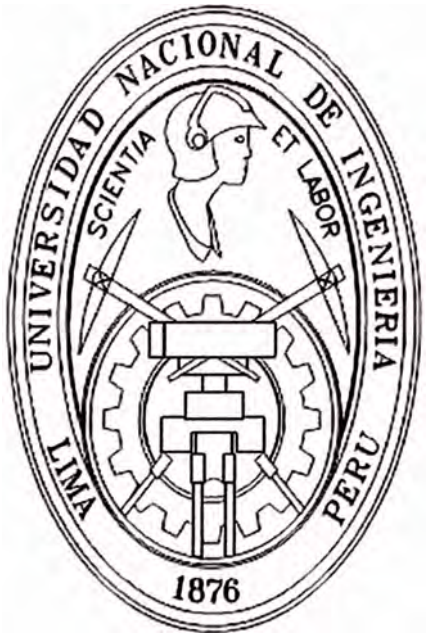
UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



IMPLEMENTACIÓN Y EVALUACIÓN DE CONTROL DE ACCESO EN REDES LOCALES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

RICARDO JAVIER ACEVEDO BERNIA

PROMOCIÓN

2003 - I

LIMA - PERÚ

2008

“IMPLEMENTACIÓN Y EVALUACIÓN DE CONTROL DE ACCESO EN REDES LOCALES”

A mi madre Glis por su apoyo constante; a mi padre Luis José por su confianza y consejos. A mis hermanos por su comprensión.

SUMARIO

El presente informe detalla el funcionamiento e implementación del control de acceso basado en puertos en un entorno Lan, empleando el protocolo 802.1X que opera en la capa 2 del modelo OSI, de esta manera se evita la utilización de la red sin previa autenticación. La implementación se basa en el estándar 802.1X, donde se define tres elementos que participan en el sistema de autenticación. El suplicante que viene a ser el cliente que solicita autenticarse, el Servidor de Autenticación es el que autentifica al cliente y el Autenticador que es el dispositivo intermedio que interactúa entre ambos.

Para nuestra solución se emplea como servidor de autenticación, FreeRadius, el cual interactúa con un servidor de directorio implementado con OpenLDAP para obtener información de los usuarios, además se adiciona un atributo y con el soporte de FreeRadius se realiza la asignación dinámica de Vlan al puerto del switch del usuario. Como dispositivo intermedio, se emplea un switch de gama intermedia que soporta el protocolo 802.1X y Vlan , que le otorga o deniega el acceso a la red a un usuario los cuales son estaciones con sistema operativo Windows XP que ya trae el soporte nativo del protocolo.

ÍNDICE

INTRODUCCIÓN

La seguridad de los datos, los servicios que se ofrecen a través de la red de comunicaciones, desde el interior son más dificiles y peligrosos en prevenir que los ataques que provienen externamente. Un usuario mal intencionado o un atacante que se conecta a la red interna, puede causar daños en los servicios y las comunicaciones a través de la red de datos. El proteger los servicios y la información proporcionando confidencialidad, integridad y disponibilidad son preocupaciones importantes hoy en día.

Nuestro trabajo se orienta en una solución para brindar la confidencialidad de los datos y servicios, asegurando que la información y los servicios protegidos sean únicamente accedidos por personas autorizadas y sistemas.

Un gran número de fabricantes están investigando y desarrollando tecnologías de seguridad de redes para proteger las intranets de anfitriones desconocidos, estas soluciones se enfrentan a la selección de tecnologías de seguridad que proporcionan un nivel deseado de seguridad a un costo razonable y con elevado desarrollo. Una de estas tecnologías de seguridad es el estándar 802.1X, su empleo es tanto para redes alámbricas como inalámbricas. El estándar 802.1X es una solución de seguridad ratificada por la IEEE, que puede autentificar a un usuario que quiere acceder a red, y esto se realiza a través de un servidor de autenticación. El estándar 802.1x se basa en el protocolo EAP (Protocolo de autenticación extensible), definido por la IETF.

Los elementos que conforman nuestra solución son: un servidor Radius que provee de autenticación, autorización y registro a los requerimientos de conexión de los usuarios, interactuando con un servidor de directorio Ldap que contiene información de los usuarios y el Autenticador que brinda la conectividad a la red, autorizando o no el acceso en el puerto, dependiendo de la respuesta que recibe por parte del servidor Radius.

El desarrollo de nuestro informe comprende el capítulo I, donde se describe la arquitectura del Control de Acceso por Puertos, la relación entre las funciones del control de acceso y la operación de los dispositivos, el capítulo II trata sobre la

funcionamiento del Protocolo de Control de Acceso por Puertos, explicando como se desarrolla el proceso de autenticación por medio de los paquetes y parámetros involucrados. En el capítulo III describimos la situación actual de la red corporativa, con que equipos de comunicación cuenta, la topología de red en funcionamiento y un resumen de los servicios de comunicaciones que se ofrece a los usuarios.

En el capítulo IV se describe la problemática y mejoras de la red corporativa, las alternativas que nos ofrece la tecnología NAC, los elementos, implementación y validación de la solución de control de acceso por puertos.

CAPITULO I
PRINCIPIOS DE OPERACIÓN DE CONTROL DE ACCESO

1.1 Objetivo del Control de Acceso

El control de acceso a los nodos de la red de datos basado en puertos evita el eventual ingreso no autorizado de dispositivos de red. El control de acceso es logrado por el sistema, implementando autenticación de los Suplicantes que se conectan a los puertos controlados del sistema; a partir del resultado del proceso de autenticación, el sistema puede determinar si es o no el suplicante autorizado a acceder a sus servicios en ese puerto controlado. Si el suplicante no es autorizado para acceder, entonces tanto el sistema del Suplicante y el sistema del Autenticador ponen el estado de sus puertos controlados en no autorizado. En el estado no autorizado, el uso del puerto controlado esta restringido de acuerdo con el valor del parámetro OperControlledDirections asociado con ese puerto controlado, previniendo la transferencia de la información no autorizada entre el sistema Suplicante y los servicios ofrecidos por el sistema Autenticador.

El mecanismo definido puede ser aplicado para permitir que algún sistema se autentique a otro sistema, que esta conectado a uno de sus puertos controlados. Los sistemas involucrados incluyen estaciones finales, servidores, routers y conmutadores.

1.2 Alcance de Operación del Control de Acceso por Puertos

La operación del control de acceso por puertos asume que los puertos en los cuales este opera, ofrece una conexión punto a punto entre un único Suplicante y un único Autenticador. Es esta suposición que permite las decisiones de autenticación puedan ser realizadas por puerto. La autenticación de múltiples Suplicantes PAE conectados a un único Autenticador PAE esta fuera del alcance de esta norma.

Esta norma proporciona un protocolo para la información de autenticación de la comunicación entre un Suplicante que esta conectado a un puerto de un sistema Auntenticador y un Servidor Autenticador, y para controlar el estado de los puertos del sistema Autenticador y Suplicante, dependiendo del resultado de intercambio del

protocolo. Esta norma no especifica la naturaleza de la información de autenticación que es intercambiado, ni las bases sobre el cual el servidor de Autenticación toma la decisión de su autenticación.

1.3 Definición de Sistemas y Puertos

Los Sistemas son dispositivos conectados a una LAN, que poseen uno o varios puntos de conexión, que se refieren como puertos de acceso a la red, o puertos.

El puerto de un sistema provee la manera en el cual este puede acceder a los servicios ofrecidos por otros sistemas accesibles vía la LAN, y para suministrar la manera del cual este puede ofrecer servicios, o el acceso a los servicios suministrados por otros sistemas accesibles vía la LAN. El control de acceso a la red basado en puertos permite la operación de un puerto del sistema ser controlado a fin de garantizar que accedan a sus servicios, y/o accedan a los servicios de otros Sistemas, esto es solo permitido para sistemas que están autorizados a hacer eso.

Para los propósitos de describir la operación del control de acceso basado en puertos, un puerto de un sistema (o más exactamente, un PAE relacionado con un puerto) es capaz de adoptar uno o ambos de los dos distintos roles en una interacción de control de acceso:

a) Autenticador: El puerto que hace cumplir la autenticación antes de permitir el acceso a los servicios que son permitidos vía ese puerto, adopta la función de Autenticador.
b) Suplicante: El puerto que desea acceder a los servicios ofrecidos por el sistema del Autenticador, adopta la función de Suplicante.

Una función adicional del sistema es descrito a continuación:

c) Servidor de Autenticación: Realiza la función de autenticación necesaria para verificar las credenciales del Suplicante en representación del Autenticador e indica si el suplicante es autorizado para acceder a los servicios del Autenticador.

Como se puede ver desde estas descripciones, los tres roles son necesarios para completar un intercambio de autenticación. Un sistema dado puede ser capaz de adoptar uno o más de estos roles; por ejemplo, un Autenticador y un Servidor de Autenticación pueden estar localizados dentro del mismo sistema, permitiendo que el sistema ejecute la función de autenticación sin la necesidad de comunicarse con un servidor externo. Asimismo, un PAE puede adoptar el rol del Suplicante en algunos intercambios de

autenticación, y el rol del Autenticador en otros. Un ejemplo de lo reciente puede ser encontrado en una red de área local conmutada, donde un nuevo conmutador adicionado a la red de área local necesitaría ser autenticado exitosamente por el PAE, asociado con el puerto del conmutador, el cual se conecta a la red de área local, antes que este pueda autenticar otros sistemas que se conectan a sus puertos.

1.4 Acceso Controlado y No Controlado

La figura 1.1, muestra que la operación del Control de Acceso por Puerto tiene el efecto de crear dos puntos de acceso distintos al punto del Sistema de conexión a la LAN. Un punto de acceso permite el intercambio no controlado de PDUs entre el Sistema y otros Sistemas en la LAN, independientemente del estado de autorización (puerto no controlado); el otro punto de acceso permite el intercambio de PDUs solo si el estado actual del puerto es autorizado (puerto controlado). Los puertos no controlado y controlado están considerado a ser parte del mismo punto de conexión a la LAN; cualquier trama recibido en el Puerto fisico es puesto a disposición de ambos puertos controlado y no controlado, sujeto al estado de autorización asociado con el puerto controlado.

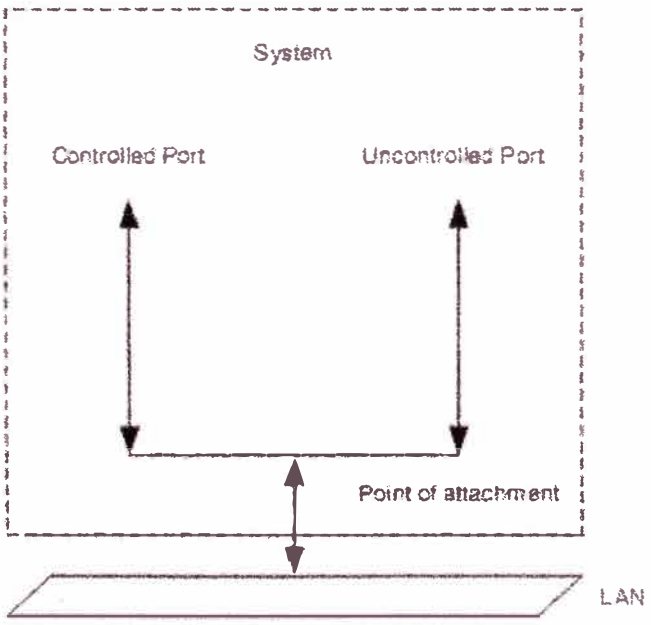


Fig.1.1 Puertos controlado y no controlado

El punto de conexión a la LAN puede ser realizado mediante un puerto fisico o lógico que puede proporcionar una conexión directa (punto a punto) a otro Sistema. Por ejemplo, el punto de conexión podría proveerse mediante una MAC en una

infraestructura LAN conmutada. En los entornos LAN donde el método MAC permite la posibilidad de una relación punto-multipunto entre un Autenticador y un Suplicante (por ejemplo, en entornos de comunicación compartida), es necesaria la creación de una asociación distinta entre dos Sistemas para los mecanismos de control de acceso indicados. Un ejemplo es la asociación entre una estación y un punto de acceso inalámbrico IEEE 802.11.

La figura 1.2, muestra el efecto del AuthControlledPortStatus asociado con el Puerto controlado, representando aquel estado como un interruptor que puede ser conectado o desconectado, permitiendo o evitando el flujo de PDUs por dicho Puerto. La figura muestra dos sistemas, cada uno con un único Puerto; se asume que se ha fijado para ambos el parámetro OperControlledDirections. En el Sistema 1, el AuthControlledPortStatus asociado con el puerto controlado está no autorizado y por consiguiente está deshabilitado (el interruptor esta desconectado); en el Sistema 2, el AuthControlledPortStatus esta autorizado y por lo tanto habilitado (el interruptor esta conectado).

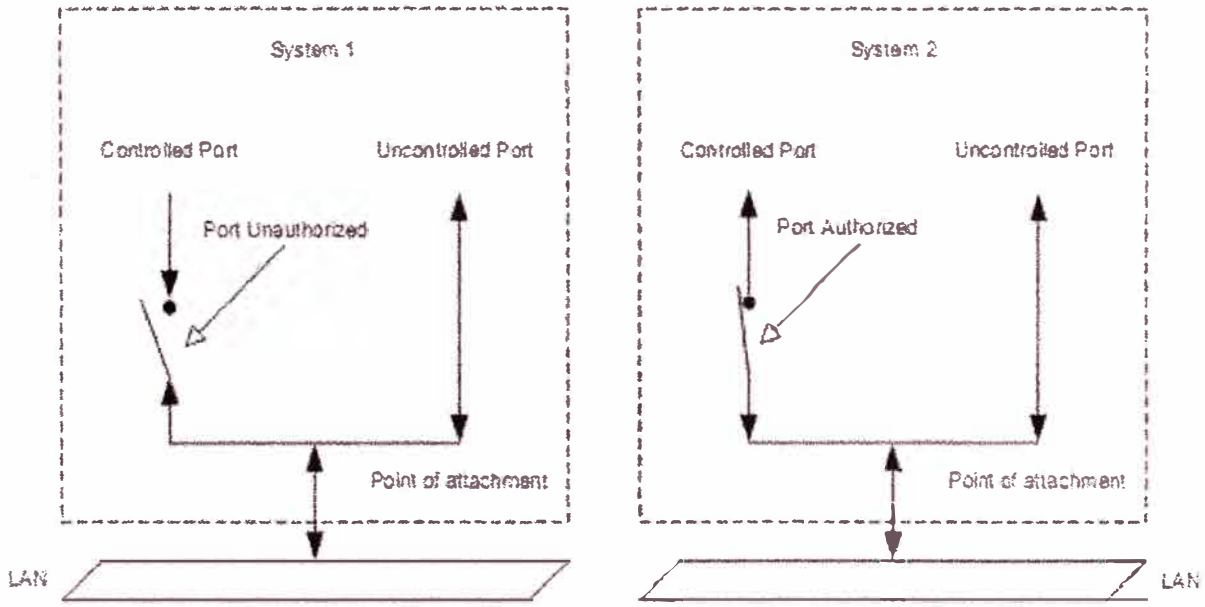


Fig.1.2 Efecto del estado de autorización en puertos controlados

Además del AuthControlledPortStatus se tiene el parámetro AuthControlledPortControl asociado con el Puerto que permite el control administrativo sobre el estado de autorización del Puerto. Este parámetro puede tomar los valores ForceUnauthorized, Auto y ForceAuthorized; su valor defecto es Auto. La relación entre los parámetros AuthControlledPortStatus y AuthControlledPortControl es como sigue:

a) El valor AuthControlledPortControl de ForceUnauthorized impone a la máquina de estados del Autenticador PAE a fijar el valor de AuthControlledPortStatus al nivel no autorizado.
b) El valor AuthControlledPortControl de ForceAuthorized impone a la máquina de estados del Autenticador PAE a fijar el valor de AuthControlledPortStatus a nivel de autorizado.
c) El valor AuthControlledPortControl de Auto permite a la máquina de estados del Autenticador PAE a controlar el valor de AuthControlledPortStatus para reflejar el resultado del intercambio de autenticación entre el Suplicante PAE, Autenticador PAE y el Servidor de Autenticación.

En los tres casos, el valor de AuthControlledPortStatus refleja directamente el valor de la variable portStatus asegurado por la máquina de estados del Autenticador PAE y Suplicante PAE. Tres factores contribuyen al valor de la variable portStatus:

d) El estado de autorización de la máquina de estados del Autenticador PAE (sobrentendido como Autorizado si la máquina de estado no esta implementado para ese puerto).
e) El estado de autorización de la máquina de estados del Suplicante PAE (sobrentendido como Autorizado si la máquina de estado no esta implementado para ese puerto).
f) El estado del parámetro de control administrativo SuplicantAccessControl con Autenticador. Este parámetro tiene dos posibles valores Active y Inactive. El valor por defecto de este parámetro de control es Inactive; el soporte del valor Active es opcional. El valor de este parámetro surte efecto solo si ambas máquinas de estados Autenticador PAE y Suplicante PAE son implementadas para este puerto. Si el valor del parámetro esta en Inactive, entonces el valor del parámetro portStatus esta determinado únicamente por el estado de autorización de la máquina de estados del Autenticador PAE. Si el valor del parámetro esta en Active, entonces el valor del parámetro porStatus esta determinado por el estado de autorización de ambas máquina de estado del Autenticador PAE y Suplicante PAE, si cualquiera de las máquinas de estado esta en un estado no autorizado, entonces el valor de porStatus es no autorizado.

El valor del parámetro AuthControlledPortControl para cada puerto de un sistema puede ser anulado mediante el parámetro SystemAuthControl. Este parámetro puede tomar los valores Enabled y Disabled; su valor por defecto es Disabled.

Si se fija SystemAuthControl como Enabled, entonces se permite la autenticación para el sistema, y el estado de autorización de cada Puerto es controlado de acuerdo al valor del parámetro AuthControlledPortControl del Puerto. Si se fija SystemAuthControl como Disabled, entonces todos los puertos se comportan como si su parámetro AuthControlledPortControl estuviera fijado a ForceAuthorized. De hecho, colocar el parámetro SystemAuthControl a Disabled causa que se deshabilite la autenticación en todos los puertos, y fuerza a que todos los puertos controlados sean autorizados.

Cualquier acceso a la LAN está sujeta al estado administrativo y operacional de la MAC asociado con el puerto, además a AuthControlledPortStatus. Si la MAC esta física o administrativamente inoperable, entonces no puede darse ningún intercambio de protocolo de cualquier clase usando esa MAC en el puerto controlado o no controlado. Esto esta ilustrado en la figura 1.3; en el sistema 1, ambos puertos controlado y no controlado están aptos para accesar a la LAN, ya que el puerto controlado esta autorizado, y la MAC abastece el punto de conexión a la LAN que esta operable. En el sistema 2 ni el puerto controlado ni el no controlado pueden acceder a la LAN, ya que la MAC que abastece el punto de conexión a la LAN esta inoperable. El estado inoperable de la MAC también ha causado al Autenticador PAE la transición del puerto controlado al estado no autorizado, como muestra en la figura 1.3.

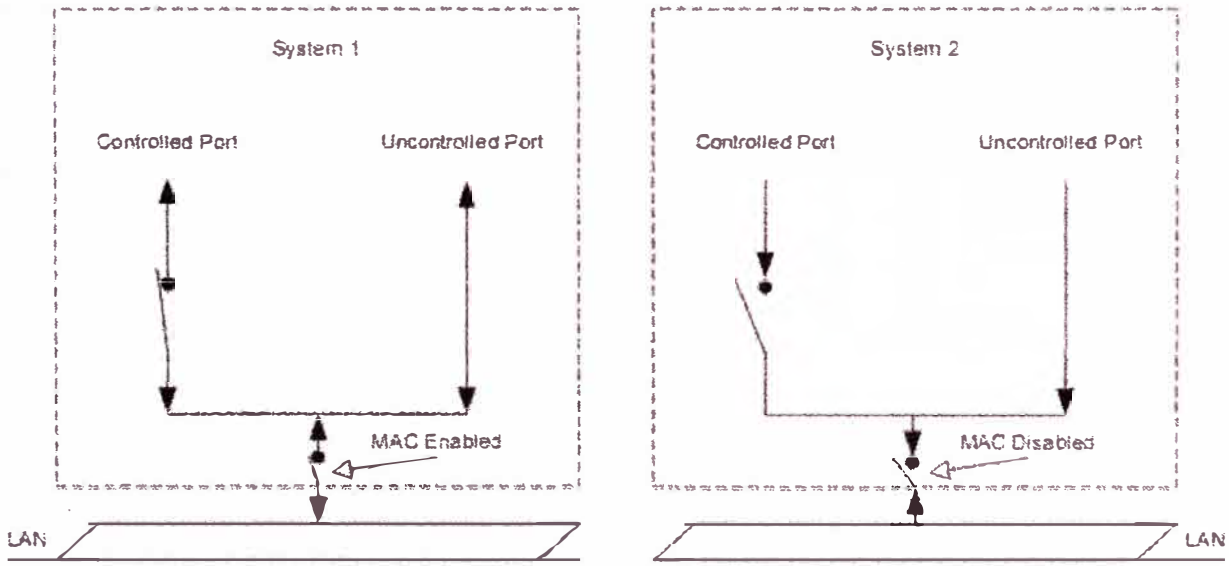


Fig.1.3 Efecto de estados habilitado/deshabilitado MAC

Los Autenticadores y Suplicantes PAE utilizan el puerto no controlado para el intercambio de información de protocolo con otro Suplicante o Autenticador PAE. El

intercambio de protocolo entre el Autenticador PAE y el Servidor de autenticación (si el servidor no esta colocado con el Autenticador PAE) se puede dar vía uno o varios de los Puertos controlados o no controlados del Sistema.

Se espera que la mayoría de los intercambios de protocolos conducidos por otras funciones del Sistema hagan uso de uno o varios de los puertos controlados del Sistema. Sin embargo, un protocolo dado puede necesitar evitar la función de autorización y hacer uso del Puerto no controlado. La figura 1.4 muestra el uso de los puertos controlados y no controlados en un sistema Autenticador y un sistema Suplicante, y la capacidad de los PAEs para cambiar el estado de autorización del puerto controlado dependiendo del resultado de un intercambio de autenticación; la figura también da un ejemplo de las entidades del protocolo (las PAEs) que requieren el uso de un puerto no controlado de acuerdo al comportamiento del intercambio de sus protocolos.

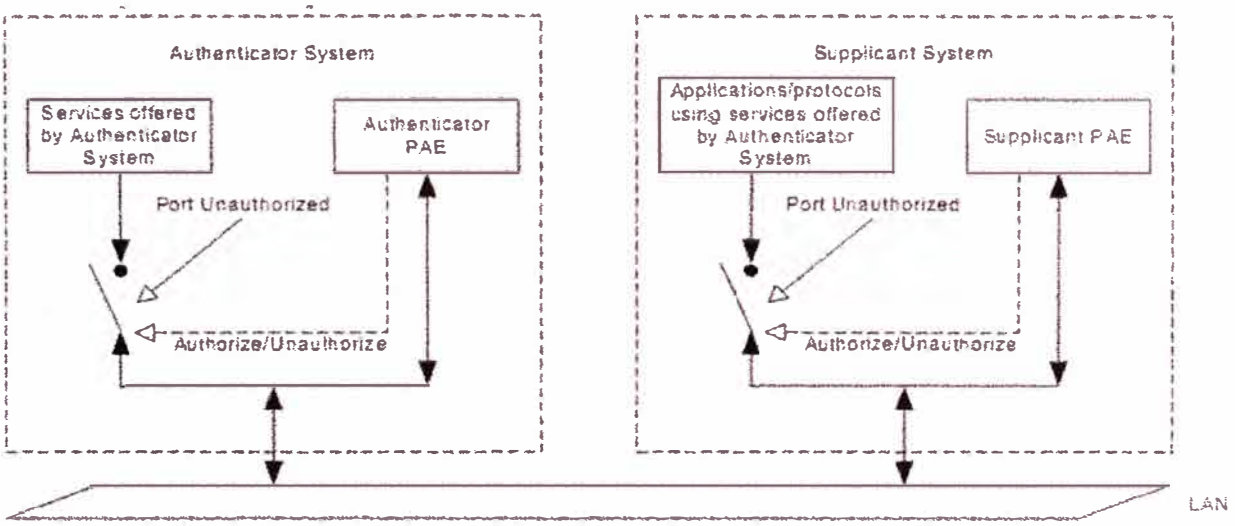


Fig.1.4 Uso de los puertos controlado y no controlado

La figura 1.5 muestra las relaciones entre el Suplicante, Autenticador y Servidor de Autenticación, y el intercambio de información entre ellos. En esta muestra, ambos puertos controlados del Autenticador y del Suplicante están en el estado no autorizado y por consiguiente son deshabilitados desde el punto de vista del acceso por el sistema del Suplicante a los servicios ofrecidos por el sistema del Autenticador. Los dos PAEs hacen uso de sus puertos no controlados para comunicarse el uno al otro, usando un protocolo de autenticación transportado en la capa de enlace de datos, y el Autenticador PAE se comunica con el Servidor de Autenticación usando un protocolo autenticación transportado en un protocolo de capa superior.

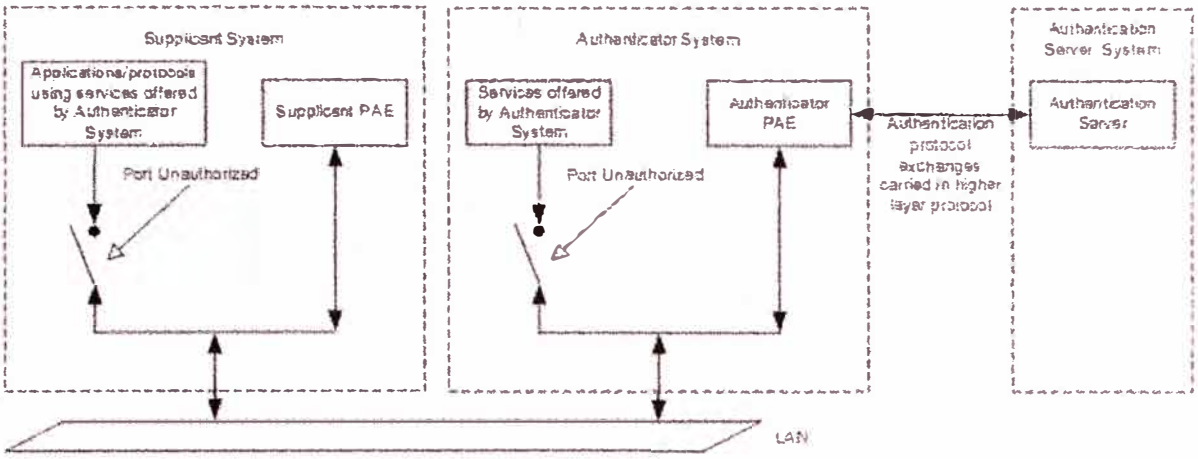


Fig.1.5 Roles Autenticador, Suplicante y Servidor Autenticación

La comunicación entre el Autenticador y el Servidor de Autenticación puede hacer uso del servicio de una LAN, o puede usar algún otro canal de comunicación. En caso que el Servidor de Autenticación sea colocado con el Autenticador, el intercambio del protocolo de autenticación entre estas dos entidades no será necesario.

1.5 Control de Transmisión y Recepción

El grado al que toma lugar el intercambio de protocolo en el puerto controlado está afectado por el estado de autorización que es determinado por dos parámetros de dirección controlada, asociado con cada puerto controlado: un parámetro AdminControlledDirections y un parámetro OperationalControlledDirections. Estos parámetros determinan si un puerto controlado que no es autorizado ejerce el control de la comunicación en ambas direcciones (deshabilitando las tramas entrantes y salientes), o solo en la dirección de entrada (deshabilitando solo la recepción de tramas entrantes). Los parámetros de dirección controlados pueden tomar uno de dos valores posibles, Both y In. La relación entre estos dos parámetros, y el significado de sus valores, es como sigue:

a) **AdminControlledDirections = Both.** Esto indica que se requiere que el control sea aplicado sobre ambos tráficos de entrada y salida a través del puerto de control. El valor de OperControlledDirections es absolutamente puesto igual para Both si AdminControlledDirections es puesto igual para Both.

b) **AdminControlledDirections = In.** Indica que se requiere que el control sea aplicado sólo sobre el tráfico de entrada a través del puerto controlado. Si se

fija AdminControlledDirections a In, el valor de OperControlledDirections es puesto a In en la inicialización y cuando la MAC del puerto esté operable. Sin embargo, se fija el valor de OperControlledDirections a Both, si se dá alguna de las siguientes condiciones:

1) El puerto es un puerto del conmutador, y la máquina de estado de detección del conmutador, detecta la presencia de otro conmutador conectado al puerto.
2) El puerto es un puerto del conmutador y el parámetro de puerto Edge Port es falso.
3) La MAC del puerto no es operable.

1.6 Entidad de Acceso por Puerto (PAE)

Una Entidad de Acceso por Puerto (PAE) maneja los algoritmos y protocolos asociados con el Protocolo de Control de Acceso por Puerto. Un PAE existe para cada puerto de un sistema que soporta la funcionalidad del control de acceso por puerto en la función Suplicante, la función Autenticador, o ambos.

En la función Suplicante, un PAE es responsable de proporcionar la información a un Autenticador que establecerá sus credenciales. Un PAE que realiza el papel Suplicante en un intercambio de autenticación se conoce como un Suplicante PAE.

En la función Autenticador, un PAE es responsable de la comunicación con un Suplicante, y el envío de la información recibida del Suplicante a un servidor de autenticación para la verificación de credenciales y consiguiente estado de autorización. Un PAE que realiza el papel Autenticador en un intercambio de autenticación se conoce como un Autenticador PAE.

Ambas funciones PAE controlan el estado autorizado/no autorizado del puerto controlado dependiendo del resultado del proceso de autenticación. Si un puerto controlado dado tiene ambas funcionalidades tanto Autenticador PAE como Suplicante PAE asociadas a este, ambos PAEs deben estar en el estado Autorizado para que el puerto controlado sea Autorizado.

1.6.1 Función Autenticador

Un Autenticador PAE es responsable de hacer cumplir la autenticación de un Suplicante PAE que conecta a su puerto controlado y en consecuencia controlar el estado de autorización del puerto controlado.

En orden a realizar la autenticación, el Autenticador PAE hace uso de un servidor de Autenticación. El servidor de autenticación puede ser colocado en el mismo sistema como el Autenticador PAE, o este puede ser localizado en algún otro sitio, accesible al mecanismo de comunicación vía remota, basado en LAN o de otra manera.

1.6.2 Función Suplicante

Un suplicante PAE es responsable de comunicar las credenciales del Suplicante al Autenticador PAE en respuesta a las peticiones del Autenticador PAE, y para controlar el estado de autorización del puerto controlado según el resultado del intercambio de autenticación comunicado por el Autenticador PAE. El Suplicante PAE también puede iniciar intercambios de autenticación y realizar intercambios de desconexión explícitos.

1.6.3 Restricciones de Acceso a Puertos

La Autenticación ocurre principalmente en el tiempo de inicialización del sistema, o cuando un sistema Suplicante se conecta a un puerto de un sistema Autenticador. Hasta que la Autenticación se complete satisfactoriamente, el sistema Suplicante sólo tiene acceso al sistema Autenticador para realizar intercambios de autenticación, o tener acceso a servicios ofrecidos por el sistema Autenticador que no están sujetos a las restricciones de control de acceso ubicados en cualquiera de los puertos controlados del Autenticador o puertos controlados del Suplicante. Una vez que la autenticación se ha completado exitosamente, ambos sistemas pueden permitir el acceso completo por el sistema Suplicante a los servicios ofrecidos vía el puerto controlado del sistema Autenticador.

El estado operacional de la MAC que soporta un puerto controlado puede ser deshabilitado o habilitado. Si el estado operacional de la MAC esta deshabilitado, entonces la MAC no esta disponible para el uso, no obstante el estado de autorización asociado con el puerto controlado.

En un sistema que implementa un PAE, el puerto controlado es ubicado en el estado no autorizado hasta que la autenticación haya tomado lugar y además este deshabilitado. Una vez que la autenticación haya tenido éxito y este haya sido determinado que el usuario autenticador esta autorizado para acceder al puerto controlado, el puerto controlado esta ubicado en el estado autorizado; asumiendo que no hay otra razón para que este aun esté deshabilitado (ejemplo; La MAC ha sido deshabilitado para propósitos administrativos), el puerto controlado esta entonces disponible para el uso.

Además para controlar el estado de autorización del puerto controlado, la operación del PAE puede soportar la culminación del estado de autorización de los puertos controlados y esto puede requerir que el Suplicante reautentique en algún momento. Los puertos controlados permanecen autorizados durante la reautenticación y la transmisión al estado no autorizado solo si la reautenticación falla.

La autenticación es configurable por puerto, porque será deseable que en algunas configuraciones no se realicen la autenticación sobre ciertos puertos (ejemplo, enlaces entre conmutadores, puertos conectados a servidores).

1.6.4 Mecanismo de Desconexión (Logoff)

Hay varios mecanismos que pueden dar lugar al estado de puerto controlado, que cambia a no autorizado y de tal modo controlar el acceso vía ese puerto conforme con su parámetro OperControlledDirections.

a) Los intercambios de autenticación entre el Suplicante y el servidor de Autenticación puede resultar en fallas de autorización del puerto.
b) Los controles de gestión pueden impedir al puerto tener la autorización, independientemente de las credenciales del Suplicante.
c) La MAC asociada con el puerto puede ser no operacional por cualquier razón (incluyendo fallas de hardware o razones administrativas).
d) La falla de conexión entre el Suplicante y el Autenticador puede causar en expiración del estado de autorización del Autenticador.
e) Puede ocurrir la expiración del temporizador de reautenticación sin reautorización.
f) El Suplicante PAE puede fallar en responder a una petición de información de autenticación por el Autenticador PAE.
g) El Suplicante PAE puede entregar una petición de desconexión explícita.

Cuando un usuario se desconecta desde una estación final, es posible que en algunos entornos para el usuario (o un usuario diferente) sea pasado un nuevo requerimiento de conexión y por lo tanto se logra accesar a la estación final y la red. Proporcionando el mecanismo de desconexión explicito se asegura que la sesión esta terminada, no solo con respecto al acceso del usuario a la estación final, sino además para el estado de autorización de la estación final con el puerto controlado del sistema Autenticador al cual este es conectado. Una desconexión explícita, por lo tanto causa que ambos, el Suplicante y Autenticador PAE fijen sus puertos controlados en el estado no autorizado.

CAPITULO II
PROTOCOLO DE CONTROL DE ACCESO POR PUERTOS

2.1 Introducción de la Funcionalidad del Protocolo

La operación del proceso de autenticación hace uso del Protocolo de Autenticación Extensible (EAP, especificado en IETF RFC 3748) como el medio de comunicación de la información de autenticación entre el Suplicante y el Servidor de Autenticación. EAP es un protocolo general que soporta múltiples mecanismos de autenticación. Por ejemplo, mediante el uso de EAP, se soporta un número de esquemas de autenticación que se puede añadir, incluyendo tarjetas inteligentes, Kerberos, Encriptado con Clave Pública, Contraseñas de Tiempo y otros.

El estándar define un formato de encapsulado que permite que los mensajes EAP se transporten directamente por un servicio MAC LAN. El formato encapsulado de EAP, conocido como EAP sobre LAN, o EAPOL, es usada para toda las comunicaciones entre el Suplicante PAE y el Autenticador PAE.

Cada PAE tiene dos componentes separados, una serie de máquinas de estado PACP, y una capa superior con las cuales estas máquinas se comunican. En el caso del Suplicante PAE, la capa superior consiste en la funcionalidad de EAP, mientras que en el caso del Autenticador PAE, la capa superior es una combinación de EAP y funciones de autenticación, autorización, y contabilización (AAA). Esta norma define las máquinas de estado PACP y el interfaz entre las máquinas de estado PACP y la funcionalidad de la capa superior.

La operación de las funciones de la capa superior con la cual las máquinas de estado de PAE se comunican no está estandarizada. Los intercambios del protocolo EAP están definidos por los estándares IETF EAP., IETF RFC 3748, y las normas sucesoras. Un ejemplo de un protocolo AAA, RADIUS, es definido por la norma IETF RADIUS, IETF RFC 2865, IETF RFC 2866, IETF RFC 3579, y las normas sucesoras.

La figura 2.1 muestra la interfaz entre las máquinas de estado PACP y la capa superior para el Suplicante y Autenticador PAE. Como se muestra, la señal portEnabled del sistema indica tanto a la capa superior como al PACP que un puerto esta activo. El

PACP pasa mensajes EAP entre el puerto físico y la capa superior. El flujo de mensajes en el Suplicante es controlado usando eapResp/eapNoResp del EAP para indicar que está listo para otro mensaje y eapReq del PACP para indicar que un mensaje está disponible para el proceso de EAP. El flujo de mensajes en el lado del Autenticador es controlado por un proceso similar, con la capa superior que usa eapReq/eapNoReq, para indicar cuando está listo para recibir un nuevo mensaje, y eapResp para indicar que un mensaje está disponible para ser procesado por la capa superior.

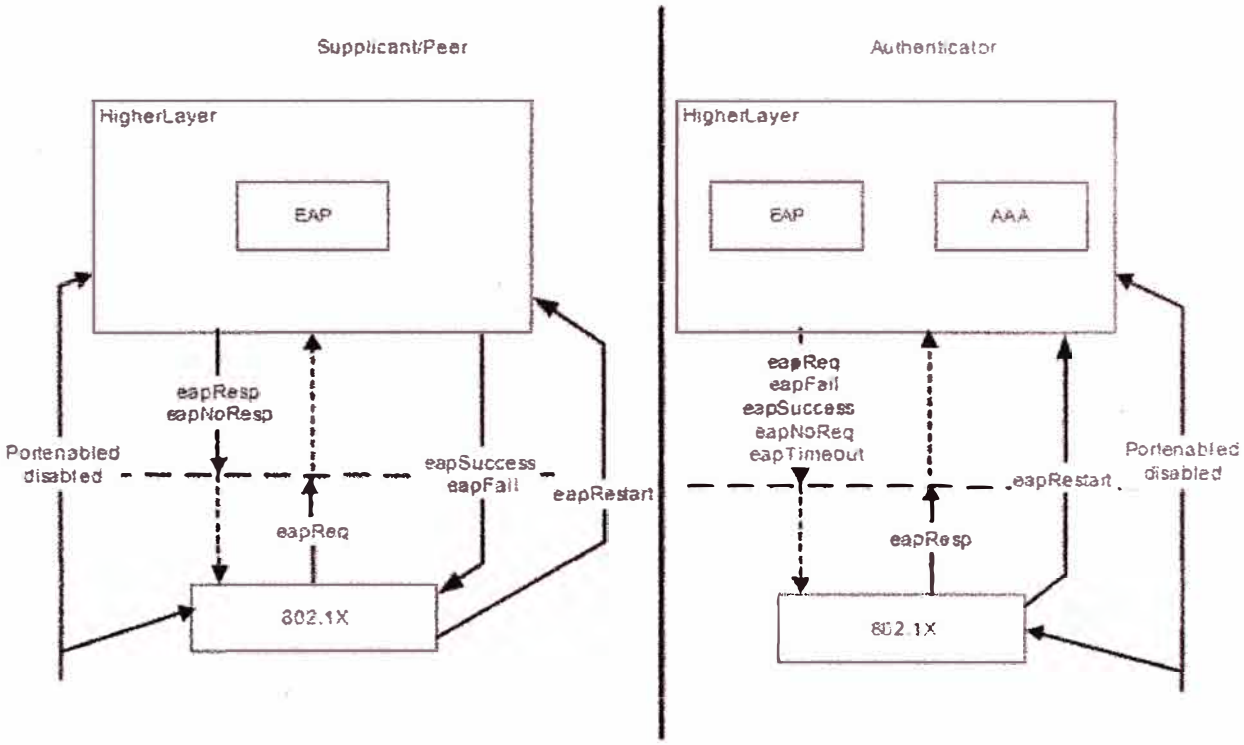


Fig.2.1 Diagrama de la interfaz de capa superior

En la capa superior, los métodos EAP y EAP asociado conducen al diálogo de autenticación, pero sobre la terminación la capa superior tomará de AAA para señalar el éxito o el fracaso al PACP, usando señales eapSuccess y eapFail. La separación entre la capa superior y el PACP es tal que todos los mensajes EAP intercambiados entre Suplicante y Autenticador son creados por el componente EAP.

El método EAP en el Autenticador actúa como un "pasante", enviando mensajes de retorno EAP y reenvío a un servidor de Autenticación que usa un protocolo AAA como transporte. La capa superior coordina el EAP y componentes AAA. RADIUS es como un protocolo de transporte que puede ser usado como una capa inferior para este mecanismo de envío. El uso de RADIUS para el envío pasante está descrito en IETF RFC 3579.

Más que sólo permitir un método predeterminado de autenticación, EAP permite al Autenticador PAE que solicite más información antes de determinar el mecanismo específico de autentificación. En EAP, el Autenticador PAE envía uno o varias peticiones (Requests) para autenticar el Suplicante PAE. La petición Request tiene un campo de tipo para indicar que esta siendo requerido. Ejemplos de tipos de petición Request incluyen Identidad, MD5, Contraseñas de tiempo y Tarjeta Token. El tipo de MD5 corresponde cercanamente al Protocolo CHAP (Challenge Handshake Authentication Protocol). Típicamente, el Autenticador enviara una petición Identity Request inicial seguido de uno o varias peticiones Requests de información de autenticación. Sin embargo, no se requiere una petición Identity Request inicial, y pueden evitarlo en casos en los cuales la identidad esta supuesta o cuando puede ser determinada por otro medio (como un método especifico de intercambio de identidad). El Suplicante PAE envía un paquete Response en respuesta a cada petición Request. Como con el paquete de petición, el paquete de respuesta Response contiene un campo de tipo que corresponde al campo de tipo de la petición Request.

El intercambio de Autenticación termina con una señal de Accept o Reject desde el Servidor de Autenticación. El Autenticador envía el paquete EAP incluido con la indicación Accept o Reject, mientras el cliente AAA que maneja como una capa inferior bajo EAP interpreta la señal e indica el éxito o fracaso al Autenticador, que establecerá el puerto controlado en autorizado o no autorizado de manera apropiada.

2.2 Inicio de Autenticación

La autenticación puede ser iniciada ya sea por el Suplicante PAE o por el Autenticador PAE. Si la autenticación esta habilitada en un puerto determinado, la autenticación es iniciada por el Autenticador PAE detectando que el estado operacional de la MAC asociada con el puerto, ha transitado de deshabilitado a habilitado. Como se indica, si el Autenticador PAE no recibe una respuesta, EAP retransmitirá el requerimiento de autenticación. Un Suplicante PAE puede iniciar la secuencia de autenticación enviando una trama EAPOL-Start.

2.2.1 Inicio del Autenticador

El Autenticador PAE típicamente iniciará la conversación cuando recibe una indicación que el puerto se ha hecho operable. Antes de que la autenticación comience, fuerzan el estado de puerto al estado no autorizado.

El Autenticador PAE inicia la secuencia de autenticación señalando la capa superior y luego enviando la trama EAP-Request dado por EAP. Típicamente, EAP comenzará el intercambio de autenticación con una trama EAP-Request; sin embargo, cualquier EAP-Request puede ser usado para iniciar el intercambio. Un Suplicante PAE que recibe una trama EAP-Request del Autenticador PAE responde con una trama EAP-Response proporcionado por EAP.

Los Autenticadores PAE pueden soportar reautenticación periódica, y pueden solicitar que un puerto se reautentique en cualquier momento. Por ejemplo, si se reinicializa el Sistema Autenticador, se puede recuperar el estado de autenticación entregando tramas EAP-Request en todos los puertos. Si un puerto controlado está en el estado autorizado previo a la reautenticación, entonces permanecerá en ese estado durante la reautenticación. Si falla la autenticación para un puerto controlado que estuvo en el estado autorizado durante la reautenticación, entonces el estado de autorización del puerto controlado es llevado a no autorizado para controlar el acceso externo a ese puerto de acuerdo al valor actual del parámetro OperControlledDirections.

2.2.2 Inicio del Suplicante

Para solicitar al Autenticador PAE inicie la autenticación, el Suplicante PAE envía un paquete EAPOL-Start. El Autenticador PAE que recibe un paquete EAPOL-Start, responde enviando un paquete EAP-Request que es elegido por EAP.

2.3 Desconexión con EAPOL

Cuando un Suplicante desea que el Autenticador PAE realice una desconexión (es decir, ponga el estado de puerto controlado a no autorizado), el Suplicante PAE genera un mensajes EAPOL-Logoff al Autenticador PAE. Por consiguiente, el Autenticador PAE inmediatamente coloca el puerto controlado en estado no autorizado.

2.4 Información de Expiración del Estado de Autorización

Los Autenticadores PAE pueden expirar la información del estado de autorización en una base periódica mediante la Máquina de Estado Reauthentication Timer. El periodo de tiempo para tales interrupciones es reAuthPeriod segundos desde la última vez que confirma el estado de autorización. La variable de estado reAuthEnabled controla si ocurre la nueva reautenticación periódica.

La reautenticación puede ser habilitado o deshabilitada, y el reAuthPeriod modificado, por gestión. Las configuraciones por defecto para el reAuthPeriod son 3600s (una hora) y para la reautenticación deshabilitada.

2.5 Retransmisión

El Autenticador PAE es responsable de la retransmisión de mensajes entre el Suplicante PAE y Autenticador PAE. En particular, EAP es el componente del Autenticador PAE que maneja la retransmisión, no las máquinas de estado IEEE 802.1X. Así, si se pierde un paquete EAP en el tránsito entre el Suplicante PAE y Autenticador PAE (o viceversa), el Autenticador PAE lo retransmitirá.

Las excepciones son los mensajes EAPOL-Start, que son retransmitidos, si fuera necesario por el Suplicante PAE, y cualquier mensaje EAP entregado durante los estados FAIL y SUCCESS. Como los mensajes entregados de los estados FAIL y SUCCESS del Autenticador (típicamente EAP-Failure y EAP-Success) no se confirman por el Suplicante PAE, no son retransmitidos por el Autenticador PAE. Si se pierde un EAP-Request, la maquina de estado del Suplicante PAE realiza una transición al estado CONNECTING en la expiración del temporizador authWhile.

En las implementaciones en las que la función de autenticación es realizada por un Servidor remoto de Autenticación, las retransmisiones pueden ser necesarias entre el Autenticador PAE y el Servidor de Autenticación. En este caso, puede ser necesario para la capa superior adoptar una estrategia de retransmisión que es más apropiada a las características de transmisión del camino de comunicación involucrado.

2.6 Consideraciones para Migración

Es preferible que la transmisión entre un entorno no autenticado y un entorno autenticado sea tan fluida como sea posible. Por ejemplo, cuando un Suplicante con capacidad de autenticación se conecta a un conmutador sin capacidad de autenticación, el Suplicante no recibirá un paquete EAP-Request. Como resultado, el Suplicante PAE iniciará una trama EAPOL-Start a la dirección MAC del grupo PAE. Como esta dirección es una de las direcciones que no son enviadas por Conmutadores (Bridges MAC), el Suplicante PAE no recibirá respuesta. De ahí, después de un período de interrupción conveniente, en el cual el EAPOL-Start ha sido retransmitido y no hubo respuesta, el suplicante puede asumir que está autorizado para acceder a la Red del Área Local.

Como el concepto de los puertos controlados y no controlados se aplica a sistemas que soportan funcionalidad Autenticador o Suplicante, un sistema que sólo soporta la funcionalidad Suplicante no puede transmitir tramas de datos antes de la terminación del proceso de Autenticación. De ahí, en el ejemplo anterior, el sistema Suplicante debe esperar hasta el final del periodo de expiración de Autenticación antes de iniciar los intercambios de datos vía el puerto del conmutador. Para permitir aplicaciones como DHCP, que se ejecutan inmediatamente en la conexión, puede ser conveniente forzar administrativamente el puerto del Suplicante al estado de Autorización en tales situaciones.

Cuando un Suplicante "conciente de no autenticación" se conecta al conmutador con autenticación habilitada, el Suplicante, sin tener PAE, ignorará las tramas EAP-Request. Como resultado el puerto permanecerá en el estado no autorizado. El suplicante será capaz de acceder a la Red de Área Local conmutada vía el puerto controlado del conmutador, sólo de acuerdo al valor del parámetro OperControlledDirections; el acceso será algunos servicios que están disponibles vía el puerto no controlado del conmutador que no están restringidos.

2.7 Retransmisión de tramas EAP

El Autenticador PAE es responsable de transmitir tramas EAP entre el Suplicante y el Servidor de Autenticación vía la capa superior. Este debería realizar algún reempaquetamiento de tramas EAP que es necesario a fin de convertir las tramas EAP transportadas como EAPOL entre el Suplicante PAE y el Autenticador PAE. Es responsabilidad de la capa superior realizar algún reempaquetamiento de tramas EAP requeridos entre el Autenticador y el Servidor de Autenticación. Desempeñando su función de transmisión, la información contenida en las tramas transmitidas EAP no es modificado si no es requerido convertir el formato de trama a/desde el formato EAPOL.

Las tramas EAPOL-Start y EAPOL-Logoff son transmitidas por el Suplicante PAE al Autenticador PAE; las tramas EAPOL-Key son transmitidas por el Autenticador PAE al Suplicante PAE y del Suplicante PAE al Autenticador PAE. Estas tramas no son transmitidas por el Autenticador PAE al Servidor de Autenticación.

La trama inicial EAP-Request es típicamente transmitida por el Autenticador PAE al Suplicante PAE y no aparece en la ruta de comunicación entre el Servidor de Autenticación y el Autenticador PAE.

Todas las tramas EAP recibidas desde el Suplicante PAE, son desencapsuladas por el Autenticador PAE de su formato EAPOL, para transferir como tramas EAP a EAP. Es responsabilidad de la capa superior formatear la trama EAP para transmitir hacia el Servidor de Autenticación de acorde con el protocolo AAA en uso entre el Servidor de Autenticación y el Autenticador PAE.

Todas las tramas del protocolo AAA recibidas por el Autenticador PAE desde el Servidor de Autenticación son convertidos a tramas EAP por la capa superior y luego pasados al Autenticador PAE. El Autenticador PAE luego convierte estas tramas EAP a formato EAPOL, según corresponda del puerto implicado, para la transmisión hacia el Suplicante PAE.

2.8 Transmisión de Información de Clave

El protocolo EAPOL opcionalmente soporta la transmisión de información de clave desde el Autenticador al Suplicante, o desde el Suplicante al Autenticador, siguiendo un intercambio de autenticación satisfactorio, en condiciones en el cual la encriptación esta disponible entre el sistema de Suplicante y Autenticador.

El uso de esta función es controlado por el parámetro keyTxEnabled, el cual puede ser modificado por el administrador. Un valor de verdad (TRUE) permite que la clave de la información sea transmitida una vez que keyAvailable y keyRun son fijados como TRUE.

keyAvailable puede ser fijado como TRUE administrativamente, puede ser fijado por la capa superior durante la autenticación. La figura 2.2 muestra la interface entre la capa superior y la capa clave IEEE 802.1X. que soporta transmitir material de la clave y señalizando keyAvailable. Note que si keyTxEnabled es verdadero (TRUE) entonces el dialogo de autenticacion EAP debe resultar en claves estando disponible en ambos Autenticador y Suplicante para que esto sea exitoso, si solo los métodos EAP que soportan a estos pueden ser usados en entornos donde se espera que EAP provee las claves.

La PACP también soporta una variable portValid que esta disponible para la capa superior (esto no es usado por implementaciones existentes, pero esta disponible para implementaciones futuras). portValid influye cuando un puerto autenticado pasa a ser autorizado. Esto permite al PACP que requiera dos condiciones antes de autorizar un puerto: autenticado y un canal de datos seguro.

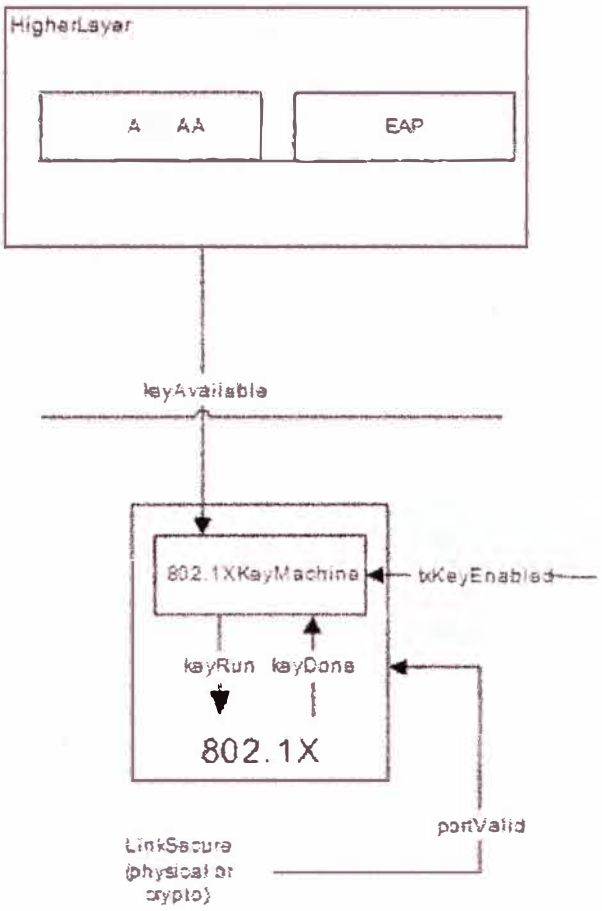


Fig.2.2 Clave de Capa Superior

En el siguiente capítulo se describe la situación de la red corporativa, detallando los equipos de comunicación que cumplen funciones principales, la topología de red en funcionamiento y los servicios de comunicaciones que se ofrece a los usuarios.

CAPITULO III
CASO DE ESTUDIO: ESCENARIO CORPORATIVO ACTUAL

3.1 Descripción

La red corporativa cuenta con una variedad de equipos de comunicación tales como hubs, switches, router. Los router brindan la salida a Internet e interconexión a la red académica (RAAP), los switches administrables establecen VLANs, tanto para conexión Publica, Privada y Raap. Estos equipos segmentan la red y se interconectan con los demás equipos de comunicación como switchs no administrables y hubs de acceso brindando conectividad a los usuarios finales.

La red corporativa soporta en mayor proporción tráfico de datos y video, generados por los servicios de correo electrónico, lista de correos, servicio Web, servicio de archivos, aplicaciones de intranet, aplicaciones administrativas y Videoconferencias que se realizan con instituciones investigativas y para exponer en conferencias los trabajos que se realizan en las institución, en menos proporción soporta tráfico de voz generados por los proyectos pilotos de las áreas de investigación. Próximamente se tiene planificado transportar voz implementando una solución de telefonía IP para toda la institución.

El rendimiento de la red de datos disminuye cuando se transmite Videoconferencias, presentando lentitud en la comunicación con las demás aplicaciones internas y navegación web que se ofrece en la institución, perjudicando el trabajo de los usuarios finales. Para mejorar la calidad de comunicación en la red corporativa y el soporte para futuros proyectos se esta apostando en invertir en equipos de comunicaciones con mayor rendimiento y características técnicas, en mejorar el cableado estructurado actual ampliando velocidad de transmisión por el medio físico y la calidad de señal. El cableado estructurado con el que se cuenta es cable UTP categoría 5, se esta implementando por etapas migrando a cable UTP categoría 6, el backbone de la red corporativa es por medio de fibra óptica multimodo que a través de media converter se interconectan a los puertos RJ45 de 1000 Mbps de los switches.

3.2 Infraestructura de la Red de Datos

3.2.1 Topología de la Red de Datos

La topología empleada consiste en estrella extendida (Fig. 3.1), donde el nodo central esta soportado por un conmutador 3com 4900, segmentando la red empleando Vlans para el acceso público, privado y Raap, al cual se interconectan los demás conmutadores del tipo 3com 3226 y 4500 configurado con Vlans, que cuentan con soporte de capa 2/3. La interconexión física entre los conmutadores remotos se realiza a través de enlaces de fibra óptica multimodo, empleando conversores de fibra 1000Base-SX a 1000Base-T en los extremos, los cuales se interconectan por medio de patch cord UTP a los puertos gigabits de los switches.

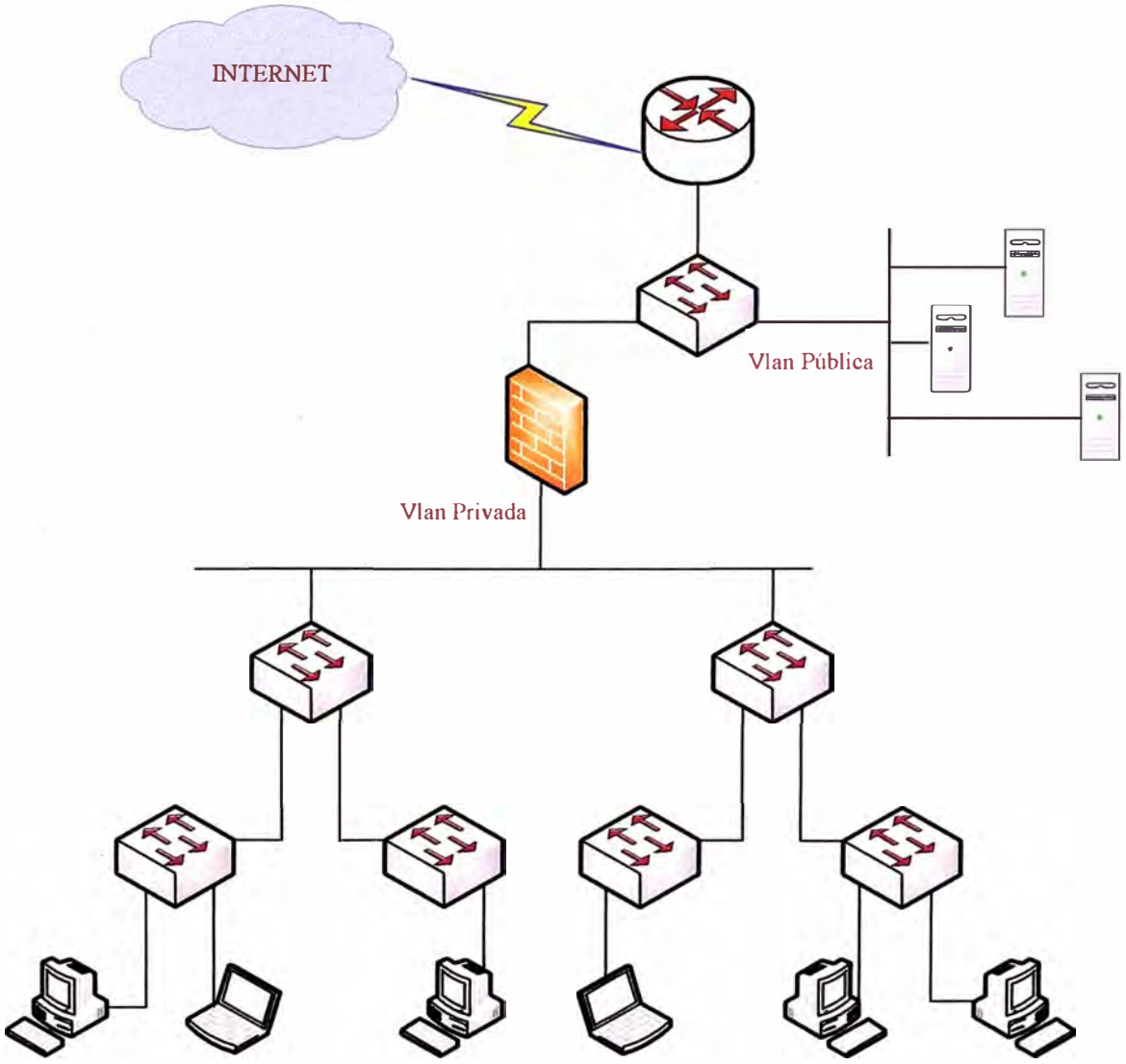


Fig.3.1 Topología de Red

3.2.2 Modelo de Red

Utilizando el modelo jerárquico, la red de datos de la institución bajo estudio se puede describir del modo siguiente:

a) Capa de Acceso

Es el nivel que brinda el acceso de los usuarios a la red de datos. Actualmente se cuenta con una variedad de equipos de comunicación tales como hubs 10Mbps, hubs 100Mbps y switches 10/100Mbps capa 2, ubicadas en las diferentes áreas de la institución.

La mayoría de equipos de comunicación soportan básicamente protocolo Ethernet IEEE 802.3i, IEEE 802.3u y IEEE 802.3x, los cuales se proyecta reemplazar con switches Fast Ethernet/Gigabit Ethernet con características de seguridad de puerto, Vlan, 802.1X, calidad de servicio (QoS), agregado de enlaces y algunos switches además que soporten Power over Ethernet (PoE) para brindar conectividad y alimentación eléctrica a los teléfonos IP con que se proyecta contar.

b) Capa de Distribución

Es el nivel que transporta los requerimientos de comunicación de un usuario hacia un servidor o sus pares. Este nivel proporciona conectividad basado en determinadas políticas establecidas, segmentación de la red y aislamiento de problemas de red. La capa de distribución se encarga de proporcionar un acceso controlado al núcleo. Dentro de este nivel se cuenta con conmutadores 3com 3226 y 3com 4500, los cuales tienen soporte de capa 2/3. Para mejorar el funcionamiento y rendimiento de la red corporativa se necesita aplicar políticas de seguridad mediante Listas de Control de Acceso (ACL), proporcionar funciones de enrutamiento entre Vlan, manejar la prioridad del tráfico que proviene de los switches de la capa de acceso aplicando QoS, asegurar la disponibilidad adecuada implementando redundancia, proporcionar tolerancia a fallas que los switches de acceso requieren mediante enlaces múltiples a los switch de distribución y una tasa de envío alta para que todo el tráfico entrante de los múltiples switches de acceso que se conectan a los switches de distribución sean enviados tan rápido como sea posible a los switches de la capa principal mediante enlaces agregados de un alto ancho de banda.

c) Capa de Núcleo Principal

Es el nivel central encargado de proporcionar la conmutación entre los diferentes segmentos de la red corporativa a alta velocidad. Ese nivel es de alta criticidad debido a que el núcleo es el elemento central de la conectividad, y por tanto debe contar con alto nivel de disponibilidad y adaptación a cambios de manera rápida. Dentro de este nivel se cuenta con conmutadores 3com 4900.

Se requiere contar con enlaces agregados de alto ancho de banda para soportar el tráfico proveniente de los switches de distribución y transportarlo a una tasa elevada. Para brindar prioridad del flujo de información requerimos que los switches soporten QoS

3.2.3 Equipos de Comunicación

En la tabla 3.1 se resume las características técnicas de los equipos de comunicación utilizados en las capas de distribución y principal.

TABLA Nº 3.1 Relación de Equipos de Comunicación

Cantidad	Descripción	Modelo
4	Switch 3com 24 puertos 10/100Mbps 2 puertos 1Gbps, capa 2/3	SuperStack Switch 3226
4	Switch 3com 24 puertos 10/100Mbps 2puertos 1Gbps, capa 2/3	3com Switch 4500
1	Switch 3com 12 puertos 10/100/1000Mbps 2puertos 1Gbps, capa 2/3	SuperStack Switch 4900
1	Router Cisco 2 puertos 10/100Mbps	Cisco 2600

Los equipos señalados poseen las siguientes capacidades y funcionalidades técnicas:

a) SuperStack Switch 3226

El switch 3226 es un equipo de alto desempeño que soporta propiedades de capa 2 de conmutación y capa 3 de enrutamiento, cuenta con 24 puertos 10/100Mbps y 2 puertos 1Gbps. Los estándares Ethernet que soporta son IEEE 802.1p, IEEE 802.1Q, IEEE 802.1w, IEEE 802.1X, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3i, IEEE 802.3u, IEEE 802.3x y IEEE 802.3z.

b) 3com Switch 4500

El switch 4500 ofrece conmutación de capa 2 y enrutamiento dinámico de capa 3. Contando con una variedad de características como control de acceso de red basado en el estándar 802.1X, listas de acceso (ACL), clase de servicio - calidad de servicio (802.1p), soporte del protocolo Spanning Tree y Rapid Spanning Tree, Vlans (802.1Q), RIP, SSHv2, SNMPv3.

c) SuperStack Switch 4900

El switch 4900 de alto rendimiento con 12 puertos 1Gbps, escalable, ofrece funcionalidades avanzadas capa 2 y capa 3 tales como filtrado multicast, servicios de mejoras QoS/CoS, Lan virtuales (802.1Q), priorización y clasificación de trafico, rutas estáticas, RIP/RIPv2 , protocolo Spanning Tree y Rapid Spanning Tree.

d) Cisco 2600

Es un router de acceso multiservicio modular que proporciona configuración flexible LAN y WAN. Soporta los estándares Ethernet IEEE 802.1Q Vlan, IEEE 802.1p CoS, IEEE 802.1D.

3.3 Servicios de Red y Comunicaciones

En la corporación se cuenta con los servicios de red, comunicación y aplicaciones informáticos para la operatividad de la institución. Así tenemos: servicio de correo, webmail, servicio web, intranet, pdc, listas de correos, videoconferencia, que facilita las comunicaciones y trabajo de los usuarios.

Mayoritariamente los servicios en producción se han implementado basados en software libre y en entornos Linux, como se indica en la Tabla 3.2, se tienen:

TABLA Nº 3.2 Relación de Servicios en Producción

Servicio	Software
Correo	postfix, spamassasin,clamav, mailscanner
Firewall	Iptables
Intranet	apache, php, mysql, tomcat
Lista de correos	Mailman
Pdc	samba, clamav
Proxy	squid, sarg
Webmail	Horde
Web	apache, php, MySQL

En el capítulo siguiente comentamos los inconvenientes que ofrece la red corporativa y nos enfocamos en el control de acceso a la red mostrando la alternativa, detallando la implementación y validación de la solución.

CAPITULO IV
INGENIERIA DE REDES Y SERVICIOS TELEMATICOS

4.1 Análisis de la problemática y mejoras

La infraestructura de red actual cuenta con limitaciones y deficiencias en torno a los equipos de comunicación con los que se cuenta en el nivel de acceso. La calidad y características técnicas de los equipos de comunicación que brindan acceso a los usuarios finales son mínimas brindado básicamente conectividad, los hubs generan un nivel elevado de colisiones no pudiendo agrupar en redes lógicas, ni evitando los dominios de colisión y broadcast que se generan en la red.

Los usuarios requieren contar con una red de alto desempeño que admita aplicaciones de misión critica, es decir que la red este diseñada para tener un nivel de operatividad de casi 99.99% del tiempo, que soporte el intercambio de diversos tipos de trafico de red, entre ellos archivos de datos, correo electrónico, telefonía IP, videoconferencia, y nuevas aplicaciones, lo que viene a ser la convergencia de servicios dentro de una única infraestructura de red. Estas necesidades requieren de contar con equipos de nivel superior, equipos de alta tecnología que están diseñados para ser confiables, con características como fuentes de alimentación redundantes y capacidades de migración en caso de fallos, además estos equipos están diseñados para transportar grandes volúmenes de tráfico de red.

Los equipos de comunicación del nivel de distribución, deben controlar el flujo de tráfico para optimizar el ancho de banda, soportar priorización de trafico si es necesario para las aplicaciones que lo requieran, filtrar el tráfico entrante y saliente con fines de seguridad y administración, garantizar que el tráfico entre los hosts de los usuarios finales en una misma red continúen a nivel local y que derive los que están destinados a otras redes mediante el soporte de enrutamiento. Para asegurar y brindar una alta disponibilidad en la operatividad de la red se puede incorporar redundancia en el nivel de distribución y principal de la red. Así se consigue proporcionar la comunicación permanente a los servicios de red sin interrupciones y la comunicación entre los usuarios finales.

El nivel principal debe proporcionar interconectividad de alta velocidad con el nivel de distribución y los servidores en producción, con conexiones redundantes, tolerancia a fallas y convergencia rápida.

El tema de seguridad y la administración de la red es un factor importante para proporcionar a los usuarios que trabajen en forma confiable. Las demandas de mejorar la seguridad contra ataques externos nos obligan a realizar cambios en la topología de la red. Es recomendable que la granja de servidores en producción se ubique en una zona física de seguridad denominada DMZ que estará protegida por el Firewall, denegando por defecto todo acceso y habilitando el tráfico únicamente a los servicios necesarios de los servidores de producción, para el acceso de usuarios internos y externos. La nueva estructura de la topología de red se muestra a continuación (Fig. 4.1):

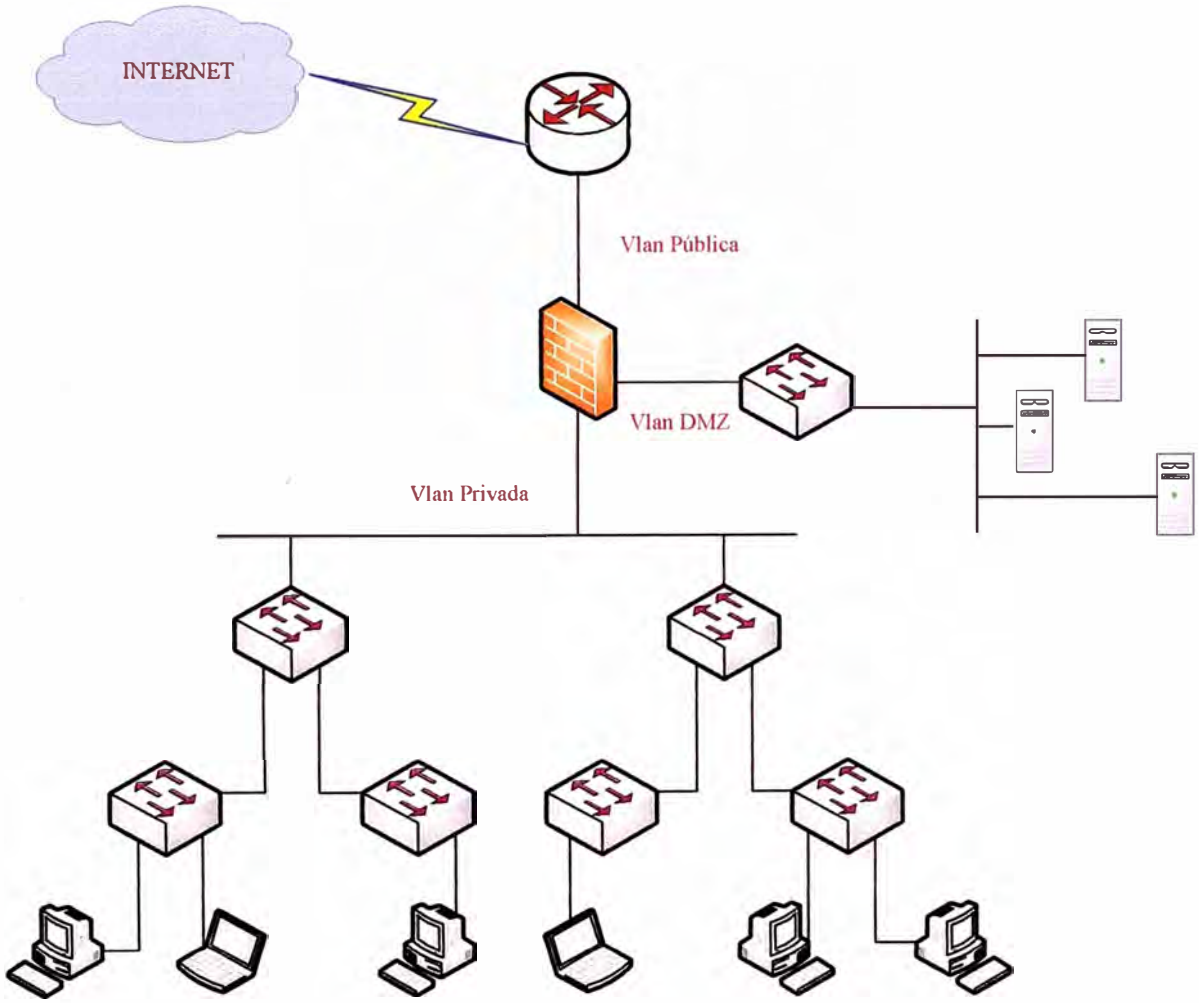


Fig. 4.1 Topología de Red Mejorada.

Con este esquema se mejora la seguridad del acceso externo e interno a los servicios de comunicación de redes en producción, los cuales se establecen en las políticas de seguridad del Firewall.

Un punto muy importante, el cual es el interés de este informe, es lo relacionado con la seguridad, accesibilidad y la disponibilidad de la red corporativa, tanto de la red como de las aplicaciones que viajan por ella. Los efectos negativos de la falta de disponibilidad se traducen en pérdida de productividad y en muchos casos pérdidas de ingresos. Estudios realizados por diferentes consultoras, llegan a la conclusión que los ataques contra los servicios de comunicaciones de redes que brindan las empresas, en mayor porcentaje provienen de usuarios dentro de su red.

El acceso a la red corporativa de dispositivos sin las mínimas medidas de seguridad, en la práctica implica riesgos. Los dispositivos como portátiles pueden estar parcial o totalmente desprotegidos, sin ningún software de seguridad instalado y estar infectados por virus, spyware, malware o cualquier otra programa malicioso, una vez conectados a la red corporativa, acaban siendo diseminados entre los dispositivos del resto de usuarios. Como una medida de prevención para evitar ataques internos, se estudia el implementar tecnologías que permitan el control de acceso a la red corporativa, los usuarios previamente autenticados recién podrán tener conectividad a la red corporativa y acceso a los servicios de comunicaciones de red.

Adicionalmente para mejorar los servicios de comunicación de la red corporativa, se implementara un servicio de DNS cache, el servidor con el servicio implementado se ubicara en la DMZ. Este servicio nos brindara que las peticiones de resolución de nombres de dominios ya no tengan q realizarse al servidor DNS del Proveedor de Internet, si no que las consultas se realizaran de manera local, consultando al DNS cache. La respuesta del DNS cache será en base a sus tablas de consultas almacenadas o realizara la consulta al servidor DNS del Proveedor de Internet y lo almacenará en sus tablas para las próximas solicitudes.

4.2 Evaluación de Alternativas

El problema con la que cuenta la mayoría de organizaciones es el de garantizar que cualquiera que se conecte a la red corporativa, sea no sólo identificado y autorizado apropiadamente, sino también que esté usando un dispositivo seguro. Lo que se propone como alternativa se denomina seguridad de extremo, control de admisiones o como es conocida más generalmente control de accesos a la red (Network Access Control - NAC), estas tecnologías marcan una nueva tendencia a la que se están adaptando todos los grandes fabricantes de soluciones de redes y seguridad. La industria no llega a un acuerdo sobre la denominación de la categoría para incluir esta clase de soluciones,

generando confusión en este mercado. Además existen diferentes ideas relativas a los estándares, funciones requeridas y enfoques tecnológicos sobre en qué tipo de dispositivo se deberían implementar estos productos. Pero lo mas importante es que hay un consenso es que NAC es una tecnología que cada vez cobra más fuerza.

4.2.1 Funcionalidades NAC

A medida que la industria amplía el abanico de soluciones que podrían considerarse NAC, la categoría de tecnologías incluidas en estas siglas se hace más confusa. Dos fabricantes que aparentemente pertenecen al mismo mercado pueden ofrecer capacidades y funcionalidades muy diferentes. Y, por el contrario, otros que aseguran estar en mercados diferentes ofrecen sistemas que se parecen en buena parte a los sistemas NAC. Tal ambigüedad complica la elección del usuario, que, en todo caso, ha de tener en cuenta qué prestaciones son las que mejor se adaptan a sus necesidades concretas. Las siguientes son las funcionalidades NAC que potencialmente se pueden encontrar en el mercado, aunque no siempre todas estarán presentes en todos los productos.

a) **Autenticación**. Algunos sistemas NAC ofrecen la capacidad de autenticar usuarios, con independencia del dispositivo que estén usando o desde dónde se estén conectando. Otros ofrecen integración con productos de autenticación ya instalados. Aquí la elección dependerá en muchos casos de las inversiones ya realizadas en soluciones de autenticación.

b) **Análisis de seguridad de extremo**. Otra función clave es la posibilidad de conocer si el dispositivo cumple con los estándares de seguridad de extremos definidos por la organización. Aunque tales estándares varían en cada empresa, el sistema NAC ha de ser capaz de chequear los sistemas operativos y programas antivirus, las actualizaciones de antispyware, antispam y antivirus, los parches, la configuración del cortafuego personal y el software de prevención de intrusiones del dispositivo cliente. El nivel de vigilancia implantado en cada caso dependerá de la tolerancia de la empresa con los riesgos y la latencia, ya que cuanto más a fondo se chequea, por lo general, más tiempo llevará poder acceder a la red. Una vez completado el chequeo, si el sistema cumple totalmente las normas de seguridad de la organización, se pasa a la siguiente fase; pero si no las cumple, se le deniega el acceso y, en algunas ocasiones, se le envía a una "zona de cuarentena". Lo que sucede aquí depende en buena medida

de la solución tecnológica elegida y de las políticas del usuario. A veces se le permite el acceso a recursos como el email o Internet pero se le deniega a cualquier otro recurso corporativo interno. En otras, se le aplica inmediatamente medidas para securizar el sistema. En este caso, es de gran utilidad que el sistema NAC pueda integrarse con otras herramientas de seguridad, como los sistemas de gestión de parches y antivirus. Algunos sistemas NAC incluso informan automáticamente de los motivos por los que se deniega el acceso y de las medidas a tomar para solucionar el problema. En general, el objetivo debería ser denegar el acceso cuando sea necesario pero sin interrumpir la actividad del usuario innecesariamente.

c) **Autorización.** Otra función potencial de NAC es participar en la autorización de los accesos a determinados recursos según la identidad del usuario. Para ello, el sistema NAC trabaja en sintonía con los sistemas de autorización ya existentes, como los directorios LDAP, Active Directory y sistemas RADIUS. La integración con estos mecanismos de autorización obvia la necesidad de almacenar nuevos datos de autenticación y permite emplear las políticas ya establecidas para esos sistemas existentes.

d) **Protección continua.** Algunos sistemas NAC siguen monitorizando el sistema incluso después de que le sea autorizado el acceso. Aquí es donde las diferencias entre fabricantes se hacen más pronunciadas, y donde los sistemas NAC comienzan a asumir funciones hasta ahora exclusivas de los IPS. Aunque el enfoque exacto puede variar según la solución de que se trate, la idea es que NAC sigue monitorizando la sesión de usuario para detectar actividades sospechosas. Como con el chequeo de integridad inicial, lo que el sistema NAC hace después de identificar tal actividad puede variar, desde cortar la sesión a enviarla a una zona de aislamiento. El objetivo es detectar actividades maliciosas incluidos gusanos y malware en general que no se adapten a las políticas y detenerlas antes de que causen algún daño. Este tipo de funciones es una parte clave de lo que ofrecen los NAC en protección del interior de la red. Incluso un dispositivo de extremo totalmente parcheado y con el software de seguridad debidamente actualizado puede ser infectado por un gusano. Solo la monitorización continua después de que el dispositivo se haya conectado a la red impedirá que el gusano se propague por ella. Asimismo, resulta útil garantizar que los dispositivos cumplen con las políticas vigentes mientras dura su

conexión a la red, pues, aún en el caso de que no exista peligro de infección activa, los recursos se pueden ver comprometidos. En este caso, de nuevo, la empresa puede optar por aislar estos puntos extremos hasta que vuelvan a cumplir las políticas.

4.2.2 Estándares NAC

Otra de las cuestiones que siembran confusión en NAC es, como sucede con la gran mayoría de las tecnologías clave, la amplia variedad de estándares en juego, cada uno con sus propios seguidores. Pero, al día de hoy, los dos enfoques con mayor peso en el mercado son las iniciativas lideradas por Cisco y Microsoft. No hay que olvidar tampoco la propuesta independiente que la Trusted Network Computing Group está desarrollando como implementación de referencia.

a) **NAC Framework.** Cisco fue el primero en escena con su tecnología Network Access Control (NAC) Framework, que, según la compañía, ya cuenta con el respaldo de más de 60 firmas de seguridad. Esta propuesta pretende integrar componentes de infraestructura de red con seguridad, y se basa en herramientas de terceros, como software antispam y antivirus.

   El Cisco NAC Framework requiere la instalación de un pequeño agente (Cisco Trust Agent) en cada dispositivo cliente encargado de pasar información de seguridad sobre tal dispositivo a un servidor de políticas. Este determina si dar acceso totalmente garantizado al dispositivo, denegárselo o tomar medidas intermedias.

   El punto más débil del enfoque de Cisco es, que funciona sólo con infraestructura del fabricante, mientras que otras propuestas como las de algunos appliances NAC trabajan con routers y conmutadores de cualquier compañía o, al menos, con aquellos que soportan determinados estándares, como 802.1X, que basa el control de los accesos en el puerto. Además, para la consultora, el hecho de que el NAC de Cisco requiera la instalación de Trust Agent en el cliente limita su utilidad en entornos abiertos donde participan socios y clientes con dispositivos fuera del control del departamento TIC de la empresa.

b) **Network Access Protection (NAP).** Al igual que la propuesta de Cisco depende fundamentalmente del equipamiento del fabricante, la iniciativa Network Access Protection (NAP) de Microsoft gira alrededor de los sistemas operativos Windows de nueva generación: el de sobremesa Windows Vista y el de servidor

Windows Server 2008. Como es lógico, Microsoft toma un enfoque centrado especialmente en la aplicación, limitando el acceso a las aplicaciones de los clientes que no cumplan las políticas y normas de seguridad. Como Cisco NAC, sin embargo, proporciona un sistema de políticas y permite el chequeo del estado de seguridad de los clientes, securizándolos cuando es preciso. Y al igual que Cisco da soporte nativo de sus iniciativas NAC en muchos de sus routers, conmutadoras y cortafuegos, NAP incluye API que permiten a los desarrolladores integrarla con los componentes de la infraestructura de red. Eso sí, aunque Microsoft asegura estar estudiando también el soporte de clientes Windows XP con Service Pack 2, de momento NAP requerirá el servidor Windows Server 2008 y el cliente Vista.

c) **TNC de Trusted Computing Group.** NAC es solo uno de los numerosos problemas de seguridad que la asociación industrial Trusted Computing Group (TCG) está intentando resolver desde 2003. Como tal, ha desarrollado la especificación Trusted Computing Module para almacenar contraseñas, claves y certificados digitales, y avanza en la definición de Trusted Network Connect (TNC) para resolver el reto que representa NAC. TNC describe una arquitectura abierta que detalla cómo determinar la seguridad en el extremo antes de dar acceso a ningún recurso de red, siguiendo un modelo basado en políticas. La arquitectura persigue la interoperatividad entre soluciones de control de acceso a la red y, por tanto, pretende integrarse con mecanismos NAC ya existentes. Según algunos expertos, todavía pasará bastante tiempo antes de que la industria soporte el estándar en sus productos. Además, la ausencia de Cisco en TCG supone un inconveniente para su adopción masiva, pese a que cuenta con un amplio soporte de la industria, incluido Microsoft.

4.2.3 Opciones de implementación

Existen distintas opciones de implementación, dos son las principales: actualizar la infraestructura de red (el enfoque de Cisco) o usar un appliance autónoma. Aunque no habría que olvidar otras dos: los dispositivos VPN SSL con determinadas funciones NAC y el recurso del outsourcing.

a) **Actualización de la infraestructura.** En esencia, Cisco NAC Framework obliga a que todos los routers y conmutadores del fabricante integrantes de la solución han de tener una versión de IOS relativamente reciente, a partir de la

12.3(8)T. Y esto podría resultar un proceso largo y costoso para algunos usuarios. La instalación del Trusted Agent en todos los dispositivos cliente añade aún más costes y complejidad. Por el lado positivo, tener varios routers y conmutadores implicados en NAC es una buena solución, por cuanto todo el tráfico tiene que pasar a través de estos dispositivos en algún punto. Además, este enfoque saca partido del resto de iniciativas de seguridad de Cisco, y muy especialmente de la estrategia Self-Defending Network, dirigida, según la compañía, a mejorar la capacidad de la red para "identificar, prevenir y adaptarse a los retos". Asimismo, la implementación de NAC en la infraestructura de red aporta un mayor grado de escalabilidad. Cisco, por supuesto, no es el único fabricante que apoya este enfoque. En realidad, cualquier suministrador de conmutadores, routers, cortafuegos y otros tipos de dispositivos de seguridad podrían seguir esta aproximación, que implica típicamente el soporte del estándar 802.1X.

b) **Dispositivos NAC.** En comparación con la creación de NAC en la infraestructura de la red, el enfoque basado en dispositivo es más fácil de implementar, ya que no exige actualizar routers, conmutadores ni cortafuegos. NAC se implementa en un dispositivo autónomo situado en un punto estratégico de la red, desde donde puede ver todas las peticiones de los clientes que intentan acceder a los recursos. Pueden ser instalados rápidamente y resultan muy efectivos, pues no implican cambios sustanciales. Hay experiencias reales en las que, incluso, se ha conseguido tener los sistemas activos en sólo uno o dos días. No es de extrañar, por tanto, que varios fabricantes ofrezcan ahora ambas soluciones, permitiendo instalar agentes donde resulta más útil y dispositivos NAC donde no es posible o simplemente no se desea. Otra ventaja de algunos dispositivos NAC es que además pueden trabajar con infraestructura de red de cualquier fabricante, así como con la mayoría de los sistemas operativos cliente y servidor. Por ello, este enfoque puede representar la mejor opción para empresas con entornos heterogéneos. En cualquier caso, la cuestión es si se quiere que la inteligencia y el reforzamiento de políticas corran en los conmutadores o en una entidad separada.

c) **Outsourcing.** El outsourcing es siempre una alternativa. Y para soluciones NAC lo es aún más para aquellas empresas que ya tienen externalizado una buena parte de sus funciones TIC. Todavía es un mercado incipiente, si se compara con

el gran interés que despierta hoy el outsourcing de otras funciones de seguridad, como las de cortafuegos e IDS.

4.2.4 Consideraciones tecnológicas

Con independencia de que camino se siga hacia NAC, siempre habrá que evaluar diversas consideraciones tecnológicas, como si usar agentes en las máquinas cliente, firmas o esquemas de detección de intrusiones basadas en el comportamiento, opciones de cuarentena, en línea o fuera de banda y cómo manejar los dispositivos que no pueden ser gestionados. Y además hay que tener en cuenta que una misma cuestión puede tener más de una respuesta. Todas las alternativas tienen pros y contras, y, muy probablemente, una solución no satisfará a todos los usuarios: este acaba siendo el reto. Los usuarios han de saber muy bien qué quieren realmente proteger y de qué peligros. Las respuestas a estos temas harán más fácil la elección de la arquitectura más adecuada para las necesidades corporativas.

a) **Elección de Agentes.** Para trabajar más eficientemente, algunos sistemas de gestión requieren un agente de software en el dispositivo a administrar. Dicho agente recoge información de la máquina en la que reside y, además, puede hacer los chequeos de seguridad que NAC implica. Los que defienden los sistemas sin agentes dirán que el enfoque contrario supone un problema de gestión en sí mismo, especialmente en empresas con cientos o miles de máquinas clientes. En su opinión, es preferible que el sistema NAC pregunte a la máquina cliente cuando necesite información, en el momento que lo necesite. Es decir, no es necesario instalar ningún software en el cliente, lo que es de utilidad cuando hay dispositivos que no son propiedad de la empresa, sino de sus socios y clientes, sin embargo, muchos fabricantes no creen que NAC pueda tener éxito si no se basa en agentes. Además, que la instalación de agentes no es tan compleja, pues, al fin y al cabo, se trata de pequeñas piezas de software que pueden ser difundidas automáticamente a las máquinas clientes, o incluso ser descargadas por los propios usuarios desde una URL. En general, si el agente aporta ventajas en cuanto a la seguridad de la red, será bien recibido por los usuarios. La elección se realizaría en cuenta los requerimientos de los clientes, habiendo muchos fabricantes de sistemas NAC ofrecen ambas alternativas. Así, el enfoque basado en agentes tiene sentido para aquellos sistemas que se encuentran bajo el control del departamento TIC, como los PC de sobremesa y

los portátiles asignados por la empresa. De este modo, se consigue una solución homogénea en la que los usuarios experimentan un acceso más ágil, al asumir el agente buena parte del procesamiento requerido en cuanto a verificación y cumplimiento de las políticas de seguridad. Por el contrario, el enfoque sin agentes es una opción correcta cuando se quiere dar acceso a socios y otros usuarios externos que disponen de dispositivos propios. También es una alternativa viable en entornos con un elevado número de clientes y no se desea tener que gestionar todos esos agentes. Además, los fabricantes están mejorando la tecnología sin agentes para que resulte más efectiva. Por ejemplo, existen hoy técnicas que permiten hacer un chequeo rápido del historial de seguridad de un cliente para detectar riesgos significativos. En este caso, el dispositivo se somete a un chequeo más a fondo; si no existen riesgos importantes, se le da acceso rápidamente, reduciendo así el problema de la latencia.

b) **Detección basada en firma.** Aún después de que un cliente pase todos los chequeos de seguridad y consiga ser conectado a la red, muchos sistemas NAC siguen monitorizando la sesión a fin de asegurar que permanece libre de virus, gusanos y otras formas de malware. Para ello, los sistemas NAC emplean distintas tecnologías, una de las cuales es la detección basada en firma, la misma que utilizan los sistemas IDS para detectar intrusiones. Por ello, es común que los fabricantes de NAC licencien esta tecnología a las firmas de IDS. Actualizando las firmas con un proceso automático, similar al de la actualización de antivirus, es posible identificar cualquier intento de sacar partido de las vulnerabilidades conocidas.

c) **Detección basada en comportamiento.** El lado negativo de la detección basada en firmas es obvio: sólo resulta eficaz con las vulnerabilidades conocidas y para las que ya existe una solución. Por tanto, otros tipos de ataques con objetivos más definidos pueden pasar inadvertidos. Más alcance tiene la detección basada en comportamiento, ya que trata de identificar cualquier tipo de tráfico que esté fuera de la norma, indicando si un dispositivo está infectado o no cumple las políticas. Los sistemas de análisis del comportamiento trabajan de tres formas principales: monitorización de direcciones IP no utilizadas, mediante sondas y monitorización de flujos de red.

   1. Monitorización de direcciones IP no utilizadas. Cualquier red cuenta con direcciones IP que no están siendo usadas en un momento dado y,

obviamente, no debería haber motivo para que un usuario legítimo intente utilizarlas, salvo que pretenda atacar a un sistema. La monitorización de estas direcciones IP puede detectar estos intentos y alertar al administrador para que tome la acción apropiada, generalmente, la denegación del acceso del usuario.

La ventaja de este enfoque es que no se producen falsos positivos, como sucede habitualmente en los sistemas basados en firma; si se detecta una conexión a una dirección IP "oscura", se sabe que es un problema real. Esto representa un gran beneficio por cuanto elimina todo el trabajo extra que generan los falsos positivos.

ii. Sondas de red. Otra forma de identificar tráfico anómalo es instalar sondas en varios puntos de la red para monitorizar el flujo de tráfico, agregar los datos obtenidos y reportarlos a un controlador inteligente central. El controlador entonces analiza toda esa información para encontrar cualquier actividad anómala o no autorizada. Aunque esta técnica puede ser efectiva, no es inmune al problema de los falsos positivos. Por ejemplo, un nuevo servidor de aplicaciones podría generar, por su propia naturaleza, un patrón de tráfico fuera de la norma pero que no es malicioso. Además, las sondas tienen el inconveniente de que han de ser instaladas y gestionadas.

iii. Detección basada en flujos. La detección basada en flujos es similar al esquema de sondas, excepto en que "aprende" las líneas básicas del tráfico normal de los routers y los conmutadores. Si bien esta técnica elimina la molestia de instalar y gestionar las sondas, también ve limitada su eficiencia por la proliferación de falsos positivos.

d) Opciones de cuarentena. Entre las diferencias existentes entre los distintos productos NAC, se encuentra el modo en que cada fabricante trata las conexiones de los sistemas que son infectados, se mueven fuera de las políticas o suponen un alto riesgo. Un enfoque popular consiste en reconfigurar el puerto cliente de modo que sólo pueda conectar con una LAN virtual específica creada para ese propósito y aislada de todos los demás recursos de la red. Allí se trata de solucionar su situación mediante acciones como, por ejemplo, actualizaciones de software antivirus. Esta técnica impide que los clientes peligrosos infecten al resto de la red, pero no es efectiva para proteger a los clientes que también se encuentran en esa VLAN de cuarentena. Un problema que se vuelve más grave

cuando uno de esos clientes finalmente es autorizado como usuario legítimo. En el mejor de los casos, los clientes autorizados tendrán que volver a ser limpiados, y en el peor, pueden sufrir daños. Se añade una nueva consideración más. ¿Qué sucede cuando el dispositivo cliente de un alto directivo, por ejemplo, no tiene el antivirus actualizado? Si el responsable de TI quiere conservar su empleo deberá poner en cuarentena a los clientes con cierta flexibilidad. Para ello, diversos fabricantes de NAC están introduciendo la técnica de cuarentena basada en políticas, según la que los sistemas NAC consideran el tipo y perfil antes de tomar una decisión. En el ejemplo anterior, el NAC podría configurarse para dar a los altos directivos acceso inmediato a los recursos al tiempo que se genera una alarma para que el departamento TIC tome medidas personalmente. Asimismo, un dispositivo que no cumpla con las políticas podría ser enviado a cuarentena para todos los recursos excepto aquellos que tratan la actualización del antivirus. Otro modo de abordar la cuarentena es aislar completamente cada cliente sospechoso, de modo que no sólo no pueda conectarse con recursos, sino tampoco con otros clientes. Esto implica enviar al cliente a su propia VLAN privada para ser tratado en consecuencia.

e) **En línea o fuera de banda.** También hay que considerar dónde se instalan los sistemas NAC, y de qué modo observará el tráfico. Los defensores del método "en línea" aseguran que es mejor que el dispositivo NAC se establezca en la red, detrás del conmutador de acceso, para que todo el tráfico pase a su través. Este enfoque permite ver todo el tráfico y aporta un gran control a la hora de detener gusanos, por ejemplo. En el lado negativo, dependiendo del tamaño y estructura de la red, puede obligar a tomar algunos pasos no agradables para asegurar que los sistemas NAC pueden "ver" todo el tráfico, como el encaminamiento de los flujos o el despliegue de un número elevado de cajas. Además, puede crear un problema de latencia, especialmente para aplicaciones sensibles a los retardos, como la telefonía IP. El enfoque "fuera de banda" es más simple de implementar porque el dispositivo no tiene que inspeccionar todo el tráfico de la red. En su lugar, usa otras técnicas más concretas, como crear los rasgos básicos del tráfico o mapear direcciones IP para identificar direcciones oscuras. Este enfoque es útil para empresas que quieran que NAC sea lo menos intrusivo posible, o que simplemente no pueden abordar el emplazamiento de dispositivos NAC en toda la red.

4.2.5 NAC y telefonía IP

Ahora que la telefonía IP empieza a ser una realidad en las empresas, es cada vez más necesario que los productos NAC también sean capaces de tratar el tráfico de telefonía IP. Por tanto, deben estar preparados para conocer qué tipos de dispositivo entran en los segmentos de la red diseñados para VoIP, así como para detectar móviles infectados y proteger a los extremos de la telefonía IP de la intervención de la comunicación. Y como no todos los sistemas NAC están preparados para tratar las redes de telefonía IP, hay que tener cuidado con la solución a elegir cuando se desea desplegar VoIP.

La adopción de tecnología NAC esta siendo impulsada por las necesidades de las empresas a facilitar el acceso a socios y clientes, la mayor implantación del trabajo móvil y la necesidad de proteger el interior de la red, tanto para cumplir con las políticas establecidas como para prevenir pérdidas financieras y de productividad. Las soluciones comerciales son variadas, pero, como sucede con todas las tecnologías, hay que elegir muy detenidamente la mejor opción en cada caso. Y con independencia del enfoque NAC que se siga, hay que tener presente que esta tecnología sólo representa un componente más de lo que debe ser una solución de seguridad global.

4.2.6 Elementos de Solución NAC

La tecnología de control de acceso a la red cuanta con una amplia gama de soluciones y estándares como se describió. Nuestra solución se basa en las funcionalidades NAC de autenticación y autorización empleando el protocolo 802.1X y servicios Ldap y Radius. Se detalla cada uno de los componentes de nuestra solución, el cual se basa en la arquitectura del protocolo 802.1x que tiene como elementos un Suplicante, un Autenticador y un Servidor de Autenticación.

a) **Servidor de Autenticación.** El soporte en hardware es un servidor HP Proliant DL380G5 Intel Xeon Quadcore 2.0Ghz, cache L2 512Kb, con 1Gb de memoria ram, 2 disco duros SAS de 132GB en arreglo 1 (Raid 1). En el cual, como sistema operativo se tendrá instalado GNU Linux, distribución Debian Etch, el servicio de autenticación con Freeradius, el servicio de directorio con Openldap, además con una herramienta de administración gráfica que es phpLDAPadmin que necesita tener instalado un servidor Web que es implementado con Apache2 con soporte de PHP y MySQL.

   1. Servicio Web.- Es el programa que implementa soporte para el protocolo HTTP, el cual permite trasferir los hipertextos, páginas Web o páginas

HTML. Por su rendimiento, confiabilidad y soporte se eligió usar Apache con soporte de Php y MySQL. Se describe los paquetes de instalación.

- Apache2.- El proyecto del servidor de HTTP, es un esfuerzo de colaboración de desarrollo de software aspirando a crear una implementación de un servidor web, robusto, de calidad comercial y de código fuente disponible libremente. El proyecto es manejado por un grupo de voluntarios situados en todo el mundo, usando el Internet y la Web para comunicar, planear, y desarrollar el servidor y su documentación relacionada. Este proyecto es parte de la Fundación del Software de Apache.
- Php5.- Es un lenguaje de programación interpretado de propósito general, ampliamente usado y que esta diseñado especialmente para desarrollo web y puede ser embebido dentro de código HTML. Fue creado por Rasmus Lerdof y actualmente implementado y soportado por The PHP Group.
- MySQL.- Es un sistema de gestión de base de datos relacional, multihilo y multiusuario, es una de las base de datos mas populares de software libre adquirido este año por Sun Microsystems.

ii. Servicio Ldap.- Nos ofrece el servicio de directorio para almacenar datos de manera jerárquica como información de los datos de los usuarios, permisos definidos por políticas de acceso y atributos, cuenta con una base de datos que esta fuertemente optimizado para el rendimiento de lectura. Se describe los paquetes del servicio.

- OpenLDAP.- Es una implementación de software libre del protocolo Lightweight Directory Access Protocol (LDAP) que funciona a nivel de aplicación, que permite el acceso a un servicio de directorio ordenado y distribuido, que facilita la búsqueda diversa de información en un entorno de red. Ldap es un protocolo de comunicación independiente de la plataforma, mantenido por el Proyecto OpenLDAP, en nuestro caso esta implementado bajo una distribución Linux.

iii. Servicio Radius.- Nos brinda el servicio de Autenticación, Autorización y Registro (AAA), el protocolo Radius hace posible la comunicación entre el Autenticador y el Servidor de Autenticación, jugando un papel importante

en la centralización de la autenticación y autorización. Se describe los paquetes del servicio.

- Freeradius.- Es el servidor Radius con más desarrollo en el mundo, proporciona soporte a las necesidades de Autenticación, Autorización y Registro (AAA) de muchas compañías y proveedores de Internet. Además es usado ampliamente en la comunidad académica. El servidor es rápido, lleno de atributos, modular y escalable. Es el único entre los servidores Radius de software libre que tiene soporte para EAP. El servidor tiene soporte para autenticación de usuarios de los métodos simples tales como PAP, CHAP, MS-CHAP, MS-CHAPv2, SIP Digest y todos los tipos de EAP.

iv. Herramienta de administración gráfica.- Se emplea para facilitar la creación, adición de datos y mejorar la administración cuentas de usuarios en el directorio LDAP, se hace uso de esta herramienta que trabaja de manera adecuada con el software OpenLDAP.

- phpLDAPadmin.- Es un cliente LDAP basado en Web. Proporciona fácil administración, acceso vía Web de cualquier lugar y soporte de múltiples lenguajes para el Servidor LDAP. Su visualizador jerárquico y las funcionalidades de búsqueda avanzada hacen posible de manera intuitiva la administración del directorio LDAP.

b) Autenticador. Funcionará en el modo EAP "Pasante", el cual significa que los paquetes EAP desde el suplicante alcanzan al Autenticador como paquetes EAPOL, y son reempaquetados dentro de un paquete RADIUS. Estos paquetes son enviados por el Autenticador al servidor Radius, el cual responde, y el proceso continua al revés. Cuando un mensaje "success" EAP es enviado desde el servidor Radius, el switch puede marcar el puerto como AUTORIZADO, hasta que el cliente finalice sesión, o el tiempo de espera es excedido.

Los equipos elegidos para proporcionar la función de Autenticador son Switch Cisco Catalyst 2950 modelo WS-C2950T-24.

4.2.7 Esquema de Funcionamiento de la Solución

El protocolo 802.1X proporciona control de acceso en la capa 2 de OSI. La norma soporta la autenticación de clientes mientras se establece la conexión a la red. El protocolo de autenticación que emplea la norma es EAP, el cual proporciona el trabajo

con varios métodos de autenticación. En nuestra implementación se emplea como método de autenticación EAP/MD5, el cual es soportado por una variedad de switches.
El switch proporciona la funcionalidad del Autenticador, traduciendo el protocolo EAPOL (EAP sobre LAN) desde el suplicante al servidor Radius. Se muestra el esquema de la solución a continuación (Fig. 4.2).

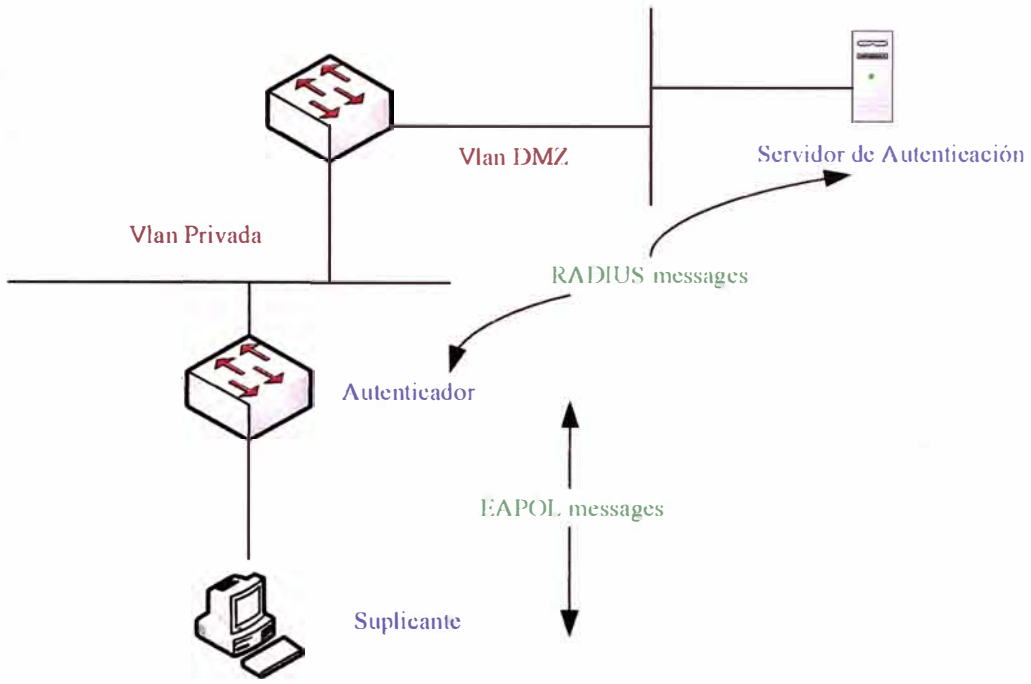


Fig. 4.2 Escenario y funcionamiento de IEEE 802.1X.

4.3 Implementación

4.3.1 Configuración del Servidor de Autenticación

Se detalla los programas instalados y la configuración respectiva de cada uno de los servicios habilitados en el Servidor de Autenticación.

a) Sistema Operativo

El sistema operativo empleado es GNU Linux, distribución Debian Etch 4.0r4, se instalo con la configuración minima en modo texto para el ahorro de recursos.
La versión instalada es la siguiente:

```
# cat /proc/version
Linux version 2.6.18-6-686 (Debian 2.6.18.dfsg.1-22) (dannf@debian.org) (gcc
version 4.1.2 20061115 (prerelease) (Debian 4.1.1-21)) #1 SMP Tue Jun 17
21:31:27 UTC 2008
```

b) Servicios de Comunicaciones

La instalación de los diferentes servicios con los que cuenta el servidor de autenticación, fueron realizados mediante la herramienta de instalación APT con que cuenta la distribución Debian, es un gestor de paquetes eficiente ya que resuelve el tema de dependencias de cada uno de los paquetes de instalación. Los procedimientos de instalación y configuración se detallan a continuación:

- Servicio Web: Proporciona resolución a las peticiones del protocolo HTTP realizadas por un navegador Web a la herramienta gráfica de administración de LDAP.

  Procedimiento de instalación.

```
# apt-get install apache2
# apt-get install php5
# apt-get install php5-mysql
# apt-get install mysql-server-5.0
```

- Servicio Ldap: Se utiliza como un servicio de directorio, donde se encuentran almacenados los datos de los usuarios y se aprovecha las funcionalidades que ofrece este protocolo del manejo de la información de manera jerárquica y la posibilidad de usar los mismos datos de usuario para la validación en diferentes servicios. El servicio Ldap se implementa usando los paquetes de Openldap.

  Procedimiento de instalación.

```
# apt-get install slapd ldap-utils
```

Procedimiento de configuración del servicio Ldap.

```
# dpkg-reconfigure slapd

Desea omitir la configuración de ldap : no
Introdusca el nombre de dominio DNS : inictel-uni.edu.pe
Instrodusca el nombre de su organizacion : Inictel-Uni
Contraseña del administrador : 1n1ct3l
Verificacion de la contraseña : 1n1ct3l
Motor de base de datos a utilizar : BDB
Desea que se borre la base de datos cuando purge el paquete slapd :NO
Desea mover la base de datos antigua : SI
Permitir el protocolo LDAPV2 : si
```

- Servicio Radius: EL uso del protocolo Radius en conjunto con el Autenticador también denominado NAS nos brindan la funcionalidad de autenticación y autorización de usuarios. Para contar con este servicio Radius se hará uso de Freeradius. Además para el soporte de Ldap es necesario instalar el paquete freeradius-ldap.

  Procedimiento de instalación.

```
# apt-get install freeradius freeradius-ldap
```

Para integrar el funcionamiento de Freeradius con Ldap se requiere contar con el esquema openldap.schema.gz que viene como soporte en Freeradius y además se necesita incluir el nuevo esquema en el archivo de configuracion de LDAP.

Procedimiento de integración de Freeradius con LDAP.

```
# cp /usr/share/doc/freeradius/examples/openldap.schema.gz .
# gunzip openldap.schema.gz
# mv openldap.schema /etc/ldap/schema/radius-ldap.schema
```

```
# vi /etc/ldap/slapd.conf
include         /etc/ldap/schema/radius-ldap.schema
```

Realizado los pasos, para tomar los cambios de los archivos de configuración modificados, no olvidemos reiniciar los servicios de Openldap y Freeradius. Continuamos con la configuración del servicio Freeradius, que consiste de tres archivos importantes que brindan las funcionalidades para el Server, Cliente y Usuario. Procedimiento de configuración del Cliente.

```
# vi /etc/freeradius/clients.conf

client 192.168.10.252 {
        secret          = testcisco
        shortname       = switch
}

client 192.168.10.0/24 {
        secret          = test
        shortname       = private-network
}
```

Procedimiento de configuración del usuario para autenticación.

```
# vi /etc/freeradius/users

DEFAULT Auth-Type = EAP
        Fall-Through = 1
```

Como se indica en la configuracion del cliente, por cada equipo Autenticador adicional se agregara su ip y el password para que se establesca la comunicacion con el Servidor de Autenticacion. Para completar la integracion de Freeradius con Ldap, se necesitara configurar el archivo radiusd.conf .

Procedimiento de configuración del Server.

```
# vi /etc/freeradius/radiusd.conf

ldap {
        server = "ldap.inictel-uni.edu.pe"
        identity = "cn=admin,dc=inictel-uni,dc=edu,dc=pe"
        password = 1n1ct3l
        basedn = "ou=usuarios,dc=inictel-uni,dc=edu,dc=pe"
        filter = "(&(uid=%{Stripped-User-Name:-%{User-
Name}})(objectclass=radiusprofile))"
        start_tls = no
        profile_attribute = "radiusProfileDn"
        dictionary_mapping = ${raddbdir}/ldap.attrmap

    }

authenticate {

    Auth-Type LDAP {
        ldap
    }

    #  Allow EAP authentication.
    eap
}
```

Para asignar de manera dinámica las VLANs en el proceso de autenticación de un usuario, se requiere agregar ciertos parámetros en el archivo ldap.attrmap de Freeradius, cuando Freeradius realiza la consulta de determinado usuario a Ldap, este le responda con las propiedades y la Vlan a la que pertenece.

Procedimiento de configuración.

```
# vi /etc/freeradius/ldap.attrmap

replyItem    Tunnel-Type                radiusTunnelType
replyItem    Tunnel-Medium-Type         radiusTunnelMediumType
replyItem    Tunnel-Private-Group-Id    radiusTunnelPrivateGroupId
```

- Herramienta de Administración Gráfica de Lda+p: Nos facilita el manejo de creación, modificación, eliminación de usuarios y tareas de administración del servicio de directorio LDAP.

  Procedimiento de instalación de phpLDAPadmin.

```
# apt-get install phpldapadmin
# apt-get install php5-ldap
```

4.3.2 Configuración del Autenticador

La configuración del equipo Autenticador, lo realizamos accediendo a la Interfaz de Línea de Comandos del IOS (CLI) que soportan los switch Catalyst, en modo configuración global, se procede a ingresar los comandos con los parámetros definidos para nuestro caso de implementación.

Teniendo configurado el Autenticador, realizamos las pruebas de autenticación de los usuarios en el sistema, no obteniendo una autenticación exitosa. Se procedió a verificar la configuración del Servidor de Autenticación y Suplicante, de nuevo se probó la configuración del sistema, no consiguiendo un resultado satisfactorio.

Como última alternativa se procedió a actualizar el IOS del switch con la última versión, por medio del CLI del switch se actualiza de manera satisfactoria, se elimina la versión antigua y se reinicia el equipo, con las configuraciones ya contenidas en la memoria del switch, se realiza de nuevo las pruebas, consiguiendo que funcione de manera exitosa el proceso de autenticación.

Procedimiento de Actualización del IOS.

```
#copy tftp:c2950-i6q4l2-mz.121-22.EA11.bin flash:
#reload
```

El tema iba por el soporte de la versión del IOS instalado en el switch, comentamos este tema sucedido como referencia para posteriores implementaciones para que tengan una alternativa en su solución. A continuación se detalla la configuración del Autenticador. La versión anterior y actual con el que cuenta el switch se detalla a continuación respectivamente:

```
#sh version

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(13)EA1,
RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Tue 04-Mar-03 02:14 by yenanh
Image text-base: 0x80010000, data-base: 0x805A8000

ROM: Bootstrap program is CALHOUN boot loader

Authentication uptime is 2 hours, 48 minutes
System returned to ROM by power-on
System image file is "flash:/c2950-i6q4l2-mz.121-13.EA1.old"

cisco WS-C2950T-24 (RC32300) processor (revision K0) with 20839K
bytes of memory
```

```
#sh version

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA11,
RELEASE SOFTWARE
 (fc2)
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Tue 08-Jan-08 10:50 by amvarma
Image text-base: 0x80010000, data-base: 0x80570000

ROM: Bootstrap program is C2950 boot loader

Authentication uptime is 17 hours, 42 minutes
System returned to ROM by power-on
System image file is "flash:/c2950-i6q4l2-mz.121-22.EA11.bin"

cisco WS-C2950T-24 (RC32300) processor (revision K0) with 20957K
bytes of memory
```

Ya actualizado con la nueva versión del IOS, se procede a configurar el switch, habilitando el método de autenticación con el protocolo 802.1X, la configuración de los

parámetros del servidor Radius, la activación para asignamiento dinámico de vlan, y la habilitación de cada una de los puertos seleccionados para la autenticación con el protocolo 802.1X.

Procedimiento de configuración del Autenticador.

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

radius-server host 192.168.10.215 auth-port 1812 acct-port 1813
timeout 3
radius-server retransmit 3
radius-server key testcisco
```

```
interface FastEthernet0/6
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport mode access
 dot1x port-control auto
 spanning-tree portfast
```

El switch ya esta listo para realizar las tareas de autenticación, para verificar que la autenticación esta activada, visualizamos ejecutando el comando:

```
Authentication#sh dot1x
Sysauthcontrol                  = Enabled
Supplicant Allowed In Guest Vlan  = Disabled
Dot1x Protocol Version          = 1
```

Se va emplear Vlan para segmentar la red, para ello solo es necesario crear previamente cada una de ellas en el Autenticador (switch). La asignación de Vlan por puertos se realiza de manera dinámica con la autenticación de los usuarios.

Procedimiento de creación de Vlan.

```
#configure terminal
(config)#vlan 2
(config)#exit
(config)#vlan 3
(config)#exit
```

4.3.3 Configuración del Suplicante

Se cuenta con herramientas para brindar el soporte de autenticación en base al protocolo 802.1X para los sistemas operativos Linux y Windows.

Los usuarios en su mayoría cuentan con computadoras de escritorio y portátiles, los cuales tienen instalado como sistema operativo Windows XP SP2. Windows brinda soporte de manera nativa del protocolo 802.1X para la autenticación del cliente en su línea de Sistemas Operativos Windows 2000 SP4 y WinXP SP2.

Procedimiento de configuración del cliente Windows XP.

a. Obtener las propiedades de la conexión en la carpeta de Conexiones de Red.
b. Elegir la ficha de Autenticación y seleccionar Habilitar la autenticación IEE802.1X en esta red y Desafio-MD5. (Fig. 4.3)
c. Se acepta y guardamos los cambios.

Los usuarios que trabajan con distribuciones Linux necesitan tener instalados una aplicación para el soporte de autenticación en base al protocolo 802.1X. Una alternativa es Open1x que es una aplicación con un desarrollo maduro, esta herramienta facilita el acceso de clientes Linux a la red corporativa.

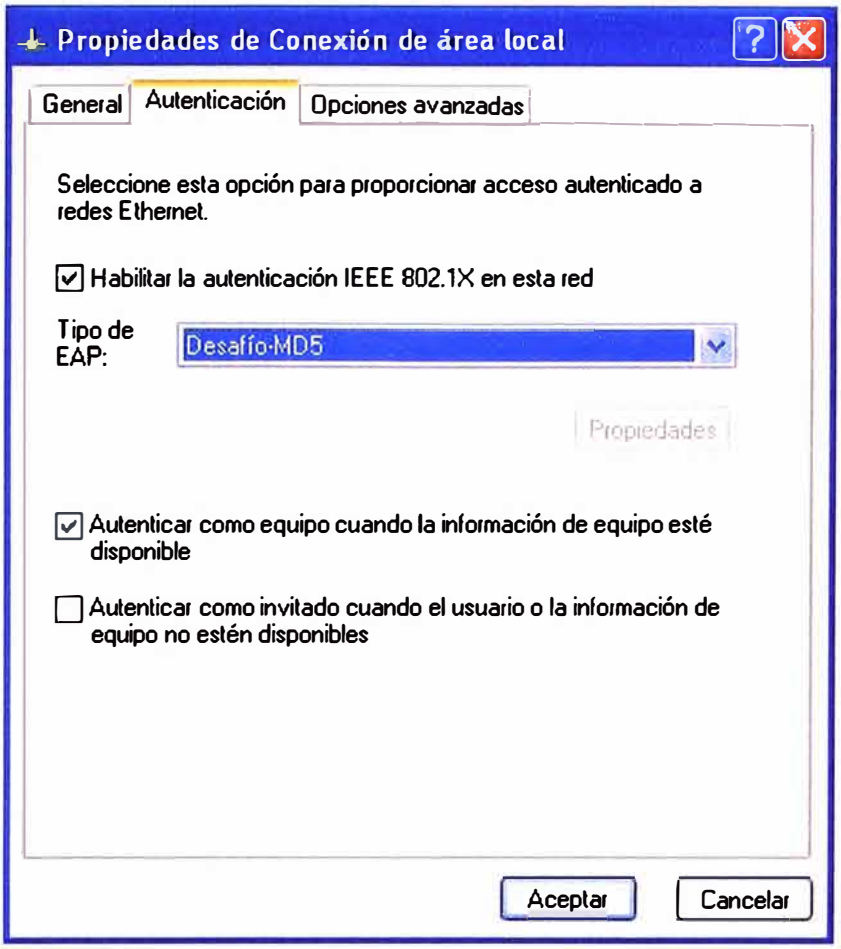


Fig. 4.3 Soporte de protocolo 802.1X en el cliente.

4.4 Validación

El funcionamiento del Sistema de Control de Acceso por Puertos implementado se basa en el control que proporciona el Autenticador, habilitado con el protocolo 802.1X, que realiza la consulta al Servidor de Autenticación para validar el método de autenticación por medio de un usuario y contraseña cuando un Suplicante solicita acceso a la red corporativa, el sistema trabaja de la siguiente manera:

Los usuarios con computadoras de escritorio o portátiles con sistema operativo Windows XP SP2 que vienen a ser los Suplicantes, están previamente configurados para el soporte del protocolo 802.1X y el método de autenticación, como se detalla en el capitulo anterior. Se conectan a la red corporativa intentando tener conectividad y acceso a los servicios que se ofrece a través de la red de datos. El puerto del conmutador no le brinda conexión a la red de inmediato, como se puede visualizar en el gráfico (Fig 4.4), donde se muestra la actividad de tráfico en la tarjeta de red del usuario, las peticiones de conexión del cliente al puerto, paquetes enviados son trasmitidos mientras que en el otro sentido, del puerto al cliente no hay respuesta alguna visualizando cero de actividad.

Fig. 4.4 Conectividad nula.

El puerto del conmutador con soporte del protocolo 802.1X que tiene implementado el control de acceso mediante autenticación, solicita la validación con un usuario y contraseña como se muestra en los gráficos (Fig. 4.5 y 4.6).

El usuario ingresa los datos de nombre de usuario y contraseña dejando en blanco el campo de Dominio de inicio de sesión, asignados previamente por el administrador de la red, el sistema lo valida y si son correctos, se establece la conectividad con la red corporativa.

Fig. 4.5 Notificación para acceso.

Fig. 4.6 Registro para acceso autorizado.

El empleo del servicio de directorio con Ldap nos da la facilidad de agregar atributos adicionales para cada cuenta de usuario. En la implementación se adiciono un atributo relacionado con la VLAN, al cual debe pertenecer el usuario de la cuenta, lo que resulta beneficioso para la administración de la red corporativa.

Para mostrar resultados del sistema de control de acceso basado en puertos, utilizando el protocolo 802.1X, en el servidor Ldap se creo las cuentas de los usuarios con sus respectivas contraseñas y se asigno a cada cuenta una Vlan al que deben pertenecer, como se muestra en la tabla 4.1:

TABLA Nº 4.1 Relación de cuentas y datos.

Usuario	Contraseña	Direccion IP	Direccion Mac	Puerto	Vlan
Racevedo	password	192.168.10.159	00-0E-7B-B6-CB-17	6	2
Jsanchez	123456	192.168.10.151	00-0A-E6-45-B1-C6	7	3
Rbernia	abc123	192.168.10.155	00-1D-92-33-77-DA	8	1

Se autenticara desde cada estación con su cuenta correspondiente, se verificara si se asignó correctamente la Vlan a cada cuenta, probando la conectividad con un ping al servidor de Autenticación, el cual tiene el IP 192.168.10.215 y se encuentra ubicado en la Vlan 1. El resultado de conectividad con el servidor de Autenticación solo debería ser exitosa con la cuenta rbernia, el cual pertenece a la misma Vlan del servidor.

El sistema tiene los siguientes datos iniciales:

- Datos del Autenticador: Se muestra el ID Vlan y puertos asociados.

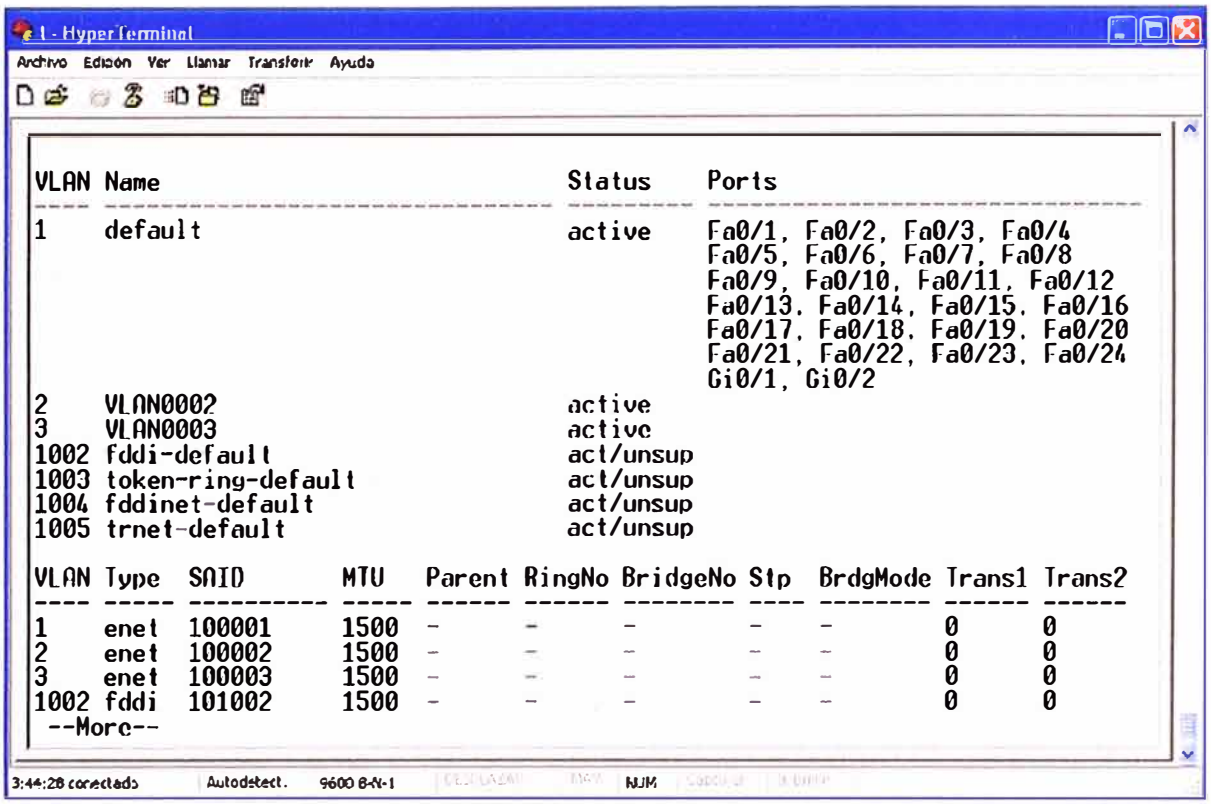


Fig. 4.7 Resultados de Vlan por puertos perteneciente.

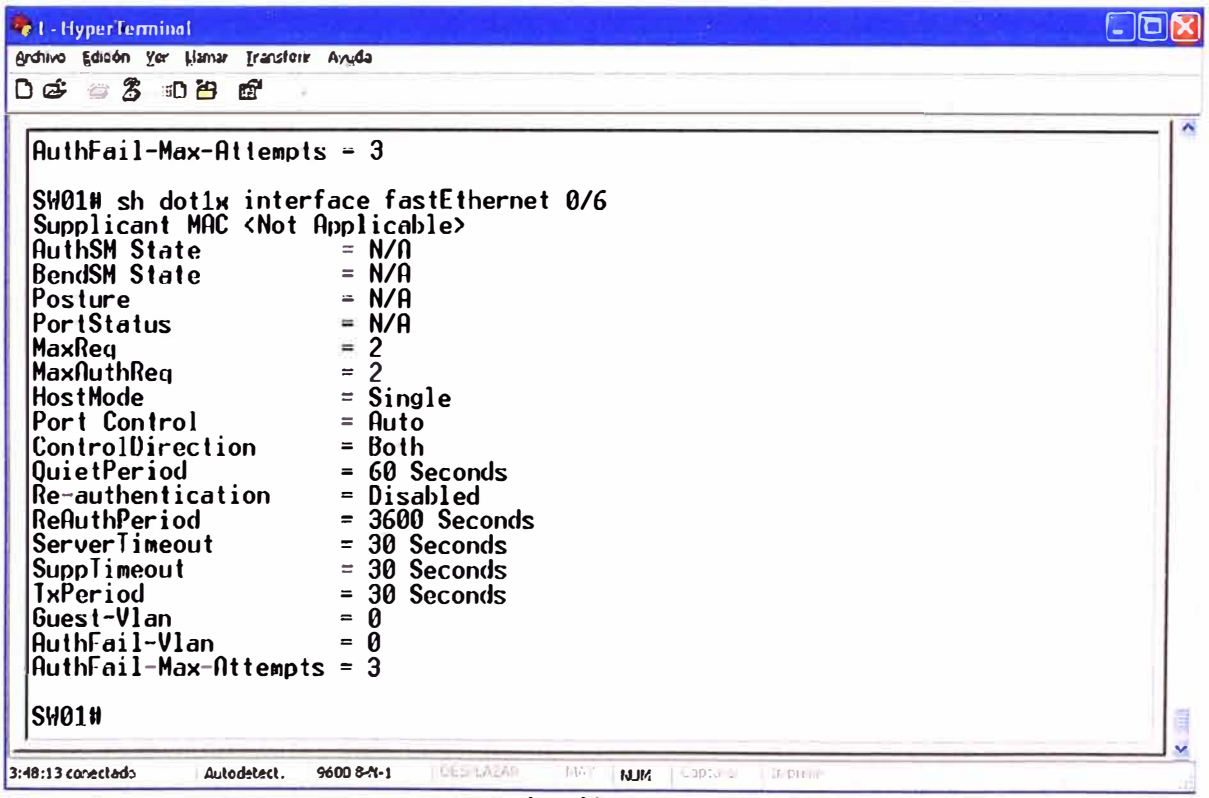


Fig. 4.8 Autenticación 802.1x por puerto.

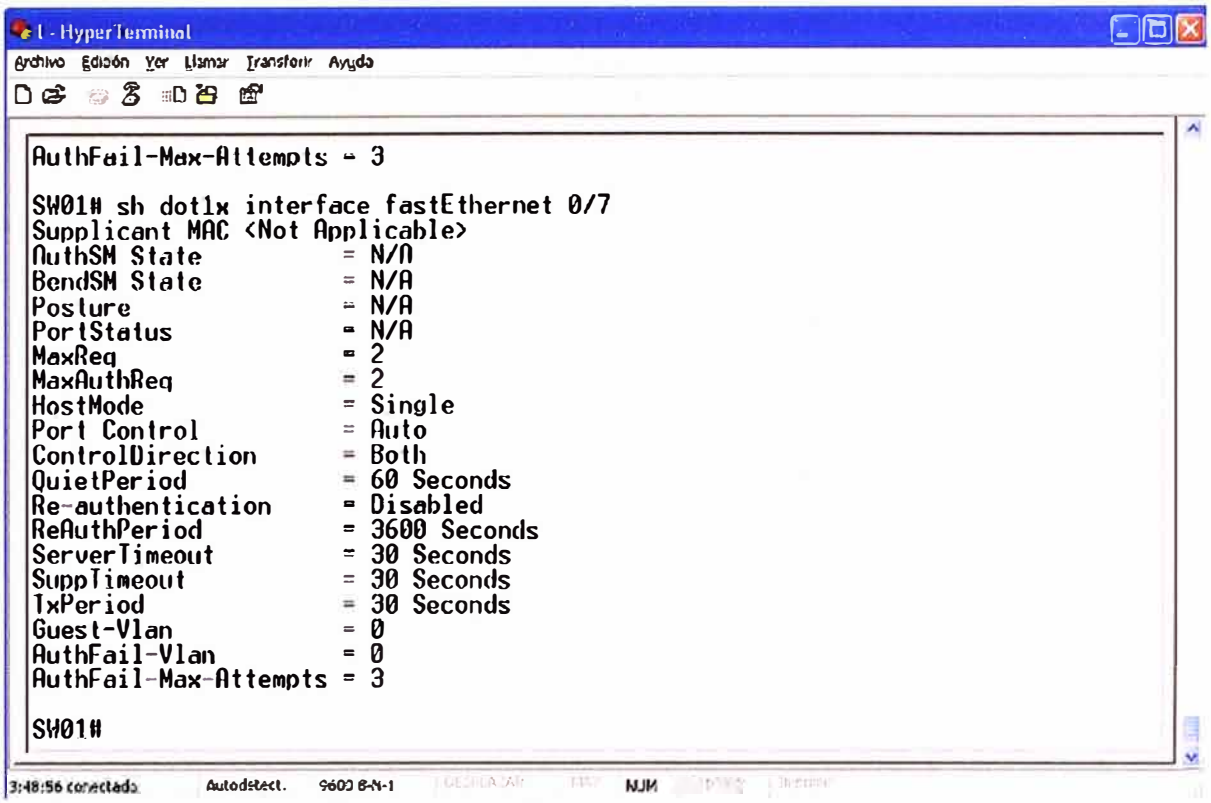


Fig. 4.9 Autenticación 802.1x por puerto.

Cada cliente accede a la red corporativa ingresando su usuario y contraseña respectiva.

Resultados de la autenticación del usuario racevedo.

- Datos del Autenticador: Se muestra el ID Vlan y puertos asociados.

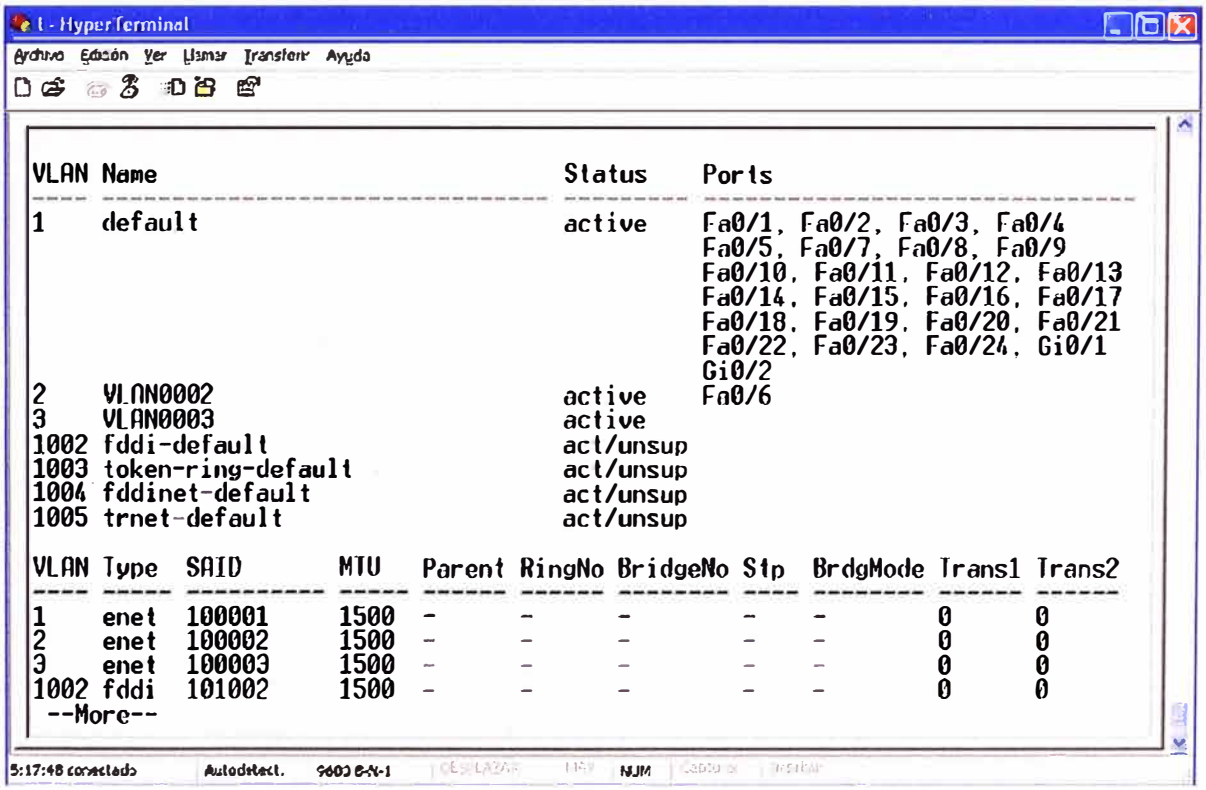


Fig. 4.10 Resultados de Vlan y puertos pertenecientes.

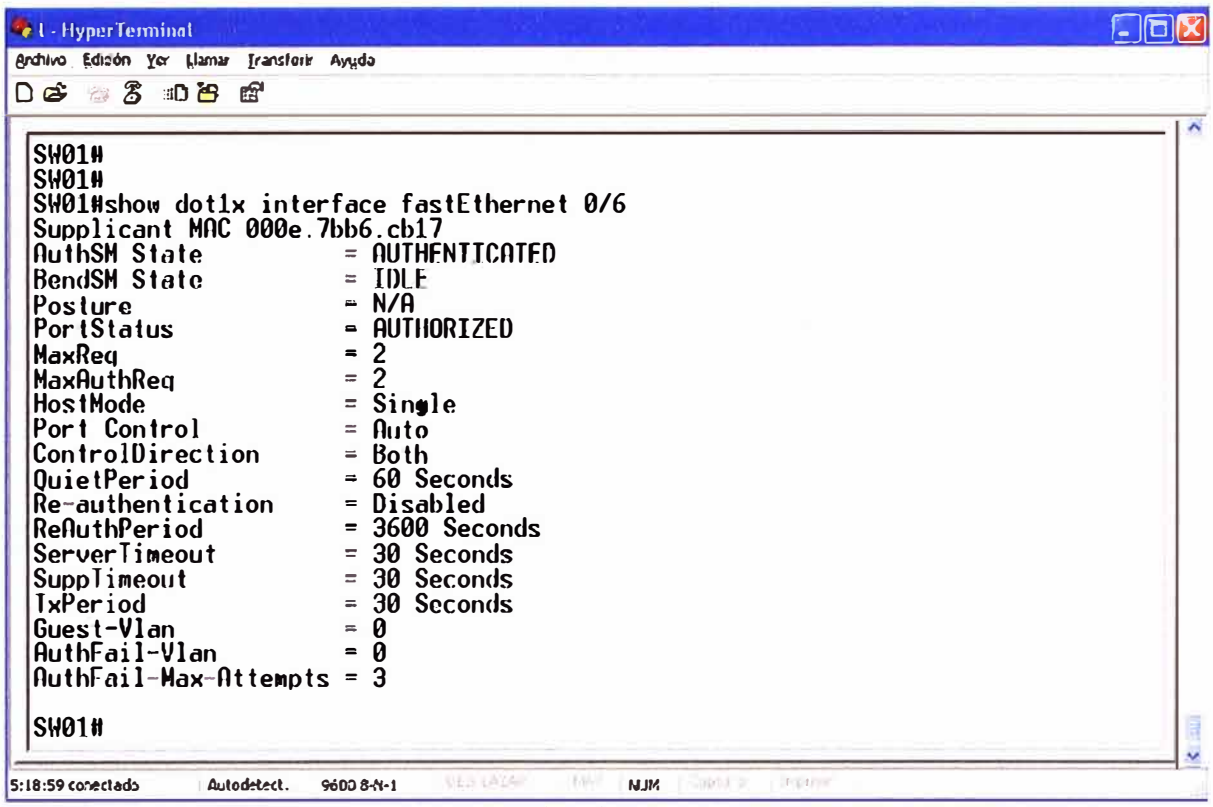


Fig. 4.11 Autenticación 802.1x por puerto.

- Datos del cliente.

  Se obtiene mediante ipconfig/all los datos de la dirección MAC de la Pc que nos servirá para comparar con el resultado q se obtiene en el Autenticador.

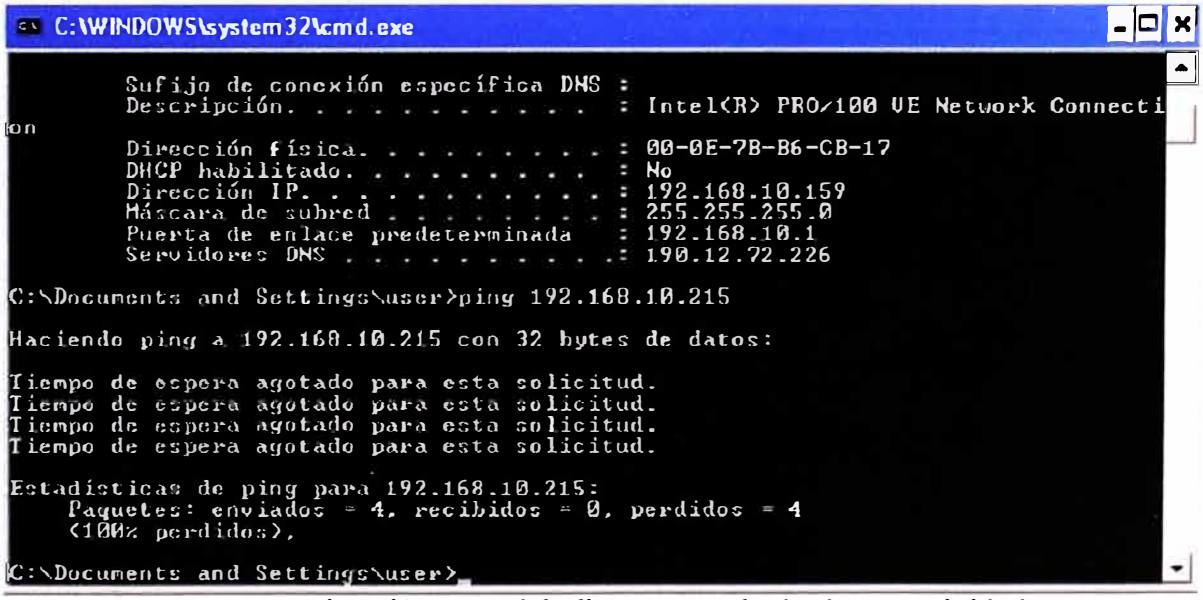


Fig. 4.12 Dirección Mac del cliente y resultado de conectividad.

Resultados de la autenticación del usuario jsanchez.

- Datos del Autenticador: Se muestra el ID Vlan y puertos asociados.

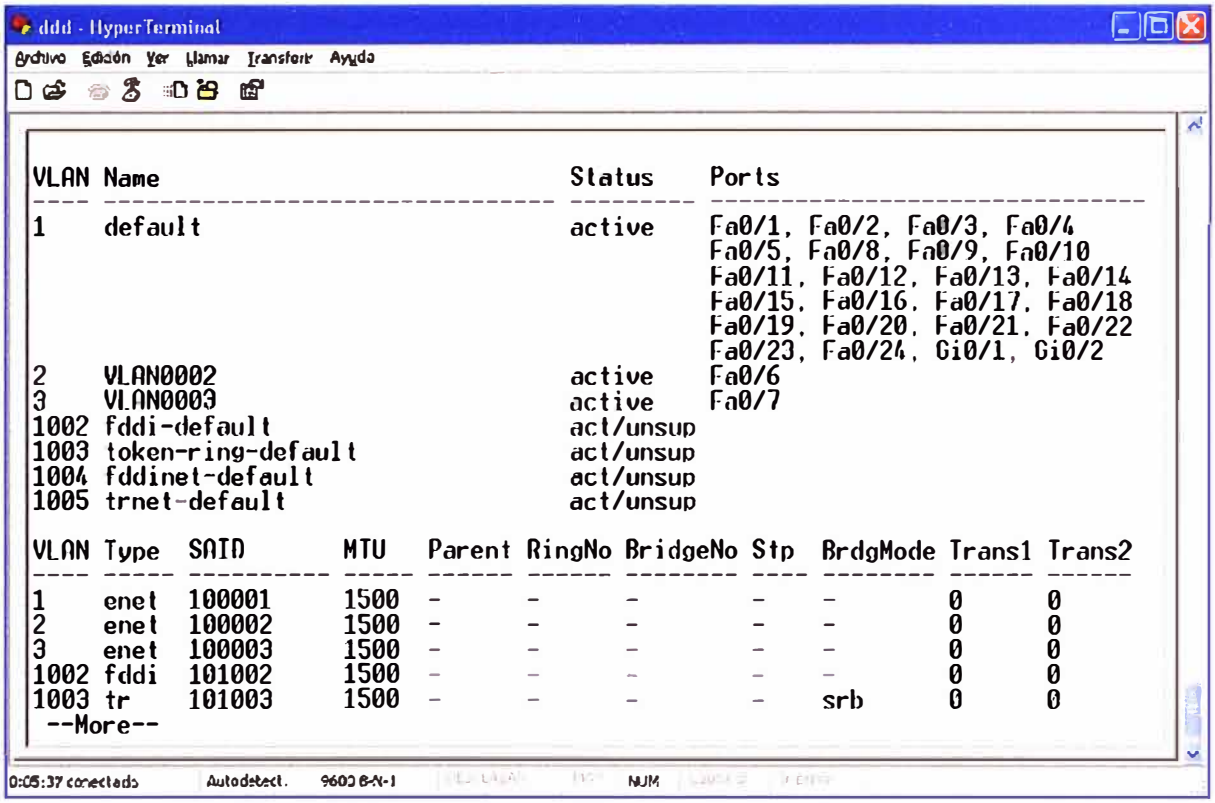


Fig. 4.13 Resultados de Vlan y puertos pertenecientes.

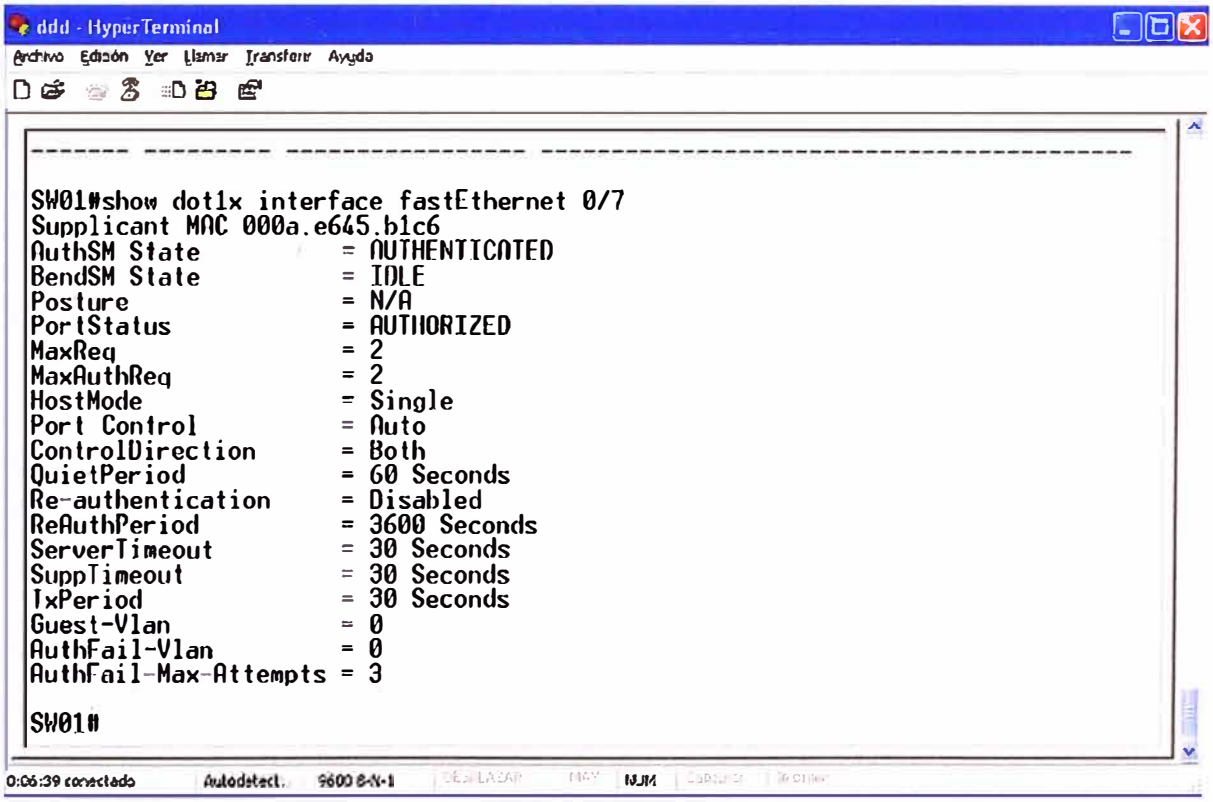


Fig. 4.14 Autenticación 802.1x por puerto.

- Datos del cliente:

  Ejecutando ipconfig/all en la PC del usuario jsanchez se obtiene la dirección Mac.

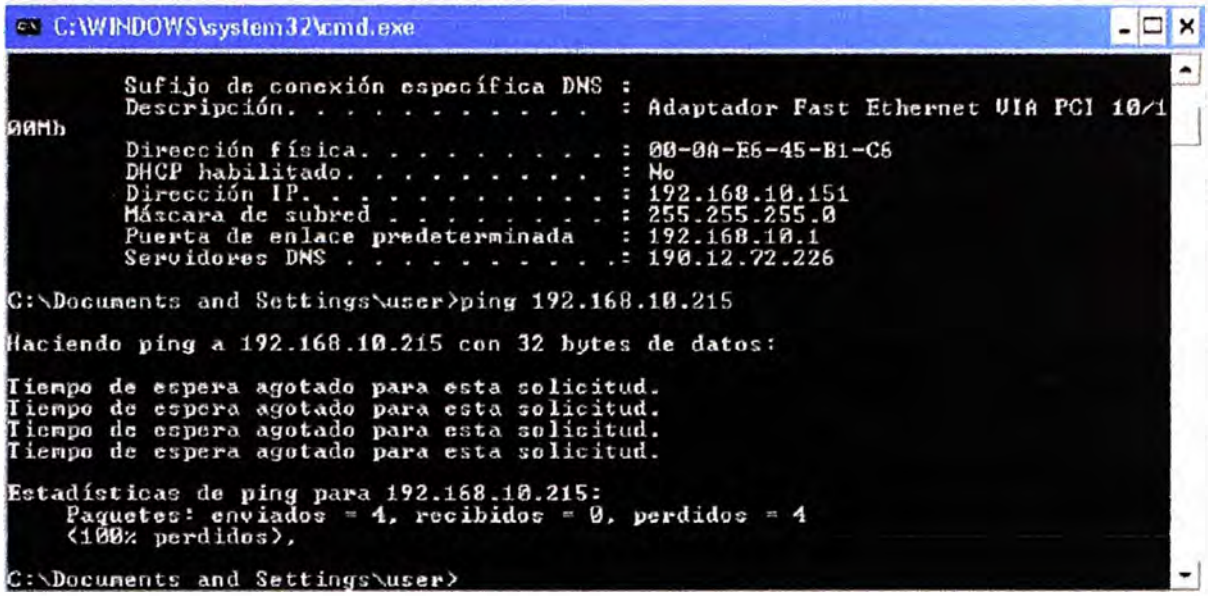


Fig. 4.15 Dirección Mac del cliente y resultado de conectividad.

En la Fig. 4.15 se prueba la conectividad al servidor de Autenticación mediante un ping, consiguiendo un resultado negativo lo cual es lo esperado ya que la PC se encuentra en la VLAN 3 y el Servidor de Autenticación pertenece a la VLAN 1.

Resultados de la autenticación del usuario rbernia.

- Datos del Autenticador: Se muestra el ID Vlan y puertos asociados.

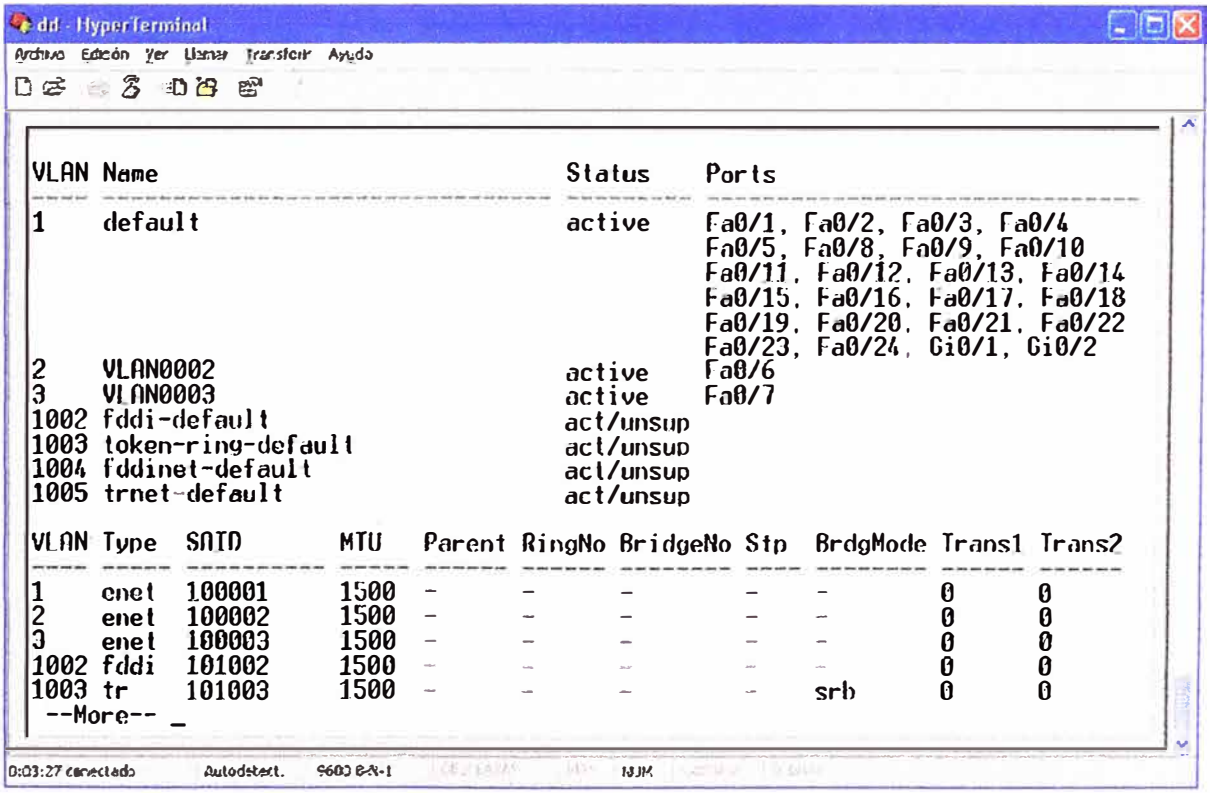


Fig. 4.16 Resultados de Vlan y puertos pertenecientes.

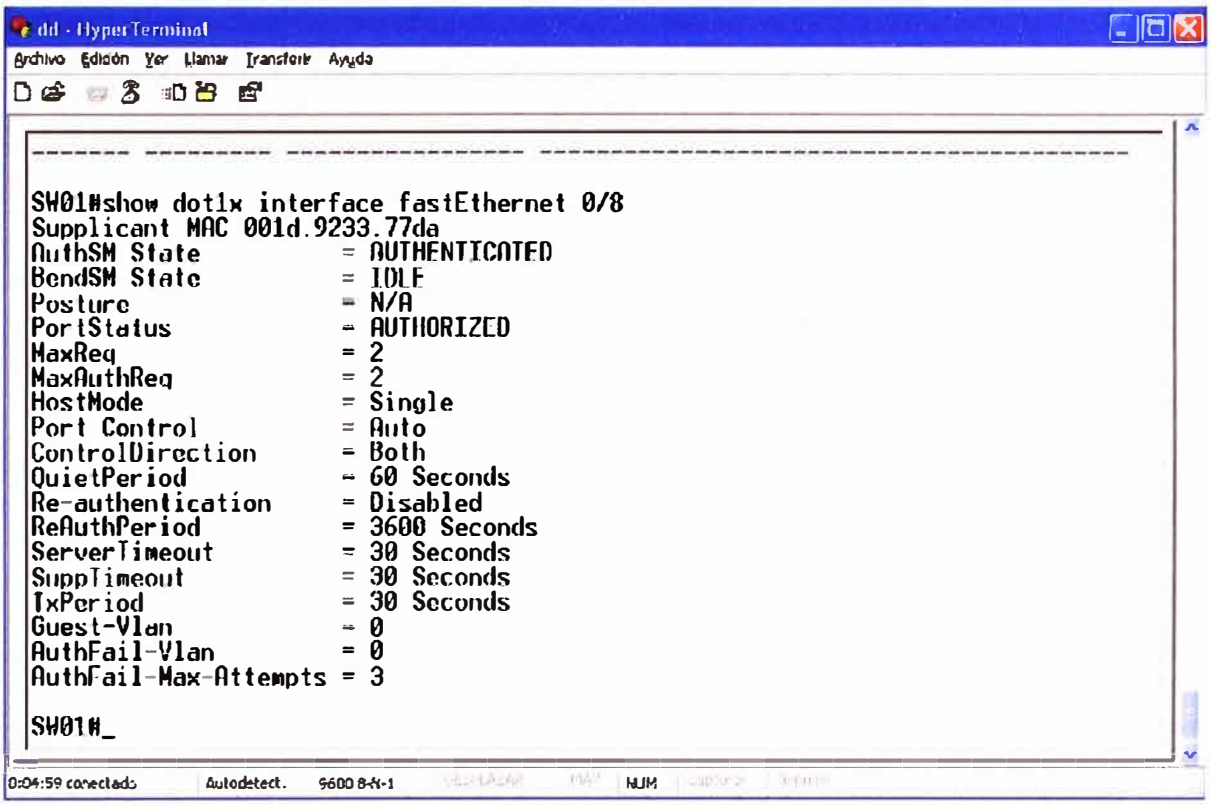


Fig. 4.17 Autenticación 802.1x por puerto.

- Datos del cliente

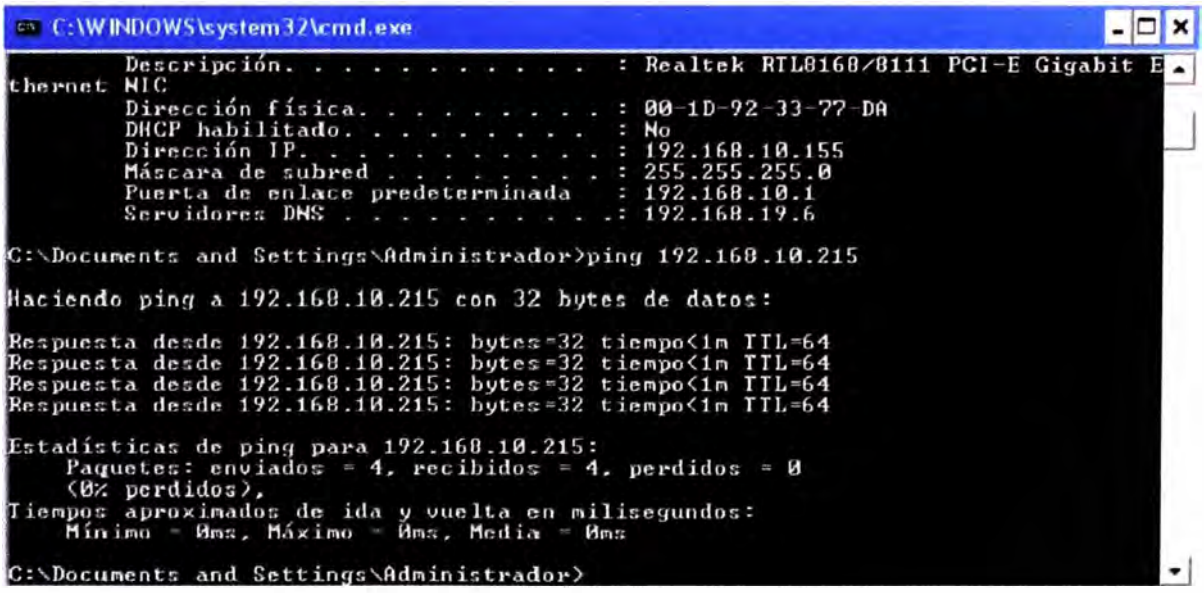


Fig. 4.18 Dirección Mac del cliente y resultado de conectividad.

La autenticación de cada uno de los usuarios en el sistema se logró con éxito, los resultados del Autenticador que se visualizan en los gráficos, muestran en cada caso la relación del puerto de acceso de cada usuario con la Vlan asociada, detalles del puerto indicando el estado de autenticación y dirección MAC del Suplicante registrado. De los resultados, en el primer registro el usuario con la cuenta racevedo, se conecta al puerto 6

del switch (Fa/06), asociado a la VLAN 2, el estado del puerto es Autorizado y el valor de la dirección MAC que se indica coincide con el valor obtenido mediante el comando ipconfig/all en la PC del usuario, en el segundo registro con la cuenta jsanchez, se conecta al puerto 7 del switch (Fa/07), asociado a la VLAN 3, el estado del puerto es Autorizado y la dirección MAC coincide con la MAC de la PC del usuario jsanchez, del mismo modo con la cuenta rbernia, se conecta al puerto 8 del switch (Fa/08), asociado a la VLAN 1, el estado del puerto es Autorizado y la dirección MAC coincide con la MAC de la PC del usuario rbernia.

Esta ultima cuenta de usuario rbernia esta asociada a la VLAN 1, probando la conectividad con el Servidor de Autenticación como se muestra en el gráfico (Fig. 4.18) el resultado es exitoso debido a que ambos se encuentran en la misma VLAN, lo que no sucede con las otras cuentas de usuario racevedo y jsanchez que están asociadas a la VLAN 2 y 3 respectivamente siendo el resultado de conectividad con el Servidor de Autenticación negativo.

Finalmente de acuerdo a los resultados verificamos el correcto funcionamiento del sistema implementado para el control de acceso por puertos a la red corporativa.

CONCLUSIONES Y RECOMENDACIONES

1. Esta solución proporciona un nivel de seguridad en la red Lan forzando a la autenticación de los usuarios para el acceso a la red, siendo una alternativa viable y no costosa para la implementación en toda red LAN alámbrica e inalámbrica.
2. Esta solución permite centralizar la administración de la red local, contando con la información de los usuarios en una base de datos, además se pueden integrar con otros servicios por medio de Ldap.
3. El método de autenticación usado en la implementación es EAP/MD5, transfiere un hash con el nombre del usuario, la contraseña y una cadena arbitraria. La limitación de este método, que no es tan seguro contra ataques tipo diccionario. Una alternativa es emplear el método de autenticación EAP/TLS, el cual hace uso de certificados X.509 tanto en el servidor como cliente.
4. El protocolo EAP soporta diferentes métodos de autenticación, tal como EAP/TLS, PEAP los cuales son más seguros por lo que serían una mejor alternativa y se recomienda su uso.
5. El protocolo 802.1X no proporciona protección criptográfica del tráfico de tramas después de la autenticación y autorización, una alternativa de solución viene a ser IPsec.
6. En nuestro trabajo la asignación de direccionamiento IP se realizó de manera estática, lo cual no limita emplear asignación de direccionamiento IP dinámico, solo se necesita contar con un servidor DHCP.

ANEXO 1
SWITCH 3COM 3226

Features

PERFORMANCE	
Switching capacity	SuperStack 3 Switch 3226, 8.8 Gbps; Switch 3250, 13.6 Gbps
Forwarding rate	Switch 3226, 6.6 Mpps; Switch 3250, 10.1 Mpps Store-and-forward switching; latency <12 µs
LAYER 2 SWITCHING	
MAC Address	8K MAC addresses
VLAN	255 VLANs (IEEE 802.1Q)
Link Aggregation	IEEE 802.1ad (LACP), Gigabit ports only
Auto-negotiation	Auto-negotiation of port speed, duplex, and connection (MDI/MDIX)
Traffic control	IEEE 802.3x full-duplex flow control Back pressure flow control for half-duplex Supports Broadcast Storm Suppression (3,000 pps threshold)
Spanning Tree Protocol / Rapid Spanning Tree Protocol	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Backward-compatible with Spanning Tree Protocol (STP) Fast-start mode Spanning tree enable/disable per port
LAYER 3 SWITCHING	
Routes	Hardware based routing 2,001 IP routes: 1,990 dynamic and 10 static Address Resolution Protocol (ARP) entries with 1 user default route
IP Routing	32 IP interfaces Multi-netting (multiple IP interfaces per VLAN) Routing Information Protocol (RIP), v1 and v2 • Split Horizon • Split Horizon with poisoned reverse • Triggered updates • MD5 authentication of the RIP packets • Password authenticated RIP packets • Host route advertisements
Multicast	Filtering for 64 multicast groups Internet Group Management Protocol (IGMP) snooping on Layer 2 interfaces IGMP v1 and v2 IGMP Querier
Network protocol	Dynamic Host Configuration Protocol (DHCP) Helper/Relay UDP Helper ARP, ARP Proxy
CONVERGENCE	
Priority Queues	Four hardware queues per port Weighted Round Robin queuing
Traffic Prioritization	Priority based on: • DiffServ Code Point (DSCP) • IEEE 802.1p Class of Service (CoS) VLAN priority • TCP/UDP destination port number • Default port priority • Auto classification of 3Com NBX® telephony traffic
Bandwidth Management	Port-based bandwidth management: • 1 Mbps increments (10/100 ports) • 8 Mbps increments (Gigabit ports)

Features *continued*

SECURITY	
Network Login	IEEE 802.1X user authentication • RADIUS authentication • Secure Mode (locks MAC address)
Access Control Lists	Port-based ACLs • Filtered on destination IP address / mask • One ACL per port • 32 unique ACLs per switch • 32 rules per ACL (10/100 ports)
Switch Protocol Security	MD5 cipher-text and clear-text authentication for RIP v2 packets
Switch Management	Local or RADIUS management of switch passwords Trusted IP Management Addresses Telnet • SSH v1 (56bit DES) • SSH v2 (requires free software upgrade) SSL (HTTPS) • 40 Bit • 56 Bit DES • 128 Bit RC4 (requires free software upgrade)
RESILIENCY	
	Support for 3Com Advanced Redundant Power Supply; provides backup power to the switch Dual software images Backup and restore of switch settings
MANAGEMENT	
Remote Management	SNMP v1
Software	Dual software images Backup and restore Trivial File Transfer Protocol (TFTP) configuration: upload/download TFTP agent: upload
Configuration	Command line Serial (9-pin, D-type connector) Telnet Web-based SNMP
Mirror port / RAP (Roving Analysis Port)	One-to-one
RMON (Remote Monitoring)	Four groups: statistics, history, alarm, and events
IP address allocation	DHCP Manual User-selectable management VLAN
Switch access levels	2 access levels 16 user accounts
Remote GUI management	3Com Network Supervisor for basic, turn-key network management for small and medium businesses (copy provided with product) • Topology discovery • Change management reporting • Capacity planning • Event logging • Fault identification and troubleshooting • Utilization monitoring Other 3Com Management Applications: • 3Com Network Director for comprehensive, turn-key network management for the enterprise. • 3Com Enterprise Management Suite for flexible, extensible management in advanced enterprise IT environments

ANEXO 2

SWITCH CATALYST 2950

In addition to Cisco Network Assistant, Cisco Catalyst 2950 Series switches provide extensive management tools using SNMP network management platforms such as CiscoWorks. Managed with CiscoWorks, Cisco Catalyst family switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Coupled with CiscoWorks, Cisco Resource Manager Essentials, a Web-based management tool, offers automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

PRODUCT FEATURES AND BENEFITS

Feature	Benefit
Availability	
Superior Redundancy for Fault Backup	• IEEE 802.1D Spanning Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • IEEE 802.1w Rapid Spanning- Tree Protocol (RSTP) provides rapid convergence of the spanning tree, independent of spanning-tree timers. • Per VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances. • Support for Cisco Spanning Tree Protocol enhancements such as UplinkFast, BackboneFast, and PortFast technologies ensures quick failover recovery and enhances overall network stability and availability. • Support for Cisco's optional RPS 675, 675-watt redundant AC power system, which provides a backup power source for one of six switches, for improved fault tolerance and network uptime. • Unidirectional link detection (UDLD) and aggressive UDLD detect and disable unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults.
Integrated Cisco IOS Software Features for Bandwidth Optimization	• Bandwidth aggregation through Cisco EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches to routers and individual servers. Port Aggregation Protocol (PagP) is available to simplify configuration. • VLAN1 minimization allows VLAN1 to be disabled on any individual VLAN trunk link. • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) allows a spanning-tree instance per VLAN, enabling Layer 2 load sharing on redundant links. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall system performance. • Per VLAN Spanning Tree Plus (PVST+) allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports in the switch. • IGMPv3 snooping provides for fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to the requestors. MVR, IGMP filtering, and fast-join and immediate leave are available as enhancements. IGMP Snooping time can be adjusted to optimize the performance of multicast data flows.
Security	
Networkwide Security Features	• A private VLAN edge provides security and isolation between ports on a switch, ensuring that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. • Support for the 802.1x standard allows users to be authenticated regardless of which LAN ports they are accessing, and it provides unique benefits to customers who have a large base of mobile (wireless) users accessing the network. – 802.1x with voice VLAN permits an IP phone access to the voice VLAN regardless of the authorized or unauthorized state of the port. – 802.1x with Port Security authenticates the port and manages network access for all MAC addresses, including

Feature	Benefit
	that of the client. – IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the Guest VLAN. – IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user regardless of where the user is connected. • SSHv2 provides network security by encrypting administrator traffic during Telnet sessions. SSHv2 requires a special cryptographic software image due to US export restrictions • Port Security secures the access to a port based on the MAC address of a user's device. The aging feature removes the MAC address from the switch after a specific time to allow another device to connect to the same port. • MAC Address Notification allows administrators to be notified of new users added or removed from the network. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • Trusted Boundary provides the ability to trust the QoS priority settings if an IP phone is present and disable the trust setting in the event that the IP phone is removed, thereby preventing a rogue user from overriding prioritization policies in the network. • TACACS+ and RADIUS authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration. • SPAN support of Intrusion Detection Systems (IDSs) to monitor, repel, and report network security violations • SNMPv3 (non-crypto) monitors and controls network devices, manages configurations, statistics collection, performance, and security. • Cisco Network Assistant software security wizards ease the deployment of security features for restricting user access to a server, a portion of the network, or access to the network.
Quality of Service	
Layer 2 QoS	• Support for reclassifying frames is based either on 802.1p class-of-service (CoS) value or default CoS value per port assigned by network manager. • Four queues per egress port are supported in hardware. • The Weighted Round Robin (WRR) scheduling algorithm ensures that low-priority queues are not starved. • Strict priority queue configuration via Strict Priority Scheduling ensures that time-sensitive applications such as voice always follow an expedited path through the switch fabric.
Management	
Superior Manageability	• SNMP and Telnet interface support delivers comprehensive in-band management, and a CLI management console provides detailed out-of-band management. • An embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • A Switched Port Analyzer (SPAN) port can mirror traffic from one or many ports to another port for monitoring all nine RMON groups with an RMON probe or network analyzer. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Layer 2 traceroute eases troubleshooting by identifying the physical path that a packet takes from the source device to a destination device. • Multifunction LEDs per port for port status, half-duplex/full-duplex, 10BASE-T/100BASE-TX/1000BASE-T indication, as well as switch-level status LEDs for system, redundant power supply, and bandwidth utilization provide a comprehensive and convenient visual management system. • Crash information support enables a switch to generate a crash file for improved troubleshooting.

ANEXO 3
CONFIGURACIÓN VLAN EN PHPLDAPADMIN

Se muestra como ejemplo los valores que se ingresan en cada atributo para crear una entrada VLAN en la estructura de nuestro servicio de directorio LDAP.

Los atributos cn (common name), sn (surname), uid (unix login) se relacionan con un nombre que identifica la VLAN creada, la clase de objetos objectClass define la colección de atributos que puede usarse para definir una entrada, por defecto se emplean top e inetOrgPerson, se adiciona radiusprofile para el soporte de los atributos radiusTunnelMediumType, radiusTunnelType, radiusTunnelPrivateGroupId que son parámetros que lee el FreeRadius de la respuesta que devuelve la entrada VLAN, al momento de que el cliente logra autenticarse exitosamente.

cn required

vlan_02

(add value)

objectClass required

top

inetOrgPerson (structural)

radiusprofile

(add value)

radiusTunnelMediumType

IEEE-802

(add value)

radiusTunnelPrivateGroupId

2

(add value)

radiusTunnelType

VLAN

(add value)

sn required

vlan_02

(add value)

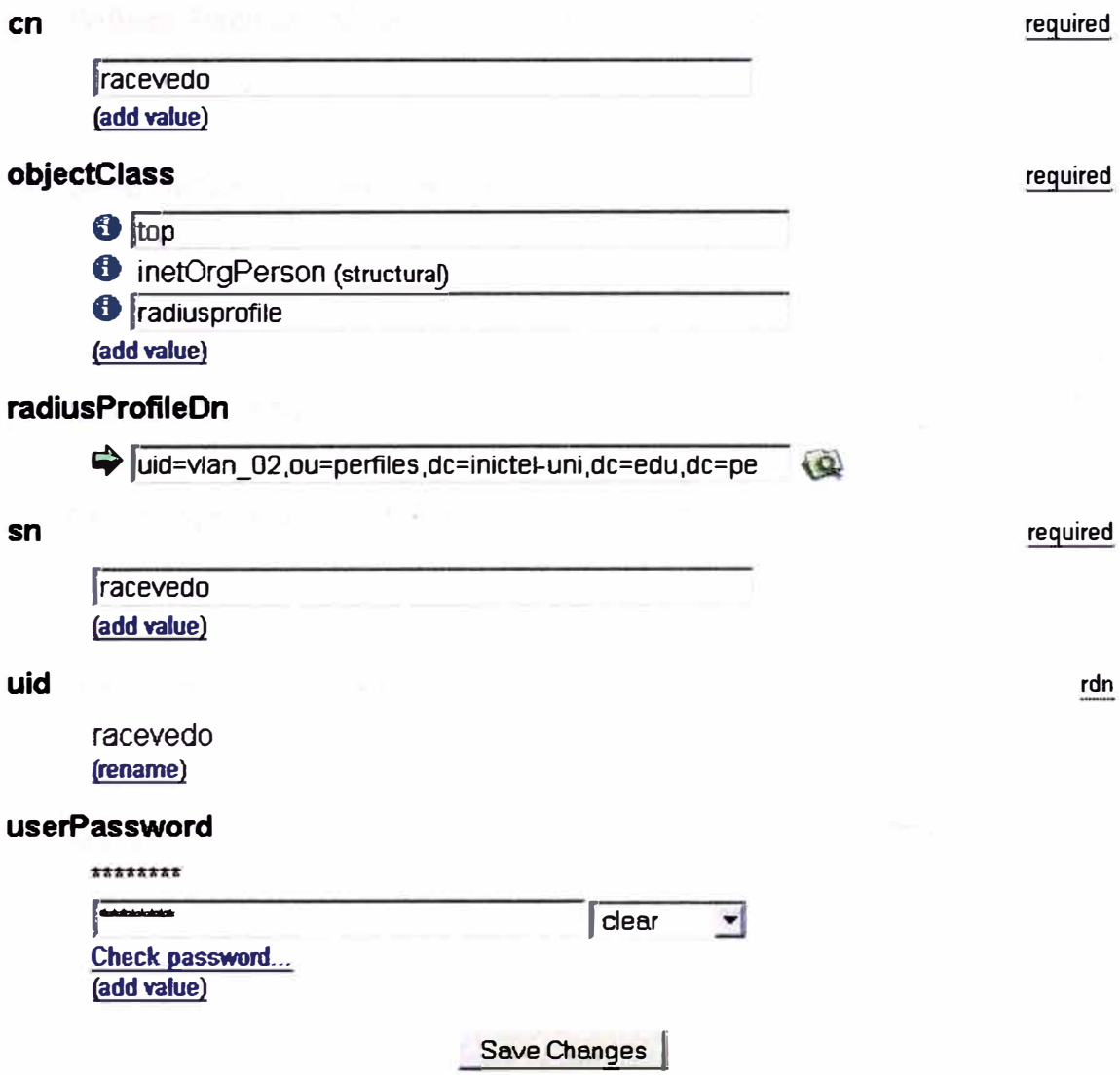
uid rdn

vlan_02

(rename)

En este anexo se muestra los valores que se ingresan en cada atributo para crear una entrada de Usuario en la estructura de nuestro servicio de directorio LDAP.

Los atributos cn (common name), sn (surname), son datos personales del cliente, el atributo uid (unix login) nos proporciona el nombre de usuario para registrase en el sistema, la clase de objetos objectClass es la misma que la entrada VLAN, la entrada radiusProfileDn indica la correspondencia con el perfil de entrada VLAN y el atributo userPassword almacena la contraseña de acceso del usuario al sistema.



BIBLIOGRAFÍA

1. IEEE Standards, IEEE Standard for Local and Metropolitan area networks - "Port-Based Network Access Control", IEEE Computer Society.

2. William Stallings, "Comunicaciones y Redes de Computadoras", Prentice Hall Sexta edición, 2000.

3. Steve McQuerry, "Interconexión de dispositivos de Red Cisco", Cisco Press, Edición 2001.

4. Michael Schwartzkopff, "Acceso seguro a redes con 802.1x, Radius y Ldap", www.linux-magazine.es

5. Charles Schwartz, "FreeRADIUS Tutorial for AD integration", http://homepages.lu/charlesschwartz/radius/freeRadius_AD_tutorial.pdf

6. José Manuel Suárez, "Curso OpenLDAP", GOA http://www.goa.es/docs/curso_openldap.pdf

7. "Configuring IEEE 802.1x Port-Based Authentication", Cisco Systems http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_8021x.pdf

8. 3com, Switches LAN, http://www.3com.com/prod/es_ES_EMEA/prodlist.jsp?tab=cat&cat=4

9. Cisco, Catalyst 2950-24 Switch, http://www.cisco.com/en/US/products/hw/switches/ps628/ps627/index.html

10. "IEEE 802.1X for Wired Networks and Internet Protocol Security with Microsoft Windows", Microsoft Corporation, https://www.microsoft.com/downloads/details.aspx?FamilyID=d9aef757-f528-41be-a01f-99a60c9a855d&displaylang=en

11. Wei Zhang,"Build a Radius server on Linux", IBM http://www-128.ibm.com/developerworks/library/l-radius/

12. FreeRADIUS, http://freeradius.org/

13. OpenLDAP, http://www.openldap.org

14. phpLDAPadmin, http://phpldapadmin.sourceforge.net/