



CompTIA Network+

認定資格試験

出題範囲

試験番号：N10-008



試験について

CompTIA Network+ (N10-008) 認定資格試験は、以下の必要な知識とスキルを持っていることを証明します：

- 有線 / 無線デバイスを設定し、ネットワーク接続を確立する
- ネットワーク文書を理解・維持する
- ネットワークサービスの目的を理解している
- データセンター、クラウド、仮想ネットワークングに関する基本的なコンセプトを理解している
- ネットワークアクティビティをモニターし、パフォーマンスと可用性に関する問題を特定する
- ネットワークのハードニング手法を実施する
- ネットワークインフラストラクチャの管理、構成、およびトラブルシューティングを行う

CompTIA Network+ は、初級ネットワーク管理者およびネットワークサポート技術者としての、9～12 カ月の実務経験で得られる知識とスキルを目安に設計されています。

出題範囲に掲載された項目は、認定資格試験の目的を明確にするためのものであり、試験の出題内容を完全に網羅したものではありません。

認定資格試験の認証

CompTIA Network+ (N10-008) 資格試験は、国際標準化機構 (ISO)17024 標準への準拠を国家規格協会 (ANSI) より認定されており、出題範囲の定期的な見直しとアップデートが行われています。

試験開発

CompTIA 試験は、エントリーレベルの IT プロフェッショナルに必要とされるスキルと知識に関して検討する、専門分野のエキスパートによるワークショップ、および業界全体へのアンケート調査結果に基づいて策定されています。

CompTIA 認定教材の使用に関するポリシー

CompTIA Certifications, LLC は、無許可の第三者トレーニングサイト（通称「ブレインダンプ」）とは提携関係がなく、これらが提供するいかなるコンテンツも公認・推薦・容認しません。CompTIA の認定資格試験の受験準備にこのような教材を使用した個人は、CompTIA 受験者同意書の規定に基づいて資格認定を取り消され、その後の受験資格を停止されます。CompTIA では、無許可教材の使用に関する試験実施ポリシーをよりよく理解していただくための取り組みを進めています。認定資格試験を受験される方は、[CompTIA 認定資格試験実施ポリシー](#)をご一読ください。CompTIA の認定資格試験を受験するための学習を始める前には、必ず CompTIA が定めるすべてのポリシーをご確認ください。受験者には、[CompTIA 受験者同意書](#)の規定を遵守することが求められています。個々の教材が無許可扱いになるかどうかを確認するには、CompTIA (examsecurity@comptia.org) までメールにてご確認ください。

注意事項

箇条書きで挙げられた項目は、すべての試験内容を網羅するものではありません。この出題範囲に掲載がない場合でも、各分野に関連する技術、プロセス、あるいはタスクを含む問題が出題される可能性があります。CompTIA では、提供している認定資格試験の内容に現在必要とされているスキルを反映するため、また試験問題の信頼性維持のため、継続的な試験内容の検討と問題の改訂を行っています。必要な場合、現在の出題範囲を基に試験を改訂する場合があります。この場合、現在の試験に関連する資料・教材等は、継続的にご利用いただくことが可能です。

試験情報

試験番号	N10-008
問題数	最大 90 問
出題形式	単一 / 複数選択、パフォーマンスベーステスト
試験時間	90 分
推奨される経験	<ul style="list-style-type: none">• CompTIA A+ 認定資格または同等の知識• CompTIA Network+ は、初級ネットワーク管理者およびネットワークサポート技術者としての、9~12 カ月の実務経験に相当するスキルを評価します
合格スコア	720 (100~900 のスコア形式)

試験の出題範囲 (試験分野)

下表は、この試験における試験分野 (ドメイン) と出題比率の一覧です。

試験分野	出題比率
1.0 ネットワーキングの基礎	24%
2.0 ネットワークの実装	19%
3.0 ネットワークオペレーション	16%
4.0 ネットワークセキュリティ	19%
5.0 ネットワークのトラブルシューティング	22%
計	100%



1.0 ネットワーキングの基礎

1.1 Open Systems Interconnection (OSI) 参照モデルの各レイヤーと、カプセル化のコンセプトを比較対照することができる。

- **OSI 参照モデル**
 - レイヤー 1 - 物理層
 - レイヤー 2 - データリンク層
 - レイヤー 3 - ネットワーク層
 - レイヤー 4 - トランスポート層
 - レイヤー 5 - セッション層
 - レイヤー 6 - プレゼンテーション層
 - レイヤー 7 - アプリケーション層
- **OSI 参照モデルのコンテキスト内におけるデータのカプセル化と非カプセル化**
 - イーサネットヘッダ
 - インターネットプロトコル (IP) スキーム
 - Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) ヘッダ
 - TCP フラグ
 - ペイロード
 - Maximum Transmission Unit (MTU)

1.2 ネットワークのトポロジーとタイプを説明することができる。

- メッシュ
- スター / ハブアンドスポーク
- バス
- リング
- ハイブリッド
- ネットワークのタイプと特性
 - ピアツーピア
 - クライアント - サーバー
 - Local Area Network (LAN)
 - Metropolitan Area Network (MAN)
 - Wide Area Network (WAN)
 - Wireless Local Area Network (WLAN)
 - Personal Area Network (PAN)
 - Campus Area Network (CAN)
- Storage Area Network (SAN)
- Software-Defined Wide Area Network (SDWAN)
- MultiProtocol Label Switching (MPLS)
- Multipoint Generic Routing Encapsulation (mGRE)
- サービスに関連するエントリーポイント
 - 責任分界点
 - スマートジャック
- 仮想ネットワークのコンセプト
 - vSwitch
 - 仮想ネットワークインターフェースカード (vNIC)
 - ネットワーク機能仮想化 (NFV)
 - ハイパーバイザー
- プロバイダーリンク
 - 衛星
 - デジタル加入者回線 (DSL)
 - ケーブル
 - リース回線
 - メトロオプティカル

1.3 ケーブルとコネクタの各タイプを要約し、どれが特定のソリューションに適したタイプかを説明することができる。

- カッパーケーブル（銅線）
 - ツイストペア
 - Cat 5
 - Cat 5e
 - Cat 6
 - Cat 6a
 - Cat 7
 - Cat 8
 - 同軸 /RG-6
 - ツインアキシャル
 - 終端処理規格
 - TIA/EIA-568A
 - TIA/EIA-568B
- 光ファイバー
 - シングルモード
 - マルチモード
- コネクタのタイプ
 - Local Connector (LC), Straight Tip (ST), Subscriber Connector (SC), Mechanical Transfer (MT), Registered Jack (RJ)
 - Angled Physical Contact (APC)
 - Ultra-Physical Contact (UPC)
- RJ11
- RJ45
- F タイプコネクタ
- トランシーバー / メディアコンバーター
- トランシーバーのタイプ
 - Small Form-factor Pluggable (SFP)
 - Enhanced Form-factor Pluggable (SFP+)
 - Quad Small Form-factor Pluggable (QSFP)
 - Enhanced Quad Small Form-factor Pluggable (QSFP+)
- ケーブル管理
 - パッチパネル / パッチベイ
 - ファイバー配線パネル
 - パンチダウンブロック
 - 66
 - 110
 - Krone
 - Bix
- イーサネット規格
 - カッパー
 - 10BASE-T
 - 100BASE-TX
 - 1000BASE-T
 - 10GBASE-T
 - 40GBASE-T
 - 光ファイバー
 - 100BASE-FX
 - 100BASE-SX
 - 1000BASE-SX
 - 1000BASE-LX
 - 10GBASE-SR
 - 10GBASE-LR
 - Coarse Wavelength Division Multiplexing (CWDM)
 - Dense Wavelength Division Multiplexing (DWDM)
 - Bidirectional Wavelength Division Multiplexing (WDM)

1.4 与えられたシナリオに基づいて、サブネットを構成し、適切な IP アドレス指定スキームを使用することができる。

- パブリックとプライベート
 - RFC1918
 - ネットワークアドレス変換 (NAT)
 - ポートアドレス変換 (PAT)
- IPv4 と IPv6
 - Automatic Private IP Addressing (APIPA)
 - Extended Unique Identifier (EUI-64)
 - マルチキャスト
 - ユニキャスト
 - エニーキャスト
 - ブロードキャスト
 - リンクローカル
 - ループバック
 - デフォルトゲートウェイ
- IP v 4 サブネット
 - クラスレス（可変長サブネットマスク）
- クラスフル
 - A
 - B
 - C
 - D
 - E
- Classless Inter-Domain Routing (CIDR) 表記
- IPv6 のコンセプト
 - トンネリング
 - デュアルスタック
 - 略記法
 - ルーター広告
 - Stateless Address Autoconfiguration (SLAAC)
- 仮想 IP (VIP)
- サブインターフェース

1.5 一般的なポートとプロトコル、それらの用途、および暗号化された代替手段を説明することができる。

プロトコル	ポート
• File Transfer Protocol (FTP)	20/21
• Secure Shell (SSH)	22
• Secure File Transfer Protocol (SFTP)	22
• Telnet	23
• Simple Mail Transfer Protocol (SMTP)	25
• ドメイン名システム (DNS)	53
• Dynamic Host Configuration Protocol (DHCP)	67/68
• Trivial File Transfer Protocol (TFTP)	69
• Hypertext Transfer Protocol (HTTP)	80
• Post Office Protocol v3 (POP3)	110
• Network Time Protocol (NTP)	123
• Internet Message Access Protocol (IMAP)	143
• Simple Network Management Protocol (SNMP)	161/162
• Lightweight Directory Access Protocol (LDAP)	389
• Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)]	443
• HTTPS [Transport Layer Security (TLS)]	443
• Server Message Block (SMB)	445
• Syslog	514
• SMTP TLS	587
• Lightweight Directory Access Protocol (over SSL) (LDAPS)	636
• IMAP over SSL	993
• POP3 over SSL	995
• Structured Query Language (SQL) サーバー	1433
• SQLnet	1521
• MySQL	3306
• Remote Desktop Protocol (RDP)	3389
• Session Initiation Protocol (SIP)	5060/5061
• IP プロトコルの種類	
- Internet Control Message Protocol (ICMP)	
- TCP	
- UDP	
- Generic Routing Encapsulation (GRE)	
- Internet Protocol Security (IPSec)	
- 認証ヘッダ (AH)/ セキュリティペイロードのカプセル (ESP)	
• コネクションレスとコネクション指向	

1.6 ネットワークサービスの使用と目的を説明することができる。

- DHCP
 - スコープ
 - 除外範囲
 - 予約
 - 動的割り当て
 - 静的割り当て
 - リース期間
 - スコープオプション
 - 利用可能なリース
 - DHCP リレー
 - IP ヘルパー /UDP フォワーディング
- DNS
 - レコードタイプ
 - アドレス (A vs. AAAA)
 - 正規名 (CNAME)
 - メールエクスチェンジ (MX)
 - Start Of Authority (SOA)
 - ポインタ (PTR)
 - テキスト (TXT)
 - サービス (SRV)
 - ネームサーバー (NS)
 - グローバル階層
 - ルート DNS サーバー
 - 内部と外部
 - ゾーン転送
- 信頼できるネームサーバー
- Time to live (TTL)
- DNS キャッシュ
- リバース DNS/逆引き検索/正引き検索
- 再帰的検索 / 反復検索
- NTP
 - 層
 - クライアント
 - サーバー

1.7 基本的な企業とデータセンターのネットワークアーキテクチャを説明することができる。

- 三層構成
 - コア
 - ディストリビューション / アグリゲーション層
 - アクセス / エッジ
- ソフトウェア定義ネットワーク
 - アプリケーション層
 - コントロール層
 - インフラストラクチャ層
 - 管理プレーン
- スパインアンドリーフ
 - ソフトウェア定義ネットワーク
 - トップオブブラックスイッチ
 - バックボーン
- トラフィックフロー
 - ノースサウス
 - イーストウエスト
- 支社、オンプレミスデータセンター、コロケーション
- ストレージ領域のネットワーク
 - 接続の種類
 - Fibre Channel over Ethernet (FCoE)
 - ファイバーチャネル
 - Internet Small Computer Systems Interface (iSCSI)

1.8 クラウドのコンセプトと接続性に関する選択肢を要約することができる。

- 導入モデル
 - パブリック
 - プライベート
 - ハイブリッド
 - コミュニティー
- サービスモデル
 - Software as a Service (SaaS)
 - Infrastructure as a Service (IaaS)
 - Platform as a Service (PaaS)
 - Desktop as a Service (DaaS)
- Infrastructure as Code
 - オートメーション / オークストレーション
- 接続オプション
 - 仮想プライベートネットワーク (VPN)
 - クラウドプロバイダーへのプライベート直接接続
- マルチテナント
- エラスティシティ (弾性)
- スケーラビリティ (拡張性)
- セキュリティ関連事項



2.0 ネットワークの実装

2.1 様々なデバイスとその機能、およびネットワークへの適切な配置を比較対照することができる。

- ネットワークデバイス
 - レイヤー 2 スイッチ
 - レイヤー 3 スイッチ
 - ルーター
 - ハブ
 - アクセスポイント
 - ブリッジ
 - ワイヤレス LAN コントローラー
 - ロードバランサー
 - プロキシサーバー
 - ケーブルモデム
 - DSL モデム
 - リピーター
- ボイスゲートウェイ
 - メディアコンバーター
 - 侵入防止システム (IPS)/ 侵入検知システム (IDS) デバイス
 - ファイアウォール
 - VPN ヘッドエンド
- ネットワークデバイス
 - Voice over Internet Protocol (VoIP) 電話
 - プリンター
 - 制御システムへの物理的アクセス
 - カメラ
 - 暖房、換気、空調 (HVAC) センサー
- モノのインターネット (IoT)
 - 冷蔵庫
 - スマートスピーカー
 - スマート温度調節器
 - スマートドアベル
- 産業用制御システム / supervisory control and data acquisition (SCADA)

2.2 ルーティング技術と帯域幅管理のコンセプトを比較対照することができる。

- ルーティング
 - 静的ルーティング
 - デフォルトルート
 - アドミニストレーティブディスタンス
 - 外部と内部
 - Time to live
 - 動的ルーティング
 - プロトコル [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)]
 - リンクステート、ディスタンスベクター、ハイブリッド
- 帯域幅管理
 - トラフィックシェーピング
 - Quality of Service (QoS)



2.3 与えられたシナリオに基づいて、イーサネットの一般的なスイッチング機能を構成、デプロイすることができる。

- Data Virtual Local Area Network (VLAN)
- ボイス VLAN
- ポート構成
 - ポートタギング /802.1Q
 - ポート集約
 - Link Aggregation Control Protocol (LACP)
 - デュプレックス
 - 速度
 - フローコントロール
 - ポートミラーリング
- ポートセキュリティ
- ジャンボフレーム
- Auto-Medium-Dependent Interface Crossover (MDI-X)
- Media Access Control (MAC) アドレステーブル
- Power over Ethernet (PoE) /Power over Ethernet plus (PoE+)
- スパニングツリープロトコル
- 搬送波感知多重アクセス / 衝突検知 (CSMA/CD)
- アドレス解決プロトコル (ARP)
- 近隣探索プロトコル

2.4 与えられたシナリオに基づいて、適切なワイヤレス規格とワイヤレステクノロジーをインストールし、構成することができる。

- 802.11 規格
 - a
 - b
 - g
 - n (WiFi 4)
 - ac (WiFi 5)
 - ax (WiFi 6)
- 周波数と帯域
 - 2.4GHz
 - 5GHz
- チャンネル
 - 規制による影響
- チャンネルボンディング
- サービスセット識別子 (SSID)
 - 基本サービスセット (BSS/Basic Service Set)
 - 拡張サービスセット (ESS/Extended Service Set)
 - 独立基本サービスセット (Adhoc)
 - ローミング
- アンテナの種類
 - 無指向性
 - 指向性
- 暗号化規格
 - WiFi Protected Access (WPA)/ WPA2 Personal [Advanced Encryption Standard (AES)/ Temporal Key Integrity Protocol (TKIP)]
 - WPA/WPA2 エンタープライズ (AES/TKIP)
- 携帯電話テクノロジー
 - 符号分割多元接続 (CDMA)
 - Global System for Mobile Communications (GSM)
 - Long-Term Evolution (LTE)
 - 3G、4G、5G
- Multiple input, multiple output (MIMO)、マルチユーザー MIMO (MU-MIMO)



3.0 ネットワークオペレーション

3.1 与えられたシナリオに基づいて、適切な統計とセンサーを使用し、ネットワークの可用性を確保することができる。

- パフォーマンス指標 / センサー
 - デバイス / 筐体
 - 温度
 - 中央演算処理装置 (CPU) 使用率
 - メモリ
 - ネットワーク指標
 - 帯域幅
 - レイテンシー
 - ジッター
- SNMP
 - トラップ
 - オブジェクト識別子 (OID)
 - 管理情報ベース (MIB)
- ネットワークデバイスログ
 - ログのレビュー
 - トラフィックログ
 - 監査ログ
 - Syslog
 - ログingleレベル / 深刻度
- インターフェースの統計情報 / ステータス
 - リンク状態 (アップ / ダウン)
 - 速度 / デュプレックス
 - 送信 / 受信トラフィック
 - 巡回冗長検査 (CRC)
 - プロトコルのパケット数とバイト数
- インターフェースのエラーまたはアラート
 - CRC エラー
 - ジャイアント
 - ラント
 - カプセル化のエラー
- 環境的要因とセンサー
 - 温度
 - 湿度
 - 電気
 - フラットディング
- ベースライン
- NetFlow データ
- アップタイム / ダウンタイム

3.2 組織の文書とポリシーの目的を説明することができる。

- 計画と手順
 - 変更管理
 - インシデントレスポンス計画
 - 災害復旧計画
 - 事業継続計画
 - システムライフサイクル
 - 標準作業書
- ハードニングとセキュリティポリシー
 - パスワードポリシー
 - 利用規約
 - デバイス持ち込み (BYOD) ポリシー
 - リモートアクセスポリシー
- オンボーディングポリシーとオフボーディングポリシー
 - セキュリティポリシー
 - データ漏洩の防止
- 一般文書
 - 物理的ネットワーク図
 - 設計図
 - ラック図
 - 中間配線盤 (IDF) / 主配線盤 (MDF) 文書
 - 論理ネットワーク構成図
 - 配線図
- 現地調査レポート
 - 監査レポートとアセスメントレポート
 - ベースライン構成
- 一般的な同意文書
 - 秘密保持契約 (NDA)
 - サービスレベルアグリーメント (SLA)
 - 覚書 (MOU)



3.3 高可用性と災害復旧のコンセプトを説明し、 どれが最適なソリューションかを要約することができる。

- ロードバランシング
- マルチパス
- ネットワークインターフェースカード (NIC) チーミング
- 冗長ハードウェア / クラスタ
 - スイッチ
 - ルーター
 - ファイアウォール
- 施設とインフラストラクチャのサポート
 - 無停電電源 (UPS)
 - 配電ユニット (PDU)
 - 発電機
 - HVAC
 - 消火
- 冗長性と高可用性 (HA) に関するコンセプト
 - コールドサイト
 - ウォームサイト
 - ホットサイト
 - クラウドサイト
 - アクティブ - アクティブと
アクティブ - パッシブ
 - 複数のインターネットサービス
プロバイダー (ISP) / 多様な経路
 - Virtual Router Redundancy
Protocol (VRRP) / First Hop
Redundancy Protocol (FHRP)
 - 平均修復時間 (MTTR)
 - 平均故障間隔 (MTBF)
 - 目標復旧時間 (RTO)
 - 目標復旧時点 (RPO)
- ネットワークデバイスのバックアップと復元
 - 状態
 - 構成



4.0 ネットワークセキュリティ

4.1 一般的なセキュリティのコンセプトを説明できる。

- 機密性、完全性、可用性 (CIA)
- 脅威
 - 内部
 - 外部
- 脆弱性
 - 共通脆弱性識別子 (CVE)
 - ゼロデイ攻撃
- エクスプロイト
- 最小権限
- ロールベースアクセス
- ゼロトラスト
- 多層防御
 - ネットワークセグメンテーションの実施
 - 境界ネットワーク
[旧称：非武装地帯 (DMZ)]
 - 職務分離
- ネットワークアクセス制御
 - ハニーポット
- 認証方法
 - 多要素
 - Terminal Access Controller Access-Control System Plus (TACACS+)
 - シングルサインオン (SSO)
 - Remote Authentication Dial-in User Service (RADIUS)
 - LDAP
 - ケルベロス
 - ローカル認証
 - 802.1X
 - Extensible Authentication Protocol (EAP)
- リスクマネジメント
 - セキュリティリスク評価
 - 脅威アセスメント
 - 脆弱性アセスメント
 - ペネトレーションテスト
 - ポスチャアセスメント
 - ビジネスリスク評価
 - プロセスアセスメント
 - ベンダーアセスメント
- セキュリティ情報とイベントマネジメント (SIEM)

4.2 一般的なタイプの攻撃を比較対照することができる。

- テクノロジー型
 - サービス拒否 (DoS)/分散型サービス拒否 (DDoS)
 - ボットネット / コマンド
 - アンドコントロール
 - On-Path 攻撃 (旧称：中間者攻撃)
 - DNS ポイズニング
 - VLAN ホッピング
 - ARP スプーフィング
 - 不正な DHCP
- 不正なアクセスポイント (AP)
 - エビルツイン
 - ランサムウェア
 - パスワード攻撃
 - ブルートフォース攻撃
 - 辞書攻撃
 - MAC スプーフィング
 - IP スプーフィング
 - 認証解除
 - マルウェア
- 人為的と環境
 - ソーシャルエンジニアリング
 - フィッシング
 - テールゲート (共連れ)
 - ビギーバック
 - ショルダーサーフィン

4.3 与えられたシナリオに基づいて、ネットワークのハードニング手法を適用できる。

- ベストプラクティス
 - セキュア SNMP
 - ルーター広告 (RA) 保護
 - ポートセキュリティ
 - 動的 ARP インспекション
 - コントロールプレーンポリシング
 - プライベート VLAN
 - 不要なスイッチポートの無効化
 - 不要なサービスの無効化
 - デフォルトパスワードの変更
 - パスワード複雑性ルール
- DHCP スヌーピングの有効化
 - デフォルト VLAN の変更
 - パッチとファームウェアの管理
 - アクセスコントロールリスト
 - ロールベースアクセス
 - ファイアウォールルール
 - 明示的な拒否
 - 暗黙の拒否
- ワイヤレスセキュリティ
 - MAC フィルタリング
 - アンテナの配置
- 電力レベル
 - ワイヤレスクライアントの隔離
 - ゲストネットワークの隔離
 - 事前共有鍵 (PSK)
 - EAP
 - ジオフェンシング
 - キャプティブポータル
- IoT アクセスの検討事項

4.4 リモートアクセスの各手法と、それがセキュリティに与える影響を比較対照できる。

- サイトツーサイト VPN
- クライアントツーサイト VPN
 - クライアントレス VPN
 - スプリットトンネルとフルトンネル
- リモートデスクトップ接続
- リモートデスクトップゲートウェイ
- SSH
- 仮想ネットワークコンピューティング (VNC)
- 仮想デスクトップ
- 認証と承認に関する検討事項
- インバンドとアウトオブバンド

4.5 物理的セキュリティの重要性について説明することができる。

- 検知手段
 - カメラ
 - 人感センサー
 - アセットタグ
 - タンパー検知
- 防止手段
 - 社員教育
 - アクセスコントロールハードウェア
 - バッジリーダー
 - 生体認証
 - 鍵のかかるラック
- キャビネットの施錠
 - アクセスコントロールが実施されている出入口 (旧称: マントラップ)
 - スマートロッカー
- 資産の処分
 - 工場出荷状態へのリセット / 構成の消去
 - 処分に向けたデバイスのサニタイズ



5.0 ネットワークのトラブルシューティング

5.1 ネットワークのトラブルシューティング方法について説明することができる。

- 問題を特定する
 - 情報を収集する
 - ユーザーに質問する
 - 症状を特定する
 - 変更された部分の有無を判定する
 - 可能であれば、問題を再現する
 - 複数の問題に個別に取り組む
- 想定される原因の仮説を立てる
 - 明白と思われる点も確認する
- 複数の方法を考える
 - 上位から下位 / 下位から上位の OSI 参照モデル
 - 分割統治
- 仮説を検証して原因を特定する
 - 仮説が証明された場合、問題解決に向けた今後の対応を決定する
 - 仮説が証明されなかった場合、仮説を立て直すか、エスカレーションする
- 問題解決のための対応計画を策定し、潜在的な影響を分析する
- 計画を実行するか、必要に応じてエスカレーションする
- システム全体の機能を検証し、必要に応じて予防対策を実施する
- 発見事項、対策、結果、および得られた教訓を文書化する

5.2 与えられたシナリオに基づいて、ケーブル接続に関する一般的な問題をトラブルシューティングし、適切なツールを選択することができる。

- 仕様と制限
 - スループット
 - 速度
 - 距離
- ケーブルに関する検討事項
 - シールドケーブルと非シールドケーブル
 - プレナムケーブルとライザーケーブル
- ケーブルの用途
 - ロールオーバーケーブル / コンソールケーブル
 - クロスオーバーケーブル
 - Power over Ethernet
- 一般的な問題
 - 減衰
 - 干渉
- デシベル (dB) ロス
 - 不正確なピンアウト
 - 不正なポート
 - オープン / ショート
 - 発光ダイオード (LED) ステータスインジケータ
 - 不正確なトランシーバー
 - デュプレックスの問題
 - 送受信 (TX/RX) の逆転
 - 光ケーブルの汚れ
- 一般的なツール
 - ケーブルクリンパー
 - パンチダウンツール
 - トーンジェネレーター
 - ループバックアダプター
- 光時間領域反射率計 (OTDR)
 - マルチメーター
 - ケーブルテスター
 - 配線図
 - タップ
 - フュージョンプライサー
 - スペクトラムアナライザー
 - はさみ / カッター
 - ケーブルストリッパー
 - ファイバー光メーター



5.3 与えられたシナリオに基づいて、ネットワークソフトウェアの適切なツールとコマンドを使うことができる。

- ソフトウェアツール
 - WiFi アナライザー
 - プロトコルアナライザー / パケットキャプチャ
 - 帯域幅速度テスター
 - ポートスキャナー
 - iperf
 - NetFlow アナライザー
 - Trivial File Transfer Protocol (TFTP) サーバー
- 端末エミュレータ
- IP スキャナ
- コマンドラインツール
 - ping
 - ipconfig/ifconfig/ip
 - nslookup/dig
 - traceroute/tracert
 - arp
 - netstat
 - hostname
- route
- telnet
- tcpdump
- nmap
- 基本的なネットワークプラットフォームコマンド
 - show interface
 - show config
 - show route

5.4 与えられたシナリオに基づいて、ワイヤレス接続に関する一般的な問題をトラブルシューティングすることができる。

- 仕様と制限
 - スループット
 - 速度
 - 距離
 - Received Signal Strength Indication (RSSI) 信号強度
 - 実効等方放射電力 (EIRP)/電力設定
- 検討事項
 - アンテナ
- 配置
- タイプ
- 偏波 (ポラリゼーション)
- チャンネルの使用状況
- AP アソシエーションタイム
- 現地調査
- 一般的な問題
 - 干渉
 - チャンネルのオーバーラップ
 - アンテナケーブルの減衰 / 信号ロス
- RF の減衰 / 信号ロス
- 正しくない SSID
- 正しくないパスフレーズ
- 暗号化プロトコルの不一致
- 不十分なワイヤレスカバー
- キャプティブポータルの問題
- クライアントの接続解除に関する問題

5.5 与えられたシナリオに基づいて、ネットワークに関する総合的な問題をトラブルシューティングすることができる。

- 検討事項
 - デバイス構成のレビュー
 - ルーティングテーブル
 - インターフェースのステータス
 - VLAN 割り当て
 - ネットワークパフォーマンスのベースライン
- 一般的な問題
 - コリジョン
 - ブロードキャストストーム
 - MAC アドレスの重複
 - IP アドレスの重複
 - マルチキャストフラッド
- 非対称ルーティング
- スイッチンググループ
- ルーティンググループ
- 不正な DHCP サーバー
- DHCP スコープの枯渇
- IP 設定の問題
 - 不正確なゲートウェイ
 - 不正確なサブネットマスク
 - 不正確な IP アドレス
 - 不正確な DNS
- 存在しないルート
- 光量不足
- 証明書の問題
- ハードウェア障害
- ホスト型 / ネットワーク型ファイアウォールの設定
- サービス、ポート、またはアドレスのブロック
- 不正確な VLAN
- DNS の問題
- NTP の問題
- BYOD にまつわる課題
- ライセンス済み機能の問題
- ネットワークパフォーマンスの問題

Network+ (N10-008) 略語リスト

下記は CompTIA Network+ 認定資格試験で使用される略語の一覧です。包括的な試験準備プログラムの一環として、リストを復習し、知識の習得に努めてください。

略語	詳細説明	略語	詳細説明
AAAA	Authentication, Authorization, Accounting, Auditing	FCoE	Fibre Channel over Ethernet
ACL	Access Control List	FHRP	First Hop Redundancy Protocol
AES	Advanced Encryption Standard	FTP	File Transfer Protocol
AH	Authentication Header	GBIC	Gigabit Interface Converter
AP	Access Point	GRE	Generic Routing Encapsulation
APC	Angled Physical Contact	GSM	Global System for Mobile Communications
APIPA	Automatic Private Internet Protocol Addressing	HA	High Availability
ARP	Address Resolution Protocol	HDMI	High-Definition Multimedia Interface
AUP	Acceptable Use Policy	HTTP	Hypertext Transfer Protocol
BGP	Border Gateway Protocol	HTTPS	Hypertext Transfer Protocol Secure
BNC	British Naval Connector/Bayonet Niell-Concelman	HVAC	Heating, ntilation, d Air Conditioning
BYOD	Bring Your Own Device	IaaS	Infrastructure as a Service
CAM	Content Addressable Memory	ICMP	Internet Control Message Protocol
CAN	Campus Area Network	ICS	Industrial Control System
CDMA	Code Division Multiple Access	IDF	Intermediate Distribution Frame
CIA	Confidentiality, Integrity, and Availability	IDS	Intrusion Detection System
CIDR	Classless Inter-Domain Routing	IGMP	Internet Group Management Protocol
CLI	Command-Line Interface	IMAP	Internet Message Access Protocol
CNAME	Canonical Name	IoT	Internet of Things
CPU	Central Processing Unit	IP	Internet Protocol
CRC	Cyclic Redundancy Check	IPS	Intrusion Prevention System
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance	IPSec	Internet Protocol Security
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection	IPv4	Internet Protocol version 4
CSU	Channel Service Unit	IPv6	Internet Protocol version 6
CVE	Common Vulnerabilities and Exposures	iSCSI	Internet Small Computer Systems Interface
CWDM	Coarse Wave Division Multiplexing	ISP	Internet Service Provider
DaaS	Desktop as a Service	LACP	Link Aggregation Control Protocol
dB	Decibel	LAN	Local Area Network
DDoS	Distributed Denial-of-Service	LC	Local Connector
DHCP	Dynamic Host Configuration Protocol	LDAP	Lightweight Directory Access Protocol
DLP	Data Loss Prevention	LDAPS	Lightweight Directory Access Protocol (over SSL)
DNS	Domain Name System	LED	Light-Emitting Diode
DoS	Denial-of-Service	LTE	Long-Term Evolution
DSL	Digital Subscriber Line	MAC	Media Access Control/Medium Access Control
DSU	Data Service Unit	MAN	Metropolitan Area Network
DWDM	Dense Wavelength Division Multiplexing	MDF	Main Distribution Frame
EAP	Extensible Authentication Protocol	MDIX	Media Dependent Interface Crossover
EIA	Electronic Industries Association	mGRE	Multipoint Generic Routing Encapsulation
EIGRP	Enhanced Interior Gateway Routing Protocol	MIB	Management Information Base
EIRP	Effective Isotropic Radiated Power	MIMO	Multiple Input, Multiple Output
ESP	Encapsulating Security Payload	MU-MIMO	Multiuser Multiple Input, Multiple Output
EUI	Extended Unique Identifier	MOU	Memorandum of Understanding
		MPLS	Multiprotocol Label Switching
		MTBF	Mean Time Between Failure
		MT-RJ	Mechanical Transfer - Registered Jack

略語	詳細説明
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
MX	Mail Exchanger
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NFV	Network Function Virtualization
NGFW	Next-Generation Firewall
NIC	Network Interface Card
NS	Name Server
NTP	Network Time Protocol
OID	Object Identifier
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
PaaS	Platform as a Service
PAN	Personal Area Network
PAT	Port Address Translation
PDU	Power Distribution Unit
PoE	Power over Ethernet
POP3	Post Office Protocol version 3
PSK	Pre-Shared Key
PTR	Pointer Record
QoS	Quality of Service
QSFP	Quad Small Form-factor Pluggable
RA	Router Advertisements
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Inexpensive (or Independent) Disks
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFC	Request for Comment
RG	Radio Guide
RIP	Routing Internet Protocol
RJ	Registered Jack
RPO	Recovery Point Objective
RSSI	Received Signal Strength Indication
RTO	Recovery Time Objective
RTSP	RealTime Streaming Protocol
SaaS	Software as a Service
SAN	Storage Area Network
SC	Standard Connector/Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Network
SDWAN	Software-Defined WAN
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol

略語	詳細説明
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLAAC	Stateless Address Auto-Configuration
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SOHO	Small Office Home Office
SQL	Structured Query Language
SRV	Service Record
SSD	Solid-State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
ST	Straight Tip or Snap Twist
STP	Spanning Tree Protocol
SYSLOG	System Log
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIA/EIA	Telecommunications Industry Association/Electronic Industries Alliance
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
TX/RX	Transmit and Receive
UDP	User Datagram Protocol
UPC	Ultra-Physical Contact
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTP	Unshielded Twister Pair
VIP	Virtual IP
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
vNIC	virtual Network Interface Card
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WAP	Wireless Access Point
WDM	Wavelength Division Multiplexing
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

Network+ ハードウェアとソフトウェアの一覧

CompTIA では、Network+ 認定資格試験の受験準備をされる方への参考用に、下記のハードウェアとソフトウェアのサンプル一覧を提示しています。トレーニングを実施している企業でも、トレーニングの提供に必要な実習室コンポーネントを作成したい場合に役立ちます。各トピックに箇条書きで挙げられた項目は例であり、すべてを網羅するものではありません。

機器

- ・光及びカッパーパッチパネル
- ・パンチダウンブロック
- ・レイヤー 2 スイッチ
- ・レイヤー 3 スイッチ
- ・PoE スイッチ
- ・ルーター
- ・ファイアウォール
- ・VPN ヘッドエンド
- ・ワイヤレスアクセスポイント
- ・仮想化をサポートするベシックノートパソコン
- ・タブレット / 携帯電話
- ・メディアコンバーター
- ・VoIP システム (電話を含む)

予備のハードウェア

- ・NIC
- ・電源
- ・GBIC
- ・SFP
- ・マネージドスイッチ
- ・ワイヤレスアクセスポイント
- ・UPS
- ・PoE インジェクター

予備のパーツ

- ・パッチケーブル
- ・RJ11 コネクタ
- ・RJ45 コネクタ、モジュージャック
- ・非シールドツイストペアケーブルスプール
- ・同軸ケーブルスプール
- ・F コネクタ
- ・ファイバーコネクタ
- ・アンテナ
- ・Bluetooth/ ワイヤレスアダプター
- ・コンソールケーブル (RS-232-USB シリアルアダプター)

ツール

- ・Telco/ ネットワーククリンパー
- ・ケーブルテスター
- ・パンチダウンツール
- ・ケーブルストリッパー
- ・同軸ケーブルクリンパー
- ・ワイヤーカッター
- ・トーンジェネレーター
- ・ファイバー終端キット
- ・光パワーメーター

ソフトウェア

- ・プロトコルアナライザー / パケットキャプチャ
- ・端末エミュレーションソフトウェア
- ・Linux OS/Windows OS
- ・ソフトウェアファイアウォール
- ・ソフトウェア IDS/IPS
- ・Nmap
- ・ハイパーバイザーソフトウェア
- ・仮想ネットワーク環境
- ・WiFi アナライザー
- ・スペクトラムアナライザー
- ・ネットワーク監視ツール
- ・DHCP サービス
- ・DNS サービス
- ・NetFlow アナライザー
- ・TFTP サーバー
- ・アップグレードに向けたファームウェアのバックアップ

その他

- ・サンプルネットワーク文書
- ・サンプルログ
- ・ケーブルの不具合
- ・ネットワーク構成図