Tecnología de Redes de Computadoras

A continuación se presenta una lista de 100 puntos clave que abarcan ampliamente el alcance de un curso o esquema de autoestudio de “Tecnología de Redes de Computadoras”, tocando conceptos fundamentales, protocolos y aplicaciones prácticas.

1. Definición de una Red de Computadoras: Un sistema de dispositivos interconectados que comparten recursos y datos.
2. Funciones Primarias de las Redes: Compartición de recursos, comunicación, transmisión de datos y colaboración.
3. Evolución de las Redes: Desde ARPANET y las primeras LAN hasta el Internet global que tenemos hoy.
4. Tipos Comunes de Redes: LAN (Red de Área Local), MAN (Red Metropolitana), WAN (Red de Área Amplia).
5. Estructuras de Topología: Bus, estrella, anillo, malla y híbrida.
6. Intranet vs. Extranet vs. Internet: Diferencias de alcance y casos de uso típicos.
7. Organizaciones Estándar: IEEE, IETF, ISO—definiendo y manteniendo estándares y protocolos de red.
8. Modelo de Referencia OSI: Un marco conceptual de siete capas para entender las funciones de la red.
9. Modelo TCP/IP: Un modelo pragmático de cuatro (o a veces cinco) capas que sustenta Internet.
10. Comparación de OSI y TCP/IP: Similitudes (enfoque en capas) y diferencias (número de capas y abstracción).
11. Propósito de la Capa Física: Se ocupa de la transmisión de bits crudos sobre un medio físico.
12. Medios de Transmisión Comunes: Cable de par trenzado, cable coaxial, fibra óptica y wireless.
13. Ancho de Banda vs. Rendimiento: Tasa máxima teórica vs. tasa de transferencia de datos real.
14. Codificación de Señales: Métodos (por ejemplo, codificación Manchester) para representar bits de datos para la transmisión.
15. Técnicas de Modulación: AM, FM, PM utilizadas en conversiones analógicas a digitales o digitales a analógicas.
16. Dispositivos de Capa Física: Hubs, repetidores—principalmente repitiendo señales sin inspección.
17. Propósito de la Capa de Enlace de Datos: Maneja el encuadre, direccionamiento, detección/corrección de errores y control de flujo.
18. Encuadre: Encapsulando paquetes en encabezados y colas de la capa de enlace de datos.
19. Dirección MAC (Control de Acceso al Medio): Un identificador de hardware único para tarjetas de interfaz de red.

20. Mecanismos de Detección de Errores: Verificación de paridad, CRC (Cyclic Redundancy Check), sumas de verificación.
21. Bases de Ethernet: La tecnología LAN más común; utiliza una estructura de trama con MAC de origen/destino.
22. Formato de Trama Ethernet: Preamble, MAC de destino, MAC de origen, tipo/longitud, carga útil, CRC.
23. Conmutación: Reenvío de tramas utilizando tablas de direcciones MAC en una LAN.
24. Proceso de Aprendizaje en Conmutadores: Construcción de una tabla de direcciones MAC a medida que los dispositivos se comunican.
25. VLAN (Red Local Virtual): Segmentación lógica de una LAN física en múltiples redes virtuales.
26. Propósito de la Capa de Red: Enrutamiento, direccionamiento lógico (IP) y determinación de ruta.
27. Formato de Dirección IPv4: Dirección de 32 bits, generalmente representada en notación decimal con puntos.
28. Clases IPv4 (Obsoletas): Clase A, B, C, D, E (contexto histórico, reemplazadas por CIDR).
29. CIDR (Enrutamiento Inter-Dominio sin Clases): Enfoque moderno para una asignación de direcciones IP más flexible.
30. IPv4 vs. IPv6: Diferencias clave (direccionamiento de 128 bits, formato de encabezado expandido, auto-configuración).
31. Subredes: Dividir una red grande en subredes más pequeñas para un uso eficiente de direcciones.
32. NAT (Traducción de Direcciones de Red): Mapeo de direcciones IP privadas a una IP pública para conservar direcciones IPv4.
33. ARP (Protocolo de Resolución de Direcciones): Resolviendo direcciones IP a direcciones MAC dentro de una LAN.
34. ICMP (Protocolo de Mensajes de Control de Internet): Herramienta de diagnóstico—utilizada por ping, traceroute.
35. Enrutamiento vs. Conmutación: El enrutamiento es para el nivel IP (Capa 3), mientras que la conmutación es para el nivel MAC (Capa 2).
36. Enrutamiento Estático: Configuración manual de rutas en la tabla de enrutamiento de un enrutador.
37. Protocolos de Enrutamiento Dinámico: RIP (Protocolo de Información de Enrutamiento), OSPF (Open Shortest Path First), BGP (Protocolo de Puerta de Enlace de Borde).
38. Bases de Enrutadores: Determina el siguiente salto de red para un paquete basado en direcciones IP.
39. Propósito de la Capa de Transporte: Entrega de datos de extremo a extremo, confiabilidad y control de flujo.

40. TCP (Protocolo de Control de Transmisión): Protocolo orientado a conexión que proporciona transferencia de datos confiable.
41. Estructura del Segmento TCP: Puerto de origen, puerto de destino, número de secuencia, número de confirmación, etc.
42. Apretón de Manos de Tres Vías de TCP: Proceso SYN, SYN-ACK, ACK para la configuración de conexión.
43. Desconexión de Cuatro Vías de TCP: Secuencia FIN, FIN-ACK, ACK para cerrar una conexión.
44. Control de Flujo TCP: Mecanismos como la ventana deslizante para gestionar tasas de transferencia de datos.
45. Control de Congestión TCP: Algoritmos (inicio lento, evitación de congestión, recuperación rápida, retransmisión rápida).
46. UDP (Protocolo de Datagramas de Usuario): Sin conexión, con sobrecarga mínima, sin garantía de entrega.
47. Estructura del Segmento UDP: Puerto de origen, puerto de destino, longitud, suma de verificación, datos.
48. Números de Puerto: Identificadores para servicios (por ejemplo, 80 para HTTP, 443 para HTTPS, 53 para DNS).
49. Socket: Combinación de una dirección IP y un puerto utilizado para identificar un punto final.
50. Propósito de la Capa de Aplicación: Proporciona servicios de red a aplicaciones de usuario.
51. HTTP (Protocolo de Transferencia de Hipertexto): La base de la comunicación de datos en la web.
52. Métodos HTTP: GET, POST, PUT, DELETE, HEAD, etc.
53. HTTPS: HTTP cifrado utilizando TLS/SSL para comunicación web segura.
54. DNS (Sistema de Nombres de Dominio): Mapa nombres de dominio (por ejemplo, example.com) a direcciones IP.
55. Proceso de Resolución DNS: Consultas recursivas e iterativas, servidores raíz, servidores TLD, servidores autoritativos.
56. FTP (Protocolo de Transferencia de Archivos): Protocolo legado para transferencias de archivos sobre TCP (puertos 20/21).
57. Protocolos de Correo Electrónico: SMTP (Enviar), POP3 e IMAP (Recuperar).
58. DHCP (Protocolo de Configuración Dinámica de Host): Asigna automáticamente direcciones IP a dispositivos.
59. Telnet vs. SSH: Protocolos de acceso remoto—SSH está cifrado, Telnet no.
60. Modelo Cliente-Servidor: Una arquitectura común donde un cliente solicita servicios de un servidor.

61. Modelo P2P (Par a Par): Cada nodo puede tanto solicitar como proporcionar servicios.
62. Tecnologías Web: URLs, URIs, cookies, sesiones, estructura básica de aplicaciones web.
63. Principios de Seguridad de Red: Confidencialidad, integridad, disponibilidad (tríada CIA).
64. Amenazas de Seguridad Comunes: Malware (virus, gusanos, troyanos), ataques DDoS, phishing, inyección SQL.
65. Firewalls: Filtra el tráfico basado en reglas, colocado en los límites de la red.
66. IDS/IPS (Sistemas de Detección/Prevención de Intrusos): Monitorea el tráfico en busca de actividades sospechosas.
67. VPN (Red Privada Virtual): Túnel cifrado sobre una red pública, asegurando conexiones remotas.
68. TLS/SSL (Seguridad de la Capa de Transporte / Capa de Sockets Segura): Cifrado para transferencia de datos segura.
69. Bases de Criptografía: Criptografía simétrica vs. asimétrica, intercambio de claves, firmas digitales.
70. Certificados Digitales: Proporcionados por CAs (Autoridades de Certificación) para validar la identidad y habilitar HTTPS.
71. Políticas de Seguridad de Red: Directrices que rigen el uso seguro de la red, controles de acceso y auditorías.
72. DMZ (Zona Desmilitarizada): Una subred que expone servicios orientados al exterior al público.
73. Seguridad WLAN: Redes inalámbricas (Wi-Fi) aseguradas por WPA2, WPA3, etc.
74. Seguridad Física: Asegurar que la infraestructura de red (servidores, cables, enrutadores) esté alojada de manera segura.
75. Ingeniería Social: Tácticas de intrusión no técnicas—phishing, pretexting, cebo.
76. Ataques de Capa OSI: Diferentes amenazas/defensas en cada capa (por ejemplo, suplantación ARP en la capa de enlace de datos).
77. Herramientas de Administración de Red: ping, traceroute, netstat, nslookup, dig.
78. Capturadores de Paquetes: Herramientas como Wireshark o tcpdump para analizar el tráfico a nivel de paquete.
79. Protocolos de Gestión de Red: SNMP (Protocolo Simple de Gestión de Red).
80. Registro y Monitoreo: Syslog, registros de eventos, soluciones SIEM para detección en tiempo real.
81. Configuración Básica de LAN: Determinar rangos IP, máscaras de subred, puerta de enlace, servidores DNS.
82. Tipos de Cable: CAT5, CAT5e, CAT6, fibra óptica, cuándo se utiliza cada uno.

83. Cableado Estructurado: Estándares para instalaciones de red a gran escala profesionales.
84. Configuración de Conmutador: Creación de VLAN, puertos trunk y protocolos de árbol de expansión.
85. Configuración de Enrutador: Configuración de rutas (estáticas/dinámicas), NAT, ACL (Listas de Control de Acceso).
86. Reglas Básicas de Firewall: Denegar todo el tráfico entrante excepto el necesario, permitir todo el tráfico saliente o limitar según sea necesario.
87. Planes de Direccionamiento de Red: Asignación eficiente de direcciones IP según el departamento o subredes.
88. Redundancia y Failover: Uso de enlaces de respaldo, balanceo de carga o VRRP/HSRP para alta disponibilidad.
89. QoS (Calidad de Servicio): Priorizar cierto tráfico (por ejemplo, VoIP) para garantizar el rendimiento.
90. Bases de Redes en la Nube: Redes virtuales, grupos de seguridad, equilibradores de carga en entornos en la nube.
91. SDN (Redes Definidas por Software): Separación del plano de control del plano de datos para gestión centralizada.
92. Virtualización: Uso de hipervisores (VMware, Hyper-V, KVM) para crear servidores/virtuales de red.
93. Contenedores y Microservicios: Redes Docker, conceptos de red Kubernetes.
94. Implementación de IPv6: Dual stack (IPv4/IPv6), auto-configuración IPv6 (SLAAC), túneles IPv6.
95. Equilibrio de Carga DNS: Distribución del tráfico entre múltiples servidores mediante DNS round robin.
96. Computación de Borde: Procesamiento en el borde de la red para reducir la latencia para IoT y servicios en tiempo real.
97. 5G y Evolución Inalámbrica: Mayores tasas de datos, menor latencia, uso en IoT y banda ancha móvil.
98. Pasos de Solución de Problemas de Red: Identificar el problema, aislar, probar hipótesis, solucionar, verificar.
99. Documentación: Importancia de mantener diagramas de red y configuraciones de dispositivos precisos.
100. Aprendizaje Continuo: La informática es siempre cambiante, requiriendo estudio continuo de nuevos protocolos y mejores prácticas.

Estos 100 puntos resumen los temas esenciales en redes de computadoras, abarcando teoría fundamental, protocolos, hardware, direccionamiento, seguridad y tendencias modernas. Deberían ayudarte a guiar tu revisión y estudio para exámenes o comprensión práctica de la informática de red.