UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE CIENCIAS ADMINISTRATIVAS, MEXICALI

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

"PROPUESTA DE IMPLEMENTACIÓN DE REDES DE ÁREA LOCAL VIRTUALES EN LA FCA-UABC"

TESIS

PARA OBTENER EL GRADO DE:

MAESTRO EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

PRESENTA:

ING. FERNANDO IRIBE PÉREZ

DIRECTOR DE TESIS

M.A. JESÚS FRANCISCO GUTIÉRREZ OCAMPO

MEXICALI, BAJA CALIFORNIA ABRIL DE 2009

PROPUESTA DE IMPLEMENTACIÓN DE REDES DE ÁREA LOCAL VIRTUALES EN LA FCA-UABC

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

AGRADECIMIENTOS

Agradezco a Dios por todas las bendiciones recibidas, a mi familia por todo su amor y apoyo incondicional; principalmente a mi esposa y a mi madre, a los encargados de las áreas de informática en la Facultad de Ciencias Administrativas y en la escuela de Enfermería por las atenciones recibidas y a mi director de tesis Maestro Jesús Francisco Gutiérrez Ocampo por todo su apoyo. Un especial agradecimiento para la Maestra Lucia E. Algravez Uranga por sus consejos, su entusiasmo, su dedicación y por motivarnos a dar siempre lo mejor de nosotros.

Fernando Iribe

CAPÍTULO I

INTRODUCCIÓN

La red de área local virtual (VLAN) es una nueva tecnología que permite incrementar la productividad de una empresa interconectando todas las computadoras de manera que los usuarios puedan tener acceso a la información con independencia de su ubicación y tipo de equipo informático. (Tanenbaum, 2003, p.338). Las VLANs han cambiado la forma de trabajar de las empresas y de los empleados, ya no es necesario mantener una ubicación física común para todos los empleados si se quiere acceder a la información que estos necesitan para realizar su trabajo. (Tanenbaum, 2003, p.329). Molina (2006) considera que las redes de área local son fiables y manejan grandes velocidades de transmisión de datos; por lo cual, constituyen una herramienta indispensable de todo trabajo empresarial. (Molina, 2006, p. XVII).

1.1 ANTECEDENTES

A partir de la década de 1980 las computadoras se empiezan a utilizar en los negocios aunque no contaban con grandes ventajas, el software de aplicación de las computadoras funcionaba sólo para un usuario a la vez y para un equipo en específico, pero conforme dicho software fue evolucionando y permitiendo su funcionamiento en diferentes equipos y para varias personas; la transmisión

electrónica de datos entre computadoras se hizo cada vez más necesaria e importante en las empresas. (Norton, 2000, p. 5).

Posteriormente surgen las redes de computadoras; las cuales aumentan el valor de las computadoras dentro de las empresas. En la actualidad la comunicación entre computadoras se puede realizar por medio de módems (a través de las líneas telefónicas) y de redes (mediante dispositivos de interconexión), donde una red de computadoras es un conjunto de computadoras y dispositivos interconectados que permiten intercambiar información, compartir recursos y comunicarse. (Norton, 2000, p. 247). Existen varios tipos de redes, uno de los más comunes es la red de área local (LAN), la cual es una red que conecta computadoras y otros dispositivos (como impresoras) en un área geográfica que abarca metros o pocos kilómetros de distancia; por ejemplo, la red de computadoras dentro de un laboratorio de computación. (Fitzgerald, 2003, p. 30). Otro tipo de redes son las de área amplia (WAN), las cuales se forman a partir de redes LAN. Una WAN no utiliza un medio de transmisión compartido y abarca áreas muy extensas como ciudades o países. A pesar de las grandes distancias que abarca la red WAN se puede obtener información y tener acceso a otros recursos (impresoras, cd's) en segundos, ya que se utilizan medios y dispositivos de comunicación muy veloces, un ejemplo de ellos es el satélite. Tres características muy importantes de las redes WAN son que tienen un mayor costo, alcanzan distancias muy grandes y son menos veloces que las redes LAN. (Zacker, 2001, p. 10).

Las redes tienen muchos beneficios; según Tanenbaum (2003) y Norton (2000), los seis principales son los siguientes:

- Se puede tener acceso simultáneamente a los mismos programas e información (los cuales pueden estar ubicados en una sola computadora a la cual acceden todos los usuarios).
- Los usuarios pueden compartir equipos periféricos como impresoras y copiadoras digitales.
- La comunicación personal se vuelve más eficiente (se puede utilizar el correo electrónico, la videoconferencia y el servicio de chat)..
- Hacen posible una administración remota (en caso de estar físicamente separado por grandes distancias).
- Los usuarios pueden utilizar respaldos de la información de una manera muy fácil (y desde un solo lugar).
- Permiten compartir una sola conexión de Internet con toda la red.

Las primeras LANs dependían de un concentrador central (hub); el cual es un dispositivo que permite crear redes, en él todos los usuarios se conectaban para crear la LAN. En estas LANs el aspecto geográfico (físico) era el que se imponía al lógico, los dispositivos que debían estar conectados y en comunicación forzosamente tenían que estar cerca físicamente. Posteriormente, aparecen los conmutadores (dispositivos para crear redes y controlar el tráfico de información), los cuales permiten configurar las LANs de manera lógica (a través de software), creando VLANs dentro de redes físicas. (Tanenbaum, 2003, p. 328).

Una VLAN es una red de área local lógica, son acomodos lógicos de dispositivos o usuarios dentro de una red independientemente de su ubicación física en una red. (Tanenbaum, 2003, p. 338). Mediante el empleo de estas redes virtuales se pueden efectuar migraciones (de un edificio a otro, por ejemplo) en un corto tiempo y muy fácilmente, lo cual no podría ocurrir sin las VLANs, ya que se necesitarían realizar cambios en los equipos y algunas veces en el cableado. Estas redes virtuales son flexibles y proporcionan grandes ahorros en tiempo, esfuerzo y dinero, además, permiten habilitar o deshabilitar recursos de la red por grupos a través de sólo software. Una gran ventaja es que se pueden segmentar conjuntos de computadoras en grupos de trabajo y si hay problemas en un grupo, éstos no afectarán a los demás. Lo anterior también nos permite detectar con mayor facilidad donde se presenta un problema dentro de toda la red (Hill, 2003, p. 528). El deseo de aprovechar las características y ventajas de esta tecnología motivó la realización de la presente investigación, la cual proporciona una propuesta de implementación de VLANs dentro de la Facultad de Ciencias Administrativas (FCA) de la Universidad Autónoma de Baja California (UABC).

A continuación se proporciona información de las instituciones UABC y FCA, ya que la propuesta de implementación va dirigida a ellas. En la revista Gaceta Universitaria de febrero, 1992, volumen 1, página 3, se publicó que el día 28 de febrero de 1957 se promulga oficialmente la Ley Orgánica de la UABC, durante la gestión gubernamental del licenciado Braulio Maldonado Sánchez y fue el resultado del trabajo conjunto de estudiantes, profesionistas, intelectuales y empresarios del estado

de Baja California. La escuela Cuauhtémoc de Mexicali fue la sede inicial y la Escuela Preparatoria de Mexicali se convirtió en la primera escuela de la UABC. En ese mismo año se creó en Ensenada la escuela preparatoria de la UABC, y para el siguiente, se incorpora la Escuela de Enfermería. Ese mismo año se crean más escuelas en Mexicali, Tijuana y Ensenada. En 1964 la UABC adopta el lema “Por la Realización Plena del Hombre”, propuesto por el estudiante Miguel Gárate Velarde. Poco después, la Universidad se identifica también por un escudo creado por el pintor José Reyes Meza. De 1975 a 1979 se realizaron más avances en materia de infraestructura y se crea Radio Universidad, la primera estación de radio cultural de Baja California y de la frontera norte del país. En 1977 se instala rectoría en el antiguo edificio del palacio de gobierno. De 1987 a 1991 se llevaron a cabo diversas obras de construcción entre las que destacan: el Laboratorio de Informática de la Escuela de Ingeniería de Mexicali, los laboratorios de Educación, Psicología y Comunicación; en este periodo se autoriza el uso del Satélite Morelos en una Red de Comunicaciones y Teleproceso para enlazar a todas las unidades académicas y administrativas de la Universidad. En diciembre del 2000 se establece la Facultad de Ciencias Administrativas.

En el primer informe de actividades 2005 del M.A.I. Hilario de Torre Pérez; director (en ese año) de la actual Facultad de Ciencias Administrativas unidad Mexicali (FCA) perteneciente a la UABC, menciona que la Facultad de Contabilidad y Administración de la UABC; Unidad Mexicali, inició sus actividades en 1967, que en 1972 la Escuela de Contabilidad y Administración de Mexicali alcanza su plena autonomía de la

Escuela de Contabilidad y Administración de Tijuana. También menciona que de 1972 a 1977 se incluyeron el programa de Licenciado en Administración de Empresas, el de Licenciado en Informática, las especialidades de Administración de Recursos Humanos, Administración Financiera y Administración en Fiscal y la Licenciatura en Negocios Internacionales. En diciembre de 2000, cambia de escuela a facultad y desde entonces se han creado las siguientes maestrías: Maestría en Contaduría, Maestría en Administración y Maestría en Tecnologías de la Información y la Comunicación. Además, se creó el Doctorado en Administración. A la fecha de febrero de 2006 la FCA contó con más de 8,000 egresados, los cuales han tenido una gran aceptación por los empleadores, tanto del sector público como privado.

En el Plan de Desarrollo 2005 para la FCA se especifican su misión y su visión. Tiene como Misión contribuir al logro de una sociedad y un mundo más justo, democrático, equitativo y respetuoso, a través de: la formación, capacitación y actualización de profesionistas de calidad, con un alto sentido ético y responsabilidad social, mediante la generación de conocimientos científicos en las áreas de negocios y administración; así como la creación, desarrollo y difusión de valores culturales que enriquezcan la calidad de vida en Baja California, el país y el mundo. La visión de la FCA se caracteriza por su desempeño eficaz, eficiente, innovador, donde los estudiantes son el centro de los procesos académicos, participan activamente en eventos deportivos y culturales; respondiendo al reto de contribuir al logro de una sociedad más justa, democrática, equitativa y respetuosa de su medio ambiente, formando profesionales e investigadores plenamente realizados.

En la revista Gaceta Universitaria de marzo, 2008, Número 205, página 2, se publicó que la FCA ha incrementado su matrícula significativamente en los últimos años. En base a referencia empírica, se conoce de la FCA lo siguiente: es la segunda de las unidades académicas con mayor población estudiantil y la tercera a nivel estatal, el crecimiento de la FCA para este año 2009 prevé una matrícula de cinco mil alumnos en los programas de Técnico Superior Universitario, Licenciatura y Posgrado. En este número 205 de la revista Gaceta Universitaria también se publicó lo siguiente: La FCA; que se encontraba en los espacios centrales de la UABC, sale y se va a la zona del Río Nuevo en mayo del 2007, donde está formada por cinco edificios de nueva creación, los cuales son edificio A, edificio B, edificio C, edificio D y el edificio CIA.

El deseo de la FCA-UABC de mejorar el rendimiento en su LAN en los laboratorios de cómputo instalados en el edificio “C” dieron origen a la presente investigación, cuyo propósito fue elaborar una propuesta de implementación de VLANs en dichos laboratorios, con el objetivo de aumentar el rendimiento de la red; beneficiando con esto a alumnos, docentes y al administrador de los laboratorios, ya que el acceso a la información será más rápido y con mayor privacidad.

La persona encargada de la operación de una LAN se conoce como administrador de la red y su objetivo es asegurarse de que los usuarios tengan acceso a la información y a los recursos que necesitan para completar su trabajo. Una de las tareas del administrador de una red es solucionar todos los problemas que se presentan en ella, cuando la red falla y no se encuentra el administrador, la tecnología de administración

remota ayuda a mantenerse en contacto con la red sin estar físicamente en la misma ubicación (Hallberg, 2007, p. 6).

Mediante el empleo de VLANs el administrador de los laboratorios puede gestionar todos los recursos de la red mediante una sola máquina y vía software, sin invertir mucho tiempo, esfuerzo y dinero de la institución. Además, es posible habilitar o deshabilitar recursos de red por grupos de usuarios o de computadoras, de manera rápida, fácil y económica. Una VLAN proporciona una forma de crear grupos de usuarios que no tienen por qué encontrarse dentro de la misma área de trabajo, dichos grupos facilitan la estructura de las diferentes áreas de la institución, debido a que personas de distintas áreas pueden integrarse en proyectos de grupos especiales a los cuales se les proporcione un ambiente privado y seguro, donde nadie más tiene acceso a su información. (Schweitzer, 2005, p.29).

El presente trabajo constituye una propuesta de implementación de redes de área local virtuales en los cinco laboratorios del edificio “C” de la Facultad de Ciencias Administrativas de la Universidad Autónoma de Baja California, aquí se proporciona información general sobre el propósito y funcionamiento de las VLANs, así como información detallada respecto a la construcción de las mismas. Esta investigación permite al personal de informática de las diferentes facultades de la UABC obtener la información necesaria para poder implementar VLANs en sus respectivos centros de cómputo, sin tener que pagar a empresas externas para realizar dicho trabajo.

En cuanto a la metodología que se empleó, esta investigación fue no experimental cuantitativa, con un alcance inicial exploratorio y uno final descriptivo. (Hernández, 2006, p. 100).

1.2 PLANTEAMIENTO DEL PROBLEMA

Las VLANs se crean con conmutadores especialmente diseñados para ese propósito (Tanenbaum, 2003, p. 328). El edificio “C” de la FCA cuenta con cinco laboratorios de cómputo con una estructura de red basada en dichos conmutadores. Actualmente existe una sola red de área local formada por varias subredes (redes de área local más pequeñas) instaladas en los cinco edificios de la FCA, esto provoca una gran lentitud en la red y caídas en las llamadas telefónicas. La información procesada en el edificio “C” no se encuentra aislada de la información procesada por los otros edificios de la FCA, provocando que aumente la lentitud de la red con cada computadora que se conecte y acceda a la información contenida en ella. El rendimiento de la red existente en el edificio “C” puede ser mejorado mediante la implementación de VLANs, beneficiando a un gran número de alumnos, docentes y administrador de los laboratorios. Mediante el uso de VLANs el administrador de los laboratorios puede administrar todos los recursos mediante una sola máquina y vía software, sin invertir mucho tiempo, esfuerzo y dinero de la institución. El problema principal a resolver mediante la propuesta de implementación de las VLANs es la disminución del rendimiento de la red de área local dentro de los cinco laboratorios del edificio “C” de la FCA conforme aumentan los accesos de los usuarios.

1.3 SUPUESTO

El supuesto que guió este trabajo de investigación fue el siguiente:

El empleo de VLANs permitirá aumentar el rendimiento de la red de área local de los laboratorios de cómputo del edificio “C” de la Facultad de Ciencias Administrativas de la Universidad Autónoma de Baja California.

1.4 OBJETIVOS.

Objetivo General.

El objetivo general de esta investigación fue crear una propuesta de implementación de redes de área local virtuales dentro de los laboratorios de cómputo instalados en el edificio “C” de la Facultad de Ciencias Administrativas de la Universidad Autónoma de Baja California.

Objetivo Particular.

El objetivo particular de esta investigación fue contar con el conocimiento necesario para poder aumentar el rendimiento de la red de área local dentro de los laboratorios de cómputo instalados en el edificio “C” de la Facultad de Ciencias Administrativas mediante la aplicación de VLANs.

1.5 IMPORTANCIA DEL ESTUDIO

Este estudio proporciona información que permite tomar la decisión de implementar las redes tipo VLAN en la FCA-UABC, con las consecuentes mejoras en el sistema por las características propias de las VLAN que permiten mejorar la administración de recursos y servicios informáticos. Además, la FCA no ocupará gastar grandes cantidades de dinero en cableado porque en la mayoría de los casos ya no será necesario volverlo a instalar. Los alumnos y maestros podrán acceder a su información de manera más rápida y segura.

La información proporcionada por esta investigación puede ser usada para realizar una propuesta de implementación de VLANs en la LAN administrativa de la FCA y aprovechar todos sus beneficios, principalmente los de seguridad, segmentación y movilidad.

A nivel nacional e internacional, la importancia científica del presente trabajo se debe al hecho de que beneficia a los estudiantes de carreras relacionadas con la informática de las distintas instituciones educativas, así como para los profesionales de la informática y las redes, ya que el tema de la virtualización es muy actual y brinda grandes beneficios, como la segmentación y la seguridad. (Sturdevant, 2008, p. 35).

La importancia humana de la presente investigación radica en que las VLANs son una herramienta que facilita al hombre el manejo y acceso a uno de sus principales recursos, la información. Se dice que la información es poder y esta herramienta permite utilizar dicho recurso de una manera más eficiente, rápida y confiable.

La importancia contemporánea del manejo de las VLANs la da el hecho de que es una tecnología joven, la cual se presenta dentro del avance tecnológico que ha caracterizado a las últimas décadas.

1.6 LIMITACIONES DEL ESTUDIO

El estudio se limita a la propuesta de implementación de VLANs dentro de los cinco laboratorios de cómputo instalados en el edificio “C” de la FCA de la UABC, pero puede ser generalizado a cualquier LAN del mundo.

Las tres variables que se manejan en esta investigación son el rendimiento de la red, las VLANs y los laboratorios de cómputo instalados en el edificio “C” de la FCA perteneciente a la UABC.

CAPÍTULO II

REVISIÓN DE LA LITERATURA

En este capítulo se explican brevemente los conceptos básicos manejados en las redes, creando un marco de referencia que permita comprender las bases de las redes virtuales de área local (VLANs). Estos conceptos son fundamentales para comprender las funciones de las redes y sus dispositivos. Aquí se expone de forma sencilla el inicio de las computadoras y su evolución al paso del tiempo hasta llegar a las VLANs, todo esto de manera muy general.

2.1 CONCEPTOS BÁSICOS DE REDES DE COMPUTADORAS.

Una computadora es una máquina que el hombre utiliza como herramienta para realizar una infinidad de tareas, la cual le permite introducir datos, almacenarlos, procesarlos y obtener información. (Norton, 2000, p. 5). Las primeras computadoras eran muy grandes y se denominaron Supercomputadoras. Al paso del tiempo se han creado computadoras cada vez más pequeñas, más baratas y más rápidas, apareciendo las mini y microcomputadoras. La primera computadora personal (PC) se desarrolló en los años 50 por la empresa IBM, pero es en la década de 1980 cuando las PCs empezaron a ser populares y utilizadas en las empresas. (Zacker, 2002, p. 3). Al ir creciendo el uso de las PCs surge la necesidad de la comunicación de información entre ellas y aparecen las redes (LAN). (Norton, 2000, p. 247).

Según Zacker (2002), una red es un conjunto de computadoras y dispositivos interconectados que permite intercambiar información, compartir recursos y comunicarse. Existen varios tipos de redes; por su distribución geográfica, uno de los más comunes es la red de área local (LAN), cuya característica es que conecta computadoras en un área geográfica que abarca metros o pocos kilómetros de distancia. Otro tipo son las redes de área amplia (WAN), las cuales se forman de redes LAN. Una WAN no utiliza un medio de transmisión compartido y abarca áreas muy extensas como ciudades o países. (Mañas, 2004, p. 6). Los enlaces WAN son manejados por empresas públicas o privadas que utilizan medios de transmisión que proporcionan gran ancho de banda y altas velocidades de transmisión. (Molina, 2006, p. 27). Estos son; desde el punto de vista geográfico, los dos tipos principales de redes existentes. Desde el punto de vista de relaciones lógicas entre computadoras, se encuentran redes que utilizan máquinas servidores (por ejemplo, servidores de archivos) y otras que no los usan (redes de igual a igual) como es el caso de la red de los laboratorios del edificio “C” de la Facultad de Ciencias Administrativas. (Norton, 2000, p. 254). Según Tanenbaum (2003) y Norton (2002) las redes tienen muchos beneficios, cuatro de los más importantes se mencionan en la Tabla 1.

Tabla 1: Los cuatro beneficios más importantes de las redes.

Acceso simultáneo a programas e información por parte de numerosos usuarios.
Compartir equipo periférico (usualmente caro), como impresoras.
Comunicación personal más eficiente mediante el empleo del correo electrónico, videoconferencia y chat.
Proceso de respaldo más fácil.

A cada uno de los equipos que se conectan directamente a una red se les llama nodo, dos de los tipos más importantes de nodos son las estaciones de trabajo (computadoras que ejecutan aplicaciones locales como el Microsoft Office) y los servidores. (Palmer, 2001, p. 8). Los servidores más comunes son los de archivos, de red, de impresión y de correo. Las máquinas que solicitan servicios a un servidor se conocen como clientes. La tecnología cliente/servidor es muy utilizada y como su nombre lo indica, está basada en clientes y servidores. (Norton, 2000, p. 258). En las redes de igual a igual, todos los nodos de la red tienen el mismo nivel y cada nodo puede tener acceso a los recursos de todos los demás nodos, así que la relación es no-jerárquica. (Habraken, 2000, p. 6). Estas redes se encuentran en empresas chicas o en escuelas, tal es el caso de la red existente en los laboratorios de cómputo del edificio “C” de la FCA perteneciente a la UABC. En organizaciones grandes por lo general se utilizan redes cliente/servidor. (Norton, 2000, p. 258).

Las redes LAN están constituidas por segmentos de red, donde un segmento es un conjunto de computadoras y dispositivos que comparten el mismo medio de transmisión y el espacio geográfico que usualmente utilizan es el de un departamento, un aula de informática, un laboratorio de cómputo, etc. A los segmentos de red también se les conoce como subredes ya que toda red contiene mínimo uno de ellos. (Molina, 2006, p. 26).

Otro tipo de red muy utilizado es la red troncal (también llamada backbone) o red principal de una red de comunicaciones que permite conectar varias redes, son de

mayor capacidad (usualmente se utiliza fibra óptica) y permiten obtener un mayor rendimiento de las conexiones LAN. Dos aspectos que se deben mencionar son que puede aumentar el costo y reducir la capacidad de transmisión. (Molina, 2006, p. 130).

Las redes; al igual que las computadoras, se componen de hardware (las partes tangibles o físicas) y software (la parte intangible). El software requerido para crear una red y poder administrar todos sus recursos es el sistema operativo de red (NOS), éste software se instala en una computadora conocida como servidor y presta servicios a estaciones de trabajo de red conocidas como clientes. (Flynn, 2001, p. 252). Según Vallejos (2001) y Flynn (2001), algunos ejemplos de NOS son Windows Server 2008, Unix, Netware de Novell, LAN Manager de Microsoft, LAN Server de IBM y VINES de Banyan.

El acomodo físico de los cables que conectan los nodos de la red se conoce como topología. Las topologías de cableado más usuales son las siguientes: bus, estrella, bus en estrella, estrella jerárquica y anillo. (St-Pierre, 2005, p. 100). Se toman una serie de factores para determinar que topología se va a usar, entre los factores considerados están el tipo de computadoras instaladas, el tipo de cableado que se está usando, el costo de los componentes y los servidores requeridos para instalar la red, la distancia entre cada computadora y la velocidad con la que la información debe viajar por la red. (Norton, 2000, p. 261). Una topología de bus está formada por un solo cable al cual se conectan todos los dispositivos de la red, los cuales

transmiten en cualquier momento, pero si un mensaje choca con otro que fue enviado por otros nodos (conocido como una colisión) cada nodo espera al azar un cierto tiempo y luego intenta de nuevo enviar la información. Para evitar los choques de transmisiones se requiere de circuitos y software extra, y una conexión rota puede derribar toda la red. La topología anillo conecta los nodos de la red en una cadena circular en la cual cada nodo está conectado al siguiente y el último nodo en la cadena se conecta al primero para completar el anillo, cada nodo examina la información enviada a través del anillo y si la información no está dirigida al nodo que se encuentra examinándola, entonces ese nodo la entrega al siguiente nodo en el anillo. La topología de anillo ofrece una ventaja importante sobre la topología bus y es que no hay riesgo de colisiones porque la información siempre fluye en una dirección, pero cuenta con la desventaja de que si una conexión se rompe toda la red se cae. (Raya, 2006, p.37).

Sin importar que tipo de red se utilice, siempre se necesitará de cables y otros medios por los que viaje la información desde su emisor a su receptor. El tipo de cableado establece la velocidad y la distancia que se puede manejar en una red. (Shaughnessy, 2000, p. 217). Los cables más comunes para la comunicación de datos son: el cable de par trenzado, el cable coaxial y el cable de fibra óptica. El cable de par trenzado esta formado por cuatro y ocho filamentos de alambres de cobre, cada uno cubierto de plástico, trenzado por pares el uno con el otro y envueltos en otra capa de aislamiento plástico. Este cable casi no tiene protección contra la interferencia externa y también lo llaman cable de par trenzado sin blindaje (UTP). El

cable de par trenzado también puede estar cubierto por una envoltura de metal y se le llama cable de par trenzado cubierto blindado (STP). (Raya, 2006, p.45). La diferencia entre las frecuencias más altas y las más bajas de un canal de transmisión se conocen como ancho de banda. El ancho de banda se reduce conforme más usuarios transmiten información a través de una red, por lo que todas las transmisiones se vuelven más lentas. El ancho de banda se expresa en ciclos por segundo (hertz) o en bits por segundo y se utiliza; en una red, para indicar que la cantidad de datos que pueden transmitirse es alta o no para un periodo de tiempo determinado. (Mañas, 2004, p.25). Otro cable es el coaxial, el cual cuenta con dos conductores, uno es un solo alambre por donde viajan los datos y se encuentra en el centro del cable, el otro es una malla de alambre que rodea al primer alambre con un aislante entre ambos. En las redes se usan dos tipos de cable coaxial: grueso y delgado. El tercer tipo de cable es la fibra óptica, la cual es un filamento delgado de vidrio o plástico que transmite una señal óptica de uno a otro extremo de la fibra. Este cable puede transportar información a 50 megabits por segundo (Mbps) debido a que la luz viaja a una frecuencia mucho más alta que las señales eléctricas. Unas ventajas de la fibra óptica son las siguientes: es inmune a la interferencia electromagnética y soporta mayores distancias y velocidades que el par trenzado y el coaxial. Unas desventajas son que es más cara que los cables par trenzado y coaxial, y es muy difícil de instalar porque no se dobla en las esquinas tan fácilmente. En la actualidad los costos han bajado y se ha vuelto popular en las industrias de comunicación como compañías de teléfonos y de cable de televisión. (Raya, 2006, p. 43).

Otro canal por el que viaja la información desde su fuente a su destino es el enlace inalámbrico. La comunicación inalámbrica compite con el cable de par trenzado, el coaxial y el de fibra óptica. La ventaja de la comunicación inalámbrica es la flexibilidad que ofrece en términos del acomodo de la red. La comunicación inalámbrica depende de señales de radio o de señales infrarrojas. (Raya, 2006, p. 51).

Toda computadora en una red requiere de hardware para poder enviar y recibir información a través de un medio de comunicación, parte de dicho hardware es la tarjeta de interfase de red o NIC por sus siglas en inglés. La NIC establece la topología a utilizarse en la red y contiene una dirección única en el mundo conocida como dirección MAC que identifica a la computadora dentro de toda la red. Se encuentra dentro de la computadora y proporciona un puerto en la parte trasera de la PC al cual se conecta el medio de comunicación. (Bigelow, 2003, p. 16). La computadora requiere software de red, que le dice a la computadora como usar la NIC. Es necesario que tanto el software de red como la NIC se apeguen a un protocolo de red, que es un conjunto de estándares para comunicación. Un protocolo de comunicación de red es un conjunto de reglas y formatos que permiten a las computadoras intercambiar información. Los protocolos más comúnmente usados en las redes son TCP/IP, IPX/SPX y NetBEUI. (Norton, 2000, p. 266).

Otro aspecto muy importante de las redes es la tecnología de red que se usa para crear una LAN. Las tecnologías más utilizadas son Ethernet, Token Ring y FDDI. Ethernet; que es la que más predomina hoy en día, actualmente utiliza una topología de estrella, un cable par trenzado, maneja velocidades hasta de 10 Mbps y es

conocida como 10BaseT. En esta tecnología cada computadora escucha el tráfico que circula por el medio común de transmisión y espera su turno para enviar información, si dos computadoras llegaran a enviar información al mismo tiempo se crearía un conflicto conocido como colisión y se volvería a retransmitir la información. Ethernet usa el algoritmo de Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD: Carrier Sense Múltiple Acces Collission Detection) para escuchar el tráfico, detectar colisiones y abortar transmisiones. La necesidad de mayores velocidades en Ethernet dio origen a Fast Ethernet, también conocida como 100Base-T, se encuentra disponible usando los mismos medios y topología que Ethernet, pero se usan diferentes tarjetas de interfaz de red para alcanzar velocidades de hasta 100 Mbps y es full duplex (puede enviar y recibir paquetes al mismo tiempo). Giga Ethernet también conocida como 1000BaseT es otra innovación de Ethernet y maneja velocidades de hasta 1000 Mbps. Token Ring es otra tecnología y fue creada por IBM, es más cara que Ethernet y maneja velocidades de 4, 16 y 100 Mbps. (Shaughnessy, 2000, p. 40). Una red Token Ring trabaja de la siguiente manera: se trasmite un conjunto de datos que incluye una dirección a cada nodo de la red varias veces por segundo, dicho conjunto de datos se nombra token. Cuando el token no se está utilizando, una computadora puede copiar la información en el token y colocar la dirección de destino, y se envía el token para que continúe alrededor del anillo. Cada computadora en el camino lee la dirección hasta que el token llega a la computadora destino. La computadora receptora copia entonces el contenido de la ficha y vuelve a fijar el estatus del token como vacío. Las redes Token Ring tienen la ventaja de que los datos viajan a través del anillo en una dirección

controlada, y no es necesario un esquema complejo como CSMA/CD, aunque tiene la desventaja de que el hardware no es barato. (Stallings, 2004, p. 128).

Las tecnologías Ethernet, Token Ring e Interfaz de datos distribuidos por fibra (FDDI) trabajan con la conmutación de paquetes, las cuales a la hora de transmitir información de una computadora a otra, la dividen en pequeños grupos conocidos como paquetes. (Zacker, 2002, p. 5). Un paquete contiene un encabezado, la carga y los elementos de control. La carga es realmente la información que se está enviando, el encabezado contiene información tanto de la computadora que envía la información como la computadora que la debe recibir, entre otros datos importantes. (Keiser, 2002, p. 240).

Las computadoras requieren un conjunto de normas para poder comunicarse unas con otras, donde cada paso de la comunicación así como los formatos para enviar y recibir información deben estar bien definidos. Dichas normas o conjunto de normas que pueden ser velocidad de transmisión, tipo de información, formato de los mensajes, etc., se conocen como protocolos. Nunca se podrá realizar una correcta comunicación si no se siguen estrictamente las reglas del protocolo. (Molina, 2006, p.18). Si dos LAN utilizan los mismos protocolos, entonces podrán comunicarse fácilmente. (Norton, 2000, p. 256).

En los inicios de las redes existían productos de red de diferentes fabricantes, donde cada fabricante no tomaba en cuenta a los otros para crear sus productos; utilizaban

sus propias normas de diseño y funcionamiento (protocolos), ocasionando que a la hora de tener que comunicar estas redes surgieran problemas de incompatibilidad. A partir de ese momento surgió la necesidad de definir un conjunto de normas estandarizado que permitiera coordinar a todos los fabricantes y proveedores. Fue por esta razón que surgieron organizaciones que crearon estándares de protocolos de red. (Zacker, 2002, p. 11).

Actualmente la mayoría de los protocolos utilizados están estandarizados, lo cual permite que productos de diferentes fabricantes puedan trabajar juntos. Zacker (2002) menciona tres organizaciones muy importantes, las cuales crearon estándares de protocolos de red y se muestran a continuación en la Tabla 2.

Tabla 2: Tres organizaciones que crearon estándares de protocolos de red.

Instituto de ingenieros eléctricos y electrónicos (Institute of Electrical and Electronics Engineers, IEEE). Creó los estándares que definen los protocolos conocidos como Ethernet y Token Ring, así como muchos otros.
Grupo de Trabajo en Ingeniería de Internet (Internet Engineering Task Force, IETF). Crea estándares para la tecnología de Internet, un ejemplo son los protocolos TCP/IP.
Asociación para la Industria de las Telecomunicaciones / Asociación de Industrias de Electrónica (Telecommunications Industry Association/Electronic Industry Association, TIA/EIA). Dos organismos que han creado estándares de telecomunicaciones por cable en edificios comerciales, que definen como debe instalarse el cableado para redes de datos.

En ocasiones se necesita compartir información entre dos o más LAN individuales y se requiere crear un enlace entre éstas, dicho enlace se conoce como interconexión de redes y existen varios dispositivos que lo permiten, los principales son los puentes, conmutadores y enrutadores. (Zacker, 2002, p. 9). Los puentes pueden dirigir la información; sólo cuando es requerido, desde una red hacia otra, para poderlos utilizar se requiere que las redes sean iguales, estos dispositivos examinan la información del encabezado de los paquetes y determinan si la computadora destino está dentro de la LAN donde se originó el mensaje o si está en la otra red. Los conmutadores son dispositivos que pueden leer la dirección de destino de los paquetes y enviarlos solamente al puerto al que está conectado el destino. Un enrutador es un dispositivo más complicado que almacena la información enviada de cada computadora en una LAN, clasifica la información y la envía por la ruta más apropiada hacia su destino. Envía paquetes sólo a la red que se desea, reduciendo el tráfico en toda la red, pueden conectar dos tipos de LAN diferentes pero sólo sabe cómo enviar la información a la ubicación correcta. (Zacker, 2002, p.10).

Las computadoras de una red utilizan varios protocolos conocidos como pila de protocolos, es responsabilidad de esta pila proporcionar comunicación entre los distintos dispositivos de la red. Una pila de protocolos es el conjunto de reglas que definen cómo ha de viajar la información a través de la red. Existe un modelo de referencia muy utilizado en las redes y se conoce como modelo de interconexión de sistemas abiertos (OSI), el cual clasifica la pila de protocolos en siete niveles o capas; vease figura 1, especifica el trabajo de cada capa y la forma en que se coordinan para

lograr la comunicación, permitiendo comprender como opera una red al visualizar la forma en que el tráfico de información circula a través de ella. (Zacker, 2002, p. 11). Este modelo es creado a inicios de los años 80 por los principales fabricantes de ese tiempo, con la finalidad de que los equipos de distintos fabricantes pudieran trabajar juntos. (Ariganello, 2007, p. 1). Según Ariganello (2007), el modelo OSI tiene dos funciones; las cuales se muestran en la Tabla 3 y tres ventajas; las cuales se muestran en la Tabla 4.

Tabla 3: Dos funciones del modelo OSI.

Permite comprender cómo trabajan los dispositivos en una red.
Sirve de guía para crear e implementar estándares de red, dispositivos y esquemas de red.

Tabla 4: Tres ventajas del modelo OSI.

Divide toda la operación de red en varios elementos más fáciles de comprender y manejar.
Permite a las personas enfocarse solamente en su campo de trabajo sin preocuparse por los otros.
Hace posible que los equipos de distintos fabricantes puedan trabajar juntos

El modelo OSI está formado por siete capas; como lo muestra la figura 1, donde cada capa proporciona información a la capa superior; con excepción de la capa de aplicación, y cada capa de la computadora emisora se comunica con su equivalente

en la computadora receptora. Las cuatro últimas capas son conocidas como de nivel inferior, inferiores o de medios y definen rutas para que las computadoras y los dispositivos finales puedan conectarse unos con otros y poder intercambiar datos. Las tres capas superiores son conocidas como de nivel superior, superiores, de aplicación o de host, están relacionadas con la interfaz de usuario, formatos y acceso a las aplicaciones y definen cómo han de comunicarse las aplicaciones de las computadoras y los dispositivos finales entre ellos y con los usuarios. (Ariganello, 2007, p. 2). Este modelo muestra cómo se transmite la información entre dos aplicaciones existentes en computadoras diferentes y conectadas en red, a través de una división de niveles. (Sánchez, 2000, p.30).

7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

Figura 1.- Capas del modelo de referencia OSI.

Existe todo un proceso para enviar y recibir datos a través de las redes, donde las pilas de protocolos del modelo OSI segmentan la información y utilizan en la parte del emisor un método de encapsulamiento y en la parte del receptor un método de desencapsulación. En el emisor cada capa agrega una cabecera e información final a

los datos, los encapsula y los baja a la siguiente capa, toda esta información viaja a través de la red y al llegar al receptor cada capa correspondiente realiza el proceso inverso, desencapsula la información recibida, quita toda la información agregada por la capa correspondiente en el emisor y la sube a la capa superior. A la información encapsulada manejada en la capa de red se le conoce como paquete y a la cabecera agregada se le conoce como cabecera IP, la cual es la dirección lógica del paquete. A la información encapsulada manejada en la capa de enlace de datos se le conoce como trama y a la cabecera agregada se le conoce como cabecera MAC, la cual es la dirección física del paquete. Cada dispositivo en una red opera en una capa diferente del modelo OSI y utiliza este proceso para realizar la comunicación entre sus capas correspondientes. (Ariganello, 2007, p. 4).

A continuación se desglosan las capas y su funcionamiento: La capa física determina toda la parte física de la red, define principalmente el tipo de medio de comunicación, tipos de conectores usados para conectar dispositivos al medio, tipos de señalización, tasas de transferencia de datos y distancias máximas de transmisión. Según Ariganello (2007), esta capa trabaja con varios estándares, los más comunes se muestran en la Tabla 5. (Ariganello, 2007, p. 6).

Tabla 5: Estándares más comunes de la capa física.

ESTÁNDAR	DESCRIPCIÓN
10Base2	Conocido como Fino. Permite segmentos de red de hasta 185 metros sobre cable coaxial para interconectar dispositivos

10Base5	Conocido como Grueso. Permite segmentos de red de hasta 500 metros sobre grandes cables coaxiales con dispositivos en el cable para recibir señales
10BaseT.	Transporta señales Ethernet hasta 100 metros de distancia en cable de par trenzado económico hasta un dispositivo centralizado denominado concentrador (hub) o conmutador (switch).
100BaseT	Transporta señales Ethernet hasta 100 metros de distancia en cable de par trenzado económico hasta un dispositivo centralizado
1000BaseT	Transporta señales Ethernet hasta 100 metros de distancia en cable de par trenzado económico hasta un dispositivo centralizado
10BaseFB	Transporta señales Ethernet hasta 100 metros de distancia en cable de fibre óptica económico hasta un dispositivo centralizado.

Los dispositivos que se manejan en esta capa sólo retransmiten los datos sin manipulación alguna. Dos ejemplos son el repetidor y el hub o concentrador.

En la tecnología Ethernet los dispositivos que están conectados a un mismo medio físico reciben todas las señales enviadas a través del medio de comunicación (usualmente por cable) por otros dispositivos. Si dos dispositivos envían una señal al mismo tiempo se producirá una colisión entre ambas, por lo cual, la estructura Ethernet dispone de reglas que permiten que sólo un dispositivo tenga acceso al medio en un momento dado. También maneja el protocolo acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD), el cual es un medio de detectar y corregir colisiones dentro de un determinado segmento. Este protocolo permite que varios dispositivos pueden tener acceso al medio de comunicación y que,

para que un dispositivo pueda acceder a él, deberá “escuchar” (detectar la portadora) para asegurarse que ningún otro dispositivo esté utilizando el mismo medio. Entre más estaciones haya en un segmento de Ethernet, mayor es la probabilidad de que tenga lugar una colisión y las colisiones excesivas son la razón principal por la cual las redes se segmentan en dominios de colisión más pequeños, mediante el uso de conmutadores (switches) y puentes (bridges). Según Ariganello (2007), para el diseño de una red es muy importante comprender los dos conceptos de dominio existentes, los cuales se explican en la Tabla 6. (Ariganello, 2007, p. 13).

Tabla 6: Dos tipos de dominios existentes en las redes.

DOMINIOS	DESCRIPCIÓN
Dominio de colisión	Conjunto de dispositivos unidos al mismo medio de comunicación, donde se provocará una colisión entre señales si dos dispositivos las envían por el medio de comunicación al mismo tiempo.
Dominio de difusión	Es un conjunto de dispositivos de red que envían y reciben mensajes de difusión entre ellos.

En esta capa se manejan estándares de cableado estructurado que detallan como debe organizarse la instalación del cableado de comunicaciones en edificios. Especifica el tipo de cable a utilizar, conectores, longitudes máximas de los tramos, organización de los elementos de interconexión, etc.. Molina (2006) menciona que existen tres estándares internacionales de cableado estructurado, los cuales se muestran en la Tabla 7.

Tabla 7: Tres estándares internacionales de cableado estructurado.

ESTÁNDAR	DESCRIPCIÓN
ISO/IEC 11801	Estándar a nivel internacional.
EN-50173	Norma europea basada en la anterior.
ANSI/EIA/TIA-568	Norma utilizada en Estados Unidos.

El estándar ANSI/EIA/TIA-568 está dividido en varios boletines técnicos que establecen los elementos de transmisión. (Molina, 2006, p. 441)

Para conectar todas las estaciones de la red, se utilizan los armarios de comunicaciones. Estos contienen los concentradores de cableado, conmutadores, puentes y encaminadores, aunque no se conectan directamente al cable de cada estación, sino que se sigue un conjunto de normas. Véase apéndice D. (Molina, 2006, p. 448)

En la capa de enlace de datos se especifica la información de los paquetes acerca de dónde ir y que debe hacer al llegar a su destino. Es la primera capa lógica del modelo OSI y maneja una dirección física de los dispositivos de la red, la cual es única para cada dispositivo y viene asignada a cada tarjeta de red (NIC, Network Access Card). (Ariganello, 2007, p. 13).

Según Ariganello (2007), la capa de enlace de datos está definida mediante dos subcapas, las cuales se muestran en la Tabla 8.

Tabla 8: Subcapas de la capa de enlace de datos del modelo OSI.

SUBCAPA	DESCRIPCIÓN
control de acceso al medio (MAC) (802.3)	La subcapa de control de acceso al medio es la responsable de determinar cómo han de ser transportados los datos a través del medio de transmisión. Sus funciones principales son: direccionamiento físico, topología de la red, disciplina de la línea, notificación de errores, distribución ordenada de tramas u control óptimo de flujo.
control de enlace lógico (LLC) (802.2).	Realiza la identificación lógica de los distintos tipos de protocolos y el encapsulado posterior de los mismos para ser transmitidos a través de la red.

Los puentes y los conmutadores (switches) capa 2 son dispositivos que funcionan en la capa de enlace de datos de la pila de protocolos. Estos dispositivos permiten dividir la red en segmentos, que a su vez son dominios de colisión. Cada puerto de un conmutador maneja un segmento de red diferente, por lo cual, la colisión producida en un segmento determinado no afecta al resto de los segmentos conectados al conmutador. Un conmutador capa 2 puede tener varios dominios de colisión pero sólo podrá tener un dominio de difusión. (Ariganello, 2007, p. 14).

Los conmutadores capa 2 almacenan en una memoria las direcciones físicas de los dispositivos pertenecientes a un segmento de red, cuando detectan una trama en la red, examinan la dirección de destino para determinar si han de filtrar, inundar o

copiar la trama en otro segmento, y se controla mediante hardware. Según Ariganello (2007), este proceso de decisión tiene lugar como se indica a continuación:

- Si el dispositivo de destino está en el mismo segmento que la trama, el conmutador bloquea el paso de la trama a otro segmento. Este proceso se conoce como filtrado.
- Si el dispositivo de destino se encuentra en un segmento diferente, el conmutador envía la trama a dicho segmento.
- Si la dirección de destino es desconocida para el conmutador, éste envía la trama a todos los segmentos excepto a aquel de donde se ha recibido la información. Este proceso se denomina inundación.

Debido a que el conmutador aprende todos los dispositivos finales a partir de las direcciones de origen, nunca aprenderá la dirección de difusión. Por tanto, todas las difusiones serán inundadas a todos los segmentos del puente o conmutador. En consecuencia, todos los segmentos de un entorno basado en puentes o conmutadores se consideran residentes en el mismo dominio de difusión. (Ariganello, 2007, p. 14).

La finalidad del dispositivo de Capa 2 es reducir las colisiones al asignar a cada segmento su propio dominio de colisión. Cuando hay dos o más paquetes que necesitan entrar en un segmento, quedan almacenados en memoria hasta que el segmento esté disponible. (Ariganello, 2007, p. 14).

Según Ariganello (2007), las redes conmutadas poseen las características especificadas en la Tabla 9.

Tabla 9: Características de las redes conmutadas.

CARACTERÍSTICAS
Cada segmento posee su propio dominio de colisión.
Todos los dispositivos conectados al mismo puente o conmutador pertenecen al mismo dominio de difusión.
Todos los segmentos deben utilizar la misma tecnología (Ethernet, Token Ring, etc).
Puede haber un dispositivo por cada segmento, y todos los dispositivos pueden enviar información al mismo tiempo.

Los conmutadores sólo permiten interconectar LAN que utilizan los mismos protocolos y su principal función consiste en segmentar una red en diferentes dominios de colisión para aumentar su rendimiento. El conmutador segmenta el tráfico de manera que los paquetes destinados a un dominio de colisión determinado, no se propague a otro segmento (Ariganello, 2007, p.134). Sólo retransmite la trama al puerto específico al que va dirigida, preservando el ancho de banda del resto de los enlaces. (Molina, 2006, p. 183). Enviar una trama a todos los puertos conectados se denomina “inundar” la trama. Las tramas de difusión y multidifusión constituyen un caso especial, un conmutador nunca aprende direcciones de difusión o multidifusión, dado que las direcciones no aparecen en estos casos como dirección de origen de la trama. Otra función del conmutador es evitar bucles. Las redes están diseñadas por lo general con enlaces y dispositivos redundantes, sin algún servicio de evitación de bucles implementado, cada conmutador inundaría las difusiones en un bucle infinito.

Esta situación se conoce como bucle de puente. La propagación continua de estas difusiones a través del bucle produce una tormenta de difusión, lo que da como resultado un desperdicio del ancho de banda, así como impactos serios en el rendimiento de la red. (Ariganello, 2007, p.134)

Un conmutador consiste en un gran número de puertos que conectan segmentos de red local (Ethernet y Token Ring) y puertos de alta velocidad (100 Mbps Fast Ethernet o FDDI) a otros dispositivos de la red y permite la asignación de menos usuarios por segmento, incrementando el promedio de ancho de banda disponible por usuario. Es posible la creación de un segmento por dispositivo, obteniendo éste todo el ancho de banda de 10 Mbps, además de que se eliminan por completo las colisiones, ya que es un solo dispositivo el que existe en el segmento. Dicho dispositivo recibe acceso instantáneo al ancho de banda asignado y no tiene que competir con el ancho de banda disponible con otros dispositivos.

El protocolo de Árbol de extensión (STP) es un protocolo de tipo puente a puente desarrollado por DEC, revisado posteriormente por IEEE 802 y publicado en la especificación IEEE 802.1. El objetivo del árbol de extensión es mantener una red libre de bucles. El STP explora constantemente la red, de forma que cualquier fallo o adición en un enlace, conmutador o puente es detectado al instante. Cuando cambia la topología de red, el algoritmo de árbol de extensión reconfigura los puertos del conmutador para evitar una perdida total de la conectividad, o la creación proporciona una topología de red libre de bucles llevando a cabo las siguientes operaciones.

Se elige un conmutador raíz, ya que en un dominio de difusión solo puede existir un conmutador raíz. Todos los puertos del conmutador raíz se encuentran en estado de retransmisión y se denominan puertos designados. Cuando está en este estado, un puerto puede enviar y recibir tráfico. La elección de un conmutador raíz se lleva a cabo determinando el conmutador que posea la menor prioridad. Los demás conmutadores del dominio se llaman conmutadores no raíz. Para cada conmutador no raíz hay un puerto raíz. El puerto raíz corresponde a la ruta de menor costo desde el conmutador no raíz, hasta el conmutador raíz. Los puertos raíz se encuentran en estado de retransmisión y proporcionan conectividad hacia atrás al conmutador raíz. La ruta de menor costo al conmutador raíz se basa en el ancho de banda.

En cada segmento hay un puerto designado. El puerto designado se selecciona en el conmutador que posee el trayecto de menor costo hacia el conmutador raíz. Los puertos designados se encuentran en estado de retransmisión y son los responsables del reenvío de tráfico por el segmento. Los puertos no designados se encuentran normalmente en estado de bloqueo con el fin de romper la topología de bucle. Los estados del árbol de extensión son: bloqueo, escucha, aprendizaje, retransmisión. (Ariganello, 2007, p.138)

La capa de red se encarga de tomar decisiones sobre rutas (busca la óptima) y enviar paquetes a nodos que no están directamente conectados en el mismo dominio de difusión (que están en diferentes redes). Según Ariganello (2007), para conseguir esto se necesitan dos elementos de información:

- Una dirección lógica asociada a cada dispositivo de origen y de destino.
- Una ruta a través de la red para alcanzar el destino deseado.

La capa de red puede conectar medios físicos diferentes ya que usa la estructura lógica de direccionamiento (conocidas como direcciones lógicas o virtuales). El direccionamiento lógico se utiliza para identificar redes y la ubicación de los dispositivos dentro del contexto de dichas redes, independientemente de su ubicación física. A diferencia de las direcciones de la capa de enlace de datos, que suelen residir en un espacio de direcciones plano, las direcciones de la capa de red poseen habitualmente una estructura jerárquica en la cual se definen primero las redes y después los dispositivos o nodos de cada red. Esto contrasta con las direcciones de la capa MAC, de naturaleza plana donde cada dispositivo posee un número único que lo identifica. (Ariganello, 2007, p. 16).

Los enrutadores son dispositivos que operan en la capa de red, registrando y grabando las diferentes redes y eligiendo la mejor ruta para las mismas. (St-Pierre, 2005, p. 206). Según Ariganello (2007), los enrutadores colocan esta información en una tabla de enrutamiento, que incluye los siguientes elementos: dirección de red, interfase y métrica (costo o distancia para llegar a la red de destino). Estos dispositivos se utilizan para separar segmentos en dominios de colisión y de difusión únicos, donde cada segmento se conoce como una red y debe estar identificado por una dirección. El enrutador utiliza la información de configuración de la NIC para

determinar la parte de la dirección correspondiente a la red, a fin de construir una tabla de enrutamiento. (Ariganello, 2007, p. 19).

Para poder conectar dos dispositivos en la construcción de una red, es necesario establecer una conexión o sesión. La capa de transporte define las directrices de la conexión entre dos dispositivos finales. Una sesión constituye una conexión lógica entre las capas de transporte iguales en los dispositivos de origen y destino. En esta capa y en la capa de red es utilizado el modelo de referencia TCP/IP creado por el departamento de defensa de Estados Unidos para poder transmitir datos de manera confiable hacia cualquier otro dispositivo conectado en red en cualquier parte del mundo. TCP/IP maneja números de puerto que permiten la conexión de dos dispositivos en la presente capa. En la capa de transporte, los datos pueden ser transmitidos de forma fiable o no fiable, el protocolo TCP es fiable u orientado a conexión, mientras que UDP no es fiable, o independiente de la conexión. (Ariganello, 2007, p. 21). TCP/IP viene integrado en el sistema operativo de la computadora y es el conjunto de protocolos más utilizado para interconectar sistemas abiertos. Además de ser el manejado en Internet, muchas empresas lo utilizan para enlazar todas sus redes. (Comer, 2000, p. 1).

En TCP/IP el usuario nunca llega a utilizar las direcciones físicas (largas y complicadas) grabadas en las tarjetas de red, en su lugar se emplean las direcciones IP. El estándar que se utiliza para direcciones IP es el IPv4, que consta de cuatro bytes, con los que en teoría se podrían direccionar un total de 4,294,967,296 equipos.

Las direcciones IP (IPv4) se suelen expresar en la notación XXX.XXX.XXX.XXX, donde cada uno de los campos separados por puntos es un número decimal que va de 0 a 255, y que representa el byte correspondiente. Toda dirección IP se compone de dos partes:

- Porción de red, que identifica la red física donde se ubica el sistema (*netid*). La componen los *r* primeros bits de la dirección IP.
- Porción de host, que identifica al equipo o host dentro de la red (*hostid*). La componen los *h* últimos bits de la dirección IP (*r+h=32 bits de la dirección IP).*

Los dígitos empleados para *netid* y para *hostid* dependen de la clase de la red, que se determina por los primeros bits de dirección. Las clases A, B y C son estándares para diálogos entre origen y destino, mientras que la clase D se emplea para el envío simultáneo a muchos destinos. La mayor ventaja de TCP/IP es que permite la comunicación entre computadoras de diferentes fabricantes y distintos sistemas operativos que se encuentren en una red. (Raya, 2003, p. 75).

El número de direcciones que se pueden manejar con IPv4 ya no son suficientes para direccionar todos los equipos del planeta; por lo cual, surge una IP de nueva generación: IPv6. Esta nueva IP utiliza direcciones de 128 bits, 96 bits más que una dirección IPv4. (García, 2002, p. 418).

La capa de sesión establece, administra y concluye las sesiones de comunicaciones entre entidades de la capa de presentación. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en máquinas diferentes.

La capa de presentación proporciona funciones de conversión y codificación que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que los datos enviados desde la capa de aplicación de un sistema podrán ser leídos por la capa de aplicación de otro sistema. Un ejemplo de funciones de codificación sería el cifrado de datos una vez que éstos salen de una aplicación.

La capa de aplicación. Aquí, el usuario o la aplicación se comunican con los protocolos para acceder a la red. Por ejemplo, se accede a un procesador de textos por el servicio de transferencia de archivos de esta capa. Se realiza el intercambio de datos entre el usuario y el sistema. (Vallejos, 2001, p.251).

2.2 REDES DE ÁREA LOCAL VIRTUALES (VLANs).

2.2.1 DEFINICIÓN Y CARACTERÍSTICAS DE LAS VLANs

Sackett (2002) define la VLAN como “una agrupación lógica de dispositivos dentro de una red física” y comenta que dicha agrupación tiene la finalidad de segmentar la red. Forouzan (2003) la define como “una subred o un segmento de una LAN configurada

por software, no por cables físicos". Véase la Figura 2. Ariganello (2007) concuerda con Sackett (2002) y comenta que las VLANs permiten agrupar usuarios de un dominio de difusión común, con independencia de su ubicación física en la red. Usando la tecnología VLAN se pueden agrupar lógicamente puertos del conmutador y los usuarios conectados a ellos en comunidades de interés común, como grupos de trabajo. Las VLAN se crean mediante el empleo de conmutadores y pueden existir en uno solo o bien abarcar varios de ellos, su función es proveer seguridad, segmentación, flexibilidad y mejorar el rendimiento de la red. (Ariganello, 2007, p.144).

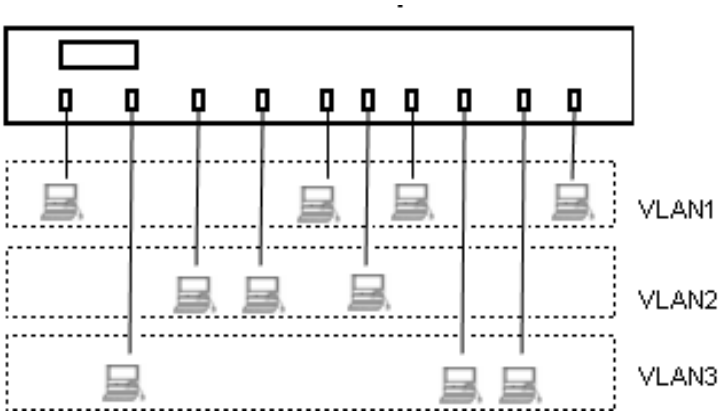


Figura 2.- Conmutador con VLANs implementadas mediante software.

Según Ariganello (2007), las características básicas de configuración de una VLAN son las que se muestran en la Tabla 10.

Tabla 10: Características básicas de configuración de una VLAN.

CARACTERÍSTICAS

Cada VLAN lógica es como un puente físico independiente; por lo tanto, la información solo podrá entrar o salir de la VLAN cuando sea requerido.
Las VLAN pueden extenderse a múltiples conmutadores.
Enlaces troncales se encargan de transportar tráfico por múltiples VLAN.

Véase el apéndice C para conocer las pantallas de configuración de un conmutador Allied Telesis At-8000S Series.

Hill (2003) y Sackett (2002) concuerdan en las ventajas básicas de una VLAN, las cuales se muestran en la Tabla 11.

Tabla 11: Ventajas básicas de una VLAN.

VENTAJA	**DESCIPCIÓN**
Segmentación	Se pueden realizar agrupaciones lógicas de usuarios distantes que pueden estar en segmentos físicos diferentes o muy grandes.
Seguridad	Las VLANs permiten que la información fluya solamente dentro de dicho grupo lógico y a pesar de que los datos pasan por varios dispositivos nadie ajeno a dicho grupo los puede accesar.
Rendimiento	La información enviada entre los integrantes del grupo lógico no se propaga a las otras VLANs y viceversa, por lo tanto, se mejora el rendimiento al controlar la propagación de la difusión (el envío de paquetes o mensajes) ya que no se satura el ancho de banda de toda la red.
Flexibilidad	Permite que los movimientos físicos de equipos de cómputo se realicen de forma rápida, económica y sin tener alterar la infraestructura existente de la red de datos

Hill (2003) escribe sobre el VLAN trunking protocol (VTP) o el protocolo de compartición para VLAN, el cual permite administrar las VLANs asignando definiciones VLAN a múltiples conmutadores de una red. El VTP se utiliza para configurar un conmutador independiente y propagarlo por toda la red, manteniendo una configuración de VLAN coherente a través de toda la red conmutada. VTP difunde la definición de las VLANs, no los miembros de dichas redes. Es un protocolo de mensajería de capa 2 que mantiene la coherencia de la configuración VLAN a través de un dominio de administración común, gestionando las adiciones, supresiones y cambios de nombre de las VLAN a través de las redes. Un dominio VTP es un conmutador o varios conmutadores interconectados que comparten un mismo entorno VTP. Cada conmutador se configura para residir en un único dominio VTP. La información VTP se propaga sólo a través de enlaces de compartición (trunking). VTP opera en uno de estos tres modos: modo servidor, modo cliente o modo transparente. El modo predeterminado es el modo servidor. En modo servidor puedes crear, modificar y suprimir VLAN y otros parámetros de configuración que afectan a todo el dominio VTP, además, las configuraciones de VLAN se guardan en la memoria de acceso aleatoria no volátil (NVRAM). En cambio, un dispositivo que opera en modo VTP cliente no puede crear, cambiar ni suprimir VLAN, sólo escucha y propaga los mensajes de VTP sobre su dominio de gestión. Un cliente VTP no guarda la configuración VLAN en memoria no volátil. Tanto en modo cliente como en modo servidor, los conmutadores sincronizan su configuración VLAN con la del conmutador que tenga el número de revisión más alto en el dominio VTP. (Ariganello, 2007, p.147)

Algunas recomendaciones para el uso de los modos antes mencionados son las siguientes: Si la VLAN va ha añadirse únicamente a un conmutador local, utilice el modo transparente, pero si se desea propagar las VLAN a otros conmutadores del dominio, utilice el modo servidor. Un conmutador se encuentra por omisión en estado VTP servidor, de modo que pueda añadirse, modificarse o suprimirse VLAN. La pertenencia de los puertos de conmutador a las VLAN se asigna manualmente puerto a puerto (pertenencia VLAN estática o basada en puertos). Cada vez que crea una VLAN puede asignar estáticamente un puerto o un número de puertos a la VLAN, donde un puerto puede pertenecer a una sola VLAN. Todos los puertos pertenecen por omisión a la VLAN predeterminada, VLAN1. (Ariganello, 2007, p.150)

En un entorno de VLAN conmutada, los paquetes se conmutan (envían o dirigen) sólo entre puertos designados para residir en el mismo “dominio de difusión”. Las VLAN llevan a cabo particiones en la red y separación de tráfico en la capa 2; por tanto, la comunicación entre VLAN no puede tener lugar sin un dispositivo de capa 3, como un enrutador o un conmutador capa 3, responsable de establecer comunicaciones entre distintos dominios de difusión, o lo que es lo mismo, entre distintas VLANs. (Sackett, 2002, p.116).

Según Ariganello (2007), para llevar a cabo funciones de enrutamiento entre VLAN, han de darse las siguientes circunstancias:

- El enrutador debe conocer como llegar a todas las VLAN interconectadas para determinar cuales son los dispositivos finales, incluidas las redes que están conectadas a la VLAN, cada dispositivo final debe estar direccionado con una dirección de capa de red, como la dirección IP.

- Cada enrutador debe conocer además la ruta hasta cada red LAN de destino.

- El enrutador tiene ya información acerca de las redes que están conectadas directamente. Por tanto, deberá aprender las rutas a las redes que no están conectadas directamente.

- Debe existir una conexión física en el enrutador para cada VLAN, o bien se debe habilitar la troncalidad en una conexión física individual.

Antes de la existencia de las VLAN y los conmutadores la segmentación de dominios de difusión la realizaban los enrutadores, los cuales son más costosos que los conmutadores. (Hill, 2003, p.528).

Según Hill (2003) existe un proceso que permite identificar las tramas (conjuntos de datos) como miembros de una VLAN, el cual se conoce como etiquetado de VLAN. Dicho etiquetado permite que dispositivos como los conmutadores y enrutadores puedan identificar la VLAN en la que se origino la trama. El etiquetado hace posible el enviar tramas desde muchas VLANs sobre el mismo puerto físico, proceso conocido como compartición (trunking). El protocolo IEEE 802.1Q es un método de etiquetado de tramas que permite la interoperatividad entre equipos de diferentes fabricantes. Según Garg (2005) este estándar define un espacio de direcciones de sólo 4096 etiquetas disponibles. Este protocolo establece un nuevo formato para el encabezado Ethernet (802.3), al cual sólo se le agrega una etiqueta VLAN que es utilizada por los dispositivos de interconexión (como los conmutadores). (Tanenbaum, 2003, p.333).

Como se ha dicho anteriormente, antes de la aparición de las VLAN, la única forma de controlar el tráfico de difusión era a través de la segmentación basada en encaminadores. Las VLAN son una extensión de la red conmutada. Contando con la posibilidad de colocar segmentos (puertos) en dominios de difusión individuales, se puede controlar donde será retransmitida cada difusión. Básicamente, cada conmutador actúa independientemente de los demás conmutadores de la red. Con el concepto de VLAN, se crea un cierto nivel de interdependencia en el entramado de conmutadores.

En este nuevo escenario, cada conmutador puede distinguir tráfico de diferentes dominios de difusión. Cada decisión de retransmisión se basa en que la VLAN actúa como un puente individual dentro de un conmutador. Para poder realizar el puenteado/conmutación entre conmutadores, es necesario conectar cada VLAN independientemente (es decir, dedicar un puerto a cada VLAN), o bien disponer de algún método de mantenimiento y retransmisión de información de la VLAN junto con los paquetes. El proceso, denominado trunking, es el que permite realizar este tipo de conexión simple.

Normalmente, un puerto transporta trafico solo para la VLAN a la que pertenece para que una VLAN pueda alcanzar múltiples conmutadores en una sola conexión, se requiere un enlace troncal. El enlace troncal se encarga de llevar el trafico por todas

las VLAN, un puerto de enlace troncal solamente puede ser configurado en los puertos fast Ethernet.

Las VLAN son una implementación en la capa 2 del entramado de conmutadores de la red. Debido a que están implementadas en la capa de enlace de datos, son independientes del protocolo. Para colocar un puerto (segmento) dado en una VLAN, es necesario asignar dicha pertenencia (ser miembro de una VLAN) en el conmutador. Según Hill (2003) la pertenencia a una VLAN se puede definir de manera estática o dinámica. La estática se basa en el puerto del conmutador al que está conectado el dispositivo y es el método más sencillo y habitual para configurar la pertenencia a una VLAN. La dinámica se basa en las direcciones MAC del dispositivo y su configuración es más complicada, pero permite desplazar equipos (como servidores) según se desee y que la pertenencia les siga (para mucho desplazamiento de empleados o portátiles). Una vez definido un puerto (asignada la pertenencia) para una VLAN dada, el tráfico que parte de ese segmento será retransmitido por los conmutadores solo a los puertos de la misma VLAN. Si se necesita establecer comunicación entre VLAN, es necesario añadir un encaminador y un protocolo de capa 3 a la red. (Komarek, 2007, p.43).

Cuando existen enlaces redundantes, dentro de la red, se hace necesario activar el protocolo de árbol de expansión (STP). Dicho protocolo determina donde se encuentran los enlaces redundantes (automáticamente) y bloquea el tráfico de datos de los puertos hasta que falla el enlace primario. STP determina cual es el mejor

camino a través de la red y envía el tráfico de datos sólo a través de ese camino. (Hill, 2003, p.508).

2.2.2 Procedimiento para crear y configurar VLANs en un conmutador Ethernet capa 2 marca Allied Telesis de la serie AT-8000S.

Combinando las VLANs y el protocolo de registro de atributo genérico (GARP) permite a los encargados de redes definir nodos de red en dominios de difusión.

Al configurar VLANs se debe tomar en cuenta lo siguiente:

- Al usar esta característica, la administración de VLAN debe existir en cada dispositivo de la serie AT-8000S que se desee administrar.
- Los puertos uplink y downlink en cada dispositivo que funcionan como los enlaces de datos etiquetados o no etiquetados entre los dispositivos deben ser ya sea miembros etiquetados o no etiquetados de la VLAN administrada.
- El puerto en el dispositivo con el cual la estación de administración está conectada, debe ser un miembro de la VLAN administrada.

Para configurar el switch, primero debemos accesar sus páginas de configuración, para lo cual, existen diferentes caminos, uno de los cuales es el siguiente: se debe conectar una computadora vía cable de red a un puerto del switch que se desea configurar, una vez conectados físicamente, se puede accesar al switch vía software, para lo cual se utiliza un navegador de internet como lo es el internet explorer, en el navegador se proporciona la dirección IP del switch y se entabla la conexión lógica. A

continuación se escriben los pasos necesarios para configurar una VLAN dentro del switch:

1.- Realizar un clic sobre la opción Layer 2 (capa 2) > VLAN. La página de VLAN proporciona la información y los parámetros globales para configurar y trabajar con VLANs. La página de VLAN se abre:

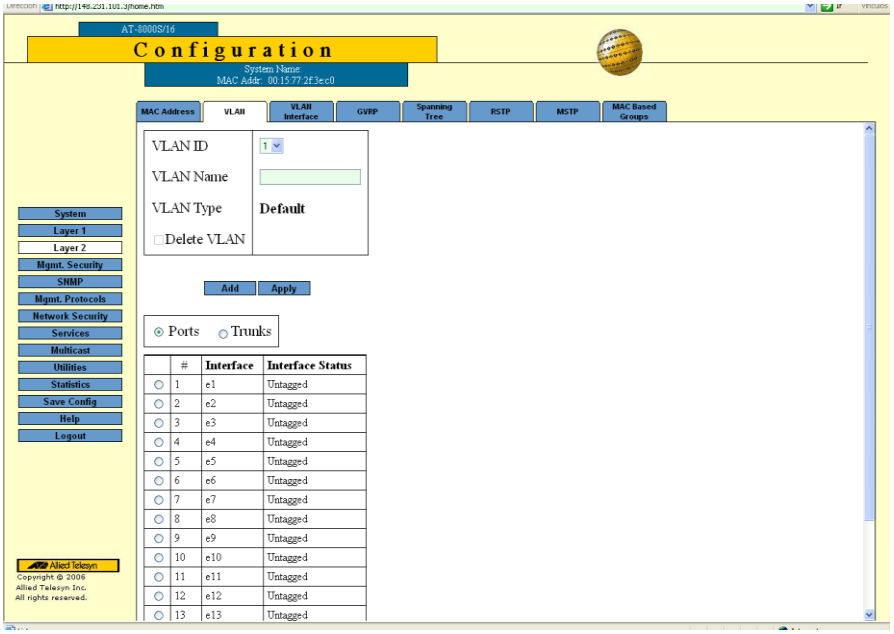


Figura 3: Página de VLAN.

La página de VLAN se divide en dos secciones. La primera sección contiene los siguientes campos:

- VLAN ID: Define la identificación de la VLAN. Las identificaciones posibles de la VLAN son de 1 a 4095, en el cual “1” es reservado para la VLAN por defecto, y se reserva el “4095” como la “discard” VLAN.
- VLAN Name: Exhibe el nombre definido por el usuario para la VLAN.
- VLAN Type: Exhibe el tipo de VLAN. Los posibles valores del campo son:

--- Dynamic--- Indica que la VLAN fue creada dinámicamente a través de GARP.

--- Static--- Indica que la VLAN es definida por el usuario.

--- Dufault--- Indica que la VLAN es la VLAN por defecto.

- Delete VLAN--- Remueve las especificaciones de una VLAN. Los valores posibles del campo son:

--- Checked--- Borra la VLAN especificada.

--- Unchecked--- Mantiene la VLAN especificada.

La segunda sección contiene una tabla que mapea los parámetros de la VLAN a

los puertos.

- Seleccione las interfaces mostradas en la tabla.

--- Ports of Unit--- Especifica el puerto y el miembro stacking para el cual el mapeo de la VLAN es exhibido.

--- Trunk--- Específica el trunk para el cual el mapeo de la VLAN es exhibido.

- Interface status--- Indica el estado de los miembros de la interface en la VLAN. Los posibles valores del campo son:
-

--- Tagged--- Indica que la interfaz es un miembro etiquetado de una VLAN. Todos los paquetes expedidos por la interfaz, son etiquetados. Los paquetes contienen la información de la VLAN.

--- Untagged--- Indica que la interfaz es un miembro de la VLAN no etiquetado. Los paquetes expedidos por la interfaz son no etiquetados. En la VLAN por defecto, este es el valor por defecto para todas las interfaces.

--- Excluded--- indica que el Puerto es excluido de la VLAN.

--- Forbidden--- indica que el Puerto no puede ser incluido en la VLAN.

2. Clic en el botón “Add” (agregar). Aparecerá la siguiente ventana para agregar una VLAN.

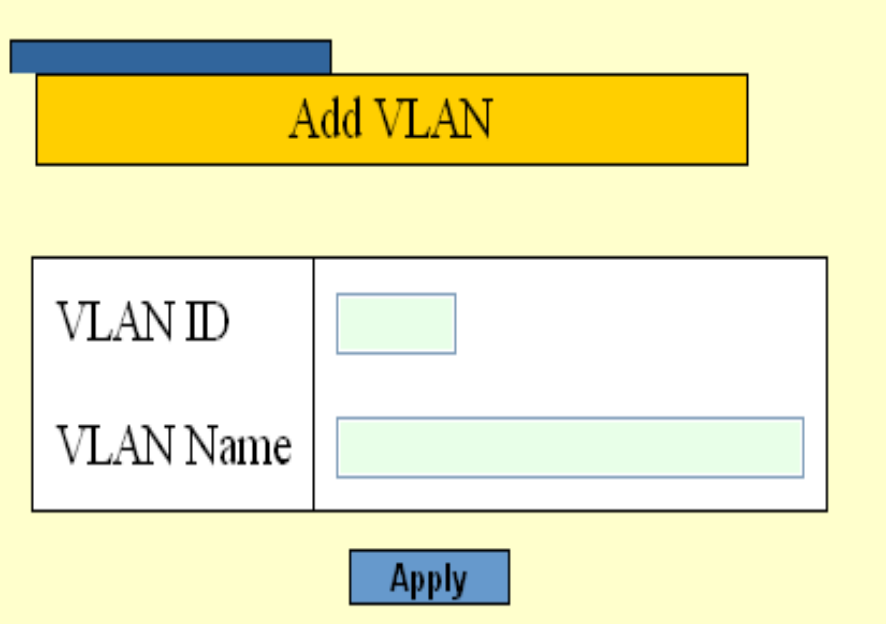


Figura 4: Página para agregar una VLAN.

3. Definir los campos.

4. Clic en “Apply” (aplicar). La VLAN es creada y el dispositivo es actualizado.

Para modificar la configuración de una VLAN:

1. Click en layer 2 > VLAN. Se abre la ventana de VLAN.
2. Seleccionar una VLAN desde la tabla.
3. Clic en Modify (modificar). La ventana de configuración de la VLAN es desplegada.
4. Cambiar la configuración de la “Interface Status”.

5. Clic en Apply (aplicar). La configuración de la VLAN es modificada y el dispositivo es actualizado.

6. Clic en “Save Config” (guardar configuración) en el menú para guardar el cambio permanentemente.

Definiendo los parámetros de la interface VLAN.

La página de la interface VLAN contiene campos para administrar los puertos que son parte de la VLAN. Para definir una interfase de VLAN:

1.- Clic en Layer 2 > VLAN interface. Se abre la ventana de la interfase VLAN:

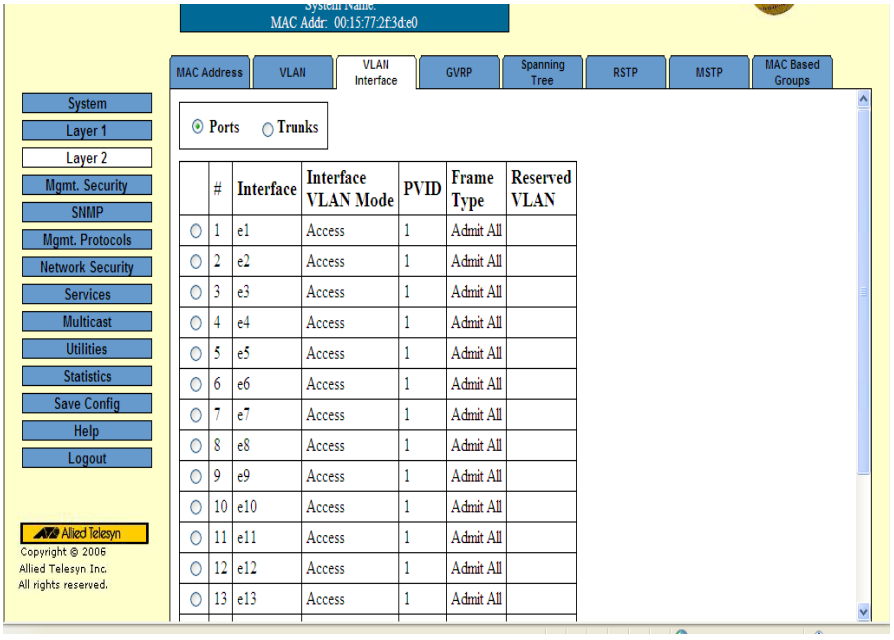


Figura 5: Página de la interfase de VLAN

La página de “VLAN Interface” muestra la información de la interfase VLAN para un puerto/unidad seleccionado o trunk.

- Selecciona la interfase mostrada en la tabla.

  - Ports of unit--especifica el puerto y el miembro de stacking para el cual el mapeo de VLAN es desplegado.

  - Trunk--especifica el trunk para el cual el mapeo de VLAN es desplegado.

- Interface--muestra el número de trunk o el puerto.

- Interface VLAN mode--indica el estado de pertenencia de la interfase en la VLAN. los valores posibles son:

  - General--indica que el puerto pertenece a VLANs, y cada interfase de VLAN es definida por el usuario como etiquetado o no etiquetado (modo IEEE802.1Q completo).

  - Access – Indica que un puerto pertenece a una sola VLAN no etiquetada. Cuando un puerto está en modo Access, los tipos de paquete que son aceptados en el puerto no pueden ser designados. El ingreso de filtrado siempre está habilitado para puertos en modo Access.

  - Trunk--indica que el puerto pertenece a VLANS en las cuales todas las VLANS son etiquetadas, excepto por una VLAN que es no etiquetada.

- PVID— Port Default VLAN ID. Asigna una identificación de VLAN a paquetes no etiquetados. los valores posibles son 1-4094. VLAN 4095 es definida según el estándar y la práctica de industria como la VLAN de descarte.

- Frame type--especifica el tipo de paquete aceptado por el puerto. Los posibles valores de campo son:

  - Admit tag only—sólo paquetes etiquetados son aceptados en el puerto.

  - Admit all— etiquetados y no etiquetados son aceptados en el puerto.

- Ingress filtering-- indica si la filtración de ingreso es permitida sobre el puerto. Los valores posibles son:

  - Enable--permite el ingreso de lo filtrado en el dispositivo. Ingresa paquetes descartados en la filtración que se definieron para VLANs de las cuales el puerto específico no es un miembro.

  --- Disabled--- inhabilita el ingreso de lo filtrado en el dispositivo.

- Reserved VLAN --- indica la VLAN que es reservada actualmente para el uso interno por el sistema.

1. seleccione una interfase de la tabla
2. clic en Modify (modificar). Se abre la página de configuración de interfase de VLAN:

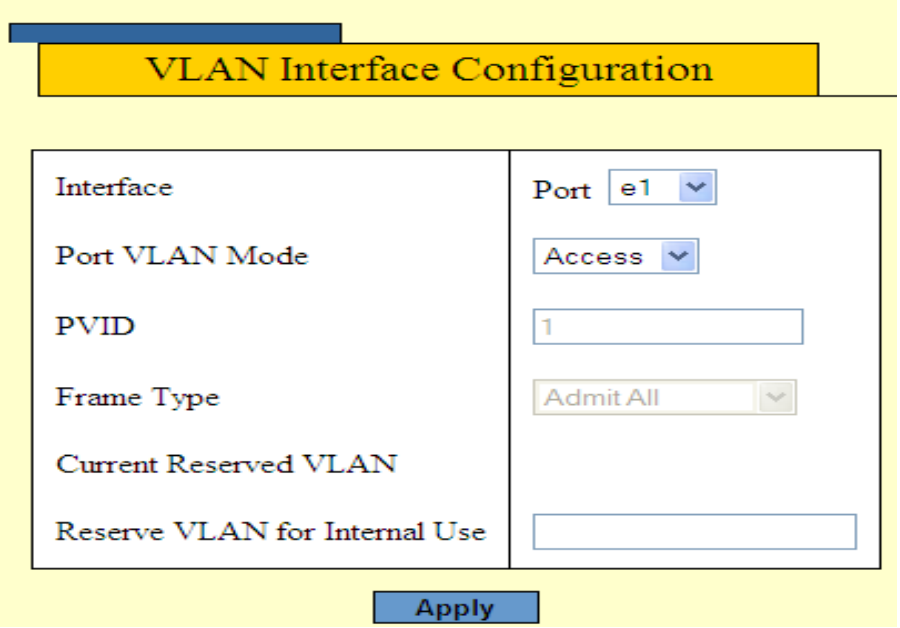


Figura 6: Página de programación de la interfase de VLAN

Además de la página de la interfase de VLAN, la página de configuración de la interfase de VLAN contiene los siguientes campos:

- Reserve VLAN for internal use--- indica qué VLAN es reservada para el uso interno por el sistema. Una VLAN debe ser reservada.

4. Defina los campos.
5. Clic Apply. la configuración de la interfase de VLAN es guardada y el dispositivo es actualizado.
6. Clic Save Config en el menú para guardar permanentemente el cambio.

Definiendo GVRP

La página de GVRP permite a usuarios configurar el protocolo de registro GARP de la VLAN en el dispositivo. GVRP se proporciona específicamente para la distribución automática de la información de pertenencia a VLAN entre puentes de VLAN-aware (enterados). GVRP permite que los puentes VLAN-enterados aprendan automáticamente VLANs evitando tener que configurar individualmente cada puente y registrar la pertenencia de VLAN. En la página de GVPR, los usuarios pueden hacer las siguientes tareas:

- configuración de GVRP
- habilitar/ deshabilitar GVRP sobre un puerto

Configuración de GVRP.

Para definir GVRP en el dispositivo:

1. Clic layer 2> GVRP. Se abre la página de GVRP:

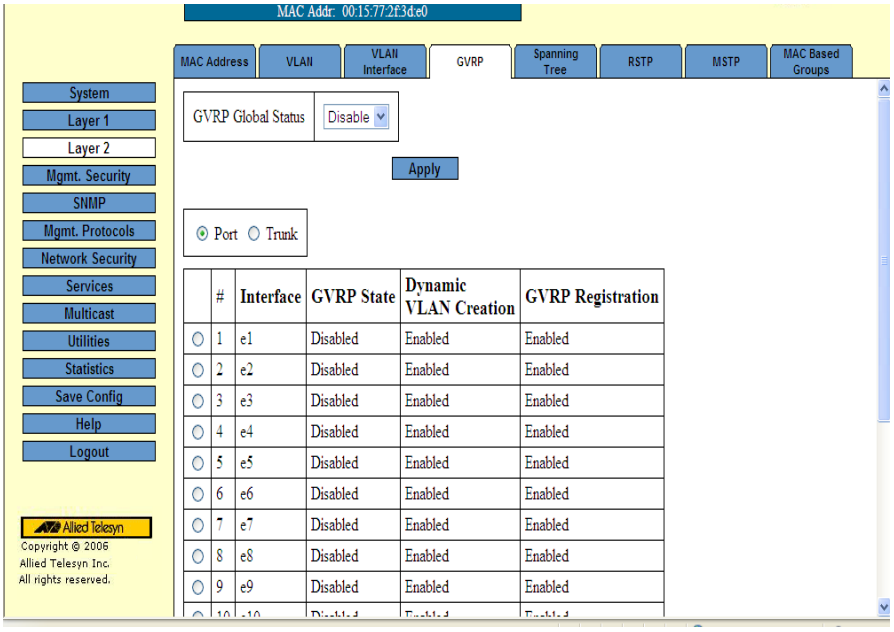


Figura 7: Primer página para configurar GVRP

La página de GVRP contiene los siguientes campos:

- GVRP Global Status (Estado global de GVRP) --- indica si GVRP está habilitado en el dispositivo. Los valores posibles del campo son:

  --- enable--- habilita GVRP en los dispositivos seleccionados.

  --- disable--- deshabilita GVRP en los dispositivos seleccionados.

- Seleccione las interfases exhibidas en la tabla.

  - Ports of Unit --- especifica el puerto y el miembro de tacking para quienes se exhibe la configuración de GVRP.

  - Trunk--- especifica el trunk para el cual se exhiben los ajustes de GVRP.

- Interface--- exhibe el puerto o el nombre del trunk en el cual GVRP está habilitado.

- GVRP State -- indica si GVRP está habilitado en el puerto. Los posibles valores del campo son:

  --- Enable -- permite GVRP en la interfase.

  --- Disable – No permite GVRP en la interfase.

- Dynamic VLAN Creation -- indica si la creación dinámica de VLAN se permite en la interfase. Los posibles valores del campo son:

  - Enable—habilita la creación de VLAN dinámica en la interfase.

  - Disable—deshabilita la creación de VLAN dinámica en la interfase.

- GVRP Registration -- indica si el registro de VLAN a través de GVRP se permite en la interfase. Los posibles valores del campo son:

  - Enable—habilita el registro de GVRP en la interfase.

  - Disable—deshabilita el registro de GVRP en la interfase.

2. Seleccione Enable GVRP.

3. Defina los parámetros de GVRP.

4. clic Apply (aplicar). Se aplican los parámetros globales de GVRP y el dispositivo es actualizado.

5. clic Save Config (guardar configuración) en el menú para guardar permanentemente el cambio.

Enabing/Disabling GVRP on a port.

Para habilitar o deshabilitar GVRP en los puertos:

1. clic Layer 2 > GVRP. Se abre la página de GVRP.

2. Seleccione un puerto en la unidad o trunk.

3. clic Modify (modificar). Se abre la página de configuración de GVRP:

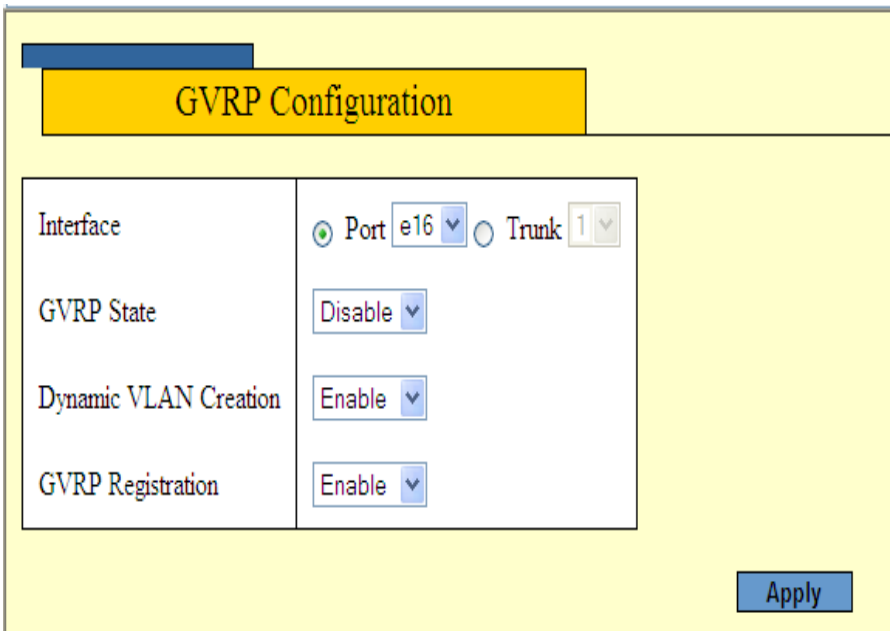


Figura 8: Segunda página de configuración GVRP

4. seleccione la interfase (puerto o trunk)

5. Defina los campos.

6. clic Apply (aplicar). El cambio al modo de GVRP se activa en la interfase seleccionada.

Definir grupos basados en MAC.

La página de grupos basados en MAC permite que los administradores de red agrupen VLANs en base en la dirección MAC de la VLAN, y para trazar grupos de protocolo a VLANs. Para estos propósitos, la página contiene dos tablas:

- Tabla de grupos basados en MAC
- Tabla de grupos trazados

Para definir grupos basados en MAC:

1. Clic Layer 2> MAC based Groups.. Se abre la página grupos basados en MAC.

La página de grupos basados en MAC contiene los siguientes campos:

MAC- Based Group

En la tabla de grupos basados en MAC, los administradores de red agrupan VLANs basadas en la dirección MAC de la VLAN.

- MAC Address--- exhibe la dirección MAC asociada al grupo VLAN.
- Prefix---exhibe el prefijo MAC asociado con el grupo MAC.
- Group ID--- exhibe la identificación de grupo de VLAN

Mapping Groups

En la tabla de grupos trazados, los encargados de red asignan grupos MAC a las interfaces.

• Interface--- indica el tipo del interfase para agregar al grupo de VLAN. Los posibles valores del campo son:

---Port (Puerto) --- indica el puerto específico agregado al grupo de VLAN.

---Trunk (Tronco)--- indica el tronco específico agregado al grupo de VLAN.

- Group ID (identificación de grupo) --- define la identificación de grupo del protocolo al cual el interfase es agregado.

- VLAN ID (identificación de VLAN) -- une la interfase a una identificación definida por el usuario de VLAN. Los puertos del grupo de VLAN se pueden unir a una identificación de VLAN. La gama posible del campo es 1-4093 y 4095 (4094 no es disponible para configuración).

2. Abajo la MAC- basada en tablas de grupos, clic el botón “ADD” (agregar). La página de agregar del grupo de direcciones de MAC se abre.

En adición a los campos en la página de MAC basado en grupos, la página de agregación de grupos de direcciones de MAC contiene los siguientes campos adicionales:

- Host- define la dirección específica de MAC como si fuera la única dirección asociada con grupos VLAN.

3. Define los campos.

4. Clic apply (aplicar). El MAC basado en grupos VLAN es definido, y el dispositivo es actualizado.

Para modificar las programaciones de MAC basado en grupos:

1. clic layer 2 (capa 2)> Mac basado en grupos. La página de MAC basado en grupos se abre.

2. clic modify (modificar). La página de grupos de direcciones de programación MAC se abre.

3. Modifica los Campos

4. Clic Apply (aplicar). El Mac basado en grupo de VLANs es modificado, y el dispositivo es la actualizado.

5. Clic Save Config (guardar configuración) en el menú para guardar los cambios permanentemente.

Para añadir un grupo trazado

1. Clic Layer 2 (capa 2)> Mac basado en grupos. La dirección MAC basada en grupos se abre.

2. Debajo de la tabla de trazado, clic el botón Add (agregar).

En adición de los campos de páginas de MAC basada en grupos, la página de dirección de grupos trazados de MAC contiene los siguientes campos adicionales:

- Group Types- indica el grupo VLANs al cual las interfaces serán trazadas. el valor posible del campo es:
    - MAC- based: indica las interfaces que son trazados por MAC basada en grupos VLANs.

3. Selecciona una VLAN para trazar el grupo

4. Selecciona Apply (aplicar). El grupo de trazado es agregado, y el dispositivo es actualizado.

Para modificar la programación de grupos trazados:

1. Clic Layer2 (capa 2)>La página de MAC basada en grupos se abre:

2. Clic Modify (modificar). La página de programación del grupo de direcciones trazadas de MAC se abre.

3. Cambia el trazado de VLAN (Identificación de VLAN)

4. Clic Apply (aplicación). El grupo de trazado es modificado, y el dispositivo es actualizado.

CAPÍTULO III

METODOLOGÍA

En este capítulo se explica la metodología bajo la cual se desarrolló la presente investigación. La información está organizada y presentada en cuatro apartados. En el primero de ellos se describe el diseño de la investigación, en el segundo los sujetos, en el tercero la descripción del material y en el cuarto el procedimiento de recolección y análisis de los datos de esta investigación.

Diseño de la investigación

Esta investigación fue no experimental cuantitativa, con un alcance inicial exploratorio y uno final descriptivo. No experimental porque no se buscan posibles efectos de una causa que se manipula. Cuantitativa porque usa la recolección de datos para probar un supuesto, con base en la medición numérica y el análisis estadístico. El alcance inicial fue exploratorio debido a que el tema era poco conocido y el alcance final fue descriptivo ya que se recogió información que detalló como son las VLANs y sus requerimientos para funcionar (Hernández, 2006, p. 100).

3.1 SUJETOS

Para efectos de este estudio se trabajó con todo el universo, constituido por los tres encargados que asisten a la red de área local ubicada dentro de los cinco laboratorios del edificio “C” de la FCA-UABC.

3.2 MATERIAL

En cuanto al material, el instrumento de recolección de datos fue la entrevista, la cual se auxilió de un cuestionario y de la observación directa, los cuales arrojaron información para la presente investigación. Se diseñó una entrevista, que contempló datos del entrevistado y del área que tiene a su cargo, así como las principales características de la red. Esta recolección permitió establecer un diagnóstico de la situación actual de la red de área local existente en el edificio “C” de la FCA-UABC.

3.3 PROCEDIMIENTO

Para este estudio se trabajó con todo el universo, formado por los encargados que asisten a la red de área local ubicada dentro de los cinco laboratorios del edificio “C” de la FCA. El instrumento de recolección de datos fue aplicado a todo el universo. Los datos obtenidos se almacenaron en un archivo magnético dentro de una computadora utilizando el software Excel y posteriormente se analizaron mediante el mismo software.

A continuación se describen detalladamente los pasos llevados a cabo en la presente investigación:

1.- Investigación documental.

Se verificó la existencia y fácil consulta de fuentes de información disponibles en Mexicali Baja California, San Diego USA e Internet. Se buscaron algunos de estos tipos de fuentes de información, los cuales fueron los siguientes: proyectos, estudios, artículos y tesis sobre el tema de VLANs en bases de datos especializadas como Ebsco Host, Difusión Científica, Thomson Gale y CSA Illumina. Se realizaron lecturas de tesis elaboradas en instituciones de educación superior: Universidad Autónoma de Tlaxcala y UNAM. Se registraron las fuentes encontradas mediante fichas bibliográficas, se almacenaron en un medio magnético y se generó una relación de la fuente y los capítulos o páginas de los temas importantes para la investigación.

2.- Delimitación del alcance del estudio.

Se delimitó el alcance del estudio, el cual fue generar una propuesta de implementación de VLANs en la LAN existente en los laboratorios del edificio “C” de la FCA de la UABC.

3.- Selección y aplicación de los instrumentos de recolección de datos.

Los instrumentos de recolección de datos utilizados fueron la entrevista, el cuestionario y la observación directa, y se aplicaron de la siguiente manera:

a) Se realizaron entrevistas dirigidas por medio de un cuestionario (véase apéndice A) a los encargados de las áreas dentro de los laboratorios de cómputo del edificio “C” de la FCA referente a lo siguiente:

- Áreas de informática dentro de los laboratorios, su ubicación, importancia y la documentación existente.
- Recursos informáticos con que cuentan los laboratorios.
- Servicios informáticos con que cuentan los laboratorios.
- Planos de los laboratorios, ubicación de las computadoras y de los dispositivos de interconexión, así como sus necesidades de interconexión.
- Problemas actualmente existentes en la red de datos.
- Problemas y necesidades futuros en la red de datos.

b) Se capturó la información obtenida en las tres entrevistas y se alimentó una base de datos mediante el software Excel.

c) Se investigó como ha sido el funcionamiento de las VLANs implementadas en la Facultad de Enfermería y en la Facultad de Ciencias Humanas.

d) Se analizó la información obtenida en las entrevistas mediante el software Excel y se buscó la posibilidad de implementación de VLANs en la FCA.

e) Se prepararon los resultados mediante gráficas.

f) Se prepararon las conclusiones en base a los resultados obtenidos.

g) Se preparó la propuesta de implementación de VLANs

h) Se integró toda la información de los puntos anteriores en un reporte final.

Constantemente se realizaron borradores del trabajo, los cuales se fueron mejorando al ir avanzando la investigación. Se realizaron presentaciones de los avances de la investigación a compañeros de clase en la maestría; obteniendo buenas críticas y sugerencias de mejora.

CAPÍTULO IV

RESULTADOS

En este apartado se muestran los resultados obtenidos en la presente investigación, mediante la entrevista a los encargados que asisten a la LAN dentro de los laboratorios de cómputo del edificio “C” de la FCA, la cual se presenta organizada en base a las preguntas realizadas. Los resultados obtenidos se presentan a continuación:

En base a la información obtenida de la pregunta “¿Trabaja la red con conmutadores capa 2?”; la cual se muestra en la figura 9, se puede observar que el total de la población comenta que la red si trabaja con conmutadores capa 2.

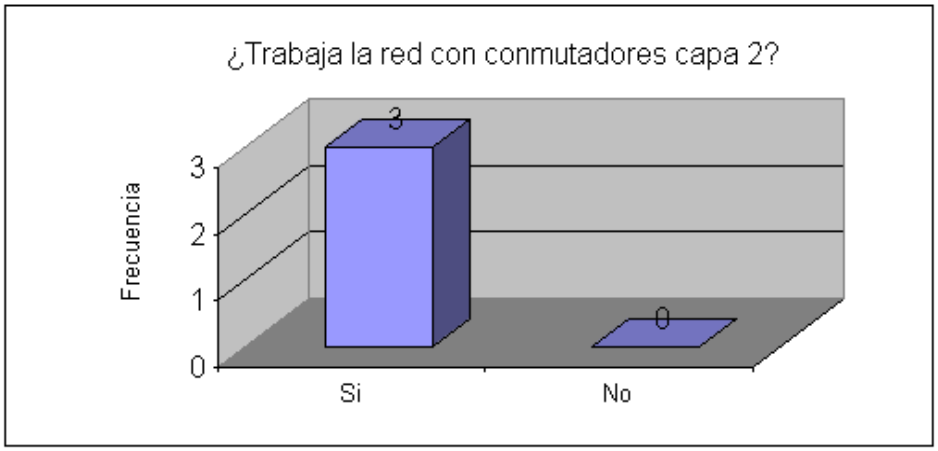


Figura 9. *Utilización de conmutadores capa 2 dentro de la LAN de los laboratorios.*

En base a la información obtenida de la pregunta “¿Trabaja la red con conmutadores capa 3?”; la cual se muestra en la figura 10 se puede observar que el total de la población comenta que la red no trabaja con conmutadores capa 3.

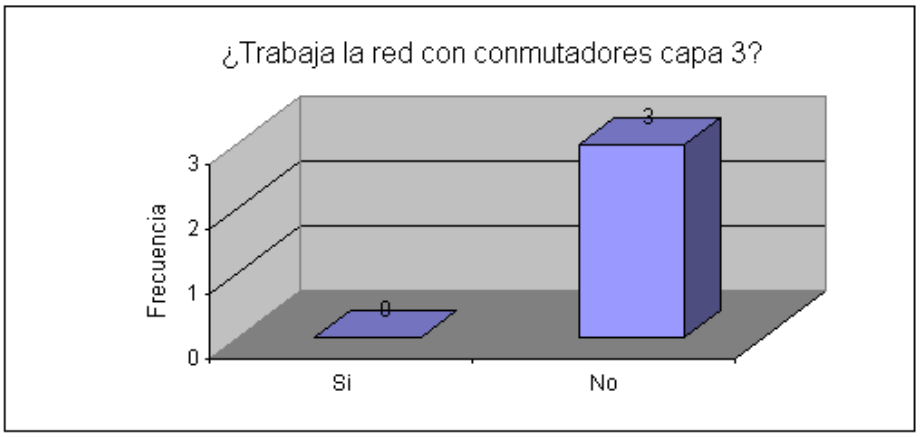


Figura 10. *Utilización de conmutadores capa 3 dentro de la LAN de los laboratorios.*

En base a la información obtenida de la pregunta “¿Existe el problema de disminución del rendimiento de la LAN conforme aumentan los accesos de los usuarios?”; la cual se muestra en la figura 11, se puede observar que el total de la población comenta que en la red si existe el problema de disminución del rendimiento conforme aumentan los accesos de los usuarios.

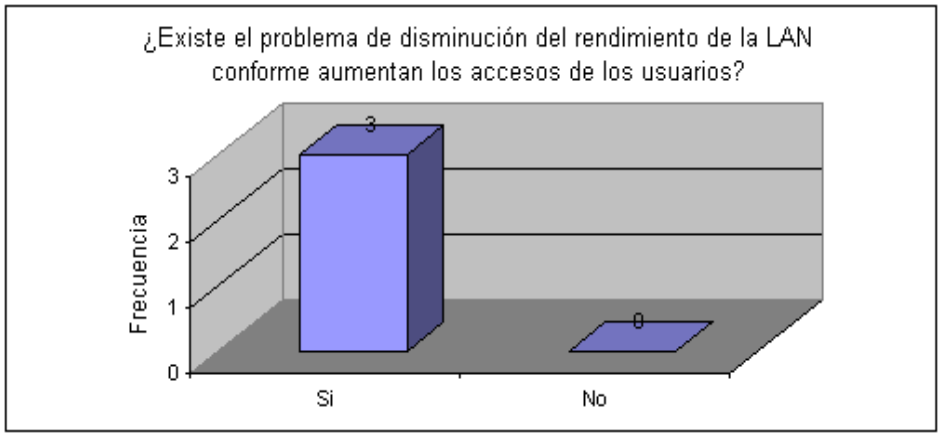


Figura 11. *Disminución del rendimiento de la LAN conforme aumentan los accesos de los usuarios.*

En base a la información obtenida de la pregunta "¿Cuenta la red con VLANs?"; la cual se muestra en la figura 12, se puede observar que el total de la población dice que la red no cuenta con VLANs.

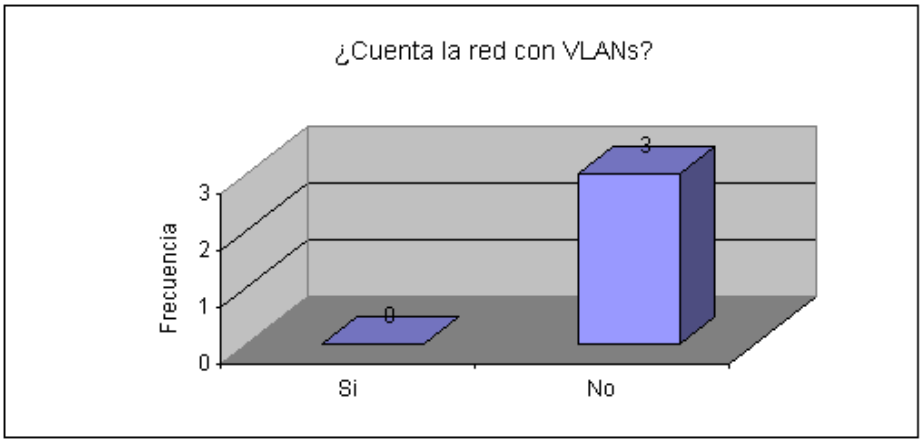


Figura 12. *Utilización de VLANs dentro de la LAN de los laboratorios.*

En base a la información obtenida de la pregunta “¿Cree usted que el empleo de VLANs puede mejorar el rendimiento de la LAN del edificio?”; la cual se muestra en la figura 13, se puede observar que el total de la población comenta que el empleo de VLANs si puede mejorar el rendimiento de la LAN del edificio “C” de la FCA.

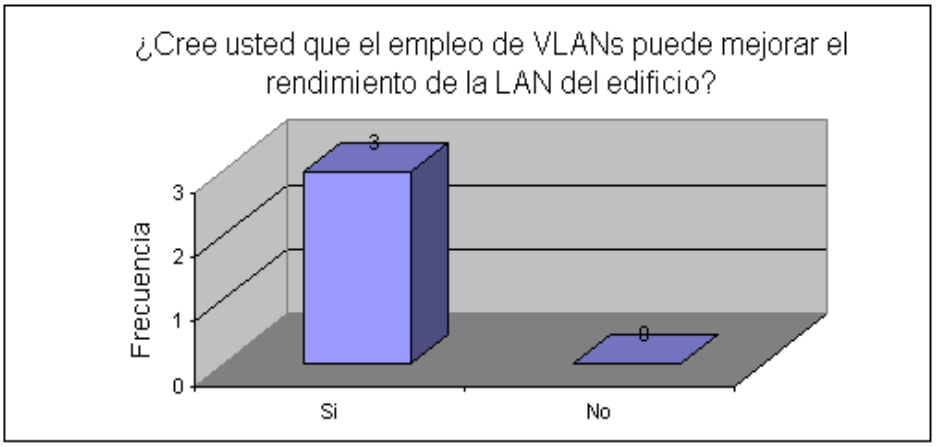


Figura 13. Mejora del rendimiento de la LAN en *los laboratorios mediante el empleo de VLANs.*

En base a la información obtenida de la pregunta “¿Cumple el cableado de la red con estándares como EIA/TIA y la categoría del cable es seis como mínimo?”; la cual se muestra en la figura 14, se puede observar que el total de la población comenta que el cableado de la red si cumple con estándares como EIA/TIA y la categoría del cable es seis como mínimo.

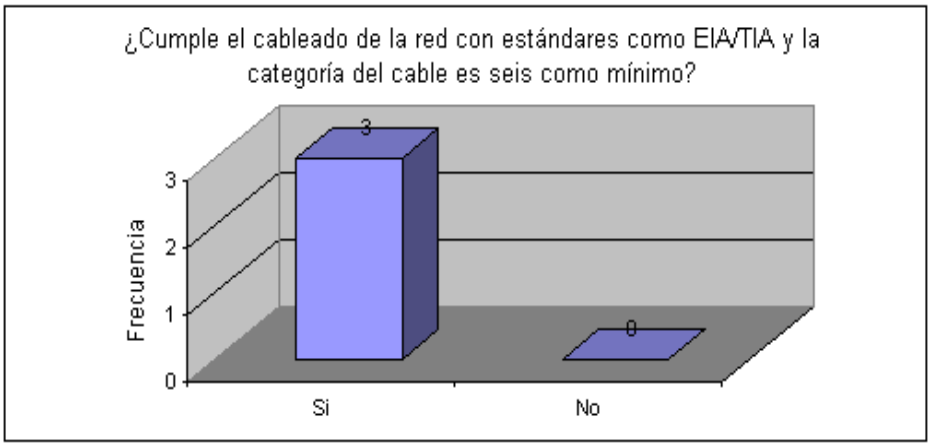


Figura 14. Cumple el cableado de la red con estándares como EIA/TIA y la categoría *del cable es seis como mínimo.*

En base a la información contenida en la memoria técnica del cableado estructurado; proporcionada por el administrador de la red en la FCA, se obtuvo la situación actual de la red existente en el edificio "C" de la FCA. La cual se detalla a continuación:

Los laboratorios de cómputo del edificio "C" de a FCA cuentan con todos los materiales que conforman una red de cableado estructurado: Rack, cable, tapas, conectores, paneles de parcheo para voz y datos, ductos que enrutan al cableado y todos los accesorios necesarios. Lo cual significa que se emplearon normas para la construcción e implementación del mismo, estas normas especifican métodos y procedimientos de cableado en sus instalaciones en cuanto a telecomunicaciones se refiere. El cableado estructurado asegura que las instalaciones proporcionen la máxima vida útil y un desempeño óptimo, además de estar garantizado por 25 años por parte del fabricante PANDUIT. Las normas son las siguientes:

- **TIA/EIA-586** Commercial Building Telecommunications Cabling Standard
- **TIA/EIA-569** Commercial Building Standard for Telecommunications Pathway and spaces.
- **TIA/EIA-570** Residential and Light Commercial Telecommunications Wiring i Standards.
- **TIA/EIA-606** Administration Standard for infrastructure or Commercial Building
- **TIA/EIA-607** Commercial Building Comding and Bonding Requirements
- **TIA/EIA-TSB-72** Centralized Optical Liber Cabling Guidelines

Las áreas que cuentan con cableado estructurado son las siguientes:

- Main Distribution Frame (MDF): Permite distribuir la señal entre equipos internos y externos de la FCA-UABC. Este se encuentra en el primer piso del edificio “B”.
- Intermedia Distributions (IDF): Permite distribuir la señal para equipos de conexión como conmutadores (por un lado) y para equipos terminales como computadoras (por el otro lado). Existen siete IDFs en toda la FCA, dos de los cuales se encuentran en el edificio “C”, uno en el primer piso y otro en el segundo.
- Cable Backbone: Un backbone es un enlace de gran caudal o una serie de nudos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red. Las redes de grandes empresas pueden estar compuestas por múltiples LAN (segmentos) y se conectan entre sí a través del backbone, que es el principal conducto que permite comunicar segmentos entre sí. En la FCA existen cuatro backbones de alta velocidad, los cuales utilizan fibra óptica. Dichos backbones salen del conmutador capa 3 principal de la red ubicado en el MDF del edificio “B” y van a los otros edificios. Uno va al edificio “C”, otro al “A”, otro al “D” y el último va al edificio del CIA. Cada uno es de 1 Gbps.

Descripción general de la planta física de instalación del edificio “C”

- El cableado estructurado de telefonía y cómputo está dimensionado para ser multifuncional con puertos de voz y puertos de datos, dicho

cableado esta basado en cable categoría 6, centralizado en los Racks de comunicaciones, ubicados en el primero y segundo nivel (piso) y un enlace de fibra óptica hacia el MDF.

- El Rack de comunicaciones instalado en Closet de comunicaciones del segundo piso está instalado sobre la loza del piso.
- El Rack de comunicaciones instalado en Closet de comunicaciones del primer piso está instalado sobre la pared.
- Se surten cables para voz y datos desde el Rack, a través de escalerilla sobre techo, derivando de la escalerilla los disparos hacia cada salida de voz y datos.
- Las salidas de voz y datos en cada laboratorio están preparadas con tubería steel de diámetro de ¾" por salida y caja de 4"x4 " x 11/16" con plaster Ring a 2 X 4.
- Se utilizan productos PANDUIT.
- La red está cableada a partir de los páneles de parcheo del Rack de comunicaciones hacia las cajas ubicadas en los puntos terminales. su función es distribuir las señales provenientes de los dispositivos concentradores de cableado del rack de comunicaciones hacia los equipos de cómputo e impresoras ubicadas en los laboratorios.

El cableado estructurado para los usuarios cuenta con 2 cables categoría 6 por cada salida en configuración 568A, rematados en paneles de parcheo todo en categoría 6, se usa un gabinete de telecomunicaciones principal (ver figuras 16, 17 y 18 en el apéndice "D"). Todos los servicios son rematados (cableados horizontales) para terminar en el usuario final. El cableado horizontal se refiere al que va del gabinete instalado en cada nivel (piso) hacia los usuarios finales cliente. De lado del usuario se remata con 2 cables UTP categoría 6 con los jacks categoría 6 montados estos en placas plásticas para 2,4,6 y 8 posiciones y basados en las normas para cableado horizontal (ANSI/EIA/TIA-568a). Todas las salidas, paneles de parcheo UTP están

debidamente identificadas (TIA/606 Standard), todo el cableado interno UTP (cableado horizontal) está probado y certificado por equipo especial para certificación de puertos. El material instalado está certificado para 25 años mínimo por parte del fabricante del sistema de cableado estructurado para servicios de datos con cable UTP (especificado y probado a 250 mhz), cuyos componentes de cableado y accesorios son de la marca Panduit-Belden.

Cableado de comunicaciones de datos categoría 6

- La distancia máxima de corrida del cable horizontal es de 90 metros, de la terminación mecánica de conexión transversal a la salida de telecomunicaciones en el área de trabajo. Es rematado por ambos extremos conforme a las normas de cableado estructurado.

- Se incluyen paneles de parcheo categoría 6, con configuración 568 A, que soportan la transmisión de tecnología Ethernet en el orden de los Gigabits, además de contar con salidas para conector RJ-45 categoría 6 en su parte frontal.

- La salida en la terminal de trabajo, es con cable UTP categoría 6 conforme a la norma EIA/TIA 568A.

- La caja terminal para usuario, cuenta con jack RJ-45 categoría 6.

Se emplea como medio de transmisión un cable conductor de cobre (par trenzado) de cuatro pares, con las siguientes características:

- UTP (Unshielded Twisted Pair) categoría 6 (enhanced) marca Belden.
- Conductor sólido de cobre de 5 mm calibre (24 AWG)
- Resistencia Ohmica: 100 Ohms.
- Atenuación máxima: 22 dB.

- Velocidad mínima de propagación del medio: 548 nseg.
- La longitud máxima de corrida del cable horizontal es de 90 metros par cada segmento.
- Material aislante: Polietileno.
    - Forro: PVC.

Cordones de parcheo (utp categoría 6) manufacturados de línea

La longitud máxima del cable de parcheo, esto es, de la salida de telecomunicaciones a la tarjeta de red, es de 7 pies de longitud máxima y esta rematado por ambos extremos con conectores plug RJ-45. En el caso del cuarto de equipo o rack, los cables de parcheo que van del panel de parcheo al equipo de telecomunicaciones, cuentan con una longitud máxima de 3 pies, además de estar rematados por ambos extremos con conectores plug RJ-45 antes mencionados.

Panel de parcheo para cable utp categoría 6

En el caso del cableado horizontal y vertical, la conexión termina en equipos de conexión que cumplen con los requerimientos del estándar EIA/TIA 568A, que soportan la transmisión de alta velocidad y la combinación de requerimientos de voz y datos, el panel de parcheo cumple con las siguientes características:

- Panel de parcheo para categoría 6 de 24 puertos, que soporta la tecnología Ethernet en el orden de los Gigabits, metálico.
- fácil montaje en rack y/o gabinetes de 19 pulgadas.

- En la parte posterior cuenta con entradas para Jack minicom.
- Los conectores cuentan con códigos de colores para mostrar los pares individuales y facilitar su cableado en configuración 568-A
- Cuenta con áreas de identificación arriba y debajo de cada puerto.

Un conmutador aísla y cataliza los datos para que cada nodo tenga acceso ilimitado al cable. El conmutador es una tecnología muy sencilla y económica para mejorar el desempeño de una red con mucho tráfico de datos.

Situación actual del segundo piso en cuanto a conmutadores.

El IDF del segundo piso cuenta con un rack instalado sobre la loza del piso, en el cual se encuentran seis conmutadores capa 2 interconectados y prestando servicio a todo el segundo piso. Cuatro son Fast Ethernet, donde tres son de 48 puertos y uno es de 16 puertos. Dando un total de 160 puertos para conexión a la red, de los cuales tan sólo se requieren 128 para los cuatro laboratorios de este piso. El quinto es un conmutador Gigabit de ocho puertos y es utilizado para el manejo de voz sobre la red. El sexto es un conmutador de 8 puertos empleado para la conexión con el primer piso y con los pisos dos, tres y cuatro del edificio “D”.

Situación actual del primer piso en cuanto a conmutadores:

El IDF del primer piso cuenta con un gabinete instalado sobre la pared, en el cual se encuentran tres conmutadores Fast Ethernet capa 2 interconectados, donde dos son de 48 puertos y uno es de 16 puertos. Dando un total de 112 puertos para conexión a la red, de los cuales sólo se requieren 34 para el laboratorio número 5 ubicado en este piso. Uno de 48 puertos es utilizado para el manejo de las computadoras del laboratorio cinco y algunos de sus puertos, así como el resto de los conmutadores, son utilizados para el manejo de las computadoras de la red administrativa.

Situación actual de SITE en cuanto a conmutadores:

La red LAN existente en la FCA-UABC maneja un modelo jerárquico, el cual se divide en las capas core (capa central), distribución y acceso. En la capa central se manejan cuatro backbones con un conmutador capa 3 de alta velocidad

ANÁLISIS

Tomando en cuenta toda la información obtenida en la entrevista a los encargados que asisten a la LAN dentro de los laboratorios de cómputo del edificio “C” de la FCA se realizó el siguiente análisis:

- La red utiliza conmutadores capa 2 marca Allied de la serie AT-8000 para su funcionamiento, los cuales permiten la implementación de VLANs. Con los conmutadores actuales es suficiente para poder implementar VLANs en el edificio “C”, lo cual significa que no será necesaria la adquisición de equipo de estas características permitiendo un gran ahorro para la FCA. Estos dispositivos se encuentran funcionando con la configuración que tienen por defecto al momento de comprarse, por lo cual, se observa que se están

desaprovechando sus capacidades. Una forma de obtener un mayor aprovechamiento de los mismos es mediante la configuración de VLANs, ya que las VLANs son la mayor ventaja de la conmutación de capa 2. (Hill, 2003, p.528).

- La red no utiliza conmutadores capa 3 para su funcionamiento, lo cual implica que se tendrá que comprar uno para poder comunicar VLANs existentes en diferentes conmutadores. Además, permitirá aislar el tráfico de información del edificio “C” del resto del tráfico de la red principal de la FCA.

- Existe el problema de disminución de rendimiento de la LAN conforme aumentan los accesos de los usuarios, el cual se seguirá incrementando ya que la población estudiantil sigue creciendo conforme pasa el tiempo. Este echo justifica la implementación de VLANs, ya que éstas mejoran el rendimiento de la red. (Ariganello, 2007, p. 144).

- La red no utiliza VLANs desaprovechando el gran potencial de los conmutadores capa 2 existentes. (Hill, 2003, p. 528).

- Los entrevistados creen que el empleo de VLANs puede mejorar el rendimiento de la red. Ya que las VLANs permitirán aislar el tráfico generado en el edificio “C” de la red principal de la FCA.

- El cableado de la red si cumple con estándares como EIA/TIA y la categoría el cable es seis. Lo anterior significa que existe un cableado estructurado, el cual asegura que las instalaciones proporcionen la máxima vida útil y un desempeño óptimo, además de estar garantizado por 25 años por parte del fabricante PANDUIT. Esta categoría de cable permitirá trabajar con las futuras tecnologías de red sin requerir modificación alguna, lo cual significa un gran ahorro de tiempo, trabajo y dinero para la facultad.

CAPÍTULO V

CONCLUSIONES

En este último capítulo se busca resaltar los resultados más relevantes y exponer las conclusiones de la presente investigación.

De acuerdo al análisis realizado en el capítulo IV, se observa que los laboratorios de cómputo instalados en el edificio “C” de la FCA-UABC disponen de una infraestructura con cableado estructurado (cables y conectores) que cumple con los estándares de la EIA/TIA, además, cuentan con hardware, software e instalaciones apropiadas para la implementación de VLANs. Los dispositivos de interconexión y comunicación son en su gran mayoría conmutadores capa 2 que permiten la implementación de VLANs, lo cual, representa un gran ahorro en caso de una implementación ya que no se requeriría comprarlos; sólo es necesario adquirir un conmutador capa 3 para poder comunicar computadoras existentes en diferentes conmutadores capa 2 pero pertenecientes a la misma VLAN. Es factible realizar la implementación de VLANs en el edificio “C” de la FCA a un bajo costo, comparado con el gasto que implicaría comprar todos los conmutadores capa 2 ya existentes.

De acuerdo a la experiencia empírica de los encargados en las VLANs de la escuela de enfermería y de la Facultad de Ciencias Humanas, al igual que los autores Sackett (2002), Hill (2003), Ariganello (2007) y a la información obtenida en la presente

investigación, se concluye que el rendimiento de la red de área local en los laboratorios de cómputo del edificio “C” de la Facultad de Ciencias Administrativas de la Universidad Autónoma de Baja California se puede mejorar mediante el empleo de VLANs.

El objetivo general de esta investigación; que fue crear una propuesta de implementación de VLANs dentro de los laboratorios de cómputo instalados en el edificio “C” de la FCA-UABC, se logró alcanzar de manera satisfactoria. Al igual que el objetivo particular, consistente en contar con el conocimiento necesario para poder aumentar el rendimiento de la LAN dentro de los laboratorios de cómputo instalados en el edificio “C” de la FCA mediante la aplicación de VLANs.

De acuerdo al análisis anterior se llega a la conclusión de que el supuesto que guió este trabajo de investigación; el cual fue que el empleo de VLANs permitirá aumentar el rendimiento de la red de área local de los laboratorios de cómputo del edificio “C” de la FCA-UABC puede ser aceptado.

La realización de un anteproyecto me permitió tomar la decisión de cambiar de tema antes de seguir adelante con la tesis, evitando una gran pérdida de tiempo, esfuerzo y dinero (Schmelkes, 2006). La aplicación de la metodología de investigación fue muy importante para buscar, ordenar y registrar datos e ideas, la utilización de este método de trabajo fue una gran experiencia que me servirá en mis trabajos futuros, ya sean personales o laborales.

PROPUESTA

En base a toda la información con la que se trabajó en la presente investigación; principalmente con la contenida en la memoria técnica del cableado estructurado del edificio, se llegó a lo siguiente:

Actualmente existe una sola red de área local en toda la FCA, esto provoca una gran lentitud en la red y caídas en las llamadas telefónicas. La propuesta del presente trabajo consiste; de manera muy general, en aislar la información procesada en el edificio “C” de la información procesada por los otros edificios de la FCA-UABC. Este aislamiento se realizará mediante la instalación y configuración de un conmutador capa 3 de nueva adquisición en el IDF del segundo piso del edificio “C”. De forma similar, también se aislará la información procesada en cada uno de los laboratorios del edificio “C”. Este aislamiento se realizará mediante la configuración de los conmutadores capa 2 ya existentes en los IDFs del primero y segundo piso del edificio “C”. El conmutador capa 3 se encargará de administrar las VLANs de nueva creación en los conmutadores capa 2.

La propuesta para el segundo piso; en cuanto a conmutadores, es la siguiente:

Se propone crear siete VLANs dentro de los seis conmutadores capa 2 existentes. Una en el conmutador de manejo de voz, otra en el conmutador que conecta al edificio “D” y cinco dentro de los cuatro conmutadores Fast Ethernet, donde cuatro

serán utilizadas para los cuatro laboratorios de este piso; una VLAN para cada uno de ellos, y la quinta será utilizada para el resto de los equipos de cómputo no pertenecientes a los cuatro laboratorios. Dichas VLANs permitirán aislar la información de los laboratorios, los teléfonos y los administrativos, incrementando el rendimiento y la seguridad de la red. Las VLANs permiten manejar voz sobre IP (VoIP) sin tener que crear redes separadas para voz y para datos. (Webster, 2006, p. 21).

También se propone instalar y configurar un conmutador capa 3 (de nueva adquisición) para que administre las nuevas VLANs creadas en los conmutadores capa 2 existentes. Este conmutador capa 3 filtrará toda la información del edificio “C” antes de enviarla al conmutador capa 3 central del MDF (conmutador central que administra la red de la FCA), aislando el edificio “C” de la red principal de la FCA y evitando darle carga y saturación innecesaria a la red principal. Del mismo modo, las VLANs de los conmutadores capa 2 filtrarán su información para no afectar a las otras VLANs del edificio “C”.

La propuesta para el primer piso; en cuanto a conmutadores, es la siguiente:

Se propone crear una VLAN dentro del conmutador de 48 puertos utilizado para las computadoras el laboratorio 5 y crear las mismas VLANs para telefonía y administrativos realizadas en el segundo piso del edificio en los otros conmutadores capa 2 de este primer piso.

Diseño de la red del edificio “C”

En la figura 15 que se muestra a continuación se presenta el diseño de las capas de un modelo jerárquico que comprende el diseño de la red propuesta. Este diseño cuenta con un backbone de fibra óptica en la capa core de 1 Gbps. El backbone sale del conmutador central capa 3 de la FCA ubicado en el edificio “B” y va al conmutador capa 3 de nueva adquisición instalado en el IDF existente en el segundo piso del edificio ”C”, este segundo conmutador capa 3 constituye la capa de distribución. Los conmutadores en la capa de acceso son los que proveen la conexión a los equipos (computadoras) de los usuarios.

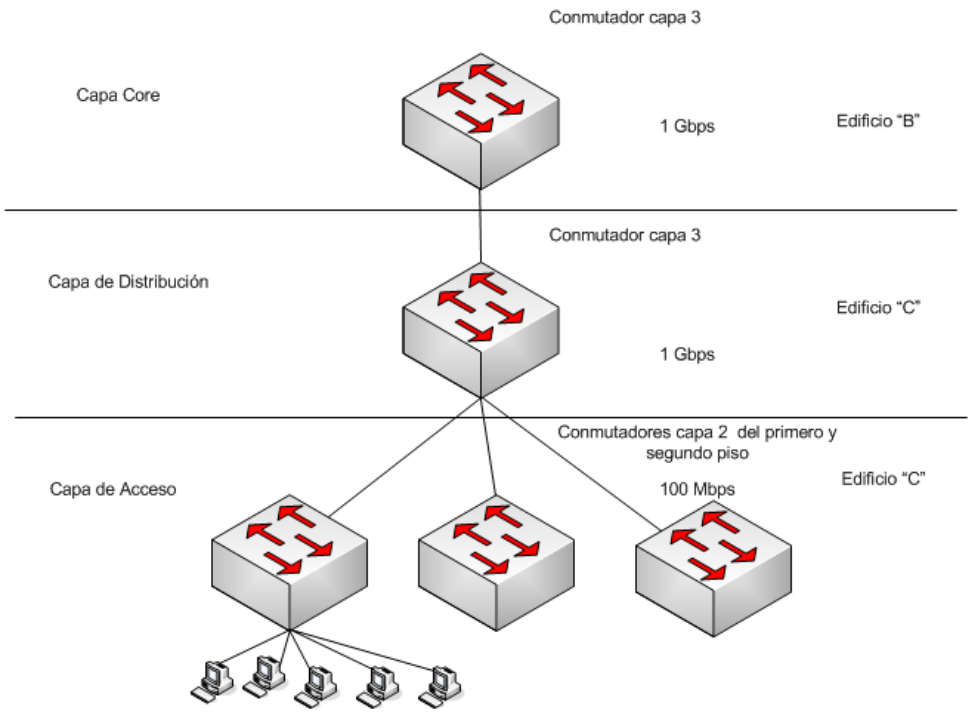


Figura 15: Diseño de capas de la nueva red.

La capa core es el corazón de la red. Su propósito es reenviar paquetes tan rápidamente como sea posible. Necesita diseñarse pensando en alta disponibilidad. Actualmente, para las interconexiones del core está creciendo el uso de Gigabit Ethernet. La capa de distribución une la capa de acceso con el core. Generalmente se usa Gigabit Ethernet para conectar el core y se usa Gigabit Ethernet o vínculos 100base-TX/FX para conectar la capa de acceso. La capa de acceso conecta las estaciones de trabajo y los servidores. Los conmutadores usados en esta capa son más chicos, usualmente 24-48 puertos. Las computadoras de escritorio y las estaciones de trabajo usualmente son conectadas a 10 Mbps y los servidores son conectados a 100 Mbps.

Principales características del diseño propuesto

A continuación se detallan las dos características más importantes del diseño de red propuesta:

- Definición de los dominios broadcast a través de la capa de acceso. Esto se logra al definir las VLANs en cada conmutador del tipo capa 2 que se encuentran en los bordes, permitiendo de esta manera que no se inunden otras partes de la red de manera innecesaria, dejando libre el ancho de banda necesario para las aplicaciones y servicios de red.
- Balance de carga a través de la capa de distribución. Al conmutador capa 3 (de nueva adquisición) instalado en la capa de distribución se le configura una subnet por cada VLAN creada en los conmutadores de la capa de acceso. Al

tener definida una subnet por VLAN no solo se evita el inundamiento de broadcast en la red si no también se controla el flujo de información a través del backbone que conecta la capa de distribución con el core.

Especificaciones del conmutador capa 3 recomendado para compra.

Marca	Allied Telesis
Modelo	AT-9724TS
Características	10/100/1000 x 24 puertos Gigabit Ethernet Conmutador capa 3 con 4 combo SFP expansion bays and 2 20 Gbps stacking ports
Información del producto	• Port mirroring • Wire speed Layer 2-3 filtering • Wire speed Layer 3 IP routing • RIP v1 and v2 and OSPF support • High-density port count • 4096 maximum VLANs • Multiple spanning tree 802.1s
Cantidad	1
Costo	1,437.82 dlls.

Tabla 12: Relación de material existente en la red actual

Num. Parte	DESCRIPCION	Unidad	Cantidad	Costo dlls
EDR19FM 45U	Rack de Aluminio color negro 7'X19"	pz	1	200
SRM19CM V3	Charola doble para servidores	pz	2	70
CMRPSH2 0	Barra de 10 contactos electricos 20 Amperes	pz	2	170
E-WMW3622 25	Gabinete empotrable en pared de 3 pies	pz	1	1200
WMPV45E	Organizador Vertical frontal y posterior	pz	2	35
PUC6004B U	Cable UTP 4 Pares Cat 6 color Azul	rollo	14	190
DP485E88 TG	Panel de parcheo cargado con 48 puertos	pz	1	45
DP245E88 TG	Panel de parcheo cargado con 24 puertos	pz	2	45
CPPL48W BL	Panel de parcheo modular de 48 puertos	pz	3	45
CPPL24W BL	Panel de parcheo modular de 24 puertos	pz	2	45
WMPH2E	Administrador horizontal de 2 U.R.	pz	12	45
WMPSE	Administrador horizontal de 1 U.R.	pz	2	35
CJ688TPR D	Jack's modulares Cat 6 color Rojo para enlace	pz	4	10
CJ688TPB U	Jack's modulares Cat 6 color azul para datos	pz	208	10
CJ688TPY L	Jack's modulares Cat 6 color amarillo para voz	pz	64	10
CFPE4E1	Placa Modular de 4 posiciones	pz	65	5
JB3510IW	Caja de sobreponer 2x4	pz	65	7
CMBE1-X	Cubre espacios para Faceplate modular	pz	14	3
UTPSP3R D	Patch Coord Cat 6 color rojo 3" para enlaces	pz	4	8
UTPSP3B U	Patch Coord Cat 6 color azul 3" para datos	pz	104	8
UTPSP3Y L	Patch Coord Cat 6 color amarillos 3" para voz	pz	32	8

UTPSP7BU	Patch Coord Cat 6 color amarillos 7" para Datos Usuario final	pz	86	12
UTPSP10BU	Patch Coord Cat 6 color amarillos 10" para Datos Usuario final	pz	7	15
UTPSP20BU	Patch Coord Cat 6 color amarillos 20" para Datos Usuario final	pz	11	22
HLWRK	Hubbell Kit Escalerilla para sujetacion de racks a pared	pz	2	80
S/N	Material Miscelaneo	lote	1	
S/N	Mano de Obra por instalación de servicios de cableado, certificado y garantía.	nodos	208	140

Relación de conmutadores capa 2 existentes

Marca	Allied Telesis
Modelo	AT-8000/8PoE
Características	10/100/TX x 8 puertos unmanaged PoE Fast Ethernet Conmutador con 1 SFP.
Cantidad	1
Costo	441.40 dlls

Marca	Allied Telesis
Modelo	AT 8000S/16
Características	Conmutador, 16 puertos, Fast Ethernet, 10-Base-T, 100Base-TX + 1x10/100/1000Base-T/SFP (mini-GBIC). 1U.
Cantidad	2
Costo	340.39 dlls

Marca	Allied Telesis
Modelo	AT 8000S/48
Características	Conmutador . 48 puertos. EN, Fast EN. 10Base-T, 100Base-TX + 2x 10/100TX x 48 port managed Fast Ethernet switch with SFP x 2 combo ports
Cantidad	5
Costo	852.60 dlls

Marca	LinkSys
Modelo	SRW2008MP
Características	8-Port 10/100/1000 Managed Gigabit Switch from Linksys brings gigabit speeds to users, while adding intelligence and security to network.
Cantidad	1
Costo	314.99 dlls

REFERENCIAS BIBLIOGRÁFICAS

Ariganello, Ernesto. (2007). *Redes cisco. Guía de estudio para la certificación CCNA-640-801*. México: Alfaomega Ra-Ma.

Bigelow, Stephen J. (2003). *Localización de averías, reparación, mantenimiento y optimización de redes.* México : Mc Graw Hill.

Comer, Douglas E. & Stevens, David L. (2000). Interconectividad de redes con TCP/IP. Volumen II. Diseño e implementación. Tercera Edición. México: Pearson Educación.

Fitzgerald, Jerry & Dennos, Alan. (2003). Redes y comunicación de datos en los negocios. 3ra Edición. Ed. Noriega Limusa Wiley.

Flynn, Ida M. & Mchoes, Ann M. (2001). Sistemas Operativos. Tercera Edición. Ed. Cengage Learning Editores.

Forouzan, Behrouz A. (2003). Local Área Networks. Ed. Mc Graw Hill.

Gaceta Universitaria (1992). Febrero de 1992. Vol. 1. p. 3. Aída Angélica García Sánchez. México.

Gaceta Universitaria (2008). Marzo de 2008. No. 205. P. 2. Rodrigo Martínez Meza. México.

García, Tomás Jesús, Raya, Cabrera José Luis & Raya, Víctor Rodrigo. (2002). Alta velocidad y calidad de servicio en Redes IP. México: Alfaomega Ra-Ma.

Garg, G., & Thirumurthy, R. (2005, October 13). Optimized learning in metro switches. EDN, 50(21), 69-74. Retrieved January 31, 2009, from Academic Search Premier database.

Habraken, Joe (2000). Routers Cisco. Ed. Prentice may.

Hallberg, Bruce A. (2007). *Fundamentos de Redes*. México: Mc Graw Hill.

Hernández, Sampieri Roberto, Fernández, Collado Carlos & Baptista, Lucio Pilar. (2006). *Metodología de la investigación*. Cuarta edición. México: Mc Graw Hill.

Hill, Brian (2003). *Manual de referencia Cisco*. México: Mc Graw Hill.

Keiser, Gerd. (2002). *Local área Networks*. Second Edition. Mc. Graw Hill.

Komarek, L. (2007, December). Plug leaks in the firewall to improve Ethernet security. Plant Engineering, 61(12), 43-43. Retrieved January 31, 2009, from Academic Search Premier database.

Mañas**,** José Antonio & Fernández, Calvo Rafael. (2004). Mundo IP: Introducción a los secretos de Internet y las redes de datos. Ed. Nowtilus S.L

Molina, Robles Francisco José. (2006). *Redes de área local*. 2ª Edición. México: Alfaomega Ra-Ma.

Norton, Peter (2000). Introducción a la computación. Tercera edición. México: Mc. Graw Hill.

Palmer, Michael J. (2001). Redes de computadoras. Ed. Thomson Learning.

Raya, Cabrera José Luis & Raya, González Laura (2006). Redes Locales. 4ta Edición. México: Alfaomega Ra-Ma.

Raya, Cabrera José Luis & Raya, Pérez Cristina (2003). Redes Locales. 2da Edición. México: Alfaomega Ra-Ma.

Sackett, George C. (2002). *Manual de Routers Cisco*. México: Mc Graw Hill.

Sánchez, Allende Jesús & López, Lérida Joaquín. (2000). *Redes.* México: Osborne Mc Graw Hill.

Schmelkes, Corina. (2006). *Manual para la presentación de anteproyectos e informes de investigación.* Segunda edición. Oxford University press México, S.A. de C.V.

Schweitzer, D. (2005, August 29). The "Virtual" Way to Better Gíreles Security. Computerworld, 39(35), 29-29. Retrieved January 31, 2009, from Academic Search Premier database.

Shaughnessy, Tom & Velte, Toby. (2000). *Manual de Cisco*. México : Osborne Mc Graw Hill.

Stallings, William. (2004). *Comunicaciones y redes de computadores. 7ª. Edición*, México : Pearson Prentice Hall.

St-Pierre, Armand & Stéphanos, William. (2005). *Redes locales e internet. Introducción a la comunicación de datos*. México: Trillas.

Sturdevant, C. (2008, September 22). SECURITY IN A VIRTUALIZED WORLD. eWeek, 25(27), 35-40. Retrieved February 8, 2009, from Academic Search Premier database.

Tanenbaum, Andrew S. (2003). *Redes de computadoras. 4ª. Edición*, México: Pearson Educación.

Vallejos, Soto Antonio M. (2001). *Sistemas microinformáticos y redes LAN.* Marcombo.

Webster, J. (2006, January 23). Lessons From the Front Lines. InfoWorld, 28(4), 21-26. Retrieved January 31, 2009, from Academic Search Premier database.

Zacker, Craig. (2002). *Redes. Manual de referencia.* México: Ed. Mc Graw Hill Osborne Media.

APÉNDICES

APÉNDICE A: FORMATO DE ENTREVISTA.

ENTREVISTA

Fecha de la entrevista _____
Lugar de la entrevista _____

DATOS GENERALES

Entrevistado (a) _____
E-mail _____
Teléfono (s) _____
Cargo _____
Actividades que realiza _____

DATOS DEL ÁREA

Área de la que está encargado (a) _____
Ubicación _____
Importancia _____

Recursos informáticos que administra _____

Servicios informáticos que presta _____

Usuarios de los servicios _____

Documentación _____

DATOS DE LA RED

Problemas que presenta _____

UABC Universidad Autónoma de Baja California

ENTREVISTA

Fecha en la que iniciaron los problemas _____

Problemas y necesidades futuras _____

_____

¿A qué atribuye los presentes problemas? _____

_____

¿Trabaja la red con conmutadores capa 2? si ◯ no ◯

¿Trabaja la red con conmutadores capa 3? si ◯ no ◯

¿Existe el problema de disminución del rendimiento de la LAN conforme aumentan los accesos de los usuarios? si ◯ no ◯

¿Cuenta la red con VLANs? si ◯ no ◯

¿Cree usted que el empleo de VLANs puede mejorar el rendimiento de la LAN del edificio? si ◯ no ◯

¿Cumple el cableado de la red con estándares como EIA/TIA y la categoria del cable es 6 como mínimo? si ◯ no ◯

APÉNDICE B: GLOSARIO.

Ancho de banda (Bandwidth): Define la cantidad de información que puede ser transmitida en un periodo de tiempo determinado a través de una Red. Es la diferencia entre la frecuencia más alta y la más baja de un canal de transmisión (en hertzs, Hz). Margen de frecuencias capaz de transmitirse por una red de telecomunicaciones.

ANSI (American National Standards Institute): El Instituto Nacional Norteamericano de Normalización es la organización responsable de aprobar las normas de los Estados Unidos en muchas áreas, ordenadores y comunicaciones, y es miembro de la ISO.

Apantallamiento: Recubrimiento de un cable por el que se transmite información en forma de señal electromagnética, con el fin de evitar las interferencias que pudiesen alterar la información.

ASCII (**American Standard Code for Information Interchange):** Código estándar americano para intercambio de la información. Esquema normalizado de codificación de caracteres introducido en 1.963 y muy utilizado en muchas máquinas. Sistema de codificación de caracteres alfanuméricos en 7 bits para la operación interna del computador y su comunicación con los periféricos. Este sistema, promovido por el

ANSI, es ampliamente utilizado por ordenadores personales, estaciones de trabajo y miniordenadores.

ATM (Asynchronous Transfer Mode): Modo de Transferencia Asíncrona. Técnica de conmutación por paquetes de alta velocidad adecuada para redes de área metropolitana (MAN), transmisión de banda ancha y redes digitales de servicios integrados (RDSI).

ARPANET (Advanced Research Projects Agency Network): Red pionera de larga distancia financiada por ARPA (hoy DARPA) con finalidades militares, que fue el eje central del desarrollo de Internet.

Backbone: Red principal de una red de comunicaciones. Permite conectar varias redes.

Banda ancha: Técnica de comunicaciones en la que las señales digitales se transmiten moduladas, pudiendo enviarse por un solo canal múltiples señales simultáneas. La UIT-T define también como banda ancha a las comunicaciones digitales a más de 2 Mbps.

Banda base: Técnica de comunicaciones en la que las señales digitales codificadas se transmiten en su forma original, es decir, sin modulación.

Bandwidth: Véase ancho de banda.

Bit (**Binary Digit):** Dígito binario. Unidad mínima de información con la que trabajan los ordenadores. Es un dígito del sistema binario que puede tener el valor 0 o 1.

Baudio (Baud): Número de veces por segundo que cambia el estado de la señal de un medio de transmisión. Aplicado al modem, la señal que envía por la línea telefónica.

Bridge (Puente): Véase puente.

Buffer: Segmento reservado de memoria que se usa para almacenar datos mientras se procesan. Conjunto de registros conectados en paralelo que actúan como memoria intermedia para almacenar datos temporalmente para compensar y adaptar diferencias de velocidad entre emisor y receptor.

Byte: Agrupación fundamental de información binaria formada por 8 bits. Es la unidad mínima que puede direccionarse, pero no la unidad mínima que puede tratarse.

CCITT (Comité Consultivo de Telegrafía y Telefonía Internacional): Antiguo órgano competente de la Unión Internacional de Telecomunicaciones de las Naciones Unidas en asuntos de telefonía, telegrafía y datos, que coordinaba los Sistemas telefónicos y de comunicación de datos de todo el mundo. Con frecuencia, sus

recomendaciones técnicas se convierten en normas reconocidas internacionalmente. Ha sido sustituido por la UIT-T (Unión Internacional de Telecomunicaciones-Telemática, ITU-T: Internacional Telecommunicacion Union-Telematics).

Cliente/Servidor: Arquitectura de sistemas de información en la que los procesos de una aplicación se dividen en componentes que se pueden ejecutar en máquinas diferentes. Modo de funcionamiento de una aplicación en la que se diferencian dos tipos de procesos y su soporte se asigna a plataformas diferentes.

Codificación: Transformación de un mensaje en forma codificada, es decir, especificación para la asignación unívoca de los caracteres de un repertorio (alfabeto, juego de caracteres) a los de otro repertorio. Conversión de un valor analógico en una señal digital según un código prefijado.

Código: Cada una de las secuencias de caracteres que transforman los elementos de un repertorio en otro.

Computadora: Es un dispositivo electrónico usado para poder procesar datos. Recibe datos a través de los dispositivos de entrada, los almacena en memoria principal o secundaria, procesa los datos y presenta la información generada mediante los dispositivos de salida.

Control de Enlace Lógico: Véase LLC.

CSMA/CD (**Carrier Sense Multiple Access with Collision Detection):** Protocolo de comunicaciones para una red de área local que utiliza una estructura en bus. Define los niveles físico y de enlace del modelo OSI para el método de acceso a la red por el cual una estación obtiene el uso del medio físico para enviar un mensaje a través de la red. La especificación de este protocolo se describe en las normas IEEE 802.3 e ISO 8802.3, ambas basadas en el estándar Ethernet.

Conmutación de paquetes: Es un método de comunicación exclusivamente digital, en el que los mensajes que se transmiten se dividen en segmentos y que, junto a la información adicional necesaria para su encaminamiento en la red, se convierten en paquetes. Éstos son transferidos a través de la red mediante procesos de almacenamiento y reenvío sobre circuitos virtuales (circuitos no físicos), que permiten la compartición de los canales físicos de comunicaciones de la red, pues solamente los ocupan durante el tiempo de transmisión.

Conmutación digital: En el entorno de telefonía se refiere al establecimiento de conexiones a través de un centro de conmutación o central telefónica mediante operaciones con señales digitalizadas, es decir, sin convertirlas a su forma analógica original. Las señales de datos están normalmente en forma digital (excepto cuando se convierten a analógicas mediante un módem), por lo tanto, el término "conmutación digital" raramente se utiliza en relación con datos porque las señales siguen siendo digitales aunque puedan conmutarse en base a un circuito conmutado.

Conmutación rápida de paquetes: Término genérico para perfeccionar tecnologías de conmutación de paquetes, como los modos de transporte denominados "Frame Relay" y "Cell Relay". Se diferencia de la conmutación de paquetes según la recomendación X.25, por su transporte a alta velocidad. También permite la transmisión de voz, datos y vídeo.

Concentrador: Equipo para diversos tipos de cables y para diversas formas de acceso que sirve de plataforma integradora para distintas clases de cables y de arquitectura.

Decodificación: Conversión de un valor digital en una señal analógica. Proceso de reconversión de un mensaje codificado al mensaje que dio lugar a la codificación.

DECnet: Red de comunicaciones de Digital, que soporta RAL de estilo Ethernet y WAN de banda base y de banda ancha en líneas públicas y privadas.

Digital: Es una forma de representar la realidad mediante unas corrientes de valores finitos formadas por unos y ceros.

Dominio: Estructura jerárquica que organiza las máquinas de Internet de forma que sea fácil recordar su nombre.

EIA/TIA (Electronic Industry Association / Telecommunication Industry Association): Asociación de la industria electrónica / Asociación de la industria de telecomunicaciones.

Encapsulación: Permite la conexión de varias redes informáticas entre sí para formar una sola red de nivel más alto. Cuando se utiliza encapsulación, se define un nuevo nivel de protocolo; esto proporciona una semántica uniforme para servicios tales como conmutación de paquetes, correo electrónico, etc. En programación orientada a objetos, es la asociación de datos y funciones que tiene el efecto de ocultar al solicitante de una función la forma en que ésta se ha desarrollado.

Equipo físico (Hardware): Circuitería electrónica. En general, todos los elementos físicos de un equipo informático.

Equipo lógico (Software): Programas del sistema, de aplicación, de utilidades, procedimientos, reglas y su documentación asociada, relacionados con la operación de un ordenador. Conjunto de instrucciones y datos que un ordenador es capaz de entender.

Estándar: Conjunto de reglas y regulaciones acordado por una organización oficial de estándares (estándar de jure) o por aceptación general en el mercado (estándar de facto).

Ethernet: Red de área local ISO 8023 que transmite a 10 Mbps y pueden conectarse en total hasta 1024 nodos. Conjunto de especificaciones que definen el funcionamiento de redes locales CSMA/CD.

Emulación de terminal: Proceso por el que nuestro ordenador simula mediante software una terminal (pantalla y teclado, sin disco, memoria ni CPU). Es necesario para usar Telnet o ejecución remota.

Encriptado: Proceso de codificación y ocultación de paquetes de datos para impedir su lectura por terceros y asegurar la confidencialidad de determinadas transacciones.

FDDI (Fiber Distributed Data Interface): Especificación de una red de área local con topología en anillo, método de acceso por paso de testigo cuya estructura se implementa sobre un cable de fibra óptica. Esta norma fue desarrollada por el ANSI.

Firewall: El "cortafuegos" es una medida de seguridad que se coloca entre una Red local e Internet, que filtra los paquetes que entran y salen hacia Internet desde una red local.

FTP (File Transfer Protocol): Protocolo para la Transferencia de Ficheros (archivos).

Gateway (Puerta de acceso, pasarela): Véase pasarela.

Hardware: Véase Equipo físico.

Host: En una red informática, es un ordenador central que facilita a los usuarios finales servicios tales como capacidad de proceso y acceso a bases de datos, y que permite funciones de control de red.

Hub: Véase concentrador.

IEEE (Institute of Electrical and Electronics Engineers): Instituto de Ingeniería Eléctricos y Electrónicos. Organismo normalizador de métodos de acceso y control para redes de área local. Es miembro de ANSI e ISO.

IP (Internet Protocol): Protocolo internet. Protocolo sin conexión (connectionless) encargado de controlar la información por la red. Permite la integración de otras subredes. Véase TCP/IP.

Kbps (Kilobits por segundo): Medida de velocidad de transmisión. Transmisión de 1024 bits por segundo.

KiloByte (Kb): Unidad de medida de memoria. Equivalencia: 1 KByte = 1,024 Bytes.

LAN (Local Area Network): Véase Red de área local.

LLC (Logical Link Control (Protocol)): Control de enlace lógico. Protocolo de nivel de enlace del modelo OSI definido para redes de área local.

MAC (Medium Access Control): Protocolo de control de acceso al medio empleado para la propagación de las señales eléctricas. Define el subnivel inferior de la capa 2 del modelo OSI (nivel de enlace).

Mbps (Megabits por segundo): Medida de velocidad de transmisión. 1Mbps = 1024*1024 bits por segundo.

Módem (Modulador/demodulador): Equipo para la transmisión de datos que convierte señales analógicas en digitales y viceversa. Elemento físico que permite transmitir información entre dos ordenadores mediante una línea telefónica.

Modulación: Modificación de alguno de los parámetros de una onda portadora por una señal moduladora que se quiere transmitir.

OSI (Open Systems Interconnection): Interconexión de Sistemas Abiertos. Estándar ISO para comunicaciones a nivel mundial que define una estructura con el fin de implementar protocolos en 7 estratos o capas. El control se transfiere de un estrato al siguiente comenzando en el estrato de aplicación en una estación, llegando hasta el estrato inferior, por el canal hasta la próxima estación y subiendo nuevamente la jerarquía. Las 7 capas o estratos son: Físico, Enlace de datos, Red,

Transporte, Sesión, Presentación y Aplicación. El OSI requiere una enorme cooperación para que sea un estándar universal como el sistema telefónico.

Paquete: Secuencia de dígitos binarios, incluyendo datos y señales de control, que se transmite y conmuta como un todo.

Pasarela: Unidad de interfuncionamiento. Dispositivo de comunicaciones que interconecta sistemas diseñados conforme a protocolos propietarios, o entre un sistema con un protocolo propietario y un sistema abierto o una red RAL, teniendo lugar una conversión completa de protocolos hasta la capa 7 del modelo de referencia OSI.

PC (Personal Computer): Computadora Personal. Ordenador generalmente monousuario y monotarea, que utiliza como CPU un microprocesador. Tradicionalmente asociado a los ordenadores de uso personal o doméstico.

Protocolo de comunicaciones: Reglas preestablecidas para efectuar la conexión electrónica entre dos sistemas de comunicación. Puede haber diferentes tipos, que establecen desde las normas para las tensiones eléctricas en los extremos de los contactos metálicos hasta reglas lógicas de alto nivel, como la organización de los datos a trasmitir, su modo de identificación, codificación, etc. Conjunto de reglas y convenios que posibilitan la transmisión de información a través de una red de

telecomunicaciones. Conjunto de reglas semánticas y sintácticas que rigen el comportamiento de las unidades funcionales en las comunicaciones.

Protocolo Internet: Véase IP.

Puente: Unidad Funcional que interconecta dos redes de área local que utilizan el mismo protocolo de control de enlace lógico pero distintos protocolos de control de acceso al medio dentro del nivel 2 de OSI.

Puerto (Port): Conector de la placa base para instalar elementos externos.

Red: Es un conjunto de computadoras y dispositivos interconectados que permiten intercambiar información, compartir recursos y comunicarse.

Red de Area Local (**Local Area Network**): Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña. Normalmente, el área de servicio está limitada a un determinado piso, a una zona de una oficina o a un edificio.

Rendimiento: Velocidad de la información que llega a, y posiblemente pase a través de un punto determinado del sistema de red.

Router (Enrutador, Direccionador): Encaminador de paquetes hacia su destino por la ruta óptima. Dispositivo que se encarga de dirigir el tráfico en una red. La información pasa de nuestro ordenador a un router, y luego de router a router, hasta que el destino está en la misma red local que el último.

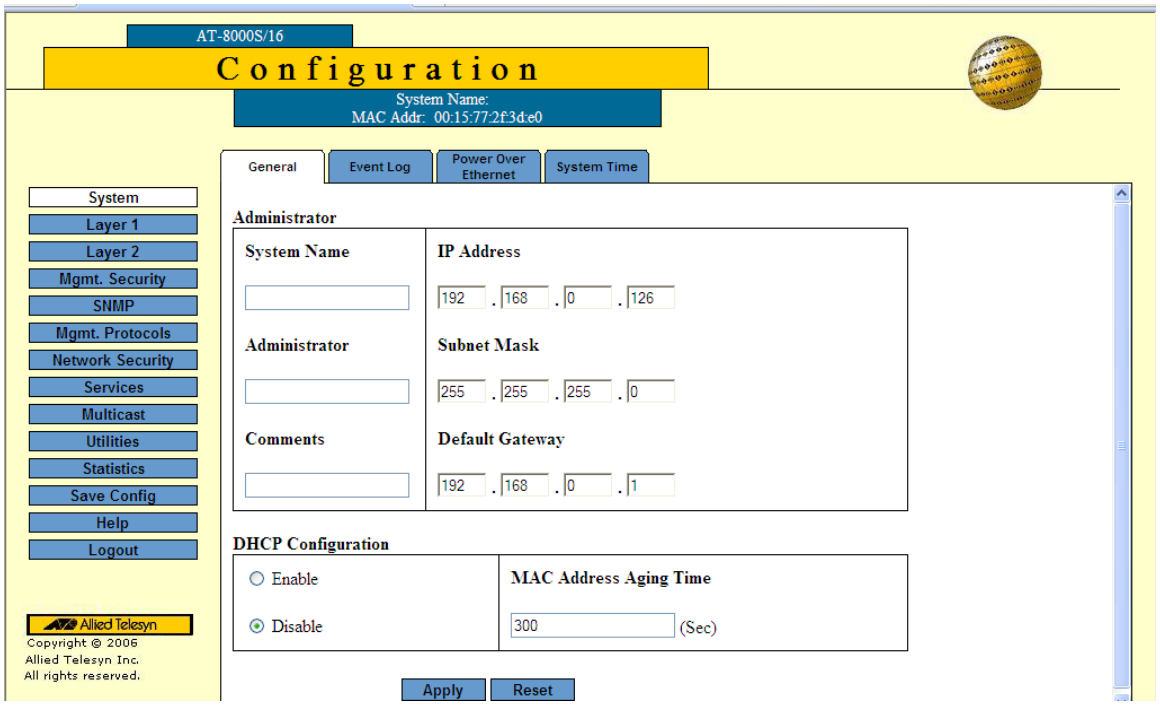
TCP/IP (Transmission Control Protocol/Internet Protocol): Protocolo de Control de Transmisión/Protocolo Interredes. Protocolo para el control de la transmisión orientado a la conexión (connection-oriented) TCP, establecido sobre el protocolo internet (IP). Su amplia extensión permite reconocerla como una norma de facto aunque no es una norma internacional. Mientras que TCP es un protocolo de transporte (nivel cuatro de OSI), el IP es un protocolo de red. Son un conjunto de normas (nivel tres de OSI) para RALs definidas en Estados Unidos para los organismos de defensa para la DARPA (Defense Advanced Research Projects Agency), donde está definida la forma en que deben comunicarse los ordenadores, las redes entre sí y el encaminamiento del tráfico de la red.

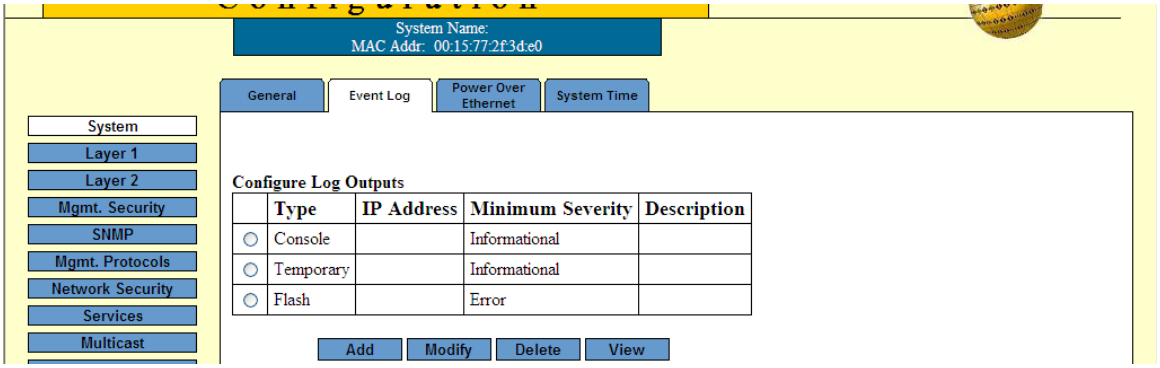
UTP (Unshielded Twisted Pair): Par trenzado no apantallado.

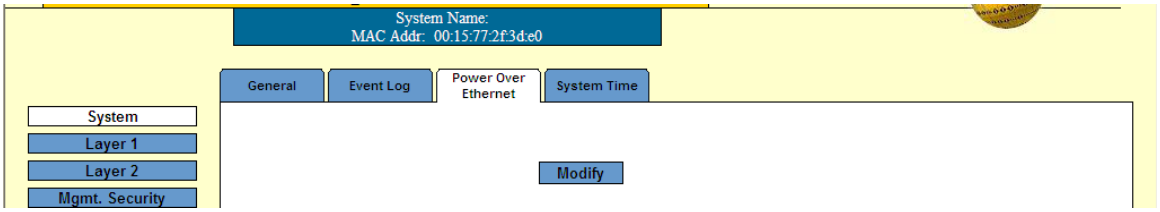
Velocidad de transmisión: Medida de velocidad en señales por segundo.

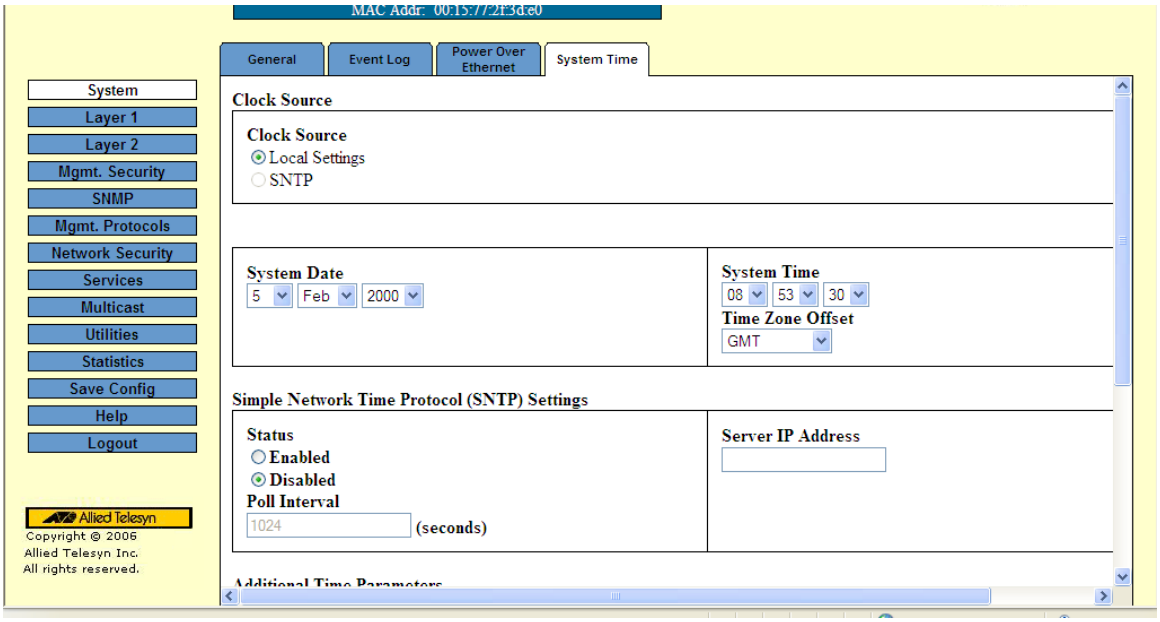
WAN (Wide Area Network): Red de área extensa.

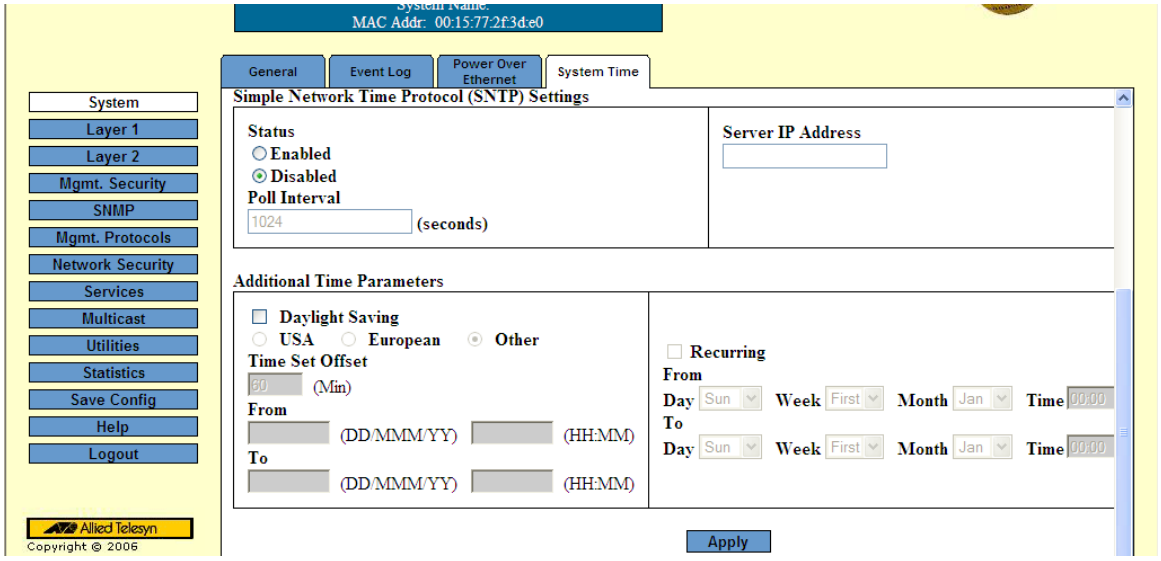
APÉNDICE C: PANTALLAS DE LA CONFIGURACIÓN DE UN SWITCH ALLIED TELESIS AT-8000S SERIES

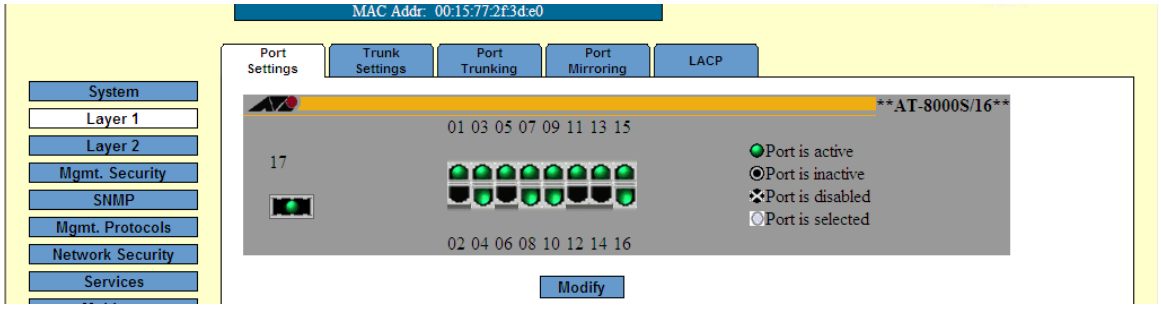


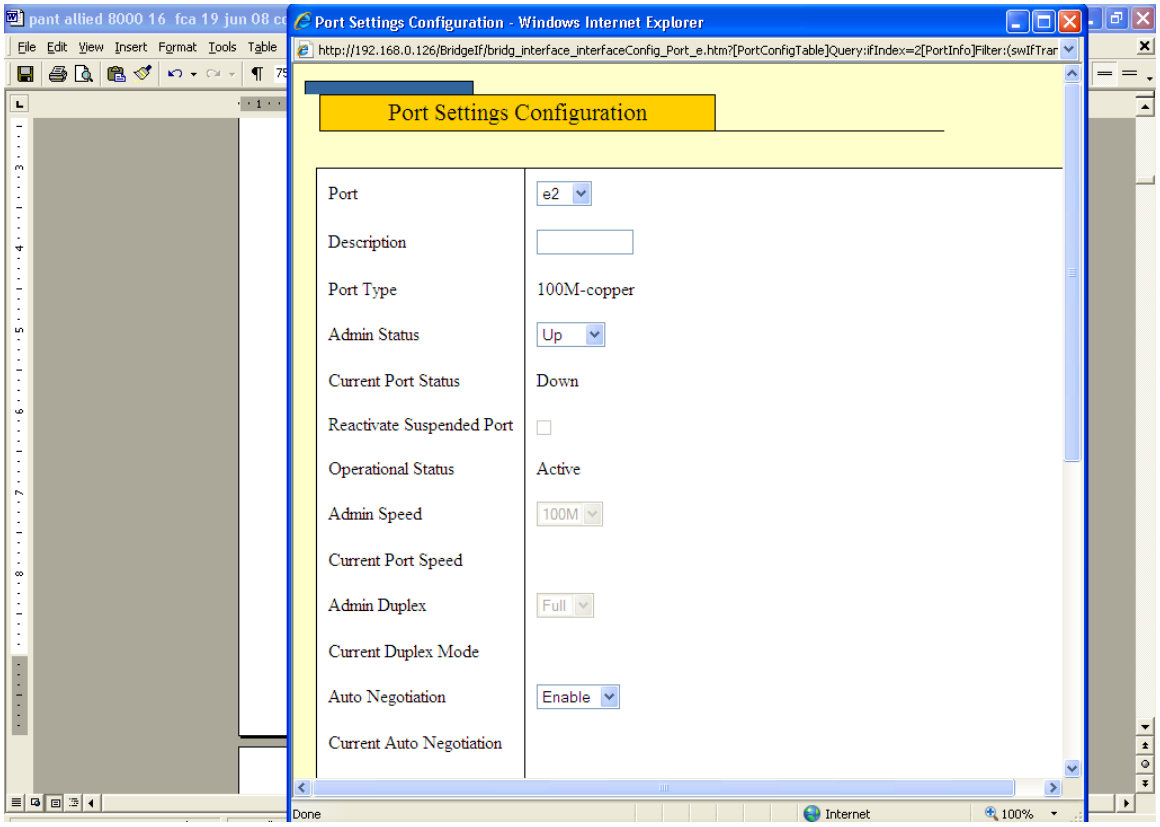

System Name:
MAC Addr: 00:15:77:2f:3d:e0
General
Event Log
Power Over Ethernet
System Time
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Configure Log Outputs
Type
IP Address
Minimum Severity
Description
Console
Informational
Temporary
Informational
Flash
Error
Add
Modify
Delete
View

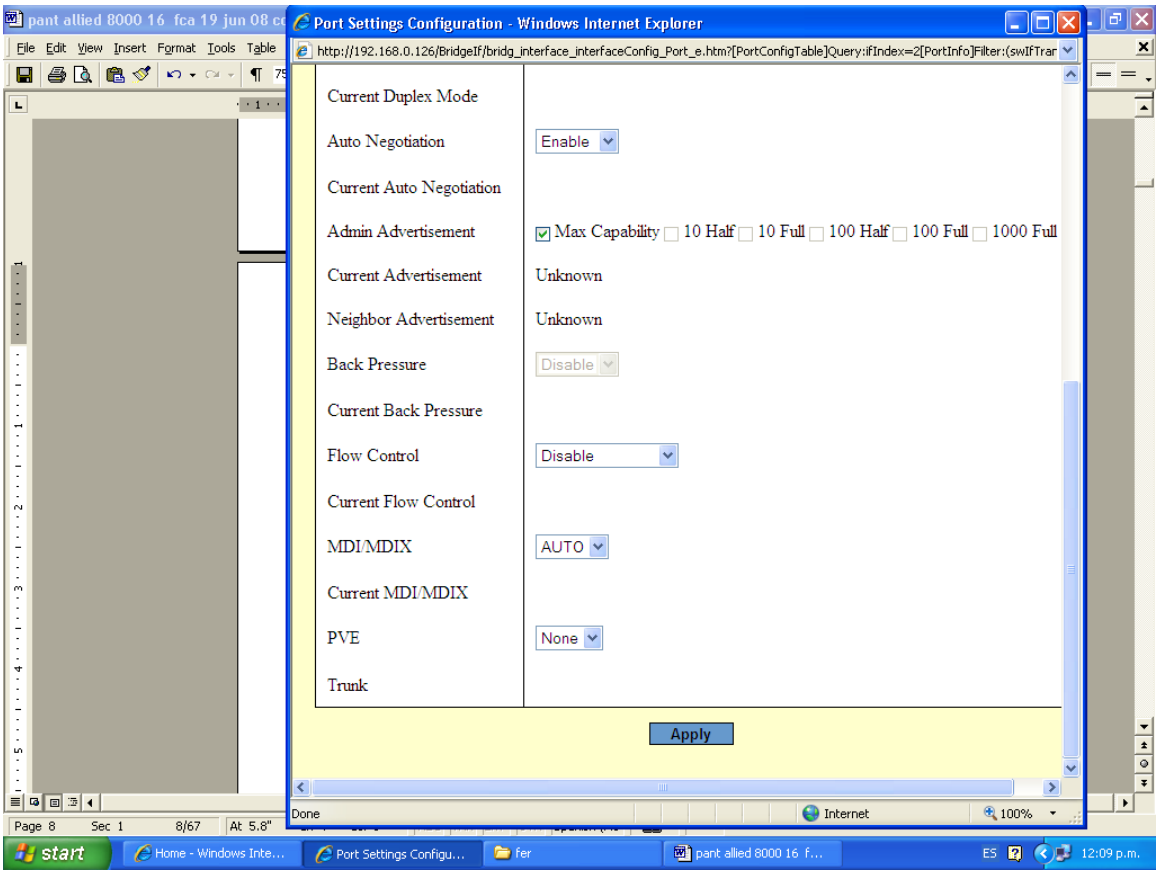

System Name:
MAC Addr: 00:15:77:2f:3d:e0
General
Event Log
Power Over Ethernet
System Time
System
Layer 1
Layer 2
Mgmt. Security
Modify

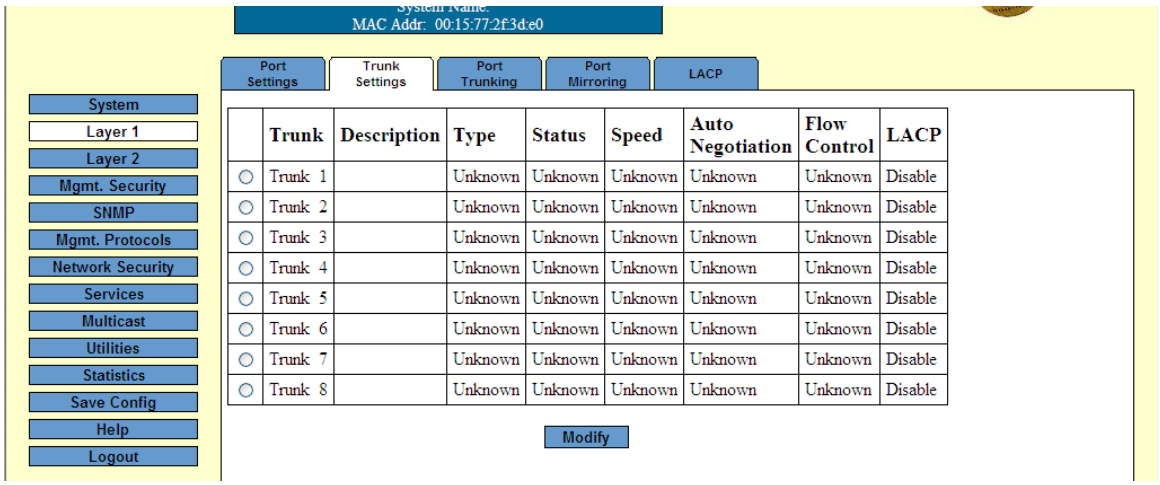

General
Event Log
Power Over Ethernet
System Time
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Clock Source
Clock Source
Local Settings
SNTP
System Date
5
Feb
2000
System Time
08
53
30
Time Zone Offset
GMT
Simple Network Time Protocol (SNTP) Settings
Status
Enabled
Disabled
Poll Interval
1024
(seconds)
Server IP Address
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

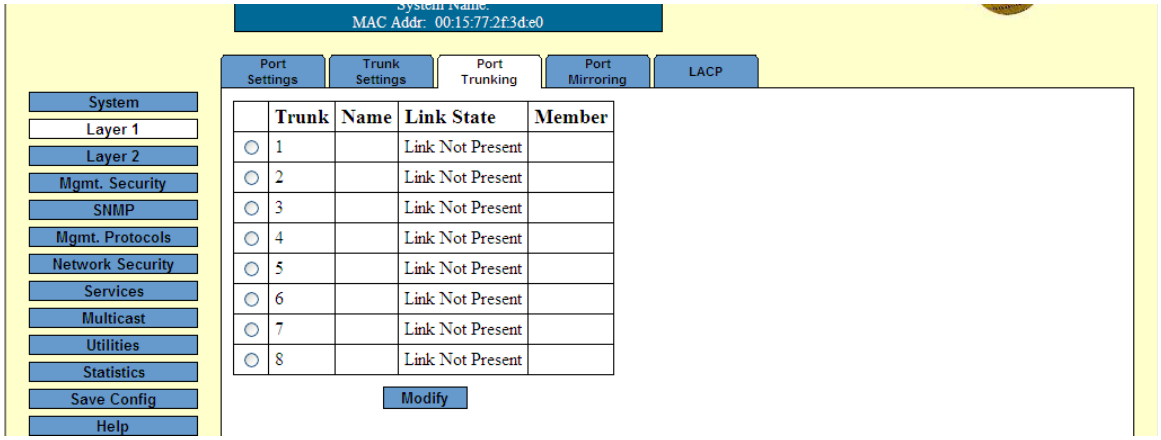

MAC Addr: 00:15:77:2f:3d:e0
General
Event Log
Power Over Ethernet
System Time
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Simple Network Time Protocol (SNTP) Settings
Status
Enabled
Disabled
Poll Interval
1024
(seconds)
Server IP Address
Additional Time Parameters
Daylight Saving
USA
European
Other
Time Set Offset
60
(Min)
From
(DD/MMM/YY)
(HH:MM)
To
(DD/MMM/YY)
(HH:MM)
Recurring
From
Day Sun Week First Month Jan Time 00:00
To
Day Sun Week First Month Jan Time 00:00
Apply
Allied Telesyn
Copyright © 2006

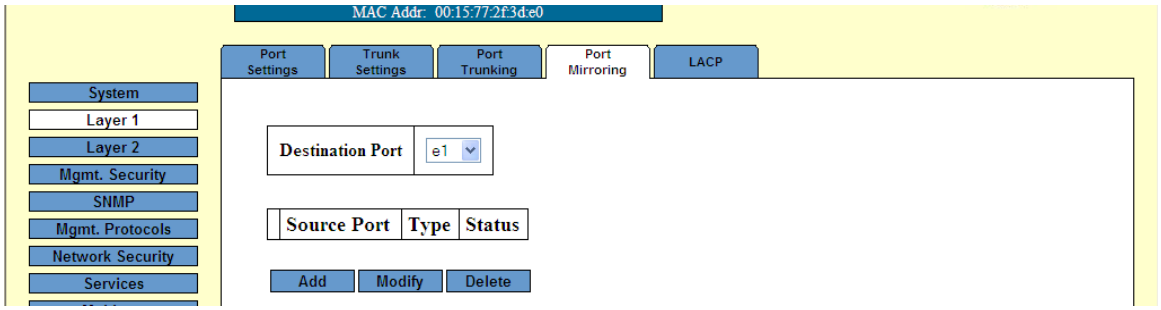

MAC Addr: 00:15:77:2f:3d:e0
Port Settings
Trunk Settings
Port Trunking
Port Mirroring
LACP
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
AT-8000S/16
01 03 05 07 09 11 13 15
17
02 04 06 08 10 12 14 16
Port is active
Port is inactive
Port is disabled
Port is selected
Modify

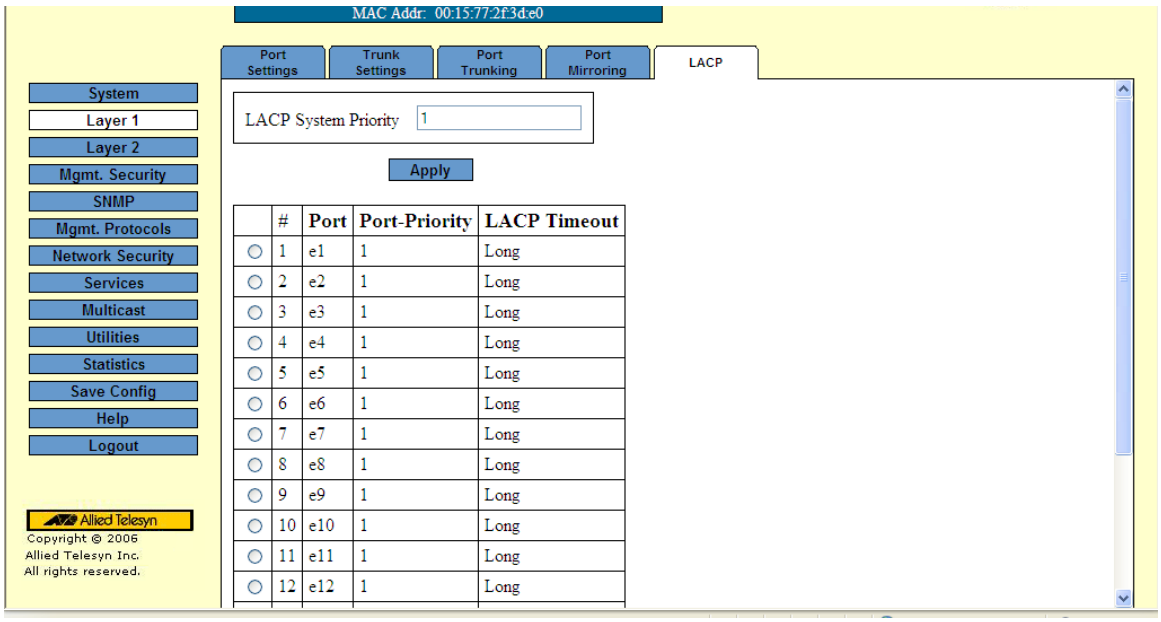

Port Settings Configuration - Windows Internet Explorer
http://192.168.0.126/BridgeIf/bridg_interface_interfaceConfig_Port_e.htm?[PortConfigTable]Query:ifIndex=2[PortInfo]Filter:(swIfTrar
Port Settings Configuration
Port
e2
Description
Port Type
100M-copper
Admin Status
Up
Current Port Status
Down
Reactivate Suspended Port
Operational Status
Active
Admin Speed
100M
Current Port Speed
Admin Duplex
Full
Current Duplex Mode
Auto Negotiation
Enable
Current Auto Negotiation
Done
Internet
100%

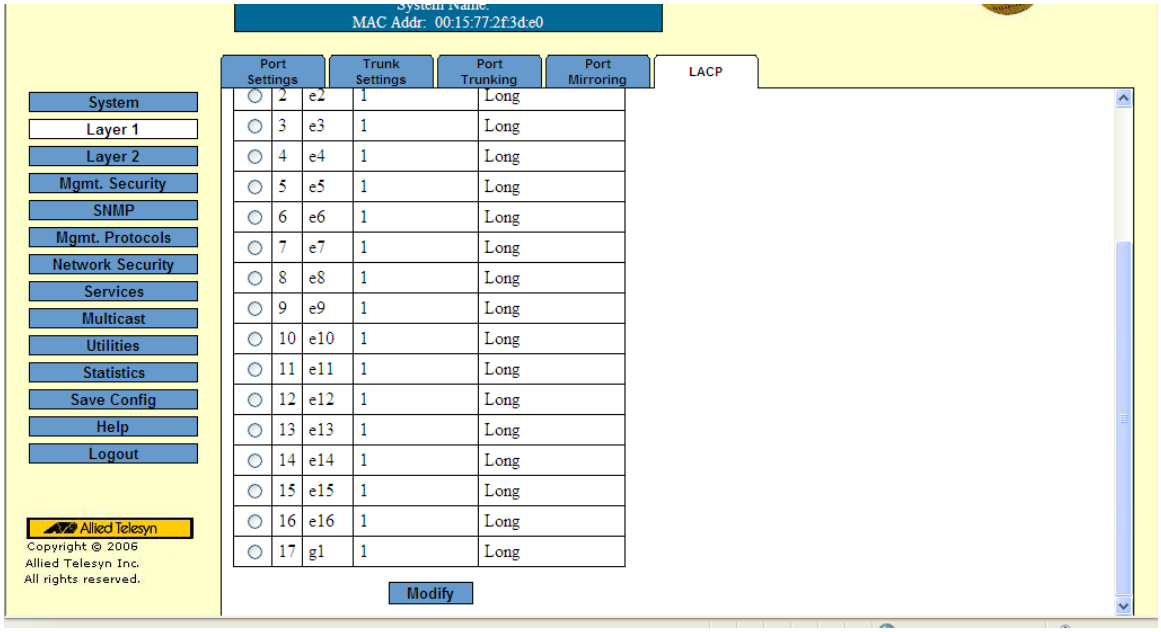

Port Settings Configuration - Windows Internet Explorer
http://192.168.0.126/BridgeIf/bridg_interface_interfaceConfig_Port_e.htm?[PortConfigTable]Query:ifIndex=2[PortInfo]Filter:(swIfTrar
Current Duplex Mode
Auto Negotiation
Enable
Current Auto Negotiation
Admin Advertisement
Max Capability
10 Half
10 Full
100 Half
100 Full
1000 Full
Current Advertisement
Unknown
Neighbor Advertisement
Unknown
Back Pressure
Disable
Current Back Pressure
Flow Control
Disable
Current Flow Control
MDI/MDIX
AUTO
Current MDI/MDIX
PVE
None
Trunk
Apply
Done
Internet
100%
start
Home - Windows Inte...
Port Settings Configu...
fer
pant allied 8000 16 f...
ES
12:09 p.m.

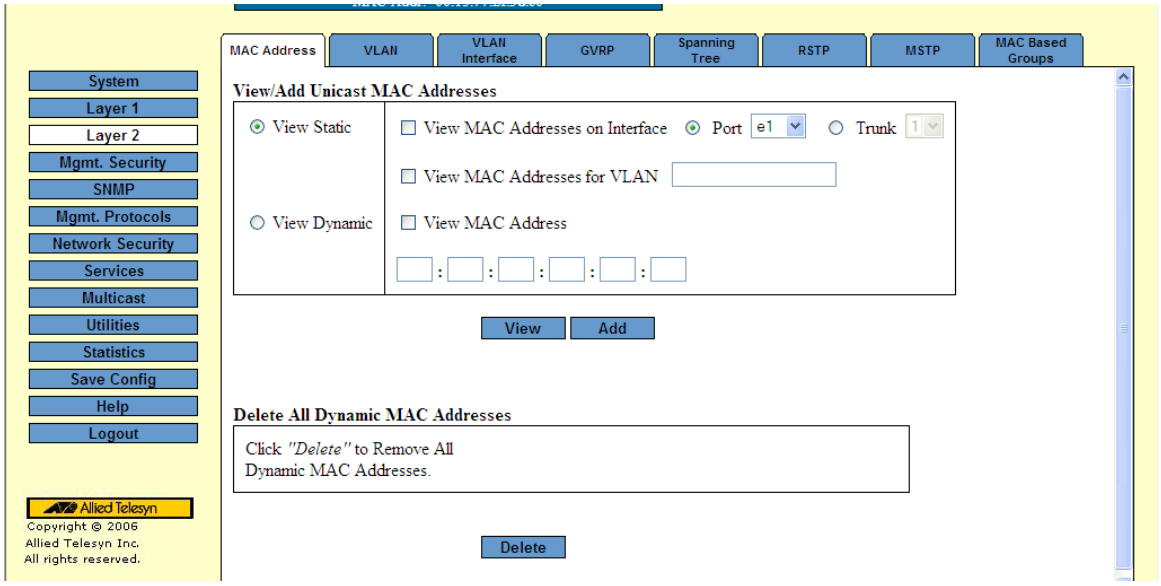

MAC Addr: 00:15:77:2f:3d:e0
Port Settings
Trunk Settings
Port Trunking
Port Mirroring
LACP
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Trunk
Description
Type
Status
Speed
Auto Negotiation
Flow Control
LACP
Trunk 1
Trunk 2
Trunk 3
Trunk 4
Trunk 5
Trunk 6
Trunk 7
Trunk 8
Unknown
Disable
Modify

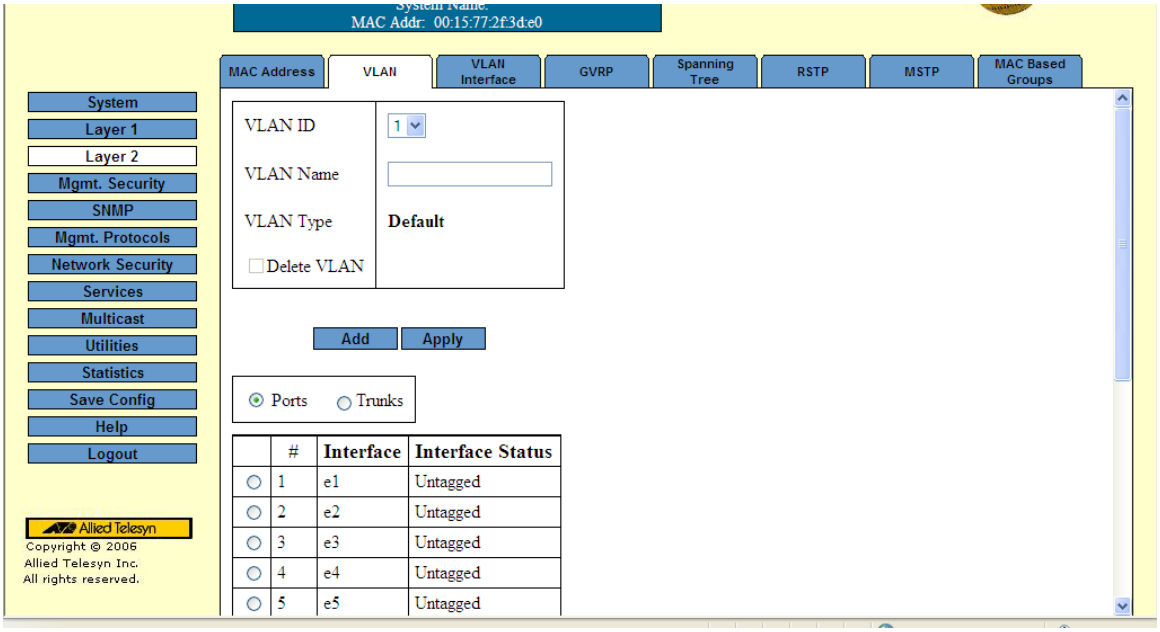

MAC Addr: 00:15:77:2f:3d:e0
Port Settings
Trunk Settings
Port Trunking
Port Mirroring
LACP
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Trunk
Name
Link State
Member
1 Link Not Present
2 Link Not Present
3 Link Not Present
4 Link Not Present
5 Link Not Present
6 Link Not Present
7 Link Not Present
8 Link Not Present
Modify

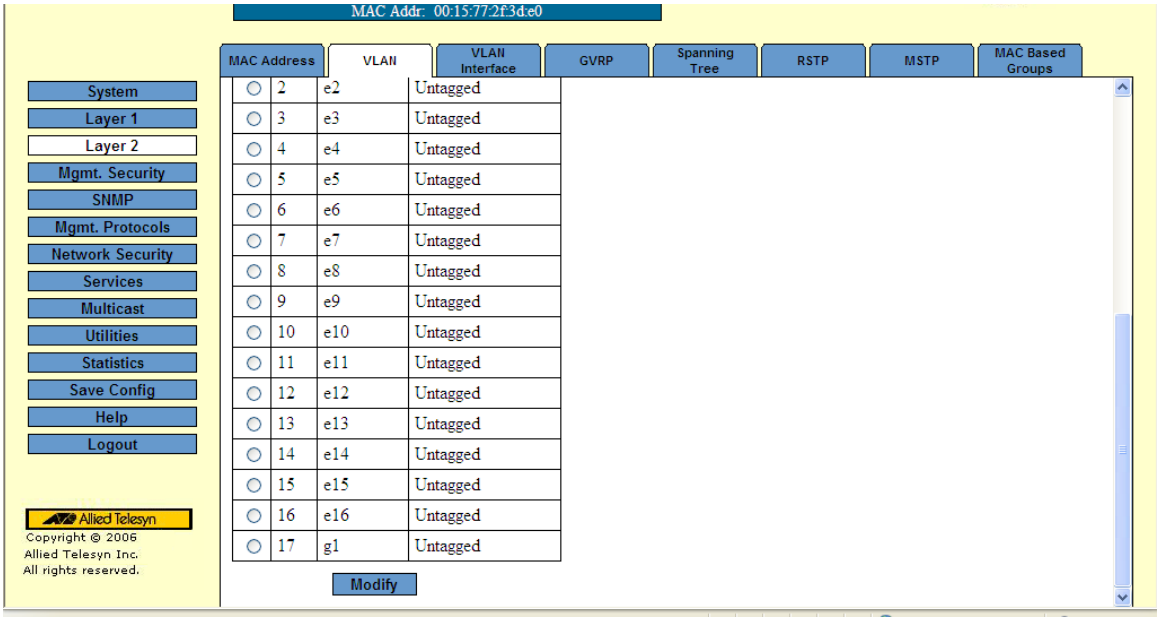

MAC Addr: 00:15:77:2f:3d:e0
Port Settings
Trunk Settings
Port Trunking
Port Mirroring
LACP
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Destination Port
e1
Source Port
Type
Status
Add
Modify
Delete

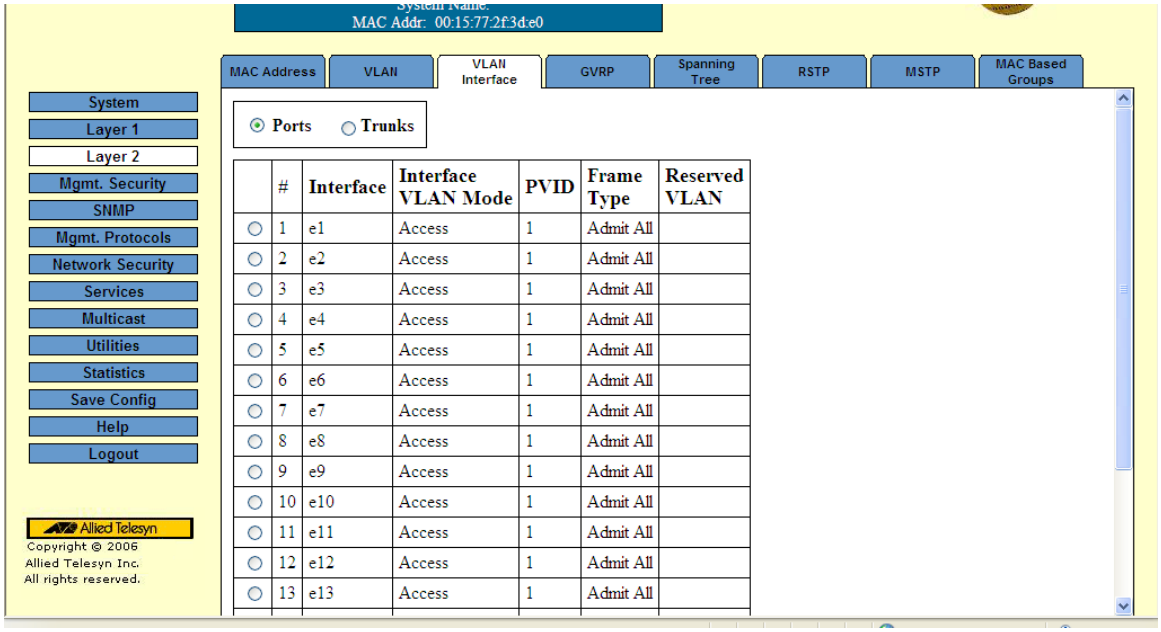

MAC Addr: 00:15:77:2f:3d:e0
Port Settings
Trunk Settings
Port Trunking
Port Mirroring
LACP
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
LACP System Priority 1
Apply
Port Port-Priority LACP Timeout
1 e1 1 Long
2 e2 1 Long
3 e3 1 Long
4 e4 1 Long
5 e5 1 Long
6 e6 1 Long
7 e7 1 Long
8 e8 1 Long
9 e9 1 Long
10 e10 1 Long
11 e11 1 Long
12 e12 1 Long

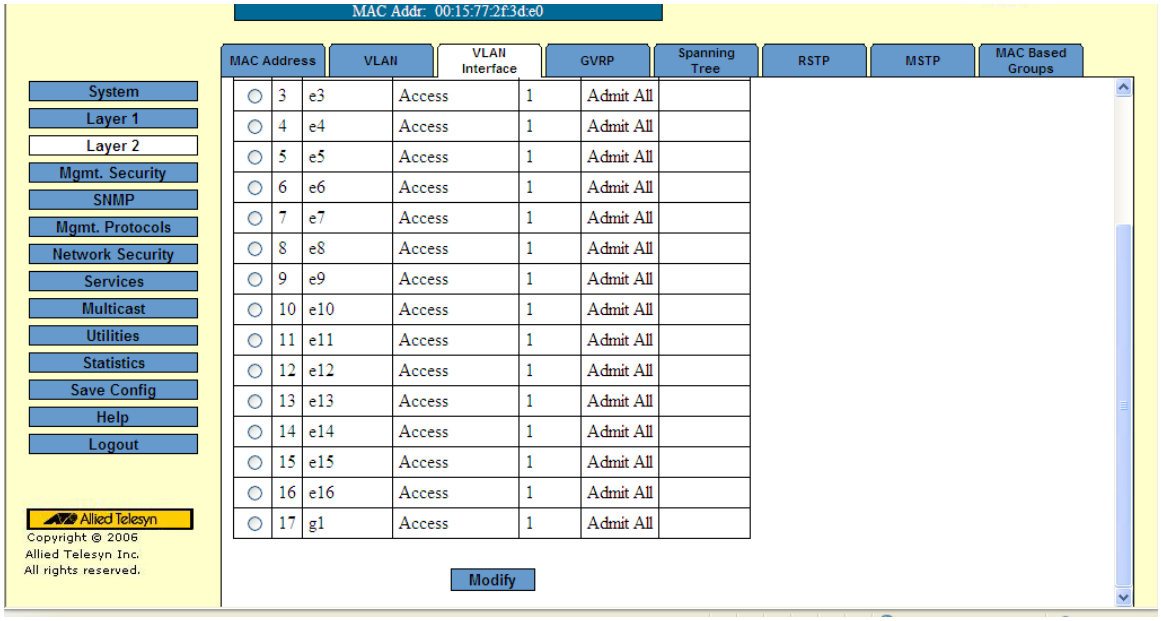

System Name:
MAC Addr: 00:15:77:2f:3d:e0
Port Settings
Trunk Settings
Port Trunking
Port Mirroring
LACP
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
2 e2 1 Long
3 e3 1 Long
4 e4 1 Long
5 e5 1 Long
6 e6 1 Long
7 e7 1 Long
8 e8 1 Long
9 e9 1 Long
10 e10 1 Long
11 e11 1 Long
12 e12 1 Long
13 e13 1 Long
14 e14 1 Long
15 e15 1 Long
16 e16 1 Long
17 g1 1 Long
Modify
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

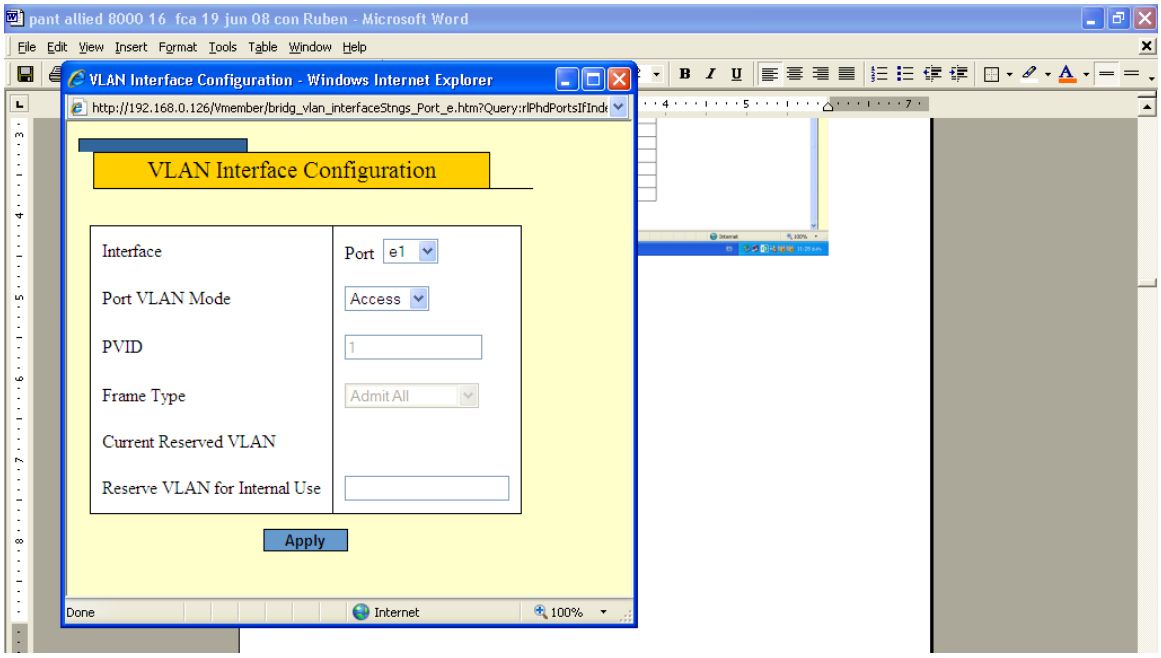

MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
View/Add Unicast MAC Addresses
View Static
View Dynamic
View MAC Addresses on Interface
Port
e1
Trunk
1
View MAC Addresses for VLAN
View MAC Address
View
Add
Delete All Dynamic MAC Addresses
Click "Delete" to Remove All
Dynamic MAC Addresses.
Delete
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

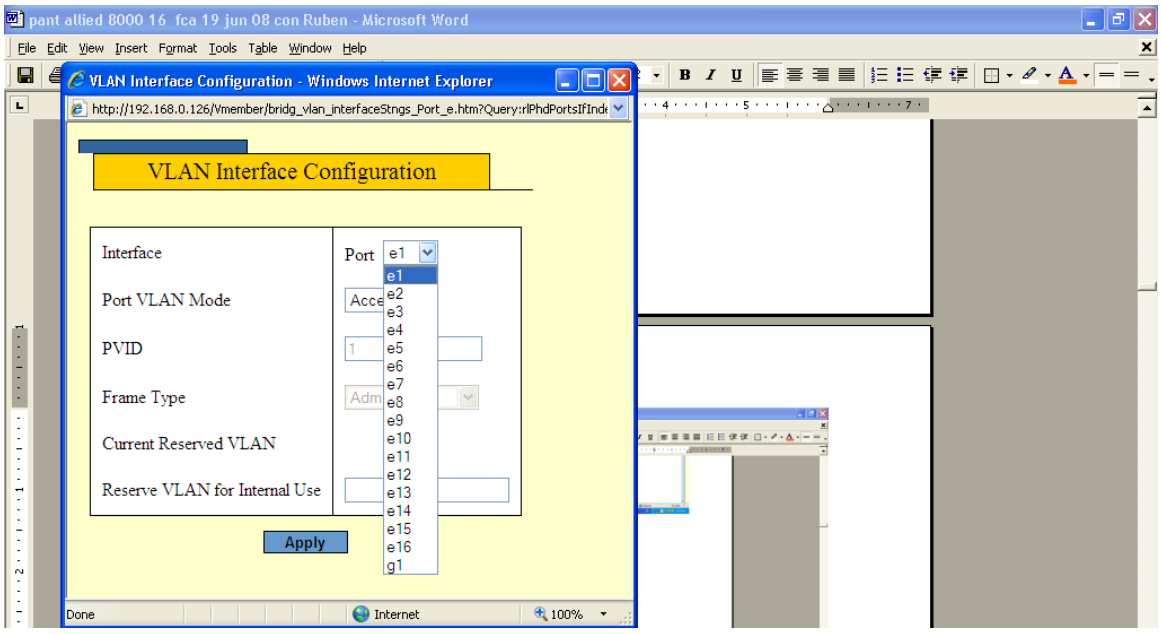

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
VLAN ID
1
VLAN Name
VLAN Type
Default
Delete VLAN
Add
Apply
Ports
Trunks
Interface Interface Status
1 e1 Untagged
2 e2 Untagged
3 e3 Untagged
4 e4 Untagged
5 e5 Untagged
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

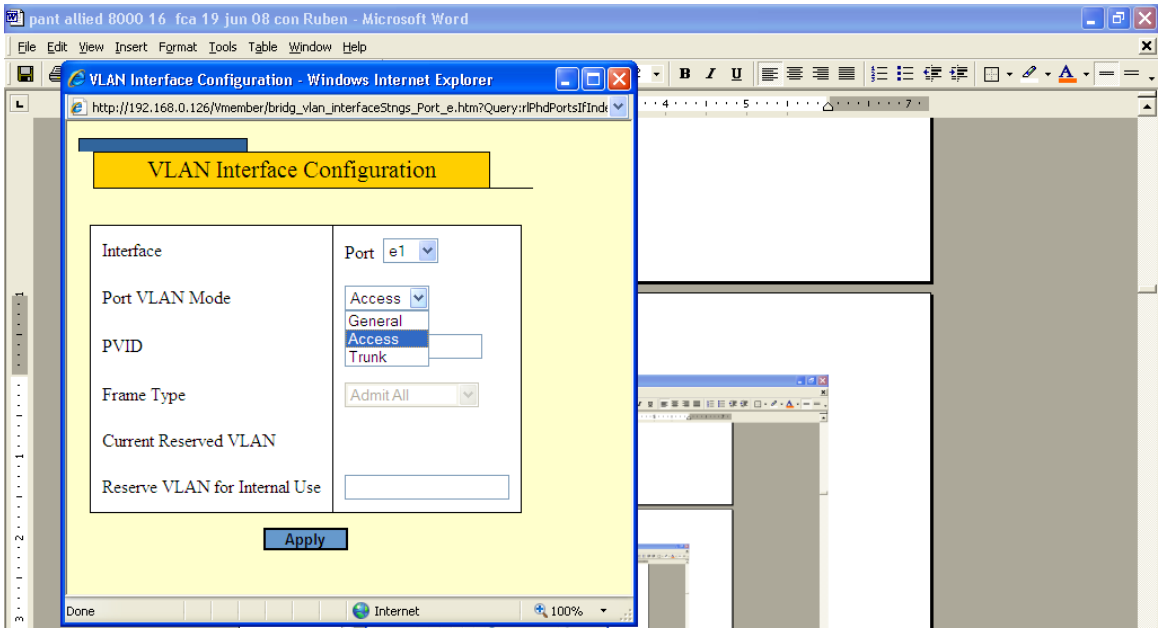

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
2 e2 Untagged
3 e3 Untagged
4 e4 Untagged
5 e5 Untagged
6 e6 Untagged
7 e7 Untagged
8 e8 Untagged
9 e9 Untagged
10 e10 Untagged
11 e11 Untagged
12 e12 Untagged
13 e13 Untagged
14 e14 Untagged
15 e15 Untagged
16 e16 Untagged
17 g1 Untagged
Modify
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

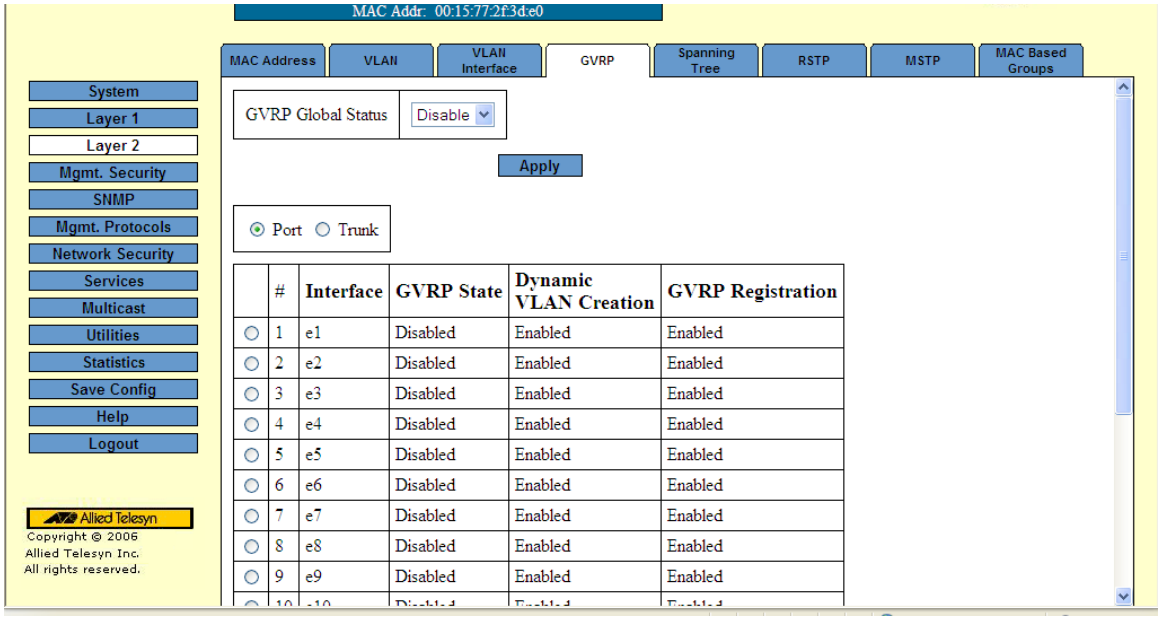

System Name:
MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Ports
Trunks
Interface Interface VLAN Mode PVID Frame Type Reserved VLAN
1 e1 Access 1 Admit All
2 e2 Access 1 Admit All
3 e3 Access 1 Admit All
4 e4 Access 1 Admit All
5 e5 Access 1 Admit All
6 e6 Access 1 Admit All
7 e7 Access 1 Admit All
8 e8 Access 1 Admit All
9 e9 Access 1 Admit All
10 e10 Access 1 Admit All
11 e11 Access 1 Admit All
12 e12 Access 1 Admit All
13 e13 Access 1 Admit All
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

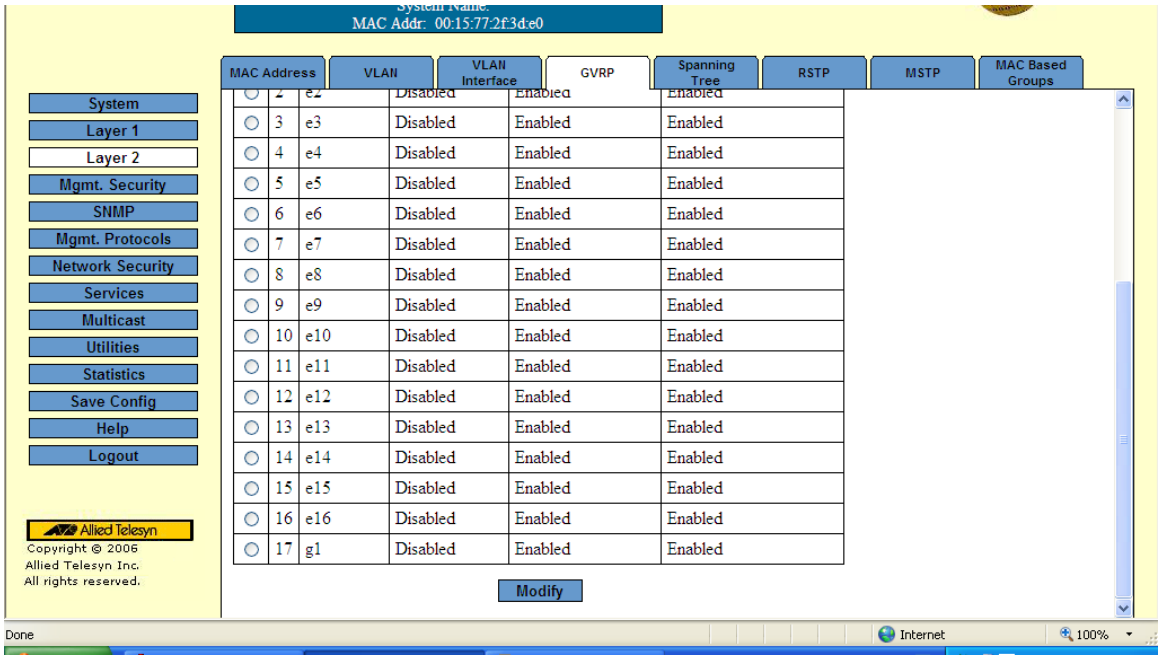

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
3 e3 Access 1 Admit All
4 e4 Access 1 Admit All
5 e5 Access 1 Admit All
6 e6 Access 1 Admit All
7 e7 Access 1 Admit All
8 e8 Access 1 Admit All
9 e9 Access 1 Admit All
10 e10 Access 1 Admit All
11 e11 Access 1 Admit All
12 e12 Access 1 Admit All
13 e13 Access 1 Admit All
14 e14 Access 1 Admit All
15 e15 Access 1 Admit All
16 e16 Access 1 Admit All
17 g1 Access 1 Admit All
Modify
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

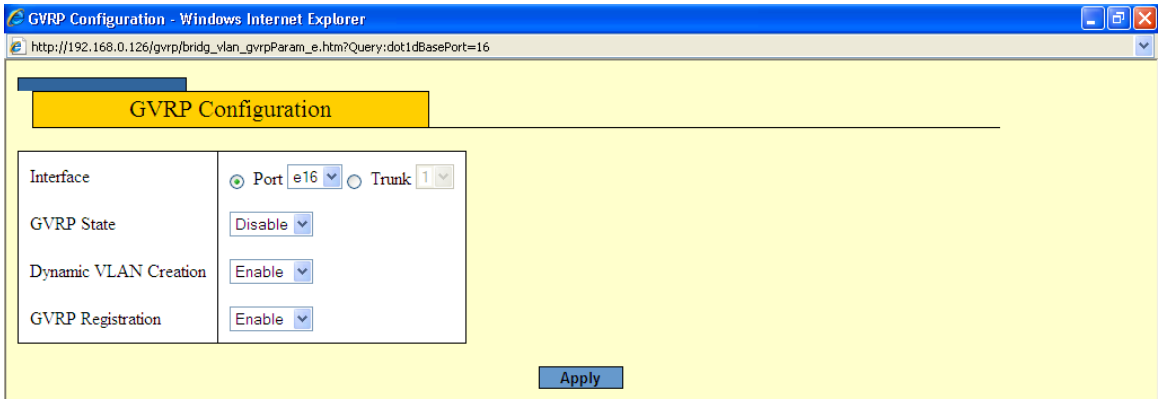

pant allied 8000 16 fca 19 jun 08 con Ruben - Microsoft Word
File Edit View Insert Format Tools Table Window Help
VLAN Interface Configuration - Windows Internet Explorer
http://192.168.0.126/Vmember/bridg_vlan_interfaceStngs_Port_e.htm?Query:rlPhdPortsIfInd
VLAN Interface Configuration
Interface
Port e1
Port VLAN Mode
Access
PVID
1
Frame Type
Admit All
Current Reserved VLAN
Reserve VLAN for Internal Use
Apply
Done
Internet
100%

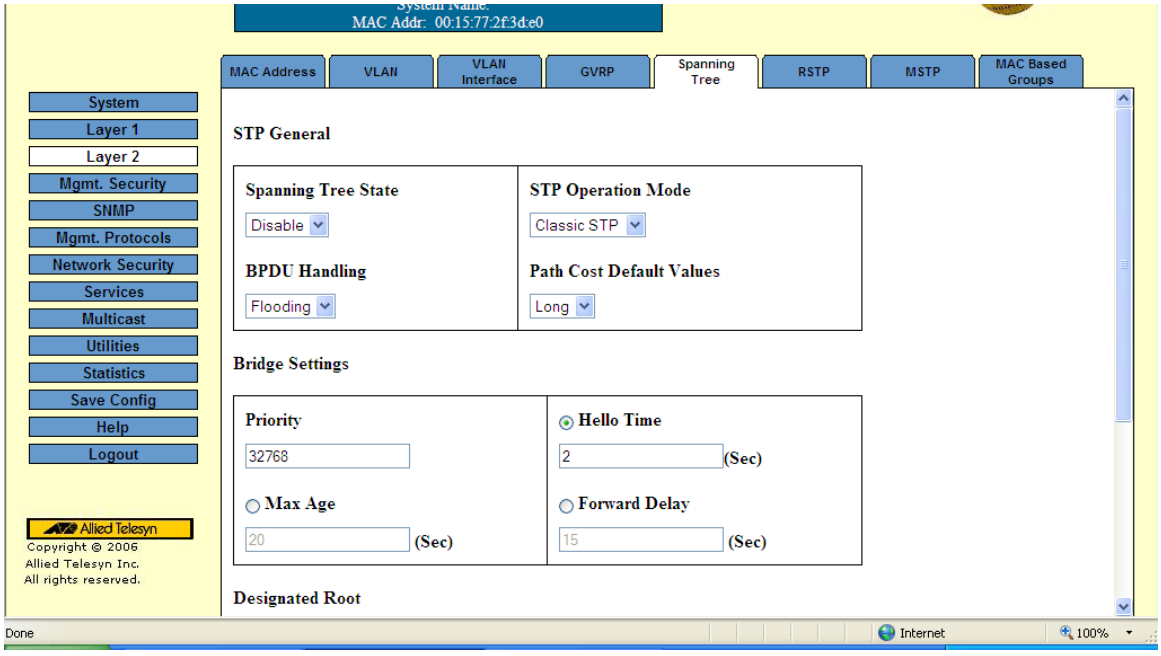

pant allied 8000 16 fca 19 jun 08 con Ruben - Microsoft Word
File Edit View Insert Format Tools Table Window Help
VLAN Interface Configuration - Windows Internet Explorer
http://192.168.0.126/Vmember/bridg_vlan_interfaceStngs_Port_e.htm?Query:rlPhdPortsIfInd
VLAN Interface Configuration
Interface
Port e1
Port VLAN Mode
PVID
Frame Type
Current Reserved VLAN
Reserve VLAN for Internal Use
Apply
e1
e2
e3
e4
e5
e6
e7
e8
e9
e10
e11
e12
e13
e14
e15
e16
g1
Done
Internet
100%

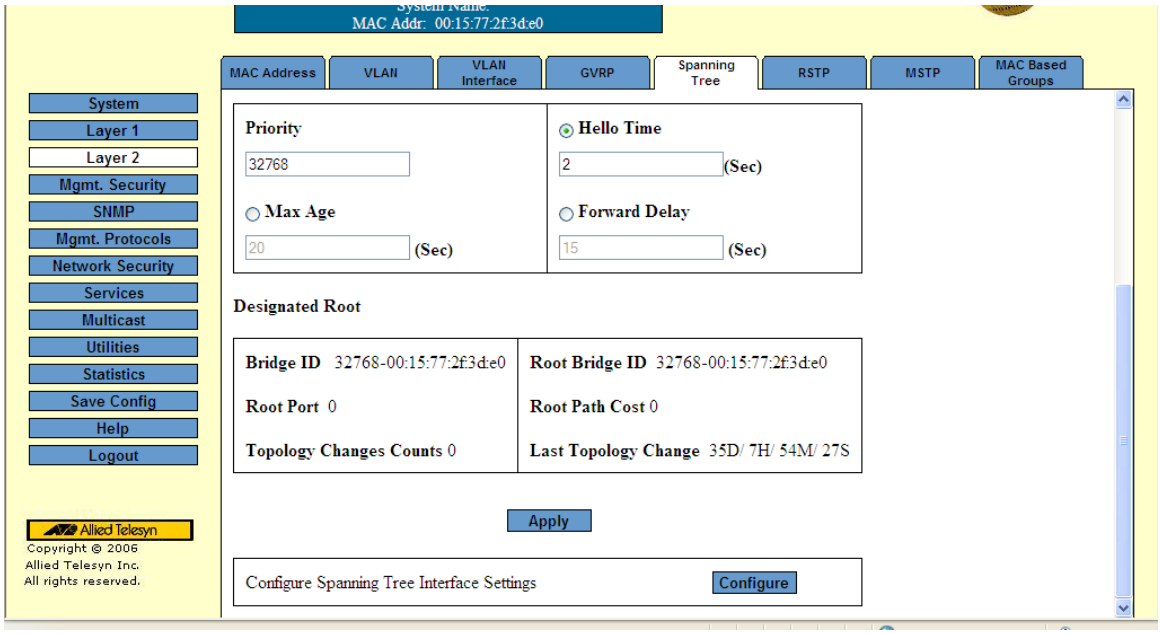

pant allied 8000 16 fca 19 jun 08 con Ruben - Microsoft Word
File Edit View Insert Format Tools Table Window Help
VLAN Interface Configuration - Windows Internet Explorer
http://192.168.0.126/Vmember/bridg_vlan_interfaceStngs_Port_e.htm?Query:rlPhdPortsIfInd
VLAN Interface Configuration
Interface
Port e1
Port VLAN Mode
Access
General
Access
Trunk
PVID
Frame Type
Admit All
Current Reserved VLAN
Reserve VLAN for Internal Use
Apply
Done
Internet
100%

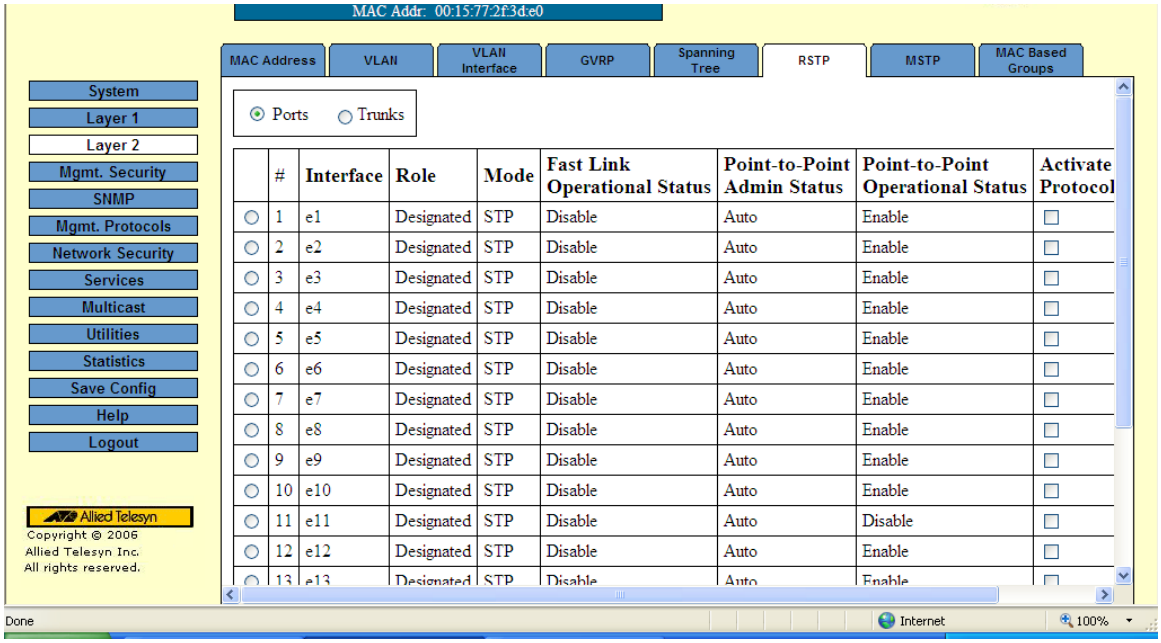

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
GVRP Global Status
Disable
Apply
Port
Trunk
Interface GVRP State Dynamic VLAN Creation GVRP Registration
1 e1 Disabled Enabled Enabled
2 e2 Disabled Enabled Enabled
3 e3 Disabled Enabled Enabled
4 e4 Disabled Enabled Enabled
5 e5 Disabled Enabled Enabled
6 e6 Disabled Enabled Enabled
7 e7 Disabled Enabled Enabled
8 e8 Disabled Enabled Enabled
9 e9 Disabled Enabled Enabled
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

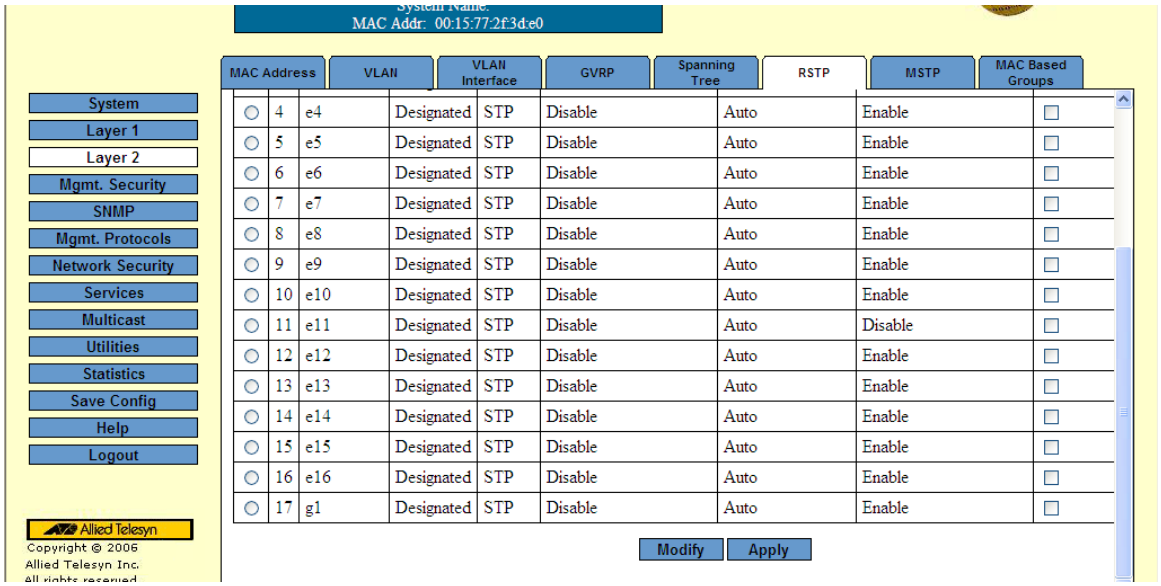

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
3 e3 Disabled Enabled Enabled
4 e4 Disabled Enabled Enabled
5 e5 Disabled Enabled Enabled
6 e6 Disabled Enabled Enabled
7 e7 Disabled Enabled Enabled
8 e8 Disabled Enabled Enabled
9 e9 Disabled Enabled Enabled
10 e10 Disabled Enabled Enabled
11 e11 Disabled Enabled Enabled
12 e12 Disabled Enabled Enabled
13 e13 Disabled Enabled Enabled
14 e14 Disabled Enabled Enabled
15 e15 Disabled Enabled Enabled
16 e16 Disabled Enabled Enabled
17 g1 Disabled Enabled Enabled
Modify
Done
Internet
100%

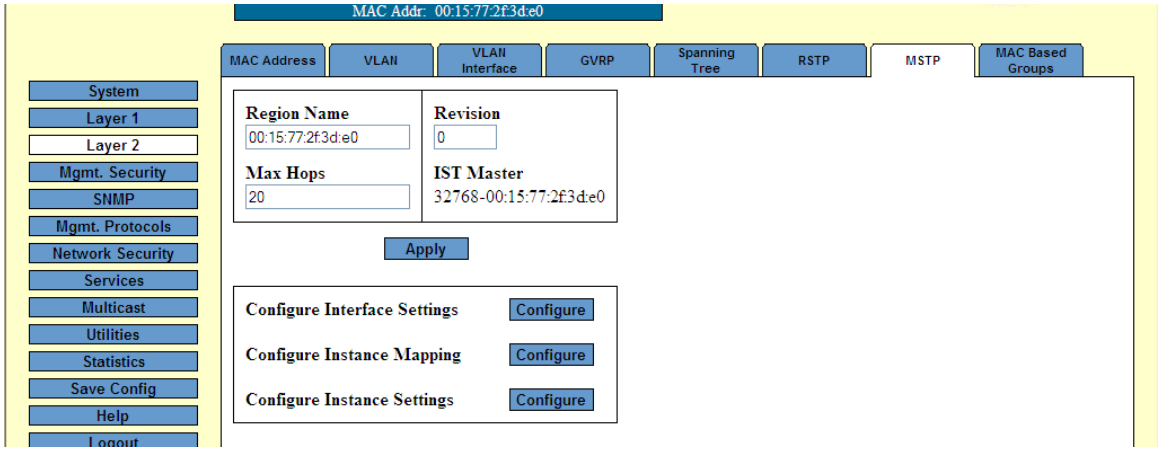

GVRP Configuration - Windows Internet Explorer
http://192.168.0.126/gvrp/bridg_vlan_gvrpParam_e.htm?Query:dot1dBasePort=16
GVRP Configuration
Interface
Port e16
Trunk 1
GVRP State
Disable
Dynamic VLAN Creation
Enable
GVRP Registration
Enable
Apply

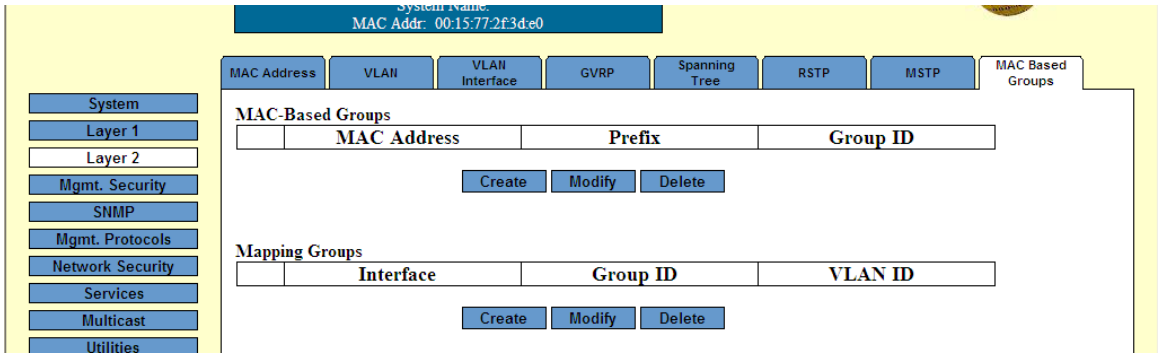

System Name:
MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
STP General
Spanning Tree State
Disable
STP Operation Mode
Classic STP
BPDU Handling
Flooding
Path Cost Default Values
Long
Bridge Settings
Priority
32768
Hello Time
2
(Sec)
Max Age
20
(Sec)
Forward Delay
15
(Sec)
Designated Root
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
Done
Internet
100%

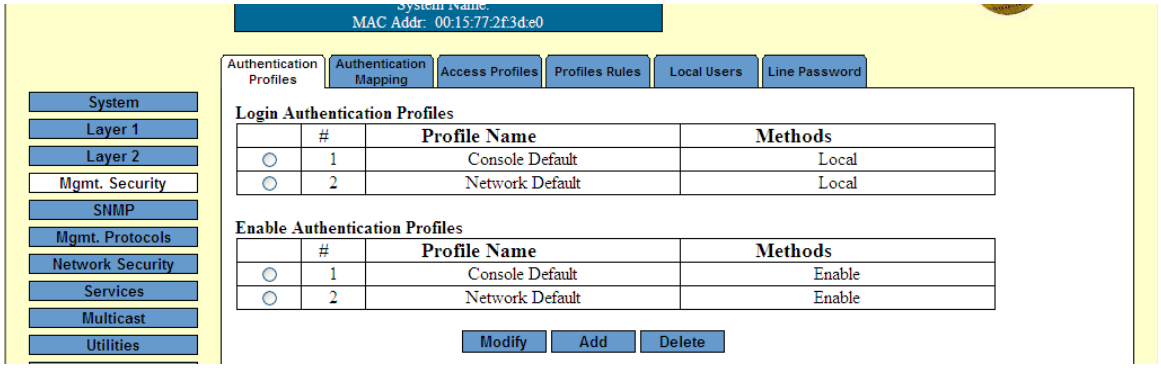

System Name:
MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Priority
32768
Hello Time
2
(Sec)
Max Age
20
(Sec)
Forward Delay
15
(Sec)
Designated Root
Bridge ID 32768-00:15:77:2f:3d:e0
Root Bridge ID 32768-00:15:77:2f:3d:e0
Root Port 0
Root Path Cost 0
Topology Changes Counts 0
Last Topology Change 35D/ 7H/ 54M/ 27S
Apply
Configure Spanning Tree Interface Settings
Configure
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

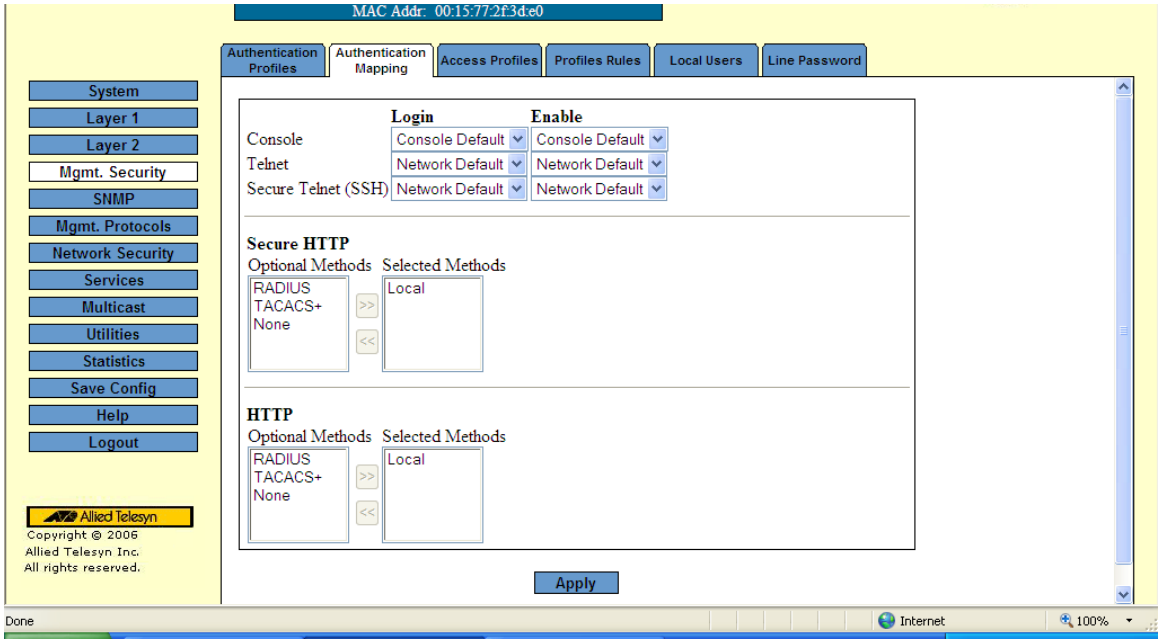

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Ports
Trunks
Interface Role Mode Fast Link Operational Status Point-to-Point Admin Status Point-to-Point Operational Status Activate Protocol
1 e1 Designated STP Disable Auto Enable
2 e2 Designated STP Disable Auto Enable
3 e3 Designated STP Disable Auto Enable
4 e4 Designated STP Disable Auto Enable
5 e5 Designated STP Disable Auto Enable
6 e6 Designated STP Disable Auto Enable
7 e7 Designated STP Disable Auto Enable
8 e8 Designated STP Disable Auto Enable
9 e9 Designated STP Disable Auto Enable
10 e10 Designated STP Disable Auto Enable
11 e11 Designated STP Disable Auto Disable
12 e12 Designated STP Disable Auto Enable
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
Done
Internet
100%

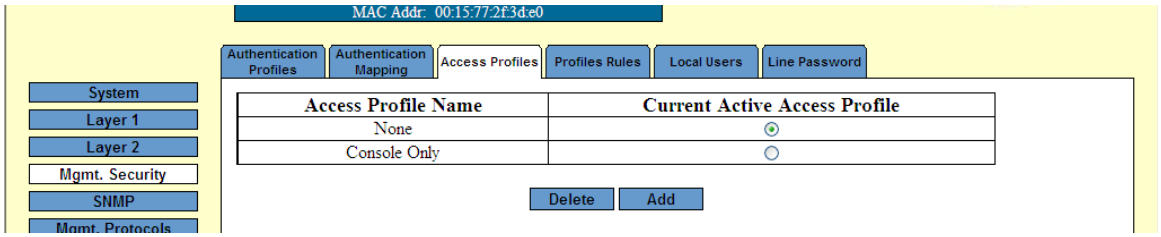

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
4 e4 Designated STP Disable Auto Enable
5 e5 Designated STP Disable Auto Enable
6 e6 Designated STP Disable Auto Enable
7 e7 Designated STP Disable Auto Enable
8 e8 Designated STP Disable Auto Enable
9 e9 Designated STP Disable Auto Enable
10 e10 Designated STP Disable Auto Enable
11 e11 Designated STP Disable Auto Disable
12 e12 Designated STP Disable Auto Enable
13 e13 Designated STP Disable Auto Enable
14 e14 Designated STP Disable Auto Enable
15 e15 Designated STP Disable Auto Enable
16 e16 Designated STP Disable Auto Enable
17 g1 Designated STP Disable Auto Enable
Modify
Apply
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.

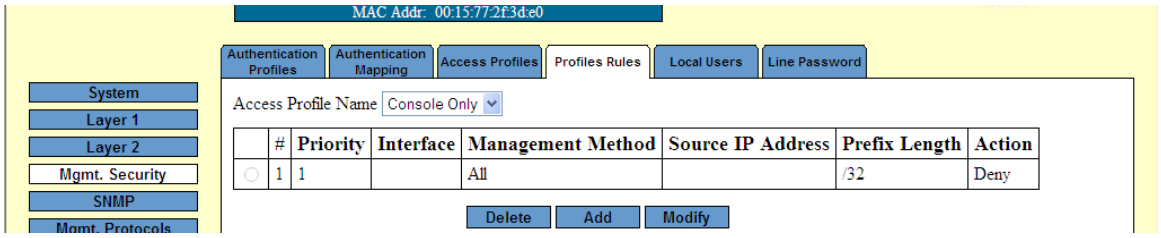

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Region Name
00:15:77:2f:3d:e0
Revision
0
Max Hops
20
IST Master
32768-00:15:77:2f:3d:e0
Apply
Configure Interface Settings
Configure
Configure Instance Mapping
Configure
Configure Instance Settings
Configure

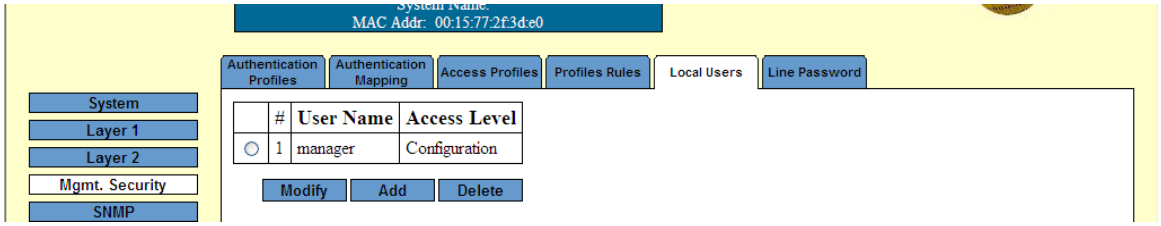

MAC Addr: 00:15:77:2f:3d:e0
MAC Address
VLAN
VLAN Interface
GVRP
Spanning Tree
RSTP
MSTP
MAC Based Groups
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
MAC-Based Groups
MAC Address
Prefix
Group ID
Create
Modify
Delete
Mapping Groups
Interface
Group ID
VLAN ID
Create
Modify
Delete

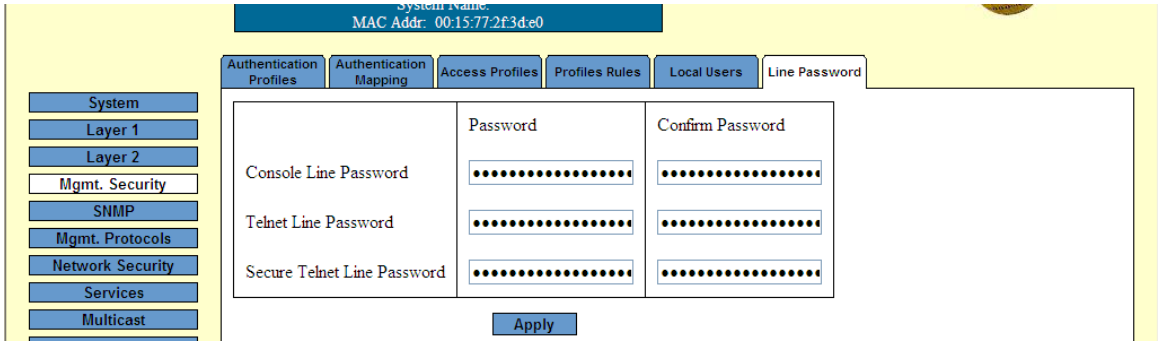

MAC Addr: 00:15:77:2f:3d:e0
Authentication Profiles
Authentication Mapping
Access Profiles
Profiles Rules
Local Users
Line Password
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Login Authentication Profiles
#
Profile Name
Methods
1
Console Default
Local
2
Network Default
Local
Enable Authentication Profiles
#
Profile Name
Methods
1
Console Default
Enable
2
Network Default
Enable
Modify
Add
Delete

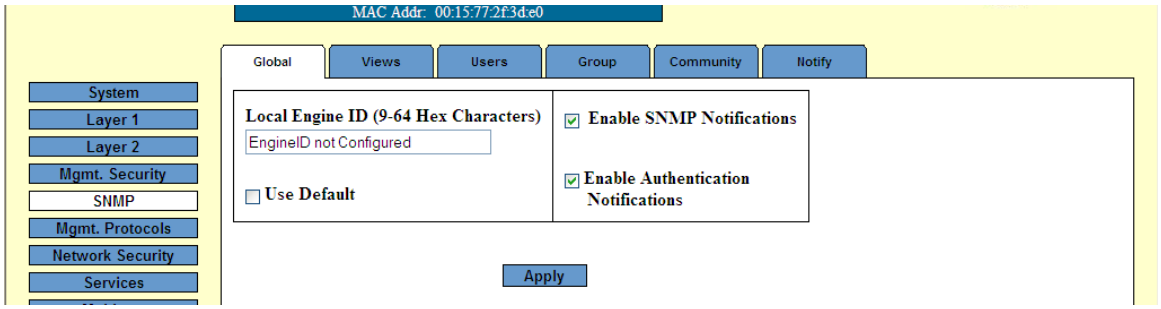

MAC Addr: 00:15:77:2f:3d:e0
Authentication Profiles
Authentication Mapping
Access Profiles
Profiles Rules
Local Users
Line Password
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Login
Enable
Console
Telnet
Secure Telnet (SSH)
Console Default
Network Default
Secure HTTP
Optional Methods
Selected Methods
RADIUS
TACACS+
None
Local
HTTP
Apply
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
Done
Internet
100%

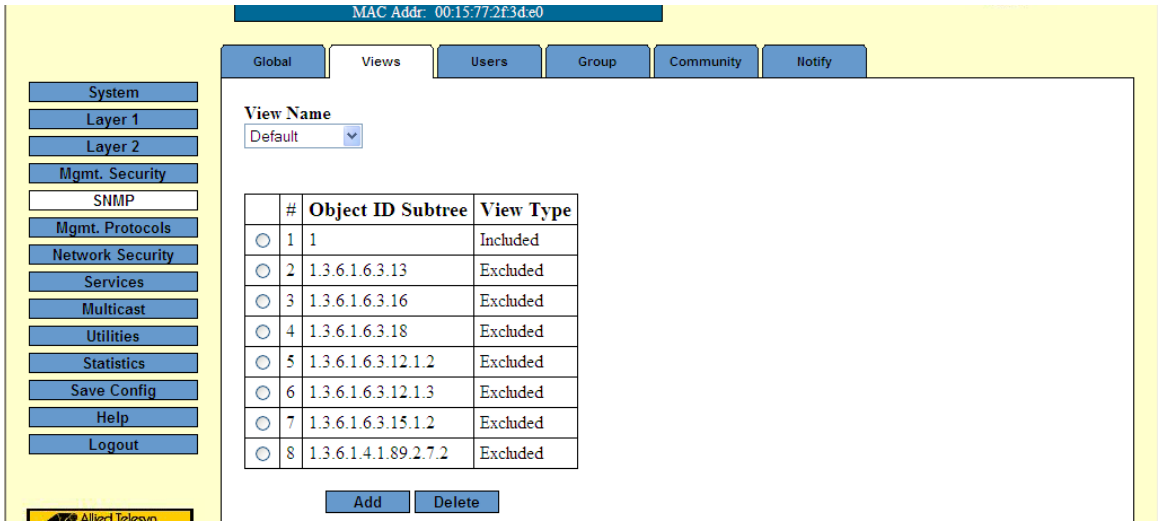

MAC Addr: 00:15:77:2f:3d:e0
Authentication Profiles
Authentication Mapping
Access Profiles
Profiles Rules
Local Users
Line Password
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Access Profile Name
Current Active Access Profile
None
Console Only
Delete
Add

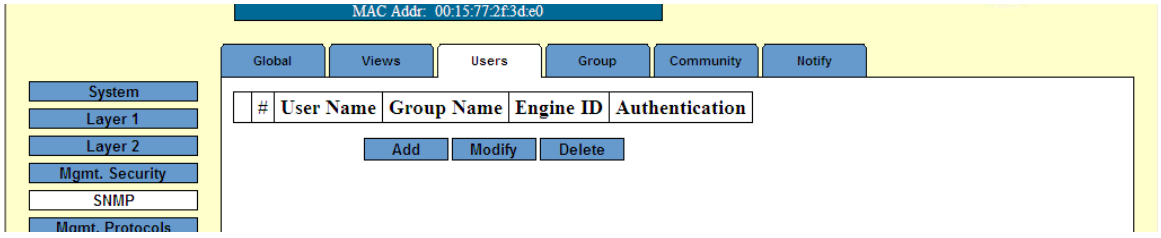

MAC Addr: 00:15:77:2f:3d:e0
Authentication Profiles
Authentication Mapping
Access Profiles
Profiles Rules
Local Users
Line Password
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Access Profile Name
Console Only
#
Priority
Interface
Management Method
Source IP Address
Prefix Length
Action
1
1
All
/32
Deny
Delete
Add
Modify

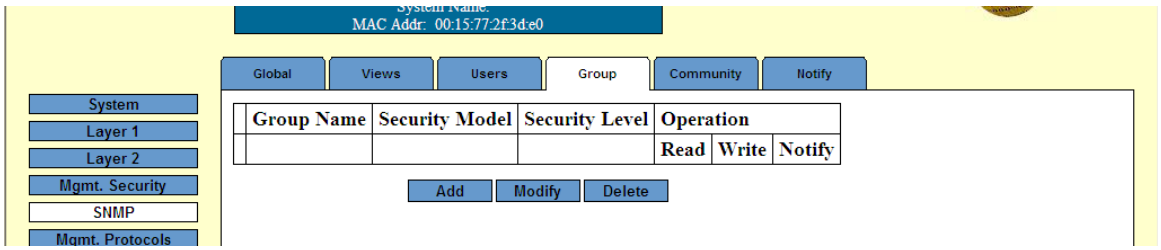

MAC Addr: 00:15:77:2f:3d:e0
Authentication Profiles
Authentication Mapping
Access Profiles
Profiles Rules
Local Users
Line Password
System
Layer 1
Layer 2
Mgmt. Security
SNMP
#
User Name
Access Level
1
manager
Configuration
Modify
Add
Delete

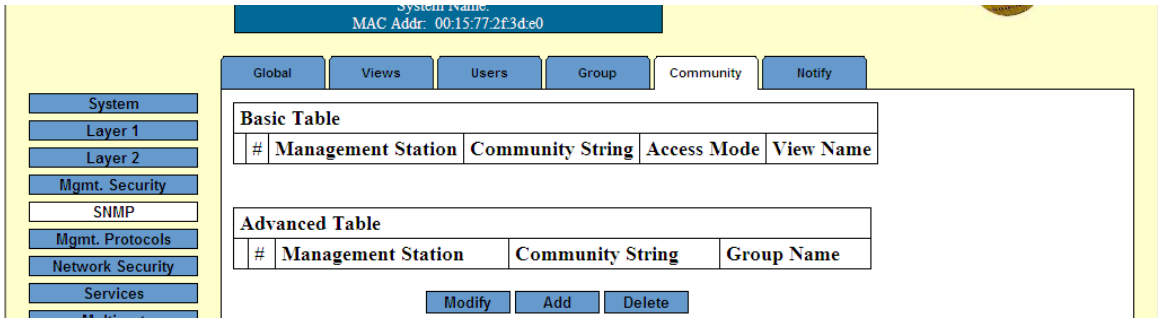

MAC Addr: 00:15:77:2f:3d:e0
Authentication Profiles
Authentication Mapping
Access Profiles
Profiles Rules
Local Users
Line Password
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Password
Confirm Password
Console Line Password
Telnet Line Password
Secure Telnet Line Password
Apply

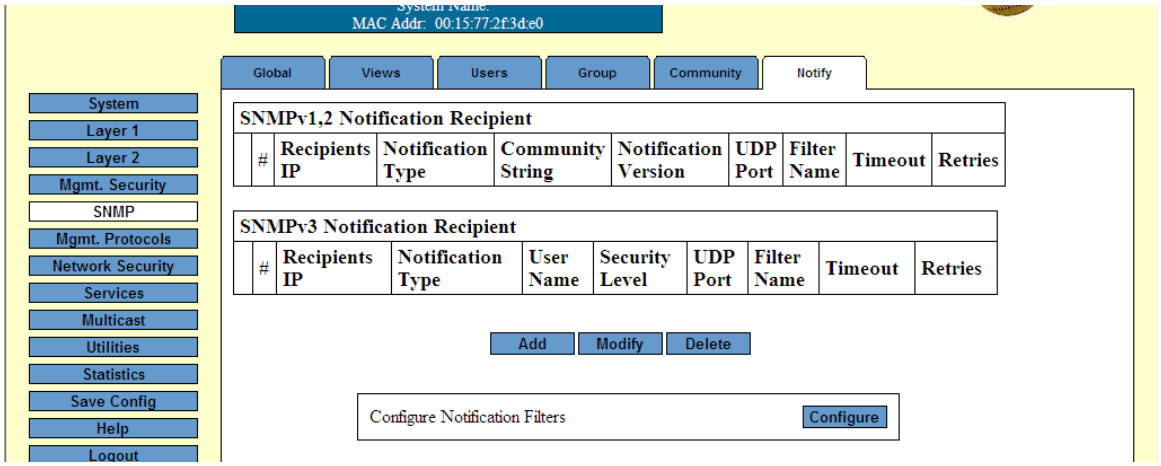

MAC Addr: 00:15:77:2f:3d:e0
Global
Views
Users
Group
Community
Notify
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Local Engine ID (9-64 Hex Characters)
EngineID not Configured
Use Default
Enable SNMP Notifications
Enable Authentication Notifications
Apply

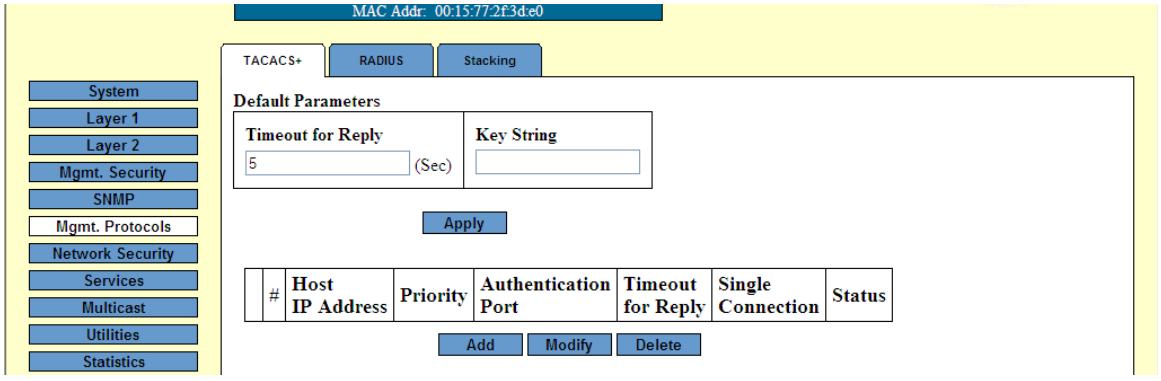

MAC Addr: 00:15:77:2f:3d:e0
Global
Views
Users
Group
Community
Notify
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
View Name
Default
Object ID Subtree View Type
1 1 Included
2 1.3.6.1.6.3.13 Excluded
3 1.3.6.1.6.3.16 Excluded
4 1.3.6.1.6.3.18 Excluded
5 1.3.6.1.6.3.12.1.2 Excluded
6 1.3.6.1.6.3.12.1.3 Excluded
7 1.3.6.1.6.3.15.1.2 Excluded
8 1.3.6.1.4.1.89.2.7.2 Excluded
Add
Delete

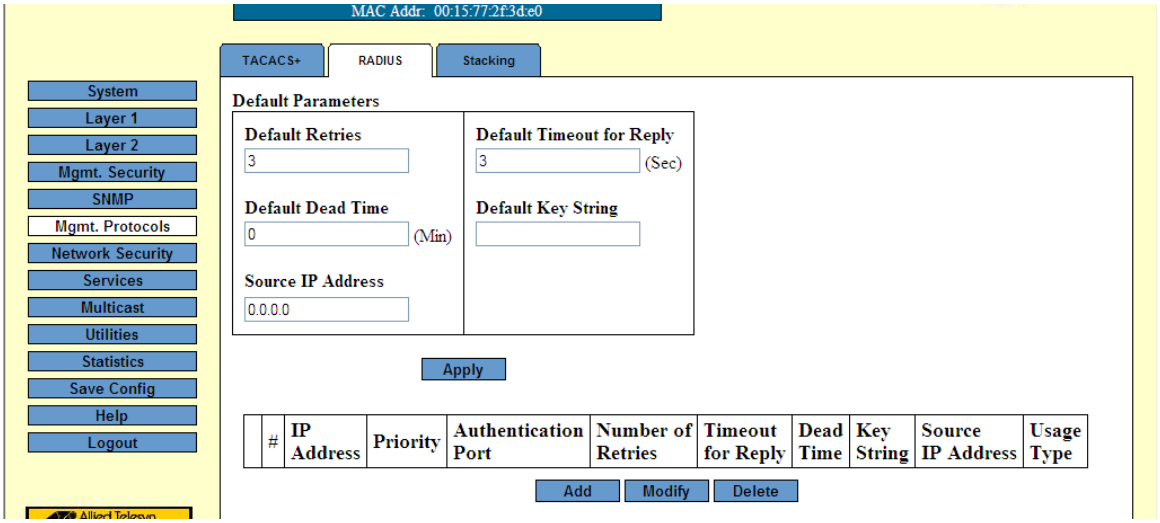

MAC Addr: 00:15:77:2f:3d:e0
Global
Views
Users
Group
Community
Notify
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
User Name Group Name Engine ID Authentication
Add
Modify
Delete

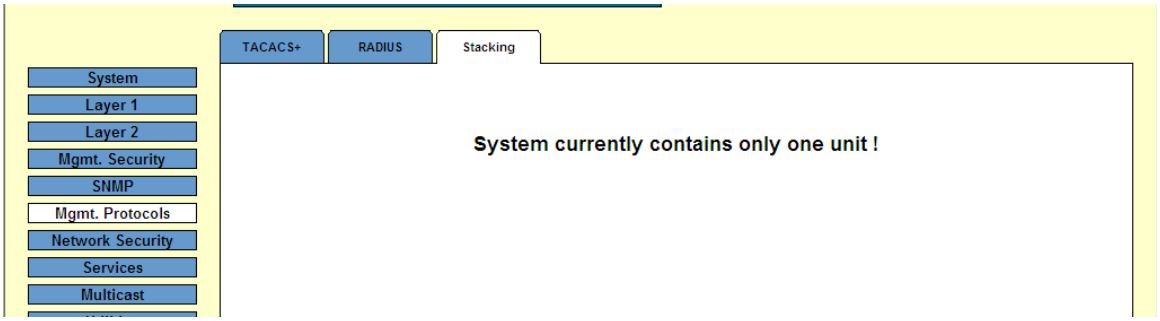

MAC Addr: 00:15:77:2f:3d:e0
Global
Views
Users
Group
Community
Notify
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Group Name
Security Model
Security Level
Operation
Read
Write
Notify
Add
Modify
Delete

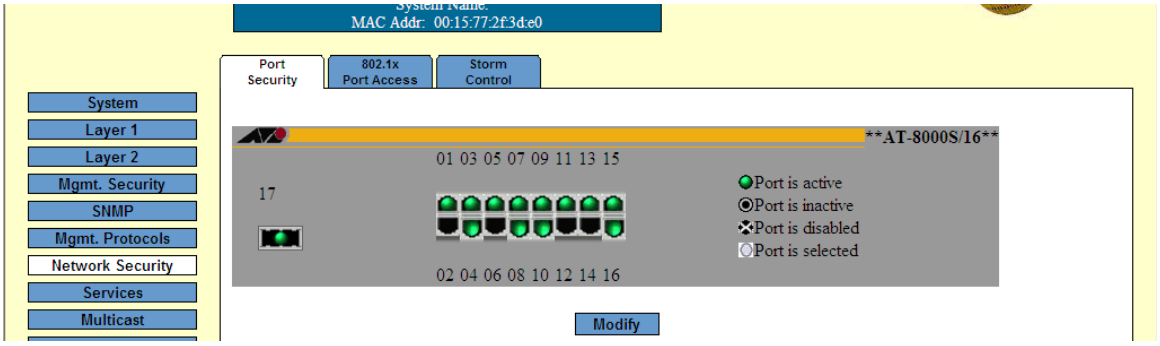

MAC Addr: 00:15:77:2f:3d:e0
Global
Views
Users
Group
Community
Notify
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Basic Table
#
Management Station
Community String
Access Mode
View Name
Advanced Table
#
Management Station
Community String
Group Name
Modify
Add
Delete

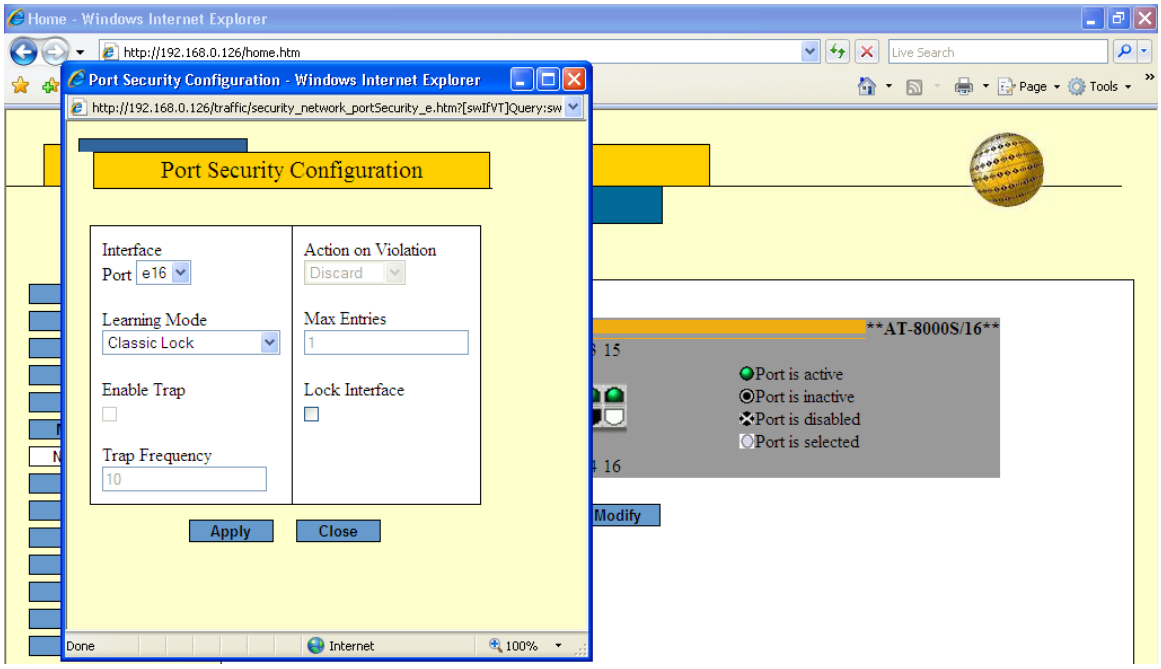

MAC Addr: 00:15:77:2f:3d:e0
Global
Views
Users
Group
Community
Notify
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
SNMPv1,2 Notification Recipient
#
Recipients IP
Notification Type
Community String
Notification Version
UDP Port
Filter Name
Timeout
Retries
SNMPv3 Notification Recipient
#
Recipients IP
Notification Type
User Name
Security Level
UDP Port
Filter Name
Timeout
Retries
Add
Modify
Delete
Configure Notification Filters
Configure

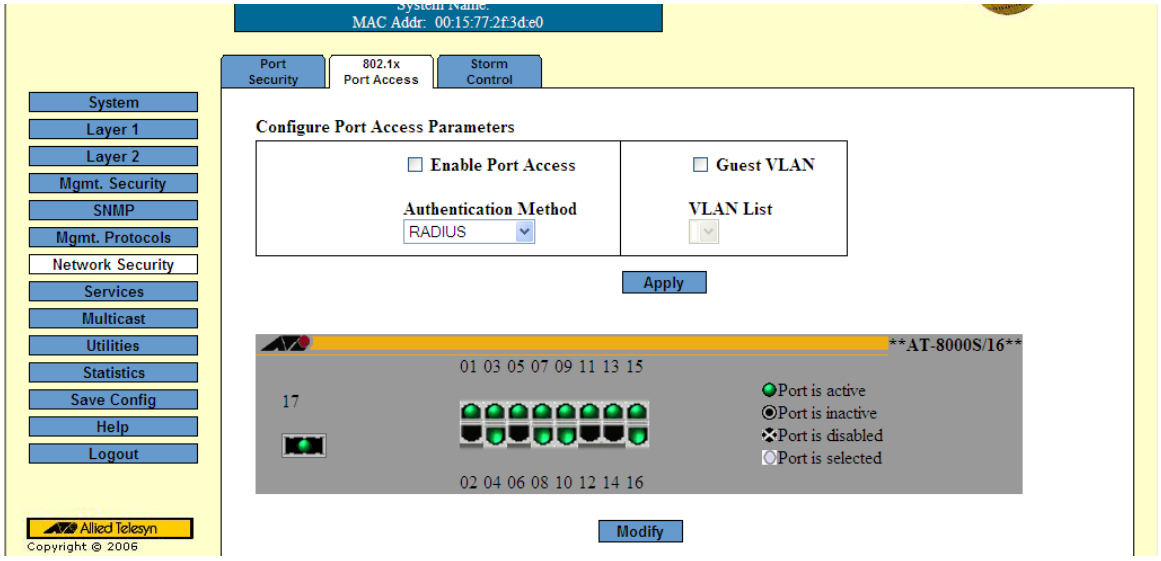

MAC Addr: 00:15:77:2f:3d:e0
TACACS+
RADIUS
Stacking
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Default Parameters
Timeout for Reply
5
(Sec)
Key String
Apply
#
Host IP Address
Priority
Authentication Port
Timeout for Reply
Single Connection
Status
Add
Modify
Delete

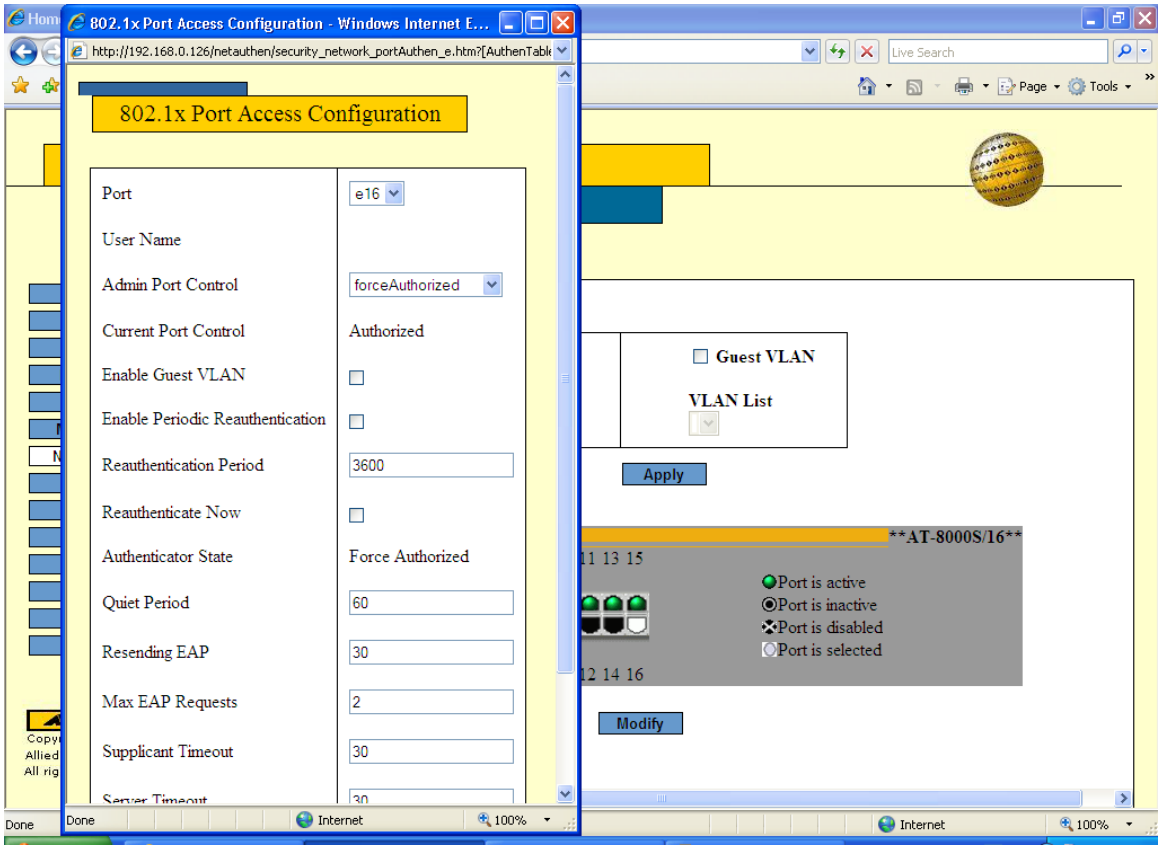

MAC Addr: 00:15:77:2f:3d:e0
TACACS+
RADIUS
Stacking
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Default Parameters
Default Retries
3
Default Timeout for Reply
3
(Sec)
Default Dead Time
0
(Min)
Default Key String
Source IP Address
0.0.0.0
Apply
#
IP Address
Priority
Authentication Port
Number of Retries
Timeout for Reply
Dead Time
Key String
Source IP Address
Usage Type
Add
Modify
Delete

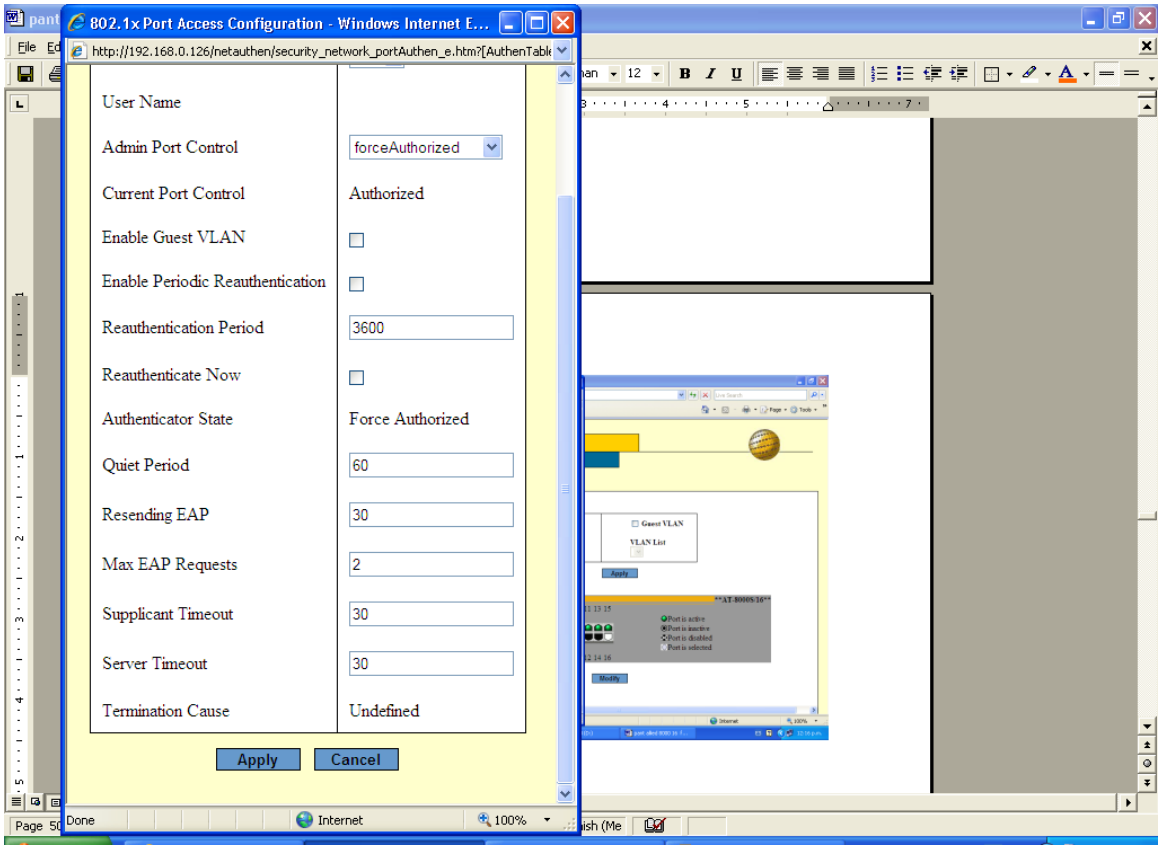

TACACS+
RADIUS
Stacking
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
System currently contains only one unit !

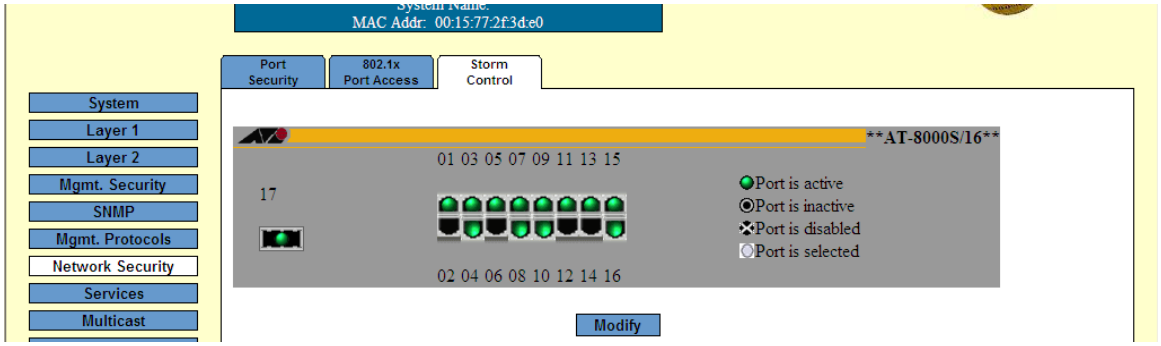

MAC Addr: 00:15:77:2f:3d:e0
Port Security
802.1x Port Access
Storm Control
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
AT-8000S/16
01 03 05 07 09 11 13 15
17
02 04 06 08 10 12 14 16
Port is active
Port is inactive
Port is disabled
Port is selected
Modify

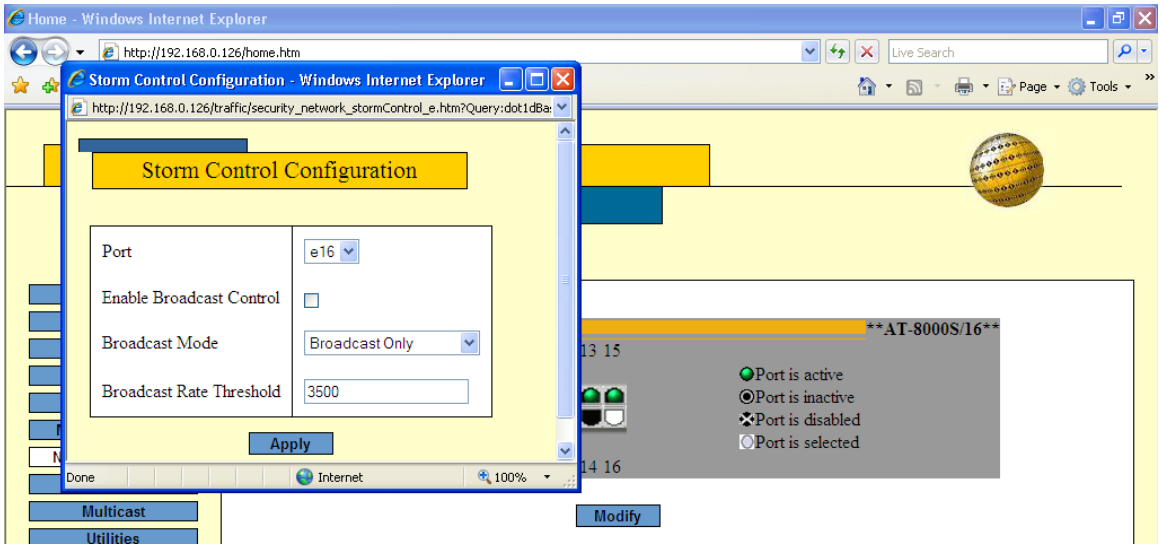

Home - Windows Internet Explorer
http://192.168.0.126/home.htm
Live Search
Page
Tools
Port Security Configuration - Windows Internet Explorer
http://192.168.0.126/traffic/security_network_portSecurity_e.htm?[swIfVT]Query:sw
Port Security Configuration
Interface
Port e16
Action on Violation
Discard
Learning Mode
Classic Lock
Max Entries
1
Enable Trap
Lock Interface
Trap Frequency
10
Apply
Close
Done
Internet
100%
AT-8000S/16
15
16
Port is active
Port is inactive
Port is disabled
Port is selected
Modify

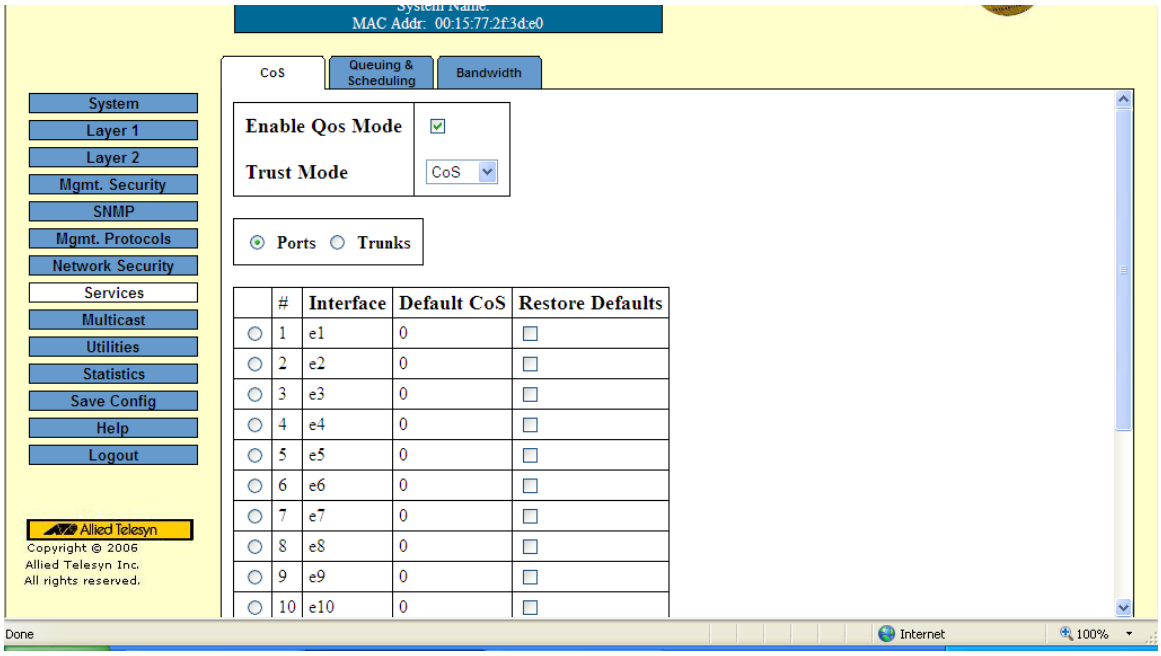

MAC Addr: 00:15:77:2f:3d:e0
Port Security
802.1x Port Access
Storm Control
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Allied Telesyn
Copyright © 2006
Configure Port Access Parameters
Enable Port Access
Guest VLAN
Authentication Method
RADIUS
VLAN List
Apply
AT-8000S/16
01 03 05 07 09 11 13 15
17
02 04 06 08 10 12 14 16
Port is active
Port is inactive
Port is disabled
Port is selected
Modify

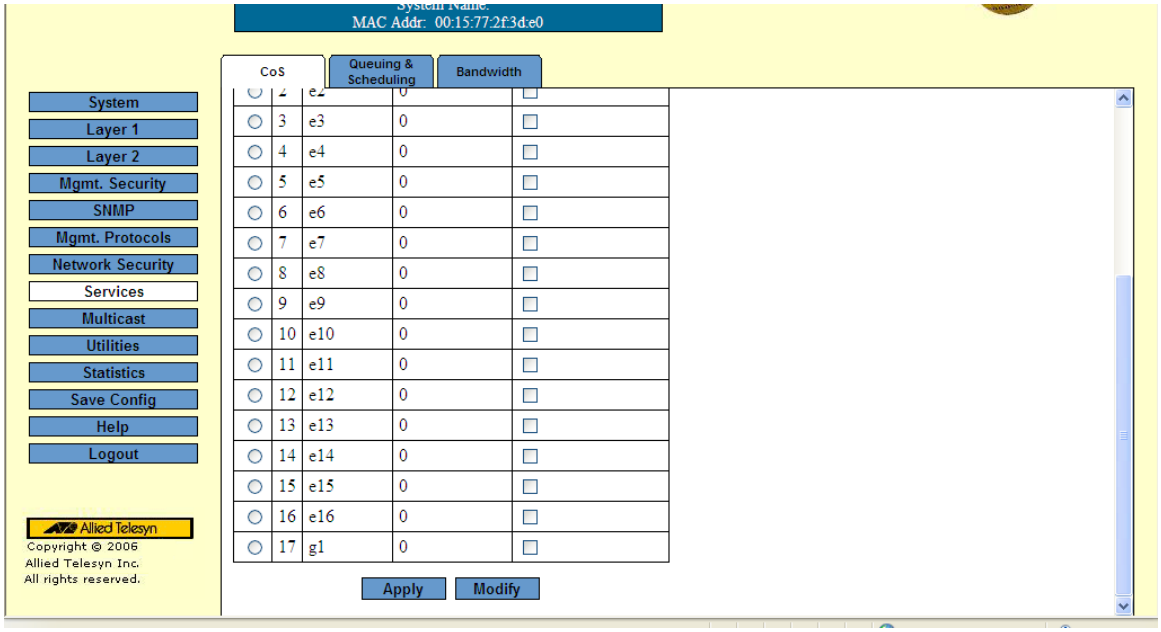

802.1x Port Access Configuration - Windows Internet E...
http://192.168.0.126/netauthen/security_network_portAuthen_e.htm?[AuthenTable
802.1x Port Access Configuration
Port
e16
User Name
Admin Port Control
forceAuthorized
Current Port Control
Authorized
Enable Guest VLAN
Enable Periodic Reauthentication
Reauthentication Period
3600
Reauthenticate Now
Authenticator State
Force Authorized
Quiet Period
60
Resending EAP
30
Max EAP Requests
2
Supplicant Timeout
30
Server Timeout
30
Done
Internet
100%
Guest VLAN
VLAN List
Apply
AT-8000S/16
11 13 15
12 14 16
Port is active
Port is inactive
Port is disabled
Port is selected
Modify
Live Search
Page
Tools

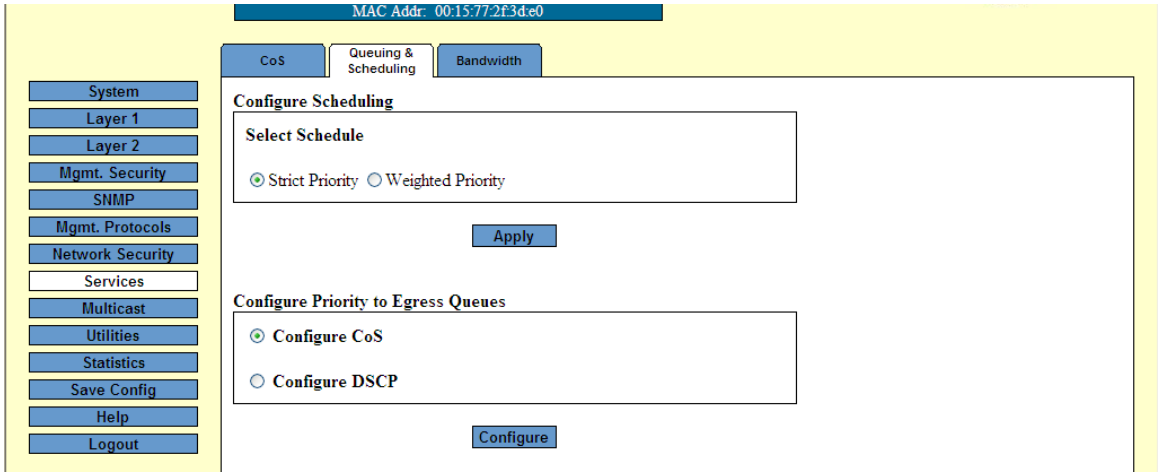

802.1x Port Access Configuration - Windows Internet E...
http://192.168.0.126/netauthen/security_network_portAuthen_e.htm?[AuthenTable
User Name
Admin Port Control
forceAuthorized
Current Port Control
Authorized
Enable Guest VLAN
Enable Periodic Reauthentication
Reauthentication Period
3600
Reauthenticate Now
Authenticator State
Force Authorized
Quiet Period
60
Resending EAP
30
Max EAP Requests
2
Supplicant Timeout
30
Server Timeout
30
Termination Cause
Undefined
Apply
Cancel
Done
Internet
100%

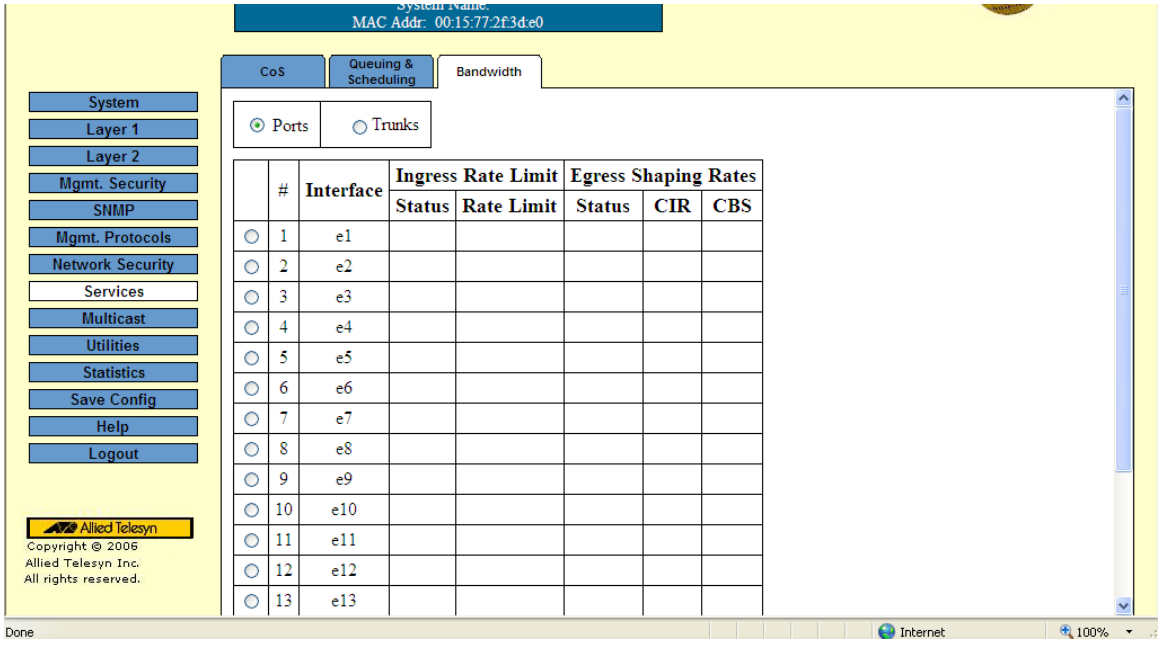

MAC Addr: 00:15:77:2f:3d:e0
Port Security
802.1x Port Access
Storm Control
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
AT-8000S/16
01 03 05 07 09 11 13 15
17
02 04 06 08 10 12 14 16
Port is active
Port is inactive
Port is disabled
Port is selected
Modify

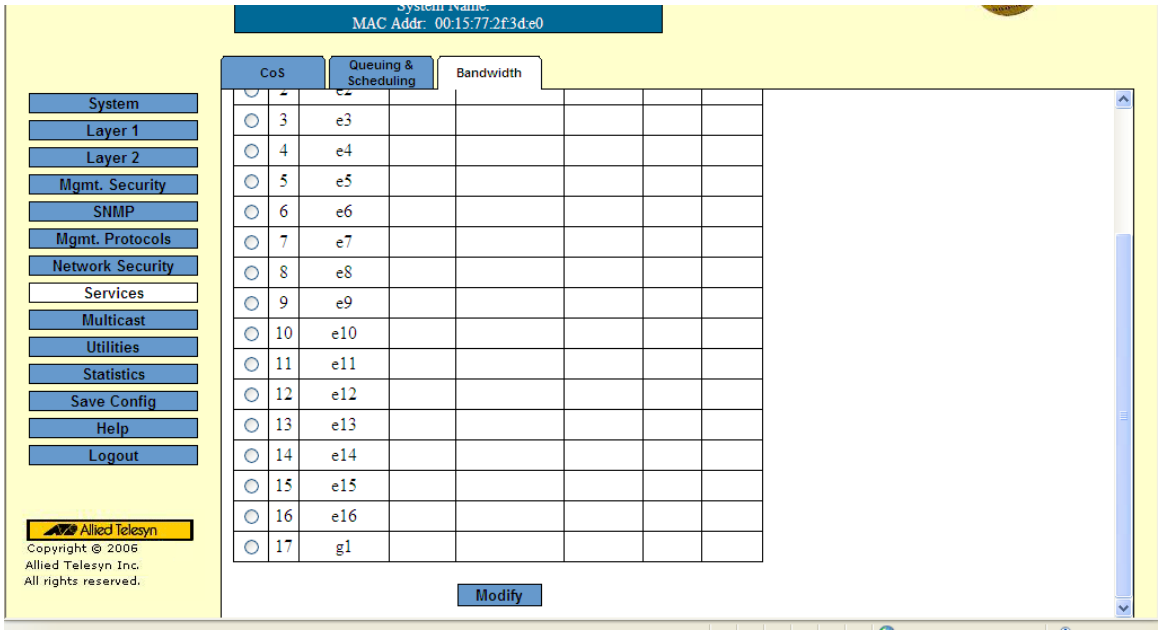

Home - Windows Internet Explorer
http://192.168.0.126/home.htm
Storm Control Configuration - Windows Internet Explorer
http://192.168.0.126/traffic/security_network_stormControl_e.htm?Query:dot1dBa
Storm Control Configuration
Port
e16
Enable Broadcast Control
Broadcast Mode
Broadcast Only
Broadcast Rate Threshold
3500
Apply
Done
Internet
100%
AT-8000S/16
13 15
14 16
Port is active
Port is inactive
Port is disabled
Port is selected
Modify
Multicast
Utilities

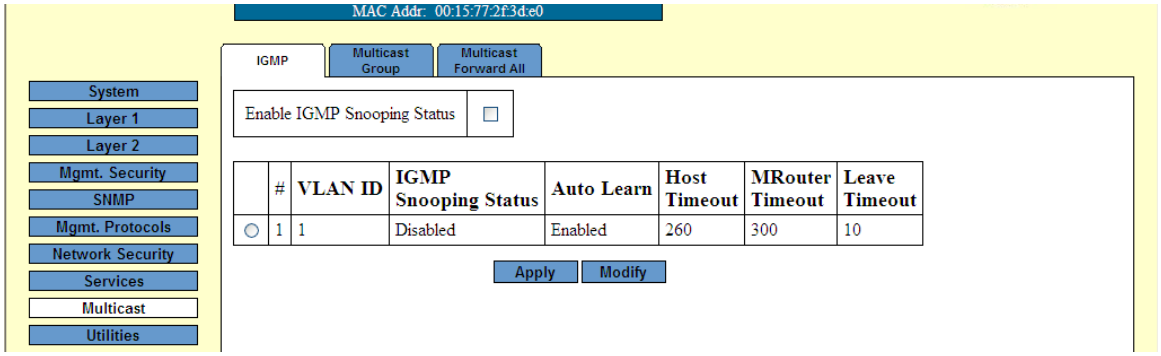

MAC Addr: 00:15:77:2f:3d:e0
CoS
Queuing & Scheduling
Bandwidth
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Enable Qos Mode
Trust Mode
CoS
Ports
Trunks
Interface Default CoS Restore Defaults
1 e1 0
2 e2 0
3 e3 0
4 e4 0
5 e5 0
6 e6 0
7 e7 0
8 e8 0
9 e9 0
10 e10 0
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
Done
Internet
100%

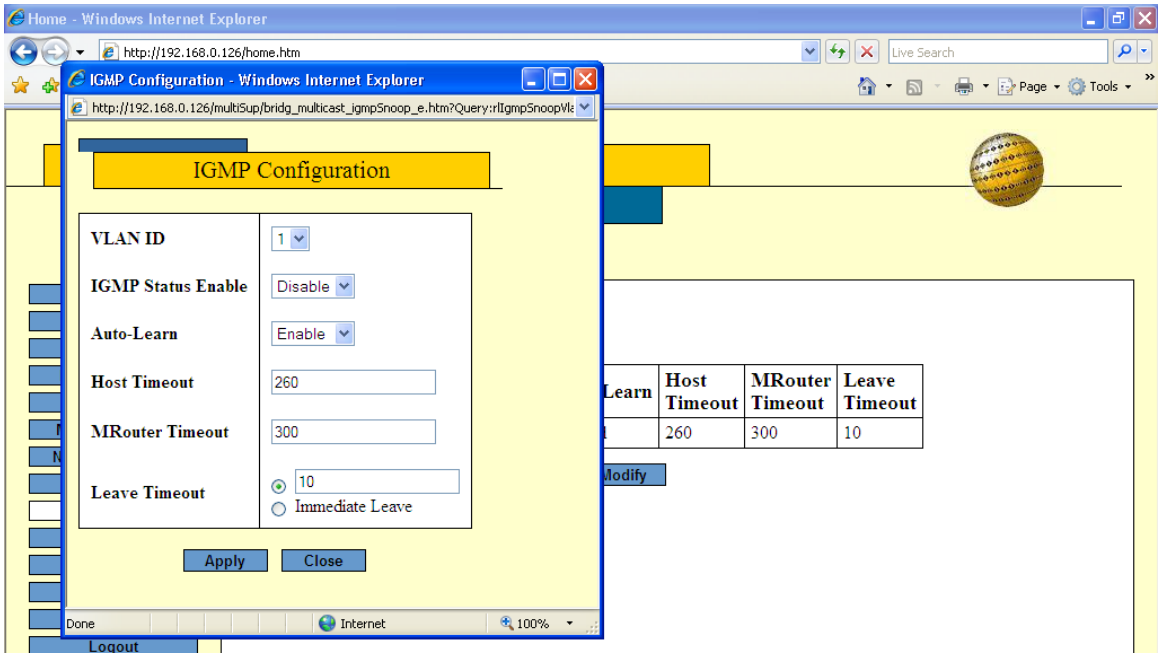

MAC Addr: 00:15:77:2f:3d:e0
CoS
Queuing & Scheduling
Bandwidth
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
3 e3 0
4 e4 0
5 e5 0
6 e6 0
7 e7 0
8 e8 0
9 e9 0
10 e10 0
11 e11 0
12 e12 0
13 e13 0
14 e14 0
15 e15 0
16 e16 0
17 g1 0
Apply
Modify

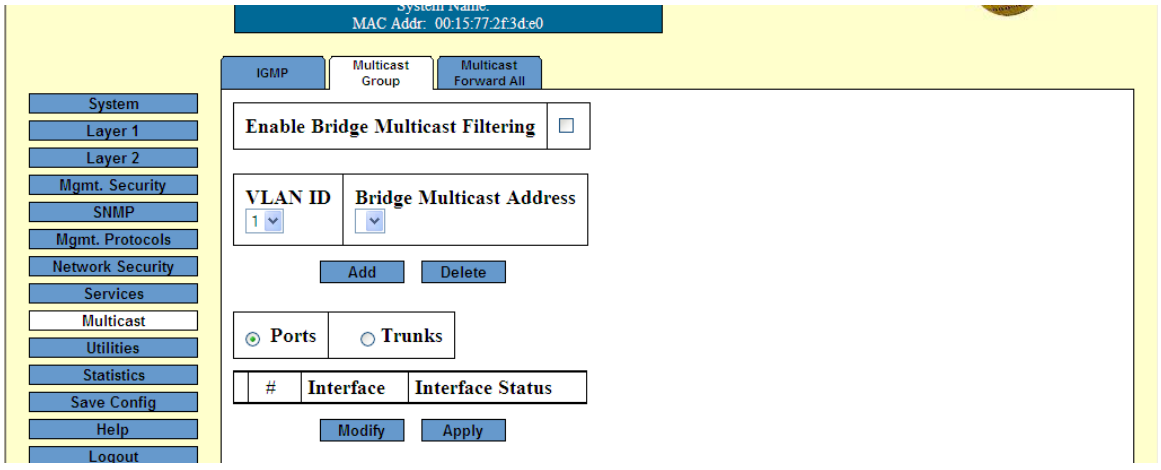

MAC Addr: 00:15:77:2f:3d:e0
CoS
Queuing & Scheduling
Bandwidth
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Configure Scheduling
Select Schedule
Strict Priority
Weighted Priority
Apply
Configure Priority to Egress Queues
Configure CoS
Configure DSCP
Configure

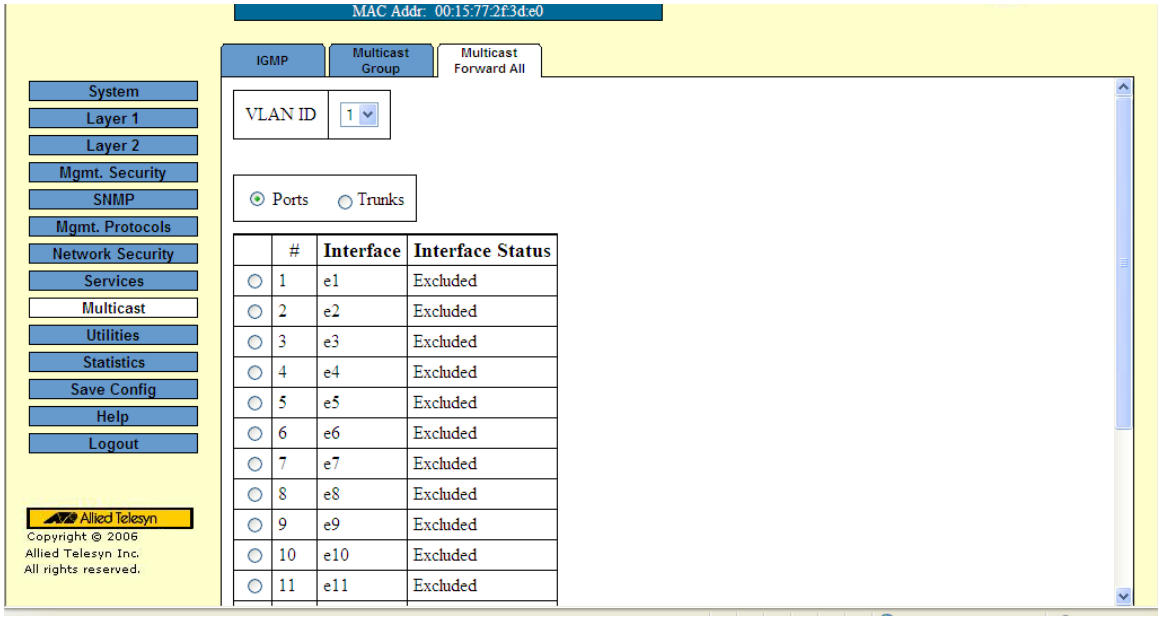

MAC Addr: 00:15:77:2f:3d:e0
CoS
Queuing & Scheduling
Bandwidth
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Ports
Trunks
Interface Ingress Rate Limit Egress Shaping Rates
Status Rate Limit Status CIR CBS
1 e1
2 e2
3 e3
4 e4
5 e5
6 e6
7 e7
8 e8
9 e9
10 e10
11 e11
12 e12
13 e13
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
Done
Internet
100%

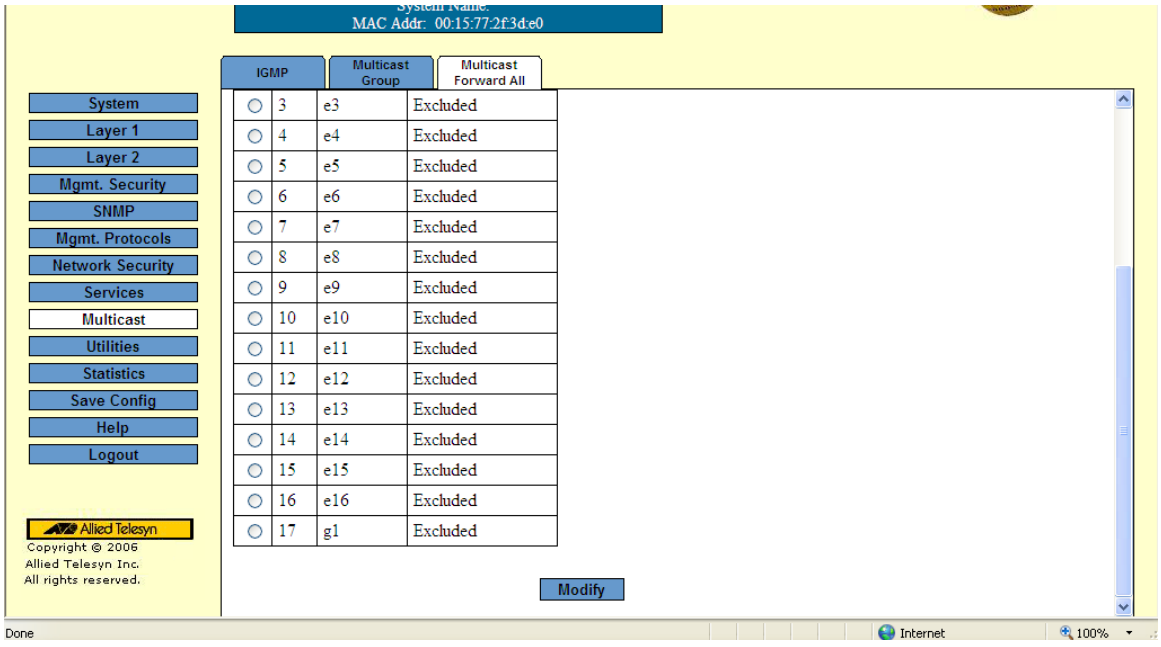

MAC Addr: 00:15:77:2f:3d:e0
CoS
Queuing & Scheduling
Bandwidth
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
3 e3
4 e4
5 e5
6 e6
7 e7
8 e8
9 e9
10 e10
11 e11
12 e12
13 e13
14 e14
15 e15
16 e16
17 g1
Modify
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

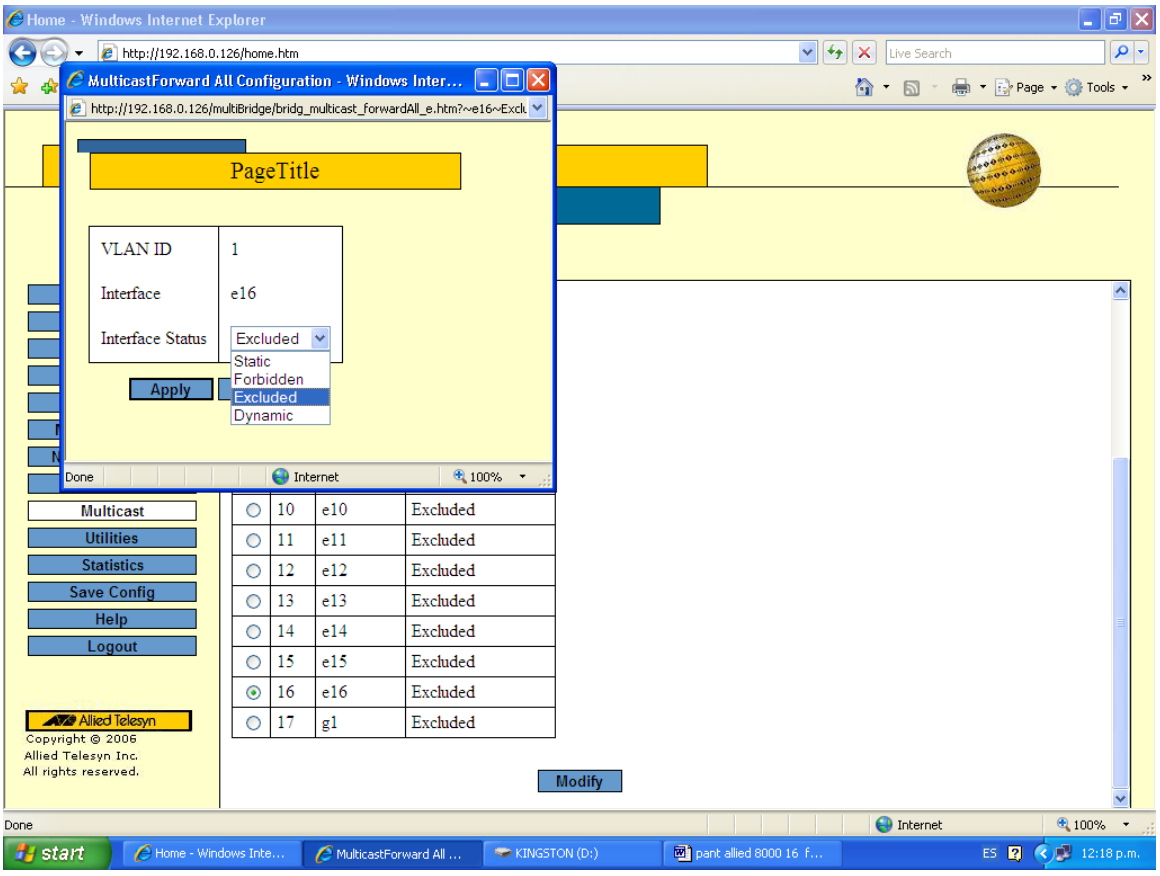

MAC Addr: 00:15:77:2f:3d:e0
IGMP
Multicast Group
Multicast Forward All
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Enable IGMP Snooping Status
VLAN ID IGMP Snooping Status Auto Learn Host Timeout MRouter Timeout Leave Timeout
1 1 Disabled Enabled 260 300 10
Apply
Modify

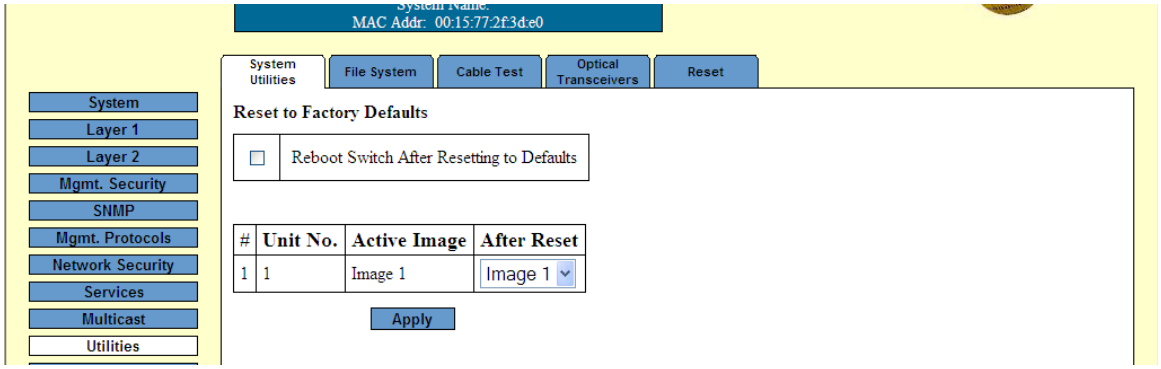

Home - Windows Internet Explorer
http://192.168.0.126/home.htm
Live Search
Page
Tools
IGMP Configuration - Windows Internet Explorer
http://192.168.0.126/multiSup/bridg_multicast_igmpSnoop_e.htm?Query:rIIgmpSnoopVl
IGMP Configuration
VLAN ID 1
IGMP Status Enable Disable
Auto-Learn Enable
Host Timeout 260
MRouter Timeout 300
Leave Timeout 10
Immediate Leave
Apply
Close
Done
Internet
100%
Learn
Host Timeout
MRouter Timeout
Leave Timeout
260
300
10
Modify
Logout

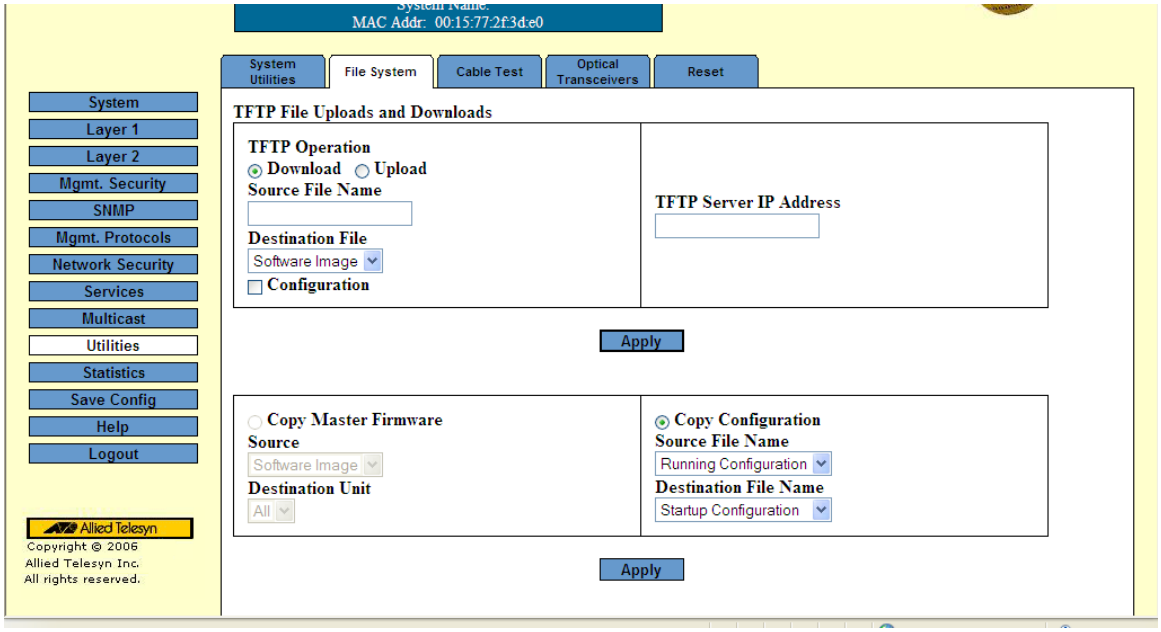

MAC Addr: 00:15:77:2f:3d:e0
IGMP
Multicast Group
Multicast Forward All
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Enable Bridge Multicast Filtering
VLAN ID
Bridge Multicast Address
1
Add
Delete
Ports
Trunks
Interface Interface Status
Modify
Apply

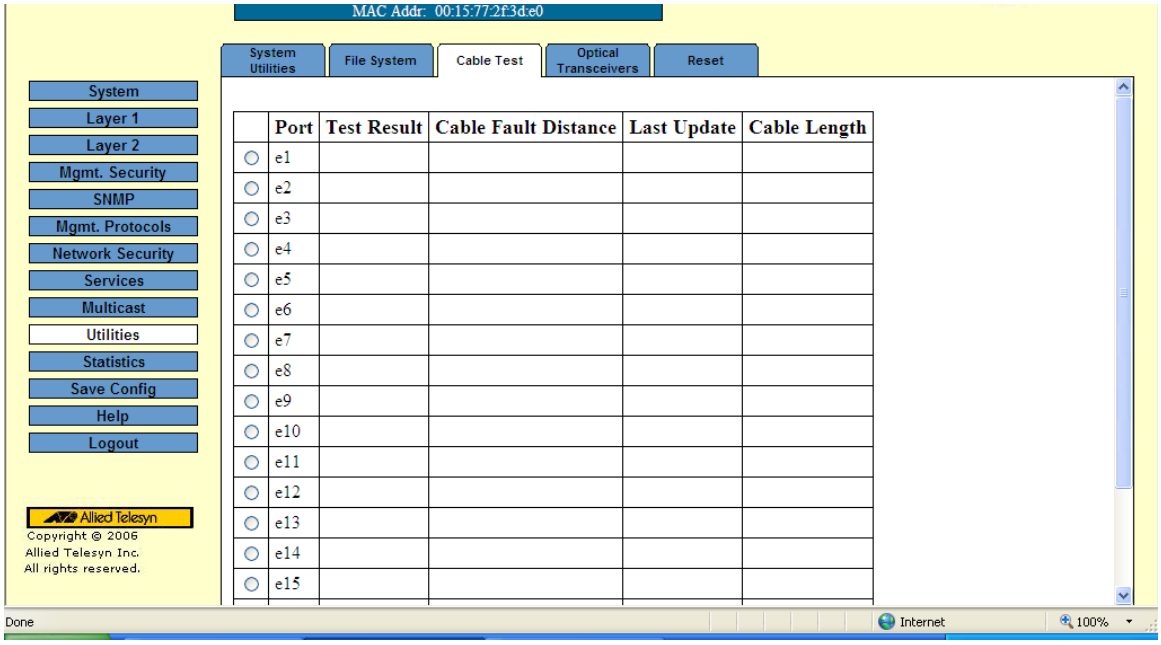

MAC Addr: 00:15:77:2f:3d:e0
IGMP
Multicast Group
Multicast Forward All
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
VLAN ID
1
Ports
Trunks
Interface Interface Status
1 e1 Excluded
2 e2 Excluded
3 e3 Excluded
4 e4 Excluded
5 e5 Excluded
6 e6 Excluded
7 e7 Excluded
8 e8 Excluded
9 e9 Excluded
10 e10 Excluded
11 e11 Excluded

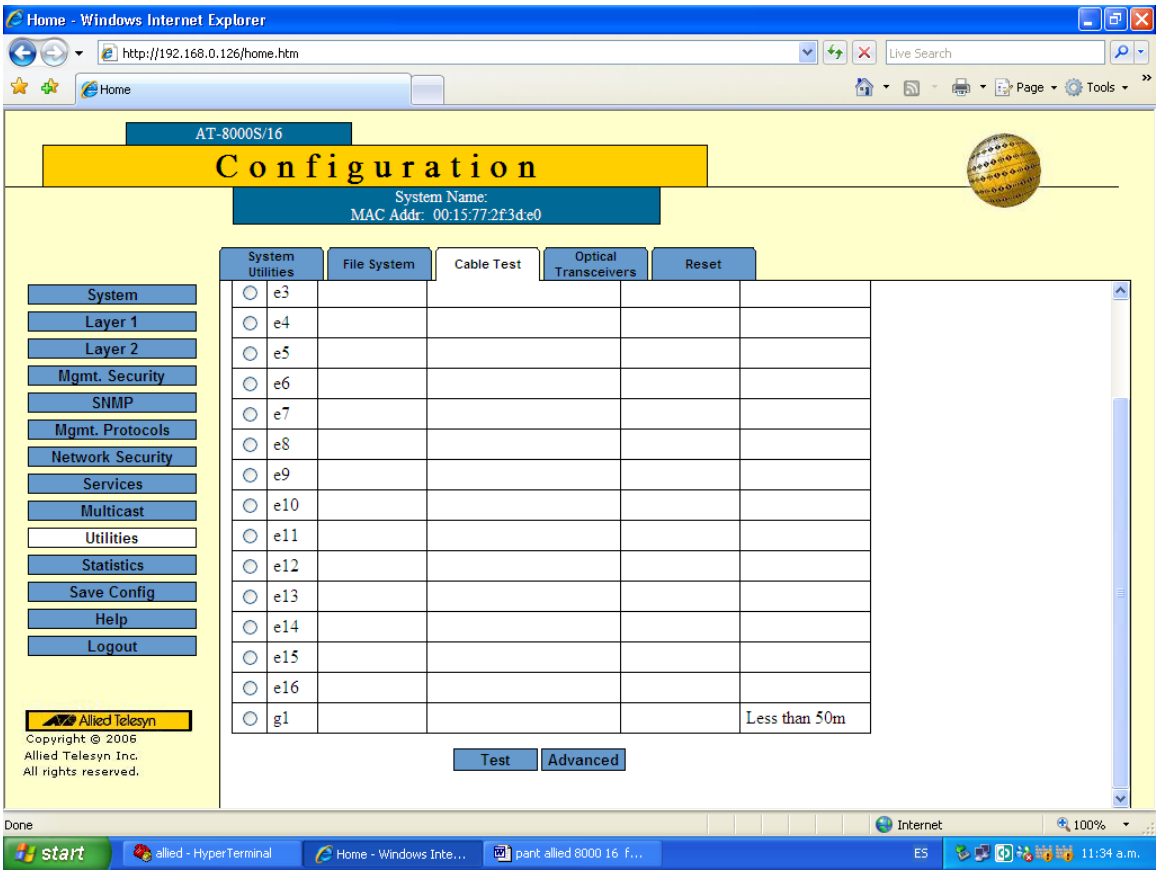

MAC Addr: 00:15:77:2f:3d:e0
IGMP
Multicast Group
Multicast Forward All
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
3 e3 Excluded
4 e4 Excluded
5 e5 Excluded
6 e6 Excluded
7 e7 Excluded
8 e8 Excluded
9 e9 Excluded
10 e10 Excluded
11 e11 Excluded
12 e12 Excluded
13 e13 Excluded
14 e14 Excluded
15 e15 Excluded
16 e16 Excluded
17 g1 Excluded
Modify
Done
Internet
100%

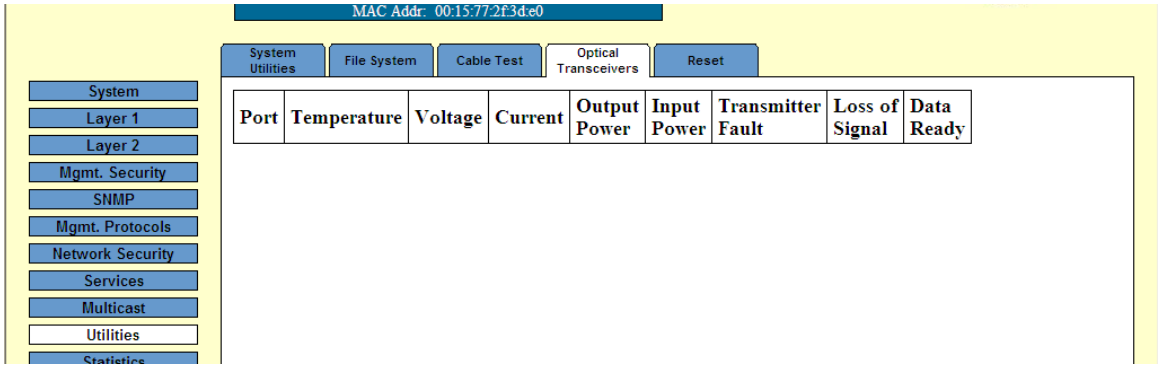

Home - Windows Internet Explorer
http://192.168.0.126/home.htm
MulticastForward All Configuration - Windows Inter...
http://192.168.0.126/multiBridge/bridg_multicast_forwardAll_e.htm?~e16~Excl
PageTitle
VLAN ID
1
Interface
e16
Interface Status
Excluded
Static
Forbidden
Excluded
Dynamic
Apply
Done
Internet
100%
Multicast
Utilities
Statistics
Save Config
Help
Logout
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
10 e10 Excluded
11 e11 Excluded
12 e12 Excluded
13 e13 Excluded
14 e14 Excluded
15 e15 Excluded
16 e16 Excluded
17 g1 Excluded
Modify
start
Home - Windows Inte...
MulticastForward All ...
KINGSTON (D:)
pant allied 8000 16 f...
ES
12:18 p.m.

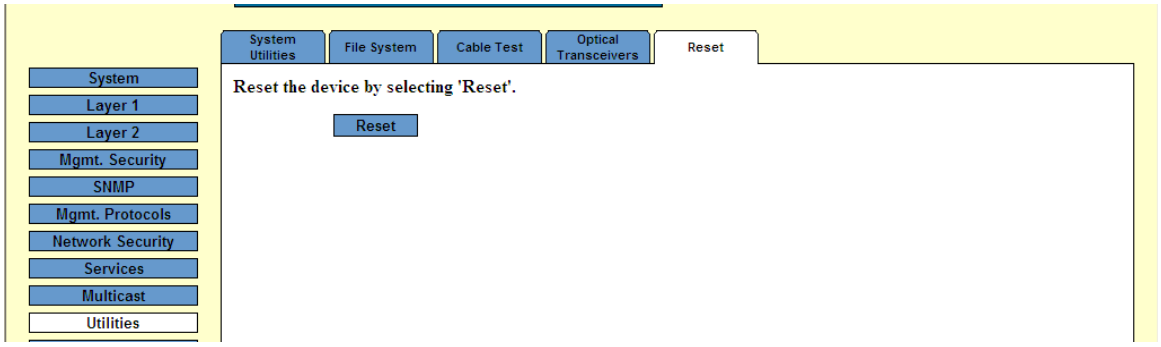

MAC Addr: 00:15:77:2f:3d:e0
System Utilities
File System
Cable Test
Optical Transceivers
Reset
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Reset to Factory Defaults
Reboot Switch After Resetting to Defaults
Unit No. Active Image After Reset
1 1 Image 1 Image 1
Apply

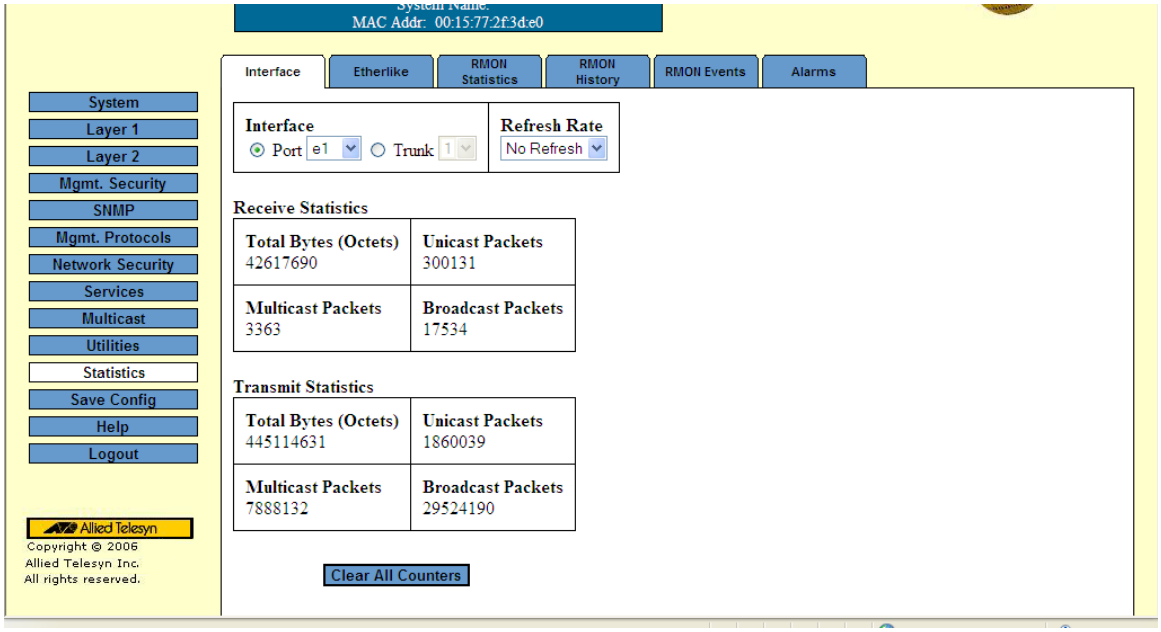

MAC Addr: 00:15:77:2f:3d:e0
System Utilities
File System
Cable Test
Optical Transceivers
Reset
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
TFTP File Uploads and Downloads
TFTP Operation
Download
Upload
Source File Name
Destination File
Software Image
Configuration
TFTP Server IP Address
Apply
Copy Master Firmware
Source
Software Image
Destination Unit
All
Copy Configuration
Source File Name
Running Configuration
Destination File Name
Startup Configuration
Apply
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

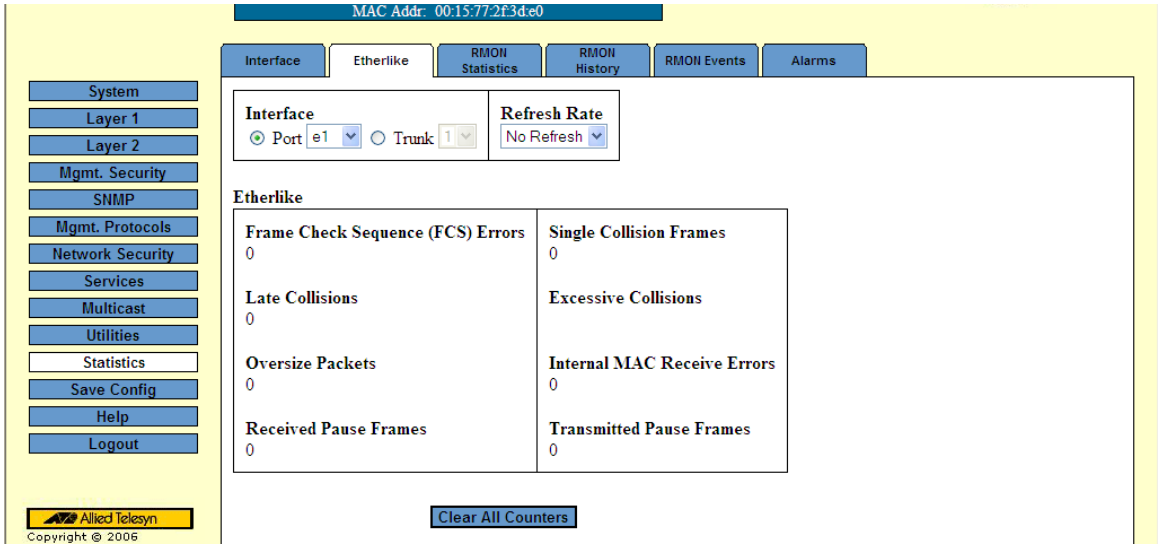

MAC Addr: 00:15:77:2f:3d:e0
System Utilities
File System
Cable Test
Optical Transceivers
Reset
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Port
Test Result
Cable Fault Distance
Last Update
Cable Length
e1
e2
e3
e4
e5
e6
e7
e8
e9
e10
e11
e12
e13
e14
e15
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
Done
Internet
100%

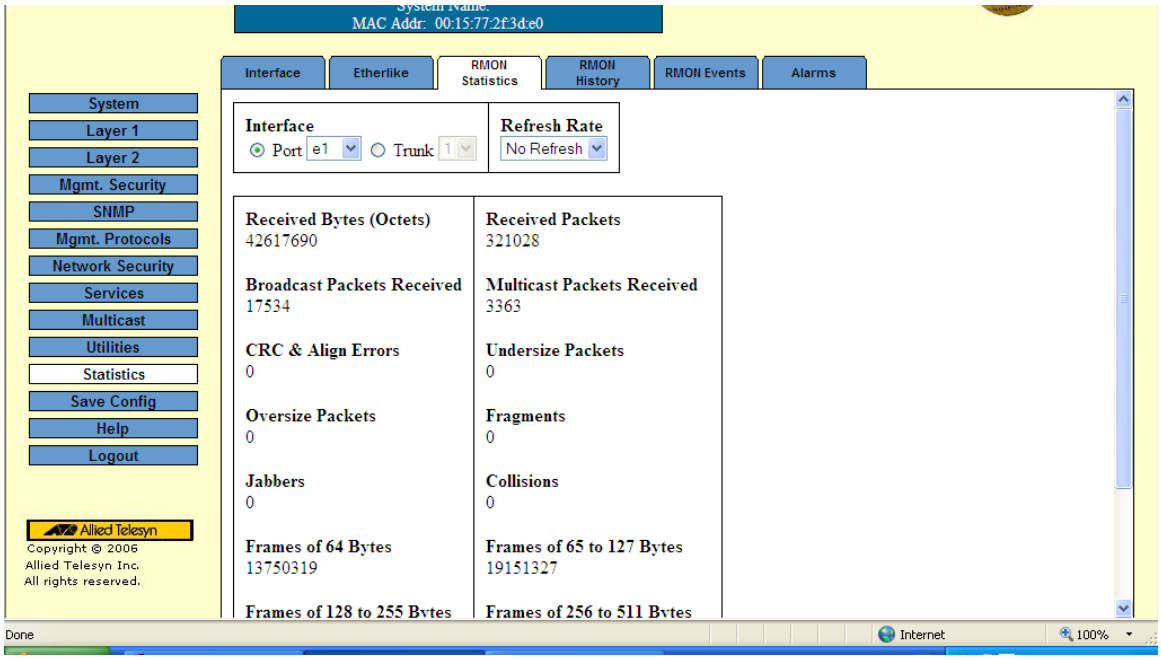

Home - Windows Internet Explorer
http://192.168.0.126/home.htm
Live Search
Home
Page
Tools
AT-8000S/16
Configuration
System Name:
MAC Addr: 00:15:77:2f:3d:e0
System Utilities
File System
Cable Test
Optical Transceivers
Reset
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
e3
e4
e5
e6
e7
e8
e9
e10
e11
e12
e13
e14
e15
e16
g1
Less than 50m
Test
Advanced
Done
Internet
100%
start
allied - HyperTerminal
Home - Windows Inte...
pant allied 8000 16 f...
ES
11:34 a.m.

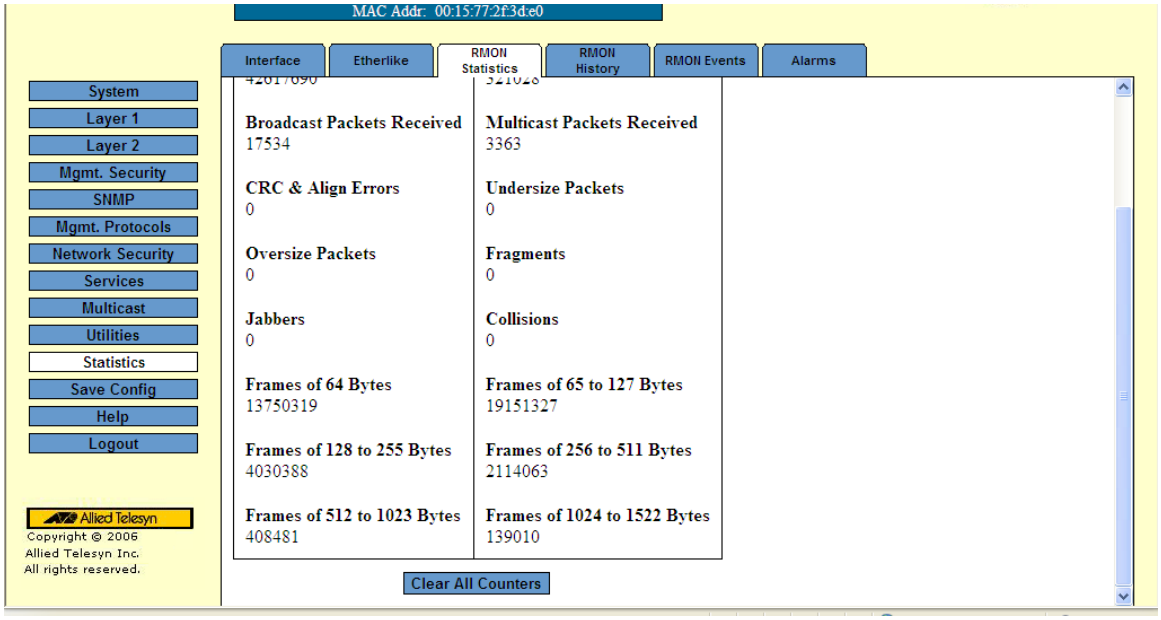

MAC Addr: 00:15:77:2f:3d:e0
System Utilities
File System
Cable Test
Optical Transceivers
Reset
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Port
Temperature
Voltage
Current
Output Power
Input Power
Transmitter Fault
Loss of Signal
Data Ready

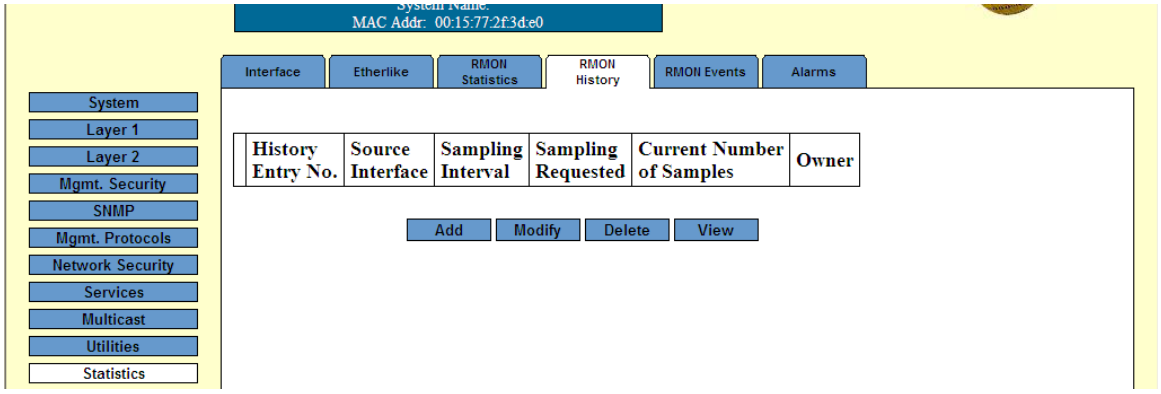

System Utilities
File System
Cable Test
Optical Transceivers
Reset
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Reset the device by selecting 'Reset'.
Reset

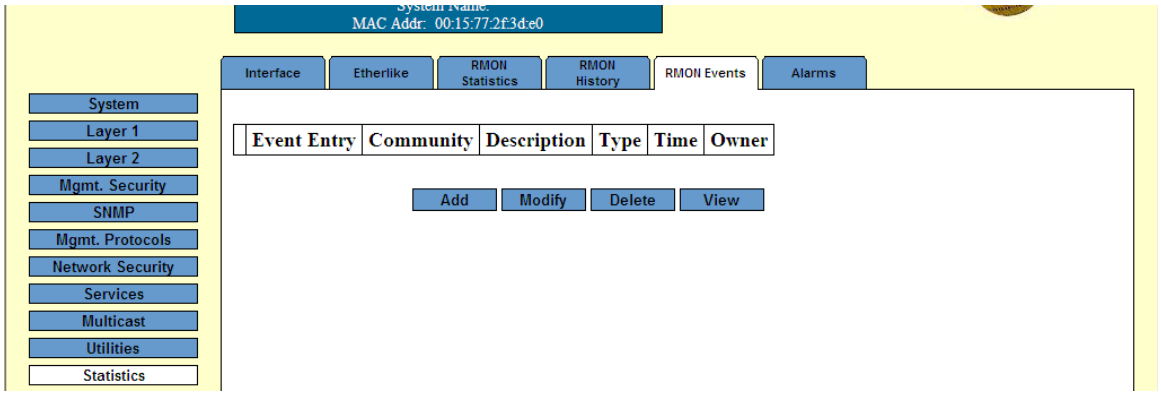

MAC Addr: 00:15:77:2f:3d:e0
Interface
Etherlike
RMON Statistics
RMON History
RMON Events
Alarms
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Interface
Port e1
Trunk 1
Refresh Rate
No Refresh
Receive Statistics
Total Bytes (Octets)
42617690
Unicast Packets
300131
Multicast Packets
3363
Broadcast Packets
17534
Transmit Statistics
Total Bytes (Octets)
445114631
Unicast Packets
1860039
Multicast Packets
7888132
Broadcast Packets
29524190
Clear All Counters
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.

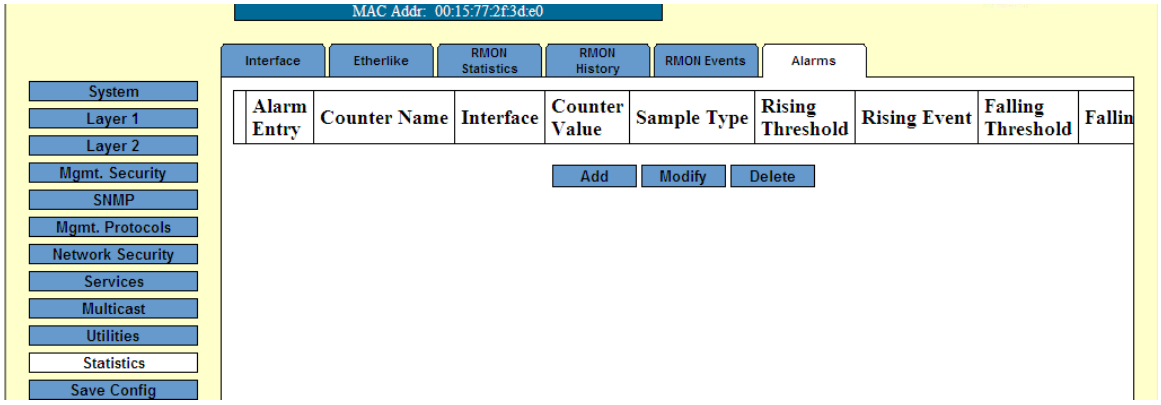

MAC Addr: 00:15:77:2f:3d:e0
Interface
Etherlike
RMON Statistics
RMON History
RMON Events
Alarms
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Interface
Port e1
Trunk 1
Refresh Rate
No Refresh
Etherlike
Frame Check Sequence (FCS) Errors
0
Single Collision Frames
0
Late Collisions
0
Excessive Collisions
Oversize Packets
0
Internal MAC Receive Errors
0
Received Pause Frames
0
Transmitted Pause Frames
0
Clear All Counters
Allied Telesyn
Copyright © 2006


MAC Addr: 00:15:77:2f:3d:e0
Interface
Etherlike
RMON Statistics
RMON History
RMON Events
Alarms
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Interface
Port e1
Trunk 1
Refresh Rate
No Refresh
Received Bytes (Octets)
42617690
Received Packets
321028
Broadcast Packets Received
17534
Multicast Packets Received
3363
CRC & Align Errors
0
Undersize Packets
0
Oversize Packets
0
Fragments
0
Jabbers
0
Collisions
0
Frames of 64 Bytes
13750319
Frames of 65 to 127 Bytes
19151327
Frames of 128 to 255 Bytes
Frames of 256 to 511 Bytes
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.
Done
Internet
100%


MAC Addr: 00:15:77:2f:3d:e0
Interface
Etherlike
RMON Statistics
RMON History
RMON Events
Alarms
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Help
Logout
Broadcast Packets Received
17534
Multicast Packets Received
3363
CRC & Align Errors
0
Undersize Packets
0
Oversize Packets
0
Fragments
0
Jabbers
0
Collisions
0
Frames of 64 Bytes
13750319
Frames of 65 to 127 Bytes
19151327
Frames of 128 to 255 Bytes
4030388
Frames of 256 to 511 Bytes
2114063
Frames of 512 to 1023 Bytes
408481
Frames of 1024 to 1522 Bytes
139010
Clear All Counters
Allied Telesyn
Copyright © 2006
Allied Telesyn Inc.
All rights reserved.


MAC Addr: 00:15:77:2f:3d:e0
Interface
Etherlike
RMON Statistics
RMON History
RMON Events
Alarms
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
History Entry No.
Source Interface
Sampling Interval
Sampling Requested
Current Number of Samples
Owner
Add
Modify
Delete
View


MAC Addr: 00:15:77:2f:3d:e0
Interface
Etherlike
RMON Statistics
RMON History
RMON Events
Alarms
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Event Entry
Community
Description
Type
Time
Owner
Add
Modify
Delete
View


MAC Addr: 00:15:77:2f:3d:e0
Interface
Etherlike
RMON Statistics
RMON History
RMON Events
Alarms
System
Layer 1
Layer 2
Mgmt. Security
SNMP
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Statistics
Save Config
Alarm Entry
Counter Name
Interface
Counter Value
Sample Type
Rising Threshold
Rising Event
Falling Threshold
Fallin
Add
Modify
Delete

APÉNDICE D: FOTOGRAFÍAS DE EQUIPOS.

Figura 16: *Fotografía de frente del equipo de conexión en el site del segundo piso en el edificio "C" de la FCA.*

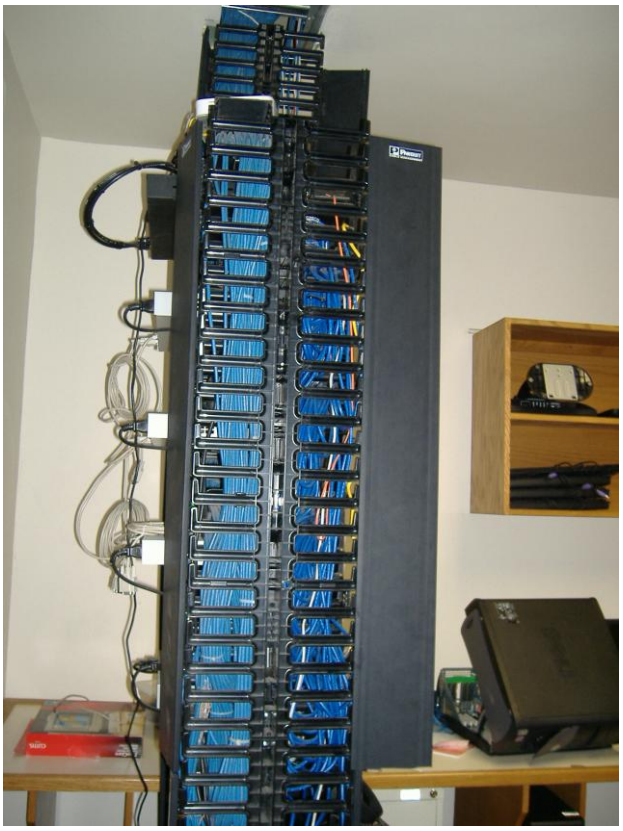


Figura 17: *Fotografía de lado del equipo de conexión en el site del segundo piso en el edificio “C” de la FCA.*

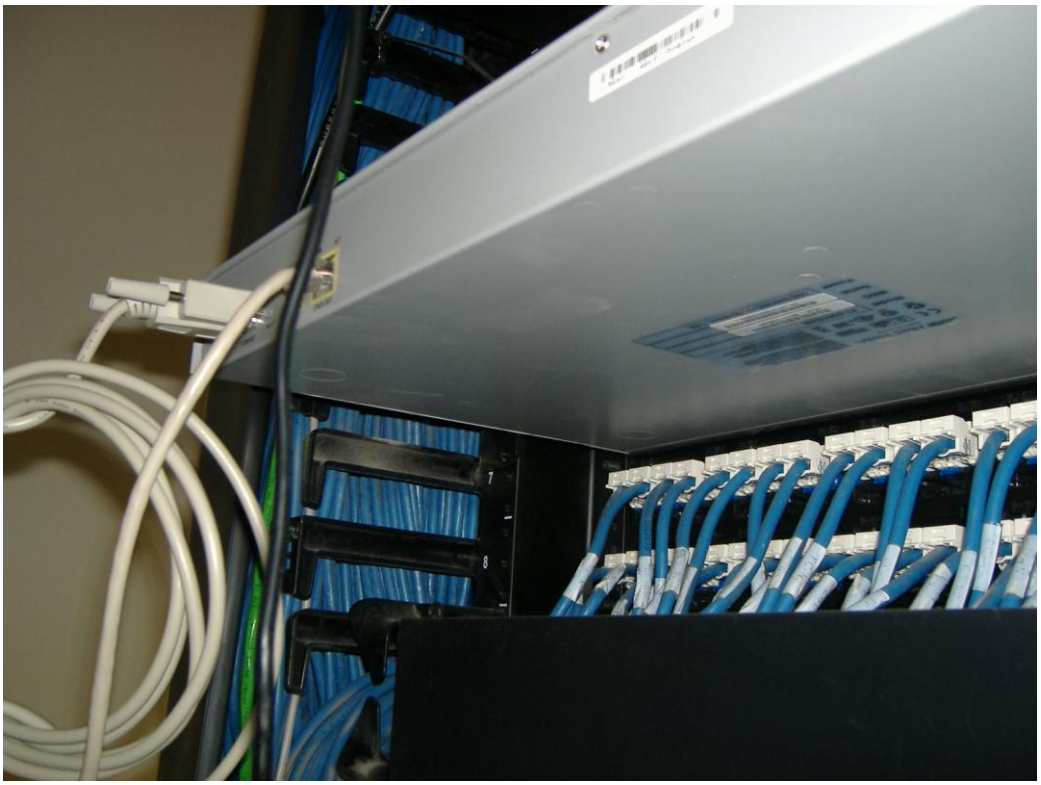


Figura 18: *Fotografía de la parte trasera del equipo de conexión en el site del segundo piso en el edificio “C” de la FCA.*