UNIVERSIDAD DE SOTAVENTO A.C.

INCORPORADA A LA UNAM

LICENCIATURA EN INFORMÁTICA

"SEGURIDAD EN EL ACCESO A LA RED CABLEADA USANDO EL PROTOCOLO IEEE 802.1X EN PPQ."

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

P R E S E N T A

JORGE ALBERTO RIVAS PÉREZ

ASESOR:

MTRO. RAÚL DE JESÚS OCAMPO COLÍN

COATZACOALCOS, VER. **SEPTIEMBRE** 2013

INDICE

DEDICATORIAS Y AGRADECIMIENTOS

Al éxito no se encuentra fácilmente, se busca incansablemente, no se logra sólo con cualidades especiales, es sobre todo un trabajo de perseverancia, de método y de organización.

Tesis dedicada a toda mi familia.

Para mis padres queridos que tanto me ha dado y con mucho esfuerzo nos han sacado a mis hermanos y a mí. Yo se que tanto es lo que se sufre sacar una familia adelante y lo digo no porque haya formado una familia, sino, porque yo he estado con ustedes siempre ayudándolos a seguir adelante como la familia que somos, y aprendiendo siempre lo duro que es la vida y lo que cuesta ganarse el dinero y valorar todo en la vida.

Les doy gracias por todo lo que soy y lo que han hecho de mi en esta vida sin esperar nada a cambio, sin ustedes no sería nada ni siquiera existiera y por eso y muchas cosas más les doy gracias a ustedes y a dios por darme la vida y aprender de ella.

Quisiera agradecer a todas las personas que me aconsejaron y me orientado con el desarrollo de mi tesis, a todos los ingenieros de Pemex Petroquímica y a mi asesor que colaboraron amablemente con su tiempo y sus conocimientos durante el tiempo del desarrollo del tema. Y en especial a mi novia Margarita que a pesar de todas las cosas que hemos pasado y vivido, ha seguido a mi lado y siempre queriéndome como soy con mis defectos y mis virtudes, ha sido una gran motivación más en mi vida. Gracias amor.

Gracias por todo, muchas Gracias a todos!!!!

“SEGURIDAD EN EL ACCESO A LA RED CABLEADA USANDO EL PROTOCOLO IEEE 802.1X EN PEMEX PETROQUIMICA”

INTRODUCCIÓN

Las empresas dependen de sus redes de datos para servir de manera eficiente a los clientes y aumentar los ingresos. La amenaza de interrupción del servicio de red por fuentes no autorizadas, crece como la fiabilidad de la red y de seguridad más críticos. Los ataques desde la red interna son más peligrosos y más difíciles de prevenir que los ataques externos.Mecanismos de control de acceso permiten a los ingenieros de red, reducir el riesgo de intrusión de amenazas hacia la red, como gusanos de internet y los virus, así como la posibilidad de que las personas o grupos no autorizados, tengan acceso a la información controlada o confidencial.

Una forma de prevenir estos ataques a la red es implementando una función de autentificación en la capa 2 (la capa MAC)del modelo OSI (en inglés *open system interconnection*)usando el protocolo 802.1x, un switch habilitado con el estándar 802.1x y un servidor RADIUS es todo lo que se necesitaría para implementar la autentificación en la capa 2.

La IEEE 802.1X es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. El estándar 802.1x es una solución de seguridad ratificada por el IEEE que puede autenticar (identificar) a un usuario que quiere acceder a la red por medio de cable ethernet. Esto se hace a través del uso de un servidor de autenticación.

IEEE 802.1x proporciona control de acceso en la capa 2del modelo OSI.IEEE 802.1x soporta la autentificación de clientes mientras se establece la conexión a la red, antes de que al cliente se la asigne una dirección IP vía DHCP (Dynamic Host Configuration Protocol). Entre otras cosas, el estándar especifica como el protocolo de autentificación (*EAP, Extensible Authentication Protocol*) se encapsula en marcos Ethernet. EAP proporciona un marco de trabajo para varios

métodos de autentificación que soporta más que la combinación normal de nombre de usuario y clave. EAP utiliza el Network Access Server (*Autenticador*) para abrir un túnel para la autenticación del servidor a través de la red.

La forma en que opera el protocolo EAP se basa en el uso de un controlador de acceso llamado *autenticador*, que le otorga o deniega a un usuario el acceso a la red. El usuario en este sistema se llama *solicitante*. El controlador de acceso es un firewall básico que actúa como intermediario entre el usuario y el *servidor de autenticación*, y que necesita muy pocos recursos para funcionar.

El servidor de autenticación (a veces llamado *NAS*, que significa *Servicio de autenticación de red* o *Servicio de acceso a la red*) puede aprobar la identidad del usuario transmitida por el controlador de la red y otorgarle acceso según sus credenciales.

802.1X define un número términos especiales.Al igual el protocolo estándar maneja la autenticación y en el servidor Radius se proporcionan los servicios AAA (Autenticación, Autorización y Contabilidado Administración) accediendo al directorio del servidor para obtener información de las cuentas.El control de acceso es la forma en que se controla quien debe accesar a los equipos y a que servicios tiene permitidos una vez que acceso. La seguridad AAA provee el primer marco a través del cual se puede configurar el control de acceso a los equipos. Su función de la seguridad de AAA es identificar quien es la persona o equipo que solicita el acceso con ayuda del servidos RADUIS (*esto es la autentificación*), una vez identificada la persona o equipo, se autoriza el acceso con sus privilegios que le corresponden (*autorización*), registrando todos los recursos que utiliza, su identidad, el tipo de servicio que utiliza y el tiempo de entrada y salida del acceso (*contabilidad o adm.).*

También en el protocolo se implementa la integración de Cisco NAC y soluciones de Microsoft NAP en conjunto proporcionan la capacidad para reunir la identidad y

el estado de salud, información de un punto final, determinar el cumplimiento de las políticas de seguridad del punto final, proporcionar rehabilitación de servicios, y hacer cumplir políticas de acceso a redes basado en el cumplimiento del punto final. NAC y NAP detectan los equipos que no cumplan con las políticas de la empresa, haciendo una verificación del sistema operativo del equipo con el que obtendrán si está en buen estado sanitario dicho equipo, verificando por ejemplo si tiene todas las actualizaciones al día, antivirus activado, parches, firewall activado, etc. Si no cumple con estas políticas de salud, será puesto en una red de cuarentena o restringida, que contiene los recursos para corregir su sistema de salud y pueda tener acceso a la red de comunicación.

Con la integración de estas dos soluciones, un administrador puede verificar el estado de salud de un cliente de Microsoft Vista, proporcionar capacidades de recuperación, y proporcionar la aplicación de políticas dinámicas en la infraestructura de red.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Hoy en día la seguridad en las empresas es muy importe ya que requieren de mucha restricción en su información. Existen muchas formas de poder ver información restringida de una empresa, una de ellas es afectando su red por medio de virus informáticos. Pemex Petroquímica es una de las empresas de las más grandes e importantes a nivel mundial, el cual requiere de una eficaz estructura de seguridad en redes.

El usuario necesita conectarse prácticamente en cualquier punto de la red ya sea a través de un cable Ethernet o de manera inalámbrica y seguir contando con los servicios de datos, voz y video propios de su perfil. Esta necesidad implica un alto riesgo para la empresa, del cual surge el problema.

El problema que se presenta, es que usuarios de fuera que llegan a la empresa y se conectan a la red con sus computadoras por medio de cable Ethernet en los puertos físicos, algunas de estas computadoras traen algún tipo de virus que se ejecuta automáticamente al conectarse a la red de la empresa sin pasar por un medio de restricciones como autentificación y autorización. Estos virus informáticos causan daños y en ocasiones perdidas de información, tal empresa como Pemex no puede tener ningún tipo de virus por seguridad a la empresa.

1.2OBJETIVO GENERAL

Para establecer objetivo es necesario partir de la pregunta de investigación y de las preguntas secundarias. El objetivo general plantea el para qué y lo que se busca con la investigación de manera general, es el propósito a largo plazo del trabajo, es decir, es el punto de partida de lo que se va a desarrollar y sobre la cual también se va a concluir. Por ello se presenta a continuación:

"Preservar la seguridad en el acceso a la red cableada usando el protocolo IEEE 802.1x en PPQ."

1.3 OBJETIVOS ESPECÍFICOS

- ✓ Determinar que usuarios puedan ser responsables de problemas en la red reduciendo esfuerzos de análisis de fallas.
- ✓ Proveer accesos seguros basados en estándares tecnológicos.
- ✓ Asegurar que algún puerto autorizado no comprometa la red.
- ✓ Verificar el control de acceso a la red a través de los puertos físicos.
- ✓ Acceso a recursos limitados para usuarios externos.
- ✓ Validar el acceso contra el dominio de Pemex Petroquímica.
- ✓ Asegurar la integridad de la Información que viaja por las redes de Pemex Petroquímica.
- ✓ Preservar la confidencialidad de los datos.
- ✓ Aprovechar la infraestructura existente en Pemex Petroquímica.

1.4 PREGUNTA DE INVESTIGACION

¿Cómo implementar la seguridad en el acceso a la red cableada usando el protocolo IEEE 802.1x en PPQ?

PREGUNTAS SECUNDARIAS

¿El protocolo es capaz de proteger la red cableada de los intrusos?

¿Cuáles son los métodos para implementar el protocolo?

¿Qué más nos proporcionara el protocolo implementado?

¿Cuáles son los beneficios de este proyecto?

¿Se contara siempre con seguridad en el acceso la red del edificio?

¿Todos los puertos físicos de la empresa estarán protegidos?

¿Existirán puertos físicos que por necesidad u otra causa no se puedan proteger?

¿Se podrá mantener la confidencialidad de los datos de cada usuario?

¿Será necesaria toda la infraestructura de Pemex para el desarrollo de este protocolo o se necesitara de más infraestructura?

1.5 JUSTIFICACIÓN

La empresa necesita en parte, de la seguridad por medio de los puertos físicos, y otra, es que muchos conocen de la seguridad por medio de señales inalámbricas, incluyendo las tecnologías que se utilizan para la implementación de ese tipo de seguridad, pero no la protección por los puertos físicos, es algo que no todos conocen o no tienen conocimientos sobre este tipo de implementación y tecnologías basadas en red, incluyendo redes de área local (LAN), por el cual he decidido realizar mi tesis sobre este tema en especifico.

Este estándar que se implementara podrá mantener la seguridad en los nodos (puertos físicos) haciendo una verificación de autentificación y autorización del usuario y clave para la conexión hacia la red de área local, la autentificación de acceso de los usuarios en el borde de la red puede tener un lugar centralizado para navegar, mientras que en la red de los administradores pueden estar seguros que el acceso no autorizado se llevara a cabo, utilizando un grupo de mecanismos para limitar, controlar y monitorear el acceso a ciertos elementos de información, o a ciertos servicios en base a la identidad y pertenecía a un grupo predefinido.

Este sistema hace uso de certificados digitales para proporcionar a los usuarios tanto servicios de autenticación como de autorización, gestionando confiabilidad en la comunicación.

1.6 HIPÓTESIS

Si se aplican los estándares tecnológicos de la implementación del protocolo IEEE 802.1x se podrá preservar la seguridad en el acceso a la red cableada, asegurando la integridad de la información en la red de PPQ.

VARIABLES

Variable independiente:

Implementación del Protocolo IEEE 802.1x

Variable dependiente:

Preservar la Seguridad a la red cableada.

1.7DELIMITACIÓN DE LA INVESTIGACIÓN

En este apartado se establecerá descriptivamente la cobertura que tendrá la investigación en lo relativo a:

Espacio geográfico, es decir, el lugar donde se realizó la investigación.

- La implementación del protocolo será realizado en PPQ de Coatzacoalcos.

Sujetos y/u objetos que participaron en la realización del estudio.

- Puertos físicos.
- Switch
- Usuarios
- Servidor RADIUS
- Red cableada

Tiempo, especificando el periodo de tiempo en el que va hacerrealizada la investigación.

- La implementación de este protocolo se tiene determinado realizarse en un periodo de diez meses.

Contenidos, se menciona la o las variables que se consideraron en el estudio.

- Seguridad
- Red cableada
- Acceso a la red

1.8LIMITACIONES

Las limitantes del tema para la implementación del protocolo estándar son:

- ✓ Toda la red debe de estar switcheada, es decir que solo tenga Switch en la red, ningún hub porque de ser así no se podría implementar el protocolo.
- ✓ Todos los dispositivos de red deberán soportar el protocolo 802.1x, para el caso de las impresoras que se encuentran por red y servidores UNIX y sistemas de almacenamiento, se deberán identificar los puertos con la finalidad de excluirlos de la aplicación de la política de acceso.
- ✓ No se cuenta con el equipo necesario para implementar el procedimiento NAC.
- ✓ No se podrá implementar en todo el edificio por cuestiones de equipos de red y requerimientos de permisos.

CAPITULO II
MARCO TEÓRICO

ANTECEDENTES DEL INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS (IEEE) 802

2.1 ANTECEDENTE DE LA IEEE 802

2.1.1. ESTANDAR IEEE 802

IEEE 802 es un estudio de estándares perteneciente al Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), que actúa sobre redes de computadoras, concretamente y según su propia definición sobre redes de área local (RAL, en inglés LAN) y redes de área metropolitana (MAN en inglés). También se usa el nombre **IEEE 802** para referirse a los estándares que proponen, y algunos de los cuales son muy conocidos: Ethernet (IEEE 802.3), o Wi-Fi (IEEE 802.11), incluso está intentando estandarizar Bluetooth en el 802.15.

El primer estándar IEEE 802 LAN se produjo en la década de 1980. Es una asociación internacional sin ánimo de lucro con sede principal en la ciudad de Piscataway en los Estados Unidos y subsedes en más de 150 países del mundo, con alrededor de *367,395* ingenieros, estudiantes de ingeniería, científicos y otros profesionistas.

El IEEE es la mayor sociedad profesional del mundo. De ámbito internacional, sus objetivos son el desarrollo de la teoría, la creatividad y la calidad de los productos en el campo de la ingeniería eléctrica, la electrónica y la radio, así como otras ramas relacionadas de la ingeniería. Como uno de sus objetivos principales, el IEEE prevé el desarrollo y adopción de estándares internacionales para computación. Su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.[1]

[1]A. Behrouz A. Transmisión de Datos y Redes de Comunicación. Pág. 12

2.1.2 IEEE 802.1X

La **IEEE 802.1X** es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. El estándar 802.1x es una solución de seguridad ratificada por el IEEE que puede autenticar (identificar) a un usuario que quiere acceder a la red por medio de cable ethernet. Esto se hace a través del uso de un servidor de autenticación.

Dicho estándar proporciona un sistema de control de dispositivos de red, de admisión, de tráfico y gestión de claves para dispositivos en una red. 802.1X se basa en puertos, para cada cliente dispone de un puerto que utiliza para establecer una conexión punto a punto. Mientras el cliente no sea validado este puerto permanece cerrado.[2]

802.1x consta de tres componentes para el control de puertos, que son los siguientes:

• *Un autentificador 802.1x:* Este es el puerto en el interruptor que tiene servicios para ofrecer a un dispositivo de cierre, siempre que el dispositivo de suministro de las credenciales adecuada sean correctas.

• *Un suplicante 802.1x:* Este es el dispositivo final, por ejemplo, un PC que se conecta a un interruptor que está solicitando a utilizar los servicios del dispositivo. El suplicante 802.1x debe ser capaz de responder a comunicarse.

• *Un servidor de autenticación 802.1X:* Este es un servidor que examina las credenciales proporcionadas al autenticador del solicitante y proporciona el servicio de autenticación, pudiéndose utilizar un servidor RADIUS (*Remote Authentication Dial-In User Server)*. El servidor de autenticación es responsable

[2]http://dns.bdat.net/seguridad_en_redes_inalambricas/x75.html

por que permitir que el autenticador pueda saber los servicios que se concederán.RADIUS (RemoteAuthentication Dial-In UserService) es un protocolo de autenticación basado en cliente y servidor que le permite a un servidor de acceso remoto comunicarse con un servidor central para poder autenticar usuarios que acceden a la red y autorizar el uso de los servicios requeridos. Este sistema, generalmente se implementa mediante software, e inicialmente su función principal fue autorizar a los usuarios de acceso conmutado (dial-in) de un proveedor de servicios de Internet (ISP) para permitir su acceso a la red pública.[3]

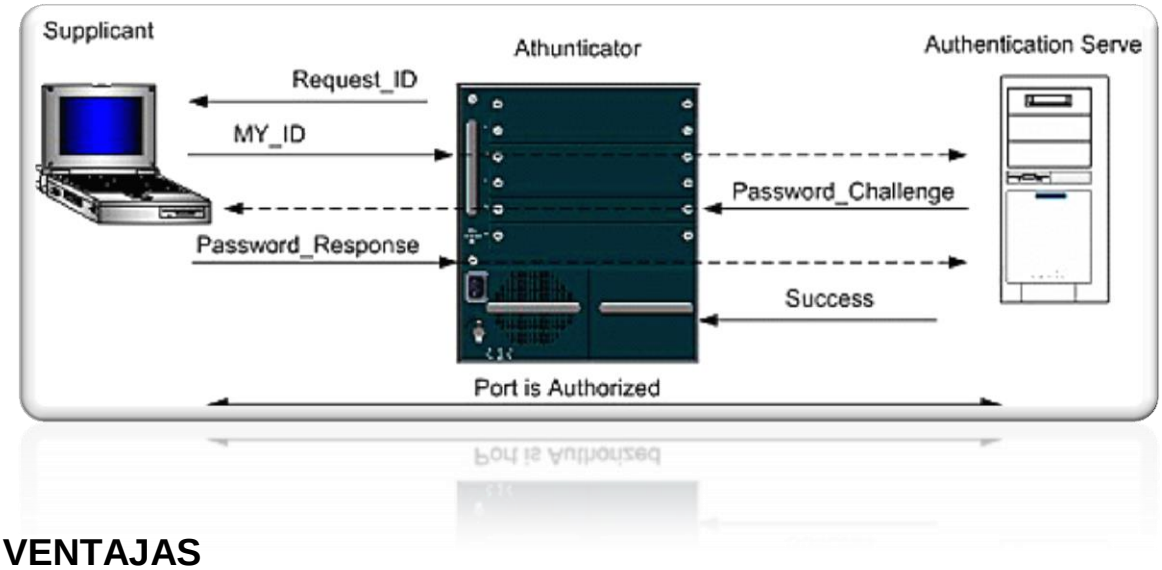
El *autentificador* 802.1X funciona como un intermediario con el solicitante y el servidor de autenticación para prestar servicios a la red. Cuando un interruptor se configura como un autenticador, los puertos del conmutador a continuación, debe estar configurado para su autorización. En una autorización puerto autenticador iniciado, un cliente se inicia o se enchufa en el puerto y el puerto autenticador envía un protocolo de autenticación extensible (EAP) al suplicante que solicita la identificación del solicitante. En este punto del proceso, el puerto en el interruptor está conectado desde un punto de vista físico, sin embargo, el proceso de 802.1X no ha autorizado el puerto y sin marcos se pasan desde el puerto en el suplicante en el tejido de conmutación. Si el PC conectado al switch no entiende que el PEA que estaba recibiendo del interruptor, no sería capaz de enviar un documento de identidad y el puerto quedaría autorizado. En este estado, el puerto nunca pasa ningún tráfico del usuario y es tan buena como discapacitados. Si el sistema cliente esté ejecutando el 802.1X EAP, que respondería a la solicitud con su identificador configurado. (Esto podría ser un nombre de usuario y una contraseña o un certificado.)

Después del cambio, el autenticador recibe el ID de la PC (el suplicante). El interruptor a continuación, pasa la información de identificación a un servidor de autenticación (servidor RADIUS) que podrá verificar la información de

[3]http://www.sans.org/reading_room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlans_1607

identificación. El servidor RADIUS responde al conmutador, ya sea con un mensaje de éxito o fracaso. Si la respuesta es un éxito, el puerto será autorizado y el tráfico de usuarios se les permitirá pasar a través del puerto como cualquier puerto del switch conectado a un dispositivo de acceso. Si la respuesta es un fracaso, el puerto seguirá siendo no autorizado y, por tanto, no se utiliza. Si no hay respuesta del servidor, el puerto seguirá siendo no autorizado y no se pasa ningúntráfico.

La figura1.1 muestra el cambio de una autorización puerto autenticador iniciado.[4]



VENTAJAS

- Ofrece seguridad basada en identidades (IBNS).
- No da acceso físico a la red hasta que se supera la fase de autenticación.
- Ideal en entornos donde la seguridad es crítica, de acuerdo a la información que viaja atreves de la red y/o aplicaciones que se usan en la red.
- Políticas o niveles distintos de accesos por usuario (autorizaciones).
- Permite implantar NAC (Network Admission Control):
  - Checklist de S.O: antivirus, parches, actualizaciones, etc.
  - Red de cuarentena.
  - Asignar VLAN por usuario.

[4]http://www.ciscopress.com/articles/article.asp?p=29600&seqNum=2

DESVENTAJAS

- Complejo de implantar.
- A mayor seguridad en una red es menor su flexibilidad.
- Curva de aprendizaje elevada.
- Personal calificado.
- Requiere mucha administración de claves y contraseñas.
- La electrónica de red y los clientes debensoportar 802.1X, RADIUS, EAP, etc.
- Desaconsejado en entornos donde laseguridad no es crítica.

TEORÍAS QUE SUSTENTAN LA INVESTIGACIÓN

2.2 TEORÍAS QUE SUSTENTAN LA INVESTIGACIÓN

2.2.1 REDES

Una red es un conjunto de dispositivos (a menudo denominados nodos, conectados por enlaces de un medio físico. Un nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red. Los enlaces conectados con los dispositivos se denominan a menudo ***canales de comunicación***.[5]

Una red está conformada por varios dispositivos que permiten la comunicación hacia los nodos, tales como enrutadores, conmutadores (switch), hubs, etc. Los cuales se denominan ***equipos activos de conectividad*** y permiten el intercambio de información entre los nodos.

Un conjunto básico de las reglas sobre cómo debe de hacer su trabajo una red de computadoras se podría ver de la siguiente manera:

- La información debe entregarse de manera confiable sin ningún daño en los datos.
- La información debe entregarse de manera consistente, la red debe de ser capaz de determinar hacia donde se dirige la información.
- Las computadoras que forman la red deben ser capaces de identificarse entre sí a lo largo de toda la red.
- Debe existir una forma estándar de nombrar e identificar las partes de la red.

Una red debe ser:

- *Confiable.* Estar disponible cuando se le requiera, poseer velocidad de respuesta adecuada.

[5]A. Behrouz A. Transmisión de Datos y Redes de Comunicación. Pag. 4

- *Confidencial*. Proteger los datos sobre los usuarios de ladrones de información.
- *Integra*. En su manejo de información.

2.2.1.1.REDES DE AREA LOCAL

Una red de área local (LAN) suele ser una red de propiedad privada que conectan enlaces de una única oficina, edificio o campus, es un sistema de transmisión de datos que permiten que un cierto número de dispositivos independientes se comuniquen entre sí dentro de un área geográfica.[6]

Las LAN están diseñadas para permitir interconectar ordenadores o equipos de computo que estén dentro de un mismo edificio o en edificios colindantes compartiendo recursos entre computadoras personales o estaciones de trabajo, intercambiando información, comunicándose y accediendo a diversos servicios; pero siempre teniendo en cuenta que el medio físico que los une no puede tener más de unos miles de metros al igual.

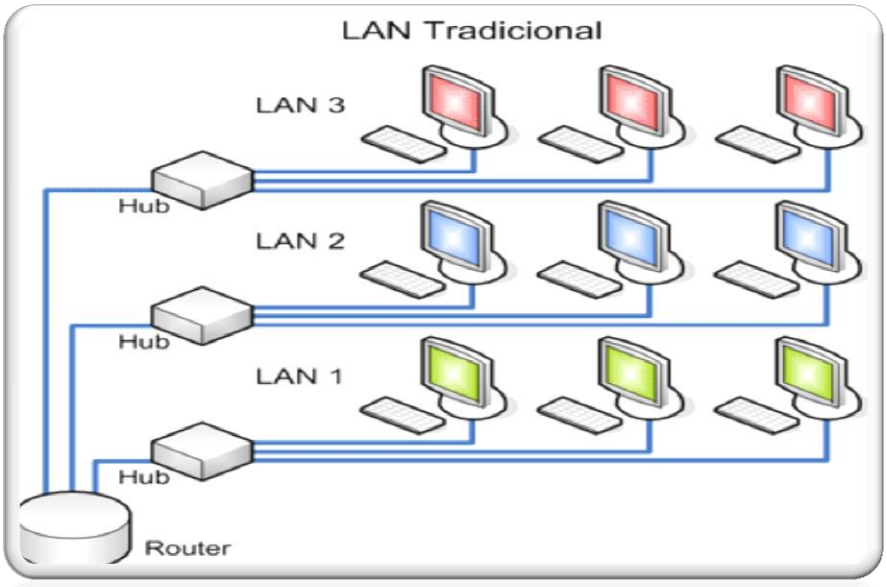


Figura 2.2.1. Representación de una LAN tradicional.

[6]A. Behrouz A. Transmisión de Datos y Redes de Comunicación. Pág. 355

2.2.1.2 REDES DE AREA LOCAL VIRTUALES (VLAN'S)

Es una red de área local que agrupa un conjunto de equipos de manera lógica y no física,[7] es una red conmutada que está lógicamente segmentada en base a funciones(trabajadores de un mismo departamento), grupos de proyectos o usuarios compartiendo lamisma aplicación, sin importar la ubicación física de los usuarios, su núcleo es el switch. Una VLAN tiene los mismos atributos que una LAN física, pero se puede agrupar a las estaciones finales aun y cuando no estén físicamente localizados en el mismo segmento físico de red.

Cualquier puerto de un switch puede pertenecer a una VLAN, y los paquetes de unicast, broadcast y multicast serán pasados y distribuidos solo en las estaciones finales de la VLAN correspondiente. Cada VLAN es considerada una red lógicamente independiente y los paquetes destinados a estaciones finales que no pertenecen a la misma VLAN deberán ser enviados atreves de un enrutador o puente.

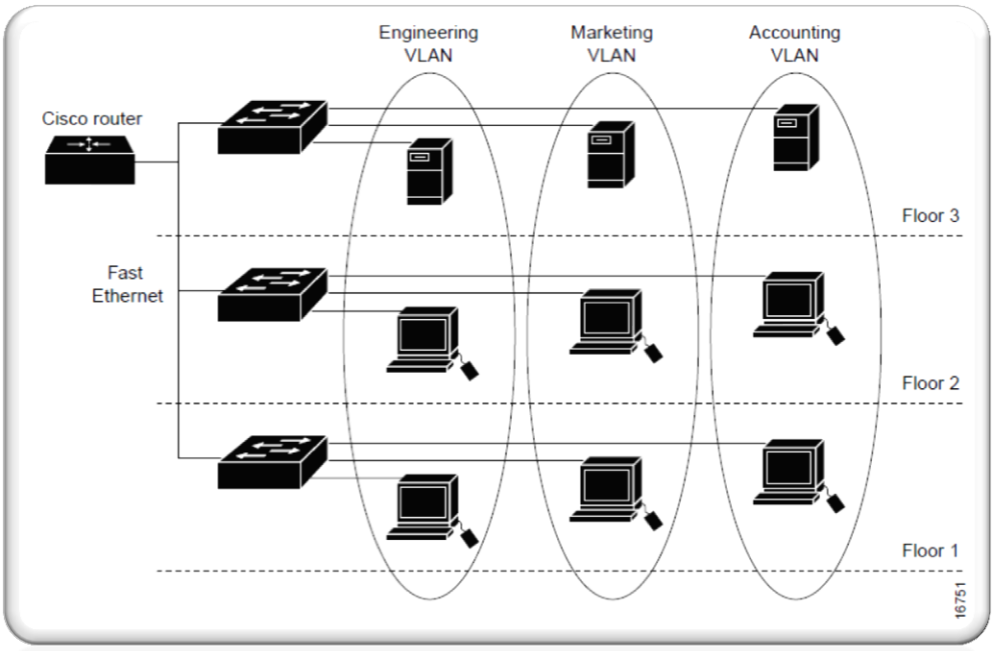


Figura 2.2.2. La imagen muestra un ejemplo de una red puede tener varias VLAN's.

[7] http://es.kioskea.net/contents/internet/vlan.php3

2.2.1.3. PROTOCOLO 802.1Q

El protocolo **IEEE 802.1Q** permite que las VLANs individual se comunique el uno con el otro con el uso de la capa de red (3), se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

La especificación IEEE 802.1Q establece un método normalizado para el marcado tramas Ethernet con VLAN información de socio. El estándar IEEE 802.1Q define la operación de la VLAN puentes que permitan la definición, funcionamiento y administración de Virtual topologías LAN dentro de una estructura en puente de LAN.

El estándar 802.1Q se propone abordar el problema de cómo romper las redes de gran tamaño en partes más pequeñas para el tráfico de difusión y multidifusión no agarrar más ancho de banda de lo necesario. La norma también ayuda a proporcionar un mayor nivel de seguridad entre segmentos de redes internas.

2.2.1.4. TIPOS DE VLAN

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

La **VLAN de nivel 1** (también denominada *VLAN basada en puerto*) define una red virtual según los puertos de conexión del conmutador; la VLAN consiste en una agrupación de puertos físicos que puede tener lugar sobre un conmutador o también, en algunos casos, sobre varios conmutadores. La asignación de los equipos a la VLAN se hace en base a los puertos a los que están conectados físicamente.

Muchas de las primeras implementaciones de las VLAN's definían la pertenencia a la red virtual por grupos de puertos (por ejemplo, los puertos 1, 2, 3,7 y 8 sobre un conmutador forman la VLAN A, mientras que los puertos 4,5 y 6 forman la VLAN

B). Además, en la mayoría, las VLANs podían ser construidas sobre un único conmutador.

La agrupación por puertos es todavía el método más común de definir la pertenencia a una VLAN, y su configuración es bastante directa. El definir una red virtual completamente basada en puertos no permite a múltiples VLANs el incluir el mismo segmento físico (o conmutador).

De todos modos, la principal limitación de definir VLANs por puertos es que el administrador de la red ha de reconfigurar la VLAN cada vez que un usuario se mueve de un puerto a otro.

La **VLAN de nivel 2** (también denominada *VLAN basada en la dirección MAC*) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación; constituye la segunda etapa de la estrategia de aproximación a la VLAN, y trata de superar las limitacionesde las VLANs basadas en puertos. Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC.

Desde que las direcciones MAC (*media access control* -control de acceso al medio-) se encuentran implementadas directamente sobre la tarjeta de interface de la red (NIC -*network interface card*-), las VLANs basadas en direcciones MAC permiten a los administradores de la red el mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. De este modo, las VLANs basadas en MAC pueden ser vistas como una VLAN orientada al usuario.

Entre los inconvenientes de las VLANs basadas en MAC está el requerimiento de que todos los usuarios deben inicialmente estar configurados para poder estar en al menos una VLAN. Después de esa configuración manual inicial, el movimiento automático de usuarios es posible, dependiendo de la solución específica que el distribuidor haya dado. Sin embargo, la desventaja de tener que configurar inicialmente la red llega a ser clara en redes grandes, donde miles de usuarios

deben ser asignados explícitamente a una VLAN particular. Algunos distribuidores han optado por realizar esta configuración inicial usando herramientas que crean VLANs basadas en el actual estado de la red, esto es, una VLAN basada en MAC es creada para cada subred.

Las VLANs basadas en MAC que son implementadas en entornos de medios compartidos se degradarán seriamente como miembros de diferentes VLANs coexistiendo en un mismo conmutador. Además, el principal método de compartición de información entre miembros de una VLAN mediante conmutadores en una red virtual basada en MAC también se degrada cuando se trata de una implementación a gran escala.

La **VLAN de nivel 3**: existen diferentes tipos de VLAN de nivel 3:

- la **VLAN basada en la dirección de red** conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.
- la **VLAN basada en protocolo** permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.[8]

Las VLANs de capa 3 toman en cuenta el tipo de protocolo (si varios protocolos son soportados por la máquina) o direcciones de la capa de red, para determinar la pertenencia a una VLAN.

Hay varias ventajas en definir VLANs de capa 3. En primer lugar, permite el particionado por tipo de protocolo, lo que puede parecer atractivo para los

[8] http://es.kioskea.net/contents/internet/vlan.php3

administradores que están dedicados a una estrategia de VLAN basada en servicios o aplicaciones. En segundo lugar, los usuarios pueden físicamente mover sus estaciones de trabajo sin tener que reconfigurar cada una de las direcciones de red de la estación (este es un beneficio principalmente para los usuarios de TCP/IP). Y en tercer lugar, definir una VLAN de capa 3 puede eliminar la necesidad de marcar las tramas para comunicar miembros de la red mediante conmutadores, reduciendo los gastos de transporte.

Una de las desventajas de definir la VLAN de capa 3 (al contrario de lo que ocurría en las dos anteriores) es su modo de trabajo. El inspeccionar direcciones de la capa 3 en paquetes consume más tiempo que buscar una dirección MAC en tramas. Por esta razón, los conmutadores que usan información de la capa 3 para la definición de VLANs son generalmente más lentos que los que usan información de la capa 2. Esta diferencia no ocurre en todas las distintas implementaciones de cada distribuidor.

Las VLANs basadas en capa 3 son particularmente efectivas en el trato con TCP/IP, pero mucho menos efectivas con protocolos como IPX, DEC *net* o AppleTalk, que no implican configuración manual. Además tienen la dificultad al tratar con protocolos no enrutables como NetBIOS (estaciones finales que soportan protocolos no enrutables no pueden ser diferenciadas y, por tanto, no pueden ser definidas como parte de una VLAN).

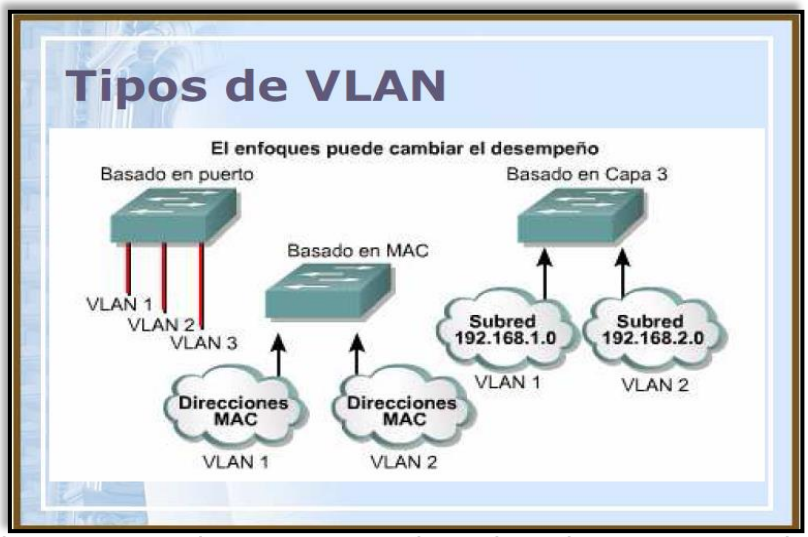


Figura 2.2.3. La imagen muestra los 3 tipos de VLANs que existen.

2.2.1.4.1.Ventajas de las VLANs

Reducción del Costospor Movimientos y Cambios.

La principal excusa para implementar una VLAN es la reducción en loscostosprovocados por cambios y movimientos de usuarios. Desde que estos costes son bastante sustanciales, este argumento es suficientemente obligatorio para la implementación de una VLAN.

Muchos fabricantes están prometiendo que la implementación de una VLAN resultará más conveniente a la hora de habilitar la administración de redes dinámicas, y que esto supondrá bastante ahorro. Esta promesa se puede aplicar con buenos resultados a redes IP, ya que, normalmente, cuando un usuario se mueve a una diferente subred, las direcciones IP han de ser actualizadas manualmente en la estación de trabajo. Este proceso consume gran cantidad de tiempo que podría ser aprovechado para otras tareas, tales como producir nuevos servicios de red. Una VLAN elimina ese hecho, porque los miembros de una red virtual no están atados a una localización física en la red, permitiendo que las estaciones cambiadas de sitio conserven su dirección IP original.

Sin embargo, cualquier implementación de VLAN no reduce este coste. Una VLAN añade una nueva capa de conexión virtual que ha de ser administrada al mismo tiempo que la conexión física. Esto no quiere decir que no se puedan reducir los costes hablados anteriormente. Sólo que no hay que precipitarse a la hora de implementar una VLAN y es mejor estar bien seguro de que la solución no genera más trabajo de administración de red que el que se pueda ahorrar.

Grupos de Trabajo Virtuales.

Uno de los objetivos más ambiciosos de una red virtual es el establecimiento del modelo de grupos de trabajo virtuales. El concepto es que, con una completa implementación de una VLAN a través de todo el entorno de red del campus, miembros del mismo departamento o sección puedan aparentar el compartir la

misma red local, sin que la mayoría del tráfico de la red esté en el mismo dominio de *broadcast (*transmisión de un paquete que será recibido por todos los dispositivos en una red) de la VLAN. Alguien que se mueva a una nueva localización física pero que permanezca en el mismo departamento se podría mover sin tener que reconfigurar la estación de trabajo.

Esto ofrece un entorno más dinámicamente organizado, permitiendo la tendencia hacia equipos con funciones cruzadas. La lógica del modelo virtual por grupos de trabajo va la siguiente forma: los equipos pueden estar conectados virtualmente a la misma LAN sin necesidad de mover físicamente a las personas para minimizar el tráfico a través de una red troncal colapsada. Además, estos grupos serán dinámicos: un equipo destinado a un proyecto puede ser configurado mientras dure ese proyecto, y ser eliminado cuando se complete, permitiendo a los usuarios retornar a sus mismas localizaciones físicas.

Seguridad.

El único tráfico de información en un segmento de un sólo usuario será de la VLAN de ese usuario, por lo que sería imposible "escuchar" la información si no nos es permitida, incluso poniendo el adaptador de la red en modo promiscuo, ya que ese tráfico de información no pasa físicamente por ese segmento.

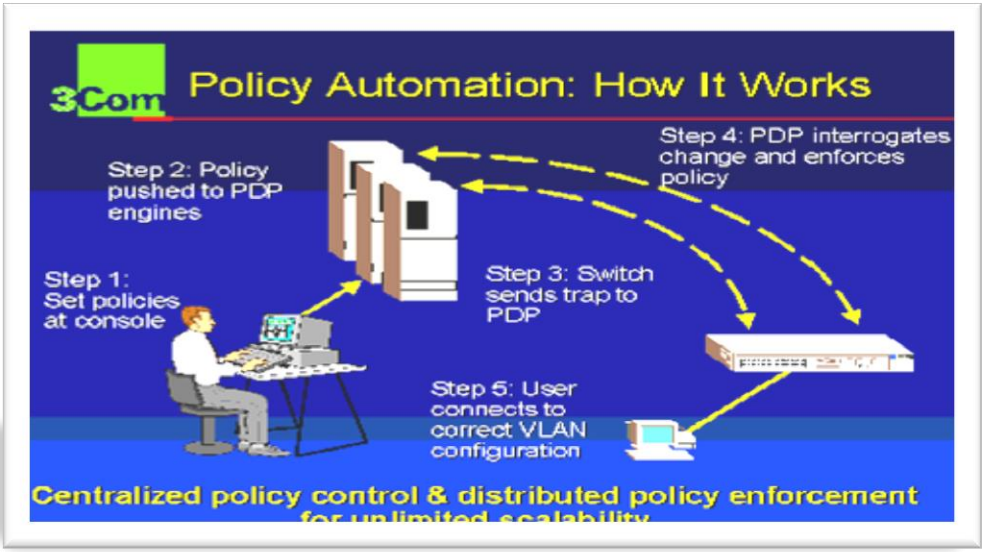
2.2.1.4.2. VLANs Basadas en Reglas (*Policy Based VLANs).*

Este esquema es el más potente y flexible, ya que permite crear VLANs adaptadas a necesidades específicas de los gestores de red utilizando una combinación de reglas. Estas reglas pueden ser, por ejemplo, de acceso, con objeto de alcanzar unos ciertos niveles de seguridad en la red. Una vez que el conjunto de reglas que

constituyen la política a aplicar a la VLAN se implementa, sigue actuando sobre los usuarios al margen de sus posibles movimientos por la red.

Gestión basada en políticas es uno de los más altos valores ofrecidos por VLAN. Este tipo de gestión define la pertenencia a una VLAN de servicio definidos o grupo de trabajo. Las políticas son establecidas por el administrador de la red basada en una variedad de requisitos de servicio que se aplican a una VLAN determinada, como una determinada cantidad de ancho de banda, grupo de trabajo o miembros del proyecto, el acceso a bases de datos específicas, etc. Además de nivel de servicio, la política de seguridad se puede asignar a una calidad de miembro de VLAN, lo que permite el acceso de sólo lugares específicos, por ejemplo, la oficina, el hogar o en la carretera. Una vez que se definen las políticas, un miembro de VLAN pueden estar asociados con una política o un conjunto de políticas y que disponga de todos los derechos asociados de que la política con un simple clic del ratón. Cuando el miembro de VLAN ya no requiere que estos derechos, la póliza puede ser retirado y una nueva política se puede asociar a ese miembro.[9]

La figura 2.2.4 muestra la función de las políticas basadas en reglas.



9 http://translate.google.com.mx/translate?hl=es&sl=en&u=http://support.3com.com/infodeli/tools/netmgt/temwin/tem6.2/evm/chap_4a3.htm&ei=yv0STK3rEcO7ngen_8yEDA&sa=X&oi=translate&ct=result&resnum=2&ved=0CCMQ7gEwAQ&prev=/search%3Fq%3DPolicy%2BBased%2BVLANs%26hl%3Des

2.2.1.5¿COMO SE CONECTAN LAS REDES?

Si se fuera a dividir una red en sus componentes más simples, tendríamos dos partes. Una es la red física: el cableado, las tarjetas de red, las computadoras y demás equipos que utiliza la red para transmitir datos. La otra parte es la disposición lógica de esos componentes físicos: las reglas que permiten a los componentes físicos trabajar en conjunto.

La parte física: el hardware

La red física es fácil de entender pues que la parte visible: “el hardware”. Está conformada por el cableado, las tarjetas de red, las computadoras, los hubs y todo el material adicional que permite que la red funcione. La parte física de la conectividad de redes es totalmente hardware que es lo más importante, es algo tangible, que puede tener en sus manos.[10]

La red lógica

La red lógica es lo que los usuarios ven cuando se encuentran trabajando en sus escritorios. Las redes lógicas son colecciones de recursos tales como espacio en disco duro, impresoras y aplicaciones a las que las computadoras no tendrían acceso si no estuviera conectada a una red. Las redes lógicas no son físicas, son el resultado de la organización de la red física.

Estos son formas similares especiales que tienen las computadoras para comunicarse entre sí, son muy similares a un idioma. Con toda su complejidad, las redes de computadoras tienen que hablar el mismo idioma, lo que en elcampo de la conectividad de redes se conocen como protocolos de red. Un gran número de servicios relacionados con las redes y paquetes de software caen en el ámbito lógico de una red.[11]

[10]Matt Hayden. Aprendiendo Redes en 24 Hrs. pág. 5
[11]Matt Hayden. Aprendiendo Redes en 24 Hrs. pág. 10

2.2.1.6. PROTOCOLOS DE SEGURIDAD EN RED

Dentro de los ejemplos de redes lógicas se incluyen cosas como los protocolos de red.

Se desarrollan protocolos que proporcionan servicios de seguridad en redes inseguras. También se introducen protocolos para establecer una asociación de seguridad y para la gestión de claves.[12]

Un protocolo de seguridad indica un conjunto de reglas que gobiernan la iteración entre procesos para proporcionar cierto tipo de servicio de seguridad. El protocolo especifica los mensajes que se van a intercambiar, el tipo de procesamiento que se va a implementar y las acciones que se van a tomar cuando ocurren ciertos eventos, diseñadas para que el sistema pueda soportar ataques de carácter maliciosos.

Algunos protocolos de la capa de red que se van a utilizar para la implementacióndel protocolo estándarson mencionados:

PROTOCOLOS DE ACCESO A LA RED

Protocolos de la capa 2 (capa de transmisión de datos)

- ARCnet.
- CDP: Protocolo de descubrimiento de Cisco.
- DCAP: Protocolo de acceso del cliente de la conmutación de la transmisión de datos.
- FDDI: Interfaz de distribución de datos en fibra.
- FrameRelay.
- HDLC: Control de enlace de datos de alto nivel.

[12]Alberto León García, Indra Widjaja. Redes de Comunicación. Conceptos Fundamentales y Arquitectura Básicas. pág. 627.

- LocalTalk.
- L2F: Protocolo de la expedición de la capa 2.
- L2TP: Protocolo de túnel capa 2.
- LAPD: Procedimientos de acceso de acoplamiento en el canal D.
- LLDP: Protocolo del descubrimiento de la capa de acoplamiento.
- LLDP-MED: Protocolo del descubrimiento de la capa de acoplamiento-Descubrimiento del punto final de los medios.
- PPP: Protocolo Punto a Punto.
- PPTP: Protocolo túnel punto a punto.
- SLIP: Protocolo de internet de Línea serial (obsoleto).
- StarLan.
- STP: Protocolo del árbol esparcido.
- VTP VLAN: Trunking virtual para LAN virtual.

Protocolos de la capa 2+3

- ATM Modo de Transferencia Asincrona.
- Capítulo el relais, una versión simplificada de X.25.
- MPLS Conmutación Multi-protocol de la etiqueta.
- Señalando el sistema 7, también llamado SS7, C7 y CCIS7; un común PSTN control protocolo.
- X.25

Protocolos de la capa 3 (capa de red)

- AppleTalk
- ARP Protocolo de resolución de Direcciones
- BGP protocolo de frontera de entrada

- EGP exterior de entrada de protocolo
- ICMP Internet de control del protocolo del mensaje
- IGMP Protocolo de la gerencia del grupo de Internet
- IPv4Protocolo de internet versión 4
- IPv6 Protocolo de internet versión 6
- IPX Red interna del intercambio del paquete
- IS-IS Sistema intermedio a sistema intermedio
- MPLSMultiprotocolo de conmutación de etiquetas
- OSPF Abrir la trayectoria más corta primero
- RARP Protocolo de resolución de direcciones inverso

PROTOCOLOS DE ENRUTAMIENTO DINAMICO

- **IGPs**(Interior Gateway Protocols). Intercambian información de encaminamiento dentro de un único sistema autónomo. Los ejemplos más comunes son:

- **IGRP**(Interior Gateway Routing Protocol). La diferencia con la RIP es la métrica de enrutamiento.
- **EIGRP**(Enhanced Interior Gateway Routing Protocol). Es un protocolo de enrutamiento vector-distancia y estado de enlace.
- **OSPF**(Open Shortest Path First). Enrutamiento jerárquico de pasarela interior.
- **RIP**(Routing Information Protocol). No soporta conceptos de sistemas autónomos.
- **IS-IS** (Intermediate System to Intermediate System). Protocolo de intercambio enrutador de sistema intermedio a sistema intermedio

- **EGPs**(Exterior Gateway Protocol). Intercambian rutas entre diferentes sistemas autónomos. Encontramos:

- **EGP**. Utilizado para conectar la red de backbones de la Antigua Internet.
- **BGP**(Border Gateway Protocol). La actual versión, BGPv4 data de 1995.

- **DHCP**

DHCP (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de *host*) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

2.2.1.7 CABLEADO DE LAS INSTALACIONES

No importa que tan bien diseñada esta una red ni la calidad de sus componentes individuales, si el cable que enlaza a las computadoras no se encuentra instalado de manera adecuada, la red no funcionará adecuadamente. El cableado de las redes es el guardián invisible de la red. Cuando la red funciona bien, ni siquiera se detecta y cuando no, es muy difícil generar un diagnostico a menos que se utilicen aparatos muy sofisticados.

En general, existen tres tipos de cableado en las redes: cable coaxial, par trenzado y fibra óptica. Cada uno de ellos tiene requerimientos diferentes si van a satisfacerlos estándares de redes y a trabajar adecuadamente.[13]

2.2.1.8. CABLEADO A UTILIZAR EN EL PROTOCOLO IEEE 802.1X

2.2.1.8.1. ACCESO: UTP CAT6

Cable de categoría 6, o Cat 6 es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retro compatible con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para crosstalk (diafonía) y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (*Gigabit Ethernet*). Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1Gbps.

2.2.1.8.2.COMPOSICIÓN DEL CABLE

El cable contiene 4 pares de cable de cobre trenzado. Aunque la categoría 6 está a veces hecha con cable *23 AWG*, esto no es un requerimiento; la especificación **ANSI/TIA-568-B.2-1**(son las asignaciones pin / par para ocho hilos y 100 ohmios balanceado de par trenzado de cables) aclara que el cable puede estar hecho

[13]Matt Hayden. Aprendiendo Redes en 24 Hrs. pág. 79

entre 22 y 24 AWG, mientras que el cable cumpla todos los estándares de pruebas indicados. Cuando es usado como un *patch cable (cable de conexión)*, Cat-6 es normalmente terminado con conectores RJ-45, a pesar de que algunos cables Cat-6 son incómodos para ser terminados de tal manera sin piezas modulares especiales y esta práctica no cumple con el estándar.

Si los componentes de los varios estándares de cables son mezclados entre sí, el rendimiento de la señal quedará limitado a la categoría que todas las partes cumplan. Como todos los cables definidos por TIA/EIA-568-B (tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones), el máximo de un cable Cat-6 horizontal es de 90 metros (295 pies). Un canal completo (cable horizontal más cada final) está permitido a llegar a los 100 metros en extensión.

Los cables UTP Cat-6 comerciales para redes LAN, son eléctricamente construidos para exceder la recomendación del grupo de tareas de la IEEE, que está trabajando desde antes de 1997.[14]

2.2.1.8.3.INTERCONEXION DE SITIOS

FIBRA ÓPTICA MONOMODO Y FIBRA ÓPTICA MULTIMODO

La *fibra óptica* es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el núcleo de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total. La fuente de luz puede ser láser o un LED.

Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de

[14]http://es.wikipedia.org/wiki/Cable_de_categor%C3%ADa_6

radio o cable. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

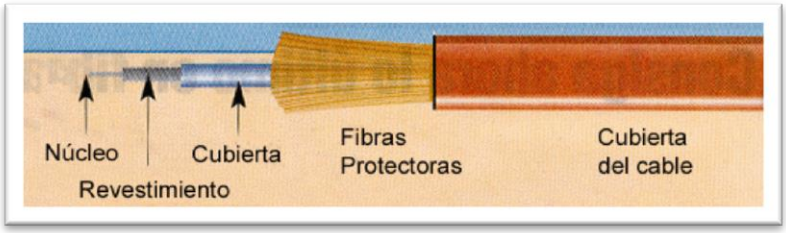


Figura 2.2.5. La imagen muestra los componentes de una fibra óptica.

2.2.1.8.4.CONECTORES

Los conectores más comunes usados en la fibra óptica para redes de área local son los conectores ST y SC.

El conector SC (Set and Connect) es un conector de inserción directa que suele utilizarse en conmutadores Ethernet de tipo Gigabit. El conector ST (Set and Twist) es un conector similar al SC, pero requiere un giro del conector para su inserción, de modo similar a los conectores coaxiales. También se puede ver como un punto de haces de luces que emiten una cantidad de información muy grande en demasiado tiempo.

La fibra es clasificada de acuerdo con su tipo de fabricación y forma de propagación de los rayos de luz, además de su capacidad de transmisión (el ancho de banda) y su facilidad de acoplar a los equipos activos en las conexiones.

Figura 2.2.6. Imágenes de conectores de fibra óptica.

2.2.1.8.5. FIBRA OPTICA MONOMODO

Una **fibra mono-modo** es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación, su transmisión es en línea recta. Su distancia va desde 2.3 km a 100 km máximo y usa centro con cañón láser de alta intensidad. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias y transmitir elevadas tasas de bit.[15]

La fibra Mono-modo utiliza un sistema más simple. Solo permite un modo de propagación. Un único haz de luz directa y más intensa, y por lo tanto de más ancho de banda con mayores distancias. Es de largo alcance pudiendo recorrer varios kilómetros sin necesidad de repetidores. Normalmente son usadas para unir diferentes localizaciones separadas entre sí y van por galerías de cable por debajo del suelo.

Características:

- **Núcleo**: La mayoría de las fibras ópticas se hacen de arena o sílice, materia prima abundante en comparación con el cobre. Con unos kilogramos de vidrio pueden fabricarse aproximadamente 43 kilómetros de fibra óptica, el núcleo es la parte más interna de la fibra y es la que guía la luz tiene un diámetro aproximado de 8,3 µm.

- **Malla**: Está a su vez rodeado por un forro o funda de plástico u otros materiales que lo resguardan contra la humedad, el aplastamiento, los roedores, y otros riesgos del entorno con un espesor de 125 µm hasta 244 µm.

- **Margen de Error**: El error de **concentridad** oscila entre 0.5 y 0.2 µm.

[15] http://serviojr.blogspot.es/i2007-12/

2.2.1.8.6.FIBRA OPTICA MULTIMODO

ESCALONADO

En este tipo de **fibra óptica** viajan varios **rayos ópticos** simultáneamente. Estos se reflejan con diferentes ángulos sobre las paredes del núcleo, por lo que recorren diferentes distancias (ver gráfico), y se desfasan en su viaje dentro de la fibra, razón por la cual la distancia de transmisión es corta.

Hay que destacar que hay un límite al ángulo de inserción del rayo luminoso dentro de la **fibra óptica**, si este límite se pasa el rayo de luz ya no se reflejará, sino que se refractará y no continuará el curso deseado.[16]

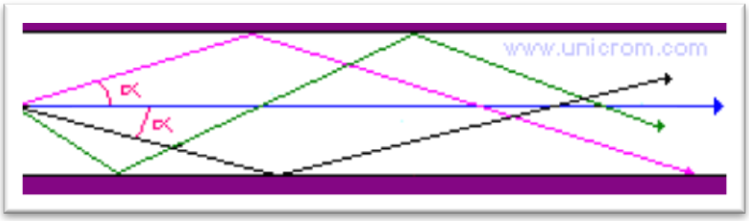


Figura 2.2.7. La imagen muestra como viajan los rayos ópticos reflejados, alcanzando a recorrer diferentes distancias.

GRADUAL

En este tipo de **fibra óptica**, el núcleo está constituido de varias capas concéntricas de material óptico con diferentes índices de refracción, causando que el **rayo de luz** se refracte poco a poco mientras viaja por el núcleo, pareciendo que el rayo se curva como se ve en el siguiente gráfico.

En estas **fibras** el número de **rayos ópticos** diferentes que viajan es menor que en el caso de la **fibra multimodo** índice escalonado y por lo tanto, su distancia de propagación es mayor. Tiene una banda de transmisión de 100 MHz a 1 GHz[17]

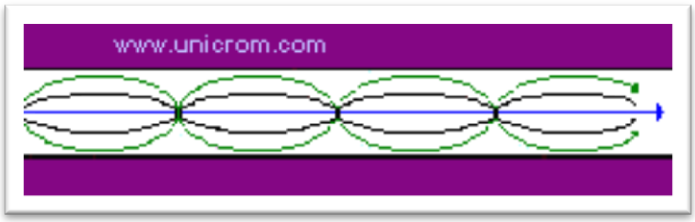


Figura 2.2.8. La imagen muestra los índices de refracción que tiene el rayo de luz viajando por el núcleo.

[16] http://www.unicrom.com/art_FibraOptica.asp
[17] http://www.unicrom.com/art_FibraOptica_multimodo_gradual_transmision_usos.asp

2.2.2 ARQUITECTURA DE LAS REDES "MODELO JERARQUICO"

Las redes de cable, que tiene una topología ramificada, contienen 3 partes:

2.2.2.1 CAPA "CORE" NUCLEO

La capa del núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia. Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

Su labor es multiplexar el ancho de banda disponible entre conexiones existentes, controlar el buen funcionamiento de todas ellas y monitorizar continuamente el estado de la red. Suele constar de varios elementos para captar los distintos tipos de señal que le pueden llegar.[18]

Red troncal: la red troncal ésta formada por anillos de fibra óptica que recorren cierto número de nodos primarios. Dichos nodos ópticos permiten que la información en formas de señales ópticas se transmita entre ellos y, a su vez, están conectados con los secundarios que formarán la siguiente parte de la red. A través de ella, se transportarán las señales generadas por las cabeceras a los puntos que alcanza la distribución de la red de cable.[19]

[18]Jesús García Tomas, José Luis Raya Cabrera, Víctor Rodrigo Raya. Alta de Velocidad y Calidad de Servicio en Redes IP. Pág. 210

[19]Jesús García Tomas, José Luis Raya Cabrera, Víctor Rodrigo Raya. Alta de Velocidad y Calidad de Servicio en Redes IP. Pág. 210

2.2.2.2 CAPA DE DISTRIBUCIÓN

La capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN.

En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

• Servir como punto de concentración para acceder a los dispositivos de capa de acceso.

• Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.

• Segmentar la red en múltiples dominios de difusión / multidifusión.

• Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet

• Proporcionar servicios de seguridad y filtrado.

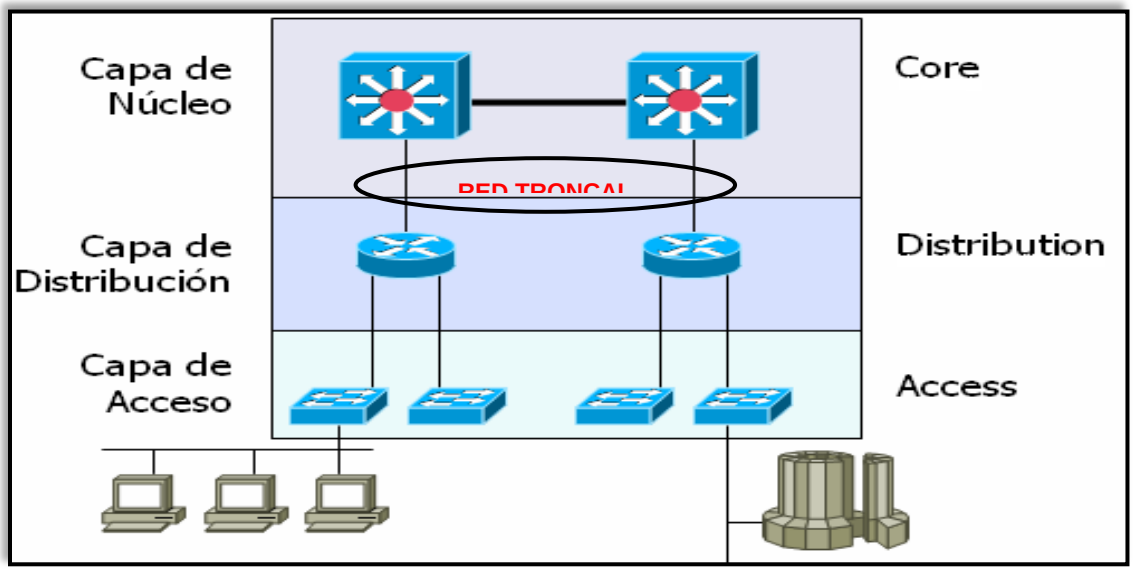
La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquete pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo. La capa de núcleo podrá entonces transportar la petición al servicio apropiado.

Red de distribución: la red de distribución está constituida por un bus de cable coaxial de banda ancha al que se conectan los diferentes usuarios mediante la correspondiente acomedida. En los nodos secundarios, desde los que parte este tipo de cable y que se conectan con los primarios, la señal óptica se convierte en eléctrica. Las conexiones entre ambos tipos de nodos son de tipo punto a punto

esencialmente, aunque se puede utilizar otro tipo de estructuras de interconexión.[20]

2.2.2.3 CAPA DE ACCESO

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo, capa de escritorio o de usuario. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales. En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al Web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.



La figura 2.2.9. Muestra las capas de modelo jerárquico de una red.

[20]Jesús García Tomas, José Luis Raya Cabrera, Víctor Rodrigo Raya. Alta de Velocidad y Calidad de Servicio en Redes IP. Pág. 210

2.2.3 SEGURIDAD EN REDES

Los aspectos de seguridad de la red incluyen proteger los datos contra accesos no autorizados y contra virus.

- **Accesos no autorizados:** para que una red sea útil, los datos sensibles deben de estar protegidos frente accesos no autorizados. La protección puede llevarse a cabo a un cierto número de niveles. En el nivel más bajo están los códigos y contraseñas de identificación de los usuarios. A un nivel más alto se encuentra las técnicas de cifrado. Con estos mecanismos, los datos se alteran de forma sistemática de forma que si son interceptados por un usuario no autorizado sean ininteligibles.

- **Virus:** debido a que la red es accesible desde muchos puntos, puede ser susceptible de sufrir ataques de virus de computadoras. Un virus es un código que se ha introducido en la red ilícitamente y que genera daños en el sistema. Una buena red está protegida ante ataques de virus mediante mecanismos software y hardware diseñados específicamente para ese propósito.[21]

[21]A. Behrouz A. Transmisión de Datos y Redes de Comunicación. Pag. 6

2.2.3.1 ¿PORQUE ES NECESARIA LA SEGURIDAD?

Objetivo: Proteger los servicios de red.

Se debe controlar el acceso a los servicios de red tanto internos como externos.
Se debe garantizar que los usuarios que tengan acceso a las redes y a los servicios de red no comprometan la seguridad de estos servicios, verificando que existen:

a) Interfaces adecuadas entre la red de la Pemex Petroquímica y las redes de otras organizaciones, o redes publicas.
b) Mecanismos de autenticación apropiados para usuarios y equipamiento.
c) Controles de acceso de usuarios a los servicios de información.

La información relevante de la empresa y los equipos de cómputo donde reside dicha información son recursos importantes y vitales para Pemex Petroquímica. La alta dirección de Pemex Petroquímica tiene el deber de preservar dichos recursos por lo que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La Gerencia de Tecnología de Información tiene entre sus funciones el establecer medidas que salvaguarden la información sensible de la empresa y garanticen el acceso seguro a la información, estas medidas están alineadas a los planes estratégicos de la empresa, encaminados a la satisfacción de clientes, apoyando los procesos sustantivos de Comercialización y Producción, así como los de apoyo de Adquisiciones, Recursos Humanos, Finanzas, etc.

La información relevante debe protegerse de acuerdo a su valor e importancia, deben emplearse medidas de seguridad sin importar la forma en que se almacena

la información (en medios electrónicos), o como se procesa (PCs o servidores), o cómo se transmite (correo electrónico, ftp, red de datos, modem, etc.), dicha protección debe incluir restricciones de acceso a los usuarios de acuerdo a las funciones que desempeña.

La seguridad de la información es un tema que comprende a las distintas áreas que integran la organización de Pemex Petroquímica, por lo que es necesario destinar tiempo y recursos para asegurar la protección de los activos de información de la empresa.

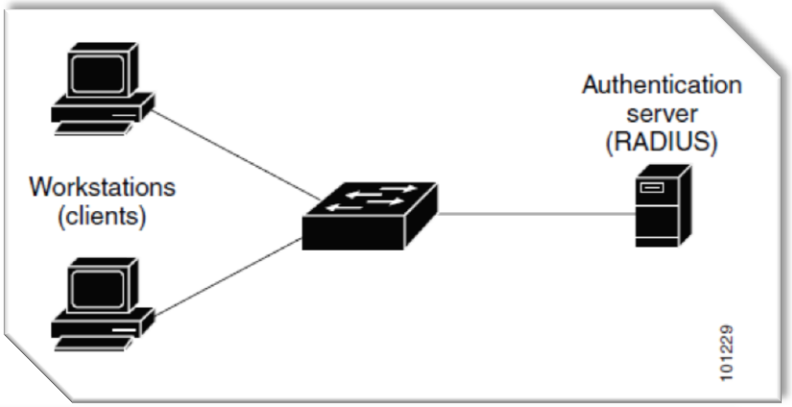
2.2.4. METODOS DE AUTENTIFICACIÓN

2.2.4.1. OPERACION DEL PROTOCOLO 802.1x EAP/EAPOL

El 802.1x se basa en el **protocolo EAP** (*Protocolo de autenticación extensible*), definido por el Internet Enginering Task Force (IETF) (en español Grupo de Trabajo en Ingeniería de Internet). *Este protocolo se usa para transportar la información de identificación del usuario.*

La forma en que opera el protocolo EAP se basa en el uso de un controlador de acceso llamado *autenticador*, que le otorga o deniega a un usuario el acceso a la red. El usuario en este sistema se llama *solicitante*. El controlador de acceso es un firewall básico que actúa como intermediario entre el usuario y el *servidor de autenticación*, y que necesita muy pocos recursos para funcionar. Cuando se trata de una red inalámbrica, el punto de acceso actúa como autenticador.

Figura 2.2.10. La imagen muestra el cliente y el autentificador conectados de manera cableada.



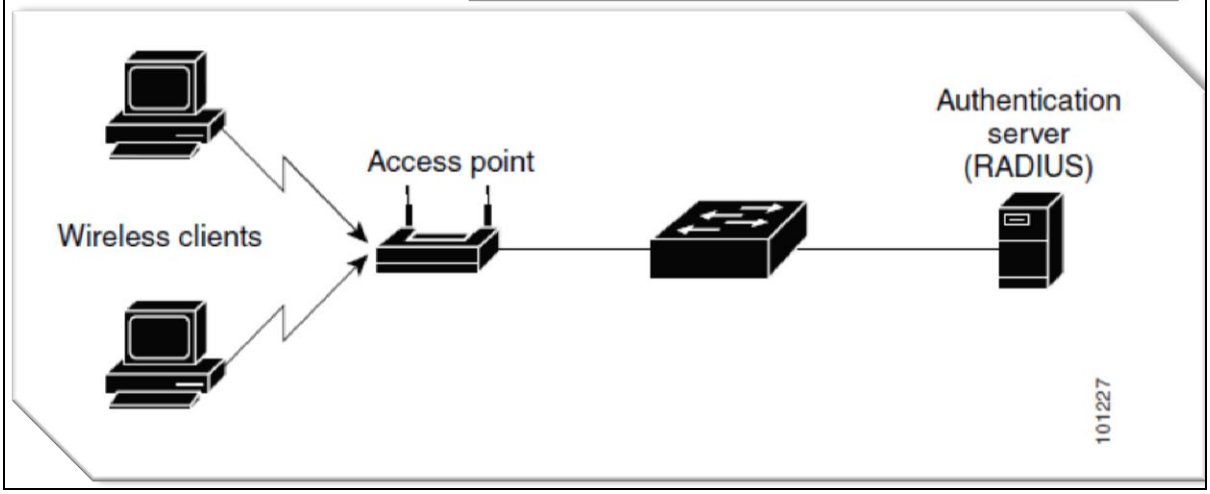


Figura 2.2.10. La imagen muestra el cliente y el autentificador conectados de manera inalámbrica.

El servidor de autenticación (a veces llamado *NAS*, que significa *Servicio de autenticación de red* o *Servicio de acceso a la red*) puede aprobar la identidad del usuario transmitida por el controlador de la red y otorgarle acceso según sus credenciales.

Los pasos que sigue el sistema de autenticación 802.1X son:

- El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
- El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajena al punto de acceso.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- El servidor pude aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.
- Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.
- Luego de que el solicitante ha terminado de ocupar la red, manda un comunicado EAPOL-Logoff que indica que ha terminado de utilizar la red.

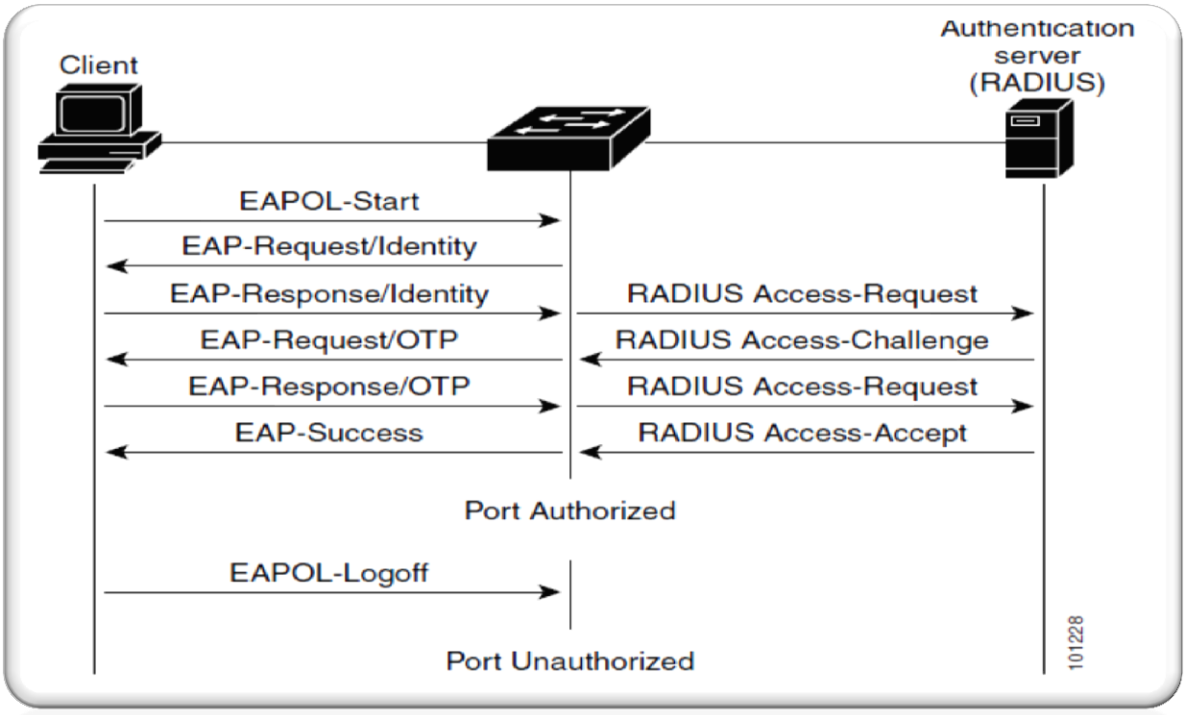


Figura 2.2.11. El cuadro nos representa cómo funciona el método de EAP.

De lo que hemos visto, el protocolo 802.1X tiene un mecanismo de autenticación independiente del sistema de cifrado. Si el servidor de validación 802.1X está configurado adecuadamente, se puede utilizar para gestionar el intercambio dinámico de claves, e incluir la clave de sesión con el mensaje de aceptación. El punto de acceso utiliza las claves de sesión para construir, firmar y cifrar el mensaje de clave EAP que se manda tras el mensaje de aceptación.

El cliente puede utilizar el contenido del mensaje de clave para definir las claves de cifrado aplicables. En los casos prácticos de aplicación del protocolo 802.1X, el cliente puede cambiar automáticamente las claves de cifrado con la frecuencia necesaria para evitar que haya tiempo suficiente como para poder averiguarla.

2.2.4.1.1. Protocolo de Autenticación Extensible (EAP) a través de LAN (EAPOL)

Tipos de paquetes que puede utilizar el EAPOL:

Tipo de Paquete	Nombre	Descripción
0000 0000	EAP-Paquete	Contiene un marco EAP encapsulado (esto es lo que la mayoría de los marcos son EAPoL)
0000 0001	EAPOL-Start	Un suplicante puede emitir un fram-Start EAPOL lugar de esperar a un desafío desde el autenticador
0000 0010	EAPOL-Logoff	Se utiliza para devolver el estado del puerto para no autorizado cuando el suplicante se termine de utilizar la red
0000 0011	EAPOL-Key	Se utiliza para el intercambio de información Introducción de cifrado
0000 0100	EAPOL-encapsulado-ASF-Alerta	Proporcionado como un método que permite Alerta Normas del Foro (ASF) alertas (por ejemplo, SNMP traps específicos) que se transmitirá a través de un puerto que está en el estado no autorizada
		Todos los posibles valores de otros son reservados para uso futuro

2.2.4.2. METODOS EAP

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP podemos citar:

EAP-MD5: MD5 requiere nombre de usuario / contraseña, y es equivalente al protocolo PPP CHAP [RFC1994]. Este método no ofrece resistencia al ataque de diccionario, autenticación mutua, o la derivación de claves, y, por tanto poca utilidad en un entorno de autenticación inalámbrica.

EAP-TLS: Es un sistema de autenticación fuerte basado en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Public Key Infraestructure) en ambos extremos. TLS (transport Layer Security) es el nuevo estándar que sustituye a SSL (Secure Socket Layer).

EAP-TTLS: El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor.

PEAP: El significado de PEAP se corresponde con Protected EAP y consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos.

EAP (LEAP): Un nombre de usuario y una contraseña se envía a un servidor de autenticación (RADIUS) para la autenticación. Salto es un protocolo propietario desarrollado por Cisco, y no se considera seguro. Cisco LEAP es la eliminación gradual en favor de PEAP.

.

EAP-MSCHAPv2: Requiere nombre de usuario / contraseña, y básicamente es una encapsulación EAP de MS-CHAP-v2 [RFC2759]. Por lo general utilizados en

el interior de un túnel cifrado PEAP. Desarrollado por Microsoft, y actualmente es un proyecto de IETF (Internet Engineering Task Force).

2.2.4.3. FUNCIONALIDAD DE AAA

Servicios de Seguridad AAA

El control de acceso es la forma en que se controla quien debe accesar a los equipos y a que servicios tiene permitidos una vez que acceso. La seguridad AAA provee el primer marco a través del cual se puede configurar el control de acceso a los equipos.

AAA provee una forma modular para realizar las siguientes funciones:

- Authentication (Autenticación):La Autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (vg. un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla.[22]Provee un método para identificar usuarios, incluyendo solicitud de cuenta y clave, respuesta, soporte de mensajería, y dependiendo del protocolo que se seleccione, encriptación. La autenticación es la manera como un usuario se identifica antes de darle el acceso a la red o dispositivos. Se configura la autenticación AAA mediante la definición de listas de métodos de autenticación EAP, y después se aplican estas listas a diversas interfaces. Mediante la lista de método se define los tipos de autenticación que se realizaran y la secuencia en la cual deberán ser ejecutadas. Todos los métodos de autenticación, excepto el local, line password y enable, deberán ser definidos a través de AAA.

[22]http://es.wikipedia.org/wiki/Protocolo_AAA

- Authorization (Autorización):Se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. La autorización provee un método para el control de accesos remotos, incluyendo autorización única (one-time authorization) o autorización por cada servicio, perfil y lista por usuario, soporte de grupo de usuarios y soporte de IP, IPX, ARA y Telnet. Autorización AAA trabaja conjuntando una serie de atributos que describen lo que el usuario puede hacer. Estos atributos son comparados con la información contenida en la base de datos de usuarios y los resultados se regresan a AAA para determinar las capacidades y restricciones actuales del usuario. La base de datos puede estar ubicada de manera local en el equipo de red o puede residir remotamente en un servidor RADIUS o TACACS+. Estos servidores autorizan a usuarios permisos específicos asociando a un atributo, el cual define los derechos del usuario. Todos los métodos se definen a través de AAA.

- Accounting (Contabilidad o Administración): La Contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios. Provee el método para colectar y enviar información del servidor de seguridad, para el costeo, auditoria y reportede los usuarios, tomando el tiempos de inicio y fin, comandos ejecutados, número de paquetes y numero de bytes enviados y recibidos. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos. La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes (en inglés *"batch*

*accounting")*consiste en la grabación de los datos de consumo para su entrega en algún momento posterior. La información típica que un proceso de contabilización registra, es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó. [23]

Aunque AAA es el primer método para el control de acceso, IOS de Cisco provee funciones adicionales para el control de acceso que están fuera del alcance de AAA, tal como, usuarios locales, autenticación, autenticación de claves de líneas, claves de autenticación de modo privilegiado (enable).

Beneficios de la implementación de AAA

- Incrementar la flexibilidad y control de la configuración de acceso.
- Escalabilidad
- Estandarización de métodos de autenticación, tales como, RADIUS, TACACS+ y Kerveros.
- Múltiples sistemas de respaldo.
- Requisito indispensable para el protocolo 802.1x en la red.

[23]http://es.wikipedia.org/wiki/Protocolo_AAA

2.2.5. INTEGRACION DE NAP Y NAC

2.2.5.1. NAP (Network Access Protection)

Una de las tareas más demandantes para los administradores de sistemas es asegurar que cualquier dispositivo que se conecte a la red corporativa en cualquiera de sus formas (PDA, Notebook, Smartphone, Workstation, Server, Virtual Server) y a través de cualquier medio de acceso (Internet, VPN, Extranet, Wireless, Wired, Dial-Up) cumplan con el modelo de seguridad definido para la organización.[24]

Network Access Protection (NAP) es una tecnología de Microsoft para acceso a la red de control de un equipo host basado en el sistema de salud del huésped.

Con Network Access Protection, los administradores del sistema de red informática de una organización pueden definir las políticas para los requisitos del sistema de salud. Cabe destacar que la solución de NAP no está diseñada para asegurar la red de usuarios maliciosos, si no que está diseñada para ayudar a los administradores de sistemas a mantener la higiene de los dispositivos con SO Microsoft NAP "conformidad" dentro de la red, que tiene como resultado mantener la integridad general de la red.

NAP provee "conformidad" sobre las siguientes tecnologías:

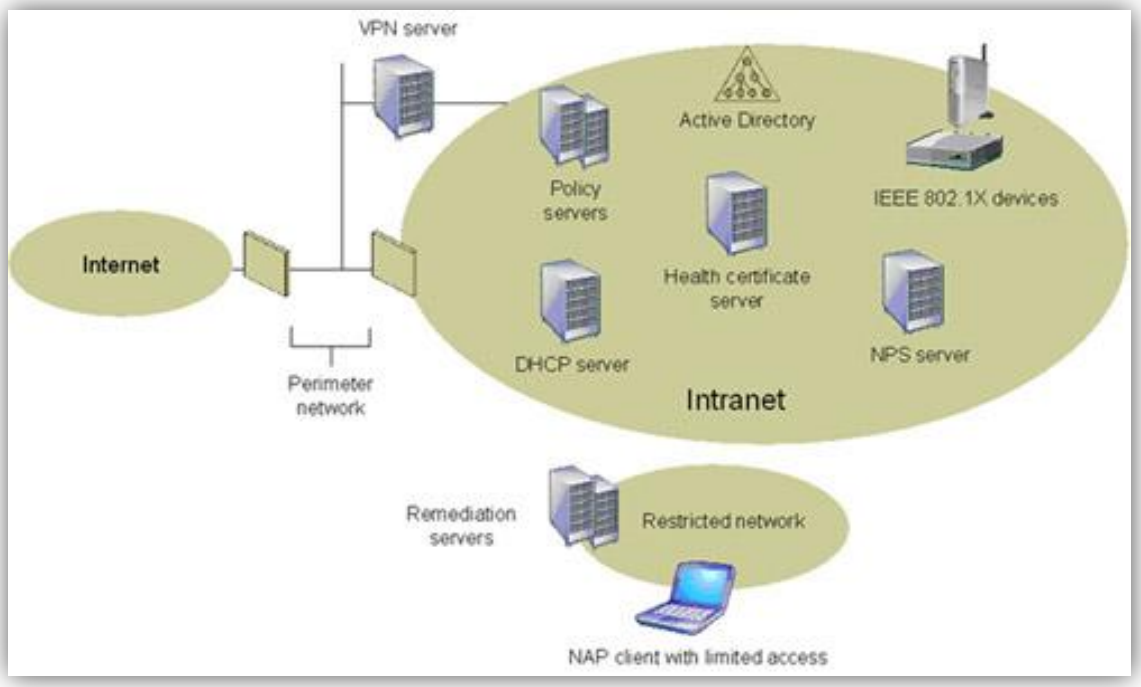
- IPSec (Internet Protocol Security).
- IEEE 802.1x Authenticated Network Connections
- VPNs (Virtual Private Networks)
- Dynamic Host Configuration Protocol (DHCP)

Estas tecnologías pueden ser utilizadas en forma conjunta o independiente en función del modelo de seguridad y la infraestructura a utilizar, el refuerzo de las políticas en estas tecnologías se realiza a través de un NPS (Network Policy Server).

[24] http://www.microsoft.com/latam/technet/articulos/tn/2007/abr-17.mspx

Para la implementación de NAP es necesario montar toda una infraestructura que soporte el framework de control de acceso, esta infraestructura cuenta con:

- Active Directory
- Policy Servers (Network Policy Server). DHCP Servers
- Dispositivos compatibles con IEEE 802.1x
- Health Certificate Servers (Windows Server Longhorn + IIS (Internet Information Server) + CA (Certificate Authority).
- VPN Servers.
- System Health Agent (Windows XP + SP2, Windows Server 2003, Windows Server Longhorn + NAP Agent).
- NAP Administration Server (Network Policy Server)
- System Health Validator (Network Policy Server)
- Health Policy (Network Policy Server).
- Accounts Database (Active Directory)
- Remediation Server (WSUS, SMS, Antivirus/Antimalware Server, DNS Server).



En la siguiente figura 2.2.12 se ve un modelo de ejemplo de alto nivel de Network Access Protection.

2.2.5.1.1. CLIENTE NAP

Clientes del NAP son los equipos que informe sobre la salud del sistema a un punto de cumplimiento NAP. Un punto de cumplimiento NAP es una computadora o dispositivo de red de acceso que puede requerir la evaluación del estado de salud de un cliente NAP y, opcionalmente, acceso restringido de la red o la comunicación.

La salud del NAP Policy Server es un equipo que ejecuta la Red Policy Server (NPS) de servicio que almacena requisito de las políticas de salud y provee evaluación de la salud para los clientes del NAP. Las políticas de servicio de salud son configurados por el administrador y puede incluir los ajustes que requieren las computadoras del solicitante (Ej.: Firewall activado, Actualizaciones del SO, Software de Antivirus/Antimalware) antes de que estos tengan acceso a la red corporativa.

Cuando un cliente contacta con capacidad NAPequipo de un punto de cumplimiento NAP, a su juicio su estado de salud actual. El punto de cumplimiento NAP envía NAPde clientes de salud del estado del servidor a la política de salud para la evaluación del NAPcon el protocolo del RADIUS. La salud del NAPPolicy Server también puede actuar como un servidor de autenticación basada en RADIUS para el cliente NAP.

La salud del NAPPolicy Server puede utilizar un servidor requisito de salud para validar el estado de salud del cliente NAP o para determinar la versión actual del software o actualizaciones que deben instalarse en el cliente NAP. Por ejemplo, un servidor de requisito de salud podría ser la última actualización del antivirus.

Si el punto de cumplimiento NAP es una HRA, obtiene los certificados sanitarios de una entidad emisora de certificados para los clientes NAP que están decididos a cumplir con los requisitos de salud.

El cliente NAP determina si no cumplen con los requisitos de salud, opcionalmente se pueden colocar en una red restringida o de cuarentena. La red restringida es un subconjunto lógico de la intranet y contiene los recursos que permiten a un cliente NAP cuando no cumplen las normas, para corregir su sistema de salud. Los servidores que contienen los componentes del sistema de salud o cambios se conocen como servidores de remediación. Un cliente NAP que no cumplen las normas, en la red de restringidos puede acceder a los servidores de remediación e instalar los componentes necesarios y actualizaciones. Después de que la rehabilitación es completada, el cliente NAP puede realizar una nueva evaluación de la salud en relación con una nueva solicitud de acceso a la red corporativa.

2.2.5.2. NAC (Network Access Control)

Son un conjunto de tecnologías desarrolladas por Cisco Systems, utiliza la infraestructura de red para forzar las políticas de seguridad definidas en el modelo de seguridad de una organización en todos los dispositivos conectados a esta.

Su objetivo es hacer cumplir la organización de seguridad de redes políticas en todos los dispositivos que buscan acceso a la red. Cisco Network Admission Control (NAC) sólo permite que conforme y de confianza dispositivos de punto final, tales como PCs, servidores y PDA, en la red, restringiendo el acceso de dispositivos no compatibles, y por lo tanto limitar el daño potencial de amenazas a la seguridad y riesgos emergentes. NAC de Cisco evita la pérdida de información confidencial por lo cualofrece a las organizaciones un método de gran alcance, basado en los roles de prevenir el acceso no autorizado y mejorar la capacidad de la red.[25]

Cisco NAC cubre los activos administrados y no administrados, se ocupa de los empleados y los dispositivos que no son empleados, y ayuda agarantizar el

[25] http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

cumplimiento de las telefonías fijas e inalámbricas conectadas,criterios de valoración, acceso VPN, y los usuarios invitados.Con los escenarios de implementación flexibles, Cisco NACayuda a asegurar que los equipos terminales conectados se ajusten asu política de seguridad.

Microsoft y Cisco han trabajado conjuntamente para garantizar la interoperabilidad en estas dos tecnologías (NAC Y NAP), como resultado de este trabajo conjunto se obtiene:

- Interoperabilidad y elección del cliente.
- Protección de la inversión.
- agente único incluido en Microsoft Windows Vista.
- proveedor de software independiente (ISV) de integración de ecosistemas.
- agente de implementación y soporte técnico de actualizaciones.
- Compatibilidad entre plataformas.[26]

2.2.5.3. INTEGRACIÓN

El NAC de Cisco y soluciones de Microsoft NAP en conjunto proporcionan la capacidad para reunir la identidad y el estado de salud- información de un punto final, determinar el cumplimiento de las políticas de seguridad del punto final, proporcionar rehabilitación de servicios, y hacer cumplir políticas de acceso a redes basado en el cumplimiento del punto final.

Con la integración de estas dos soluciones, un administrador puede verificar el estado de salud de un cliente de Microsoft Vista, proporcionar capacidades de recuperación, y proporcionar la aplicación de políticas dinámicas en la infraestructura de red.

[26] http://www.microsoft.com/latam/technet/articulos/tn/2007/abr-17.mspx

2.2.5.4. ARQUITECTURA

El NAC y la arquitectura de interoperabilidad del NAP consisten enlos siguientes componentes:

• Cliente NAP (Microsoft): El equipo cliente NAP es un equipo que ejecuta Windows Vista o Windows Server, queenvía sus credenciales de salud ya sea como una lista de declaraciones de Salud (SoHs) o un certificado de salud.

La arquitectura cliente consiste en una capa de Agentes del Sistema de la Salud (SHAS), el Agente del NAP, laEAPHost NAP Aplicación cliente, EAP métodos para realizarcuenta de autenticación de credenciales y la indicación del estado de salud,EAP y suplicantes que permiten que el cliente envíe mensajes EAPsobre 802.1X o UDP.

Para obtener un certificado de salud actual, el cliente NAP utiliza el Protocolo de inscripción de Certificado de Salud (Perfil Ambiental de Honduras)para enviar una solicitud de certificado y su lista de declaraciones de Salud a laAutoridad de Registro de la Salud (HRA).

• Dispositivos de acceso de red (Cisco): NAC dispositivos habilitados para la red de acceso(Que incluyen switches, routers, puntos de acceso inalámbricos, VPNconcentradores, etc) proporcionar acceso a la red a los clientes ysirven como puntos de aplicación de red.

• Control de acceso Server (ACS) (Cisco): Cisco Secure ACS autoriza red de acceso para los clientes mediante la validación de la vía administrativaatributos especificados cliente, que podría incluir la identidad de lausuario y / o el ordenador, y el estado general de salud delcliente. Cisco Secure ACS envía un perfil de acceso a la reddispositivo de acceso (s), a conceder el nivel apropiado de acceso a la redel cliente basado en el resultado de

autorización. Tenga en cuenta que la validación del cliente de los atributos de salud del estado y la asignación del total de clientesestado de salud en la arquitectura de interoperabilidad esrealizada porla red de Microsoft Servidor de Políticas.

• Red de Policy Server (NPS) (Microsoft):Un NPS Microsoft realiza la validación de losequipo de salud del sistema y proporciona rehabilitacióninstrucciones si es necesario.

• Autoridad de Registro de la Salud (HRA) (Microsoft):Una HRA obtiene certificados de salud en nombrede los clientes NAP de una infraestructura de clave pública(PKI).

• Política de servidores (de Microsoft o de terceros):Los servidores que ofrecen el estado actual del sistema de saludNPSs de Microsoft. Política de integración con servidoresMicrosoft NPSs a través del Sistema de Salud de fuentes de energía nuclearValidator (SHV) API.Para adaptarse a esta arquitectura de interoperabilidad,el NAP y las plataformas NAC apoyará el texto siguiente:

• Cisco Secure ACS hará llegar la lista de SoHsdel agente del NAP a un total de clientes de fuentes de energía nuclearla salud de validación.

• Microsoft NPS prestará apoyo a la acogida de CiscoAutorización de Verificación de Poderes Protocolo (HCAP) pararecibirá la lista de SoHs de Cisco Secure ACSy devolver la lista de las respuestas SoH (SoHRs).

• Realizará acceso a la redvalidación basada en un certificado sanitario.

2.2.5.5. ¿Cómo trabaja la arquitectura de interoperabilidad NAC-NAP?

Al conectarse a la red, el cliente proporciona un conjunto de credenciales que se validan para autenticar y autorizar el nivel apropiado de acceso a la red. Estas

credenciales cliente puede incluirusuario y / o credenciales de equipo, además de la identidad de las credenciales de salud. Los clientes que no cumplen las normas se pueden ser puestos en cuarentena, de saneamiento, o tratados de manera similar antes de ser concedido el acceso normal de la red. [27]

A alto nivel la integración que tienen estas dos plataformas funciona de la siguiente manera:

1- Al momento de realizar una conexión con la red, los clientes presentaran un set de credenciales (usuarios o identidad de computadoras) las cuales luego de ser validadas definirán cual es el nivel apropiado de acceso que tendrán dentro de la red.

2- Los clientes “non-compliance (no-conformidad)” serán ubicados en una red de cuarentena para ser provistos de los componentes que les permitirán ser “conformidad” y acceder a la red en forman normal.

3- Los clientes que utilicen el agente NAP proveen credenciales (usuarios o identidad de computadoras), esto conjuntamente con una lista de SoHs (Estado de las respuestas de Salud) los cuales son enviados a un Cisco Secure ACS con EAP-FAST sobre 802.1x o EAPoverUDP.

4- Cisco Secure ACS enviara la lista de SoHs a un Microsoft NPS (Network Policy Server) para validar al cliente.

5- El servidor de Microsoft NPS evaluara la SoHRs (Estado de las respuestas de Salud) en función del modelo de seguridad definido y devolverá el HVS (Estado de Validación de Salud) al Cisco Secure ACS.

27 http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns617/net_implementation_white_paper0900aecd8051fc24.pdf

6- Cisco Secure ACS va a evaluar el resultado de todas las validaciones realizadas para enviar el perfil de acceso correspondiente al dispositivo de acceso para permitir el acceso del cliente a la red corporativa.

7- Todos aquellos clientes “no-conformidad” que fueron puestos en el segmento de cuarentena, van a ser re-validados posteriormente a la provisión de los requerimientos faltantes para garantizar el acceso a la red dentro del modelo de seguridad definido.[28]

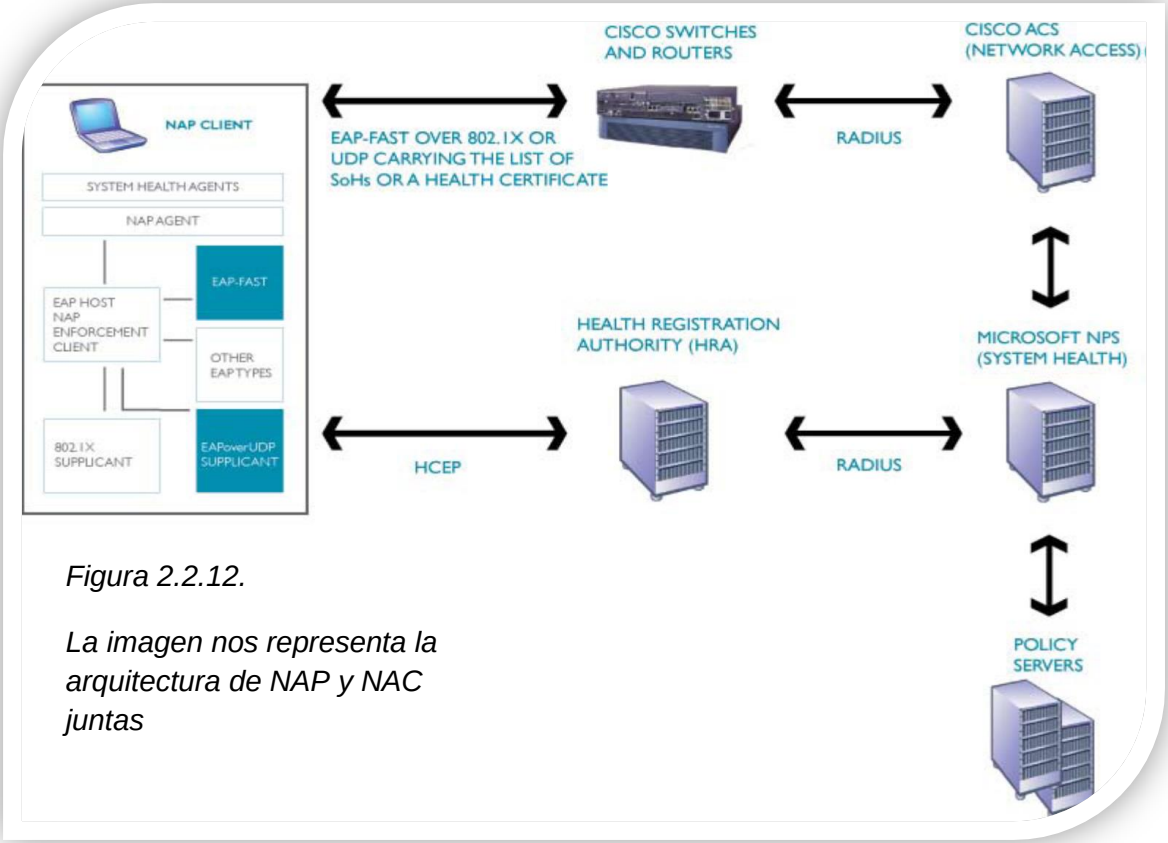


Figura 2.2.12.

La imagen nos representa la arquitectura de NAP y NAC juntas

[28] http://www.microsoft.com/latam/technet/articulos/tn/2007/abr-17.mspx

IMPLEMENTACIÓN DEL PROTOCOLO

2.3 IMPLEMENTACIÓN

2.3.1. DIAGRAMA DE OPERACIÓN

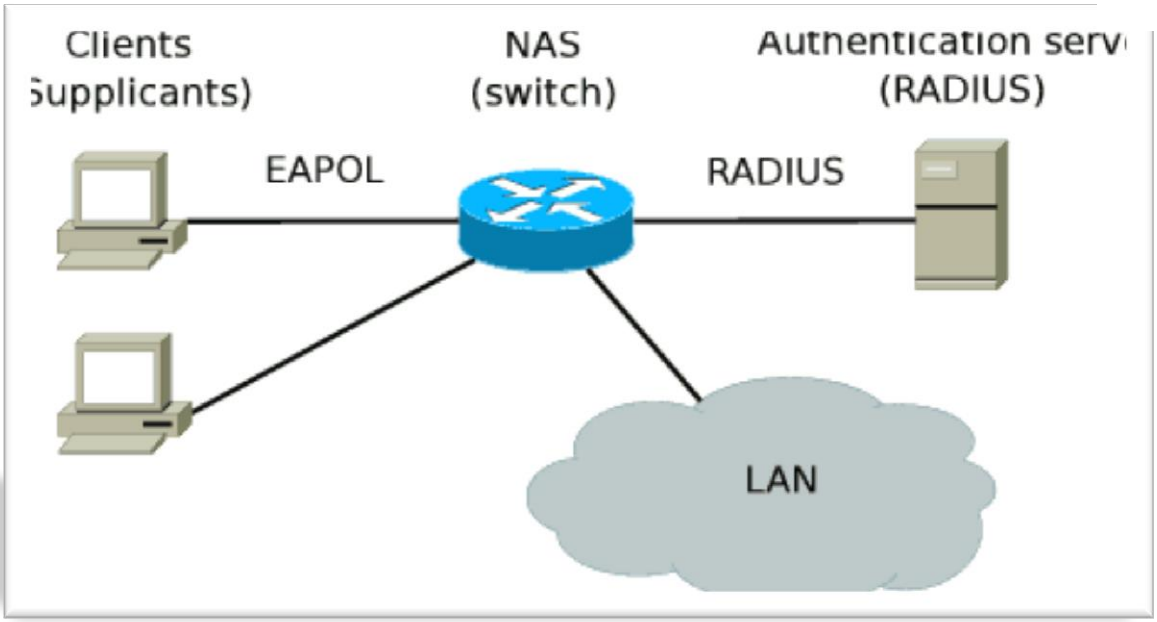


Figura 2.3.1 Muestra un esquema de cómo se estructura el protocolo 802.1x

2.3.2. CONFIGURACION DE 802.1X

2.3.2.1. CLIENTE

a) Configurar switch para meterlo a la LAN

Proceso de login:

1. El usuario inicia una conexión para el router.
2. El router y RADIUS emiten un “Access-request” para el servidor.
3. El servidor checa los usuarios contra la base de datos de autentificación y emite un “Access-reject”, “Access-challenge” o “Access-accept” con los privilegios apropiados.
4. El router concede acceso al usuario con los privilegios apropiados.
5. El router puede enviar al servidor RADIUS daos de contabilidad cuando los usuarios estén fuera.

- Se configura el switch en cero para introducirle los comandos del protocolo 802.1x, con el cual hará el acceso de remutación con el servidor de autenticación (RADIUS).
- Se habilita la AAA.
- Se configuran los mensajes de la línea de comando.
- Se crea la lista de métodos para la autentificación de usuario y usuario privilegiado.
- Se crea la lista de método para 802.1x.
- Se da la interface del RADIUS.
- Se da la IP del RADIUS, el puerto de autentificación y el puerto de acción junto con la llave del RADIUS.

b) Probar la conexión en switch

Una vez introducidos estos comandos en el director activo, se verifica que haya conexión, de un usuario con privilegios hacia el switch y que el switch tenga comunicación con el RADIUS, en el que nos tiene que dar una dirección de IP con el que podremos tener acceso a internet. Una vez que tengamos la dirección IP se comprueba realmente que hay conexión.

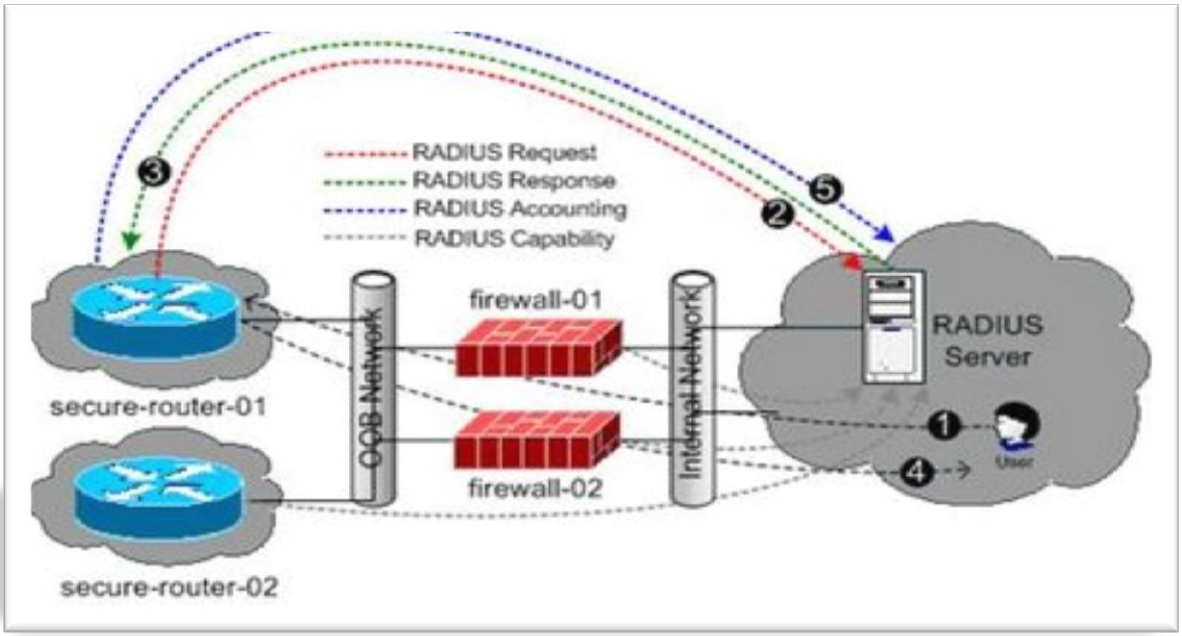


Figura 2.3.2 Muestra todos los pasos del cómo se ejecuta el protocolo.

2.3.2.2. SERVIDOR RADIUS

a) Dar de alta al RADIUS

- Se debe tener instalado el software del RADUIS.
- Se le pondrá un nombre cualquier para identificarlo.
- Se introducirá la dirección IP del RADIUS.
- Y se le pone una “Shared secret” que deseemos y se repetirá nuevamente.

2.3.2.3. REGLAS DE AUTENTICACIÓN (POLITICAS IAS PARA EL ACCESO A LA RED CABLEADA).

- Una de las condiciones de la política es que debe de agregar *NAS-Port-Type matches “Ethernet” y Windows-Groups matches “AD\Domain Computers”* y *Authentication-Type matches “EAP”.*
- Dentro de estas mismas reglas de autentificación se configura el método de *EAP (EAP Methods).*
- Se oprime el botón de *Edit Profile* para configurarlo.
- Nos ubicamos en la pestaña de *Autentication,* donde encontramos el botón de *EAP Methods*.
- El método debe ser de tipo *Protected* EAP *[PEAP].Ok.*
- Las casillasque deben de estar marcadas debajo del botón de *EAP Methods* son: Microsoft Encrypted Authentication versión 2 [MS-CHAP v2], *User can change password after it has expired, Microsoft Encrypted Authentication [MS-CHAP] y User can change password after it has expired.* Las demas casillas deben de estar desmarcadas.
- Una vez realizado esto, se oprime el botón de Apply y luego el de OK.
- Debe de estar activada la casilla de Gran permiso de acceso remoto (*Grant remote access permission*).

2.3.2.4. REGLAS DE AUTENTICACIÓN (POLITICA PARA EL USUARIO).

- Una de las condiciones de la política es que debe de agregar *NAS-Port-Typematches "Ethernet" y Windows-Groupsmatches "AD\DomainComputers".*
- Dentro de estas mismas reglas de autentificación se configura el método de *EAP (EAP Methods).*
- Se oprime el botón de *Edit Profile* para configurarlo.
- Nos ubicamos en la pestaña de *Autentication,* donde encontramos el botón de *EAP Methods*.
- El método debe ser de tipo *Protected* EAP *[PEAP].Ok.*
- Las casillas que se encuentran debajo del botón de *EAP Methods* deben de estar desmarcadas todas.
- Una vez realizado esto, se oprime el botón de Apply y luego el de OK.
- Debe de estar activada la casilla de Gran permiso de acceso remoto (*Grant remote access permission*).

2.3.2.5. 802.1x EN LA PC DEL USUARIO.

- Para configurar el 802.1x en la PC del usuario se debe ir a *Inicio-Equipo-clic derecho-administrar*.
- Una vez que estemos en la ventana de "*Administrar equipos*" buscamos los servicios y aplicaciones-servicios
- Nos muestra una gran cantidades servicios de la computadora, buscamos el servicio de "*Configuración automática de redes cableada*s"- clic derecho-propiedades.
- Nos va a salir una ventana en la cual solo configuramos la parte de "*Tipo de inicio*"lo cambiamos por automático, aceptar.
- Ya realizado esto, nos vamos al *"Estado de conexión de área local-propiedades-autenticación"* dentro de la pestaña de autenticación se marca la casilla de "*Habilitar autenticación de IEEE 802.1x"* y se elige el método de autentificación de red el cual debe ser "*EAP protegido [PEAP]*", lo demás queda igual sin configurar nada.

MARCO CONCEPTUAL

2.4. MARCO CONCEPTUAL

Para llevar adelante un proyecto de investigación, es necesario tener la claridad en los objetivos del mismo, la base de pensamiento sobre lo que hacemos y lo ello significa, con la influencia de otras ideas e investigaciones, así como en el conjunto de conceptos eideasy métodos o prácticasque son indispensables para llevarlo adelantede tal manera que sean fáciles de comunicar a los demás.

2.4.1. CONCEPTUALIZACIÓN

Implementación del Protocolo IEEE 802.1x

Es la realización o la ejecución de un conjunto de estándares que controlan las normas del protocolo estándar IEEE 802.1x para el control de acceso a la red basada en puertos físicos.

Preservar la Seguridad a la red cableada.

Es conservar, resguardar,asegurar y proteger los recursos de la organización de los usuarios "invitados" que se conectan a la red, que está conformada por medio de cable ethernet, permitiendo solo a las personas que se encuentren acreditadas y autorizadas.

2.4.2. OPERACIONALIZACIÓN

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENCIONES	INDICADORES	ITEMS	ESCALA DE LIKERT
Implementación del protocolo 802.1x	Es la realización o la ejecución de un conjunto de estándares que controlan las normas del protocolo estándar IEEE 802.1x para el control de acceso a la red basada en puertos físicos.	Es la realización de un conjunto de reglas que se llevan a cabo para hacer cumplir la seguridad en los puertos físicos con el protocolo 802.1x	Cumplimiento y eficacia de los protocolos de seguridad en red	1.- ¿los usuarios que ingresen como invitados, solo podrán tener acceso internet? 2.- ¿los protocolos de seguridad en red que se aplican son especialmente para las el buen funcionamiento de las IP? 3.- ¿Con la implementación del protocolo 802.1x, es más eficiente la seguridad dentro de la empresa? 4.- ¿se tienen beneficios ventajosos en la empresa con la eficiencia del protocolo?	(a)Muy de acuerdo (b) De acuerdo (c) Ni de acuerdo, ni en desacuerdo (d) En desacuerdo (e) Muy en desacuerdo

				5.- ¿los riesgos de seguridad de la empresa son menos vulnerables aplicando el protocolo? 6.- ¿las reglas de acceso alcanzan ciertos niveles de seguridad en la red, permitiendo acceso a lugares específicos?	

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENCIONES	INDICADORES	ITEMS	ESCALA DE LIKERT
Preservar la Seguridad a la red cableada.	Es conservar, resguardar, asegurar y proteger los recursos de la organización, de los usuarios "invitados"	Es asegurar los servicios que brinda la red de la empresa a los usuarios invitados que se conectan a ella por medio de cable ethernet.	Métodos de autentificación EAP	1.- ¿el servidor de autentificación es que el que prueba la identidad del solicitante y sus credenciales, para poder dar acceso a la red?	(a)Muy de acuerdo (b) De acuerdo (c) Ni de acuerdo, ni en desacuerdo

	que se conectan a la red, que está conformada por medio de cable ethernet, permitiendo solo a las personas que se encuentren acreditadas y autorizadas.			2.- ¿si algunos de los tipos de métodos de autentificación EAP llega a fallar, protocolo 802.1x sigue funcionando normalmente?	(d) En desacuerdo (e) Muy en desacuerdo
			Servicios de seguridad AAA (authentication, authorization, and accounting)	3.- ¿Aplicando el método de autentificación, autorización y contabilidad (AAA) se tiene una gran restricción a usuarios? 4.- ¿dentro de la autentificación de la AAA se va a identifica	(a)Muy de acuerdo (b) De acuerdo (c) Ni de acuerdo, ni en desacuerdo (d) En desacuerdo (e) Muy en desacuerdo

				cada usuario antes de darle acceso a la red? 5.- ¿los mensajes de contabilidad que se reciben, podrían perderse por malas condiciones de la red?	
			NAP (Network Access Protection) ycliente NAP	6.- ¿con la tecnología NAP se tiene una buena salud dentro de la empresa, detectando el estado de salud del que solicita el acceso? 7.- ¿el cliente NAP requiere que las computadoras del solicitante de acceso tengan ajustes como firewall activo, actualizaciones recientes, antivirus/antimalware	(a)Muy de acuerdo (b) De acuerdo (c) Ni de acuerdo, ni en desacuerdo (d) En desacuerdo (e) Muy en desacuerdo

				activo, etc. antes de que tengan acceso a la red corporativa? 8.- ¿si el solicitante no pasa la evaluación de salud NAP, es mandado a un área restringida del cual los servidores de remediación instalan los componentes y actualizaciones necesarias? 9.- ¿la remediación de apoyo deja un espacio de reparación de los equipos cliente para lograr el cumplimiento de las políticas?	
			NAC (Network Access Control)	10.- ¿Cisco NACayuda a asegurar que los equipos terminales conectados se ajusten	(a)Muy de acuerdo (b) De acuerdo

				asu política de seguridad? 11.- ¿NAC de Cisco evita la pérdida de información confidencial?	(c) Ni de acuerdo, ni en desacuerdo (d) En desacuerdo (e) Muy en desacuerdo

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 ENFOQUE DE METODOLÓGICO

La metodología del tema es un conjunto de tácticas, pasos o procedimientos empleados a seguir por una disciplina con el fin de alcanzar la profundidad de los conocimientos validos y demostrarlos rigurosamente mediante el uso de instrumentos confiables. Esta metodología utilizada en la recolección de datos esta en acorde con el enfoque teórico conceptual que se ha desarrollado en el resto del estudio.

En este tema que se habla de aplicación del protocolo estándar el método de investigación que se aplicara será cuantitativo (habrá resultado que se puedan medir).

3.2 TIPO DE ESTUDIO

El tipo de estudio será de tipo exploratorio.Ya que los estudios de este estándar son muy pocos conocidos y escasamente estudiados por la sociedad, es un fenómeno para muchos no tan novedoso, es el punto de partida para estudios posteriores de mayor profundidad.

Además la investigación tiene el propósito de responder las causas, motivos, condiciones y soluciones de la implementación del estándar, así también se explicara cómo se desarrollara paso a paso el estándar y la programación de cada objeto utilizado en la implementación.

3.3 POBLACIÓN

Se denomina población al mundo ideal, teórico cuyas características se quieren conocer y estudiar, es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado.

La población que se tomara como estudio en la elaboración del protocolo, son los individuosdel edificio de PPQ (Pemex Petroquímica) en la ciudad de Coatzacoalcos, Ver.

3.4 MUESTRA

Es un subconjunto fielmente extraído de la población mediante técnicas de muestreo cuyo objetivo sirve para inferir características de toda la población de la que fue extraída, lo cual nos indica que es representativa. Por lo tanto, la validez de la generalización depende de la validez y tamaño de la muestra.

La muestra en este caso será el departamento de Redes, será una muestra de tipo No Probabilístico.

3.5 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Consiste en obtener información de los sujetos en estudio, proporcionados por ellos mismos, sobre opiniones, conocimientos, actitudes o sugerencias, seleccionando un método de medición y aplicarlo para luego analizar las mediciones obtenidas. La encuesta será utilizada para la recolección de datos en este tipo de investigación, ya que es un método fácil de entender y muy claro con sus preguntas cerradas y además convenientes para la recopilación de datos sobre una parte de la población denominada muestra,es una técnica de las más utilizadas frecuentemente para recolectar información de una muestra de individuos con características comunes, todos bajo un estudio.

3.6. APLICACIÓN DE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS.

“Una vez ordenada, tabulada y elaborada la información recogida, se hace necesaria su presentación en forma sistemática”.

En este apartado se describirá la aplicación del instrumento que se utilizo para la recolección de datos, el cual es la encuesta. La encuesta será aplicada al personal de Pemex Petroquímica al término de la elaboración de este proyecto cuando el protocolo este funcionando completamente.

Sera aplicado de forma que sea clara y comprensible la cuesta para que el personal no tenga problemáticas en responder a las preguntas.

3.7. ANÁLISIS DE DATOS

"Analizar significa establecer categorías, ordenar, manipular y resumir los datos". En esta etapa del proceso de investigación se determina como analizar los datos y que herramientas de análisis estadístico son utilizadas para este tipo de investigación, luegose procede a racionalizar los datos recolectados a fin de explicar e interpretar las posibles relaciones que expresan las variables estudiadas y responder a las distintas cuestiones planteadas de la investigación.

Los datos recogidos con el método de investigación que es la encuesta se trataran de manera que se pueda realizar un estudio de lo que opinan los individuos del edificio PPQ acerca del protocolo estándar IEEE 802.1x, representándolo por medio de una grafica utilizando una aplicación de la paquetería de Office, donde se ilustre que tanto porcentaje de la muestra de nuestra población es beneficioso para ellos y para la empresa.

En relación con la encuesta no es ver que dicen los datos, sino que dicen en relación con el problema y la hipótesis que se planteo previamente. La codificación de las respuestas que se obtengan serán legibles y congruentes para que sea más precisa y clara la presentación de la información.

CAPITULO IV:

ANÁLISIS E INTERPRETACIÓN DE LA INFORMACIÓN

4.1 CUADROS

1.- ¿Los usuarios que ingresen como invitados, solo podrán tener acceso internet?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	2
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*En este cuadro podemos observar que más de la mitad están de acuerdo con forme a la pregunta realizada en la encuesta.*

2.- ¿Los protocolos de seguridad en red que se aplican son especialmente para el buen funcionamiento de las IP?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	1
(b) De acuerdo	4
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*Este cuadro nos muestra que la mayoría de las respuestas están de acuerdo con los protocolos de seguridad implementados*.

3.- ¿Con la implementación del protocolo 802.1x, es más eficiente la seguridad dentro de la empresa?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	2
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*las respuestas de esta pregunta nos da un resultado de que 3 están de acuerdo y 2 muy de acuerdo con la implementación del protocolo dentro de la empresa.*

4.- ¿Se tienen beneficios ventajosos en la empresa con la eficiencia del protocolo?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	0
(b) De acuerdo	5
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*las respuestas a esta pregunta de los beneficios ventajosos del protocolo nos muestra el cuadro que están de acuerdo con los beneficios.*

5.- ¿Los riesgos de seguridad de la empresa son menos vulnerables aplicando el protocolo?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	2
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*este cuadro nos muestra que la mayoría están de acuerdo con pregunta realizada en la encuesta.*

6.- ¿Las reglas de acceso alcanzan ciertos niveles de seguridad en la red, permitiendo acceso a lugares específicos?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	2
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*los resultados de esta pregunta sobre los niveles de seguridad nos muestra los resultados que están 2 muy de acuerdo y 3 solo de acuerdo.*

7.- ¿El servidor de autentificación y el contralor de dominios son los que prueban la identidad del solicitante y sus credenciales, para poder dar acceso a la red?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	3
(b) De acuerdo	2
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*los resultados en esta pregunta nos muestra que la mayoría de los encuestados están muy de acuerdo con los servicios del servidor de autentificación.*

8.- ¿Si algunos de los tipos de métodos de autentificación EAP llega a fallar, protocolo 802.1x sigue funcionando normalmente?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	0
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	2
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA*:* *en este cuadro se representa que la 3 encuestados están de acuerdo y 2 están en duda, ósea ni de acuerdo, ni en desacuerdo.*

9.- ¿Aplicando el método de autentificación, autorización y contabilidad (AAA) se tiene una gran restricción a usuarios?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	2
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*el cuadro no presenta que la mayoría de los resultados están de acuerdo con la aplicación del método de autentificación.*

10.- ¿Dentro de la autentificación de la AAA se va a identificar cada usuario antes de darle acceso a la red?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	3
(b) De acuerdo	2
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*los resultados de esta pregunta nos muestra que la mayoría de los encuestados están muy de acuerdo con la identificación del usuario.*

11.- ¿Los mensajes de contabilidad que se reciben, podrían perderse por malas condiciones de la red?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	0
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	1
(d) En desacuerdo	1
(e) Muy en desacuerdo	0

NOTA:*los resultados de esta pregunta encuestada nos muestra que la mayoría están de acuerdo con la pérdida de información y solo 1 está indeciso ni de acuerdo ni en desacuerdo.*

12.- ¿Con la tecnología NAP se tiene una buena salud dentro de la empresa, detectando el estado de salud del solicitante que pide acceso?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	3
(b) De acuerdo	1
(c) Ni de acuerdo, ni en desacuerdo	1
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*los resultados de esta pregunta nos representa que 3 está muy de acuerdo con la tecnología NAP y 1 de acuerdo y 1 ni de acuerdo ni desacuerdo.*

13.- ¿El cliente NAP requiere que las computadoras del solicitante de acceso tengan ajustes como firewall activo, actualizaciones recientes, antivirus/antimalware activo, etc. antes de que tengan acceso a la red corporativa?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	3
(b) De acuerdo	2
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*los resultados de este cuadro están a favor de la respuesta muy de acuerdo ya que tiene 3 a favor y solo 2 está de acuerdo con el cliente NAP.*

14.- ¿Si el solicitante no pasa la evaluación de salud NAP, es mandado a red de cuarentena del cual los servidores de remediación instalan los componentes y actualizaciones necesarias?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	4
(b) De acuerdo	1
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*la respuesta de esta pregunta son favorable para la primera respuesta que es muy de acuerdo.*

15.- ¿La remediación de apoyo deja un espacio de reparación de los equipos cliente para lograr el cumplimiento de las políticas?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	2
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*este cuadro nos muestra que 2 están muy de acuerdos y 3 solo de acuerdo a la remediación de apoyo.*

16.- ¿Cisco NACayuda a asegurar que los equipos terminales conectados se ajusten asu política de seguridad?

RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	2
(b) De acuerdo	3
(c) Ni de acuerdo, ni en desacuerdo	0
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

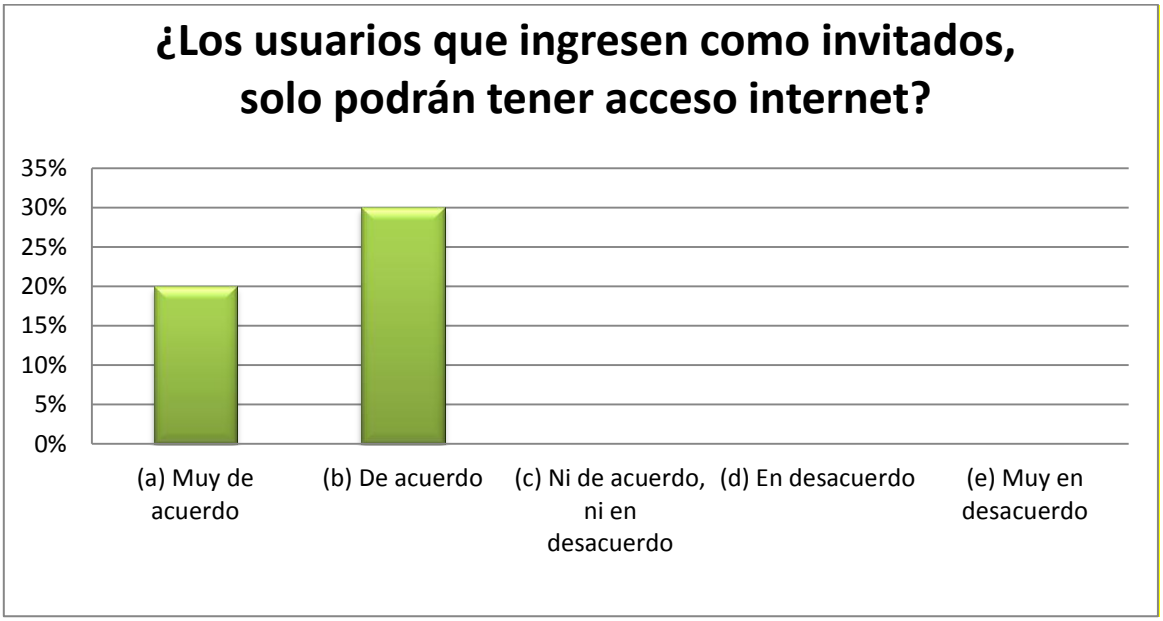
NOTA*: los resultados de este cuadro nos representa que 2 personas estuvieron muy de acuerdo con la pregunta y 3 personas solo mencionaron de acuerdo.*

17.- ¿NAC de Cisco evita la pérdida de información confidencial?

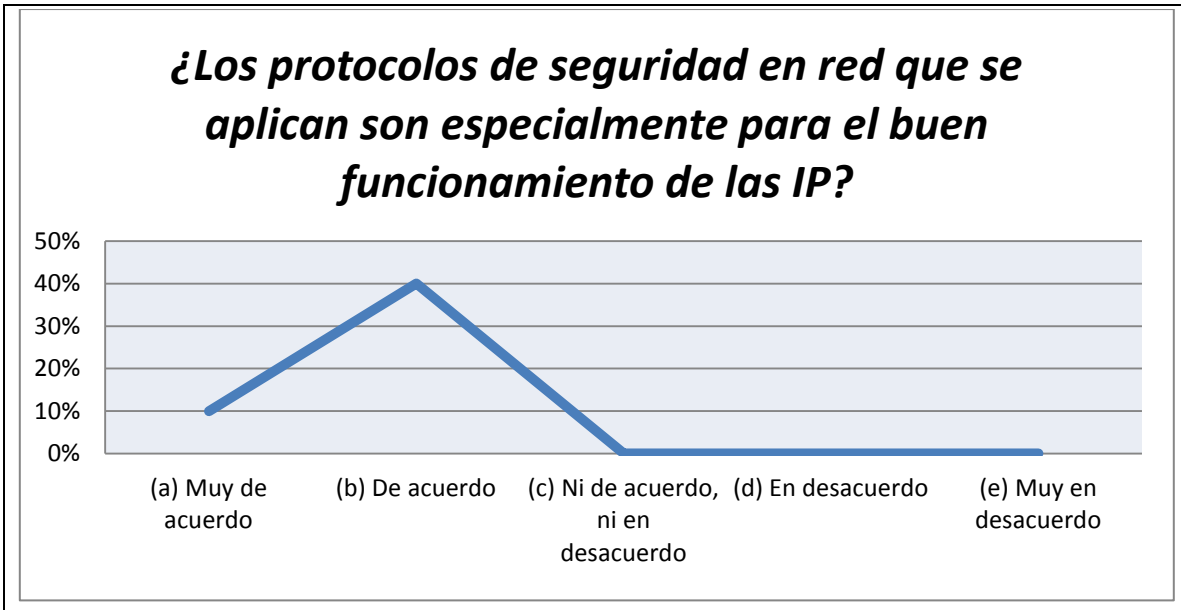
RESPUESTAS	No. DE INGENIEROS
(a) Muy de acuerdo	0
(b) De acuerdo	4
(c) Ni de acuerdo, ni en desacuerdo	1
(d) En desacuerdo	0
(e) Muy en desacuerdo	0

NOTA:*los resultados de esta pregunta nos representa que la mayoría de los encuestados estuvieron de acuerdo con la evitación de pérdida de información.*

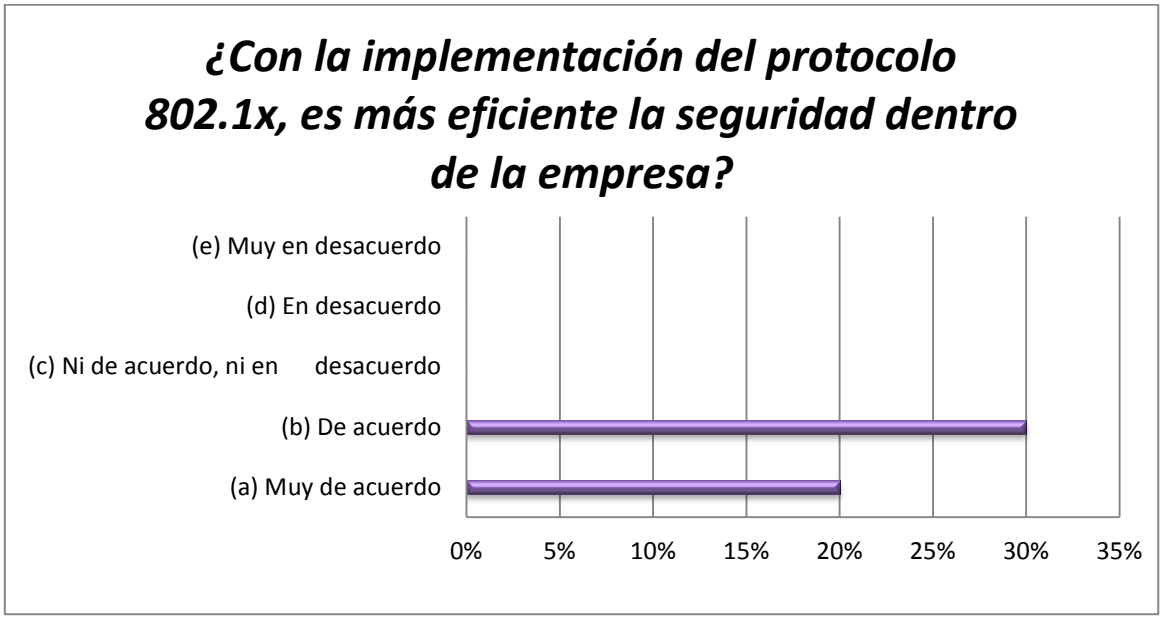
4.2 GRÁFICOS



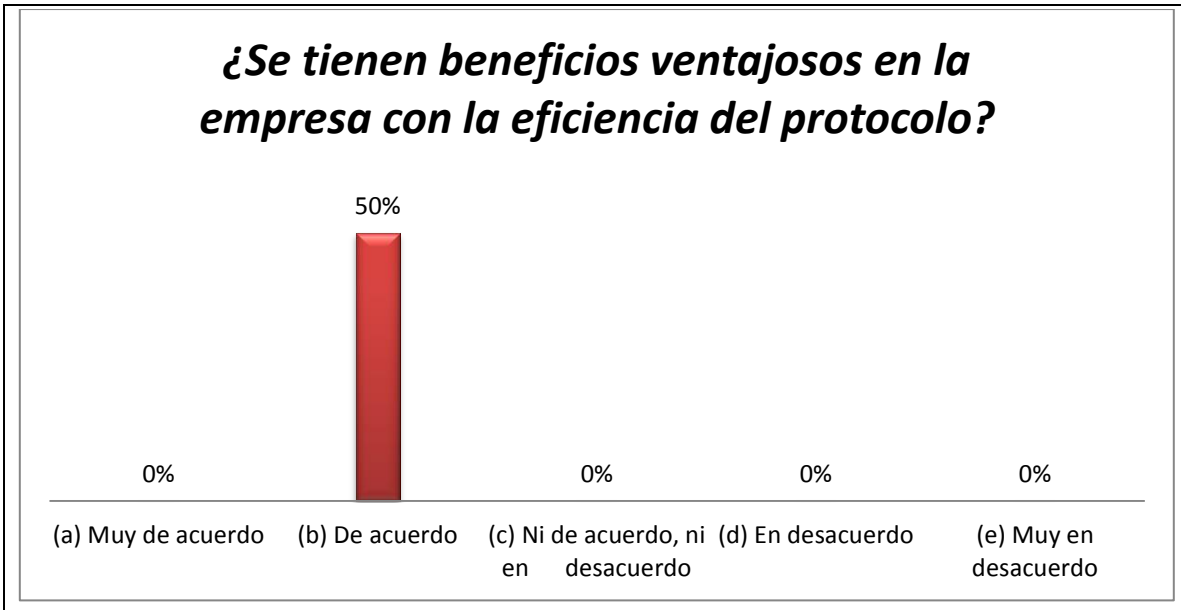
NOTA:*en esta grafica se representa que el 20% de los encuestados estuvieron muy de acuerdo y el 30% solo de acuerdo respecto a la pregunta.*



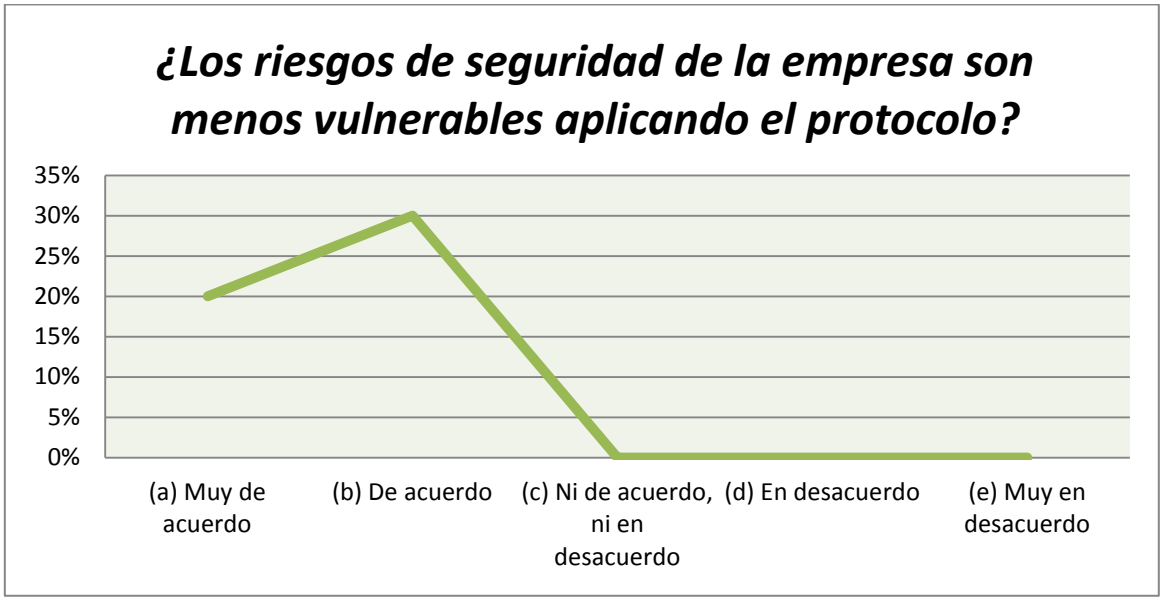
NOTA:*esta grafica nos representa que el 40% de las personas encuestas estuvieron de acuerdo y solo 1 persona estuvo muy de acuerdo con los protocolos de seguridad.*



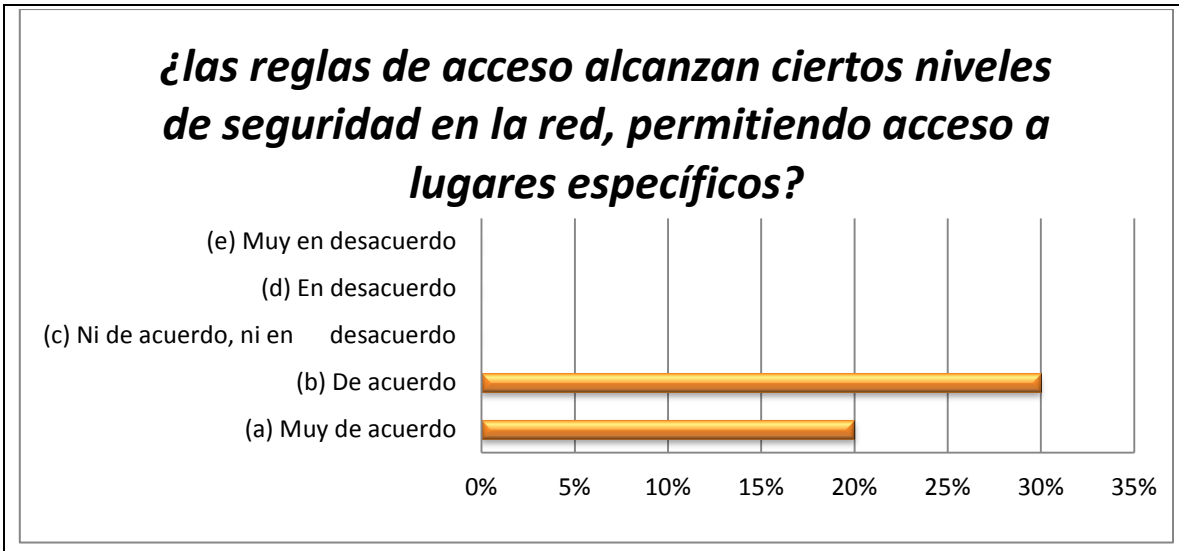
NOTA:*en esta grafica nos podemos dar cuenta que el 30% de las personas encuestas estuvieron de acuerdo y el 20% de las demás muy de acuerdo con la implementación del protocolo.*



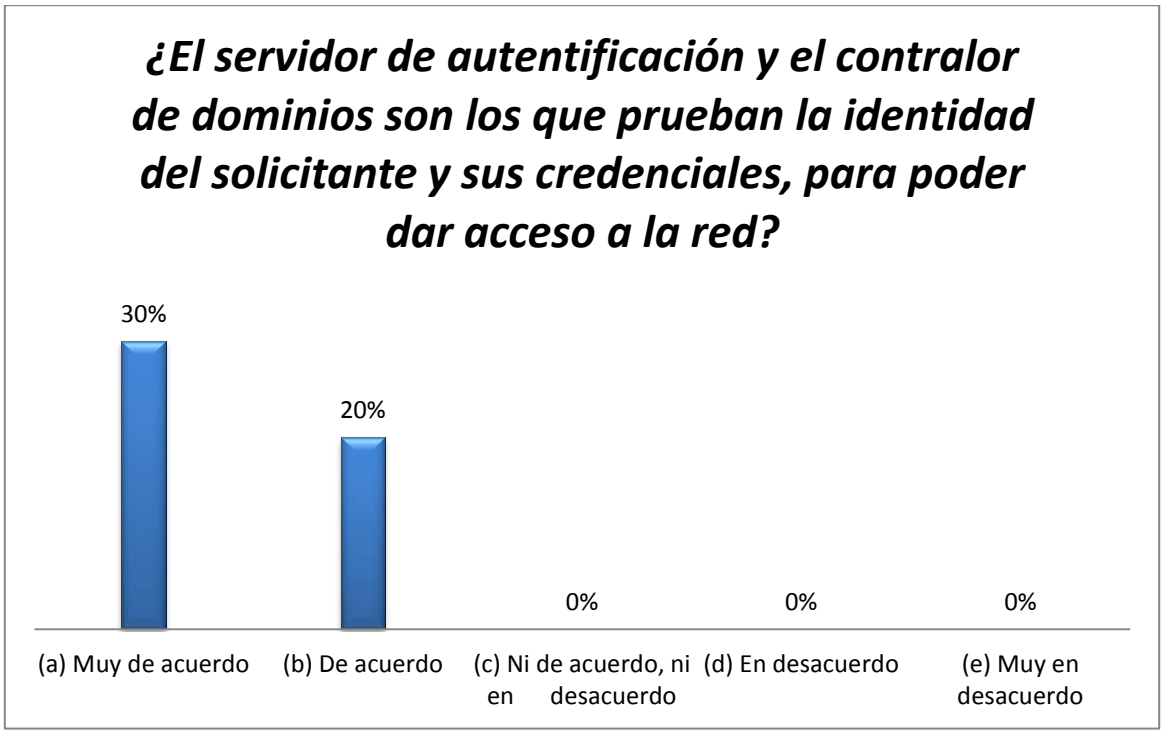
NOTA:*en esta grafica se muestra que todas las personas encuestadas estuvieron de acuerdo con los beneficios ventajosos dentro de la empresa.*



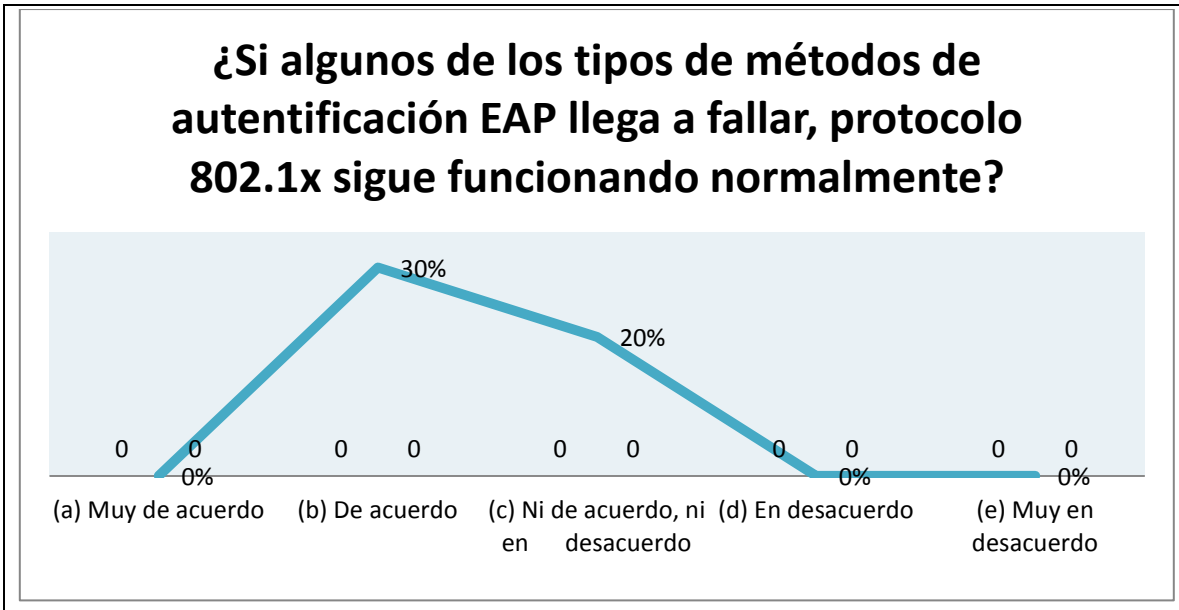
NOTA:*esta grafica nos representa que un 30% de las personas estuvieron de acuerdo y un 20% muy de acuerdo a los riesgos de seguridad.*



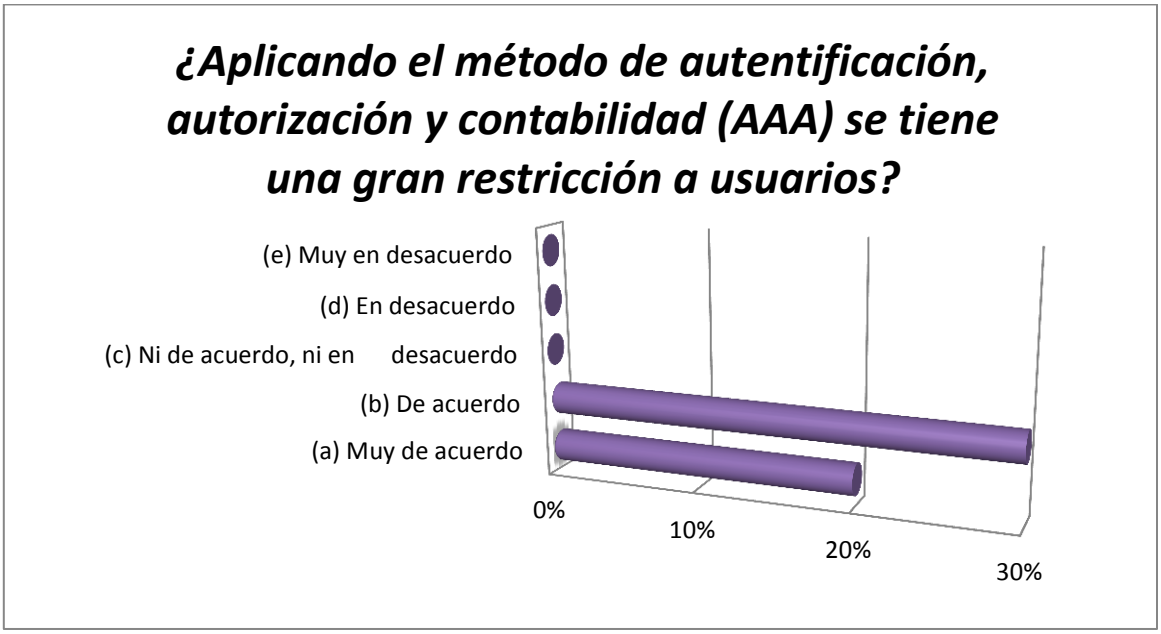
NOTA:*la grafica nos muestra que un 30% de las personas están de acuerdo y un 20% muy de acuerdo con las reglas de acceso de seguridad en la red, el cual nos indica que las reglas si son importantes para darle un lugar a cada usuario.*



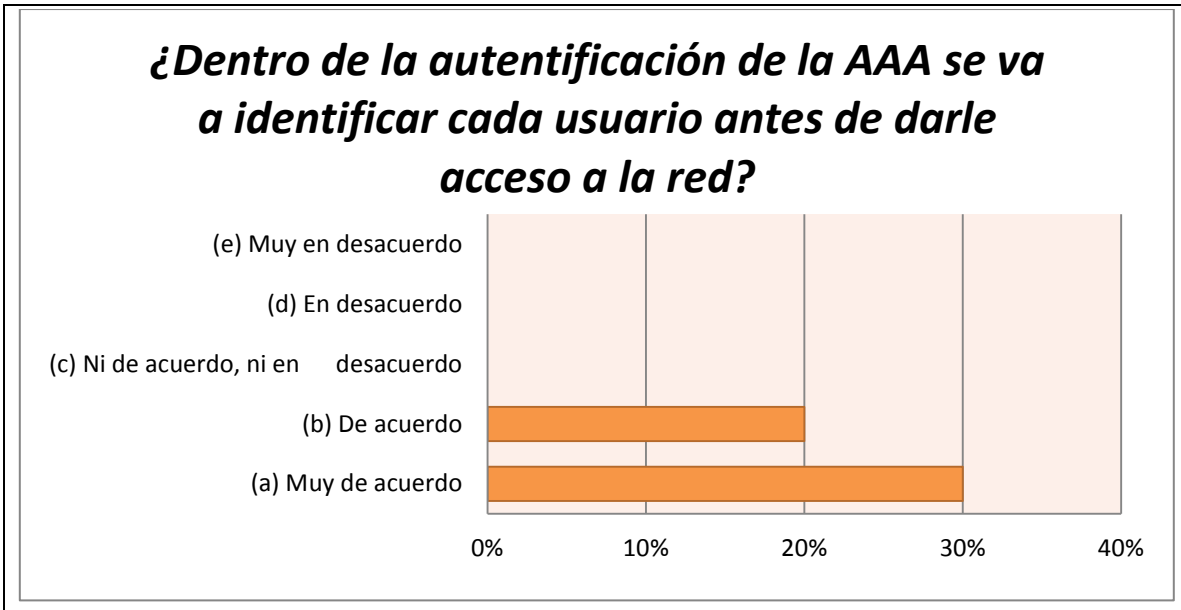
NOTA:*esta grafica nos muestra que los resultados son un 30% muy de acuerdo y un 20% están de acuerdo con los servicios del autentificador y el controlador de dominios, lo que nos indica que si es necesario el servidor de autentificación y el controlador de dominios.*



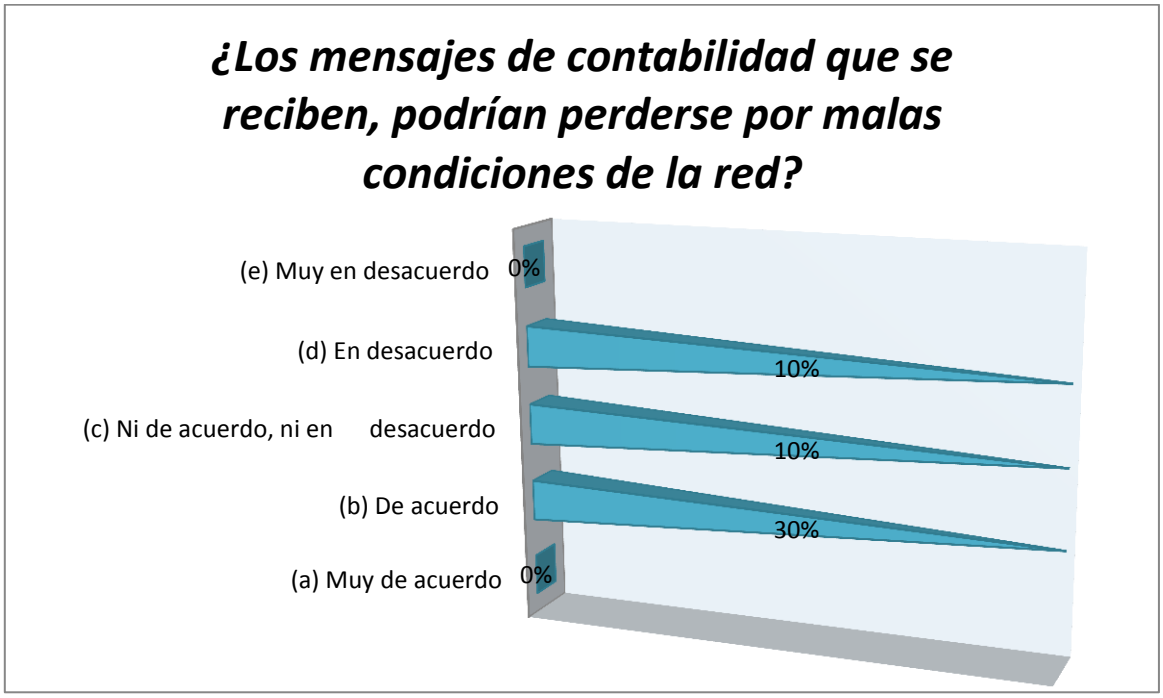
NOTA:*la grafica que se muestra nos da resultados de un 30% de personas están muy de acuerdo y un 20% de acuerdo con los métodos de autentificación EAP.*



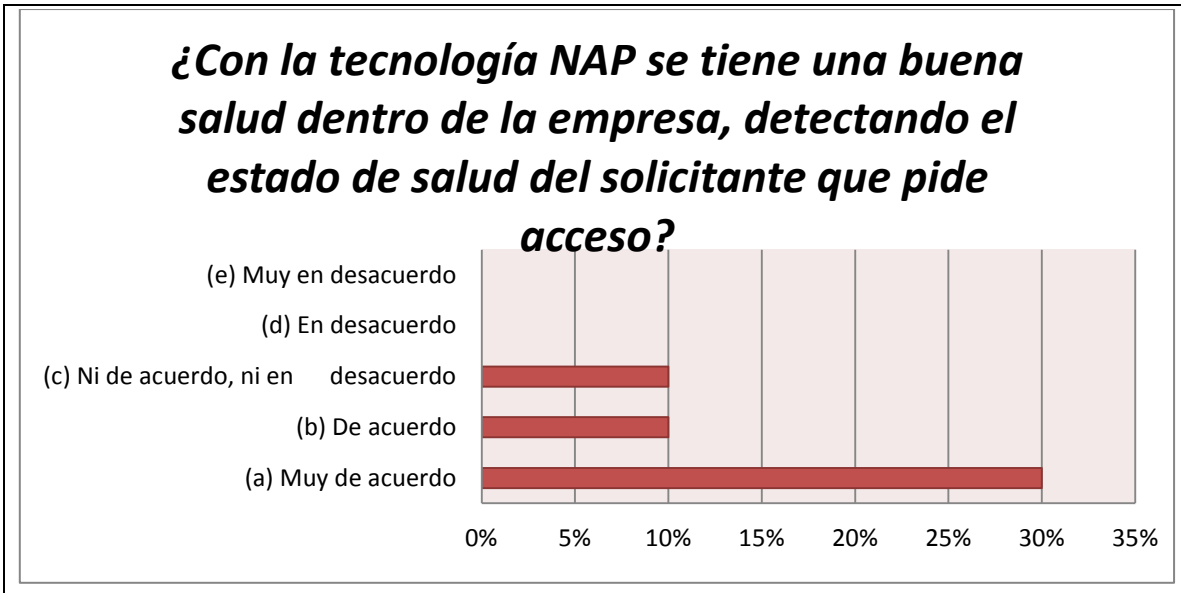
NOTA:*la grafica que se muestra nos indica que el 30% de las personas encuestas están de acuerdo y un 20% están muy de acuerdo, lo cual nos indica que si se tiene gran restricción a usuarios aplicando el método de la AAA.*



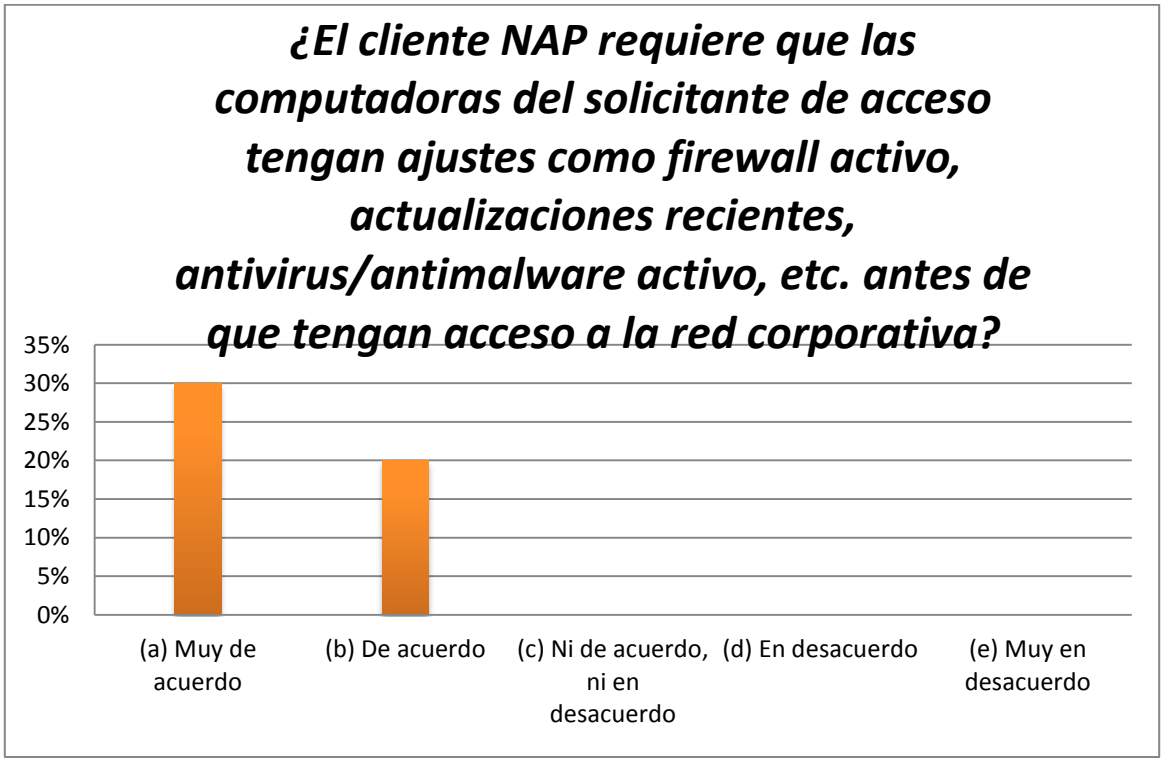
NOTA:*en esta grafica se muestra que un 30% están muy de acuerdo con la identificación de usuario que realiza el método de autentificación AAA y un 20% nos indica que solo están de acuerdo.*



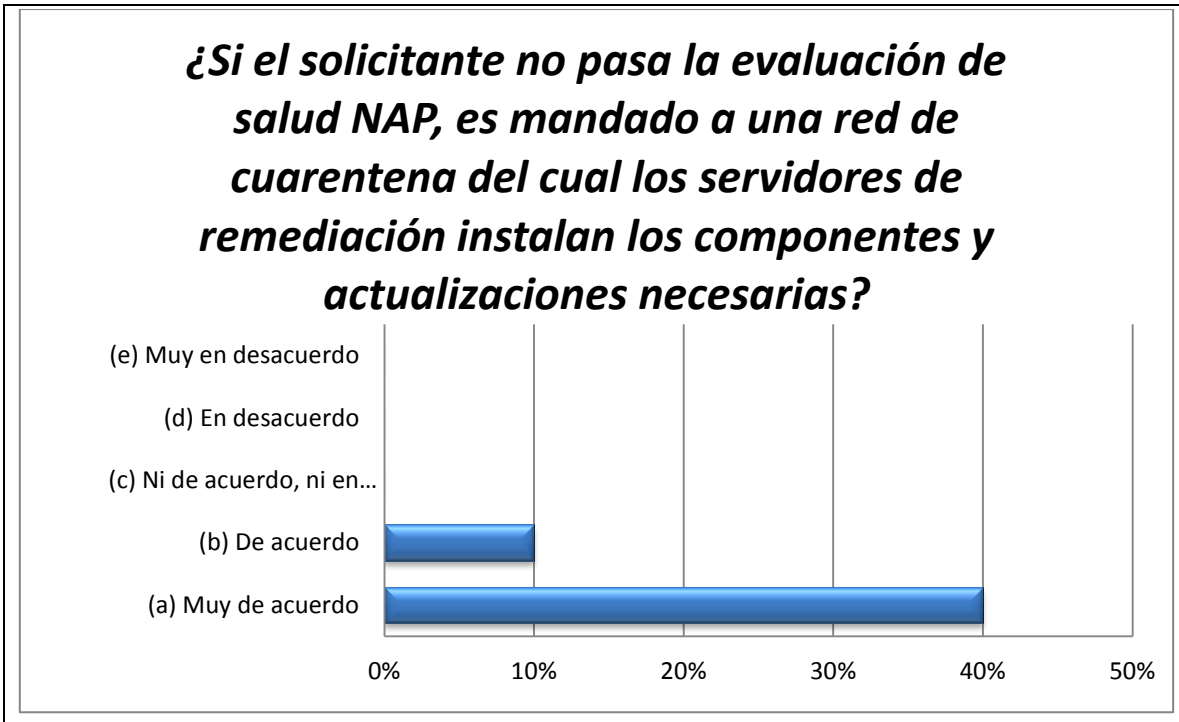
NOTA:*esta grafica nos representa que un 30% están de acuerdo con las perdida de mensajes, un 10% en duda y otro 10% en desacuerdo, lo cual nos indica que la mayoría de los encuestados nos dice que si se podrían perder los mensajes de contabilidad de la red.*



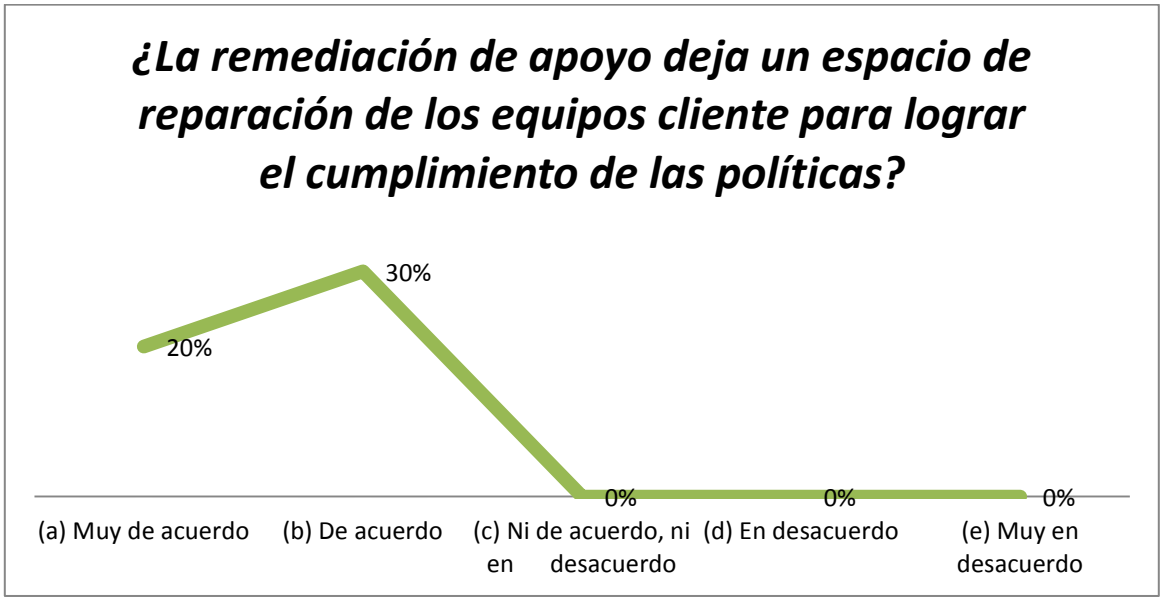
NOTA:*en esta grafica los resultados que nos muestra son un 30% de personas que están muy de acuerdo, un 10% de acuerdo y otro 10% en duda ósea ni de acuerdo ni en desacuerdo, lo que nos indica que con la tecnología NAP se puede tener una buena salud dentro de la empresa.*



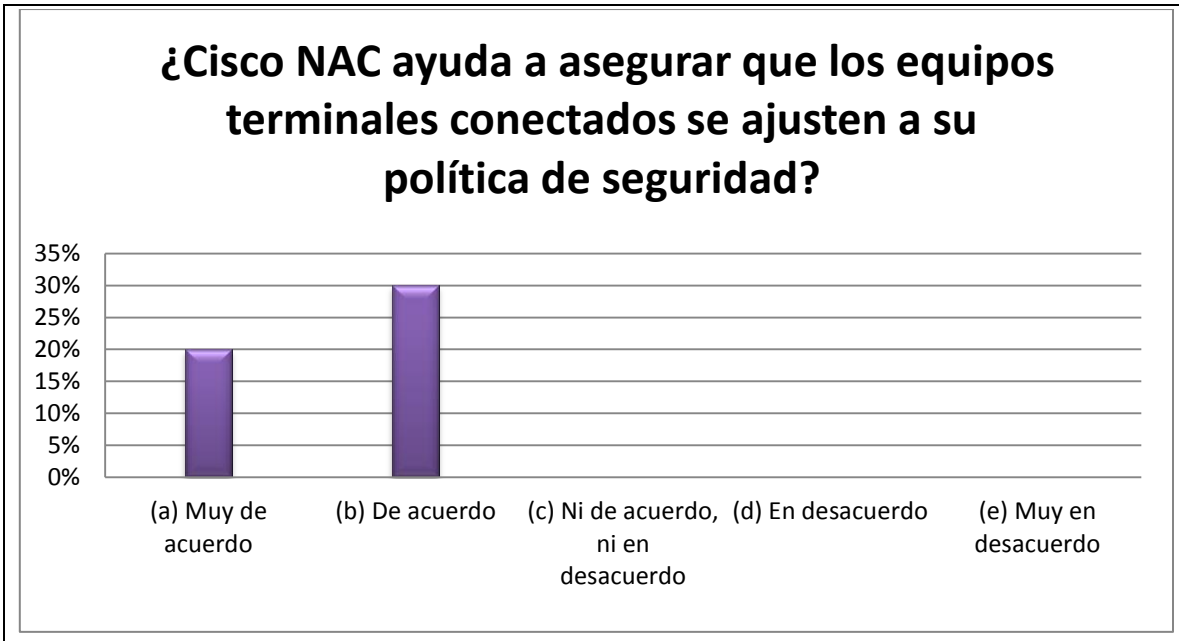
NOTA:*en esta grafica nos muestra que el 30% de las personas encuestadas están muy de acuerdo y un 20% están de acuerdo con lo que requiere la tecnología NAP antes de darle acceso al equipo de entrar en la red corporativa*.



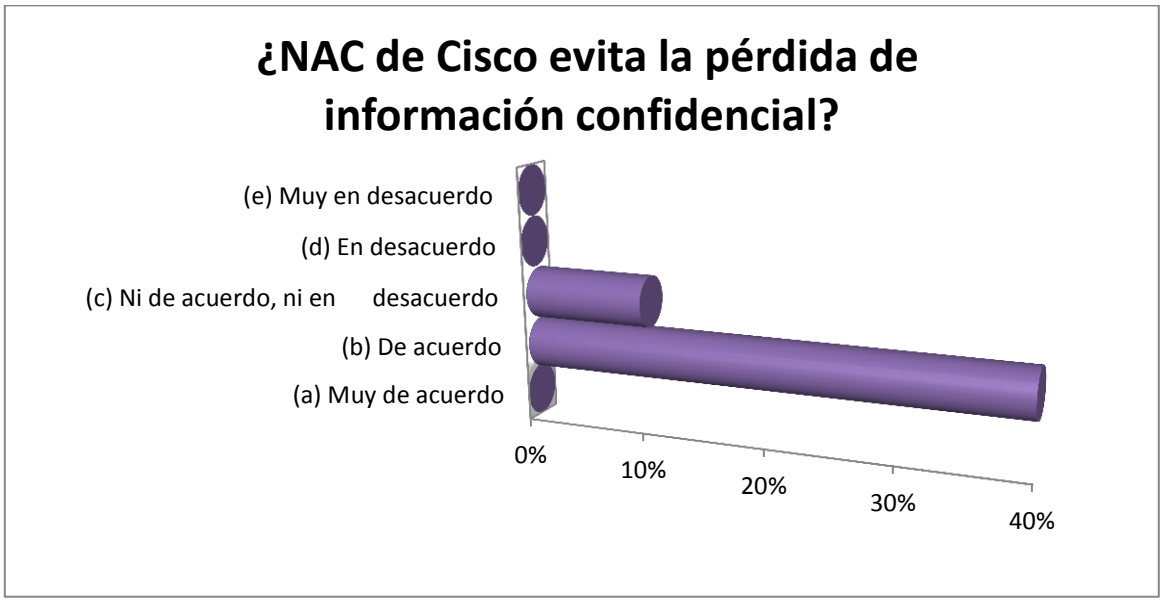
NOTA:*los resultados de esta grafica nos muestra que un 40% de las personas encuestadas están muy de acuerdo y un 10% están de acuerdo, con que si un equipo no pasa la evaluación de NAP es mandado a una red de cuarentena.*



NOTA:*esta grafica nos representa que la remediación de apoyo deja un espacio para la reparación de los quipos que no logran pasar las políticas de la empresa, teniendo un 30% de persona que están de acuerdo y un 20% que están muy de acuerdo con esta remediación de apoyo.*

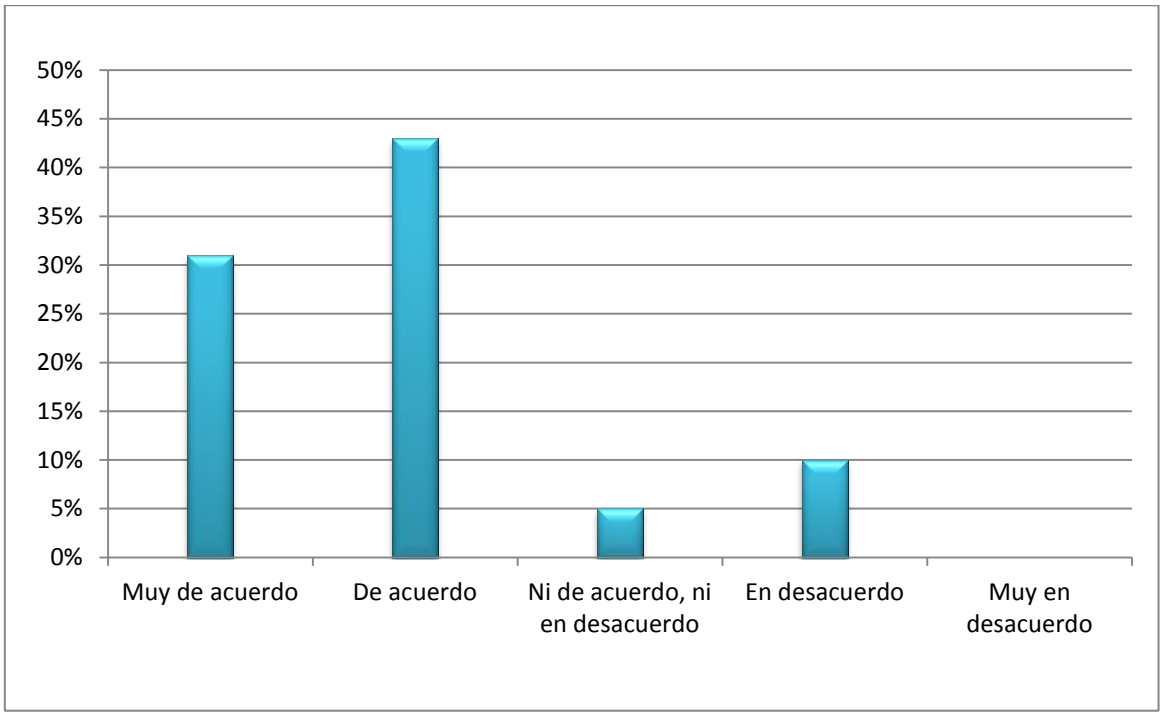


NOTA:*en esta grafica nos muestra que el 30% de las personas están de acuerdo y un 20% están muy de acuerdo con la ayuda de Cisco NAC.*



NOTA:*los resultados de esta grafica nos indica que el 40% de las personas encuestadas están de acuerdo con que NAC de Cisco evita la pérdida de información mientras que un 10% de las personas están en duda.*

Grafica General de la opinión de los encuestados



NOTA:*En esta grafica se representa el porcentaje de todos los resultados de las preguntas encuestadas, el cual se tiene que un 31% de personas están muy de acuerdo, el 43% están de acuerdo, el 5% están ni de acuerdo ni en desacuerdo, el 10% están en desacuerdo y un 0% muy en desacuerdo con la implementación y eficacia del protocolo 802.1x en Pemex Petroquímica, teniendo en general un 80% de opiniones.*

4.3PRESENTACIÓN DE RESULTADOS

La presentación de información debe tener un informe que registre completamente los procesos y resultados del estudio. Una vez terminado el informe, puede extraer partes de éste y preparar resúmenes para su difusión entre los interesados que esperan conocer sus resultados. En esta sección, primero trataremos la elaboración del informe completo y luego haremos algunas sugerencias para difundirlo entre grupos de interés específico.

Como ya se menciono la técnica de análisis se elaborara por medio de la encuesta aplicando el método de escalamiento tipo Likert teniendo opciones múltiples para responder, la presentación de informe será poniendo las preguntas en una parte y las opciones de respuesta en otra, que al final de aplicar el método de investigación se analizaran las respuestas obtenidas verificando que opción fue la que tuvo más moda en la encuesta.

Después se realizarandiferentes cuadros y graficas de diferentes tipos con porcentajes, mostrando que tanto por ciento de los usuarios en el edificio Pemex Petroquímica están muy de acuerdo o de acuerdo con el estándar implementado, quienes están en desacuerdo o muy en desacuerdo y que tantos usuarios prácticamente lo ven como un desarrollo más de tecnología en el edificio.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES DEL ESTUDIO

Tomando en cuenta la hipótesis, nuestras variables, los objetivos y las preguntas de investigación, se puede decir que el protocolo estándar IEEE 802.1x es fiable y eficaz para preservar la seguridad en el acceso a la red cableada en la empresa de Pemex Petroquímica. Contando la infraestructura adecuada y los estándares tecnológicos del protocolo IEEE 802.1x, se puede proteger todos los nodos de la empresa de cualquier equipo que no esté adecuadamente protegido, obteniendo seguridad, integridad y confidencialidad en la información que viaja a través de la red de PPQ.

La autenticaciónIEEE802.1X proporcionaunaprotección de losnodosde la redde acceso libre(que se encuentraen los pasillos osalas) contrael acceso no autorizadoa la red LAN. También es útilpara garantizar el accesode usuario invitadodurante las conferenciaso talleres.Mientras que losusuarios locales se autentificana través de802.1X yun completo accesoa la red,a losvisitantesse les asignan unaVLAN restringidacon accesoa Internet. IEEE 802.1Xofreceuna excelente visibilidadyseguridad, de identidad, control de accesoen elborde de la red. Con los componentes apropiadosde diseñoy bien elegida, puede satisfacer las necesidades desu política deseguridad y reducir losefectos negativos sobrela infraestructuray los usuarios finales.

Después de describir los principales mecanismos para la seguridad de la red, se puede percibir que la implementación de 802.1x en entornos cableados es un componente primordial de las mejores recomendaciones de seguridad actuales y futuras, por lo cual su adopción es una práctica que no solo leva el nivel de seguridad de las infraestructuras de acceso inalámbrico actuales, si no que prepara a las organizaciones para llegar a cumplir con los futuros estándares de seguridad para este tipo de tecnología.Adicionalmente, implementar 802.1x en ambientes inalámbricos y cableados es una posibilidad real que las organizaciones pueden llevar a cabo con su infraestructura tecnológica actual, y que se adecuará, sin mayores impactos económicos o funcionales, a su crecimiento y modernización.

5.2 GLOSARIO

ACOMEDIDA: Servicial, oficioso, complaciente.

ANCHO DE BANDA: Característica de la línea telefónica que determina la cantidad de conexiones simultáneas que se pueden establecer entre los usuarios y el servidor. Cuando mayor sea el ancho de banda de la línea que ofrece un servidor, más usuarios podrán conectarse

He a la vez, y más rápida será la conexión. El ancho de banda es la máxima cantidad de datos que pueden pasar por un camino de comunicación en un momento dado, normalmente medido en segundos. Cuanto mayor sea el ancho de banda, más datos podrán circular por ella al segundo.

ANGULO DE REFLEXIÓN: Ángulo que forma un rayo reflejado con la normal a la superficie del medio en el punto de incidencia.

AWG: Calibre de alambre estadounidense (CAE, en inglés AWG - *American Wire Gauge*) es una referencia de clasificación de diámetros. En muchos sitios de Internet y también en libros y manuales, especialmente de origen norteamericano, es común encontrar la medida de conductores eléctricos (cables o alambres) indicados con la referencia AWG. Cuanto más alto es este número, más delgado es el alambre. El alambre de mayor grosor (AWG más bajo) es menos susceptible a la interferencia, posee menos resistencia interna y, por lo tanto, soporta mayores corrientes a distancias más grandes.

BROADCAST (DIFUSIÓN): Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

BLUETOOTH: Es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos.

CIFRADO: Es el proceso que se aplica a unos datos para hacerlos incomprensibles y evitar que puedan ser observados por otras personas. Este proceso o transformación precisa de una clave de cifrado, que es una cadena aleatoria de bits.

CONECTORES: «Enchufe» que facilita la unión mecánica entre dos dispositivos y, a la vez, la comunicación de datos entre ambos o el intercambio de corriente. Por extensión, se entiende por conector el terminal de un sistema al que se conectan determinados periféricos.

CONMUTADOR: Dispositivo electrónico que forma el centro de una red. Los conmutadores usan la dirección destino de un cuadro para determinar la computadora que debe recibirlo.

CROSSTALK (DIAFONÍA): Se dice que entre dos circuitos existe **diafonía**, denominada en inglés *Crosstalk* (XT), cuando parte de las señales presentes en uno de ellos, considerado perturbador, aparece en el otro, considerado perturbado.

CUARENTENA: Función de protección característica de los antivirus que nos permite dejar sin efecto a archivos que puedan estar infectados, hasta que nuestros sistemas de seguridad tengan una nueva actualización para poder desinfectarlos o hasta que el administrador decida qué hacer con ellos, si desinfectarlos o borrarlos directamente.

DATAGRAMAS: Cada paquete se trata de forma independiente, conteniendo cada uno la dirección de destino. La red puede encaminar (mediante un router) cada fragmento hacia el Equipo Terminal de Datos (ETD) receptor por rutas distintas.

ENCAPSULAMIENTO: Es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. El encapsulado consiste pues en ocultar los detalles de implementación

de un objeto, pero a la vez se provee una interfaz pública por medio de sus operaciones permitidas.

ENCRIPTACIÓN: Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor.

ENRUTADOR DIRECCIONADOR, **RUTEADOR** O **ENCAMINADOR:** es un dispositivo de hardware para interconexión de red de ordenadores (computadoras) que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

ETHERNET:(también conocido como *estándar IEEE 802.3*) Es un estándar de transmisión de datos para redes de área local.

FRAMEWORK: Esun conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular, que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar. Es una estructura conceptual y tecnológica de soporte definida, normalmente con artefactos o módulos de software concretos, con base en la cual otro proyecto de software puede ser organizado y desarrollado.

GESTORES DE RED: Consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones.

GIGABIT ETHERNET: Es una ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet (También llamado 100-Base/T).

HARDWARE: Corresponde a todas las partes físicas y tangibles[1] de una computadora.

HUBS: Dispositivo que integra distintas clases de cables y arquitecturas o tipos de redes de área local. Existe una palabra castellana para identificar un Hub, Concentrador.

IEEE: Instituto de Ingenieros Electricistas y Electrónicos.

LAN:LAN (del inglés *local area network*), red de área local o red local es la interconexión de varias computadoras y periféricos.

MAC:(siglas en inglés de **Media Access Control** o *control de acceso al medio*) es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una ethernet de red. Se conoce también como la dirección física en cuanto a identificar dispositivos de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada.

MAN: Red de área metropolitana (*metropolitan area network* o *MAN*, en inglés) es una red de alta velocidad (banda ancha) dando cobertura en un área geográfica extensa.

MULTICAST (MULTIDIFUSIÓN): es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

NODO: Es un punto de intersección o unión de varios elementos que confluyen en el mismo lugar.

OSI: Modelo de interconexión de sistemas abiertos, también llamado OSI (en inglés *open system interconnection).*

PROTOCOLO: Se denomina protocolo a un conjunto de normas y/o procedimientos para la transmisión de datos que ha de ser observado por los dos extremos de un proceso comunicacional (emisor y receptor).

RADIUS (RemoteAuthentication Dial-In UserService): Es un protocolo de autenticación basado en cliente y servidor que le permite a un servidor de acceso

remoto comunicarse con un servidor central para poder autenticar usuarios que acceden a la red y autorizar el uso de los servicios requeridos.

RATIFICADA: Aprobar o confirmar una cosa [que se ha dicho o hecho].

REDES DE COMPUTADORAS: Es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos), etc. incrementando la eficiencia y productividad de las personas.

TRAMAS: Es una unidad de envío de datos. Viene a ser el equivalente de paquete de datos o Paquete de red, en el Nivel de enlace de datos del modelo OSI.

UNICAST: Es el envío de información desde un único emisor a un único receptor.

ANEXOS

Aquí se ubicarán los instrumentos y otro tipo de documento que han sido necesarios para el desarrollo del trabajo y que no se ha considerado otro lugar para ellos en el documento.

Los anexos son secciones adicionales que se adjuntan al documento escrito, el objetivo es presentar información adicional importante, ya sea para prolongar la explicación de los datos, como también para confirmarlos. Se ubica después de las conclusiones y recomendaciones, antes de la bibliografía.

Codificación de preguntas

1.- ¿Los usuarios que ingresen como invitados, solo podrán tener acceso internet?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

2.- ¿Los protocolos de seguridad en red que se aplican son especialmente para el buen funcionamiento de las IP?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

3.- ¿Con la implementación del protocolo 802.1x, es más eficiente la seguridad dentro de la empresa?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

4.- ¿Se tienen beneficios ventajosos en la empresa con la eficiencia del protocolo?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

5.- ¿Los riesgos de seguridad de la empresa son menos vulnerables aplicando el protocolo?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

6.- ¿Las reglas de acceso alcanzan ciertos niveles de seguridad en la red, permitiendo acceso a lugares específicos?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

7.- ¿El servidor de autentificación es que el que prueba la identidad del solicitante y sus credenciales, para poder dar acceso a la red?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

8.- ¿Si algunos de los tipos de métodos de autentificación EAP llega a fallar, protocolo 802.1x sigue funcionando normalmente?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

9.- ¿Aplicando el método de autentificación, autorización y contabilidad (AAA) se tiene una gran restricción a usuarios?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

10.- ¿Dentro de la autentificación de la AAA se va a identificar cada usuario antes de darle acceso a la red?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

11.- ¿Los mensajes de contabilidad que se reciben, podrían perderse por malas condiciones de la red?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

12.- ¿Con la tecnología NAP se tiene una buena salud dentro de la empresa, detectando el estado de salud del solicitante que pide acceso?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

13.- ¿El cliente NAP requiere que las computadoras del solicitante de acceso tengan ajustes como firewall activo, actualizaciones recientes, antivirus/antimalware activo, etc. antes de que tengan acceso a la red corporativa?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

14.- ¿Si el solicitante no pasa la evaluación de salud NAP, es mandado a un área restringida del cual los servidores de remediación instalan los componentes y actualizaciones necesarias?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

15.- ¿La remediación de apoyo deja un espacio de reparación de los equipos cliente para lograr el cumplimiento de las políticas?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

16.- ¿Cisco NACayuda a asegurar que los equipos terminales conectados se ajusten asu política de seguridad?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

17.- ¿NAC de Cisco evita la pérdida de información confidencial?

5= Muy de acuerdo

4= De acuerdo

3= Ni de acuerdo, ni en desacuerdo

2= En desacuerdo

1= Muy en desacuerdo

Decodificación de preguntas

	NÚMERO DE INGENIEROS					
PREGUNTAS	**1**	**2**	**3**	**4**	**5**	**TOTAL**
1	5	4	5	1	4	**19**
2	4	5	4	4	4	**21**
3	5	4	4	5	4	**22**
4	4	4	4	4	4	**20**
5	4	4	5	5	4	**22**
6	5	4	4	4	5	**22**
7	4	5	4	5	5	**23**
8	4	3	4	3	4	**18**
9	4	4	4	5	5	**22**
10	5	5	5	4	4	**23**
11	4	4	2	4	3	**17**
12	5	4	5	5	3	**22**
13	5	5	4	4	5	**23**
14	5	5	5	5	4	**24**
15	5	5	4	4	4	**22**
16	4	5	4	5	4	**22**
17	4	4	3	4	4	**19**
TOTAL	**71**	**70**	**74**	**76**	**70**	**361**

//Habilita AAA/Radius
aaa new-model
!
!
//Se configura los mensajes de la línea de comando
aaa authentication password-prompt contrasenia:
aaa authentication username-prompt usuario:
//Se crea la lista de métodos para la autentificación de usuario y usuario privilegiado
aaa authentication login default group radius local
aaa authentication enable default group radius enable
//Se crea lista de método para 802.1x
aaa authentication dot1x default group radius
!
!
!
aaa session-id common
!
//Se habilita la autentificación dot1x en el switch
dot1x system-auth-control
!
!
//Se configuración de las interfaces
interface FastEthertnet0/1
//Definición de la VLAN por defecto a la que pertenecerán los puertos
switchport access vlan3
//Definición de los puertos de acceso (dot1x no se configura en puertos troncales)
switchport model access
switchport port-security
//Habilita 802.1x en los puertos
dot1x pae authenticator
dot1x port-control auto
dot1x violation-mode protect
//Definición de parámetros adicionales de dot1x
dot1x guest-vlan 80
dot1x auth-fail vlan 80
dot1x auth-fail max-attempts 1
ip dhcp snooping limit rate 90
!
Ip radius source-interface GigabitEthernet0/1
!
//Se configure la IP del RADIUS, el puerto de autentificación y el puerto de autorización
radius-sever host 145.111.34.20 auth-port 1645 acct-port 1547 key 7 345934052D49395B942

BIBLIOGRAFIA

1. A. Behrouz A. Transmisión de Datos y Redes de Comunicación. Editorial Mc Graw Hill. Edición segunda. España. 2002. Pág.887.
2. Alberto León García, Indra Widjaja. Redes de Comunicación. Conceptos Fundamentales y Arquitectura Básicas. Editorial Mc Graw Hill. Primera Edición en Español. España. 2002. Pág. 771.
3. Berenice Ibáñez Brambila. Manual para Elaboración de Tesis. Editorial Trillas. Edición segunda. México. 1995. Pág. 303.
4. Craig Zacker. Redes. Manual de Referencias. Editorial Mc Graw Hill. Edición Primera en español.España. 2002. Pág.1046.
5. Drew Heywood. Redes con Microsoft TCP/IP. Editorial Prentice Hall. Edición Segunda. Madrid, España. 1998. Pág. 538.
6. Jesús García Tomas, José Luis Raya Cabrera, Víctor Rodrigo Raya. Alta de Velocidad y Calidad de Servicio en Redes IP. Editorial Alfa Omega Ra-Ma. Edición original. Madrid, España. 2002. Pág. 674.
7. Jesús Sánchez Allende, Joaquín López Lérida. Redes. Editorial Mc Graw Hill.Edición Primera en Español. España. 2000. Pág.318.
8. José Luis Raya. Redes Locales y TCP/IP. Editorial Alfa Omega Ra-Ma. Edición Original. Madrid, España. 1995. Pág. 185.
9. Jesús García Tomas. Sistemas y Redes Teleinformáticas. Editorial Ra-Ma. Edición Primera. España. 1990. Pág. 616.
10. Luis Guijarro Coloma. Redes ATM, Principio de Interconexión y su Aplicación. Editorial Alfa Omega Ra-Ma. Edición Original. Madrid, España. 2000. Pág. 155. Capitulo 5: Modelo OSI.
11. Luis Medina Lozano. Métodos de Investigación I y II. Editorial Emma E. Paniagua Roldan. Treceava reimpresión. México. 2004. Pág. 235.
12. Laura Cazares Hdez., María Christen Y otros. Técnicas actuales de investigación documental. Editorial Trillas. Edición tercera. México. 1990. Pág. 194.
13. Matt Hayden. Aprendiendo Redes en 24 Hrs. Primera Edición. Editorial Prenticee Hall. México. 1999. Pág. 445.

14. Merilee Ford, H. Kim Lew. Tecnologías de Interconectividad de Redes. Edición Segunda. Editorial Pearson Cisco System. España. 2000. Pág. 716.
15. Philip Cox, Tom Sheldon. Manual de Seguridad. Editorial Mc Graw Hill. Pág.739.
16. Roberto Hernández Sampieri. Metodología de la investigación. Editorial Mc. Graw Hill. Edición cuarta. México. 2007. Pág. 850.
17. Raúl Rojas Soriano. Guía para realizar investigaciones sociales. Editorial plaza y Valdes. Edición 14ª. México. 1994. Pág. 286.
18. Raúl Rojas Soriano. El Proceso de la Investigación científica. Editorial Trillas. Edición Cuarta. México. 1990. Pág. 151.
19. Uylees Black. Redes de computadoras, Protocolos, Normas e Interfaces. Editorial Alfa Omega Ra-Ma. Edición Segunda. España. 1997. Pág. 585.

PAGINAS DE INTERNET

http://www.manual-wifi.com/802.1x.html

http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm

http://www.unincca.edu.co/boletin/indice.htm

http://www.virusprot.com/Whitepap1.html

http://dns.bdat.net/seguridad_en_redes_inalambricas/x75.html

http://www.laflecha.net/articulos/wireless/redes_inalambricas/

http://www.intel.com/support/sp/wireless/wlan/sb/cs-025323.htm

http://www.microsoft.com/spain/technet/recursos/articulos/11110308.aspx

http://www.ciscopress.com/articles/article.asp?p=29600&seqNum=2

http://es.kioskea.net/contents/internet/vlan.php3

http://es.wikipedia.org/wiki/VLAN

http://es.kioskea.net/contents/initiation/vpn.php3

http://ccc.inaoep.mx/~cferegrino/cursos/redscomp/Filminas_14_Aplicacion_seguridad.pdf

http://translate.google.com.mx/translate?hl=es&sl=en&u=http://en.wikipedia.org/wiki/Network_Access_Protection&ei=eMoPTLPVDcz9nQf_qrTEDQ&sa=X&oi=translate&ct=result&resnum=3&ved=0CDIQ7gEwAg&prev=/search%3Fq%3Dnap%26hl%3Des

http://translate.google.com.mx/translate?hl=es&sl=en&u=http://support.3com.com/infodeli/tools/netmgt/temwin/tem6.2/evm/chap_4a3.htm&ei=yv0STK3rEcO7ngen_8yEDA&sa=X&oi=translate&ct=result&resnum=2&ved=0CCMQ7gEwAQ&prev=/search%3Fq%3DPolicy%2BBased%2BVLANs%26hl%3Des

http://es.wikipedia.org/wiki/Cable_de_categor%C3%ADa_6

http://serviojr.blogspot.es/i2007-12/

http://www.cisco.com/

http://www.unicrom.com/art_FibraOptica_multimodo_gradual_transmision_usos.asp

http://www.unicrom.com/art_FibraOptica.asp

http://www.microsoft.com/latam/technet/articulos/tn/2007/abr-17.mspx

http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns617/net_implementation_white_paper0900aecd8051fc24.pdf

http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

http://diccionarios.glosarium.com/list/14/3,P,PR,xhtml

http://www.cisco.com/en/US/products/ps6662/products_ios_protocol_option_home.html

http://www.linux-magazine.es/issue/05/Radius.pdf

http://es.wikipedia.org/wiki/Protocolo_AAA

http://www.cesnet.cz/doc/techzpravy/2007/802.1x-wired-authentication/

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/guide_c07-627531.html

http://www.sans.org/reading_room/whitepapers/wireless/consideraciones-para-la-implementacion-de-8021x-en-wlans_1607