**Resumen Exhaustivo del Tema 7: Gestión de Sistemas en Red**

*(Preparación para Examen - Nivel Profundidad Máxima)*

**1. Modelos de Referencia: OSI vs TCP/IP**

**Modelo OSI (Open Systems Interconnection)**

**Definición**: Marco teórico de **7 capas** que estandariza la comunicación en red. Cada capa tiene funciones específicas y se comunica con las adyacentes.

**Capas del Modelo OSI**

1. **Capa Física (Capa 1)**
   * **Función**: Transmisión de **bits** (señales eléctricas, ópticas o electromagnéticas).
   * **Ejemplos**: Cable Ethernet (RJ-45), fibra óptica, WiFi (radiofrecuencia).
   * **Dispositivos**: Hubs, repetidores, módems.
2. **Capa de Enlace de Datos (Capa 2)**
   * **Función**:
     + **Direccionamiento físico** (MAC).
     + **Detección y corrección de errores** (CRC).
     + **Control de acceso al medio** (CSMA/CD en Ethernet, CSMA/CA en WiFi).
   * **Unidad de datos**: **Trama** (Frame).
   * **Protocolos**: Ethernet (IEEE 802.3), WiFi (IEEE 802.11), PPP.
   * **Dispositivos**: Switches, bridges.
3. **Capa de Red (Capa 3)**
   * **Función**: **Enrutamiento** (selección de la mejor ruta).
   * **Unidad de datos**: **Paquete** (Packet).
   * **Protocolos**: IP (IPv4, IPv6), ICMP, ARP, RIP, OSPF.
   * **Dispositivos**: Routers.
4. **Capa de Transporte (Capa 4)**
   * **Función**:
     + **Segmentación** de datos.
     + **Control de flujo** (ventana deslizante).
     + **Garantía de entrega** (solo en TCP).
   * **Protocolos**:
     + **TCP** (Transmission Control Protocol): Orientado a conexión, confiable.
     + **UDP** (User Datagram Protocol): No orientado a conexión, rápido.
   * **Unidad de datos**: **Segmento** (TCP) o **Datagrama** (UDP).
5. **Capa de Sesión (Capa 5)**
   * **Función**: Establece, mantiene y finaliza **sesiones** entre aplicaciones.
   * **Protocolos**: NetBIOS, RPC.
6. **Capa de Presentación (Capa 6)**
   * **Función**:
     + **Traducción** de formatos (ASCII, Unicode).
     + **Cifrado/Descifrado** (SSL/TLS).
     + **Compresión** (ZIP, JPEG).
7. **Capa de Aplicación (Capa 7)**
   * **Función**: Interfaz entre el usuario y la red.
   * **Protocolos**: HTTP, FTP, SMTP, DNS, DHCP, SSH.

**Modelo TCP/IP**

**Definición**: Modelo práctico usado en Internet, con **4 capas**.

| **Capa TCP/IP** | **Equivalente OSI** | **Protocolos** |
| --- | --- | --- |
| **Aplicación** | Aplicación + Presentación + Sesión | HTTP, FTP, DNS, SMTP |
| **Transporte** | Transporte | TCP, UDP |
| **Internet** | Red | IP, ICMP, ARP |
| **Acceso a la Red** | Enlace + Física | Ethernet, WiFi, PPP |

**Diferencias clave**:

* TCP/IP combina las 3 capas superiores del OSI en una sola (Aplicación).
* OSI es teórico, TCP/IP es el estándar real en Internet.

**2. Direccionamiento IP (IPv4 e IPv6)**

**IPv4 (32 bits)**

* **Formato**: 192.168.1.1 (4 octetos en decimal).
* **Clases de direcciones**:

| **Clase** | **Rango** | **Máscara por defecto** | **Uso** |
| --- | --- | --- | --- |
| A | 1.0.0.0 – 126.255.255.255 | 255.0.0.0 | Grandes redes |
| B | 128.0.0.0 – 191.255.255.255 | 255.255.0.0 | Empresas |
| C | 192.0.0.0 – 223.255.255.255 | 255.255.255.0 | Pequeñas redes |
| D | 224.0.0.0 – 239.255.255.255 | - | Multicast |
| E | 240.0.0.0 – 255.255.255.255 | - | Reservado |

* **Direcciones privadas**:
  + Clase A: 10.0.0.0/8
  + Clase B: 172.16.0.0/12
  + Clase C: 192.168.0.0/16
* **Máscara de red**:
  + Define qué parte de la IP es **red** y qué parte es **host**.
  + Ejemplo: 192.168.1.10/24 → 255.255.255.0 (primeros 24 bits son red).
* **Operación AND para calcular red**:

Copy

IP: 192.168.1.10 → 11000000.10101000.00000001.00001010

Máscara: 255.255.255.0 → 11111111.11111111.11111111.00000000

AND: 192.168.1.0 → 11000000.10101000.00000001.00000000

* + **Dirección de red**: 192.168.1.0
  + **Broadcast**: 192.168.1.255 (todos los bits de host en 1).
  + **Hosts válidos**: 192.168.1.1 – 192.168.1.254.

**CIDR (Classless Inter-Domain Routing)**

* Permite dividir redes en subredes más pequeñas.
* Ejemplo:
  + 192.168.1.0/26 → 255.255.255.192 → 62 hosts por subred.
  + Fórmula: Nº hosts = 2^(32 - n) - 2 (donde n es el número de bits de red).

**IPv6 (128 bits)**

* **Formato hexadecimal**: 2001:0db8:85a3::8a2e:0370:7334
* **Ventajas**:
  + Mayor espacio de direcciones.
  + Autoconfiguración (SLAAC).
  + Seguridad integrada (IPsec).
* **Tipos de direcciones**:
  + **Unicast** (1 a 1).
  + **Multicast** (1 a muchos).
  + **Anycast** (1 al más cercano).

**3. Protocolos Clave**

**TCP vs UDP**

| **Característica** | **TCP** | **UDP** |
| --- | --- | --- |
| **Orientado a conexión** | Sí (3-way handshake) | No |
| **Fiabilidad** | Confirmación de recepción (ACK) | No garantiza entrega |
| **Control de flujo** | Sí (ventana deslizante) | No |
| **Velocidad** | Más lento | Más rápido |
| **Uso típico** | HTTP, FTP, SSH | DNS, VoIP, streaming |

**ARP (Address Resolution Protocol)**

* **Función**: Asocia una **dirección IP** con una **dirección MAC**.
* **Proceso**:
  1. Host A envía **ARP Request** (¿Quién tiene 192.168.1.2?).
  2. Host B responde con **ARP Reply** (Yo tengo 192.168.1.2 → MAC: 00:1A:2B:3C:4D:5E).

**DHCP (Dynamic Host Configuration Protocol)**

* **Función**: Asigna IPs automáticamente.
* **Proceso (DORA)**:
  1. **Discover** (Cliente busca servidor DHCP).
  2. **Offer** (Servidor ofrece IP).
  3. **Request** (Cliente acepta IP).
  4. **Acknowledge** (Servidor confirma asignación).

**DNS (Domain Name System)**

* **Función**: Traduce nombres de dominio (google.com) a IPs (142.250.190.46).
* **Tipos de registros**:
  + **A** (IPv4).
  + **AAAA** (IPv6).
  + **MX** (Correo).
  + **CNAME** (Alias).

**4. Dispositivos de Red**

| **Dispositivo** | **Capa OSI** | **Función** |
| --- | --- | --- |
| **Hub** | Física (1) | Repite señales a todos los puertos (obsoleto). |
| **Switch** | Enlace (2) | Filtra tramas por MAC (evita colisiones). |
| **Router** | Red (3) | Enruta paquetes entre redes diferentes. |
| **Firewall** | Transporte/Aplicación (4-7) | Filtra tráfico por reglas de seguridad. |

**5. Seguridad en Redes**

**Amenazas Comunes**

* **Ataques pasivos**:
  + **Sniffing** (interceptación de datos).
* **Ataques activos**:
  + **DoS/DDoS** (sobrecarga de servicios).
  + **Spoofing** (suplantación de IP/MAC).
  + **Man-in-the-Middle** (interceptación y modificación de datos).

**Mecanismos de Defensa**

1. **Firewalls**:
   * **Filtrado de paquetes** (reglas por IP/puerto).
   * **Stateful Inspection** (monitorea conexiones activas).
2. **VPN (Red Privada Virtual)**:
   * Cifra conexiones en redes públicas (OpenVPN, IPsec).
3. **Cifrado**:
   * **Simétrico** (AES, misma clave para cifrar/descifrar).
   * **Asimétrico** (RSA, clave pública + privada).
4. **Protocolos Seguros**:
   * **HTTPS** (HTTP + SSL/TLS).
   * **SSH** (Secure Shell, reemplaza Telnet).

**6. Monitorización y Resolución de Problemas**

**Comandos Esenciales**

| **Comando** | **Función** | **Ejemplo** |
| --- | --- | --- |
| ping | Verifica conectividad | ping 8.8.8.8 |
| traceroute | Ruta de paquetes | tracert google.com (Windows) |
| netstat | Conexiones activas | netstat -tuln |
| nmap | Escaneo de puertos | nmap -sV 192.168.1.1 |
| ipconfig / ifconfig | Configuración de red | ipconfig /all |

**Herramientas Avanzadas**

* **Wireshark**: Analizador de tráfico (captura tramas).
* **Nessus**: Escáner de vulnerabilidades.

**🔧 Comandos Avanzados de Monitorización**

**1. Escaneo con Nmap (Detallado)**

* **Escaneo sigiloso (SYN Stealth)**:

bash

Copy

nmap -sS 192.168.1.1 # Envía paquetes SYN sin completar la conexión (evita logs).

* + **Usos**: Identificar puertos abiertos sin ser detectado.
* **Detección de SO y versiones**:

bash

Copy

nmap -A 192.168.1.1 # Combina -O (detección de SO) y -sV (versiones de servicios).

* **Escaneo de vulnerabilidades**:

bash

Copy

nmap --script vuln 192.168.1.1 # Usa scripts de NSE (Nmap Scripting Engine).

**2. Análisis de Tráfico con Tcpdump**

* **Filtrado por protocolo y puerto**:

bash

Copy

tcpdump port 80 and host 192.168.1.1 # Captura tráfico HTTP de un host específico.

* **Guardar capturas en un archivo**:

bash

Copy

tcpdump -w captura.pcap # Para analizar luego con Wireshark.

**📶 Estándares WiFi (IEEE 802.11)**

**Comparativa de Estándares**

| **Estándar** | **Frecuencia** | **Ancho de Banda** | **Alcance** | **Notas** |
| --- | --- | --- | --- | --- |
| **802.11a** | 5 GHz | 54 Mbps | Corto | Poca interferencia. |
| **802.11n (Wi-Fi 4)** | 2.4/5 GHz | 600 Mbps | Medio | MIMO (múltiples antenas). |
| **802.11ac (Wi-Fi 5)** | 5 GHz | 7 Gbps | Medio | Beamforming (enfoque de señal). |
| **802.11ax (Wi-Fi 6)** | 2.4/5/6 GHz | 11 Gbps | Largo | OFDMA (eficiencia en alta densidad). |

**Conceptos Clave**

* **MIMO (Multiple Input Multiple Output)**: Usa múltiples antenas para mejorar la velocidad.
* **Beamforming**: Enfoca la señal hacia el dispositivo cliente.
* **OFDMA (Orthogonal Frequency Division Multiple Access)**: Permite servir a múltiples dispositivos simultáneamente (clave en Wi-Fi 6).

**🌐 IPv6 en Profundidad**

**1. Características Únicas**

* **Direcciones Link-Local**:
  + Formato: fe80::/10 (ej: fe80::1).
  + **Uso**: Comunicación en la red local (sin necesidad de DHCP).
* **Autoconfiguración (SLAAC)**:
  + Los dispositivos generan su propia IP usando:
    1. Prefijo de red (anunciado por el router).
    2. **Identificador de interfaz (EUI-64)**:
       - Se deriva de la MAC (ej: MAC 00:1A:2B:3C:4D:5E → EUI-64 021A:2BFF:FE3C:4D5E).

**2. Tipos de Direcciones IPv6**

| **Tipo** | **Prefijo** | **Ejemplo** | **Uso** |
| --- | --- | --- | --- |
| **Unicast** | 2000::/3 | 2001:0db8::1 | Comunicación 1 a 1. |
| **Multicast** | ff00::/8 | ff02::1 (todos los nodos) | 1 a muchos (ej: streaming). |
| **Anycast** | Mismo que Unicast | 2001:db8::1234 | 1 al más cercano (ej: servidores DNS). |

**3. Transición IPv4/IPv6**

* **Dual Stack**: Dispositivos soportan ambos protocolos.
* **Túneles 6to4**: Encapsula IPv6 en IPv4 para redes mixtas.

**🛡️ Seguridad Adicional**

**1. Hardening de Redes WiFi**

* **Protocolos de Seguridad**:
  + **WPA3**: Reemplaza a WPA2, usa **AES-256** y **Protección contra ataques de diccionario**.
  + **OWE (Opportunistic Wireless Encryption)**: Elimina contraseñas, usa cifrado automático (público en aeropuertos).
* **Configuraciones críticas**:
  + Desactivar **WPS** (vulnerable a fuerza bruta).
  + Usar **filtrado MAC** (solo dispositivos autorizados).

**2. Detección de Intrusos**

* **Herramientas**:
  + **Snort**: IDS (Sistema de Detección de Intrusos) basado en reglas.
  + **Suricata**: Similar a Snort, pero con soporte para IPv6 y multihilo.