistema DVR el escaneo de una imagen se realiza de manera entrelazada; donde para cada

cuadro de imagen se requiere de campos pares para las líneas horizontales pares y campos impares para las líneas horizontales impares estos campos se entrelazan secuencialmente (un campo par seguido de un campo impar) para componer la imagen completa; cuando hay presencia de objetos en movimientos rápidos surgen retrasos entre las actualizaciones de las líneas pares e impares provocando una distorsión y pérdida de nitidez de la imagen. Mientras que en un sistema con cámaras IP se realiza un escaneo progresivo que utiliza sensores para escanear y transferir la imagen completa línea a línea solucionando la pérdida de nitidez de los sistemas DVR.

Resolución: La resolución de una imagen en un sistema análogo esta dado en términos de líneas de televisión (TV, Television) los estándares de video analógico de Comisión Nacional de Sistema de Televisión (NTSC, National Television System Committee) y analógico de Línea de Fase Alternada (PAL, Phase Alternating Line) tienen una resolución de 480 y 576 líneas horizontales, cuando las líneas de TV se digitalizan tienen un tamaño máximo de 704x480 píxeles en NTSC y de 720x576 píxeles en PAL, mientras que en los sistemas con

cámaras IP. La resolución de las imágenes pueden llegar hasta 2596x1944 pixeles (5 Mega pixeles). Las resoluciones en megapixeles son muy valiosas en los sistemas de video vigilancia porque con una imagen de alta resolución se puede identificar a un delincuente.

Cableado: En un sistema DVR se debe tender un cable coaxial por cámara, mientras que los sistemas con cámaras IP hacen uso de un solo cable para la transferencia de audio y video. Las cámaras se alimentan sobre la red Ethernet reduciendo la cantidad de cables de alimentación y pueden re-utilizar cableados existentes de red; solo se necesita un Cable Par Trenzado sin Apantallar (UTP, Unshielded Twisted Pair) para poder transportar a través del protocolo IP el video de múltiples cámaras.

Analíticas: Con la aparición de las cámaras IP son muchos más los análisis que se pueden hacer a un video como: Reconocimiento de rostros, reconocimiento de vehículos, contar objetos en movimiento que permiten automatizar y mejorar un sistema de video vigilancia con el fin de aumentar la seguridad, reduciendo las necesidades de ordenadores potentes y costosos

para descomprimir y analizar el video digital cuando el mismo software de gestión de video puede indicar cualquier anomalía a las personas adecuadas en cualquier momento.

Integración: Los sistemas de seguridad que tienen un software de gestión de video permiten integraciones ilimitadas donde se pueden acoplar muchos eventos como detección de movimiento, alarmas contra robos e incendios y otras características inteligentes que se requieran integrar para tener un mejor control. Estas integraciones permiten que los sistemas de vigilancia sean escalables y más flexibles.

Seguridad: En los sistemas analógicos el video transferido por el cable coaxial puede ser interceptado por un monitor o DVR, mientras que en un sistema de cámaras IP antes de transferir el video se lo cifra de tal manera que solo puede ser reproducido cuando se ingrese la contraseña correcta de reproducción, también se puede autentificar las conexiones con la cámara, además a cada cuadro de video se lo puede asignar una identificación para establecer y garantizar su autenticidad.

La tabla 2.2 resume las comparativas entre los sistemas de video vigilancia análogos e IP.

Característica	Video IP	DVR
Escaneo de imagen	Progresivo	Entrelazado
Resolución	Multi-Megapixel	0.4 Megapixel
Cableado	Cable único para audio, video, alimentación y control PTZ	Se requieren múltiples cables
Analítica	Implementada en la cámara	Implementada en el servidor
Integración	Aplicaciones de software abiertas que funcionan con una multitud de equipos y aplicaciones de software	Sistemas estándares privadas con capacidad de integración limitada
Seguridad	Transferencia de video cifrado	No hay cifrado en la transferencia

Tabla 2.2. Comparación de Tecnologías Video IP y DVR

2.3.4.3 COMPONENTES DE UN SISTEMA DE VIDEOVIGILANCIA IP

Actualmente los componentes que conforman un sistema de video vigilancia IP, poseen características digitales donde la información por su naturaleza es más flexible, segura y fiable. (5) En un sistema de Video Vigilancia IP intervienen los siguientes componentes:

- Una red de cámaras de seguridad (fijas y domos) de video digital de alta definición, con tecnología IP y su correspondiente infraestructura física. Esta red debe contar con las características mínimas de seguridad y cifrado.
- Servidores de almacenamiento de imágenes, puestos de visualización o acceso a internet para visualizar el video en tiempo real.

- Centro de monitoreo desde el cual se accede a cada uno de los puntos de captura, sin importar su ubicación o distancia.

- Una Plataforma de Gestión de video que permita operar y administrar todo el sistema, capaz de detectar a usuarios y todos los componentes instalados en la red.

2.4 TECNOLOGÍAS

En esta sección se describen a las tecnologías para transmitir los servicios de la familia X-Play, tanto la tecnología de la Línea de Abonado Digital Asimétrica (ADSL, Asymmetric Digital Subscriber Line), la más utilizada actualmente para la conexión a internet de banda ancha, la tecnología Fibra Hasta el Hogar (FTTH, Fiber To The Home), que surge ante la necesidad de un ancho de banda

superior para compartir, vender y comprar servicios X-Play, esta tecnología será utilizada para el estudio y análisis de la Red Óptica Pasiva Gigabit-Ethernet (GEPON, Gigabit Ethernet Passive Optical Network) que se propone en la tesis para brindar un mejor servicio y tener un mayor alcance.

2.4.1 TECNOLOGÍA ADSL

Línea de Abonado Digital Asimétrica (ADSL, Asymmetric Digital Subscriber Line) (6) es una tecnología que permite transmitir datos a través de las líneas telefónicas convencionales (cables de cobre) a una velocidad desde 512 Kbps hasta 4 Mbps, se la denomina asimétrica debido a que la velocidad de transmisión de datos de subida y de bajada no es la misma en una conexión a internet, por lo general la velocidad de bajada suele ser mayor que la de subida. Además permite la conexión a internet sin problemas de interferencia por llamadas telefónicas dado que la voz y los datos son transmitidos por canales diferentes.

El ADSL consiste en modular la señal de datos a ser transmitida en una banda de frecuencia alta mediante un ruteador ADSL. Requiere del uso de filtros denominados divisores ópticos o splitter

para evitar distorsiones al transmitir las señales; este dispositivo se encarga de dividir la señal telefónica (baja frecuencia) de las señales de datos moduladas (alta frecuencia).

En el blog Actualidad (7), el administrador del blog, FTTH: la fibra óptica llega hasta el hogar, expresa exactamente que la tecnología FTTH ofrece un ancho de banda superior al que ofrece la tecnología ADSL: “En estos últimos 10 años la tecnología ADSL ha sido la más utilizada para la conexión a Internet de banda ancha por parte de los hogares españoles, ya que su coste es mucho menor que las inversiones en fibra, equipos y canalizaciones necesarias para cubrir toda las demarcaciones del estado. Pero las nuevas necesidades, cada vez son más evidentes, de compartición y compra de servicios, exigen un ancho de banda muy superior, y de momento sólo el FTTH (Fiber To The Home) puede ofrecerlo.”

2.4.1.1 VENTAJAS E INCONVENIENTES DE LA TECNOLOGÍA ADSL

A continuación se presenta las ventajas e inconvenientes de la tecnología ADSL que más adelante ayudarán en la orientación

para seleccionar la tecnología por la cual se debe transmitir los servicios X-Play. (6)

Ventajas

- Permite realizar llamadas telefónicas mientras se navega por Internet.
- Permite una conexión permanente al internet.

- Usa la infraestructura existente de la red telefónica básica lo cual implica menos costo y tiempo invertido para implementar esta tecnología.

- Ofrece una velocidad de conexión mucho mayor que la obtenida mediante marcación telefónica a Internet.

- La posibilidad de usar la telefonía IP para llamadas de larga distancia, hace que el servicio telefónico básico se ofrezca actualmente por las operadoras como un servicio añadido.

Inconvenientes

- No todas las líneas telefónicas pueden ofrecer este servicio.

- No se pueden emplear líneas en mal estado (presencia de atenuaciones y ruidos), con mala calidad del cableado o cuyos abonados se encuentran a mucha distancia de la central, el límite teórico para un servicio aceptable equivale a 5,5 km.
- El ruteador o módem necesario para disponer de conexión es caro. Una solución es que los proveedores del servicio de internet subvencionen los dispositivos, este caso ya se da en algunos países.

- En la mayoría de los casos se requiere de una línea telefónica para su funcionamiento.

- Los servicios X-Play requieren una alta velocidad para ser transmitidos con una excelente calidad de servicio.

Muchos abonados conocen las características que ofrece la tecnología ADSL pero muchos de ellos no conocen las tecnologías nuevas en telecomunicaciones que ofrecen acceso a conexiones de banda ancha a mayores velocidades a través de la fibra óptica.

2.4.2 TECNOLOGÍA FTTH

En esta sección mencionamos a la fibra óptica dado que es el medio de transmisión de datos que utiliza la tecnología Fibra Hasta el Hogar FTTH, pero nos concentraremos en la tecnología FTTH.

2.4.2.1 FIBRA ÓPTICA

La Fibra de Óptica es el medio de transmisión más avanzado y el único actualmente capaz de brindar los servicios de nueva generación con alta disponibilidad y calidad, permite enviar gran cantidad de datos a grandes distancias con transmisiones inmunes a las interferencias electromagnéticas. (8)

Dentro de las principales características de la Fibra Óptica se puede mencionar:

- La cobertura de los hilos de fibra es más resistente.
- Resistencia al agua y emisiones ultravioleta.
- El tiempo de vida de la fibra es confiable y útil.

- Mayor protección en lugares húmedos.

- Empaquetado de alta densidad con menos espacio utilizado y fácil instalación.

Ventajas de la Fibra Óptica sobre el Cable de Cobre

- Mayor ancho de banda.

- Mayores distancias desde la central hasta el abonado.

- Mayor resistencia a la interferencia electromagnética.

- Mayor seguridad de la red.

- Menor degradación de las señales.

- Reducción de repetidores.

- Menor inversión inicial, consumo eléctrico, espacio y puntos de fallo, etc.

2.4.2.2 TECNOLOGÍA FTTH

La tecnología que está comenzando a revolucionar la transmisión de servicios avanzados como: televisión por internet, video bajo demanda, servicios X-Play y servicios futuros los cuales necesitan mayor capacidad de transmisión de la que ofrece la tecnología ADSL (20 Mb/s) es la tecnología Fibra Hasta el Hogar (FTTH, Fiber To The Home), alcanza velocidades de transmisión de 100 megas simétricos (9).

FTTH se basa en la utilización de cables de fibra óptica y sistemas de distribución ópticos adaptados a esta tecnología para la distribución de servicios avanzados, como el Triple Play y Cuádruple Play a los hogares y negocios de los abonados.

En países como Estados Unidos y Japón los operadores están reduciendo la promoción de servicios ADSL en beneficio de la fibra óptica para proponer servicios de banda ancha que requieren alta velocidad de transmisión.

Dentro de los estándares FTTH se encuentran las Redes PON que usan una estructura con una fibra en el lado de la red y varias fibras en el lado usuario.

2.4.2.3 VENTAJAS Y DESVENTAJAS DE FTTH

Ventajas

- Transportar en una única red todos los servicios posibles y abaratar la operación, el mantenimiento y la gestión de la red.

- Tener un solo proveedor de todos los servicios.

- Mejorar la calidad de los servicios, llegando hasta los hogares la calidad digital.

- Facilidad para integrar nuevos servicios y tecnología.

Desventajas

- La unión de los servicios de comunicación en una sola red (basada en IP) podría causar un daño o bien un colapso en todas las vías de comunicación (sea esto por catástrofes naturales, terrorismo, defectos técnicos) debido a que se crea un único punto de falla.

2.4.3 DIFERENCIAS ENTRE FTTH Y ADSL

La tabla 2.3 resume las diferencias entre la tecnología actual ADSL y la nueva tecnología sobre fibra óptica FTTH que permite la transmisión de servicios de última generación. (10)

CARACTERISTÍCAS	FTTH	ADSL
Ventajas en resumen	Alta velocidad Alta seguridad	Facilidad de instalación Bajo costo
Velocidad máxima de descarga(Mbps)	100	50
La distancia al centro de operaciones afecta la velocidad	No	Si
Servicios disponibles de teléfonos IP	Si, con pago únicamente por llamadas realizadas	Si, con pago únicamente por llamadas realizadas
Usuarios (cableados e inalámbricos) simultáneos permitidos	Entre 10 y 50	Hasta 5
Velocidad de subida o de carga para datos de mayor tamaño	Máximo 100 Mbps (mejor esfuerzo)	De 512 Kbps hasta 5 Mbps
Construcción	Se requiere en su ubicación.	La construcción sólo se realiza en el centro de las operaciones de NTT.
Tiempo promedio desde la solicitud hasta el inicio del servicio	De 1 a 2 meses	De 9 a 20 días hábiles

Tabla 2.3 Diferencias entre FTTH y ADSL (10)

CAPÍTULO 3

3. TECNOLOGÍAS Y REDES PON

3.1 REDES PON

Una Red Óptica Pasiva (*Passive Optical Network*) PON es una tecnología de acceso mediante la implementación de una red de fibra óptica que permite reemplazar todos los componentes activos existentes entre el proveedor de servicios y el cliente, por componentes ópticos pasivos para encaminar el tráfico por la red, lo que permite que se reduzcan considerablemente los costes de instalación y mantenimiento (11).

PON es una tecnología punto - multipunto. En las redes PON intervienen elementos que son: Terminal de Línea Óptica (OLT, Optical Line Terminal) o Central Office (CO), localizada en el Proveedor de Servicios; y, la Unidad de Red Óptica (ONU, Optical Network Unit) localizada en el domicilio del usuario. El OLT se interconecta con una red de transporte que recoge los flujos procedentes de varios OLT's y los lleva a la cabecera de la red.

Brindado así servicios llamados FTTx, ya que los acrónimos de éstas tecnologías son FTTH (Fiber To The Home), FTTB (Fiber To The Building) y FTTA (Fiber To The Apartament) conocidas como fibra hasta el hogar, Edificio y Apartamento, respectivamente (11). En la figura 3.1 podemos observar un ejemplo de Arquitectura punto-a-punto vs punto-multipunto.

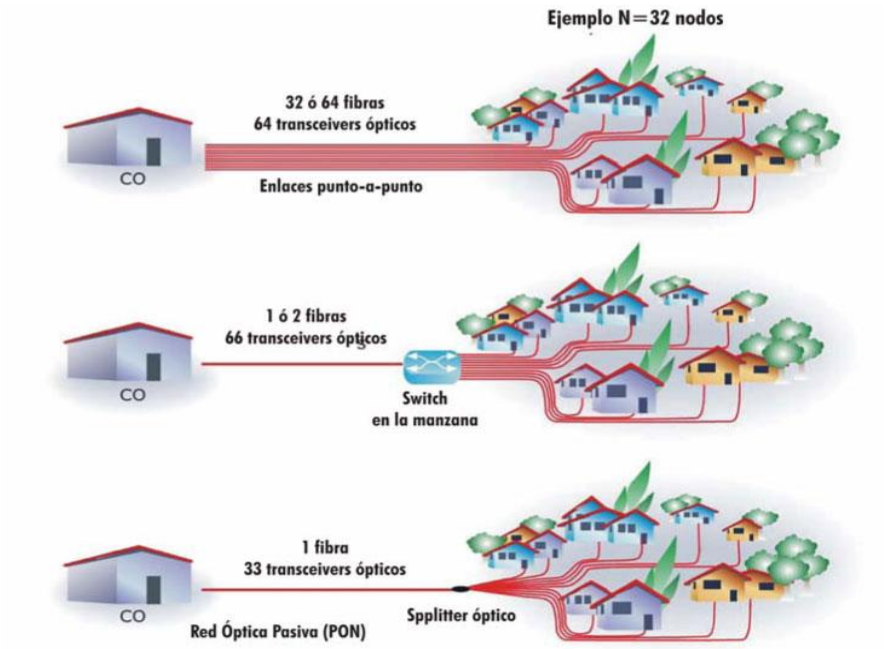

Figura 3.1. Arquitectura punto-a- punto vs punto-multipunto con conmutador en la manzana vs PON (11)

Existen varios tipos de topologías diseñadas para este tipo de red las cuales son (12):

- Las topologías árbol se utilizan en zonas residenciales. Ver figura 3.2.

- Las topologías anillo son poco aplicables, se las utiliza para zonas comerciales. Ver figura 3.3.

- Las topologías Bus son usadas para zonas de campus. Ver figura 3.4.

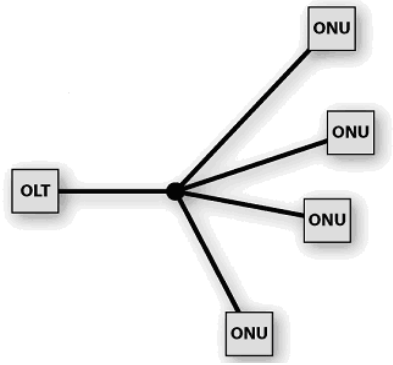

Figura 3.2. Topología Árbol (12)

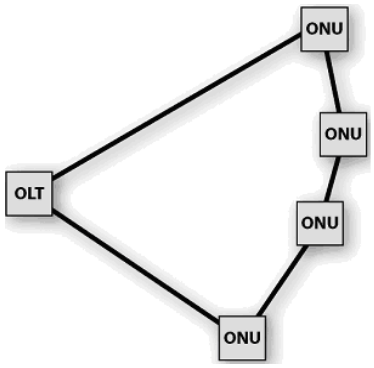

Figura 3.3. Topología Anillo (12)

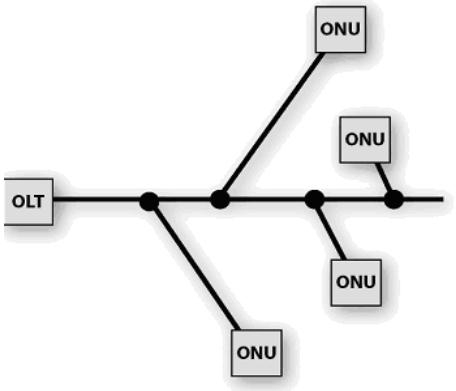

Figura 3.4. Topología Bus (12)

3.2 TIPOS DE REDES PON

Las redes PON se dividen en APON, BPON, GPON, EPON y GEPON.

3.2.1 RED APON

En el libro Tecnologías de redes PON (13), Definición, características y clasificación de redes PON, Juan Sebastián Henao Guevara expresa cabalmente los beneficios de este tipo de redes: “A-PON o ATM-PON (Redes Ópticas Pasivas ATM) está definida en la revisión del estándar de la ITU-T G.983, el cual fue el primer estándar desarrollado para las redes PON. Las especificaciones iniciales definidas para las redes PON fueron hechas por el comité FSAN (Full Service Access Network), el cual utiliza el estándar ATM como protocolo de señalización de la capa 2 (Enlace de Datos). Los sistemas APON usan el protocolo ATM como portador. A-PON se adecua a distintas arquitecturas de redes de acceso, como, FTTH (Fibra hasta la vivienda), FTTB/C (fibra al edificio) y FTTCab” (13). En la figura 3.5 podemos observar un ejemplo de Arquitectura de una red APON.

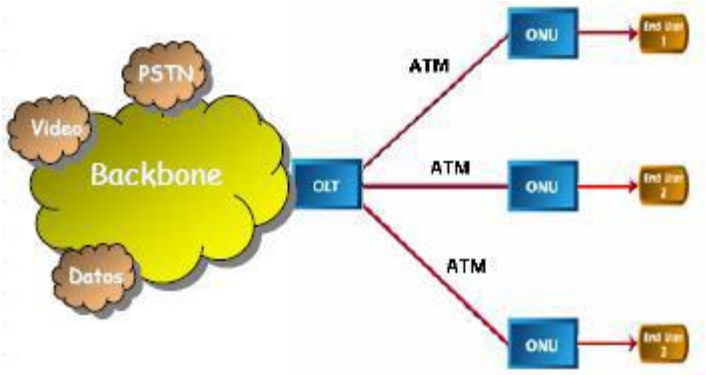

Figura 3.5. Arquitectura básica de una red APON (13)

La transmisión de datos en el canal de bajada (downstream) está formada por ráfagas de celdas ATM de 53 bytes cada una con un identificador de 3 bytes para el equipo generador de la ráfaga (ONU). Estas ráfagas tienen una máxima velocidad bajada de 155.52 Mbps que se reparten entre el número de usuarios que estén conectados al nodo óptico.

Para el canal de subida (upstream), la trama se construye a partir de 54 celdas ATM en las cuales intercalan dos celdas PLOAM (Capa física –administración y mantenimiento) que están designadas a tener información de los destinos de cada celda e información para efectos de operación y mantenimiento de la red.

Dentro de la clasificación de las redes PON existentes, la APON es la que presenta más características en cuanto a OAM (operación y administración).

3.2.2 RED BPON

La tecnología BPON nació como una mejora de la tecnología A-PON para integrar y obtener acceso a más servicios como Ethernet, distribución de video, VPL, y multiplexación por longitud de onda (WDM), obteniendo de esta manera un mayor ancho de banda, entre otras mejoras.

Broadband-PON se especifica en la recomendación ITU-T 983 de las cuales están desde la G.983.1 que es la original de esta tecnología, hasta la G.983.8. En esta tecnología se define una arquitectura de forma simétrica, con un ancho de banda total (canal de bajada + canal de subida) de 155 Mbps.

Esta norma fue modificada en el 2001 para lograr un aumento en las velocidades de transmisión y así permitir arquitecturas asimétricas (155 Mbps de subida y 622 Mbps de bajada).

En el libro Tecnologías de redes PON (13), Definición, características y clasificación de redes PON, Juan Sebastián Henao Guevara expresa cabalmente los beneficios de este tipo de estándar: “Las otras revisiones relacionadas con el estándar son

las siguientes: G.983.2 para la capa de gestión y mantenimiento, G.983.3 para QoS, G.983.4 para la asignación de ancho de banda dinámico, G.983.5 para mecanismos de protección, G.983.6 para la capa de control de red OTN, G.983.7 para la capa de gestión de red para el ancho de banda dinámico, G.983.8 para dar soporte al protocolo IP, Video, VALN y VC" (13).

3.2.3 RED GPON

Gigabit-Capable PON (GPON) tiene como principal objetivo ofrecer un ancho de banda mucho más alto que las anteriores tecnologías, y alcanzar una mayor eficiencia para el transporte de servicios basados en IP. GPON está aprobada por la ITU-T en 4 recomendaciones, la G.984.1, G.984.2, G.984.3 y G.984.4.

Las velocidades manejadas por esta tecnología son de hasta 2,488 Gbps con la posibilidad de tener arquitecturas asimétricas, por lo cual deja al descubierto el gran avance en cuanto a eficiencia y escalabilidad se refiere.

El estándar GPON soporta tasas de transferencia de 2.488 Gbps para el canal de bajada y de 1.244 para el canal de subida. Esto

proporciona velocidades muy altas para los abonados, llegando hacer de hasta 100 Mbps por cada usuario, dependiendo también de factores importantes tales como el número de usuarios y de la calidad de los equipos que se usen, entre otras.

Esta tecnología ofrece OAM avanzado, es decir, grandes facilidades de gestión, operación y mantenimiento, esto se da gracias a que GPON usa su propio método de encapsulamiento (GEM o Método de Encapsulamiento GPON), el cual permite el soporte de todo tipo de servicios.

La arquitectura básica de las Redes GPON está diseñada de un OLT (Línea Terminal Óptica) cerca del operador y las ONT (Red Terminal Óptica) cerca de los abonados con FTTH (13).

3.3 ETHERNET EN PRIMERA MILLA (EFM)

La IEEE 802.3ah fue creada en el 2001 para habilitar el Ethernet en redes de acceso. El estándar Ethernet en la Primera Milla (Ethernet in the First Mile o EFM) fue aceptado en julio de 2004 y un año después se incluyo en el Estándar IEEE 802.3.

El tráfico de Internet comienza y termina como IP y Ethernet, por ello para desarrollar a Ethernet como una tecnología de transporte de red se escoge la primera milla.

El desarrollo de Ethernet en la primera milla permitirá a la gestión de la red beneficiarse de las ventajas de sus equipos instalados, herramientas de administración y análisis (12).

3.4 TOPOLOGÍA ETHERNET EN LA PRIMERA MILLA (EFM)

El estándar Ethernet en la primera milla dispone de dos tipos de tecnologías (12):

- Topología Punto a Punto

- Topología Punto Multipunto

3.4.1 TOPOLOGÍA PUNTO A PUNTO

La topología punto a punto tiene velocidades de hasta 1 Gbps, se identifica por su bajo costo, mayor rendimiento y gran acceso para un ambiente familiar en condiciones normales. Con vista al futuro, la fibra óptica es el medio de transmisión más adecuado por

los beneficios que ofrece para la entrega de datos, voz y video, también usada para el acceso con gran velocidad al Internet, video streaming y telefonía IP.

Esta topología tiene un alcance de hasta 100 Km y funciona con similares condiciones de potencia de Ethernet con cable de cobre, de acceso local inalámbrico, etc (12). En la figura 3.6 podemos observar un ejemplo de Topología Punto a Punto.

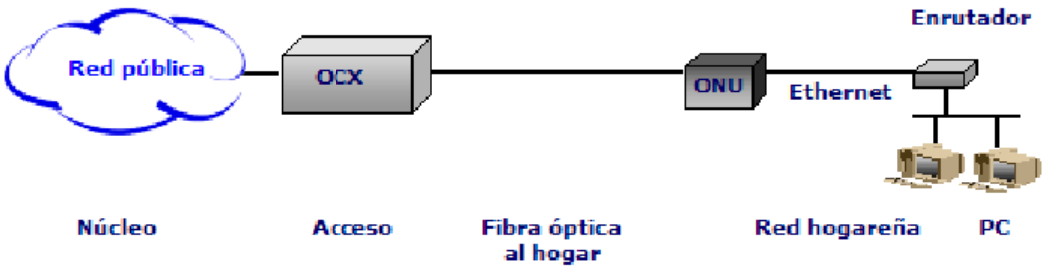

Figura 3.6. Topología Punto a Punto (12)

Ethernet bajo una red óptica sobre topologías punto a punto, podría brindar grandes ventajas a bajos costos de transceivers 1000BASE-X.

La fibra óptica, brinda a los hogares o negocios una velocidad de navegación de hasta 1 Gbps. Los proveedores de servicio habilitan nuevas alternativas para utilizar funciones de capa 3

que disponen de velocidad limitada, la misma combinada con SLA (Acuerdos del Nivel de Servicio –Service Level Agreements) un enlace físico de 1000 Mbps podría ser usada para proveer servicios de 10, 100, o 200 Mbps. Como consecuencia las redes con topología punto a punto pueden ofrecer una gran flexibilidad y escalabilidad.

Gigabit Ethernet sobre fibra óptica con topología punto a punto suministra suficiente ancho de banda y garantiza una larga vida a la infraestructura de la red, la misma que es de aproximadamente 20 años. Por tanto EFM con fibra óptica representa bajos costos en servicios y al mismo tiempo entrega un excelente ancho de banda para garantizar múltiples servicios (12).

3.4.1.1 TECNOLOGÍA GIGABIT ETHERNET

Gigabit Ethernet tolera tanto fibra óptica como cobre. Transmite través de fibra señales de aproximadamente 1 Gbps 1. Se aplica láseres debido a la gran velocidad con la que deben funcionar. En la tabla 3.1 se observa tipos de cable Gigabit Ethernet con sus respectivos detalles (12).

[1] Un Gbps es una velocidad muy alta, por ello, si un receptor está ocupado con otra tarea por incluso 1 ms y no vacía el búfer de entrada en alguna línea, podrían haberse acumulado ahí hasta 1953 tramas en ese espacio de tiempo.

NOMBRE	CABLE	LONGITUD MÁXIMA	ESPECIFICACIÓN
1000Base-SX	Fibra Óptica	550 m	Fibra multimodo (50, 62.5 micras)
1000Base-LX	Fibra Óptica	550 m	Fibra monomodo (10 micras) o Fibra Multimodo (50, 62.5 micras)
1000Base-CX	2 pares de STP	25 m	Cable de par trenzado blindado
1000Base-T	2 pares de STP	100 m	UTP categoría 6

Tabla 3.1. Cableado de Gigabit Ethernet (12)

3.4.1.2 TOPOLOGÍA PUNTO MULTIPUNTO (P2MP) (GEPON)

Esta topología alcanza una velocidad máxima de hasta 1 Gbps (Gigabit Ethernet) con una distancia máxima de hasta 20 km.

Las arquitecturas GEPON nacen con el propósito de solucionar la problemática de la última milla, puesto que esta tecnología presenta varias ventajas. Las redes GEPON permiten brindar servicios a usuarios localizados a una distancia máxima de 20 Km, ubicados desde la central u OLT hasta la ONU (ubicada en el usuario). Esta distancia resalta de forma significativa la cobertura de las tecnologías DSL (máximo 5Km desde la central).

En la figura 3.7 podemos observar un ejemplo de Topología Punto a Multipunto.

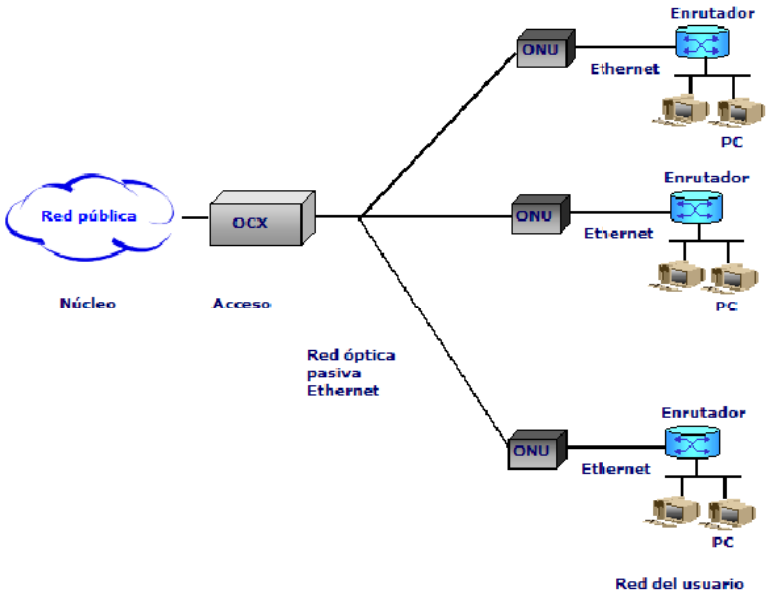

Figura 3.7. Topología Punto Multipunto (12)

Las redes GEPON minimizan el tendido de fibra en la última milla al utilizar topologías punto multipunto, con este tipo de arquitecturas se simplifica el equipamiento central, y por ende se reduce los costos.

GEPON (Gigabit Ethernet PON) como estándar de la IEEE/EFM usa fibra óptica como medio de transmisión, por lo cual utiliza paquetes de datos Ethernet, determinado en la IEEE 802.3ah (12). En la figura 3.8 podemos observar un ejemplo de distancia entre la OLT y las ONTs.

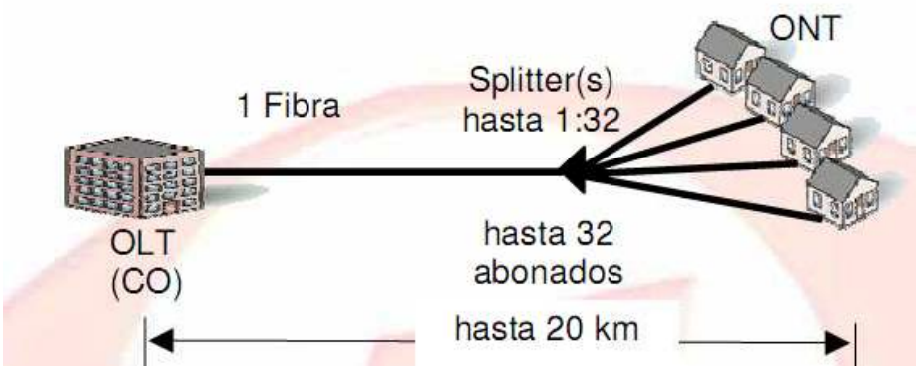

Figura 3.8. Distancia con GEPON (12)

GEPON al emplear arquitecturas punto multipunto ofrece servicios como FTTP (Fiber To The Premises-Fibra hacia los nodos) y FTTH (Fiber To The Home-Fibra hacia el hogar) utilizando una sola fibra para ofrecer múltiples servicios y usuarios.

GEPON tiene como origen principal Japón y puede llegar a brindar velocidades de hasta 1 Gbps en ambos sentidos (subida y bajada), así como dar múltiples servicios al mismo tiempo.

GEPON proporciona una conectividad similar a una red IP y a otros tipos de comunicaciones basadas en paquetes, como es, Ethernet que emplea IP para transportar datos, voz, y video. También administra una comunicación segura, ya que brinda mecanismos de encriptación en los sentidos de subida y bajada (12).

3.5 RED GEPON

GEPON (GIGABIT ETHERNET PASSIVE OPTICAL NETWORK), es una tecnología creada para el uso de las telecomunicaciones y acopla las tecnologías Gigabit Ethernet y Passive Optical Network dentro de su estructura. Este sistema simplifica y abarata la gestión de la red ya que la fibra facilita la llegada hasta los abonados y los equipos con los que se accede son más económicos al usar interfaces Ethernet (13). Es un sistema que se inclina a la convergencia con el estándar ITU GPON elaborado por un grupo de estudio de la IEEE de Ethernet (14).

Este sistema es una mejora de las tecnologías PON, presenta una variedad de beneficios que lo hacen más destacado como el transporte de tráfico Ethernet, el uso de fibra óptica en el transporte vía Ethernet y la norma IEEE 802.3 que funciona con velocidades de Gigabit, por lo cual la velocidad para cada usuario final depende del número de ONU's que se interconecten a cada OLT. Una ventaja de este sistema es que ofrece QoS (Calidad de Servicio) en ambos canales (13). En la figura 3.9 podemos observar un ejemplo de Red GEPON.

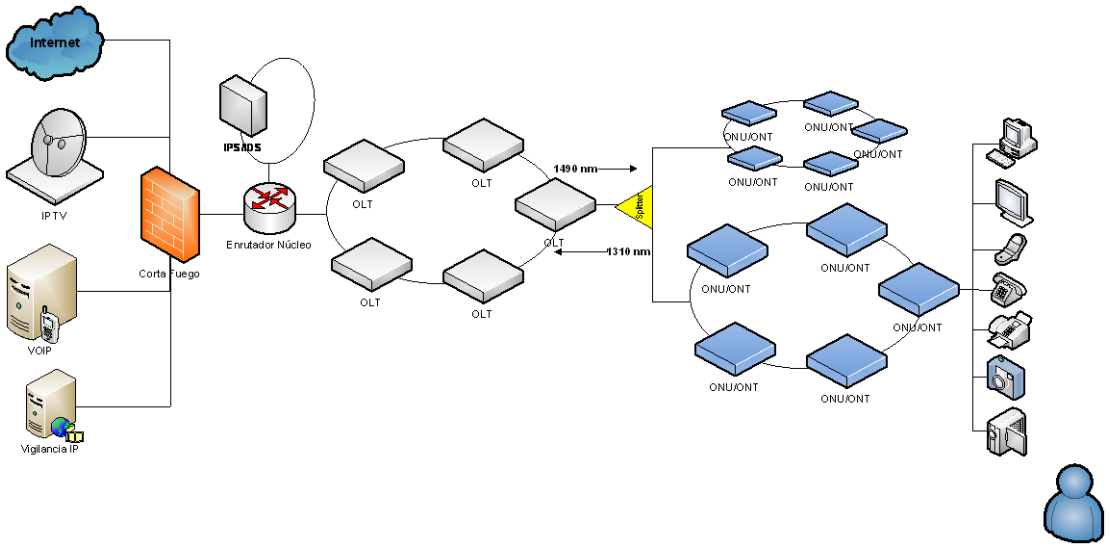

Figura 3.9. Red Gepon

3.5.1 ELEMENTOS DE UNA RED GEPON

GEPON es desarrollada como una aplicación punto-multipunto y está compuesta por:

- OLT: Terminal de Línea Óptica (Optical Line Terminal)
- ONU: Unidad Óptica de Red (Optical Network Unit)
- ODN: Red de Distribución Óptica (Optical Distribution Networks)
- OAN: Red Óptica de Acceso (Optical Network Access)

- POS: Splitter Óptica Pasiva (Passive Optical Splitter)

3.5.1.1 TERMINACIÓN DE LÍNEA OPTICA (OLT)

Facilita una interfaz de red entre la OAN y permite la conexión con una o varias ODN.

La OLT se conecta a la red mediante interfaces normalizadas. Presenta interfaces de acceso ópticas compatibles con las normas GEPON, en términos de velocidad binaria, balance de potencia, fluctuación de fase, etc. (15)

La OLT consta de tres partes principales. En la figura 3.10 podemos observar un ejemplo de los Elementos de la OLT.

- Función de interfaz de puerto de servicio.

- Función de conexión cruzada.

- Interfaz de red de distribución óptica (ODN)

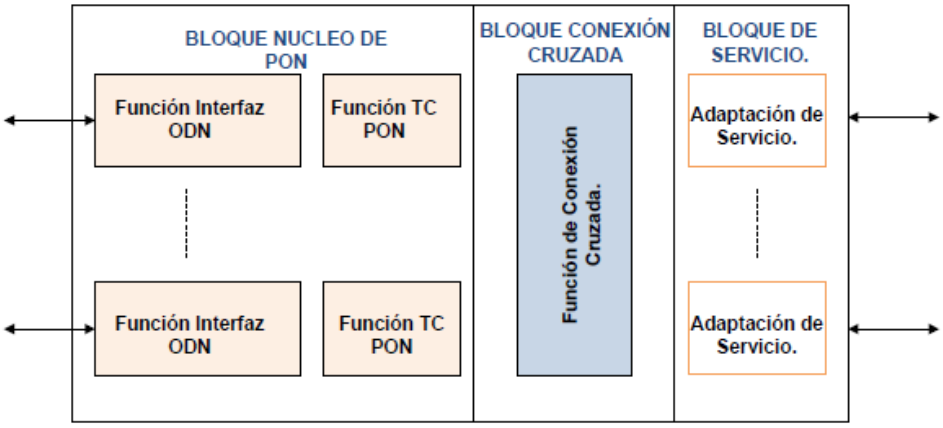

Figura 3.10. Elementos de la OLT (15)

Bloque Núcleo de PON: Consta de 2 partes con las siguientes funciones (15):

Función de Interfaz ODN y TC PON: incluyen el esqueleto de la red, control de acceso al medio, operación, administración y mantenimiento, la ordenación de las unidades de datos de protocolo (PDU, Protocol Data Unit) para la función de conexión cruzada, y la gestión de la ONU.

Bloque de Conexión Cruzada: facilita un camino de comunicación entre el bloque núcleo de PON y el bloque de servicio. Las tecnologías para la conexión de este camino están a cargo de los servicios, la arquitectura interna de OLT y otros factores.

Bloque de Servicio: provee la interpretación entre las interfaces de servicio y la interfaz de trama TC de la sección PON.

Funciones y características del OLT (12)

- Provee una interfaz de multiservicios al núcleo de la WAN.
- Provee una interfaz Gigabit Ethernet a la PON
- Switching y Routing en Capa 2 y Capa 3.
- Calidad de Servicio (QoS) y Acuerdos de nivel de Servicio (SLA).
- Tráfico Agregado.

3.5.1.2 UNIDAD DE RED ÓPTICA (ONU)

Elemento que sirve de vínculo entre el usuario y la OAN, conectada a la ODN.

Los elementos de la ONU GEPON son similares a los elementos de la OLT. Debido a que la ONU trabaja con una única interfaz PON (máximo 2 interfaces por protección), entonces puede descartarse la función de conexión cruzada (15). En la figura 3.11 podemos observar un ejemplo de los Elementos de la ONU.

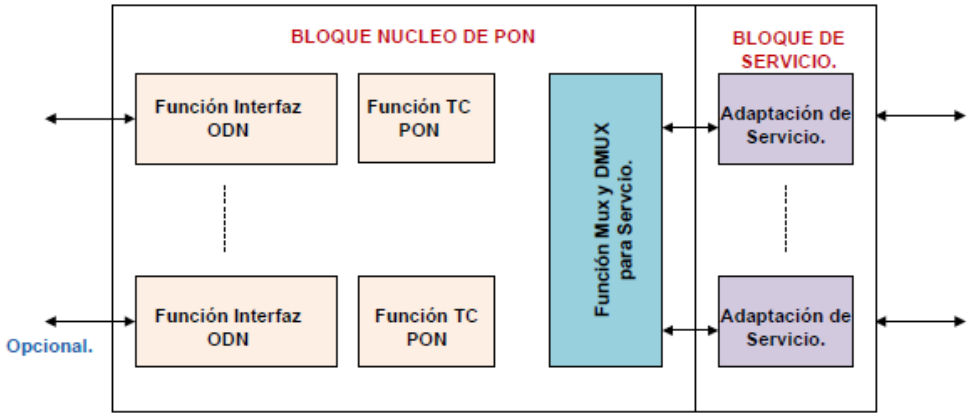

Figura 3.11. Elementos de la ONU (15)

3.5.1.3 RED DE DISTRIBUCIÓN ÓPTICA (ODN)

Permite la comunicación entre un OLT y el usuario, y viceversa. Vincula una OLT y una o más ONUs a través de un dispositivo óptico pasivo (15).

3.5.1.4 RED ÓPTICA DE ACCESO (OAN)

Bloque de enlaces de acceso similares con interfaces iguales del lado de la red aceptadas por los sistemas de transmisión de tipo óptico (16).

3.5.1.5 SPLITTER (DIVISOR ÓPTICO PASIVO)

Dispositivo que comunica la señal óptica sin necesidad de provisión externa multiplexando y/o demultiplexando la señal (16). Es un elemento pasivo que sirve para dividir la señal óptica, que entra por un extremo, en varias señales de salida. En la figura 3.12 podemos observar un ejemplo del Splitter.

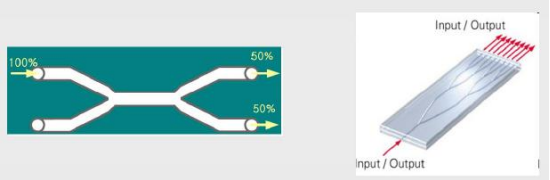

Figura 3.12. Splitter (17)

Permiten la conexión punto a multipunto y distribuye las señales ópticas de una fibra a otras. Una sola fibra conectada al OLT puede distribuirse y conectar hasta 64 ONU's diferentes.

En el libro Características Generales De Una Red De Fibra Óptica Al Hogar (FTTH) (17), Memoria de trabajos de difusión científica y técnica, Abreu Marcelo, Castagna Aldo, Cristiani Pablo, Zunino Pedro, Roldós Enrique y Sandler Gustavo expresan cabalmente los beneficios de este tipos de dispositivos: “Los splitters ópticos se implementan cascadeando splitters físicos con relación 1:2, donde la señal de entrada se distribuye en dos caminos diferentes resultando en una pérdida de potencia aproximadamente de 3,5 dB. Cada camino vuelve a separarse en dos permitiendo mayor distribución pero también adicionando nuevamente una pérdida de potencia” (17).

En la Tabla 3.2 se pueden apreciar algunas pérdidas típicas ocasionadas por splitter comercialmente disponibles.

Relación de Split	Pérdida de inserción (dB)
1:2	3,6
1:4	7,2
1:8	11
1:16	14
1:32	17,5

Tabla 3.2. Pérdidas en Splitters (17)

Dado que los splitters provocan pérdidas importantes de potencia en relación a los demás componentes de la red, el

diseño de la red debe ser cuidadosamente balanceada entre: ramificación alta de fibras, distancias a los clientes, y las potencias manejadas por los equipos; de modo que satisfagan las especificaciones de los mismos. En la figura 3.13 podemos observar un ejemplo de Diseño de red con Splitter.

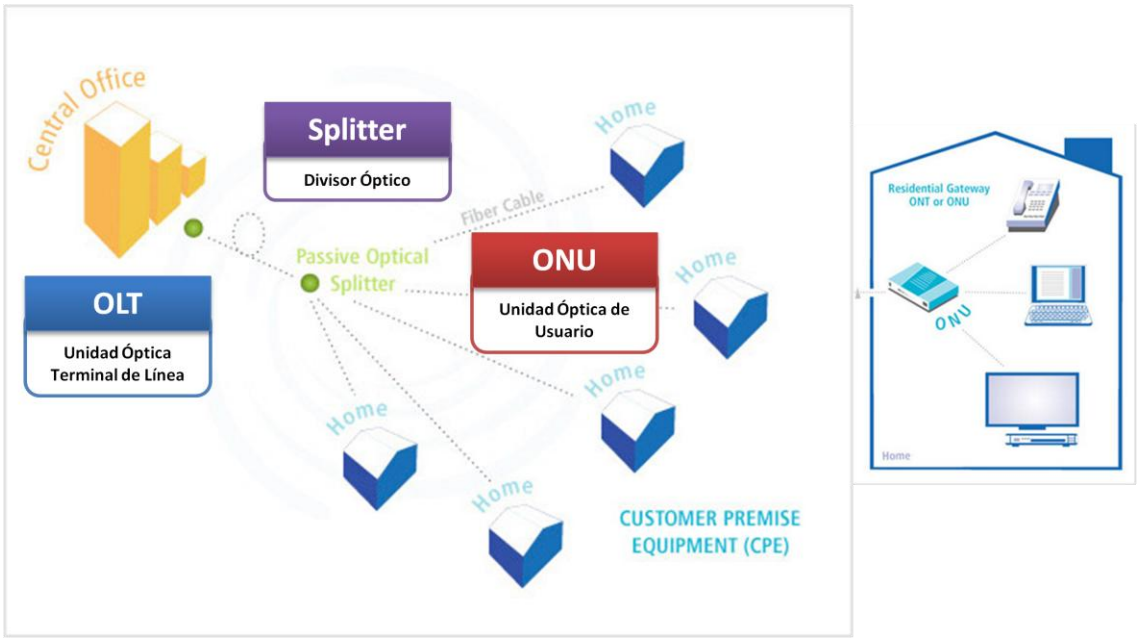

Figura 3.13. Diseño Red con Splitters

Fuente: http://www.pmc-sierra.com/ftth-pon/ftth_overview.html

3.5.2 EMS, ELEMENTO DE ADMINISTRACIÓN DEL SISTEMA

Otro componente de la red GEPON es el Elemento Administrador del Sistema denominado EMS quien se encarga de analizar, administrar y controlar todos los elementos de la red (OLT, ONU)

en enlaces ascendentes incluyen funcionalidades como detención de fallas, configuraciones, rendimiento, cumplimiento de estándares, consumo de ancho de banda y seguridad además se proporciona una interfaz en el proveedor para que puedan manejar los servicios que proveen. En enlaces descendentes las redes GEPON proporcionan interfaces para la comunicación con todas las redes de servicios como PSTN, IP, LAN, telefonía IP, televisión por cable o IPTV, servidores streaming, Video bajo demanda (12)

Características y funciones del EMS

- Funciones de seguridad, configuración, administración y rendimiento.

- Capacidad de administrar decenas de sistemas GEPON.

- Permite la conexión de múltiples usuarios en la interfaz. Interfaces estandarizadas que permiten realizar todas las operaciones de la red.

3.5.3 FUNCIONAMIENTO DE LAS REDES GEPON

En las redes GEPON la transmisión de datos se realiza entre la OLT y la ONU que se comunican a través del divisor óptico pasivo cuya función depende si el envío de datos es de manera ascendente o descendente.

3.5.3.1 ADMINISTRACIÓN DE TRÁFICO SUBIDA/BAJADA EN GEPON

En una red GEPON el proceso de trasmitir datos de bajada o de manera descendente comienza desde el OLT hacia las múltiples ONU's y de sentido de subida o forma ascendente la transmisión de datos es desde múltiples ONU's al OLT.

Tráfico de Bajada

El tráfico de bajada en una red GEPON utiliza la tecnología de Multiplexación por División de Tiempo (TDM, Time Division Multiplexing) para transmitir paquetes desde el OLT hacia múltiples ONU's en paquetes de longitud variable, de acuerdo con el protocolo IEEE 802.3.

Cada paquete tiene una cabecera de identificación única, la cual permite a las ONU's conocer si el dato recibido le pertenece a la ONU adecuada. Además, algunos paquetes pueden estar destinados a todos las ONU (broadcast) o un grupo particular de ONU's (multicast). Cuando el tráfico llega al divisor óptico pasivo, es separado en tres señales para ser llevado a sus ONU's pertinentes, cuando el tráfico llega a las ONU's, ésta acepta los paquetes enviados a cada ONU específico y descarta los paquetes dirigidos a otras ONU's en otras palabras filtra los paquetes como se puede observar en la figura 3.14, la ONU recibe los paquetes 1, 2, 3 y lo que hace es tomar el paquete que le corresponde descartando los otros.

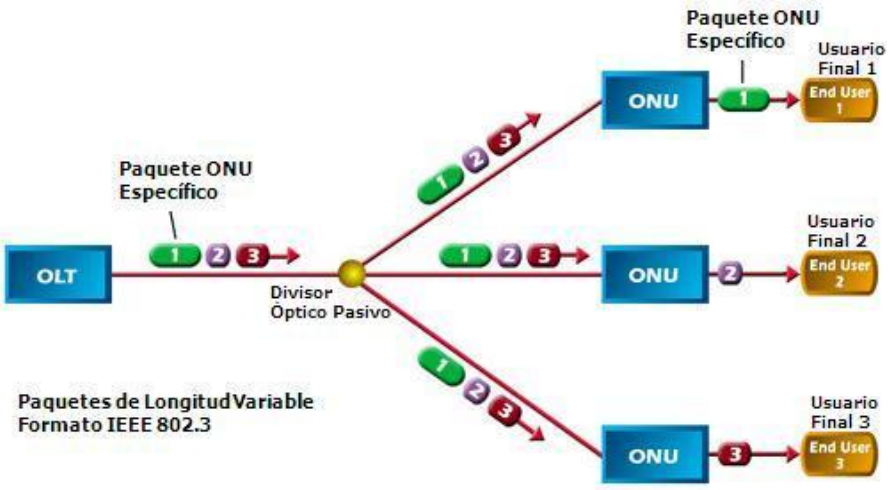

Figura 3.14. Flujo de tráfico en sentido de bajada en una GEPON

Fuente: http://www.infocellar.com/networks/new-tech/EPON/EPON.htm

Tráfico de Subida

El tráfico de subida en una red GEPON utiliza la tecnología Acceso múltiple por división de tiempo (TDMA, Time División Múltiple Access) para transmitir los paquetes por segmentos de tiempo establecidos para cada ONU. Estos segmentos son sincronizados a fin de que los paquetes en sentido de subida de las ONU's no interfieran con cada uno de los datos que son enviados por el divisor óptico pasivo (splitter) una sola fibra, el divisor óptico requiere de una perfecta sincronización de los paquetes ascendentes que recibe, para formar la trama GEPON, es por ello necesario que la OLT conozca la distancia a la que están las ONU's para considerar el retardo.

Como se muestra en la figura 3.15, la ONU-1 en un primer segmento de tiempo transmite el paquete 1, en el segundo segmento la ONU-2 transmite el paquete 2, en el tercer segmento la ONU-3 transmite el paquete 3, de esta manera se consigue que los segmentos no se superpongan, (12).

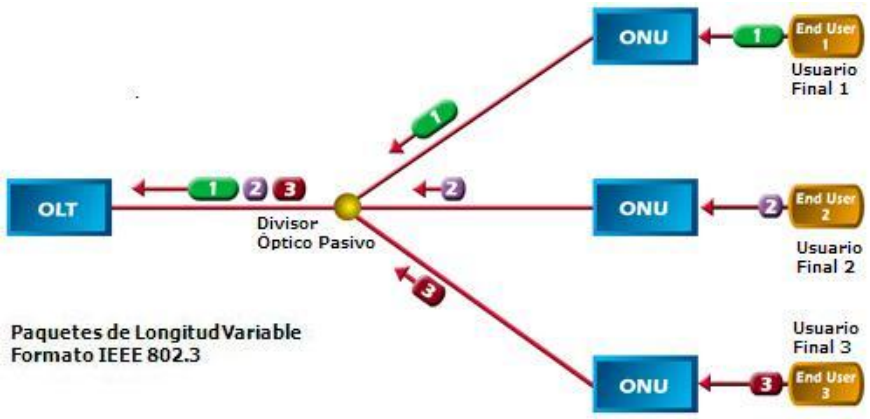

Figura 3.15. Flujo de tráfico en sentido de subida en una GEPON

Fuente: http://www.infocellar.com/networks/new-tech/EPON/EPON.htm

3.5.3.2 PROTOCOLO DE CONTROL MULTIPUNTO MPCP

El protocolo MPCP es utilizado para el control de acceso a la red GEPON en una topología Punto-Multipunto, es decir, en un enlace ascendente.

Características del MPCP

- Detecta y registra ONU's conectadas y descubiertas recientemente.

- Proporciona un plan de control para la coordinación en la transmisión de datos en sentido ascendente.

- Utiliza algoritmos de Asignación Dinámica de Ancho de Banda (DBA,Dynamic bandwith Allocation).

- Usa mensajes de señalización básicos que se denominan Grant o Gate usado por la OLT y Report por la ONU, estos mensajes se encargan de la administración entre las ONU's conectadas a la PON.

- Las ONU's contienen paquetes predefinidos para obtener priorización y políticas de paquetes de datos.

- El MPCP ofrece recursos de optimización para la red.

En la figura 3.16 se puede apreciar la administración de las ONU's mediante el protocolo MPCP, en donde se envía el mensaje Report por la ONU para hacer la petición de ancho de banda o a su vez encolar al mensaje Report (se permiten 8 reportes en estado de encolamiento como máximo), una vez que la OLT recibe la petición de ancho de banda, se calcula la planificación de las posteriores transmisiones con el algoritmo de DBA luego se envía la asignación del ancho de banda a la ONU que hizo la petición mediante el mensaje Grant.

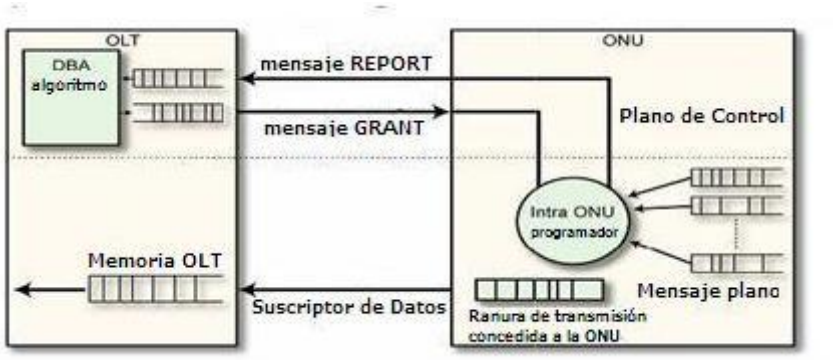

Figura 3.16. Administración de las ONU's

3.5.3.2.1 OPERACIÓN BÁSICA DEL MPCP

Los mensajes Report y el Grant son usados para asignar requerimientos de ancho de banda (18). También son usados como mecanismos para la compensación del retardo.

A continuación se detalla paso a paso el funcionamiento del protocolo MPCP con sus respectivas figuras 3.17 y 3.18.

a) La ONU envía un mensaje de Report al OLT.

b) El OLT recibe el mensaje de Report.

c) El algoritmo DBA estima el tamaño del segmento de tiempo para la ONU en sentido de subida.

d) El organizador del OLT estima un tiempo de transmisión para la ONU.

e) El mensaje Grant es creado para la ONU.

f) El mensaje Grant tiene un tiempo definido con el valor del reloj del OLT.

g) El mensaje Grant es transmitido hacia la ONU.

h) El mensaje Grant es enviado en broadcast.

i) La ONU recibe el mensaje Grant.

j) El reloj local actualiza a la ONU con el valor de sincronización en el mensaje Grant.

k) La ONU transmite en su segmento de tiempo.

l) Una vez establecido el tiempo de transmisión, la ONU crea una trama de subida y agrega un nuevo Report.

m) La ONU envía una trama de datos en el enlace de subida.

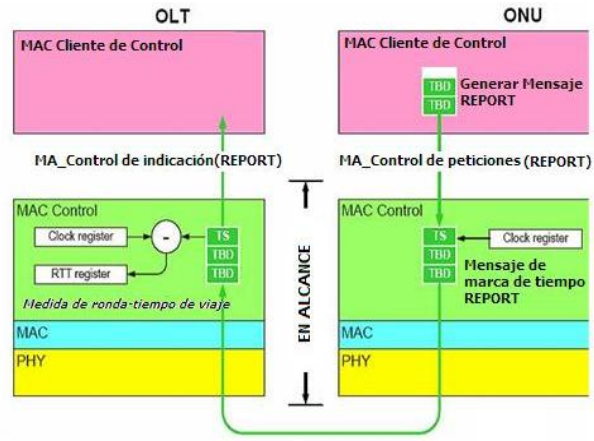

Figura 3.17. Mensaje de Report (12)

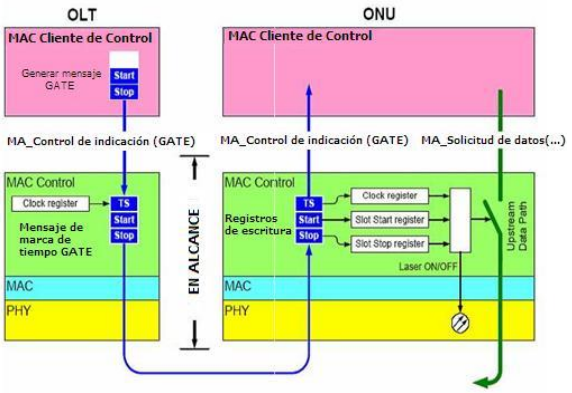

Figura 3.18. Mensaje Grant (12)

3.5.3.2.2 PROCESO RANGING

El OLT local especifica un tiempo de transmisión para cada ONU, los datos enviados por las ONU pueden colisionar porque se envían en diferentes tiempos, para prevenir estas colisiones, el protocolo MPCP hace uso del proceso Ranging, quien se encarga de medir o calcular un retardo específico

por cada ONU, el proceso Ranging tal como se muestra en la figura 3.19 genera retardos y asigna tiempos más largos para la transmisión de los datos de cada ONU, eliminando las colisiones (12). Existen dos tipos de Ranging:

- Ranging Áspero (coarse ranging).

- Ranging Fino (Ranging Fine).

El Ranging áspero (coarse ranging) es usado como una secuencia inicial, mientras que el Ranging fino (Ranging Fine) es usado constantemente como retardo, que puede ser alterado debido a cambio de ambiente en la fibra. El Ranging se fundamenta básicamente en los mensajes de Grant o Gate y Report.

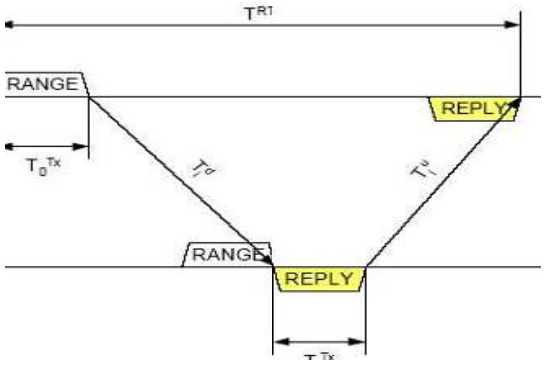

Figura 3.19. Proceso Ranging (12)

3.5.3.2.3 FORMATO DE UNA TRAMA GEPON

Para un tráfico en sentido de bajada que es transmitido por el OLT hacia la ONU en paquetes de longitud variable es segmentado en tramas, cada una de las cuales son múltiples paquetes de longitud variable. Se incluye información de reloj al inicio de trama para sincronización; un código de un byte que se transmite cada 2 ms tal como se muestra en la figura 3.20.

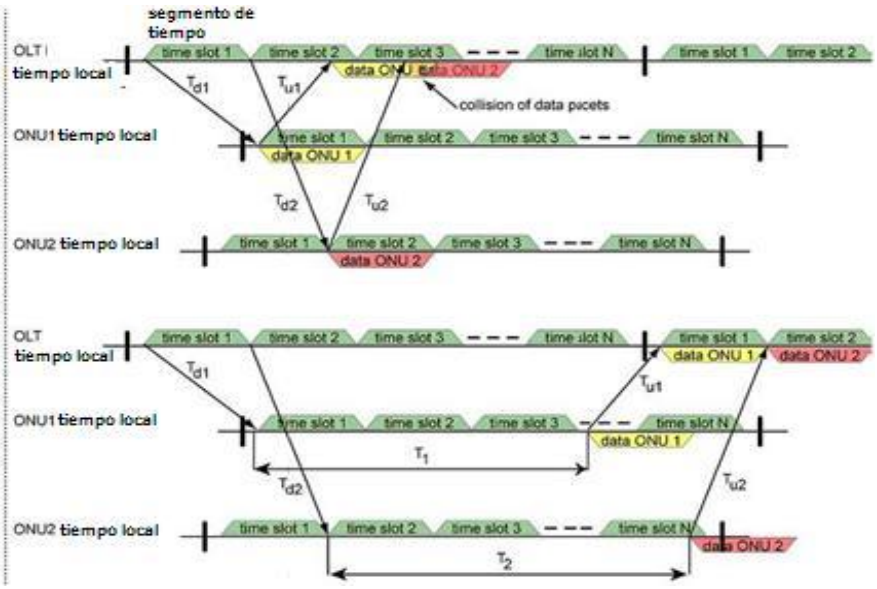

Figura 3.20. Trabajo del Proceso Ranging (12)

Los paquetes de longitud variable son direccionados a la ONU específica. Los cuales están formados de acuerdo al estándar

IEEE 802.3 que se los transmite en sentido de bajada a 1 Gbps. La estructura de cada paquete de longitud variable, que representa la cabecera, carga y el campo de detección de errores, se muestra a continuación en la figura 3.21.

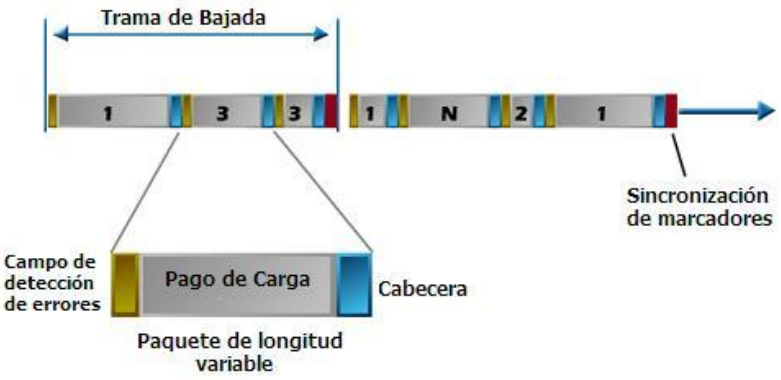

Figura 3.21. Formato de una trama GEPON (12)

El tráfico de subida es segmentado en tramas, a su vez cada trama es segmentada en ranuras de tiempo específicos dentro de la ONU. Estas tramas de subida están formadas por intervalos de transmisiones continuas de 2 ms. La cabecera de la trama indica el inicio de una trama. En la figura 3.23 se muestra un formato de la trama del tráfico en sentido de subida.

Los segmentos de tiempo destinados a cada ONU son intervalos de transmisión específicos para paquetes de

longitud variable a las ONU's. A cada ONU le corresponde un segmento de tiempo, el cual está dedicado dentro de la trama de subida.

Para controlar el tiempo de transmisión del tráfico de subida dentro de los segmentos de tiempo dedicados se lo hace con TDM por cada ONU, en conjunto con el tiempo de información del OLT. En la figura 3.22 se muestra un segmento de tiempo de una ONU que incluye dos paquetes de longitud variable con un encabezado de segmento de tiempo. Este encabezado consta de una banda de guarda, indicadores de tiempo y señal. Cuando no se transmite tráfico de la ONU en el segmento de tiempo indicado, este puede ser llenado por otra señal (12).

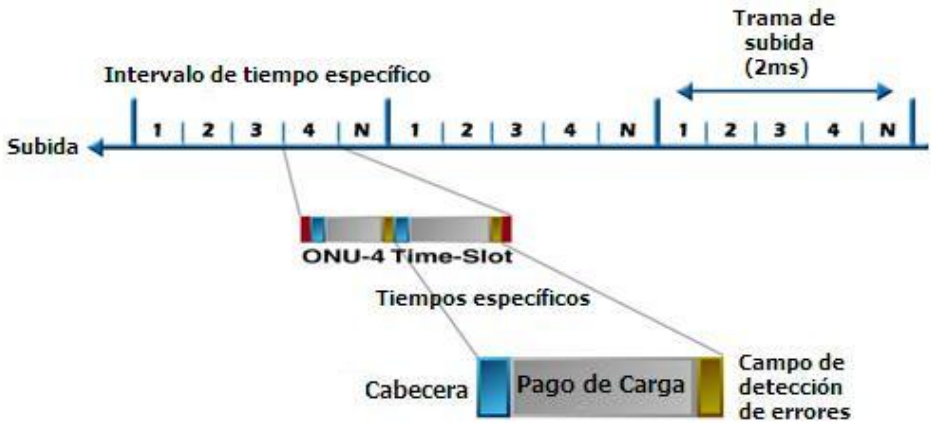

Figura 3.22. Formato de una trama GEPON en sentido de subida (12)

3.5.3.3 SISTEMAS DE TRANSMISIÓN CON GEPON

Las redes GEPON pueden ser implementadas usando arquitecturas con dos o tres longitudes de onda. Para transmisión de datos, voz y video IP es aconsejable utilizar una arquitectura con dos longitudes de onda. En cambio para transmitir señales de RF, servicios de video como TV CABLE o sistemas con multiplexación de onda densa (DWDM), se emplea la arquitectura con tres longitudes de onda.

Un esquema óptico para un sistema GEPON con dos longitudes de onda se lo muestra en figura 3.23. En esta arquitectura para transportar datos, video y voz en la dirección de bajada se utiliza una longitud de onda de 1510 nm, mientras que la para transportar video bajo demanda, así como también voz y datos, en el sentido de subida se emplea una longitud de onda de 1310 nm.

Figura 3.23. GEPON con dos longitudes de onda (12)

En el esquema óptico para un sistema GEPON con tres longitudes de onda, las longitudes de 1510 nm y de 1310 nm son usadas en las direcciones de subida y bajada, respectivamente; mientras que la longitud de onda de 1550 nm, se reserva para la transmisión de video en el sentido de bajada.

El video es codificado con MPEG2 y es transmitido mediante modulación QAM (Amplitud Cuadrada Modulada - Quadrature Amplitude Modulation), tal como se muestra en figura 3.24.

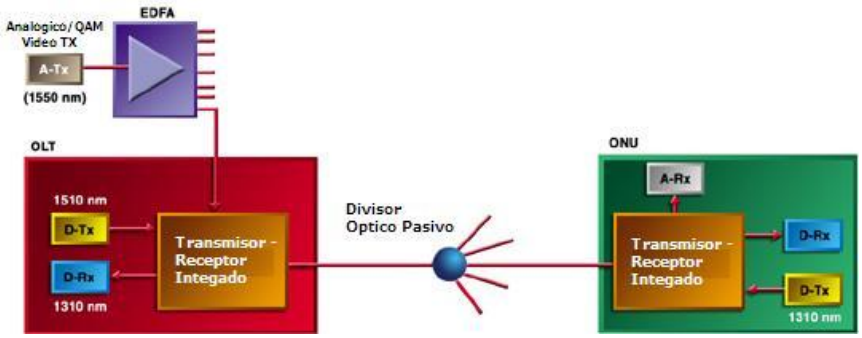

Figura 3.24. GEPON con tres longitudes de onda (12)

En este tipo de arquitectura que utilizan tres longitudes de onda puede ser usada para proveer una sobrecarga DWDM para una red GEPON. Esta solución basada en DWDM, usa una fibra monomodo con longitud de onda de 1510 nm para el tráfico de bajada y 1310 nm para el tráfico de subida. La ventana entre 1530–1565 nm no se la utiliza y los transceivers son

diseñados para que permitan que canales DWDM se transmitan de manera transparente mediante la tecnología PON (12).

3.5.3.4 CONFIGURACIÓN ESTÁNDAR GEPON

La configuración típica de una red GEPON involucran algunos componentes, siendo el más básico e importante el uso de la fibra óptica, bien en una o dos fibras (por cliente), pudiendo adoptar dichas redes desde una configuración básica, sin diversidad alguna, hasta arquitecturas con redundancia total (19). En la figura 3.25 se muestra la estructura interna de una fibra óptica.

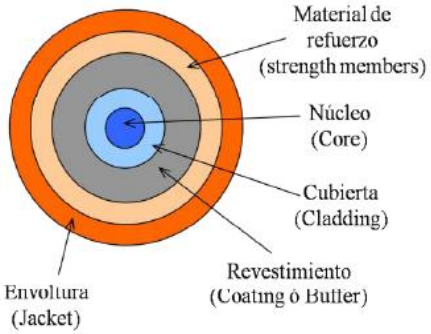

Figura 3.25. Estructura interna de una Fibra Óptica

Fuente: www.arcesio.net/capa_fisica/componentes_fisicos.ppt

La gran optimización que se logra en la utilización de la fibra óptica (20) la podemos ver ilustrada en la siguiente figura 3.26:

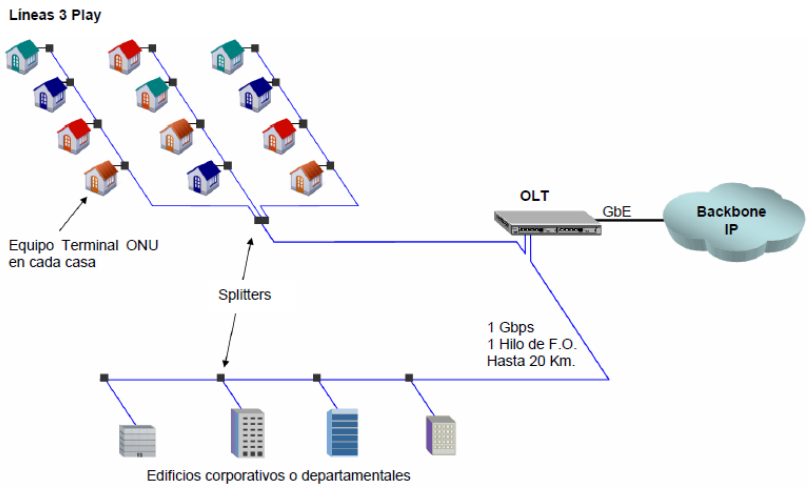

Figura 3.26. Utilización óptima de fibra óptica (12)

Se puede apreciar un equipo distribuidor OLT que se conecta a la red principal, de este salen múltiples trayectorias, cada una de estas trayectorias constan de un solo hilo de fibra óptica con capacidad de transportar 1Gbps de información. Este ancho de banda es repartido entre las conexiones terminales de la trayectoria, y culminan en un equipo llamado ONU, ubicado en la instalación del subscriptor o nodo de red.

Existen varios modelos de ONU a proporcionar desde un puerto de Ethernet para la conexión del subscriptor:

- Hasta 24 puertos de Ethernet en el caso de un edificio departamental, o
- Modelos de ONUs que incluyen puertos para conectar directamente una TV en el caso de aplicaciones Triple Play.

La distribución del ancho de banda entre los subscriptores que comparten una misma trayectoria es totalmente ajustable. La fibra óptica se comparte a través de los splitters, que son equipos pasivos.

La fibra puede derivar en bus, estrella, o una combinación de ambas. Esto brinda la facilidad de manejar el tráfico a nivel de capa 2 o 3, y se pueden configurar VLAN's para mantener el tráfico totalmente aislado entre distintos subscriptores, así, si existen subscriptores que requieran tener comunicación directa, pueden agruparse dentro de una misma VLAN. Las posibilidades de conexión en el punto terminal de servicio (20) (casa, habitación, oficina, etc), se ilustran en la siguiente figura 3.27:

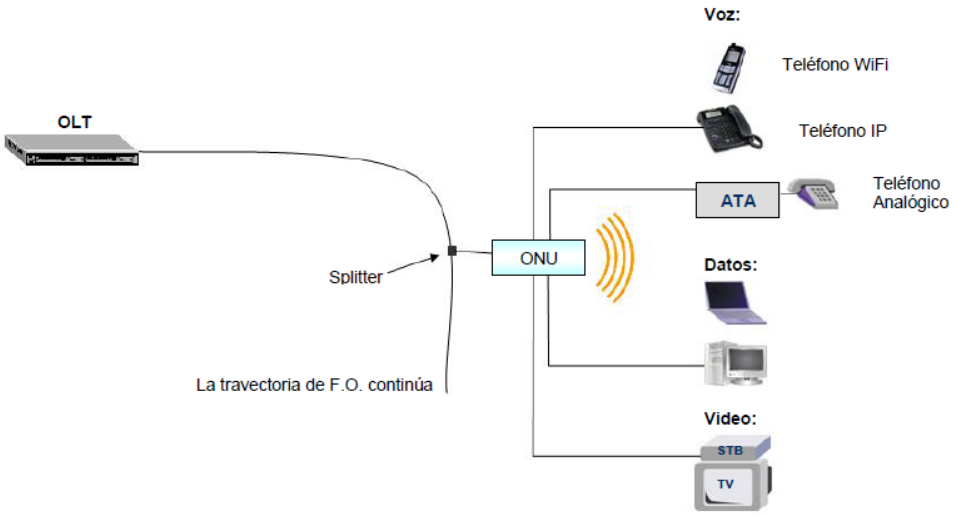

Figura 3.27. Posibles conexiones en el lado del cliente (12)

3.5.3.5 ARQUITECTURA DE RED GEPON

Una red GEPON es elaborada en base a una estructura de equipos OLT con divisores PLC (Circuitos de Onda de Luz Plana - Planar Lightwave Circuits) que terminan al llegar a los equipos ONU. Estos proporcionan los servicios de datos, voz y video.

Los OLT funcionarán como servidores de la señal digital. Los splitters PLC (Circuitos de Onda de Luz Plana - Planar Lightwave Circuits) se encargarán de distribuir el ancho de banda entre las ONU. Existen un número muy variado de equipos ONU, los cuales cuentan con distintas características que proporcionan la solución adecuada a las necesidades de la red (13). En la figura 3.28 se ilustra una Arquitectura Red GEPON.

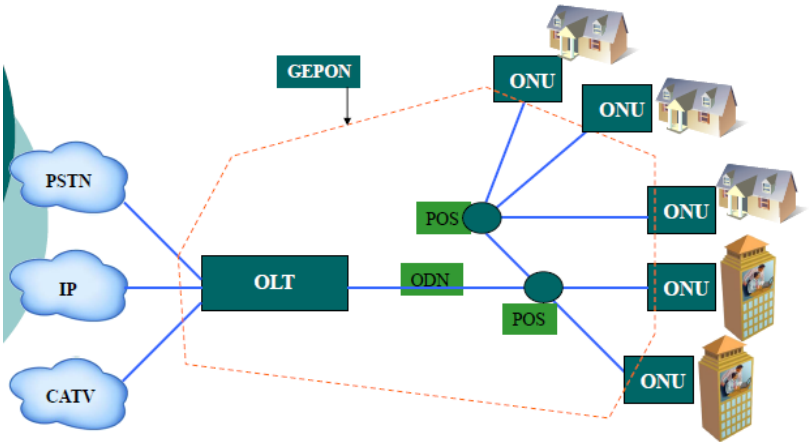

Figura 3.28. Arquitectura Red Gepon (12)

3.5.3.6 DISEÑO DE UNA RED GEPON

A la hora del diseño de las redes GEPON, se debe tener muy en cuenta los requisitos de los clientes, dependiendo de eso, se obtiene un diseño en particular.

En la figura 3.29 se puede observar el diseño de una red GEPON, está conformada básicamente por los equipos OLT, ONU y divisores ópticos.

La construcción de las redes mediante el uso de la tecnología GEPON es mediante la estructura de equipos OLT con divisores PLC y que terminan al llegar a los equipos ONU; que proporcionan los servicios de datos, voz y video.

Los OLT funcionarán como servidores de la señal digital. Los PLC (Splitters) se encargarán de distribuir el ancho de banda entre las ONU. Existen un número muy variado de equipos ONU, los cuales cuentan con distintas características que proporcionan la solución adecuada a las necesidades de la red.

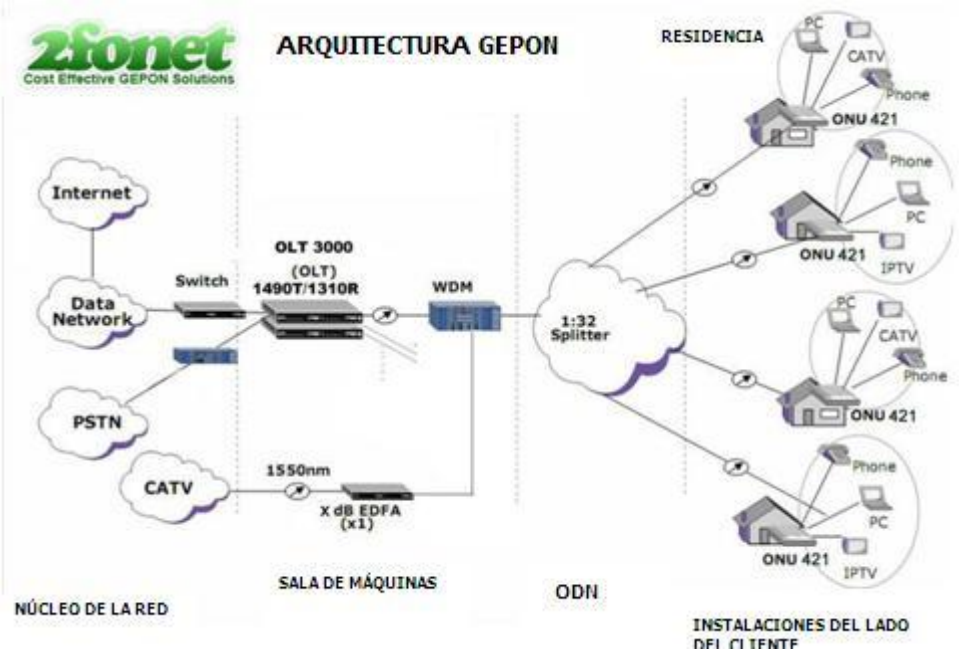

Figura 3.29. Diseño Red Gepon

Fuente: http://www.2fonet.com/home/tuolima-tecnologia-gepon/

3.5.3.7 CALIDAD DE SERVICIO (QOS)

Las redes GEPON ofrecen algunas ventajas en costo y rendimiento, lo que habilita a los proveedores de servicios entregar y generar servicios en una plataforma económica. Sin embargo, el principal desafío de los proveedores de servicio de GEPON es mejorar las capacidades del Ethernet para asegurar la voz sobre IP, y vídeo en tiempo real que pueden ser entregados a través de una única

plataforma con el mismo QoS y con la facilidad de administración que presta ATM o SONET.

Los proveedores de GEPON atacan este problema desde varios ángulos. Los cuales consisten en diferenciar servicios 802.1p, el cual prioriza el tráfico por niveles de servicio. Una técnica es TOS Field; el cual presenta ocho capas de prioridades para asegurarse que los paquetes pasen por orden de importancia. Otra técnica es llamada Reserva de ancho de banda (Reserve Bandwidth), el cual provee una reserva del ancho de banda con garantía de latencia para tráfico POTS que no tienen que lidiar con los datos (12).

3.5.3.8 CARACTERÍSTICAS Y BENEFICIOS DE GEPON

GEPON ofrece mejoras notables sobre las tecnologías PON que le precedieron, como por ejemplo (12):

Características

- Tiene un gran alcance entre los equipos distribuidores y los subscriptores (20 km).

- Brinda una solución completa a los servicios Triple Play, para lograr tener en una misma plataforma los servicios de TV, Internet y Teléfono.

- Posee un ancho de banda seguro y garantizado para diferentes servicios (Triple Play: voz, datos y video) al ser el número de abonados por trayectoria de fibra de un máximo de 32.

- Brinda soporte para datos, voz y video (servicio Triple Play).

- Varios usuarios pueden usar una sola fibra para ahorrar costos.

- Se disminuyen las tasas de administración y mantenimiento en la red al usarse equipos de fibra pasivos.

- Posee una topología Punto Multipunto con splitter sin requerir un campo de energía.

- Fácil administración, fácil contabilidad y fácil actualización con flexibilidad y escalabilidad.

- Soporte multicast para la transmisión de videos con IPTV.

- Fácil administración, fácil contabilidad y fácil actualización con flexibilidad y escalabilidad.

- La instalación del equipo ONU no requiere ninguna configuración especializada en el domicilio del subscriptor, desde una interface gráfica de administración centralizada, se le asignan los atributos necesarios.

- Permite la combinación con otras tecnologías backbone y acceso de forma simple.

- Las ONU's proveen una traslación de direcciones IP, el cual reduce el número de direcciones IP e interfaces con la PC y los equipos de datos que usan interfaces Ethernet.

- La ONU ofrece similares características a los ruteadores, conmutadores y repetidores, sin costos adicionales.

- Utiliza VLAN's.

- Arquitectura de red completa, con sistemas de respaldo.

- Implementación de Firewall en las ONU sin necesidad de separar de la PC.

- Sistema de redundancia a las ONU lo que provee alta rentabilidad y confiabilidad.

- Simplifica la administración de red, reduce tiempo y costos.

- Facilita los servicios del usuario y reduce el manejo de consulta de usuario.

- Sistema automática de identificación.

- Administración remota y actualizaciones de software.

- Brinda el estatus de los servicios de voz datos y video para uno o un grupo de usuarios que se pueden monitorear simultáneamente.

- Las ONU's están sujetas a estándares.

Beneficios

- Los usuarios pueden hacer cambios de configuración, sin la coordinación del direccionamiento de ATM que son menos flexibles.

- Consolida funciones en una sola estructura, con ello reduce costos y permite a los proveedores de servicios, generar nuevos servicios.

- Permite a los proveedores de servicios garantizar los niveles de servicio, y evitar costosas interrupciones.

- Permite rápida restauración de servicios en caso de fallas.

- Simplifica la administración de red, reduce tiempo y costos.

- Facilita los servicios del usuario y reduce el manejo de consulta de usuario

- Elimina la necesidad de DSL y/o cable MODEM a los usuarios

CAPÍTULO 4

4. SEGURIDAD

4.1 ASEGURANDO LA RED GEPON

Las vulnerabilidades del protocolo IP, vienen dadas tanto por los dispositivos que lo emplean, como las redes que lo soportan y la manera en que se explota, y ligado a esto están las diferentes amenazas y consecuencias que pueden darse, descritas en la tabla 4.1. (21)

La diversidad de soportes de transporte de comunicaciones IP también han afectado las líneas de comunicaciones, sistemas de alimentación de antenas inalámbricas, también problemas lógicos como la infección por virus, pueden afectar de manera importante la disponibilidad de redes IP (22).

El proceso Estándar de Cifrado Avanzado (AES, Advanced Encryption Standard) forma parte del estándar ITU-T en las redes

GEPON, pero, el cifrado en las redes GEPON se realiza solamente en el canal de retorno.

Amenazas	***Consecuencias***
Integridad	
Datos modificados	Información perdida
Caballo de Troya	Máquina penetrada
Memoria cambiada	Vulnerabilidad a otras amenazas
Datos modificados	Información perdida
Confidencialidad	
Mensajes escuchados en la red	Pérdida de privacidad
Datos robados de servidores	Revela contraseñas etc
Análisis de tráfico	Identifica patrones de acceso
Detecta configuración de la red	Facilita otros ataques
Denegación de Servicios	
Procesos matados	Molestias
Inundación con paquetes	Interferencia con trabajo
Llenado de discos	Disminución de espacio en disco
Autentificación	
Identidades falsas	Acciones atribuidas al usuario
Datos falsos	Daño al nombre institucional

Tabla 4.1. Amenazas y Consecuencias Protocolo IP (21)

En las redes GEPON, la seguridad no ha sido uno de los puntos más destacados. En Ethernet Punto a Punto (PtP, Point-to-Point) full duplex, la seguridad no es una cuestión crítica, pues sólo hay dos estaciones comunicándose mediante un canal privado. En el modo half-duplex compartido, los problemas de seguridad son mínimas

porque los usuarios pertenecen a un sólo dominio administrativo y con sus respectivas políticas.

Pero GEPON tiene un conjunto de requerimientos distintos, pues su uso va dirigido al acceso de subscriptores, sirve a usuarios privados no-cooperativos, y además tiene un canal difusión de descarga, altamente accesible por cualquier estación final, por lo que podría ser manipulada y accesada sin autorización.

Para un mecanismo completo de seguridad en una red GEPON, se debe tener en cuenta lo siguiente:

- **Autenticación fuerte**: las contraseñas no deben ser enviadas en texto plano para evitar los ataques Hombre en la Mitad (MITM, Man in the Middle).

- **Autenticación mutua**: para evitar falsas OLT's, estas deben ser autenticadas por las ONT's / ONU's.

- **Autenticación de mensajes**: para evitar la inyección de paquetes de activos durante los ataques MITM, los mensajes más sensibles deben ser autenticados.

- **Claves de la administración**: podemos evitar violaciones de privacidad si las claves utilizadas para el cifrado del tráfico de bajada se generan e intercambian en forma segura.

Con el cifrado de las transmisiones de bajada se evita la escucha ilegítima cuando no se conoce la clave de cifrado. Para esto se crea un túnel Punto a Punto (PtP, Point-to-Point) para una comunicación privada entre la OLT y diferentes ONU's.

Con el cifrado de las transmisiones de subida se evita la interceptación del tráfico de subida cuando se obstruye la transmisión, si pueden oír, pero no comprender el mensaje en el divisor PON. Con esto se previene la suplantación de ONU's, así los datos que llegan desde una ONU deben estar cifrados con una clave solo disponible para esa ONU.

Los procesos de cifrado y descifrado pueden ser implementados en la capa física, o capas más altas. Al implementar cifrado por encima de la capa MAC, ocultará solamente el contenido de la trama MAC, dejando las cabeceras en texto plano. En este caso, la MAC emisora calculará la Secuencia de Verificación de Trama (FCS, Frame Check Sequence) para la carga cifrada, y la MAC receptora confirmará la

trama recibida antes de pasar su contenido a la capa superior para ser descifrada. Este esquema evita que ONU's maliciosas puedan leer la carga, pero aun así pueden obtener las direcciones MAC de otras ONU's.

Si el cifrado se implementa por debajo de la capa MAC, se cifra todo la secuencia de bits, junto con las cabeceras de la trama y FCS. Una vez en el receptor, todos los datos se descifrarán antes de pasarlos a la capa MAC para comprobarlos. Como las claves de cifrado son distintas para todas las ONU's, las tramas no dirigidas a ninguna ONU no serán descifradas correctamente, y la MAC las rechazará. De esta forma las ONU's maliciosas no podrían obtener ninguna información, por lo que se concluye que implementar el sistema de cifrado por debajo de la capa MAC es el método más seguro y fiable.

Método de Cifrado

En una red GEPON, la transmisión de bajada es un canal de comunicación basado en tramas, donde cada trama se envía a un destino diferente. Cada trama contiene información y es independiente, por lo que es preferible cifrar cada trama por separado.

El campo linkID localizado en la cabecera de cada trama identifica el túnel entre la OLT y una ONU (PtP emulation), y también soporta el mecanismo de cifrado de GEPON. Para esto, uno de los bytes reservados en la cabecera será usado como clave de índice (key identifier). Este valor determina si la trama está cifrada, y que clave fue usado. Todo lo mencionado lo podemos visualizar en la figura 4.1, donde observamos el etiquetado de tramas Ethernet ubicado en el preámbulo antes de cada fotograma.

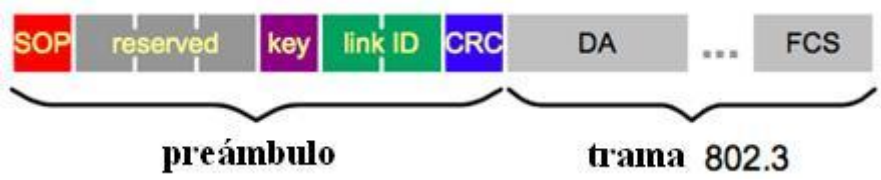

Figura 4.1. Modelo de encriptación de paquetes

Fuente: http://es.wikitel.info/wiki/UA-Redes_PON_EPON_derivados

Durante la sesión actual, cada ONU posee una clave que es validada y referenciada por la keyID, lo que permite una transición suave desde una sesión válida a la siguiente. El keyID por defecto es usado por las tramas no cifradas.

Este proceso permite mantener la seguridad de forma indefinida en los túneles ya establecidos. Si los cifrados por bloques usan un tamaño fijo, y las tramas Ethernet usan un tamaño variable, entonces

el límite del bloque puede diferir al límite del paquete, y en este caso el último bloque será rellenado según el tamaño requerido. Sabiendo que el rellenado con ceros es potencialmente débil en el cifrado, se puede aplicar un XOR a los últimos n bits (n<128) con el resultado de la segunda iteración del cifrado del próximo bloque.

El algoritmo Estándar de Cifrado Avanzado (AES, Advanced Encryption Standard), diseñado para reemplazar al Estándar de cifrado de datos (DES, Data Encryption Standard) se puede usar en redes GEPONs. Este algoritmo permite el uso de claves de 128, 192 y 256 bits (23).

En las tablas 4.2, 4.3, 4.4 y 4.5 se detallan los Ataques, Vulnerabilidades, Consecuencias y Contramedidas que se pueden presentar en los cuatro servicios que presta GEPON.

SERVICIO	ATAQUES O AMENAZAS	VULNERABILIDADES	CAPAS TCP/IP					ITEM	CONSECUENCIAS O AFECTACIÓN	CONTRAMEDIDAS
			Física	Enlace de Datos	Red	Transporte	Aplicación			
TELEFONÍA IP	Ataques de 1. Gusanos y virus, 2. Cortafuegos e IPS/IDS mal configurados.	a) Mala administración de los equipos – para ataques 1 y 2.	X					1	Acceso a la infraestructura de la red corporativa. Gatekeeper comprometido. Fraude telefónico.	Mantener el sistema operativo y antivirus actualizados y parcheados. Mantener activo el firewall. Configuración de los equipos adecuada a la red.
	Entradas malintencionadas a la red y el robo de datos a través de: 1. Ataques DoS, 2. Secuestro de	Aplica Vulnerabilidades de ITEM 1 para ataques 1 y 2 a) Robo de ancho de banda - para ataques 1. b) Inundación del sistema con llamadas comprometidas - para ataques 1.	X	X	X			2		El uso de autenticación evita portátiles no autorizadas o la conexión de visitantes sin derecho de acceso.

	sesiones (Hijacking), (Eavesdroping)	c) Falta de validación y secuenciación para - ataques 2. d) Cifrado limitado - para ataques 2.								
	Ataques 1. DoS 2. DDoS 3. ICMP unreachable 4. SYN floods 5. Gran variedad de floods 6. SQL injections 7. Denegación en DHCP 8. Man-in-the-middle 9. Buffer overflows 10. SPIT (SPAM) 11. Vishing (Phising) 12. Fuzzing 13. Floods(INVITE,REGISTER, etc) 14. Secuestro de sesiones (Hijacking)	a) Se aplica las vulnerabilidades del ataque 1 del ITEM 2 para ataques 1,2,3,4,5,6,7,9,10,12,13 b) Se aplica las vulnerabilidades del ataque 2 del ITEM 2 para ataques 8,11,14,15, 16,17 c) Inundación del sistema con llamadas comprometidas.			X	X	X	3	Tráfico malicioso que afecte la calidad del servicio.	Configurar dispositivos para que utilicen autenticación, autorización y cifrado. Establecer VLAN's. Establecer un número máximo de direcciones MAC por cada puerto, asignar estáticamente las direcciones MAC por puerto. Como medida adicional se deben separar las redes de voz y datos en VLAN's distintas. Los dispositivos de telefonía IP también deben ser aislados para tráfico entrante

	15. Interceptación (Eavesdropping) 16. Redirección de llamadas (CALL redirection) 17. Reproducción de llamadas (CALL replay)									y saliente. Llevar a cabo una auditoría del riesgo.

Tabla 4.2 Ataques, Vulnerabilidades, Consecuencias y Contramedidas GEPON – Telefonía IP

SERVICIO	ATAQUES O AMENAZAS	VULNERABILIDADES	CAPAS TCP/IP					ITEM	CONSECUENCIAS O AFECTACIÓN	CONTRAMEDIDAS
			Física	Enlace de Datos	Red	Transporte	Aplicación			
IPTV	1. Ataque de captura de tráfico, cuando los datos de bajada de los usuarios llegan a todos los CM (Cable-Modems)	a) El desvío de los cables de conexión hacia otros sistemas - para ataque 1	X					4	Acceso no autorizado a los equipos con los que la red opera	Aplica contramedidas ITEM 1
	1. Ataque MAC: en el fichero de configuración de un CM viene el número de equipos que pueden acceder a la red. El CM	a) Interceptación intrusiva de comunicación entre equipos para - ataque 1	X	X	X	X	X	5		Asignar la dirección MAC de host en cada puerto del conmutador físico - Utilizar la función de seguridad de puerto. Crear filtros o listas de acceso. Enrutar todos los

	registra las MAC								paquetes a través del CMTS (cablemodems terminales del sistema).
	1. Ataque de Modificación IP 2. Suplantación de mensajes. 3. Denegación de mensajes. 4. Aplica ataques de ITEM 3	a) Bajo nivel de autenticación (IP) - para ataques 1, 2, 3 y 4			X	X	X	6	Acceso malintencionado a los datagramas IP	DHCP snooping: puede ser configurado en los interruptores del LAN para alentar la seguridad en el LAN para permitir solamente a clientes con el IP específico. Utilizar el complemento DHCP de MMC para supervisar el DHCP. Usar protocolos seguros. Usar PGP para cifrar mails con información sensible

										- utilizar conmutadores, en lugar de repetidores convencionales. Aplica contramedidas de ITEM 3
	1. Aplica ataques de ITEM 3	a) Problemas de autenticación, integridad y de confidencialidad - para ataques 8, 11, 14, 15 del ítem 3			X	X	X	7	Acceso a protocolos de comunicación entre capas – Intercepción de sesiones TCP establecidas	Filtrado ISP, o rediseño de la implementación TCIP/IP. Filtrar los paquetes ICMP_ECHO a nivel de enrutador. Usar https o SSL para el correo electrónico, además de la digital. Aplica contramedidas de ITEM 6
	Ataques de: 1. Suplantación de DNS.	a) Deficiencias de programación – Telnet - para			X	X	X	8	Acceso malintencionado a información	Filtrar el tráfico TCP al puerto 53.

	2. Suplantación de IP. 3. Husmear. 4. Exploit de desbordamiento de buffer.	ataque 3. b) Deficiencias en proceso de autenticación - para ataques 1 y 2							almacenada en la BD del servidor DNS.	Aplica contramedidas de ITEM 1 y 6.

Tabla 4.3 Ataques, Vulnerabilidades, Consecuencias y Contramedidas GEPON – IPTV

SERVICIO	ATAQUES O AMENAZAS	VULNERABILIDADES	CAPAS TCP/IP					ITEM	CONSECUENCIAS O AFECTACIÓN	CONTRAMEDIDAS
			Física	Enlace de Datos	Red	Transporte	Aplicación			
INTERNET	Ataques de: 1. Virus, 2. Troyanos Spyware, 3. Malware, 4. Código malicioso en general	a) Se aplica las vulnerabilidades del ataque 1 del ITEM 1 – para ataques 1,2,3 y 4	X		X	X	X	9	Información de la Organización Comprometida	Poner atención a los correos que llegan con archivos adjuntos, y nunca debemos ejecutar aquellos archivos cuyas extensiones son .exe, .bat, .com. Es recomendable utilizar un segmento separado de la red, conocido como Red de Servicio o DMZ. Realizar un análisis de vulnerabilidades para identificar las debilidades actuales del sistema. Aplica contramedidas de ITEM 1.
										El uso de verificación

	1. Ataque de envío y recepción de correo basura	a) Registro de cuenta de correo en foros, colocado a disposición de todo el mundo - para ataque 1. b) Falta de cultura de las personas que se dedican a estas actividades - para ataque 1.			X	X		10	Saturación de la red. Enviados a listas negras lo que produce el rebote de todos mis correos.	por dominio, evita ser presa del relay.

	1. Ataque de Phishing (ataque transparente) 2	a) Falta de cultura de la gente al revisar correos mal intencionados. (spam) - para ataque 1.			X	X	X	11	Robo de credenciales. Robo de datos al ingresar en páginas web falsas por ejemplo en entidades bancarias.	No responder a solicitudes de información personal a través de correo electrónico. No abrir correos de procedencia extraña ni pinchar enlaces maliciosos. Para visitar sitios Web, introducir la dirección URL en la barra de direcciones.
	Ataque de: 1. Sniffing[3]. 2. Aplica Ataques de ITEM 6	a) Se aplica las vulnerabilidades de los ataque 8 y 15 del ITEM 3 - para ataque 1. b) Se aplica las vulnerabilidades de los ataques 1, 2, 3			X	X	X	12	Aplica consecuencias del ITEM 6	Bloquear ataques de Husmear a través de repetidores activos o conmutadores quienes solo reconocen direcciones propias, a las demás no las

[2] Envío de correos electrónicos que aparentan provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas Web falsificadas.

[3] Utiliza técnicas como la predicción de números de secuencia TCP, el envenenamiento de tablas caché, etc.

		y 4 del ITEM 6 – para ataque 2								deja pasar. Aplica contramedidas de ITEM 6
	Ataque de: 1. Hijacking [4](Secuestro)	a) Se aplica las vulnerabilidades del ataque 2 del ITEM 1 – para ataque 1			X	X	X	13	Secuestro de identidad del usuario. Aplica consecuencias del ITEM 11	Aplica contramedidas de ITEM 1 y 6
	Ataque de: 1. Inundación 2. Desbordamiento de buffer[5].	a) Se aplican las vulnerabilidades de los ataques 4, 9 y 13 del ITEM 3 - para ataques 1 y 2			X	X	X	14	Bloqueo de la red impidiendo su normal funcionamiento	Es recomendable que si se usa TCP todos los terminales usen el mismo protocolo. Aplica contramedidas de ITEM 3 y 6

Tabla 4.4. Ataques, Vulnerabilidades, Consecuencias y Contramedidas GEPON – Internet

[4] Toma el control de una conexión ya establecida, suplanta la identidad del usuario autorizado, mientras éste parece quedar "colgado".

[5] Inundación de la red con una enorme cantidad de mensajes inútiles. Se interceptan paquetes selectivamente y se re-direccionan a otros destinos.

SERVICIO	ATAQUES O AMENAZAS	VULNERABILIDADES	CAPAS TCP/IP					ITEM	CONSECUENCIAS O AFECTACIÓN	CONTRAMEDIDAS
			Física	Enlace de Datos	Red	Transporte	Aplicación			
VIDEO VIGILANCIA IP	1. Ataques de Autenticación[6]	a) La interfaz Web de la Cámara IP tiene como usuario y contraseña del administrador a los que vienen por defecto - para ataque 1. b) No hay Control de acceso mediante direcciones IP - para ataque 1. c) Los servidores web de las cámaras IP están desactualizados - para ataque 1.					X	15	El atacante conociendo el usuario y la clave podría controlar en su totalidad el sistema de Video Vigilancia IP.	Modificar usuario y contraseña que vienen por defecto o de fábrica. Denegar el acceso a todos los ordenadores excepto a los que tengan una dirección IP determinada.
	1. Ataque de Diccionario[7]	a) Contraseña débil - para ataque 1					X	16	El atacante puede descubrir la contraseña.	La contraseña debe seguir todos los protocolos de

[6] El usuario mal intencionado con la ayuda de un browser, conociendo la dirección IP y el puerto de la cámara podría encontrar diferentes sitios donde reporten vulnerabilidades asociadas a la interfaz web de la cámara como el usuario y contraseña del administrador por defecto.

[7] El atacante prueba muchas contraseñas que tiene en un diccionario previo y logra loguearse con una de esas contraseñas.

										seguridad necesarios.
	Ataques de: 1. Inundación de direcciones MAC/Ataques de Envenenamiento[8]	a) Tamaño limitado de la tabla CAM – para ataque 1. b) Mala segmentación de la memoria asignada a la tabla CAM – para ataque 1.		x				17	Desbordamiento de la tabla CAM(Content Addressable Memory) Podría producir una Denegación de servicio. Inundación de los puertos. El atacante puede ver todas las tramas enviados de un host victima a otro host sin entrar a la tabla CAM.	Protección y Seguridad en los puertos. Limitar e identificar el número de direcciones MAC de las estaciones de acceso permitido a a los puertos. Aplica contramedidas del ITEM 3
	Ataque: 1. Suplantación del Servidor DHCP	a) Falta de control para que exista otro DHCP en la red – para ataque 1.		x				18	Suplantación del Servidor DHCP.	Definir puertos de confianza para servidores DHCP legítimos de la red servidores DHCP que puede enviar peticiones y hacer ofertas. Al interceptar todos los

[8] El atacante bombardea al switch con tramas de direcciones MAC falsas o invalidas para que la tabla CAM del switch se llene hasta al punto que nuevas entradas no pueden ser aceptadas, cuando esto ocurre el switch envía a todos los puertos las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM inundando los puertos.

										mensajes DHCP dentro de la VLAN. Identificar los puertos confiables y no confiables. Aplica contramedidas del ITEM 6
	Ataque: 1. Al Protocolo de Resolución de direcciones (ARP Attacks) 2. Suplantación ARP, 3. Envenenamiento de enrutamiento ARP	a) No usar mecanismos de control que asocien direcciones IP con MAC – para ataques 1, 2 y 3.		x				19	Un atacante puede husmear los paquetes de datos en la red LAN, modificar el tráfico, o incluso detener el tráfico ocasionando DoS.	Configurar tanto en los conmutadores como en los servidores que una IP solo puede estar relacionado con una MAC. Proteger y almacenar las direcciones IP origen. Realizar inspecciones dinámicas del ARP. Uso de tablas ARP estáticas, añadir entradas estáticas ARP. Registro de las direcciones MAC con DHCP

										snooping. Establecer redes VLAN's privadas. Aplica contramedidas del ITEM 6

Tabla 4.5. Ataques, Vulnerabilidades, Consecuencias y Contramedidas GEPON – Video Vigilancia IP

4.1.1 NIVELES DE SERVICIOS

En la red GEPON se van a prestar cuatro servicios, los cuales se detallan a continuación:

4.1.1.1 INTERNET (IP PÚBLICA)

Hoy en día el Internet se ha convertido en una herramienta indispensable y de uso masivo, por el cual podemos comunicarnos y así compartir conocimientos y demás. Pero así como el internet nos ofrece cosas buenas y útiles, también existen ciertas amenazas que atentan contra nuestra seguridad, dichas amenazas van desde el contagio con un virus a ser hackeado por un troyano. (24). Entre los diferentes ataques que se pueden dar en este servicio están (Tabla 4.4):

- **Spam (correo basura):** tiene que ver con el envío y recepción de correos electrónicos, donde los spamer (personas que se dedican a mandar correo basura) se valen de nuestra cuenta de correo para lucrarse con la venta de bases de datos con miles de correos y mandar millones de correos basura anunciando cualquier producto.

- El spamer busca correos en páginas web usando programas llamados **spam bots**, intercambian entre ellos bases de datos de millones de correos, los localizan en grupos de noticias, los compran, los sacan de formularios falsos y reales, de otros correos (ya que al reenviar queda nuestro correo), etc.

- **Virus, Spyware y Malware:** son programas que tienen como finalidad robar la privacidad del usuario. Se instalan sin que el usuario lo sepa y actúan como un cliente (agente) que manda información (privada) del usuario de ese ordenador a servidores. Pueden saber las web por las que navegamos, los enlaces a los que accedemos, se adjudican las contraseñas almacenadas por defecto en el navegador, ralentizan nuestro ordenador, nos redirigen a otras web, etc.

  Las principales vías de infección son:

  - Ejecutar algún archivo que contiene spyware oculto.

  - Navegando por webs especialmente diseñadas para aprovechar alguna vulnerabilidad del sistema.

- Pinchando sobre algún POP-UP (ventana emergente).

- En la instalación de herramientas shareware o freeware.

- **Phishing:** consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

Medidas de Seguridad

He aquí algunas medidas de seguridad para protegernos de los ataques anteriormente mencionados:

- **Spam:** para proteger nuestra cuenta de correo contra correo basura, debemos evitar que nuestro correo este a disposición de todo el mundo, sino solo a personas de confianza.

- **Virus, Spyware y Malware:** para protegernos de ataques e infección de virus, es necesario:

  - Instalar un antivirus, un programa anti-spy y un firewall eficaces

  - Poner atención a los correos que llegan con archivos adjuntos, y no ejecutar archivos cuyas extensiones sean:

    - .exe (programa ejecutable)

    - .com (programa ejecutable)

    - .vbs (scripts de Visual Basic)

    - .src (salvapantallas de Windows)

    - .pif (archivos de información de programa)

    - .bat (archivos de proceso por lotes)

    - .eml (mensajes de correo electrónico, Microsoft Outlook)

- .dll (librería de vínculos dinámicos)

- **Phishing:** entre las medidas que se debe tener en cuenta tenemos:

  - Nunca responder a solicitudes de información personal a través de correo electrónico.

  - Para visitar sitios web, introducir la dirección URL en la barra de direcciones.

  - Asegúrese de que el sitio web utiliza cifrado.

  - Consultar frecuentemente los saldos bancarios y de sus tarjetas de crédito.

  - Informar de los posibles abusos a las autoridades competentes.

4.1.1.2 IPTV

La seguridad en los sistemas IPTV es un aspecto delicado, esencialmente en aquellos soportados por redes P2P, donde un

fallo puede provocar caídas parciales o totales del sistema. Así de manera similar a las aplicaciones P2P, podemos distinguir tres categorías principales (Tabla 4.3):

- Ataques por inundación de tráfico, dando lugar a rechazos de acceso (ataque DoS, Denial of Service) a suscriptores del servicio.

- Acceso no autorizado y ataques enmascarados, donde se puede robar el servicio (ToS, Theft of Service), disfrutándolo en lugar del subscriptor, además de comprometer información restringida.

- Eavesdropping (escuchas secretas), intercepción y modificación de información, los cuales pueden dar lugar a DoS, ToS, y de nuevo captura de información confidencial.

Para intentar combatir estos ataques, son necesarios mecanismos de control de acceso específicos, que se encarguen además de validar el contenido ofrecido por los nodos, comprobar que no es un video ilegítimo, con imágenes no

apropiadas. Estos mecanismos están basados en la arquitectura de seguridad ilustrada en la figura 4.2:

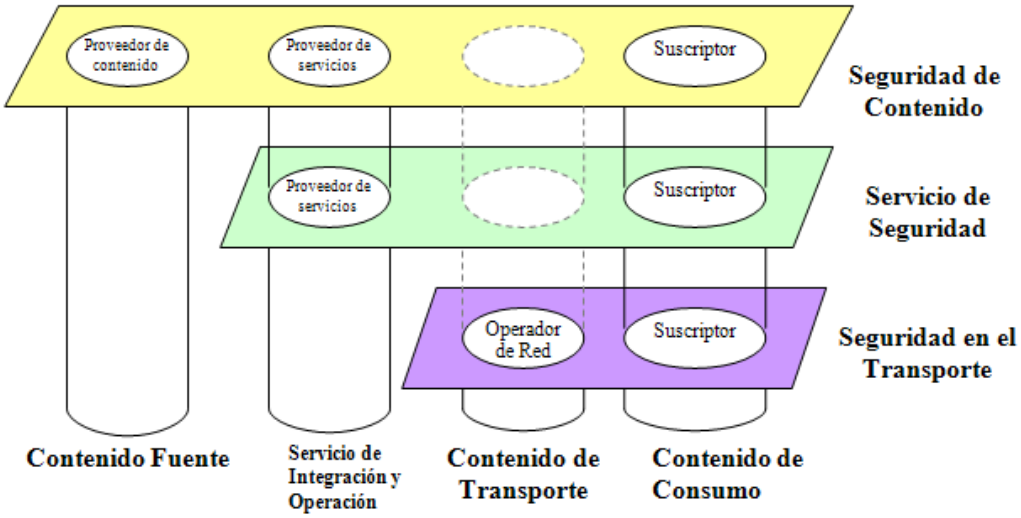

Figura 4.2. Arquitectura de Seguridad IPTV

Fuente: http://www.itu.int/md/dologin_md.asp?lang=en&id=T05-FG.IPTV-C-0140!!MSW-E

En el libro IPTV Security Protecting High-Value Digital Contents (25), un texto que destaca el alto valor de brindar protección a los contenidos digitales y a tener una visión más amplia de los desafíos a los que nos enfrentamos, David Ramírez da a conocer los resultados de un profundo estudio, y menciona: “Un caso de estudio realizado, concerniente a la seguridad en redes IPTV puso de manifiesto una serie de amenazas críticas que podrían materializarse en el futuro. La cantidad de posibles

vulnerabilidades encontradas fueron muy altas, lo que demuestra la importancia de analizar el diseño y posterior implementación de un servicio de IPTV.

De acuerdo a una evaluación de este servicio, se han identificado 69 activos de información relevantes. Estos activos se distribuyeron a través de la aplicación de IPTV, servicios e infraestructura de las capas", como se ilustra en la figura 4.3 (25):

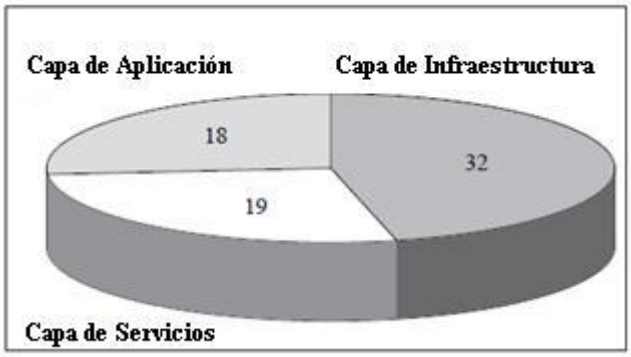

Figura 4.3. Activos Identificados

Fuente: IPTV Security Protecting High-Value Digital Contents

El estudio descrito anteriormente manifiesta que el número de activos de información incluidos en una oferta de servicios IPTV pueden variar dependiendo de los proveedores de estos servicios, que el riesgo de la vulnerabilidad obedece al tipo de

amenaza asociada (25). El estudio encontró cerca 478 vulnerabilidades potenciales, con aproximadamente 209 vulnerabilidades de alto riesgo, como indica la figura 4.4, en donde podremos visualizar una gráfica vulnerabilidades vs niveles de prioridades en las capas de aplicación, servicios e infraestructura:

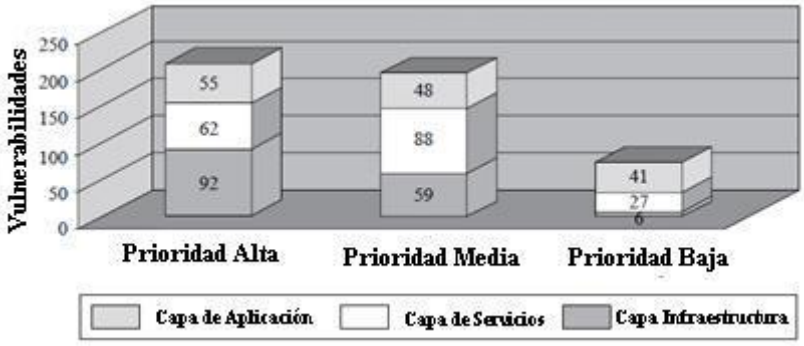

Figura 4.4. Vulnerabilidades encontradas

Fuente: IPTV Security Protecting High-Value Digital Contents

Dado que IPTV hereda todas las vulnerabilidades de seguridad de la red utilizada para el transporte y, como tal, mantendrá las vulnerabilidades presentes en los protocolos TCP/IP y dentro de los componentes de la red de transporte. Por lo tanto, se aplicarán las mismas medidas básicas necesarias para proteger a cualquier otra red TCP/IP. En la figura 4.5 podemos observar la estructura del modelo TCP/IP.

Modelo TCP/IP	
Capa	Protocolos y Dispositivos.
Aplicación	HTTP, Telnet, SMTP, DNS, FTP, TFTP
Transporte	TCP, UDP
Internet	ICMP, IP, ARP
Acceso a la Red	Driver de Red, Tarjeta de Red

Figura 4.5. Modelo TCP/IP

IPTV utiliza una pila de protocolos definida en la ITU-T Rec. J.2819. Esta pila se divide en 2 partes:

a) El grupo de capas debajo de la capa RTP, responsables de la transmisión de la información.

b) El grupo de capas por encima de la capa MPEG-2 TS, responsables de los servicios.

La Figura 4.6 muestra la pila de protocolos:

[9] The International Telecommunication Union (ITU) es un organismo de las Naciones Unidas especializado en el ámbito de las telecomunicaciones. Esta recomendación establece los requisitos para las transmisiones de señal de vídeo multicanal sobre fibra óptica basada en IP.

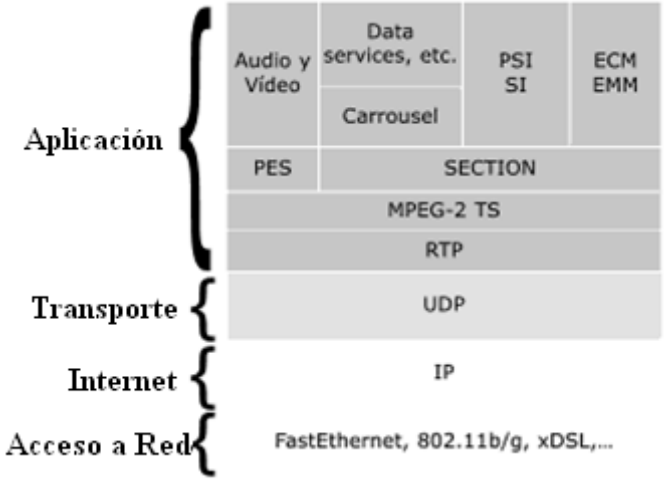

Figura 4.6. Pila de protocolos de IPTV

La multiplexación de los campos MPEG-2 TS, Section, PES y Carrousel viene definido en la recomendación ITU-R BT.1300 10y en la ITU-T Rec.

J.18311. ECM/EMM vienen definidos en el estándar ARIB STD-B25 12sobre el sistema de acceso condicional sobre broadcast digital. PSI/SI viene incluido en la ITU-T Rec. J.9413 y en el estándar ARIB STD-B1014 sobre información de servicio para sistemas de broadcast digital. El campo Data Services viene

[10] Servicio múltiplex, transporte y los métodos de identificación para la radiodifusión de televisión digital terrestre.
[11] Describe una multiplexación por división de tiempo (TDM), formato para la transmisión de múltiples MPEG-2, flujos de transporte con una implementación sencilla en los sistemas de televisión por cable
[12] Sistema de Acceso Condicional para la radiodifusión digital
[13] Servicios de información para la radiodifusión digital en los sistemas de televisión por cable
[14] Servicio de Información para el sistema de radiodifusión digital

definido en la ITU-T Rec. J.200/201.202 15y en el estándar ARIB STD-B2416. El audio y video viene definido en la ISO /IEC 13818.

Ahora bien, teniendo en cuenta que protocolo opera en cada capa, debemos considerar las vulnerabilidades de cada protocolo para prevenir posibles ataques, esto se aprecia en la tabla 4.6:

En un **ataque MAC**, que pasa si cambio la MAC de mi tarjeta de red por la de otro usuario? Lo que sucederá es que llegará el tráfico de llegada de otro equipo que está conectado al mismo CMTS (cablemodems terminales del sistema) pero con otro CM (Cablemodems), pero, igualmente al otro usuario le llegará mi tráfico de bajada, lo que levantará una alerta de duplicidad de MACs en la red, es decir, que el sistema ve que recibe paquetes pero que esa IP no es la suya. Esta alerta se puede eludir sencillamente no generando tráfico de red.

[15] J.200: Worldwide common core- Aplicación de Medio Ambiente para series de televisión digital / J.201: Armonización del formato de contenido declarativo para aplicaciones de televisión interactiva / J.202: define las API, las garantías de semántica y los aspectos del sistema de comportamiento plataforma para armonizar los formatos de contenido de procedimiento para aplicaciones de televisión interactiva

[16] Especifica el sistema de codificación monomedia, multimedia, y el sistema de transmisión de datos utilizado para los datos de difusión de la radiodifusión digital

Es importante enfocarnos en la seguridad en la capa 2, pues allí las direcciones MAC no pueden ser falsificadas, un conmutador no permite hacer sniffing, y las VLAN's están aisladas completamente unas de otras.

El **Espionaje DHCP** es una serie de técnicas de la capa de internet. Trabaja con la información de un servidor de DHCP. Asegura integridad del IP en un dominio cambiado de la capa 2.

En cuanto al **secuestro de sesión**, al tratar de usar la firma digital con archivos o mensajes de correo electrónico, no impedirá el secuestro de sesión, pero sin duda evitará que se alternen los mensajes reales por los intrusos. Este ataque es muy difícil de detectar por los dispositivos de detección de intrusos y sistemas de prevención, por lo que la mayor parte de su prevención depende de la aplicación de software de correo electrónico (como "cookie" es controlado en una sesión de Internet).

PROTOCOLO	CAPA	AMENAZAS	VULNERABILIDADES	ATAQUES	CONTRAMEDIDAS
TCP	Transporte	Interrupción del servicio	Conexiones abiertas	Ataques de denegación de servicio, (TCP SYN) – Secuestro de conexión (IP Spoofing attacks)	SYN cookies - Soluciones de cifrado - Filtrado de paquetes del tráfico de entrada desde el exterior del sistema
IP	Internet	Entrega equivocada o falta de entrega de paquetes – Datos corruptos o duplicados	Falta de validación y secuenciación	El robo de identidad - Hacking	Transmission Control Protocol (TCP) - Address Resolution Protocol (ARP) - IPv6 e IPSec
UDP	Transporte	Interrupción del servicio	Débil Validación	Ataques UDP flood (Ping de la muerte)	Control de acceso ICMP
Ethernet	Acceso a la Red	Suplantación de identidad	Reutilización de frame buffers	De denegación de servicio (DoS) – Eavesdropping (Espionaje)	Segmentación – Filtrado – Cifrado

Tabla 4.6. Vulnerabilidades por protocolo

4.1.1.3 TELEFONIA IP

Telefonía IP es una tecnología que va de la mano con capas y protocolos de las redes de datos. Por eso en cierto modo la telefonía IP va a heredar ciertos problemas clásicos de seguridad que afectan al mundo de las redes de datos (26). Por ello posee una arquitectura de seguridad ilustrada en la figura 4.7:

Figura 4.7. Arquitectura de Seguridad para Telefonía IP

Fuente: http://www.uv.es/montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf

En la tabla 4.7 se muestran algunos de los puntos débiles y ataques que afectan a cada una de las capas (26).

CAPA	ATAQUES Y VULNERABILIDADES
Políticas y Procedimientos	Contraseñas débiles. Ej: Mala política de privilegios Accesos permisivos a datos comprometidos.
Seguridad Física	Acceso físico a dispositivos sensibles. Ej: Reinicio de máquinas. Denegaciones de servicio.
Seguridad de Red	DDoS ICMP inalcanzable Inundación de sincronización (SYN floods) Gran variedad de inundaciones
Seguridad en los Servicios	Inserción de SQL Denegación en DHCP DoS
Seguridad en el S.O.	Sobrecarga de Buffer Gusanos y virus Malas configuraciones.
Seguridad en las Aplicaciones y protocolos de Telefonía IP	Fraudes SPIT (SPAM) Vishing (Phising) Fuzzing Floods (INVITE,REGISTER,etc..) Secuestro de sesiones (Hijacking) Interceptación (Eavesdroping) Redirección de llamadas (CALL redirection) Reproducción de llamadas (CALL replay)

Tabla 4.7. Ataques y Vulnerabilidades VoIP por Capa (26)

TIPOS DE ATAQUES

Durante los siguientes apartados se va a intentar detallar cuáles son las amenazas más significativas que afectan a la telefonía sobre redes IP (26) (Tabla 4.2).

Fuzzing

- Envío de paquetes malformados en busca de errores en la programación.

- Desbordamientos de buffer, sobreescritura de memoria.

- Fallos de segmentación.

Inundación

Ataques de denegación de servicio (DoS) por inundación. La víctima se ve saturada de paquetes inservibles y es incapaz de procesar peticiones válidas, como se observa en la figura 4.8.

Diferentes opciones:

- Inundación de mensajes SIP.

- Inundación UDP.

- Inundación RTP.

Herramientas

- Inviteflood

.

- Udpflood.

- Rtpflood.

- Sipsak.

- Sipp.

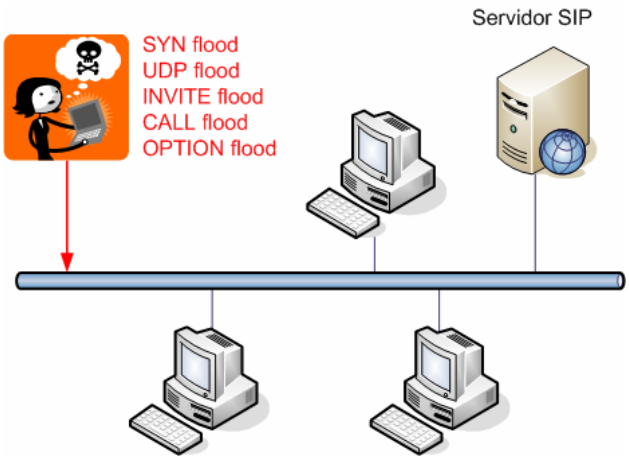

Figura 4.8. Ataque Flooding (26)

Call Hijacking

- Inundaciones en destinos de teléfono.

- Falsos de registro.

- Las llamadas se enrutan a la ubicación descrita en el nuevo registro (figura 4.9).

- Elaborar una solicitud de registro.

- En el encabezado "Contacto" inserte su dirección IP.

- Enviar la solicitud de registro para el proxy SIP.

- Hacer una llamada telefónica al usuario que imitan a ver si la llamada es desviada (figura 4.10).

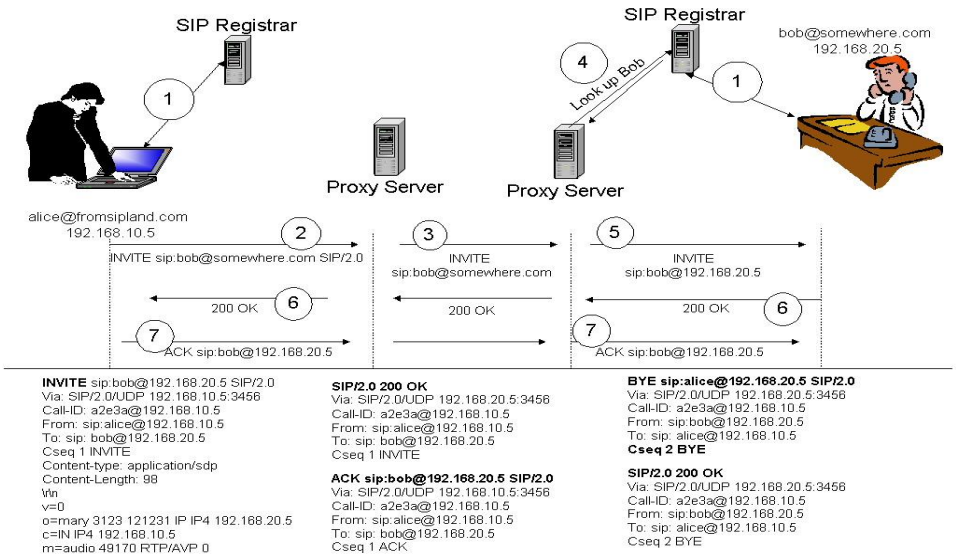

Figura 4.9. Ejemplo de una llamada SIP

Fuente: http://www.slideshare.net/Catharine24/attacks-against-voip

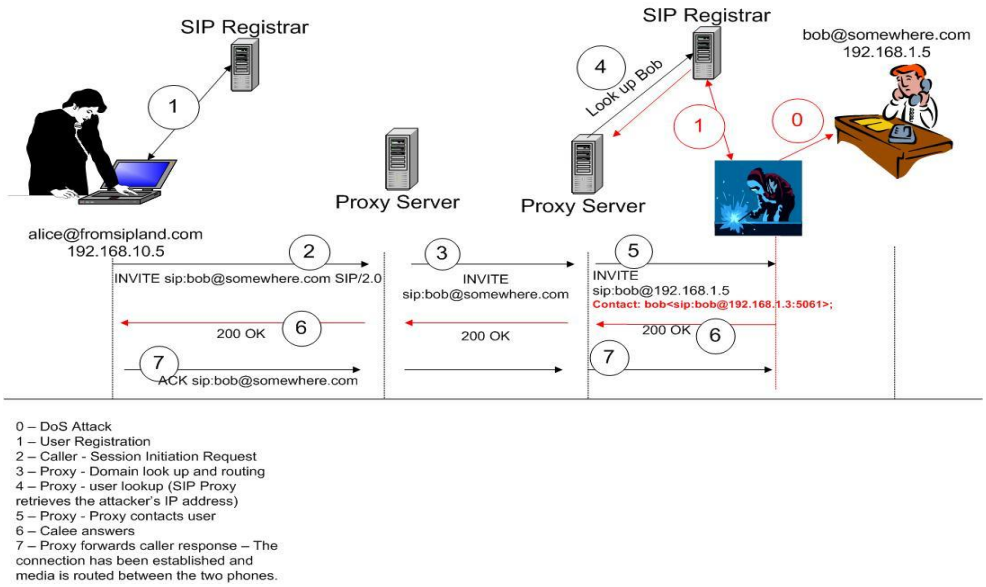

Figura 4.10. Ejemplo de un ataque Call Hijacking

Fuente: http://www.slideshare.net/Catharine24/attacks-against-voip

Espionaje y análisis de tráfico (Eavesdropping)

- El ataque más temido / impactante.

- A través del ataque de un Hombre en la Mitad (MITM, Man-In-The-Middle) previo, el atacante consigue "ver" toda la información, como indica la figura 4.11.

- Señalización.

- Flujo multimedia.

- Se compromete la privacidad del usuario.

- Análisis de tráfico.

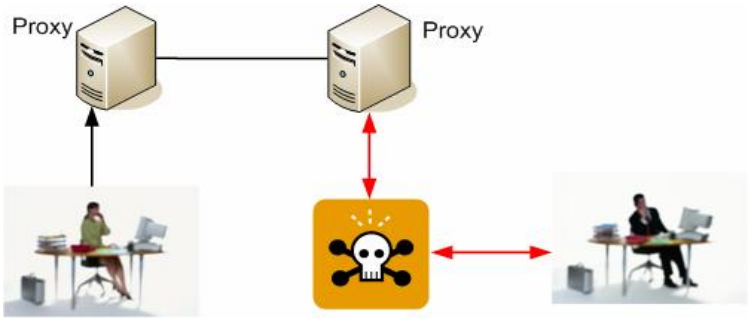

Figura 4.11. Hombre en el medio

ASEGURANDO LA RED DE TELEFONÍA IP

Mantener los sistemas actualizados y parcheados. Es estrictamente requerido, y no tan solo en infraestructura de telefonía IP, si no para todos los servicios, que el administrador de la red esté al corriente de los nuevos parches y actualizaciones y los aplique en sus sistemas.

Es fundamental para los servicios que brinda GEPON, que estos sobre una infraestructura de red segura, protegidas por **cortafuegos** bien administrados y **antivirus** actualizados que la

protejan de ataques de virus, gusanos y troyanos. Una medida de alerta ante la posible presencia de muchos ataques se puede realizar instalando sistemas de detección de intrusos (**IDS**) o de prevención (**IPS**) en los lugares estratégicos de la red. Estos sistemas son capaces de detectar y prevenir ataques contra los protocolos (fuzzing), ataques contra servicios (exploits y vulnerabilidades), escaneos y ciertos tipos de ataques DoS. Es esencial que el IDS/IPS sea configuración adecuada de acuerdo a los requerimientos de la red en que funcione para conseguir su fiabilidad adecuada.

Es aconsejable alterar los protocolos y configurar dispositivos para que utilicen **autenticación** en todos los mensajes que se intercambia. Además de la autenticación, existen dos medidas adicionales para la seguridad en telefonía IP, estas son, la **autorización** y el **cifrado**. Los dispositivos deben tener un restringido grupo de elementos o direcciones IP de los que pueden recibir tráfico. Por ende si se realiza una correcta configuración en dichos dispositivos es posible limitar muchos de los ataques de denegación de servicio.

El **cifrado** es una de las medidas más importantes que se debe implementar para lograr tener una segura infraestructura de telefonía IP. El uso de TLS/SSL (Transport Layer Security – Seguridad Capa de Transporte/Secure Sockets Layer – Seguridad Capa de Conexión) ayuda a establecer canales de comunicación seguros que resolverá la mayoría de problemas de **eavesdroping**, manipulación y reproducción de los mensajes que se intercambian.

Los teléfonos IP pueden utilizar el protocolo SRTP para cifrar el audio que transfieren. **Secure RTP** es un protocolo mejorado del RTP que ofrece confidencialidad, autenticación de mensajes y protección evitando los ataques de interceptación e inserción de audio. El uso de SRTP es ideal para proveer telefonía IP ya que ofrece una compresión de las cabeceras y no afecta prácticamente a las Qos. Es recomendable que el canal de señalización vaya completamente cifrado.

El necesario el uso **VLAN's** en los equipos de la red con el fin de priorizar y proteger el tráfico de telefonía IP separándolo los canales lógicos de las redes de datos.

Limitar los volúmenes de datos y ráfagas de paquetes en puntos estratégicos de la red para evitar gran cantidad de ataques DoS (26).

Y finalmente algunos consejos para protegerse de ataques de enumeración:

- Corregir los protocolos que contestan de modo diferente si el usuario existe o no.

- Configurar correctamente los servicios para que no muestren más información de la necesaria.

- No usar nombres por defecto para archivos de configuración.

- En lugar de usar TFTP, FTP, es mejor utilizar un canal cifrado.

- Desactivar puertos de administración http y snmp.

- Cambiar el password por defecto de todos los lugares.

Telefonía IP y Firewalls

En la tabla 4.8 se aprecia problemas vs soluciones para prevenir posibles ataques.

Problemas	Soluciones
NAT transversal	Puertas de Enlace de la Capa de Aplicación (ALGs , Application Layer Gateways)
SIP spam	Controladores de sesión de frontera (Session Border Controllers)
Varios ataques, incluyendo denegación de servicio	ICE - Establecimiento de conectividad interactiva (STUN, TURN, MIDCOM)

Tabla 4.8. Telefonía IP and Firewalls

Fuente: http://www.slideshare.net/Catharine24/attacks-against-voip

VLAN

A pesar de que nos permiten separar las redes:

- Voz.
- Datos.

Restricciones de acceso:

- Filtrado por MAC.
- Filtrado por puerto 802.x.
- QoS.

No imposibilitan los ataques pero lo ponen más difícil.

SIP sobre TCP/TLS

- Evitamos la inundación en gran medida
    - Números de secuencia.
    - Saludo de tres vías.
- Si se usa TCP es necesario que todos los terminales usen exclusivamente TCP.
- Posibilidad de usar TLS (RFC2246)

- Cifrado de la señalización.

- Mecanismo fuerte de autenticación.

- No es Terminal – Terminal.

- Se garantiza la autenticidad, confidencialidad, integridad y no repudio.

    - A menos que sea un interno.

SRTP y ZRTP

Objetivo de SRTP (RFC3711): Asegurar el tráfico RTP

- Cifrado

- Autenticación

- Integridad

Mecanismo de clave maestra y claves derivadas para el cifrado (AES)

- Obtención de la primera clave maestra
    - ZRTP
    - MIKEY

Túneles VPN

- Posibilidad de establecer conexiones seguras en medios hostiles.
    - Internet.
- Relativamente sencillas de implementar.
- Bajo costo.
- Algunos terminales implementan soluciones VPN.

- Snom 370 (OpenVPN).

Sistemas de Detección de Intrusos (IDS)

- Sistema para detectar accesos no autorizados.

- Sistema IDS/IDP.

  - Software Libre.

  - Plugins libres (Community).

  - Plugins propietarios (VRT).

  - Plugins para telefonía IP y SIP.

Herramientas

- SIVuS – Escaneo de vulnerabilidades de telefonía IP – www.vopsecurity.org

Más herramientas se están desarrollando basándose en la Ocurrencia vs Herramientas vs Dificultad de Ataque. Ver figura 4.12.

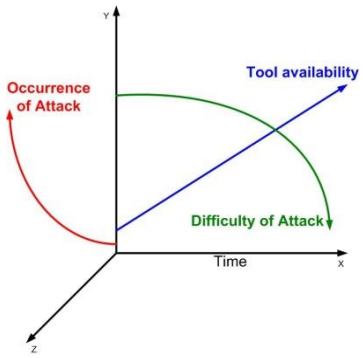

Figura 4.12. Ocurrencia vs Herramientas vs Dificultad de Ataque

Fuente: http://www.slideshare.net/Catharine24/attacks-against-voip

4.1.1.4 VIDEO VIGILANCIA

Los sistemas de Video Vigilancia IP utilizan direccionamiento IP y direcciones MAC para poder funcionar correctamente, por esta razón heredan las vulnerabilidades más comunes en los servicios IP como:

- Acceso no autorizado.

- Denegación de servicios.

- Escucha de tráfico.
- Alteración de información.

- Suplantación de identidad de usuario y terminal.

Para evitar que estas vulnerabilidades se conviertan en amenazas que atenten contra un sistema de Video Vigilancia IP se debe aplicar las mismas políticas y contramedidas de seguridad ya descritas en los servicios de IPTV, VoIP, telefonía IP y demás servicios tradicionales, las cuales deben ser aplicadas en PCs y servidores.

Protocolos de Transmisión de Video

El protocolo de transmisión de video más utilizado es el conjunto de protocolos TCP/IP para poder establecer la comunicación entre computadoras y enviar los datos por la red.

Dentro de este conjunto de protocolos se encuentra el Protocolo de Transferencia de Hipertexto (HTTP, Hypertext Transfer Protocol) que es utilizado en los sistemas de video vigilancia para que los usuarios con permisos de acceso y que se

encuentren en cualquier localidad puedan acceder a las cámaras empleando un navegador web.

En la tabla 4.9 se muestran los protocolos más comunes de transmisión de video con los puertos más atacados, se indican algunas de las vulnerabilidades que hacen que los posibles ataques se materialicen y además se proporcionan unas contramedidas para evitar que el sistema de video vigilancia IP sea vulnerable.

Para implementar un sistema de Video Vigilancia seguro se debe considerar las vulnerabilidades de la tabla 4.9, también se debe dar la protección necesaria contra ataques de virus, malware, acceso no autorizado a las cámaras, uso incorrecto y no autorizado de los datos para garantizar la integridad, confidencialidad y disponibilidad de los datos y la privacidad de las personas.

Protocolo	Protocolo de Transporte	Uso de Video en red	Vulnerabilidades	Ataques	Contramedidas Solución
FTP Protocolo de Transferencia de Archivos (File Transfer Protocol)	TCP, puerto 21	Transferencia de imágenes o vídeo desde una cámara de red o servidor de vídeo a un servidor FTP o a una aplicación	Contraseñas por defecto	Alteración de la información	Cambiar automáticamente las claves de las cuentas de usuario por defecto.
			Contraseñas débiles	Ataques de Fuerza Bruta[17] y Ataques de Diccionario[18]	Establecer políticas robustas de contraseñas. Monitoreo de Sesiones. Mayor control en las listas de acceso de los enrutadores.
			Mala configuración del servidor	Transferencia de archivos, virus, programas	A cerciorarse de que el servidor FTP está bien configurado[19]
			No bloqueo de entradas muy largas	Desborda-miento del buffer	Limitar el tamaño de las entradas.
			Mal uso del	Ataque de Rebote[20]	Garantizar que el

[17] Un ataque de Fuerza Bruta se da cuando un usuario malicioso descubre la clave de acceso a un sistema probando con todas las posibles combinaciones.

[18] Los ataques de Diccionario son más eficientes que los ataques de fuerza bruta, los usuarios maliciosos para descubrir la clave de acceso prueban con todas las palabras de un diccionario predeterminado.

[19] Consideraciones al momento de configurar un servidor FTP: las cuentas anónimas debe tener permiso de solo lectura y no se les debe permitir ver lo que hay dentro de los directorios, restringir el acceso al servidor FTP con las cuentas de usuario del sistema, controlar el acceso a cualquier demonio FTP, se recomienda utilizar herramientas para revisar la integridad de los directorios y archivos en el servidor (registro de entradas al subir y bajar archivos)

[20] Ataques de rebote a FTP se dan con el fin de tener acceso a puertos restringidos el intruso utiliza otra máquina como intermediario para acceder al objetivo.

			comando PORT		comando PORT no puede ser usado para establecer conexiones con máquinas de IP o MAC restringidas.
SMTP Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol)	TCP puerto 25	Una cámara de red o servidor de vídeo puede enviar imágenes o notificaciones de alarma utilizando su cliente integrado de e-mail	Mala configuración del servidor	Acceso a información confidencial	Verificar la correcta configuración del servidor[21]
			Carencia de autenticación.	Suplantación de identidad SMTP Spoofing[22]	Configuración de autenticación, desactivación de acceso anónimo
			Dirección de correo pública o expuesta en foros, blogs, etc.	El correo electrónico comercial no solicitado Spam	Utilizar listas de distribución restringidas, herramientas y creación de filtros anti-spam, ocultar correo
			Limites de mensajes no establecidos	Denegación de Servicio	Limitar almacenamiento en buzones y carpetas públicas, número máximo de destinatarios por

[21] Consideraciones al momento de configurar un servidor SMTP: no colocar el directorio del spool de correos en volúmenes compartido NFS debido a que no mantiene control de usuarios lo cual hace sensible a que otros usuarios puedan leer los correos de otros, los usuarios de correo electrónico solo deben acceder al servidor usando un programa de correo

[22] SMTP Spoofing en este tipo de ataque se falsifica el origen de los mensajes de correo electrónico (identidad falsa) para enviar una gran cantidad de correos basura.

					mensaje y un tamaño máximo de mensaje.
			Acceso a enlaces financieros falsos recibidos por correo electrónico	Robo de datos Phishing	Digitar la dirección no por enlace. Verificar que la url comience con "https://" y la vigencia del certificado digital
			Protección contra virus inadecuada	Ataques de virus	Bloqueo de datos adjuntos ejecutables.
HTTP HyperText Transfer Protocol()	TCP puerto 80	El modo más común de transferencia de vídeo desde una cámara de red o servidor de vídeo donde el dispositivo trabaja como un servidor web, proporcionando vídeo al usuario o servidor de aplicación	Eludir la autentificación23	Alteración de información	Actualizar versiones del software de gestión de video con la mayor brevedad posible.
			Validaciones de entradas inseguras, permitiendo inyección de código	Cross-Site Scripting XSS[24]	Verificar y limpiar la información ingresada por el usuario antes de utilizarla, filtrar código malicioso ingresado.
HTTPS Hypertext Transfer Protocol over	TCP puerto 443	La transmisión de vídeo desde	Falta de solicitud de autenticación	**Surf jacking**	No usar el mismo navegador para sitios

[23] Salto del paso de autenticación, colocando una barra más en la url así http://IP-de-la-camara//admin/admin.shtml

[24] Un ataque **XSS** (Cross Site Scripting) consiste en ingresar código malicioso en formularios de aplicaciones Web y si estos no están validados correctamente el código ingresado puede alterar la información de la aplicación.

Secure Socket Layer		una cámara de red o servidor de vídeo puede ser utilizada para autenticar los envíos de la cámara utilizando certificados digitales X.509	después de un largo periodo		con http y https. Usar cookies con banderas de seguridad activado
RTP Protocolo de Transporte en Tiempo Real - Real Time Protocol	UDP/TCP	Un modo común de transmitir vídeo en red MPEG. La transmisión puede ser unicast (uno a uno) o multicast (uno a varios)	Límites de tiempo no establecidos	Ataque de Repetición Replay Attack	Utilizar el protocolo Usar periodos de sesión y SRTP Secure Real-time Transport Protocol

Tabla 4.9. Protocolos de Transmisión de Video (27)

CONSIDERACIONES EN LOS COMPONENTES DE UN SISTEMA DE VIDEO VIGILANCIA IP

A continuación se detallan consideraciones necesarias que deben cumplir los componentes de los sistemas de video vigilancia IP para minimizar sus vulnerabilidades y ataques (28).

Consideraciones en las cámaras IP

Es necesario utilizar video cámaras IP que cumplan las siguientes medidas de seguridad:

- Bloquear el sistema.
- Cifrar los datos a transmitir.
- Restringir la introducción de software no autorizado.
- Protocolo HTTPS/SSL integrado en la cámara para certificar el servidor de envío y la garantía de que los datos de entrada no fueron modificados.

- Proteger al sistema de ataques

- Incorporar marcas de agua cifradas al flujo de datos (datos como hora, ubicación, usuarios, alarmas).

CONSIDERACIONES EN EL SOFTWARE DE ADMINISTRACIÓN DE VIDEO

El software de Administración de video debe contemplar las siguientes características:

- Activar el nivel de acceso para que solo puedan acceder las IP autorizadas.

- Solicitud de autentificación de usuario y contraseña.

- Establecer permisos de acceso creando diferentes niveles y grupos de usuarios para ciertas funcionalidades.

- Detección de intrusión en los ataques de fuerza bruta (combinación de usuarios y contraseñas), la petición de acceso no autorizada será negada e informada al

administrador del sistema y se bloqueará las direcciones IP que realizaron las peticiones de acceso no autorizado.

- Ofrecer el mecanismo de huella digital para evitar la alteración de los archivos de imagen.

- Protección contra inyecciones SQL.

- Protección contra Cross-Site Scripting (XSS).

- Procesamiento de Cifrado HTTPS (SSL).

- Balanceo de carga de tráfico de visitas.

- Reportes y registros de los accesos y transacciones realizadas.

CONSIDERACIONES EN LA RED DE UN SISTEMA DE VIDEO VIGILANCIA IP

En la figura 4.13 se aprecia una Arquitectura de Red de Video Vigilancia IP, la cual debe considerar los siguientes aspectos:

- Restringir el acceso remoto no autorizado con túneles VPN.

- Colocar firewalls o cortafuegos, implementar una configuración de software a un enrutador o en un dispositivo independiente.

- Instalar antivirus en los servidores y host.

- Utilizar listas de control de acceso ACL donde se restringe el re-envío de tráfico a un determinado destino sobre la base de alguna regla o política administrativa.

- Segmentar la red con VLAN's incluyendo cortafuegos para permitir la comunicación en redes segmentadas.

- Utilizar métodos de cifrado como WEP (Privacidad equivalente cableada) o WPA (Acceso protegido WiFi) en redes WLAN (red de área local inalámbrica-Wireless Local Area Network)

- Actualizar los sistemas operativos regularmente con los paquetes de servicio y parches del fabricante.

- Utilizar IDS/IPS para detectar accesos no autorizados y prevenir ataques.

- Utilizar proxy de seguridad para HTTP, HTTPS, FTP, SMTP, DNS.

- Protección contra ataques de DoS, escaneo de puertos, botnets y desbordamientos.

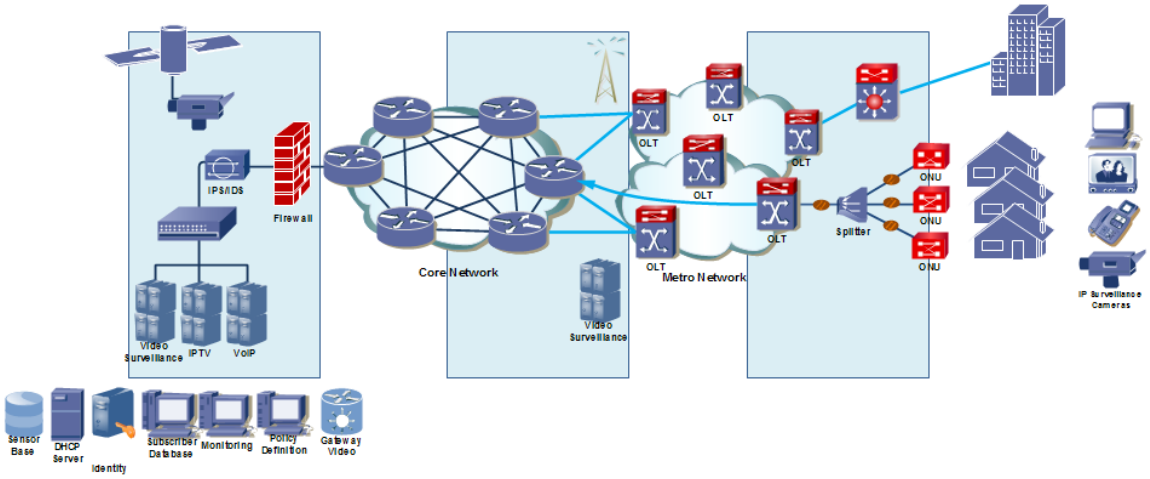

Figura 4.13. Arquitectura de Red de Video Vigilancia IP

Configuración del flujo de trabajo

En la figura 4.14 se observa todo el proceso de la Configuración del flujo de trabajo.

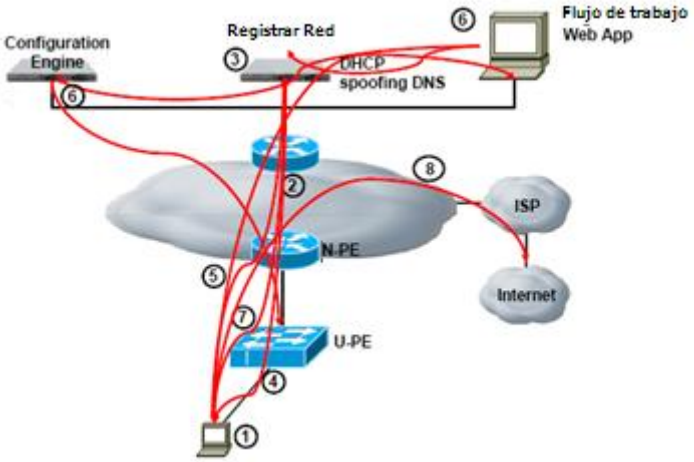

Figura 4.14. Configuración del flujo de trabajo

a) El usuario cliente se conecta a la PC.
b) La PC envía solicitud DHCP y el conmutador agrega la opción 82.
c) Se verifica si el cliente existe.
d) Si no encuentra al cliente, devuelve dirección IP temporal con IP de DNS server.

Spoofing.- uso de técnicas de suplantación de identidad generalmente con usos malware.

El usuario abre el browser; se envía una petición HTTP para redirigir al usuario a la aplicación de registro por Spoofing server.

El usuario se registra y selecciona el ISP proveedor de servicio, luego la aplicación web agrega al usuario como cliente, y se configura la VLAN en la configuración del conmutador.

El usuario se reinicia; PC envía peticiones al DHCP, el enrutador añade opción de 82; y se extrae los controles de acceso para el cliente.

En el caso de que el usuario exista como cliente, se le proporciona la dirección IP del ámbito de aplicación del ISP y de esta manera el usuario puede navegar por la web.

4.1.2 REQUISITOS DE SEGURIDAD

4.1.2.1 DISPONIBILIDAD

Con la tecnología GEPON existen mayores ventajas en la disponibilidad comparadas con otras topologías (ver figura 4.15), por ejemplo:

Topología Switch: Existen algunos componentes activos en la red, pero la falla de uno de ellos representa un problema potencial de la red, seguido de una caída del servicio.

Topología GEPON: Existe una trayectoria pasiva entre los nodos OLT y el ONU. Se esperan menos problemas que los del equipo activo, por lo que la red tiene un mayor grado de disponibilidad.

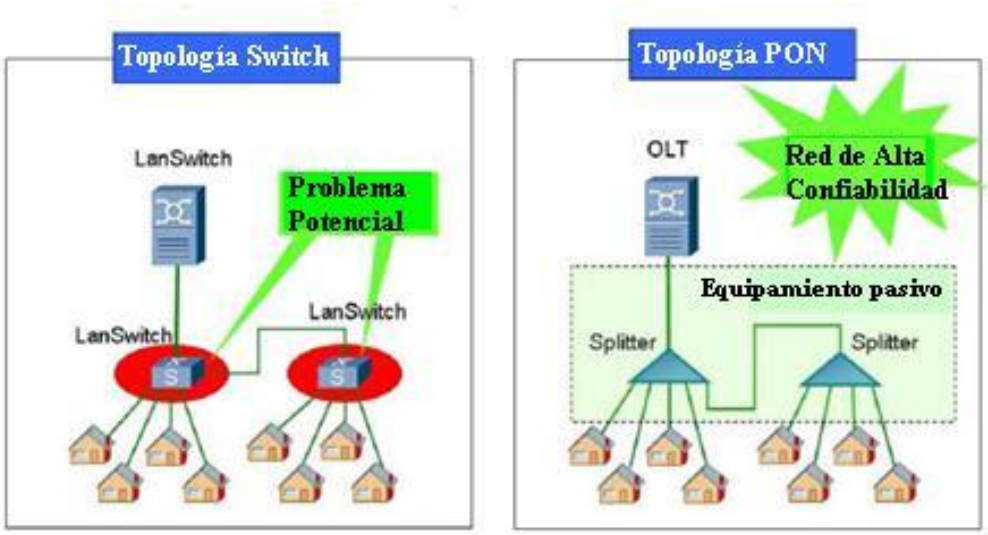

Figura 4.15. Ventajas de Disponibilidad con GEPON

Fuente: http://www.revistaitnow.com/bajar.php?a=td10/p/gt/16-_amnet.pdf

Otra ventaja que presenta GEPON es un ahorro neto en lo referente a inversión y mantenimiento de los equipos, lo cual lo hace más accesible (29). En la figura 4.16 se ilustran las ventajas de GEPON:

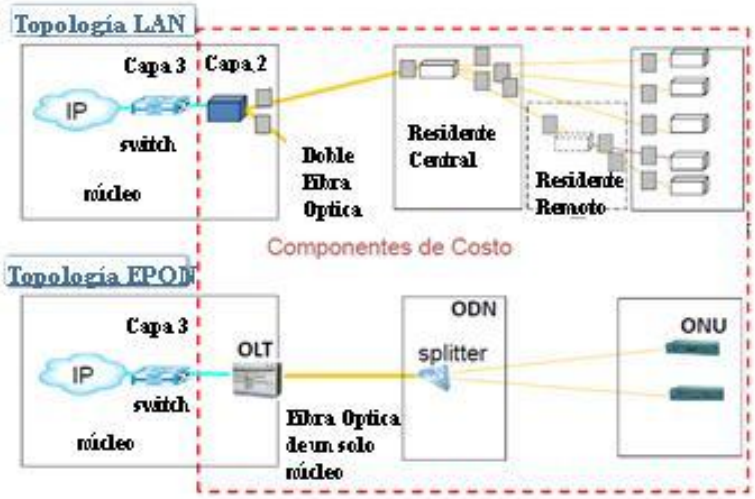

Figura 4.16. Ventajas de GEPON - Ahorro

Fuente: http://www.revistaitnow.com/bajar.php?a=td10/p/gt/16-_amnet.pdf

4.1.2.2 CONFIDENCIABILIDAD

Como ya se mencionó antes, la seguridad no ha sido uno de los puntos fuertes de las redes Ethernet; en general, para establecer la seguridad en redes GEPON, los operadores de red deben ser capaces de garantizar la privacidad del subscriptor, y deben proveer mecanismos para el control de acceso de los subscriptores a la infraestructura.

En un entorno de acceso residencial, los usuarios individuales esperan que sus datos permanezcan privados. Los dos grandes problemas asociados a la falta de privacidad son la

susceptibilidad de que los subscriptores sean "escuchados a escondidas" por sus vecinos (asunto de suscriptores), y la susceptibilidad de que el servicio sea usado sin el consentimiento el proveedor (asunto del proveedor). Exploremos estos dos problemas (23):

- **Escucha sin consentimiento**

En GEPON, este ataque puede darse al manipular una ONU en modo promiscuo, así la ONU puede escuchar el tráfico dirigido a otras ONU’s durante el tráfico de bajada.

PtPE (Point-to-Point Emulation) agrega links IDs para que cada ONU pueda reconocer tramas dirigidas a ella y descartar el resto, pero esto no es suficiente, pues una ONU puede deshabilitar este filtrado y monitorizar todo el tráfico.

Pero la transmisión de subida en GEPON es un poco más segura, ya que el tráfico de subida es visible solamente para la OLT, pero puede suceder que ocurran reflejos en el combinador pasivo, enviando alguna señal de subida por el de bajada otra vez, entonces la transmisión de bajada se produce con una

longitud de onda diferente a las de las transmisiones de subida, quedando así la ONU "ciega" para el tráfico reflejado.

- **Acceso ilegítimo al servicio**

Sucede cuando un suscriptor suplanta la identidad de su vecino, transmitiendo y recibiendo tramas que serán cobradas a cuenta del vecino. La OLT obtiene la identidad del subscriptor mediante el link ID insertado por cada ONU en las cabeceras de las tramas. Este link ID puede ser falsificado por ONU’s maliciosas al transmitir en sentido de subida. Para poder transmitir en el intervalo de tiempo "secuestrado", la ONU ilegítima debe poder "escuchar" los mensajes GATE que van dirigidos a la víctima.

4.1.2.3 INTEGRIDAD

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace

que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información.

4.1.3 AMENAZAS Y VULNERABILIDADES

ACTIVO DE INFORMACIÓN	AMENAZAS	RIESGO	VULNERABILIDADES
Fibra Óptica	Mala configuración	Crítico	Contratar personal No calificado
	Fallas Técnicas	Medio	Problemas de atenuación debido a varios factores: la absorción interna de la fibra, la difusión de la fibra, las conexiones y las discontinuidades
			Instalación ineficiente
	Daño de hardware	Medio	Envejecimiento del hidrógeno por el tiempo que tiene la fibra óptica
			Comprar de hardware de mala calidad
			Fragilidad de las fibras
			Dificultad de reparar un cable de fibra roto en el campo
	Fallas Naturales	Bajo	Utilizar tramos largos de fibra hacia cada abonado
			Descargas atmosféricas
			Incendios
			Impactos Peligrosos
			Agresividad Química de la atmósfera
OLT	Daño de hardware	Medio	Compra de hardware no compatible
	Mala configuración	Crítico	Falta de políticas, Control de Cambios
Optical splitters	Pérdida o atenuación	Crítico	Dispositivo pasivos no requiere alimentación

	Falla de conexión	Alto	Pérdidas por fallas en la señal del OTDR
	Cambio del equipo	Bajo	Causar molestia en los clientes durante la conexión
ONU	Daño de hardware	Medio	Compra de hardware no compatible
	Mala configuración	Crítico	Falta de políticas, Control de Cambios
Red GEPON	Pérdida de Óptica	Alto	Larga duración de la fibra
	Alteración de la información	Medio	Falta de especificación de tipos de identificación OLT y mecanismos de autenticación.
	Ataque "Man In The Middle (MITM)"	Alto	contraseña y clave enviada en texto plano
	Ataque de DOS	Alto	Ataque a nivel GPON durante las fases de activación
	Daño de hardware	Medio	Mayor capacidad de servicios soportados por un mismo cable de FO, vuelve más crítico los incidentes de roturas
	Error de transmisión	Medio	Inconvenientes en el OLT, ONU,etc
	Mal diseño de la red	Bajo	No se estableció la atenuación
	Falla Humana	Bajo	Tecnología nueva y requiere un mayor esfuerzo de capacitación y adaptación de las estructuras operativas

Tabla 4.10. Amenazas y Vulnerabilidades Red GEPON

4.2 ESCENARIOS DE ATAQUE

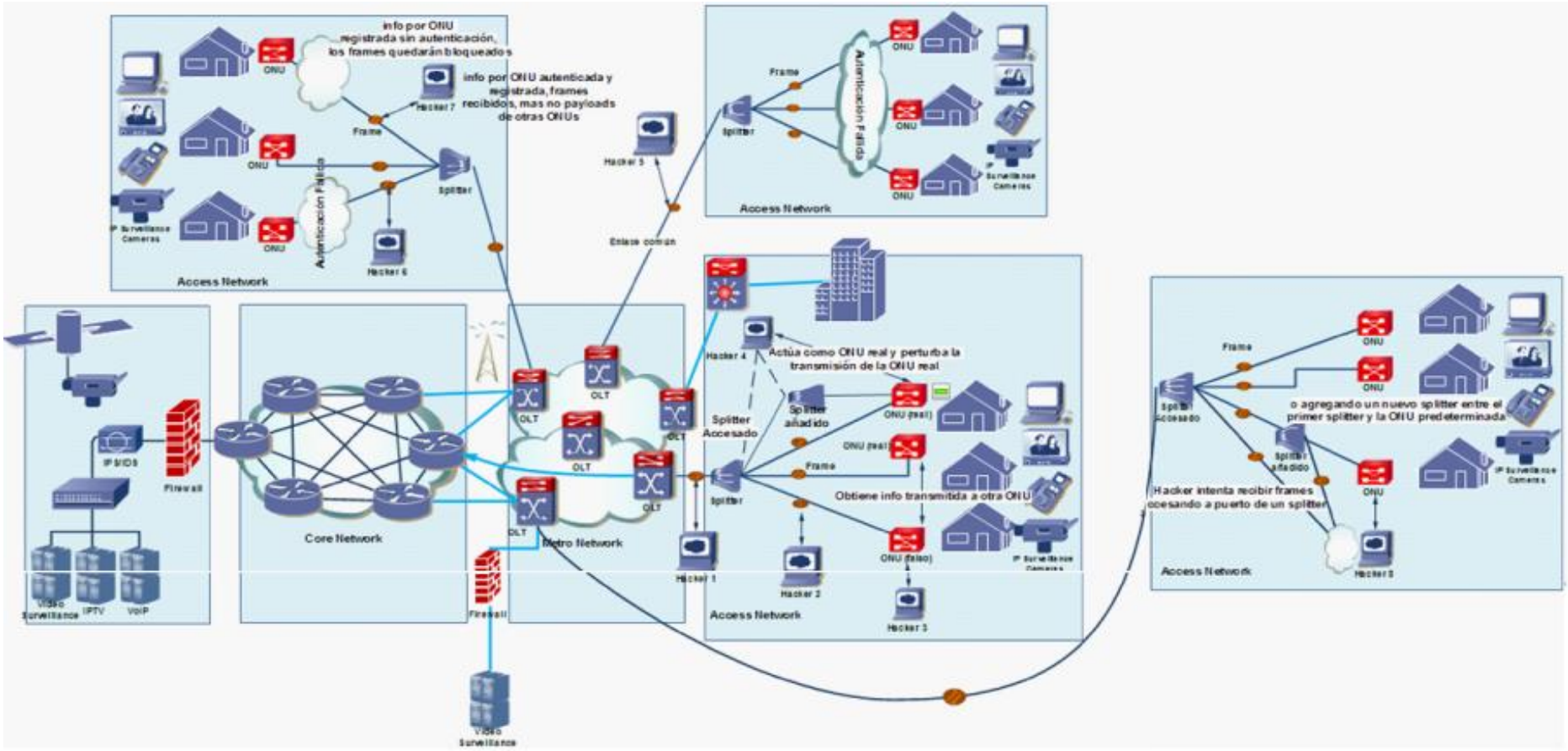

Figura 4.17. Diseño de una Red GEPON con algunos escenarios de ataques

Considerando el hecho de que siempre estamos en riesgo de que la red sea interceptada, y así terceros puedan acceder a servicios de manera ilegal y gratis, es conveniente estar conscientes de ciertos escenarios de ataques a los cuales podemos estar sometidos. Ver figura 4.17:

Primer escenario: Modificación y vigilancia de la información entre OLT y Divisor (Hacker 1)

El hacker 1 puede obtener información ilegalmente desde las tramas de enlace descendente GTC (GPON, Transmission Convergence) transmitidos a todas las ONUs por el acceso al vínculo común entre la OLT y el divisor óptico que distribuye la señal óptica desde la OLT a todas las ONU's. Aquí las tramas de enlace descendente GTC son atacadas a través de modificación, interceptación o vigilancia. Aunque el hacker 1 tuvo éxito al hackear las tramas de enlace descendente GTC, no puede hackear la carga de las tramas de enlace descendente GTC, porque la carga está cifrada. Este primer tipo de intento de intrusión debió cortar el enlace al traspasar, por lo tanto es muy difícil realizar un método de intrusión para una persona normal, sin embargo existen grandes posibilidades de que la red pueda ser hackeada por expertos.

Solución: Tener a los OLT's en capa 3 para poder configurar las ACL's.

Segundo Escenario: Obtención de información mediante ataque de descifrado, modificación y vigilancia de tramas entre Splitter y ONU (Hacker 2)

En el segundo tipo de intento de intrusión, el hacker 2 puede obtener información a través de un ataque de cifrado como modificación, interrupción o vigilancia de las tramas de enlace descendente GTC transmitidos a la ONU mediante el acceso al enlace entre el divisor y la ONU. Aquí se debe traspasar el enlace, por lo tanto para una persona normal es muy difícil realizar un método de intrusión, sin embargo existen grandes posibilidades de que la red pueda ser hackeada por expertos.

Solución: Establecer filtros MAC en cada ONU. Port Security con un conjunto de medidas de seguridad a nivel de puertos, restringe el acceso a los puertos según la MAC, restringe el número de MAC's por puerto, reacciones ante situaciones de violación. Renovar en cada ONU la clave establecida en cada sesión para mayor seguridad. Recurrir a un buen método de cifrado o encriptación, seguido de unas políticas de firewall muy seguras.

Tercer Escenario: Creación de ONU falso (Hacker 3)

En el tercer tipo de intento de intrusión, el hacker 3 crea un ONU falso y obtiene información transmitida a otra ONU sin filtrar por simple modificación del programa. Aquí se usa un ONU falso que actúa como un ONU real, perturbando la transmisión del enlace ascendente de la ONU real.

Solución: Utilizando la información de registro y los mensajes de puerta puede ser posible hacerse pasar por otro ONU, por esta razón es necesario recurrir a un buen método de cifrado, seguido de unas políticas de firewall muy seguras.

Cuarto Escenario: Acceso a un puerto de Divisor y adición de nuevo Divisor (Hacker 4)

En el cuarto tipo de intento de intrusión, el hacker 4 hackea el sistema mediante el acceso a un puerto que quedaba de un divisor entre la OLT y la ONU, recibe las tramas de enlace descendente GTC sin filtrar mediante la adición de un divisor o divisor al enlace entre el primer divisor y la ONU. Aquí el hacker 4 actúa como una ONU real, perturbando la transmisión de enlace ascendente de la ONU real. En este caso de intrusión se puede interceptar el cifrado de la clave transmitida desde la ONU real mediante el enlace ascendente, el hacker 4 puede obtener los datos cifrados en la trama. Por lo tanto este método puede ser letal y causar un gran daño.

Solución: Utilizando la información de registro y los mensajes de puerta puede ser posible hacerse pasar por otro ONU, por esta razón es necesario recurrir a un buen método de cifrado, seguido de unas políticas de firewall muy seguras.

Quinto Escenario: Intrusión por acceso a enlace entre OLT y Divisor por cifrado de autenticación (Hacker 5)

Este escenario es una vista conceptual que ilustra un intento de intrusión hecho para proporcionar una transmisión segura a través de un cifrado de autenticación.

En este diagrama, si el hacker 5 modifica una trama accesando a un enlace común entre una OLT y un divisor, los módulos de autenticación en todas las ONU's determinarán que la autenticación de las tramas de enlace descendente GTC han fallado. Por lo tanto la trama modificada por el hacker está bloqueada.

Solución: En este caso, la OLT debe chequear el estado de las ONU's y reemplazar los enlaces.

Sexto Escenario: Intrusión por Acceso a enlace entre Divisor y ONU predeterminada (Hacker 6)

En este diagrama, si el hacker 6 modifica una trama accesando a un enlace entre un divisor y una ONU predeterminada, un módulo de autenticación de la ONU predeterminada determinará que la autenticación de las tramas de enlace descendente GTC ha fallado en bloquear la trama modificado por el hacker 6.

En los diagramas de los 2 últimos escenarios, el hacker es incapaz de vigilar o monitorear los paquetes porque él no puede recibir las tramas GTC transmitidos a lo largo del enlace descendente en el paso de la autenticación.

Solución: Implementar un protocolo en el que si una ONT estándar transmite paquetes fuera de su horario, la OLT apaga el servicio de dicha ONT.

Séptimo Escenario: Intrusión por Modificación en programa de ONU (Hacker 7)

En este diagrama, si el hacker 7 intenta recibir la información de las tramas de enlace descendente GTC a través de una ONU registrada sin autenticación por una simple modificación del programa, el módulo de autenticación de las ONU's correspondiente determina que la autenticación de las tramas de enlace descendente GTC ha fallado debido a que la autenticación no puede ser realizada en las tramas de enlace descendente GTC. Por lo tanto la trama GTC correspondiente está bloqueado.

Además, si el hacker 7 intenta recibir información de las tramas de enlace descendente GTC a través de una ONU autenticada y registrada mediante una simple modificación de un programa, el módulo de autenticación de la ONU correspondiente determina que la autenticación de las tramas de enlace descendente GTC ha sido satisfactoria. Por lo tanto el hacker puede recibir las tramas de enlace descendente GTC pero no puede escuchar la información de la carga de otras ONU's porque cada ONU tiene su propia clave.

Solución: Establecer filtros MAC en cada ONU. Renovar en cada ONU la clave establecida en cada sesión para mayor seguridad. Implementar un protocolo en el que si una ONT estándar transmite paquetes fuera de su horario, la OLT apaga el servicio hacia el ONT (30).

Octavo Escenario: Intrusión a través de Divisor

En este diagrama, si el hacker 8 intenta recibir las tramas de enlace descendente GTC por divisor a un puerto que quedaba de un divisor, o agregando un nuevo divisor entre el primer divisor y una ONU predeterminada, entonces la autenticación de las tramas de enlace descendente GTC fallará porque el hacker no está registrado en el OLT. Por lo tanto el hacker 8 estará bloqueado para recibir las tramas de enlace descendente GTC.

Solución: Implementar una arquitectura genérica para desconectar a los atacantes mediante controladores ópticos en el divisor. Estos conmutadores también pueden servir para probar a la ONU. En caso de ataque de envío de una señal permanente desde algunos ONU's, el controlador primero detecta que señal continua se envía, luego identifica el puerto con una breve desconexión de los usuarios, invocando los conmutadores, este tiempo de desconexión debe ser muy corto pero lo suficientemente alto como para permitir la detección. Una vez que el puerto atacado es identificado, mientras que la desconexión de la señal permanente desaparece, el puerto correspondiente se puede apagar y personal de mantenimiento puede reaccionar al mal funcionamiento de la ONU. Lo negativo es que durante este proceso los demás usuarios pueden salir afectados (31).

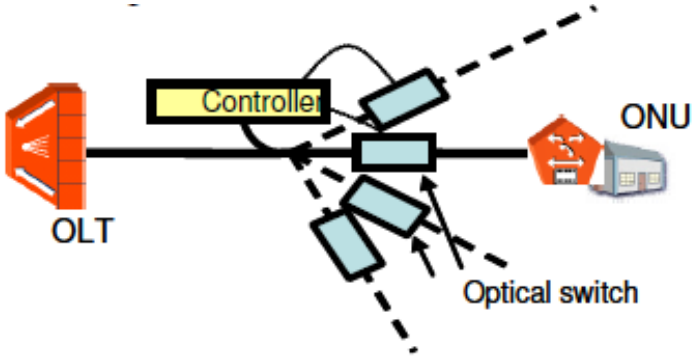

Figura 4.18. Arquitectura para desconectar atacantes en un Splitter

Fuente: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.1419&rep=rep1&type=pdf

Noveno Escenario: Ataque IP Spoofing

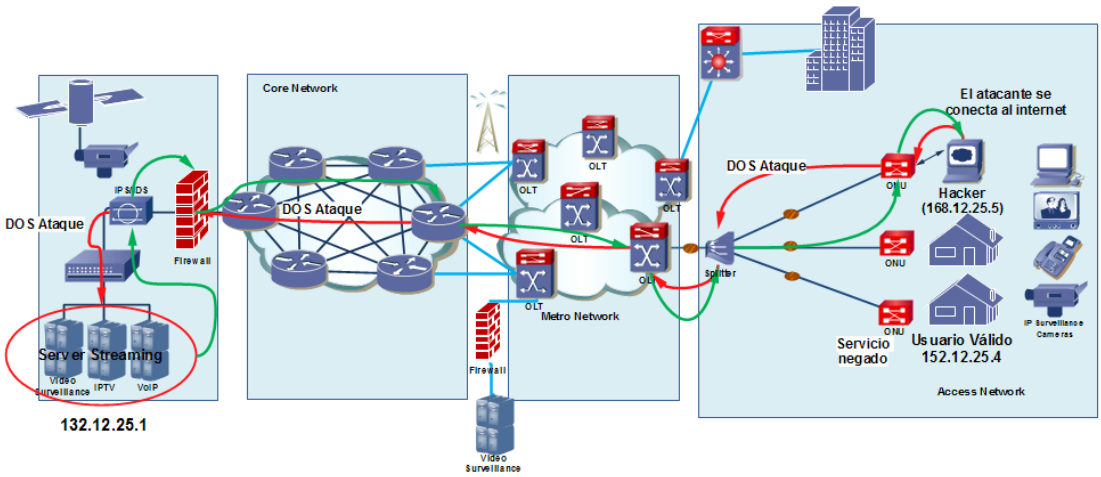

Figura 4.19. Escenario de Ataque DOS por IP Spoofing

La figura 4.19 muestra un ataque de suplantación de IP, donde un atacante intenta reemplazar la dirección IP del remitente (152.12.25.4), quien es un usuario válido, o en ciertos casos también suelen cambiar la dirección IP del destinatario, con el único fin de negar los servicios que proporciona el servidor a sus usuarios, por lo que se concluyen que en este tipo de ataques la dirección IP del remitente puede ser falsa.

En este escenario el atacante establece una conexión normal a internet desde una estación de trabajo con una IP válida (168.12.25.5), conectándose con el servidor cuya dirección IP es (132.12.25.1), el paquete de solicitud se construye con una dirección IP origen 168.12.25.5 y una dirección IP destino de 132.12.25.1.

Así, el servidor devuelve la petición mediante la dirección IP origen especificado en la solicitud como la IP destino

(168.12.25.5) y su propia IP como la dirección IP origen (132.12.25.1), de esta manera evita que el servicio proporcionado por el servidor llegue a sus respectivos usuarios, como se aprecia en la figura 4.20:

Figura 4.20. Paquetes de solicitud y envío de respuesta en ataque IP Spoofing

Solución:

Eliminar las relaciones de confianza basadas en la dirección IP o el nombre de las máquinas, sustituyéndolas por relaciones basadas en claves criptográficas.

El cifrado y filtrado de las conexiones que pueden aceptar nuestras máquinas también son medidas de seguridad importantes para evitar la suplantación. El filtrado de entrada verifica que los paquetes provengan de una fuente legítima, esto sirve como protección contra los ataques perpetuados a través de suplantación de IP.

El filtrado de salida, examina los paquetes que se envían fuera de la red interna a través de un enrutador o firewall, y los paquetes

cuestionables son detenidos, a menudo se utiliza en combinación con el filtrado de entrada. Este tipo de ataques pueden generar los siguientes problemas:

- Conocimiento de las direcciones MAC utilizado por los vecinos puede ser un problema de privacidad.
- Tráfico en sentido descendente de Mensajes MPCP puede revelar características del tráfico en sentido ascendente de cada ONU.

- En las redes PON, el tráfico en sentido ascendente puede, en determinadas condiciones, detectar los puntos de acceso ONU.

- Si los usuarios finales tienen éxito en interceptar el canal ONU OAM, pueden ser capaces de cambiar la configuración del sistema GEPON.

- Si los usuarios finales tienen éxito para introducirse en los canales de OAM, se puede tener acceso a los operadores de red de TMN [25] más allá del sistema GEPON.

- El usuario final puede tratar de perturbar el sistema PON mediante el envío de señales ópticas con tráfico en sentido

[25] Es un modelo de protocolo definido por la UIT-T para la gestión de sistemas abiertos en una red de comunicaciones

ascendente, esto podría generar un reinicio que puede facilitar la piratería de los mecanismos de protección.

- Si el usuario final puede decodificar los mecanismos de intercambio de claves, que pueden pasar por alto el sistema de protección.

En la figura 4.21 se aprecian otros posibles ataques que pueden presentarse en GEPON.

Décimo escenario: Dinamic ARP Inyection (Hacker 1)

La figura 4.21 muestra un ataque Dinamic ARP Inyection. En el décimo tipo de intento de intrusión, el hacker 1 envía paquetes entrantes ACLs Deny ARP con una asociación de IP/MAC incorrecta con el fin de obtener información del usuario.

Solución:

- Utiliza una lista de acceso para permitir o denegar determinados IP/MAC asociados a la tabla ARP.

- La tabla vinculante que contiene la dirección IP y dirección MAC pueden ser configuradas de forma estática o dinámica por medio de DHCP Snooping.

- También se puede usar ACL ARP para negar todo intento de unión IP/MAC inválido para quien DHCP no asignó direcciones IP.

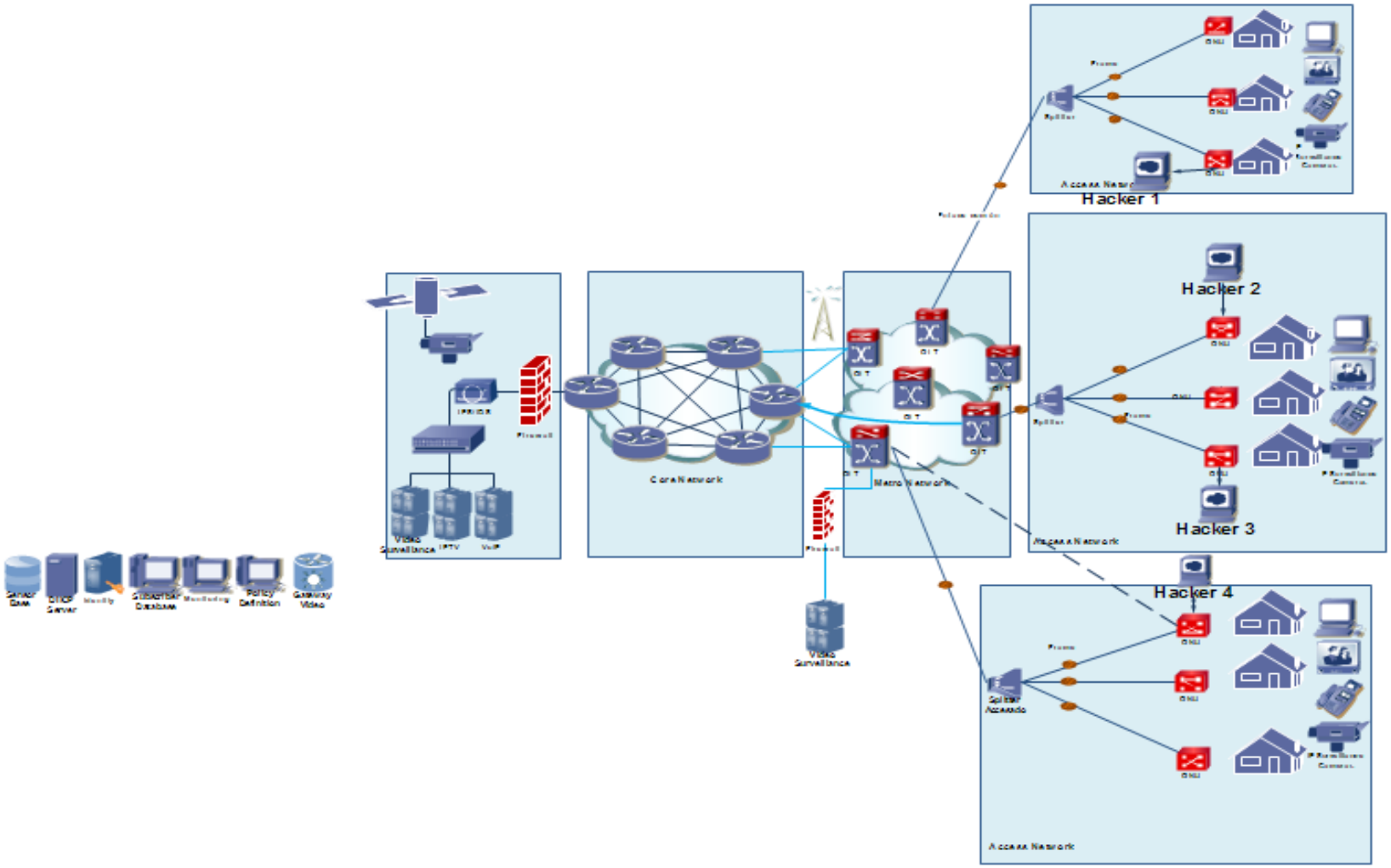

Figura 4.21. Diseño de una Red GEPON con más escenarios de ataques

Décimo Primer escenario: Ataque que afecte un datagrama IP (Hacker 2)

En este diagrama el hacker 2 suplanta un paquete indicando que proviene de otro sistema, enviando un mensaje dando una respuesta a otro mensaje antes de que lo haga el suplantado.

Solución:

La autenticación de los paquetes se realiza a nivel de máquina (por dirección IP) y no a nivel de usuario. Si un sistema suministra una dirección de máquina errónea, el DHCP opción 82 propiamente configurado filtra si el cliente existe (todos sus datos concuerden), en el caso de que no sea así no recibirá por lo que el secretario de red proporciona la dirección IP del ámbito de aplicación y de esta manera se evita la suplantación de identidad.

Décimo Segundo escenario: Falta de Cifrado ONU (Hacker 3)

Este escenario es una vista conceptual que ilustra un intento de intrusión hecho para proporcionar una transmisión segura a través de un cifrado de autenticación.

CPE (Equipo Terminal del Cliente) alias ONU o ONT, pueden afectar el tráfico de otros clientes y comprometer la seguridad si no está debidamente cifrado y autenticado.

Solución:

Los dispositivos deben de tener limitado los grupos de elementos o direcciones IP de los que pueden recibir tráfico. Realizando, de este modo, una correcta configuración es posible limitar muchos de los ataques de denegación de servicio.

Décimo Tercer escenario: Suplantación de identidad OLT DHCP server (Hacker4)

En este diagrama el hacker 4 realiza algunos pasos para llevar a cabo su ataque:

a) El usuario conecta PC.

b) PC envía solicitud DHCP;

c) Conmutador agrega la opción 82.

d) DHCP opción 82 controla si el cliente existe.

e) No existe cliente, por lo que devuelve dirección IP temporal con IP DNS spoofing servidor.

f) El usuario abre el explorador.

g) HTTP envía solicitud redirigida al registro de aplicación del servidor de suplantación de identidad.

h) El usuario registra y selecciona ISP.

i) La aplicación web agrega entrada del cliente en el registro de la red y empuja a través de Cisco Configuration Engine ISP VLAN la configuración en el interruptor.

j) El usuario se reinicia.

k) PC envía peticiones DHCP.

l) El conmutador añade opción 82.

m) DHCP opción 82 controla si el cliente existe.

n) Cliente existe, por lo que el secretario de red proporciona la dirección IP del ámbito de aplicación del ISP.

o) Usuario puede navegar por la web.

Solución:

Configuración de VLAN’s, las razones principales para su uso son:

- Gestión de Dirección.
- Reducción de la L2 de dominio de difusión.
- El aislamiento del usuario.
- Seguridad de acceso.
- Distribución Multicast en L2 Arquitectura anillo.

4.3 RECOMENDACIONES GENERALES DE PROTECCIÓN CONTRA ATAQUES

Para prevenir cualquier tipo de ataque y de esta manera tener una red segura se debe tener total visibilidad y total control sobre la red, por ello es recomendable aplicar controles de seguridad los cuales clasificaremos en dos grandes grupos que detallaremos a continuación:

Total Visibilidad.- Ayuda a identificar, monitorear y correlacionar eventos, tráfico, comportamiento y cumplimientos de políticas en toda la red.

Mencionaremos puntos estratégicos que cumplen con este control de seguridad para evitar ser atacados:

- Tener elementos de monitoreo que controlen el tráfico en la red.

- Se recomienda modificar los protocolos y configurar dispositivos para que utilicen autenticación en cada servicio de la red.

- Se recomienda la autenticación y el cifrado para cada uno de sus usuarios ya que los dispositivos deben de tener limitado los grupos de elementos o direcciones IP de los que pueden recibir tráfico.

- Se recomienda configurar correctamente los servicios para que no muestren más información de la necesaria.

- Tener a los OLT's en capa 3 para poder configurar las ACLs[26].

- Utilizar VLAN's para priorizar y proteger el tráfico en la red separándolo de canales lógicos de las redes de datos.

- No se debe permitir los volúmenes de datos y ráfagas de paquetes en puntos estratégicos de la red para evitar gran cantidad de ataques DoS.

- No se debe permitir inter-routing entre las ACL's ni entre los distintos servicios.

[26] Es la manera de controlar el flujo de red y la transferencia de datos

- Se recomienda que la OLT cumpla con el principio de total visibilidad para que identifique, clasifique y asigne niveles de confianza a los suscriptores, servicios y tráfico en toda la red.

Total Control.- Ayuda a aislar y cumplir con los servicios, aplicaciones, sistemas y políticas en la red aplicando para esto resistencia, redundancia y tolerancia a fallos y respondiendo dinámicamente a estos eventos anómalos.

Mencionaremos puntos estratégicos que cumplen con este control de seguridad para evitar ser atacados:

- Antes de conectarse a internet, es aconsejable tener un dispositivo IPS/ IDS para detección y prevención de intrusos.

- Tener un Firewall con fuertes políticas de seguridad.

- Tener buenos sistemas de antivirus actualizados para protegerse de ataques de virus, gusanos y troyanos.

- Tener los sistemas actualizados y parchados es totalmente imprescindible para prevención de posibles ataques.

- Se recomienda colocar filtros MAC ADDRESS en las ONU’s.

- Se recomienda fijar una MAC estáticamente y limitar el rango, para así prevenir suplantaciones de MAC.

- Se recomienda que el firewall cumpla con el principio de total control para que nos dé la certeza de tener una arquitectura segura.

- El módulo de APS es el componente básico de la propuesta que realiza la detección de errores y los procesos de cambio automático. El módulo de APS se conecta a las fibras, tanto a la entrada y como a la salida y protege la fibra. Cada circuito dispone de un filtro CWDM 1x2, dos detectores p-i-n, y un circuito de control para configurar el sistema operativo.

Total Visibilidad y Total Control

- Se recomienda que la gestión de administración de la red GEPON cumpla con los dos principios básicos para una red segura que son total control y total visibilidad.

4.3.1 HERRAMIENTAS DE SEGURIDAD

Verificar o aumentar el nivel de seguridad de un sistema (atacantes / defensores):

- Firewalls (control de tráfico).
    - Tablas de direcciones IP.
    - Firewall-1.
- Detectores de intrusos.
    - Snort.
    - Real Secure.
- Analizadores de logs.
    - Swatch.
    - LogWatch.

- Verificadores de integridad.
    - Tripwire.
- Analizadores de puertos.
    - Nmap.
    - PortScan.
- Detectores de vulnerabilidades.
    - Nessus.
    - Saint.
- Sniffers (captura de tráfico).
    - Ethereal.
    - Sniffer.

- Password crackers (contraseñas).
    - Passware.
    - John the Ripper.
- Troyanos (programas ocultos).
    - Back Oriffice.
- Rootkits (ocultación y expansión).

CAPÍTULO 5

5. ESTABILIDAD GEPON

5.1 LA PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE RED

Los sistemas de gestión GEPON suelen poder integrarse con soluciones que ya dispone el operador, como HPOpenView o similares, ya que GEPON está basado en sistemas de gestión Ethernet sobre SNMP[27], mucho más simplificados que los modelos de gestión y mantenimiento de capa 2 de ATM.

Un Sistema de Gestión de Red (NMS - Network Management System) combina hardware y software para controlar y administrar una red, y así detectar automáticamente los dispositivos conectados a la red.

Los elementos individuales de la red (NEs) en una red son administrados por un sistema de gestión de elementos.

[27] Es un protocolo basado en UDP (User Datagram Protocol), utilizado principalmente en sistemas de gestión de red para supervisar los dispositivos conectados a la red para las condiciones que requieren atención administrativa

La eficacia de un sistema de gestión de red depende de que se ejecuten una serie de tareas referentes a la operación, administración, mantenimiento y aprovisionamiento de sistemas en red, donde:

- La **Operación** se encarga del mantenimiento de la red, mediante un monitoreo para detectar problemas, preferiblemente antes de que los usuarios sean afectados.

- La **Administración** se ocupa de hacer un seguimiento de los recursos en la red y la forma en que son asignados, y así mantener la red bajo control.

- El **Mantenimiento** se ocupa de realizar reparaciones y mejoras, por ejemplo, cuando el equipo debe ser reemplazado. Aquí se suman medidas correctivas y preventivas para gestionar la red de mejor manera.

- El **Aprovisionamiento** se refiere a la configuración de los recursos en la red para incluir un nuevo servicio, como por ejemplo, permitir a un nuevo cliente puede recibir servicio de voz.

Los sistemas NMS hacen uso de varios protocolos para sus propósitos (SNMP, ICMP, HTTP, SSH, LDAP, POP, FTP, MySQL, Java, TCP / IP). Por ejemplo, el protocolo **SNMP** (Simple Network Management Protocol) permite recoger sólo la información de los distintos dispositivos por la jerarquía de la red. Los sistemas NMS son responsables de la identificación de la fuente exacta del problema y su solución. Además deben recoger las estadísticas de los dispositivos durante un período de tiempo. Pueden incluir una recopilación de datos históricos, relacionados con los problemas y soluciones que funcionaron en el pasado, y así recurrir a ellos cuando una falla es encontrada para buscar el mejor método posible para resolver el problema. Este tipo de sistemas gestionan los elementos de red bajo el concepto de **FCAPS** :

a) Gestión de Fallos (Fault).

b) Gestión de Configuración (Configuration).

c) Gestión de Contabilidad (Accounting).

d) Gestión de Rendimiento (Performance).

e) Gestión de Seguridad (Security).

Entre las funciones básicas en un sistema de gestión de redes se incluyen el control, la planificación, la asignación, la implementación, coordinación y seguimiento de los recursos de una red, en donde se ejecutan tareas de planificación de la red, la frecuencia de asignación predeterminada de tráfico de enrutamiento para apoyar el equilibrio de carga, de claves criptográficas de distribución de la autorización, gestión de ancho de banda, análisis de la ruta y las ya mencionadas, (32).

5.1.1 TECNOLOGÍAS A UTILIZAR EN EL DESARROLLO DE UN SISTEMA NMS

Puede ser desarrollado en Java ejecutándose sobre aplicaciones APACHE TOMCAT, usando XML para la configuración de varios módulos. La figura 5.1 muestra una arquitectura de este tipo de sistemas.

Existen ciertos métodos que dan soporte a las redes y administran los dispositivos de red. Los métodos de acceso incluyen el SNMP, interfaz de línea de comando (CLI), XML personalizado, CMIP

[28](Common management information protocol), Windows Management Instrumentation (WMI[29]), TL1[30], CORBA [31](Common Object Request Broker Architecture), NETCONF[32], y el de Java Management Extensions (JMX[33]). Los esquemas incluyen la WBEM [34](Web-Based Enterprise Management), el Modelo de Información Común, y MTOSI entre otros (33) (32).

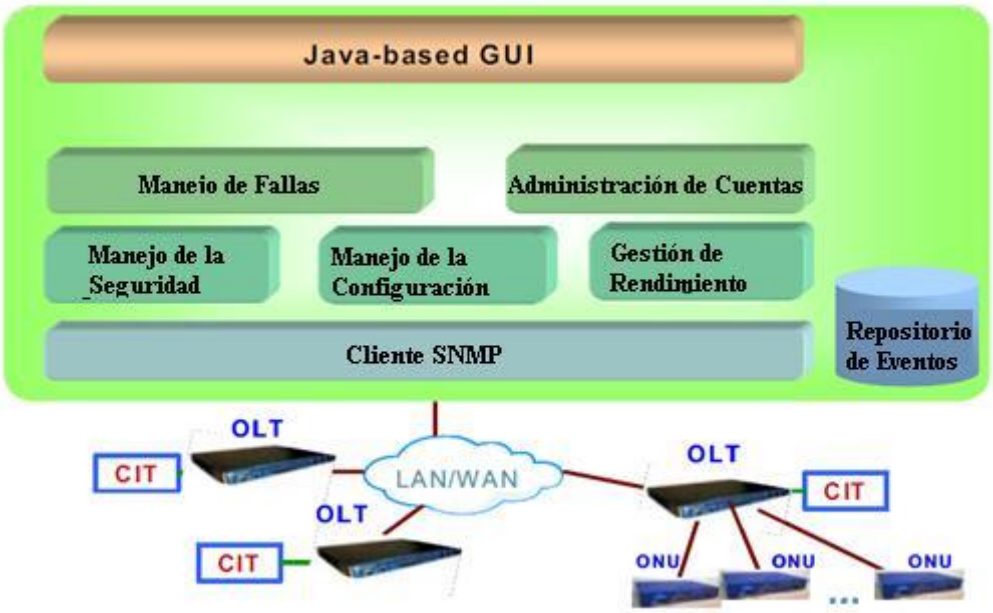

Figura 5.1. Arquitectura Sistema NMS

Fuente: http://ir.itri.org.tw/bitstream/987654321/4900/1/E520003.pdf

[28] Es un protocolo para la gestión de la red

[29] Permite a los lenguajes de scripting como VBScript o Windows PowerShell para administrar Microsoft Windows ordenadores personales y servidores, tanto local como remotamente

[30] Es un protocolo de gestión utilizado ampliamente en las telecomunicaciones, se utiliza en la entrada y salida de mensajes que pasan entre los sistemas de operaciones (OSS) y elementos de red (NE).

[31] Permite a los componentes de software escritos en varios lenguajes de programación, ejecutarse en varios equipos al trabajar juntos (es decir, soporta múltiples plataformas).

[32] Proporciona mecanismos para instalar, manipular y eliminar la configuración de dispositivos de red.

[33] Es una tecnología Java que proporciona herramientas para la gestión y seguimiento de aplicaciones, objetos del sistema, dispositivos (impresoras) y servicios orientados a redes

[34] Es un conjunto de sistemas de gestión de tecnologías desarrolladas para unificar la gestión de entornos de computación distribuida

5.1.2 SEGURIDAD EN SISTEMAS DE GESTIÓN DE RED

Las interfaces de gestión de dispositivos de Ethernet usualmente están basadas sobre capa IP, como SNMP, HTML o Telnet, lo que puede originar ciertos problemas de seguridad, especialmente si los usuarios tienen acceso directo a la capa 2 de la red. Existen maneras de anular las limitaciones de acceso provistas por las VLAN's, y por tanto, un atacante puede conectarse directamente a los módulos de gestión de red Ethernet, lo que hace que sea imposible la protección mediante servidores de seguridad. La única solución viable es utilizar una fuerte autenticación en la capa IP, autorización y contabilidad para controlar el acceso a los módulos de gestión y el uso de cifrado fuerte, por ejemplo, SSL o SSH, para hacer un túnel de la gestión del tráfico.

La presentación de informes de eventos puede ser otra debilidad en las redes de acceso basado en Ethernet. Algunos sistemas pueden reportar sucesos en el sistema de gestión de red (NMS), utilizando mensajes UDP, los mismos que pueden ser fácilmente falsificados, provocando falsas alarmas y, posiblemente, la sobrecarga de NMS. Si bien es cierto que para la falsificación de mensajes de eventos se requiere información detallada acerca de

los NMS, sería mejor utilizar otros métodos más seguros para realizar estos informes. El Protocolo Simple de Administración de Red (SNMP, Simple Network Management Protocol) es una alternativa, pero no se obtienen mejoras de seguridad a menos que se utilice SNMPv3.

SNMPv3 (Simple Network Management Protocol Version 3) es un protocolo de interoperabilidad regido en estándares de gestión de la red. Provee un acceso seguro a los dispositivos mediante autenticación y cifrado de paquetes a través de la red, mejorando las carencias de seguridad en las versiones anteriores. Sus características son:

- Garantizar la integridad de los mensajes, evitar la violación de la información contenida en los paquetes durante la transmisión.

- Verificar que los mensajes provienen desde una fuente válida.

- Cifrar el contenido de los paquetes y evitar que sea visto por fuentes no autorizadas.

Herramientas y Recursos

Hay algunas herramientas para los ataques de la capa de Ethernet que son gratis y están disponibles en internet, como el Yersinia o el Dsniff, entre otros (34) (35).

5.1.3 SISTEMAS DE GESTIÓN DE REDES RECOMENDADOS

Hemos explicado cómo podría implementarse un Sistema de Gestión de Redes, pero existen otros programas de Administración para redes, de entre los cuales podemos recomendar los siguientes:

IQUEUE: GESTOR DE OLTS Y ONUS GEPON

iQUEUE, en colaboración con HP OpenView y/o SNMPc permite la gestión de una red GEPON compuesta por múltiples nodos ópticos y sus respectivos controladores OLT. Puede controlar SLAs (Service Level Agreements) y OLAs (Operating Level Agreements) de un máximo de 25000 equipos ONU Fast Ethernet y Gigabit Ethernet. La licencia depende del número de ONU’s supervisadas. Cada paquete se personaliza con una protección USB.

Desde iQUEUE se pueden asignar anchos de banda en canal ascendente y descendente a cualquier elemento remoto. También es posible realizar un filtrado de tráfico a niveles 2 y 3, además de establecer diferentes reglas de encaminamiento (bridging, VLAN por ONU, VLAN privada, translación de VLAN's, etc). Cuando el equipo ONU opera a nivel 3, entonces se puede trabajar con los protocolos IPv4 e IPv6.

iQUEUE interactúa con las cabeceras OLT, la transmisión de parámetros a las ONU's las realiza vía OAM (tramas de Operación y Mantenimiento) definidas en el protocolo IEEE 802.3ah (36). Ver figuras 5.2 y 5.3.

Especificaciones

Requerimientos S.O.

Entorno operativo WINDOWS (XP, 2003 Server).

Hardware

Equipo PC industrial con Pentium III o superior.

2GB de memoria RAM

10GB libres de HDD

Puerto USB libre

Doble tarjeta XVGA

Doble monitor

Interfaz de usuario

Grafico e intuitivo

Licencia: iQUEUE se licencia por número de equipamiento ONU a gestionar

Interoperabilidad: iQUEUE interopera e intercambia información con consolas de gestión como SNMPc, o HP OV para posicionar chasis OLT's en la topología.

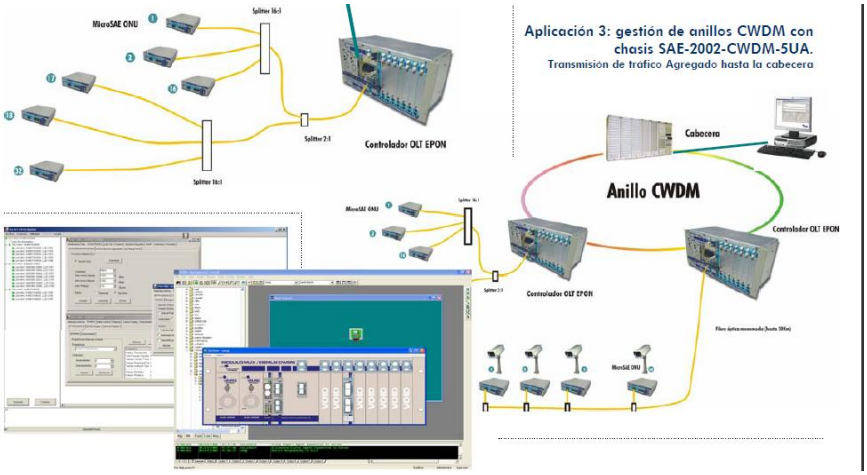

Figura 5.2. iQUEUE 1 (36)

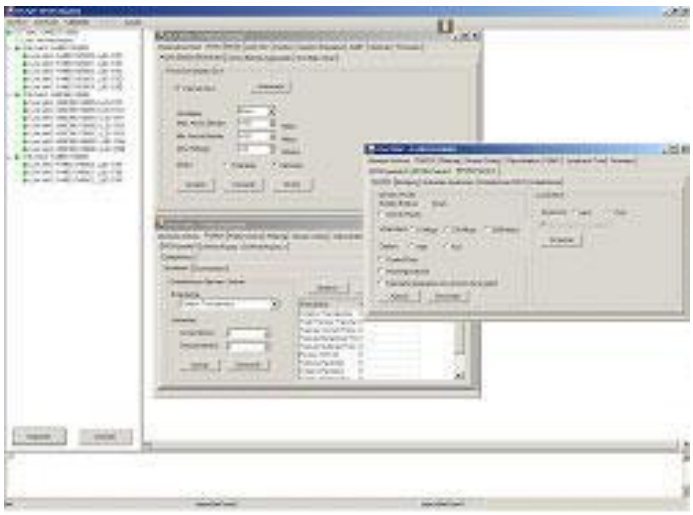

Figura 5.3. iQUEUE 2 (36)

NETATLAS PON, GEPON MANAGER

Es un EMS, compatible con una gama completa de funciones para la gestión de soluciones de ZyXEL GEPON, tales como la gestión del sistema, configuración de red, monitoreo de desempeño, detección de fallas y control de la seguridad. Es compatible con la arquitectura de capa 2.

Es simple y eficiente con una capacidad de administración remota para un máximo de 100.000 líneas ONU, facilita la gestión de la red, reduce el tiempo para la recuperación de las fallas, y aumenta la disponibilidad de la red (37). Ver figuras 5.4, 5.5, 5.6, 5.7, 5.8 y 5.9.

Especificaciones

Requerimientos S.O.

Solaris 9, Solaris 10

X11R6/Motif 2.2

HP OpenView Network Node Manager 7.5

MySQL 4.1.8

[Optional] Apache 2.2.4 (for OSS interface)

Hardware

Sun Ultra60 SPARC Workstation

1 GB RAM

60 GB hard disk

1024 x 768 graphical adapter

10/100/1000 Mbps Ethernet adaptor

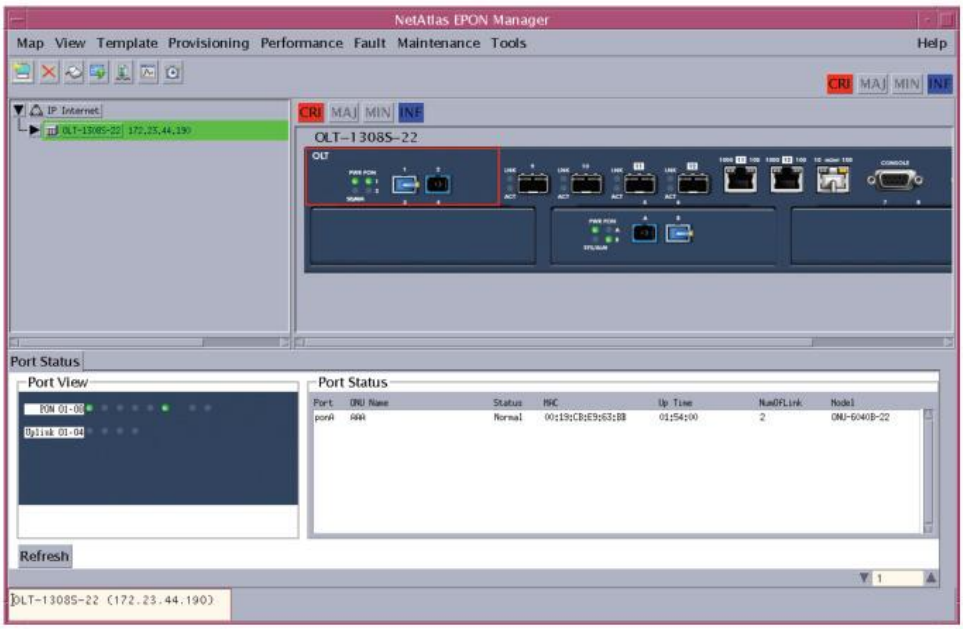

Figura 5.4. Vista de árbol y Vista de dispositivos para el acceso rápido y aprovisionamiento

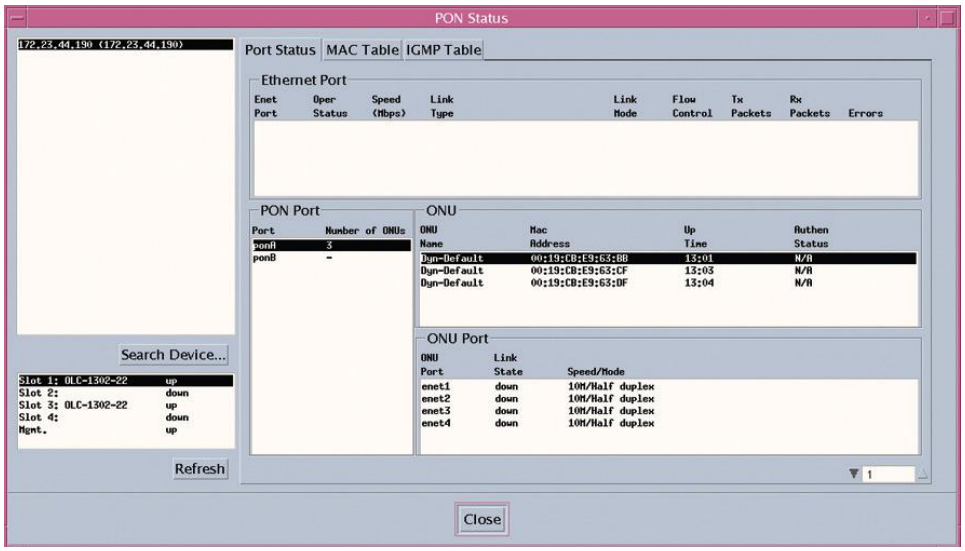

Figura 5.5. Supervisión del estado de la red

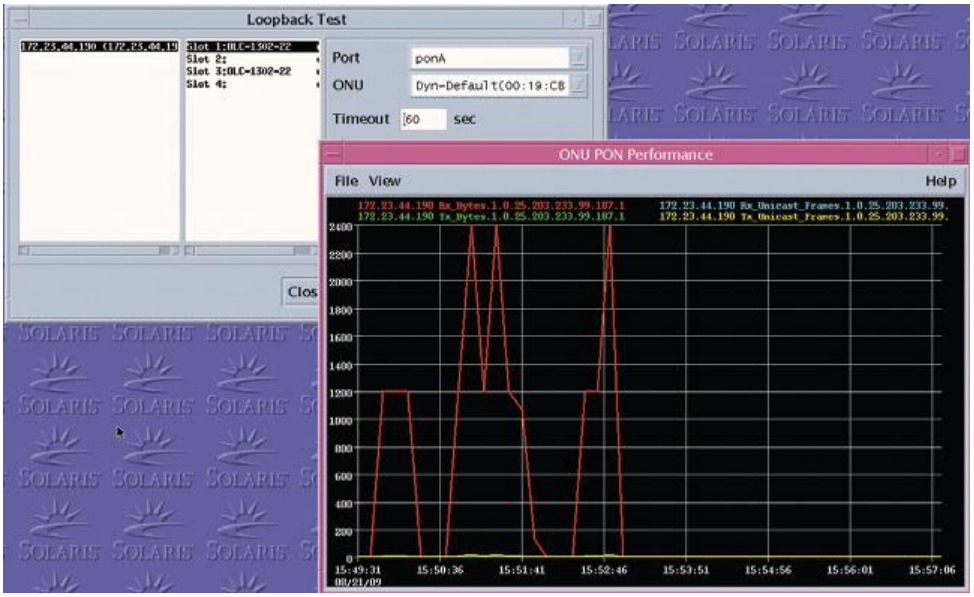

Figura 5.6. Prueba para solucionar problemas (37)

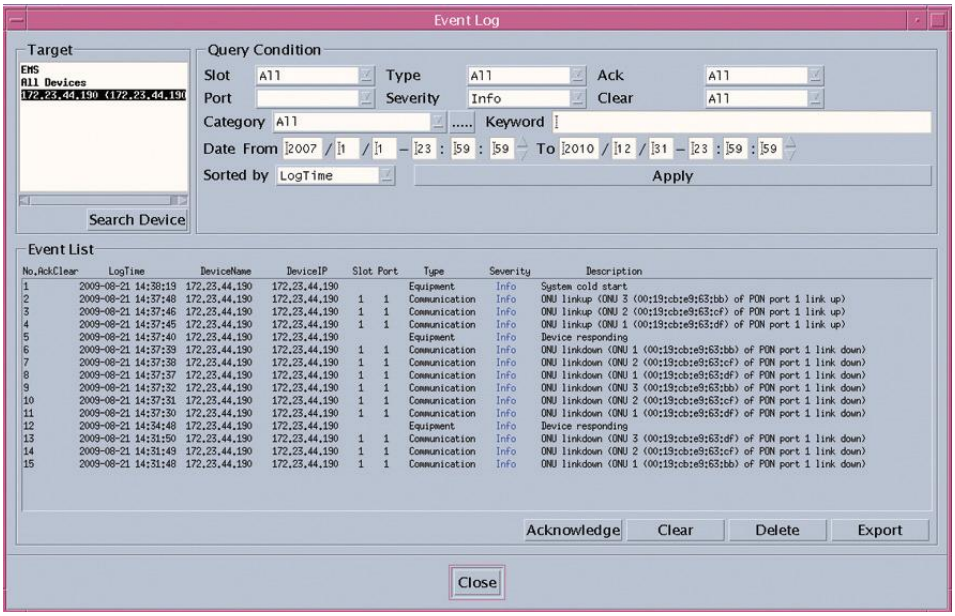

Figura 5.7. Alarma / Gestión de Eventos (37)

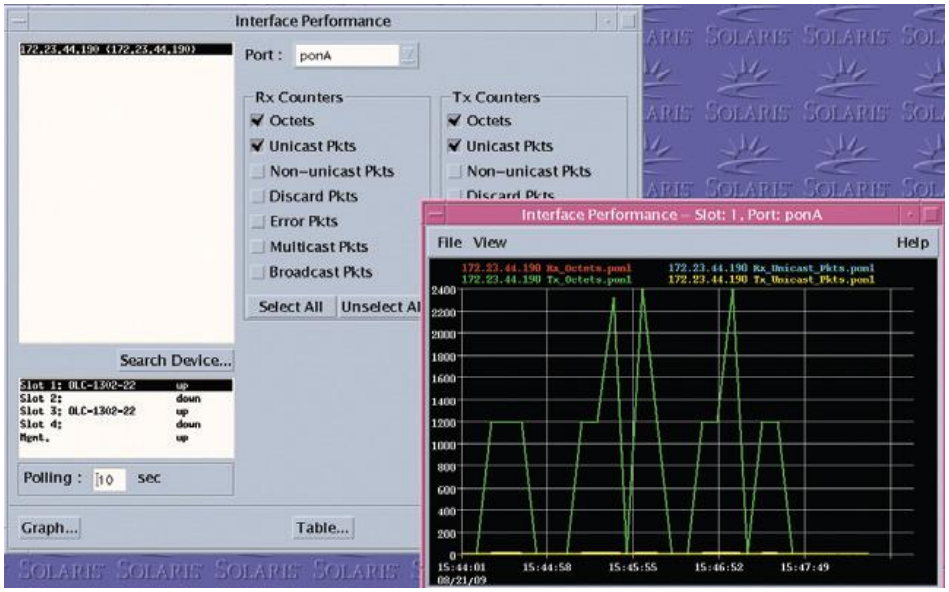

Figura 5.8. Control del rendimiento y Estadística; Informe que brinda facilidad en la operación diaria (37)

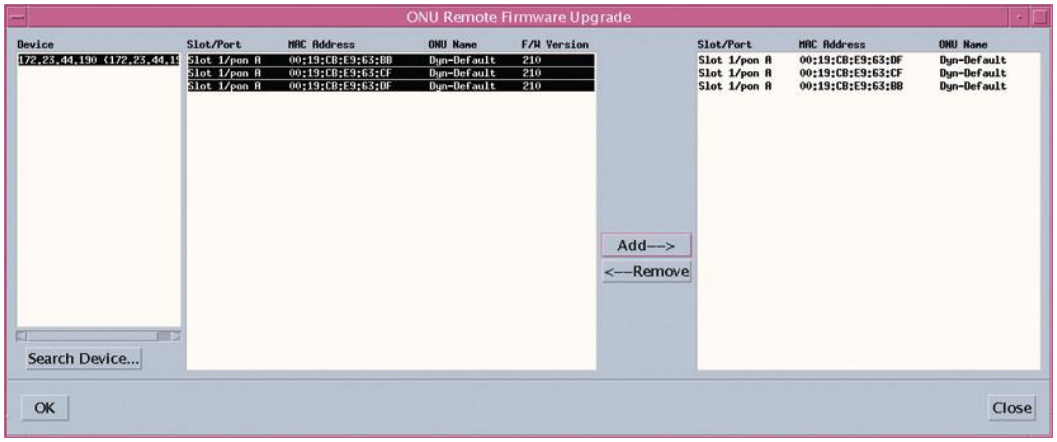

Figura 5.9. Automatización para el control remoto (37)

GEMS - GIGAFORCE SISTEMA DE ADMINISTRACION DE ELEMMENTO (GIGAFORCE ELEMENT MANAGEMENT SYSTEM)

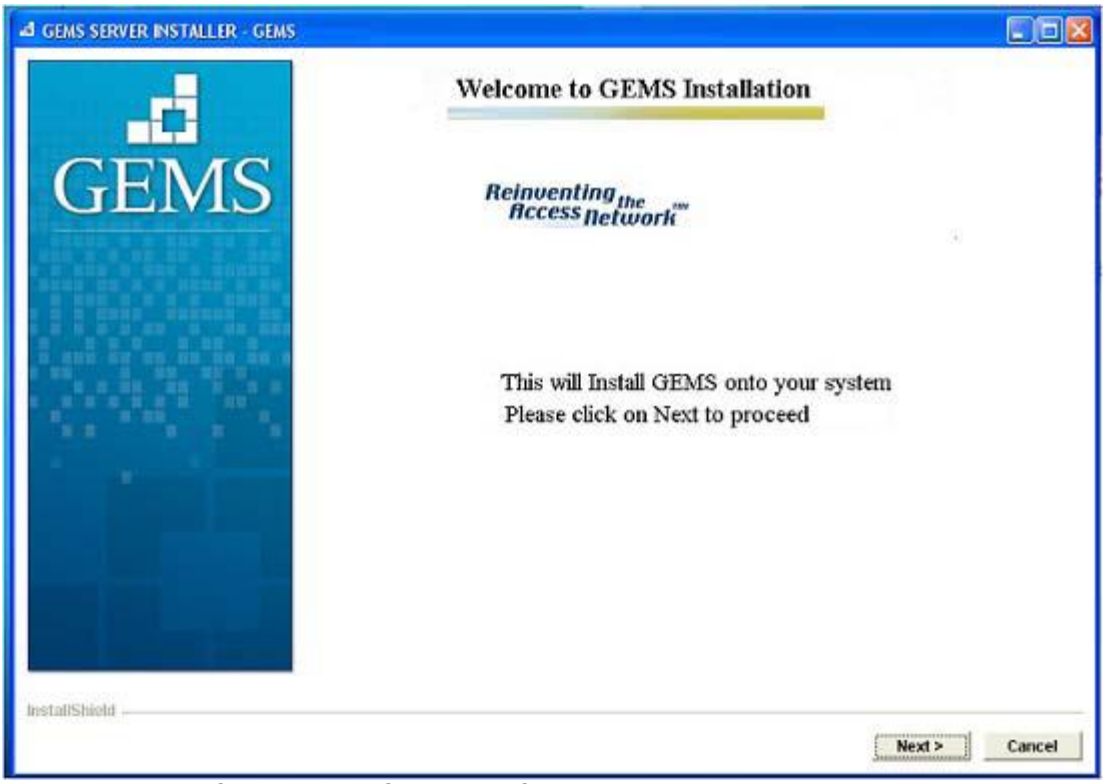

Figura 5.10. GigaForce Element Management System

GEMS tal como se aprecia en la figura 5.10, anunciado por Alloptic, Inc., líder mundial en el suministro de Gigabit Ethernet Passive Optical Network (EPON), es un sistema de gestión de elementos que proporciona un único punto de control para redes de proveedores de servicios.

GEMS Alloptics ofrece a los proveedores de servicios la capacidad de manejar sus despliegues PON efectiva, brindando una plataforma flexible a integrarse a sus entornos operativos respectivos. Corrige fallas de configuración, contabilidad, rendimiento y funcionalidad de Seguridad (FCAPS), según lo definido por la Unión Internacional de Telecomunicaciones (UIT-T).

GEMS ofrece también características avanzadas y fáciles de utilizar en las funciones de gestión de servicios. Estas funciones permiten a los operadores dar soporte a los clientes, y proporcionar las herramientas necesarias para gestionar la red.
La plataforma de GEMS se basa en estándares abiertos y soporta una amplia variedad de interfaces. Además genera informes de alarma que le permiten interactuar con los sistemas de operaciones en general.

La capacidad de GEMS permite al proveedor de servicios configurar rápidamente, supervisar y solucionar problemas de grandes despliegues PON con una amplia gama de servicios tal como se muestra en la figura 5.11. GEMS promueve la eficiencia en toda la red de proveedores de servicios, asegurando el mejor uso de tiempo y recursos. (38).

Figura 5.11. Pantallas del Sistema Carrier Class EMS

CAPÍTULO 6

6. DISEÑO DE LA RED GEPON

6.1 DIMENSIONAMIENTO DE EQUIPOS

Puesto que no contamos con los equipos físicos para elaborar una red Gepon, asumiremos un escenario para analizar algunos puntos importantes a tomar en cuenta en el desarrollo.

Utilizaremos:

- OLT’s.
- Divisores ópticos.
- Fibra óptica.
- ONU’s.

Supongamos que los equipos que brindan los diferentes servicios, se encuentran ubicados en una oficina central, y están interconectados con la fibra óptica, que sirve como medio de transmisión para los servicios de voz, datos y video. Luego se conecta al divisor, donde la señal se dispersa hacia cada ONU.

6.2 EQUIPAMIENTO GEPON

A continuación en la tabla 6.1 se van a presentar tres empresas pioneras en equipos para redes GEPON. Estas empresas ofrecen una guía de productos compatibles para esta tecnología, los cuales detallaremos a continuación con la respectiva ubicación que ocupa cada equipo en la red, también se debe considerar que en una instalación de fibra óptica y elementos ópticos pasivos intervienen materiales que si bien no son mencionados, son importantes para la parte práctica (12) (39) (40).

En la Oficina Central tenemos el OLT (Optical Line Terminal).

En la Red de Distribución Óptica encontramos la fibra óptica, divisores, acopladores, etc.

En el equipamiento de usuario tenemos las ONU's.

EMPRESA	MODELO	CARACTERÍSTICAS					DISPOSITIVOS COMPATIBLES
ZyXEl	**OLT-1308S-22** 	**Interfaces:** 8 puertos compatibles IEEE 802.3ah GEPON, 4 GbE puertos de enlace ascendentes	**Redundancia y Calidad de Servicio:** VLAN, multicast y prioridad de colas.	**Seguridad Avanzada:** autenticación de puertos 802.1x. IGMP v1/v2 espionaje y filtrado, algoritmo AES 128 bits	**Gestión:** Interfaz web, Telnet, FTP, CLI, SNMP, SSH, consola local RS-232, EMS	**Especial:** Tarjeta de línea intercambiable en caliente, módulo de alimentación DC y módulos de ventilador.	**ONU-6040B-22/21**  **ONU-6040BF-22**  **ONU-6100B-22/21** 
Allopic	**Edge2000** 	**Seguridad y servicios de datos:** Switch interno (16Gbps). Interfaz de red que soporta todas las PON's. VLAN's y QoS24 basados en prioridades. Garantiza VoIP y Video Streaming.	**Estándar de Telefonía TDM25 para industrias:** DS335 con interfaces para conexiones TDM/POTS. Entrega sincrónica y servicios punto a punto de T1/E1	**Distribución de video Universal:** Video RF38 utilizando medios ópticos. Controla servicios de video remoto	**Gestión:** Centralizada. Interfaz web, SNMP, consola local RS-232		**ONUH4081 home** 

D-Link	**DPN-2016** 	**Interfaces:** 16 1000BASE-LX PON, 16 10/100/1000BASE-T/SFP	**17 Ranuras en el chasis OLT**	**Módulos:** tarjeta de control, suministro de energía	**Puertos PON:** soporta hasta 20 km cable de fibra óptica	**DPN-204**  **DPN-301**  **DPN-540** 

Tabla 6.1. Equipos para redes GEPON (12) (39) (40)

6.3 ANÁLISIS DE LA RED

Suponiendo que nuestro proyecto asignará para cada usuario:

- Un canal de acceso a internet, a razón de 1.5 Mbps
- Un canal para servicio de IPTV, a razón de 3.5 Mbps
- Un canal para servicio de telefonía IP, a razón de 11 kbps (0.011 Mbps)
- Un canal de video vigilancia, con codificación MPEG-2, a razón de 3.5 Mbps

Con una disponibilidad del 99.999%, la capacidad de 1 Gbps de la red GEPON, la atenuación de una unión óptica es de 0.08 dB, y que la atenuación de cada divisor es de 3 dB, tenemos los siguientes cálculos:

Cada usuario requiere de un ancho de banda total de:

1.5 Mbps + 3.5 Mbps + 0.011 Mbps + 3.5 Mbps = 8,511 Mbps

Es decir, aproximadamente 9 Mbps (la suma de todos los servicios)

Con una capacidad de 1 Gbps y una disponibilidad del 100%, tenemos que cada OLT alcanzaría para:

(1 Gbps / 9 Mbps) * (1000 Mbps / 1 Gbps) = 111 usuarios

Sabemos que en GEPON se tienen divisores a razón de 1:32, entonces, para conseguir la relación 1:111 se necesitarían de 2 divisores 1:32, el segundo en cada salida del primer divisor. Así tendremos:

(32 x 32) = 1024 > 111 usuarios necesarios para ofrecer el servicio.

Las pérdidas de la señal estarían definidas por:

- En los divisores de 1:32, la atenuación viene dada por: 10.log(Pin / Pout) = 10.log(32) = 15.05 dB. El total de pérdidas seria de: (2 * 15.05 dB) = 30.1 dB

- En la fibra la atenuación promedio es de 0.01*K, donde K es la longitud de la fibra en Km.

Calculo de la atenuación para el enlace más cercano

Para estos cálculos se considerará las atenuaciones de los divisores, fibra óptica, y uniones ópticas a realizarse en cada punto. Asumamos una atenuación de 0.08 dB por cada unión óptica.

Supongamos que intervienen 5 puntos para este enlace, entonces la atenuación en las uniones ópticas seria de: (5 x 0.08 dB) = 0.4 dB
De acuerdo a este cálculo tenemos:

Atenuación por divisores: 30.1 dB
Atenuación por fibra óptica: suponiendo una distancia de 100 metros = 0.1 Km, la atenuación seria de 0.01*K = 0.01 * 0.1 = 0.001 dB.
Atenuación por uniones ópticas: 0.4 dB
Con esto tenemos una atenuación total de: 30.1 dB + 0.001 dB + 0.4 dB = 30.501 dB

Calculo de la atenuación para el enlace más lejano

En este cálculo realizamos los mismos pasos que el cálculo anterior.
Asumamos una atenuación de 0.08 dB por cada unión óptica
Supongamos que intervienen 10 puntos para este enlace, entonces la atenuación en las uniones ópticas seria de: (10 x 0.08 dB) = 0.8 dB

De acuerdo a este cálculo tenemos:

Atenuación por divisores: 30.1 dB

Atenuación por fibra óptica: suponiendo una distancia de 1500 metros = 1.5 Km, la atenuación seria de 0.01*K = 0.01 * 1.5 = 0.015 dB.

Atenuación por uniones ópticas: 0.8 dB

Con esto tenemos una atenuación total de: 30.1 dB + 0.015 dB + 0.8 dB = 30.915 dB

CONCLUSIONES

1) Con el desarrollo de esta tecnología, se puede obtener una red óptica en su totalidad, en donde la información viaja en longitudes de onda, independientes en cada servicio, mejorando así su calidad.

2) GEPON ha superado las grandes distancias, llegando hasta los abonados con un recorrido de hasta 20 kilómetros desde la central, mejorando a la tecnología DSL que cubre una distancia de 5km. Esto ha generado un cambio definitivo que solucionará los problemas de acceso a internet.

3) Para los usuarios es indiferente la infraestructura mediante la cual se le provea los servicios que solicitan, lo que requieren son mejores precios con una mayor calidad. Por este motivo el brindar el servicio cuádruple play permite que el usuario pueda recibir los servicios de Internet, IPTV, Telefonía IP y Video Vigilancia sin la necesidad de instalar cuatro equipos finales o trabajar con cuatro proveedores diferentes.

4) Para los usuarios es indiferente la infraestructura mediante la cual se le provea los servicios que solicitan, lo que requieren son mejores

precios con una mayor calidad. Por este motivo el brindar el servicio triple play permite que el usuario pueda recibir los servicios de televisión por cable, Internet y telefonía sin la necesidad de instalar tres equipos finales o trabajar con tres proveedores diferentes.

5) Si los sistemas X- Play no funcionaran correctamente, entonces el costo de invertir en ellos se coinvertiría en una pérdida financiera, por lo cual es importante adoptar todas las medidas necesarias, operativas y de seguridad, que me permita proteger servicios sensibles a fallos en especial IPTV.

6) La migración a una nueva tecnología, conlleva cambios en equipos activos y pasivos, pero se debe tomar en cuenta que utilizar las tecnologías GEPON no produce cambios bruscos en la red, ya que dichas tecnologías usan como plataformas base el Ethernet, el cual actualmente esta implementado en todas las redes de los proveedores de servicios.

7) En la actualidad las amenazas más comunes que atentan contra los activos de información se materializan gracias a que al diseñar la red no fueron contempladas las vulnerabilidades del sistema y no se tomaron las medidas necesarias para mantener la seguridad en la

red, permitiendo de esta manera que los atacantes puedan tomar el control de las redes, accediendo a sus recursos e información.

8) Para evitar todo esto se debe realizar un análisis efusivo de los activos, amenazas y vulnerabilidades del sistema para implementar las contramedidas necesarias para cada situación.

9) GEPON hereda todas las vulnerabilidades de la capa IP, volviéndose críticas aquellas relacionadas a la inundación de ancho de banda, puesto que la misma capacidad de los usuarios GEPON permitiría este tipo de ataques teniendo un mayor impacto a nivel local.

10) Si se analiza la adecuación de cada tecnología para prestar el servicio x play (internet, telefonía IP, IPTV, video vigilancia IP), el resultado es que en las tecnologías actuales no se pueden brindar estos servicios juntos, por lo que se hace necesario emplear una combinación de redes de acceso. Este tipo de situaciones, caracterizado por la operación de múltiples infraestructuras de red, ha sido objeto de numerosos trabajos de telecomunicaciones.

11) Una red GEPON con Arquitectura Tecnológica es aquella donde se analizan todos los componentes y recursos que intervienen para

entregar sus servicios, lo que quiere decir que se debe realizar un análisis minimalista de cada uno de los activos que están fuertemente vinculados con el negocio para proveer los servicios con Alta Visibilidad y Control total.

RECOMENDACIONES

1) Se deberá tener una correcta planificación acerca del crecimiento de los servicios de telecomunicaciones por parte de las diferentes operadoras debido a que se debe mejorar la calidad de servicio que se ofrece y por ello trabajar con arquitecturas FTTX, es la mejor opción para poder abastecer satisfactoriamente las redes a edificios, barrios, ciudades, urbanizaciones.

2) Se recomienda la utilización de la red GEPON, con respecto a GPON debido a su gran ancho de banda, seguridad y principalmente bajo costo en los equipos.

3) Es necesario contar con personal capacitado en estas nuevas tendencias tecnológicas ya que indiscutiblemente la infraestructura de telecomunicaciones apunta al crecimiento con mayores y mejores servicios y de igual manera nuevos tipos de ataques a los que tendrían que contrarrestar.

4) Para establecer una red GEPON segura no basta realizar el Análisis de Riesgo de sus activos, sino que también se debe estudiar los casos o escenarios críticos que puede sufrir la red y analizar las

contramedidas a tomar para brindar servicios de calidad y para que esta tecnología siga teniendo acogida, de esta manera la Arquitectura de la red GEPON sería eficiente, robusta y segura.

5) Para lograr una Alta Visibilidad de toda la infraestructura tecnológica se debe identificar, clasificar y asignar niveles de confianza a los suscriptores, servicios y tráfico a través del software de gestión de la red y por medio de la interfaz entre el proveedor y el abonado, también se debe monitorear cada uno de los recursos como a los servidores, analizar el tráfico de la conexiones concurrentes y verificar que las políticas establecidas se cumplan y finalmente para lograr una alta visibilidad se debe correlacionar y analizar eventos más significantes de todo el sistema.

6) Para lograr un Control Total la infraestructura tecnológica de la red debe ser capaz de hacer cumplir con todas las reglas de acceso a los sistemas y recursos de la red. Un caso muy importante en esto es que cada vez que se configure un servidor como el DHCP Server, Streaming Server, Servidor de correo, entre otros, sus configuraciones de acceso deben ser denegadas en su totalidad, y poco a poco ir estableciendo permisos de acceso para que las instrucciones sean mínimas.

7) Es necesario contar también con equipos de seguridad perimetral, como IPS/IDS, detectores de anomalías, detectores de botnet, puesto que es muy común que en este tipo de redes se encuentren máquinas infectadas, o máquinas que pertenecen a alguna botnet. Las tareas de detección de botnet deben estar intrínsecas en las operaciones de la empresa, es decir, que en su centro de monitoreo deben tener herramientas que permitan detectar las máquinas que pertenecen a botnet para así avisarle a los clientes; también tener en el borde del internet una plataforma contra ataques de denegación de servicio, análisis de anomalías, las comunicaciones con los otros proveedores de Internet.

REFERENCIAS BIBLIOGRÁFICAS

1. **Torres García, José.** *Análisis y Evaluación Comparada de redes de acceso GPON Y EP2P.* s.l. : Gestión Académica-FIB, 2009.

2. **Rodriguez, Ariel.** *Comunicaciones HOY.* s.l. : http://martinezfazzalari.com/articulos/Clase%20UBA%20201106.pdf., 2010.

3. **Soto Julio Alba, Millan Ramon Jesús.** *Consultoria Estrategia en Tecnologías de la Información y la Comunicación.* s.l. : http://www.ramonmillan.com/tutoriales/tripleplay.php, 2006.

4. **AXXON.** *Comparación de tecnologías.* s.l. : http://www.axxonsoft.com/sp/ip_video_surveillance/technology_comparison.php, 2003.

5. **Digitales, Ciudadanías.** *Cómo la tecnología puede mejorar nuestra vida cotidiana.* s.l. : http://ciudadaniasdigitales.blogspot.com/2010/03/componentes-de-un-sistema-de-video_29.html, 2010.

6. **Wikipedia.** *Asymmetric Digital Subscriber Line.* s.l. : http://es.wikipedia.org/wiki/Asymmetric_Digital_Subscriber_Line, 2011.

7. **BlogActualidad.** *FTTH: la fibra óptica llega hasta el hogar.* s.l. : http://ofertadescuentos.com/ftth-fibra-optica/, 2010.

8. **Bates, Regis J.** *Fibra Óptica.* s.l. : http://es.wikipedia.org/wiki/Fibra_%C3%B3ptica, 2001.

9. **Bates, Regis J.** *FTTH.* s.l. : http://es.wikipedia.org/wiki/FTTH, 2010.

10. **ASAHINET.** *Diferencias entre FTTH y ADSL.* s.l. : http://asahi-net.jp/en/service/ftth_vs_adsl.html, 2010.

11. **TELNET.** *Introducción a las redes PON.* s.l. : http://www.telnet-ri.es/soluciones/acceso-gpon-y-redes-ftth/la-solucion-gpon-doctor-a-la-interoperabilidad-gpon/, 2010.

12. **Paredes Albuja, Mercedes Margarita.** *Estudio de las tecnologías EPON/GEPON como tecnologías de última milla para el transporte de voz, datos y video, aplicado a una zona residencial del distrito metropolitano de Quito.* s.l. : http://bibdigital.epn.edu.ec/bitstream/15000/1289/1/CD-2666.pdf, 2010.

13. **Henao Guevara, Juan Sebastián.** *Tecnologías de redes PON.* s.l. : http://www.todotecnologia.net/wp-content/uploads/2010/06/Definicion_caracteristicas_PON_APOn_BPON_GEPON_GPON_EPON.pdf, 2010.

14. **Sanguña Guevara, Paul Fernando.** *Estudio Tecnico de la Red de comunicaciones para brindar los servicios de voz, internet y video por demanda de una urbanización.* s.l. : http://bibdigital.epn.edu.ec/bitstream/15000/1764/1/CD-2763.pdf, 2010.

15. **Pabón Taco, Diana Patricia.** *DISEÑO DE UNA RED DE ACCESO GPON PARA PROVEER SERVICIOS TRIPLE PLAY.* s.l. : http://bibdigital.epn.edu.ec/bitstream/15000/1099/1/CD-1943.pdf, 2009.

16. **Acuario Vargas Hilda Patricia, Sangurima Sangurima Jorge Enrique.** *Diseño de una Red GPON para la empresa eléctrica regional centro Sur C.A.* s.l. : http://dspace.ups.edu.ec/bitstream/123456789/31/6/Indice.pdf, 2009.

17. **Abreu Marcelo, Castagna Aldo, Cristiani Pablo, Zunino Pedro, Roldós Enrique, Sandler Gustavo.** *Carácterísticas Generales De Una Red De Fibra Óptica Al Hogar (FTTH).* s.l. : http://www.um.edu.uy/_upload/_descarga/web_descarga_179_CaractersticasgeneralesredfibrapticaalhogarFTTH.-VVAA.pdf, 2009.

18. **Glen Kramer and Biswanath Mukherjee, Sudhir Dixit and Yinghua Ye, Ryan Hirth.** *Supporting differentiated classes of service in Ethernet passive optical networks.* s.l. : http://wwwcsif.cs.ucdavis.edu/~kramer/papers/cos_jon.pdf, 2002.

19. **Vargas, A.** *Tecnología y Arquitectura de las Redes Ópticas GPON.* s.l. : http://dspace.ups.edu.ec/bitstream/123456789/31/8/Capitulo2.pdf, 2009.

20. **Interabs.** *Redes De Acceso Para Banda Ancha Por Fibra Óptica Gepon.* s.l. : http://interabs.net/PDFs/GEPON.pdf, 2010.

21. **Anónimo.** *Seguridad en Redes.* s.l. : http://ldc.usb.ve/~poc/Seguridad-viejo/tcpip.pdf, 2000.

22. **Wagner, Douglas.** *La ubicuidad de redes IP y sus vulnerabilidades.* s.l. : http://www.revista-ays.com/DocsNum08/PersEmpresarial/douglas.pdf, 2007.

23. **Wikitel.** *UA-Redes PON EPON derivados.* s.l. : http://es.wikitel.info/wiki/UA-Redes_PON_GPON_derivados, 2010.

24. **Asensio, Gonzalo.** *Seguridad en Internet, Una guía práctica y eficaz para proteger su PC con software gratuito.* s.l. : http://www.seguridadeninternet.es/images/descarga_promo_SEGURIDAD%20EN%20INTERNET,%20Nowtilus.pdf, 2006.

25. **Ramirez, David.** *IPTV Security Protecting High-Value Digital Contents.* s.l. : http://www.amazon.co.uk/IPTV-Security-Protecting-Digital-Contents/dp/047051924X, 2008.

26. **Gil Gutierrez, Roberto.** *Seguridad en VOIP: Ataques, Amenazas y Riesgos.* s.l. : http://www.uv.es/montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf, 2010.

27. **Garzón, Jesús.** *Videovigilancia segura.* s.l. : http://www.revista-ays.com/docsnum34/persempresarial/Garzon.pdf, 2009.

28. **Communications, Axis.** *Guía técnica de vídeo IP.* s.l. : http://www.axis.com/files/brochure/bc_techguide_33337_es_0902_lo.pdf, 2009.

29. **AMNET.** *Introducción a las redes de Alta Capacidad.* s.l. : http://www.google.com/url?sa=t&source=web&cd=1&sqi=2&ved=0CBYQFjAA&url=http%3A%2F%2Fwww.revistaitnow.com%2Fbajar.php%3Fa%3Dtd10%2Fp%2Fgt%2F16-_amnet.pdf&rct=j&q=Introducci%C3%B3n%20a%20las%20redes%20de%20%20Alta%20Capacidad&ei=RkPeTYzEBszOgAfTs_DVCg&usg=A, 2010.

30. **Otfried Kistner, Christa Tauer, Barrett Klosterneuburg, Wolfgang Mundt.** *Unites States Patent Application Publication.* s.l. : http://www.theoneclickgroup.co.uk/documents/vaccines/Baxter%20Vaccine%20Patent%20Application.pdf, 2009.

31. **Harald Rohde, Dominic A. Schupke.** *Securing Passive Optical Networks Against Signal Injection Attacks.* s.l. : Digital Library, 2007.

32. **Wikipedia.** *Gestión de la Red.* s.l. : http://en.wikipedia.org/wiki/Network_management, 2011.

33. **Tzung-Pao Lin, Kuo-Pao Fan.** *EPON Testbed and Field Trial Environment in Taiwan.* s.l. : http://ir.itri.org.tw/bitstream/987654321/4900/1/E520003.pdf, 2006.

34. **Cisco.** *SNMPv3.* s.l. : http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html#wp4364, 2010.

35. **Y., Valles P. Kirssy.** *SNMPV3.* s.l. : http://neutron.ing.ucv.ve/revista-e/No6/Valles%20Kirssy/SNMPV3/Snmpv3.htm, 2010.

36. **Telnet.** *iQueue, gestor de OLTs y ONUs Epon.* s.l. : http://www.telnet-ri.es/iqueue/, 2011.

37. **Zyxel.** *Powerful Network Management Solution for Passive Optical Networks.* s.l. : ftp://ftp.zyxel.com/NetAtlas_PON,_EPON_Manager/datasheet/NetAtlas%20PON,%20EPON%20Manager_1.pdf, 2009.

38. **AllBusiness.** *GEMS.* s.l. : http://www.allbusiness.com/company-activities-management/operations-customer/5681509-1.html, 2003.

39. **Corp., ZyXEL Communications.** *Product Guide Business & Consumer.* s.l. : http://www.zyxel.es/ZyPartner11/PG-Business-Consumer11.pdf, 2010.

40. **D-Link.** *Product Guide.* s.l. : D-Link, 2008.