



PROGRAMA DE AÑO SABÁTICO APUNTES:
ADMINISTRACIÓN DE REDES
CLAVE: ISIC-2010-224

DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN
INGENIERÍA EN SISTEMAS COMPUTACIONALES
AUTORIZACIÓN AÑO SABÁTICO No. AS-1-038/2023
ELABORADO POR: CARLOS ALBERTO CAMACHO ANDRADE

ZIHUATANEJO GUERRERO, MÉXICO
JUNIO DE 2023



ÍNDICE DE CONTENIDO	i
ÍNDICE DE FIGURAS	v
ÍNDICE DE TABLAS	v
INTRODUCCIÓN	vi
PROPUESTA DE HORAS TEÓRICO-PRÁCTICA POR TEMA/SUBTEMA	vii
1 FUNCIONES DE LA ADMINISTRACIÓN DE REDES	1
1.1 Fault Management (Administración de Fallas)	4
1.2 Configuration Management (Administración de Configuración)	5
1.3 Accounting Management (Administración de la Contabilidad)	6
1.4 Performance Management (Administración del Rendimiento)	6
1.5 Security Management (Administración de la Seguridad)	8
2 SERVICIOS DE RED	9
2.1 DHCP (Dynamic Host Configuration Protocol)	12
2.2 DNS (Domain Name System)	15
2.3 SSH (Secure Shell)	19
2.3.1 Cifrado Simétrico	20
2.3.2 Cifrado Asimétrico	20
2.3.3 Hashing	21
2.3.4 Funcionamiento del Protocolo SSH con las Técnicas de Cifrado	22
2.4 FTP (File Transfer Protocol) y TFTP (Trivial File Transfer Protocol)	24
2.4.1 FTP	24



2.4.2 TFTP	27
2.5 HTTP (Hypertext Transfer Protocol) y HTTPS (HyperText Transfer Protocol Secure).	28
2.5.1 HTTP	28
2.5.2 HTTPS	33
2.6 NFS (Network File System)	35
2.7 LDAP (Lightweight Directory Access Protocol)	38
2.8 SMTP, POP, IMAP Y SASL	42
2.8.1 SMTP (Simple Mail Transfer Protocol)	43
2.8.2 POP (Post Office Protocol)	45
2.8.3 IMAP (Internet Message Access Protocol)	48
2.8.4 SASL (Simple Authentication and Security Layer)	50
2.9 Proxy	51
3 ANÁLISIS Y MONITOREO	55
3.1 Protocolos de administración de red	56
3.1.1 Administrador de SNMP	57
3.1.2 Agente SNMP	57
3.1.3 Base de datos de información de gestión o base de información gestionada (MIB)	58
3.1.4 Dispositivo administrado	59
3.1.5 OID	59
3.1.6 Trampas SNMP	59
3.1.7 Métricas de SNMP	60



3.2 Bitácoras	61
3.3 Analizadores de protocolos (scanners y sniffers)	64
3.3.1 scanners	64
3.3.2 sniffers	67
3.4 Análisis de desempeño de la red: tráfico y servicios	69
3.5 QoS	71
4 SEGURIDAD BÁSICA	77
4.1 Elementos de seguridad	78
4.2 Tipos de riesgos y amenazas	80
4.3 Políticas de seguridad	83
4.4 Mecanismos de seguridad física y lógica: Control de acceso, respaldos, autenticación y elementos de protección perimetral	84
4.5 Resolución de problemas	87
5 REFERENCIAS BIBLIOGRÁFICAS	90
6 GLOSARIO	99



ÍNDICE DE FIGURAS

2.1	Funcionamiento del Protocolo DHCP	13
2.2	Funcionamiento del Protocolo DNS	16
2.3	Funcionamiento del Protocolo SSH	19
2.4	Funcionamiento del Protocolo FTP	24
2.5	Elementos de la comunicación web	29
2.6	Arquitectura de los sistemas basados en HTTP	29
2.7	Conexión NFS	35
2.8	Protocolo LDAP	39
2.9	Almacenamiento en LDAP	41
2.10	Protocolo SMTP	43
2.11	Protocolo de Oficina de Correo POP	45
2.12	Protocolo IMAP	48
2.13	Funcionamiento Servidor Proxy	52
3.1	Componentes del protocolo SNMP	56
3.2	Organización y jerarquía de datos en una MIB	58
3.3	Visor de eventos	62
3.4	Software de escaneo de red	65
3.5	Análisis del tráfico de red	69
3.6	Tecnología QoS	72
4.1	Delitos informáticos	79



4.2	Políticas de seguridad	83
-----	------------------------	----

ÍNDICE DE TABLAS

2.1	Estructura del protocolo DNS	17
-----	------------------------------	----



INTRODUCCIÓN.

Esta asignatura integra los conocimientos y habilidades para soportar y mantener los servicios y recursos de una red; implementa políticas de seguridad con el propósito de mejorar la fiabilidad y el desempeño de la misma.

La materia de Administración de redes se ubica en el 8vo. semestre de la carrera de Ingeniería en Sistemas Computacionales, plan ISIC-2010-224, clave SCA 1002.

Es parte esencial de la carrera ya que se proporcionan los conocimientos teórico y prácticos para conocer y realizar la administración de un sistema operativo de red (Windows Server) en función de la organización en la que se labora.

Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales las siguientes habilidades:

- Coordina y participa en equipos multidisciplinarios para la aplicación de soluciones innovadoras en diferentes contextos
- Desarrolla y administra software para apoyar la productividad y competitividad de las organizaciones cumpliendo con estándares de calidad
- Evalúa tecnologías de hardware para soportar aplicaciones de manera efectiva • Detecta áreas de oportunidad empleando una visión empresarial para crear proyectos aplicando las Tecnologías de la Información y Comunicación
- Diseña, configura y administra redes de computadoras para crear soluciones de conectividad en la organización, aplicando las normas y estándares vigentes
- Integra la capacidad de conocer, analizar y aplicar los diversos componentes tanto físicos como lógicos involucrados en la administración y configuración de una red local, mediante el análisis de los fundamentos, estándares y normas vigentes.



PROPUESTA DE HORAS TEÓRICO-PRÁCTICA POR TEMA/SUBTEMA.

Tema / Subtema	Propuesta de horas teórico-práctica
1. Funciones de la Administración de redes. 1.1 Configuración. 1.2 Fallas. 1.3 Contabilidad. 1.4 Desempeño. 1.5 Seguridad.	0-12 0-3 0-2 0-2 0-3 0-2
2. Servicios de Red. 2.1 DHCP. 2.2 DNS. 2.3 SSH. 2.4 FTP y TFTP. 2.5 HTTP y HTTPS. 2.6 NFS. 2.7 LDAP. 2.8 SMTP, POP, IMAP y SASL. 2.9 Proxy	9-18 1-2 1-2 1-2 1-2 1-2 1-2 1-2 1-2 1-2
3. Análisis y Monitoreo. 3.1 Protocolos de administración de red. 3.2 Bitácoras. 3.3 Analizadores de protocolos (scanners y sniffers). 3.4 Análisis de desempeño de la red: tráfico y servicios. 3.5 QoS.	5-11 1-2 1-2 1-3 1-3 1-1
4. Seguridad Básica. 4.1 Elementos de la Seguridad 4.2 Tipos de riesgos y amenazas. 4.3 Políticas de seguridad. 4.4 Mecanismos de seguridad física y lógica: Control de acceso, respaldos, autenticación y elementos de protección perimetral. 4.5 Resolución de problemas	2-8 0-1 0-1 0-2 1-2 1-2



Tema I

FUNCIONES DE LA ADMINISTRACIÓN DE REDES

Competencia Específica: Aplica las funciones de la administración de redes para la optimización del desempeño y el aseguramiento de las mismas.

INTRODUCCIÓN.

Este tema está orientado a la comprensión de las funciones de la administración de redes para aplicarlas en el aseguramiento y optimización del desempeño de las mismas.





1. Funciones de la Administración de Redes

Objetivo General: Conocer las funciones de la administración de redes, así como cada una de las áreas de la metodología FCAPS.

La tecnología está cambiando el mundo porque conecta dispositivos y mejora nuestra forma de vivir y trabajar. Las empresas cada día están optando por crear y desarrollar sus propias redes corporativas, adoptando tecnologías escalables y flexibles que se adapten a los cambios, pero para esto es necesario el personal especializado en la administración de redes. Cada año aumenta la tasa de incidencias en ciberataques dirigidos a empresas y esto obliga a que toda organización con un sitio web, dominio propio y correo electrónico necesitará un profesional en administración de redes. La administración de redes es uno de los ámbitos laborales con un mayor crecimiento en los últimos años.

Algunos conceptos de la Administración de redes son:

Es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada, con una planeación adecuada y propiamente documentada. (Trejo, s. f.).

Proceso que consiste en la planeación, organización y control de las actividades que envuelven el funcionamiento de los datos dentro de una organización. [R2] (Microsoft, s.f.)

Administración de redes según la ISO (Internacional Organization for Standardization, Organización Internacional para la Normalización). Los términos como administrador de red, especialista de red y analista de red se designan a aquellas posiciones laborales en las que los ingenieros se ven involucrados en redes de computadoras, o sea, las personas que se encargan de la administración de la red. Los administradores de red son básicamente el equivalente de red de los administradores de sistemas: mantienen el hardware y software de la red.

Esto incluye el despliegue, mantenimiento y monitoreo de la estructura de la red: switches, routers, cortafuegos, etc. Las actividades de administración de una red por lo general incluyen la asignación de direcciones, asignación de protocolos de ruteo y configuración de tablas de ruteo, así como, configuración de autenticación y autorización de los servicios. (Isotools, s.f.).



Existen varios modelos sobre arquitecturas de administración de redes. Tanto el modelo TNM (Telecommunications Management Network, Red de Telecomunicaciones de Gestión) de la UIT (Unión Internacional de Telecomunicaciones), como el modelo OSI-NM (Open Systems Interconnection-Network Management, Interconexión de Sistemas Abiertos-Administración de Redes) que son modelos funcionales que dividen la administración de una red en áreas funcionales (Configuración, Fallas, Desempeño, Contabilidad y Seguridad), definiendo de esta forma una estructura organizacional con funciones bien establecidas. De esto se deriva el nombre de modelos funcionales.

Metodología FCAPS.

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano introduce en 1997 el modelo FCAPS con base a la recomendación M.3400 (Funciones de gestión de la red de gestión de las telecomunicaciones (RGT)) que proporciona conjuntos de funciones de gestión de la RGT genéricos y especializados para el soporte de algunos de los servicios de gestión de la RGT más importantes.

FCAPS es el modelo y framework de red de gestión de telecomunicaciones de ISO para la gestión de redes. Es un acrónimo de Fault, Configuration, Accounting, Performance, Security (Falla, Configuración, Contabilidad, Desempeño, Seguridad) que son las categorías en las cuales el modelo ISO define las tareas de gestión de redes.

Pensar que una red se administra sola es algo común, a veces se cree que la única carga de trabajo de los administradores de redes se lleva a cabo en la fase de implantación, olvidando la operativa y mantenimiento diario. Un administrador de red no sólo tiene que resolver problemas, también tiene que monitorizar la red para adelantarse a los problemas, debe ser pro-activo, capaz de entender el comportamiento de la red evitando la no disponibilidad y maximizando los recursos disponibles adaptándose a los cambios de la empresa.



Así que es necesario conocer metodologías y procedimientos que ayuden a identificar y evaluar las herramientas, aplicaciones y recursos necesarios para mantener la red eficientemente. Existen varias metodologías como ITIL, FCAPS, TMN o PPDIOO, pero en este tema se explicará la metodología FCAPS que definió la ISO, la cual está compuesta por los siguientes cinco procesos:

1.1 Fault Management (Administración de Fallas)

Consiste en detectar, aislar y resolver los problemas de red, es el proceso donde los problemas son descubiertos y corregidos. Es obligatorio ser pro-activos para minimizar los tiempos medios de reparación (MTTR, Mean Time to Repair) y maximizar los tiempos medios entre fallo (MTBF, Mean Time Between Failures), para ello se utilizan mecanismos o plataformas de notificación como SNMP (Simple Network Management Protocol), protocolo simple de gestión entre redes basadas en TCP/IP, que permiten medir y controlar el estado actual de la infraestructura de red.

Una plataforma de administración de redes implementada administra una infraestructura que consta de elementos de red de varios proveedores. La plataforma recibe y procesa eventos de los elementos de red en la red. Los eventos de los servidores y de otros recursos importantes también pueden ser reenviados a una plataforma de administración.

Las plataformas de administración de red pueden verse como la consola principal para las operaciones de red en la detección de fallas en la infraestructura. La capacidad de detectar problemas rápidamente en cualquier red es fundamental. El personal de operaciones de redes puede basarse en un mapa gráfico de la red para visualizar los estados operativos de elementos críticos de la red, tales como routers y switches. Algunas de las plataformas más utilizadas son HP OpenView, Computer Associates Unicenter y SUN Solstice, pueden llevar a cabo una búsqueda de dispositivos de red.

El modelo FCAPS identifica las siguientes tareas de administración necesarias para un sistema de “Fault Management”:



- Detección de la falla
- Corrección de falla
- Aislamiento de la falla
- Recuperación de la red
- Manejo de alarmas
- Filtrado de alarmas
- Generación de alarmas
- Borrado de correlación
- Pruebas de diagnóstico
- Error de registros
- Manejo de errores
- Estadísticas de errores

1.2 Configuration Management (Administración de Configuración)

El objetivo de la administración de la configuración es supervisar la red y la información de configuración del sistema para que los efectos de varias versiones de elementos de hardware y software sobre la operación de la red puedan rastrearse y administrarse. Se basa en la obtención y almacenamiento de la configuración de los sistemas y de la red, es el concepto de asegurar una consistencia, repetición y auditable configuración en todos los equipos de la red, basados en una política de configuración. Todos los cambios de hardware y software son coordinados a través de este proceso, todas las operaciones diarias son monitoreadas y controladas.

El modelo FCAPS identifica las siguientes tareas de administración necesarias para un sistema de “Configuration Management”:

- Recursos de inicialización
- Provisionamiento de red
- Autodescubrimiento
- Copia de seguridad y restauración
- Apagado de recursos
- Gestión del cambio
- Pre-provisión
- Inventario/gestión de activos
- Copia de configuración
- Configuración remota
- Automatización de distribución de software
- Iniciación de Job, tracking y ejecución



1.3 Accounting Management (Administración de la Contabilidad)

Este proceso mide la distribución de los recursos, es decir, trata de conocer los recursos utilizados por usuarios y/o servicio para ayudar a reducir el costo operacional, de esta manera se sabe el beneficio y el costo en un determinado momento del día, ayudando a planificar los mantenimientos o cortes de la red.

Con base a la plataforma utilizada existen varios softwares para medir el uso de la red (NetFlow y Cisco IP Accounting). El análisis de los datos generados a través de estos métodos permite conocer los patrones actuales de uso.

Un sistema de facturación y contabilización basado en el uso es una parte esencial de cualquier acuerdo de nivel de servicio (SLA). Brinda tanto una manera práctica para definir las obligaciones según un SLA y las consecuencias evidentes del comportamiento fuera de los términos del SLA.

El modelo FCAPS identifica varias tareas de administración necesarias para un sistema de “Accounting Management”:

- Realizar un seguimiento de servicio o el uso de los recursos
- Costo de los servicios
- Contabilidad límite
- Uso de las cuotas
- Auditorías
- Reporte de Fraudes
- Combine los costos de múltiples recursos
- Apoyo a diferentes modos de gestión de rendimiento

1.4 Performance Management (Administración del Rendimiento)

La Gestión del Rendimiento consiste en monitorizar la red para conocer su estado de salud, esto nos ayudará a conocer la red para saber si es posible añadir nuevos servicios y adelantarnos a los futuros problemas de red, asegurando la disponibilidad del servicio y niveles óptimos de red.

Es imprescindible realizar un acuerdo de nivel de servicio (SLA) entre el proveedor del servicio y sus clientes sobre el nivel de rendimiento esperado de los servicios de red. El SLA



consta de métricas acordadas entre el proveedor y sus clientes. Los valores configurados para las mediciones deben ser realistas, significativos y cuantificables para ambas partes. Se pueden recopilar diferentes estadísticas de interfaz de los dispositivos de red para medir el nivel de rendimiento. Estas estadísticas pueden incluirse como métricas en el SLA. Las estadísticas, como las caídas de colas de entrada, las caídas de colas de salida y los paquetes ignorados, son útiles para diagnosticar problemas relacionados con el rendimiento.

Utilizar un analizador de tráfico (WireShark, MRTG, IP-TRAF, Snoort, NetFlow entre otros) implica monitorear la red 24/7 para descubrir quién ha estado utilizando el ancho de banda y para qué. Con una clara comprensión de la distribución de protocolos de la red, puede ver todas las aplicaciones que se utilizan en la red y sus conversaciones relacionadas.

Los protocolos de red son un conjunto estándar de reglas y formatos que garantizan que las transferencias de datos entre dos o más dispositivos a través de una red sean fáciles, fiables y seguras. Algunos protocolos de red incluyen:

- Protocolo de control de transmisión (TCP)
- Protocolo de Internet (IP)
- Protocolo de datagramas de usuario (UDP)
- Protocolo de oficina de correos (POP)
- Protocolo de transferencia de hipertexto (HTTP))
- Protocolo de transferencia de archivos (FTP)

El analizador de protocolos de red es una herramienta que captura y analiza el ancho de banda y los datos de tráfico a través de una red. Puede ayudar a:

- Ver las estadísticas de ancho de banda de cada protocolo de la red.
- Evitar que las aplicaciones inactivas utilicen un ancho de banda valioso.
- Controlar la distribución de protocolos de red y resolver los problemas de red rápidamente ofreciendo una visibilidad clara del problema existente.

Cuando se administra el rendimiento, se buscan los siguientes ocho atributos:

- Utilización y tasas de error
- El performance y recolección de datos
- Niveles consistentes de performance
- Realización de análisis de datos
- Reporte de problemas



- Capacidad de planificación
- Generación de informes de rendimiento
- Mantener y examinar los registros históricos

1.5 Security Management (Administración de la Seguridad)

El objetivo de la administración de la seguridad es controlar el acceso a los recursos de red de acuerdo con las pautas locales, de modo que la red no pueda ser sabotada. Un subsistema de administración de seguridad, por ejemplo, puede monitorear a los usuarios que ingresan a un recurso de la red, rechazando el acceso a aquellos que ingresan códigos de acceso inapropiados. Mediante la administración de la Seguridad se protege la confidencialidad de los usuarios y de la empresa, se protege la red de usuarios no autorizados y se aseguran los datos mediante la autenticación y el cifrado, además de utilizar técnicas de prevención y detección de intrusos.

Se consideran las siguientes actividades fundamentales para un eficaz sistema de gestión de seguridad:

- Acceso restrictivo a los recursos
- Registros de acceso
- Protección de datos
- Control de los derechos de acceso de usuario
- Seguridad de auditoria de registro
- Seguridad de alarma / reporte de eventos
- Violaciones de seguridad e intentos
- Seguridad de información relacionada con las distribuciones



Tema II

SERVICIOS DE RED

Competencia Específica: Instala, configura y administra diferentes servicios de red para satisfacer las necesidades específicas de las organizaciones.

INTRODUCCIÓN.

En este tema se explican los conceptos de los servicios de red comprendidos en Windows Server para poder realizar las prácticas propuestas sobre la instalación, configuración y administración diferentes servicios de red para satisfacer las necesidades de las organizaciones.





2. Servicios de Red.

Para la prestación de los servicios de red se requiere que existan sistemas en la red con capacidad para actuar como servidores. Los servidores y servicios de red se basan en los sistemas operativos de red.

Un sistema operativo de red es un conjunto de programas que permiten y controlan el uso de dispositivos de red por múltiples usuarios. Estos programas interceptan las peticiones de servicio de los usuarios y las dirigen a los equipos servidores adecuados. Por ello, el sistema operativo de red, le permite a ésta ofrecer capacidades de multiproceso y multiusuario.

Según la forma de interacción de los programas en la red, existen dos formas de arquitectura lógica:

1. Cliente-servidor.

Este es un modelo de proceso en el que las tareas se reparten entre programas que se ejecutan en el servidor y otros en la estación de trabajo del usuario. En una red cualquier equipo puede ser el servidor o el cliente. El cliente es la entidad que solicita la realización de una tarea, el servidor es quien la realiza en nombre del cliente. Este es el caso de aplicaciones de acceso a bases de datos, en las cuales las estaciones ejecutan las tareas del interfaz de usuario (pantallas de entrada de datos o consultas) y el servidor realiza las actualizaciones y recuperaciones de datos en la base.

Las ventajas de este modelo incluyen:

- Incremento en la productividad, centralización del control de los recursos, datos y accesos.
- Facilidad de administración, al concentrarse el trabajo en los servidores toda la información es almacenada en el lado del servidor, el cual suele tener mayor seguridad que los clientes.
- Facilidad de adaptación, existen muchas herramientas cliente-servidor probadas, seguras y con un entorno amigable para el usuario.
- Facilidad de mantenimiento y actualización del lado del servidor.



2. Redes de pares (peer-to-peer).

Este modelo permite la comunicación entre usuarios (estaciones) directamente sin tener que pasar por un equipo central para la transferencia. Las principales ventajas de este modelo son:

- Sencillez y facilidad de instalación, administración y uso.
- Flexibilidad. Cualquier estación puede ser un servidor y puede cambiar su rol, de proveedor a usuario según los servicios.
- Costos reducidos, ya que las redes punto a punto no requieren administradores de sistema para controlar y mantener los servidores

Existen varios servicios que se pueden proveer en una red de comunicaciones:

- Acceso.

Los servicios de acceso a la red comprenden, tanto la verificación de la identidad del usuario para determinar cuáles son los recursos a los cuales puede acceder en ella, como servicios que permiten la conexión de usuarios de la red desde lugares remotos.

Control de acceso.

Para el control de acceso, el usuario debe identificarse conectando con un servidor en el cual se autentifica por medio de un nombre de usuario y una clave de acceso. Si ambos son correctos, el usuario puede conectarse a la red.

Acceso remoto.

En este caso, la red de la organización está conectada con redes públicas que permiten la conexión de estaciones de trabajo situadas en lugares distantes. Dependiendo del método utilizado para establecer la conexión el usuario podrá acceder a unos u otros recursos.

- Archivos.

El servicio de archivos consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.



- **Impresión.**
Permite compartir impresoras de alta calidad, capacidad entre múltiples usuarios, reduciendo costos. Existen equipos servidores con capacidad de almacenamiento propio donde se almacenan los trabajos en espera de impresión, lo cual permite que los clientes se descarguen de esta información con más rapidez.
- **Correo.**
El correo electrónico es la aplicación de red más utilizada. Permite claras mejoras en la comunicación frente a otros sistemas, tiene un costo mucho menor para transmitir grandes cantidades de información.
- **Información.**
Los servidores de información pueden almacenar bases de datos para su consulta por los usuarios de la red u otro tipo de información, como por ejemplo documentos de hipertexto.

Para atender estos servicios de red, un sistema operativo de red ofrece una serie de protocolos que se describirán a continuación.

2.1 DHCP (Dynamic Host Configuration Protocol).

El protocolo de configuración dinámica de host, es un estándar TCP/IP que simplifica la administración de la configuración IP (Internet Protocol, Protocolo de Internet) haciéndola automática.

El host TCP/IP que solicita la información de configuración TCP/IP se denomina cliente DHCP y el host que provee dicha información se llama servidor DHCP. El protocolo DHCP se describe en la norma RFC2131 –Protocolo de configuración dinámica de host–. (ver Figura 2.1).

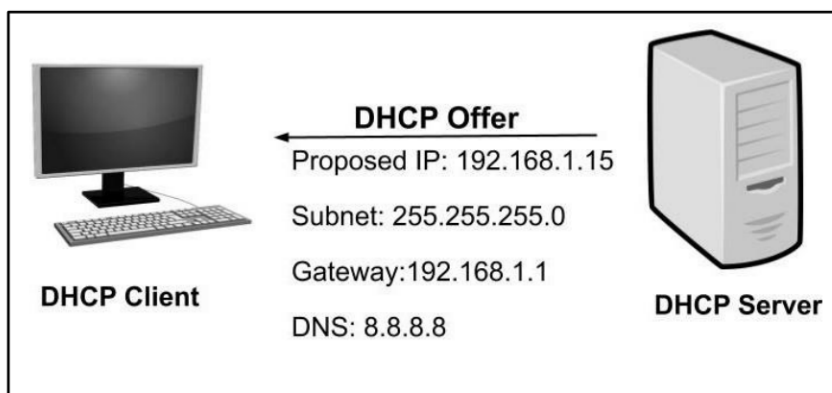


Figura 2.1 Funcionamiento del Protocolo DHCP

El protocolo DHCP usa los siguientes métodos para asignar las direcciones IP:

- Asignación manual. El administrador de red configura manualmente la dirección IP del cliente DHCP en el servidor DHCP. El DHCP se usa para asignar al cliente DHCP el valor de esta dirección IP configurada manualmente.
- Asignación automática. No se requiere asignar manualmente direcciones IP. El servidor DHCP asigna al cliente DHCP, en su primer acceso a la red, una dirección IP permanente que no podrá reutilizar ningún otro cliente DHCP.
- Asignación dinámica. El DHCP asigna una dirección IP al cliente DHCP por un tiempo determinado. Después que expire este lapso, se revoca la dirección IP y el cliente DHCP tiene que devolverla. Si el cliente aún necesita una dirección IP para efectuar sus operaciones, deberá solicitarla nuevamente.

La asignación de direcciones con DHCP se basa en un modelo cliente-servidor: el terminal que quiere conectarse solicita la configuración IP a un servidor DHCP que, por su parte, recurre a una base de datos que contiene los parámetros de red asignables. Este servidor, puede asignar los siguientes parámetros al cliente con ayuda de la información de su base de datos:

- Dirección IP única
- Máscara de subred



- Puerta de enlace estándar.
- Dirección del servidor DNS.

Al configurar el servidor DHCP se tienen que comprender los siguientes conceptos:

- Subneteo. La función del Subneteo o Subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.
- Ámbito servidor DHCP. Agrupamiento administrativo de equipos o clientes de una subred que utilizan el servicio DHCP.
- Rango servidor DHCP. Grupo de direcciones IP en una subred que el servidor puede conceder a los clientes
- Concesión o alquiler de direcciones. Período de tiempo que los servidores DHCP especifican, durante el cual un equipo cliente puede utilizar una dirección IP.
- Reserva de direcciones IP. Direcciones IP que se asignan siempre a los mismos equipos. Es similar a configurar una dirección IP estática, pero de forma automática desde el servidor DHCP, la forma de hacerlo es asociar direcciones MAC (Media Access Control, Control de Acceso al Medio, el cual es un identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos) conectados a direcciones IP.
- Exclusiones. Conjunto de direcciones IP pertenecientes al rango que no se van a asignar.

Cuando se debe configurar el DHCP.

Dependiendo de qué situación, activar el servidor DHCP puede resultar provechoso. Lo más recomendable es utilizarlo cuando se cuenta con una cantidad alta de dispositivos conectados a la red. De esta forma, será posible:

- Evitar el desplazamiento del administrador de la red, por lo que es posible realizar el cambio de configuración del administrador de red directamente desde el servidor DHCP y no tener que realizarlo desde cada equipo.



- Permite que los nuevos clientes puedan solicitar al servidor una dirección IP para integrarse a la red de forma sencilla y rápida.
- Se basa en un modelo cliente/servidor.
- Evita los errores por IPs repetidas, ya que el propio servidor DHCP evita que existan estos conflictos.
- Centraliza las direcciones IP para mantener un control de las redes, su configuración y estatus.

Ventajas de DHCP.

- Sólo se debe configurar el servidor para que asigne un rango de direcciones IP a los clientes.
- Fácil configuración.
- Facilita el seguimiento y supervisión de las direcciones IP, ya que son controladas por el servidor.
- Permite asignar direcciones IP de forma automática en redes con múltiples usuarios.

Desventajas de DHCP.

- Se debe configurar los DNS de forma independiente para indicar las direcciones IP en caso de requerir.
- Cuando existe un fallo en el servidor DHCP, los dispositivos renovarán su dirección IP, interrumpiendo la conexión e impidiendo su funcionamiento.
- Como los servidores DHCP no tienen un mecanismo seguro para la autenticación del cliente, cualquier nuevo cliente puede unirse a la red.

2.2 DNS (Domain Name System).

Es un sistema de nombres de dominio de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los hosts participantes. Su función más importante es «traducir» nombres inteligibles para las personas en

identificadores binarios (direcciones IP) asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. (ver Figura 2.2).



Figura 2.2 Funcionamiento del Protocolo DNS

La Corporación de Internet para la Asignación de Nombres y Números mejor conocida como ICANN por sus siglas en inglés (Internet Corporation for Assigned Names and Numbers), es la asociación internacional sin ánimo de lucro fundada en septiembre de 1998, encargada de reunir a personas de todo el mundo con el objetivo de preservar la estabilidad operacional y la seguridad de Internet.

Si bien la ICANN no controla el contenido ni los accesos que existen en Internet, si es la responsable de asignar el espacio de las direcciones numéricas IP y coordinar el sistema de nombres de dominio (DNS).

De no existir los servidores DNS los usuarios tendrían que escribir la dirección IP del sitio web en lugar de escribir la URL (Uniform Resource Locator, Localizador de Recursos Uniforme) de este lo cual generaría confusiones y la navegación en internet se tornaría muy complicada para los usuarios.

El DNS se utiliza para distintos propósitos. Los más comunes son:

- **Resolución de nombres:** Dado el nombre completo de un *host* (por ejemplo *blog.smaldone.com.ar*), obtener su *dirección IP* (en este caso, *208.97.175.41*).



- **Resolución inversa de direcciones:** Es el mecanismo inverso al anterior. Consiste en, dada una *dirección IP*, obtener el nombre asociado a la misma.
- **Resolución de servidores de correo:** Dado un *nombre de dominio* (por ejemplo *gmail.com*) obtener el servidor a través del cual debe realizarse la entrega del correo electrónico (en este caso, *gmail-smtp-in.l.google.com*).

Con base a la Solicitud de Recomendación (RFC, Request for Comments) 1591 y 1035 de la ICANN sobre la Estructura y Delegación del Sistema de Nombres de Dominio, la tabla 2.1 muestra la estructura del DNS.

Tabla 2.1 Estructura del protocolo DNS

https://	www	.itcostagrande	.edu	.mx
protocolo	Dominios de Tercer Nivel.	SLD Second Level Domain Dominios de Segundo Nivel.	TLD Top-Level Domain Name “Nombres de dominio de nivel superior”.	ccTLD country code Dominio de Nivel Superior Geográfico.

Protocolo. Es el protocolo utilizado para enviar datos entre un navegador web y un sitio web, los más utilizados son http (Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto) ó https (Hypertext Transfer Protocol Secure, Protocolo seguro de transferencia de hipertexto) (versión segura de http), el cual es un protocolo encriptado para aumentar la seguridad de las transferencias de datos, permite establecer una conexión segura entre el servidor y el cliente, que no puede ser interceptada por personas no autorizadas.

Dominios de Tercer Nivel. www (World Wide Web, red mundial o red global) indica a los usuarios que se encuentran ante una aplicación web, en la actualidad no es necesario introducir este dominio de tercer nivel para poder visitar una página web.

Dominios de Segundo Nivel. Se define al nombre elegido libremente que precede al dominio de nivel superior.



Dominios de Nivel Superior. Representan el nivel más alto de la resolución de nombres en la jerarquía del Sistema de Nombres de Dominio, también conocido como extensión. Entre los más importantes están:

- .com Dominio para las webs comerciales.
- .org Dominio para organizaciones sin ánimo de lucro.
- .net Dominio para proveedores de servicio de Internet.
- .int Dominio muy limitada a las empresas, organizaciones y programas internacionales.
- .edu Dominio para universidades y escuelas de formación profesional.
- .gov Dominio para instituciones del gobierno estadounidense.
- .mil Dominio solo disponible para departamentos, servicios y agencias del ministerio de defensa de los estados unidos.

Dominio de Nivel Superior Geográfico. Forman una categoría especial de extensiones de dominio que cada país administra, algunos de ellos son:

- .mx México.
- .us Estados Unidos.
- .fr Francia.
- .it Italia.
- .ru Rusia.
- .uk Reino Unido.

2.3 SSH (Secure Shell).

Es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet mediante un mecanismo de autenticación y con la información cifrada, (ver Figura 2.3), está definido en la el RFC4253.

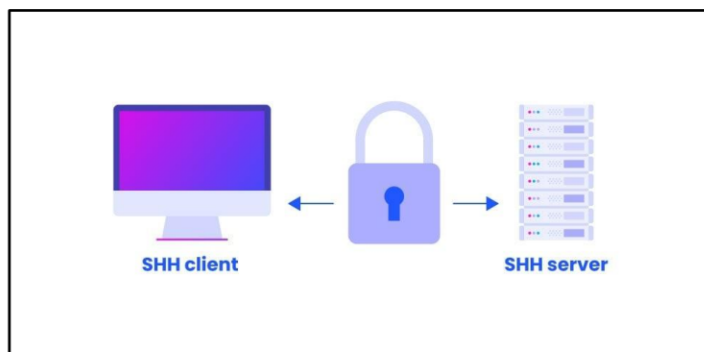


Figura 2.3 Funcionamiento del Protocolo SSH

El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.

La ventaja significativa ofrecida por el protocolo SSH sobre sus predecesores es el uso del cifrado para asegurar la transferencia segura de información entre el host y el cliente. Host se refiere al servidor remoto al que estás intentando acceder, mientras que el cliente es el equipo que estás utilizando para acceder al host. Hay tres tecnologías de cifrado diferentes utilizadas por SSH:

1. Cifrado simétrico.
2. Cifrado asimétrico.
3. Hashing.



2.3.1 Cifrado Simétrico.

El cifrado simétrico es una forma de cifrado en la que se utiliza una clave secreta tanto para el cifrado como para el descifrado de un mensaje, tanto por el cliente como por el servidor. Efectivamente, cualquiera que tenga la clave puede descifrar el mensaje que se transfiere.

El cifrado simétrico a menudo se llama clave compartida (shared key) o cifrado secreto compartido. Normalmente sólo hay una clave que se utiliza, o a veces un par de claves donde una clave se puede calcular fácilmente con la otra clave.

Las claves simétricas se utilizan para cifrar toda la comunicación durante una sesión SSH. Tanto el cliente como el servidor derivan la clave secreta utilizando un método acordado, y la clave resultante nunca se revela a terceros. El proceso de creación de una clave simétrica se lleva a cabo mediante un algoritmo de intercambio de claves. Esta clave simétrica es en específico para cada sesión SSH, y se genera antes de la autenticación del cliente. Una vez generada la clave, todos los paquetes que se transfieren entre las dos máquinas deben ser cifrados por la clave privada. Esto incluye la contraseña escrita en la consola por el usuario, por lo que las credenciales siempre están protegidas.

Existen varios códigos cifrados simétricos, incluyendo, pero no limitado a, AES (Advanced Encryption Standard), CAST128, Blowfish, entre otros. Antes de establecer una conexión segura, el cliente y un servidor deciden qué cifrado usar, publicando una lista de cifrados soportados por orden de preferencia.

2.3.2 Cifrado Asimétrico.

A diferencia del cifrado simétrico, el cifrado asimétrico utiliza dos claves separadas para el cifrado y el descifrado. Estas dos claves se conocen como la clave pública (public key) y la clave privada (private key). Juntas, estas claves forman el par de claves pública-privada (public-private key pair).



La clave pública, como sugiere el nombre, se distribuye abiertamente y se comparte con todas las partes. Si bien está estrechamente vinculado con la clave privada en términos de funcionalidad, la clave privada no se puede calcular matemáticamente desde la clave pública.

La relación entre las dos claves es altamente compleja: un mensaje cifrado por la clave pública de una máquina, sólo puede ser descifrado por la misma clave privada de la máquina. Esta relación unidireccional significa que la clave pública no puede descifrar sus propios mensajes ni descifrar nada cifrado por la clave privada.

La clave privada debe permanecer privada, es decir, para que la conexión sea segura, ningún tercero debe conocerla. La fuerza de toda la conexión reside en el hecho de que la clave privada nunca se revela, ya que es el único componente capaz de descifrar mensajes que fueron cifrados usando su propia clave pública. Por lo tanto, cualquier parte con la capacidad de descifrar mensajes firmados públicamente debe poseer la clave privada correspondiente.

A diferencia de la percepción general, el cifrado asimétrico no se utiliza para cifrar toda la sesión SSH. En lugar de eso, sólo se utiliza durante el algoritmo de intercambio de claves de cifrado simétrico. Antes de iniciar una conexión segura, ambas partes generan pares de claves públicas-privadas temporales y comparten sus respectivas claves privadas para producir la clave secreta compartida.

Una vez que se ha establecido una comunicación simétrica segura, el servidor utiliza la clave pública de los clientes para generar, desafiar y transmitirla al cliente para su autenticación. Si el cliente puede descifrar correctamente el mensaje, significa que contiene la clave privada necesaria para la conexión, es entonces que inicia la sesión SSH.

2.3.3 Hashing.

El hashing unidireccional es otra forma de criptografía. Las funciones de hash unidireccionales difieren de las dos formas anteriores de encriptación en el sentido de que nunca están destinadas a ser descifradas. Generan un valor único de una longitud fija para



cada entrada que no muestra una tendencia clara que pueda explotarse. Esto los hace prácticamente imposibles de revertir.

Es fácil generar un hash criptográfico de una entrada dada, pero imposible de generar la entrada del hash. Esto significa que, si un cliente tiene la entrada correcta, pueden generar el hash criptográfico y comparar su valor para verificar si poseen la entrada correcta.

SSH utiliza hashes para verificar la autenticidad de los mensajes. Esto se hace usando HMACs, o códigos de autenticación de mensajes basados en hash. Esto asegura que el comando recibido no se altere de ninguna manera.

Mientras se selecciona el algoritmo de cifrado simétrico, también se selecciona un algoritmo de autenticación de mensajes adecuado. Esto funciona de manera similar a cómo se selecciona el cifrado, como se explica en la sección de cifrado simétrico.

2.3.4 Funcionamiento del Protocolo SSH con las Técnicas de Cifrado.

La forma en que funciona SSH es mediante el uso de un modelo cliente-servidor para permitir la autenticación de dos sistemas remotos y el cifrado de los datos que pasa entre ellos. SSH opera en el puerto TCP 22 de forma predeterminada (aunque esto se puede cambiar si es necesario).

El host (servidor) escucha en el puerto 22 (o cualquier otro puerto SSH asignado) para las conexiones entrantes. Organiza la conexión segura mediante la autenticación del cliente y la apertura del entorno de shell correcto si la verificación tiene éxito.

El cliente debe iniciar la conexión SSH iniciando el protocolo TCP con el servidor, asegurando una conexión simétrica segura, verificando si la identidad mostrada por el servidor coincide con los registros anteriores (normalmente grabados en un archivo de almacén de claves) y presenta las credenciales de usuario necesarias para autenticar la conexión.



Hay dos etapas para establecer una conexión: primero ambos sistemas deben acordar estándares de cifrado para proteger futuras comunicaciones, y segundo, el usuario debe autenticarse. Si las credenciales coinciden, se concede acceso al usuario.

En la primera etapa, cuando un cliente intenta conectarse al servidor a través de TCP, el servidor presenta los protocolos de cifrado y las versiones respectivas que soporta. Si el cliente tiene un par similar de protocolo y versión, se alcanza un acuerdo y se inicia la conexión con el protocolo aceptado. El servidor también utiliza una clave pública asimétrica que el cliente puede utilizar para verificar la autenticidad del host.

Una vez que esto se establece, las dos partes usan lo que se conoce como Algoritmo de Intercambio de Claves Diffie-Hellman para crear una clave simétrica. Este algoritmo permite que tanto el cliente como el servidor lleguen a una clave de cifrado compartida que se utilizará en adelante para cifrar toda la sesión de comunicación. Ahora que se ha establecido la sesión cifrada segura simétricamente, el usuario debe ser autenticado.

En la etapa final, antes de que se conceda al usuario acceso al servidor se realiza la autenticación de sus credenciales. Para ello, la mayoría de los usuarios de SSH utilizan una contraseña. Se le solicita al usuario que introduzca su nombre de usuario, seguido de la contraseña. Estas credenciales pasan con seguridad a través del túnel cifrado simétricamente, así que no hay ninguna posibilidad de que sean capturadas por un tercero.

2.4 FTP (File Transfer Protocol) y TFTP (Trivial File Transfer Protocol).

El Protocolo de transferencia de archivos es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

2.4.1 FTP.

Las siglas FTP que se traducen como “Protocolo de Transferencia de Archivos”, es un servicio utilizado para el envío y obtención de archivos entre dos equipos remotos. Los casos más usuales son transferencias entre el equipo local de un cliente y el servidor del proveedor, aunque también se pueden establecer conexiones FTP entre dos servidores. (ver Figura 2.4).

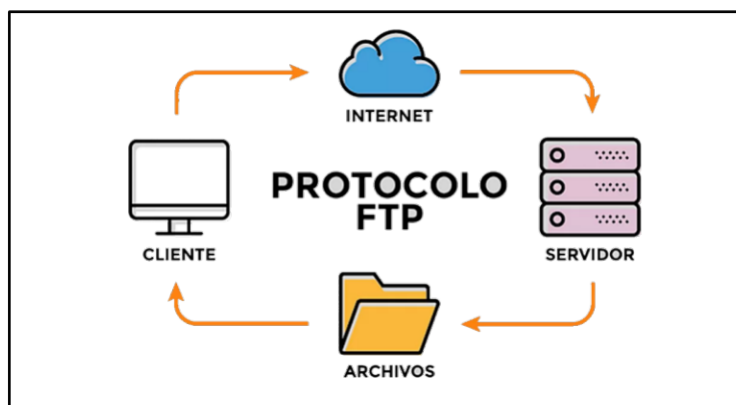


Figura 2.4 Funcionamiento del Protocolo FTP

Los puertos típicos utilizados para conectarse al FTP son el 20 y el 21 para la gran mayoría de los casos, aunque en algunos proveedores esto puede variar. Por lo general se usan dos tipos de transferencia: una es la ASCII y la otra es la de tipo Binario. La primera de estas solamente transfiere texto plano del tipo ASCII, como serían por ejemplo páginas HTML sin imágenes, mientras que la segunda clase se usa para transferir archivos como imágenes, audios, videos, etc.



En la conexión intervienen dos conceptos servidor y cliente FTP:

- El servidor FTP es un software que corre en los servidores conectados a Internet (o bien a una red local LAN), y tiene como función primordial permitir que diferentes clientes FTP puedan conectarse a él, para luego descargar o subir información (archivos).
- Un cliente FTP no es otra cosa que un software que se instala en la máquina del usuario y permite conectar mediante el protocolo FTP hacia el servidor FTP remoto que está en Internet.

Existen tres tipos de FTP bien diferenciados a la hora de establecer una conexión:

1. FTP Anónimo: Cualquiera puede descargar un archivo sin identificarse.
2. FTP Autenticado: Hay que conectarse al servidor utilizando un nombre y una contraseña. Es el más común hoy en día, ya que ofrece una seguridad básica para no permitir que nadie sin los privilegios necesarios pueda acceder a los archivos que están en el servidor FTP.
3. FTP Embebido: Es el que se realiza desde las Páginas Web, a través de navegadores. Es una opción dentro del FTP Anónimo.

Ventajas de un servidor FTP:

- Realiza una conexión rápida con el servidor.
- Es ideal para subir muchos archivos o pocos, según se necesite.
- Es multiplataforma, funciona en cualquier sistema operativo.
- Permite subir y bajar archivos bi-direccionalmente.
- Soporta conexiones encriptadas con certificados SSL.
- No necesitas saber comandos ni usar la terminal, tiene clientes gráficos.
- No se requiere de conocimientos técnicos para usarlo.

Desventajas de un servidor FTP:

- Si no hay un SSL de por medio, los datos de usuario, contraseña y la información que se sube o baja se envían sin encriptación.
- No permite la automatización de diferentes procesos como lo permiten otros protocolos más modernos, como por ejemplo conectar a través de un servidor SSH.



- Es un protocolo viejo, que, si bien ha recibido actualizaciones, no se ha adaptado al desarrollo web moderno.
- No permite paralelizar las descargas o subidas de archivos, estos deben hacerse uno a uno.
- No permite resumir las descargas o subida de archivos, pueden quedar corruptos los archivos si hay errores en la red.

Existen dos tipos de servidores FTP debido a su ubicación y la arquitectura de red que usan:

- FTP local, en una red de área local o LAN.
- FTP en Internet, en una red mundial o WAN.

Servidor FTP local.

Este tipo de servidores FTP se suelen usar en entornos empresariales, donde el servidor FTP escucha en una IP local y que sólo permite conexiones desde las computadoras conectadas a la misma red. Es ideal para compartir documentos de trabajo, archivos, planillas de Excel y demás en entornos de una oficina. Lo bueno de este tipo de servidores FTP locales es que no suelen ser atacados debido a que no salen nunca a Internet.

Servidor FTP en Internet.

Este servicio es cuando se tiene la necesidad de contratar un paquete de web hosting con un proveedor del servicio, con colaboradores que trabajan desde diferentes zonas geográficas, en donde se comparte con muchos otros clientes de diferentes lugares del mundo. En este caso el servidor se configura para escuchar en una IP pública, de esta forma todos usan esa IP al momento de conectar. Esta forma de usar el FTP requiere de SSL pues es bastante inseguro conectar sin encriptación.

Seguridad de FTP.

FTP se orientó a ofrecer la máxima velocidad en la conexión, pero debido a su antigüedad no fue diseñado con mecanismos de seguridad. Uno de los inconvenientes que tiene es que todo el intercambio de información se realiza en texto plano. Todo el proceso, desde el acceso



del usuario en el servidor y la transferencia de los archivos se realiza sin cifrar. Por lo tanto, un posible atacante podría capturar este tráfico, acceder al servidor o hacerse con los archivos transferidos.

Existen dos variantes de FTP que han sido desarrolladas para aplicar una capa segura sobre este protocolo, FTPS y SFTP.

FTPS.

Se trata de una conexión FTP empleando el protocolo SSL (Secure Socket Layers) o TLS (Transport Layer Security), estas conexiones utilizan un certificado de seguridad que cifra todo el proceso, desde la identificación, hasta el intercambio de ficheros.

SFTP.

Se trata de una conexión FTP utilizando el protocolo SSH (Secure Shell) para cifrar el proceso de conexión y el intercambio de información entre el cliente y el servidor.

2.4.2 TFTP.

Las siglas TFTP que se traducen como “Protocolo de Transferencia de Archivos Simple”, es un protocolo cliente-servidor muy simple que regula la transferencia de archivos.

Se trata de un protocolo de transferencia de archivos que funciona mediante paquetes de datos. Forma parte de la familia de protocolos TCP/IP y fue específicamente diseñado para que su implementación fuese lo más sencilla y ligera posible. Por esta razón, su funcionalidad consiste principalmente en la lectura o escritura de un archivo o un correo electrónico de un servidor.

La transferencia de archivos a través de TFTP se basa siempre en una solicitud de acceso del cliente, bien de lectura bien de escritura. Esta solicitud funciona al mismo tiempo como petición de conexión que se concede automáticamente en el momento en el que el servidor acepta el acceso. A continuación, el cliente o el servidor envía el archivo que corresponda en bloques de tamaño fijo. En las primeras versiones del protocolo, se utilizaba un valor fijo de 512 bytes, pero, a partir del RFC 2348, el servidor y el cliente tienen la posibilidad de negociar en cada caso el tamaño del bloque.



Una de las principales ventajas del protocolo TFTP es su simplicidad, pues está diseñado para permitir la escritura y la lectura de archivos sin tener que establecer una conexión entre el cliente y el servidor. Por ello, el protocolo TFTP no solo es fácil de implementar, sino que también es el precursor de la transferencia rápida de archivos.

Sin embargo, la falta de cifrado y de un mecanismo de control de autenticación y acceso hacen que el envío de archivos confidenciales a través del protocolo TFTP suponga riesgos altos. En su lugar, pueden utilizarse otras alternativas más seguras como FTP, un protocolo más complejo. Además, muchos servidores TFTP no permiten eliminar y renombrar archivos.

2.5 HTTP (Hypertext Transfer Protocol) y HTTPS (HyperText Transfer Protocol Secure).

Son los protocolos de transmisión de información de la internet.

2.5.1 HTTP.

Las siglas HTTP que se traducen como “Protocolo de Transferencia de Hiper Textos”, es el nombre de un protocolo el cual permite realizar una petición de datos y recursos, como pueden ser documentos HTML. Es la base de cualquier intercambio de datos en la Web, y un protocolo de estructura cliente-servidor en donde se establecen criterios de sintaxis y semántica informática (forma y significado) para el establecimiento de la comunicación entre los diferentes elementos que constituyen la arquitectura web: servidores, clientes, proxies, texto, imágenes, vídeos, scripts. (Figura 2.5).

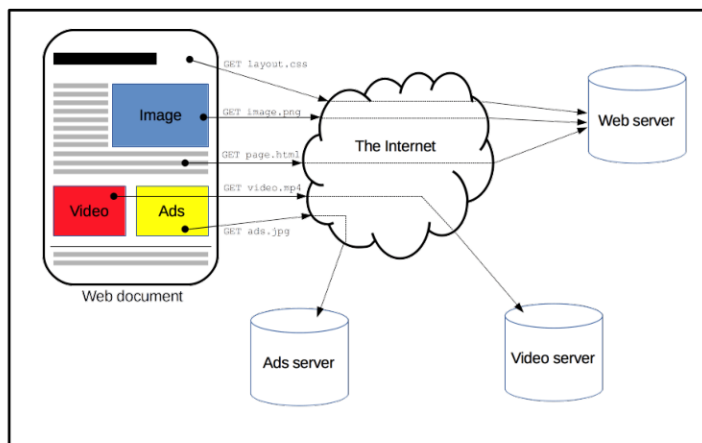


Figura 2.5 Elementos de la comunicación web

Se trata de un protocolo “sin estado”, es decir, que no lleva registro de visitas anteriores, sino que siempre empieza de nuevo. La información relativa a visitas previas se almacena en las llamadas “cookies”, almacenadas en el sistema cliente.

Arquitectura de los sistemas basados en HTTP.

HTTP es un protocolo basado en el principio de cliente-servidor: las peticiones son enviadas por una entidad: el agente del usuario (o un proxy a petición de uno). La mayoría de las veces el agente del usuario (cliente) es un navegador Web, pero podría ser cualquier otro programa, como por ejemplo un programa-robot, que explore la Web, para adquirir datos de su estructura y contenido para uso de un buscador de Internet.

Cada petición individual se envía a un servidor, el cual la gestiona y responde. Entre cada petición y respuesta, hay varios intermediarios, normalmente denominados proxies, los cuales realizan distintas funciones, como: gateways o caches. (Figura 2.6).

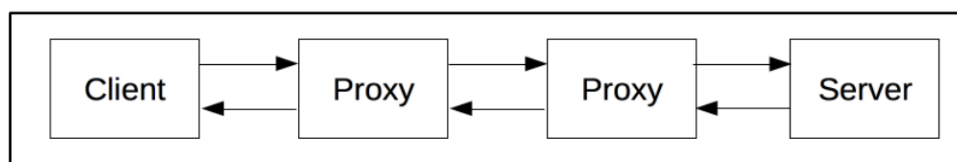


Figura 2.6 Arquitectura de los sistemas basados en HTTP



Cliente: el agente del usuario.

El agente del usuario, es cualquier herramienta que actúe en representación del usuario. Esta función es realizada en la mayor parte de los casos por un navegador Web. Hay excepciones, como el caso de programas específicamente usados por desarrolladores para desarrollar y depurar sus aplicaciones. El navegador es siempre el que inicia una comunicación (petición), y el servidor nunca la comienza (hay algunos mecanismos que permiten esto, pero no son muy habituales).

Para poder mostrar una página Web, el navegador envía una petición de documento HTML al servidor. Entonces procesa este documento, y envía más peticiones para solicitar scripts, hojas de estilo (CSS), y otros datos que necesite (normalmente vídeos y/o imágenes). El navegador, une todos estos documentos y datos, y compone el resultado final: la página Web. Los scripts, los ejecuta también el navegador, y también pueden generar más peticiones de datos en el tiempo, y el navegador, gestionará y actualizará la página Web en consecuencia.

Una página Web, es un documento de hipertexto (HTTP), luego habrá partes del texto en la página que puedan ser enlaces (links) que pueden ser activados (normalmente al hacer click sobre ellos) para hacer una petición de una nueva página Web, permitiendo así dirigir su agente de usuario y navegar por la Web. El navegador, traduce esas direcciones en peticiones de HTTP, e interpretará y procesará las respuestas HTTP, para presentar al usuario la página Web que desea.

El servidor Web.

Al otro lado del canal de comunicación, está el servidor, el cual "sirve" los datos que ha pedido el cliente. Un servidor conceptualmente es una única entidad, aunque puede estar formado por varios elementos, que se reparten la carga de peticiones, (load balancing), u otros programas, que gestionan otros computadores (como cache, bases de datos, servidores de correo electrónico), y que generan parte o todo el documento que ha sido pedido.



Un servidor no tiene que ser necesariamente un único equipo físico, aunque sí que varios servidores pueden estar funcionando en un único computador. En el estándar HTTP/1.1 y Host, pueden incluso compartir la misma dirección de IP.

Proxies.

Entre el cliente y el servidor, existen distintos dispositivos que gestionan los mensajes HTTP. Dada la arquitectura en capas de la Web, la mayoría de estos dispositivos solamente gestionan estos mensajes en los niveles de protocolo inferiores: capa de transporte, capa de red o capa física, siendo así transparentes para la capa de comunicaciones de aplicación del HTTP, además esto aumenta el rendimiento de la comunicación. Aquellos dispositivos, que sí operan procesando la capa de aplicación son conocidos como proxies. Estos pueden ser transparentes, o no (modificando las peticiones que pasan por ellos), y realizan varias funciones:

- caching (la caché puede ser pública o privada, como la caché de un navegador)
- filtrado (como un anti-virus)
- balanceo de carga de peticiones (para permitir a varios servidores responder a la carga total de peticiones que reciben)
- autenticación (para el control al acceso de recursos y datos)
- registro de eventos (para tener un histórico de los eventos que se producen)

Características clave del protocolo HTTP.

- HTTP es sencillo, incluso con el incremento de complejidad, que se produjo en el desarrollo de la versión del protocolo HTTP/2, en la que se encapsularon los mensajes, HTTP está pensado y desarrollado para ser leído y fácilmente interpretado por las personas, haciendo de esta manera más fácil la depuración de errores, y reduciendo la curva de aprendizaje para las personas que empiezan a trabajar con él.
- HTTP es extensible, presentadas en la versión HTTP/1.0, las cabeceras de HTTP, han hecho que este protocolo sea fácil de ampliar y de experimentar con él. Funcionalidades nuevas pueden desarrollarse, sin más que un cliente y su servidor, comprendan la misma semántica sobre las cabeceras de HTTP.



- HTTP es un protocolo con sesiones, pero sin estados, es decir: no guarda ningún dato entre dos peticiones en la misma sesión. Esto crea problemáticas, en caso de que los usuarios requieran interactuar con determinadas páginas Web de forma ordenada y coherente, por ejemplo, para el uso de "cestas de la compra" en páginas que utilizan en comercio electrónico. Pero, mientras HTTP ciertamente es un protocolo sin estado, el uso de HTTP cookies, si permite guardar datos con respecto a la sesión de comunicación. Usando la capacidad de ampliación del protocolo HTTP, las cookies permiten crear un contexto común para cada sesión de comunicación.
- HTTP y conexiones, una conexión se gestiona al nivel de la capa de transporte, y por tanto queda fuera del alcance del protocolo HTTP. Aún con este factor, HTTP no necesita que el protocolo que lo sustenta mantenga una conexión continua entre los participantes en la comunicación, solamente necesita que sea un protocolo fiable o que no pierda mensajes (como mínimo, en todo caso, un protocolo que sea capaz de detectar que se ha pedido un mensaje y reporte un error). De los dos protocolos más comunes en Internet, TCP es fiable, mientras que UDP, no lo es. Por lo tanto, HTTP, se apoya en el uso del protocolo TCP, que está orientado a conexión, aunque una conexión continua no es necesaria siempre.

Versiones del protocolo HTTP.

- La versión 1.0 y 1.1 establecieron los elementos básicos, por ejemplo los códigos 2xx, 3xx, 4xx o 5xx (1xx: Respuestas informativas, 2xx: Peticiones correctas, 3xx: Redirecciones, 4xx: Errores del cliente, 5xx: Errores del servidor).
- La versión 2.0 requiere del uso de un sistema de cifrado. Sigue funcionando por el sistema TCP y añade un sistema principal de streams. Esto permite mejorar la paralización de peticiones.
- La versión 3.0 mejora el sistema funcionando por UDP mediante QUIC.
- La mayor diferencia entre el HTTP2 y el HTTP3 es el protocolo sobre el que funciona. El sistema TCP tiene sistemas que permiten saber que algo que se manda a un usuario desde un servidor llega a su destino, mientras que UDP no, aunque el sistema UDP,



al no tener estos sistemas de verificación funciona mucho más rápido. Con el sistema QUIC se añaden ciertas medidas de fiabilidad en la interconexión de datos.

Esta nueva versión (HTTP3) tiene un cambio muy importante, pues será la que deje de utilizar el protocolo TCP que hasta ahora se había venido utilizando, lo sustituye un nuevo protocolo llamado QUIC, e inicialmente desarrollado por Jim Roskind en Google, aunque al ser un proyecto de código abierto el desarrollo ha sido conjunto por la comunidad de Internet.

QUIC, siglas que significan Quick UDP Internet Connections (Conexiones UDP Rápidas en Internet), está basado en otro viejo protocolo de los años 80 llamado UDP, y que a diferencia del TCP no requiere del intercambio continuo de información entre el emisor y el receptor del paquete de información. El protocolo de transferencia ya no se encarga de la integridad de los datos, ese peso recaerá de cada aplicación que lo use.

2.5.2 HTTPS.

El Protocolo de Transferencia de Hipertexto Seguro, es la versión segura de HTTP. El HTTPS está encriptado para aumentar la seguridad de las transferencias de datos. Esto es especialmente importante cuando los usuarios transmiten datos confidenciales, como al iniciar sesión en una cuenta bancaria, un servicio de correo electrónico o un proveedor de seguros médicos.

Cualquier sitio web, especialmente los que requieren credenciales de inicio de sesión, debe utilizar HTTPS. En los navegadores modernos, como Chrome, los sitios web que no utilizan HTTPS se señalan de forma diferente a los que sí lo hacen. Identifica un candado en la barra de URL que te indicará que la página web es segura. Los navegadores web se toman en serio el protocolo HTTPS. Google Chrome y otros navegadores marcan todas las páginas web que no utilizan HTTPS como no seguras.

HTTPS utiliza un protocolo de encriptación para encriptar las comunicaciones. El protocolo se conoce como Transport Layer Security (TLS), aunque antes se conocía como Secure Sockets Layer (SSL). Este protocolo asegura las comunicaciones mediante el uso de lo que



se conoce como infraestructura de clave pública asimétrica. Este tipo de sistema de seguridad utiliza dos claves diferentes para encriptar las comunicaciones entre dos partes:

1. La clave privada: esta clave la controla el propietario de un sitio web y se mantiene, como el lector ya habrá supuesto, privada. Esta clave está ubicada en un servidor web y se utiliza para descryptar la información encriptada por la clave pública.
2. La clave pública: esta clave está disponible para todos los que quieran interactuar con el servidor de forma segura. La información encriptada por la clave pública solo puede ser descryptada por la clave privada.

Ventajas.

- Privacidad en línea
- No requiere ninguna instalación de software adicional. Esto significa que puede ser utilizado sin restricciones por cualquier usuario. La autenticación con un certificado también inspira confianza en los clientes potenciales.

Desventajas.

- Hay cargos adicionales por certificados y costos crecientes con el aumento del tráfico. Estos pueden ser particularmente altos. Especialmente para sitios web nuevos y pequeños, estas tarifas pueden llegar a ser relativamente altas.
- Con conexiones HTTPS, el contenido no puede almacenarse en caché. Pero la tendencia hacia un mayor ancho de banda contrarresta esta desventaja.
- Un punto débil es también el menor rendimiento resultante del uso del cifrado SSL. El servidor debe realizar muchos más cálculos, aumentando así el tiempo de respuesta.
- Los hosts virtuales no funcionan con HTTPS.

2.6 NFS (Network File System).

El Sistema de Archivos de Red es un mecanismo para almacenar archivos en una red. Es un sistema de archivos distribuido que permite a los usuarios acceder a los archivos y directorios ubicados en sistemas remotos y tratar dichos archivos y directorios como si fueran locales.

Para que esto sea posible es necesario que haya un cliente y un servidor. No obstante, clientes puede haber muchos. Puede haber muchos equipos que se conecten a los archivos que hay en un servidor. Todo esto se hace de forma remota, sin necesidad de estar físicamente delante del equipo al que se quiere acceder. Por ejemplo, los usuarios pueden utilizar mandatos del sistema operativo para crear, eliminar, leer, grabar y establecer atributos de archivo para archivos y directorios remotos. (ver Figura 2.7)

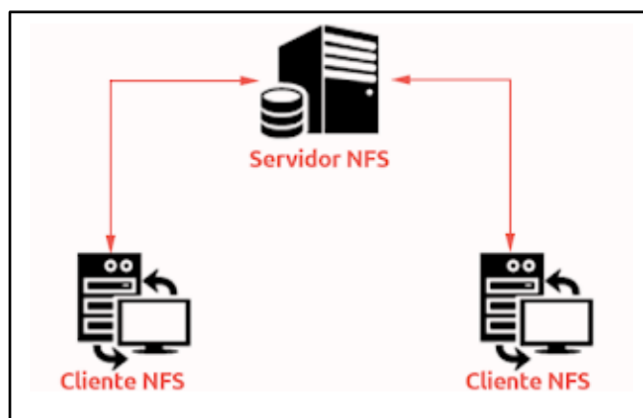


Figura 2.7 Conexión NFS

Algunos usos de NFS son:

- Cuando se necesita compartir archivos en modo lectura, NFS puede incluir los archivos correspondientes en un directorio que exportará con permiso de lectura y al que los usuarios podrán acceder.
- Un grupo de usuarios está realizando un trabajo y deben compartir una serie de archivos y trabajar sobre ellos, NFS permite crear un directorio en el servidor y se exporta a todas las máquinas/usuarios que colaboran en el trabajo.



- En un entorno de red donde se requiere tener centralizados los directorios home de todos ellos, NFS permite exportar y montar estos directorios /home de cada usuario de forma transparente. De esta forma se pueden controlar los accesos de los usuarios, la información almacenada en sus directorios de trabajo y la salvaguarda de dicha información.
- En un entorno de red en el que las máquinas de los usuarios disponen de poca capacidad y necesitan trabajar con aplicaciones que 'no caben' localmente, NFS permite exportar los directorios que contienen estas aplicaciones desde el servidor y los usuarios podrán ejecutarlas en sus máquinas.
- El administrador de red necesita que todas las máquinas tengan el mismo software y con idéntica configuración, NFS permite exportar del servidor el directorio que contiene el software requerido y el directorio que contiene las configuraciones correspondientes.

Este protocolo de red tiene diferentes ventajas y desventajas:

Ventajas.

- Múltiples clientes pueden acceder a los archivos
- Reduce la necesidad de tener espacio en disco
- Cualquier usuario puede modificar y actualizar los archivos
- Compatibilidad con muchos equipos

Desventajas.

- Seguridad: solo hay que usarlo en redes seguras y detrás de un firewall
- Requiere de una gran sobrecarga para leer archivos
- No es sencillo bloquear archivos o dar permisos

Rendimiento.

- NFS es un sistema de archivos muy utilizado alrededor del mundo. Esto es porque es compatible con una gama muy amplia de sistemas operativos, se incluyen los más conocidos como Linux, Unix y Windows.
- Minimiza la sobrecarga en la red y optimizar la velocidad en cuanto a transferencia de datos. Para lograr esto, se implementa un sistema de caché que almacena los datos



más utilizados de forma local. De forma que el sistema cliente, puede acceder a ellos de una forma rápida. Sin necesidad de buscarlos dentro de la red.

- Capacidad de manejar grandes volúmenes de datos. Esto lo hace ideal para entornos que requieren transferencias de datos muy rápidas y eficientes.
- NFS puede manejar diferentes solicitudes de lectura y escritura de forma simultánea, lo cual quiere decir que los clientes pueden tener acceso y modificar el contenido.
- Totalmente escalable, ya que tiene la capacidad de manejar de forma sencilla, gran cantidad de clientes y servidores. Lo cual, combinado con la flexibilidad del sistema, hace que se pueda adaptar a prácticamente cualquier tipo de necesidad y requisitos de red que tenga una organización.

Versiones de NFS.

Este protocolo salió a la luz en el año 1984, desarrollado por la compañía Sun Microsystems. Para ello lanzaron varias versiones, entre las que está NFSv2, que es la más utilizada y la más compatible con los diferentes sistemas operativos. En todo caso, presenta algunos errores y ciertos problemas de seguridad.

Luego apareció la versión NFSv3, la cual está ubicada en el Request for Comments 1813, siendo más eficiente que su versión anterior. El gran problema de esta versión 3, es que presenta problemas en cuanto a la compatibilidad con algunos clientes de los principales sistemas.

Estas dos versiones, permitieron utilizar el protocolo UDP para que ofrezca conexiones de red entre diferentes clientes y servidores NFS. Por otro lado, representaban una gran facilidad en cuanto a la gestión de todo el montaje y a la hora de exportar los sistemas de archivo. Pero estas no permitían el acceso al sistema de archivos. Por lo cual pronto presenta desventajas en este aspecto, y en cuanto a la seguridad.

Más adelante se lanzó la versión 4 o NFS4, la cual se hizo con la premisa de que fuera más segura que sus versiones anteriores. En todo caso requiere algunos ajustes y servicios de terceros para disponer de sistemas como puede ser el de autenticación de los usuarios. Esta



versión añadió el uso de las listas de control de acceso, y los permisos para que los usuarios que acceden a los archivos tuvieran algunas restricciones o privilegios.

Actualmente se dispone de la versión NFSv4.1, ubicada en el RFC 5661. Está específicamente diseñada para disponer de una mejora en la estabilidad y los accesos paralelos por servidores distribuidos bajo su propio soporte. Lo cual incluso puede llegar a considerarse otra pequeña limitación dependiendo el lugar de instalación o el uso que se le vaya a dar.

2.7 LDAP (Lightweight Directory Access Protocol).

LDAP son las siglas de Protocolo Ligero de Acceso a Directorio, se trata de un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en una red. Este protocolo se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.

Un directorio remoto es un conjunto de objetos que están organizados de forma jerárquica, tales como nombre claves direcciones. Estos objetos estarán disponibles por una serie de cliente conectados mediante una red, normalmente interna o LAN, y proporcionarán las identidades y permisos para esos usuarios que los utilicen.

LDAP está basado en el protocolo X.500 para compartir directorios, y contiene esta información de forma jerarquizada y mediante categorías para proporcionar una estructura intuitiva desde el punto de vista de la gestión por parte de los administradores. Es, por así decirlo, una guía telefónica, pero con más atributos y credenciales. En este caso se utiliza el término directorio para referirnos a la organización de estos objetos.

De forma general, estos directorios se utilizan básicamente para contener información virtual de usuarios, para que otros usuarios accedan y dispongan de información acerca de los contactos que están aquí almacenados. Pero es mucho más que esto, ya que es capaz de comunicarse de forma remota con otros directorios LDAP situados en servidores que pueden

estar en el otro lado del mundo para acceder a la información disponible. De esta forma se crea una base de datos de información descentralizada y completamente accesible.

La versión actual se denomina LDAPv3 y se encuentra definida en una hoja de documentación RFC 4511 accesible de forma pública.

LDAP es un protocolo basado en la conexión entre cliente y servidor. En el servidor LDAP se almacenarán los datos relativos al directorio, el cual podrá usar una amplia variedad de bases de datos para este almacenamiento, llegando a ser de grandes dimensiones. (ver Figura 2.8).

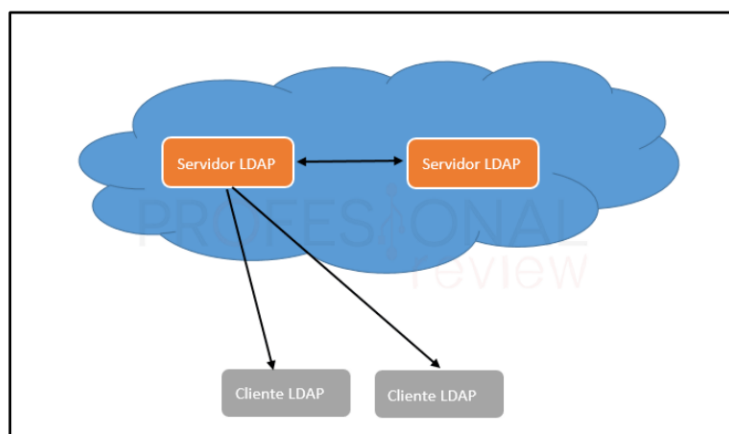


Figura 2.8 Protocolo LDAP

El funcionamiento de acceso y administración es muy similar a Active Directory de Windows. Cuando el cliente LDAP se conecta con el servidor, podrá realizar dos acciones básicas, bien consultar y obtener información del directorio, o modificarla.

- Si un cliente consulta la información el servidor LDAP puede conectarla directamente si tienen un directorio alojado en él, o bien redirigir la solicitud hasta otro servidor que efectivamente tenga esta información. Este podrá ser local, o remoto.



- Si un cliente quiere modificar la información del directorio, el servidor comprobará si el usuario que está accediendo a este directorio tiene permisos de administrador o no. Entonces, la información y gestión de un directorio LDAP se podrá hacer de forma remota.

Almacenamiento en LDAP.

En un directorio LDAP se almacenan básicamente la misma información que en un Directorio Activo de Windows. El sistema está basado en la siguiente estructura: (ver Figura 2.9).

- Entradas, llamadas objetos en Active Directory. Estas entradas son colecciones de atributos con un Nombre Distinguido (DN) Este nombre se utiliza para dar un identificador único e irrepetible a una entrada del directorio. Una entrada puede ser el nombre de una organización y de ella colgarán unos atributos. También una persona puede ser una entrada.
- Atributos: los cuales poseen un tipo identificador y los correspondientes valores. Los tipos se utilizan para identificar los nombres de atributos, por ejemplo “mail”, “name”, “jpegPhoto”, etc. Algunos de los atributos que pertenecen a una entrada debe ser obligatorios y otros opcionales.
- LDIF: el Formato de Intercambio de Datos de LDAP es la representación en texto ASCII de las entradas LDAP. Este debe ser el formato de los archivos que se utilicen para importar información a un directorio LDAP. Cuando se escriba una línea en blanco, significará el final de una entrada.
- Árboles: Es la organización jerarquizada de entradas. Por ejemplo, en una estructura de árbol se puede encontrar un país en la parte superior como principal, y dentro de éste tendremos los distintos estados que conforma el país. Dentro de cada estado se encuentran los distritos, ciudadanos y direcciones de donde viven, y así sucesivamente.

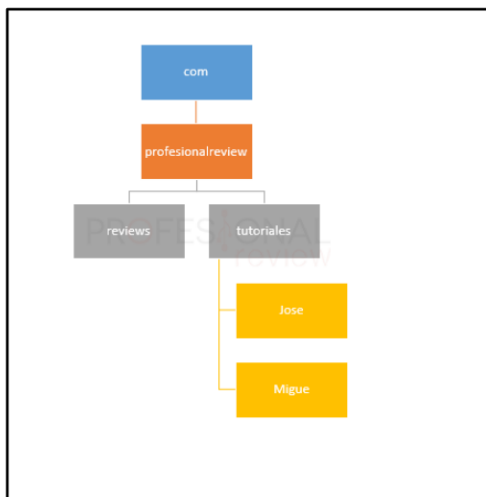


Figura 2.9 Almacenamiento en LDAP

En la actualidad existen diversas herramientas que utilizan este protocolo para la comunicación cliente servidor de un servicio de directorio. Lo más relevante es que incluso Active Directory de Windows utiliza este protocolo de comunicación:

- OpenLDAP: es la implementación libre del protocolo LDAP. Tiene su propia licencia y es compatible con otros servidores que utilicen el mismo protocolo. Es utilizado por distintas distribuciones Linux y BSD.
- Active Directory: es un almacén de datos de directorio con licencia Microsoft e implementado en sus sistemas operativos server desde Windows 2000. Realmente bajo la estructura de Active Directory se encuentra un esquema LDAPv3, por lo que también es compatible con otros sistemas que implemente este protocolo en sus directorios.
- Red Hat Directory Server: es un servidor que también se basa en LDAP similar a Active Directory, pero mediante una herramienta de código abierto. Dentro de este directorio se puede almacenar objetos como usuarios claves, grupos, políticas de permisos, etc.
- Apache Directory Server: otra de las grandes implementaciones que utilizan LDAP es el directorio con licencia de Apache Software.



- Open DS: Directorio basado en java de SUN Microsystems, que posteriormente se liberaría para todos los usuarios.

Ventajas de servicios de LDAP.

- Permite consolidar la información, sustituir bases de datos específicas de la aplicación y, así, reducir el número de bases de datos que se deben gestionar.
- Permite que diferentes servicios de nombres compartan los datos.
- Proporciona un repositorio central para los datos.
- Permite la sincronización de datos más frecuente y las réplicas.
- Compatible con varias plataformas y varios proveedores.

Desventajas de servicios LDAP.

- Un servidor LDAP actualmente no se admite como su propio cliente.
- La configuración y la gestión de servicios de nombres LDAP son más complejas y exigen una cuidadosa planificación.
- Un cliente NIS (Network Information System, Servicio de Información de Red, es un protocolo de servicio de directorio cliente-servidor) y un cliente LDAP nativo no pueden coexistir en la misma máquina cliente.

2.8 SMTP, POP, IMAP y SASL.

El email es una parte esencial de la comunicación online, comercial y personal. Los protocolos de correo definen el mecanismo de intercambio de email entre servidores y clientes. De esta forma, nos permiten enviar y recibir mensajes correctamente a través de la red.

Un protocolo de email es un grupo de reglas que aseguran que los correos electrónicos se transmitan correctamente a través de Internet. De hecho, hay una lista de protocolos de email que manejan las transacciones de email. Gracias a ellos se puede enviar y recibir correos desde diferentes máquinas, redes y sistemas operativos.

La lista de protocolos de email estándar incluye SMTP, POP3 e IMAP, cada uno de ellos funciona de manera diferente y proporciona un servicio diferente para administrar tu cuenta de email, a continuación, se describirá cada uno de ellos.

2.8.1 SMTP (Simple Mail Transfer Protocol).

El protocolo simple de transferencia de correo (SMTP) es uno de los protocolos más importantes del correo electrónico, es el protocolo utilizado cuando se envía un correo electrónico a través de un servidor de correo. Todos los proveedores de correo electrónico disponen de datos de conexión de POP/IMAP para el correo electrónico entrante, SMTP es el protocolo encargado de enviar los correos electrónicos desde un cliente de correo como Thunderbird o Outlook para Windows. (ver Figura 2.10).

SMTP utiliza el protocolo de la capa de transporte TCP, y hace uso de diferentes puertos dependiendo de si el tráfico va cifrado o no va cifrado:

- Puerto 25 TCP para tráfico sin cifrar.
- Puerto 465 TCP para tráfico cifrado SSL (SMTPS).
- Puerto 587 TCP como puerto alternativo para SMTPS con TLS.

Actualmente la gran mayoría de proveedores de servicios de correo electrónicos disponen de soporte para SSL/TLS, con la finalidad de cifrar y proteger todos los datos que se envían en el correo electrónico, por tanto, generalmente se usan los puertos 465 y 587, dependiendo de cómo esté configurado el servidor de correo. Por ejemplo, en el caso de Gmail no se permite utilizar el puerto 25 TCP porque no tiene ningún tipo de cifrado, sin embargo, soporta tanto el puerto 465 para conexiones SSL como el puerto 587 para conexiones TLS.

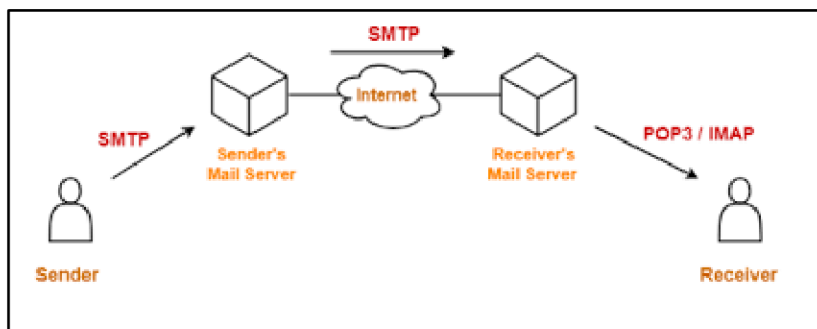


Figura 2.10 Protocolo SMTP



El protocolo SMTP está orientado específicamente al envío de correos electrónicos, en dirección «subida» o saliente, desde el cliente de correo local hasta el servidor de correo, para posteriormente enviarlo a su destinatario final. Por supuesto, el cliente de correo local almacenará estos emails en la sección de emails enviados, independientemente del cliente que se esté utilizando Thunderbird o Outlook de Windows.

SMTP permite realizar la autenticación con usuario/contraseña en texto claro a partir del puerto 25, pero actualmente, pocos servicios soportan este protocolo sin utilizar ningún tipo de cifrado, con el objetivo de proporcionarnos confidencialidad a la autenticación y también al correo electrónico enviado. Con las últimas versiones de SMTPS podremos usar los puertos 465 o 587 para tener cifrado de datos, autenticidad y comprobación de la integridad de los mensajes enviados.

Este protocolo cuenta con una serie de ventajas que pueden hacer una mejora importante dentro del sistema de cualquier empresa u organización, algunas son:

- **Eficiencia:** tiene la capacidad de manejar de forma rápida y precisa grandes volúmenes de mensajes de correo electrónico.
- **Confiabilidad:** es increíblemente confiable y seguro. Los mensajes de correo electrónico se envían directamente al servidor de correo del destinatario, lo que minimiza la posibilidad de pérdida o retraso en la entrega.
- **Versatilidad:** funciona con una variedad de hardware y sistemas operativos. Es utilizado por una variedad de clientes de correo electrónico, incluidos Outlook, Gmail, Yahoo, etc. Además, funciona con varios dispositivos, incluidas tablets, smartphones y computadoras.
- **Flexibilidad:** es muy adaptable y se puede configurar para cumplir con los requisitos individuales de cada usuario. Para enviar correos electrónicos desde varios dispositivos, por ejemplo, los usuarios pueden configurar la autenticación SMTP.
- **Personalización:** permite la personalización de los mensajes de correo electrónico, lo que mejora la experiencia del usuario. Las firmas de correo electrónico, los cambios de fuente y tamaño, así como la adición de imágenes y videos son opciones para los usuarios.

Algunas desventajas son:

- Spam: los spammers se han aprovechado para enviar una gran cantidad de correo electrónico no solicitado. Se requieren filtros de spam para dejar de recibir estos mensajes no deseados.
- Falta de notificación: no ofrece notificaciones de entrega y lectura de correo electrónico. Es posible que los usuarios no se den cuenta de la lectura o recepción de su mensaje por parte del destinatario.
- Limitaciones del tamaño: los mensajes de correo electrónico solo se pueden enviar en cierto tamaño. Esto puede ser un inconveniente al enviar mensajes con numerosos archivos adjuntos o al transferir archivos de gran tamaño.
- Dependencia del servidor: depende de un servidor de correo para enviar y recibir correos electrónicos. Los usuarios no pueden enviar ni recibir correos electrónicos si el servidor está inactivo o no está disponible.

2.8.2 POP (Post Office Protocol).

El Protocolo de Oficina de Correo, es usado en clientes de correo electrónico locales. Este protocolo se emplea para descargar los correos electrónicos desde el servidor al cliente local. (ver Figura 2.11).

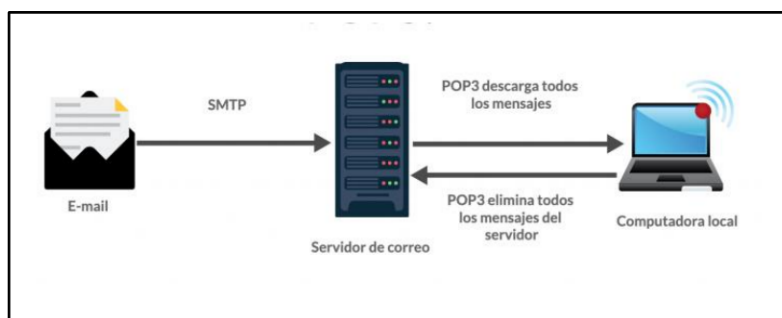


Figura 2.11 Protocolo de Oficina de Correo POP

El protocolo POP se encuentra dentro del nivel de aplicación. La primera versión del protocolo POP, conocida como POP1 estaba regulada por la RFC918 estando ya obsoleta. La RFC937 describe las características de la versión 2 (POP2), la última versión (POP3) y sus características se encuentran descritas en la RFC1939.



El protocolo POP se diseñó en una época donde los tiempos de conexión no eran muy buenos y su objetivo principal era poder gestionar los mensajes sin tener que estar conectado.

La principal característica de POP3 consiste en conectarse al servidor, descargar todos los mensajes, guardarlos en el equipo donde está configurada la cuenta de email y posteriormente eliminarlos del servidor (depuración automática). Actualmente los programas cliente en las configuraciones POP3 ofrecen un ajuste para dejar una copia de los mensajes en el servidor y eliminarlos después cierto tiempo, por defecto asigna 14 días, pero lo recomendado son 7.

Es importante destacar que el POP3 sólo permite recibir los mensajes, y no enviarlos. Por eso, al configurar una cuenta de correo electrónico en un cliente como Microsoft Outlook, por ejemplo, se tiene que indicar al programa que utilice para el envío.

Ventajas.

- Una cuenta POP se autentica en la computadora sin necesidad de estar en la web, basta con usar un programa de correo (Microsoft Outlook, Mail de Mac, entre otros).
- Uso optimizado del espacio en buzón en el servidor. Si se configura correctamente la depuración automática, el usuario no tendrá qué preocuparse que el buzón de su cuenta se sature.

Desventajas.

- Si el equipo donde está configurada la cuenta sufre algún desperfecto, se extravía o es robado, se pierde toda la información. Por eso es importante que, de forma periódica, se haga un respaldo en un dispositivo externo.
- Si el usuario tiene una configuración adicional, a través de Internet, no verá todos sus mensajes por la depuración activa en la configuración POP3.

El proceso de acceso al servidor de correo se hace a través de TCP/IP usando el puerto 110. Si la conexión está encriptada, se usa el puerto 995. Una vez se han conectado el cliente y el servidor, estos se comunican con comandos. Los comandos POP3 están compuestos por tres o cuatro cifras y, uno o más parámetros. Las respuestas del servidor incluyen: “+ OK” para un valor positivo y “ERR” para un mensaje negativo, o que requiere mayores especificaciones.



Cada sesión POP3 se divide en tres pasos: El primer paso es el inicio de sesión, donde el cliente accede al servidor con su nombre de usuario y contraseña. En el segundo paso se descargan los mensajes y, para terminar, el cliente se desconecta y elimina todos los mensajes del servidor. En caso de que la conexión sea interrumpida, los mensajes no serán eliminados, sino que se mantendrán ahí hasta que el cliente POP3 se conecte nuevamente y finalice la descarga.

Algunas características:

- Conexión en el puerto 110 (995).
- Conexión únicamente para descargar mensajes.
- Los comandos deben ser respondidos inmediatamente.
- Los mensajes son eliminados automáticamente una vez descargados.
- Acceso a los mensajes únicamente desde un cliente.
- Se descargan todos los mensajes.

Los comandos que son posibles enviar entre el cliente y el servidor durante las diferentes fases de comunicación son:

- “USER”, esta orden envía el usuario en cuestión al servidor. Este envío ocurre una sola vez durante la sesión.
- “PASS”, se envía la contraseña correspondiente al usuario para completar el proceso de autenticación.
- “STAT”, mediante esta orden es posible conocer la cantidad de mensajes no eliminados en el buzón y el tamaño total del mismo.
- “LIST”, permite obtener todos los mensajes no borrados y la longitud de cada uno de ellos.
- “RETR”, con esta orden podemos obtener un mensaje específico el cual no se elimina del buzón.
- “TOP”, se emplea para mostrar la cabecera y el número de líneas que ocupa un mensaje específico.
- “DELE”, con esta orden se solicita eliminar un mensaje específico al servidor.
- “RSET”, se utiliza para restaurar los mensajes que se hayan solicitado eliminar en la sesión actual.
- “UIDL”, esta orden devuelve una cadena de caracteres específica de cada mensaje. Esta cadena es persistente en cada sesión para cada mensaje y no varía.

- “QUIT”, cierra la sesión actual.

En un inicio el protocolo POP no era muy seguro. Esto se debía a que las credenciales eran transmitidas entre el cliente de correo y el servidor mediante texto plano, sin ningún cifrado. Aunque aún es posible encontrar este defecto de seguridad, actualmente POP3 ha implementado diversos mecanismos de autenticación y cifrado para mantener la seguridad en la comunicación.

2.8.3 IMAP (Internet Message Access Protocol).

Es un protocolo de correo entrante cuya mayor virtud es su capacidad de llevar a cabo una sincronización de los mensajes, que hay actualmente en el servidor, con todos los dispositivos donde sé que se consulten. IMAP sincroniza en tiempo real los cambios entre dispositivo y servidor, por lo que si son eliminados los mensajes en un dispositivo cuando se vuelva a sincronizar serán eliminados del servidor. (ver Figura 2.12)

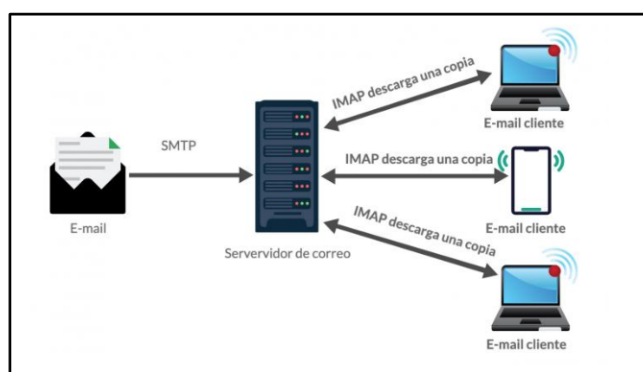


Figura 2.12 Protocolo IMAP

Por defecto, IMAP funciona en dos puertos:

- 143, Es el puerto predeterminado que no proporciona ningún cifrado.
- 993, Es el puerto seguro para IMAP y funciona a través de cifrado TLS / SSL.



Versiones de IMAP.

IMAP es un desarrollo que data de mediados la década de 1980, precisamente de 1985, y por supuesto que con el paso del tiempo ha ido mejorando su capacidad y flexibilidad, lo que se ve reflejada en las distintas versiones del protocolo que se sucedieron a través de los años.

- IMAP2 es la primera de las versiones de IMAP que fue distribuida públicamente. Sus bases fueron definidas en 1988 en el RFC1064. Esta normativa fue más tarde actualizada mediante el RFC1176 en enero de 1990, edición en la que se introdujeron algunos cambios en el etiquetado y los comandos.
- IMAP3 fue una contrapuesta del RFC1176, que fuera definida por el RFC1203 en febrero del año 1991 pero que no alcanzó el nivel de aceptación debida en estos casos, y por lo tanto se abandonó.
- IMAP2bis considerada una revisión experimental. Añade funcionalidades de crear, eliminar y guardar como borradores os mensajes en sus respectivos buzones.
- IMAP4 permite a os clientes manipular los mensajes, almacenarlos en el servidor, así como la manipulación de las carpetas locales. Ofrece la posibilidad a los usuarios de apps de clientes de correo electrónico, gestionar tanto los mensajes electrónicos almacenados en el servidor
- IMAP4rev1 solución a problemas de seguridad además incluye las funciones de escuchar los mensajes antes de descargar e cuerpo entero del correo electrónico.

Diferencias entre POP3 e IMAP con base a necesidades:

- POP3, Se descargan los mensajes del servidor a un dispositivo en concreto o varios, son borrados del servidor al cabo de un tiempo.
- IMAP, Se sincronizan los mensajes del servidor con toda clase de dispositivos y no se borran del servidor, más allá de aquellos que se borren manualmente.
- POP3, Se necesita conexión a Internet para descargar los mensajes, pero después se pueden consultar sin conexión.
- IMAP, Se necesita conexión a internet permanentemente, para acceder al servidor a leer los mensajes y borrar los que no se necesiten. Sincronización permanente.
- POP3, Los mensajes no ocupan espacio en el hosting, ya que se descargan en el dispositivo en el que se consulten.
- IMAP, Los mensajes ocupan espacio en el hosting, ya que se conservan dentro del mismo.



POP3 e IMAP manejan los correos entrantes y funcionan de diferentes maneras para recuperar o acceder a sus mensajes de email. Por lo tanto, se consideran protocolos de acceso al correo.

Por otro lado, el Protocolo SMTP está detrás de la transferencia de mensajes de servidor a servidor, o de cliente a servidor. Como este es el protocolo que maneja el envío de email desde una cuenta de email, se etiqueta como el protocolo saliente.

En resumen, gracias a IMAP y POP3, se puede recibir emails y con SMTP enviar mensajes.

2.8.4 SASL (Simple Authentication and Security Layer).

El Nivel de Seguridad y Autenticación Simple, es una estructura de autenticación y protección de datos en los protocolos de internet. Es un entorno de trabajo para la autenticación y seguridad de datos en protocolos de internet. SASL separa los mecanismos de autenticación de los protocolos de aplicación, en teoría permitiendo cualquier mecanismo de autenticación soportado por SASL para ser usado en cualquier protocolo de aplicación que utilice SASL. Los mecanismos de autenticación pueden también soportar proxy de autorización, una facilidad que permite a un usuario asumir la identidad de otro.

Los mecanismos de autenticación también pueden proveer una capa de seguridad de datos ofreciendo integridad de datos y servicios de confidencialidad de datos. DIGEST-MD5 (Cuando un cliente utiliza Digest-MD5, la contraseña no se transmite en texto simple y el protocolo impide ataques de reproducción) es un ejemplo de mecanismos que pueden proveer una capa de seguridad de datos. Los protocolos de aplicación que soportan SASL, generalmente también pueden soportar TLS (Transport Layer Security, Seguridad de la Capa de Transporte) para complementar los servicios ofrecidos por SASL.

SASL proporciona los siguientes servicios:

- Carga de cualquier complemento.
- Determinación de las opciones de seguridad necesarias de la aplicación para ayudar a elegir un mecanismo de seguridad.



- Listado de los complementos que están disponibles para la aplicación.
- Elección del mejor mecanismo de una lista de los mecanismos disponibles para un determinado intento de autenticación.
- Enrutamiento de datos de autenticación entre la aplicación y el mecanismo elegido.
- Proporción de información sobre la negociación de SASL a la aplicación.

Entre los protocolos que utilizan SASL se incluyen IMAP, LDAP, POP3 y SMTP.

2.9 Proxy

Un servidor proxy es un equipo que intercepta y administra el tráfico entre dos dispositivos, redes o protocolos. Los proxies son pasarelas que actúan como intermediarios entre su equipo y los sitios web y servicios de Internet que utiliza. Pueden actuar como cortafuegos, filtros o cachés, o facilitar las conexiones de red compartidas.

Un servidor proxy retransmite el tráfico entre su dispositivo y la Web, con lo que evita que su navegador esté en contacto directo con los sitios que visita. Sus solicitudes web pasan primero a través del servidor proxy. A continuación, este envía su solicitud al servidor web correspondiente y reenvía la respuesta a su dispositivo.

Al actuar como intermediarios, los proxies ayudan a proteger su privacidad y a reforzar la seguridad de su red local. Estas son otras funciones útiles de los servidores proxy.

- Capacidades de cortafuegos y filtro web: puede restringir el acceso a determinados sitios web y proteger su red frente a los hackers.
- Conexiones de red compartidas: puede conectar varios dispositivos a una red.
- Caché de datos: puede aumentar la velocidad de navegación guardando copias de las páginas web.

Un servidor proxy retransmite sus peticiones de Internet a sus respectivos destinos, luego agrupa las respuestas y se las devuelve. Con un servidor proxy, el único punto de contacto entre la red local de su dispositivo y los sitios web que visita es el propio servidor proxy. (ver Figura 2.13).

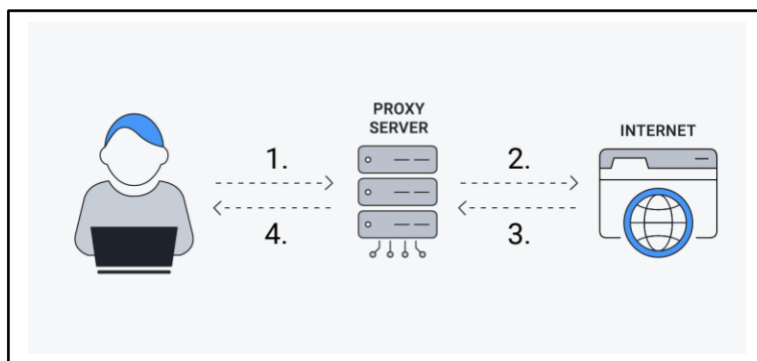


Figura 2.13 Funcionamiento Servidor Proxy

Paso 1: Las peticiones web se envían desde su dirección IP al servidor proxy.

Paso 2: El servidor proxy pasa su tráfico al sitio web que quiere visitar usando una dirección IP diferente.

Paso 3: Las respuestas del sitio web se envían de vuelta al servidor proxy.

Paso 4: El servidor proxy le devuelve los datos solicitados sin que el sitio web se comuniquen directamente con su dispositivo.

Un servidor proxy web puede enmascarar su dirección IP, lo cual dificulta al servidor web rastrear su ubicación física. No obstante, al ocultar la dirección IP no se cifra el tráfico de Internet, esto quiere decir que sus solicitudes de datos, incluidos los nombres de usuario, las contraseñas y otros datos de las cuentas, no están protegidas ni ocultas.

Tipos de proxy

- Proxy Transparente, informa al servidor web de que es un proxy y le comunica su dirección IP real, de modo que revela su identidad al servidor web. Los proxies transparentes no se usan por motivos de seguridad ni privacidad. Generalmente, los proxies transparentes los usan instituciones educativas, empresas y redes públicas, como las bibliotecas, para filtrar el contenido o usar la caché de datos.
- Proxy distorsionador, facilita una dirección IP falsa al servidor web, aunque se identifica como proxy. La dirección falsa proporciona anonimato, pero su auténtica



ventaja es que puede confundir al servidor web para que piense que está en otra ubicación.

- Proxy anónimo, mantendrá oculta su dirección IP a las páginas web que visite. Esto ayuda a combatir el robo de identidad y permite la navegación anónima. Pero los proxies anónimos se identifican como servidores proxy, y algunas páginas podrían negarles el acceso.
- Proxy de gran anonimato cambia periódicamente la dirección IP que comunica a los servidores web de los sitios que visite. Esto dificulta que las páginas web usen técnicas de seguimiento en línea para espiar su actividad de navegación. Si le preocupa la ciberseguridad, los proxies de gran anonimato son la mejor solución.

Prácticas Propuestas

Tema I Funciones de la administración de redes

1. Instalación de un Sistema Operativo de Red: Windows Server, Unix, Linux
2. Configurar los Clientes de Acceso

Tema II Servicios de Red

1. Configurar el servicio DNS (Usuarios, Grupos, Derechos, Restricciones)
2. Configurar el servicio DHCP
3. Configurar el servicio WEB (POP3, IMAP, SMTP)
4. Configurar el servicio FTP
5. Configurar el servicio e-mail



Tema III

ANÁLISIS Y MONITOREO

Competencia Específica: Analiza y monitorea la red para medir su desempeño y fiabilidad con herramientas de software

INTRODUCCIÓN.

En este tema se abordan los protocolos utilizados en Windows Server y las herramientas de análisis y monitoreo de redes para medir su desempeño y fiabilidad bajo la implementación de métricas de seguridad vigentes.



3. Análisis y Monitoreo.

3.1 Protocolos de administración de red.

El Protocolo Simple de Gestión de Redes (SNMP, Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de administración de la información entre dispositivos de red. Este es parte del protocolo de control de transmisión / protocolo de Internet (TCP/IP). SNMP posibilita a un administrador de red manejar el funcionamiento de la red, encontrar y manejar problemas, y planear el crecimiento de la red.

Dos versiones de SNMP existen: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras, como son operaciones de protocolo adicionales.

En Figura 3.1 se muestran los componentes básicos de SNMP enseguida se describen sus funcionalidades.

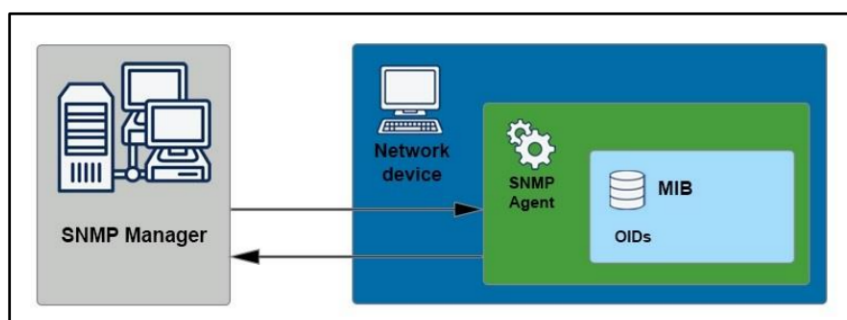


Figura 3.1 Componentes del protocolo SNMP

- Sistema de administración de red (NMS). Administra elementos de red en una red.
- Agente SNMP. El software que se ejecuta en el hardware o servicio monitoreado, recopila datos de métricas y realiza las operaciones solicitadas en la MIB del dispositivo administrado.



- Una base de información de gestión (MIB). La MIB es una base de datos de información que contiene los parámetros del dispositivo administrado.
- Dispositivo administrado. Un nodo en la red (enrutadores, servidores de acceso, conmutadores, concentradores, etc.) que contiene el agente SNMP y la MIB (Base de información de administración).

3.1.1 Administrador de SNMP.

El administrador SNMP (o servidor SNMP) es una estación de administración centralizada responsable de comunicarse con los dispositivos que ejecutan el agente SNMP. El administrador envía solicitudes al agente SNMP y recibe respuestas a intervalos regulares. Por lo general, es una máquina que ejecuta uno o más sistemas de administración de red. Las funciones clave de un administrador SNMP son:

- Envía consultas y solicitudes a los agentes SNMP.
- Reciba las respuestas de los agentes SNMP.
- Establecer o cambiar diferentes variables en los agentes SNMP.
- Confirme los eventos asincrónicos de los agentes.

3.1.2 Agente SNMP.

El agente es un programa que está empaquetado dentro del elemento de la red. La habilitación del agente le permite recopilar la base de datos de información (MIB) de gestión del dispositivo localmente y la pone a disposición del administrador de SNMP, cuando éste la solicita. Según el tipo de dispositivo, el agente SNMP puede ser estándar o específico del proveedor. Las funciones clave de un agente SNMP son:

- Recopila información de gestión sobre su entorno local
- Almacena y recupera la información de gestión según se define en el MIB.
- Señala un evento al administrador.
- Actúa como un proxy para algún nodo de la red no gestionable de SNMP.

3.1.3 Base de datos de información de gestión o base de información gestionada (MIB).

Cada agente de SNMP mantiene una base de datos de información que describe los parámetros del dispositivo gestionado. Es una estructura de datos que contiene valores de dispositivos de red local que se pueden recopilar, configurar y modificar, todo esto en un archivo de texto que describe todos los objetos de datos utilizados por un dispositivo en particular que se puede consultar o controlar a través de SNMP.

Normalmente estas MIB contienen un conjunto estándar de valores estadísticos y de control definidos para los nodos hardware de una red. SNMP también permite la ampliación de estos valores estándar con valores específicos para un agente determinado mediante el uso de MIB privadas.

En resumen, los archivos del MIB son el conjunto de preguntas que el administrador de SNMP puede hacer al agente. El agente recopila estos datos localmente y los almacena, tal como se define en el MIB. Por lo tanto, el administrador de SNMP debe estar al tanto de estas preguntas estándar y privadas para cada tipo de agente. La figura 3.2 muestra la organización y la jerarquía de datos dentro de una MIB.

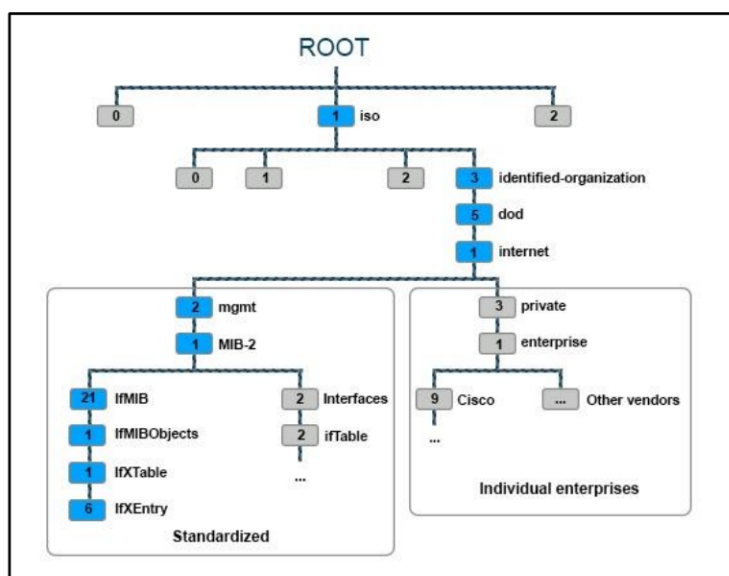


Figura 3.2 Organización y jerarquía de datos en una MIB



3.1.4 Dispositivo administrado.

Un dispositivo administrado es un nodo de red que contiene un agente SNMP. Casi todos los dispositivos de una red (enrutadores, conmutadores, servidores, impresoras,) funcionan como un dispositivo administrado. El NMS monitorea y controla los dispositivos administrados mediante tres comandos SNMP:

- ***read***, utilizado por el NMS para monitorear dispositivos administrados.
- ***write***, utilizado por el NMS para controlar los dispositivos administrados.
- ***trap***, utilizado por los dispositivos administrados para informar eventos al NMS.

El NMS sondea los dispositivos periódicamente, solicita información de estado o envía cambios de configuración cuando es necesario.

3.1.5 OID.

La MIB contiene muchos objetos administrados identificados mediante identificadores de objetos (OID). Un OID es un identificador MIB numérico que se utiliza para distinguir entre diferentes dispositivos en la base. El sistema utiliza los OID para acceder a los objetos administrados por MIB. Existen dos tipos de objetos gestionados:

- Objetos escalares. Único, definido por una sola instancia de objeto.
- Objetos tabulares. Definido por varias instancias de objetos relacionados que se agrupan en tablas MIB.

3.1.6 Trampas SNMP.

Las trampas SNMP son mensajes que el agente SNMP envía para notificar al NMS sobre eventos o alarmas en un dispositivo de red. Las trampas informan al administrador de la red sobre el estado y los eventos de un dispositivo.

Hay dos tipos de mensajes de notificación: trampas e informes. Si bien tienen el mismo objetivo de informar al administrador sobre un evento, difieren en el hecho de que un mensaje de información requiere una respuesta del NMS, mientras que el mensaje de captura no.



Cada mensaje de captura contiene la siguiente información:

- Empresa. El dispositivo que genera el mensaje trap (trap source).
- Dirección del agente. La dirección IP de origen de la captura.
- Trampa genérica. Especifica el tipo de captura.
- Trampa específica. Incluye información trampa privada de una empresa.
- Marca de tiempo. Especifica el tiempo transcurrido entre la reinicialización de la entidad de red y la creación del mensaje de captura.
- Enlaces variables. Una lista de nombres de variables y valores correspondientes.

3.1.7 Métricas de SNMP.

SNMP permite a los usuarios recopilar varias métricas de dispositivos conectados a una red.

Las métricas incluyen:

- Tiempo de actividad, es el tiempo que un dispositivo ha estado encendido y conectado a la red.
- Rendimiento, es la cantidad de datos transferidos desde el origen al destino dentro de un período de tiempo determinado.
- Temperatura, es la temperatura de funcionamiento actual del dispositivo.
- Errores de interfaz, es una lista de errores que ocurrieron durante el funcionamiento del dispositivo.
- Utilización de CPU y uso de memoria, son las estadísticas de rendimiento y recursos del dispositivo.

Los administradores de red pueden usar las herramientas de monitoreo de SNMP para analizar los datos obtenidos del dispositivo, visualizar los datos y recibir alertas basadas en algunas métricas que superan ciertos umbrales.



3.2 Bitácoras.

El uso de bitácoras en el ambiente de la seguridad ha tomado mucha importancia para el análisis de alguna posible brecha de seguridad, los vectores de ataque están a la orden del día y si no se tiene una visión de lo que está pasando en los equipos o la red corporativa, no hay mucho que hacer, incluso podría estar en medio de un ataque sin darse cuenta.

Una gran opción es hacer un modelo de gestión de bitácoras, que permita mostrar los eventos en los dispositivos conectados a la red corporativa, una de las herramientas importantes para lograr este propósito es el ya conocido Active Directory o Directorio Activo de Windows.

Al ser la parte central de la administración del dominio Windows, Active Directory es un componente con un nivel crítico, pues si falta puede afectar toda la red. Todas las operaciones de Active Directory afectan directamente al usuario que accede y al funcionamiento de las máquinas de la red, en cuanto al servicio del directorio y contexto de nombres de origen.

Cada operación de los objetos de Active Directory se convierte en una evidencia. El poder conocer que pasa día a día con la red beneficia directamente al nivel de seguridad, pues cada vez que exista la sospecha de un incidente en la infraestructura de red, basta con la revisión de las bitácoras correspondientes para tomar una acción antes de sufrir cualquier tipo de impacto. Para muchos administradores de red, hablar de bitácora es hablar de "logs" o registros.

Existen distintos tipos de bitácoras:

- Inicio de sesión.
- Cambios de un objeto.
- Caída de un servidor.
- Posible ataque.

Sin duda, hay muchas más que aumentan el nivel de seguridad y minimizan el nivel de riesgos; pues cuando se instala algún nuevo elemento en la red, por una mala práctica se deja en valores por defecto, no se habilitan las bitácoras y no se tiene visión de los eventos.

Si algún ataque enfocado en saltarse las medidas de seguridad es perpetrado no se podrían ver estas anomalías y por ende no se vería que se está siendo atacado.

Por tanto, para tener un buen control de las bitácoras se hace necesario:

- Contar con un gestor de bitácoras.
- Activar bitácoras que vayan de acuerdo al perfil de las soluciones implementadas y enviarlas al gestor.
- Gestor capaz de correlacionar eventos y generar alertas.
- Implementar una política interna que obligue a todo dispositivo a enviar sus bitácoras.
- Equipo especializado para la revisión y gestión de las bitácoras.
- Plan de acción en caso de detectar algún problema de seguridad.

En Windows Server se puede activar el visor de eventos (Figura 3.3) como bitácora y ver ciertos errores, para activarlo puede ser de dos formas:

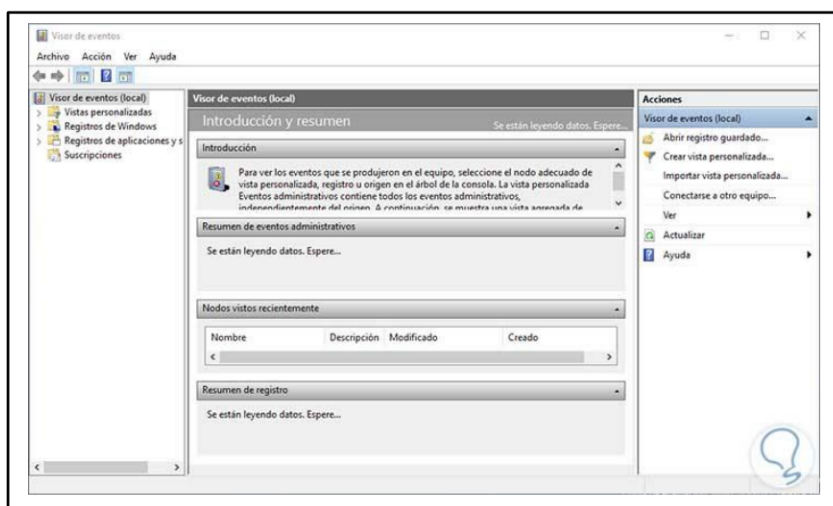


Figura 3.3 Visor de eventos



1. Para iniciar el Visor de eventos mediante la interfaz de Windows

- Haga clic en el botón Inicio.
- Haga clic en Panel de control.
- Haga clic en Sistema y mantenimiento.
- Haga clic en Herramientas administrativas.
- Haga doble clic en Visor de eventos.

2. Para iniciar el Visor de eventos mediante una línea de comandos

- Abra un símbolo del sistema.
- Escriba eventvwr.

Los tipos de eventos que se registran entran en alguna de estas categorías:

Registros de Windows.

Los registros de Windows están destinados a almacenar eventos de aplicaciones heredadas y eventos que se aplican a todo el sistema.

Registro de aplicaciones.

El registro de la aplicación contiene eventos registrados por aplicaciones o programas. Por ejemplo, un programa de base de datos podría registrar un error de archivo en el registro de la aplicación. Los desarrolladores de programas deciden qué eventos registrar.

Registro de seguridad.

El registro de seguridad contiene eventos como intentos de inicio de sesión válidos y no válidos, así como eventos relacionados con el uso de recursos, como la creación, apertura o eliminación de archivos u otros objetos. Los administradores pueden especificar qué eventos se registran en el registro de seguridad. Por ejemplo, si ha habilitado la auditoría de inicio de sesión, los intentos de iniciar sesión en el sistema se registran en el registro de seguridad.

Registro de configuración.

El registro de configuración contiene eventos relacionados con la configuración de la aplicación.



Registro del sistema.

El registro del sistema contiene eventos registrados por los componentes del sistema de Windows. Por ejemplo, la falla de carga de un controlador u otro componente del sistema durante el inicio se registra en el registro del sistema. Los tipos de eventos registrados por los componentes del sistema están predeterminados por Windows.

Registro de eventos reenviados.

El registro de ForwardedEvents se utiliza para almacenar eventos recopilados de equipos remotos. Para recopilar eventos de equipos remotos, debe crear una suscripción de eventos.

Registros de aplicaciones y servicios.

Los registros de aplicaciones y servicios son una nueva categoría de registros de eventos. Estos registros almacenan eventos de una sola aplicación o componente en lugar de eventos que podrían tener un impacto en todo el sistema.

3.3 Analizadores de protocolos (scanners y sniffers).

El analizador de protocolos de red es una herramienta que captura y analiza el ancho de banda y el tráfico de los datos en una red de computadoras. Puede ayudar a:

- Ver las estadísticas de ancho de banda de cada protocolo de la red.
- Evitar que las aplicaciones inactivas utilicen un ancho de banda valioso.
- Controlar la distribución de protocolos de red y resolver los problemas de red rápidamente ofreciendo una visibilidad clara del problema existente.

3.3.1 scanners.

El escaneo en red se refiere al uso de un software para recopilar información sobre sistemas informáticos. El escaneo en red se utiliza principalmente para la evaluación de la seguridad, el mantenimiento del sistema y también para realizar ataques de piratas informáticos (Figura 3.4).

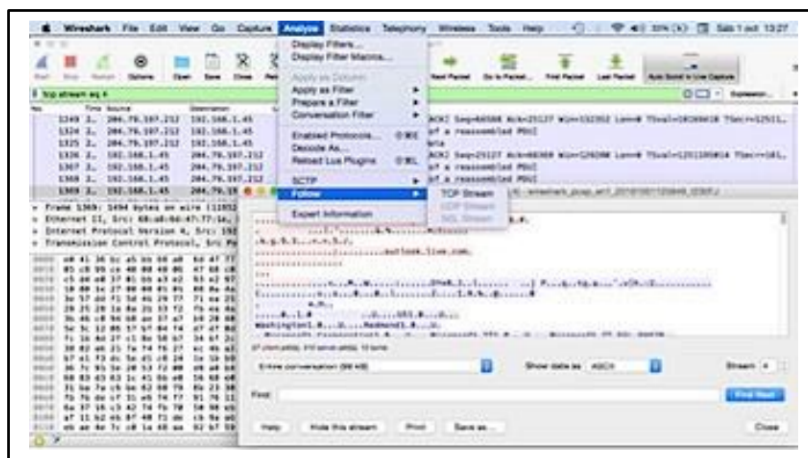


Figura 3.4 Software de escaneo de red

El propósito del escaneo en red es el siguiente:

- Reconocer los servicios de red UDP y TCP disponibles que se ejecutan en los hosts de destino.
- Reconocer los sistemas de filtrado entre el usuario y los hosts de destino.
- Determine los sistemas operativos (SO) en uso evaluando las respuestas de IP.
- Evaluar la previsibilidad del número de secuencia TCP del host objetivo para determinar el ataque de predicción de secuencia y la suplantación de TCP.

Funcionamiento.

El escaneo de red consiste en escaneo de puertos de red, así como escaneo de vulnerabilidades.

- El escaneo de puertos de red se refiere al método de enviar paquetes de datos a través de la red a los números de puerto de servicio especificados de un sistema informático (por ejemplo, el puerto 23 para Telnet, el puerto 80 para HTTP, etc.). Esto es para identificar los servicios de red disponibles en ese sistema en particular. Este procedimiento es efectivo para solucionar problemas del sistema o para reforzar la seguridad del sistema.



- El escaneo de vulnerabilidades es un método utilizado para descubrir vulnerabilidades conocidas de los sistemas informáticos disponibles en una red. Ayuda a detectar puntos débiles específicos en un software de aplicación o en el sistema operativo, que podrían usarse para bloquear el sistema o comprometerlo para fines no deseados.

En un sentido general, los administradores de red usan el escaneo de red para identificar hosts activos en una red mediante la evaluación de direcciones IP. Los mismos tipos de principios también se pueden usar en ataques cibernéticos para encontrar debilidades en un sistema.

En un sentido práctico, existen diferentes herramientas y técnicas para el escaneo en red. Los administradores de red pueden realizar barridos de ping, donde encuentran un rango de direcciones IP que se asignan a hosts en vivo en la red.

Los administradores también pueden usar escaneos de puertos, que envían mensajes a cada puerto de una red, para ver dónde esa red es fuerte o débil. Los diferentes tipos de escaneos de puertos incluyen un escaneo de puertos regular donde el escáner envía comunicaciones a todos los puertos de un sistema.

El escaneo en red es un método utilizado por un atacante para recopilar información, organizado en tres etapas:

- Etapa de huella, el atacante crea un perfil de la organización objetivo. Esto incluye datos como el sistema de nombres de dominio (DNS) de la organización y los servidores de correo electrónico, además de su rango de direcciones IP.
- Etapa de escaneo, el atacante descubre detalles sobre las direcciones IP especificadas a las que se puede acceder en línea, su arquitectura del sistema, sus sistemas operativos y los servicios que se ejecutan en cada computadora.
- Etapa de enumeración, el atacante recopila datos, incluidas tablas de enrutamiento, nombres de usuarios y grupos de red, datos del Protocolo Simple de Administración de Redes (SNMP) u otros.



Scanners más utilizados, algunos son de uso libre otros de paga:

- IP Address Manager
- PRTG Network Monitor
- Angry IP Scanner
- IP Scanner by Spiceworks
- NMAP
- Acunetix
- Solarwinds
- OpenVAS
- Wireshark

3.3.2 sniffers.

Un Sniffer es un software que se encarga de capturar paquetes en tránsito (entrada y salida) en una cierta red y analizarlos. En otras palabras, es un programa que puede observar la información en tránsito en una red y obtener información de esta. Está hecho para recibir información que no está destinada para él, lo que es muy útil, pero a la vez un gran peligro.

Los sniffers están disponibles para varias plataformas, tanto en las variaciones comerciales como en código abierto. Algunos de los paquetes más simples son muy fáciles de implementar en C o Perl, utilizando una interfaz de línea de comandos y descargando los datos capturados a la pantalla.

Los proyectos más complejos utilizan una interfaz gráfica de usuario. Las estadísticas de tráfico de gráficos, realizan un seguimiento de varias sesiones y ofrecen varias opciones de configuración.

Los sniffers de red son también los motores para otros programas. Los llamados “Sistemas de Detección de Intrusos” (IDS) utilizan sniffers para localizar paquetes que coincidan con las reglas designadas para marcar algo como malicioso o extraño. La utilización de la red y los programas de vigilancia a menudo los utilizan para recoger los datos necesarios para mediciones y análisis. Las fuerzas de seguridad que necesitan controlar los correos



electrónicos durante sus investigaciones, probablemente emplean un sniffer diseñado para capturar tráfico muy específicos.

Funcionamiento.

El sniffer le ordena al computador, específicamente a su tarjeta de red, que deje de ignorar a todo el tráfico dirigido a otros equipos y preste atención a ellos. Para esto, la tarjeta de red se coloca en un estado conocido como “modo promiscuo”, el cual no descarta los paquetes que no son para su dirección MAC (Media Access Control, Control de Acceso al Medio), sino que los almacena y lee.

Una vez que esto sucede, una máquina puede ver todos los datos transmitidos en ese segmento de red. El programa entonces comienza una lectura constante de toda la información que entra en el computador, a través de la tarjeta de red.

Los datos que viajan por la red se presentan como paquetes o ráfagas de bits con formato para protocolos específicos. Debido a este formato estricto, un sniffer puede filtrar las capas de encapsulación y decodificar la información pertinente almacenada en el equipo de origen, equipo de destino, número previsto de puerto, capacidad de carga y, en pocas palabras, en cada paquete de información que se intercambia entre dos equipos.

Un Sniffer más que una herramienta de ataque en manos de un administrador de red puede ser una valiosa arma para la auditoría de seguridad en la red. Puesto que el acceso a la red externa debe estar limitado a un único punto. Un Sniffer puede ser la herramienta ideal para verificar como se está comportando la red.

Las ventajas en las que más se destacan los sniffers son:

- Control del tráfico en la red administrada.
- Verificar el comportamiento de los usuarios de acuerdo a la normativa de la red.
- Observar el uso indebido de un recurso que dañe el normal tráfico de la red.
- Obtención de estadísticas de tráfico.
- Se puede analizar qué servicios son los más utilizados en la red.

- En base a esta información, se pueden definir políticas de adquisición de software y hardware.

Sniffers más utilizados, algunos son de uso libre otros de paga:

- Wireshark
- Microsoft MA
- Tcpdump
- Windump

3.4 Análisis de desempeño de la red: tráfico y servicios.

Un análisis de tráfico en redes basadas en tecnología Ethernet se basa normalmente en el uso de sondas (software) con interfaz Ethernet. Dichas sondas capturan el tráfico que será analizado y constituye la plataforma en la que se pueden ejecutar aplicaciones propietarias o de dominio público; Con dichas aplicaciones se puede determinar el tipo de información que circula por la red y el impacto que tiene sobre la misma. (Figura 3.5)

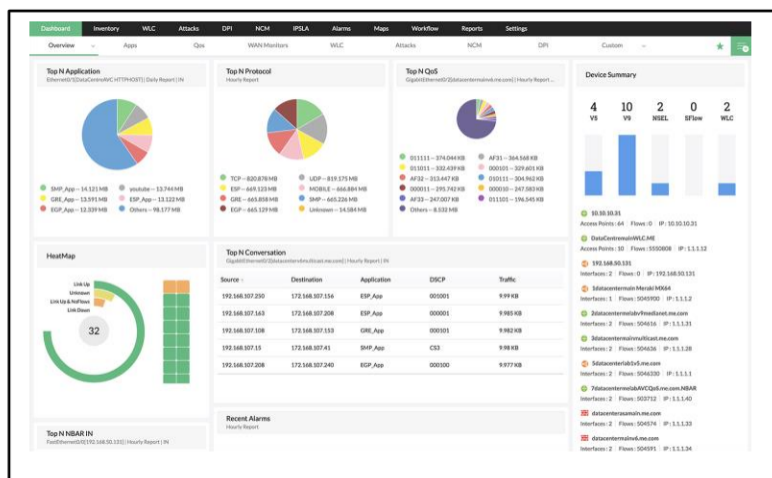


Figura 3.5 Análisis del tráfico de red

El análisis de tráfico permite determinar las capacidades y métricas bajo las cuales se está comportando la red, y evitar tener problemas de desempeño. Por ejemplo, se podrá determinar la existencia de virus o el uso excesivo de aplicaciones que comúnmente degradan



las prestaciones de la red, sobre todo si hablamos de los enlaces principales que dan acceso a Internet.

Las tecnologías de transmisión de datos a través de redes de computadores son el eje central del funcionamiento de un entorno informático que presta servicios de tipo cliente/servidor.

Realmente casi toda la información que circula en la red, dependiendo de la capacidad de captura de los agentes, algunos de los parámetros que se pueden observar en el análisis de tráfico son:

- Porcentaje de uso de la red y errores presentados.
- Tamaño de las tramas.
- Distribución de los protocolos presentes en la red: es posible evaluar los protocolos presentes en la red para identificar los protocolos que están en uso dentro de la red. Con esta información un administrador de red puede conocer para qué se está utilizando realmente la red de la empresa y establecer directivas en base a estos resultados.
- Consumo de los dispositivos de red.
- Verificación de los paquetes enviados en la red.
- Equipos con más envío o recepción de paquetes.
- El análisis de tráfico es una técnica que permite analizar problemas en las redes, y conocer las causas y efectos de dichos problemas, verificando los datos que viajan por la red.

Circunstancias legales para el análisis de tráfico de la red:

- Monitorear el rendimiento de la red.
- Verificar la seguridad de la red.
- Verificar las transacciones de las comunicaciones en la red.
- Mantener un registro del tráfico.
- Descubrir las fuentes de tráfico no deseado.
- Descubrir las estaciones de trabajo que pueden ser vulnerables.
- Asegurarse que los usuarios siguen las políticas de usuarios definidas.



Circunstancias ilegales para el análisis de tráfico de la red:

- Capturar información de la red.
- Leer información confidencial.
- Determinar información general de la red.

En una red WAN:

- En el caso de las redes WAN el análisis de tráfico es importante ya que el ancho de banda es un recurso escaso y de alto costo, primordialmente porque este depende de las capacidades ofrecidas por la infraestructura de un proveedor de servicio.
- En el caso de las conexiones a Internet el análisis de tráfico debe ser minucioso, ya que hoy en día aplicaciones básicas pueden verse afectadas por virus o ataques de negación del servicio, este tipo de incidentes repercuten de forma directa sobre el desempeño óptimo de este tipo de redes.

En una red LAN:

- Los aspectos cruciales a nivel de las redes LAN están basados en el monitoreo y revisión del consumo de los recursos de red por parte de los equipos que se encuentran internamente, en muchos casos también para atacar eventos como virus o fallas en las tarjetas de red que pueden causar un gran número de broadcast, y por ende la disminución del ancho de banda disponible en la red entre otras cosas.

Un administrador de red debe comprender los siguientes conceptos para realizar el análisis de tráfico de la red:

- Diagrama de la red.
- Información sobre los servidores.
- Información sobre aplicaciones.
- Información sobre el direccionamiento.
- Protocolos (DNS, DHCP, HTTP, FTP, POP, entre otros)
- Direcciones MAC.
- Direcciones IP.
- Protocolos orientados a conexión (TCP).

- Protocolos no orientados a conexión (UDP).
- Información sobre las tramas de ethernet y los campos que la componen.

3.5 QoS.

QoS son las siglas de Quality of Service, que en español significa calidad de servicio, se refiere a cualquier tecnología que gestiona el tráfico de datos para reducir la pérdida de paquetes, la latencia y el jitter, o fluctuación, en una red. Esta frase, en el mundo de las comunicaciones, hace referencia a la calidad de la conexión que esperan tener distintos clientes conectados en una misma red.

Las redes empresariales deben proporcionar servicios predecibles y medibles como aplicaciones, como voz, video y datos sensibles a retrasos, para atravesar una red. Las organizaciones utilizan QoS para cumplir con los requisitos de tráfico de aplicaciones sensibles, como voz y video en tiempo real, y para evitar la degradación de la calidad causada por la pérdida de paquetes, el retraso y la fluctuación, Figura 3.6.

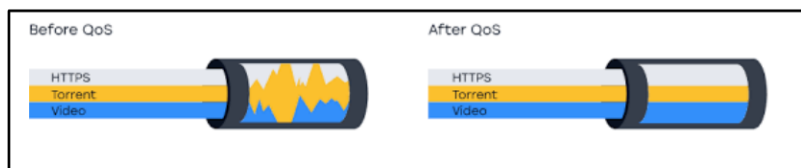


Figura 3.6 Tecnología QoS

Las organizaciones pueden alcanzar una QoS mediante el uso de ciertas herramientas y técnicas, como el búfer de fluctuación y la configuración del tráfico. Para muchas organizaciones, QoS se incluye en el acuerdo de nivel de servicio (SLA) con su proveedor de servicios de red para garantizar un cierto nivel de rendimiento de la red.

QoS es un servicio que viene incluido en prácticamente todos los routers que ofrecen las compañías de internet. Aunque su funcionamiento es indiferente según el router (se basa en



los mismos principios para priorizar el tráfico), en los routers de baja gama apenas tiene efecto alguno, a pesar de venir implementado de serie.

El servicio QoS permite priorizar el tráfico entre varios dispositivos conectados al mismo router. Una vez que se selecciona cual IP interna tiene prioridad sobre el resto, se puede seguir configurando minuciosamente para que, además, cierto tipo de tráfico tenga prioridad sobre otro para llegar a esta IP. Algunos routers de media y alta gama ya incorporan algoritmos preconfigurados que nos muestran en una lista qué tipo de tráfico que se desea priorizar, por lo que las opciones para configurarlo según las necesidades son muy amplias.

También es posible utilizar el servicio QoS para asignar un ancho de banda máximo a cada dispositivo. Esto se traduce en limitar el ancho de banda de otros dispositivos de la red, especificando en el QoS un host o una IP estática. De esta manera, si disponemos de 100 Mbps de conexión y se limita algún dispositivo a 10 Mbps, nunca podrá ir a una velocidad mayor.

El servicio QoS es algo inherente al router, que es donde se centraliza todo el tráfico, por lo que si hay varios routers en la misma LAN habrá que configurar el QoS adecuadamente en cada uno de ellos.

Parámetros de QoS,

Las organizaciones pueden medir la QoS cuantitativamente mediante el uso de varios parámetros, incluidos los siguientes:

- Pérdida de paquetes. Esto sucede cuando los enlaces de red se congestionan y los enrutadores y conmutadores comienzan a descartar paquetes. Cuando los paquetes se eliminan durante la comunicación en tiempo real, como en llamadas de voz o video, estas sesiones pueden experimentar fluctuaciones y lagunas en el habla. Los paquetes se pueden descartar cuando se desborda una cola o una línea de paquetes en espera de ser enviados.



- Jitter. Este es el resultado de la congestión de la red, la desviación del tiempo y los cambios de ruta. Demasiada inestabilidad puede degradar la calidad de la comunicación de voz y video.
- Latencia. Se refiere al tiempo que tarda un paquete en viajar desde su origen hasta su destino. La latencia debe ser lo más cercana a cero posible. Si una llamada de voz sobre IP tiene una gran cantidad de latencia, los usuarios pueden experimentar eco y audio superpuesto.
- Ancho de banda. Esta es la capacidad de un enlace de comunicaciones de red para transmitir la cantidad máxima de datos de un punto a otro en un período de tiempo determinado. QoS optimiza el rendimiento de la red administrando el ancho de banda y otorgando más recursos a las aplicaciones de alta prioridad con requisitos de rendimiento más estrictos que a otras.
- Puntuación media de opinión (MOS, Mean Opinion Score). Esta es una métrica para calificar la calidad de la voz que utiliza una escala de cinco puntos, donde cinco indica la calidad más alta.

Los beneficios incluyen:

- Las aplicaciones de misión crítica tienen acceso a los recursos que necesitan.
- Los administradores pueden gestionar mejor el tráfico.
- Las organizaciones pueden reducir costos al eliminar la necesidad de comprar nueva infraestructura de red.
- Se mejora la experiencia del usuario.

Implementación de QoS.

Al implementar herramientas y estrategias de QoS, las organizaciones deben seguir estos pasos:



- **Planificación.** La organización debe comprender las necesidades y requisitos de servicio de cada departamento, elegir un modelo adecuado y cultivar la aceptación de las partes interesadas.
- **Diseño.** Luego, la organización debe tomar nota de todos los cambios significativos de software y hardware, y aplicar el modelo de QoS elegido a las características específicas de su arquitectura de red.
- **Prueba.** La organización debe probar la configuración y las políticas de QoS en un entorno de prueba seguro y controlado donde se puedan solucionar los errores.
- **Despliegue.** Las políticas deben implementarse de manera iterativa, en fases. Una organización puede optar por implementar políticas por segmento de red o por función de QoS separada (lo que hace cada política).
- **Seguimiento y análisis.** Las políticas deben ajustarse para mejorar el desempeño de acuerdo con los datos de desempeño.

Existen tres modelos para implementar QoS: Mejor Esfuerzo, Servicios Integrados y Servicios Diferenciados.

- **Mejor esfuerzo.** Un modelo de QoS en el que todos los paquetes reciben la misma prioridad y no hay una entrega garantizada de paquetes. El mejor esfuerzo se aplica cuando las redes no han configurado políticas de QoS o cuando la infraestructura no es compatible con QoS.
- **Servicios integrados (IntServ).** Un modelo de QoS que reserva ancho de banda a lo largo de una ruta específica en la red. Las aplicaciones solicitan a la red la reserva de recursos y los dispositivos de red monitorean el flujo de paquetes para asegurarse de que los recursos de la red puedan aceptar los paquetes. La implementación de IntServ requiere enrutadores compatibles con IntServ y utiliza el Protocolo de reserva de recursos (RSVP) para la reserva de recursos de red. IntServ tiene una escalabilidad limitada y un alto consumo de recursos de red.
- **Servicios diferenciados (DiffServ).** Un modelo de QoS en el que los elementos de red, como enrutadores y conmutadores, se configuran para dar servicio a múltiples clases de tráfico con diferentes prioridades. El tráfico de la red debe dividirse en



clases según la configuración de la empresa. Por ejemplo, al tráfico de voz se le puede asignar una prioridad más alta que a otros tipos de tráfico. A los paquetes se les asignan prioridades mediante el uso de puntos de código de servicios diferenciados (DSCP) para su clasificación. DiffServ también utiliza el comportamiento por salto para aplicar técnicas de QoS a los paquetes, como la puesta en cola y la priorización.

Herramientas de QoS.

Las herramientas de QoS generalmente se incluyen en estas categorías:

- Clasificación. Identifican el tráfico y lo marca para asegurarse de que otros dispositivos de red puedan identificarlo y priorizarlo.
- Hacer cola. Reservan ancho de banda para almacenar paquetes en un búfer para procesarlos más tarde.
- Vigilancia. Hacen cumplir un ancho de banda específico y limita y descartan los paquetes que no se adhieren a la regla. Esto es parte de la prevención de la congestión.
- Formación. Similar a la vigilancia, pero ponen en cola el exceso de tráfico en un búfer en lugar de eliminarlo por completo. Esto, junto con las colas, es parte de la gestión de la congestión.
- Descarte temprano aleatorio ponderado (WRED). Eliminan los flujos de datos de baja prioridad para preservar los datos de alta prioridad de los efectos negativos de la congestión de la red.
- Fragmentación y compresión. Reducen el ancho de banda en una red para evitar retrasos y fluctuaciones.

Las herramientas de QoS pueden realizar solo una de estas funciones o una combinación de ellas. Muchas herramientas de QoS se administran y realizan estas funciones automáticamente, lo que brinda a los administradores acceso para modificar la configuración y las políticas según sea necesario. Algunas herramientas populares de monitoreo de QoS son:



- Analizador de tráfico SolarWinds NetFlow
- Monitor de red Paessler PRTG
- Analizador de red Nagios
- Analizador ManageEngine NetFlow
- OpenNMS (código abierto)
- Ntopng (código abierto)
- Bandwidthd (código abierto)

Prácticas Propuestas.

1. Configurar en Windows Server el protocolo SNMP.
2. Utilizando Packet Tracer, elaborar un diagrama con Servidor, estaciones de trabajo, router, switch y configurar en protocolo SNMP en los dispositivos de interconexión.
3. Utilizando Packet Tracer, configurar, verificar y resolver problemas de calidad de servicio (QoS) en los puertos host de router Cisco.



Tema IV

SEGURIDAD BÁSICA

Competencia Específica: Aplica mecanismos de seguridad para proporcionar niveles de confiabilidad en una red.

INTRODUCCIÓN.

En este tema se abordan las recomendaciones para la seguridad básica que debe tener toda organización y así garantizar la protección física y lógica de una red de computadoras.



4. Seguridad Básica.

4.1 Elementos de la Seguridad.

La seguridad en la red comprende software, hardware y procedimientos diseñados para mejorar la defensa de la red contra amenazas internas y externas a los sistemas informáticos de una organización. Existen múltiples capas de software y hardware que impiden que numerosas amenazas penetren, dañen y se propaguen a través de la red.

Adicional se ha convertido en algo crucial para las organizaciones de hoy en día, ya que el aumento exponencial de hackers criminales podría aumentar las pérdidas globales por delitos informáticos, Figura 4.1.



Figura 4.1 Delitos informáticos

Para evitar pérdidas financieras y de reputación, es importante que las organizaciones se centren en la seguridad de su infraestructura de red, teniendo en cuenta estos elementos básicos:

- Network Access Control (NAC, Control de Acceso a la Red). NAC básicamente le permite al administrador entender y controlar quién puede y quién no puede acceder a la red, identificando qué usuarios y dispositivos están permitidos en esta, ayudándolo a permanecer al tanto de qué dispositivos están bloqueados.



Las herramientas de análisis de comportamiento para identificar conductas anómalas en una red ayudan a los administradores a monitorear sus redes en busca de tráfico atípico, una vez identificado dicho tráfico anormal envía notificaciones al usuario.

El NAC también se puede programar para un "acceso basado en roles", en el que el acceso del usuario está restringido en función de su perfil para que, una vez dentro de la red, solo puedan acceder a archivos o datos aprobados.

- **Firewalls (Cortafuegos).** Un firewall es un dispositivo de seguridad de red que controla el tráfico entrante y saliente, formando un tipo de barrera entre una red confiable y no confiable, decidiendo si bloquear o permitir dicho tráfico, convirtiéndose en una de las primeras líneas de defensa. Existen varios tipos de firewall, como lo son: stateful firewall, application firewall, packet filtering firewall, deep packet inspection firewall y proxy firewall.
- **Servidor proxy.** Se trata de un dispositivo que actúa como intermediario entre Internet y las conexiones del navegador, y filtra los paquetes que circulan entre ambos puntos. Gracias al proxy se bloquean sitios web que se estima que pueden ser peligrosos o de los que esté prohibida su visita dentro del ambiente laboral. Gracias al proxy también se define un sistema de autenticación que limita el acceso a la red externa.
- **Protección de puntos finales.** La seguridad de puntos finales, que a menudo requiere un enfoque multicapa, implica la protección de todos los puntos finales (computadoras portátiles, tabletas, teléfonos inteligentes, dispositivos portátiles y otros dispositivos móviles) que se conectan a su red.
- **End Point Disk Encryption.** También llamado cifrado de punto final, se trata de un proceso de codificación de datos para que nadie que no guarde la clave de descifrado pueda leerlo. Protege los sistemas operativos de la instalación de archivos corruptos, al bloquear los archivos almacenados en ordenadores, servidores y otros puntos finales.



- Seguridad en la nube. La seguridad en la nube protege los recursos en línea, como datos confidenciales, aplicaciones, IP virtualizados y servicios, de filtraciones, pérdidas o robos.

Mantener seguros los sistemas basados en la nube requiere políticas de seguridad sólidas, así como la superposición de métodos de seguridad como la arquitectura de firewall, los controles de acceso, las redes privadas virtuales (VPN), la encriptación o enmascaramiento de datos, el software de inteligencia de amenazas y los programas de recuperación de desastres.

- Redes privadas virtuales (VPN). Es un software que protege la identidad de un usuario cifrando sus datos y enmascarando su dirección IP y ubicación. Cuando un usuario usa una VPN, ya no se conecta directamente a Internet, sino a un servidor seguro que luego se conecta a Internet en su nombre.
- Escáner de vulnerabilidades. Por último, el escáner de vulnerabilidades es una herramienta de seguridad informática fundamental para todo tipo de empresas, no importa el tamaño o el sector. El escáner es un software que detecta, analiza y gestiona los puntos débiles que tenga el sistema.

4.2 Tipos de riesgos y amenazas.

Actualmente vivimos no solo en una sociedad del conocimiento, si no en una sociedad interconectada, inmersa en una revolución tecnológica que accede, comparte, crea y gestiona conocimiento de todo tipo constantemente, esto gracias en gran medida a toda la infraestructura de redes mediante las cuales viajan los datos e información hasta llegar a nuestras manos.

4.2.1 Riesgos.

Los riesgos informáticos son exposiciones como atentados y amenazas a los sistemas de información, entre los tipos de riesgos se encuentran:



- **Riesgos de Identidad.** Abarca los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos se manifiestan en los siguientes componentes de un sistema:
 - 1. Interface del usuario.
 - 2. Procesamiento.
 - 3. Procesamiento de errores.
 - 4. Administración de cambios.
 - 5. Información.
- **Riesgos de Relación.** Se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones.
- **Riesgos de Acceso.** Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información.

Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

 - 1. Administración de la información.
 - 2. Entorno de procesamiento.
 - 3. Redes.
- **Riesgo de Utilidad.** Estos riesgos se enfocan en tres diferentes niveles de riesgo:
 - 1. Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
 - 2. Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
 - 3. Backups y planes de contingencia controlan desastres en el procesamiento de la información.
- **Riesgos de Infraestructura.** En las organizaciones no existe una estructura de información tecnológica efectiva para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Están asociados con los



procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente, pago de cuentas, etc.).

- Riesgos de Seguridad General. Los estándar IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo.
 1. Riesgos de choque eléctrico: Nivel de voltaje alto.
 2. Riesgos de incendios: Inflamabilidad de materiales.
 3. Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
 4. Riesgos mecánicos: Inestabilidad de las piezas eléctricas.

4.2.2 Amenazas.

Es todo elemento o acción capaz de atentar contra la seguridad de la información, se consideran como exteriores a cualquier sistema, es posible establecer medidas para protegerse de las amenazas, pero prácticamente imposible controlarlas y menos aún eliminarlas.

Aunque todas las amenazas tienen la característica de ser las posibles causantes de destrucción a los sistemas, las amenazas pueden tener diferentes orígenes. El conectar el sistema a internet, lo expone a numerosas amenazas que se incrementan diariamente. Los tipos más generales de amenazas son:

- Vulnerabilidad de información.
- Vulnerabilidad en el software.
- Debilidades en el sistema físico.
- Transmisión de debilidades.

Las formas y estilos comúnmente utilizados en ataques realizados vía Internet en redes corporativas están divididos en nueve categorías:

- Ataques basados en password.
- En base a escuchar el tráfico de red.
- Ataques que explotan los accesos confiables.
- Basándose en las direcciones IP.
- Introduciendo información sin darse cuenta.

- Predicción de números secuenciales.
- Secuestrando sesiones.
- Ataques enfocados a explotar las debilidades de la tecnología.
- Explotando el sistema de librerías compartidas.

4.3 Políticas de seguridad.

Una política de seguridad es una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología e información. Puede ser tan simple como una política de uso aceptable o contener muchas páginas y detallar cada aspecto de conectividad de los usuarios, así como los procedimientos de uso de redes. La política de seguridad debe ser el punto central acerca de la forma en la que se protege, se supervisa, se evalúa y se mejora una red. Mientras que la mayoría de los usuarios domésticos no tiene una política de seguridad formal por escrito, a medida que una red crece en tamaño y en alcance, la importancia de una política de seguridad definida para todos los usuarios aumenta drásticamente, Figura 4.2.



Figura 4.2 Políticas de seguridad

Sin una política de seguridad, la disponibilidad de su red puede verse comprometida. La política comienza por evaluar el riesgo para la red y la creación de un equipo de respuesta. La continuación de la política requiere la implementación de una práctica de administración del cambio en la seguridad y supervisión de la red para detectar violaciones de seguridad.



Por último, el proceso de revisión del estudio modifica la política existente y se adapta a las lecciones aprendidas.

Cuando se crea y desarrolle una política de seguridad, se deben tener claros los objetivos.

Los objetivos de seguridad entran dentro de una o más de estas categorías:

- Protección de recursos (Autenticación). El esquema de protección de recursos garantiza que solo los usuarios autorizados podrán acceder a los objetos del sistema.
- Autorización. La autorización es el proceso de determinar quién o qué puede acceder a los recursos del sistema o ejecutar determinadas actividades en un sistema. Normalmente, la autorización se realiza en el contexto de la autenticación.
- Integridad. Es la seguridad de que la información entrante es la misma que la que se ha enviado. Proteger los datos para que no se puedan husmear ni interpretar, lo que se suele hacer cifrándolos.
- No repudio. Prueba de que se ha producido una transacción o de que se ha enviado o recibido un mensaje. El uso de certificados digitales y de la criptografía de claves públicas para firmar transacciones, mensajes y documentos es la base del no repudio. El remitente y el destinatario están ambos de acuerdo en que el intercambio tiene lugar. La firma digital de los datos es una prueba suficiente.
- Confidencialidad. Es la seguridad de que la información confidencial permanece privada. La confidencialidad es fundamental para la seguridad total de los datos. El cifrado de los datos con certificados digitales y la capa de sockets segura (SSL) o con una conexión de redes privadas virtuales (VPN) permite asegurar la confidencialidad al transmitir datos entre varias redes que no sean de confianza. La política de seguridad debe indicar qué métodos se emplearán para proporcionar la confidencialidad de la información dentro de la red y de la información que sale de ella.
- Actividades de seguridad de auditoría. Consiste en supervisar los eventos relacionados con la seguridad para proporcionar un archivo de anotaciones de los accesos satisfactorios y de los no satisfactorios (denegados).



4.4 Mecanismos de seguridad física y lógica: control de acceso, respaldos, autenticación y elementos de protección perimetral.

- Seguridad física, protección desde el interior. La mayoría de los expertos coincide en que toda seguridad comienza con la seguridad física. El control del acceso físico a los equipos y a los puntos de conexión de red es posiblemente el aspecto más determinante de toda la seguridad. Cualquier tipo de acceso físico a un sitio interno deja expuesto el sitio a grandes riesgos. Si el acceso físico es posible, normalmente se pueden obtener archivos protegidos, contraseñas, certificados y todo tipo de datos.
- Seguridad Lógica. El Control de Acceso a la Red, también conocido por las siglas NAC (Network Access Control) tiene como objetivo asegurar que todos los dispositivos que se conectan a las redes corporativas de una organización cumplen con las políticas de seguridad establecidas para evitar amenazas como la entrada de virus, salida de información, etc. El fenómeno BYOD (Bring Your Own Device) en el que los empleados utilizan sus propios dispositivos (tabletas, portátiles, smartphones) para acceder a los recursos corporativos está acelerando la adopción de las tecnologías NAC para autenticar al dispositivo y al usuario.

Existen una serie de fases como:

1. Detección: es la detección del intento de conexión física o inalámbrica a los recursos de red reconociendo si el mismo es un dispositivo autorizado o no.
2. Cumplimiento: es la verificación de que el dispositivo cumple con los requisitos de seguridad establecidos como por ejemplo dispositivo autorizado, ubicación, usuario, antivirus actualizado.
3. Cuando un dispositivo no cumple los requerimientos se puede rechazar la conexión o bien mandarlo a un portal cautivo “Cuarentena”.
4. Remediación: es la modificación lógica de dichos requisitos en el dispositivo que intenta conectarse a la red corporativa.



5. Aceptación: es la entrada del dispositivo a los recursos de red en función del perfil del usuario y los permisos correspondientes a su perfil que residen en un servicio de directorio.
 6. Persistencia: es la vigilancia durante toda la conexión para evitar la vulneración de las políticas asignadas.
- Respaldos. Una copia de seguridad o backup (su nombre en inglés) en tecnología de la información o informática es una copia de seguridad o proceso de copia de seguridad con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.

Tipos de copias de seguridad:

1. Copia de seguridad normal. Copia todos los archivos seleccionados y los marca como copiados (es decir, se desactiva el atributo de modificado). En las copias de seguridad normales solo necesita la copia más reciente del archivo o la cinta que contiene la copia de seguridad para restaurar todos los archivos. Las copias de seguridad normales se suelen realizar al crear por primera vez un conjunto de copia de seguridad.
2. Copia de seguridad incremental. Solo copia los archivos creados o modificados desde la última copia de seguridad normal o incremental. Respalda solo los datos modificados, pero solo respaldan los datos que han cambiado desde la última copia de seguridad, ya sea una copia de seguridad completa o incremental. Marca los archivos como respaldos como copiados (es decir, se desactiva el atributo de modificado). Si usa una combinación de copias de seguridad normal e incremental, la restauración de los datos debe realizarse con el último conjunto copia de seguridad normal y todos los conjuntos de copia de seguridad incremental.
3. Copia de seguridad diferencial. Copia de archivos creados o modificados desde la última copia de seguridad normal o incremental. Respalda solo los archivos que cambiaron desde la última copia de seguridad completa, en lugar de la última copia de seguridad diferencial. Los archivos no se marcan como copiados (es decir, no se desactiva el atributo de modificado). Si realiza una



combinación de copias de seguridad normal y diferencial, para restaurar los archivos y las carpetas deben disponer de la última copia de seguridad normal y de la última copia de seguridad diferencial.

- Autenticación. Se comprende que es cualquier método que permita comprobar de manera segura alguna característica sobre un objeto. Dicha característica puede ser su origen, su integridad, su identidad, etc. Se consideran tres grandes tipos dentro de los métodos de autenticación:
 1. Autenticación de mensaje. Garantizar la procedencia de un mensaje conocido, de forma que se asegure de que no es una falsificación. Este mecanismo se conoce habitualmente como firma digital.
 2. Autenticación de usuario mediante contraseña. En este caso se trata de garantizar la presencia de un usuario legal en el sistema. El usuario deberá poseer una contraseña secreta que le permita identificarse.
 3. Autenticación de dispositivo. Se trata de garantizar la presencia de un dispositivo válido. Este dispositivo puede estar solo o tratarse de una llave electrónica que sustituye a la contraseña para identificar a un usuario.
- La seguridad perimetral es un concepto emergente, asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles. Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), según el principio físico de actuación (cable de fibra óptica, cable de radiofrecuencia, cable de presión, cable microfónico, etc.) o bien por el sistema de suportación (autosoportados, soportados, enterrados, detección visual, etc.).



4.5 Resolución de problemas.

Si una red o una parte de la red queda fuera de servicio, esto puede tener un impacto negativo importante en la empresa. Cuando ocurren problemas en la red, los administradores deben usar un enfoque sistemático de resolución de problemas a fin de que la red vuelva a funcionar completamente lo antes posible.

La capacidad de un administrador de red para resolver problemas de red de manera rápida y eficaz es una de las habilidades más buscadas en TI. Las empresas necesitan personas con habilidades sólidas de resolución de problemas de red, y la única forma de obtener estas habilidades es a través de la experiencia práctica y el uso de métodos sistemáticos de resolución de problemas.

Hay tres etapas principales en el proceso de resolución de problemas, estas etapas no son mutuamente excluyentes. En cualquier parte del proceso, es posible que sea necesario volver a las etapas anteriores.

Para cada etapa, se debe establecer una política de resolución de problemas que incluya procedimientos de control de cambios. Una política proporciona una forma coherente de llevar a cabo cada etapa.

Etapas 1. Recolección de síntomas.

La resolución de problemas comienza con la recolección y el registro de los síntomas de la red, los sistemas finales y los usuarios. Además, el administrador de red determina qué componentes de la red se vieron afectados y de qué forma cambió la funcionalidad de la red en comparación con la línea de base.

Los síntomas pueden aparecer de distintas maneras, que incluyen alertas del sistema de administración de red, mensajes de la consola y quejas de los usuarios. Mientras se recolectan los síntomas, es importante que el administrador de red realice preguntas e investigue el problema para restringirlo a una variedad de posibilidades más reducida.

Etapas 2. Aislamiento del problema.

El aislamiento es el proceso mediante el que se eliminan variables hasta que se identifica como la causa a un único problema o a un conjunto de problemas relacionados. Para realizar



esto, el administrador de red examina las características de los problemas en las capas lógicas de la red para poder seleccionar la causa más probable. En esta etapa, el administrador de red puede recopilar y registrar más síntomas, según las características que se identifiquen.

Etapa 3. Implementación de la medida correctiva.

Una vez que se identificó la causa del problema, el administrador de red trabaja para corregir el problema mediante la implementación, la puesta a prueba y el registro de posibles soluciones.

Después de encontrar el problema y determinar una solución, es posible que el administrador de red deba decidir si la solución se puede implementar inmediatamente o si se debe posponer.

Esto depende del impacto de los cambios en los usuarios y en la red. La gravedad del problema se debe ponderar en comparación con el impacto de la solución.

Si la medida correctiva no soluciona el problema o genera otro nuevo, se registra la solución probada, se eliminan los cambios y el administrador de red vuelve a recolectar síntomas y a aislar el problema.



REFERENCIAS BIBLIOGRÁFICAS



Referencias Bibliográficas.

- A. (2023, enero 20). *El perfil del administrador de red*. Computerworld.es. <https://www.computerworld.es/archive/el-perfil-del-administrador-de-red>.
- Alva, I. (s/f). *LA IMPORTANCIA DEL USO DE BITÁCORAS EN COMPONENTES CLAVE COMO ACTIVE DIRECTORY*. Smartekh.com. Recuperado el 12 de junio de 2023, de <https://blog.smartekh.com/bitacoras-componentesclave-activedirectory>.
- Analizador de protocolos: monitoree sus redes con PRTG*. (s/f). Paessler.com. Recuperado el 14 de junio de 2023, de https://www.paessler.com/es/protocol-analyzer?gad=1&gclid=CjwKCAjwp6CkBhB_EiwAlQVyxZxzi9fDpP3Htb4YK-cQBBc8D3CGsu7hDSZLaknowaYkA-Lgf2m8wBoCj6EQAvD_BwE.
- Ankush. (2019, febrero 2). *12 analizadores de paquetes de red para administradores de sistemas y analistas de seguridad*. Geekflare. <https://geekflare.com/es/network-packet-analyzers/>.
- Archiveddocs. (s/f-a). *Event logs*. Microsoft.com. Recuperado el 13 de junio de 2023, de [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc722404\(v=ws.11\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc722404(v=ws.11)?redirectedfrom=MSDN).
- Archiveddocs. (s/f-b). *Start event viewer*. Microsoft.com. Recuperado el 13 de junio de 2023, de [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc766401\(v=ws.10\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc766401(v=ws.10)).
- Ariganello, E. (2014a). *Redes Cisco: Guía de estudio para la certificación CCNA security*.
- Ariganello, E. (2014b). *Redes Cisco: Guía de estudio para la certificación CCNA security*.
- Axarnet. (s/f). *Diferencias entre IMAP y POP3: ventajas y desventajas*. Axarnet.es. Recuperado el 6 de junio de 2023, de <https://axarnet.es/blog/diferencias-imap-pop3>.
- BalaDelli. (s/f). *Server event logs*. Microsoft.com. Recuperado el 13 de junio de 2023, de <https://learn.microsoft.com/en-us/mem/configmgr/protect/tech-ref/bitlocker/server-event-logs>.
- Blokdyk, G. (2018). *Fcaps: Third Edition*. Createspace Independent Publishing Platform.
- Borges, S. (2020, junio 26). *Servidor POP: ¿Qué es y para qué sirve?* Infranetworking. <https://blog.infranetworking.com/servidor-pop/>.



- Callaghan, B., Pawlowski, B., & Staubach, P. (1995). *NFS Version 3 Protocol Specification*. RFC Editor.
- Carballar, J. A. (2021, junio 11). *Qué son los DNS y cómo funcionan*. Carballar.com; J.A. Carballar. <https://carballar.com/que-son-los-dns-y-como-funcionan>.
- Castillo, J. A. (2019, enero 5). *LDAP: Qué es y para qué se utiliza este protocolo*. Profesional Review; Miguel Ángel Navas. <https://www.profesionalreview.com/2019/01/05/ldap/>.
- Certificación ISO*. (s/f). Com.mx. Recuperado el 8 de mayo de 2023, de <https://www.iso.com.mx/>.
- Citar una Página Web con Normas APA [Generador Gratis]*. (2019, enero 3). Referencias Bibliográficas. <https://referenciasbibliograficas.com/citar-pagina-web-apa/>.
- ¿Cómo funciona el escaneo en red?* (s/f). Icy Science. Recuperado el 14 de junio de 2023, de <https://es.theastrologypage.com/how-does-network-scanning-work>.
- Completo, V. mi P. (s/f). *SEGURIDAD BASICA*. Blogspot.com. Recuperado el 14 de julio de 2023, de <http://ramsesseguridadbas.blogspot.com/p/45-resolucion-de-problemas.html>.
- Conceptos básicos de HTTP*. (s/f). Mozilla.org. Recuperado el 31 de mayo de 2023, de https://developer.mozilla.org/es/docs/Web/HTTP/Basics_of_HTTP.
- Conocimiento*. (s/f). Certerus.com. Recuperado el 5 de junio de 2023, de <https://mi.certerus.com/knowledgebase/5/Correo-POP3.html>.
- Crispin, M. R. (1988). *Interactive Mail Access Protocol: Version 2*. RFC Editor.
- Crispin, M. R. (1990). *Interactive Mail Access Protocol: Version 2*. RFC Editor.
- De, C. (2021, febrero 22). *Calidad de servicio o QoS*. ComputerWeekly.es; TechTarget. <https://www.computerweekly.com/es/definicion/Calidad-de-servicio-o-QoS>.
- De Luz, S. (2021, septiembre 24). *Aprende cómo funciona el protocolo SMTP para correo saliente*. RedesZone. <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-smtp-email-configuracion/>.



Deland-Han. (s/f). *Configuración del servicio SNMP - Windows Server*. Microsoft.com. Recuperado el 12 de mayo de 2023, de <https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/configure-snmp-service>.

Delgado, S. (2022, junio 13). *Wireshark: casi todo lo que debes saber*. MuyComputerPRO. <https://www.muycomputerpro.com/2022/06/13/wireshark-todo-lo-que-debes-saber>.

Descripción general de la puntuación de opinión media (MOS) - Centro de recursos de Genesys Cloud. (2019, noviembre 12). Centro de recursos en la nube de Genesys. <https://es-help.mypurecloud.com/articles/mean-opinion-score-mos-overview/>.

Descripción general de LDAP. (s/f). Netapp.com. Recuperado el 2 de junio de 2023, de <https://docs.netapp.com/es-es/ontap/nfs-admin/using-ldap-concept.html>.

Deyimar, A. (2017, septiembre 7). *¿Cómo funciona el SSH?* Tutoriales Hostinger. <https://www.hostinger.mx/tutoriales/que-es-ssh>.

Direcciones IP y el Sistema de Nombres de Dominio · Gobernanza de Internet bit a bit. (s/f). Gitbooks.io. Recuperado el 24 de mayo de 2023, de <https://embinternet.gitbooks.io/gobernanza-de-internet-bit-a-bit/content/como-funciona-internet/direcciones-ip-y-el-sistema-de-nombres-de-dominio.html>.

Ejemplo de Configuración de QoS en los Puertos de Acceso Catalyst 6800ia. (2022, marzo 13). Cisco. https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-6500-series-switches/119140-config-qos-cat6800-00.html.

El DHCP y la configuración de redes. (s/f). IONOS Digital Guide. Recuperado el 24 de mayo de 2023, de <https://www.ionos.mx/digitalguide/servidores/configuracion/que-es-el-dhcp-y-como-funciona/>.

Expósito, I. (2019, febrero 12). *¿Qué es un servidor DNS?* Ayuda | dinahosting; dinahosting. <https://dinahosting.com/ayuda/que-es-un-servidor-dns/>.

Fundamentals of (IPS) intrusion prevention system. (2016, febrero 26).

Ghimiray, D. (2022, febrero 15). *¿Qué es un servidor proxy y cómo funciona? ¿Qué es un servidor proxy y cómo funciona?*; Avg. <https://www.avg.com/es/signal/proxy-server-definition>.

Glosario- Qué es DHCP y Para qué Sirve. (s/f). Netec. Recuperado el 24 de mayo de 2023, de <https://www.netec.com/que-es-dhcp-y-para-que-sirve>.



- Gomez, Y. L. (2021, noviembre 24). *Todo lo que Necesita Saber Sobre el Protocolo POP*. LovTechnology. <https://lovtechnology.com/todo-lo-que-necesita-saber-sobre-el-protocolo-pop/>.
- Hosting, S. W. (s/f). *¿Qué son los Protocolos de Correo (POP3, SMTP e IMAP) y sus Puertos predeterminados?* Recursos de conocimiento de SiteGround. Recuperado el 6 de junio de 2023, de <https://es.siteground.com/tutoriales/email/protocolos-pop3-smtp-imap/>.
- HTTP*. (s/f). Concepto. Recuperado el 31 de mayo de 2023, de <https://concepto.de/http/>.
- HTTPS*. (s/f). Ryte.com. Recuperado el 6 de junio de 2023, de <https://es.ryte.com/wiki/HTTPS>.
- IBM Documentation*. (2021, marzo 3). Ibm.com. <https://www.ibm.com/docs/es/control-desk/7.6.0.4?topic=server-manually-configuring-microsoft-active-directory>.
- IBM Documentation*. (2023, marzo 24). Ibm.com. <https://www.ibm.com/docs/es/aix/7.1?topic=system-nfs-services>.
- I. E. (s/f). *Fundamentos de gestión de Seguridad de la Información*. Isotools.us. Recuperado el 8 de mayo de 2023, de <https://info.isotools.us/ebook-fundamentos-de-gestion-de-seguridad-de-la-informacion>.
- IMAP o POP3: una comparativa de protocolos de acceso*. (s/f). IONOS Digital Guide. Recuperado el 5 de junio de 2023, de <https://www.ionos.mx/digitalguide/correo-electronico/cuestiones-tecnicas/imap-o-pop3-que-protocolo-elegir/>.
- Insight to SASL vulnerabilities*. (2018, octubre 12). Tweaklibrary. <https://tweaklibrary.com/insight-to-sasl-vulnerabilities/>.
- Introducción a FCAPS: ¿Qué es y cómo funciona?* (2021, octubre 5). SGRwin. <https://www.sgrwin.com/es/introduccion-a-fcaps-que-es-y-como-funciona/>.
- JasonGerend. (s/f). *Introducción al Administrador de recursos del servidor de archivos (FSRM)*. Microsoft.com. Recuperado el 12 de mayo de 2023, de <https://learn.microsoft.com/es-es/windows-server/storage/fsrm/fsrm-overview>.
- Jessie. (2021, septiembre 6). *Understanding variable length subnet masks (VLSM)*. Study CCNA; Study-CCNA.com. <https://study-ccna.com/variable-length-subnet-mask-vlsm/>.



- Jiménez, J. (2021, octubre 14). *Qué es el protocolo NFS y cómo se puede usar*. RedesZone. <https://www.redeszone.net/tutoriales/internet/protocolo-archivos-nfs/>.
- Kourmentza, E. (2020, enero 8). *Descripción del puesto: Administrador de red (m/h/x)*. Recruiting Resources: How to Recruit and Hire Better; Workable. <https://resources.workable.com/es/administrador-de-red-descripcion-del-puesto>.
- La terminología de la ICANN sobre la seguridad*. (s/f). Iann.org. Recuperado el 24 de mayo de 2023, de <https://www.icann.org/es/blogs/details/icanns-security-terminology-8-7-2013-es>.
- M.3400 Funciones de gestión de la red de gestión de las telecomunicaciones*. (s/f). Itu.int. Recuperado el 8 de mayo de 2023, de <https://www.itu.int/rec/T-REC-M.3400-200002-I/es>.
- Mammedov, D. (2021, agosto 16). SASL. www.wiki3.es-es.nina.az. <https://www.wiki3.es-es.nina.az/SASL.html>.
- ManageEngine. (s/f). *Tutorial: Fundamentos de SNMP*. Manageengine.com. Recuperado el 12 de junio de 2023, de <https://www.manageengine.com/latam/network-monitoring/tutorial-fundamentos-protocolo-snmp.html>.
- Manuls. (2011, enero 29). *Cómo funciona Internet: ¿Qué son y para qué sirven las DNS?* Xatakamovil.com; Xataka Móvil. <https://www.xatakamovil.com/conectividad/como-funciona-internet-dns>.
- Marijan, B. (2022, octubre 20). *What is SNMP? {Versions, Monitoring, and Components}*. Knowledge Base by PhoenixNAP; phoenixNAP. <https://phoenixnap.com/kb/what-is-snmp>.
- Marker, G. (2020, enero 4). *El protocolo IMAP*. Tecnologia-facil.com; Tecnología Fácil. <https://tecnologia-facil.com/que-es/protocolo-imap/>.
- Morgan, K. (2021). *Redes de Computadoras para Principiantes: La Guía básica para la Seguridad de la Red Central, la Arquitectura Informática, la Tecnología Wireless y los Sistemas de Comunicaciones, Cisco, CCNA y OSI* (P. Gomez, Trad.). Computer Publishing.
- Networking, cloud, and cybersecurity solutions*. (2023, mayo 4). Cisco. <https://www.cisco.com/site/us/en/index.html>.



- PatAltimore. (s/f). *Anexo L: Eventos para supervisar*. Microsoft.com. Recuperado el 21 de junio de 2023, de <https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>.
- Pavas, A. (2016). Visibilidad de la Revista Ingeniería e Investigación. *Ingeniería e Investigación*, 36(3), 3. <https://doi.org/10.15446/ing.investig.v36n3.61596>.
- Prieto, A. (2013). *Windows Server 2008/R2. Administracion de Redes*. Createspace.
- ¿Qué es el monitoreo de red? (2022, abril 22). Cisco. https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html.
- ¿Qué es la seguridad de redes y cuál es su importancia? (s/f). UNIR México. Recuperado el 14 de julio de 2023, de <https://mexico.unir.net/ingenieria/noticias/seguridad-redes/>.
- ¿Qué es un respaldo de datos? (s/f). Quest.com. Recuperado el 14 de julio de 2023, de <https://www.quest.com/mx-es/what-is-data-backup/>.
- ¿Qué hace ICANN? (s/f). Ican.org. Recuperado el 24 de mayo de 2023, de <https://www.icann.org/resources/pages/what-2012-02-25-es>.
- Sepúlveda, M. (2020, noviembre 29). Ejercicio de calculo de VLSM - eClassVirtual - Cursos Cisco en línea. *eClassVirtual - Cursos Cisco en línea*. <https://eclassvirtual.com/ejercicio-de-calculo-de-vlsm/>.
- Sermersheim, J. (2006). *Lightweight directory access protocol (LDAP): The protocol* (J. Sermersheim, Ed.). RFC Editor.
- SERVIDOR LDAP*. (2009, noviembre 10). Tux Para todos. <https://comunicacionestux.wordpress.com/2009/11/10/servidor-ldap/>.
- Shepler, S., Eisler, M., & Noveck, D. (2010). *Network file system (NFS) version 4 minor version 1 protocol* (S. Shepler, M. Eisler, & D. Noveck, Eds.). RFC Editor.
- Shirley. (2021, diciembre 29). *Programar fácilmente un respaldo automático de Windows Server 2022 (3 maneras)*. Ubackup.com; AOMEI Backupper Utility. <https://www.ubackup.com/es/windows-server/programar-respaldo-automatico-de-windows-server-2022.html>.



Sistema de administración de red: Informe oficial de Mejores Prácticas. (2022, marzo 15). Cisco. https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15114-NMS-bestpractice.html.

SMTP: Protocolo para transferencia simple de correo. (2023, mayo 12). *Blog de VADAVO*. <https://www.vadavo.com/blog/smtp-protocolo-para-transferencia-de-correo/>.

Soluciones de seguridad empresarial. (s/f). Ibm.com. Recuperado el 14 de julio de 2023, de https://www.ibm.com/mx-es/security?utm_content=SRCWW&p1=Search&p4=43700057927479620&p5=e&gclid=CjwKCAjw5MOIBhBTEiwAAJ8e1odbY79W5s5nD5G_YpbjBaUebreYhLgn4g2y9ZpKF8izkP-zdjAm6BoCs2UQAvD_BwE&gclsrc=aw.ds.

Subredes VLSM paso a paso. (s/f). Direccionamiento IPv4 y Subredes. Recuperado el 11 de junio de 2023, de <https://arcadio.gq/subredes-vlsm-paso-a-paso.html>.

Tanenbaum, A. S. (2003). *Redes de computadoras*. Prentice Hall.

Teresa-Motiv. (s/f). *Herramientas de rendimiento de las cargas de trabajo de la red*. Microsoft.com. Recuperado el 12 de mayo de 2023, de <https://learn.microsoft.com/es-es/windows-server/networking/technologies/network-subsystem/net-sub-performance-tools>.

Tipos de dominios. (s/f). IONOS Digital Guide. Recuperado el 24 de mayo de 2023, de <https://www.ionos.mx/digitalguide/dominios/extensiones-de-dominio/tipos-de-dominios/>.

Tipos de Registros de Eventos en Windows. (s/f). Reydes.com. Recuperado el 13 de junio de 2023, de https://www.reydes.com/d/?q=Tipos_de_Registros_de_Eventos_en_Windows.

Trejo, D. R. (s/f). *Metodología de redes (FCAPS)*. Davidromerotrejo.com. Recuperado el 8 de mayo de 2023, de <http://www.davidromerotrejo.com/2013/04/metodologia-de-redes-fcaps.html>.

UNIDAD 4: SEGURIDAD BÁSICA. (s/f). Blogspot.com. Recuperado el 14 de julio de 2023, de <http://aru4santiagoadameromantaboda.blogspot.com/p/44-mecanismos-de-seguridad-fisica-y.html>.

What is DHCP and how does it work? (s/f). Afteracademy.com. Recuperado el 6 de junio de 2023, de <https://afteracademy.com/blog/what-is-dhcp-and-how-does-it-work/>.



- (S/f-a). Ingenieroseninformatica.org. Recuperado el 8 de mayo de 2023, de http://ingenieroseninformatica.org/recursos/tutoriales/ad_redes/index.php.
- (S/f-b). Microsoft.com. Recuperado el 8 de mayo de 2023, de <http://www.microsoft.com/windowsxp>.
- (S/f-c). Normas-apa.org. Recuperado el 10 de mayo de 2023, de <https://normas-apa.org/ya-te-enviamos-la-plantilla/>.
- (S/f-d). Uma.es. Recuperado el 15 de mayo de 2023, de <https://vgg.sci.uma.es/redes/servicio.html>.
- (S/f-e). Com.ar. Recuperado el 6 de junio de 2023, de <https://www.alegsa.com.ar/Dic/sasl.php#gsc.tab=0>.
- (S/f-f). Wnpower.com. Recuperado el 21 de junio de 2023, de <https://help.wnpower.com/hc/es/articles/360028218172-Utilizando-el-Visor-de-Eventos-en-Windows>.



6. GLOSARIO

DNS: El DNS (Domain Name System, Sistema de Nombres de Dominio) es un conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

DHCP: El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como “Dynamic Host Configuration Protocol” es un protocolo de red que utiliza una arquitectura cliente-servidor para asignar de manera dinámica las direcciones IP.

FCAPS: Es un acrónimo de Fault, Configuration, Accounting, Performance, Security (Falla, Configuración, Contabilidad, Desempeño, Seguridad) que son las categorías en las cuales el modelo ISO define las tareas de administración de redes cuyo objetivo es ayudar a los operadores de redes y a los proveedores de servicios a comprender fácilmente el funcionamiento de los sistemas de administración y monitorización de redes.

IMAP: Las siglas IMAP quiere decir: Internet Message Access Protocol (protocolo de acceso a mensajes de Internet) y es uno de los dos protocolos para recibir mensajes de email a través de internet.

ISO: Las siglas ISO (de las siglas en inglés: Open Systems Interconnection, o sea, “Organización Internacional de Normalización”), es un organismo responsable de regular un conjunto de normas para la fabricación, comercio y comunicación en todas las industrias y comercios del mundo. Este término también se le adjudica a las normas fijadas por el mismo organismo, para homogeneizar las técnicas de producción en las empresas y organizaciones internacionales.

LDAP: LDAP (Lightweight Directory Access Protocol) o también conocido como “Protocolo Ligero de Acceso a DirectorioS” es un protocolo de la capa de aplicación



TCP/IP que permite el acceso a un servicio de directorio ordenado y distribuido, para buscar cualquier información en un entorno de red.

MAC: La dirección MAC (Media Access Control, Control de Acceso al Medio), es un identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados. Una dirección MAC está formada por 48 bits representados generalmente por dígitos hexadecimales. Como cada hexadecimal equivale a cuatro binarios ($48:4=12$), la dirección acaba siendo formada por 12 dígitos agrupados en seis parejas separadas generalmente por dos puntos, aunque también puede haber un guión o nada en absoluto. De esta manera, un ejemplo de dirección MAC podría ser 00:1e:c2:9e:28:6b. Las primeras tres parejas, identifican al fabricante, y la otra mitad al modelo. Por ejemplo, los números 00:1e:c2 pertenecen al fabricante Apple Inc, mientras que los números 9e:28:6b determinan el modelo de dispositivo.

MTBF: Maximizar los Tiempos Medios entre Fallos (Mean Time Between Failures); es la media de tiempo entre fallos reparables de un producto tecnológico. La métrica se utiliza para controlar tanto la disponibilidad como la fiabilidad de un producto. Cuanto mayor sea el tiempo entre fallos, más fiable será el sistema.

MTTR: Minimizar los Tiempos Medios de Reparación (Mean Time to Repair); es un indicador de facilidad de mantenimiento (mide la facilidad en que un equipo puede repararse). Un Tiempo Medio de Reparación elevado puede indicar que la sustitución de un determinado activo es más barato o preferible que la reparación. Por otro lado, un MTTR más bajo puede sugerir que «usar hasta averiar» no es una mala opción para ese equipo. Para calcular el MTTR, divide el tiempo total de mantenimiento correctivo durante un determinado periodo por el número de acciones de mantenimiento correctivo realizadas.

NFS: Las sigas NFS (Network File System - Sistema de archivos de red) es un mecanismo para almacenar archivos en una red.



OSI: El Modelo OSI (de las siglas en inglés: Open Systems Interconnection, o sea, “Interconexión de Sistemas Abiertos”), es un modelo de referencia para los protocolos de comunicación de las redes informáticas o redes de computadores. Fue creado en la década de 1980 por la Organización Internacional de Normalización (ISO)

POP: El protocolo POP, siglas de Post Office Protocol (Protocolo de Oficina Postal), sirve para sincronizar el correo electrónico de Gmail con cualquier cliente de correo compatible, como Outlook, Thunderbird o Apple Mail.

PPDIOO: Metodología de Cisco (Preparar, Planear, Diseñar, Implementar, Operar y Optimizar); cuyo enfoque principal es definir las actividades mínimas requeridas por tecnología y complejidad de red con el fin de brindar el mejor servicio a los clientes para optimizar el funcionamiento del ciclo de vida de su red.

SASL: Las siglas SASL (Simple Authentication and Security Layer, Autenticación Simple y Capa de Seguridad) es un protocolo que se utiliza para añadir soporte de autenticación a los protocolos de conexión.

SMTP: SMTP son las siglas de Simple Mail transfer Protocol, “Protocolo Simple de Transferencia de Correo” y es un protocolo de red utilizado en el envío y recepción de correos electrónicos.

SNMP: El SNMP (Simple Network Management Protocol, Protocolo Simple de Administración de Redes); es un protocolo que permite monitorear y controlar redes que operan sobre TCP/IP, además de permitir capturar y alterar información de la red, aunado a esto el administrador de red puede utilizar este protocolo para diagnosticar y corregir problemas en la red utilizando un host remoto o host administrativo.

SSH: El protocolo SSH (Secure Shell) tiene la función de preservar la seguridad de los códigos en Internet con la criptografía de conexiones.



TI: Tecnologías de la Información, es el proceso de creación, almacenamiento, transmisión y percepción de la información y los métodos de aplicación de dichos procesos.

TMN: Red de Telecomunicaciones de Gestión (Telecommunications Management Network)

Es una arquitectura cuyo objetivo es proporcionar funciones de gestión y comunicaciones para la operación, administración y mantenimiento de una red de telecomunicaciones y provisionamiento de sus servicios en un entorno de múltiples fabricantes.