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

Cervantes, Margie; Pesantez, Dolores; Rosales, Giomayra; Aranda, Alfonso Ing.
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador

Resumen

Empresas de telecomunicaciones en el mundo están en continua competencia, por lo que optan por innovar servicios, utilizando banda ancha basadas en IP, brindando servicios a bajos precios y con una baja 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. Esta tecnología 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. Su implementación permitirá a los proveedores de internet maximizar el valor de sus activos, atraer nuevos clientes y mantener a los actuales, 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 que provocan ciertos escenarios desfavorables que hacen que una red GEPON no sea segura. Por tal motivo este paper propone 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.

Abstract

Telecommunications companies in the world are in constant competition, so they choose to innovate services using IP-based broadband, providing services to low prices and low investment in network equipment. Among the most interesting technologies at the moment, we have GEPON, which is an access technology trough fiber optic with point to multipoint architecture. This technology is new in our country, supports X-Play services such as voice, Digital TV, Video Security, Video on Demand Data and Internet through fiber optic with a high speed connectivity and minimum installation costs. Its implementation will allow to the internet providers to maximize the value of their assets, attract new customers and keep the current ones, by offering more and better services at competitive prices, with a small investment in equipment and network maintenance. However in the real world we found factors that cause certain unfavorable scenarios that make that network GEPON be insecure. Therefore this paper proposes the design and GEPON Network Security for Quadruple-Play services, based on the analysis of different Quadruple-Play Services, Types of Networks, Protocols, Architecture, Design and Security Network GEPON applying Deming cycle.

1 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.

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.

2 Problema

2.1 Definición

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.

2.2 Objetivos

El presente trabajo tiene como objetivo analizar y proporcionar información oportuna, precisa y concisa de 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.

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

- Estudiar el ambiente actual de seguridad de la red GEPON.
- Definir el mejor diseño de una red GEPON.
- Comprensión y manejo de las tecnologías de acceso multimedia, altamente utilizadas en la actualidad.
- Mantener los sistemas generando resultados.
- Identificar 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.

2.3 Alcance

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.

3 Análisis

3.1 ¿Qué estamos resolviendo?

En las redes GEPON, la seguridad no ha sido uno de los puntos más destacados, ya que la red puede llegar hacer accesada sin autorización.

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.

La diversidad de soportes de transporte de comunicaciones IP también ha 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.

3.2 ¿Por qué lo estamos resolviendo?

Una vez llevado a cabo el estudio de la red GEPON, se podría dar paso a la implementación de esta red, que permitirá a los proveedores de internet maximizar el valor de sus activos, atraer nuevos clientes y mantener a sus actuales clientes, ofreciéndoles un mejor servicio a los usuarios en términos de velocidad, seguridad, variedad de servicios, tiempo y precios competitivos, con una inversión reducida en el equipamiento y mantenimiento de la red.

3.3 ¿Cómo lo estamos resolviendo?

Realizamos un estudio basado en todos los posibles ataques a los que la red GEPON es susceptible, esto lo logramos 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 alteren la disponibilidad, confidencialidad o integridad de la información logrando que se comporte de una forma débil a los diferentes ataques.

Una vez analizados todos los posibles puntos recomendamos soluciones a dichas vulnerabilidades que logren que la red GEPON sea robusta

3.4 ¿Qué datos se deben proteger?

GEPON requiere de un mecanismo completo de seguridad ya que 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.

3.5 Ataques, Vulnerabilidades y Consecuencias de los Servicios X-Play

Ataques a Video Vigilancia IP	Vulnerabilidades	Consecuencias
Ataques de Autenticación	Contraseña por defecto. Acceso de IP sin control Servidores desactualizados	Control total del sistema de Video Vigilancia
Ataque de Diccionario	Contraseña débil	Contraseña descubierta.
Inundación de direcciones MAC	Tabla CAM con tamaño limitado y memoria mal segmentada	Desbordamiento de la tabla CAM, denegación de servicio, puertos inundados.
Suplantación del Servidor DHCP	Falta de control para que exista otro DHCP	Suplantación del Servidor DHCP.
Ataque al Protocolo de Resolución de direcciones ARP	No usar mecanismos de control que asocien direcciones IP con MAC	Paquetes de datos atrapados y modificados.

Ataques a Telefonía IP	Vulnerabilidades	Consecuencias
Gusanos, virus y cortafuegos e IPS/IDS mal configurados.	Mala administración de equipos.	Acceso a la infraestructura de red corporativa. Gatekeeper comprometido. Fraude telefónico.
DoS, Secuestro de sesiones (Hijacking), (Eavesdroping)	Ataques 1 Robo ancho de banda. Inundación de sistema con llamadas comprometidas Ataques 2 Falta de validación y secuenciación. Cifrado limitado.	
ICMP unreachable Variedad de floods SQL injections Denegación en DHCP Man-in-the-middle Buffer overflows SPIT (SPAM) Vishing (Phising) Fuzzing Floods Interceptación Redirección de llamadas Reproducción de llamadas	Inundación sistema con llamadas comprometidas.	Tráfico malicioso que afecte la calidad del servicio.

Ataques a IPTV	Vulnerabilidades	Consecuencias
Captura de tráfico, cuando datos de bajada de usuarios llegan a todos los CM (Cable-Modems) – En capa Física	Desvío de cables de conexión hacia otros sistemas	Acceso no autorizado a los equipos con los que la red opera
MAC: en fichero de configuración de un CM viene el número de equipos que pueden acceder a la red. El CM registra las MAC – En todas las capas	Interceptación intrusiva de comunicación entre equipos	
Modificación IP Suplantación de mensajes. Denegación de mensajes.- En capa de Red, Transporte y Aplicación	Bajo nivel de autenticación (IP)	Acceso malintencionado a los datagramas IP
Suplantación de DNS. Suplantación de IP. Husmear. Exploit de desbordamiento de buffer. - En capa de Red, Transporte y Aplicación.	Deficiencias de programación – Telnet - para ataque 3. Deficiencias en proceso de autenticación - para ataques 1 y 2.	Acceso malintencionado a BD del servidor DNS.

Ataques a Internet Banda Ancha	Vulnerabilidades	Consecuencias
Virus, Troyanos Spyware, Malware, Código malicioso en general - En capa Física, de Red, Transporte y Aplicación	Mala administración de los equipos	Información de la Organización Comprometida
Envío y recepción de correo basura - En capa de Red y Transporte	Registro de cuenta de correo en foros. Falta de cultura de las personas.	Saturación de red. Enviados a listas negras lo que produce el rebote de todos mis correos.
Phishing (ataque transparente) - En capa de Red, Transporte y Aplicación.	Falta de cultura de la gente al revisar correos mal intencionados. (spam).	Robo de credenciales. Robo de datos al ingresar en páginas web falsas.
Hijacking (Secuestro) En capa de Red, Transporte y Aplicación.	Mala administración de los equipos	Secuestro de identidad del usuario.
Inundación Desbordamiento de buffer. - En capa de Red, Transporte y Aplicación.	Robo de ancho de banda Inundación del sistema con llamadas comprometidas	Bloqueo de la red impidiendo su normal funcionamiento

4 Solución

4.1 Diseño Propuesto

Se propone como solución para disminuir posibles ataques y fallo en la transmisión de los servicios, utilizar la topología anillo, para que así la transmisión, si no es posible que se dé por un camino, dada alguna situación que lo provoque, pues entonces existan otros caminos, de manera que el usuario final siempre cuente con los servicios.

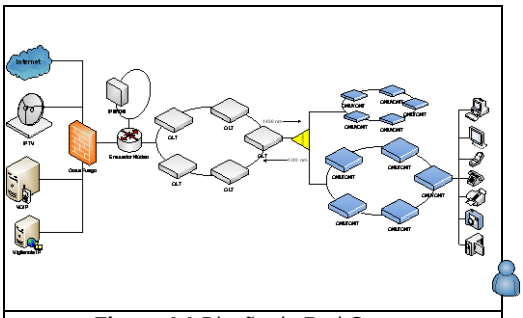

Figura 4.1 Diseño de Red Gepon

Para tener un mayor control sobre la red, existen sistemas de gestión de red, que combinan hardware y software para controlar y administrar una red, y así detectar automáticamente los dispositivos conectados a ella.

4.2 Medidas de Seguridad

Se citan las siguientes medidas de seguridad de manera general:

- **Autenticación fuerte:** no enviar contraseñas 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.
- Antivirus, anti-spy, cortafuegos, IPS/IDS y un firewall eficaces.
- Atención a correos con extensiones: .com, .exe, .bat, etc.
- **Espionaje DHCP:** Asegura integridad del IP.
- Mantener los sistemas actualizados y parcheados.
- Tener a los OLT's en capa 3 para poder configurar las ACL's.
- Establecer filtros MAC en cada ONU.

5 Conclusiones

- Las redes Gepon heredan las amenazas y vulnerabilidades de sus antecesoras (Metro Ethernet, GPON), maximizando la posibilidad de generar mayor tráfico malicioso debido a los grandes anchos de banda que las mismas manejan en conjunto con las malas prácticas de los usuarios residenciales.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

6 Recomendaciones

1.- Las empresas proveedoras de servicios X-play deben controlar el inter-routing entre los diferentes servicios que se ofrecen, es decir que de un servicio de red de telefonía no se pueda ir a un servicio de televisión IP, o a sus diferentes combinaciones.

2.- Los proveedores de soluciones de redes GEPON deben contar con equipos de inspección de tráfico que posean la capacidad de descubrir canales encubiertos comúnmente usados por las malwares y/o botnets.

3.- Implementación de un sistema automático de monitoreo y control en tiempo real de vulnerabilidades para los dispositivos o activos más importantes de la red.

4. 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.

5. Utilización de la red GEPON, con respecto a GPON debido a su gran ancho de banda, seguridad y principalmente bajo costo en los equipos.

6. Contar con personal capacitado en estas nuevas tendencias tecnológicas ya que apuntan al crecimiento con mayores y mejores servicios y de igual manera nuevos tipos de ataques a los que tendrían que contrarrestar.

7. Realizar el Análisis de Riesgo de activos y estudiar casos o escenarios críticos que puede sufrir la red, analizando contramedidas para que esta tecnología siga teniendo acogida con una arquitectura eficiente, robusta y segura.

8. Lograr una Alta Visibilidad identificando, clasificando y asignando niveles de confianza a los suscriptores, servicios y tráfico a través de software de gestión de red y por medio de la interfaz entre el proveedor y el abonado, monitoreando recursos.

9. Lograr un Control Total haciendo cumplir las reglas de acceso a los sistemas y recursos de la red.

10. Contar con equipos de seguridad perimetral, como IPS/IDS, detectores de anomalías, detectores de botnet, etc.

7 Referencias

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.