IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

QUE PARA OBTENER EL TITULO DE: INGENIERO EN COMPUTACIÓN

NOMBRE DEL SEMINARIO: AUDITORIA DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

VIGENCIA: DES/ESIME-CUL-2009/38/02/12

DEBERA DESARROLLAR: CUEVAS OLIVARES JACOBO.
ENRÍQUEZ PRADO JORGE ALBERTO.
JIMÉNEZ VELÁZQUEZ NORMA LETICIA.
REYES DIONICIO IVONNE.
RODRÍGUEZ OLIVO ANA BERTHA.

NOMBRE DEL TEMA

"AUDITORÍA DE ROUTER DE LA DIRECCIÓN GENERAL DE CALIDAD Y EDUCACIÓN EN SALUD"

INTRODUCCIÓN

La importancia de la auditoría de los routers, procura examinar los temas pertinentes a la revisión de los dispositivos antes y después de ser asegurados. El router es analizado con más detenimiento, teniendo en cuenta la importancia de las posibilidades que provee. Es importante resaltar que el tratamiento del aseguramiento es un tema muy importante en la actividad de un administrador de seguridad, ya que permite identificar las vulnerabilidades de los dispositivos y por ende desarrollar las herramientas y medidas necesarias para minimizar los riesgos ante posibles amenazas.
Se analizaran las vulnerabilidades del enrutador al ser configurado por defecto, estableciendo mecanismos de seguridad.

CAPITULADO

Fecha: México D.F, a 28 de Abril del 2012.

M. EN C. RAYMUNDO SANTANA ALQUICIRA
Coordinador del Seminario

ING. MIGUEL ÁNGEL MIRANDA HERNÁNDEZ
Instructor del Seminario

DR. JOSE VELAZQUEZ LOPEZ
Jefe de la carrera de I.C.

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA

MECÁNICA Y ELÉCTRICA UNIDAD CULHUACAN

Seminario de Auditoría de las Tecnologías de la Información y Comunicaciones

AUDITORÍA DE ROUTER DE LA DIRECCIÓN GENERAL DE CALIDAD Y EDUCACIÓN EN SALUD

INTEGRANTES

Cuevas Olivares Jacobo.
Enríquez Prado Jorge Alberto.
Jiménez Velázquez Norma Leticia.
Reyes Dionicio Ivonne.
Rodríguez Olivo Ana Bertha.

ASESORES

M. en C. Raymundo Santana Alquicira.
M. en C. Jaime Ibarra Reyes.
Ing. Miguel Ángel Miranda Hernández.
Ing. Eduardo Martínez Corona.

MÉXICO, D.F, Abril 2012.

ÍNDICE

INTRODUCCIÓN

La importancia de la auditoría de los routers, procura examinar los temas pertinentes a la revisión de los dispositivos antes y después de ser asegurados. El router es analizado con más detenimiento, teniendo en cuenta la importancia de las posibilidades que provee. Es importante resaltar que el tratamiento del aseguramiento es un tema muy importante en la actividad de un administrador de seguridad, ya que permite identificar las vulnerabilidades de los dispositivos y por ende desarrollar las herramientas y medidas necesarias para minimizar los riesgos ante posibles amenazas.

Se analizaran las vulnerabilidades del enrutador al ser configurado por defecto, estableciendo mecanismos de seguridad.

OBJETIVO

Auditar el Router de la Dirección General de Calidad y Educación en Salud, en su configuración actual.

PROBLEMÁTICA

La red deja de prestar sus servicios en la interconectividad con los demás sitios de la corporación.

JUSTIFICACIÓN

Administrar al router con las mejores prácticas Mediante normas y políticas del NIST *(National Institute of Standards and Technology).*

ALCANCE

Se pretende realizar una auditoría para descubrir las vulnerabilidades y configuraciones de riesgo en la seguridad del router en la Dirección General de Calidad y Educación en Salud.

CAPÍTULO 1. INTRODUCCIÓN A LAS AUDITORÍAS DE TIC'S

1.1 TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN (TIC'S)

Las TIC'S (tecnologías de la información y de la comunicación) son aquellas tecnologías que permiten la manipulación de la información y su transmisión masiva a toda la sociedad**.** La importancia de la información en la vida actual es de tal magnitud que muchos sociólogos han llamado a esta sociedad **"sociedad de la información".**

Los primeros pasos hacia esta Sociedad de la Información se remontan a la invención del telégrafo eléctrico, pasando posteriormente por el teléfono fijo, la radio y por último, la televisión.

Los satélites artificiales, la computadora, internet, los celulares y el GPS pueden considerarse como las nuevas tecnologías de la información y la comunicación. El **17 de mayo** se celebra el **día mundial de las TICs** y de la Sociedad de la Información, recordando la fecha en que se creó la Unión Internacional de Telecomunicaciones.

Las TIC tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

TIC'S para la educación

El uso de las TIC en la educación puede fomentar el aprendizaje y desarrollo personal, en un marco mucho más flexible que los niveles educativos existentes.

La incorporación de las Tecnologías de Información y comunicación (TIC) al proceso educativo de niños y niñas con discapacidad o *Necesidades Educativas Especiales (NEE)*, podría facilitar su integración educativa e inclusión escolar. Un efecto derivado sería la mejora de sus condiciones laborales y calidad de vida.

TIC'S en las empresas y en el recurso humano

Las TIC'S están cambiando la forma tradicional de hacer las cosas, las personas que trabajan en gobierno, en empresas privadas, que dirigen personal o que trabajan como profesional en cualquier campo utilizan tecnologías de información cotidianamente mediante el uso de internet, tarjetas de crédito, pago electrónico de la nómina de trabajadores, entre otras funciones; es por eso que la función de las TIC'S en los procesos empresariales, como manufactura y ventas, se han expandido grandemente.

La primera generación de computadoras estaba destinada a guardar los registros y monitorear el desempeño operativo de la empresa, pero la información no era oportuna ya que el análisis obtenido en un día determinado en realidad describía lo que había pasado una semana antes.

Los avances actuales hacen posible capturar y utilizar la información en el momento que se genera, es decir, tener procesos en línea. Este hecho no sólo ha cambiado la forma de hacer

el trabajo y el lugar de trabajo, sino que también ha tenido un gran impacto en la forma en la que las empresas compiten.

Utilizando eficientemente las TIC'S se pueden obtener ventajas competitivas, pero es preciso encontrar procedimientos acertados para mantener tales ventajas como una constante, así como disponer de cursos y recursos alternativos de acción para adaptarlas a las necesidades del momento, pues las ventajas no siempre son permanentes.

El sistema de información tiene que modificarse y actualizarse con regularidad si se desea percibir ventajas competitivas continuas. El uso creativo de la tecnología puede proporcionar a los administradores una herramienta eficaz para diferenciar sus recursos humanos, productos y/o servicios respecto de sus competidores.

Las TIC'S representan una herramienta importante en los negocios, sin embargo, el implementar un sistema de información no garantiza que ésta obtenga resultados de manera automática o a largo plazo.

En la implementación de un sistema de información intervienen muchos factores siendo uno de los principales el factor humano. Es previsible que ante una situación de cambio el personal se muestre renuente a adoptar los nuevos procedimientos o que los desarrolle plenamente y de acuerdo a los lineamientos que se establecieron.

De todo lo anterior es necesario hacer una planeación estratégica tomando en cuenta las necesidades presentes y futuras de la empresa. Así como una investigación preliminar y estudio de factibilidad del proyecto que deseamos.

Ventajas de las TIC'S en la organización empresarial

Las TIC'S son esenciales para mejorar la productividad de las empresas, la calidad, el control y facilitar la comunicación entre otros beneficios, aunque su aplicación debe llevarse a cabo de forma inteligente.

El mero hecho de introducir tecnología en los procesos empresariales no es garantía de gozar de estas ventajas. Para que la implantación de nueva tecnología produzca efectos positivos hay que cumplir varios requisitos: tener un conocimiento profundo de los procesos de la empresa, planificar detalladamente las necesidades de tecnología de la información e incorporar los sistemas tecnológicos paulatinamente, empezando por los más básicos.

Antes de añadir un componente tecnológico, hay que conocer bien la organización y/o empresa. Se ha investigado por qué fracasan algunos proyectos de implantación de tecnología de la información y se ha descubierto que el 90% de las veces el fracaso no es debido al software ni a los sistemas, sino al hecho de que la gente no tiene suficientes conocimientos sobre su propia empresa o sus procesos empresariales.

Otro aspecto importante a considerar es que las empresas que tienen una gran capacidad de beneficiarse de la tecnología son organizaciones que, antes de añadir un componente tecnológico, describen detalladamente cuál será la repercusión para su empresa. Así pues, el objetivo debe ser que toda decisión relativa a la tecnología ayude a mejorar la productividad de la empresa, la organización o de uno mismo.

1.2 INTRODUCCIÓN A LA AUDITORÍA

La palabra auditoría proviene del latín *auditorius,* y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

Auditoría es un proceso, de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organización, y utiliza eficientemente los recursos. Es un proceso metodológico para valorar y evaluar la confianza que se puede depositar en TI. La realización de las Auditorías corresponde a los auditores, pudiéndose dividirla en dos grandes grupos: ***La auditoría externa y la auditoría interna.***

1.2.1 Auditoría de TIC'S

El entorno tecnológico en el que viven las empresas ha experimentado un cambio muy significativo en los últimos 15 años. Actualmente cualquier organización cuenta con una red de ordenadores, siendo muchas las que ya cuentan con sus propias páginas web o utilizan el comercio electrónico para comunicarse con sus clientes, proveedores o trabajadores.[1]

Las nuevas tecnologías más que una dificultad pueden ser una oportunidad para mejorar la posición de la auditoría dentro de las organizaciones, convirtiéndose en un apoyo de la alta dirección para mejorar la gestión y garantizar la existencia de un entorno de control adecuado *(véase en la figura 1.1).* Evaluando y comprobando los controles y procedimientos más complejos, esto mediante la realización de cualquier procedimiento, la emisión de los informes o la comunicación con auditados o receptores de los informes todo se realiza ahora utilizando las posibilidades que los ordenadores y las diferentes aplicaciones ponen a nuestra disposición.

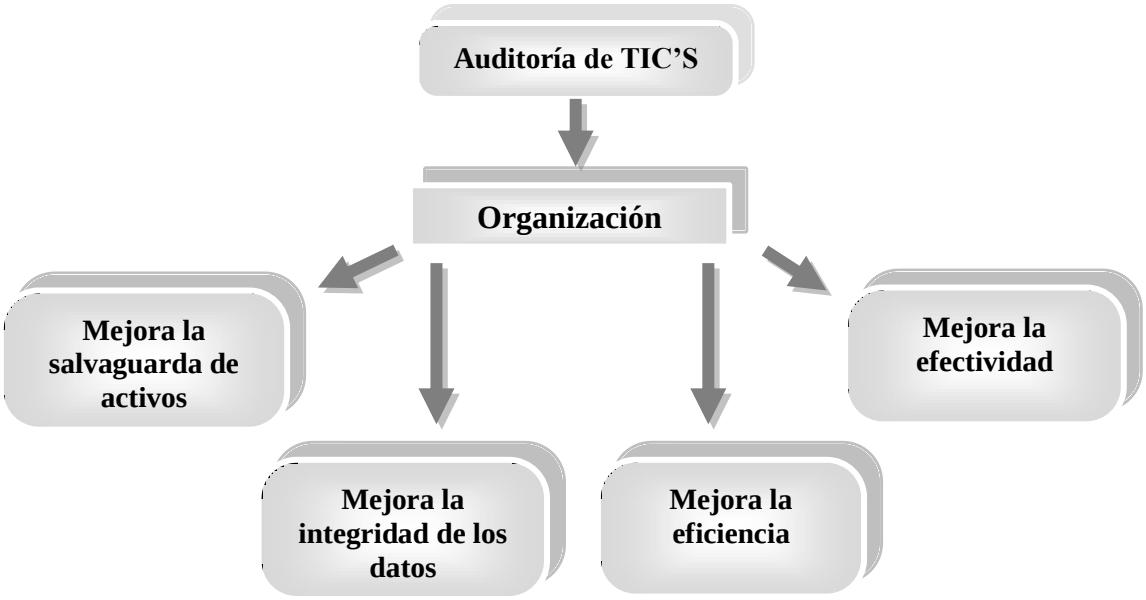


Figura 1.1 Diagrama de Auditoría de Tic's

[1] Auditoría interna y nuevas tecnologías, Sergio Martín Díaz, www.ey.com/es Pag.1

1.3 EL PAPEL DE LOS ROUTERS EN LAS REDES MODERNAS

En una red de ordenadores muy pequeños, es factible utilizar transmisión simple o mecanismos secuenciales para mover datos de punto a punto. Una red Ethernet de área local (LAN) es esencialmente una red de difusión. En las redes de ordenadores más grandes, más complejas, los datos deben estar dirigidos específicamente al destino previsto.

Los routers de la red de datos directos mensajes o paquetes, basadas en las direcciones internas y las tablas de rutas o destinos conocidos que sirven a determinadas direcciones. Directivo de datos entre partes de una red es el propósito principal de un router. Las redes de ordenadores más grandes utilizan el protocolo TCP / IP. A continuación se ilustra la función principal de un router en una red IP pequeña *(véase Figura 1.2)*.

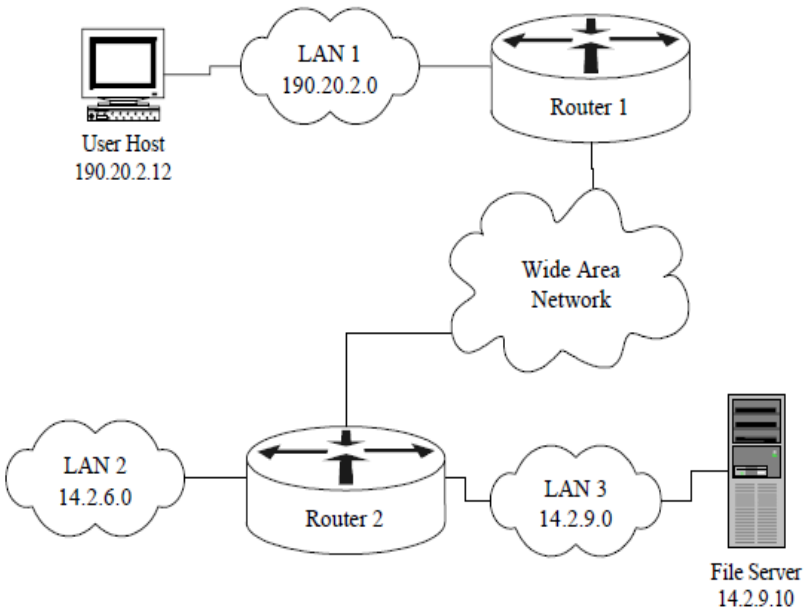


Figura 1.2 Una red simple con dos routers

Si el host de usuario (arriba a la izquierda) tiene que enviar un mensaje al servidor de archivos (abajo a la derecha), simplemente crea un paquete con la dirección 14.2.9.10, y envía el paquete a través de LAN 1 a su puerta de enlace, Router 1. Consultar con su tabla de enrutamiento interna, 1 router envía el paquete al enrutador 2. Consultar con su propia

tabla de enrutamiento, el router envía el paquete de 2 a través de LAN 3 al servidor de archivos. En la práctica, el funcionamiento de cualquier gran red depende de las tablas de encaminamiento en todos sus routers constituyentes. Sin ruteo robusto, las redes más modernas no pueden funcionar. Por lo tanto, la seguridad de los routers y sus valores de configuración es vital para el funcionamiento de la red.

Además de dirigir los paquetes, un router puede ser responsable de filtrar el tráfico, permitiendo que algunos paquetes de datos para pasar y rechazar otros. El filtrado es una responsabilidad muy importante para los routers, sino que les permite proteger los ordenadores y otros componentes de red de tráfico ilegítimo u hostil.

En la Auditoría en ruteador se debe revisar:

- Control de Accesos.
- Confidencialidad y Autenticación.
- Manejo de Bitácoras.
- Políticas de Respaldo de Configuraciones.
- Seguridad en Protocolos de Ruteo.
- Acceso Remoto.
- Vulnerabilidades Conocidas.
- Servicios Activos.

1.4 METODOLOGÍAS DE GOBIERNO EN TI (NIST, COBIT, ITIL)

Hoy en día, casi todas las organizaciones están utilizando la Tecnología de la Información (TI) en sus modelos y procesos de negocio. El Gobierno de TI deberá alinear proyectos tecnológicos con los objetivos estratégicos de la organización, asegurando el resultado prometido, un resultado económico y una obtención de ventajas competitivas. Para un buen Gobierno de TI, éste debe apoyarse en un marco de estándares y normas de comportamiento para garantizar que la unidad de TI soporte los objetivos de negocio de la organización.

Respecto a las metodologías, no existe una metodología unificada para la Gobernanza de TI. Existen metodologías que ayudan y facilitan un buen Gobierno de TI como son:

- NIST
- COBIT
- ITIL

NIST

NIST (Instituto Nacional de Estándares y Tecnología). Para llevar un control de riesgos dentro de TI, NIST nos presenta la Guía de Gestión de Riesgo en Sistemas de Tecnología de la Información la cual abarca: Evaluación de riesgos, Reducción de riesgos. Para la evaluación de riesgos tenemos abarcar nueve pasos los cuales se describen a continuación:

1. **Caracterización del sistema**
   El primer paso es definir el alcance del esfuerzo.
2. **Identificación de amenazas**
   Una amenaza es la posibilidad de que una determinada fuente de amenaza para ejercer con éxito una determinada vulnerabilidad.
3. **Identificación de las vulnerabilidades**
   El análisis de la amenaza a un sistema de TI debe incluir un análisis de las vulnerabilidades asociadas con el entorno del sistema (fallas o debilidades).
4. **Análisis de control**
   El objetivo de este paso es analizar los controles que se han implementado, o están previstos para su ejecución, por la organización para minimizar o eliminarla posibilidad (o probabilidad) de una amenaza que está ejerciendo una vulnerabilidad del sistema.
5. **Determinación de probabilidad**
   Para obtener una calificación de riesgo global que indica la probabilidad de que una vulnerabilidad potencial que puede ejercer en la construcción del entorno de las amenazas asociadas.

6. **Análisis del impacto**

   Este paso se enfoca en la importancia de determinar la medición del nivel de riesgo que tiene el impacto adverso como resultado de un ejercicio de éxito la amenaza de una vulnerabilidad.

7. **Determinación del riesgo**

   El propósito de este paso es evaluar el nivel de riesgo para el sistema de TI.

8. **Las recomendaciones de control**

   Durante este paso del proceso, los controles que podrían mitigar o eliminarlos riesgos identificados, según corresponda a las operaciones de la organización.

9. **Resultados de la documentación**

   Una vez que la evaluación del riesgo se ha completado (las fuentes de amenazas y vulnerabilidades identificadas, los riesgos evaluados, y los controles recomendados previstos), los resultados deben ser documentados en un informe oficial o la rueda de prensa.

COBIT

El marco de trabajo COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

Orientado al negocio: La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio *(véase Figura 1.3).*

El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

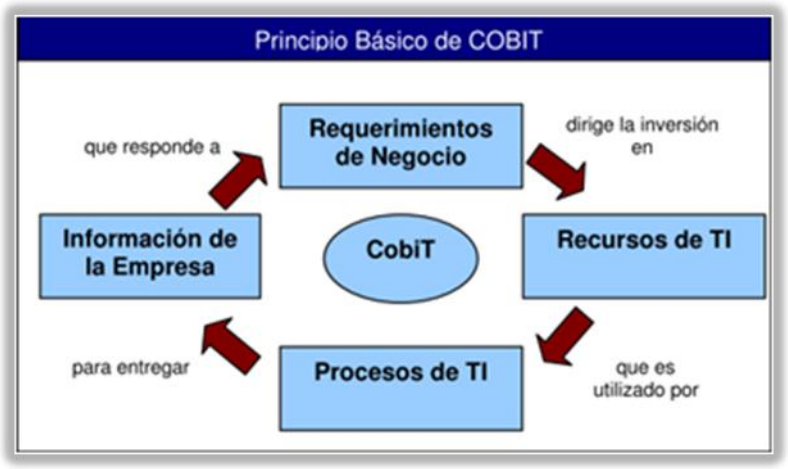


Figura 1.3 Marco de Trabajo Cobit

Criterios de información de COBIT: Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- La **efectividad** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- La **eficiencia** consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
- La **confidencialidad** se refiere a la protección de información sensitiva contra revelación no autorizada.
- La **integridad** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La **disponibilidad** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento.

  También concierne a la protección de los recursos y las capacidades necesarias asociadas.

- El **cumplimiento** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- La **confiabilidad** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

Orientado a Procesos: COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son **Planear y Organizar, Adquirir e Implementar, Entregar y dar Soporte y Monitorear y Evaluar**. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. La incorporación de un modelo operativo y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iníciales más importantes hacia un buen gobierno. Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco de COBIT, estos dominios. *(véase Figura 1.4)*

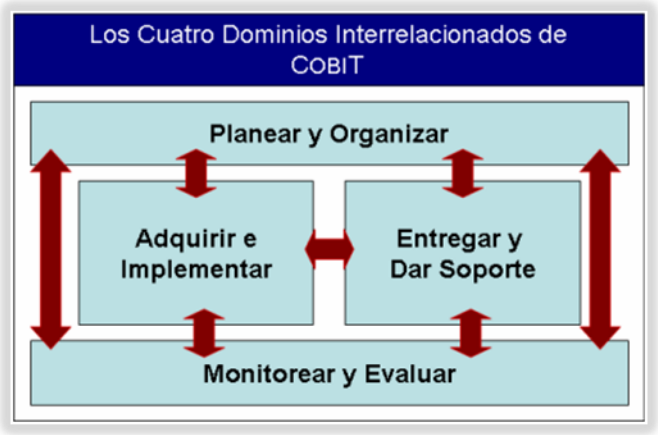


Figura 1.4 Dominios del Cobit

1. **Planear y Organizar (PO)**: Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
2. **Adquirir e Implementar (AI)**: Proporciona las soluciones y las pasa para convertirlas en servicios.
3. **Entregar y Dar Soporte (DS)**: Recibe las soluciones y las hace utilizables por los usuarios finales.
4. **Monitorear y Evaluar (ME)**: Monitorear todos los procesos para asegurar que se sigue la dirección provista.

ITIL

Los departamentos de informáticas; por la complejidad de sus procesos, de sus activos, de sus profesionales, de su "deslinde" del resto de la organización, y en general, por su difícil e indescifrable entramado, requieren de un conjunto de metodologías y herramientas que los ayuden a prestar sus servicios de una manera eficaz y efectiva. Por muchos años, todo estuvo centralizado y controlado desde una especie de jefatura superior. Sin embargo, con el advenimiento de Internet, la complejidad de los negocios, la globalización, la fuerte competencia, y la necesidad de sobrevivir en un contexto cada vez más enrarecido, los directores de informática han necesitado herramientas que les ayuden a añadir valor y al mismo tiempo les permita gestionar sus recursos, en muchos casos intangibles y estratégicos, de manera óptima. ITIL® es una de esas herramientas que saltan a la palestra para proporcionar al gerente IT la ayuda necesaria para que pueda lograr los objetivos organizaciones de manera productiva.

ITIL® (*Information Technology Infrastructure Library*) es un conjunto de mejores prácticas (procedimientos, técnicas, métodos, o actividades eficientes y efectivos en proporcionar un determinado resultado), enmarcadas en un conjunto de procesos (biblioteca) cuyo objetivo es organizar de manera productiva y holística los diferentes servicios que proporciona el departamento de tecnología de la información (informática) de una organización.

Definido en los años 80 y popularizado durante los 90s, ITIL® trata de "poner en cintura" a los departamentos de informática, al organizar el "caos" generado por la generación Cliente/Servidor, concepto que estuvo influenciado por la conocida tendencia de sistemas abiertos (Open Systems), compuesta por herramientas tecnológicas (Hardware, Software y Telecomunicaciones) integradas de manera "armónica", e interactuando perfectamente entre sí. Todo después de un fuerte dominio de mercado por parte del gigante azul IBM.

Creado por la OGC (Office of Government Commerce) del Reino Unido[2] y popularizado por analistas, consultores, y empresas de software. ITIL se ha convertido en un estándar de facto, presenta entre sus principales beneficios los siguientes:

1. Abre el camino a un concepto en boga (el Gobierno IT) que trata de auditar y controlar de alguna manera las decisiones de inversión y presupuesto de muchos departamentos de IT.
2. Introduce un orden en los elementos técnicos y tecnológicos que conformar la infraestructura informática de una organización, relaciona esos elementos, facilitando la gestión y legalidad de todos sus componentes, y en general.
3. Trata de ahorrar el coste de la prestación de servicios de IT en el largo plazo. En resumen, se trata de una nueva "moda" informática, que trata de cubrir las mismas deficiencias que han prevalecido siempre, y que de algún modo han legitimado la evolución conceptual y pragmática de la informática.

Para poder cumplir con los acuerdos de servicios con los clientes denominados (*Service Level Agreements* – SLA), la biblioteca ITIL® se divide en dos grandes bloques:

1. Soporte a los Servicios IT.
2. Entrega o Provisión de Servicios.

A su vez, cada una de las dos grandes bibliotecas que conforman ITIL se divide en los siguientes procesos:

[2] www.itil.co.uk

Soporte a los Servicios IT	Entrega o Provisión de Servicios
Service Desk *	Gestión del Nivel de Servicios (SLA)
Gestión de Incidencias	Gestión Financiera
Gestión de Problemas	Gestión de Capacidad (Capacity Planning)
Gestión de Configuración	Gestión de Continuidad
Gestión de Cambios	Gestión de Disponibilidad
Gestión de Versiones	
*El único que es una función, no un proceso	

Tabla 1.1 Procesos de ITIL

Cada uno de estos procesos tiene vida y/o autonomía propia. Organizándose de acuerdo a sus necesidades. Quizás el más popular y utilizado es el Service Desk (el cual es una función organizacional), la gestión de incidencias, la de problemas y gestión de cambios.

ITIL es un intento interesante de organizar y "poner en cintura" a los departamentos de informática o IT. Persigue, entre otras cosas, el ahorre de costes en el largo plazo, así como el incremento en productividad y eficiencia de los informáticos.

Algunas debilidades de ITIL se manifiestan en lo complejo y costoso que resulta su implantación en grandes organizaciones. Nuevas versiones de ITIL aparecerán e irán realizando "correcciones" a las mejores prácticas, el ciclo de la tecnología seguirá su curso, nuevos conceptos, herramientas, tecnologías y técnicas emergerán, y validarán si el concepto de ITIL es una intento válido de mantener en orden, sin duda alguno, uno de los departamentos más difíciles de gestionar para la alta gerencia de cualquier organización.

Para clarificar el concepto, *(véase Figura 1.5)* presenta una puesta en marcha estándar simulada de ITIL en una organización. Teóricamente se describen los puntos y pasos para su efectiva implantación.

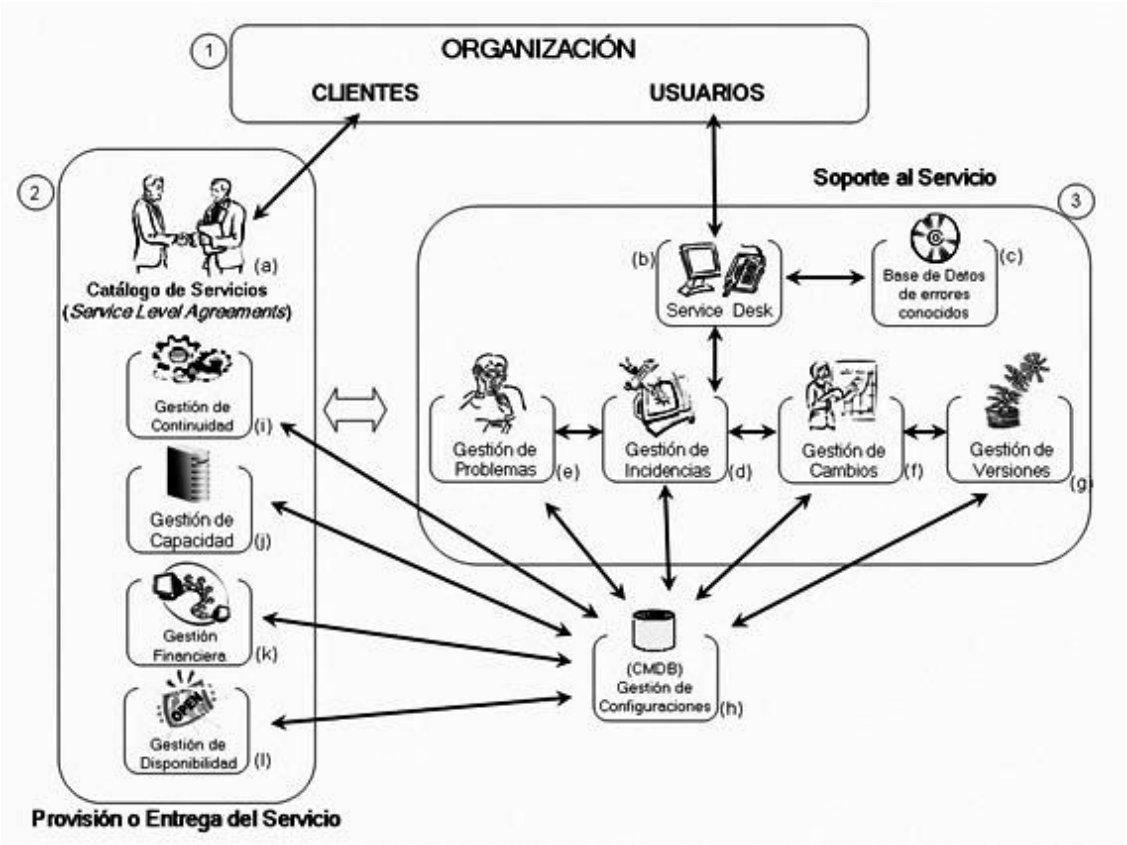


Figura 1.5 Cómo funciona ITIL

Paso 1 y 2 (a) – Todo comienza con la organización como gran demandante de servicios informáticos, el cliente o el que asigna y decide el presupuesto para estos servicios de la organización acuerda o negocia los acuerdos de servicios (SLA) con la dirección de informática.

Paso 3 (b) – Una vez puestos en marcha los servicios se define e instala un departamento o unidad de Service Desk (escritorio de ayuda), el cual será el punto de contacto de los usuarios de los servicios con el departamento de informática.

Paso 3 (c) – Los responsables del Service Desk, reciben y registran las solicitudes de los usuarios. En casos de incidentes de los servicios, primero buscan en la base de datos de errores conocidos o una especie de base de datos de conocimientos, para verificar si la solución al incidente existe, y así dar la solución al usuario de forma inmediata.

Paso 3 (d) – En caso de no poder solucionar el incidente al usuario, el operador de Service Desk lo escala a la persona apropiada para que lo soluciones. En otras palabras se pasa a la Gestión de Incidentes para que se busque la solución al usuario.

Paso 4 (e) – Si el incidente es recurrente y/o no es encontrado, se pasa a la Gestión de problemas en donde se buscará la solución definitiva.

Paso 4 (f) – Muchas veces los usuarios solicitan nuevos servicios a la gerencia de informática. Service Desk en este caso abre una petición de servicios y lo pasa a la Gestión del Cambio para que se abra un Cambio y se proceda, previa evaluación por parte de un comité asesor (CAB), con su implementación. Un cambio es toda petición de servicios que cambia la infraestructura informática de la organización.

Paso 4 (g) – La gestión de versiones se refiere, como su nombre lo indica, al mantenimientos de versiones de software por parte de la dirección informática. Abarca la gestión tecnológica y control legal de las versiones de software instaladas en la infraestructura de la organización.

Paso 4 (h) – La base de datos de configuración o CMDB mantiene el inventario de todos los ítems de configuración (por ejemplo, PCs, impresoras, software, documentación, personas, etc.) de la organización, la cual es accedida y actualizada por los diferentes procesos que conforman ITIL.

Pasos 2 (i), (j), (k) y (l) – Son necesarios y estratégicos para mantener los servicios informáticos operando de manera efectiva y eficaz.

CAPÍTULO 2. ANTECEDENTES HISTÓRICOS DE LOS ROUTER

2.1 ROUTER

Un **router** o **enrutador**, es un dispositivo de hardware tiene como principal característica conectar múltiples redes y enviar paquetes destinados ya sea a sus propias redes o a otras redes.

Es considerado como un dispositivo de capa tres o capa de red, porque su decisión principal de envío se basa en la información del paquete IP de capa tres, específicamente la dirección IP de destino. Este proceso se conoce como **enrutamiento**.

El **enrutamiento** es un esquema de organización jerárquico que permite que se agrupen direcciones individuales. Estas direcciones individuales son tratadas como unidades únicas hasta que se necesita la dirección destino para la entrega final de los datos.

El enrutamiento es el proceso de hallar la ruta más eficiente desde un dispositivo a otro. El dispositivo primario que realiza el proceso de enrutamiento es el router.

Las dos funciones principales de un router:

- Los routers deben mantener tablas de enrutamiento y asegurarse de que otros routers conozcan las modificaciones a la topología de la red.
  Esta función se lleva a cabo utilizando un protocolo de enrutamiento para comunicar la información de la red a otros routers.
- Cuando los paquetes llegan a una interfaz, el router debe utilizar la tabla de enrutamiento para establecer el destino.
  El router envía los paquetes a la interfaz apropiada, agrega la información de entramado necesaria para esa interfaz, y luego transmite la trama.

Un router es un dispositivo de la capa de red que usa una o más métricas de enrutamiento para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red.

Las métricas de enrutamiento son valores que se utilizan para determinar las ventajas de una ruta sobre otra.

Los protocolos de enrutamiento utilizan varias combinaciones de métricas para determinar la mejor ruta para los datos.

Los routers interconectan segmentos de red o redes enteras. Los routers toman decisiones lógicas con respecto a cuál es la mejor ruta para la entrega de datos.

Luego dirigen los paquetes al puerto de salida adecuado para que sean encapsulados para la transmisión. En la figura 2.1, se observa la representación del proceso de enrutamiento a través de las capas del modelo OSI.

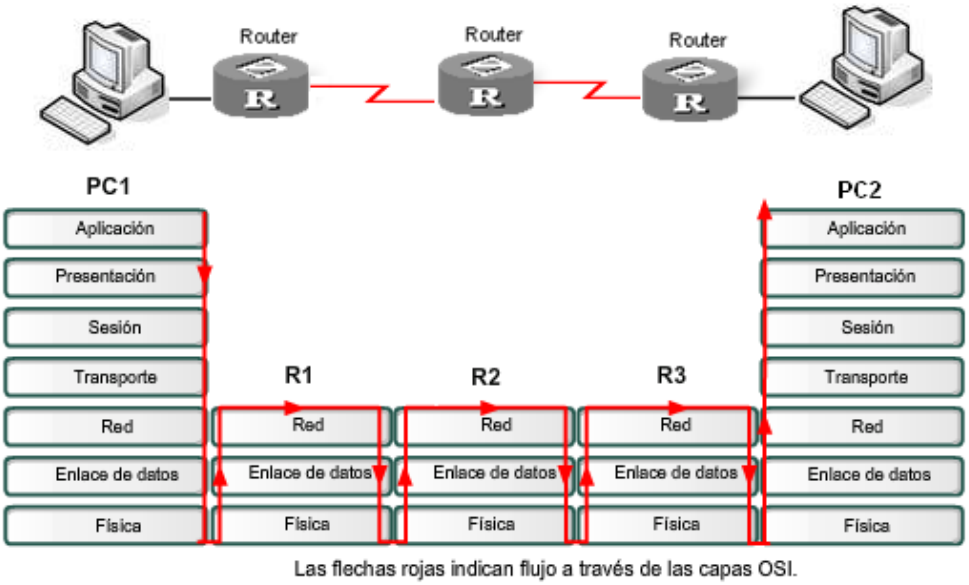


Figura 2.1 Proceso de Enrutamiento

Importancia de un Ruteador

1. Es el equipo de comunicaciones central de toda red de datos.
2. Es el elemento esencial de Internet.
3. A través de este equipo se interconectan los segmentos de red de usuarios.
4. Su funcionamiento se basa en la configuración establecida por el administrador.

2.1.1 Partes que integran un router

El router está integrado por partes internas y partes externas y son las siguientes:

Partes Externas. Por detrás podemos observar que incluye el conector de corriente, su botón de encendido y apagado, su puerto de consola, que es a través del cual lo conectamos a una PC para configurarlo, ya que por defecto ningún otro puerto de comunicación el router está activo. Además podemos ver puertos seriales (si los posee) y puertos fast-ethernet para conectar a la red. Ahora bien, un router posee dos conexiones, una hacia la red LAN y otra hacia los servicios de conexión para redes WAN.

Partes internas. Las partes internas de un router son:

- **Memoria RAM:** memoria de acceso aleatorio de tipo volátil (su contenido se pierde al apagar el router) se emplea para guardar tablas de ruteo, cache de conmutación y un ambiente de ejecución para el sistemas operativo del router.
- **Memoria NVRAM:** es una RAM no volátil que permite cargar la configuración del router.
- **Memoria Flash:** almacena una imagen del software del sistema operativo de cisco.
- **Memoria ROM:** almacena el código del POST.

2.2 TCP / IP Y EL MODELO OSI

TCP/IP está basado en un modelo de referencia de cuatro niveles. Todos los protocolos que pertenecen al conjunto de protocolos TCP/IP se encuentran en los tres niveles superiores de este modelo.[3]

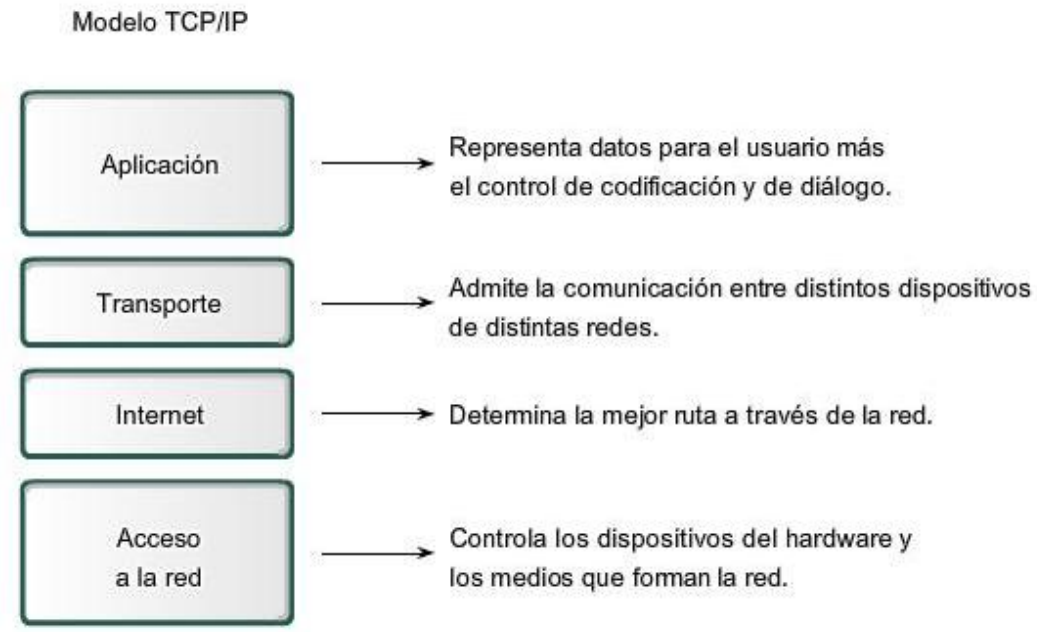


Figura 2.2 Modelo TCP/IP

[3] http://technet.microsoft.com/es-es/library/cc786900(v=ws.10).aspx

2.2.1 Origen de TCP / IP

El Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP) comprenden lo que se ve a menudo escrita como TCP / IP. De la Defense Advanced Research Projects Agency (DARPA) se originó TCP / IP. La esencia de Internet se ejecuta en los protocolos TCP / IP. La fuente definitiva de información sobre TCP / IP son las RFC, o "Solicitud de comentarios" emitidos por la Internet Engineering Task Force.[4]

Tenga en cuenta que además de TCP / IP existen otros protocolos como IPX de Novell (Intercambio de paquetes) que se puede utilizar con los routers. Además, algunos routers se pueden utilizar para "traducir" entre los diferentes protocolos que se ejecutan en uno y otro lado de sí mismos.

2.2.2 El modelo OSI

Después de TCP / IP fue bien establecidos y otros protocolos de red, tales como DECnet e IPX de Novell estaban en funcionamiento, la Organización Internacional de Normalización (ISO) ha desarrollado el Open Systems Interconnection (OSI), modelo de referencia de siete capas. **El modelo OSI es una colección de varias capas de protocolo compatibles.**

Estas siete capas son las que se mencionan a continuación:

- **Capa 7:** Capa de aplicación - se ocupa de los servicios como el correo electrónico y transferencia de archivos.
- **Capa 6:** Capa de presentación - se ocupa de formato, codificación y compresión de datos.
- **Capa 5:** Capa de Sesión - se ocupa de la configuración y gestión de sesiones entre las aplicaciones.

[4] RFC significa solicitud de comentarios, http://www.ietf.org/rfc.html

- **Capa 4:** Capa de transporte - con un extremo a otro de recuperación de errores y la entrega de mensajes completos.
- **Capa 3:** Capa de red - se ocupa de la transmisión de paquetes y conexiones que se establecen.
- **Capa 2:** Capa de enlace de datos - se ocupa de la transmisión de paquetes en un enlace físico dado.
- **Capa 1:** Capa Física - se ocupa de la transmisión de un flujo de bits y la definición del enlace físico.

Desde el desarrollo de TCP / IP precedió a la norma ISO, el "mapeo" de TCP e IP con el modelo de siete capas es sólo una aproximación. *(Véase la Figura 2.3)*

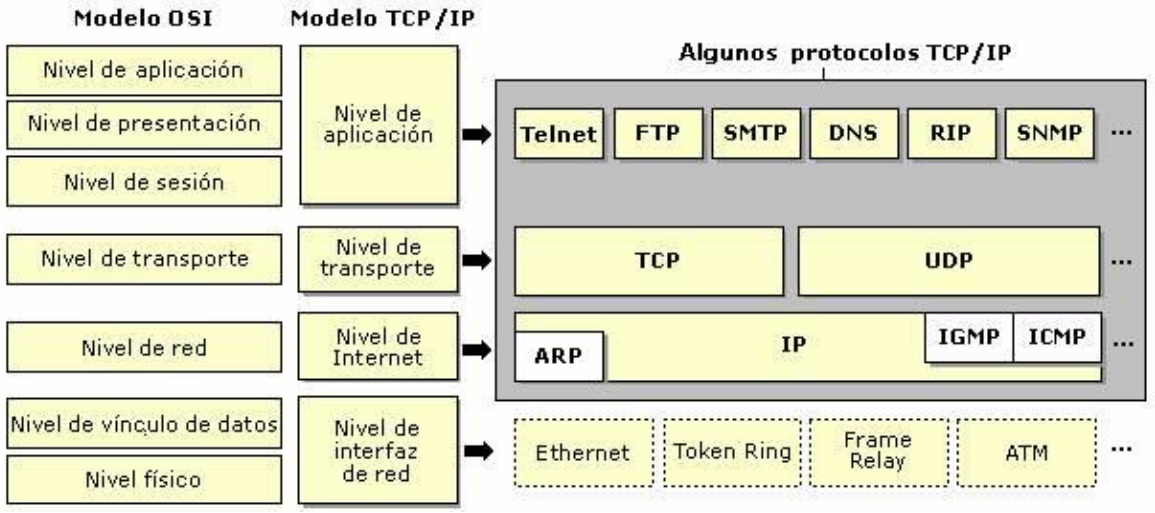


Figura 2.3 Capas de red y estándares

Enrutamiento se produce en tres capas, la capa de red. Para entender completamente el enrutamiento que es útil para apreciar algo de lo que pasa debajo de ella en la capa de enlace de datos, y algunos de esto se discute en las secciones siguientes.

Sin embargo, la capa física está en un nivel de detalle muy por debajo de las preocupaciones de este documento. Se refiere a la transmisión de un flujo de bits no

estructurada sobre un enlace físico. Se trata de detalles tales como el voltaje de la señal y la duración, o detalles de señalización ópticos de fibra. También cubre los aspectos mecánicos de los conectores y cables. También puede cubrir algún tipo de control de bajo nivel de error.

Revisión de enrutamiento IP y Arquitecturas de propiedad intelectual

Si uno está tratando con una red de área local (LAN), generalmente no hay necesidad de encaminamiento, los routers, TCP / IP, o direcciones IP. Dentro de un todo, LAN estará a cargo de Media Access Control (MAC) y un protocolo de red LAN, como Ethernet. En este nivel, la mayoría de los protocolos se definen por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE normas). Por ejemplo, IEEE 802.3 es el Ethernet (CSMA/CD), es 802.4 token bus y token ring es 802,5. Por encima de las normas de la MAC, pero aún dentro de la capa de enlace de datos, es el estándar IEEE 802.2 Control de enlace lógico.

El estándar IEEE 802.1 Alto Nivel de la interfaz corresponde a la parte de la capa de red OSI. Si esto le parece confuso, no te preocupes, no es esencial para la comprensión de los routers.

Lo que es importante tener en cuenta es que las direcciones MAC se utilizan dentro de una LAN.

Cada dispositivo de la LAN tiene un algo así como una tarjeta de interfaz de red (NIC), que tiene una única dirección MAC. Por ejemplo, en una LAN Ethernet que cada dispositivo tiene una adecuada tarjeta de red Ethernet, por ejemplo 100BaseT. La dirección MAC se añade a la parte delantera de los datos antes de que se coloque en la LAN. Cada dispositivo de la LAN a la escucha de los paquetes con la dirección.

Una vez que el mensaje está destinado a salir de una LAN con destino a un viaje a través de una red de área amplia (WAN) a otra LAN, se debe utilizar una dirección IP.

Mientras que uno puede imaginar las conexiones lógicas en varias capas en una pila de protocolos, en realidad, los bits sólo se pueden mover de un dispositivo a otro en la capa física. Así, los datos comienzan en una aplicación de forma relativamente alto en una pila de protocolos y trabaja su manera abajo de la pila de la capa física. En este punto, se transfiere a otro dispositivo y se abre camino hasta la pila de protocolos en ese punto.

¿Hasta qué punto la pila va depende de si ese dispositivo es el destinatario final de los datos o simplemente un dispositivo intermedio?

La Figura 2.4, ilustra este proceso. Tenga en cuenta que los datos pueden pasar a través de muchos dispositivos intermedios en su camino desde el host emisor al destinatario final.

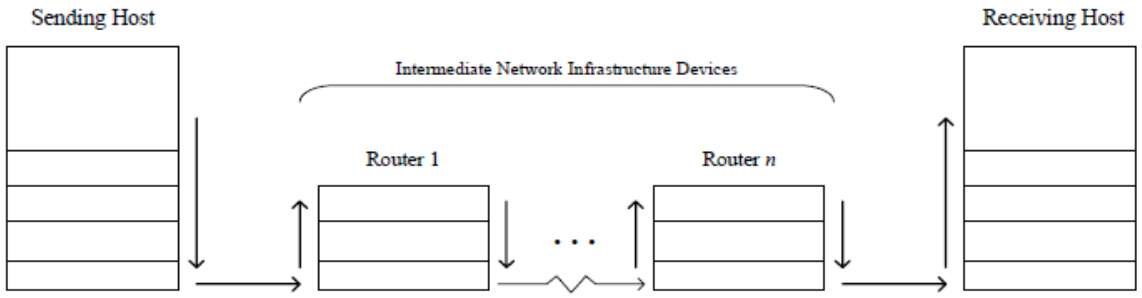


Figura 2.4 Transferencia de datos a través de pilas de protocolos

En el camino de abajo de la pila, cada capa añade un encabezado relevante para el paquete. La cabecera lleva el nombre de la capa de protocolo que se añade. Cada nueva cabecera se añade delante de todas las cabeceras de nivel superior. En la capa de red, la cabecera IP añadida contendrá la dirección IP de destino (además de otra información).

En la capa de enlace de datos, también llamado a veces la capa de acceso de medios, una nueva cabecera que contiene una dirección MAC se añade delante de la cabecera IP. En el camino hacia la pila, una cabecera se eliminará en cada capa. En la Figura 2.5, le ayudará a visualizar la forma en que las cabeceras se añaden.

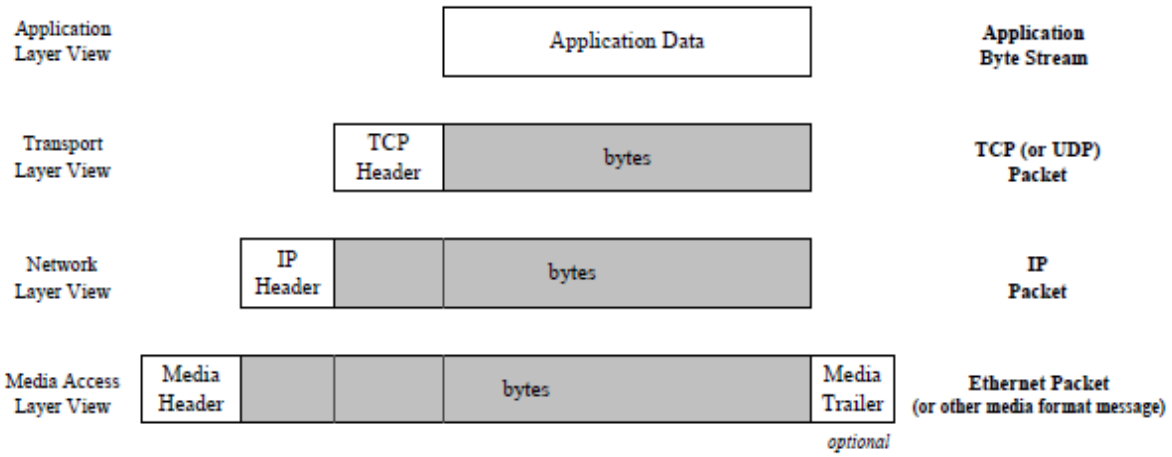


Figura 2.5 Ajuste de los cabezales inferiores de nivel alrededor de los datos

Direcciones MAC

Las direcciones MAC, a veces se denominan direcciones Ethernet de 48 bits de longitud. Ellos son asignados por el dispositivo (o tarjeta) fabricante. Cada dirección es única y fija a una pieza particular de hardware. (En algunos dispositivos más recientes, es posible cambiarlas, pero normalmente esto no se debe hacer.)

Como se mencionó anteriormente, las direcciones MAC se utilizan dentro de una LAN mediante dos capas (enlace de datos) protocolos.

Tradicionalmente 24 bits identifican al fabricante y 24 bits de acto como un número de serie para identificar la unidad. Algunos fabricantes han tenido más de un número de identificación (más de un bloque de números de serie).

Además, debido a las fusiones y adquisiciones de la identificación del fabricante no es tan "limpia" como lo era antes. Sin embargo, todos los dispositivos de interfaz de red tienen direcciones únicas en el mundo a menos que sus PROM han sido reescritos.

Direcciones IP

Actualmente, las direcciones IP son de 32 bits de longitud. Son utilizados por la capa de tres dispositivos tales como routers. A diferencia de las direcciones MAC, direcciones IP son jerárquicas. Hay cuatro "clases" de direcciones IP, a que se refiere como: Clase A, Clase B, Clase C, y D. Además, hay una serie de direcciones especiales.

Las **direcciones especiales** se utilizan para cosas como para transmitir a todos los hosts de una red o para especificar un paquete de loopback que nunca dejará el host. La clase determina qué parte de la dirección de 32 bits se utiliza para especificar la dirección de red y la cantidad que se utiliza para especificar el host dentro de dicha red. La clase está determinada por los primeros uno a cuatro bits de la dirección.

Para cualquier clase, también es posible tomar la parte del host de la dirección y la brecha más amplia que en dos campos, que especifican una dirección de subred y una dirección de host, respectivamente. Esto se hace mediante la especificación de un parámetro llamado una **máscara de subred.**

2.3 REVISIÓN DE REDES TCP/IP

En una pequeña red informática, es factible el uso de difusión simple o secuenciales mecanismos (token) para mover datos de punto a punto. Una **red de área local** se compone de un número relativamente pequeño de los hosts conectados a través de un área física relativamente pequeña. "Relativamente pequeña" es la frase importante. Para dar un significado al término "relativamente", considera que una red Ethernet 10BaseT (10 megabits por segundo utilizando cable de par trenzado) tiene un máximo habitual de 1024 estaciones en una distancia máxima de cable de 2500 metros.

Por ejemplo, una LAN de la oficina típica, usando Ethernet 100BaseT, podría tener 100 computadoras (y las impresoras) conectados a un conmutador o un conjunto de centros.

Una red Ethernet de área local (LAN) es esencialmente una red de autobuses (lógica) de difusión basado en, aunque la ejecución física puede usar cubos (con una topología en estrella física). Como era de esperar, las redes LAN de difusión deben hacer frente a las colisiones, ya sea por prevenir su aparición o detección de los mismos y tomar las medidas oportunas. Token basado en redes de área local a evitar colisiones, permitiéndose sólo un huésped en el momento de transmitir.

Normas que se relacionan con redes de área local son los principales de la serie IEEE 802.x. Por ejemplo, 802.3 es el Media Access Control (MAC) estándar para CSMA / CD (el estándar de Ethernet), mientras que 802.5 es el estándar MAC para Token Ring. Justo por encima del nivel de MAC es el Control de enlace lógico (802.2) estándar y por encima de que la interfaz de alto nivel (802.1) estándar.

Dentro de una LAN, se hace frente con una dirección MAC. Entre las redes LAN utilizando TCP / IP se realiza mediante direcciones IP. Si se pierde en este punto, sigue leyendo porque gran parte de esto se explica a continuación.

Propósito de un router

En las redes de ordenadores más grandes, más complejas, los datos deben ser dirigidos con más cuidado. En casi todos los casos, las grandes redes se compone en realidad de una colección de LAN que se interconectan o "interconectados". Aquí es donde los routers entrar routers toman mensajes de la red de datos de una red LAN y convertirlos en paquetes adecuados para la transmisión más allá de la LAN en una red de área amplia (WAN). El objetivo es casi siempre para obtener estos paquetes a otro LAN y finalmente al host correcto en que LAN. Parte de la "conversión" proceso consiste en agregar un encabezado de un paquete.

Otros routers por lo general sólo se ven en la información del encabezado de un paquete, no en el contenido o datos en el paquete.

Los routers también tomar decisiones acerca de dónde enviar estos paquetes, basado en: las direcciones contenidas en las cabeceras de los paquetes y una tabla de rutas mantenidas en el router. Actualización de las tablas de enrutamiento y reenvío de paquetes de datos entre las partes de una red es uno de los propósitos principales de un router.

Paquetes de construcción y paquetes de desenvolver son las funciones adicionales del router realizadas por los routers de la primera y última, respectivamente, que pasa a través de un mensaje. Además de dirigir los paquetes, un router puede ser responsable de filtrar el tráfico, permitiendo que algunos paquetes para pasar a través y rechazar otros.

El filtrado puede ser una función muy importante de los routers, sino que les permite ayudar a proteger las computadoras y otros componentes de red.

Tablas de enrutamiento

Como se mencionó, una de las tareas de un router es para mantener las tablas de enrutamiento que se utilizan para decidir dónde un paquete es para ir y por lo tanto la interfaz que debe ser enviado. En el pasado estas tablas fueron construidas y actualizadas a mano y esto se conoce como enrutamiento estático. En el enrutamiento dinámico, el router se entera de que varias direcciones son relativas a sí mismo y construye las tablas de enrutamiento basadas en esta información. Hay una serie de planes o protocolos de enrutamiento de los routers para adquirir y compartir información de la tabla de enrutamiento.

2.4 ARQUITECTURA FUNCIONAL BÁSICA DEL ROUTER

¿Por qué tener un router para fines especiales?, ¿Cuáles son algunas de las motivaciones para el uso de una dedicada, purpose-built del router en lugar de una máquina de propósito general con un sistema "estándar" operativo (SO)?, ¿Qué justifica este gasto, y lo que justifica la molestia de aprender un nuevo sistema?

La respuesta, en parte, se refiere a rendimiento: un router con fines especiales pueden tener un rendimiento mucho más alto que un ordenador de propósito general, con la funcionalidad de enrutamiento clavada en ella. Además, una potencialmente puede añadir más conexiones de red a una máquina diseñada para tal fin, porque puede estar diseñado para soportar más ranuras para tarjetas de interfaz. Así, un dispositivo de propósito especial será probablemente una solución de menor costo para un nivel dado de funcionalidad.

Pero también hay una serie de prestaciones de la seguridad a un router de propósito especial, en general, la consolidación de enrutamiento de red y las funciones relacionadas en unos dispositivos dedicados restringe el acceso y los límites de la exposición de las funciones críticas. Por un lado, un sistema operativo del router especializado (como el sistema operativo de Cisco Internetwork o IOS) puede ser más pequeño, mejor entendido y más probado a fondo de un sistema operativo de propósito general. (Tenga en cuenta que por razones de brevedad, el IOS se utilizará como término en este documento para hacer referencia del sistema operativo del router y el software asociado). Esto significa que es potencialmente menos vulnerable.

Además, el mero hecho de que se trata de diferentes medios que un atacante tiene una cosa más que aprender, y que las vulnerabilidades conocidas en otros sistemas no son de ayuda para el atacante del router. Por último, el enrutamiento especializado de software permite a una aplicación más completa y más robusto de filtrado. Filtrado es útil como un "cortafuegos" técnica, y también se puede utilizar para redes de partición y prohibir o restringir el acceso a ciertas redes o servicios. Utilización de filtros, algunos protocolos de enrutamiento puede prohibir la publicidad de las rutas a los vecinos, ayudando así a proteger ciertas partes de la red.

Descripción del hardware del router típico

Un router es esencialmente sólo otro equipo. Por lo tanto, similar a cualquier otro equipo, que tiene una unidad central de proceso (CPU), varios tipos de memoria, y las conexiones a

otros dispositivos. Por lo general, un router no tiene un disco duro, unidad de disquete o CD-ROM.

Velocidad de la CPU y el tamaño de la memoria son consideraciones importantes para el rendimiento y las capacidades (por ejemplo, algunas de las características de Cisco IOS requieren más de la cantidad predeterminada de la memoria, y sofisticados servicios de seguridad por lo general requieren de cálculo considerable).memoria almacena el IOS (u otro enrutador OS), y si hay suficiente de flash puede almacenar más de una versión de IOS. La Figura 2.6, muestra una simple representación de la estructura de hardware de un router hipotético.

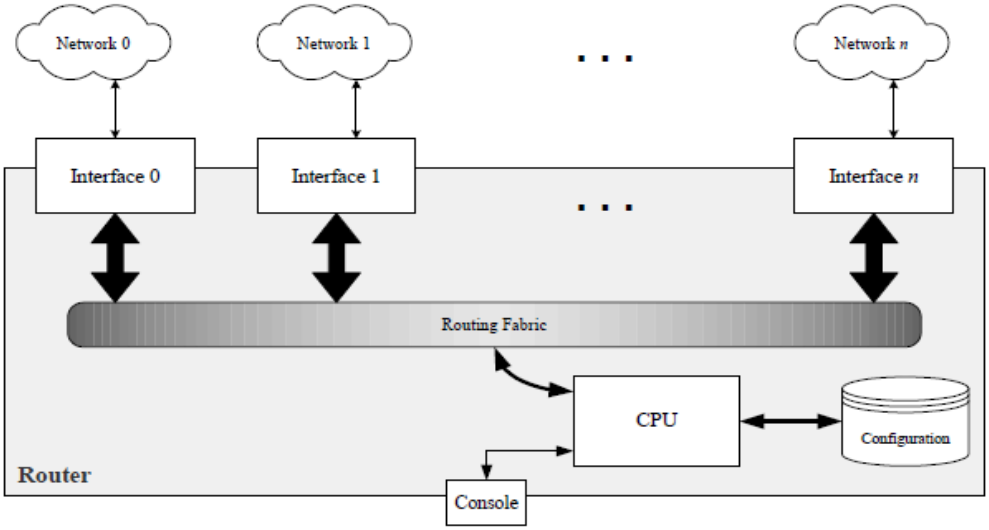


Figura 2.6 Estructura de de un router hipotético

Las interfaces proporcionan las conexiones físicas de un router a las redes. Tipos de interfaz incluyen Ethernet, Fast Ethernet, Token Ring, FDDI, de baja velocidad de serie en serie, rápido, HSSI, ISDN BRI, etc. Cada interfaz se nombre y un número.

Las tarjetas de interfaz encajan en las ranuras de un router, y un cable externo del tipo adecuado está conectado a la tarjeta. Además de un número de interfaces, casi todos los routers tienen un puerto de consola proporcionando una conexión serie asíncrona (RS-232).

Además, la mayoría de los routers tienen un puerto auxiliar, que se utiliza con frecuencia para la conexión de un módem para la gestión del router. Estos puertos de hardware no se debe confundir con el concepto de los números de puerto de red del protocolo, tales como los "bien conocidos" los números de puerto asociados con protocolos y servicios específicos, tales como el puerto TCP 23 se utiliza para Telnet.

Descripción del software del router típico

Al igual que en cualquier otro ordenador, un router se ejecutará un programa de control o sistema operativo (SO). Cada vendedor del router proporciona su sistema operativo propio router. En el caso de los routers de Cisco, corren sistema Cisco Internetwork Operating (IOS).

Es el IOS que interpreta la lista de control de acceso (ACL) y otros comandos en el router.

La configuración de inicio o de copia de seguridad se almacena en la NVRAM. Se ejecuta cuando se inicia el router. Como parte del proceso de arranque una copia de esta configuración se carga en la RAM. Los cambios realizados en una configuración en ejecución se hacen generalmente sólo en la memoria RAM y por lo general entran en vigor inmediatamente. Si los cambios en la configuración se escriben en la configuración de inicio, entonces también tendrá efecto en el reinicio. Los cambios realizados sólo en la configuración en ejecución se perderán al reiniciar el sistema.

Un router de funcionamiento tendrá un gran número de procesos de ejecución para apoyar los servicios y protocolos que el router debe apoyar.

Todos los routers soportan una gran variedad de comandos que muestran información sobre los recursos de qué procesos se están ejecutando y lo que, como el tiempo de CPU y memoria, que están consumiendo. Servicios innecesarios e instalaciones deberán ser desactivados para evitar el desperdicio de recursos de la CPU y la memoria.

Cada router debe tener un nombre único para identificar, y cada interfaz debe tener una única dirección de red asociada con ella. Además, la configuración básica de seguridad debe establecerse en cualquier router antes de que se conecte a una red operativa. Este tipo de consideraciones se discuten con más detalle más adelante en esta guía.

2.4.1 Protocolos del router y sus capas

Los protocolos se agrupan en función de la capa del modelo OSI al que corresponden.

Capa Física 1

Como se mencionó anteriormente, la capa física está definida por los estándares IEEE o normas similares que definen cuáles son las características físicas y eléctricas, principalmente.

Nivel de Enlace 2

El IEEE y otras normas que se aplican en este nivel también se han discutido previamente.

Red de Nivel 3

- **IP:** Internet Protocol (IP) proporciona una especificación para el formato de paquete y un poco confiables, sin conexión, en el mejor esfuerzo de entrega de los paquetes.
- **ARP:** Hosts utilizar el Address Resolution Protocol (ARP) para obtener la dirección MAC de otros hosts

La capa de transporte 4

- **TCP:** Transmission Control Protocol (TCP) es uno orientado a la conexión, el protocolo fiable. Antes de transmitir datos de una conexión debe ser establecido y después de la transmisión de datos se complete la conexión debe ser cerrada.
- **UDP:** User Datagram Protocol (UDP) es un protocolo sin conexión, el mejor esfuerzo sin garantía de entrega o la confirmación de la entrega. Tiene menos gastos generales de TCP. Cuando se habla de TCP / IP que están por lo general incluyendo implícitamente UDP.

- **ICMP:** Internet Control Message Protocol (ICMP) proporciona los mecanismos para hosts y routers para informar las condiciones de red y los errores a otros hosts y routers. (Por ejemplo, el comando ping se basa en ICMP.)
- **OSPF:** Open Shortest Path First es un relativamente complejo y de rápida convergencia de protocolo de enrutamiento.

  Se trata de un protocolo de pasarela interior que utiliza un algoritmo de enrutamiento de estado de enlace y requiere que una jerarquía de áreas de ser diseñado. Un área es una colección lógica de routers y redes.
- **RIP:** Protocolo de información de enrutamiento es un protocolo de enrutamiento dinámico que permite a los routers de la red para compartir información entre sí.

  Se trata de un protocolo de vector-distancia que permite que los routers para compartir sólo información con sus vecinos más cercanos. Se utiliza como un protocolo de pasarela interior.

Sesión Capa 5 y capa de presentación 6 y capa de aplicación 7

Estos protocolos han sido etiquetados (TCP) o (UDP) en función de la capa 5 de protocolo que se basan.

- **Telnet:(**TCP) Permite terminales orientados a los procesos de comunicación.
- **FTP:** File Transfer Protocol (TCP) permite transferencias de archivos entre ordenadores.
- **SMTP:** Simple Mail Transport Protocol (TCP) es bastante auto-explicativo.
- **DNS:** Domain Name System (tanto TCP como UDP) realiza servicio de nombres de la resolución mediante la traducción de nombres de host en direcciones IP y viceversa.
- **TFTP:** Trivial File Transfer Protocol (UDP), establece las transferencias de archivos sin ningún tipo de autenticación o seguridad.
- **SNMP:** Simple Network Management Protocol (UDP) permite a una estación de administración para atrapar a ciertos mensajes de información de los dispositivos de red.

CAPÍTULO 3. PRINCIPIOS GENERALES DE SEGURIDAD E IMPLEMENTACIÓN EN LOS ROUTER BAJO EL ESTANDAR NIST

3.1 PRINCIPIOS DE SEGURIDAD DEL ROUTER

Los routers pueden jugar un papel en la seguridad de las redes. En este capítulo se describen los principios generales para la protección de uno mismo router, la protección de una red con un router, y la gestión de un router de forma segura.

Protocolos TCP/IP "seguros"

- Protocolos de Red

  Aumentando el protocolo IP: IPSec, que permite Cifrado y autenticación.

- Librerías de programación

  Independientes del protocolo de aplicación: SSL, TLS (sobre los BSD Sockets), que permite Cifrado y autentificación.

- Pasarelas de Aplicación

  Dependientes del protocolo y la aplicación
- SSH (inicialmente, sobre Telnet) que permite Cifrado y autentificación.
- SOCKS (sobre los BSD Sockets), que permite autenticación y control de acceso localizado en los cortafuegos.

3.1.1 Protección del router

Seguridad física

Hay un número de maneras de proporcionar seguridad física aun router. La habitación que contiene el router debe estar libre de interferencia electrostática o magnética. Se debe tener controles de temperatura y humedad. Si se considera necesario por razones de disponibilidad o criticidad, una fuente de alimentación interrumpida (SAI) deben ser instalados y componentes de repuesto y piezas a la mano.

Para ayudar a proteger contra algunos ataques de denegación de servicio, y para que pueda soportar la más amplia gama de servicios de seguridad, el router debe estar configurado con la máxima cantidad de memoria posible. Además, el router debe ser colocado en una habitación cerrada con acceso a un solo pequeño número de personal autorizado.

Por último, los dispositivos físicos (por ejemplo, tarjetas PC, módems) que se utilizan para conectarse al router de almacenamiento requieren protección.

Sistema operativo

El sistema operativo del router es un componente crucial. Decide lo que cuenta con las necesidades de la red y utilizar la lista de funciones para seleccionar la versión del sistema operativo.

Sin embargo, la última versión de cualquier sistema operativo tiende a no ser el más confiable debido a su limitada exposición en una amplia gama de entornos de red.

Se debe utilizar la última versión estable del sistema operativo que cumpla con los requisitos de características.

Configuración de endurecimiento

Un router es similar en muchos equipos, ya que tiene muchos servicios habilitados por defecto. Muchos de estos servicios no son necesarios y puede ser utilizada por un atacante para la recopilación de información o para la explotación. Todos los servicios sin necesarios deben ser desactivados en la configuración del router.

Algunas personas se resisten a esta recomendación, usted puede sentir que el dinero de la memoria y por lo tanto los costos de un router se debe comprar con la cantidad mínima de memoria que necesita para apoyar su tarea.

Esto es un ahorro falso. El costo incremental de memoria adicional suele ser pequeño en comparación con el costo total de un router configurado totalmente, y el mayor rendimiento y flexibilidad que la memoria adicional proporcionará casi siempre vale la pena cuando amortizan en el número de usuarios y servicios que dependen en el router para la conectividad.

Además, la adición de memoria a un router operativo requiere tomar ese router fuera de servicio.

En la comunidad de Internet Service Provider, por ejemplo, se considera una mejor práctica del sector para dotar a todos los routers con la memoria operativa en medida de lo que puede contener.

3.1.2 Protección de la red con el router

Funciones en el perímetro de la Seguridad y la Política de Seguridad

Un router proporciona una capacidad para ayudar a asegurar el perímetro de una red protegida. Se puede hacer esto por sí mismo. El siguiente diagrama se muestra una topología típica con el router que es el componente que conecta a la red protegida a Internet. *(Véase la Figura 3.1)*

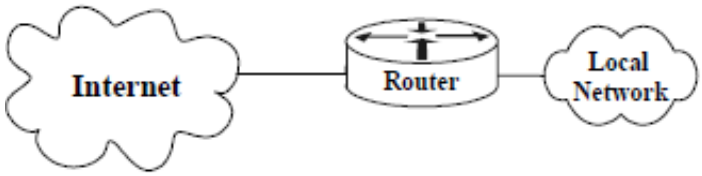


Figura 3.1 Topología típica con el router

Un router también se puede utilizar como parte del enfoque de defensa en profundidad, como se muestra en el diagrama siguiente. Actúa como la primera línea de defensa y se conoce como un encaminador de cifrado. Contiene una ruta estática que pasa todas las conexiones destinadas a la red protegida con el firewall. El servidor de seguridad proporciona control de acceso adicional sobre el contenido de las conexiones. También se puede realizar la autenticación del usuario. Se recomienda este enfoque sobre el uso de sólo un router, ya que ofrece más seguridad. *(Véase la Figura 3.2)*

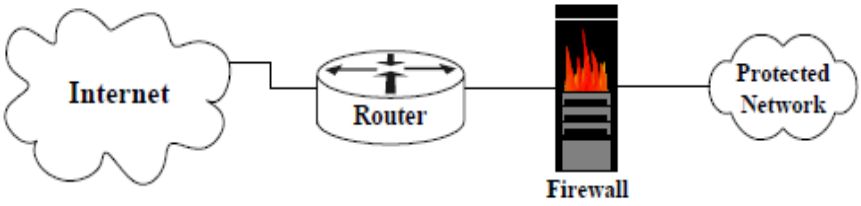


Figura 3.2 Topología típica de un router de Internet Configuración de la conexión

Otro método consiste en colocar un router en la conexión entre las instalaciones locales y de Internet, y luego otro router entre el firewall y la red protegida.

Esta configuración nos ofrece dos puntos en los que la política se puede hacer cumplir. También ofrece una zona intermedia, a menudo llamada la zona desmilitarizada (DMZ) entre los dos routers. La DMZ se usa a menudo para los servidores que deben ser accesibles desde Internet o una red externa. *(Véase la Figura 3.3)*

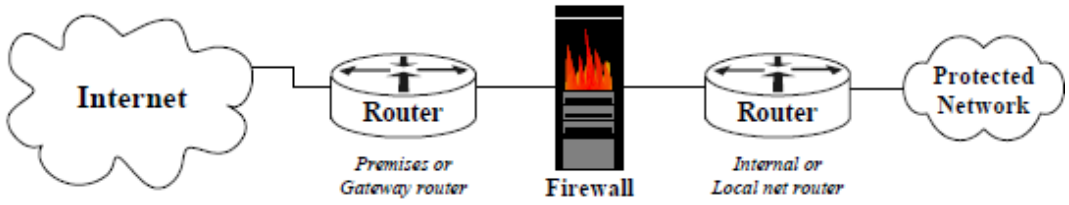


Figura 3.3 Topología típica de dos de configuración del router de conexión a Internet

3.1.3 Función del router en la Inter-Red de Seguridad

Al considerar la tarea de unirse a la seguridad IP con funcionalidad de router IP, el administrador de la red (NA o AN) o ingeniero de seguridad (SE), puede verse desbordado.

La gran cantidad de literatura disponible y la jerga técnica puede causar al AN hacer caso omiso de todas las características disponibles de seguridad.

Para reducir esta tarea de enormes proporciones para una que es manejable y de fácil comprensión.

Cada paquete pasa a través de o es creada por el router tiene la dirección de origen y está llevando los datos que pueden necesitar algún tipo de protección.

Al centrarse en este bloque de construcción fundamental de las redes IP, podemos dedicar nuestra energía a la que le proporciona algunos conceptos básicos de criptografía, y los comandos específicos de Cisco IOS que los implementan.

Estos pueden ser fácilmente incorporados en configuraciones de los routers actuales para ayudar a cumplir con los requisitos de seguridad específicos.

Los routers se utilizan para el suministro de la protección de paquetes casi siempre se posiciona como dispositivos de puerta de enlace. Estos dispositivos se conectan entre redes no confiables, tales como el Internet, y redes locales de confianza.

En 1996, Cisco IOS versión 11.2 lanzado, que incluye la tecnología de encriptación de Cisco (CET). Esta solución patentada fue un esfuerzo provisional para los clientes hasta que una solución basada en estándares, estaba en su lugar.

A pesar de que siempre algún nivel de protección de paquetes de Cisco a las comunicaciones de Cisco, que no permiten que los productos de Cisco para inter-operar con otros productos de seguridad IP.

Desde la aprobación de la IETF de seguridad IP (IPSec) las normas, tanto de Cisco (IOS 11.3 y superior) y otros fabricantes de productos de propiedad intelectual han puesto en marcha y ofreció soluciones IPSec para la protección de paquetes a sus clientes. Este enfoque basado en estándares permite la interoperabilidad entre los routers de Cisco y otros productos de seguridad IP, por ejemplo, no de Cisco routers, firewalls, servidores, etc.

Por lo tanto, los túneles IPSec se pueden construir entre las interfaces de los dos routers utilizando el protocolo IPSec marco. Este marco ha sido analizado por muchos evaluadores calificados en la industria y la academia. Funciona en conjunto con la basada en estándares Internet Key Exchange (IKE) para proporcionar a los usuarios una plataforma IP de seguridad muy sólido.

3.1.4 Seguridad en Red IP

Antes de establecer una configuración de IPSec en el router, la red de seguro y los actuales controles de configuración del router debe hacerse para eliminar los problemas de conectividad del router.

Desde IPSec utiliza protocolos IP 50 y 51, y el Protocolo de datagramas de usuario (UDP) el puerto 500 en sus comunicaciones, las restricciones de acceso en la lista de estos puertos o protocolos deben ser eliminados o cambiados para permitir que los paquetes IPSec pueda ser transmitida y recibida por los países participantes routers. Además, los routers pueden ser configurados utilizando varios modos de operación diferentes.

Para el ejemplo, se supone que los routers tienen dos modos de funcionamiento: modo básico y modo EXEC privilegiado.

En el modo básico de funcionamiento, cualquier persona con acceso al router se puede ver la información seleccionada acerca de la configuración actual en ejecución. En el modo EXEC privilegiado, el administrador puede actualizar y / o cambiar la configuración actual en ejecución.

La guía de seguridad no cubre de manera exhaustiva todas las opciones de IPSec. Más bien, ofrece un conjunto de opciones (por ejemplo, los algoritmos para su uso) y los comandos de Cisco IOS apropiados para su aplicación en un formato fácil de seguir, pasó a paso, ejemplo para ayudarle a configurar y probar IPSec en la red.

En el ejemplo que sigue, las interfaces externas del router del Norte, 14.2.0.20, y el router remoto, 7.12.1.20, se utilizará para ayudar a demostrar de los conceptos *(véase la Figura 3.4).*

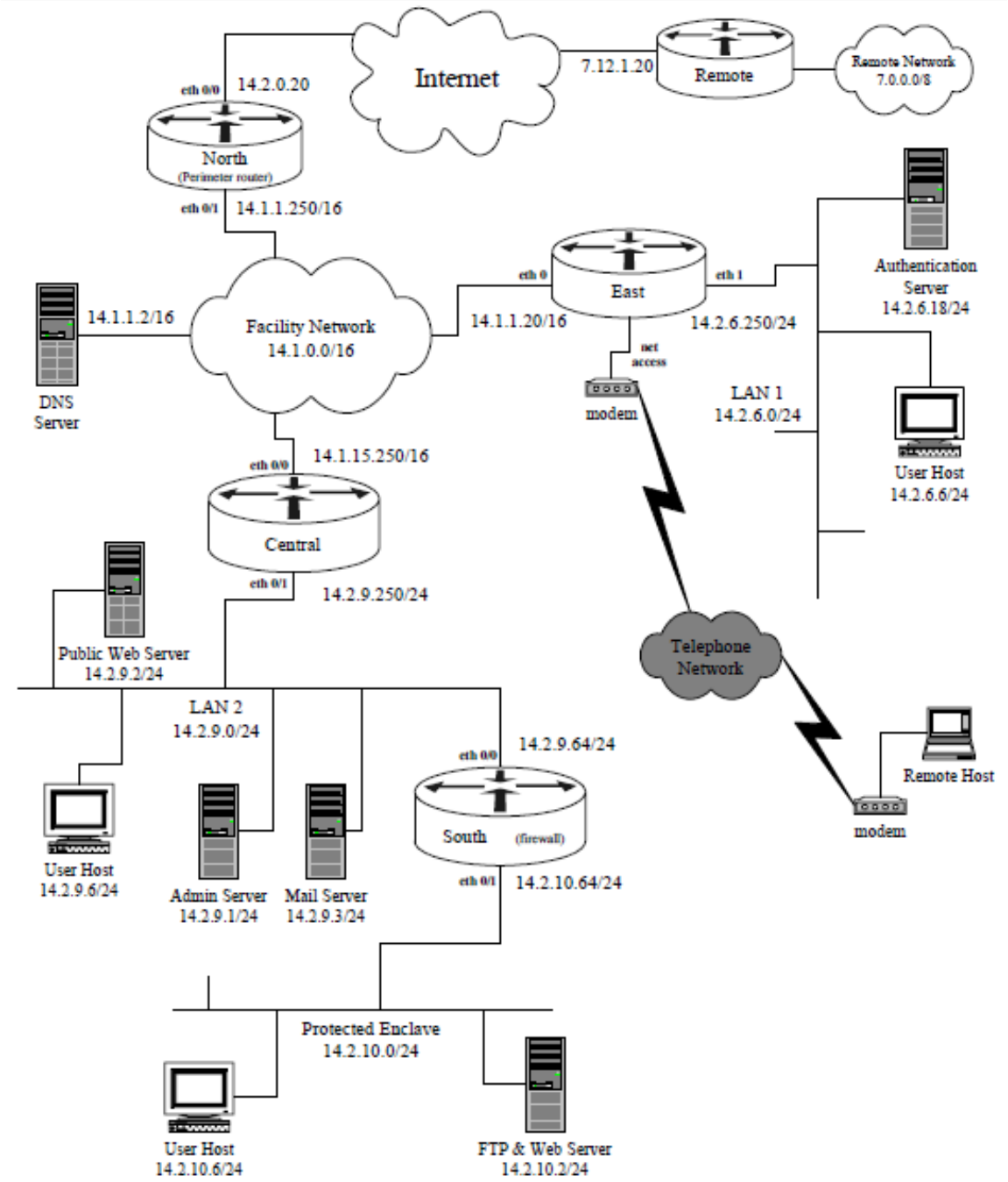


Figura 3.4 Ejemplo de diagrama de red

3.2 POLÍTICA DE SEGURIDAD PARA LOS ROUTERS

Los routers son una parte importante de una red y su seguridad es una parte vital de la seguridad general de las redes a las que sirven. ¿Qué significa para un router para ser seguro? Una forma sencilla de definir la seguridad de un router es la siguiente: la operación, configuración y administración del router para satisfacer su política de seguridad.

Una base conceptual para la política de seguridad del router

En la Figura 3.5, a continuación, muestra una vista en capas de la seguridad de un router. La seguridad de cada capa depende de la seguridad de las capas en su interior.

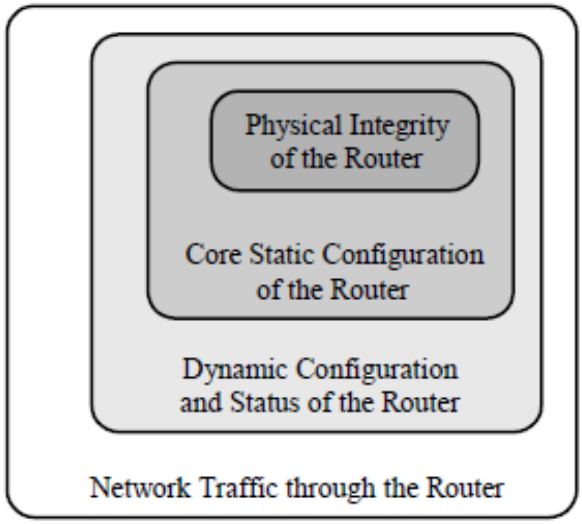


Figura 3.5 Capas de seguridad del router

Las capas de seguridad de del router son:

1. Tráfico de red a través del router
2. Configuración dinámica y el estado del router

3. Configuración del núcleo estático del router
4. La integridad física del router

Los accesos correspondientes de las capas de seguridad del router son:

- El acceso físico
- Acceso eléctrico
- El acceso administrativo
- Actualizaciones de software
- Los protocolos de enrutamiento
- El acceso a las redes que el router sirve
- Protocolos de gestión

La zona más interna es la seguridad física del router. Cualquier router puede estar comprometido por un atacante con acceso físico completo, por lo tanto, el acceso físico debe ser controlado para proporcionar una base sólida para la seguridad global del router.

La mayoría de los routers ofrecen una o más conexiones directas, generalmente llamados "Consola", o "puertos de control"; estos puertos suelen proporcionar mecanismos especiales para el control del router. La política de seguridad del router debe definir las reglas para dónde y cómo estos puertos pueden ser utilizados.

La siguiente zona más interna del diagrama es el software de almacenamiento y estado de la configuración del propio router. Si un atacante puede comprometer cualquiera de ellos, sobre todo la configuración almacenada, entonces él también va a hacerse con el control de las dos capas exteriores.

Algunos aspectos importantes de la configuración almacenada son las direcciones de interfaz, los nombres de usuario y contraseñas, así como los controles de acceso para el acceso directo a la interfaz de comandos del router.

La política de seguridad por lo general incluye normas estrictas sobre el acceso a este nivel, tanto en términos de funciones administrativas y los mecanismos de la red.

La siguiente zona más externa del diagrama es la configuración dinámica del router. Las propias tablas de rutas son la parte más evidente de ello. Otras piezas de información dinámica, como el estado de la interfaz, tablas ARP y registros de auditoría, son también muy importantes. Si un atacante puede comprometer la configuración dinámica de un router, se puede poner en peligro la capa más externa también. La política de seguridad de un router debe incluir normas sobre el acceso a esta capa, aunque a veces se pasa por alto.

La zona exterior del diagrama representa el tráfico intra-red y entre redes que el router gestiona. La política de seguridad de la red general puede incluir reglas sobre esto, la identificación de protocolos permitidos y servicios, mecanismos de acceso y las funciones administrativas. Los requisitos de alto nivel de la política de seguridad de la red deben reflejarse en la configuración del router, y probablemente en la política de seguridad del router.

Política de seguridad del router y de la red general

Por lo general, la red que sirve un router tendrá una política de seguridad, la definición de roles, permisos, normas de conducta y responsabilidades. La política de un router debe encajar en el marco general. Las funciones definidas en la política de seguridad del router suele ser un subconjunto de los de la política de la red. Las normas de conducta de la administración del router debe aclarar la aplicación de las reglas de red al router. Por ejemplo, una política de seguridad de la red puede definir tres funciones: administrador, operador y usuario.

La política de seguridad del router podría incluir sólo dos: el administrador y operador. Cada una de las funciones que se otorgan privilegios en la política de router que les permitan cumplir con sus responsabilidades como se indica en la directiva de red. El

operador, por ejemplo, podría ser responsable por la política de seguridad de la red para la revisión periódica de los registros de auditoría.

La política de seguridad del router podría conceder los privilegios de acceso del operador para el router para que puedan acceder a los registros del router.

En otros aspectos, la política de router se involucra mucho más detalle que la directiva de red. En algunos casos, el router aplica las políticas de red, y la política de router debe reflejar esto. Por ejemplo, la política de seguridad de la red podría prohibir la administración del router desde cualquier lugar, pero la red local.

La política del router puede especificarlas normas concretas que van a cumplir por el router para evitar que la administración remota.

Creación de una política de seguridad de un router

Hay varios consejos importantes a tener en cuenta al crear la política de seguridad de un router:

- Especificar los objetivos de seguridad, los comandos no particulares o mecanismos: Cuando la política se especifican los resultados de seguridad que debe alcanzarse, en lugar de un comando en particular o mecanismo, la política es más portable a través de versiones de software del router y entre los diferentes tipos de routers
- Especificar la política para todas las zonas identificadas en la figura anterior: Comience con la seguridad física, y trabajar hacia el exterior a la seguridad de la configuración estática, la configuración dinámica, y para el flujo de tráfico.
- Los servicios y protocolos que no se permita de manera expresa se le debe negar cuando en representación de la política de la red en el router de la política, se concentran en los servicios y protocolos que han sido identificados como de forma explícita necesaria para el funcionamiento de la red, permite de forma explícita aquellos, y negar todo lo demás.

En algunos casos, puede no ser práctico para identificar y enumerar todos los servicios y protocolos que el router de forma explícita se lo permitan.

Un router que debe enrutar el tráfico a muchas otras redes no siempre puede hacer cumplir las políticas altamente adaptados a las necesidades del tráfico que fluye a través de él, debido a problemas de rendimiento o las diferencias en las políticas de seguridad de las diferentes redes servidas. En este tipo de casos, la política debe establecer claramente las limitaciones o restricciones que pueden ser aplicadas.

En la elaboración de una política, mantener la mayor parte de las directivas y los objetivos de alto nivel; evitar la especificación de los mecanismos particulares de la póliza.

Una política de seguridad debe ser un documento vivo. Hágalo parte de las prácticas de seguridad de la red para revisar regularmente la política de seguridad de la red y la política de seguridad del router. Actualización de la política de router para reflejar los cambios en la directiva de red, o cuando los objetivos de seguridad para el cambio de router.

Puede ser necesario revisar la política de seguridad del router cada vez que hay un cambio importante en la arquitectura de red o de la estructura organizativa de la administración de la red. En particular, examinará la política de seguridad del router y modificar según sea necesario cada vez que alguno de los siguientes eventos.

Las nuevas conexiones entre la red local y las redes exteriores, los principales cambios en las prácticas administrativas, procedimientos o personal son:

- Principales cambios en la política de seguridad de la red general.
- El despliegue de nuevas capacidades substanciales (por ejemplo, una nueva VPN) o nuevos componentes de la red (por ejemplo, un nuevo servidor de seguridad).
- La detección de un ataque o un compromiso serio.

Cuando la política de seguridad del router se somete a una revisión, notificará a todas las personas autorizadas para Adminístrese el router y todas las personas autorizadas para el acceso físico a ella. El mantenimiento de la conciencia política es crucial para el cumplimiento de la política.

Lista de verificación de la seguridad del router Política

La siguiente lista ha sido diseñada como una ayuda para la creación de la política de seguridad del router. Después de la redacción de una política, el paso por la lista y verificar que cada elemento se trata en su póliza.

Seguridad Física

- Designa quién está autorizado a instalar, de instalar, y mover el router.
- Designa quién está autorizado para realizar el mantenimiento de hardware y para cambiar la configuración física del router.
- Designa quién está autorizado para hacer las conexiones físicas para el router.
- Define los controles sobre la colocación y el uso de la consola y otras conexiones directas de acceso a puertos.
- Define los procedimientos de recuperación para el caso de daño físico al router, o evidencia de manipulación con el router.

Seguridad de Configuración Estática

- Designa quién está autorizado para acceder directamente al router a través de la consola o de otras conexiones directas de acceso a puertos.
- Designa que está autorizado a asumir privilegios de administrador en el router.
- Define los procedimientos y prácticas para realizar cambios en la configuración del router estático (por ejemplo, libro de registro, grabación de cambio, los procedimientos de revisión).

- Define la política de contraseñas para contraseñas de usuario / inicio de sesión y las contraseñas administrativas o de privilegio.
- Designa quién está autorizado a entrar en el router de forma remota.
- Designa los protocolos, procedimientos, y las redes permitidos para iniciar sesión en el router de forma remota.
- Define los procedimientos de recuperación y se identifican las personas responsables de la recuperación, en el caso de compromiso de la configuración estática del router.
- Define la política de registro de auditoría para el router, incluyendo las líneas de actuación de registro y procedimientos de gestión y las responsabilidades de registro de la revisión.
- Designa los procedimientos y los límites sobre el uso de la gestión automatizada a distancia y los medios de vigilancia (por ejemplo, SNMP).
- Describe los procedimientos de respuesta o directrices para la detección de un ataque contra el propio router.
- Define la política de gestión de claves de largo plazo, las claves de cifrado (si existe).

Seguridad de Configuración Dinámica

- Identifica los servicios de configuración dinámica permitidas en el router, y de las redes permite el acceso a esos servicios.
- Identifica los protocolos de ruteo a ser usado, y las características de seguridad a emplear en cada uno.
- Designa mecanismos y políticas para la creación o el mantenimiento de la automatización del reloj del router (por ejemplo, ajuste manual, NTP).
- Identifica acuerdo de claves y algoritmos criptográficos autorizados para su uso en el establecimiento de túneles VPN con otras redes (si existe).

Seguridad en el servicio de Red

- Enumera los protocolos, puertos y servicios que se permita o se filtra por el router, para cada interfaz o conexión (por ejemplo, entrante y saliente), e identifica los procedimientos y las autoridades para que les autorice.
- Describe los procedimientos de seguridad y funciones de las interacciones con los proveedores de servicios externos y técnicos de mantenimiento.

Compromiso de respuesta

- Enumera las personas u organizaciones para ser notificados en caso de un compromiso de la red.
- Define los procedimientos de respuesta, las autoridades, y los objetivos de respuesta después de un ataque con éxito contra la red, incluida la provisión para la preservación de pruebas y para la notificación de la aplicación de la ley.

3.3 SEGURIDAD DE ACCESO DEL ROUTER

Este capítulo trata sobre los diversos mecanismos utilizados para proteger el propio router. Estos incluyen el acceso físico, la protección de la cuenta de usuario, protección de software, las preocupaciones de administración remota y problemas de configuración. Al pensar en la seguridad de su red, es importante tener en cuenta estas cuestiones para todos sus sistemas, en su caso, así como para sus routers.

Seguridad Física

Una vez que una persona tiene acceso físico a un pedazo de equipo de red no hay forma de detenerlo para que modifique el sistema. Este problema no se limita solamente a los dispositivos de red, pero también es cierto de las computadoras y cualquier otro dispositivo

eléctrico o mecánico. Es siempre una cuestión de tiempo y esfuerzo. Hay cosas que se pueden hacer para hacer esto más difícil, pero un atacante experto con acceso nunca puede ser derrotado por completo, sólo se desaceleró.

Una de las mejores adiciones a las características de seguridad de una red de ordenadores es limitar el acceso. Componentes de infraestructura de red como routers, son especialmente importantes porque a menudo se utilizan para proteger a los segmentos de la red y también puede ser utilizado para lanzar ataques contra otros segmentos de red.

Equipos de red especialmente los routers y switches, debe estar ubicado en una zona de acceso limitado. Si es posible, esta área debe ser sólo accesible por el personal con responsabilidades administrativas para el router. Esta área debe estar bajo algún tipo de supervisión 24 horas al día y 7 días a la semana. Esto se puede lograr a través del uso de los guardias, el personal del sistema o la vigilancia electrónica.

En la práctica, los mecanismos de seguridad física y las políticas no deben hacer muy difícil el acceso del personal autorizado, o pueden encontrar formas de burlar las medidas de seguridad físicas.

Si la administración remota se utiliza para configurar y controlar los routers, y luego considerar la manera de proteger las máquinas utilizadas para la administración remota y las redes que utilizan para comunicarse con el router. Use las listas de acceso para limitar el acceso de administración remota a los hosts que gozan de la seguridad física razonable. Si es posible, utilizar el cifrado para proteger la confidencialidad e integridad de la conexión de administración remota.

Para ilustrar una de las razones por qué la seguridad física es fundamental para la seguridad del router en general, consideran que el procedimiento de recuperación de contraseña para los routers de Cisco. Este procedimiento es capaz de adquirir pleno privilegio (enable) al acceso a un router Cisco sin necesidad de utilizar una contraseña.

Los detalles del procedimiento varían entre los modelos de router, pero siempre incluye los siguientes pasos básicos. Un administrador (o un atacante) puede simplemente conectar un terminal o un ordenador al puerto de consola y los siguientes pasos:

- **Paso 1.** Configurar el router para arrancar sin necesidad de leer la memoria de configuración (NVRAM). A veces se denomina el modo de sistema de prueba.
- **Paso 2.** Reinicie el sistema.
- **Paso 3.** Acceder a modo de habilitación (que se puede hacer sin una contraseña si se encuentra en modo de prueba del sistema).
- **Paso 4.** Ver o cambiar la contraseña o borrar la configuración.
- **Paso 5.** Vuelva a configurar el router para arrancar y leer la NVRAM como hace normalmente.
- **Paso 6.** Reinicie el sistema.

Cualquier persona con experiencia o formación utilizando los routers de Cisco puede parlamentar acceso físico a la plena privilegiada administrativa en un router Cisco, el procedimiento toma sólo un par de minutos. *(Nota: El paso 5 es muy importante, y si es necesario utilizar el procedimiento de recuperación de la contraseña por cualquier razón, no deje de restaurar la configuración de arranque del sistema después de recuperar el acceso a la falta router para hacer lo que normalmente se traducirá en el router viene. en un estado de inseguridad en los reinicios posteriores).*

Una segunda razón para el control de acceso físico al router incluye tarjetas de memoria flash. Muchos modelos de router de Cisco ofrecen ranuras PCMCIA que pueden contener memoria flash adicional. Los routers equipados con este tipo de ranuras darán preferencia a la memoria instalada en una ranura en la memoria instalada en el chasis.

Un atacante con acceso físico a un enrutador de la red se puede instalar una tarjeta de memoria flash, o sustituir uno antiguo. A continuación, puede iniciar el router con su flash, haciendo así que el router para ejecutar la versión de IOS y la configuración. Si se hace con

cuidado y bien, este tipo de ataque puede ser muy difícil de detectar. La mejor defensa contra la seguridad física es buena.

Una de las preocupaciones de seguridad operacional estrechamente relacionada con la seguridad física es el entorno operativo físico.

Al igual que la mayoría de equipos de red, los routers son sensibles a la temperatura y humedad extremas. Si un router no se encuentra en una zona ambientalmente amigable, entonces puede operar de forma inesperada y degradan su seguridad. Esta es también una cuestión de seguridad personal.

Una habitación donde se encuentran los routers deberá estar libre de la interferencia electrostática y magnética. El área también debe ser controlada para la temperatura y la humedad. Si es posible, todos los routers se debe colocar en una fuente de alimentación ininterrumpida (SAI), ya que se cortara la alimentación puede dejar un poco de equipo de red en los Estados indeterminados.

La consola (CON) y auxiliar (AUX) en los puertos de los routers de Cisco se utilizan para conexiones en serie con el router. La mayoría de routers Cisco tienen tanto una consola y un puerto auxiliar, algunos de los modelos más pequeños tienen sólo un puerto de consola.

La diferencia primaria entre los dos puertos es que el mecanismo de recuperación de contraseña puede ser utilizado en el puerto de la consola solamente. En muchos casos, el puerto auxiliar no se utiliza.

Algunos administradores de conectar un módem al puerto auxiliar para facilitar la administración remota a través de dial-up. Permisos de acceso telefónico directo a cualquier parte vital de la infraestructura de la red es potencialmente muy peligrosa, y debe establecerse sólo cuando el acceso oportuno por otros medios no es factible. En general, el puerto auxiliar debe estar deshabilitada.

3.4 ENRUTADOR DE LA RED DEL SERVICIO DE SEGURIDAD

Los routers de Cisco apoyan un gran número de servicios de red, algunos de estos servicios pueden ser restringidos o discapacitados, para la mejora de la seguridad sin degradar el uso operativo del router. Algunos de estos servicios son de aplicación, los protocolos de la capa que permiten a los usuarios y los procesos de acogida para conectar con el router. Otros son procesos automáticos y la configuración de la intención de apoyar la herencia o especializados configuraciones, pero que son perjudiciales para la seguridad.

Desactivación de un servicio de red en el propio router no le impide apoyar una red en la que utiliza este protocolo. Por ejemplo, un router puede soportar una red en la que se emplea el protocolo BOOTP, pero algún otro host actúa como BOOTP. En este caso, el servidor del router bootp debe estar deshabilitada.

En muchos casos, Cisco IOS soporta convertir un servicio por completo, o restringir el acceso a los segmentos de red particulares o conjuntos de los ejércitos. Si una porción particular de una red necesita un servicio, pero el resto no, entonces las características de las restricciones deben ser empleados limitar el alcance del servicio.

Desactivación de una función automática de la red por lo general impide que un cierto tipo de red el tráfico de ser procesado por el router o le impide atravesar el router. Por ejemplo, el enrutamiento IP de origen es una característica poco usada de IP que pueden ser utilizados en ataques a la red. A menos que se requiere para la red de operar, fuente de enrutamiento IP deben ser desactivados.

3.5 SEGURIDAD DE LOS SERVICIOS DE ACCESO DE RED DEL ROUTER

Seguridad de los servicios de acceso de red se ocupa fundamentalmente de control de usuarios remotos que tienen acceso a los recursos locales. Un proveedor de servicios de

Internet sería un buen ejemplo de esto. Cisco ofrece esta seguridad con su autenticación, autorización, y contabilidad (AAA) de servicios. La sub-sección a continuación trata con usuarios de acceso telefónico dará una introducción al control de los usuarios remotos que accedan a recursos de red.

Visión general, conceptos básicos y mecanismos de apoyo

La autenticación de Cisco, autorización y contabilidad proporcionan crítica es de seguridad necesarias para proporcionar acceso remoto a los routers de la red y funciones de recursos. AAA es el mecanismo de Cisco este se recomienda para el control de acceso. AAA es diseñado para permitir al administrador configurar sus servicios a nivel mundial o por línea e interfaz.

Cuando los servicios de AAA están habilitados en un router Cisco, las viejas formas de control de acceso están desactivadas. Esto significa que ya no se puede acceder a los comandos para configurar los protocolos de más edad de inicio de sesión (incluyendo los comandos locales y de inicio de sesión). Cuando los mayores mecanismos de control de acceso trataron casi exclusivamente con la autenticación de usuarios, la AAA también tiene la capacidad para controlar el acceso de cada usuario a los recursos y proporcionar adicionales funciones de contabilidad más allá de las facilidades de registro del router. AAA le permite emplear las siguientes fuentes de información del usuario: RADIUS, TACACS + Kerberos, la base de datos local, y habilita contraseñas de línea.

Mediante el uso de la AAA junto con un servidor de seguridad que usted puede controlar el acceso a los routers y otros servicios de red desde una ubicación centralizada. Esto permite una más fácil gestión de cuentas de usuario y privilegios, y proporciona capacidades adicionales para auditoría de uso de la red de servicio.

Además, la AAA también le permite configurar los métodos de copia de seguridad para los diferentes servicios que utilizan las listas de los métodos.

Autenticación

La autenticación es el mecanismo para la identificación de los usuarios antes de permitir el acceso a los componentes de red o servicios. En otras palabras, la autenticación controla la capacidad de un usuario u otro componente de la red para acceder a un dispositivo de red o servicio. AAA de autenticación proporciona los medios para identificar a los usuarios a través de usuario/contraseña, desafío/diálogos en respuesta de los mecanismos y tecnologías de apoyo simbólico.

La autenticación de la AAA es la configuración con las listas de los métodos. La configuración de la autenticación AAA requiere: habilitar la autenticación AAA de configuración, protocolo de seguridad, listas de parámetros del servidor de configuración de métodos de autenticación AAA, y aplicar las listas de método a una interfaz de línea en particular o, si es necesario.

Autorización

La autorización controla el acceso a los recursos del sistema. La autorización es el método utilizado para describir lo que un usuario tiene derecho a hacer una vez de que se autentiquen en el router.

La autorización incluye una sola vez la autorización, la autorización para cada servicio, y autorización para cada usuario. Además, la autorización sólo se puede configurar utilizando AAA.

Al igual que con la autenticación, las listas definen qué método de protocolos de autorización se utilizarán y en qué orden. Tipos de autorización AAA son:

- **exec -** que controla la capacidad de los usuarios para ejecutar una shell EXEC.

- **comandos <level>** - que controla el acceso a todos los comandos en el que se especifica el nivel de privilegio.

- **red** - permite la autorización de todos los servicios relacionados con la red como: PPP, PPP NCP, SLIP, y los Protocolos de ARA.
- **acceso inverso** - controla el acceso a todas las conexiones de acceso inverso como Reverse Telnet.

Las listas de autorización son específicas para el tipo de autorización que se está definiendo. Si no hay lista de autorizaciones son definidas para el tipo de autorización, entonces no se producirá la autorización para ese tipo.

Los requisitos previos a la autorización de la AAA: habilitan los servicios de AAA, AAA configura la autenticación (ya que la autorización se basa en la autenticación de la producción de), definir la seguridad de servidores, y definir los derechos de cada usuario.

Contabilidad

La contabilidad de AAA se utiliza para el registro y seguimiento de las actividades de los usuarios (personas o otros componentes de red), utilizando un recurso de red. Estos registros pueden ser utilizados para la gestión de red, análisis de la seguridad, el seguimiento de la utilización de recursos y generación de informes.

Los routers envían sus registros contables a la seguridad del servidor para su almacenamiento. La información está en un registro contable que incluye la identidad de los usuarios, el inicio de uso y tiempos de parada, número de paquetes y bytes, y el comando que se ejecutó.

Al igual que con la autenticación y autorización, se configuran mediante la definición de la contabilidad AAA de una lista de métodos de contabilidad. Hay varios tipos de contabilidad que se pueden activar: exec, red, conexión, un comando del sistema. Todos los

tipos son compatibles con TACACS + RADIUS, pero no es compatible con comandos o sistema.

- **Contabilidad de red** - Proporciona información para el PPP, SLIP y los protocolos ARAP. La información incluye el número de paquetes y bytes.
- **EXEC contable** - Proporciona información sobre las sesiones de usuario EXEC en el servidor de acceso a la red. La información incluye el nombre de usuario, fecha, de inicio y fin, la dirección IP del servidor de acceso y número de teléfono de la llamada de su origen en la línea de los usuarios.
- **La contabilidad de conexión** - Proporciona información sobre todas las salidas de conexiones realizadas desde el servidor de acceso a la red. Esto incluye telnet, login, etc., (de área local de transporte (LAT), TN3270, el paquete ensamblador / desensamblador (PAD)).
- **Comandos** - Esto se aplica a los comandos que se registran en un shell EXEC. A esta opción se aplicará la contabilidad de todas las órdenes emanadas en la que se especifica el nivel de privilegio. Si la contabilidad está activada para el nivel 15 y el usuario registrado a nivel de habilitación de 15 carreras de nivel 1 con comando exec ningún caso de auditoría será generada. Los registros de la cuenta se generan en función del nivel del comando no a nivel del usuario. En los registros contables se incluyen el comando, fecha, hora, y el usuario. La implementación de Cisco de la RADIUS no es compatible con la contabilidad de comandos.
- **Sistema** - Proporciona información sobre los eventos a nivel de sistema. Esto haría incluir información cuando el sistema se reinicia, lo que representa ser encendido o apagado, etc. Tenga en cuenta que en la contabilidad del sistema sólo se utiliza la lista predeterminada. La implementación de Cisco de RADIUS no es compatible con un sistema de contabilidad.

AAA contable requiere que AAA está habilitada, los servidores de seguridad se definen, y que un servidor de seguridad se especifica para cada tipo de contabilidad que se desea. Cada registro contable se compone de pares de AV de contabilidad y se almacena en el acceso de control del servidor. La contabilidad también puede ser configurada de tal

manera que un usuario solicite la acción y no puede ocurrir hasta un reconocimiento que se recibe desde el servidor de seguridad que indica que el registro contable se ha guardado.

Las listas de métodos

Las listas de métodos se utilizan para especificar uno o más protocolos de seguridad o mecanismos de AAA. En los métodos de las listas también se especifican la secuencia en que los mecanismos de seguridad deben ser utilizados. Estas listas se pueden utilizar para proporcionar mecanismos de respaldo para cuando el método de seguridad principal no está disponible.

Los métodos de las listas pueden dar un nombre específico o pueden utilizar la palabra clave default. Cuando una lista de métodos se especifica mediante la palabra clave por defecto de la lista será automáticamente aplicado a todas las interfaces adecuadas y líneas. Con nombre de listas de acceso pueden ser definidos y después se aplica a la interfaz de línea en particular o para anular el valor predeterminado de comportamiento. El siguiente ejemplo muestra una lista de métodos de autenticación de nombre de AAA, y listas predeterminadas para la autorización y contabilidad para el tráfico de red:

```
aaa authentication login remote authen radius local
aaa authorization network default radius local
aaa accounting network default start-stop radius
```

CAPÍTULO 4. HERRAMIENTAS DE AUDITORÍA

4.1 AUDITORÍA Y ADMINISTRACIÓN

Conceptos y mecanismos

Los routers son una parte fundamental de las operaciones de red y seguridad de la red. La cuidadosa administración y diligente Auditoría de las operaciones del router pueden reducir el tiempo de inactividad de la red, mejorar la seguridad, y la ayuda en el análisis de las brechas de seguridad sospechosas. Los routers Cisco y los Cisco IOS están diseñados para apoyar la auditoría y gestión centralizada.

- **Inicio de sesión:** Los routers de Cisco soportan tanto a los registros on-board y remote logs.
- **Time:** El tiempo exacto es importante para la buena auditoría y gestión de routers Cisco totalmente compatible con el protocolo de sincronización de tiempo estándar, NTP.

- **Network Management:** El protocolo estándar para la gestión distribuida de componente de red es el Simple Network Management Protocol (SNMP). SNMP deberá ser deshabilitado o configurado cuidadosamente para una buena seguridad.
- **Network Monitoring:** Los Routers de Cisco soportan servicios básicos para el Remote Network Monitoring (RMON). Las características RMON dependerán de SNMP, y deben ser también deshabilitadas o configuras con cuidado.
- **Software Maintenance:** Mantenerse al día con nuevas versiones de software es importante, porque los nuevas versiones incluyen correcciones de vulnerabilidades de seguridad. Instalación nueva de software de Cisco IOS de un router no es especialmente difícil.
- **Debugging and Diagnostics:** La solución de problemas del router requiere habilidad con comandos de cisco de diagnóstico y herramientas de depuración.

Las secciones siguientes describen las configuraciones recomendadas para una buena seguridad:

Servicios de tiempo, sincronización de hora de red y NTP

El éxito de la auditoría de una gran red puede depender de la sincronización de los diversos registros, así como datos para los anfitriones en la red. Todos los routers de Cisco tienen un reloj que mantiene la fecha y la hora, aunque algunos modelos más antiguos de Cisco pierden el tiempo cuando están apagados. Es muy importante para establecer la hora en un router cuando se instala por primera vez, y luego mantener sincronizada la hora cuando el router está en uso operacional.

Es posible realizar la sincronización manual de tiempo de red, ajustando el tiempo en cada router y host en una red de forma manual sobre una base regular. La sincronización manual de la hora es tedioso, propenso a errores, y poco fiable. Los routers de Cisco son totalmente compatibles con la sincronización automática de tiempo de red basado en el estándar Network Time Protocol (NTP).

Visión general y motivaciones para el registro

Los routers de Cisco pueden registrar los errores del sistema, los cambios en la red y el estado de la interfaz, errores de inicio de sesión, acceso a las listas y muchos más tipos de eventos. Algunas motivaciones para el mantenimiento de los registros del router se enumeran a continuación:

- Registro de los cambios de configuración del router y reinicios.
- Registro de la recepción de tráfico que viole las listas de acceso.
- Registro de los cambios en la interfaz y el estado de la red.
- Registro de las violaciones de seguridad criptográficas del router.

4.2 CONFIGURACIÓN DE UN ROUTER

Después de conectarse a un router y se conecte inicialmente, el sistema está en modo de usuario también conocido como el modo EXEC. Modo EXEC da acceso limitado al conjunto de comandos de la router.

El acceso a todos los comandos de router, incluyendo la capacidad de cambiar la configuración, se reserva para el modo EXEC privilegiado. Escribiendo la habilitación comando en un indicador del modo EXEC le dará acceso al modo EXEC privilegiado. Modo EXEC privilegiado se llama a veces “activar el modo”.

Hay varios modos de configuración en un router Cisco. Para entrar en el mundial el modo de configuración ***(config)*** escriba el comando configure terminal, comúnmente abreviada ***config t.*** En el modo de configuración global una amplia variedad de general funciones de router y la configuración se puede cambiar: banners, sistemas de autenticación, acceso, listas, registros, protocolos de enrutamiento, y mucho más.

Hay sub-modos que son utiliza para configurar los parámetros específicos para las interfaces, líneas, protocolos de enrutamiento, etc. La lista a continuación se describe algunos de los sub-modos:

- Interfaz ***(config-if):*** Se utiliza para configurar los aspectos de una interfaz en particular como FastEthernet0, Ethernet 0/1, o VLAN2.
- Línea ***(config-line)***: Se utiliza para configurar el puerto de la consola, puerto auxiliar y las líneas de terminal virtual.
- Acceso a la lista: Hay dos tipos de listas de acceso IP con nombre, extendido ***(Config-ext-n)*** y estándar ***(configuración-STD-n),*** que puede utilizarse en lugar de listas numeradas. La lista de acceso modo se utiliza para la construcción de listas de acceso nombradas.
- Ruta ***(config-route)***: Es donde los parámetros específicos se pueden establecer y modificar de un protocolo de enrutamiento seleccionado.

Inicios de sesión, privilegios, contraseñas y cuentas

Los inicios de sesión: Una pancarta de inicio de sesión, que incluye un aviso legal, se debe configurar en cada router operativo.

Información de la red la arquitectura y los detalles de configuración del router no debe ser incluido en el mensaje de bandera. Modelo de router y la información de ubicación debe ser incluido sólo si es necesario. Tenga especial cuidado de no proporcionar la información en la bandera de mensaje que no se debe compartir con el público en general, o la información que no es visible desde el modo EXEC privilegiados. Para configurar el router bandera debe utilizar el comando: ***banner motd*** delimitador de mensaje.

El puerto es la ubicación predeterminada para la realización de la gestión de router y configuración. Está bien salir de una conexión al puerto de consola conectado todo el

tiempo, pero que el terminal (o equipo) debe ser independiente, y protegido del acceso no autorizado. La conexión con el puerto de la consola no se debe dejar conectado.

Configurar la línea de la consola el tiempo de espera, de modo que si un administrador olvida cerrar la sesión, el router inicie sesión o cierre ella de forma automática. Cada usuario autorizado debe acceder utilizando su propia cuenta. El siguiente ejemplo muestra cómo configurar la línea de la consola para hacer cumplir de inicio de sesión de usuario y un tiempo de espera de cinco minutos.

```
Central# config t
Enter configuration commands, one per line. End with CNTL/Z.
Central(config)# line con 0
Central(config-line)# transport input none
Central(config-line)# login local
Central(config-line)# exec-timeout 5 0
Central(config-line)# end
Central#
```

Tenga en cuenta que, para hacer cumplir la consola de acceso, como se muestra arriba, es necesario crear al menos un usuario cuenta, de lo contrario quedarán fuera de la consola. Si usted aún no tiene los usuarios de las cuentas configuradas, a continuación, crear al menos una antes de la consola para utilizar inicio de sesión local. La sintaxis para crear un usuario local es el nombre de usuario el nivel de privilegio contraseña de cadena. El siguiente ejemplo muestra cómo crear una cuenta con una contraseña.

```
Central# config t
Enter configuration commands, one per line. End with CNTL/Z.
Central(config)# username brian privilege 1 password g00d+pa55w0rd
Central(config)# end
Central#
```

Un aviso legal suele incluir una advertencia de "prohibido el paso", y una declaración de que "todo uso del router debe estar autorizado por la organización propietaria". Una notificación legal apropiada protege la capacidad de la organización propietaria

de emprender acciones legales contra un atacante. Consulte a su personal jurídico de la organización o el consejero general de un lenguaje adaptado para su uso en el aviso legal.

En el ejemplo a continuación muestra cómo desactivar inicio de sesión en el puerto auxiliar (login para habilitar el modo en primer lugar):

```
Central# config t
Enter configuration commands, one per line. End with CNTL/Z.
Central(config)# line aux 0
Central(config-line)# transport input none
Central(config-line)# login local
Central(config-line)# exec-timeout 0 1
Central(config-line)# no exec
Central(config-line)# end
Central#
```

Si el puerto auxiliar se requiere para una segunda conexión en serie local, entonces configurarlo como se muestra a continuación:

```
Central# config t
Enter configuration commands, one per line. End with CNTL/Z.
Central(config)# line aux 0
Central(config-line)# exec-timeout 5 0
Central(config-line)# login local
Central(config-line)# transport input none
Central(config-line)# exec
Central(config-line)# end
Central#
```

Configuración de Logging and Time Services

El login es una parte crítica de la seguridad del router, los buenos logs pueden ayudar a encontrar errores de configuración, comprender las intrusiones del pasado, solucionar las interrupciones del servicio, y reaccionar a los sondeos y escaneos de la red.

Los routers de Cisco tienen la capacidad de registrar una gran parte de su estado.

Comandos de Router de estado y configuración

Cada uno de los puntos siguientes describe una consulta solo sobre el estado. Hay literalmente cientos de las consultas de ese tipo disponibles, incluso en los más simples de routers Cisco. Los que se muestran aquí se utilizan comúnmente para solución de problemas simples, y son útiles para entender la disposición de un router de Cisco en una típica red TCP / IP.

1. **Visualización del registro actual:** Para ver los actuales almacenados en el búfer de los mensajes de registro, utilice el comando ***show logging***. La producción consta de dos partes: un resumen de la actual configuración del registro, y los mensajes de registro. Los mensajes se muestran en el orden de aparición, los mensajes son tan recientes al final de la lista. Los mensajes de registro almacenados en el búfer se borran cuando se reinicia el router, por lo que los primeros pocos mensajes puestos en el registro reflejan la actividad de inicio. En el siguiente ejemplo, un intento no autorizado a telnet al propio router ha sido registrado:

```
East# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes)
Console logging: level debugging, 56 message lines logged
Monitor logging: level debugging, 32 message lines logged
Buffer logging: level debugging, 56 message lines logged
Trap logging: level informational, 33 message lines logged
Logging to 14.2.9.6, 33 message lines logged
Log Buffer (16000 bytes):
00:00:17: %LINK-3-UPDOWN: Interface Ethernet0, changed
state to up
.
.
Mar 3 12:51:52 EST: %SEC-6-IPACCESSLOGP: list 131 denied
tcp 172.17.101.250(47746) -> 0.0.0.0(23), 1 packet
East#
```

Nota: *Los mensajes de registro deben incluir siempre la hora del evento. En un router mediante NTP, los primeros mensajes de registro se incluyen en el tiempo transcurrido desde arrancar en lugar de la hora correcta, porque los mensajes se generan antes de NTP sincronizado.*

2. **Viendo la tabla de rutas actual:** Para verla tabla de rutas actual, utilice el comando ***show ip route.*** Dependiendo del tamaño de la red y los tipos de protocolos de enrutamiento utilizado, esta lista puede ser muy grande. Una parte muy importante de la revisión de las tablas de rutas está comprobando los códigos de la ruta y el control del destino de puerta de enlace. Cada código de ruta se identifica como una de las rutas de unión al table, el port de entrada de destino no es más que el siguiente salto en esa ruta. Comprobar la ruta de códigos para asegurarse de que todas las rutas se unieron al table, ya sea directamente (código C), o se han añadido como rutas estáticas (código S), o fueron añadidos por un configurado del protocolo de enrutamiento (códigos R, S, y otros). La siguiente figura 4.1, muestra cómo interpretarla salida de show ip route.

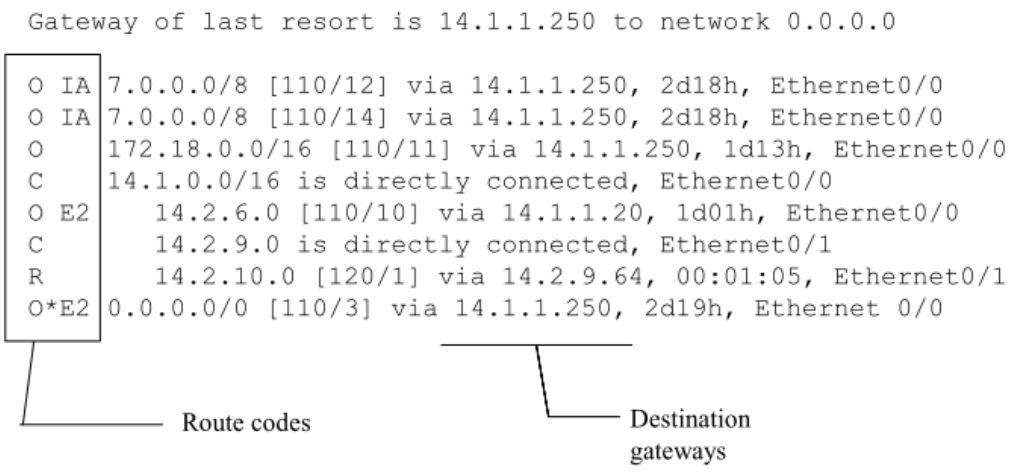


Figura 4.1 Interpretación de la salida de la tabla del router.

3. **Visualización de los protocolos de enrutamiento en uso:** El comando ***show ip protocol*** da una lista detallada de la ruta a actualizar los mecanismos utilizados actualmente en el router. La salida es diferente para cada tipo de protocolo. El

comando ***show ip protocol*** ofrece un resumen de una visión general rápida. Todos los protocolos individuales de encaminamiento también tienen comandos extensos de estado. El siguiente ejemplo muestra el protocolo de enrutamiento IP en resumen y de salida (abreviado) por un comando de estado.

```
Central# show ip protocol summary
Index Process Name
0     connected
1     static
2     ospf 1
3     rip
Central# show ip ospf neighbor
Neighbor ID  Pri   State     Dead Time Address   Interface
14.2.1.20     1   FULL/DR   00:00:33  14.2.1.20   Eth0/0
14.2.1.250    1   FULL/DR   00:00:38  14.2.1.250  Eth0/0
Central#
```

4. **Viendo la actual tabla ARP:** Dispositivos extraños, dispositivos mal conectados y dispositivos no autorizados en un segmento de red a menudo puede ser detectado por su presencia en un encaminador de resolución de direcciones (ARP) del table.

   Para mostrarla tabla ARP, utilice el comando ***show arp***, como en el ejemplo siguiente.

```
Central# show arp
Protocol  Address    Age(min) Hardware Addr   Type Interface
Internet  14.2.9.6     57     0004.acd5.f3f6  ARPA   Eth0/1
Internet  14.2.1.20    10     0010.7bf9.127a  ARPA   Eth0/0
Internet  14.2.9.64    43     0050.0f03.3680  ARPA   Eth0/1
Internet  14.1.1.250   53     0010.7bb6.baa0  ARPA   Eth0/0
.
.
Central#
```

5. **Visualización de la sesión de los usuarios:** El comando ***show users*** muestra una lista de usuarios que están actualmente conectados. En la salida siguiente, hay un usuario conectado en la consola, y dos se registran en la red.

```
Central# show users

Line         User    Host(s)  Idle  Location
0 con 0    jsmith   idle     00:00:56
130 vty 0    andrew   idle     00:01:02  14.2.1.20
*131 vty 1    neal     idle     00:00:00  14.2.9.6
Central#
```

6. **Ver el nombre de host y la información de búsqueda de nombre:** Cisco IOS utiliza dos mecanismos para la asignación entre direcciones IP y nombres: los nombres definidos localmente, y DNS. Nombres definidos localmente toman prioridad sobre los nombres DNS. Utilice el anfitrión de la demostración de comando para mostrar la configuración del DNS y la lista de nombres definidos localmente.

```
Central# show host
Default domain is not set
Name/address lookup uses domain service
Name servers are 14.1.1.2, 14.2.9.1
Host      Flags       Age  Type   Address(es)
east     (perm, OK)    4    IP     14.1.1.20
central  (perm, OK)   **    IP     14.1.15.250
south    (perm, OK)   52    IP     14.2.9.64
Central#
```

7. **Ver el estado de la interfaz y configuración:** Utilice el comando ***show ip*** interface para ver una presentación detallada de los estados y la configuración de las interfaces de red del router.

   Para una rápida mirada, utilice el breve comando ***show ip*** interface. En todos los casos, el listado incluirá tanto las activas como las interfaces inactivas. En el ejemplo a continuación muestra el formato de salida breve, ligeramente abreviada.

```
Central# show ip interf brief
Interface       IP-Address     OK? Method Status  Protocol
Ethernet0/0     14.1.15.250    YES NVRAM  up          up
Ethernet0/1     14.2.9.250     YES NVRAM  up          up
```

```
Ethernet0/2    unassigned    YES unset  down       down
Ethernet0/3    unassigned    YES unset  down       down
Central#
```

8. **Ver el estado de la línea**: Cada router Cisco tiene al menos una conexión de la línea física, la consola, y por lo general cinco conexiones de las líneas virtuales, las líneas vt y telnet. Utilice el de la línea de comando ***sshow*** para mostrar un resumen de las líneas disponibles en un router. Para visualizar el estado completo de una línea, utilice mostrar el número de línea para el nombre, por ejemplo, mostrar la línea auxiliar0.

9. **Viendo actualmente sockets UDP abiertos:** Utilice el comando **show ip** para mostrar la lista de la UDP abierto tomando el servicio de red en el router. La salida es un poco críptico, pero pueden proporcionar valiosas pistas a los servicios que el router está en realidad proporcionando.

   El siguiente ejemplo muestra la salida de un router que ejecuta servicios de muy pocos:

```
Central# show ip sockets
Proto Remote   Port  Local      Port  In Out Stat TTY
17  0.0.0.0    520 14.1.15.250  520   0   0   1    0
17  14.2.9.1 36269 14.1.15.250  161   0   0   1    0
17  0.0.0.0    123 14.1.15.250  123   0   0   1    0
17  14.2.9.6   514 14.1.15.250 6082   0   0  10  132
Central#
```

La primera línea es la ruta RIP de servicio de protocolo (puerto local 520). La segunda línea es el servicio SNMP para un host que ejecute un SNMP/RMON de herramienta de gestión (puerto local 161). La tercera línea es la hora de la red servicio (NTP, el puerto 123). La cuarta línea es el registro de cliente, el envío de mensajes de syslog a un host Unix (puerto remoto 514).

10. **Visualización de la configuración actual:** Para ver la configuración actual que se ejecuta IOS, utilice el comando **show running**. La salida resultante será típicamente

bastante larga. Para revisar la configuración de profundidad, salvo los resultados de los comandos en un archivo, imprimirlo, y revise el papel. Para verla configuración de inicio guardado (en NVRAM). Normalmente, estas dos configuraciones deben ser muy similares. Si las configuraciones son muy grandes y complejas, utilizar una herramienta de comparación de archivos, tales como diff de Unix o Windows FC, para poner de relieve las diferencias. Archive una copia de la configuración después de cualquier cambio importante, o en una base mensual. Esto puede ayudar con los problemas, y también acortar el tiempo de inactividad si el router pierde su configuración almacenada. El siguiente ejemplo muestra cómo guardar un archivo de una configuración a un servidor FTP, con IOS 12.0.

```
Central# config t
Enter configuration commands, one per line. End with
CNTL/Z.
Central(config)# ip ftp password 0 r0ut3rQQ
Central(config)# ip ftp user rscg
Central(config)# exit
Central# copy running-config ftp
Address or name of remote host []?14.2.9.1
Destination filename [central-confg]? central-config.txt
Writing central-config.txt !!
5699 bytes copied in 12.716 secs (474 bytes/sec)
Central#
```

En IOS 11.3 y anteriores, no es compatible con FTP, TFTP, pero se puede utilizar para la realización de copias de archivos de una manera muy similar. Debido a que TFTP es inseguro, debe utilizarse con cuidado y se desactiva cuando no está en uso. Otra forma de obtener una copia del archivo de la carrera de configuración es utilizar las funciones de texto de registro de Telnet y terminal de aplicaciones de emulación.

11. **Ver los procesos actualmente en ejecución:** Muchos servicios de IOS y las instalaciones se ejecutan como procesos separados IOS. Utilice el comando demostrar el proceso para listar los procesos en ejecución. La salida suele ser bastante larga. Compruebe los procesos no deseados y de servicios.

Mantener la hora correcta en un router también es importante para los registros precisos. Los Routers de Cisco soportan totalmente el estándar de Network Time Protocol (NTP), que se utiliza en Internet y en todas las principales redes DoD para distribuirla hora exacta.

4.3 METODOLOGÍA NIST

Para llevar un control de riesgos dentro de TI, NIST nos presenta la Guía de Gestión de Riesgo en Sistemas de Tecnología de la Información la cual abarca: Evaluación de riesgos, Reducción de riesgos. Para la evaluación de riesgos tenemos que abarcar nuevos pasos los cuales se describen a continuación:

PASO 1: Caracterización del sistema

El primer paso es definir el alcance del esfuerzo. En este paso, los límites del sistema informático se identifican, junto con los recursos y la información que constituyen el sistema.

La caracterización de un sistema que establece el alcance del esfuerzo de evaluación de riesgos, de line a la autorización de operación(o acreditación) de límites, y proporciona información (por ejemplo, hardware, software, conectividad del sistema, y la división responsable o personal de apoyo) esencial para definir el riesgo.

Sistema Relacionado de Información: Las personas que llevan a cabo la evaluación del riesgo deben primero recoger la información relacionada del sistema, que usualmente es clasificada como:

- Hardware.
- Software.
- Las interfaces del sistema (por ejemplo, la conectividad interna y externa).
- Los datos y la información.

- Las personas que apoyan y utilizan el sistema de TI.
- Misión del sistema (por ejemplo, los procesos realizados por el sistema de TI).
- El sistema y los datos de criticidad (por ejemplo, el valor del sistema o la importancia de una organización).
- El Sistema y datos sensitivos.

Información adicional relacionada con el ambiente operacional del sistema de TI y sus datos incluidos, pero esto no está limitada a lo siguiente:

- Los requisitos funcionales del sistema de TI.
- Los usuarios del sistema.
- Las políticas del sistema de seguridad que rijan el sistema de TI.
- Sistema de seguridad de la arquitectura.
- Actual topología de red.
- Protección de la información de almacenamiento que el sistema salvaguarda y los datos de disponibilidad, integridad y confidencialidad.
- Flujo de información relacionada con el sistema informático.
- Los controles técnicos utilizados en el sistema.
- Gestión de los controles utilizados para el sistema de TI.
- Los controles operativos utilizados para el sistema de Entorno de seguridad física del sistema informático.
- El ambiente de seguridad implementado por el sistema de TI de procesamiento del ambiente.

Las técnicas de recopilación de información

- Cuestionario: Para recopilar la información pertinente.
- Las entrevistas en sitio. Entrevistas con el apoyo del sistema de TI y personal de administración.

- Revisión de documentos: Los documentos de política, documentación del sistema, y la documentación relacionada.
- Uso de herramienta de análisis automatizado: Por ejemplo, una herramienta de mapeo de la red puede identificar los servicios que se ejecutan en un grupo grande de los ejércitos y proporcionar una forma rápida de crear perfiles individuales de la meta de sistema(s) informático(s).

PASO 2: identificación de amenazas

Una amenaza es la posibilidad de que una determinada fuente de amenaza para ejercer con éxito una determinada vulnerabilidad. Una vulnerabilidad es una debilidad que puede ser acciona accidentalmente o explotada intencionalmente.

Identificación de fuentes de amenazas: El objetivo de este paso es identificar las posibles fuentes de amenazas y compilar una lista de declaración de amenazas de las fuentes que son aplicables al sistema de TI que se evalúan.

Motivación y acciones de amenazas: La motivación y los recursos para llevar a cabo un ataque hacen potencialmente que los seres humanos se conviertan en una peligrosa fuente de amenaza.

PASO 3: Identificación de las Vulnerabilidades

El análisis de la amenaza a un sistema de TI debe incluir un análisis de las vulnerabilidades asociadas con el entorno del sistema (fallas o debilidades).

Fuentes de vulnerabilidad: Las vulnerabilidades técnicas y no técnicas asociadas con el procesamiento de un sistema informático de medio ambiente pueden ser identificadas a través de las técnicas de recopilación de información. Una revisión de otras fuentes de la industria (por ejemplo, las páginas web de proveedores que identifican los errores del

sistema y defectos) serán útiles en la preparación de las entrevistas y en el desarrollo de cuestionarios eficaces para identificar las vulnerabilidades que pueden ser aplicables a los sistemas informáticos específicos (por ejemplo, una versión específica de un sistema operativo específico).

Sistema de Pruebas de Seguridad: Métodos proactivos, empleados en las pruebas del sistema, se pueden utilizar para identificarlas vulnerabilidades del sistema de manera eficiente, en función de la criticidad del sistema de TI y los recursos disponibles (por ejemplo, los fondos asignados, la tecnología disponible, las personas con los conocimientos necesarios para realizar la prueba).

Los métodos de prueba incluyen:

- Automatizar la herramienta de análisis de vulnerabilidad.
- Seguridad de prueba y evaluación (ST & E).
- Prueba de penetración.

Desarrollo de la lista de verificación de seguridad de requerimientos: Durante esta etapa, el personal de evaluación del riesgo determinar si los requisitos de seguridad estipulados por el sistema de información y recogidos durante la caracterización del sistema se están cumpliendo los controles de seguridad existentes o en proyecto.

Por lo general, los requisitos de seguridad del sistema se pueden presentaren forma de tabla, con cada requerimiento acompañado de una explicación de cómo el diseño del sistema o la aplicación o no cumple este requisito de control de seguridad.

Una lista de verificación de requisitos de seguridad contiene las normas básicas de seguridad que se pueden utilizar para evaluar de forma sistemática e identificarlas vulnerabilidades de los activos (personal, hardware, software, información), los procedimientos, los procesos no automatizados, y las transferencias de información asociados a un determinado sistema de TI en las siguientes zonas de seguridad:

- Gestión.
- Operación.
- Técnicos.

Área de seguridad	Criterios de seguridad
Gestión de la Seguridad	▪ Asignación de responsabilidades ▪ La continuidad de soporte ▪ La capacidad de respuesta de incidentes ▪ Revisión periódica de los controles de seguridad ▪ Personal de acreditación y investigaciones de fondo ▪ Evaluación de riesgos ▪ Seguridad y la capacitación técnica ▪ Separación de funciones ▪ Sistema de autorización y reautorización ▪ Sistema o un plan de seguridad de las aplicaciones
Seguridad Operacional	▪ Control de los contaminantes transportados por el aire(humo, polvo, productos químicos) ▪ Controles para garantizar la calidad del suministro de energía eléctrica ▪ Los datos de acceso al medio y la eliminación ▪ Distribución de datos externa y el etiquetado ▪ Fondo para la protección (por ejemplo, sala de informática, centro de datos, oficina) ▪ Control de humedad ▪ Control de temperatura ▪ Estaciones de trabajo, equipos portátiles y equipos independientes de carácter personal
Seguridad Técnica	▪ Las comunicaciones (por ejemplo, acceso telefónico, la interconexión de sistemas, los routers) ▪ Criptografía ▪ control de acceso discrecional ▪ Identificación y autenticación ▪ Detección de intrusos ▪ Reutilización de objetos ▪ Sistema de auditoría

Tabla 4.1 Lista de verificación de requisitos de seguridad

PASO 4: Análisis de control

El objetivo de este paso es analizarlos controles que se han implementado, o están previstos para su ejecución, por la organización para minimizar o eliminarla posibilidad (o probabilidad) de una amenaza que está ejerciendo una vulnerabilidad del sistema.

Métodos de control: Controles de seguridad abarcan el uso de métodos técnicos y no técnicos. Los controles técnicos son las garantías que se incorporan en hardware, software o firmware (por ejemplo, mecanismos de control de acceso, identificación y mecanismos de autenticación, los métodos de encriptación, software de detección de intrusos). Los controles no técnicos son los controles de gestión y de funcionamiento, tales como las políticas de seguridad, los procedimientos operacionales; y personal, físicos y seguridad ambiental.

Categorías de Control: Las categorías de control para los métodos de control, tanto técnico como no técnico pueden ser clasificadas ya sea como preventivos o de detección. Estas dos subcategorías se explican como sigue:

- Los controles preventivos inhiben los intentos de violarlas política de seguridad de incluyen tales como la ejecución de los controles de control de acceso, cifrado y autenticación.
- Los controles Detectives advierten de violaciones de los intentos de la política de seguridad e incluyen controles tales como pistas de auditoría, los métodos de detección de intrusos, y las sumas de comprobación.

Técnica de control de análisis: El desarrollo de una lista de verificación de requisitos de seguridad o el uso de una lista de verificación disponible será de utilidad en el análisis de los controles de una manera eficiente y sistemática. La lista de verificación de requisitos de seguridad se puede utilizar para validar el incumplimiento de seguridad, así como el cumplimiento.

Por lo tanto, es esencial para actualizar esas listas de control para reflejar los cambios en el entorno de control de una organización (por ejemplo, cambios en las políticas de seguridad, métodos y requisitos) para garantizar la validez de la lista de verificación.

PASO 5: Determinación de probabilidad

Para obtener una calificación de riesgo global que indica la probabilidad de que una vulnerabilidad potencial que puede ejercer en la construcción del entorno de las amenazas asociadas, los siguientes factores que gobiernan deben ser considerados:

- Amenaza de código motivación y la capacidad
- La naturaleza de la vulnerabilidad
- Existencia y eficacia de los controles a ctuales.

La probabilidad de que una vulnerabilidad potencial podría ser ejercida por una determinada fuente de amenaza puede ser descrito como alto, medio o bajo.

PASO 6: Análisis del impacto

Este paso se enfoca en la importancia de determinar la medición del nivel de riesgo que tiene el impacto adverso como resultado de un ejercicio de éxito la amenaza de una vulnerabilidad. Antes de comenzar el análisis de impacto, es necesaria la siguiente información:

- Misión del sistema (por ejemplo, los procesos realizados por el sistema de TI)
- Sistema y los datos de criticidad (por ejemplo, el valor del sistema o la importancia de una organización)
- Sensibilidad del sistema y los datos.

Esta información puede ser obtenida de la documentación existente de organización, tales

como el informe de la misión el análisis de impacto o informe de activos respecto a la criticidad de evaluación. Un análisis del impacto de la misión (también conocido como análisis de impacto en el negocio para algunas organizaciones) da prioridad a los niveles de impacto asociados con el compromiso de los activos de información de una organización basada en una evaluación cualitativa o cuantitativa de la sensibilidad y criticidad de los activos.

Un activo crítico identifica y prioriza los bienes sensibles y críticos de la organización de la información (por ejemplo, hardware, software, sistemas, servicios y bienes relacionados con la tecnología) que apoyan las misiones fundamentales de la organización.

PASO 7: Determinación del riesgo

El propósito de este paso es evaluar el nivel de riesgo para el sistema de TI. La determinación de riesgo para una determinada amenaza/vulnerabilidad puede expresar como una función de:

- La probabilidad de una determinada fuente de amenaza está tratando de ejercer una vulnerabilidad determinada
- La magnitud del impacto en caso de una amenaza de código con éxito el ejercicio de vulnerabilidad
- La adecuación de los controles de seguridad existente o prevista para reducir o eliminar riesgo.

Para medir el riesgo, una escala de riesgo y una matriz de riesgo de nivel debe ser desarrollado.

PASO 8: Las recomendaciones de control

Durante este paso del proceso, los controles que podrían mitigar o eliminarlos riesgos identificados, según corresponda a las operaciones de la organización, se proporcionan. El

objetivo de los controles recomendados es el de reducir el nivel de riesgo para el sistema de TI y sus datos a un nivel aceptable. Los siguientes factores deben ser considerados en la recomendación de los controles y las soluciones alternativas para minimizar o eliminarlos riesgos identificados:

- Eficacia de las opciones recomendadas (por ejemplo, la compatibilidad del sistema)
- Legislación y regulación
- La política de la organización
- Impacto operacional
- Seguridad y fiabilidad

Las recomendaciones de control son los resultados del proceso de evaluación de riesgos y aportaciones al proceso de mitigación de riesgos, durante el cual los controles de seguridad recomendados técnicos y de procedimiento son evaluados, priorizados, e implementado.

PASO 9: Resultados de la documentación

Una vez quela evaluación del riesgo se ha completado (las fuentes de amenazas y vulnerabilidades identificadas, los riesgos evaluados, y los controles recomendados previstos), los resultados deben ser documentados en un informe oficial o la rueda de prensa.

Un informe de evaluación de riesgos es un informe de gestión que ayuda ala alta gerencia, los dueños de la misión, tomar decisiones sobre la política, el presupuesto y el sistema de cambios operativos y de gestión. A diferencia de un informe de auditoría o investigación, que se ve por las malas acciones, un informe de evaluación de riesgos no debe ser presentada en forma acusatoria, sino como un enfoque sistemático y analítico para la evaluación del riesgo por lo que en la alta dirección se entienden los riesgos y asignaciones de recursos para reducir y corregirlas posibles pérdidas. Por esta razón, algunas personas prefieren hacer frente a los pares de amenazas/vulnerabilidad como observaciones en lugar de los hallazgos en el informe de evaluación de riesgos.

CAPÍTULO 5. AUDITORÍA DEL ROUTER

5.1 INTRODUCCIÓN A LA AUDITORÍA DEL ROUTER

Se pretende estudiar la importancia de la auditoría de routers, procurando examinar los temas pertinentes a la revisión de los dispositivos antes y después de ser asegurados.

El router es analizado con más detenimiento, teniendo en cuenta la importancia de las posibilidades que provee.

Es importante resaltar que el tratamiento del aseguramiento es un tema muy importante en la actividad de un administrador de seguridad, ya que permite identificar las vulnerabilidades de los dispositivos y por ende desarrollar las herramientas y medidas necesarias para minimizar los riesgos ante posibles amenazas.

En el ***Anexo 1,*** se presenta el Cronograma de actividades realizada de la presente auditoria.

Este capítulo se analiza las vulnerabilidades del enrutador al ser configurado por defecto, establece el mecanismo para realizar su aseguramiento, y verifica el mejoramiento del sistema con la nueva configuración, además de emitir las observaciones correspondientes para su mejor funcionamiento y por último el cierre de la auditoria.

5.2 SOFTWARE UTILIZADO PARA AUDITORÍA (ROUTER AUDIT TOOL)

La Herramienta de Auditoría router o RAT fue diseñado para ayudar a auditar las configuraciones de los routers Cisco de forma rápida y eficiente. Pruebas RAT configuraciones del router Cisco en contra de una línea de base. Después de realizar la prueba de referencia, no sólo proporciona una lista de las posibles vulnerabilidades de seguridad descubiertas, sino también una lista de comandos que se aplicará al router con el fin de corregir los posibles problemas de seguridad descubiertos.

La herramienta de auditoría router (RAT) está disponible en el sitio web de Centro de Internet Security (CIS).[5]

Además de proporcionar un punto de referencia aceptada por la industria para el Cisco IOS, RAT ayuda a resolver las siguientes cuestiones:

- Dificultad para mantener la coherencia.
- Dificultad para detectar cambios.
- Necesidad de fijar rápidamente una configuración incorrecta.
- Necesidad de información y personalización.
- Necesidad de comprobar los dispositivos IOS.

Aunque RAT prevé muchas funciones útiles, no se actualizarán activamente y por lo tanto requiere que el usuario compruebe de vez en cuando las últimas notas de la versión y los

[5] http://www.cisecurity.org/bench_cisco.html

parches. Además, tan potente como lo es, hay una serie de problemas que no se ocupa, tales como:

- Asuntos Gerenciales.
- Pobre de Operaciones Prácticas.
- Código de proveedor.
- Protocolos debilidades.
- Basados en host (problemas de virus, código de color rojo).
- Ancho de banda de base vulnerabilidades de denegación de nuevas.
- Opciones de configuración local.
- Necesidad de la competencia y la vigilancia.
- No CISCO dispositivos aún no son compatibles.

¿Cómo funciona RAT?

La Herramienta de Auditoría router ha sido escrito en Perl. Se compone de 4 otros programas de Perl a saber NCAT, ncat_report, ncat_config y snarf.

- **Snarf:** Se utiliza para descargar la configuración del router.
- **NCAT:** Lee la base de reglas y archivos de configuración y proporciona una salida en un archivo de texto.
- **Ncat_report:** Crea las páginas HTML desde los archivos de texto.
- **Ncat_config:** Se utiliza para realizar la localización de la base de reglas.

Las normas y documentos de referencia están autorizados por el Centro para la Seguridad de Internet. RAT realiza una auditoría al comparar cadenas de texto en el archivo de configuración del router con las expresiones regulares en las reglas.

Cada regla tiene ya sea un elemento regular de la expresión "necesaria" o "prohibido". A partir del RAT el elemento que determina si una norma se aprueba o no. Debido al uso de

expresiones regulares, la base de reglas RAT es extremadamente flexible. En este momento hay Nivel 1 y Nivel 2 auditorías que se pueden realizar.

- El Nivel 1 de la auditoría se basa en las directrices de la NSA.
- El Nivel 2 incluye pruebas adicionales de auditoría de varias fuentes, incluyendo Cisco.

La mayoría de las reglas para la protección del router. Hay, sin embargo, varias reglas que proporcionan una protección limitada a las redes que sirven. Reglas adicionales pueden ser añadidas a la base de reglas con relativa facilidad. Esto permite RAT para trabajar con cualquier configuración.

Cómo ejecutar RAT

Antes de ejecutar RAT, primero debe determinar si las configuraciones del router van a ser obtenidos directamente desde el router o si ya se han descargado y guardado en un archivo. En el caso de este último, la ruta de acceso a ese archivo debe ser especificado al invocar RAT en la línea de comandos.

Alternativamente, con el uso del ***snarf*** interruptor, RAT registrará en los routers especificados (usted tiene que proporcionar información de acceso y dirección IP del router), tirar hacia abajo las configuraciones, auditar contra un conjunto de reglas y produce varios archivos de salida. Existen varias opciones o "interruptores" que pueden ser utilizados para controlar el comportamiento de RAT.

Además, hay varias maneras de guardar el archivo de configuración del router en un archivo. Sin embargo, los métodos de HTTP, TFTP o Telnet no son recomendables, ya que producir una salida en texto sin cifrar, por lo que representa un riesgo para la confidencialidad. Varios archivos se han creado después de ejecutar RAT con el archivo de configuración, la generada con el RAT es el archivo **index.html**. Los detalles de los archivos de salida que se crean por RAT se incluyen en el ***Anexo 2.***

5.3 INICIO DE AUDITORÍA

En la Ciudad de México, Distrito Federal, siendo las diez horas del día primero de Marzo de dos mil doce, el ciudadano Ing. Joaquín Zarco Rabágo, Director de Automatización de Procesos y Soporte Técnico, y los C. Cuevas Olivares Jacobo, Enríquez Prado Jorge Alberto, Jiménez Velázquez Norma Leticia, Reyes Dionicio Ivonne, Rodríguez Olivo Ana Bertha, alumnos del seminario de titulación de ESIME Culhuacan, I.P.N., hacen constar que se constituyeron legalmente en las oficinas que ocupa la Dirección General de Calidad y Educación en Salud, ubicadas en la calle Homero número Doscientos trece, piso diez, Colonia Chapultepec Morales, Delegación Miguel Hidalgo, Distrito Federal, México, a efecto de iniciar la auditoría, denominada "Auditoria de ROUTERS", por el periodo de Marzo a Abril del dos mil doce, con la presencia del C. Ing. Víctor Hugo Higuera Muñoz, Subdirector de Sistemas de Información y Soporte Técnico, a fin de proceder a levantar la presente acta de inicio de auditoría. ***(Véase el Anexo 3)***

Checklist

El checklist o lista de verificación, es una técnica muy utilizada en el campo de la auditoría, es una lista de comprobación o cuestionario que detalla los distintos aspectos que se deben analizar, comprobar, verificar, etc., en una organización, empresa, etc., siguiendo pautas determinadas dependiendo de qué estemos evaluando o que objetivos queramos alcanzar.

El auditor crea un checklist para evaluar y sacar conclusiones, guiándose por las respuestas que el cliente ha dado a través del cuestionario o checklist. Los Checklists deben ser contestados oralmente, ya que superan en riqueza y generalización a cualquier otra forma, según la claridad de las preguntas y el talento del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable.

Es por ello, que se aplico un checklist al personal correspondiente de la Dirección General de Calidad y Educación en Salud.

No	Sección	NO	SI	Recomendación
	Seguridad de Configuración Estática			
1	Designación de autorizaciones para acceder directamente al router a través de la consola o de otras conexiones directas de acceso a puertos.	No		
2	Designar quien está autorizado para asumir privilegios de administrador en el router.	No		
3	Definición de políticas para las contraseñas de usuario/inicio de sesión y las contraseñas administrativas o de privilegios.	No		
4	Designación de los protocolos, procedimientos, y las redes permitidas para iniciar sesión en el router de forma remota.	No		
5	Definición de los procedimientos de recuperación y asignación o identificación de las personas responsables de la recuperación de la configuración estática del router.	No		
6	Designa los procedimientos y los límites sobre el uso de la gestión automatizada a distancia y los medios de vigilancia (por ejemplo, SNMP).	No		
7	Define la política de gestión de claves de largo plazo, las claves de cifrado (si existe).	No		
	Seguridad de Configuración Dinámica			
8	Identifica los servicios de configuración dinámica permitidas en el router, y de las redes permite el acceso a esos servicios.	No		
9	Identifica los protocolos de ruteo a ser usado, y las características de seguridad a emplear en cada uno.	No		
10	Designa mecanismos y políticas para la creación o el mantenimiento de la automatización del reloj del router (por ejemplo, ajuste manual, NTP).	No		
11	Identifica acuerdo de claves y algoritmos criptográficos autorizados para su uso en el establecimiento de túneles VPN con otras redes (si existe).	No		

Tabla 5.1 Checklist implementado en la Auditoria

5.4 ANALIZANDO EL ROUTER

El dispositivo en estudio es un router Cisco Serie 2500. Contiene cuatro interfaces: Ethernet 0, Ethernet 1, Serial 0 y Serial 1, las cuales facilitan la conexión a otros dispositivos tales como computadores, switches, hubs, entre otros; con la ventaja que pueden activarse administrativamente (ponerse up o down) de acuerdo a las necesidades; es decir que cualquiera de las cuatro interfaces puede activarse para que funcione o no lo haga de acuerdo a lo que el administrador desee.

El router cuenta con una conexión para consola y otra auxiliar (ambas para cable RJ45) y desde luego la conexión de potencia. El router está compuesto por memoria ROM, NVRAM, Flash RAM, RAM y registro de configuración. Brevemente se describen estos aspectos:

- **ROM:** contiene el Autotest de encendido (POST) y el programa de carga del router (éste depende del que esta por defecto o el de la última configuración). Los circuitos integrados de la ROM también contienen parte o todo el sistema operativo (IOS) del router.
- **NVRAM (No Volatil Random Access Memory):** almacena el archivo de configuración de arranque para el router; ya que la memoria NVRAM mantiene la información incluso si se interrumpe la corriente en el router.
- **Flash RAM:** es un tipo especial de ROM que puede borrarse y reprogramarse. Utilizada para almacenar el sistema operativo que ejecuta el router; algunos routers ejecutan la imagen del sistema operativo directamente desde la Flash sin cargarlo en la RAM, como la serie 2500.

  Habitualmente, el fichero del sistema operativo almacenado en la memoria Flash, se almacena en formato comprimido.
- **RAM**: Proporciona el almacenamiento temporal de la información (los paquetes se guardan en la RAM mientras el router examina su información de

direccionamiento), además de mantener otro tipo de información crítica, como la tabla de enrutamiento que se esté utilizando en ese momento.

- **Registro de Configuración:** Se utiliza para controlar la forma en que inicia el router.

Considerando lo anterior, es necesario pasar al análisis de la consola que es la parte básica para los procesos que se explican posteriormente. Para el presente caso, se conectó el router (consola) a un computador (puerto com) por medio del cable Rj45, y se configuró por hyperterminal[6] de la siguiente manera:

Parámetro	Configuración
Emulación de terminal	Automático
Velocidad en baudios	9600
Paridad	Ninguna
Bits de datos	8
Bits de parada	1

Tabla 5.2 Configuración por hyperterminal del router

El primer paso teniendo lo anteriormente establecido, es recobrar el password del router, por que tanto el login como el password por defecto son "admin", lo cual no genera seguridad alguna. Los pasos para recobrar el password son los siguientes:

1. Apague el router y vuelva a encenderlo. Cuando el router se arranque, pulse **Ctrl+Enter**.
2. A continuación aparece en pantalla el modo Monitor ROM. Introduzca **e/s2000002**, y después pulse **Enter**. Escriba en un papel el número de configuración virtual que aparezca en la pantalla.

[6] Consola que presenta Windows, en la cual se configuran dispositivos de red tales como routers.

3. En el indicador introduzca ahora **o/r0x2142** y pulse **Enter**. Con ello el router ignorará el archivo de configuración incluido en la NVRAM. Introduzca la letra **"i"** en el indicador y pulse **Enter**.

   El router volverá a iniciar y presentará el cuadro de diálogo de configuración. Seleccione **No** para que no se inicie una autoconfiguración y pulse **Enter**.
4. En el indicador del router, escriba **enable** para lanzar el modo privilegiado. Introduzca **copy startup-config running-config**, y después pulse **Enter** para acceder a la configuración original del router almacenada en la RAM.
5. En el indicador de activación, introduzca **config**. Ya se encuentra en el modo configuración. Escriba **enable secret [NuevaContraseña]**, para el caso presente [1qazxsw2].
6. Escriba en número de configuración virtual **config-register 0x**, que no es más que el número que escribió antes en el papel, y pulse **Enter**.
7. Ahora escriba **end** y pulse **Enter** para salir del modo configuración.
8. Reinicie el router. Ya tiene asignada la nueva contraseña.

En la Dirección General de Calidad y Educación en Salud cuenta con un router modelo Cisco 2500, el cual da servicio a seis pisos. El router está conectado a seis switch que brinda el servicio a cada uno de los pisos. La Dirección general de Calidad y Educación en Salud cuenta con diez equipos por piso dando un total general de sesenta maquinas.

La arquitectura inicial de prueba que se utilizó, es la que se muestra en la ***Anexo 4,*** donde el dispositivo 192.168.10.27 se habilitó como consola de configuración del enrutador, a quien se le asignó la dirección IP 192.168.10.21 por la interfaz ethernet 0. Para el ejercicio de aseguramiento se utilizó una configuración inicial como se indica en el ***Anexo 5.***

El primer paso a seguir es localizar la base de reglas del sitio C:\CIS\RAT\bin>. Con la actual configuración, se ejecutó **ncat_config.exe**[7] por medio del cual se actualizó el archivo

[7] Ncat_config.exe es un archivo de configuración, componente de RAT.

de configuración del enrutador, a través de la realización de algunas preguntas sobre el estado del mismo.

Se utilizó RAT (Router Audit Tool) en su ejecución, teniendo como parámetros la dirección IP del enrutador, para este caso 192.168.10.21, y el flag *–a* (snarf), indicando que la configuración deberá ser descargada del archivo de configuración previamente establecido.

En la pantalla se muestra una serie de comandos donde en primer lugar indicamos la configuración que deberá ser cargada del archivo de configuración previamente establecido introduciendo el password en este caso es 3edcxsw2, registrando la dirección IP del router. Posteriormente da inicio la ejecución del programa que se audita contra un conjunto de reglas, de la cual producirá varios archivos de salida dando el resultado del estado en que se encuentra la configuración. Como se muestra en el ***Anexo 6.***

Tras la ejecución de RAT, se genera un archivo index.html, en el que se muestran una lista de vulnerabilidades para cada una de las pruebas ejecutadas desde ncat.conf. El archivo se muestra en el ***Anexo 7.*** Donde las líneas sombreadas reflejan una configuración inadecuada que puede sugerir riesgos de accesos no autorizados al enrutador.

Sección	NO	SI	Observaciones
Designación de un administrador del router, así como, Designar quien está autorizado para asumir privilegios de administrador en el router.		Si	Capacitar al personal encargado para el mejor funcionamiento de administración
Se tiene passwords para acceder directamente al router a través de la consola o de otras conexiones directas de acceso a puertos.	No		Especificar un password para línea de acceso y auxiliar
Están seguros los paquetes que contienen rutas especificas de envío	No		Deshabilitar la opción de envió de rutas especificas en paquetes
Identifica los protocolos de ruteo a ser usado, y las características de seguridad a emplear en cada uno.	No		Desactivar el protocolo CDP[3]

Se tiene para cada una de los enlaces de acceso (vty, console, aux) control de tiempo para sesiones.	No		Controlar el tiempo de Abandono de una sesión por parte de un usuario
Los passwords pueden ser vistos en plano, tienen algún tipo de cifrado.	No		Encriptar los passwords para que no sean mostrados en pantalla, vistos o aprendidos por personas no autorizadas
Esta asegurada la conexión de sesión al salir abruptamente.	No		Interrumpir sesiones que No responden inmediatamente
Definición de los procedimientos de recuperación y asignación o identificación de las personas responsables de la recuperación de la configuración estática del router.	No		Deshabilitar la configuración por defecto
Esta seleccionado el tipo de protocolo a usarse			Seleccionar solo los protocolos admitidos por cada uno de los enlaces
Identifica los servicios de configuración dinámica permitidas en el router, y de las redes permite el acceso a esos servicios.	No		Bloquear cualquier tipo de protocolo de acceso

Tabla 5.3 Checklist implementado en la Auditoria

Análisis de riesgo

El router de la Dirección General de Calidad y Educación en Salud, se encuentra expuesto a riesgo. No solo degradan el recurso, sino que impactan en menor o mayor grado el cumplimiento de los objetivos.

Se lograra estimar la frecuencia con la cual se materializan esos riesgos, así como determinar la magnitud de sus posibles consecuencias, podemos de modo preventivo tomar medidas utilizando controles para reducir su impacto.

Tomando en cuenta que el recurso tecnológico es considerado hoy, algo muy importante y valioso en la Dirección General de Calidad y Educación en Salud, por ende generador de mayores consecuencias negativas cuando sufre fallas, es nuestra responsabilidad mantener

una adecuada administración del riesgo del mismo, que nos permita identificar no solo las oportunidades, sino evitar o mitigar las pérdidas económicas y de imagen asociadas con ellos.

Matriz de análisis de riesgo

La Matriz, no dará un resultado detallado sobre los riesgos y peligros de cada recurso (elemento de información) de la Dirección, sino una mirada aproximada y generalizada de estos. Entonces lo que se pretende con el enfoque de la Matriz es localizar y visualizar el router de la Dirección General de Calidad y Educación en Salud, que están en peligro de sufrir un daño por algún impacto negativo, para posteriormente ser capaces de tomar las decisiones y medidas adecuadas para la superación de las vulnerabilidades y la reducción de las amenazas.

La matriz para el Análisis de Riesgo, el resultado se obtiene mediante la siguiente fórmula:

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

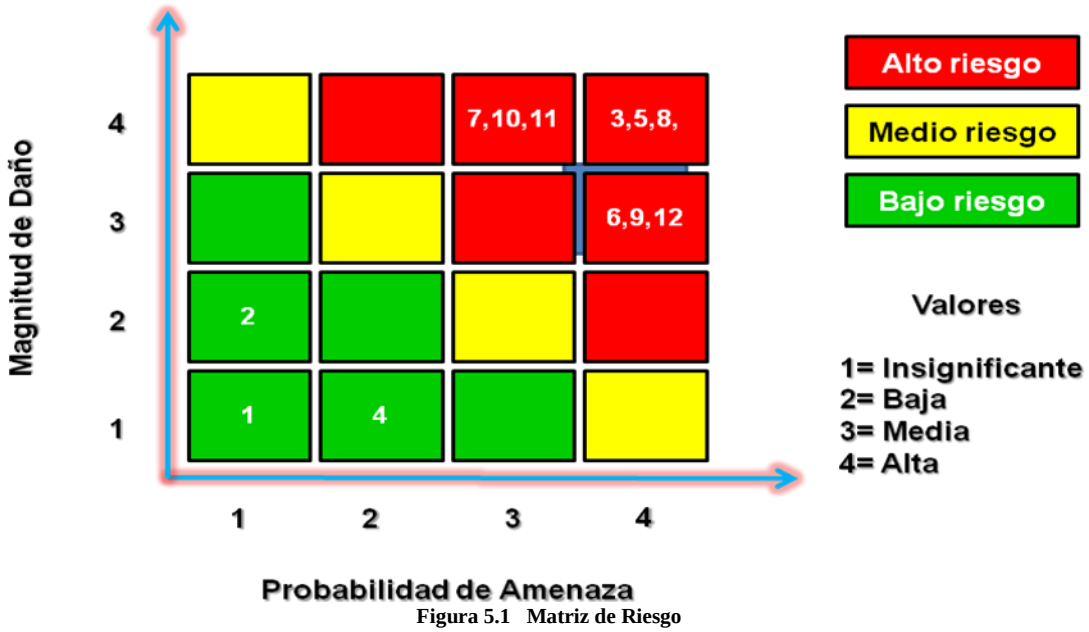


Figura 5.1 Matriz de Riesgo

Observaciones	Impacto	Recomendación
Capacitar al personal encargado para el mejor funcionamiento de administración	Al no tener la adecuada administración y seguridad del router es una vulnerabilidad alta para ataques, asi como, perdida de información o denegación del mismo router	
Especificar un password para línea de acceso y auxiliar	Si no se tiene un password para las diferentes líneas de acceso cualquiera podría entrar y hacer daños	Asignar un Password para las diferentes líneas de acceso (config)# line console 0 (config-line)# password 0okmnji9 (config-line)# exit (config)# line aux 0 (config-line)# password 9ijnbhu8 (config-line)# exit
Deshabilitar la opción de envió de rutas especificas en paquetes	Pueden ser utilizadas en diferentes tipos de ataque como por ejemplo “spoofing”	Aplicar el comando siguiente para deshabilitar esta función (config)# no ip source-route
Desactivar el protocolo	Podrían saber que clase de enrutador se tiene, así como, la versión de IOS pudiendo ser utilizada esta información para ataques de denegación del servicio(DenialService)	(config)# no cdprun Con el comando arriba escrito deja de estar habilitado el protocolo CDP para identificar otros dispositivos dentro de la misma red.
Controlar el tiempo de Abandono de una sesión por parte de un usuario	Se trata de prevenir que usuarios no autorizados ingresen a través de sesiones abandonadas	Comando para: vty, console, aux (config-line)# exec-timeout 5esto permite que tras cinco minutos de abandono por parte del usuario la comunicación sea interrumpida
Encriptar los passwords para que no sean mostrados en pantalla, vistos o aprendidos por personas no autorizadas	Previene que los passwords sean mostrados en pantalla y asi sean vistos y robados por personas no autorizadas	(config)# service password encryption
Interrumpir sesiones que No responden inmediatamente	Impedir que usuarios malintencionados se adueñen de la conexión	(config)# service tcp-keepalives-in Esto hace que las sesiones que no responden se corten inmediatamente
Deshabilitar la configuración por defecto	Prevenir que sea una vulnerabilidad ya que	En las interfaces serial 0,1 y en las interfaces ethernet 0,1

	cualquiera al consultar el manual podría ver la misma y utilizarla para fines malintencionados	(config-if)# no ip proxy-arp
Seleccionar solo los protocolos admitidos por cada uno de los enlaces	Prevenir la aceptación de cualquier protocolo	(config)# line vty 0 4 (config-line)# transport input telnet
Bloquear cualquier tipo de protocolo de acceso		(config)# line aux 0 (config-line)# no exec (config-line)# transport input none

Tabla 5.4 Observación, Impacto y Recomendación

Aplicación de las recomendaciones

A. La primera de estas fallas señala que las diferentes líneas de acceso al sistema requieren un password. Los siguientes comandos especifican un password para cada unas de las líneas (consola y auxiliar):

```
(config)# line console 0
(config-line)# password 0okmnji9
(config-line)# exit

(config)# line aux 0
(config-line)# password 9ijnbhu8
(config-line)# exit
```

B. La siguiente falla hace referencia al establecimiento de restricciones sobre los paquetes que puedan especificar rutas específicas de envió, controladas por opciones de enrutamiento contenidas en los datagramas, las cuales pueden ser utilizadas en diferentes clases de ataques, tales como “spoofing”. La siguiente instrucción hace que este servicio no esté disponible:

```
(config)# no ip source-route
```

C. El protocolo CDP[8] utilizado por Cisco Routers para identificar otros dispositivos enrutadores dentro de la misma red. Este protocolo permite que dispositivos puedan determinar la clase de enrutador que se tiene, así mismo como la versión de IOS, pudiendo ser esta información utilizada en diseño de ataques de denegación del servicio (Denial Of Service) y debería estar no disponible dentro de los servicios del enrutador. La siguiente instrucción, logra establecer esta condición:

```
(config)# no cdp run
```

D. Dentro de las siguientes fallas se reporta, para cada unas de los enlaces de acceso (vty, console y aux), que no tienen un control de tiempo para sesiones de usuarios; es decir, se trata de prevenir que usuarios no autorizados ingresen a través de sesiones abandonadas.

La ejecución del comando **exec-tiemout 5** en cada una de las conexiones hace que tras 5 minutos de abandono por parte del usuario, la comunicación sea interrumpida.

```
(config)# line vty 0 4
(config-line)# exec-timeout 5
(config-line)# exit

(config)# line console 0
(config-line)# exec-timeout 5
(config-line)# exit

(config)# line aux 0
(config-line)# exec-timeout 5
(config-line)# exit
```

E. Al mostrarse la configuración del enrutador por pantalla, los passwords de acceso son mostrados en texto plano; para evitar esto, la ejecución del comando **service password-encryption** hace que los passwords mostrados por pantalla no sean vistos y aprendidos por personas no autorizadas.

[8] Cisco Discovery Protocol

```
(config)# service password-encryption
```

F. De igual forma, otro problema que puede presentarse, sucede cuando se establecen conexiones al enrutador, donde después de establecida la conexión, el usuario remoto corta su sesión inesperadamente, pero mantiene la conexión en línea. Esto podría ocasionar que usuarios malintencionados se adueñen de la conexión. La ejecución del comando **service tcp-keepalives-in**, hace que las sesiones que no responden se corten inmediatamente.

```
(config)# service tcp-keepalives-in
```

G. Es importante resaltar que los enrutadores Cisco en su configuración por defecto permiten ser usados como servidores Proxy de direcciones de red (MAC), actuando como intermediarios en el manejo de ARP (Address Resolution Protocol) entre diferentes segmentos LAN. Con la ejecución de **no ip proxy-arp**, se establece que esta función no sea asumida por el enrutador para cada unas de las interfaces. La ejecución es la siguiente:

```
(config)# interface serial 0
(config-if)# no ip proxy-arp
(config-if)# exit

(config)# interface serial 1
(config-if)# no ip proxy-arp
(config-if)# exit

(config)# interface ethernet 0
(config-if)# no ip proxy-arp
(config-if)# exit

(config)# interface ethernet 1
(config-if)# no ip proxy-arp
(config-if)# exit
```

H. La configuración inicial del enrutador incluía la aceptación de cualquier protocolo para la comunicación remota al enrutador a través del enlace vty 0 4. Con el comando

transport input se quiere seleccionar solo los protocolos admitidos por cada unos de los enlaces.

Para el caso del enrutador Cisco Router Series 2500 se opto por telnet como protocolo, pero se advierte que este protocolo envía los mensajes por texto plano.

Se puede seleccionar otros protocolos como ssh pero la versión de enrutador que trabajamos no lo reconoce.La instrucción es:

```
(config)# line vty 0 4
(config-line)# transport input telnet
(config-line)# exit
```

I. Para la actual arquitectura, el puerto **aux** no se encuentra en uso, siendo una potencial ruta de acceso para ataques, por lo tanto se considera importante no activarla y bloquear cualquier tipo de protocolo de acceso.

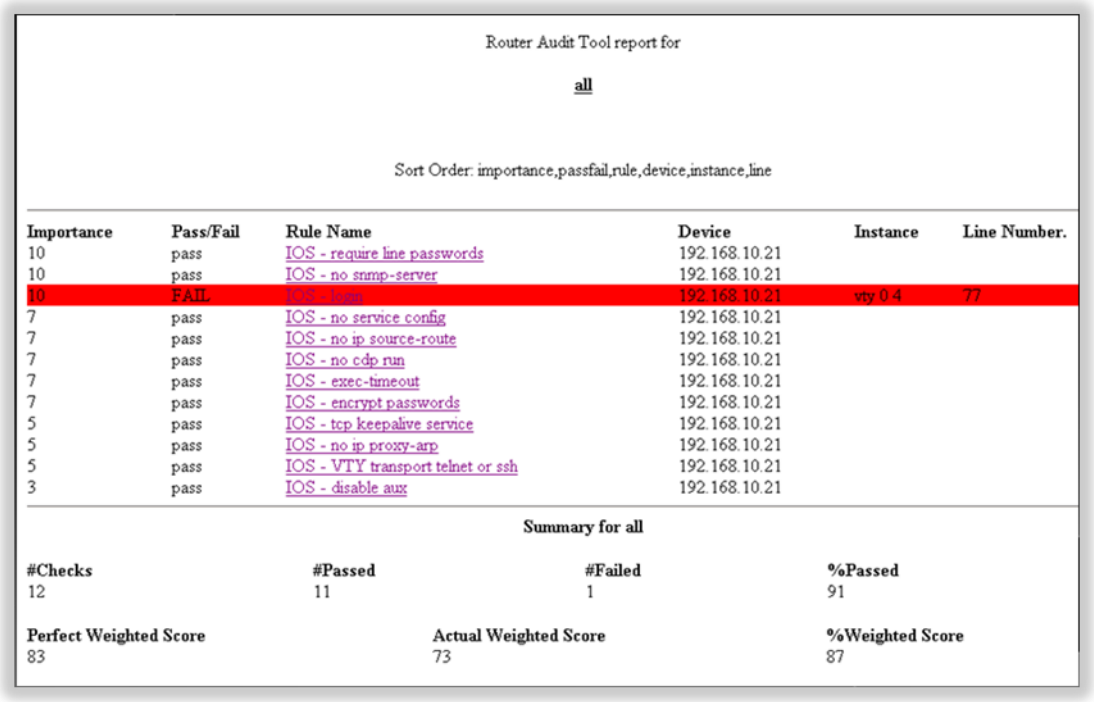
Hay que advertir que ante cualquier contingencia es útil tener el puerto abierto para comunicaciones vía MODEM, esto siendo una decisión de configuración. La siguiente instrucción, deshabilita protocolos de comunicación:

```
(config)# line aux 0
(config-line)# no exec
(config-line)# transport input none
(config-line)# exit
```

Al finalizar las instrucciones de hardening, se salvó la configuración, ejecutando la siguiente línea de comando:

```
# write memory
```

Realizada la configuración anterior, la herramienta RAT es de nuevo ejecutada sobre el enrutador, obteniéndose el siguiente resultado.



Router Audit Tool report for

all

Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	pass	IOS - require line passwords	192.168.10.21		
10	pass	IOS - no snmp-server	192.168.10.21		
10	FAIL	IOS - login	192.168.10.21	vty 0 4	77
7	pass	IOS - no service config	192.168.10.21		
7	pass	IOS - no ip source-route	192.168.10.21		
7	pass	IOS - no cdp run	192.168.10.21		
7	pass	IOS - exec-timeout	192.168.10.21		
7	pass	IOS - encrypt passwords	192.168.10.21		
5	pass	IOS - tcp keepalive service	192.168.10.21		
5	pass	IOS - no ip proxy-arp	192.168.10.21		
5	pass	IOS - VTY transport telnet or ssh	192.168.10.21		
3	pass	IOS - disable aux	192.168.10.21		

Summary for all

#Checks	#Passed	#Failed	%Passed
12	11	1	91

Perfect Weighted Score	Actual Weighted Score	%Weighted Score
83	73	87

Figura 5.2 Resultado final RAT

En la nueva salida de RAT, reporta un fallo de seguridad con respecto a la autenticación de logins de acceso. Esto debido a que debería implantarse un servidor de logins, por medio del protocolo **tacacs+** [9] y hacer la autenticación y centralización de nombres.

La ejecución del siguiente comando verifica este requerimiento:

```
(config)# line vty 0 4
(config-line)# login authentication default
(config-line)# exit
```

Con la actual configuración, se realizó otra prueba de scanner con otro analizador llamado Nessus, el cual reportó fallos de bajo riesgo. Estos fallos se resumen a continuación:

[9] Terminal Access Controller Access Control System Plus – protocolo de seguridad que provee centralización de autenticación, autorización y registro de usuarios que acceden a un enrutador o servidor de acceso. TACACS+ es definido por Cisco

Se encuentra habilitado Service Finger, quien hace parte de la familia de pequeños servicios disponibles por IOS y puede liberar información de usuarios a posibles atacantes. Aunque no constituye alto riesgo, se pueden deshabilitar si no se están utilizando, con la siguiente ejecución:

```
(config)# no service finger
```

Siendo el servicio Finger un integrante de los pequeños servicios de UTP/TCP, deshabilitando estos servicios se inhabilitan el servicio Finger. Esto se consigue con la ejecución de:

```
(config)# no service tcp-small-servers
(config)# no service udp-small-servers
```

Dentro del concepto de "endurecimiento" (hardening) se incluye el aseguramiento de logs generados por IOS donde existen varias estrategias para el manejo de los mismos, en estas se incluyen, guardar los logs generados en un sector de memoria del enrutador, y establecer una conexión con otro dispositivo donde se quieran enviar, para su posterior análisis en incidentes de seguridad.

Para la primera opción se asigna un sector de memoria, lo que se consigue con la ejecución de **logging buffered,** al cual se le da el tamaño de la memoria de asignación, verificando previamente la capacidad de la memoria actual. La instrucción se muestra a continuación:

```
(config)# logging buffered 16000
```

Para el segundo caso, se envían los logs generados a un dispositivo que alberga un administrador de logs; en este caso Syslogd en sistemas Linux y WSyslogD en sistemas WinNT. Se ejecuta el comando **logging** indicando la dirección IP del dispositivo al que se pretende enviar los logs, como se indica:

```
(config)# logging 192.168.10.26
```

```
(config)# logging 192.168.10.28
(config)# logging trap 7
```

El dispositivo con dirección IP 192.168.10.26 tiene a Syslogd como administrador de logs, mientras que el dispositivo con dirección 192.168.10.28 tiene instalado WSyslogD. Los logs se pueden ver en su visor, como se muestra a continuación:

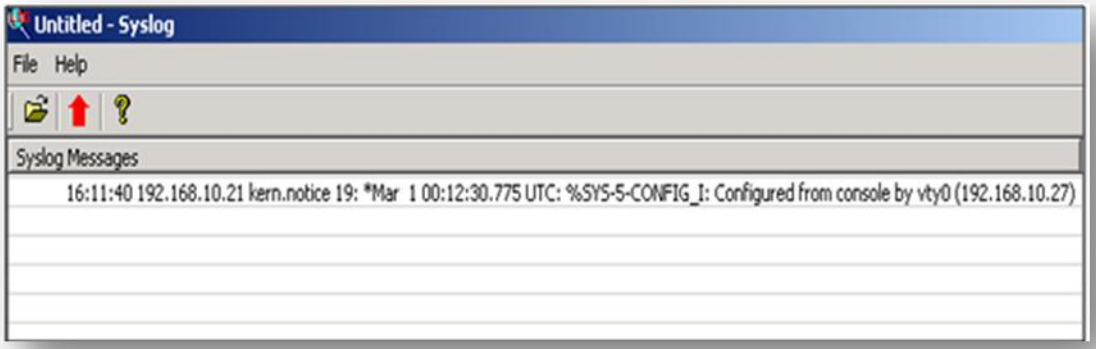


Figura 5.3 Visor de logs en WSyslogD

La ejecución **logging trap 7** establece la clase de logs que se quieren registrar, en este caso 7 (debugging).

La salida del comando **show logging** muestra por consola los logs generados por IOS, como se muestra:

```
# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0
overruns)
    Console logging: level debugging, 21 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level informational, 25 message lines logged
```

```
        Logging to 192.168.10.26, 25 message lines logged
.
.
.

 09:31:08.515 UTC: %SYS-5-CONFIG_I: Configured from console by
console
 09:33:53.439 UTC: %SYS-5-CONFIG_I: Configured from console by
console
#
```

La estructura de los logs generados está compuesta por 3 partes: la fecha y hora cuando el mensaje fue generado, nombre del mensaje y nivel de severidad (ver Tabla 1) y por último el testo del mensaje. El último mensaje mostrado, se genero a las **9:33.53 a.m.**, el nivel de severidad es **5** que corresponde **notifications** y por último muestra el texto, notificando que ha habido una actualización de la configuración por medio de consola.

Nivel	Nombre de Nivel	Descripción
0	Emergencias	Enrutador no funciona
1	Alerta	Acción necesaria Inmediata
2	Critico	Condición crítica
3	Errores	Condición de error
4	Advertencias	Condición de advertencia
5	Notificaciones	Eventos normales
6	Informacional	Mensaje de información
7	Debugging	Mensaje de debugging

Tabla 5.5 Niveles de severidad en Cisco logs

Por último, el establecimiento de usuarios autorizados para sesiones remotas de acceso (telnet), se establece por medio de la creación de modelos de acceso. Estos permiten establecer una conexión para un usuario, por medio de la autenticación de login y password.

La siguiente instrucción, establece un modelo en el que se requiere el nombre de usuario (login) y password correspondiente, y luego verifica acceso a IOS y la configuración del enrutador, por medio del parámetro enable., como se muestra:

```
(config)# aaa new-model
(config)# aaa authentication login default local
(config)# aaa authentication enable default enable
```

A continuación se crean usuarios autorizados para acceso remoto:

```
(config)# username camilo password 8uhbvgy7
```

Lo anterior señala la creación del usuario con el password 8uhbvgy7. La configuración final del enrutador se presenta en el ***Anexo 8.***

Teniendo en cuenta que las conexiones remotas (Telnet) son enviadas en texto plano, conlleva un alto riesgo que un usuario no autorizado pueda ver login y password y establezca una conexión no permitida.

La solución propuesta, es restringir los accesos IOS, tan solo permitiendo la comunicación a través del puerto de consola. Esto se logra, estableciendo restricción al protocolo Telnet, sobre el enlace vty 0 4, como se presenta a continuación:

```
(config)# line vty 0
(config-line)# transport input none
(config-line)# exit
```

5.5 OBSERVACIONES DE LA AUDITORÍA

No.	Recomendaciones	Solución
1	Especificar un password para línea de acceso y auxiliar	(config)# line console 0 (config-line)# password 0okmnji9 (config-line)# exit (config)# line aux 0 (config-line)# password 9ijnbhu8 (config-line)# exit
2	Deshabilitar la opción de envió de rutas especificas en paquetes	(config)# no ip source-route
3	Desactivar el protocolo	(config)# no cdp run
4	Controlar el tiempo de Abandono de una sesión por parte de un usuario	Comando para: vty, console, aux (config-line)# exec-timeout 5
5	Encriptar los passwords para que no sean mostrados en pantalla, vistos o aprendidos por personas no autorizadas	(config)# service password encryption
6	Interrumpir sesiones que No responden inmediatamente	(config)# service tcp-keepalives-in
7	Deshabilitar la configuración por defecto	En las interfaces serial 0,1 y en las interfaces ethernet 0,1 (config-if)# no ip proxy-arp
8	Seleccionar solo los protocolos admitidos por cada uno de los enlaces	(config)# line vty 0 4 (config-line)# transport input telnet
9	Bloquear cualquier tipo de protocolo de acceso	(config)# line aux 0 (config-line)# no exec (config-line)# transport input none

Tabla 5.6 Observaciones de la auditoría

5.6 CIERRE DE AUDITORÍA

En la Ciudad de México, Distrito Federal, siendo las diez horas del veinte de Abril de dos mil doce, queda concluida la auditoría realizada en la Dirección General de Calidad y Educación en Salud notificándose al titular el Ing. Joaquín Zarco Rabágo, Director de Automatización de Procesos y Soporte Técnico. ***(Vease el Anexo 9)***

CONCLUSIONES

Es importante resaltar la importancia del aseguramiento de los dispositivos tales como los routers puesto que generan graves riesgos de seguridad para una red si no se toman las medidas adecuadas. En el caso del router la configuración por defecto es bastante deficiente en cuestiones de seguridad, ya que teniendo en cuenta lo observado las vulnerabilidades están a la orden del día (o del atacante).

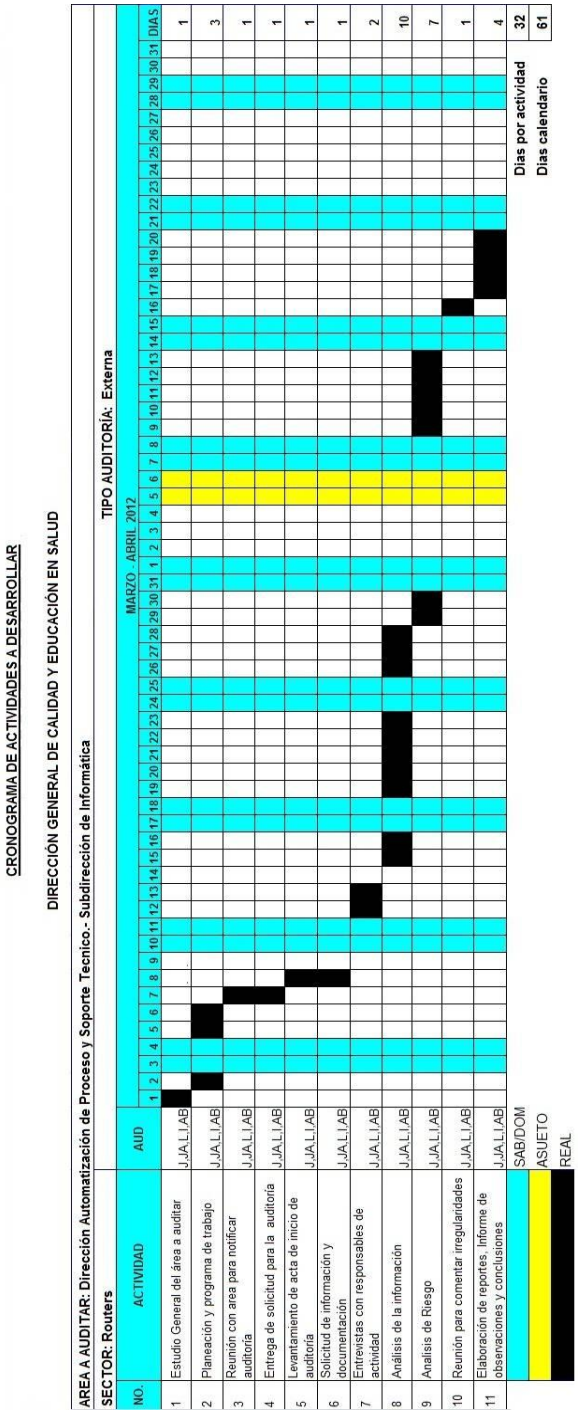
Es necesario conocer en profundidad los dispositivos para poder comprender lo que sucede con los mismos y como se pueden proteger adecuadamente. Así mismo es necesario revisar los diferentes documentos relacionados con seguridad para entender los propósitos de cada medida y apoyarse en software (RAT) que ayuda realmente en la identificación de las vulnerabilidades de los dispositivos.

De acuerdo con la National Security Agency (NSA), los enrutadores proveen servicios que son esenciales, así mismo el comprometer un enrutador puede dejar varios problemas de seguridad para el segmento que sirven o aun con otras redes que intercomunican, hace que se conviertan en un blanco para los atacantes. Como se dijo anteriormente, la utilización de herramientas como RAT, provee una guía para el aseguramiento del enrutador, pero hay que tener en cuenta que estas decisiones deben ser tomadas en base a los requerimientos del segmento, y cada unas de las vulnerabilidades dadas por el reporte son sugerencias, y que la decisión recae sobre la persona responsable de la configuración, de corregirlas o no.

La Dirección General de Calidad y Educación en Salud, considero e implemento las recomendaciones hechas en la auditoria. Teniendo como resultados el buen funcionamiento en los servicios de red y mejor aseguramiento del router.

ANEXOS

➢ Anexo 1. Cronograma de Actividades



CRONOGRAMA DE ACTIVIDADES A DESARROLLAR

DIRECCIÓN GENERAL DE CALIDAD Y EDUCACIÓN EN SALUD

AREA A AUDITAR: Dirección Automatización de Proceso y Soporte Tecnico.- Subdirección de Informática — TIPO AUDITORÍA: Externa

SECTOR: Routers — MARZO - ABRIL 2012

NO.	ACTIVIDAD	AUD	DIAS
1	Estudio General del área a auditar	J,JA,L,I,AB	1
2	Planeación y programa de trabajo	J,JA,L,I,AB	3
3	Reunión con area para notificar auditoria	J,JA,L,I,AB	1
4	Entrega de solicitud para la auditoría	J,JA,L,I,AB	1
5	Levantamiento de acta de inicio de auditoria	J,JA,L,I,AB	1
6	Solicitud de información y documentación	J,JA,L,I,AB	1
7	Entrevistas con responsables de actividad	J,JA,L,I,AB	2
8	Análisis de la información	J,JA,L,I,AB	10
9	Analisis de Riesgo	J,JA,L,I,AB	7
10	Reunión para comentar irregularidades	J,JA,L,I,AB	1
11	Elaboración de reportes. Informe de observaciones y conclusiones	J,JA,L,I,AB	4
		SAB/DOM	Dias por actividad 32
		ASUETO	Dias calendario 61
		REAL	

- **Anexo 2. Archivos de salida creadas por RAT**

syd_1760rt_06082007.txt	**Archivo RAW contiene configuraciones del router.**
syd_1760rt_06082007.txt.ncat_out.txt	Salida de NCAT prima. Se trata de una "," archivo delimitado mostrando pasa / no pasa los datos de cada Estado
syd_1760rt_06082007.txt.html	Un informe basado en HTML que muestra los detalles full de resultados, con enlaces en rules.html
syd_1760rt_06082007.txt.ncat_fix.txt	Un archivo que contiene comandos para solucionar los problemas encontrados.
syd_1760rt_06082007.txt.ncat_report.txt	Un informe basado en texto mostrando el resumen de los resultados, con enlaces en rules.html.
Cisco IOS benchmark.html	Lista de las normas que se utilizaron para realizar la auditoría.
rules.html	Una versión HTML de los datos de referencia.
all.ncat_report.txt	Un informe basado en texto mostrando el resumen de los resultados, con enlaces en rules.html, de todos los routers incluidos en la auditoría. En nuestra muestra, ya que sólo hay un router, este fichero es el mismo que syd_1760rt_06082007.txt.ncat_report.txt.

all.ncat_fix.txt	Un archivo que contiene comandos para solucionar los problemas que se encuentran en todos los routers incluidos en la auditoría. En nuestra muestra, ya que sólo hay un router, este archivo es el mismo que syd_1760rt_06082007.txt.ncat_fix.txt.
all.html	Un informe resumen de HTML lista de pasa / no pasa de estado de todas las normas marcadas en todos los dispositivos.
index.html	Un índice de los informes HTML. Este es probablemente el archivo que la mayoría de los usuarios tendrá que examinar (con la ayuda de un navegador) después de ejecutar el RAT.

- **Anexo 3. Acta de Inicio de Auditoria**

Nombre:	Dirección General de Calidad y Educación en Salud		
Ubicación:	Homero No.213, Col. Chapultepec Morales Delegación Miguel Hidalgo, México D.F.	**Asunto:**	Acta de inicio de auditoría
Servidor Público:	Ing. Joaquín Zarco Rabágo	**Fecha:**	01 de Marzo del 2012.

ACTA DE INICIO DE AUDITORÍA, QUE SE PRACTICA A LA DIRECCIÓN GENERAL DE CALIDAD Y EDUCACIÓN EN SALUD, SSA.----------

---

---------En la Ciudad de México, Distrito Federal, siendo las diez horas del día primero de Marzo de dos mil doce**,** el ciudadano Ing. Joaquín Zarco Rabágo, Director de Automatización de Procesos y Soporte Técnico, y los C. Cuevas Olivares Jacobo, Enríquez Prado Jorge Alberto, Jiménez Velázquez Norma Leticia, Reyes Dionicio Ivonne, Rodríguez Olivo Ana Bertha, alumnos del seminario de titulación de ESIME Culhuacan, I.P.N., hacen constar que se constituyeron legalmente en las oficinas que ocupa la Dirección General de Calidad y Educación en Salud, ubicadas en la calle Homero número Doscientos trece, piso diez, Colonia Chapultepec Morales, Delegación Miguel Hidalgo, Distrito Federal, México, a efecto de iniciar la auditoría, denominada "Auditoria de ROUTERS", por el periodo de Marzo a Abril del dos mil doce, con la presencia del C. Ing. Víctor Hugo Higuera Muñoz, Subdirector de Sistemas de Información y Soporte Técnico, a fin de proceder a levantar la presente acta de inicio de auditoría, con el objeto de consignar los siguientes .----------

---

----------**HECHOS**----------En la hora y fecha mencionadas, los responsables de llevar a cabo esta diligencia, se presentaron en la oficina citada y ante la presencia del ciudadano Ing. Víctor Hugo Higuera Muñoz, Subdirector de Sistemas de Información y Soporte Técnico, procedieron a identificarse y hacer constar el inicio de auditoría, se entregó en las oficinas de la Dirección de Automatización de Procesos y Soporte Técnico, el día seis de noviembre de dos mil doce, acto con el que se dio formalmente por notificada la orden de inicio de auditoría, para los efectos de desahogo de los trabajos en él indicados; durante esta misma visita se hace petición de solicitud de información, de fecha seis de noviembre de dos mil doce, para su atención y efectos procedentes. Acto seguido, se solicitó a la servidor público que recibe la orden de auditoría se identificara, exhibiendo como identificación oficial credencial para votar expedida por el Instituto Federal Electoral, documento que se tiene a la vista y en el que aparece una fotografía que concuerda con sus rasgos físicos y la firma que utiliza en todos sus actos, tanto públicos como privados, a quien en este acto se le devuelve por así solicitarlo. ----------

---

----------Acto seguido, el ciudadano Ing.

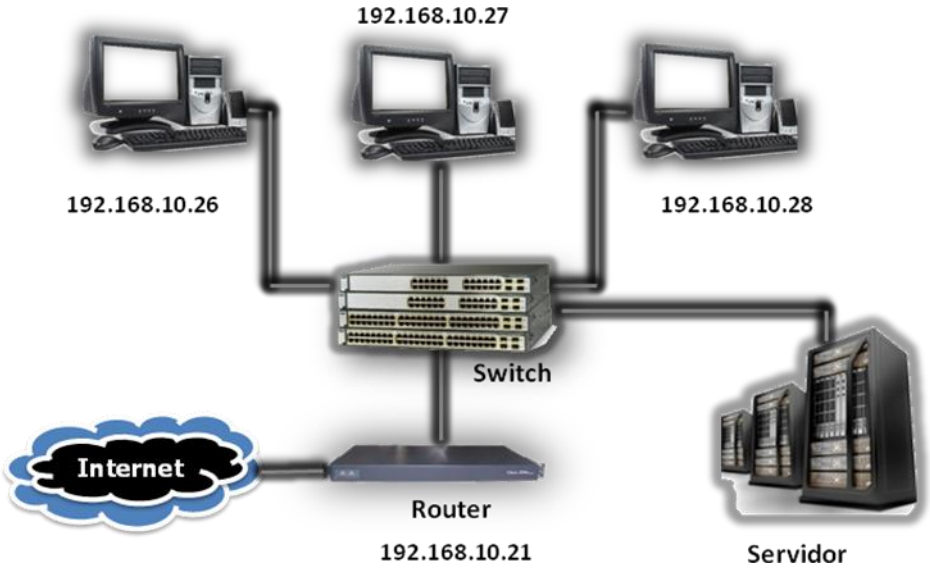
Joaquín Zarco Rabágo, Director de Automatización de Procesos y Soporte Técnico, expone el alcance de los trabajos a desarrollar, los cuales se ejecutarán en amparo y en cumplimiento de lo acordado para llevar a cabo la auditoría y solicita al C. Ing. Víctor Hugo Higuera Muñoz, Subdirector de Sistemas de Información y Soporte Técnico, designe a un Encargado de atender la revisión y a dos testigos de asistencia. ----------
---
---------- El Ing. Víctor Hugo Higuera Muñoz, Subdirector de Sistemas de Información y Soporte Técnico, procede a designar al ciudadano Ingeniero Fernando Martínez Resendiz, como Encargado para atender la auditoría, quien se identifica con credencial para votar con fotografía expedida por el Instituto Federal Electoral, quien desempeña el puesto de Jefe del Depto. de Sistemas de Información de la Director de Automatización de Procesos y Soporte Técnico, hecho con el que se da por formalmente notificado y se pone a las órdenes del personal actuante para atender los requerimientos que le formulen en el cumplimiento de su cometido; asimismo se designa como testigos de asistencia a los ciudadanos _____, con domicilio en calle _____, colonia _____, código postal _____, en la ciudad de _____, México, y _____, con domicilio en calle _____, colonia _____, código postal _____, en la ciudad de _____, México, ambos de nacionalidad mexicana, quienes en este acto aceptan la designación de que son objeto y señalan estar adscritos a la Dirección General de Administración de la Delegación Coyoacán.----------
---
---------- No habiendo más hechos que hacer constar, se da por concluida la práctica de esta diligencia, siendo las diecinueve treinta horas de la fecha de su inicio. Así mismo, previa lectura de lo plasmado la firman al margen y al calce, todos y cada uno de los que en ella intervienen, asentándose que este documento consta de dos fojas y que fue elaborado en tres tantos originales, de las que se entrega una legible al servidor público con el que se atendió la diligencia----------
---

Dirección de Automatización **Auditores**

Ing. Joaquín Zarco Rabágo

Cuevas Olivares Jacobo.
Enríquez Prado Jorge Alberto.
Jiménez Velázquez Norma Leticia.
Reyes Dionicio Ivonne.
Rodríguez Olivo Ana Bertha.

- **Anexo 4. Arquitectura Propuesta**



- **Anexo 5. Configuración inicial del router**

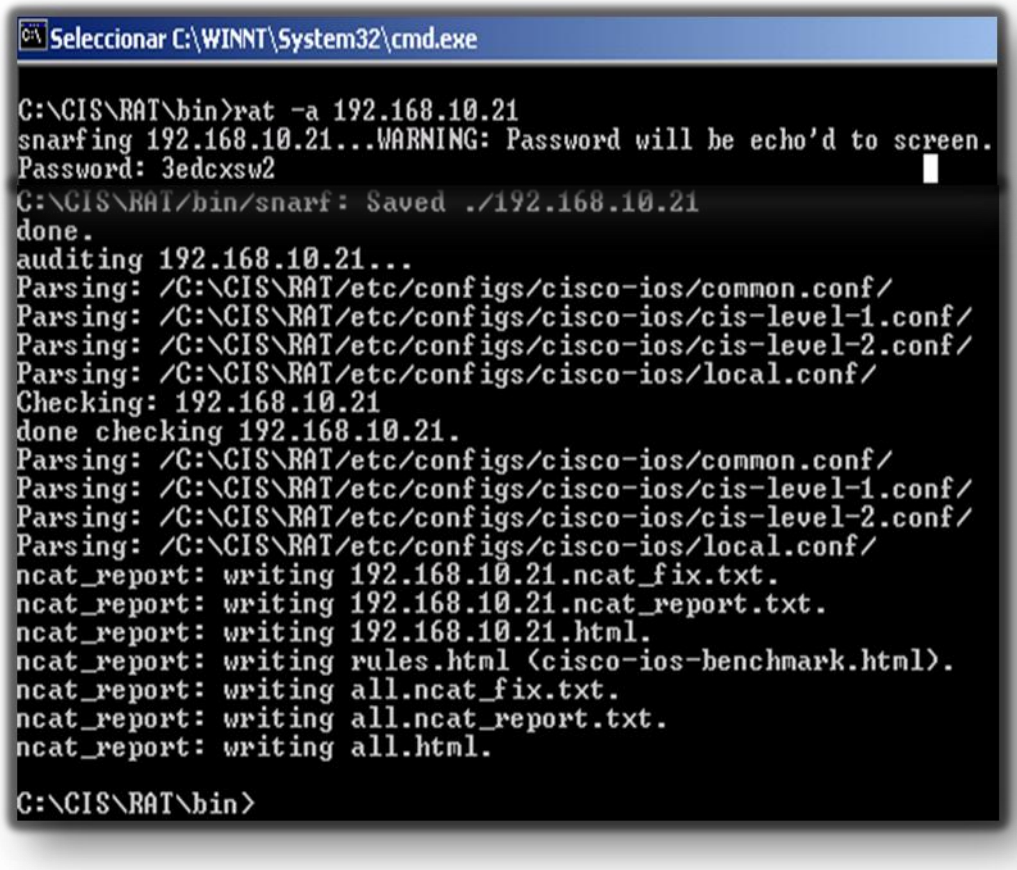
```
Router# setup

--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes]:

First, would you like to see the current interface summary?
[yes]:

Interface IP-Address OK? Method Status
Protocol
Ethernet0
     unassigned
     YES  not set
     administratively down
down
```

```
Ethernet1
     unassigned
     YES  not set
     administratively down
down
Serial0
     unassigned
     YES  not set
     administratively down
down
Serial1
     unassigned
     YES  not set
     administratively down
down

Configuring global parameters:
  Enter host name [Router]:

The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.

  Enter enable secret [<Use current secret>]: 1qazxsw2

The enable password is used when there is no enable secret
and when using older software and some boot images.

  Enter enable password: 2wsxzaq1
  Enter virtual terminal password: 3edcxsw2
  Configure SNMP Network Management? [no]:
  Configure IP? [yes]:

    Configure IGRP routing? [yes]:
      Your IGRP autonomous system number [1]:

Configuring interface parameters:

Configuring interface Ethernet0:
  Is this interface in use? [no]: yes
  Configure IP on this interface? [no]: yes
IP address for this interface: 192.168.10.21
```

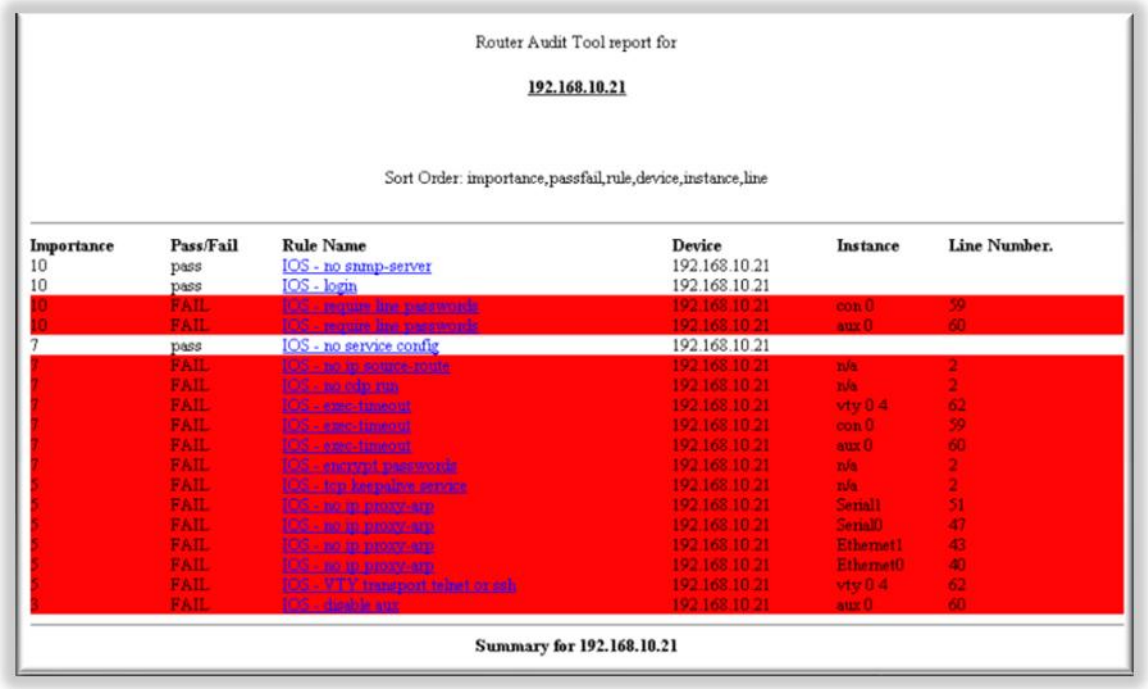
```
    Number of bits in subnet field [0]:
    Class C network is 192.168.10.0, 0 subnet bits; mask is
255.255.255.0

Configuring interface Ethernet1:
  Is this interface in use? [no]:

Configuring interface Serial0:
  Is this interface in use? [no]:

Configuring interface Serial1:
  Is this interface in use? [no]:

The following configuration command script was created:

hostname
enable secret 5 $1$xpDi$VNsqKR9m8rHE/sEJdbDs2.
enable password 2wsxzaq1
linevty 0 4
password 3edcxsw2
nosnmp-server
!
ip routing
!
interface Ethernet0
no shutdown
ip address 192.168.10.21 255.255.255.0
!
interface Ethernet1
shutdown
noip address
!
interface Serial0
shutdown
noip address
ip routing
!
interface Serial1
shutdown
noip address
!
```

```
routerigrp 1
network 192.168.10.0
!
end
Use this configuration? [yes/no]: yes
Building configuration...

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed
state to up

%LINK-3-UPDOWN: Interface Ethernet0, changed state to up[OK]
Use the enabled mode 'configure' command to modify this
configuration.
#
```

- **Anexo 6.Ejecución RAT**



➢ Anexo 7. Resultado Inicial RAT



Router Audit Tool report for

192.168.10.21

Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	pass	IOS - no snmp-server	192.168.10.21		
10	pass	IOS - login	192.168.10.21		
10	FAIL	IOS - require line passwords	192.168.10.21	con 0	59
10	FAIL	IOS - require line passwords	192.168.10.21	aux 0	60
7	pass	IOS - no service config	192.168.10.21		
7	FAIL	IOS - no ip source-route	192.168.10.21	n/a	2
7	FAIL	IOS - no cdp run	192.168.10.21	n/a	2
7	FAIL	IOS - exec-timeout	192.168.10.21	vty 0 4	62
7	FAIL	IOS - exec-timeout	192.168.10.21	con 0	59
7	FAIL	IOS - exec-timeout	192.168.10.21	aux 0	60
7	FAIL	IOS - encrypt passwords	192.168.10.21	n/a	2
5	FAIL	IOS - tcp keepalive service	192.168.10.21	n/a	2
5	FAIL	IOS - no ip proxy-arp	192.168.10.21	Serial1	51
5	FAIL	IOS - no ip proxy-arp	192.168.10.21	Serial0	47
5	FAIL	IOS - no ip proxy-arp	192.168.10.21	Ethernet1	43
5	FAIL	IOS - no ip proxy-arp	192.168.10.21	Ethernet0	40
5	FAIL	IOS - VTY transport telnet or ssh	192.168.10.21	vty 0 4	62
5	FAIL	IOS - disable aux	192.168.10.21	aux 0	60

Summary for 192.168.10.21

➢ Anexo 8. Configuracion Final del router

```
Using 1265 out of 32762 bytes
!
! Last configuration change at 15:19:32 UTC Sat
! NVRAM config last updated at 15:19:40 UTC Sat
!
version 10.3
no service finger
servicetcp-keepalives-in
service timestamps log datetimemsec show-timezone
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname
!
aaa new-model
aaa authentication login default local
aaa authentication enable default enable
```

```
enable secret 5 $1$O2UC$sb3HDxVKeKPMdD3WX1D.N1
enable password 7 08735B5D1103040643
!
usernamecamilo password 7 10161C11070115125B
noip source-route
!
interface Ethernet0
ip address 192.168.10.21 255.255.255.0
noip proxy-arp
!
interface Ethernet1
noip address
noip proxy-arp
shutdown
!
interface Serial0
noip address
noip proxy-arp
shutdowd
!
interface Serial1
noip address
noip proxy-arp
shutdown
!
routerigrp 1 [10]
network 192.168.10.0
!
logging buffered 16000
logging facility auth[11]
logging 192.168.10.26
logging 192.168.10.28
nocdp run
!
line con 0
exec-timeout 5 0
password 7 101E06120819180255
line aux 0
no exec
exec-timeout 5 0
password 7 035D5201080D295916
```

[10] Número de segmentos autónomos existentes, en este caso 1, segmento 192.168.10.0

[11] auth es el nombre que se utilizara para la configuración de logs en el servidor de syslog.

```
transport input none
linevty 0 4
exec-timeout 5 0
password 7 135612160814173D79
logging synchronous level 7 [12]
transport input none
!
end
```

➢ Anexo 9. Cierre de Auditoria

México, D. F., a 20 de Abril de 2012.

CIERRE DE AUDITORÍA

Descripción:	"Auditoria de Routers"
Unidad Administrativa, Dependencia, Órgano Político Administrativo, Órgano Desconcentrado o Entidad:	Dirección General de Calidad y Educación en Salud
Unidad:	610
Área(s) especifica(s):	Dirección Automatización de Procesos y Soporte Técnico
Número de observaciones:	09

OBJETIVO:
Auditar los Routers de la Dirección General de Calidad y Educación en Salud, en su configuración actual.

ALCANCE:
Se pretende realizar una auditoría para descubrir las vulnerabilidades y configuraciones de riesgo en la seguridad de los routers en la Dirección General de Calidad y Educación en Salud.
Período: Marzo de 2012 a Abril de 2012.
Ejercicio: 2012.

RESULTADOS:
De las entrevistas, investigación, inspección y análisis efectuado a la configuración del equipo del router, en el periodo de Marzo – Abril de 2012, se detectó lo siguiente:

1.- Configuración del núcleo estático del router:
Algunos aspectos importantes de la configuración almacenada son las direcciones de interfaz, los nombres de usuario y contraseñas, así como los controles de acceso para el acceso directo a la interfaz de comandos del router. La política de seguridad por lo general incluye normas estrictas sobre el acceso a este nivel, tanto en términos de funciones administrativas y los mecanismos de la red.

Sobre este particular, la Subdirección de Sistemas de Información y Soporte Técnico, no logra tener la disponibilidad

[12] Nivel de sincronización en la introducción de comandos EXEC y los mensajes mostrados por consola.

continua de los servicios de red y mensajería instantánea, ya que no se cuenta con un programa o procedimiento para la revisión de la configuración de los routers.

En este rubro, la Subdirección de Sistemas de Información y Soporte Técnico, no ha elaborado una metodología ni la documentación técnica y de usuario del router. Falta la configuración inicial del router ya que permite la aceptación de cualquier protocolo para la comunicación remota.

2.-Configuración dinámica y el estado del router

Si un atacante puede comprometer la configuración dinámica de un router, se puede poner en peligro la capa más externa también. La política de seguridad de un router debe incluir normas sobre el acceso a esta capa, aunque a veces se pasa por alto.

En este aspecto, la Subdirección de Sistemas de Información y Soporte Técnico, no cuentan los enlaces de acceso con un control de tiempo para las sesiones de usuario. Evitar que las contraseñas del usuario que viajan al servidor puedan ser interceptadas y conocidas; encriptar la transferencia de datos en los enlaces. El router tiene la configuración de fábrica. No hay una administración de cuentas de usuarios,

3.- Tráfico de red a través del router

Esta representa el tráfico intra-red y entre redes que el router gestiona. La política de seguridad de la red general puede incluir reglas sobre esto, la identificación de protocolos permitidos y servicios, mecanismos de acceso y las funciones administrativas. Los requisitos de alto nivel de la política de seguridad de la red deben reflejarse en la configuración del router, y probablemente en la política de seguridad del router.

En este apartado, la Subdirección de Sistemas de Información y Soporte Técnico, no existe un programa de mantenimiento preventivo y correctivo o control que administre y asegure los requerimientos de seguridad y funcionalidad que debería de brindar adecuadamente el router, no se lleva un registro donde se indique el número de fallas del router.

LIMITANTES:

Existió retraso en la entrega de la información solicitada.

CONCLUSIÓN:

La Subdirección de Sistemas de Información y Soporte Técnico, representa una función estratégica para las operaciones de la Dirección General de Calidad y Educación en Salud.

La ejecución de la auditoría evidenció que se debe fortalecer la seguridad física y lógica del router así mismo sus servicios asociados, por presentar vulnerabilidades que ponen en riesgo la continuidad de las operaciones de la Dirección al afectarse disponibilidad de la información que maneja; a fin de incrementar la productividad y capacidad de respuesta del área ante situaciones de trabajo o contingencias.

Resulta relevante señalar que se debe observar la normatividad en materia de tecnologías de información, a efecto de implementar las acciones inmediatas para su aplicación y, complementariamente, marcos de referencia internacionales NIST cuyos dominios y procesos permitirán a la Subdirección de Sistemas de Información y Soporte Técnico mejorar su operación cotidiana en los rubros de planeación, organización, adquisición, implementación, entrega, soporte y monitoreo.

ELABORO

Cuevas Olivares Jacobo.
Enríquez Prado Jorge Alberto.
Jiménez Velázquez Norma Leticia.
Reyes Dionicio Ivonne.
Rodríguez Olivo Ana Bertha.

➢ Anexo 10. Comandos básicos de interacción con Cisco IOS

- **Show interfaces:** muestra información sobre las interfaces del enrutador.
- **show interface [interfaz]:** muestra información de una interfaz específica.
- **show clock:** muestra los parámetros de la fecha y hora para el enrutador.
- **show versión:** muestra información de la configuración de hardware.
- **show protocols:** lista los protocolos de red configurados actuales.
- **show processes:** muestra información sobre la utilización de la CPU.
- **show cdpneighbor:** muestra los vecinos de interconexión.
- **show running-config:** muestra la configuración actual que se ejecuta.
- **show startup-config:** muestra la configuración de arranque del enrutador.
- **show logging:** muestra los logs generados y almacenados en memoria.
- **show flash:**muestra la cantidad de memoria flash disponible y no disponible.
- **clock set [hora] [fecha]:** modifica la fecha actual del enrutador.
- **config terminal:** establece al enrutador en modo de configuración.
- **line console 0:** establece la conexión por consola en modo de configuración.
- **line vty 0 4:** establece la conexión de sesiones telnet en modo de configuración.
- **copyrunning-configstartup-config:** guarda cambios hechos a la configuración actual.
- **setup:** inicializa asistente de configuración.
- **?:** muestra las posibles opciones de comandos actuales con su explicación.
- ^**z:**salir de modo de configuración.
- **enable:** instrucción para entrar en modo privilegiado.
- **disable:** sale del modo privilegiado.
- **show ip interface brief:** muestra las interfaces IP y su estado.
- **loggingsynchronous:** establece sincronización entre los mensajes mostrados por consola y las entradas del usuario.

ÍNDICE FIGURAS Y TABLAS

GLOSARIO

AAA Autenticación, autorización y contabilidad - El usuario avanzado de control de acceso y de auditoría en las instalaciones Cisco IOS 11 y 12.

ACL Lista de Control de Acceso.

Access List Un conjunto de reglas que identifican, permitir o restringen la red tráfico, por lo general basado en direcciones y otra información de las cabeceras de los paquetes. Cisco IOS depende en gran medida las listas de acceso para filtrar el tráfico, el acceso a los servicios del router, Configuración de IPSec, y mucho más.

AH Authentication Header - una parte de IPSec, el formato del paquete y el protocolo IP para los servicios de garantía de la integridad.

ARP Address Resolution Protocol - capa de enlace de protocolo utilizado para la asignación de direcciones IP a direcciones MAC en LAN ambientes. ARP está estandarizado en el RFC 826.

ATM Asynchronous Transfer Mode - circuito virtual orientado enlace de protocolo de capa, que se utiliza para conexiones troncales de red, redes de área local e instalaciones de telecomunicaciones.

BGP Border Gateway Protocol – es un avanzado protocolo de enrutamiento sobre todo con los routers de red troncal. BGP es estandarizada en RFC 1267.

CBAC El contenido basado en el Control de acceso - sistema de inspección de paquetes utilizada para la funcionalidad de la aplicación de firewall en los routers Cisco.

CDP Cisco Discovery Protocol – es un protocolo de capa de enlace de propiedad que los routers de Cisco utiliza para identificarse unos a otros en una red. No es de uso común hoy en día.

CEF Cisco Express Forwarding - es un paquete de transferencia de propiedad tecnología utilizada en el interior la mayoría de los modelos de router de Cisco.

DHCP Dynamic Host Configuration Protocol - basado en UDP protocolo para la asignación de atributos de la red de acogida, al igual que IP direcciones y puertas de enlace, sobre la marcha. DHCP está estandarizado en el RFC 2131.

DNS Domain Name System - esquema de nombres jerárquico utilizado para nombres de host y de red en la mayoría de las redes IP, incluyendo Internet. DNS es también el red que impiden que un componente de red de la prestación de sus funciones operativas, o que choque.

DDoS Distributed Denial of Service - Esta abreviatura se utiliza para los ataques DoS que utilizan múltiples (por lo general cientos o más) coordinó las fuentes de la red de datos para atacar a una sola víctima.

EIGRP Extended Interior Gateway Routing Protocol – Cisco propiedad de protocolo de enrutamiento, no de uso general.

Enablemode Una expresión coloquial para una sesión de EXEC privilegiado en un Routers de Cisco, que se deriven del comando utilizado para solicitar el modo EXEC privilegiado: enable.

ESP Carga de seguridad encapsulada - una parte de IPSec, el formato de paquete y el protocolo para los servicios de confidencialidad de propiedad intelectual.

FTP File Transfer Protocol - ampliamente utilizado en TCP basado en la transferencia de archivos y el archivo de protocolo de gestión. Por lo general, el control de FTP mensajes se transmiten en el puerto TCP 21. FTP está estandarizado en RFC 959.

ICMP Internet Control MessageProtocol - un protocolo de apoyo utilizado junto con la IP para el control y el mensaje de estado. ICMP es una red de protocolo de la capa que proporciona mensajes de error y capacidades de gestión en redes IP. ICMP es estandarizada en el RFC 792.

IETF Internet Engineering Task Force - técnica y órgano consultivo que define los estándares para Internet. Los estándares del IETF se publican en la RFC número, la lista de las normas actuales es el RFC 2400.

IKE Internet Key Exchange - la negociación de seguridad estándar y el protocolo de gestión de claves se utiliza con IPSec. IKE es estandarizada en el RFC 2409.

IOS Sistema operativo de internet - el nombre de Cisco para el sistema modular software del sistema que se ejecuta en sus routers y algunos otros dispositivos de red.

IP Protocolo de internet - El protocolo de capa de red en la que el Internet está construida. Hay dos versiones existentes de IP: IPv4 e IPv6. IPv4 está estandarizado en el RFC 791. IPv6 es estandarizada en el RFC 1883.

IPSec Seguridad del protocolo de Internet – es un conjunto de normas que definen la confidencialidad y la protección de la integridad para el tráfico IP. IPSec está estandarizado por un conjunto de RFCs, incluyendo el RFC 2401.

ISAKMP Internet Security Association Key Management Protocol – uno de los precursores de IKE.

Kerberos Kerberos fue desarrollado por el Instituto de Tecnología de Massachusetts como un sistema de autenticación de red, y proporciona autenticación fuerte para aplicaciones cliente/servidor mediante el uso de criptografía de clave secreta. Kerberos está estandarizado en el RFC 1510 (ver también RADIUS).

LAN Red de Área Local - término general para un segmento de una o red de conmutación física limitada y de organización medida.

LANE Emulación de LAN - un mecanismo estándar para el enrutamiento IP de paquetes a través de cajeros automáticos.

L2TP Layer 2 Tunnel Protocol - protocolo estándar para la transmisión de protocolos de bajo nivel a través de redes IP. L2TP es estandarizada en el RFC 2661.

MAC Address Media Access Control Address - La dirección de la capa de enlace de un interfaz de red, interfaces de Ethernet en particular. Una Dirección MAC de Ethernet es de 48 bits de longitud.

MD5 Message Digest algoritmo 5- un cifrado ampliamente utilizado algoritmo de control, estandarizado en el RFC 1321.

MIB Gestión de información - los datos jerárquicos la organización utilizada por SNMP.

MPOA Multi-Protocolo sobre ATM - Un proyecto de norma y mecanismo de protocolos de red de alojamiento (como IP) más ATM.

Multicast Una característica operativa de la propiedad intelectual, en el que los paquetes pueden ser transmitir a los destinatarios particulares basados en la dirección. En IPv4, las direcciones de 224.0.0.0 a 225.255.255.255 son por lo general direcciones de grupo multicast.

NNTP Network News Transfer Protocol - una aplicación basada en TCP protocolo que normalmente se ejecuta en el puerto 119.

NTP Network Time Protocol - el tiempo de red estándar protocolo de sincronización, puede usar UDP o TCP, pero por lo general utiliza UDP, el puerto 123. NTP está estandarizado en el RFC 1305.

OSPF Open Shortest Path First - un protocolo de enrutamiento IP que utiliza un estado de enlace métrica de distancia. OSPF está estandarizado en el RFC 2328.

PKI Infraestructura de Clave Pública - mecanismos y componentes para gestión de claves, certificados y la inscripción.

Proxy Cualquier aplicación que actúa como intermediario en la red y los intercambios entre las dos aplicaciones o servicios. Apoderando las aplicaciones se emplean a menudo para los intercambios moderados a través de un firewall.

Proxy-ARP Una instalación que ofrece algunos routers donde un router responde a las consultas de ARP de una red LAN conectada en nombre de los ejércitos de otras LAN. Rara vez se utiliza.

RADIUS El acceso telefónico de autenticación remota en Servicio de usuario (RADIUS) se especifica por el IETF RFC 2058. Usar RADIUS, el acceso servidores pueden comunicarse con un servidor central para autenticar, autorizar y las actividades de auditoría de los usuarios.

RFC Request For Comments - un documento que describe un estándar de Internet, norma propuesta, o la información relacionada que soporta un estándar.

RIP Router Information Protocol - una simple puerta de enlace inter- protocolo de enrutamiento que utiliza el número de saltos como medida de distancia. RIP es estandarizado por RFC 1088, 1388 y 1723.

RMON Monitoreo Remoto - instalaciones para el funcionamiento a distancia y de monitoreo de tráfico de dispositivos de red, basado en SNMP.

Routing La dirección y la gestión de los caminos a través de un segmento multi- red.

RSVP Protocolo de reserva de recursos - muy nuevo estándar protocolo para solicitar la calidad de servicio garantías en materia de IP las redes. RSVP es estándar en el RFC 2205.

SMTP Simple Mail Transfer Protocol - un protocolo basado en TCP para la envío y transmisión de mensajes de correo electrónico. SMTP es estandarizado en RFC 821.

SNMP Simple Network Management Protocol - Protocolo de datagramas que utiliza para supervisar y configurar dispositivos de red. SNMP utiliza los puertos UDP 161 y 162. SNMP es estándar en el RFC 1157 y RFC otros.

SSH Secure Shell - un protocolo de acceso remoto que proporciona confidencialidad, integridad y servicios de autenticación.

Syslog Una muy simple basado en UDP protocolo utilizado para el registro de Unix y los routers de Cisco. Syslog emplea generalmente el puerto UDP 514.

TACACS+ Terminal Access Controller Access Control System Plus – el protocolo de seguridad para proporcionar una autenticación centralizada, autorización y contabilidad de los usuarios que acceden a un router o acceder al servidor. TACACS + se define por Cisco.

TCP Protocolos de control de transmisión - orientados a la conexión de datos, protocolo que se utiliza con la propiedad intelectual. TCP soporta un gran número de aplicación a los servicios de capa de red, incluidos Telnet, web, FTP y correo electrónico.

Telnet Un sencillo protocolo basado en TCP de acceso remoto, por lo general en el puerto 23. También se utiliza para referirse a las aplicaciones cliente que apoyan el protocolo.

TFTP Trivial File Transfer Protocol - simple basado en UDP archivo el protocolo de transferencia, que se distingue por su falta de apoyo a autenticación. TFTP normalmente se utiliza el puerto UDP 69. TFTP es estandarizada en el RFC 1350.

UDP User Datagram Protocol - protocolo orientado a mensajes de datos se utiliza con la propiedad intelectual. UDP es la base para la red de núcleo de muchos servicios, incluyendo DNS, RIP, y NTP. UDP es estandarizada en el RFC 768.

VPDN Acceso telefónico a redes virtuales de lujo - una aplicación de tecnología VPN para asegurar conexiones remotas dialup, dando una conectividad de usuario remoto seguro a su "hogar base" red.

VPN Virtual Private Network - una red cerrada de comunicación de los ordenadores o redes de área local, con el público red como el transporte. Por lo general, el tráfico entre miembros de la VPN está protegido por IPSec durante el tránsito través de la red pública.

VTY Teletipo virtual - una interfaz de un host o router que proporciona los servicios interactivos de un terminal. Los routers Cisco utilizar las líneas de VTY para acoger sesiones de Telnet.

BIBLIOGRAFÍA

1. Auditoría interna y nuevas tecnologías, Sergio Martín Díaz, www.ey.com/es Pag.1
2. www.itil.co.uk
3. http://technet.microsoft.com/es-es/library/cc786900(v=ws.10).aspx
4. RFC significa solicitud de comentarios, http://www.ietf.org/rfc.html
5. http://www.cisecurity.org/bench_cisco.html
6. http://www.itil.org.uk
7. http://www.isaca.org
8. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
9. CISCO http://cisco.com
10. http://www.cisco.comCisco. Router Installation and Configuration Guide.Configuring the Router, Chapter 4.
11. Hatta, Mohammed Shafri. Institute. Securing IP Routing and Telnet Access On Cisco Routers. SANS Reading Room. September 20, 2001. URL: http://rr.sans.org/netdevices/telnet.php
12. Cisco. Improving Security on Cisco Routers.URL:http://www.cisco.com/warp/public/707/21.html
13. Brian Stewart. Router Audit Tool: Securing Cisco Routers Made Easy! March 29th 2002. Version 1.3
14. Jones, George. Router Audit Tool and Benchmark.SANS Webcast. February 20, 2002.
15. RAT. Router Audit Tool, Software. URL: http://www.cisecurity.org
16. WSyslogD, Software. Syslog for WinNT.URL:http://support.3com.com/software/utilities_for_windows_32_bit.html
17. National Security Agency.Router Security Configuration Guide.November 21, 2001. URL: http://nsa2.www.conxion.com/cisco/
18. Manual Cisco CCNA, capítulo 3. Las interfaces de un router. http://willie.sintax.info/cisco03.asp
19. http://www.intel.com/support/express/switches/410/
20. Nessus http://www.nessus.org
21. RFC 3164 http://www.rfc-editor.org
22. Manual Cisco CCNA http://willie.sintax.info/cisco.asp