Technologie des Réseaux Informatiques

Voici une liste de 100 points clés qui couvrent globalement le domaine d'un cours ou d'un plan d'auto-apprentissage sur la "Technologie des Réseaux Informatiques", abordant les concepts fondamentaux, les protocoles et les applications pratiques.

1. Définition d'un Réseau Informatique : Un système de dispositifs interconnectés qui partagent des ressources et des données.
2. Fonctions Principales des Réseaux : Partage de ressources, communication, transmission de données et collaboration.
3. Évolution des Réseaux : De ARPANET et des premiers LAN à l'Internet mondial d'aujourd'hui.
4. Types de Réseaux Courants : LAN (Réseau Local), MAN (Réseau Métropolitain), WAN (Réseau Étendu).
5. Structures de Topologie : Bus, étoile, anneau, maillage et hybride.
6. Intranet vs. Extranet vs. Internet : Différences de portée et cas d'utilisation typiques.
7. Organisations de Normalisation : IEEE, IETF, ISO—définissant et maintenant les normes et protocoles de réseau.
8. Modèle de Référence OSI : Un cadre conceptuel à sept couches pour comprendre les fonctions de réseau.
9. Modèle TCP/IP : Un modèle pragmatique à quatre couches (ou parfois cinq couches) qui sous-tend l'Internet.
10. Comparaison de OSI et TCP/IP : Similarités (approche en couches) et différences (nombre de couches et abstraction).
11. But de la Couche Physique : Concernée par la transmission de bits bruts sur un support physique.
12. Supports de Transmission Courants : Câble à paires torsadées, câble coaxial, fibre optique et sans fil.
13. Bande Passante vs. Débit : Taux théorique maximum vs. taux de transfert de données réel.
14. Codage de Signal : Méthodes (par exemple, codage Manchester) pour représenter les bits de données pour la transmission.
15. Techniques de Modulation : AM, FM, PM utilisées dans les conversions analogique-numérique ou numérique-analogique.
16. Dispositifs de Couche Physique : Hubs, répéteurs—principalement répétant les signaux sans inspection.
17. But de la Couche de Liaison de Données : Gère le cadrage, l'adressage, la détection/correction d'erreurs et le contrôle de flux.

18. Cadrage : Encapsulation des paquets dans des en-têtes et des trailers de couche de liaison de données.
19. Adresse MAC (Media Access Control) : Un identifiant matériel unique pour les cartes d'interface réseau.
20. Mécanismes de Détection d'Erreurs : Parité, CRC (Cyclic Redundancy Check), sommes de contrôle.
21. Bases de l'Ethernet : La technologie LAN la plus courante ; utilise une structure de trame avec MAC source/destination.
22. Format de Trame Ethernet : Préambule, MAC destination, MAC source, type/longueur, charge utile, CRC.
23. Commutation : Transmission de trames en utilisant des tables d'adresses MAC dans un LAN.
24. Processus d'Apprentissage dans les Commutateurs : Construction d'une table d'adresses MAC lorsque les dispositifs communiquent.
25. VLAN (Réseau Local Virtuel) : Segmentation logique d'un LAN physique en plusieurs réseaux virtuels.
26. But de la Couche Réseau : Routage, adressage logique (IP) et détermination du chemin.
27. Format d'Adresse IPv4 : Adresse 32 bits, généralement représentée en notation décimale pointée.
28. Classes IPv4 (Obsolètes) : Classe A, B, C, D, E (contexte historique, remplacées par CIDR).
29. CIDR (Classless Inter-Domain Routing) : Approche moderne pour une allocation d'adresses IP plus flexible.
30. IPv4 vs. IPv6 : Différences clés (adressage 128 bits, format d'en-tête étendu, auto-configuration).
31. Sous-réseautage : Division d'un grand réseau en sous-réseaux plus petits pour une utilisation efficace des adresses.
32. NAT (Network Address Translation) : Mappage des adresses IP privées à une adresse IP publique pour conserver les adresses IPv4.
33. ARP (Address Resolution Protocol) : Résolution des adresses IP en adresses MAC au sein d'un LAN.
34. ICMP (Internet Control Message Protocol) : Outil de diagnostic—utilisé par ping, traceroute.
35. Routage vs. Commutation : Le routage est pour le niveau IP (Couche 3), tandis que la commutation est pour le niveau MAC (Couche 2).
36. Routage Statique : Configuration manuelle des routes dans la table de routage d'un routeur.
37. Protocoles de Routage Dynamique : RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol).
38. Bases du Routeur : Détermine le prochain saut de réseau pour un paquet en fonction des adresses IP.
39. But de la Couche Transport : Livraison de données de bout en bout, fiabilité et contrôle de flux.

40. TCP (Transmission Control Protocol) : Protocole orienté connexion fournissant un transfert de données fiable.
41. Structure du Segment TCP : Port source, port destination, numéro de séquence, numéro d'accusé de réception, etc.
42. Établissement de Connexion TCP à Trois Voies : Processus SYN, SYN-ACK, ACK pour l'établissement de connexion.
43. Fermeture de Connexion TCP à Quatre Voies : Séquence FIN, FIN-ACK, ACK pour fermer une connexion.
44. Contrôle de Flux TCP : Mécanismes comme la fenêtre coulissante pour gérer les taux de transfert de données.
45. Contrôle de Congestion TCP : Algorithmes (démarrage lent, évitement de congestion, récupération rapide, retransmission rapide).
46. UDP (User Datagram Protocol) : Sans connexion, faible surcharge, sans garantie de livraison.
47. Structure du Segment UDP : Port source, port destination, longueur, somme de contrôle, données.
48. Numéros de Port : Identifiants pour les services (par exemple, 80 pour HTTP, 443 pour HTTPS, 53 pour DNS).
49. Socket : Combinaison d'une adresse IP et d'un port utilisée pour identifier un point de terminaison.
50. But de la Couche Application : Fournit des services réseau aux applications utilisateur.
51. HTTP (Hypertext Transfer Protocol) : La base de la communication de données sur le web.
52. Méthodes HTTP : GET, POST, PUT, DELETE, HEAD, etc.
53. HTTPS : HTTP chiffré utilisant TLS/SSL pour une communication web sécurisée.
54. DNS (Domain Name System) : Mappe les noms de domaine (par exemple, example.com) aux adresses IP.
55. Processus de Résolution DNS : Requêtes récursives et itératives, serveurs racine, serveurs TLD, serveurs d'autorité.
56. FTP (File Transfer Protocol) : Protocole hérité pour les transferts de fichiers sur TCP (ports 20/21).
57. Protocoles de Courrier Électronique : SMTP (Envoi), POP3 et IMAP (Récupération).
58. DHCP (Dynamic Host Configuration Protocol) : Assigne automatiquement des adresses IP aux dispositifs.
59. Telnet vs. SSH : Protocoles d'accès à distance—SSH est chiffré, Telnet ne l'est pas.
60. Modèle Client-Serveur : Une architecture courante où un client demande des services à un serveur.
61. Modèle P2P (Pair-à-Pair) : Chaque nœud peut à la fois demander et fournir des services.

62. Technologies Web : URLs, URIs, cookies, sessions, structure de base d'application web.
63. Principes de Sécurité Réseau : Confidentialité, intégrité, disponibilité (triade CIA).
64. Menaces de Sécurité Courantes : Malware (virus, vers, chevaux de Troie), attaques DDoS, phishing, injection SQL.
65. Pare-feu : Filtre le trafic en fonction des règles, placé aux frontières du réseau.
66. IDS/IPS (Systèmes de Détection/Prévention d'Intrusion) : Surveille le trafic pour des activités suspectes.
67. VPN (Réseau Privé Virtuel) : Tunnel chiffré sur un réseau public, sécurisant les connexions à distance.
68. TLS/SSL (Transport Layer Security / Secure Sockets Layer) : Chiffrement pour le transfert de données sécurisé.
69. Bases de la Cryptographie : Chiffrement symétrique vs. asymétrique, échange de clés, signatures numériques.
70. Certificats Numériques : Fournis par les AC (Authorities Certificates) pour valider l'identité et permettre HTTPS.
71. Politiques de Sécurité Réseau : Directives gouvernant l'utilisation sécurisée du réseau, les contrôles d'accès et l'audit.
72. DMZ (Zone Démilitarisée) : Un sous-réseau qui expose les services orientés vers l'extérieur au public.
73. Sécurité WLAN : Réseaux sans fil (Wi-Fi) sécurisés par WPA2, WPA3, etc.
74. Sécurité Physique : Assurer que l'infrastructure réseau (serveurs, câbles, routeurs) est logée en toute sécurité.
75. Ingénierie Sociale : Tactiques d'intrusion non techniques—phishing, prétexte, appât.
76. Attaques par Couche OSI : Différentes menaces/défenses à chaque couche (par exemple, usurpation d'ARP à la couche de liaison de données).
77. Outils d'Administration Réseau : ping, traceroute, netstat, nslookup, dig.
78. Analyseurs de Paquets : Outils comme Wireshark ou tcpdump pour analyser le trafic au niveau des paquets.
79. Protocoles de Gestion Réseau : SNMP (Simple Network Management Protocol).
80. Journalisation et Surveillance : Syslog, journaux d'événements, solutions SIEM pour la détection en temps réel.
81. Configuration de Base de LAN : Détermination des plages IP, masques de sous-réseau, passerelle, serveurs DNS.
82. Types de Câbles : CAT5, CAT5e, CAT6, fibre optique, quand chacun est généralement utilisé.

83. Câblage Structuré : Normes pour les installations de réseau à grande échelle professionnelles.
84. Configuration du Commutateur : Création de VLAN, ports de tronc, et protocoles d'arbre couvrant.
85. Configuration du Routeur : Configuration des routes (statiques/dynamiques), NAT, ACL (Listes de Contrôle d'Accès).
86. Règles de Pare-feu de Base : Refuser tout le trafic entrant sauf les requis, autoriser tout le trafic sortant ou le limiter selon les besoins.
87. Plans d'Adressage Réseau : Attribution efficace des adresses IP en fonction du département ou des sous-réseaux.
88. Redondance et Basculement : Utilisation de liaisons de secours, équilibrage de charge ou VRRP/HSRP pour une haute disponibilité.
89. QoS (Qualité de Service) : Priorisation de certains trafics (par exemple, VoIP) pour assurer les performances.
90. Bases du Réseau Cloud : Réseaux virtuels, groupes de sécurité, équilibreurs de charge dans les environnements cloud.
91. SDN (Software-Defined Networking) : Séparation du plan de contrôle du plan de données pour une gestion centralisée.
92. Virtualisation : Utilisation d'hyperviseurs (VMware, Hyper-V, KVM) pour créer des serveurs/virtualiser des réseaux.
93. Conteneurs et Microservices : Réseaux Docker, concepts de mise en réseau Kubernetes.
94. Déploiement IPv6 : Double pile (IPv4/IPv6), auto-configuration IPv6 (SLAAC), tunnels IPv6.
95. Équilibrage de Charge DNS : Distribution du trafic à travers plusieurs serveurs via DNS round robin.
96. Calcul à la Périphérie : Traitement à la périphérie du réseau pour réduire la latence pour l'IoT et les services en temps réel.
97. 5G et Évolution Sans Fil : Taux de données plus élevés, latence plus faible, utilisation dans l'IoT et le large bande mobile.
98. Étapes de Dépannage Réseau : Identifier le problème, isoler, tester les hypothèses, réparer, vérifier.
99. Documentation : Importance de maintenir des diagrammes de réseau et des configurations de dispositifs précis.
100. Apprentissage Continu : Le réseau informatique évolue constamment, nécessitant une étude continue des nouveaux protocoles et des meilleures pratiques.

Ces 100 points résument les sujets essentiels en réseaux informatiques, couvrant la théorie de base, les protocoles, le matériel, l'adressage, la sécurité et les tendances modernes. Ils devraient aider à guider votre révision et votre étude pour les examens ou la compréhension pratique des réseaux informatiques.