



MINISTERIO
DE TRABAJO
Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO
DE EMPLEO ESTATAL
SEPE
SERVEI PÚBLIC
D'Ocupació Estatal



MINISTERIO
DE EDUCACIÓN, FORMACIÓN PROFESIONAL
Y DEPORTES



**Generalitat
de Catalunya**

SOC

Servei d'Ocupació de Catalunya



SPAIN

Gestión de servicios en el sistema informático.

IFCT0109 – Seguridad informática

MF0490_3 (90 horas)

Confección del proceso de monitorización de sistemas y comunicaciones

- Introducción
- Identificación de los dispositivos de comunicaciones
- Análisis de los protocolos y servicios de comunicaciones
- Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones
- Procesos de monitorización y respuesta
- Herramientas de monitorización de uso de puertos y servicios tipo sniffer
- Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti
- Sistemas de gestión de información y eventos de seguridad (SIM/SEM)
- Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)
- Resumen

Introducción

La gestión efectiva y la supervisión detallada de los sistemas de información son elementos importantes para facilitar una toma de decisiones acertada en cualquier organización. Paralelamente, el sistema de comunicaciones desempeña un papel importante, ya que es el encargado de asegurar que la información se distribuya correctamente y llegue a su destino. Por ello, una evaluación profunda y la monitorización de dicho sistema son esenciales para mantener la fluidez de la información, tanto interna como externa, y para evitar problemas relacionados con la seguridad de los datos.

Relevancia del Sistema de Comunicaciones en las Organizaciones

- Flujo de Información: Los sistemas de comunicaciones tienen la responsabilidad de asegurar el correcto envío y recepción de información.
- Monitoreo y Mejora Continua: La evaluación meticulosa y el monitoreo continuo son determinantes para asegurar el rendimiento y la integridad de los sistemas de comunicación.

Configuración de un Sistema de Comunicaciones Efectivo.

- Elección de Dispositivos Adecuados: Seleccionar los componentes de la red que se alineen con las necesidades de la organización.
- Ajuste de Configuraciones: Definir y aplicar configuraciones que promuevan un funcionamiento eficiente y seguro.
- Uso de Herramientas de Mejora: Implementar soluciones que incrementen la eficacia y confiabilidad de las comunicaciones.

Introducción

Seguridad en los Sistemas de Comunicaciones

La seguridad es un aspecto de suma importancia por:

- Exposición a Riesgos Externos: Las conexiones con entidades fuera de la organización presentan potenciales riesgos de seguridad.
- Protección contra Intrusiones: Es imprescindible establecer defensas robustas para minimizar el riesgo de accesos indebidos y ciberataques.
- Adopción de Prácticas Seguras: Establecer y mantener prácticas de seguridad para proteger la integridad de la información y los activos de la empresa.

Identificación de los dispositivos de comunicaciones

Los dispositivos de comunicación constituyen una parte fundamental de las redes informáticas, permitiendo la interacción y el intercambio de información entre distintos nodos o computadoras. Estos dispositivos se categorizan en equipos de red, medios de comunicación y conectores, cada uno desempeñando roles específicos dentro de la estructura de la red.

Equipos de Red

- Servidores: Son nodos dedicados a suministrar datos en respuesta a las solicitudes de otros nodos denominados clientes. Funcionan como centros de distribución de información dentro de la red.
- Ordenadores: Actúan como puntos de origen o destino para la transmisión de datos. Cualquier computadora dentro de la red tiene la capacidad de enviar o recibir información, lo que facilita una comunicación bidireccional entre los usuarios.



Identificación de los dispositivos de comunicaciones

Medios de Comunicación

- Módems y ONTs: dispositivos de terminación de red que funcionan como puente entre la red de comunicaciones de un proveedor de servicios y los dispositivos finales del usuario. Ambos convierten las señales recibidas desde la red externa a un formato utilizable por los dispositivos domésticos o de oficina, y viceversa, permitiendo la comunicación bidireccional entre el usuario y la red.
- Tarjetas de Interfaz de Red (NIC): Proporcionan la conexión física entre el ordenador y el cable de red, siendo cruciales para mantener la red local interconectada y facilitar la transferencia de datos a alta velocidad.
- Concentradores (Hubs) y Conmutadores (Switches): Mientras los hubs permiten la interconexión básica entre múltiples dispositivos, distribuyendo señales entre sus puertos, los switches realizan esta tarea de manera más eficiente, dirigiendo datos específicamente al destinatario adecuado y mejorando el rendimiento de la red.
- Repetidores y Puentes (Bridges): Los repetidores amplifican y regeneran la señal en la red, mientras que los puentes conectan segmentos de red, actuando como elementos que filtran y encaminan datos entre redes con diferentes protocolos o topologías.
- Enrutadores (Routers): Encargados de dirigir el tráfico de datos dentro de la red y hacia otras redes, utilizando protocolos para determinar la ruta más eficiente para la entrega de la información.
- Pasarelas (Gateways): Facilitan la comunicación entre redes que utilizan diferentes protocolos, traduciendo la información de un sistema a otro para asegurar una comunicación fluida.

Identificación de los dispositivos de comunicaciones

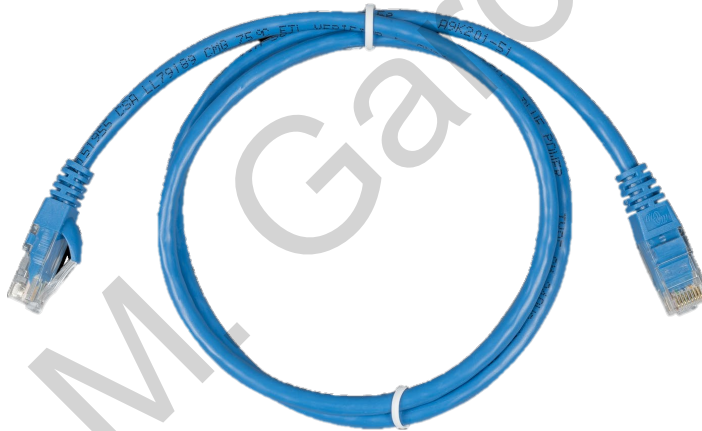
Medios de Comunicación



Identificación de los dispositivos de comunicaciones

Conectores

- Sistemas de Cableado: Incluyen tanto el cableado estructurado convencional como el cableado de fibra óptica, este último preferido en entornos que requieren alta velocidad de transmisión y resistencia a interferencias electromagnéticas.
- Enlaces Inalámbricos: Ofrecen la capacidad de transmitir datos a través de ondas electromagnéticas, eliminando la necesidad de cableado físico y brindando mayor flexibilidad en la configuración de la red.



5G

Análisis de los protocolos y servicios de comunicaciones

Introducción

Los servicios y protocolos de comunicaciones constituyen la base sobre la cual se edifica el intercambio de información en las redes de ordenadores. Un servicio de comunicación se refiere a la finalidad para la cual se destina la información que un dispositivo recibe. Para lograr una comunicación efectiva entre diferentes entidades y transmitir información, es imperativo seguir un conjunto estandarizado de normas y reglas, conocido como protocolo.

Protocolos de Comunicación

Un protocolo de comunicación establece cómo debe ser enviada, recibida y procesada la información dentro de una red. Los protocolos garantizan el flujo coherente de información entre dispositivos, incluso cuando estos operan bajo diferentes sistemas o tecnologías. Permiten que dos ordenadores en la misma red, pero con diferentes "lenguajes" de comunicación, puedan entenderse y compartir datos. Esto se logra mediante la adopción de un "lenguaje" común o protocolo entre los dispositivos. Aunque existen múltiples protocolos, con variadas características y propósitos, la mayoría comparte ciertas propiedades fundamentales:

- Detección de la Conexión: Identifica si la conexión se realiza a través de medios cableados o inalámbricos.
- Inicio de Comunicación (Handshaking): Define los pasos preliminares para empezar a comunicarse entre dispositivos.
- Negociación de Características: Acuerda cómo se iniciarán y finalizarán los mensajes, y cómo se negociarán las características de la conexión.
- Formato de Mensajes: Estipula cómo se deben formatear los mensajes para su correcta interpretación.
- Corrección de Errores: Determina el método para manejar mensajes erróneos o corruptos y la respuesta ante la pérdida de conexión.
- Seguridad de la Comunicación: Incluye estrategias como la autenticación y el cifrado para proteger la información intercambiada.
- Construcción de la Red Física y Conexión de Ordenadores: Describe cómo se estructura físicamente la red y cómo los dispositivos se conectan a ella.

Análisis de los protocolos y servicios de comunicaciones

Modelo OSI

El modelo OSI (Interconexión de Sistemas Abiertos) establecido por la Organización Internacional de Normalización (ISO) en 1978, es un marco conceptual utilizado para entender la estructura de comunicaciones en una red de ordenadores. Este modelo esencialmente divide las funciones de la red en siete capas distintas, desde la física hasta la aplicación, proporcionando un enfoque estandarizado para el diseño de arquitecturas de red.

La creación del modelo OSI se fundamentó en varios principios clave:

- Abstracción: Cada capa representa un nivel de abstracción distinto, simplificando la complejidad de las funciones de la red.
- Especialización: Las funciones de cada capa se definen claramente, con el objetivo de estandarizar los protocolos y las interfaces de comunicación.
- Optimización del Número de Capas: El modelo busca equilibrar la simplicidad y la complejidad, agrupando las funciones de la red de manera que el modelo sea ni demasiado granular ni demasiado abstracto.
- Interoperabilidad: Los límites entre las capas están diseñados para maximizar la eficiencia en la transmisión de datos y facilitar la interacción entre capas mediante interfaces definidas.

Análisis de los protocolos y servicios de comunicaciones

Modelo OSI

Las Siete Capas del Modelo OSI

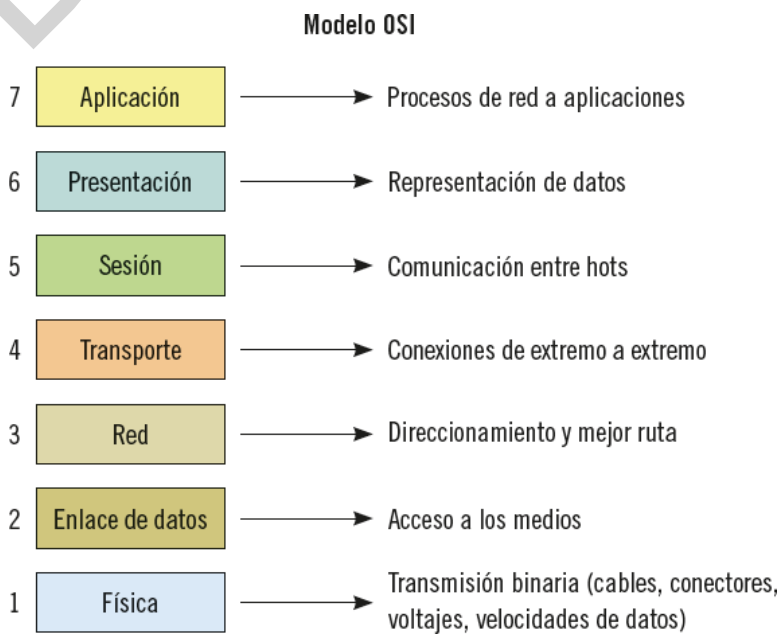
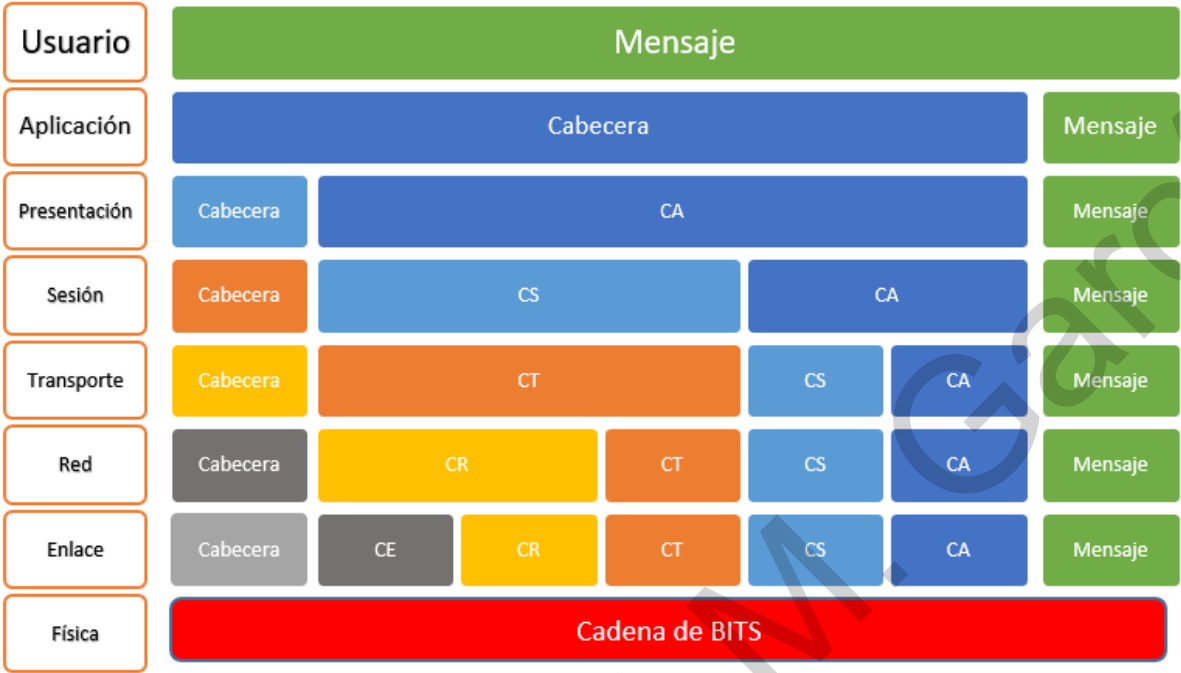
- Física: Se ocupa de la transmisión y recepción de la información cruda a través del medio físico, incluyendo especificaciones de cables, conectores y señales eléctricas.
- Enlace de Datos: Gestiona la conexión, la transmisión segura de datos entre dos puntos de una red y la detección y corrección de errores.
- Red: Responsable del enrutamiento de paquetes de datos entre distintas redes, asegurando su llegada desde el origen hasta el destino.
- Transporte: Proporciona la transferencia de datos entre puntos finales, asegurando la entrega correcta y en orden de los mismos.
- Sesión: Facilita el establecimiento, gestión y terminación de sesiones entre aplicaciones en diferentes dispositivos, manteniendo la conexión para una comunicación continua.
- Presentación: Traduce los datos entre el formato que la red requiere y el que es utilizado por las aplicaciones, incluyendo la compresión y cifrado de datos.
- Aplicación: Permite el acceso a servicios de red para aplicaciones de usuario final, definiendo protocolos para el intercambio de datos.

Cada una de estas capas funciona de manera independiente, pero interactúa con las capas adyacentes a través de interfaces claramente definidas, asegurando la cohesión y la eficacia en el procesamiento y la transmisión de datos.

Análisis de los protocolos y servicios de comunicaciones

Modelo OSI

Las Siete Capas del Modelo OSI (Encapsulamiento)



Análisis de los protocolos y servicios de comunicaciones

Modelo TCP/IP

La arquitectura TCP/IP, establecida en la década de 1970 por el Departamento de Defensa de los Estados Unidos, es fundamental en la historia de la informática, sirviendo como base para el desarrollo de la Internet. A diferencia del modelo OSI, que fue conceptualizado por la Organización Internacional de Normalización (ISO) y presenta una estructura de siete capas, la arquitectura TCP/IP se organiza en cuatro capas.

Este modelo no solo detalla un conjunto de directrices para el diseño e implementación de protocolos de red, sino que también especifica cómo deben ser formateados, direccionados, transmitidos, y recibidos los datos dentro de una red.

Comparación entre TCP/IP y OSI

Capas del TCP/IP:

- Acceso al Medio: Se enfoca en las rutinas de acceso al medio físico, análoga a las capas física y de enlace de datos del modelo OSI.
- Internet: Gestiona el enrutamiento de información, comparable a la capa de red del modelo OSI.
- Transporte: Abarca los servicios de entrega de datos entre nodos, similar a la capa de transporte en OSI.
- Aplicación: Incluye procesos y aplicaciones que usan la red, englobando las funciones de las capas de sesión, presentación y aplicación del modelo OSI.

Análisis de los protocolos y servicios de comunicaciones

Modelo TCP/IP

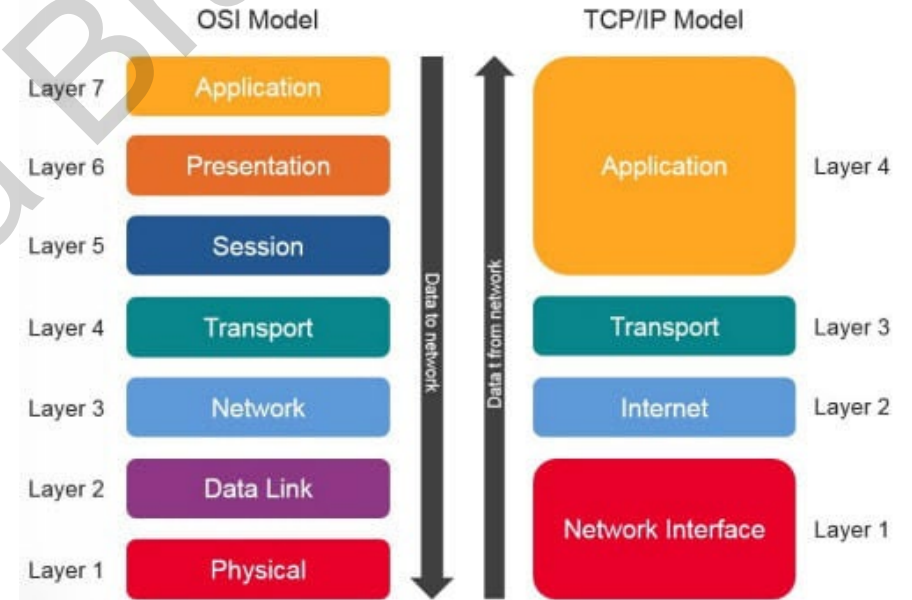
Comparación entre TCP/IP y OSI

Diferencias Principales:

- Estructura Conceptual: Mientras el modelo OSI se basa en una división clara de servicios, interfaces y protocolos, el modelo TCP/IP se centra más en la descripción práctica de los protocolos existentes.
- Independencia de Protocolos: Los protocolos en el modelo OSI están más aislados y definidos de manera independiente en comparación con TCP/IP.
- Desarrollo: OSI fue diseñado teóricamente antes de la creación de protocolos específicos, mientras que TCP/IP se desarrolló basándose en la práctica y necesidades reales, describiendo protocolos ya implementados.
- Simplicidad: TCP/IP es percibido como más simple por tener menos capas que OSI.

Importancia Práctica de TCP/IP

A pesar de las diferencias y la mayor simplicidad estructural de TCP/IP en comparación con OSI, la arquitectura TCP/IP ha ganado una amplia adopción práctica, convirtiéndose en el estándar de facto para la comunicación en redes, incluida Internet. El modelo OSI, por otro lado, se mantiene como un referente teórico importante para la comprensión de las redes de comunicaciones y la estandarización de los protocolos de red.



Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

Introducción

La arquitectura TCP/IP es fundamental en la infraestructura de comunicaciones moderna, especialmente en Internet. Constituida por cuatro capas esenciales, esta arquitectura proporciona servicios cruciales para la transmisión eficiente de la información. Entre estos servicios se incluyen el control de errores, la gestión del flujo de datos, la fragmentación y reensamblaje de ficheros, la gestión de conexiones, el direccionamiento mediante direcciones IP, y la multiplexación, que permite la coexistencia de múltiples sesiones en una única conexión.

Modelo TCP/IP

Compuesto por el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP), el TCP/IP abarca además otros protocolos y aplicaciones, siendo la piedra angular de Internet. Facilita la conexión entre dispositivos con distintos sistemas operativos a través de la segmentación de datos en paquetes, que incluyen tanto información de control como los datos propiamente dichos.

Parámetros de Configuración y Funcionamiento

- TCP: Este protocolo de la capa de transporte garantiza la entrega precisa y ordenada de los paquetes de datos, asegurando que el contenido enviado sea exactamente el recibido.
- IP: Actuando en la capa de red, el IP posibilita la ejecución de aplicaciones sobre redes interconectadas sin importar el hardware subyacente. Asigna una dirección IP única a cada dispositivo conectado a la red, facilitando su identificación y comunicación.

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

Introducción

Modelo TCP/IP

Direccionamiento IP

- Direcciones IP Fijas: Son comunes en sitios de Internet que requieren una conexión constante, proporcionando una identificación permanente y única en la red. (Fijas, dinámicas, públicas y privadas)
- IPv4 vs. IPv6: La versión 4 del protocolo IP (IPv4) ha sido el estándar durante años, pero su limitada capacidad de direcciones ha llevado al desarrollo y gradual implementación de IPv6, que ofrece un espacio de direccionamiento prácticamente ilimitado.

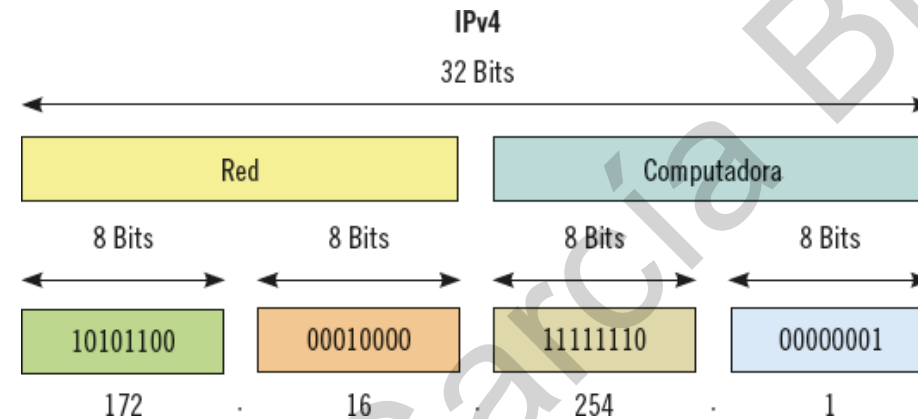
Importancia de IPv6

La transición de IPv4 a IPv6 es un aspecto crucial en la evolución de Internet y las redes de comunicaciones. IPv6 no solo resuelve el problema de agotamiento de direcciones de IPv4 sino que también introduce mejoras significativas en términos de eficiencia de enrutamiento, seguridad y configuración automática de dispositivos.

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

IPv4

Este protocolo estructura las direcciones IP en 32 bits divididos en cuatro octetos, cada uno representando un número decimal entre 0 y 255. Esta estructura permite una amplia, aunque limitada, asignación de direcciones únicas en toda la red de Internet.



Estructura de Dirección IPv4

Las direcciones IPv4 constan de dos segmentos principales: el identificador de la red y el identificador del equipo (host) dentro de esa red. La distribución de los bits entre estos dos identificadores define varias clases de direcciones IP:

- Clase A: Reserva el primer octeto para la identificación de la red y los tres restantes para los hosts.
- Clase B: Utiliza los dos primeros octetos para la red y los dos últimos para los hosts.
- Clase C: Asigna tres octetos para la red y uno para los hosts.
- Clase D: Se dedica a las direcciones IP para transmisiones multicast.
- Clase E: Se reserva para usos experimentales y de investigación.

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

IPv4

Parámetros Adicionales de Configuración

- Máscara de Subred: Esencial para distinguir la porción de la dirección IP que corresponde a la red de la que pertenece al host, compuesta también por 32 bits. Los bits que identifican la red se marcan con un '1', y los bits del host con un '0'.
- Dirección de Red: Define la red a la que pertenece un dispositivo, donde todos los bits de host son '0'.
- Dirección Broadcast: Utilizada para enviar paquetes de datos a todos los hosts dentro de una red específica. Todos los bits del host en esta dirección se configuran como '255' (siempre que la red no se encuentre segmentada /subneteadada)
- Dirección IP de la Puerta de Enlace: Corresponde al router de la red, facilitando la comunicación entre diferentes redes.
- Dirección de Bucle Local (Loopback): Direcciones "127.x.x.x" reservadas para designar la máquina del usuario, útiles para pruebas de conectividad interna.

Transición hacia IPv6

Dado el agotamiento de las direcciones IPv4, la versión IPv6 ha sido desarrollada para proporcionar un espacio de direccionamiento prácticamente ilimitado, gracias a su estructura de 128 bits. IPv6 no solo aborda la escasez de direcciones sino que también introduce mejoras en la eficiencia del enrutamiento, seguridad y autoconfiguración.

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

IPv4

Clase	Bits del Primer Octeto	Descripción / Uso	Pertenencia a clase definido por:	Identificación de red Núm. redes	Máscara de red Rango Privado Publico Reservado	Núm. de hosts por red
A	0xxxxxx	Red grande	Primer bit es 0.	7 bits de 24 bits $2^7 = 128$ redes.	255.0.0.0 0.0.0.0 a 127.255.255.255 10.0.0.0 a 10.255.255.255 Resto público 127.0.0.0 a 127.255.255.255 (loopback)	$2^{24} - 2$ (Id de red y Broadcast) 16.777.214 hosts por red
B	10xxxxxx	Red mediana	Primeros dos bits son 10.	14 bits de 24 $2^{14} = 16.384$ redes.	255.255.0.0 128.0.0.0 a 191.255.255.255 172.16.0.0 a 172.31.255.255 Resto público Ninguna reserva	$2^{16} - 2$ (Id de red y Broadcast) 65.534 hosts por red
C	110xxxxx	Red pequeña	Primeros tres bits son 110.	21 bits de 24 $2^{21} = 2.097.152$ redes	255.255.255.0 192.0.0.0 a 223.255.255.255 192.168.0.0 a 192.168.255.255 Resto público Ninguna reserva	$2^8 - 2$ (Id de red y Broadcast) 254 hosts por red
D	1110xxxx	Multicast	Primeros cuatro bits son 1110.		Rango reservado para multicast: 224.0.0.0 a 239.255.255.255	
E	1111xxxx	Experimental	Primeros cuatro bits son 1111.		Rango reservado para investigación: 240.0.0.0 a 255.255.255.255	

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

Configuración de una red IPv4

Preparación de Hardware y Software

- Instalación de Controladores: Es crucial instalar los controladores de los componentes de la red para asegurar su correcta detección y funcionamiento en el sistema.
- Selección del Protocolo: Generalmente, el protocolo TCP/IP es la opción predeterminada, dado su uso extendido en redes.

Definición de Parámetros del Protocolo TCP/IP

- Dirección de Red IP: Asignar una dirección IP única a cada dispositivo para su identificación en la red.
- Máscara de Red: Establecer la máscara de subred que determina el segmento de red al que pertenece el dispositivo.
- Puerta de Enlace: Indicar la dirección IP del router o dispositivo que conecta la red local con otras redes, como Internet.
- Dirección de Broadcast: Configurar la dirección utilizada para enviar mensajes a todos los dispositivos de la red. Derivado de la segmentación y se determina utilizando la máscara de entrada.
- Rango de Direcciones IP para Hosts: Definir el conjunto de direcciones IP disponibles para asignar a los dispositivos en la red.

Configuración de Recursos y Servicios Compartidos

- Recursos Compartidos: Carpetas, impresoras y otros dispositivos que serán accesibles para los usuarios de la red.
- Servicios de Red: Implementar servicios como servidores web o FTP según las necesidades de la organización.

Seguridad de la Red

- Restricciones de Acceso: Aplicar políticas de acceso para controlar quién puede acceder a ciertos recursos y servicios.
- Control de Accesos: Implementar medidas como listas de control de acceso (ACLs) y autenticación para proteger la red.

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

Configuración de una red IPv4

Consideraciones sobre Direcciones IP

Es importante distinguir entre direcciones IP públicas fijas y dinámicas:

- Direcciones IP Fijas: Asignadas de manera permanente por el proveedor de servicios de Internet, o por el administrador de la red interna, manteniendo la misma dirección IP a lo largo del tiempo.
- Direcciones IP Dinámicas: Asignadas temporalmente desde un pool de direcciones disponibles, cambiando con cada nueva conexión a Internet (dependiendo del proveedor de servicios) o dentro de la red interna (asignación por servidor DHCP o router)

La mayoría de los hogares y pequeñas empresas optan por direcciones IP dinámicas debido a su conveniencia y coste reducido. Sin embargo, las direcciones IP fijas pueden ser necesarias para ciertas aplicaciones o servicios empresariales que requieren una ubicación o conexión constante a Internet.

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

IPv6

IPv6, la sexta versión del Protocolo de Internet, fue diseñada para superar las limitaciones de IPv4, especialmente la escasez de direcciones IP disponibles. A diferencia de IPv4, que utiliza direcciones de 32 bits, IPv6 emplea direcciones de 128 bits, ofreciendo un espacio de direccionamiento prácticamente ilimitado.

Esto permitiría asignar una dirección única a cada dispositivo en Internet, facilitando la conectividad directa y eliminando la necesidad de técnicas como la Traducción de Direcciones de Red (NAT).

Estructura de una Dirección IPv6

Una dirección IPv6 típica se representa en ocho grupos de cuatro dígitos hexadecimales, separados por dos puntos.

(por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Los ceros a la izquierda en cada bloque pueden omitirse para simplificar la notación, y una sucesión de bloques con valor cero puede representarse por "::" una sola vez en la dirección para acortarla aún más.

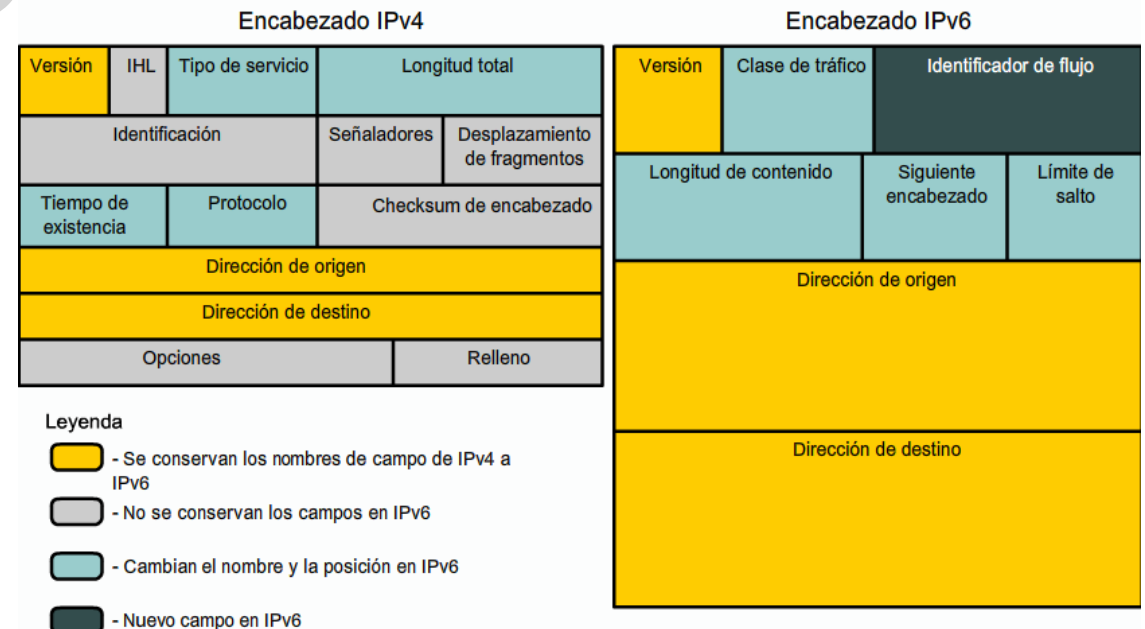
2001:db8:85a3::8a2e:370:7334

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

IPv6

Características Clave de IPv6

- Espacio de Direccionamiento Expandido: Con direcciones de 128 bits, IPv6 puede soportar 2^{128} direcciones únicas, un elevadísimo número que satisface las necesidades de direccionamiento a largo plazo de Internet.
- Autoconfiguración: IPv6 permite que los dispositivos configuren automáticamente su propia dirección IP sin necesidad de un servidor DHCP, facilitando la gestión de la red.
- Seguridad Integrada: IPv6 fue diseñado con la seguridad en mente, incluyendo soporte nativo para el Protocolo de Seguridad de Internet (IPsec), que proporciona confidencialidad, autenticación e integridad de los datos.
- Soporte para Nuevos Servicios: Las características de IPv6, como la asignación de múltiples direcciones IP a un solo dispositivo y la optimización para la transmisión de paquetes multimedia, permiten el desarrollo de nuevos servicios y aplicaciones en Internet.
- Simplificación del Encabezado: El encabezado de un paquete IPv6 es más simple que el de IPv4, lo que mejora el procesamiento de paquetes y la eficiencia del enrutamiento.



Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

IPv6

Las direcciones IPv6 se clasifican en varios tipos, cada uno con sus propósitos y ámbitos de aplicación específicos. Entre estas clasificaciones, las direcciones Unicast Globales y las direcciones Únicas Locales juegan roles similares a las direcciones públicas y privadas de IPv4, respectivamente.

Direcciones Unicast Globales (Públicas)

Las direcciones Unicast Globales en IPv6 son equivalentes a las direcciones IP públicas en IPv4. Están diseñadas para ser utilizadas en Internet y pueden ser enrutadas globalmente. Su estructura incluye un prefijo global, que identifica la red, y un identificador de interfaz, que identifica el dispositivo dentro de esa red.

Prefijo: Generalmente, los primeros 48 bits son el prefijo global, seguido de 16 bits para el identificador de subred, dejando 64 bits para el identificador de interfaz del host.

Ejemplo: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Estas direcciones son asignadas por autoridades de asignación de números de Internet, como la IANA (Internet Assigned Numbers Authority) y sus registros regionales, asegurando su unicidad a nivel global.

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

IPv6

Direcciones Únicas Locales (Privadas)

Las Direcciones Únicas Locales (Unique Local Addresses, ULAs) en IPv6 cumplen un papel similar al de las direcciones privadas en IPv4, como las direcciones en los rangos 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16.

Las ULAs están destinadas al uso dentro de redes privadas y no son enrutables en Internet, pero pueden atravesar diferentes subredes dentro de una organización, lo que permite la comunicación interna segura y sin conflictos de direcciones en redes privadas o corporativas.

Prefijo Fc00::/8: Todas las direcciones ULAs comienzan con este prefijo, seguido de un identificador de subred y un identificador de interfaz.

Ejemplo: fc00:0db8:85a3:0000:0000:8a2e:0370:7334

A diferencia de IPv4, no hay necesidad de NAT (Network Address Translation) en IPv6, incluso para las direcciones ULAs, gracias a la abundancia de direcciones disponibles y al diseño inherente de IPv6 que facilita la autoconfiguración y la gestión de redes.

Principales parámetros de configuración y funcionamiento de los equipos de comunicaciones

IPv6

Otros Tipos de Direcciones IPv6

Además de las direcciones globales y locales únicas, IPv6 introduce varios otros tipos de direcciones para usos específicos, incluyendo:

- Direcciones de Enlace Local: Usadas para la comunicación entre dispositivos en la misma red física o segmento de red. No son enrutables más allá de su enlace local. (p.e. `fe80::1234:5678:9abc:def0`)
- Direcciones Multicast: Permiten la transmisión de paquetes a múltiples destinos en una sola operación.
`ff02::1:ff00:0001` (Multicast de todos los nodos en el enlace local)
`ff0e::2:fc00:0001` (Multicast para un grupo específico en un ámbito global)
- Direcciones Anycast: Son asignadas a múltiples interfaces, con el paquete enviado a la interfaz más cercana identificada por la dirección. (p.e. `2001:db8::1` (Asignada a dos routers en diferentes sitios para balanceo de carga))

Transición de IPv4 a IPv6

La transición de IPv4 a IPv6 implica desafíos significativos, ya que ambos protocolos no son directamente compatibles. Sin embargo, se han desarrollado varias estrategias para facilitar la coexistencia y transición gradual, incluyendo:

- Túneles: Encapsulan paquetes IPv6 dentro de paquetes IPv4 para su transporte a través de redes IPv4.
- Traducción de Direcciones de Protocolo: Convierte paquetes IPv6 en paquetes IPv4 y viceversa, permitiendo la comunicación entre redes que utilizan diferentes versiones del protocolo.
- Implementación Dual: Los dispositivos y servidores se configuran para soportar tanto IPv4 como IPv6 simultáneamente, garantizando la conectividad durante la transición.

Procesos de monitorización y respuesta

La monitorización de procesos permite mantener un control efectivo y optimizar los rendimientos. Este principio se extiende a los procesos de comunicación, donde la detección temprana de fallos y la supervisión de los elementos de la red son fundamentales para garantizar un servicio de calidad y satisfacer las necesidades de los usuarios.

Fases de la administración del rendimiento de la red

La administración del rendimiento de la red se divide en dos fases principales: monitorización y análisis de resultados.

Monitorización

La monitorización implica la recolección y análisis continuo de datos sobre el comportamiento de la red. Algunos aspectos clave que se observan durante este proceso incluyen:

- Utilización de enlaces: Se monitorea la cantidad de ancho de banda utilizado por cada enlace de área local, permitiendo identificar posibles cuellos de botella y optimizar el rendimiento de la red.
- Caracterización de tráfico: Se analizan los diferentes tipos de tráfico que circulan por la red para comprender los servicios de red más utilizados y establecer patrones de uso.
- Porcentaje de transmisión y recepción de información: Consiste en obtener información sobre los elementos de la red que más solicitudes hacen y atienden, lo cual es crucial para identificar los nodos más activos y distribuir eficientemente los recursos de red.
- Utilización de procesamiento: Se observa la carga de trabajo de los servidores para determinar el rendimiento de la CPU y garantizar un funcionamiento óptimo de las aplicaciones y servicios.

Procesos de monitorización y respuesta

Fases de la administración del rendimiento de la red

Análisis

Una vez recopilada la información, se procede al análisis detallado para identificar patrones y comportamientos relevantes, como:

- Tráfico inusual: El análisis de patrones de comportamiento permite detectar tráfico anómalo que podría indicar posibles ataques o problemas de rendimiento.
- Elementos principales de la red: Al observar el rendimiento de los elementos de red, se pueden identificar aquellos que generan mayor tráfico y requieren una supervisión más exhaustiva.
- Utilización elevada: Se monitorea la carga de trabajo en los enlaces para evitar la saturación y garantizar un rendimiento óptimo de la red.
- Control de tráfico: La implementación de herramientas de control de tráfico permite gestionar de forma proactiva la congestión y garantizar la disponibilidad de los servicios críticos.
- Calidad del servicio: La monitorización constante y el análisis de datos facilitan la entrega de servicios de alta calidad al garantizar la asignación adecuada de recursos y la priorización de servicios sensibles al tiempo, como la voz IP.

Es esencial emplear herramientas especializadas para la monitorización y respuesta, permitiendo una gestión eficiente de aspectos como el uso de puertos y servicios, la seguridad de sistemas, y la administración de elementos de red y filtrado.

Herramientas de monitorización de uso de puertos y servicios tipo sniffer

Las herramientas de monitorización de uso de puertos y servicios tipo **sniffer** son programas diseñados para capturar y analizar el tráfico de datos que circula a través de las redes. Estos programas son esenciales para la administración y la seguridad de las redes, ya que permiten a los administradores y profesionales de seguridad informática inspeccionar la información que se transmite entre dispositivos y equipos.

Una de las características distintivas de los sniffers es su capacidad para operar en modo promiscuo, el cual permite a una tarjeta de red capturar todo el tráfico que circula por ella, independientemente de si los datos están dirigidos a esa tarjeta o no. Esta funcionalidad es crítica para el análisis exhaustivo del tráfico de red, permitiendo a los usuarios acceder a toda la información intercambiada entre computadoras dentro de una red.

Sin embargo, el uso de sniffers también plantea significativos riesgos de seguridad. Si bien estas herramientas pueden aumentar la seguridad de una red local al permitir la detección de problemas y vulnerabilidades, también pueden ser utilizadas para fines malintencionados, como el acceso no autorizado a información confidencial y la comisión de delitos informáticos. Por lo tanto, es crucial un manejo responsable y ético de estas herramientas.

Entre las funcionalidades más valiosas de los sniffers se incluyen:

- Análisis de fallos: Identificación y diagnóstico de problemas en la red.
- Medición del tráfico de datos: Detección de cuellos de botella y análisis de la utilización de la red.
- Captura de credenciales: Registro de nombres de usuario y contraseñas que se transmiten sin cifrar.
- Análisis de aplicaciones cliente-servidor: Inspección del tráfico de datos reales que se transmite por la red para fines de desarrollo de software y protocolos.

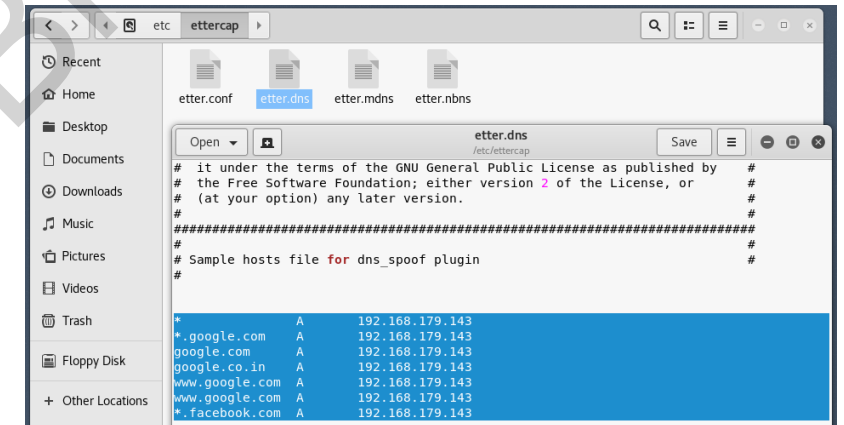
Herramientas de monitorización de uso de puertos y servicios tipo sniffer

Entre las herramientas sniffer más utilizadas se encuentran:

Ettercap: Interceptor/sniffer para redes LAN con capacidad para modificar el tráfico de datos, soporta activamente diversos protocolos y es compatible tanto con Linux como con Windows.

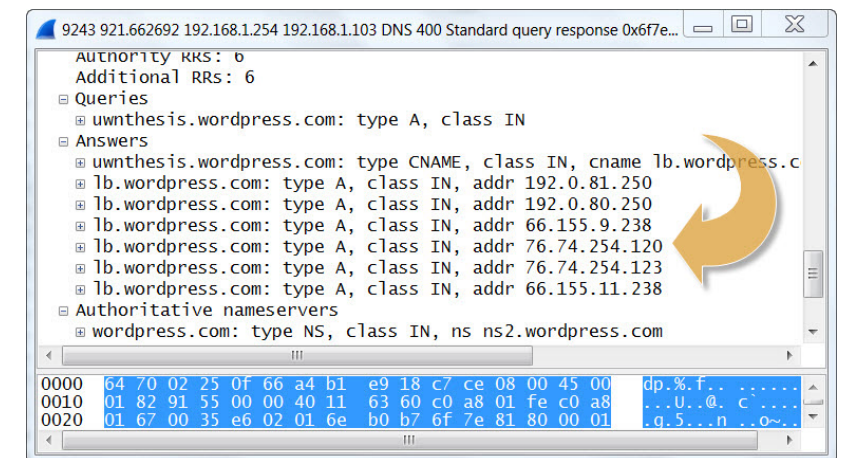
Destaca por:

- Ataques MITM: Puede realizar ataques de intermediario para interceptar y modificar el tráfico entre dos partes sin que ellas se den cuenta.
- Detección de hosts y análisis de sesión: Capaz de escanear la red en busca de hosts vivos y sesiones activas.
- Soporte de plugins: Permite ampliar sus capacidades mediante el uso de plugins, algunos de los cuales pueden automatizar tareas específicas o añadir nuevas funcionalidades.
- Soporte para múltiples sistemas operativos: Funciona en Linux, macOS y Windows, lo que le permite ser utilizado en una amplia variedad de entornos de red.



TCPDump: Herramienta de línea de comandos que facilita la captura y análisis de paquetes de red. Aunque primordialmente diseñada para sistemas Unix y Linux, su variante **WinDump** permite su uso en entornos Windows. **Destaca por:**

- Flexibilidad de captura: Los usuarios pueden definir filtros complejos que especifican exactamente qué tráfico capturar, basado en una variedad de atributos como dirección IP, tipo de protocolo y puerto.
- Formato de salida detallado: La salida de TCPDump es extremadamente detallada, proporcionando una vista a bajo nivel de los paquetes capturados, lo cual es crucial para el análisis técnico profundo.
- Compatibilidad amplia: TCPDump puede usarse en casi cualquier sistema operativo basado en Unix, incluidos Linux, BSD y macOS. Para entornos Windows, WinDump ofrece funcionalidades similares.
- Herramienta ligera: A diferencia de otras herramientas de análisis de red, TCPDump tiene requisitos mínimos de sistema y puede ejecutarse en hardware con recursos limitados.



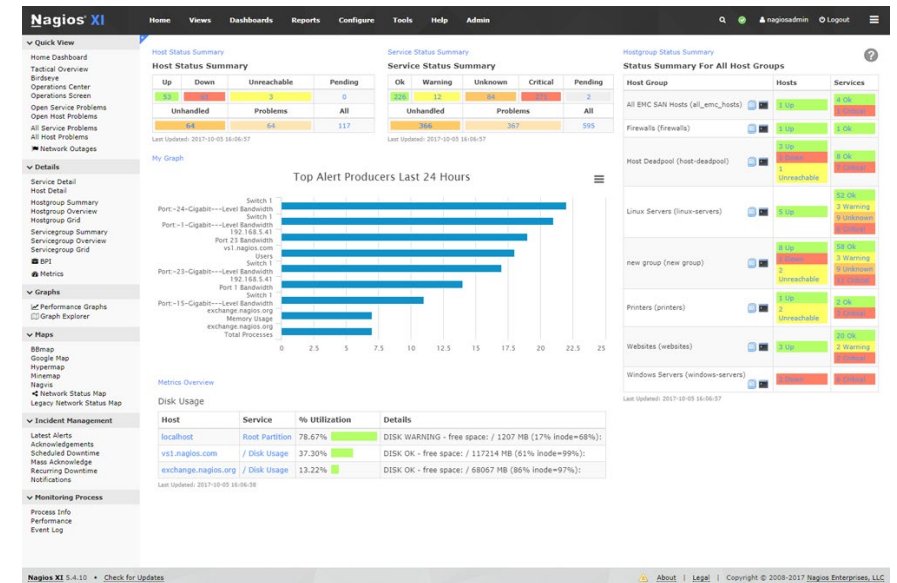
Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti

Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti

Nagios

Solución más compleja en términos de configuración pero destaca por su robustez y potencia. Originalmente diseñada para sistemas basados en GNU/Linux, Nagios es ampliamente aplicable en diferentes entornos UNIX. Sus principales características incluyen:

- Monitorización exhaustiva de servicios de red (como SMTP, POP3, HTTP) y recursos del hardware.
- Funciona en una amplia variedad de sistemas operativos, asegurando una monitorización remota efectiva.
- Flexibilidad para programar plugins específicos, adaptándose así a necesidades particulares.
- Sistema de notificaciones avanzado para alertar sobre problemas y sus resoluciones.
- Soporte para la implementación de monitores de hosts redundantes y visualización del estado de la red en tiempo real a través de su interfaz web.
- Generación de informes detallados y visualización de historiales de problemas.

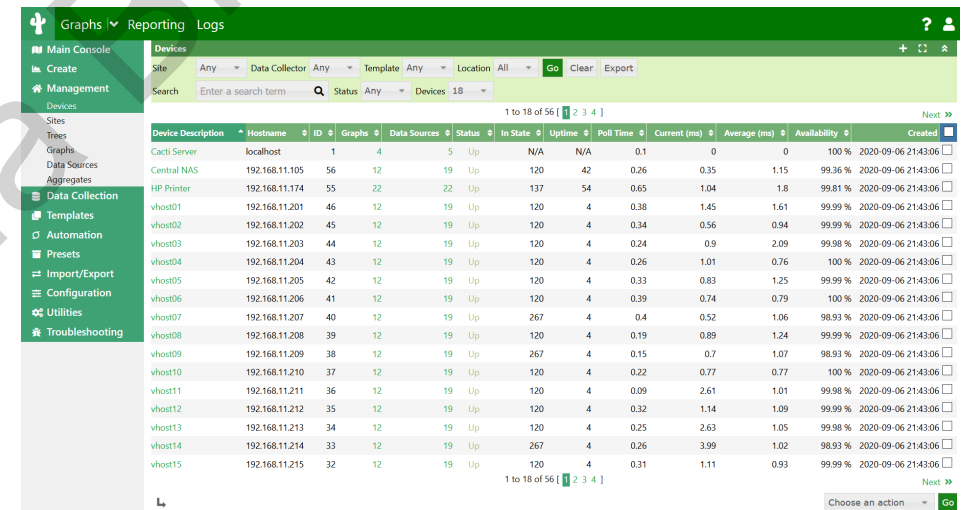


Herramientas de monitorización de sistemas y servicios tipo Hobbit, Nagios o Cacti

Cacti

Se enfoca en la visualización gráfica y el monitoreo estadístico de la red utilizando el protocolo SNMP. Ideal para administradores que requieren un seguimiento visual del rendimiento de la red, Cacti destaca por:

- Facilitar la monitorización y generación de gráficos estadísticos de dispositivos de red.
- Interfaz intuitiva y de fácil manejo.
- Configuración flexible del período de sondeo para ajustar la cantidad y precisión de los datos recopilados.
- Capacidad para manejar sondeos a múltiples hosts, optimizando el seguimiento de parámetros de red específicos.



Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime	Poll Time	Current (ms)	Average (ms)	Availability	Created
Cacti Server	localhost	1	4	5	Up	N/A	N/A	0.1	0	0	100 %	2020-09-06 21:43:06
Central NAS	192.168.11.105	56	12	19	Up	120	42	0.26	0.35	1.15	99.36 %	2020-09-06 21:43:06
HP Printer	192.168.11.174	55	22	22	Up	137	54	0.65	1.04	1.8	99.81 %	2020-09-06 21:43:06
vhost01	192.168.11.201	46	12	19	Up	120	4	0.38	1.45	1.61	99.99 %	2020-09-06 21:43:06
vhost02	192.168.11.202	45	12	19	Up	120	4	0.34	0.56	0.94	99.99 %	2020-09-06 21:43:06
vhost03	192.168.11.203	44	12	19	Up	120	4	0.24	0.9	2.09	99.98 %	2020-09-06 21:43:06
vhost04	192.168.11.204	43	12	19	Up	120	4	0.26	1.01	0.76	100 %	2020-09-06 21:43:06
vhost05	192.168.11.205	42	12	19	Up	120	4	0.33	0.83	1.25	99.99 %	2020-09-06 21:43:06
vhost06	192.168.11.206	41	12	19	Up	120	4	0.39	0.74	0.79	100 %	2020-09-06 21:43:06
vhost07	192.168.11.207	40	12	19	Up	267	4	0.4	0.52	1.06	98.93 %	2020-09-06 21:43:06
vhost08	192.168.11.208	39	12	19	Up	120	4	0.19	0.89	1.24	99.99 %	2020-09-06 21:43:06
vhost09	192.168.11.209	38	12	19	Up	267	4	0.15	0.7	1.07	98.93 %	2020-09-06 21:43:06
vhost10	192.168.11.210	37	12	19	Up	120	4	0.22	0.77	0.77	100 %	2020-09-06 21:43:06
vhost11	192.168.11.211	36	12	19	Up	120	4	0.09	2.61	1.01	99.98 %	2020-09-06 21:43:06
vhost12	192.168.11.212	35	12	19	Up	120	4	0.32	1.14	1.09	99.99 %	2020-09-06 21:43:06
vhost13	192.168.11.213	34	12	19	Up	120	4	0.25	2.63	1.05	99.98 %	2020-09-06 21:43:06
vhost14	192.168.11.214	33	12	19	Up	267	4	0.26	3.99	1.02	98.93 %	2020-09-06 21:43:06
vhost15	192.168.11.215	32	12	19	Up	120	4	0.31	1.11	0.93	99.99 %	2020-09-06 21:43:06

Sistemas de gestión de información y eventos de seguridad (SIM/SEM/SIEM)

Los Sistemas de Gestión de Información y Eventos de Seguridad (SIM/SIEM) forman parte de la estrategia de seguridad de una organización al ofrecer una plataforma integral para la gestión de la seguridad de la información. Estos sistemas se encargan de recopilar, analizar y correlacionar la información de eventos de seguridad de diversos dispositivos en la red, con el objetivo de detectar, prevenir y responder a incidentes de seguridad de manera eficaz.

Sistemas de Gestión de la Seguridad de la Información (SIM)

Sistemas diseñados para la supervisión y análisis retrospectivo de la seguridad, enfocados en la recolección, almacenamiento, y análisis de datos de seguridad. Estos sistemas crean un repositorio centralizado de información que facilita la correlación de eventos y la detección de patrones de comportamiento anómalos o potenciales amenazas a la seguridad. Entre las principales funciones de los SIM se incluyen:

- Recolección y almacenamiento de datos: Consolidan registros de eventos de seguridad (logs) de diversos dispositivos dentro de la red.
- Correlación y análisis: Analizan los datos recopilados para identificar patrones sospechosos o anomalías que podrían indicar una amenaza de seguridad.
- Centralización de la gestión de eventos: Ofrecen una plataforma unificada para la gestión de eventos de seguridad, facilitando la estandarización y priorización de respuestas a incidentes.
- Optimización de la detección de amenazas: Reducen el tiempo necesario para identificar y responder a ataques y vulnerabilidades, minimizando el impacto en la organización.
- Automatización: Automatizan la colección y análisis de eventos, reduciendo la carga de trabajo manual y mejorando la eficiencia de los procesos de seguridad.

Sistemas de gestión de información y eventos de seguridad (SIM/SIEM)

Sistemas de Gestión de Eventos de Seguridad (SEM)

Proporcionan capacidad para monitorizar en tiempo real y gestionar gestión de eventos de seguridad. A través de la recolección y el análisis de información proveniente de registros de seguridad de sistemas, equipos y dispositivos de la red, los SEM ofrecen una visión integral y actualizada de las actividades de seguridad, permitiendo a las organizaciones detectar y responder a incidentes con rapidez.

Funcionalidad de los SEM. Operan recopilando datos de eventos (logs) generados por dispositivos, protocolos y aplicaciones dentro de una red. Estos registros de eventos son listas cronológicas de las actividades detectadas por los sistemas de monitoreo, que incluyen tanto operaciones normales como posibles señales de alerta de incidentes de seguridad. El propósito de los SEM es procesar y analizar estos datos en tiempo real o casi en tiempo real, facilitando una respuesta ágil ante potenciales amenazas.

Beneficios de los SEM

- Centralización de registros: Ofrecen una interfaz unificada para acceder a los registros de eventos de toda la organización, mejorando la eficiencia en la gestión de la seguridad.
- Garantizan la integridad y seguridad de los datos de eventos, preservándolos de alteraciones no autorizadas o pérdidas accidentales.
- Facilitan la interpretación de la actividad de la red mediante visualizaciones gráficas, lo que simplifica la generación de informes de seguridad.
- Permiten configurar notificaciones automáticas ante eventos que cumplan con ciertos criterios predefinidos, acelerando la detección de incidentes.
- Pueden integrarse y gestionar eventos de una amplia variedad de entornos de sistema operativo, ampliando su aplicabilidad.
- Recuperación de registros: En situaciones de pérdida de datos, ya sea por bloqueo del sistema o eliminación, ofrecen mecanismos para recuperar la información perdida, asegurando la continuidad del monitoreo de seguridad.

Sistemas de gestión de información y eventos de seguridad (SIM/SIEM)

Sistemas de gestión de información y eventos de seguridad, SIEM

Son una solución integral en el ámbito de la seguridad cibernética, fusionando y ampliando las capacidades de los Sistemas de Gestión de la Seguridad de la Información (SIM) y los Sistemas de Gestión de Eventos (SEM). Estas plataformas avanzadas recopilan, almacenan y analizan los registros de actividad (logs) de todos los dispositivos monitorizados dentro de una red, ofreciendo una gestión de seguridad cohesiva y completa.

Funcionalidades Clave de los SIEM

- Detección de Anomalías y Amenazas: Capacidad para identificar comportamientos inusuales en la red que podrían indicar la presencia de amenazas cibernéticas o vulnerabilidades.
- Análisis Integral del Ataque: Proporciona visibilidad antes, durante y después de un ataque, permitiendo un entendimiento completo de las tácticas, técnicas y procedimientos (TTP) de los atacantes.
- Captura Completa de Paquetes: Almacena y analiza copias de los paquetes de datos que circulan por la red para una inspección detallada y análisis forense.
- Monitoreo del Comportamiento del Usuario: Evalúa el comportamiento de los usuarios dentro de la red, incluyendo el contexto de sus acciones, para detectar posibles abusos o actividades sospechosas.
- Cumplimiento Normativo: Ayuda a las organizaciones a cumplir con regulaciones y normativas vigentes, facilitando la generación de reportes y la auditoría de seguridad.
- Gestión de Riesgos: Proporciona información valiosa sobre la topología de red, vulnerabilidades, configuraciones de dispositivos y análisis de fallas para una mejor administración del riesgo.
- Correlación Avanzada de Eventos: Utiliza algoritmos complejos para correlacionar eventos de diferentes fuentes en tiempo real, mejorando la detección de incidentes y la priorización de vulnerabilidades.

Sistemas de gestión de información y eventos de seguridad (SIM/SIEM)

Con el avance tecnológico y la evolución constante de las amenazas cibernéticas, los SIEM han incorporado nuevas tecnologías y metodologías para reforzar la seguridad informática. Estos avances incluyen:

- Inteligencia Artificial y Aprendizaje Automático: Mejoran la detección de amenazas y la respuesta a incidentes mediante el análisis predictivo y la identificación de patrones complejos.
- Integración con Otras Soluciones de Seguridad: Los SIEM ahora se integran con sistemas de prevención de intrusiones, protección contra malware, y otras soluciones de seguridad para una respuesta más coordinada a las amenazas.
- Visibilidad Ampliada de la Red: Extienden la monitorización más allá de los límites tradicionales de la red, abarcando entornos en la nube, dispositivos móviles y sistemas de IoT.

En el entorno actual de ciberseguridad, las soluciones globales de SIEM (Security Information and Event Management) juegan un papel crucial al proporcionar una gestión integrada de la seguridad que abarca tanto la gestión de la información de seguridad (SIM) como la gestión de eventos de seguridad (SEM).

Estas soluciones están diseñadas para satisfacer las necesidades complejas de las organizaciones, ofreciendo desde la agregación de logs hasta análisis avanzados y gestión de incidentes. Debido a la diversidad en el enfoque y las capacidades de estas plataformas, es fundamental que las organizaciones evalúen sus necesidades específicas de seguridad para seleccionar la solución SIEM que mejor se alinee con sus objetivos.

Sistemas de gestión de información y eventos de seguridad (SIM/SIEM)

IBM Tivoli Security Information and Event Manager

Ejemplo destacado de una solución SIEM que combina funciones avanzadas de SIM y SEM. Algunas de sus características clave incluyen:

- Consola de Gestión Basada en la Web: Facilita el acceso y la gestión de la seguridad de la información de manera centralizada, permitiendo a los usuarios supervisar y gestionar incidentes de seguridad de forma eficiente.
- Seguimiento y Gestión Priorizada de Incidentes: Permite la identificación y el manejo prioritario de incidentes en curso, asegurando una respuesta rápida a las amenazas más críticas.
- Agregación Automática de Logs: Recopila y consolida automáticamente los registros de eventos de seguridad de diversos sistemas y dispositivos dentro de la red.
- Cuadro de Mando Unificado: Ofrece una visión integrada del análisis de los registros, facilitando la detección de patrones y la toma de decisiones basada en datos.
- Acceso Privilegiado para Auditoría: Proporciona capacidades de monitorización y auditoría que permiten el seguimiento de incidentes sin alertar a los posibles autores, mejorando la investigación y la respuesta a incidentes.

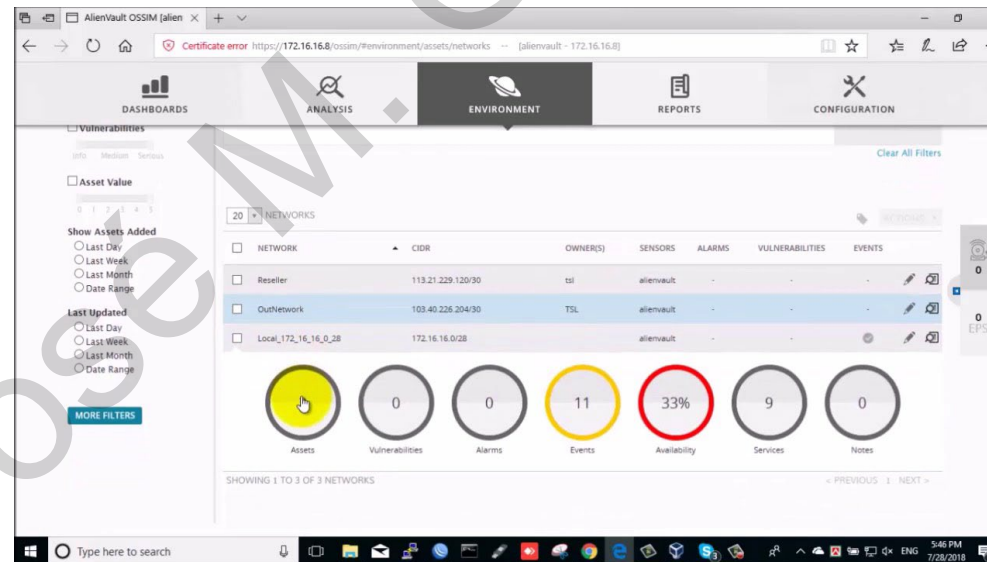
La riqueza de patentes y la innovación continua de IBM respaldan el desarrollo y la eficacia de esta herramienta, reafirmando su posición como líder en el mercado de soluciones de seguridad.

Sistemas de gestión de información y eventos de seguridad (SIM/SIEM)

OSSIM: Open Source Security Information Management

Por otro lado, OSSIM ofrece una alternativa gratuita y funcional para la gestión de la seguridad de la red. Características destacadas de OSSIM incluyen:

- Motor de Correlación: Analiza los eventos de seguridad recopilados de diversas fuentes para identificar patrones y señales de actividades maliciosas o no autorizadas.
- Colección de Herramientas Open Source: Integra una variedad de herramientas de código abierto para el análisis y la gestión de la seguridad, proporcionando una solución comprehensiva y versátil.
- Visión Global de la Seguridad: Facilita a los administradores de red una perspectiva integral sobre la seguridad de su infraestructura, permitiendo una gestión efectiva y una respuesta proactiva a los incidentes.



Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

La gestión de redes y el filtrado de la información implican no solo el control y la coordinación de los recursos de red para satisfacer los requerimientos de tiempo real, calidad de servicio, y costes, sino también la protección eficaz de la red contra amenazas externas e internas. Una herramienta fundamental en la gestión de redes es el Protocolo Simple de Gestión de Red o SNMP (Simple Network Management Protocol), que facilita el monitoreo y la administración de dispositivos en la red.

Gestión de Registros de Elementos de Red

La gestión eficiente de registros de los diferentes elementos de la red, como routers, switches, firewalls, e IDS/IPS, facilita el mantenimiento de una red segura y eficiente. El SNMP permite la consulta y respuesta sobre el estado de los dispositivos.

Entre las métricas que se pueden obtener a través del SNMP se incluyen:

- Tráfico de Datos: Medido por los octetos entrantes y salientes, proporciona una visión del volumen de datos por segundo.
- Rendimiento del Dispositivo: Incluyendo la carga de la CPU, memoria utilizada y disponible, y el tiempo de operación.
- Estado de las Sesiones y Protocolos de Red: Como las sesiones BGP (enrutamiento) y las tablas ARP.
- Gestión y Configuración de Dispositivos: Permitiendo acciones como el apagado y encendido de puertos y el reinicio remoto de dispositivos.

Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

Gestión de Filtrado de Red

Con la creciente sofisticación de software malicioso, la gestión del filtrado de red se ha convertido en una necesidad imperante. Las herramientas clave en esta gestión son los firewalls y los sistemas de detección/preventivos de intrusiones (IDS/IPS), que sirven para filtrar la información entrante y saliente y proteger la red contra ataques.

Firewalls. Actúan como barreras entre la red interna y el acceso externo, controlando el tráfico basado en una serie de criterios predefinidos:

- Control de Servicios: Definiendo qué servicios de red son accesibles.
- Control de Direcciones: Especificando qué direcciones pueden solicitar servicios y cuáles están autorizadas a cruzar el firewall.
- Control de Usuarios: Restringiendo el acceso a la red basado en la identidad del usuario.
- Control de Comportamiento: Regulando cómo se utilizan los servicios, incluyendo el filtrado de contenido web y SPAM.

CORTAFUEGOS O FIREWALL

Características	Funciones	Limitaciones
Control de servicios	Protección ante servicios potencialmente vulnerables	No hay protección frente a lo que no pasa por el cortafuegos
Control de direcciones	Simplificación de la administración de la red	No hay protección frente a amenazas internas
Control de usuarios	Protección ante usuarios no autorizados	Puede dar falsa sensación de seguridad
Control de comportamiento	Protección frente a ataques de suplantación de IP	
	Elección de la ubicación de la supervisión de eventos de seguridad	

Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

Gestión de Filtrado de Red

Los (IDS/IPS) están diseñados para identificar, prevenir y reportar ataques y vulnerabilidades. Estas tecnologías complementan otros mecanismos de seguridad, fortaleciendo la defensa contra amenazas cibernéticas.

Sistemas de Detección de Intrusiones (IDS).

Los IDS monitorean el tráfico de red en busca de actividades sospechosas o no autorizadas, alertando a los administradores sobre posibles intrusos. A diferencia de los firewalls, que controlan el acceso entre redes basándose en un conjunto de reglas definidas, los IDS se centran en la vigilancia y la alerta de intrusiones en tiempo real. Los IDS pueden ser:

- Basados en Red (NIDS): Analizan el tráfico de toda la red, buscando patrones o firmas de ataques conocidos.
- Basados en el Host (HIDS): Se instalan en dispositivos específicos para monitorizar el tráfico entrante y saliente de esos dispositivos, así como cambios sospechosos en los archivos del sistema.

Gestión de registros de elementos de red y filtrado (router, switch, firewall, IDS/IPS, etc.)

Gestión de Filtrado de Red

Los (IDS/IPS) están diseñados para identificar, prevenir y reportar ataques y vulnerabilidades. Estas tecnologías complementan otros mecanismos de seguridad, fortaleciendo la defensa contra amenazas cibernéticas.

Sistemas de Prevención de Intrusiones (IPS). Los IPS, por otro lado, no solo detectan las actividades maliciosas sino que también toman medidas para bloquearlas antes de que causen daño. Funcionan colocándose directamente en el flujo de tráfico de la red, inspeccionando cada paquete en busca de comportamientos maliciosos y actuando según lo definido por sus configuraciones.

Tipos de detección:

- Basada en Firmas: Identifican ataques mediante la comparación del tráfico de red con una BBDD de firmas conocidas.
- Basada en Políticas: Requieren la definición de políticas especifiquen qué actividades son permitidas y cuáles no.
- Basada en Anomalías: Monitorean el tráfico de red en busca de desviaciones respecto a un patrón de comportamiento normal establecido.
- Honey Pot: Utilizan trampas para atraer y detectar intrusos, simulando ser sistemas vulnerables para capturar y analizar los métodos de ataque.

El funcionamiento de los IPS incluye varias etapas para garantizar una protección eficaz:

- Clasificación de Paquetes: Cada paquete se examina para determinar su naturaleza en base a la cabecera y la información de flujo.
- Aplicación de Filtros: Según la clasificación, se aplican filtros relevantes en paralelo para evaluar el estado del flujo de información del paquete.
- Identificación y Descarte: Los paquetes sospechosos se marcan y se descartan, actualizando el estado del flujo para bloquear futuras comunicaciones malintencionadas.

Resumen

Una red informática es una infraestructura esencial que permite la comunicación entre ordenadores y otros dispositivos digitales dentro de una organización, facilitando el intercambio de información y recursos. Esta infraestructura se compone de hardware específico, como servidores y ordenadores (equipos de red), dispositivos de conectividad como routers y switches (medios de comunicación), así como conectores y medios de transmisión, que pueden ser tanto cableados como inalámbricos.

Para garantizar una comunicación eficaz entre los distintos dispositivos de la red, se requiere adherirse a un conjunto de normas y reglas conocidas como protocolos de red. Estos protocolos varían ampliamente en sus especificaciones, aunque generalmente comparten principios fundamentales que facilitan su interoperabilidad. La estandarización de estos protocolos comenzó con el desarrollo del modelo OSI (Interconexión de Sistemas Abiertos), que proporciona un marco teórico para la arquitectura de la comunicación entre sistemas. Sin embargo, en la práctica, el modelo TCP/IP es el más utilizado para describir y aplicar los protocolos de red.

La monitorización de la red es un aspecto crucial de su gestión, permitiendo a los administradores recopilar datos sobre el rendimiento de sus componentes, analizar esta información y tomar decisiones informadas. Esta supervisión es vital para mantener la eficiencia y la seguridad de la red, adaptando la estrategia de red según sea necesario para responder a los cambios y desafíos emergentes.

En cuanto a la seguridad, se destacan tres tipos de sistemas diseñados para proteger la información y los recursos de la red: los Sistemas de Gestión de la Seguridad de la Información (SIM), los Sistemas de Gestión de Eventos (SEM), y los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM). Estos sistemas ofrecen un conjunto de herramientas para la detección, prevención y respuesta a amenazas de seguridad, asegurando así la integridad, disponibilidad y confidencialidad de los datos.