UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

PROYECTO DE GRADUACIÓN

APLICACIÓN 802.1X RADIUS SERVER EN LA RED INTERNA DEL SNE 911 - SPS

PREVIO A LA OBTENCIÓN DEL TÍTULO
INGENIERO EN TELECOMUNICACIONES

PRESENTADO POR:

21221077 **STEFANIE YADIRA CIBRIAN RIVERA**

ASESOR: ING. LUIS ALONZO MILIÁN

CAMPUS SAN PEDRO SULA

MAYO, 2018

RESUMEN EJECUTIVO

En el presente trabajo se muestra el trabajo realizado en Dynamic Corp., una empresa encargada en soluciones de ciberseguridad. Siendo de suma importancia la seguridad en un ambiente de red, identificando y eliminando vulnerabilidades.

Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización en organización. Independientemente, cualquier compañía con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación. Ahora las corporaciones necesitan reducir el tiempo de detección y el tiempo de resolución.

La asignación del proyecto consistió en la implementación del estándar 802.1x en Radius server para la autenticación de puertos y agilizar el trabajo y seguridad, ya que uno de los problemas que estaban teniendo en el data center era que cuando en el SNE(Sistema Nacional de Emergencias) pedían que se les habilitaran puertos temporalmente había que hacer el trabajo manualmente ya que por seguridad se mantenían los puertos que no se estaban utilizando apagados y había que esperar a ser habilitados nuevamente y cuando se dejaban de utilizar quedaban habilitados por un tiempo hasta que se desactivaban.

I. TABLA DE CONTENIDO

I. TABLA DE CONTENIDO 5
II. INTRODUCCIÓN 7
III. PLANTEAMIENTO DEL PROBLEMA 8
3.1 ANTECEDENTES DEL PROBLEMA 8
3.2 DEFINICIÓN Y ENUNCIADO DEL PROBLEMA 8
3.3 PREGUNTAS DE INVESTIGACIÓN 8
IV. OBJETIVOS 10
4.1 OBJETIVO GENERAL 10
4.2 OBJETIVOS ESPECÍFICOS 10
V. RESEÑA HISTÓRICA DE LA EMPRESA 11
5.1. VISIÓN 12
5.2. MISIÓN 13
5.3. VALORES ORGANIZACIONALES 13
5.4. SECTORES ATENDIDOS 13
VI. MARCO TEÓRICO 15
6.1. REDES DE ORDENADORES 15
6.1.1. CLASIFICACIÓN DE LAS REDES 15
6.2. NORMAS Y ESTÁNDARES EN TELECOMUNICACIONES 26
6.2.1. ESTÁNDAR DE RED 26
6.2.2. PROTOCOLO 27
6.2.3. ISO (ORGANIZACIÓN INTERNACIONAL PARA LA NORMALIZACIÓN) 27
6.2.4. NORMAS Y ESTÁNDARES EN TELECOMUNICACIONES IEEE 31
6.2.5. SWITCH 37
6.2.6. IEEE 802.1X 40
6.2.7. CONMUTADORES ETHERNET CABLEADOS COMPATIBLES CON IEEE 802.1X 41
6.2.8. ETHERNET IEEE 802.3 41
6.2.9. SERVIDOR DE DIRECTIVAS DE REDES 41
6.2.10. PROTOCOLO AAA 42

6.2.11. CERTIFICADOS DE SERVIDOR 44
6.2.12. EAP 45
6.2.13. RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE) 45
6.2.14. COMPARACIÓN DE TACACS + Y RADIUS 48
VII. METODOLOGÍA 53
7.1. VARIABLES DE ESTUDIO 53
7.2. ENFOQUE Y MÉTODOS 53
7.3. MATERIALES 53
7.4. TÉCNICAS EN INSTRUMENTOS APLICADOS 54
7.5. FUENTES DE INFORMACIÓN 54
VIII. CRONOLOGÍA 55
IX. RESULTADOS Y ANÁLISIS 56
X. CONCLUSIONES 63
XI. RECOMENDACIONES 64
RECOMENDACIONES A LA EMPRESA 64
RECOMENDACIONES A LA UNIVERSIDAD 64
XII. IMPLEMENTACIÓN 65
XIII. BIBLIOGRAFÍA 70
XIX. ANEXOS 71

II. INTRODUCCIÓN

El presente documento contiene conceptos y desarrollo del proyecto asignado en fase I, utilizando los conocimientos aprendidos. Se Describe cómo configurar el acceso autenticado mediante 802.1X del Instituto de ingenieros de electricidad y electrónica (IEEE) para conexiones cableadas Ethernet IEEE 802.3. También se proporciona información sobre tecnologías estrechamente relacionadas con el acceso cableado autenticado mediante 802.1X o relevantes al acceso cableado de algún otro modo.

La autenticación IEEE 802.1X en Radius server proporciona una barrera de seguridad adicional para la intranet que puede usar para impedir que equipos invitados, no autorizados o no administrados que no pueden autenticarse correctamente se conecten a la intranet.

Los administradores implementan la autenticación IEEE 802.1X para redes inalámbricas IEEE 802.11 para lograr una seguridad mejorada. Por el mismo motivo, los administradores de red desean implementar el estándar IEEE 802.1X para proteger sus conexiones de red cableadas. Del mismo modo en que un cliente inalámbrico autenticado debe enviar un conjunto de credenciales para su validación con el fin de poder enviar tramas inalámbricas a la intranet, un cliente cableado mediante IEEE 802.1X también debe autenticarse para poder enviar tráfico a través de su puerto de conmutador.

La autenticación IEEE 802.1x evita que los dispositivos no autorizados (clientes) accedan a la red. La autenticación de la red del Sistema Nacional de Emergencias SNE 911 utilizando el estándar 802.1x en radius server, el cual se trata de una parte importante de las redes Wi-Fi y el acceso a banda ancha de los operadores. Se explicará en qué consiste un servidor servidor RADIUS y cuáles son las aplicaciones más comunes que se le pueden dar.

III. PLANTEAMIENTO DEL PROBLEMA

3.1 ANTECEDENTES DEL PROBLEMA

El estándar del IEEE 802.1X define un protocolo basado servidor del cliente del control de acceso y de autenticación que restrinja los dispositivos desautorizados de la conexión con un LAN a través de los puertos públicos accesibles. El 802.1x controla el acceso a la red por la creación de dos puntas de acceso virtual distintas en cada puerto. Un Punto de acceso es un puerto incontrolado; el otro es un puerto controlado. Todo el tráfico a través del puerto único está disponible para ambos Puntos de acceso. El 802.1x autentica cada dispositivo del usuario que esté conectado con un puerto del switch y asigna el puerto a un VLA N antes de que haga disponible cualquier servicio que sea ofrecido por el switch o el LAN. Hasta que se autentique el dispositivo, el control de acceso del 802.1x permite solamente el protocolo extensible authentication sobre el tráfico LAN (EAPOL) a través del puerto con el cual el dispositivo está conectado. Después de que la autenticación sea acertada, el tráfico normal puede pasar a través del puerto.

3.2 DEFINICIÓN Y ENUNCIADO DEL PROBLEMA

Actualmente en la red del Sistema Nacional de Emergencias, cualquier computadora que conecte a uno de los Switches de acceso puede tener conexión a la LAN principal. No se puede mantener los puertos apagados debido a que son utilizados dinámicamente por los usuarios, esto nos retrasaría en las labores diarias.

Realizar la implementación, validación del protocolo 802.1x en los switches de Acceso, inducción al usuario final con el proceso de conexión a la red.

3.3 PREGUNTAS DE INVESTIGACIÓN

1. ¿Cuál es el riesgo de que alguien ingrese a la red mediante puertos habilitados sin autenticación?

2. ¿Por qué usar radius server en lugar de Cisco TACACS+?
3. ¿Qué factores hacen a la red insegura?
4. ¿Por qué es importante implementar el estándar 802.1x?
5. ¿Qué factores se debe tener en cuenta al momento de implementar 802.1x?
6. ¿Tiene la empresa estrategias preventivas y planes de contingencia para minimizar los riesgos en el manejo de la información ante incidentes?

IV. OBJETIVOS

4.1 OBJETIVO GENERAL

Tener un control de acceso y de autenticación que restrinja los dispositivos desautorizados de la conexión con un LAN a través de los puertos públicos accesibles. Solo permitiendo la captura del tráfico del usuario en un primer momento, siendo redirigido a un portal cautivo en el que tendrá que introducir las credenciales necesarias.

4.2 OBJETIVOS ESPECÍFICOS

- Implementar el estándar 802.1x en Radius server para autenticar la red inalámbrica y por cable para mejorar la seguridad de la red. Controlando el acceso físico a la red basada en el estado de autenticación del cliente.
- Mejorar la seguridad, flexibilidad y capacidad de gestión.
- Permitirle al administrador de la red controlar en todo momento el inicio y final del periodo de navegación y la posibilidad de facturar en función de los recursos utilizados.

V. RESEÑA HISTÓRICA DE LA EMPRESA

Constituida en Tegucigalpa, Honduras en 2002, Dynamic Corp. ha evolucionado y mejorado constantemente y es hoy en día una de las empresas en la región con la misión de entregar soluciones corporativas con la utilización de las mejores tecnologías de información y comunicaciones para el crecimiento de las empresas e instituciones gubernamentales.

Desde su creación hemos entregado a nuestros clientes, soluciones robustas y que se adecuan a las necesidades cambiantes de las empresas públicas y privadas.

Dynamic Corp. se ha mantenido como una compañía financieramente estable con una capacidad probada para desarrollar y apoyar nuevas tecnologías innovadoras, representando una garantía de confiabilidad para nuestros clientes.

Dynamic Corp. con oficina principal en Honduras, posee una capacidad en el diseño, planificación y ejecución de proyectos en toda Centro América y el Caribe, por medio de una red de socios tecnológicos estratégicos que permiten brindar a nuestros clientes un alcance regional.

Dynamic Corp. ofrece 3 Divisiones de Soluciones, Productos y Servicios las cuales ha venido desarrollando a través de 16 años de experiencia con proyectos exitosos en cada una de ellas. Cada solución es diseñada generalmente a la medida, convirtiéndonos en un asesor corporativo que implementa soluciones tecnológicas tomando en cuenta los requerimientos y presupuestos de cada cliente.

Dynamic Corp. cuenta con personal certificado en cada vertical de negocio que le ayudara a definir su proyecto y con un musculo financiero donde podemos encontrar la mejor forma económica de hacerlo viable.

Identificación

Brindan Soluciones de Alta Seguridad basadas en Productos, Soluciones y Servicios de Identificación para distintos requerimientos. Nuestras tecnologías tienen los más altos fabricantes y estándares en la industria de la Identificación Biométrica, Soluciones de control de Acceso, Soluciones de Emisión de Documentos Seguros y todo lo que se refiere a la identificación de Personas y Seguridad, tanto a nivel Gubernamental como Corporativo.

Seguridad

La seguridad ha supuesto desde tiempo inmemorial una de las principales preocupaciones de los seres humanos. En la actualidad, y debido a la explosión de las redes de comunicación, de Internet y de las redes sociales, a la necesidad de una seguridad física se ha sumado otra de una seguridad online que tiene que ver con ese nuevo mundo virtual. Sin embargo, la importancia de la primera sigue siendo muy importante y la aportación de la tecnología es básica para mejorarla y hacerla mucho más efectiva. En las empresas e instituciones la seguridad electrónica se basa en el uso de tecnologías de última generación, lo que incluye sistemas CCTV (circuitos cerrados de televisión), controles de acceso y presencia, sistemas de intrusión, control de activos y control de acceso gestionado, centros de control de alarmas. La seguridad electrónica, de la mano de las TIC, ha experimentado un gran desarrollo en los últimos años, pero tiene todavía mucho camino por recorrer.

Ciber seguridad

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno. Puesto simple, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades.

• Reducir el riesgo empresarial. Proteger el negocio

• Aumentar la visibilidad sobre el medio ambiente

• Pasar de la respuesta reactiva a la mitigación proactiva

• Numerosas soluciones puntuales para problemas de cumplimiento normativo

5.1. VISIÓN

"Al 2021 somos líderes mundiales en soluciones innovadoras e integrales de alta tecnología, satisfaciendo a todos los clientes."

5.2. MISIÓN

"Somos un grupo corporativo sólido y sostenible en Centro América y en el Caribe, que ofrece tecnologías de avanzada de seguridad y eficiencia del sector público, privado y empresas asociadas, utilizando normas y metodologías de alta calidad fundamentados en nuestros valores."

5.3. VALORES ORGANIZACIONALES

- **Lealtad**: Apego a los principios organizacionales y humanos que procuran el bienestar común de la Empresa, Miembros y Clientes.
- **Entrega**: Cada empleado sea capaz de dar más allá de lo esperado en sus asignaciones mostrando un desempeño excepcional.
- **Innovación**: En todas las operaciones de la organización procurando siempre una mejor manera de hacer las cosas utilizando permanentemente tecnologías de información y comunicaciones.

5.4. SECTORES ATENDIDOS

Ciudades digitales / Ciudades seguras

Son un conjunto de herramientas tecnológicas, operativas y estratégicas para salvaguardar nuestras ciudades, municipios, instalaciones críticas, puertos, aeropuertos, transporte, etc., representando una ayuda altamente eficaz para que las fuerzas policiales y de administración de justicia, superen y prevengan el delito, el terrorismo y el crimen organizado, por medio de una única plataforma central, un sistema de control y comando para la gestión eficiente de Las actividades delictivas, intrusión e infiltraciones ilegales, seguridad nacional, seguridad local y municipal, y el orden público. Igualmente, nuestras soluciones de seguridad y monitoreo pueden ser aplicadas al apoyo en la prevención de situaciones médicas, de rescate, de control de desastres naturales, incendios y cuerpos de socorro, permitiendo una plataforma integral, como ya es utilizada en países del primer mundo.

Sector Privado

Para este sector dinamizante de las economías de los países ofrece una propuesta de valor al proponer soluciones a la medida en grandes proyectos como pequeños. Apoya las áreas operativas, gerencias, de seguridad, de identificación, de sistemas de información, que son adaptables a las realidades de cada empresa o corporación respaldadas por los altos niveles de satisfacción de parte de nuestros clientes en este sector.

Gobierno

Cuentan con la experiencia y el profesionalismo para poder atender la mayoría de las instancias de gobierno y sus necesidades, cabe mencionar que conocen muy bien los procesos y el respaldo que se requiere para poder atender a un sector tan demandante y con múltiples requerimientos. Con experiencias regionales en atención a este sector, dispone de los mecanismos, conocimiento operativo y mejores prácticas que permiten mucha flexibilidad en la ejecución de proyectos con gobiernos locales, municipales y centrales.

VI. MARCO TEÓRICO

6.1. REDES DE ORDENADORES

Es el conjunto de ordenadores conectados junto con un sistema de telecomunicaciones con el fin de comunicarse y compartir recursos e información.

(Clasificacion de Redes, 2018)

6.1.1. CLASIFICACIÓN DE LAS REDES

6.1.1.1. POR ALCANCE

Red de área personal (PAN)

Wireless Personal Area Networks, Red Inalámbrica de Área Personal o Red de área personal o Personal area network es una red de computadoras para la comunicación entre distintos dispositivos (tantas computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella.
(Clasificacion de Redes, 2018)

Red de área local (LAN)

Una red de área local, red local o LAN (del inglés local area network) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.
(Clasificacion de Redes, 2018)

Red de área metropolitana (MAN)

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano, sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Este tipo de redes es una versión más grande que la LAN y que normalmente se basa en una tecnología similar a esta. Las redes Man también se aplican en las organizaciones, en grupos de oficinas corporativas cercanas a una ciudad, estas no contienen elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Estas redes pueden ser públicas o privadas.

Las redes de área metropolitana, comprenden una ubicación geográfica determinada "ciudad, municipio", y su distancia de cobertura es mayor de 4 km. Son redes con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos.

(Clasificacion de Redes, 2018)

Red de área amplia (WAN)

Un área amplia o WAN (Wide Area Network) se extiende sobre un área geográfica extensa, a veces un país o un continente, y su función fundamental está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí. Para ello cuentan con una infraestructura basada en poderosos nodos de conmutación que llevan a cabo la interconexión de dichos elementos, por los que además fluyen un volumen apreciable de información de manera continua. Por esta razón también se dice que las redes WAN tienen carácter público, pues el tráfico de información que por ellas circula proviene de diferentes lugares, siendo usada por numerosos usuarios de diferentes países del mundo para transmitir información de un lugar a otro. A diferencia de las redes LAN (siglas de "local area network", es decir, "red de área local"), la velocidad a la que circulan los datos por las redes WAN suele ser menor que la que se puede alcanzar en las redes LAN. Además, las redes LAN tienen carácter

privado, pues su uso está restringido normalmente a los usuarios miembros de una empresa, o institución, para los cuales se diseñó la red.

(Clasificacion de Redes, 2018)

6.1.1.2. POR MÉTODO DE LA CONEXIÓN

6.1.1.2.1. Medios guiados

Cable de par trenzado

Es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes. Dependiendo de la red se pueden utilizar, uno, dos, cuatro o más pares trenzados.

(Blog Redes, 2015)

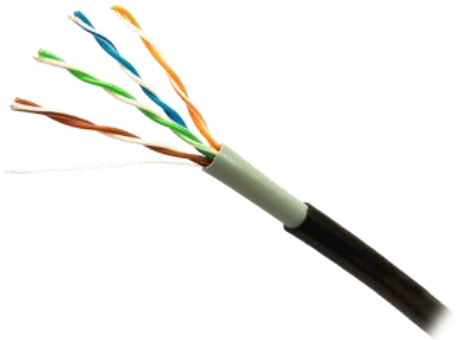

Ilustración 1. Cable de par trenzado

Cable coaxial

Se utiliza para transportar señales electromagnéticas de alta frecuencia, el cual posee un núcleo sólido (generalmente de cobre) o de hilos, recubierto por un material dieléctrico y una malla o blindaje, que sirven para aislar o proteger la señal de información contra las interferencias o ruido exterior.

(Blog Redes, 2015)

Ilustración 2. Cable coaxial

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.

(Blog Redes, 2015)

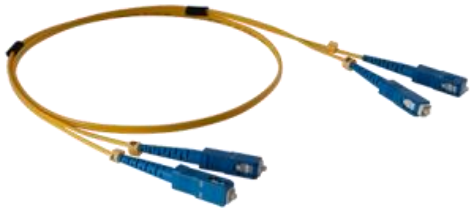

Ilustración 3. Fibra Óptica

6.1.1.2.2. Medios no guiados

Red por radio

Es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red.

(Alonso, 2009)

Red por infrarrojos

(Infrared Data Association, IrDA), permiten la comunicación entre dos nodos, usando una serie de ledes infrarrojos para ello. Se trata de emisores/receptores de ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita al otro para realizar la comunicación por ello es escasa su utilización a gran escala. No disponen de gran alcance y necesitan de visibilidad entre los dispositivos.

(Alonso, 2009)

Red por microondas

Es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. Los protocolos más frecuentes son: el IEEE 802.11b y transmite a 2,4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo); el rango de 5,4 a 5,7 GHz para el protocolo IEEE 802.11a; el IEEE 802.11n que permite velocidades de hasta 600 Mbps; etc.

(Alonso, 2009)

IEEE 802.11b

802.11b tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la

velocidad máxima de transmisión con este estándar es de aproximadamente 5,9 Mbit/s sobre TCP y 7,1 Mbit/s sobre UDP.

Los productos que usan esta versión aparecieron en el mercado a principios del 2000, ya que 802.11b es una extensión directa de la técnica de modulación definida en la norma original. El aumento dramático del rendimiento de 802.11b y su reducido precio llevó a la rápida aceptación de 802.11b como la tecnología de LAN inalámbrica definitiva.

Los dispositivos que utilizan 802.11b pueden experimentar interferencias con otros productos que funcionan en la banda de 2,4 GHz.

(Alonso, 2009)

IEEE 802.11G

802.11g, que es la evolución de 802.11b. Este utiliza la banda de 2,4 Ghz (al igual que 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del nuevo estándar lo tomó el hacer compatible ambos modelos. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación que fue dada aprox. el 20 de junio de 2003. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de más de 50 km con antenas parabólicas o equipos de radio apropiados. Existe una variante llamada 802.11g+ capaz de alcanzar los 108Mbps de tasa de transferencia. Generalmente sólo funciona en equipos del mismo fabricante ya que utiliza protocolos propietarios.

(Alonso, 2009)

IEEE 802.11n

A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física.

(Alonso, 2009)

6.1.1.3. POR RELACIÓN FUNCIONAL

Cliente-servidor

La red Cliente/Servidor es aquella red de comunicaciones en la que todos los clientes están conectados a un servidor, en el que se centralizan los diversos recursos y aplicaciones con que se cuenta; y que los pone a disposición de los clientes cada vez que estos son solicitados. Esto significa que todas las gestiones que se realizan se concentran en el servidor, de manera que en él se disponen los requerimientos provenientes de los clientes que tienen prioridad, los archivos que son de uso público y los que son de uso restringido, los archivos que son de sólo lectura y los que, por el contrario, pueden ser modificados, etc.

(Microsystem, 2009)

Igual-a-Igual (p2p)

Una red peer-to-peer (P2P) o red de pares, es una red de computadoras en la que todos o algunos aspectos de ésta funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

(Microsystem, 2009)

6.1.1.4. POR TOPOLOGÍA DE RED

Red en bus

Red cuya topología se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

(Casillas, 2009)

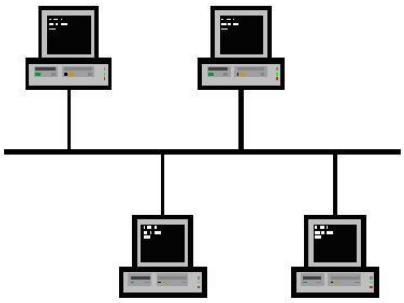

Ilustración 4. Red en bus

Red en estrella

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes.

(Casillas, 2009)

Ilustración 5. Red en estrella

Red en anillo (o doble anillo)

Topología de red en la que cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

(Casillas, 2009)

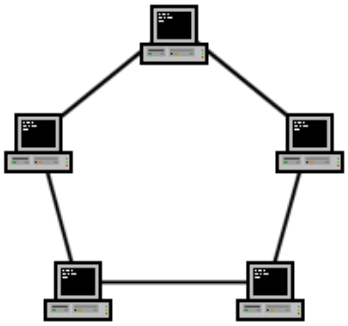

Ilustración 6. Red en anillo

Red en malla (o totalmente conexa)

La topología en malla es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

(Casillas, 2009)

Ilustración 7. Red en malla

Red en árbol

Topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

(Casillas, 2009)

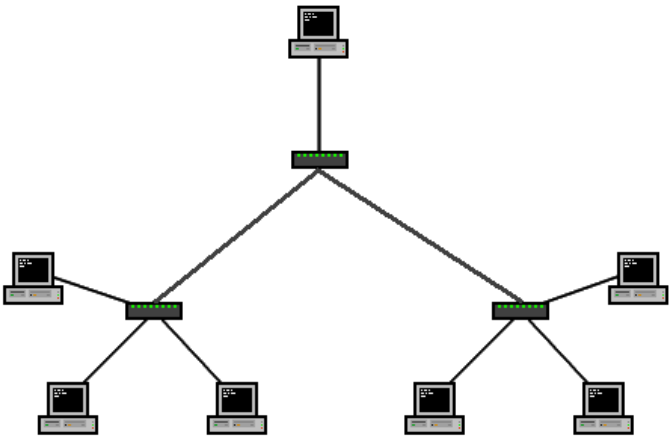

Ilustración 8. Red en árbol

Red mixta

Cualquier combinación de las anteriores.

(Casillas, 2009)

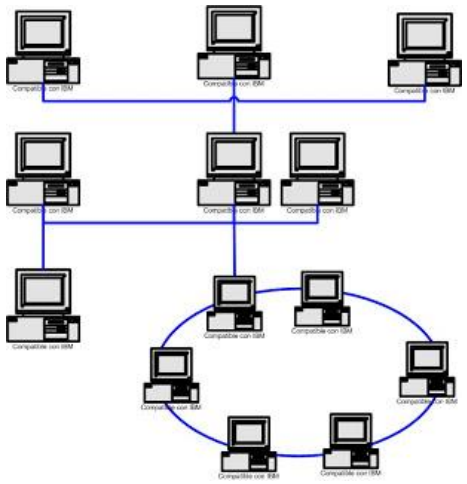

Ilustración 9. Red mixta

6.1.1.5. Por la direccionalidad de los datos

Simplex o unidireccional

Un equipo terminal de datos transmite y otro recibe.

(Diaz, 2013)

Half-duplex o semidúplex

El método o protocolo de envío de información es bidireccional pero no simultáneo bidireccional, solo un equipo transmite a la vez.

(Diaz, 2013)

Full-duplex o dúplex

Los dos equipos involucrados en la comunicación lo pueden hacer de forma simultánea, transmitir y recibir.

(Diaz, 2013)

6.1.1.6. Por grado de autentificación

Red privada

Es una red que solo puede ser usada por algunas personas y que está configurada con clave de acceso personal.
(Stalling)

Red de acceso público

Una red pública se define como una red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. Es una red de ordenadores interconectados, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.
(Stalling)

6.2. NORMAS Y ESTÁNDARES EN TELECOMUNICACIONES

6.2.1. ESTÁNDAR DE RED

Un estándar es un acuerdo común que se estableció para que la comunicación se llevara a cabo y para que los diferentes fabricantes o desarrolladores de tecnologías se fundamentaran en esto para sus trabajos y de esta forma se garantizara la operatividad de la red.

(Redes de Computadora, n.d.)

6.2.2. PROTOCOLO

Cuando dos equipos intentan establecer una comunicación deben hablar el mismo lenguaje y ponerse de acuerdo en una serie de normas. Estas normas son lo que denominamos protocolo. Protocolo es, por tanto, el conjunto de normas mutuamente aceptadas que van a regir el diálogo entre los equipos de una red.

(Redes de Computadora, n.d.)

6.2.3. ISO (ORGANIZACIÓN INTERNACIONAL PARA LA NORMALIZACIÓN)

Organización internacional que tiene a su cargo una amplia gama de estándares incluyendo aquellos referidos al networking. ISO desarrolló el modelo de referencia OSI, un modelo popular de referencia de networking. La ISO establece en julio de 1994 la norma ISO 11801 que define una instalación completa (componente y conexiones) y valida la utilización del cable de 100 Ω o 120 Ω.

(Redes de Computadora, n.d.)

6.2.3.1. Modelo de referencia OSI

El modelo de referencia OSI intenta crear una estructura de manera que el problema de la comunicación entre equipos pueda ser abordado del mismo modo por todas aquellas personas encargadas de desarrollar hardware y software para una red.

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

Evidentemente, este modelo se tuvo que crear debido a la complejidad del problema y, aunque

es simplemente un marco de referencia teórico, ha permitido y potenciado el extraordinario desarrollo que se está dando tanto en las LAN como en Internet.

(Redes de Computadora, n.d.)

Capas del modelo OSI

Las siete capas del modelo de referencia OSI El problema de trasladar información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo. Las siete capas del modelo de referencia OSI son:

Capa 7: La capa de aplicación

Capa 6: La capa de presentación

Capa 5: La capa de sesión

Capa 4: La capa de transporte

Capa 3: La capa de red

Capa 2: La capa de enlace de datos

Capa 1: La capa física

Ilustración 10. Capas del modelo OSI

Funciones de cada capa

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. A continuación, presentamos una breve descripción de cada capa del modelo de referencia OSI tal como aparece en la figura.

(El Modelo OSI, n.d.)

Capa 7: La capa de aplicación La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos. Si desea recordar a la Capa 7 en la menor cantidad de palabras posible, piense en los navegadores de Web.
(El Modelo OSI, n.d.)

Capa 6: La capa de presentación La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común. Si desea recordar la Capa 6 en la menor cantidad de palabras posible, piense en un formato de datos común.

(El Modelo OSI, n.d.)

Capa 5: La capa de sesión Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación. Si desea recordar la Capa 5 en la menor cantidad de palabras posible, piense en diálogos y conversaciones.
(El Modelo OSI, n.d.)

Capa 4: La capa de transporte La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos. La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte. Si desea recordar a la Capa 4 en la menor cantidad de palabras posible, piense en calidad de servicio y confiabilidad.
(El Modelo OSI, n.d.)

Capa 3: La capa de red La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Si desea recordar la Capa 3 en la menor cantidad de palabras posible, piense en selección de ruta, direccionamiento y enrutamiento.
(El Modelo OSI, n.d.)

Capa 2: La capa de enlace de datos La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Si desea recordar la Capa 2 en la menor cantidad de palabras posible, piense en tramas y control de acceso al medio.

(El Modelo OSI, n.d.)

Capa 1: La capa física La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física. Si desea recordar la Capa 1 en la menor cantidad de palabras posible, piense en señales y medios
(El Modelo OSI, n.d.)

Características fundamentales del modelo OSI

En el modelo de referencia OSI se pueden distinguir tres características fundamentales:

- Arquitectura, en la cual se definen los aspectos básicos de los sistemas abiertos.
- Servicios, proporcionados por un nivel al nivel inmediatamente superior.
- Protocolos, es decir, la información de control transmitida entre los sistemas y los procedimientos necesarios para su interpretación.

(El Modelo OSI, n.d.)

6.2.4. NORMAS Y ESTÁNDARES EN TELECOMUNICACIONES IEEE

Corresponde a las siglas de (Institute of Electrical and Electronics Engineers) en español Instituto de Ingenieros Electricistas y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías, como ingenieros electricistas, ingenieros en electrónica, científicos de la computación, ingenieros en informática, ingenieros en biomédica, ingenieros en telecomunicación e ingenieros en mecatrónica.

(El Modelo OSI, n.d.)

6.2.4.1. Modelo IEEE

Con un fin similar al que inspiró a la ISO para crear el modelo OSI, el Institute of Electrical and Electronic Engineers desarrolló una serie de estándares de comunicación de dispositivos para redes LAN y WAN de manera que se pudieran compatibilizar los productos de las distintas empresas orientados a este sector de comunicación. Así, se creó el Comité 802 que elaboró, entre otros, el estándar 802.3, siendo esta familia de protocolos la más extendida en la actualidad, afectando a los niveles físicos y de enlace del modelo OSI en redes LAN.

(Overview and Guide to the IEEE 802 , 2012)

1. Nivel físico: Cumpliría exactamente las mismas funciones que se le asignan a este nivel en el modelo OSI.

(Overview and Guide to the IEEE 802 , 2012)

2. Nivel de enlace: El estándar IEEE subdivide este nivel en dos capas:

    2.1 Control de enlace lógico (LLC, Logical Link Control): Maneja los distintos tipos de servicios de comunicación.

    2.2 Control de acceso al medio (MAC, Media Access Control): Aporta la dirección física del equipo y las herramientas para el uso del medio.

El resto de los niveles del sistema OSI no los contempla. La IEEE es la responsable de la elaboración de la mayoría de los estándares creados hasta este momento y que están vigentes en la comunicación de ordenadores. Por ejemplo, el IEEE 802.11a, 802.11b, 802.11g para comunicación inalámbrica, IEEE 802.5 para redes token ring, el IEEE 802.3u para redes fast ethernet, etc.
(Overview and Guide to the IEEE 802 , 2012)

6.2.4.2 IEEE 802

IEEE 802 fue un proyecto creado en febrero de 1980 paralelamente al diseño del Modelo OSI. Se desarrolló con el fin de crear estándares para que diferentes tipos de tecnologías pudieran integrarse y trabajar juntas. El proyecto 802 define aspectos relacionados con el cableado físico y la transmisión de datos.

(Overview and Guide to the IEEE 802 , 2012)

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, algunos de los cuales son muy conocidos: Ethernet (IEEE 802.3), o Wi-Fi (IEEE 802.11). Está, incluso, intentando estandarizar Bluetooth en el 802.15 (IEEE 802.15).

(Overview and Guide to the IEEE 802 , 2012)

Se centra en definir los niveles más bajos (según el modelo de referencia OSI o sobre cualquier otro modelo). Concretamente subdivide el segundo nivel, el de enlace, en dos subniveles: el de Enlace Lógico (LLC), recogido en 802.2, y el de Control de Acceso al Medio (MAC), subcapa de la capa de Enlace Lógico. El resto de los estándares actúan tanto en el Nivel Físico, como en el subnivel de Control de Acceso al Medio.

(Overview and Guide to the IEEE 802 , 2012)

Estándar IEEE 802

Nombre	Descripción	Nota
IEEE 802.1	Normalización de interfaz	
802.1d	*Spanning Tree Protocol*	
802.1p	Asignación de Prioridades de tráfico	
802.1q	*Virtual Local Area Networks* (VLAN)	
802.1x	Autenticación en redes LAN	
802.1aq	*Shortest Path Bridging* (SPB)	
IEEE 802.2	Control de enlace lógico LLC	Activo
IEEE 802.3	CSMA / CD (ETHERNET)	
IEEE 802.3a	Ethernet delgada 10Base2	
IEEE 802.3c	Especificaciones de Repetidor en Ethernet a 10 Mbps	
IEEE 802.3i	Ethernet de par trenzado 10BaseT	
IEEE 802.3j	Ethernet de fibra óptica 10BaseF	
IEEE 802.3u	Fast Ethernet 100BaseT	

Nombre	Descripción	Nota
IEEE 802.3z	Gigabit Ethernet parámetros para 1000 Mbps	
IEEE 802.3ab	Gigabit Ethernet sobre 4 pares de cable UTP Cat5e o superior	
IEEE 802.3ae	10 Gigabit Ethernet	
IEEE 802.4	Token bus LAN	Disuelto
IEEE 802.5	Token ring LAN (topología en anillo)	Inactivo
IEEE 802.6	Redes de Área Metropolitana (MAN) (ciudad) (fibra óptica)	Disuelto
IEEE 802.7	Grupo Asesor en Banda ancha	Disuelto
IEEE 802.8	Grupo Asesor en Fibras Ópticas	Disuelto
IEEE 802.9	Servicios Integrados de red de Área Local (redes con voz y datos integrados)	Disuelto
IEEE 802.10	Seguridad de red	Disuelto
IEEE 802.11	Redes inalámbricas WLAN. (Wi-Fi)	
IEEE 802.12	Acceso de Prioridad por demanda 100 Base VG-Any Lan	Disuelto
IEEE 802.13	Se ha evitado su uso.	Sin uso

Nombre	Descripción	Nota
IEEE 802.14	Módems de cable	Disuelto
IEEE 802.15	WPAN (Bluetooth)	
IEEE 802.16	Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX)	
IEEE 802.17	Anillo de paquete elástico script	
IEEE 802.18	Grupo de Asesoría Técnica sobre Normativas de Radio	En desarrollo a día de hoy
IEEE 802.19	Grupo de Asesoría Técnica sobre Coexistencia	
IEEE 802.20	*Mobile Broadband Wireless Access*	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	*Wireless Regional Area Network*	

Tabla 1. Estándares IEEE 802

(Tanenbaum)

6.2.5. SWITCH

Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

(Gonzales, 2013)

6.2.5.1. ¿Para qué sirve un switch?

La función básica de un switch es la de unir o conectar dispositivos en red. Es importante tener claro que un switch no proporciona por si solo conectividad con otras redes tampoco proporciona conectividad con Internet. Para ello es necesario un router.

(Gonzales, 2013)

6.2.5.2. Características básicas de los switches

Puertos

Los puertos son los elementos del switch que permiten la conexión de otros dispositivos al mismo. El número de puertos es una de las características básicas de los switches.

El estándar Ethernet admite básicamente dos tipos de medios de transmisión cableados: el cable de par trenzado y el cable de fibra óptica. El conector utilizado para cada tipo lógicamente es diferente así que otro dato a tener en cuenta es de qué tipo son los puertos. Normalmente los switches básicos sólo disponen de puertos de cable de par trenzado (cuyo conector se conoce como RJ-45) y los más avanzados incluyen puertos de fibra óptica (el conector más frecuente, aunque no el único es el de tipo SC).

(Gonzales, 2013)

Ilustración 11. Switch con puertos RJ-45 y SC

Velocidad

Dado que Ethernet permite varias velocidades y medios de transmisión, otra de las características destacables sobre los puertos de los switches es precisamente la velocidad a la que pueden trabajar sobre un determinado medio de transmisión. Podemos encontrar puertos definidos como 10/100, es decir, que pueden funcionar bajo los estándares 10BASE-T (con una velocidad de 10 Mbps) y 100BASE-TX (velocidad: 100 Mbps). Otra posibilidad es encontrar puertos 10/100/1000, es decir, añaden el estándar 1000BASE-T (velocidad 1000 Mbps). También se pueden encontrar puertos que utilicen fibra óptica utilizando conectores hembra de algún formato para fibra óptica. Existen puertos 100BASE-FX y 1000BASE-X.

Por último, los switches de altas prestaciones pueden ofrecer puertos que cumplan con el estándar 10GbE, tanto en fibra como en cable UTP.

(Gonzales, 2013)

Gestión y configuración

La función básica que llevan a cabo los switches, que es la conmutación de tramas Ethernet, no necesita ninguna configuración manual. Una de las características incluidas en el estándar

Ethernet (concretamente en la especificación IEEE 802.3u) es la auto negociación. Esta función permite que se establezca un diálogo entre el switch y cualquier equipo que se conecte a uno de sus puertos para que "negocien" los parámetros de la comunicación de forma transparente al usuario.

Sin embargo, las funciones avanzadas que ofrecen algunos modelos (como, por ejemplo, la configuración de redes VLAN) sí requieren una configuración manual. A los switches que proporcionan mecanismos de configuración y gestión se les conoce como switches gestionables (managed switches).

(Gonzales, 2013)

El acceso a la configuración de dichos switches se puede hacer, o bien por un puerto especial de configuración, o por un servicio web interno que proporciona el propio switch. En el primer caso, es necesario conectar un PC a dicho puerto y acceder mediante algún software específico (como por ejemplo un programa de terminal de comandos). En el segundo caso basta con utilizar un navegador web en algún PC conectado en un puerto Ethernet del switch. El acceso a la interfaz de configuración del switch requiere que se configure en el mismo una dirección IP dentro del rango de la red donde esté conectado.

(Gonzales, 2013)

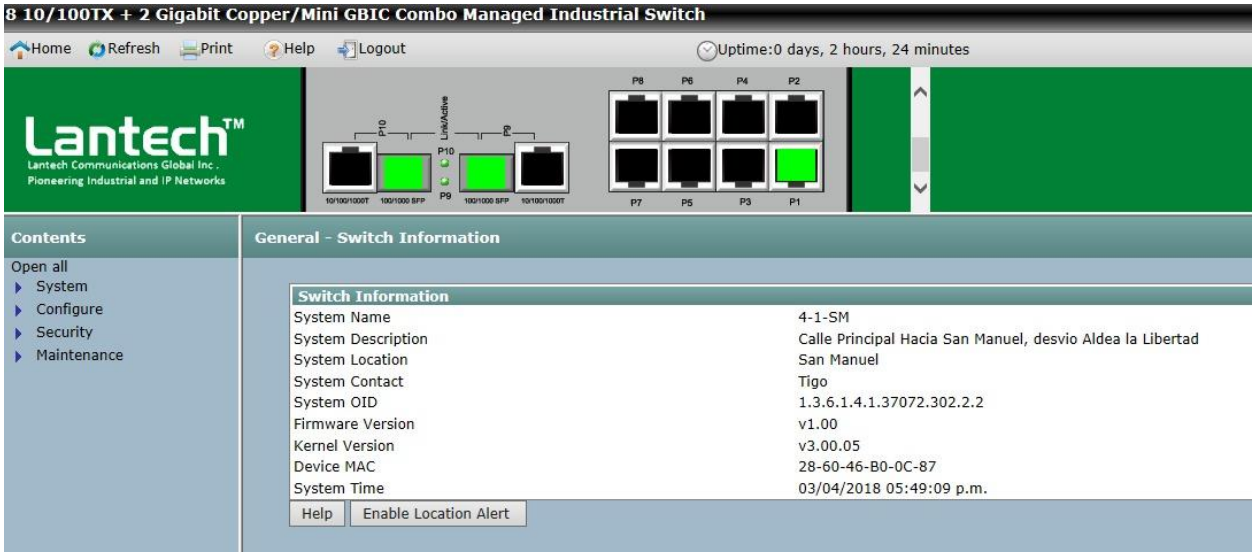

Ilustración 12. Pantalla de configuración de un switch gestionable

Algunas de las características que suelen incluir los switches gestionables:

- Gestión de VLAN
- Monitorización de puertos (Port Mirroring)
- Agregación de enlaces (Link Aggregation / Port Trunking)
- Seguridad IEEE 802.1X
- Control de bucles: Spanning Tree

(Gonzales, 2013)

6.2.6. IEEE 802.1X

El estándar IEEE 802.1X define el control de acceso a la red basado en puerto que se usa para proporcionar acceso cableado autenticado a las redes Ethernet. Este control de acceso a la red basado en puerto usa las características físicas de la infraestructura de red de área local (LAN) conmutada para autenticar los dispositivos conectados a un puerto de la LAN. Se puede denegar el acceso al puerto si se produce un error en el proceso de autenticación. Si bien este estándar se diseñó para redes Ethernet cableadas, también se ha adaptado para usarlo en LAN inalámbricas 802.11.

El 802.1x se comprende de tres componentes primarios. Se refiere cada uno como una entidad del acceso del puerto (PAE).

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

Supplicant

Dispositivo del cliente que pide el acceso a la red, por ejemplo, los Teléfonos IP y los PC asociados.

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

Authenticator

Dispositivo de red que facilita los pedidos de autorización del supplicant, por ejemplo, el Cisco Catalyst 3560.

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

Servidor de autenticación

Un Remote Authentication Dial-In User Server (RADIUS), que proporciona el servicio de autenticación, por ejemplo, Cisco Secure Access Control Server.

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

6.2.7. CONMUTADORES ETHERNET CABLEADOS COMPATIBLES CON IEEE 802.1X

Para implementar el acceso cableado 802.1X, debe instalar y configurar uno o varios conmutadores Ethernet compatibles con 802.1X en la red. Los conmutadores deben ser compatibles con el protocolo Servicio de autenticación remota telefónica de usuario (RADIUS). Cuando se implementan conmutadores compatibles con 802.1X y RADIUS en una infraestructura de RADIUS (con un servidor RADIUS, como un servidor NPS), estos se denominan clientes RADIUS.

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

6.2.8. ETHERNET IEEE 802.3

IEEE 802.3 es una colección de estándares que define el nivel 1 (nivel físico) y el nivel 2 (Media Access Control (MAC) del nivel de vínculo de datos) de Ethernet cableado. Por lo general, Ethernet 802.3 se implementa en una LAN y en algunas aplicaciones de red de área extensa (WAN).

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

6.2.9. SERVIDOR DE DIRECTIVAS DE REDES

El Servidor de directivas de redes (NPS) le permite configurar y administrar de manera centralizada las directivas de red mediante los tres componentes siguientes: servidor RADIUS, proxy RADIUS y servidor de directivas de Protección de acceso a redes (NAP). NPS se requiere para implementar el acceso cableado 802.1X.

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

6.2.10. PROTOCOLO AAA

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y contabilización (en inglés, Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

Por lo general, Ethernet 802.3 se implementa en una LAN y en algunas aplicaciones de red de área extensa (WAN).

(Comparación de TACACS+ y RADIUS, 2012)

6.2.10.1. Autenticación

La autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente y la segunda un servidor. La Autenticación se consigue mediante la presentación de una propuesta de identidad (un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, o los números de teléfono en la identificación de llamadas.

(Comparación de TACACS+ y RADIUS, 2012)

6.2.10.2. Autorización

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.

(Comparación de TACACS+ y RADIUS, 2012)

6.2.10.3. Contabilización

La contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios. 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 (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.

(Comparación de TACACS+ y RADIUS, 2012)

6.2.10.4. Lista de protocolos AAA

- RADIUS
- DIAMETER
- TACACS
- TACACS+

(Lopez, 2015)

6.2.10.5. Proceso AAA IEEE 802.1x

Paso 1 Un usuario se conecta a un puerto en el interruptor.

Paso 2 Autenticación se realiza.

Paso 3 La asignación de VLAN está habilitada, según corresponda, en función de la configuración del servidor RADIUS.

Paso 4 El interruptor envía un mensaje de inicio a un servidor de contabilidad.

Paso 5 Se realiza una nueva autenticación, según sea necesario.

Paso 6 El conmutador envía una actualización de contabilidad provisional al servidor de contabilidad que se basa en el resultado de la nueva autenticación.

Paso 7 El usuario se desconecta del puerto.

Paso 8 El conmutador envía un mensaje de detención al servidor de contabilidad.

(Lopez, 2015)

6.2.11. CERTIFICADOS DE SERVIDOR

La implementación del acceso cableado requiere certificados de servidor para cada servidor NPS que realice la autenticación 802.1X.
(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

Un certificado de servidor es un documento digital que se usa normalmente para la autenticación y para ayudar a proteger la información en redes abiertas. Un certificado enlaza de manera segura una clave pública a la entidad que contiene la clave privada correspondiente. Los certificados se firman digitalmente por una entidad de certificación (CA) emisora y pueden emitirse para un usuario, un equipo o un servicio.

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

Una CA es una entidad responsable de establecer y garantizar la autenticidad de las claves públicas que pertenecen a firmantes (por lo general, usuarios o equipos) o a otras CA. Entre las actividades de una CA, se pueden incluir el enlace de claves públicas a nombres distintivos (DN) mediante certificados firmados, la administración de números de serie de certificados y la revocación de certificados.

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

Servicios de certificados de Active Directory (AD CS) es un rol del servidor de Windows Server 2012 que emite certificados como una CA de red. Una estructura de certificados de AD CS, también denominada infraestructura de clave pública (PKI), proporciona servicios personalizables para emitir y administrar certificados para empresas.

(Introducción al acceso inalámbrico autenticado mediante 802.1X, n.d.)

6.2.12. EAP

El Protocolo de autenticación extensible (EAP) extiende el Protocolo punto a punto (PPP) permitiendo métodos de autenticación adicionales que usan intercambios de credenciales y de información de longitudes arbitrarias. Con la autenticación EAP, tanto el cliente de acceso a redes como el autenticador (por ejemplo, un servidor NPS) deben admitir el mismo tipo de EAP para que la autenticación se lleve a cabo correctamente.

(Microsoft, 2018)

6.2.13. RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE)

El protocolo de servicio de usuario de acceso telefónico de autenticación remota (RADIUS) fue desarrollado por Livingston Enterprises, Inc., como un protocolo de autenticación y contabilidad del servidor de acceso.

RADIUS comprende tres elementos:

- Un protocolo con un formato de trama que utiliza el User Datagram Protocol (UDP) /IP.

- Un servidor.
- Un cliente.

La comunicación entre un servidor de acceso a la red (NAS) y un servidor RADIUS se basa en el Protocolo de datagramas de usuario (UDP). En general, el protocolo RADIUS se considera un servicio sin conexión. Los problemas relacionados con la disponibilidad del servidor, la retransmisión y los tiempos de espera son manejados por los dispositivos habilitados para RADIUS en lugar del protocolo de transmisión.

(¿Cómo el RADIUS trabaja?, 2006)

RADIUS es un protocolo cliente / servidor. El cliente RADIUS suele ser un NAS y el servidor RADIUS suele ser un proceso daemon que se ejecuta en una máquina UNIX o Windows NT. El cliente pasa información del usuario a servidores RADIUS designados y actúa sobre la respuesta que se devuelve. Los servidores RADIUS reciben solicitudes de conexión de usuarios, autentican al usuario y luego devuelven la información de configuración necesaria para que el cliente entregue el servicio al usuario. Un servidor RADIUS puede actuar como un cliente proxy para otros servidores RADIUS u otros tipos de servidores de autenticación.

(¿Cómo el RADIUS trabaja?, 2006)

6.2.13.1. Autenticación y autorización

El servidor RADIUS puede admitir una variedad de métodos para autenticar a un usuario. Cuando se proporciona con el nombre de usuario y la contraseña original dados por el usuario, puede admitir PPP, PAP o CHAP, inicio de sesión de UNIX y otros mecanismos de autenticación.

(¿Cómo el RADIUS trabaja?, 2006)

Por lo general, un inicio de sesión de usuario consiste en una consulta (Solicitud de acceso) desde el NAS al servidor RADIUS y una respuesta correspondiente (Access-Accept o Access-Reject) desde el servidor. El paquete de solicitud de acceso contiene el nombre de usuario, la contraseña

cifrada, la dirección IP NAS y el puerto. La implementación temprana de RADIUS se realizó utilizando el número de puerto UDP 1645, que entra en conflicto con el servicio "datametrics". Debido a este conflicto, RFC 2865 asignó oficialmente el número de puerto 1812 para RADIUS. La mayoría de los dispositivos y aplicaciones de Cisco ofrecen soporte para cualquier conjunto de números de puerto. El formato de la solicitud también proporciona información sobre el tipo de sesión que el usuario desea iniciar. Por ejemplo, si la consulta se presenta en modo de caracteres, la inferencia es "Tipo de servicio = Usuario-Exec", pero si la solicitud se presenta en modo de paquete PPP, la inferencia es". Cuando el servidor RADIUS recibe la solicitud de acceso del NAS, busca en una base de datos el nombre de usuario que figura en la lista. Si el nombre de usuario no existe en la base de datos, se carga un perfil predeterminado o el servidor RADIUS envía inmediatamente un mensaje de rechazo de acceso. Este mensaje de rechazo de acceso puede ir acompañado de un mensaje de texto que indique el motivo del rechazo.

(¿Cómo el RADIUS trabaja?, 2006)

En RADIUS, la autenticación y la autorización se combinan. Si se encuentra el nombre de usuario y la contraseña es correcta, el servidor RADIUS devuelve una respuesta de aceptación de acceso, que incluye una lista de pares de atributos y valores que describen los parámetros que se utilizarán para esta sesión. Los parámetros típicos incluyen el tipo de servicio (shell o enmarcado), tipo de protocolo, dirección IP para asignar al usuario (estático o dinámico), lista de acceso para aplicar, o una ruta estática para instalar en la tabla de enrutamiento NAS. La información de configuración en el servidor RADIUS define qué se instalará en el NAS.

(¿Cómo el RADIUS trabaja?, 2006)

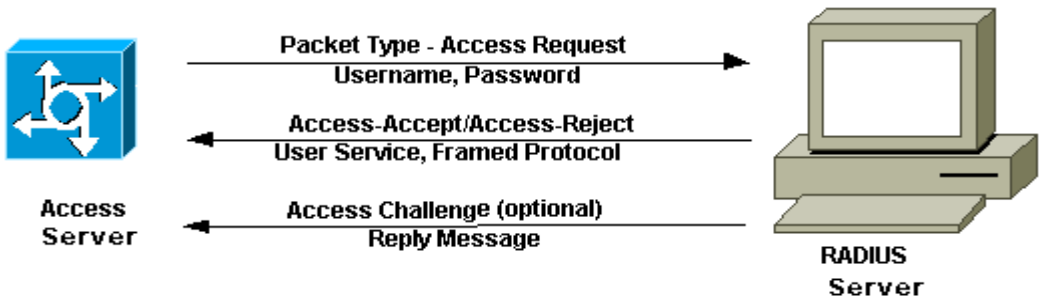

Ilustración 13. Secuencia de autenticación y autorización de RADIUS

6.2.13.2. Contabilidad

Las características contables del protocolo RADIUS se pueden usar independientemente de la autenticación o autorización RADIUS. Las funciones de contabilidad de RADIUS permiten que los datos se envíen al inicio y al final de las sesiones, lo que indica la cantidad de recursos (como el tiempo, los paquetes, los bytes, etc.) utilizados durante la sesión. Un proveedor de servicios de Internet (ISP) puede usar el software de control de acceso y contabilidad RADIUS para cumplir con las necesidades especiales de seguridad y facturación. El puerto de contabilidad para RADIUS para la mayoría de los dispositivos de Cisco es 1646, pero también puede ser 1813.
(¿Cómo el RADIUS trabaja?, 2006)

Las transacciones entre el cliente y el servidor RADIUS se autentican mediante el uso de un secreto compartido, que nunca se envía a través de la red. Además, las contraseñas de los usuarios se envían cifradas entre el cliente y el servidor RADIUS para eliminar la posibilidad de que alguien fisgoneando en una red insegura pueda determinar la contraseña de un usuario.

(¿Cómo el RADIUS trabaja?, 2006)

6.2.14. COMPARACIÓN DE TACACS + Y RADIUS

6.2.14.1. UDP y TCP

RADIUS utiliza UDP mientras que TACACS+ utiliza TCP. El TCP ofrece varias ventajas en comparación con el UDP. TCP ofrece un transporte orientado por conexión, mientras que UDP ofrece el mejor esfuerzo para entregar. RADIUS necesita variables programables adicionales tales como los intentos de retransmisión y tiempos de espera para compensar el transporte de producto de un esfuerzo razonable, pero carece del nivel de soporte incluido que ofrece un transporte TCP:

- El uso del TCP proporciona un reconocimiento independiente acerca de que se ha recibido una solicitud, dentro (aproximadamente) del trayecto de ida y vuelta (RTT),

independientemente de la carga que soporte el mecanismo de autenticación de segundo plano y de su velocidad (un reconocimiento de TCP).

- TCP proporciona una indicación inmediata de un servidor caído o que no funciona a través de un reinicio (RST). Puede determinar cuándo un servidor falla y vuelve a estar en servicio si utiliza las conexiones TCP de larga duración. UDP no puede indicar la diferencia entre un servidor desactivado, uno lento y uno inexistente.
- Mediante las señales de mantenimiento de TCP, las caídas del servidor pueden ser detectadas fuera de banda con peticiones actuales. Se pueden mantener conexiones a servidores múltiples simultáneamente, y sólo debe enviar mensajes a los que están activos y en funcionamiento.
- TCP permite mayor ampliación y se adapta a las redes en crecimiento y congestionadas.

(Comparación de TACACS+ y RADIUS, 2012)

6.2.14.2. Cifrado de Paquetes

RADIUS sólo cifra la contraseña en el paquete de solicitud de acceso, del cliente al servidor. El resto del paquete no está cifrado. Otra información, tal como el nombre de usuario, los servicios autorizados, y la cuenta, pueden capturarse a través de una tercera parte.

(Comparación de TACACS+ y RADIUS, 2012)

TACACS+ cifra todo el cuerpo del paquete, pero deja un encabezado estándar de TACACS+. Dentro del encabezado se encuentra un campo que indica si el cuerpo se ha cifrado o no. Para facilitar el debugging, resulta útil que el cuerpo de los paquetes no esté cifrado. Sin embargo, durante el funcionamiento normal, el cuerpo del paquete se cifra completamente para lograr comunicaciones más seguras.

(Comparación de TACACS+ y RADIUS, 2012)

6.2.14.3. Autenticación y autorización

RADIUS combina autenticación y autorización. Los paquetes access-accept enviados por el servidor de RADIUS al cliente contienen la información de autorización. Esto dificulta la tarea de desacoplar la autenticación y autorización.

(Comparación de TACACS+ y RADIUS, 2012)

TACACS+ usa la arquitectura AAA, la que separa a AAA. Esto permite soluciones de autenticación separada que pueden todavía usar TACACS+ para autorización y conteo. Por ejemplo, con TACACS+, es posible utilizar la autenticación de Kerberos y la autorización TACACS+ y el conteo. Después de que un NAS se autentique en un servidor de Kerberos, solicita la información de autorización de un servidor TACACS+ sin tener que volver a autenticarse. El NAS le informa al servidor TACACS+ que se ha autenticado de manera exitosa en un servidor Kerberos y luego el servidor le proporciona información de autorización.

Durante una sesión, si se requiere una verificación de autorización adicional, el servidor de acceso verifica con un servidor TACACS+ para determinar si el usuario tiene permiso para utilizar un comando determinado. Esto permite un mayor control de los comandos que pueden ejecutarse en el servidor de acceso mientras se desconecta del mecanismo de autenticación.

6.2.14.4. Tráfico

Ejemplo de tráfico de TACACS+

En este ejemplo se asume que la autenticación del inicio de sesión, la autorización exec, la autorización de comandos, el exec iniciar-detener y los comandos fueron implementados con TACACS cuando un usuario se conecta mediante Telnet a un router, ejecuta un comando y sale del router (no están disponibles otros servicios de administración):

(Comparación de TACACS+ y RADIUS, 2012)

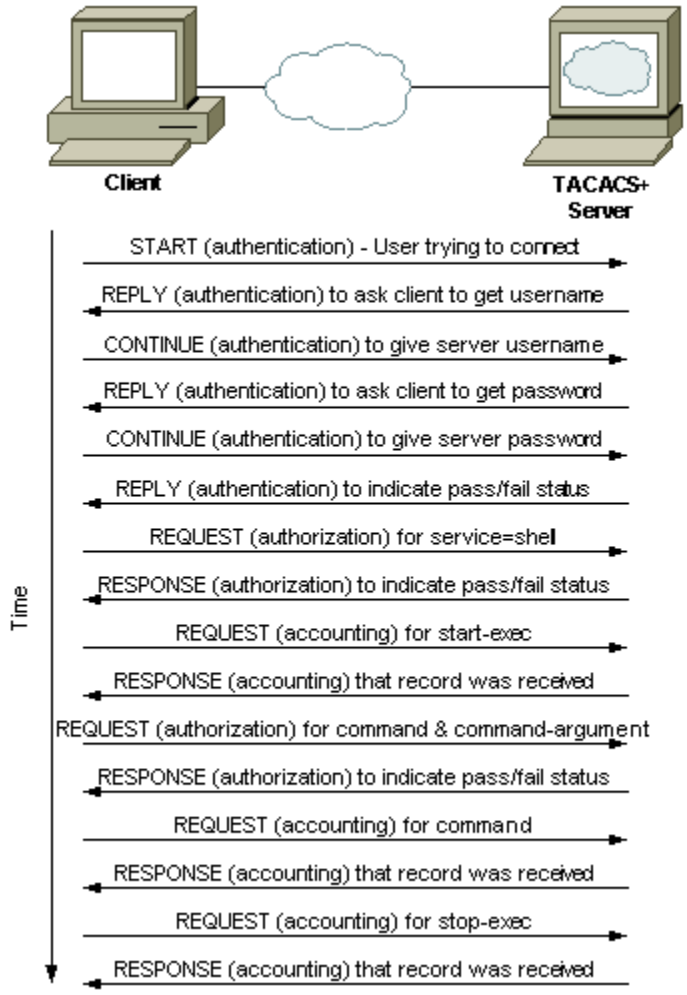

Ilustración 14. Trafico en TACACS+

Ejemplo de tráfico de RADIUS

En este ejemplo se asume que las cuentas de autenticación de usuario, la autorización exec y el exec iniciar-detener fueron implementadas con RADIUS cuando un usuario se conecta mediante Telnet a un router ejecuta un comando y sale del router (no están disponibles otros servicios de administración):

(Comparación de TACACS+ y RADIUS, 2012)

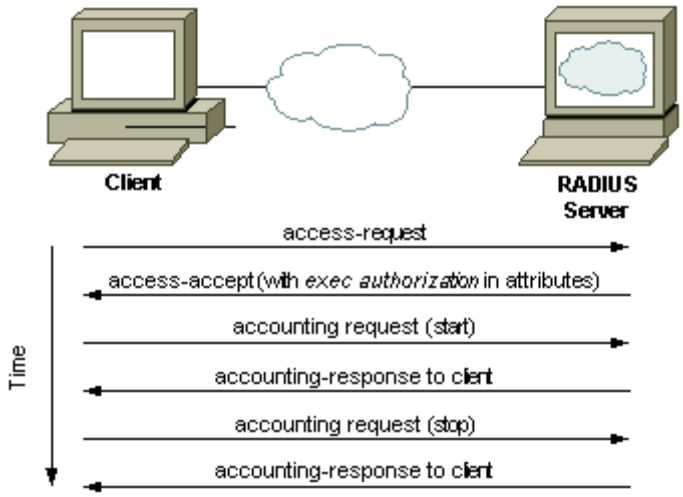

Ilustración 15. Trafico en Radius

VII. METODOLOGÍA

7.1. VARIABLES DE ESTUDIO

Para realizar la aplicación de un método de salvaguardar los puertos se toman en cuenta diversas variables que juegan un papel muy importante en el desempeño y seguridad de la red, estas variables se describen a continuación:

- Cantidad de puertos
- Throughput
- Frecuencia de riesgos a los recursos de información
- Incidencias de seguridad por los usuarios

7.2. ENFOQUE Y MÉTODOS

El tema de la seguridad de la información en las redes internas de las empresas es importante por las amenazas a los recursos de su información, por tanto, la metodología ha sido la consulta a expertos del área de Tecnología de Información y Redes de la empresa, el cual fue el guía en esta implementación.

Para lograr el cumplimiento de los objetivos de la investigación, se acude al empleo de técnicas de investigación. En el trabajo de campo, procesamiento y análisis de los resultados obtenidos fue necesario el uso de las herramientas de aplicación como Microsoft Office, de la misma forma para la preparación y presentación del informe definitivo.

7.3. MATERIALES

Microsoft Office

Herramientas de simulación

7.4. TÉCNICAS EN INSTRUMENTOS APLICADOS

Recopilación de datos

El cuestionario y la entrevista se aplicó al personal experto de Redes de la empresa, la cual estableció las consecuencias lógicas de los objetivos y variables de estudio planteados.

Así como también un diagrama de flujo donde se analiza el funcionamiento del estándar 802.1x.

7.5. FUENTES DE INFORMACIÓN

Una de las fuentes principales de información fue el ingeniero encargado del área de redes de la empresa. Así como también lo fueron libros, internet y NetAcad Cisco.

VIII. CRONOLOGÍA

Actividades	Semanas									
	1	2	3	4	5	6	7	8	9	10
Inducción en el data center										
Asignación de tareas										
Inducción de las configuraciones de los equipos										
Investigación sobre IEEE 802.1X Y Radius										
Pruebas realizadas con Radius										
Configuraciones										
Periodo de prueba										
Implementación										
Evaluación de la implementación										

Tabla 1. Cronograma de Actividades

IX. RESULTADOS Y ANÁLISIS

El proyecto asignado fue realizado en el área de data center, en el que se implementó el estándar IEEE 802.1x como resultado de la inseguridad de los puertos para tener un mejor control del acceso a los mismos.

El estándar IEEE 802.1x define un protocolo de autenticación y control de acceso basado en cliente-servidor que evita que los clientes se conecten a una LAN a través de puertos de acceso público a menos que estén autenticados. El servidor de autenticación autentica cada cliente conectado a un puerto de conmutador antes de poner a disposición los servicios ofrecidos por el conmutador o la LAN.

Hasta que el cliente sea autenticado, el control de acceso IEEE 802.1x solo permite el Protocolo de Autenticación Extensible sobre LAN (EAPOL), el Protocolo de Descubrimiento de Cisco (CDP) y el Protocolo de Árbol de Extensión (STP) a través del puerto al que está conectado el cliente. Después de la autenticación, el tráfico normal puede pasar por el puerto.

Roles del dispositivo

Con la autenticación basada en puertos IEEE 802.1x, los dispositivos en la red tienen roles específicos, como se muestra en la Figura.

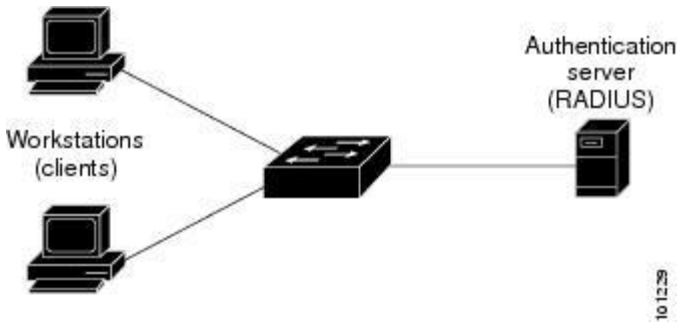

Ilustración 16. Roles del dispositivo IEEE 802.1X

Cliente: el dispositivo (estación de trabajo) que solicita acceso a la LAN y cambia de servicio y responde a las solicitudes del conmutador. La estación de trabajo debe ejecutar un software cliente compatible con IEEE 802.1x, como el que se ofrece en el sistema operativo Microsoft Windows XP.

Servidor de autenticación: realiza la autenticación real del cliente. El servidor de autenticación valida la identidad del cliente y notifica al conmutador si el cliente está autorizado o no para acceder a la LAN y cambiar de servicio. Como el conmutador actúa como proxy, el servicio de autenticación es transparente para el cliente. En esta versión, el sistema de seguridad RADIUS con Extensiones de Protocolo Extensible de Autenticación (EAP) es el único servidor de autenticación compatible.

• Interruptor (interruptor de borde o punto de acceso inalámbrico): controla el acceso físico a la red en función del estado de autenticación del cliente. El conmutador actúa como intermediario (proxy) entre el cliente y el servidor de autenticación, solicitando información de identidad del cliente, verificando esa información con el servidor de autenticación y retransmitiendo una respuesta al cliente. El conmutador incluye el cliente RADIUS, que se encarga de encapsular y descapsular los cuadros EAP e interactuar con el servidor de autenticación.

Cuando el conmutador recibe tramas EAPOL y las retransmite al servidor de autenticación, el encabezado Ethernet se elimina y la trama EAP restante se vuelve a encapsular en el formato RADIUS. Las tramas EAP no se modifican durante la encapsulación, y el servidor de autenticación debe admitir EAP dentro del formato de trama nativo. Cuando el conmutador recibe tramas del servidor de autenticación, se elimina el encabezado de trama del servidor, dejando la trama EAP, que luego se encapsula para Ethernet y se envía al cliente.

Los dispositivos que se usaron para actuar como intermediarios fueron los Catalyst 3750-E, Catalyst 3560-E y un punto de acceso inalámbrico.

Como punto de acceso inalámbrico se eligió el Cisco WAP321 el cual ejecutan un software que admite el cliente RADIUS y la autenticación IEEE 802.1x.

Proceso de Autenticación

Cuando la autenticación basada en puertos IEEE 802.1x está habilitada y el cliente admite el software cliente compatible con IEEE 802.1x, estos eventos ocurren:

• Si la identidad del cliente es válida y la autenticación IEEE 802.1x tiene éxito, el cambio le otorga al cliente acceso a la red.

• Si se agota el tiempo de espera de la autenticación IEEE 802.1x mientras se espera un intercambio de mensajes EAPOL y se habilita la omisión de autenticación MAC, el conmutador puede usar la dirección MAC del cliente para la autorización. Si la dirección MAC del cliente es válida y la autorización tiene éxito, el cambio otorga al cliente acceso a la red. Si la dirección MAC del cliente no es válida y la autorización falla, el conmutador asigna al cliente una VLAN invitada que proporciona servicios limitados si se configura una VLAN invitada.

• Si el conmutador obtiene una identidad no válida de un cliente compatible con IEEE 802.1x y se especifica una VLAN restringida, el conmutador puede asignar al cliente a una VLAN restringida que proporciona servicios limitados.

• Si el servidor de autenticación RADIUS no está disponible (inactivo) y está habilitado el bypass de autenticación inaccesible, el switch otorga al cliente acceso a la red colocando el puerto en estado de autenticación crítica en la VLAN de acceso configurado por RADIUS o por el usuario.

Si Multi Domain Authentication (MDA) está habilitada en un puerto, este flujo se puede usar con algunas excepciones que se aplican a la autorización de voz.

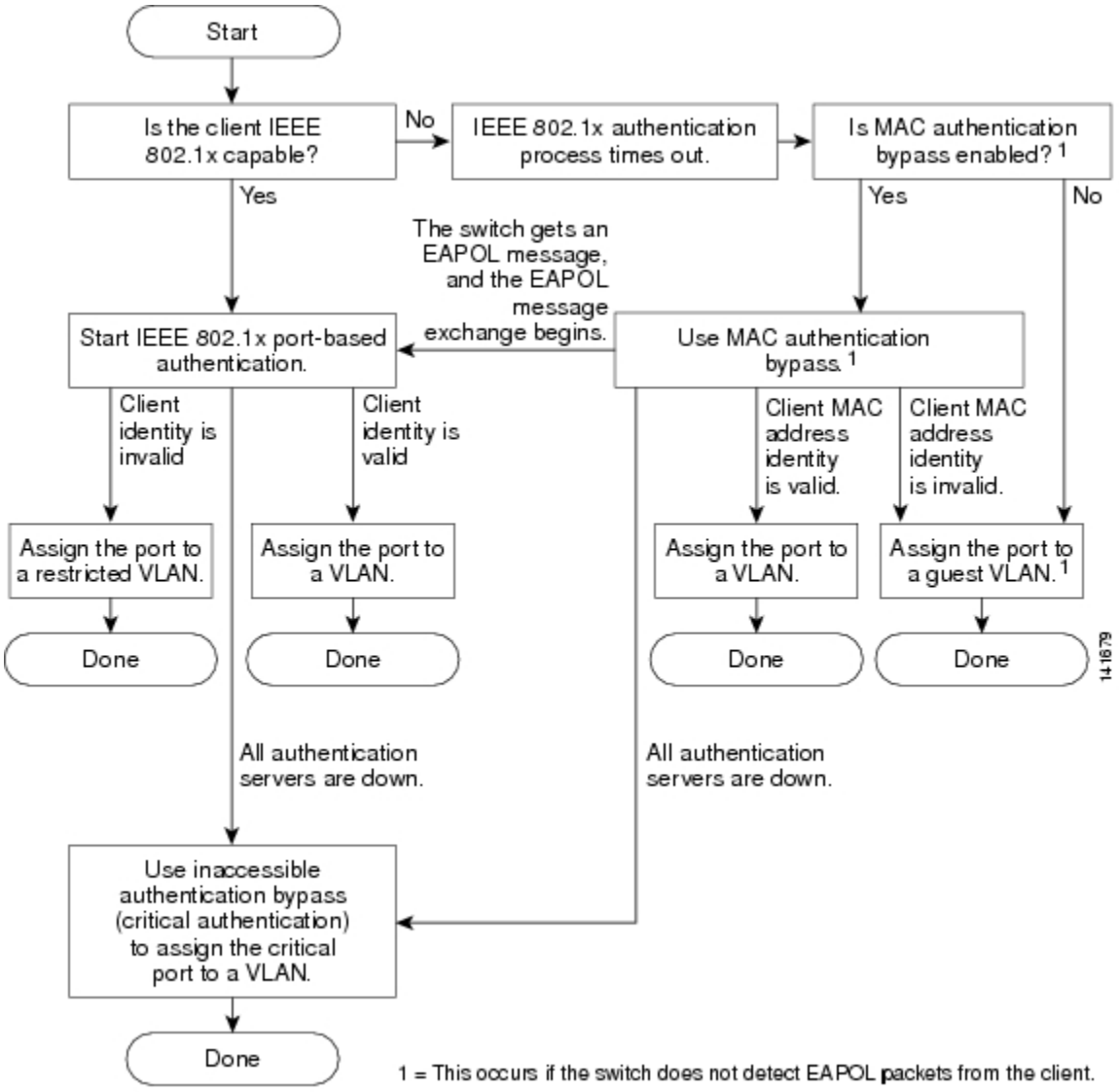

Ilustración 17. Diagrama de flujo de autenticación

El conmutador vuelve a autenticar a un cliente cuando ocurre una de estas situaciones:

• La reautenticación periódica está habilitada y el temporizador de reautenticación expira.

Puede configurar el temporizador de reautentificación para usar un valor específico del conmutador o basarse en los valores del servidor RADIUS.

Después de que se configura la autenticación IEEE 802.1x utilizando un servidor RADIUS, el conmutador usa temporizadores basados en el atributo RADIUS de sesión-tiempo de espera (atributo [27]) y el atributo RADIUS de acción de terminación (atributo [29]).

El atributo RADIUS Session-Timeout (Attribute [27]) especifica el tiempo después del cual se produce la reautenticación.

El atributo RADIUS de Termination-Action (Attribute [29]) especifica la acción a tomar durante la reautenticación. Las acciones son Initialize y ReAuthenticate . Cuando se establece la acción Initialize (el valor del atributo es DEFAULT), la sesión IEEE 802.1x finaliza y la conectividad se pierde durante la reautenticación. Cuando se establece la acción ReAuthenticate (el valor del atributo es RADIUS-Request), la sesión no se ve afectada durante la nueva autenticación.

• Usted vuelve a autenticar manualmente al cliente ingresando el comando EXIT privilegiado de interfaz de interfaz de interfaz de interfaz de usuario dot1x.

Iniciación de autenticación e intercambio de mensajes

Durante la autenticación IEEE 802.1x, el conmutador o el cliente puede iniciar la autenticación. Si habilita la autenticación en un puerto mediante el comando de configuración de interfaz automática dot1x port-control, el switch inicia la autenticación cuando el estado del enlace cambia de abajo hacia arriba o periódicamente, siempre que el puerto permanezca activo y no autenticado. El conmutador envía un marco de solicitud / identidad de EAP al cliente para solicitar su identidad. Al recibir el marco, el cliente responde con un marco de EAP / respuesta / identidad.

Sin embargo, si durante el inicio, el cliente no recibe un marco de petición / identidad de EAP desde el conmutador, el cliente puede iniciar la autenticación enviando un marco de inicio EAPOL, que solicita al conmutador que solicite la identidad del cliente.

Cuando el cliente proporciona su identidad, el conmutador comienza su rol de intermediario, pasando cuadros EAP entre el cliente y el servidor de autenticación hasta que la autenticación sea exitosa o falle. Si la autenticación tiene éxito, el puerto del conmutador queda autorizado. Si la autenticación falla, la autenticación puede reintentarse, el puerto puede asignarse a una VLAN que proporciona servicios limitados, o no se concede el acceso a la red.

Puertos en estados autorizados y no autorizados

Durante la autenticación IEEE 802.1x, dependiendo del estado del puerto del conmutador, el conmutador puede otorgar a un cliente acceso a la red. El puerto comienza en el estado no autorizado. Mientras está en este estado, el puerto que no está configurado como un puerto de VLAN de voz no permite el ingreso de todo el tráfico, excepto para los paquetes de autenticación IEEE 802.1x, CDP y STP. Cuando un cliente se autentica con éxito, el puerto cambia al estado autorizado, lo que permite que todo el tráfico del cliente fluya normalmente. Si el puerto está configurado como un puerto de VLAN de voz, el puerto permite el tráfico VoIP y los paquetes de protocolo IEEE 802.1x antes de que el cliente se autentique correctamente.

Si un cliente que no admite la autenticación IEEE 802.1x se conecta a un puerto IEEE 802.1x no autorizado, el conmutador solicita la identidad del cliente. En esta situación, el cliente no responde a la solicitud, el puerto permanece en estado no autorizado y el cliente no tiene acceso a la red.

Por el contrario, cuando un cliente habilitado para IEEE 802.1x se conecta a un puerto que no ejecuta el estándar IEEE 802.1x, el cliente inicia el proceso de autenticación enviando el marco EAPOL-start. Cuando no se recibe respuesta, el cliente envía la solicitud por un número fijo de veces. Como no se recibe respuesta, el cliente comienza a enviar marcos como si el puerto estuviera en el estado autorizado.

Usted controla el estado de autorización de puerto utilizando el comando de configuración de interfaz de control de puerto dot1x y estas palabras clave:

• fuerza autorizada: deshabilita la autenticación IEEE 802.1x y hace que el puerto cambie al estado autorizado sin necesidad de un intercambio de autenticación. El puerto envía y recibe tráfico normal sin la autenticación basada en IEEE 802.1x del cliente. Esta es la configuración predeterminada.

• fuerza no autorizada: causa que el puerto permanezca en el estado no autorizado, ignorando todos los intentos del cliente de autenticarse. El conmutador no puede proporcionar servicios de autenticación al cliente a través del puerto.

• habilita automáticamente la autenticación IEEE 802.1x y hace que el puerto comience en un estado no autorizado, permitiendo que solo se envíen y reciban tramas EAPOL a través del puerto. El proceso de autenticación comienza cuando el estado del enlace del puerto cambia de abajo hacia arriba o cuando se recibe un marco de inicio de EAPOL. El conmutador solicita la identidad del cliente y comienza a transmitir mensajes de autenticación entre el cliente y el servidor de autenticación. Cada cliente que intenta acceder a la red se identifica de manera única mediante el interruptor utilizando la dirección MAC del cliente.

Si el cliente se autentica correctamente (recibe un marco de aceptación del servidor de autenticación), el estado del puerto cambia a autorizado, y todos los marcos del cliente autenticado se permiten a través del puerto. Si la autenticación falla, el puerto permanece en el estado no autorizado, pero se puede volver a intentar la autenticación. Si no se puede llegar al servidor de autenticación, el conmutador puede volver a enviar la solicitud. Si no se recibe respuesta del servidor después del número especificado de intentos, la autenticación falla y no se concede el acceso a la red.

Cuando un cliente cierra sesión, envía un mensaje EAPOL-logoff, causando que el puerto del switch cambie al estado no autorizado.

Si el estado del enlace de un puerto cambia de arriba a abajo, o si se recibe un marco EAPOL-logoff, el puerto regresa al estado no autorizado.

X. CONCLUSIONES

- Se realizó la implementación del estándar 802.1x radius server en el Sistema Nacional de Emergencias, ya que implementar 802.1x es una posibilidad real que la organización puede llevar a cabo con su infraestructura tecnológica actual, y que se adecuará, sin mayores impactos económicos o funcionales, a su crecimiento y modernización.

- Las empresas con un manejo de información tan importante necesitan dotar su infraestructura informática de políticas y medidas de protección adecuadas que garanticen el desarrollo y sostenibilidad de sus actividades, sin correr el riesgo de algún ataque a su información. Ya que la información se ha convertido en un activo de mucho valor el cual se debe proteger y garantizar su integridad, disponibilidad y confidencialidad.

- Se configuro en el server RADIUS la opción de contabilidad, las funciones de contabilidad de RADIUS permiten que los datos se envíen al inicio y al final de las sesiones, lo que indica la cantidad de recursos (como el tiempo, los paquetes, los bytes, etc.) utilizados durante la sesión.

XI. RECOMENDACIONES

RECOMENDACIONES A LA EMPRESA

Los meses que estuve en la empresa, lo que note es que uno de los problemas que se tenia era con el generador eléctrico el cual no estaba funcionando correctamente y al no haber flujo eléctrico ocasionaba que se descargaran los UPS y se apagaran los equipos.

Otra recomendación seria que capacitaran mas al personal.

RECOMENDACIONES A LA UNIVERSIDAD

Para el área en la que nos estamos especializando como ser las telecomunicaciones, considero que es de suma importancia la práctica. La universidad debería de contar con mejores laboratorios y las clases ser más prácticas.

XII. IMPLEMENTACIÓN

La implementación del estándar 802.1x permitió mejorar la parte de seguridad en los puertos de acceso. La mayor parte de la implementación fue realizada en el switch principal S6000-Pri.

A continuación, los comandos utilizados:

Configurando la Autenticación IEEE 802.1x

Para configurar la autenticación basada en puertos IEEE 802.1x, debe habilitar la autenticación, autorización y contabilidad (AAA) y especificar la lista de métodos de autenticación. Una lista de métodos describe la secuencia y el método de autenticación que se debe consultar para autenticar a un usuario.

S6000-Pri > enable

S6000-Pri# configure terminal

S6000-Pri (config) # aaa new-model

S6000-Pri (config) # aaa authentication dot1x default method1

S6000-Pri (config) # dot1x system-auth-control

S6000-Pri (config) # radius-server host 192.168.0.163

S6000-Pri (config) # radius-server key Dyn911SPS

S6000-Pri (config) # Interface g0/0

S6000-Pri (config-if) # switchport mode access

S6000-Pri (config-if) # dot1x port-control auto

S6000-Pri (config-if) # end

Configurar la comunicación del servidor Switch-to-RADIUS

Los servidores de seguridad RADIUS se identifican por su nombre de host o dirección IP, nombre de host y números de puerto UDP específicos, o dirección IP y números de puerto UDP específicos. La combinación de la dirección IP y el número de puerto UDP crea un identificador único, que permite que las solicitudes RADIUS se envíen a múltiples puertos UDP en un servidor con la misma dirección IP. Si se configuran dos entradas de host diferentes en el mismo servidor RADIUS para el mismo servicio, por ejemplo, autenticación, la segunda entrada de host configurada actúa como la copia de seguridad de conmutación de fallas a la primera. Las entradas del host RADIUS se prueban en el orden en que se configuraron.

S6000-Pri > enable

S6000-Pri# configure terminal

S6000-Pri (config) # radius-server host 192.168.0.5 auth-port 1812 clave radDyn911

S6000-Pri# copy running-config startup-config

Configurando el Modo Anfitrión

S6000-Pri > enable

S6000-Pri# configure terminal

S6000-Pri (config) # radius-server vsa send authentication

S6000-Pri (config) # interface g0/0

S6000-Pri (config-if) # dot1x host-mode single-host

S6000-Pri (config-if) # end

S6000-Pri# copy running-config startup-config

Configurando la Re-Autenticación Periódica

Puede habilitar la reautenticación periódica del cliente IEEE 802.1x y especificar la frecuencia con la que ocurre. Si no especifica un período de tiempo antes de habilitar la reautenticación, el número de segundos entre intentos es 3600.

S6000-Pri > enable

S6000-Pri# configure terminal

S6000-Pri (config) # interface g0/0

S6000-Pri (config-if)# dot1x reauthentication

S6000-Pri (config-if)# dot1x timeout reauth-period 3600

S6000-Pri# copy running-config startup-config

Cambiar el período de silencio

Cuando el conmutador no puede autenticar al cliente, el conmutador permanece inactivo durante un período de tiempo determinado y luego lo intenta de nuevo. El comando de configuración de interfaz de período de tiempo de espera de punto1x controla el período de inactividad.

S6000-Pri > enable

S6000-Pri# configure terminal

S6000-Pri (config) # interface g0/0

S6000-Pri (config-if)# dot1x timeout quiet-period 60

S6000-Pri# copy running-config startup-config

Cambiar el tiempo de retransmisión de conmutación a cliente y la cantidad de veces que el conmutador envía una solicitud EAP

El cliente responde al marco de solicitud / identidad de EAP desde el conmutador con un marco de respuesta EAP / identidad. Si el interruptor no recibe esta respuesta, espera un período de tiempo establecido (conocido como el tiempo de retransmisión) y luego reenvía el cuadro. Además de cambiar el tiempo de retransmisión de conmutación a cliente, puede cambiar el número de veces que el conmutador envía un marco de solicitud / identidad de EAP (suponiendo que no se reciba respuesta) antes de reiniciar el proceso de autenticación.

S6000-Pri > enable

S6000-Pri# configure terminal

S6000-Pri (config) # interface g0/0

S6000-Pri (config-if)# dot1x timeout tx-period 60

S6000-Pri (config-if)# dot1x max-req 5

S6000-Pri (config-if)# end

S6000-Pri# copy running-config startup-config

Configurando la Contabilidad IEEE 802.1x

La habilitación de la contabilidad del sistema AAA con la contabilidad IEEE 802.1x permite que los eventos de recarga del sistema se envíen al servidor RADIUS de contabilidad para el registro. El servidor puede inferir que todas las sesiones IEEE 802.1x activas están cerradas.

Debido a que RADIUS usa el protocolo de transporte UDP no confiable, los mensajes de contabilidad podrían perderse debido a malas condiciones de la red. Si el conmutador no recibe el mensaje de respuesta de contabilidad del servidor RADIUS después de un número configurable de retransmisiones de una solicitud de contabilidad, aparece este mensaje del sistema:

El mensaje de contabilidad% s para la sesión% s no pudo recibir respuesta de contabilidad.

Cuando el mensaje de detención no se envía correctamente, aparece este mensaje:

00:09:55:% RADIUS-4-RADIUS_DEAD: el servidor RADIUS 172.20.246.201:1645,1646 no responde.

S6000-Pri (config) # radio-servidor host 172.120.39.46 auth-port 1812 acct-port 1813 clave Dyn911SPS

S6000-Pri (config) # aaa accounting dot1x default start-stop group radius

S6000-Pri (config) # aaa accounting system default start-stop group radius

Configuración de la característica de omisión de autenticación inaccesible

S6000-Pri(config)# radius-server dead-criteria time 30 tries 20

S6000-Pri(config)# radius-server deadtime 60

S6000-Pri(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 key Dyn911SPS test username user1 idle-time 30

S6000-Pri(config)# dot1x critical eapol

S6000-Pri(config)# dot1x critical recovery delay 2000

S6000-Pri(config)# interface gigabitethernet 0/1

S6000-Pri(config)# radius-server deadtime 60

S6000-Pri(config-if)# dot1x critical

S6000-Pri(config-if)# dot1x critical recovery action reinitialize

S6000-Pri(config-if)# dot1x critical vlan 20

S6000-Pri(config-if)# end

XIII. BIBLIOGRAFÍA

¿Cómo el RADIUS trabaja? (2006). Retrieved from Cisco: https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

(2015). Retrieved from Blog Redes: https://pondalpar113.wordpress.com/tipos-de-cable/

(2018). Retrieved from Microsoft: https://technet.microsoft.com/es-es/library/hh945105(v=ws.11).aspx

Alonso, D. G. (2009). *5 Medios de transmision no guiados* . Retrieved from issu: https://issuu.com/dgainformaticacarlos3/docs/5-medios-de-transmision-no-guiados

Casillas, M. A. (2009). *Topologia de Redes*. Retrieved from Redes Topologias: http://redestipostopologias.blogspot.com/2009/03/topologia-de-redes.html

Clasificacion de Redes. (2018). Retrieved from Redes-De-Computadora: https://redes-de-computadoras.wikispaces.com/Clasificaci%C3%B3n

Comparación de TACACS+ y RADIUS. (2012). Retrieved from Cisco: https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

Diaz, I. A. (2013). *Clasificación Por la direccionalidad de los datos.* Retrieved from https://prezi.com/rjmdim_uqfs5/clasificacion-por-la-direccionalidad-de-los-datos/

El Modelo OSI. (n.d.). Retrieved from http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

Gonzales, M. (2013). *Redes Telematicas*. Retrieved from http://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

Introducción al acceso inalámbrico autenticado mediante 802.1X. (n.d.). Retrieved from Miscrosoft: https://msdn.microsoft.com/es-es/library/hh994700(v=ws.11).aspx

Lopez, A. (2015). *CERTSI*. Retrieved from https://www.certsi.es/blog/protocolos-aaa-radius

Microsystem, S. (2009). Retrieved from Distributed Application Architecture: http://java.sun.com/developer/Books/jdbc/ch07.pdf

Overview and Guide to the IEEE 802 . (2012). Retrieved from http://www.ieee802.org/IEEE-802-LMSC-OverviewGuide-02SEPT%202012.pdf

Redes de Computadora. (n.d.). Retrieved from Modelos conceptuales: https://redesdecomputadoras.es.tl/Estandares-y-Protocolos.htm

Stalling, W. (n.d.). *Data and Computer Communications.*

Tanenbaum, A. (n.d.). *Computer Networks.* Prentice Hall.

XIX. ANEXOS

Ilustración 18. Access Point Cisco WAP321-A-K9

Ilustración 19. Catalyst 3750-E

Ilustración 20. Catalyst 3560-E

Instalación de Radius server

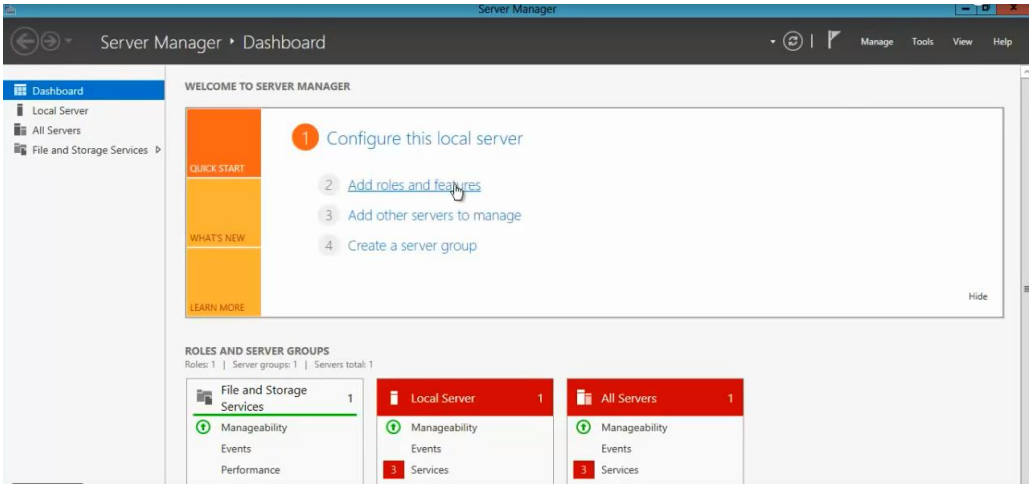

Ilustración 21. Instalación Radius server

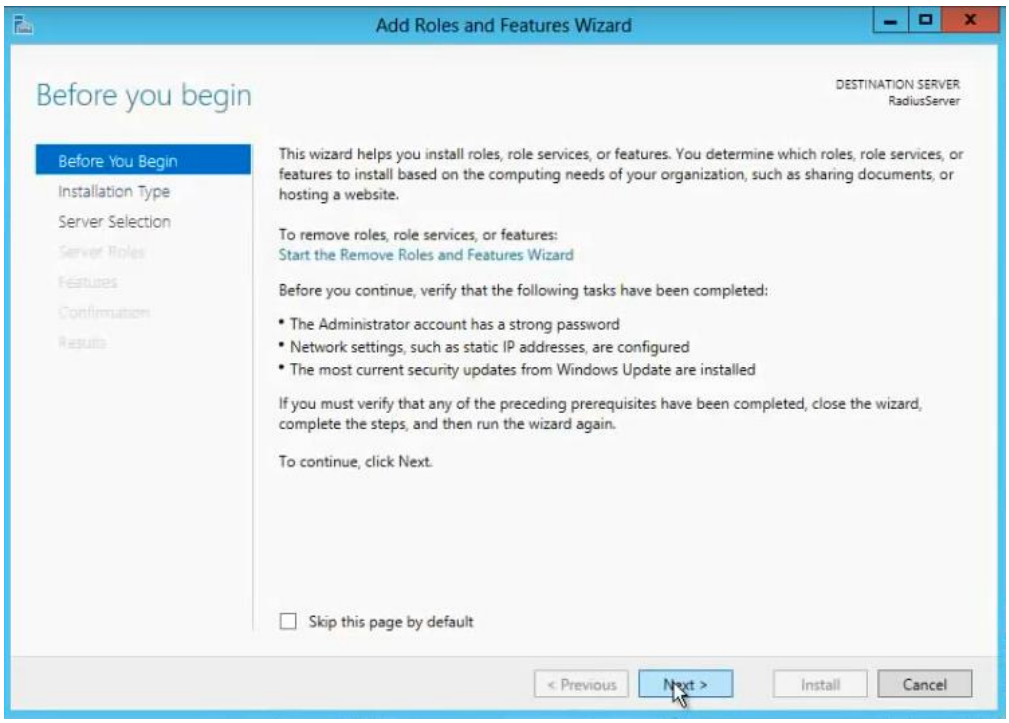

Ilustración 22. Instalación Radius server

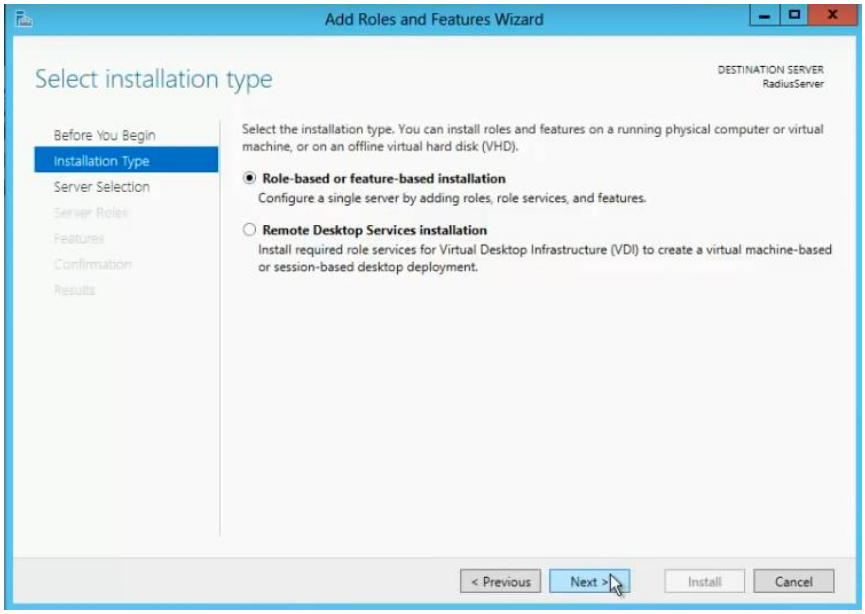

Ilustración 23. Instalación Radius server

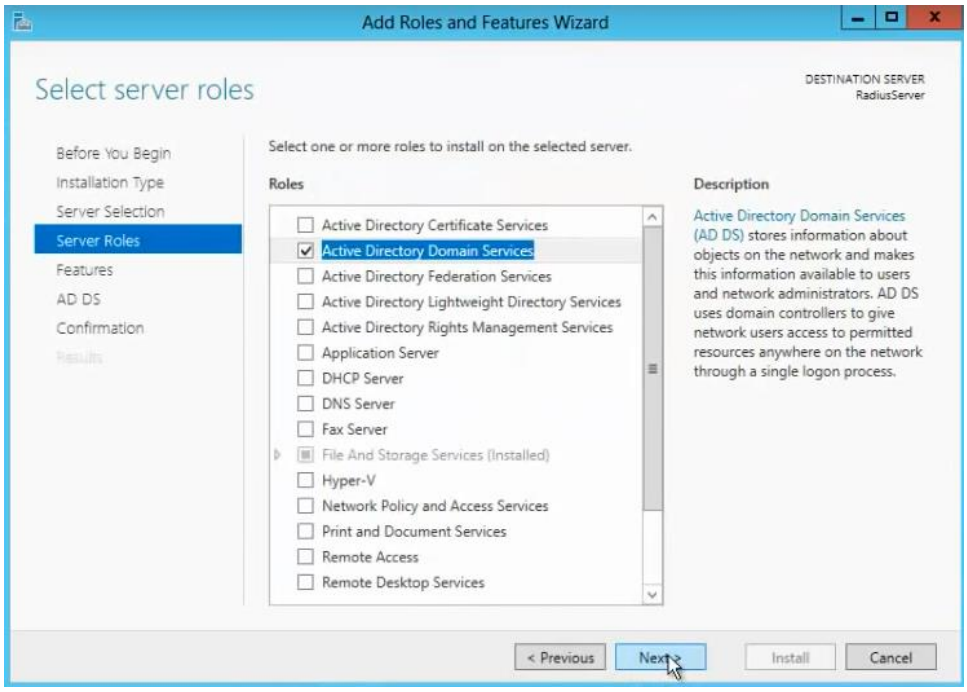

Ilustración 24. Instalación Radius server

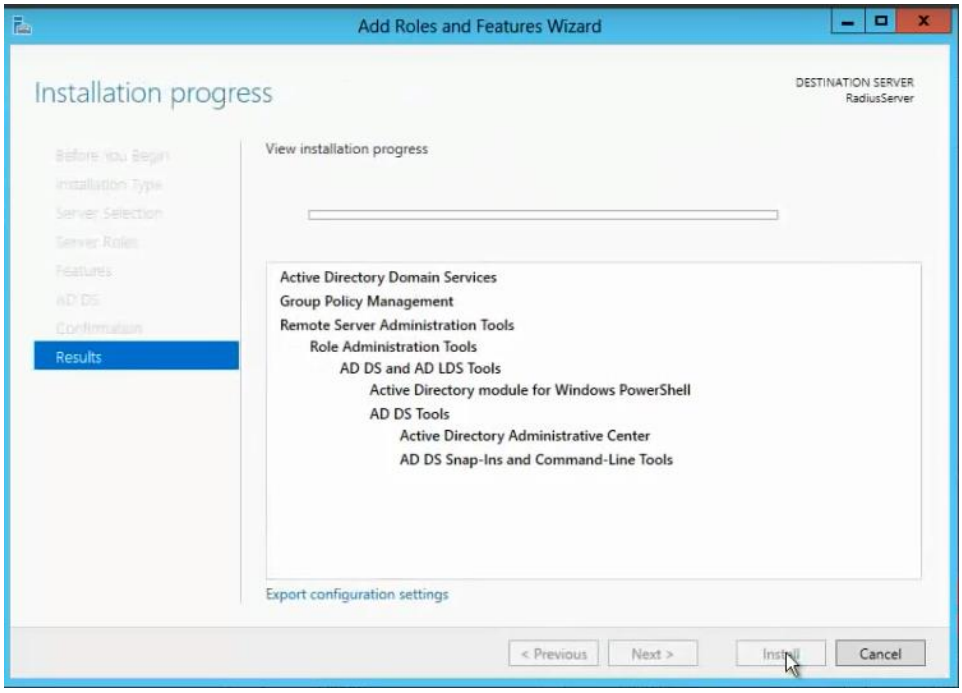

Ilustración 25. Instalación Radius server

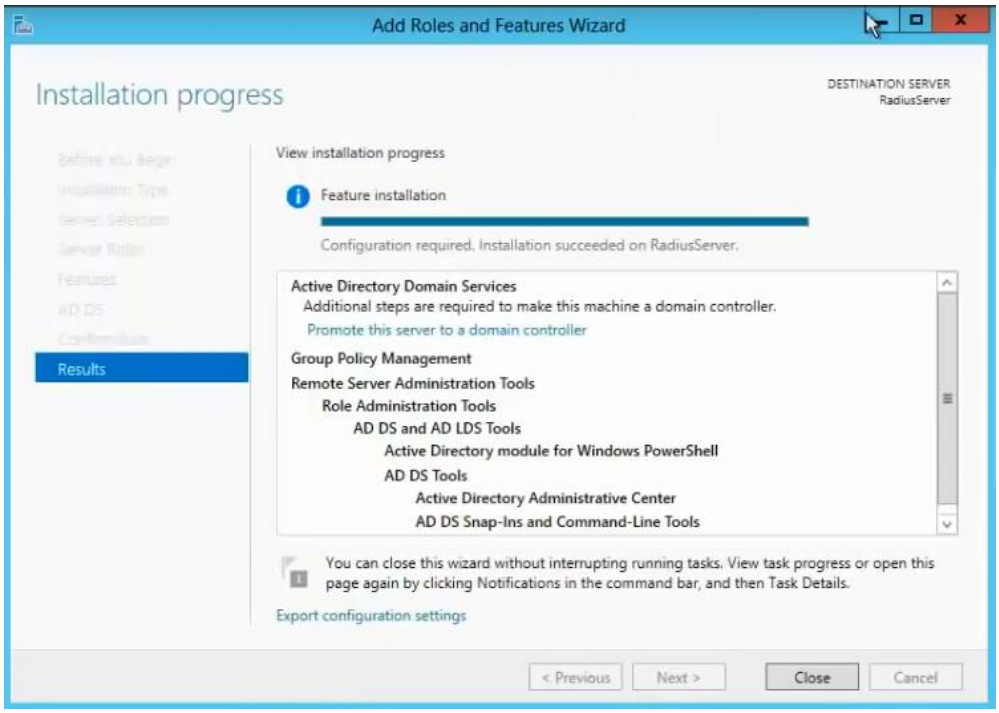

Ilustración 26. Instalación Radius server

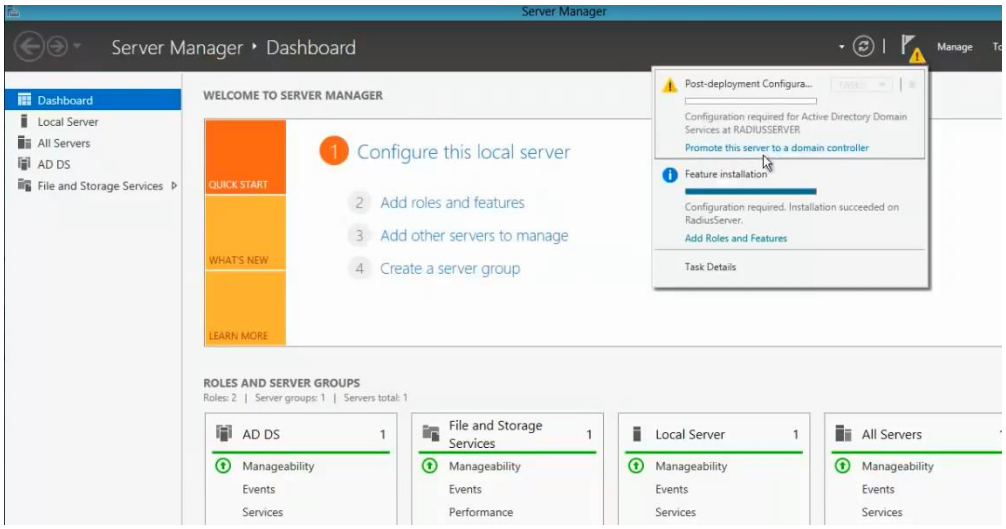

Ilustración 27. Instalación Radius server

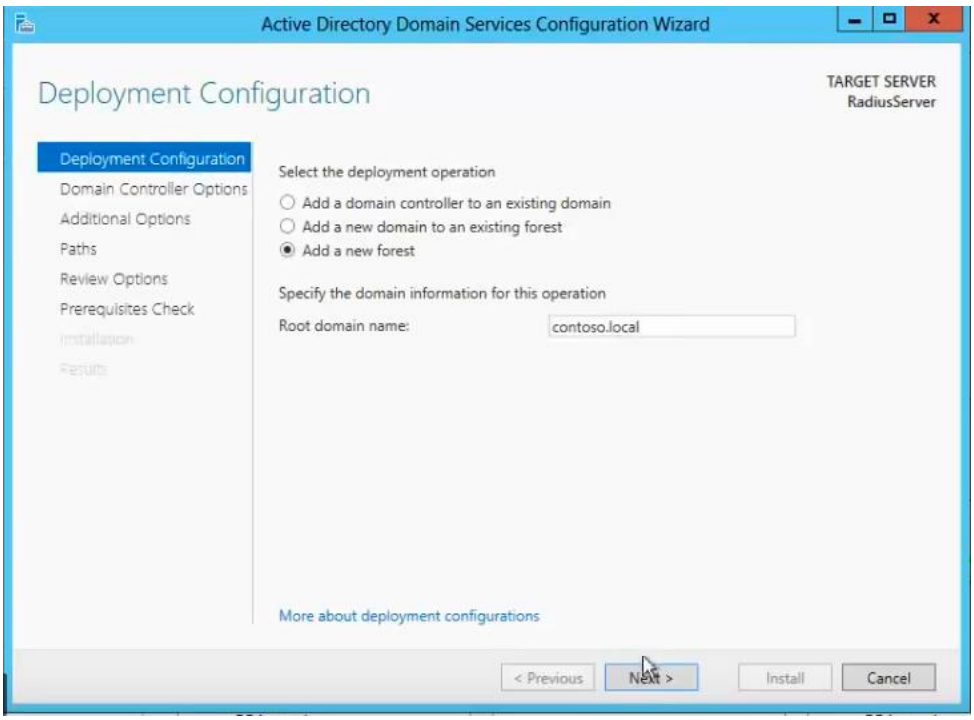

Ilustración 28. Instalación Radius server

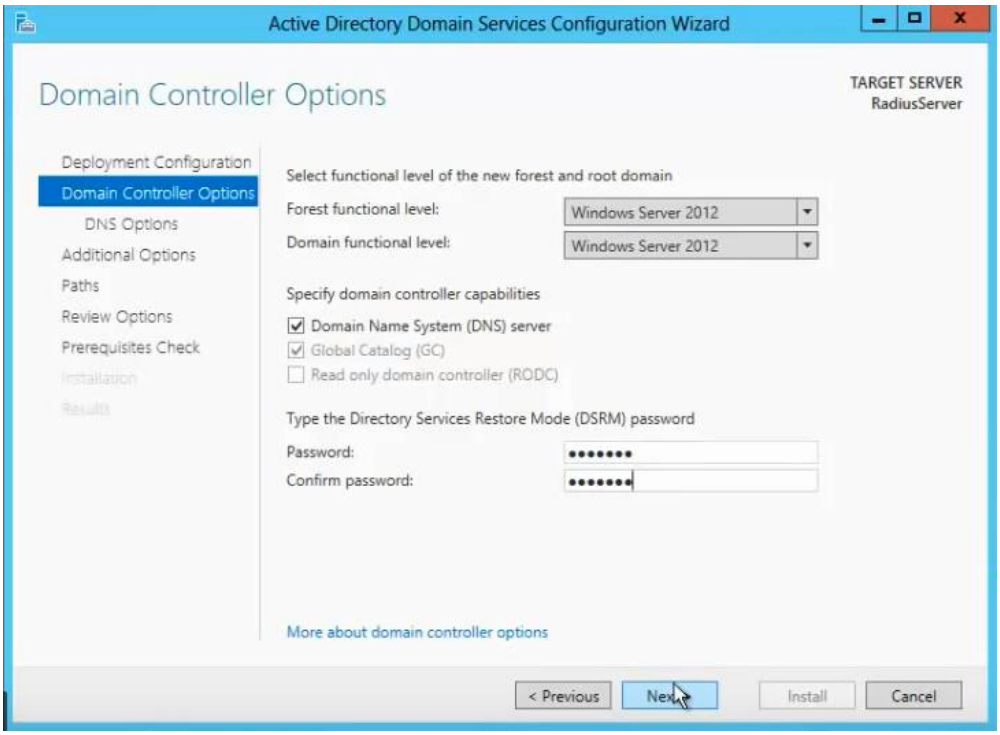

Ilustración 29. Instalación Radius server

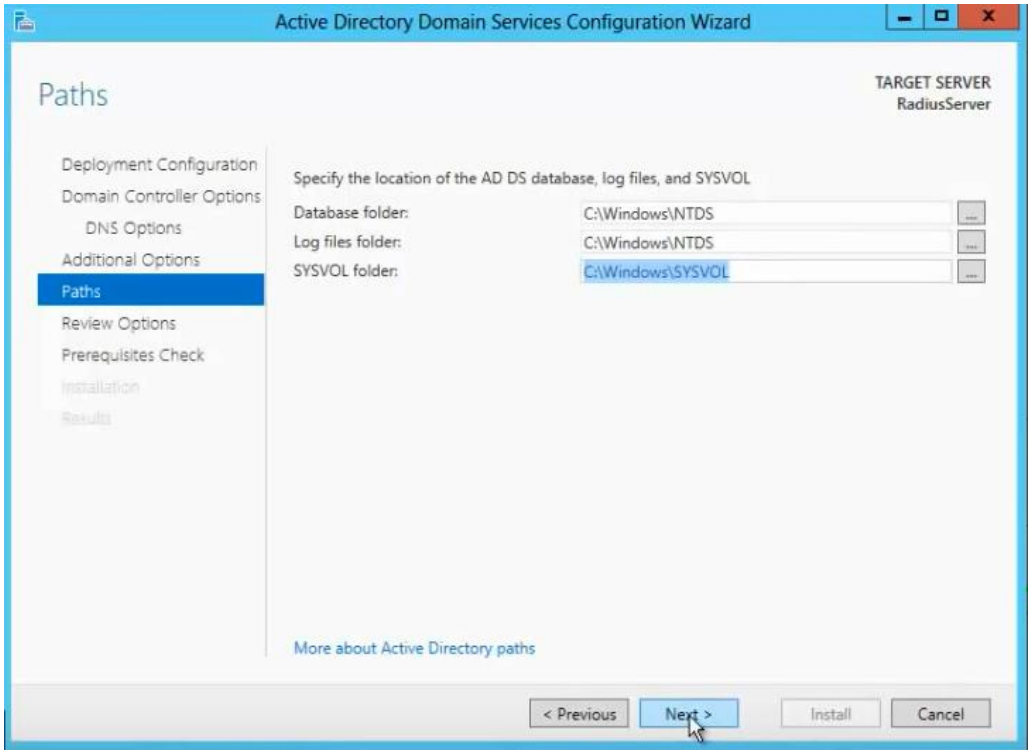

Ilustración 30. Instalación Radius server

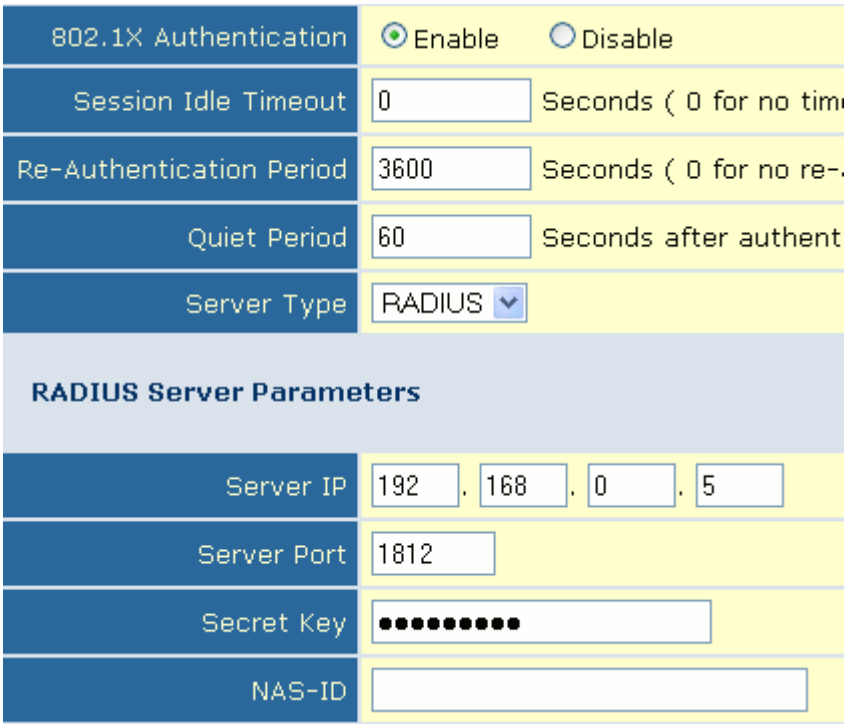

Ilustración 31. Configuración

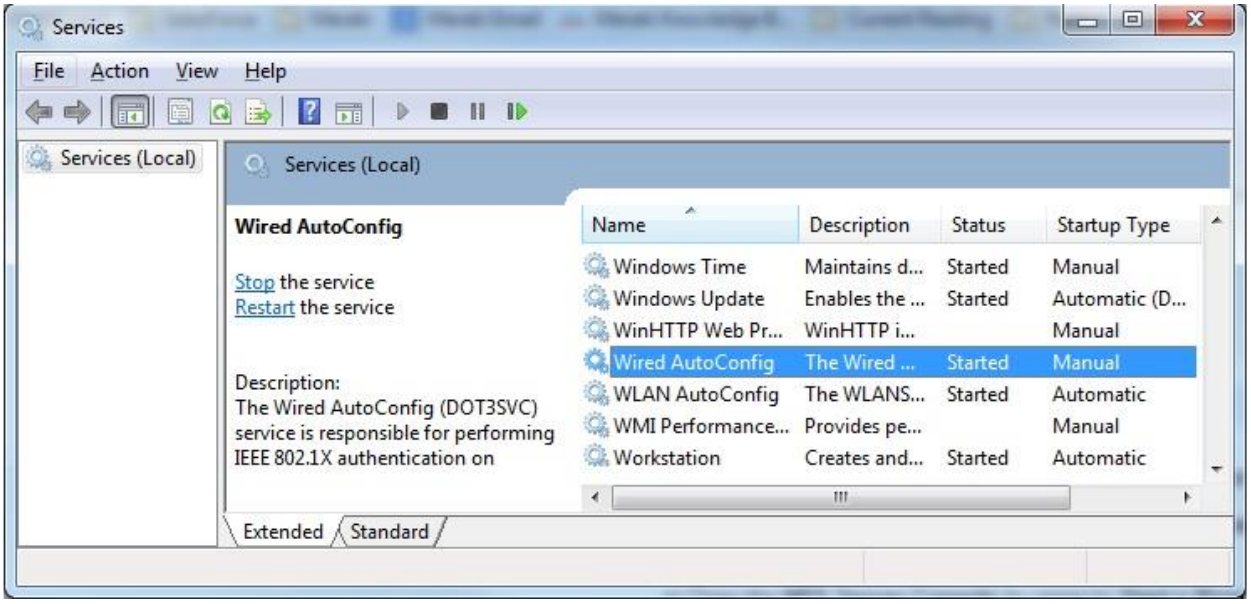

Ilustración 32. Servicio AutoConfig

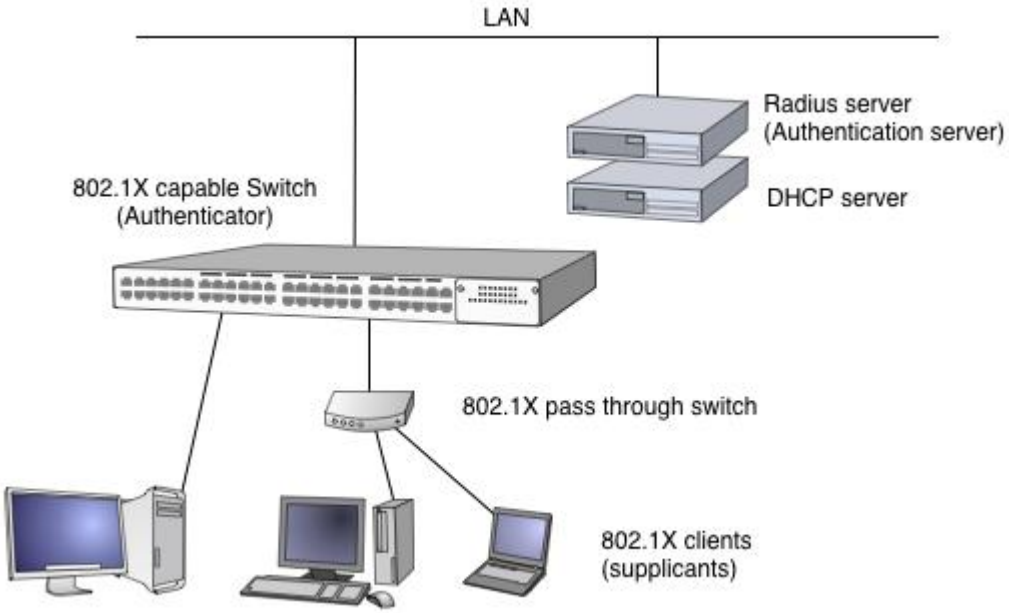

Ilustración 33. Topologìa

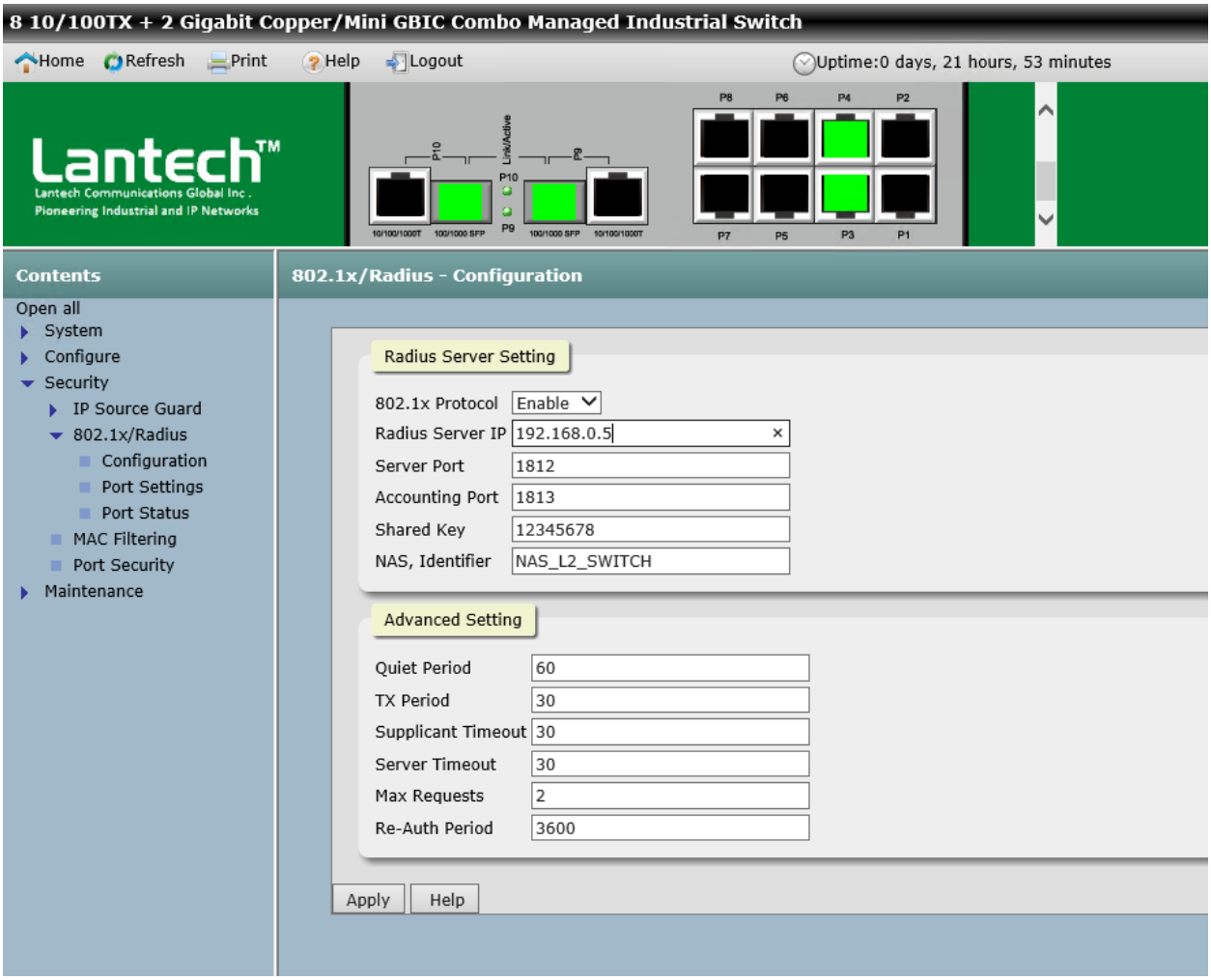

Ilustración 34. Configuracion del switch administrable