Bloque 5: Sistemas en Red. Configuración, conexión y explotación.

Introducción

Cualquier sistema informático está unido a algo, por lo que entendemos que están en red. Los sistemas informáticos en red se basan en modelos de referencia, aquel sistema que establece las características necesarias para comunicarse con otros sistemas. Siguen las arquitecturas de red para dividir los modelos de referencia entre varios niveles, donde se tratan distintos protocolos y estándares. Su objetivo es reducir la complejidad y facilitar una evolución natural en la comunicación.

Hay dos modelos principales:

Modelo OSI

Cada capa se comunica con su capa inmediatamente superior e inferior, si estamos en el nivel 5 solo podemos ir a la 4 o la 6, no saltarlas. Cada capa tiene una traza con metainformación. Los 7 niveles de las capas de red OSI se ven en los sistemas emisores y receptores, el emisor en descendiente y el receptor en ascendente:

> **Capa 7. Aplicación:** Une al humano con el equipo.
> **Capa 6. Presentación:** Comprime o cifra los datos dándoles formato
> **Capa 5. Sesión:** Define los mecanismos para mantener y controlar el diálogo entre las aplicaciones de origen y destino.
> **Capa 4. Transporte:** Prepara la información, y la encapsula en *segmentos* asegurándose de que llegan en el orden correcto
> **Capa 3. Red:** Encapsula los datos en *paquetes* y los envía por diferentes rutas calculadas para llegar al receptor.
> **Capa 2. Enlace de datos:** Encapsula los paquetes en *tramas* para transmitirlas de emisor a receptor, detectando y corrigiendo errores.
> **Capa 1. Física:** Establece las especificaciones físicas de los equipos que intervienen en la comunicación

Las 3 capas de arriba se refieren al host, y las otras 4 se basan más en el flujo de datos.

Entre capa y capa el mensaje pasa por una serie de tramas, que añaden o eliminan datos. Cuando se va añadiendo información de capa en capa se conoce como “encapsulamiento”, mientras cuando se eliminan los datos extra se llama “desencapsulamiento”

Modelo TCP/IP

Constituye el estándar de Internet, y se adapta al modelo OSI. Existe una correspondencia entre OSI y TCP/IP:

- La capa Aplicación del TCP/IP se corresponde con las capas de Aplicación, Presentación y Sesión de OSI
- La capa de Transporte de TCP/IP corresponde a la capa de Transporte de OSI
- La capa de Internet de TCP/IP corresponde con la capa Red de OSI
- La capa de Acceso a la Red de TCP/IP corresponde a las capas de Enlace de Datos y Física de OSI.

Protocolos principales de red

Los protocolos más importantes son:

Aplicación	HTTP, HTTPS	Publicar e interpretar texto y otros en Internet
	SMTP, POP3, IMAP	Enviar y recibir correo electrónico
	DHCP (Dynamic Host Conf Protocol)	Configurar el equipo para recibir una IP automáticamente
	DNS (Domain Name System)	Traducir nombres de dominios a IP
	FTP, FTPS	Transferir archivos
	RCP (Remote Control Protocol)	Establecer conexiones remotas
	SSL, TSL	Encriptar información en el emisor para que el receptor pueda descifrarla
Transporte	UDP (User Datagram Protocol)	Enviar información sin comprobar la llegada y sin sincronizarse
	TCP (Transmision Control Protocol)	Enviar información estableciendo conexión previa y confirmando la llegada en el mismo orden
Internet	IP (Internet Protocol)	Envía paquetes por la mejor ruta posible, y su trazado se realiza a través del mecanismo de enrutamiento.
	NAT (Network Address Translate)	Traduce IPs privadas en públicas
Acceso a la red	ETHERNET	Establece reglas que rigen el cableado
	WLAN	Establece reglas que rigen la comunicación WiFi
	FDDI	Establece reglas para la comunicación por fibra óptica en redes de área local.
	ARP, RARP	Asignar direcciones MAC con IP y viceverda

Ethernet

El protocolo Ethernet es la forma de conexión y transmisión de datos por cable (coaxial, par trenzado y fibra óptica) donde se especifican las características del cableado, su señalización y su formato de tramas de datos, todo ello por medio del estándar IEEE 802.3.

Emplea CDMA/CD: Modelo que nos sirve para, cuando varios equipos comparten información y un host quiere enviar un mensaje, comprobar el comportamiento del medio y cuando éste no está ocupado, manda el mensaje. Evita la colisión de información

Sus ventajas son el bajo coste, la facilidad de su implementación y seguridad ante accesos no permitidos. Es el protocolo más empleado en redes locales LAN

Wi-Fi

El protocolo WiFi establece especificaciones para redes de área local de forma inalámbrica. Sigue los estándares IEEE 802.11, teniendo subestándares según su banda y su ancho de banda máximo.
Emplea CSMA/CA: Antes de transmitir, envía una notificación sobre su intención, y solo envía la información si se le autoriza, por lo que evita mejor la colisión de información.

Sus ventajas son la facilidad de instalación y su movilidad

Su principal desventaja es la inseguridad

IPv4 e IPv6

El protocolo IP se encarga del enrutamiento de paquetes, decidiendo la ruta mas adecuada para transportar los paquetes. Este protocolo no se encarga de saber si los paquetes han llegado correctamente, de eso encarga el protocolo TCP.

La dirección IP o dirección lógica se asigna a cada interfaz de red de un equipo. Son imprescindibles para enviar y recibir paquetes unívocamente. ***No pueden existir dos direcciones IP iguales en una misma red.*** Se usan dos protocolos IP actualmente: IPv4 e IPv6.

Las direcciones IP suelen ser automáticas, que se asignan mediante la configuración del protocolo TCP/IP, pero se pueden hacer estáticas o manuales.

IPv4

Su estructura es de 32 bits (4 bloques de 1 byte). Su separador se realiza por un punto.
Hay un total de 2^{32} direcciones posibles, lo cual parece mucho, pero acabó siendo insuficiente, haciendo que la dirección IPv4 quede relegada parcialmente a redes locales y metiendo la importancia a la dirección IPv6.

La dirección IP se divide en una porción de red y una porción de host.

- **La porción de red** son los bits de la IP (de izquierda a derecha) que se encuentran en la misma posición que los 1 de la máscara de red
- **La porción de host** son los bits de la IP (de izquierda a derecha) que se encuentran en la misma posición que los bits 0 de la máscara de red.

La máscara de red tiene el mismo formato que la dirección IP, va en pareja con la IP y ayuda asacar cálculos. También se puede representar como un prefijo en notación CIDR (192.168.0.1/24).

Dentro del rango de IP, hay varios tipos de direcciones:

- Dirección de red: Especifica la red. Es la primera dirección del rango de direcciones de la red. Es la del host. Se consigue haciendo una operación AND de la IP de la red y la máscara de red (192.168.1.0)
- Dirección de Broadcast: Se utiliza para enviar paquetes a todos los hosts de la red. Se identifica por la parte de posición de host (192.168.1.255)
- Dirección de Host: Dirección susceptible de asignarse a hosts dentro de una red. Son las comprendidas entre la dirección de red y la de broadcast (192.168.1.1 – 192.168.1.254)

Las direcciones IP se pueden catalogar en públicas y privadas:

- **Públicas:** Únicas a nivel mundial, uso por Internet.
- **Privadas:** Para redes de acceso restringido o nulo con Internet (redes locales por ejemplo)

El router, por el protocolo NAT, se encarga en traducir las IP privadas en públicas.

Los adaptadores de red disponen también de una dirección física o MAC asociada a cada interfaz de red. Es única en el mundo y se forma de 48 bits en hexadecimal: XX:XX:XX:XX:XX:XX

IPv6

Su estructura es de 128 bits (8 bloques de 2 bytes), Su separador son los puntos y tiene un total de 2^{128} direcciones posibles.

Su estructura es XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
(8 bloques de 4 caracteres hexadecimales (2 bytes))

Sus ventajas son el aumento de seguridad y tratamiento de paquetes, y el numero de IPs para implantar el IoT

Abreviación:

- **Bloques de 0000 se reduce a 0**
- **Dos o mas bloques consecutivos de 0 se reducen a "::" en una única ocasión por dirección**
- **Los ceros a la izquierda se descartan.**

TCP y UDP

Los protocolos TCP y UDP se diferencian en que, aunque los dos transmitan información, el protocolo TCP garantiza que todos los paquetes llegan al destino, por lo que llevan una observación de todo el proceso de comunicación, y reenvía segmentos si no le llegan al receptor; mientras que el UDP manda los segmentos de forma rápida, sin importar cómo lleguen, porque no compromete la confiabilidad del mensaje

En resumen, el TCP es más confiable que el UDP, pero es más lento.

El TCP lo usan el FTP y el HTTP, mientras que las aplicaciones de Streaming usan el UDP.

Interconexiones de redes. Componentes

Los dispositivos de interconexión de redes se dividen en 3 capas:

- **Capa física:** Con el *Repetidor*, que regenera la señal entre dos puntos, y el *Hub,* que replica la información entrante a todos sus puertos de salida.
- **Capa de enlace de datos:** Con el *switch*, que conecta la información de uno de los puertos al puerto de destino, y el *punto de acceso*, que extiende la red cableada mediante un medio inalámbrico
- **Capa de red:** Con el router, que conecta redes diferentes

Switch

Los switch conectan la información únicamente por cada uno de los puertos de entrada y salida sabiendo cuál es el destino en todo momento. Gran ventaja en direccionamiento de red, divide una red en subredes y evita colisiones en paquetes de datos

Cuando un paquete llega al switch, en vez de hacer broadcast con él, lo manda directamente al puerto destino.

Router. Tablas de enrutamiento

Al conectarse host en una red, se guarda la dirección del host destino para saber a cuáles se pueden enviar paquetes. Puede ser a él mismo, a un host local o a un host remoto mandando primero el paquete a la dirección 0.0.0.0

Se verán las tablas con netstat –r

Mascara de red sera la que se va a aplicar

Puerta de enlace es la que está vinculada para llegar a ese destino, será el primer salto

Métrica será cómo de buena es esa ruta. Cuanto menor sea el número, mejor será la ruta

El linux con ip route show

Topología física y lógica. Mapas

Física:

Es la organización física de los elementos y componentes de la zona. Existen **inalámbricas** y **cableadas**

Inalámbricas:

- **Distribuida:**
- **Centralizada**

Cableadas:

- **WAN:** (punto a punto(un equipo conectado a otro), estrella(varios nodos conectados a uno central) o malla(varios nodos conectados entre sí parcial o totalmente))
- **LAN:** (estrella, estrella extendida (varias estrellas unidas entre sí), bus o anillo)
- **Topología en bus:** se comparte un único bus central para todos los nodos
- **Topología en anillo:** todos los nodos conectados cada uno con el posterior y el anterior

Lógica:

Cada elemento de la red indica las dependencias y características de su conexión

- Redes Wan: punto a punto entre 2 equipos
- Redes LAN: acceso controlado(dando turnos) o por contienda (peleando por el envío)

Dominios de colisión y difusión

Los dominios de colisión son áreas donde pueden colisionar paquetes. Los routers y switches dividen los dominios de colisión

Los dominios de difusión son áreas donde se reciben tramas de broadcast, haciendo que los paquetes no colisionen. Entre ellos. Los dispositivos

La segmentación de una red en dominios de colisión y difusión mejora la eficiencia de red y aumenta el ancho de banda, además de que ayuda a evitar colisiones de datos

Tipos de redes

Según su tamaño son:

- **PAN** (Bluetooth, NFC…) [Personal Area Network]
- **LAN** (Red local, tiene su variante WLAN que es inalámbrica) [Local Area Network]
- **MAN** (Red más amplia, *CAN:* Cuando une varios edificios [Campus]) [Metropolitan Area Network]
- **WAN** (Conectando a nivel más masivo, conectando hasta ciudades lejanas) [Wide Area Network]

Según su transmisión son: **Punto a Punto** y **Multipunto**

Según su función son: **Entre Iguales** (Hosts interconectados ofreciendo y recibiendo servicios) y **Cliente-Servidor** (Hosts que ofrecen servicios(servidor) y hosts que los solicitan(cliente)

Según sus medios son: **Inalámbricas** (Wireless, medio aéreo), **Mixtas** y **Cableadas** (Medio físico)

Acceso a redes WAN. Tecnologías

Cuando se quieren conectar redes LAN a larga distancia, o equipos que están fuera de su área de actuación, se utilizan las redes WAN. Se paga a una compañía para contratar un ISP, un proveedor de servicios de Internet.

Las redes WAN requieren una serie de normas distintas en las LAN

Conexiones WAN privadas

Dentro de estas, se encuentran tres tipos:

- Conmutación de circuitos: Requiere el establecimiento de un circuito dedicado que va entre los nodos y terminales. RDSI es una red telefónica conmutada
- Conmutación de paquetes: Se dividen los datos en paquetes y se transmiten por la red. Una vez llegan a su destino, se vuelven a juntar. No es necesaria la existencia de un circuito permanente. Es más económico que la conmutación de circuitos pero tiene una latencia más alta. Internet es un ejemplo de conmutación de paquetes
- Dedicada: Se usa una conexión directa y permanente entre dos nodos de la red. Es una conexión exclusiva. Es un servicio de mayor calidad, pero mucho más caro. Un ejemplo es el VOIP (Voice Over IP)

Conexiones WAN públicas

- DSL: Familia de tecnologías que permiten acceder a internet por medio de cables de cobre de par trenzado de la red telefónica, con un ancho de banda aceptable
- FTTH: Fiber To The Home (Fibra Hasta El Hogar), tiene velocidades más altas que el DSL, ya que usa fibra óptica. Usan una serie de equipos que usa la tecnología GPON para transmitir los datos por la fibra.
    - OLT Operadora: Terminación de Fibra Óptica: De donde parte la fibra hacia los hogares
    - Splitter o Divisor Óptico: Divide la señal en partes iguales de menor potencia para sacar la fibra a distintas ramas.
    - ONT: Terminador de Red Óptica. Se encuentran en los routers de las casas y oficinas. Convierten las señales ópticas a eléctricas y viceversa
- HFC: Hibrido de Fibra Coaxial: Es una mezcla entre fibra óptica y el cable coaxial (se hace el híbrido en un punto cercano a nuestra casa. Empieza siendo fibra, pero se distribuye de forma coaxial.
- Inalámbricas: Usan las ondas electromagnéticas para pasar datos. Se emplean mucho en las redes LAN. Ejemplos: WiMAX (Permite alcanzar distancias hasta 60km con una velocidad de 1Gb/s) y LTE.A (4G y 5G)

Redes cableadas

Además de ser más veloces, son más fiables frente a los inalámbricos, ya que su conexión es directa y tiende a saturarse con más dificultad

Tipos y características

- **Cable de cobre de par trenzado**

  Se forman por una cubierta de PVC que tiene en su interior 8 cables de cobre aislados y entrelazados. Los colores de los cables son: Azul (enlazado con blanco azul), naranja (enlazado con blanco naranja), verde (enlazado con blanco verde) y marrón (enlazado con blanco marrón). Se entrelazan para evitar interferencias.
  Hay diferentes blindajes que pueden afectar a las conexiones.
  Los conectores de la terminación de los cables son los RJ45 (salvo el telefónico, RJ11), que pueden ser normales o apantallados (para cables blindados). Todas las tomas de usuario tienen conectores hembra RJ45

  Es necesario el blindaje para proteger los cables, y hay varios tipos, distinguidos por cable/pares.

  - U/FTP (Unprotected (sin cubierta)/ Foiled (Lámina) Twisted (Retorcido) Pair (Par))
  - F/FTP (Foiled (lámina) / Foiled (Lámina) Twisted (Retorcido) Pair (Par))
  - S/FTP (Shield (Malla) / Twisted (Retorcido) Pair (Par))
  - F/UTP (Foiled (lámina) / Unprotected (sin cubierta) Twisted (Retorcido) Pair (Par))
  - SF/UTP (Shield Foiled / Unprotected Twisted Pair)

  Hay un estándar que regula la normativa de los colores de los cables: TIA/EIA-568-B

T-568A	**T-568B**
1) Blanco/Verde	1) Blanco
2) Verde	2) Naranja
3) Blanco/Naranja	3) Blanco/Verde
4) Azul	4) Azul
5) Blanco/Azul	5) Blanco/Azul
6) Naranja	6) Verde
7) Blanco/Marrón	7) Blanco/Marrón
8) Marrón	8) Marrón

  Esta categoría determina características eléctricas y funcionales, dando modelos CAT (CAT5, 6, 5.e, 8, 9…)

- **Cable de fibra óptica**

  Su instalación es más compleja y es más caro que el par trenzado, pero es mucho más rápido. Está formado por uno o varios hilos de fibra de vidrio recubierto de varias capas para darle protección y rigidez. Tiene dos tipos:

  - Monomodo: Es un único haz de luz por el canal, utilizado en largas distancias, usando estándares OS1 y OS2
  - Multimodo: Son varios haces de luz con diferentes trayectorias en el mismo tubo. Sus estándares son OM1, OM2, OM3, OM4 y OM5, y sirve para cortas distancias (una casa o un edificio)

  Sus partes son:

  - Núcleo
  - Revestimiento
  - Recubrimiento primario (silicona o acrilato

- Recubrimiento secundario (PP, PVC o Nilón)

Los conectores de cables de fibra óptica más utilizados son:

- ST (en giro, 1 fibra)
- SC (a presión, 1 fibra)
- LC (a presión, 1 fibra)
- FC (rosca, 1 fibra)
- MT-RJ (a presión, 2 fibras)
- MPO (a presión, 4-72 fibras)

Los cables de fibra óptica son los medios de transmisión de información intercontinental debido a sus altas velocidades. Son instaladas también por el medio submarino, usando barcos y grúas para transportarlos de lado a lado del océano

Dispositivos de interconexión

El estándar TIA/EIA-568-B establece el diseño e implementación del cableado de un edificio, además de una topología de red en estrella (un nodo central que se divide en varias ramas. El nodo central controla el flujo de información de la red).

Los elementos de la electrónica de red para conectar los cables con el nodo central son switches y routers. Estos elementos se alojan en los **armarios de distribución o racks**.

Los rack suelen contener paneles de parcheo, dispositivos de electrónica de red (switches y routers), y otros elementos.

En los extremos de los rack encontramos las tomas de usuario (rosetas)

Ejemplo del instituto:

- **Rack principal:** En secretaría llega la red
- **Racks de edificio:** De secretaría llega la conexión a un rack
- **Racks de planta:** Cada rack de edificio llega a varios racks de cada planta
- **Racks secundarios:** Cada x metros, necesita un rack más.

Adaptadores

Los adaptadores de red o NIC son necesarios para que los host puedan conectarse a una red. Un host puede conectarse a varias redes, siempre y cuando tenga varios adaptadores.

Hay diferentes tipos, según el medio de transmisión, conectividad, modo de transmisión, velocidad de conexión y Wake On LAN

- **Medio de transmisión:** Coaxial, Par trenzado, Inalámbrico, fibra óptica
- **Conectividad con el host:** PCIe,

Redes inalámbricas

Aportan ventajas como movilidad (no tienes un cable limitándote), flexibilidad (no tienes un cable que se puede romper si lo mueves), y facilidad de instalación.

Emplean ondas electromagnéticas para transmitir datos, y su capacidad de transmisión depende de la frecuencia y la longitud de onda del espectro electromagnético.

- La longitud de onda es la longitud en metros entre 2 crestas
- La frecuencia (en Hercios Hz), es el número de veces que se repite la onda en un segundo

Tipos y características

- WiFi: Alcanzan teóricamente 10Gb/s con un alcance aproximado de 1km. Sigue el estándar IEEE 801.11. Trabaja con frecuencias entre 2.4GHz y 5GHz. **A menor frecuencia, mayor alcance y mayor ancho de banda.**
  Necesitan **punto de acceso WiFi** para poder conectarse por medio de los dispositivos
- WiMAX: Dan comunicación a áreas geográficas poco densas o lejanas porque el despliegue de fibra óptica resulta caro. Necesitan **estaciones base** con dispositivos electrónicos potentes que envían microondas y receptores WiMAX
- 4G y 5G: Las siglas hacen referencia a las siglas de las generaciones de dispositivos, y se usan para WMAN y WWAN. LTe Advanced es el estándar del 4G, y su ancho de banda es de 1GB/s, mientras que el 5G usa los estándares de la quinta generación y puede alcanzar los 20Gb/s con un consumo más bajo.
- WPAN:
    - Bluetooth(Facilitar la transmisión de datos entre dispositivos cercanos por medio de la **vinculación** de dispositivos. Hasta 230m y varias decenas de bits por segundo)
    - Zigbee (Bajo consumo y baja tasa de transferencia. Sensores y domótica),
    - NFC (Conexión excesivamente cercana, a menos de 20mm).

Dispositivos de interconexión

Cada tipo de red inalámbrica requiere de un dispositivo de interconexión:

- WiMAX, 4G y 5G: Estaciones base provistos de equipos de telecomunicaciones que tienen antenas para proporcionar cobertura en esa zona.
- WiFi: Usa puntos de acceso con topologías de acceso:
    - AdHoc (IBSS) (Conjunto de servicios básicos , para WiFi, BT y NFC
    - Modo de infraestructura (Zigbee): Puntos de acceso inalámbricos conectados al sistema de distribución
        - Servicios básicos (BSS) Un único punto de acceso con servicios básicos
        - Servicios extendidos (ESS) Varios puntos de acceso conectados inalámbricamente o por cable, pudiendo moverse sin perder la cobertura.

Adaptadores

Hay diferentes tipos según:

- Estándares WiFi soportados (IEEE 802.11 a/b/g/n…)
- Bandas de trabajo (frecuencia)
- Velocidad de transferencia en Mb/s o Gb/s
- Conectividad con el host (USB, PCIe, M.2)
- Numero de antenas
- Seguridad: Protocolos WEB, WPA2, WPA3…

Ficheros de configuración de red (Ubuntu y Windows)

Ubuntu

Si lo que quiero saber es qué interfaces de red hay en el sistema, se puede usar los comandos:
ip a para ver la red
lshw -class network para ver la interfaz de red

Ubuntu Linux actualmente utiliza la herramienta NetPlan para administrar la configuración de la red, y su configuración está en /etc/netplan/, pero para tocar su configuración hay que tener permisos de super usuario.

Estructura del networkManager:

- Renderer: Nombre del gestor de red (NetworkManager en desktop, networkd en server)
- NombreDispositivo
- Dhcp4: yes o no, si se configura por DHCP (automático) o estático (manual)
- Addresses: Se indica la IP con prefijo
- Gateway4: Señala la puerta de enlace
- Nameservers: Direcciones IP de los DNS, siguiendo el formato indicado

Windows:

Se accede al fichero C:\Windows\System32\drivers\etc\hosts para editar la configuración de hosts. Mantendría una organización entre los hosts y los dominios.

Para agilizar la traducción es: Memoria caché de web – Archivo host – Servidores DNS

Para editar el archivo, es necesario tener privilegios de anfitrión.

Monitorización y verificación de una red mediante comandos

Ubuntu:

- *ip a*: Lista interfaces activas e inactivas
- *ip link set <interfaz> down*: Deshabilitar interfaz
- *ip link set <interfaz> up*: Habilitar interfaz
- *ip addr add <ip/mascara> dev <interfaz>:* Configurar una interfaz
- *ip addr del <ip/mascara> dev <interfaz>*: Eliminar ip
- *ip route show*: Mostrar tabla de enrutamiento
- *ip route del 0.0.0.0/0 via dir_IP dev <interfaz>:* Borrar puerta de enlace predeterminada
- *ip route add 0.0.0.0/0 via dir_IP dev <interfaz>:* Añadir puerta de enlace predeterminada
- *ip neighbour show*: Mostrar la tabla ARP
- *arp (Windows):* Ver direcciones MAC e IPs

Para enviar paquetes a un destino par probar si el adaptador funciona correctamente (o tiene acceso a la red), se usa ***ping [opciones] destino***.

Otro comando, para conocer la ruta del paquete en la red, es ***tracert servidor*** en Windows y ***traceroute servidor***.

El comando ***nmap*** permite monitorizar la red y hacer estudios genéricos (auditorías y seguridad). Es un programa de código libre, instalable en el apt de Linux y por archivo en la web para Windows

Gestión de puertos

Los puertos pueden hacer referencia a:

- Puerto físico: Entrada o conector a dispositivos de red (Ergo: Puerto RJ-45 para Ethernet)
- Puerto lógico: Número que se asocia a la aplicación de origen o destino en una comunicación. Se usan en la capa de transporte, y siempre se especificarán los puertos origen y destino:
    - Origen: Numero que identifica la aplicación que origina la comunicación
    - Destino: Número que asocia la aplicación de destino en el host remoto.

En el protocolo TCP/UDP siempre tiene que estar de cabecera esta especificación.

Hay varios puertos lógicos:

- Puertos bien conocidos (Del 1 al 1023), reservados para aplicaciones y servicios como HTTP (80), FTP (20), HTTPS (443), SMTP (25), etc.
- Puertos registrados (Del 1024 a 49151): Son aplicaciones de usuario cuando se conectan a servidores.
- Puertos dinámicos, privados o efímeros (49152 a 65535): Son utilizadas por aplicaciones de intercambio de archivos punto a punto.

Parte de la información encapsulada en la capa de red del modelo OSI son la IP de origen y la IP de destino.

- A la combinación de una IP y un puerto es un **socket**
- La comunicación entre hosts se establece por parejas de sockets.

Monitorización de puertos: *netstat* (Windows) y ***ss*** (Linux)

Sintaxis de Linux: ss [opción]

- -a: Mostrar conexiones asociadas a los sockets
- -l: Listar los sockets en escucha del host
- -t: Mostrar sockets TCP
- -s: Mostrar estadísticas.

Resolución de problemas

Se necesita llevar un mantenimiento para evitar que haya problemas y, de haberlos, saber cómo actuar

Tipos de mantenimiento:

- Predictivo: Prever futuros fallos en el sistema

- Preventivo: Prevenir fallos en el sistema antes de que pasen y reducir sus posibilidades. Se detallan acciones técnicas donde se especifican procedimientos y técnicas, además de su frecuencia.
- Correctivo: Reparar el fallo por medio de un procedimiento que establece el modo de resolver las averías del sistema.

Fallos en los sistemas informáticos en red más comunes:

- Fallos en hosts:
    - Fallos en tarjeta de red
        - Tarjeta averiada: Probar otra red para comprobar
        - Tarjeta mal insertada: Comprobar la correcta instalación de hardware
    - Fallos en la configuración de la tarjeta de red
        - Configuración TCP/IP inadecuada: Revisar la IP, DNS, mascara de red y habilitar DHCP
        - Configuración WiFi inadecuada y baja señal: Comprobar la autenticación y contraseña. Tambien testear la cobertura inalámbrica, tratando de evitar ruido electromagnético o la mala ubicación del punto de acceso
- Fallos en el medio:
    - Fallo en cableado: Chequear que no se sobrepasa el radio de curvatura máximo y que no está roto o forzado. También mirar si el tipo de cableado es adecuado al ruido electromagnético. En la fibra óptica, la perdida de señal tiene que ser la mínima posible
    - Fallo en conectores: ver que no están forzados o sucios. También comprobar si los cables están bien engastados (con los colores en su situo), y comprobar el mapa de cableado del par trenzado
- Fallos en la electrónica de red:
    - Configuración inadecuada de puntos de accesos WiFi: Revisar la autenticación WiFi, filtros MAC, SSID oculto, DHCP, direcciones estáticas…
    - Problemas en switches: Comprobar que los switches estén encendidos, que el testigo está encendido, ver la conexión y **la temperatura de los equipos**. Se debería tener la temperatura más baja posible, ya que el calor va inversamente proporcional al rendimiento

Herramientas Hardware:

- Tester de cable: Tiene un módulo principal y uno secundario. Comprueban si el cable está en correcto estado y si es óptimo
- Certificadora de continuidad: Hay de fibra óptica y de cobre, y permite comprobar la señal que transmite un cable. Detecta los cortes que tiene, e indica incluso la distancia en la que tiene los cortes.
    - Comprobador de fibra óptica: Muestra el rayo de luz de fibra óptica.
- Inspector de fibra óptica: Es un microscopio donde se conecta el cable y se puede ver cuán buena es la calidad
- Medidor de potencia óptica: Detecta la frecuencia y enseña las características de la fibra óptica
- Analizador de cableado: Tiene dos partes: El emisor (pinzas que se unen al cable, y el receptor (una especie de lápiz que, siguiendo el cable, sonará por donde se toque). Se

usa para buscar cables, emitiendo señales acústicas dependiendo de la distancia a la que estemos del cable

Seguridad en las comunicaciones

Todos los sistemas informáticos están relacionados directamente con la seguridad de sus comunicaciones.

Para que sean seguras, las comunicaciones se basan en 4 pilares fundamentales:

- Confidencialidad. Los accesos a la información, sistemas y recursos han de ser confidenciales (solo pueden acceder los que tengan permiso)
- Disponibilidad. Los recursos han de estar disponibles para los usuarios o procesos con sus permisos
- Integridad. La modificación debe hacerse por procesos o usuarios autorizados (que tengan permisos de modificación)
- Autenticidad. Se debe garantizar que se confirma la identidad del emisor y el receptor. El emisor debe asegurar que los datos han sido enviados por él y el receptor que los datos han sido recibidos por él.

Para lograr esos pilares, se establecen las políticas de seguridad a partir de los planes de contingencia de seguridad

Políticas de seguridad

Van a estar siempre basados en los elementos a proteger. Para ello, periódicamente se realizarán análisis de riesgos. Con estos, se descubren los puntos débiles que tiene el sistema, y se definirán unos planes de contingencia de seguridad en base a esos puntos débiles.

En cualquier entorno empresarial o institución pública o privada, se difunde la política de seguridad, y todos los usuarios del sistema deben conocer dicha política.

Las más destacadas son:

- Políticas de contraseñas
- Politicas de actualizaciones
- Políticas de uso de correo electrónico
- Política de aplicaciones permitidas
- Politica de uso de conexiones externas
- Políticas de almacenamiento y copias de seguridad
- Políticas de uso de portátiles corporativos
- Políticas de dispositivos personales

En estas políticas se detallan aspectos de seguridad como:

- Empleo de contraseñas robustas y actualización periódica de las mismas
- Uso de aplicaciones conocidas y actualizadas
- Actualización y mantenimiento de cuentas de usuario
- No difusión de cuentas y contraseñas a terceros
- No ejecución de aplicaciones desconocidas y externas (correo y USBs u otras redes)
- Actualización y mantenimiento de sistemas operativos y aplicaciones
- Creación y mantenimiento de las copias de seguridad
- Monitorización de la red
- Protección Antimalware

- Control de acceso físico a los sistemas y medios de red
- Configuración segura de redes inalámbricas

Tipos de ataques

Los ataques informáticos son acciones ofensiva que intentan tomar información, dañar o destruir los datos, informaciones o sistemas informáticos. Se distinguen en ataques activos y pasivos

- Ataques activos: Organizan cambios en la información
- Ataques pasivos: Registran o acceden a recursos sin alterar su información

Los ataques más usuales son:

- Reconocimiento y detección de vulnerabilidades: Se aprovechan de la vulnerabilidad para realizar futuros ataques
- Interceptación de información: Interceptan información de la red y vulneran la confidencialidad.
- Modificación de información: Necesita interceptar información para poder modificarla y reenviarla a la red. Vulnera la integridad, la confidencialidad y la autenticidad
- Suplantación de identidad: Son los más comunes. Afectan a la integridad, autenticidad y la confidencialidad. Los más comunes son la captura de cuentas (entran en la cuenta), SMTP Spoofing (Envian correos electrónicos suplantando la identidad del emisor), IP Spoofing (Envian paquetes desde un host distinto al original), DNS Spoofing (Redirige de forma errónea los dominios)

Mecanismos de seguridad en las comunicaciones

Con el objeto de proteger las comunicaciones, se emplean unas herramientas variadas en función de los planes de contingencia:

- Filtros de contenido: Software encargado de gestionar el acceso a sitios web para evitar contenidos maliciosos o de dudosa intención
- VPN: Redes privadas virtuales: Crean una extensión de una red local a través de una red pública, con lo que se puede establecer una conexión punto a punto segura. Se hace por aplicaciones específicas.
- Firewall: Cortafuegos: Herramientas hardware y software que controlan el tráfico de red y bloquean el tráfico externo para evitar accesos no autorizados
- Software Antimalware: Sirven para detectar amenazas en el equipo y blouearla.
- Herramientas de Cifrado: Cifran datos a través de redes inseguras para asegurar la integridad, autenticidad y confidencialidad. Por medio de claves cifradas, se protege el mensaje. Hay dos tipos:
    - Cifrado simetrico: Se usa una misma clave para cifrar y descifrar
    - Cifrado asimétrico: Usa dos claves: Una privada, y otra pública. A partir de la pública no se averigua la privada. Aporta autenticidad, integridad y no repudio (no se puede negar el envío y recibimiento de un mensaje).
      La clave pública cifra el mensaje, y la privada (solo conocida por el emisor) la descifra. El emisor es el único que puede enviar la clave privada al receptor.
- Protocolos seguros: HTTPS, SFTP, OpenSSL… Permiten firmar documentos