コンピュータネットワーク技術

以下は、「コンピュータネットワーク技術」のコースまたは自習の概要を広くカバーする 100 の重要なポイントのリストです。基本的な概念、プロトコル、および実用的な応用について触れています。

1. コンピュータネットワークの定義：リソースとデータを共有するために相互に接続されたデバイスのシステムです。
2. ネットワークの主要な機能：リソース共有、通信、データ伝送、協力。
3. ネットワークの進化：ARPANET と初期の LAN から、今日のグローバルなインターネットまで。
4. 一般的なネットワークの種類：LAN（ローカルエリアネットワーク）、MAN（都市エリアネットワーク）、WAN（ワイドエリアネットワーク）。
5. トポロジ構造：バス、スター、リング、メッシュ、ハイブリッド。
6. イントラネット対エクストラネット対インターネット：範囲の違いと一般的な使用例。
7. 標準化機関：IEEE、IETF、ISO—ネットワークの標準とプロトコルを定義し維持する。
8. OSI 参照モデル：ネットワーク機能を理解するための 7 層の概念的フレームワーク。
9. TCP/IP モデル：インターネットの基盤となる 4 層（または時には 5 層）の実用的なモデル。
10. OSI と TCP/IP の比較：類似点（層化アプローチ）と違い（層の数と抽象化）。
11. 物理層の目的：物理的なメディアを通じて生のビットの伝送に関する。
12. 一般的な伝送媒体：トワイストペアケーブル、同軸ケーブル、光ファイバー、無線。
13. バンド幅対スループット：理論的な最大率対実際のデータ転送率。
14. シグナルエンコーディング：データビットを伝送するための方法（例：マンチェスターエンコーディング）。
15. 変調技術：AM、FM、PM はアナログからデジタルまたはデジタルからアナログの変換に使用されます。
16. 物理層デバイス：ハブ、リピーター—主に信号を検査せずに繰り返します。
17. データリンク層の目的：フレーミング、アドレス付け、エラーチェック/修正、フロー制御を処理します。
18. フレーミング：データリンク層のヘッダーとトレーラーでパケットをカプセル化します。
19. MAC（メディアアクセス制御）アドレス：ネットワークインターフェースカードの一意のハードウェア識別子。
20. エラーチェック機構：パリティチェック、CRC（サイクリックレダンドシーチェック）、チェックサム。
21. イーサネットの基本：最も一般的な LAN 技術；ソース/デスティネーション MAC を使用するフレーム構造。

22. イーサネットフレーム形式：プレアブル、デスティネーション MAC、ソース MAC、タイプ/長さ、ペイロード、CRC。
23. スイッチング：LAN で MAC アドレステーブルを使用してフレームを転送します。
24. スイッチの学習プロセス：デバイスが通信する際に MAC アドレスのテーブルを構築します。
25. VLAN（仮想 LAN）：1 つの物理 LAN を複数の仮想ネットワークに論理的に分割します。
26. ネットワーク層の目的：ルーティング、論理アドレス（IP）、パス決定。
27. IPv4 アドレス形式：32 ビットアドレス、通常はドット付き 10 進数表記で表示されます。
28. IPv4 クラス（廃棄）：クラス A、B、C、D、E（歴史的背景、CIDR に置き換えられました）。
29. CIDR（クラスレスインタードメインルーティング）：より柔軟な IP アドレス割り当てのための現代的なアプローチ。
30. IPv4 対 IPv6：主要な違い（128 ビットアドレス、拡張ヘッダー形式、自動構成）。
31. サブネット化：効率的なアドレス使用のために大きなネットワークを小さなサブネットに分割します。
32. NAT（ネットワークアドレス変換）：IPv4 アドレスを節約するためにプライベート IP アドレスをパブリック IP にマッピングします。
33. ARP（アドレス解決プロトコル）：LAN 内で IP アドレスを MAC アドレスに解決します。
34. ICMP（インターネット制御メッセージプロトコル）：診断ツール—ping、traceroute で使用されます。
35. ルーティング対スイッチング：ルーティングは IP レベル（層 3）、スイッチングは MAC レベル（層 2）です。
36. 静的ルーティング：ルーターのルーティングテーブルにルートを手動で構成します。
37. 動的ルーティングプロトコル：RIP（ルーティング情報プロトコル）、OSPF（オープンショートパスファースト）、BGP（ボーダーゲートウェイプロトコル）。
38. ルーターの基本：IP アドレスに基づいてパケットの次のネットワークホップを決定します。
39. トランスポート層の目的：エンドツーエンドのデータ配送、信頼性、フロー制御。
40. TCP（トランスミッションコントロールプロトコル）：信頼性のあるデータ転送を提供する接続指向型プロトコル。
41. TCP セグメント構造：ソースポート、デスティネーションポート、シーケンス番号、アクノウレジメント番号など。
42. TCP の 3 ウェイハンドシェイク：接続設定のための SYN、SYN-ACK、ACK プロセス。
43. TCP の 4 ウェイテアダウン：接続を閉じるための FIN、FIN-ACK、ACK シーケンス。
44. TCP フロー制御：スライディングウィンドウなどのメカニズムを使用してデータ転送率を管理します。

45. TCP 混雑制御：アルゴリズム（スロースター、混雑回避、ファストリカバリー、ファストリトランスミット）。
46. UDP（ユーザーデータグラムプロトコル）：接続なし、最小限のオーバーヘッド、配送の保証なし。
47. UDP セグメント構造：ソースポート、デスティネーションポート、長さ、チェックサム、データ。
48. ポート番号：サービスの識別子（例：80 は HTTP、443 は HTTPS、53 は DNS）。
49. ソケット：IP アドレスとポートの組み合わせを使用してエンドポイントを識別します。
50. アプリケーション層の目的：ユーザーアプリケーションにネットワークサービスを提供します。
51. HTTP（ハイパーテキスト転送プロトコル）：ウェブ上のデータ通信の基盤。
52. HTTP メソッド：GET、POST、PUT、DELETE、HEAD など。
53. HTTPS：TLS/SSL を使用して暗号化された HTTP—安全なウェブ通信。
54. DNS（ドメインネームシステム）：ドメイン名（例：example.com）を IP アドレスにマッピングします。
55. DNS 解決プロセス：再帰的および反復的なクエリ、ルートサーバー、TLD サーバー、権威サーバー。
56. FTP（ファイル転送プロトコル）：TCP（ポート 20/21）を使用したファイル転送のレガシープロトコル。
57. メールプロトコル：SMTP（送信）、POP3 および IMAP（取得）。
58. DHCP（動的ホスト構成プロトコル）：デバイスに自動的に IP アドレスを割り当てます。
59. Telnet 対 SSH：リモートアクセスプロトコル—SSH は暗号化されていますが、Telnet は暗号化されていません。
60. クライアントサーバーモデル：クライアントがサーバーからサービスをリクエストする一般的なアーキテクチャ。
61. P2P（ピアツーピア）モデル：各ノードがサービスをリクエストおよび提供できます。
62. ウェブ技術：URL、URI、クッキー、セッション、基本的なウェブアプリケーション構造。
63. ネットワークセキュリティの原則：機密性、整合性、利用可能性（CIA 三要素）。
64. 一般的なセキュリティ脅威：マルウェア（ウイルス、ワーム、トロイの木馬）、DDoS 攻撃、フィッシング、SQL インジェクション。
65. ファイアウォール：ルールに基づいてトラフィックをフィルタリングし、ネットワークの境界に配置します。
66. IDS/IPS（侵入検出/防止システム）：トラフィックを監視して疑わしい活動を検出します。
67. VPN（仮想プライベートネットワーク）：パブリックネットワーク上の暗号化されたトンネル、リモート接続のセキュリティを確保します。
68. TLS/SSL（トランスポートレイヤセキュリティ/セキュアソケットレイヤ）：セキュアなデータ転送のための暗号化。

69. 暗号化の基本：対称式暗号化対非対称暗号化、キー交換、デジタル署名。
70. デジタル証明書：CA（証明書認証局）から提供され、ID を検証し HTTPS を有効にします。
71. ネットワークセキュリティポリシー：安全なネットワーク使用、アクセス制御、監査のガイドライン。
72. DMZ（デミリタライズドゾーン）：外部向けサービスを公開するサブネット。
73. WLAN セキュリティ：WPA2、WPA3 などでセキュリティが確保された無線ネットワーク（Wi-Fi）。
74. 物理的セキュリティ：サーバー、ケーブル、ルーターなどのネットワークインフラが安全に収納されていることを確認します。
75. ソーシャルエンジニアリング：非技術的な侵入手法—フィッシング、プレテキスト、エサ。
76. OSI 層攻撃：各層（例：データリンク層の ARP スプーフィング）の異なる脅威/防御。
77. ネットワーク管理ツール：ping、traceroute、netstat、nslookup、dig。
78. パケットスニッファー：Wireshark や tcpdump などのツールを使用してパケットレベルでトラフィックを分析します。
79. ネットワーク管理プロトコル：SNMP（シンプルネットワーク管理プロトコル）。
80. ロギングとモニタリング：Syslog、イベントログ、SIEM ソリューションによるリアルタイム検出。
81. 基本的な LAN 設定：IP 範囲、サブネットマスク、ゲートウェイ、DNS サーバーを決定します。
82. ケーブルの種類：CAT5、CAT5e、CAT6、光ファイバー、それぞれの一般的な使用例。
83. 結構化ケーブリング：プロフェッショナルな大規模ネットワークインストールのための標準。
84. スイッチの設定：VLAN の作成、トランクポート、スパニングツリープロトコル。
85. ルーターの設定：ルート（静的/動的）、NAT、ACL（アクセス制御リスト）の設定。
86. 基本的なファイアウォールルール：必要なもの以外はすべての受信を拒否し、すべての送信を許可または必要に応じて制限します。
87. ネットワークアドレス計画：部門またはサブネットに基づいて効率的に IP アドレスを割り当てます。
88. 冗長性とフェイルオーバー：バックアップリンク、ロードバランシング、または VRRP/HSRP を使用して高可用性を実現します。
89. QoS（サービス質）：VoIP などの特定のトラフィックを優先してパフォーマンスを確保します。
90. クラウドネットワーキングの基本：クラウド環境の仮想ネットワーク、セキュリティグループ、ロードバランサ。
91. SDN（ソフトウェア定義ネットワーク）：中央管理のために制御プレーンをデータプレーンから分離します。
92. バーチャライゼーション：ハイパーバイザ（VMware、Hyper-V、KVM）を使用して仮想サーバー/ネットワークを作成します。

93. コンテナとマイクロサービス：Docker ネットワーク、Kubernetes ネットワーキング概念。
94. IPv6 展開：デュアルスタック（IPv4/IPv6）、IPv6 自動構成（SLAAC）、IPv6 トンネル。
95. DNS ロードバランシング：DNS ラウンドロビンを使用して複数のサーバーにトラフィックを分配します。
96. エッジコンピューティング：IoT およびリアルタイムサービスの遅延を減らすためにネットワークエッジで処理します。
97. 5G と無線の進化：より高いデータレート、低遅延、IoT およびモバイルブロードバンドの使用。
98. ネットワークトラブルシューティングの手順：問題を特定し、分離し、仮説をテストし、修正し、検証します。
99. ドキュメント化：正確なネットワーク図とデバイス設定を維持する重要性。
100. 継続的な学習：ネットワーキングは常に進化しているため、新しいプロトコルとベストプラクティスの継続的な学習が必要です。

これらの 100 のポイントは、コンピュータネットワークの基本理論、プロトコル、ハードウェア、アドレス付け、セキュリティ、現代のトレンドを網羅する基本的なトピックをまとめたものです。試験の準備やコンピュータネットワーキングの実用的な理解をサポートするためのガイドとして役立つでしょう。