

Examen 109 - Fundamentos de Redes

Este examen cubre los conceptos básicos de redes TCP/IP, configuración de red, resolución de problemas y configuración de DNS del lado del cliente.

109.1 Fundamentos de protocolos de Internet

Teoría

Las redes modernas de Internet se basan en una suite de protocolos conocida como TCP/IP. Este conjunto de protocolos define cómo los datos se empaquetan, direccionan, transmiten y reciben entre dispositivos.

1. Modelos de Referencia:

- **Modelo OSI (Open Systems Interconnection):** Un modelo conceptual de 7 capas que describe las funciones de un sistema de comunicaciones. Aunque útil para entender conceptos, la implementación práctica se basa más en el modelo TCP/IP. (Capas: Física, Enlace de Datos, Red, Transporte, Sesión, Presentación, Aplicación).
- **Modelo TCP/IP:** Un modelo más práctico y ampliamente utilizado, con 4 o 5 capas que se corresponden aproximadamente con el modelo OSI.
 - **Capa de Enlace (Link Layer):** Maneja la comunicación entre dispositivos directamente conectados en la misma red local (ej: Ethernet, Wi-Fi). Aquí operan las direcciones MAC.
 - **Capa de Internet (Internet Layer):** Encargada del direccionamiento y enrutamiento de paquetes a través de diferentes redes. Aquí opera el protocolo IP.
 - **Capa de Transporte (Transport Layer):** Proporciona comunicación de extremo a extremo entre procesos en diferentes hosts. Los protocolos principales son TCP y UDP. Define conceptos como puertos.
 - **Capa de Aplicación (Application Layer):** Contiene los protocolos que las aplicaciones utilizan para interactuar (ej: HTTP, FTP, SSH, DNS, SMTP).

2. Direccionamiento:

- **Dirección MAC (Media Access Control):** Un identificador único asignado a la interfaz de red (tarjeta de red) por el fabricante. Opera en la Capa de Enlace. Se utiliza para la comunicación dentro de la red local (segmento Ethernet o Wi-Fi). Son direcciones físicas, típicamente representadas en formato hexadecimal (ej: 00:1A:2B:3C:4D:5E).
- **Dirección IP (Internet Protocol):** Un identificador lógico asignado a un dispositivo en una red IP. Opera en la Capa de Internet. Se utiliza para identificar dispositivos a través de diferentes redes en Internet y para el enrutamiento.

- **IPv4:** El protocolo IP más común actualmente. Direcciones de 32 bits, típicamente representadas en notación decimal con puntos (ej: 192 . 168 . 1 . 100). El espacio de direcciones IPv4 se está agotando.
- **IPv6:** El sucesor de IPv4. Direcciones de 128 bits, típicamente representadas en notación hexadecimal con dos puntos (ej: 2001 : 0db8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334). Ofrece un espacio de direcciones mucho mayor.
- **Máscara de Subred (Subnet Mask):** Define qué parte de una dirección IP (IPv4) identifica la red y qué parte identifica el host dentro de esa red. Se utiliza para determinar si una dirección IP destino está en la misma red local o en una red remota (que requiere enrutamiento). Típicamente representada en notación decimal con puntos (ej: 255 . 255 . 255 . 0) o en notación CIDR (Classless Inter-Domain Routing), que es un /prefijo que indica el número de bits de red (ej: 192 . 168 . 1 . 0 /24 donde /24 significa que los primeros 24 bits son para la red).
- **Puerta de Enlace Predeterminada (Default Gateway):** La dirección IP del router al que un dispositivo envía paquetes IP cuando el destino no está en la misma red local. Permite la comunicación con redes remotas e Internet.

3. Protocolos de la Capa de Transporte:

- **TCP (Transmission Control Protocol):** Protocolo orientado a la conexión, confiable. Establece una conexión antes de transmitir datos, garantiza la entrega de paquetes en orden, retransmite paquetes perdidos y controla el flujo de datos. Usado para aplicaciones donde la integridad de los datos es crítica (ej: HTTP, HTTPS, SSH, FTP).
- **UDP (User Datagram Protocol):** Protocolo no orientado a la conexión, no confiable. Envía paquetes sin establecer una conexión previa, sin garantía de entrega, orden o duplicación. Es más rápido y ligero que TCP. Usado para aplicaciones donde la velocidad es más importante que la confiabilidad estricta (ej: DNS, DHCP, streaming de video/audio, juegos en línea).

4. Puertos (Ports):

- Son números (0-65535) que identifican servicios o aplicaciones específicas en un host. Permiten que múltiples aplicaciones se comuniquen a través de la red simultáneamente en un mismo host.
- Los puertos bien conocidos (0-1023) están reservados para servicios estándar (ej: 80 para HTTP, 443 para HTTPS, 22 para SSH, 25 para SMTP, 53 para DNS, 67/68 para DHCP).
- Los puertos registrados (1024-49151) se asignan a aplicaciones específicas.
- Los puertos dinámicos/privados (49152-65535) son de uso temporal por las aplicaciones cliente.
- Una **socket** es la combinación de una dirección IP y un número de puerto (ej: 192 . 168 . 1 . 100 : 80, [2001 : db8 : : 1] : 22). Representa un punto final de comunicación.

5. Nombres de Interfaces de Red:

- Los dispositivos de red se representan en Linux como interfaces lógicas con nombres.
- **Convenciones Antiguas:** `eth0`, `eth1` (Ethernet), `wlan0`, `wlan1` (Wi-Fi).
- **Convenciones Modernas (Systemd/Udev "Nombres de Interfaces Predecibles"):** Nombres más largos basados en la topología del hardware (ej: `enp3s0` - Ethernet en bus PCI slot 3 device 0, `wlp2s0` - Wireless en bus PCI slot 2 device 0). **Esta es una diferencia visual entre sistemas más nuevos y más antiguos.**
- `lo`: La interfaz de loopback. Es una interfaz virtual que permite a un dispositivo comunicarse consigo mismo (`127.0.0.1` para IPv4, `::1` para IPv6). Se usa para pruebas y para que las aplicaciones se comuniquen localmente.

Herramientas de Línea de Comandos (Identificación):

- **ip (iproute2):** La herramienta moderna y recomendada para configurar y mostrar información de red (direcciones IP, rutas, interfaces).
 - `ip addr show`: Muestra direcciones IP, interfaces y su estado.
 - `ip route show`: Muestra la tabla de enrutamiento.
 - `ip link show`: Muestra el estado de las interfaces (incluyendo MAC).
- **ifconfig (net-tools):** Herramienta más antigua, considerada obsoleta y reemplazada por `ip`. Todavía se encuentra en muchos sistemas y es útil para visualización rápida.
 - `ifconfig`: Muestra información de las interfaces.
- **ss (iproute2):** La herramienta moderna y recomendada para ver información de sockets (conexiones TCP/UDP activas, puertos a la escucha).
 - `ss -tulnp`: Muestra sockets TCP/UDP a la escucha con nombres de procesos.
 - `ss -antup`: Muestra sockets TCP/UDP en cualquier estado (listening, established, etc.) con direcciones/puertos numéricos y nombres de procesos.
- **netstat (net-tools):** Herramienta más antigua, considerada obsoleta y reemplazada por `ss`. También útil para visualización.
 - `netstat -tulnp`: Similar a `ss -tulnp`.
 - `netstat -antup`: Similar a `ss -antup`.
- **Nota:** `net-tools` (que provee `ifconfig`, `netstat`) y `iproute2` (que provee `ip`, `ss`) son paquetes diferentes. Las distribuciones más nuevas tienden a favorecer `iproute2`. Puedes instalar ambos si lo deseas.