CompTIA Network+認定資格試験出題範囲

試験番号：N10-006

はじめに

CompTIA Network+は、IT ネットワークプロフェッショナルに必要なスキルと知識を証明する国際的に認知されている認定資格です。

CompTIA Network+を取得することにより、トラブルシューティング、ネットワーク構成/設定、一般的な有線/無線ネットワークデバイスの管理、基本的なネットワーク設計と構築、ネットワークを管理する上で必要とされるドキュメントへの理解、ネットワークの制限や脆弱性への認識、ネットワークにおけるセキュリティの確立、業界標準、プロトコルなどに対し求められるスキルと知識を有していることが証明されます。

CompTIA Network+の受験者は、ユニファイドコミュニケーションやモバイル、クラウド、仮想化といった新しいテクノロジーに対するスキルが求められます。
CompTIA Network+は、ISO 17024より認定 （Personnel Certification Accreditation）を受けており、定期的な出題範囲の見直しおよびアップデートが行われています。

CompTIA Network+認定資格試験は、以下の条件を満たすITプロフェッショナルを対象としています。

- CompTIA A+認定資格、またはそれ同等の知識・スキルを所有していること（CompTIA A+は、CompTIA Network+受験の際の前提条件ではありません。）
- ITネットワークにおける最低9～12ヶ月の業務経験

この出題範囲には、試験分野、出題比率、出題例が含まれています。出題例は出題範囲を明確にするためであり、試験の出題内容そのものを反映している訳ではありませんので、ご注意ください。

以下は試験分野および各分野の出題比率表です。

試験分野	出題比率
第1章　ネットワーク設計	22%
第2章　ネットワーク運用	20%
第3章　ネットワークセキュリティ	18%
第4章　トラブルシューティング	24%
第5章　業界標準、標準手法、ネットワーク理論	16%
合計	100%

※分野別に取扱例があげられていますが、これらがすべての出題傾向を網羅しているわけではありません。また、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、あるいはタスクについて、試験に含まれる可能性があります。

※CompTIAは、配信されている試験内容を継続的にセキュリティ上問題がなく、最新の状態であることを監視しています。そのため、試験問題/本出題範囲は、必要に応じて、予告なく変更される場合がございます。予めご了承ください。

CompTIA Authorized Materials Use Policy

CompTIA では、パートナー契約を締結していない、もしくは承認、推奨、許可されていないサードパーティーのトレーニングサイトで提供されるコンテンツは容認、許可をしていません。CompTIA 認定資格試験の受験のためこれらの教材を利用することは、CompTIA Candidate Agreement の取り決めにより、将来的に受験ができなくなる可能性があります。認定を受けていない教材を利用することに対する CompTIA 認定資格試験の方針をより明確にするため、CompTIA では全ての受験者に対して CompTIA Certification Exam policy を下記の Web サイトにて公開しています。
https://certification.comptia.org/testing/test-policies/unauthorized-training-materials

CompTIA 認定資格試験への学習を始める前に、CompTIA のポリシーをご確認ください。また、全ての受験者は、全ての試験に対して CompTIA Candidate Agreement を遵守する必要があります。
http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx

受験者の方が、教材を利用する前に、これらの教材が不正な教材かどうかを判断していただくために、Cert Guard を利用して検索をしていただくことができます。
http://www.certguard.com/search.asp

もしくは、下記のリストを参照していただくことも可能です。
http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

※ 分野別に取扱例があげられていますが、これらがすべての出題傾向を網羅しているわけではありません。また、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、あるいはタスクについて、試験に含まれる可能性があります。

CompTIA は、配信されている試験内容を継続的にセキュリティ上問題がなく、最新の状態であることを監視しています。そのため、試験問題/本出題範囲は、必要に応じて、予告なく変更される場合がございます。予めご了承ください。また、変更がされた場合においても、全ての学習教材は、問題なくご活用いただけます。

第1章　ネットワーク設計（22%）

1.1　様々なネットワークデバイスの機能と役割について説明することができる。

- ルーター
- スイッチ
- マルチレイヤースイッチ
- ファイアウォール
- HIDS
- IDS/IPS
- アクセスポイント（無線/有線）
- コンテンツフィルタ
- 負荷分散装置（ロードバランサー）
- ハブ
- アナログモデム
- パケットシェイパー（ネットワーク帯域制御装置）
- VPN コンセントレーター

1.2　ネットワークサービスとアプリケーションの利用について比較対照することができる。

- VPN
  - サイト間/ホストとサイト間/ホスト間
  - プロトコル
    - IPsec
    - GRE
    - SSL VPN
    - PTP/PPTP
- TACACS/RADIUS
- RAS
- ウェブサービス
- ユニファイドボイスサービス
- ネットワークコントローラー

1.3　以下のネットワークサービス/アプリケーションの設置や設定を実施することができる。

- DHCP
  - 静的 IP アドレスの割り当てと動的 IP アドレスの割り当ての違い
  - 予約
  - スコープ
  - リース
  - オプション（DNS サーバー、サフィックス）
  - IP ヘルパー/DHCP リレー
- DNS
  - DNS サーバー
  - DNS レコード（A、MX、AAAA、CNAME、PTR）
  - ダイナミック DNS
- プロキシ/リバースプロキシ
- NAT
  - PAT
  - SNAT
  - DNAT

- ポートフォワーディング

1.4 様々な WAN テクノロジーの特徴とメリットを説明することができる。

- 光ファイバー
  - SONET
  - DWDM
  - CWDM
- フレームリレー
- 人工衛星（サテライト）
- 広域ケーブル（ブロードバンドケーブル）
- DSL/ADSL
- ISDN
- ATM
- PPP/マルチリンク PPP
- MPLS
- GSM/CDMA
  - LTE/4G
  - HSPA+
  - 3G
  - Edge
- ダイヤルアップ
- WiMAX
- メトロイーサー
- 専用線
  - T-1
  - T-3
  - E-1
  - E-3
  - OC3
  - OC12
- サーキットスイッチとパケットスイッチの違い

1.5 様々なケーブルとコネクタを適切なツールを使用して設置し、適切に接続することができる。

- コネクタ
  - RJ-11
  - RJ-45
  - RJ-48C
  - DB-9/RS-232
  - DB-25
  - UTP カプラ
  - BNC カプラ
  - BNC
  - F-connector
  - 110 ブロック端子
  - 66 ブロック端子
- カッパー・ケーブル（銅線）
  - シールド有無によるケーブル特性の違い
  - CAT3、CAT5、CAT5e、CAT6、CAT6a
  - PVC ケーブルとプレナムケーブルの違い

- RG-59
- RG-6
- ストレートスルー、クロスオーバー、ロールオーバーの違い

- 光ファイバーコネクタ
  - ST
  - SC
  - LC
  - MTRJ
  - FC
  - 光ファイバーカプラ
- 光ファイバーケーブル
  - シングルモード
  - マルチモード
  - APC と UPC の違い
- メディアコンバーター
  - イーサネットへのシングルモード光ファイバー
  - イーサネットへのマルチモード光ファイバー
  - 同軸ファイバー
  - マルチモードへのシングルモード
- ツール
  - ケーブルクリンパー
  - パンチダウンツール
  - ワイヤーストリッパー
  - スニッパー
  - OTDR
  - ケーブル認証テスター

1.6 一般的なネットワークトポロジーの違いを理解できる。

- メッシュ
  - パーシャル
  - フル
- バス
- リング
- スター
- ハイブリッド
- ポイントツーポイント
- ポイントツーマルチポイント
- クライアントサーバー
- ピアツーピア

1.7 ネットワーク構成の違いを理解できる。

- WAN
- MAN
- LAN
- WLAN
  - ホットスポット
- PAN
  - Bluetooth
  - 赤外線（IR）

- NFC
- SCADA/ICS
  - ICS サーバー
  - DCS/クローズドネットワーク
  - リモートターミナル装置
  - プログラマブルロジックコントローラ
- メディアネット
  - VTC
    - ISDN
    - IP/SIP

1.8 与えられたシナリオに基づいて、適切なアドレッシングスキームで実装、設定を行うことができる。

- IPv6
  - 自動生成
    - EUI 64
  - DHCP6
  - リンクローカル
  - アドレス構成
  - アドレス圧縮
  - IPv6 から IPv4、IPv4 から IPv6 へのチューニング
    - Teredo、miredo
- IPv4
  - アドレス構成
  - サブネッティング
  - APIPA
  - クラスフル A、B、C、D
  - クラスレス
- プライベートとパブリックの違い
- NAT/PAT
- MAC アドレッシング
- マルチキャスト
- ユニキャスト
- ブロードキャスト
- ブロードキャストドメインとコリジョンドメインの違い

1.9 基本的なルーティングコンセプトとプロトコルを説明することができる。

- ループバックインターフェース
- ルーティングループ
- ルーティングテーブル
- 静的ルーティングと動的ルーティングの違い
- デフォルトルーティング
- ディスタンスベクタールーティングプロトコル
  - RIP v2
- ハイブリットルーティングプロトコル
  - BGP
- リンクステートルーティングプロトコル
  - OSPF
  - IS-IS
- 内部ゲートウェイルーティングプロトコルと外部ゲートウェイルーティングプロトコルの違い

- AS 番号（Autonomous system number）
- ルートの再分配
- 高可用性
  - VRRP
  - Virtual IP
  - HSRP
- ルート集約
- ルートメトリック
  - ホップカウント
  - MTU、帯域幅
  - コスト
  - レイテンシー
  - アドミニストレーティブ ディスタンス
  - SPB

1.10 通信技術の基本要素を識別することができる。

- VoIP
- ビデオ
- リアルタイムサービス
  - プレゼンス
  - マルチキャストとユニキャストの違い
- QoS
  - DSCP
  - COS
- デバイス
  - UC サーバー
  - UC デバイス
  - UC ゲートウェイ

1.11 クラウドや仮想化をサポートするテクノロジーを比較対照することができる。

- 仮想化
  - 仮想スイッチ
  - 仮想ルーター
  - 仮想ファイアウォール
  - 仮想 NIC と物理 NIC の違い
  - SDN（Software defined networking）
- ストレージエリアネットワーク
  - iSCSI
  - ジャンボフレーム
  - ファイバーチャネル
  - NAS（Network attached storage）
- クラウドの概念
  - パブリック IaaS、SaaS、PaaS
  - プライベート IaaS、SaaS、PaaS
  - ハイブリッド IaaS、SaaS、PaaS
  - コミュニティ I IaaS、SaaS、PaaS

1.12 与えられた要件に応じて、基本的なネットワークを実装することができる。

- 要件のリスト
- デバイスの種類/デバイスの要件
- 環境の制限
- 機器の制限
- 互換性の要件
- 有線/無線の検討
- セキュリティの検討

第2章 ネットワーク運用（20%）

2.1 与えられたシナリオに基づいて、適切な監視ツールを使用することができる。

- パケットアナライザー/ネットワークアナライザー
- インターフェース監視ツール
- ポートスキャナー
- Top talker/ Top listener
- SNMP 監視ソフトウェア
  - Trap
  - Get
  - Walk
  - MIBS
- アラート
  - Email
  - SMS
- パケットフロー監視ツール
- syslog
- SIEM
- 環境監視ツール
  - 温度
  - 湿度
- 電源監視ツール
- ワイヤレスサーベイツール
- ワイヤレスアナライザー

2.2 与えられたシナリオに基づき、監視ツールやパフォーマンストラッキングツールから得た情報を分析、レポートすることができる。

- ベースライン
- ボトルネック
- ログ管理
- グラフ化
- 使用率
  - 帯域幅
  - ストレージ
  - ネットワークデバイス CPU
  - ネットワークデバイスメモリー
  - ワイヤレスチャネルの使用率
- リンクステータス
- インターフェース監視
  - エラー
  - 使用率
  - 破棄
  - パケットドロップ
  - インタフェースリセット
  - スピードと二重化

2.3 与えられたシナリオに基づいて、構成管理をサポートする適切なリソースを使用することができる。

- アーカイブ/バックアップ
- ベースライン
- モバイルデバイスのオンボードとオフボード
- NAC（Network Admission Control）
- 管理文書
  - ネットワーク構成図（論理構成/物理構成）
  - アセットマネジメント
  - IP アドレスの使用率
  - ベンダーより提供された文書
  - 内部の運用手順/ポリシー/標準

2.4 ネットワークをセグメント化する重要性について説明することができる。

- SCADA システム/産業制御システム（ICS）
- レガシーシステム
- プライベート/パブリックネットワークの分離
- ハニーポット/ハニーネット
- テストラボ
- ロードバランス
- パフォーマンスの最適化
- セキュリティ
- コンプライアンス

2.5 与えられたシナリオに基づき、パッチやアップデートを適用、インストールすることができる。

- OS アップデート
- ファームウェアアップデート
- ドライバーアップデート
- 変更/アップデートの特性
- メジャー/マイナーアップデートの違い
- 脆弱性に対するパッチ
- アップグレードとダウングレードの違い
  - コンフィグレーションのバックアップ

2.6 与えられたシナリオに基づき、適切な機能を利用してスイッチを設定することができる。

- VLAN
  - ネイティブ VLAN/デフォルト VLAN
  - VTP
- スパニングツリー（802.1d）/ラピッドスパニングツリー（802.1w）
  - フラッディング
  - フォワーディング/ブロッキング
  - フィルタリング
- インターフェース設定
  - トランキング/802.1q
  - タグ VLAN とアンタグ VLAN の違い
  - ポートボンディング（LACP）
  - ポートミラーリング（ローカルとリモートの違い）
  - スピードと二重化

- IP アドレスの割り当て
  - VLAN の割り当て
- デフォルトゲートウェイ
- PoE と PoE+（802.3af, 802.3at）
- スイッチの管理
  - ユーザー/パスワード
  - AAA の設定
  - コンソール
  - バーチャルターミナル
  - インバウンド/アウトバウンドの管理
- マネージドスイッチとアンマネージドスイッチの違い

2.7 ワイヤレス LAN の環境を実装、構成し、ワイヤレス対応デバイスを適切に実装することができる。

- スモールオフィス/ホームオフィス用ワイヤレスルーター
- ワイヤレスアクセスポイント
  - 高密度無線 LAN
  - ローミング
  - ワイヤレスコントローラー
    - VLAN プーリング（VLAN Select 機能）
    - LWAPP
- ワイヤレスブリッジ
- サイト調査
  - ヒートマップ
- 周波数
  - 2.4 Ghz
  - 5.0 Ghz
- チャネル
- グットプット
- 接続の種別
  - 802.11a-ht
  - 802.11g-ht
- アンテナの位置
- アンテナの種別
  - 無指向性
  - 一方向性
- MIMO と MU-MIMO の違い
- 信号強度
  - 範囲
  - デバイスのアンテナによる違い
- SSID ブロードキャスト
- トポロジー
  - アドホック
  - メッシュ
  - インフラストラクチャー
- モバイルデバイス
  - 携帯電話（スマートフォン）
  - ラップトップ（ノートパソコン）
  - タブレット
  - ゲーム機
  - メディアデバイス

第3章 ネットワークセキュリティ（18%）

3.1 リスクに関連する概念を比較参照することができる。

- 災害復旧
- 事業継続
- バッテリーバックアップ/UPS
- 第一応答者（ファーストレスポンダー）
- データ漏洩
- エンドユーザの意識向上とトレーニング
- 単一障害点
  - クリティカルノード
  - クリティカルアセット
  - 冗長化
- 規格とポリシーの遵守
- 脆弱性のスキャン
- ペネトレーションテスト

3.2 一般的なネットワークの脆弱性と脅威について比較参照することができる。

- 攻撃/脅威
  - DoS 攻撃
    - DDoS 攻撃
      - ボットネット
      - トラフィックスパイク
      - 調整攻撃
  - リフレクション攻撃/アンプ攻撃
    - DNS
    - NTP
    - Smurf 攻撃
  - 知人から/故意ではない DoS 攻撃
  - 物理攻撃
    - permanent DoS
  - ARP キャッシュポイズニング
  - パケット/プロトコルの悪用
  - スプーフィング
  - ワイヤレス
    - エビルツイン
    - 不正な AP
    - ウォードライビング
    - ウォーチョーキング
    - ブルージャッキング
    - ブルースナーフィング
    - WPA/WEP/WPS 攻撃
  - ブルートフォースアタック攻撃
  - セッションハイジャック
  - ソーシャルエンジニアリング
  - 中間者攻撃（マンインザミドル）
  - VLAN ホッピング
  - 感染したシステム
  - ネットワーク上のマルウェアの影響

- 内部者の脅威/悪意のある社員
- ゼロディ攻撃

- 脆弱性
  - 不必要なサービスの実行
  - 開いているポート
  - パッチがあてられていない/レガシーなシステム
  - 暗号化されていないチャネル
  - クリアテキスト証明書
  - セキュアではないプロトコル
    - TELNET
    - HTTP
    - SLIP
    - FTP
    - TFTP
    - SNMPv1 と SNMPv2
  - TEMPEST/RF emanation（漏洩電磁波）

3.3 与えられたシナリオに基づき、ネットワーク堅牢化の手法を実装することができる。

- アンチマルウェアソフトウェア
  - ホストベース
  - クラウド/サーバーベース
  - ネットワークベース
- スイッチポートセキュリティ
  - DHCP スヌーピング
  - ARP インスペクション
  - MAC アドレスフィルタリング
  - VLAN アサイメント
    - ネットワークセグメント
- セキュリティポリシー
- 不必要なネットワークサービスの無効化
- セキュアプロトコルの使用
  - SSH
  - SNMPv3
  - TLS/SSL
  - SFTP
  - HTTPS
  - IPsec
- アクセスリスト
  - ウェブ/コンテンツフィルタリング
  - ポートフィルタリング
  - IP フィルタリング
  - 暗黙の拒否
- ワイヤレスセキュリティ
  - WEP
  - WPA/WPA2
    - エンタープライズ
    - パーソナル
  - TKIP/AES
  - 802.1x
  - TLS/TTLS

- MAC フィルタリング
- ユーザー認証
  - CHAP/MSCHAP
  - PAP
  - EAP
  - Kerberos
  - 多要素認証
  - 二要素認証
  - シングルサインオン
- ハッシュ
  - MD5
  - SHA

3.4 物理的なセキュリティ制御を比較参照することができる。

- マントラップ
- ネットワーククローゼット
- ビデオモニタリング
  - IP カメラ/CCTV
- 入退出管理
- 非接触カード/キーフォブ
- バイオメトリック
- キーパッド/暗号ロック
- セキュリティガード
- サイファーロック錠

3.5 与えられたシナリオに基づき、基本的なファイアウォールの実装、設定をすることができる。

- ファイアウォールの種類
  - ホストベース
  - ネットワークベース
  - ソフトウェアとハードウェアの違い
  - アプリケーションアウェアネス/コンテクストアウェアネス
  - スモールオフィス/ホームオフィスファイアウォール
  - ステートフル、ステートレスインスペクションの違い
  - UTM
- 設定と手法
  - ACL
  - Virtual wire と Routed wire の違い
  - DMZ
  - 暗黙の拒否
  - ブロック/許可
    - アウトバウンドトラフィック
    - インバウンドトラフィック
  - ファイアウォールの場所
    - 内部/外部

3.6 様々なネットワークアクセスコントロールのモデルの目的について説明することができる。

- 802.1x
- Posture assessment

- ゲストネットワーク
- Persistent agent と non-persistent agent の違い
- 検疫ネットワーク
- エッジコントロールとアクセスコントロールの違い

3.7 基本的なフォレンジックの概念を要約することができる。

- 第一応答者（ファーストレスポンダー）
- エリアの保護
  - 必要時にエスカレーション
- 時系列の記録
- eDiscovery（電子証拠開示制度）
- 証拠/データの収集
- 証拠保管の継続性（チェインオブカストディ/Chain of custody）
- データのトランスポート
- フォレンジックレポート
- 訴訟ホールド

第4章 トラブルシューティング（24%）

4.1 与えられたシナリオに基づき、ネットワークトラブルシューティングを実行することができる。

- 問題を特定する
  - 情報を収集する
  - 可能であれば現象を再現する
  - 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
  - 個別に複数の障害に取り組む
- 可能性の高い原因の仮説を立てる
  - 明白な質問をする
  - 複数のアプローチを検討する
    - OSI 参照モデル 上位層から下位層へ/下位層から上位層へ
    - 分割統治法（Divide and conquer algorithm）
- 原因を判断する理論をテストする
  - 理論が裏付けられたら、問題解決のための次のステップを決定する
  - 理論が裏付けられない場合は、新しい理論を確立するか、エスカレーションを行う
- 問題を解決するための対応計画を策定し、可能性のある影響を特定する
- 解決策を実行するか、必要に応じてエスカレーションを行う
- システム全体の機能を確認し、該当する場合には、適切な予防策を講じる
- 発見事項、対応、結果を文書化する

4.2 与えられたシナリオに基づき、トラブルシューティングツールからのアウトプットを分析、判断することができる。

- コマンドラインツール
  - ipconfig
  - netstat
  - ifconfig
  - ping/ping6/ping -6
  - tracert/tracert -6/traceroute6/traceroute -6
  - nbtstat
  - nslookup
  - arp
  - mac address lookup table
  - pathping
- ラインテスター
- Certifiers
- マルチメーター
- ケーブルテスター
- ライトメーター
- トナープローブ
- 速度のテストサイト
- Looking Glass サイト
- WiFi アナライザー
- プロトコルアナライザー

4.3 与えられたシナリオに基づき、一般的なワイヤレス障害のトラブルシューティングと解決をすることができる。

- 信号消失

- 干渉
- チャネルの重複
  - チャネルの不一致
- SN 比（Signal-to-noise ratio：信号対雑音比）
- デバイスのサチュレイション
- 帯域幅のサチュレイション
- 未テストアップデート
- 不適切な SSID
- 電力レベル
- オープンネットワーク
- 不正なアクセスポイント
- 不適切なアンテナの種類
- 非互換性
- 不適切な暗号化
- 干渉（バウンス）
- MIMO
- AP の位置
- AP の設定
  - LWAPP
  - Thin AP と Thick AP の違い
- 環境要因
  - コンクリートの壁
  - ウィンドウフィルム
  - メタルスタッド
- ワイヤレス規格に関連する問題
  - スループット
  - 周波数
  - 距離
  - チャネル

4.4 与えられたシナリオに基づき、一般的なケーブルの問題についてトラブルシューティングと解決をすることができる。

- ショート
- 断線
- 不適切な終端処理（規格にそっていない）
  - ストレート
  - クロスオーバー
- クロストーク
  - ニアエンド
  - ファーエンド
- 電磁妨害（EMI）/無線周波妨害（RFI）
- 距離制限
- 減衰/損失
- コネクタ不良
- 配線不良
- スプリットペア
- Tx および Rx 極性反転
- ケーブルの配置
- SFP / GBIC 不良－ケーブル、またはトランシーバー

4.5 与えられたシナリオに基づき、一般的なファイバーケーブルの問題についてトラブルシューティングと解決をすることができる。

- 減衰/損失
- SFP / GBICーケーブルの不適合
- SFP / GBIC 不良ーケーブル、またはトランシーバー
- 波長の不適合
- 種類の不適合
- コネクタの汚れ
- コネクタの不適合
- 最小曲げ半径の制限
- 距離の制限

4.6 与えられたシナリオに基づき、一般的なネットワークの問題についてトラブルシューティングと解決をすることができる。

- 不適切な IP 構成/デフォルトゲートウェイ
- ブロードキャストストーム/スイッチループ
- 重複 IP アドレス
- 速度とデュプレックスの不適合
- エンドツーエンド接続性
- 不適切な VLAN アサイメント
- ハードウェアの故障
- 正しく設定されていない DHCP
- 正しく設定されていない DNS
- 不正なインターフェース/正しく設定されていないインターフェース
- ケーブルの配置
- インターフェースエラー
- 同時有線/無線接続
- 近くにあるデバイス/ノードの検索
- 電源障害/電源異常
- MTU/ MTU ブラックホール
- 存在しない IP ルート
- 正しく設定されていない NIC チーミング
  - アクティブ/アクティブとアクティブ/パッシブの違い
  - マルチキャストとブロードキャストの違い

4.7 与えられたシナリオに基づいて、一般的なセキュリティの問題についてトラブルシューティングと解決をすることができる。

- 正しく設定されていないファイアウォール
- 正しく設定されていない ACL/アプリケーション
- マルウェア
- DoS 攻撃
- 開いている/閉じているポート
- ICMP に関連する問題
  - PoD（Ping of death）
  - 到達しないデフォルトゲートウェイ
- パッチのあてられていないファームウェア/OS
- 悪意のあるユーザー
  - 信頼されたユーザー

- 信頼されていないユーザー
- パケットスニファー

- 認証の問題
  - 正しく設定されていない TACACS/RADIUS
  - デフォルトパスワード/デフォルト設定
- 不正アクセス/バックドアアクセス
- ARP の問題
- バナーグラビング/OUI
- ドメイン/ローカルグループの設定
- ジャミング

4.8 与えられたシナリオに基づいて、一般的な WAN の問題についてトラブルシューティングと解決をすることができる。

- インターネット接続の切断
- インターフェースのエラー
- スプリットホライズン
- DNS の問題
- 干渉
- ルーターの設定
- 顧客側の機材
  - スマートジャック/NIU
  - Demarc（デマーク：責任分界点）
  - ループバック
  - CSU/DSU
  - ドライバー/リピーター
- 企業のセキュリティポリシー
  - スロットリングポリシー
  - ブロック
  - フェアアクセスポリシー（FAP）/利用制限
- サテライトの問題
  - レイテンシー（遅延）

第5章 業界標準、標準手法、ネットワーク理論（16%）

5.1 シナリオを分析し、関連する OSI 参照モデルのレイヤーを判断することができる。

- 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

5.2 基本的なネットワークの理論と概念について説明することができる。

- カプセル化/非カプセル化
- 変調
  - 多重化
  - 非多重化
  - アナログ技術/デジタル技術
  - TDM
- 基数について
  - 2 進数
  - 16 進数
  - 8 進数
- ブロードバンド/ベースバンド
- ビットレートとボーレートの違い
- サンプリングサイズ
- CSMA/CD と CSMA/CA の違い
- キャリアディテクト/キャリアセンス
- 波長
- TCP/IP プロトコル・スイート
  - ICMP
  - UDP
  - TCP
- コリジョン

5.3 与えられたシナリオに基づいて、適切な規格のワイヤレス接続を実装することができる。

- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac

5.4 与えられたシナリオに基づいて、適切な規格の有線接続を実装することができる。

- イーサネット規格
  - 10BaseT
  - 100BaseT
  - 1000BaseT
  - 1000BaseTX

- 10GBaseT
- 100BaseFX
- 10Base2
- 10GBaseSR
- 10GBaseER
- 10GBaseSW
- IEEE 1901-2013
  - Ethernet over HDMI
  - Ethernet over power line

- 結線規格
  - EIA/TIA 568A/568B
- ブロードバンド規格
  - DOCSIS

5.5 与えられたシナリオに基づいて、適切なポリシーと手順を実行することができる。

- セキュリティポリシー
  - 監視に同意する
- ネットワークポリシー
- 利用規約
- 標準的なビジネス文書
  - SLA
  - MOU
  - MLA
  - SOW

5.6 安全対策について要約することができる。

- 電気を取り扱う際の安全性
  - グランディング
- ESD（静電気放電）への安全性
  - 帯電
- 設置時の安全性
  - 持ち上げ用機材
  - ラックへの設置
  - 設置
  - ツール利用の安全性
- MSDS（安全データシート）
- 緊急時の手順
  - 建物のレイアウト
  - 避難計画
  - 安全出口/緊急出口
  - フェイルオープン/フェイルクローズ
  - 緊急アラートシステム
- 消防システム
- HVAC（冷暖房空調設備）

5.7 与えられたシナリオに基づいて、機材をベストプラクティスから考えられる適切な位置に設置、設定することができる。

- 中間配線盤（IDF/Intermediate distribution frame）

- 主配線盤（MDF/Main distribution frame）
- ケーブル管理
  - パッチパネル
- 電源管理
  - 電力変換装置
  - サーキット
  - UPS
  - インバーター
  - 冗長電源
- デバイスの位置
- 空気の流れ
- ケーブルトレイ
- ラックシステム
  - サーバレールラック
  - ツーポストラック
  - フォーポストラック
  - フリースタンドラック
- ラベル付
  - ポートへのラベル付
  - システムへのラベル付
  - サーキットへのラベル付
  - 命名規則
  - パッチパネルへのラベル付
- ラックの監視
- ラックのセキュリティ

5.8 基本的な変更管理の手順について説明することができる。

- 変更の理由を文書化する
- 変更要求
  - 構成手順
  - ロールバックプロセス
  - 潜在的な影響
  - 通達
- 承認プロセス
- メンテナンスウィンドウ
  - 承認されたダウンタイム
- 変更の通達
- 文書化
  - ネットワーク構成図
  - 追加されたネットワーク
  - 物理的な位置の変更

5.9 以下のポートとプロトコルを比較参照することができる。

- 80 HTTP
- 443 HTTPS
- 137-139 Netbios
- 110 POP
- 143 IMAP
- 25 SMTP

- 5060/5061 SIP
- 2427/2727 MGCP
- 5004/5005 RTP
- 1720 H.323
- TCP
  - コネクション型
- UDP
  - コネクションレス型

5.10 与えられたシナリオに基づいて、適切なポートとプロトコルを設定、適用することができる。

- 20、21 FTP
- 161 SNMP
- 22 SSH
- 23 Telnet
- 53 DNS
- 67、68 DHCP
- 69 TFTP
- 445 SMB
- 3389 RDP

CompTIA Network+ 略語一覧

下記はCompTIA Network+認定資格試験で使用される略語の一覧です。受験者は、試験準備の一環として、これら用語を復習し、理解することをお勧めします。

A	—	Address
AAA	—	Authentication Authorization and Accounting
AAAA	—	Authentication, Authorization, Accounting and Address
ACL	—	Access Control List
ADSL	—	Asymmetric Digital Subscriber Line
AES	—	Advanced Encryption Standard
AH	—	Authentication Header
AP	—	Access Point
APC	—	Angle Polished Connector
APIPA	—	Automatic Private Internet Protocol Addressing
APT	—	Advanced Persistent Protocol
ARIN	—	American Registry for Internet Numbers
ARP	—	Address Resolution Protocol
AS	—	Autonomous System
ASIC	—	Application Specific Integrated Circuit
ASP	—	Application Service Provider
ATM	—	Asynchronous Transfer Mode
AUP	—	Acceptable Use Policy
BERT	—	Bit-Error Rate Test
BGP	—	Border Gateway Protocol
BLE	—	Bluetooth Low Energy
BNC	—	British Naval Connector/Bayonet Niell-Concelman
BootP	—	Boot Protocol/Bootstrap Protocol
BPDU	—	Bridge Protocol Data Unit
BRI	—	Basic Rate Interface
BSSID	—	Basic Service Set Identifier
CAM	—	Channel Access Method
CAN	—	Campus Area Network
CARP	—	Common Address Redundancy Protocol
CAT	—	Computer and Telephone
CCTV	—	Closed Circuit TV
CDMA	—	Code Division Multiple Access
CDMA/CD	—	Carrier Sense Multiple Access/Collision Detection
CHAP	—	Challenge Handshake Authentication Protocol
CIDR	—	Classless Inter Domain Routing
CNAME	—	Canonical Name
COS	—	Class of Service
CPU	—	Central Processing Unit
CRAM-MD5	—	Challenge-Response Authentication Mechanism–Message Digest 5
CSMA/CA	—	Carrier Sense Multiple Access/Collision Avoidance
CSU	—	Channel Service Unit
CWDM	—	Course Wave Division Mutliplexing
dB	—	Decibels
DCS	—	Distributed Computer System
DDoS	—	Distributed Denial of Service
DHCP	—	Dynamic Host Configuration Protocol

DLC	–	Data Link Control
DLP	–	Data Leak Prevention
DMZ	–	Demilitarized Zone
DNAT	–	Destination Network Address Translation
DNS	–	Domain Name Service/Domain Name Server/Domain Name System
DOCSIS	–	Data-Over-Cable Service Interface Specification
DoS	–	Denial of Service
DSCP	–	Differentiated Services Code Point
DSL	–	Digital Subscriber Line
DSSS	–	Direct Sequence Spread Spectrum
DSU	–	Data Service Unit
DWDM	–	Dense Wavelength Division Multiplexing
E1	–	E-Carrier Level 1
EAP	–	Extensible Authentication Protocol
EDNS	–	Extension Mechanisms for DNS
EGP	–	Exterior Gateway Protocol
EIA/TIA	–	Electronic Industries Alliance/Telecommunication Industries Association
EMI	–	Electromagnetic Interference
ESD	–	Electrostatic Discharge
ESP	–	Encapsulated Security Packets
ESSID	–	Extended Service Set Identifier
EUI	–	Extended Unique Identifier
FC	–	Fibre Channel
FDM	–	Frequency Division Multiplexing
FHSS	–	Frequency Hopping Spread Spectrum
FM	–	Frequency Modulation
FQDN	–	Fully Qualified Domain Name
FTP	–	File Transfer Protocol
FTPS	–	File Transfer Protocol Security
GBIC	–	Gigabit Interface Converter
Gbps	–	Gigabits per second
GPG	–	GNU Privacy Guard
GRE	–	Generic Routing Encapsulation
GSM	–	Global System for Mobile Communications
HDLC	–	High-Level Data Link Control
HDMI	–	High Definition Mutlimedia Interface
HIDS	–	Host Intrusion Detection System
HIPS	–	Host Intrusion Prevention System
HSPA	–	High-Speed Packet Access
HSRP	–	Hot Standby Router Protocol
HT	–	High Throughput
HTTP	–	Hypertext Transfer Protocol
HTTPS	–	Hypertext Transfer Protocol Secure
HVAC	–	Heating, Ventilation and Air Conditioning
Hz	–	Hertz
IaaS	–	Infrastructure as a Service
IANA	–	Internet Assigned Numbers Authority
ICA	–	Independent Computer Architecture
ICANN	–	Internet Corporation for Assigned Names and Numbers
ICMP	–	Internet Control Message Protocol
ICS	–	Internet Connection Sharing/Industrial Control System

IDF	—	Intermediate Distribution Frame
IDS	—	Intrusion Detection System
IEEE	—	Institute of Electrical and Electronics Engineers
IGMP	—	Internet Group Multicast Protocol
IGP	—	Interior Gateway Protocol
IKE	—	Internet Key Exchange
IMAP4	—	Internet Message Access Protocol version 4
InterNIC	—	Internet Network Information Center
IP	—	Internet Protocol
IPS	—	Intrusion Prevention System
IPsec	—	Internet Protocol Security
IPv4	—	Internet Protocol version 4
IPv6	—	Internet Protocol version 6
ISAKMP	—	Internet Security Association and Key Management Protocol
ISDN	—	Integrated Services Digital Network
IS-IS	—	Intermediate System to Intermediate System
ISP	—	Internet Service Provider
IT	—	Information Technology
ITS	—	Intelligent Transportation System
IV	—	Initialization Vector
Kbps	—	Kilobits per second
KVM	—	Keyboard Video Mouse
L2F	—	Layer 2 Forwarding
L2TP	—	Layer 2 Tunneling Protocol
LACP	—	Link Aggregation Control Protocol
LAN	—	Local Area Network
LC	—	Local Connector
LDAP	—	Lightweight Directory Access Protocol
LEC	—	Local Exchange Carrier
LED	—	Light Emitting Diode
LLC	—	Logical Link Control
LTE	—	Long Term Evolution
LWAPP	—	Light Weight Access Point Protocol
MAC	—	Media Access Control/Medium Access Control
MAN	—	Metropolitan Area Network
Mbps	—	Megabits per second
MBps	—	Megabytes per second
MDF	—	Main Distribution Frame
MDI	—	Media Dependent Interface
MDIX	—	Media Dependent Interface Crossover
MGCP	—	Media Gateway Control Protocol
MIB	—	Management Information Base
MIBS	—	Management Information Bases
MIMO	—	Multiple Input, Multiple Output
MLA	—	Master License Agreement
MMF	—	Multimode Fiber
MOU	—	Memorandum of Understanding
MPLS	—	Multi-Protocol Label Switching
MS-CHAP	—	Microsoft Challenge Handshake Authentication Protocol
MSDS	—	Material Safety Data Sheet
MT-RJ	—	Mechanical Transfer-Registered Jack

MTU	—	Maximum Transmission Unit
MUMIMO	—	Multiuser Multiple Input, Multiple Output
MX	—	Mail Exchanger
NAC	—	Network Access Control
NAS	—	Network Attached Storage
NAT	—	Network Address Translation
NCP	—	Network Control Protocol
NetBEUI	—	Network Basic Input/Output Extended User Interface
NetBIOS	—	Network Basic Input/Output System
NFS	—	Network File Service
NIC	—	Network Interface Card
NIDS	—	Network Intrusion Detection System
NIPS	—	Network Intrusion Prevention System
NIU	—	Network Interface Unit
nm	—	Nanometer
NNTP	—	Network News Transport Protocol
NTP	—	Network Time Protocol
OCx	—	Optical Carrier
OS	—	Operating Systems
OSI	—	Open Systems Interconnect
OSPF	—	Open Shortest Path First
OTDR	—	Optical Time Domain Reflectometer
OUI	—	Organizationally Unique Identifier
PaaS	—	Platform as a Service
PAN	—	Personal Area Network
PAP	—	Password Authentication Protocol
PAT	—	Port Address Translation
PC	—	Personal Computer
PDU	—	Protocol Data Unit
PGP	—	Pretty Good Privacy
PKI	—	Public Key Infrastructure
PoE	—	Power over Ethernet
POP	—	Post Office Protocol
POP3	—	Post Office Protocol version 3
POTS	—	Plain Old Telephone System
PPP	—	Point-to-Point Protocol
PPPoE	—	Point-to-Point Protocol over Ethernet
PPTP	—	Point-to-Point Tunneling Protocol
PRI	—	Primary Rate Interface
PSK	—	Pre-Shared Key
PSTN	—	Public Switched Telephone Network
PTP	—	Point-to-Point
PTR	—	Pointer
PVC	—	Permanent Virtual Circuit
QoS	—	Quality of Service
RADIUS	—	Remote Authentication Dial-In User Service
RARP	—	Reverse Address Resolution Protocol
RAS	—	Remote Access Service
RDP	—	Remote Desktop Protocol
RF	—	Radio Frequency
RFI	—	Radio Frequency Interference

RG	–	Radio Guide
RIP	–	Routing Internet Protocol
RJ	–	Registered Jack
RSA	–	Rivest, Shamir, Adelman
RSH	–	Remote Shell
RTP	–	Real Time Protocol
RTSP	–	Real Time Streaming Protocol
RTT	–	Round Trip Time or Real Transfer Time
SA	–	Security Association
SaaS	–	Software as a Service
SC	–	Standard Connector/Subscriber Connector
SCADA	–	Supervisory Control and Data Acquisition
SCP	–	Secure Copy Protocol
SDLC	–	Software Development Life Cycle
SDP	–	Session Description Protocol
SDSL	–	Symmetrical Digital Subscriber Line
SFP	–	Small Form-factor Pluggable
SFTP	–	Secure File Transfer Protocol
SGCP	–	Simple Gateway Control Protocol
SHA	–	Secure Hash Algorithm
SIEM	–	Security Information and Event Management
SIP	–	Session Initiation Protocol
SLA	–	Service Level Agreement
SLIP	–	Serial Line Internet Protocol
SMF	–	Single Mode Fiber
SMS	–	Short Message Service
SMTP	–	Simple Mail Transfer Protocol
SNAT	–	Static Network Address Translation/Source Network Address Translation
SNMP	–	Simple Network Management Protocol
SNTP	–	Simple Network Time Protocol
SOA	–	Start of Authority
SOHO	–	Small Office/Home Office
SONET	–	Synchronous Optical Network
SOW	–	Statement of Work
SPB	–	Shortest Path Bridging
SPI	–	Stateful Packet Inspection
SPS	–	Standby Power Supply
SSH	–	Secure Shell
SSID	–	Service Set Identifier
SSL	–	Secure Sockets Layer
ST	–	Straight Tip or Snap Twist
STP	–	Spanning Tree Protocol / Shielded Twisted Pair
SVC	–	Switched Virtual Circuit
SYSLOG	–	System Log
T1	–	Terrestrial Carrier Level 1
TA	–	Terminal Adaptor
TACACS	–	Terminal Access Control Access Control System
TACACS+	–	Terminal Access Control Access Control System+
TCP	–	Transmission Control Protocol
TCP / IP	–	Transmission Control Protocol/Internet Protocol
TDM	–	Time Division Multiplexing

TDR	–	Time Domain Reflectometer
Telco	–	Telephone Company
TFTP	–	Trivial File Transfer Protocol
TKIP	–	Temporal Key Integrity Protocol
TLS	–	Transport Layer Security
TMS	–	Transportation Management System
TOS	–	Type of Service
TTL	–	Time to Live
TTLS	–	Tunneled Transport Layer Security
UC	–	Unified Communications
UDP	–	User Datagram Protocol
UNC	–	Universal Naming Convention
UPC	–	Ultra Polished Connector
UPS	–	Uninterruptible Power Supply
URL	–	Uniform Resource Locator
USB	–	Universal Serial Bus
UTM	–	Unified Threat Management
UTP	–	Unshielded Twisted Pair
VDSL	–	Variable Digital Subscriber Line
VLAN	–	Virtual Local Area Network
VNC	–	Virtual Network Connection
VoIP	–	Voice over IP
VPN	–	Virtual Private Network
VRRP	–	Virtual Router Redundancy Protocol
VTC	–	Video Teleconference
VTP	–	VLAN Trunk Protocol
WAN	–	Wide Area Network
WAP	–	Wireless Application Protocol/Wireless Access Point
WEP	–	Wired Equivalent Privacy
WINS	–	Window Internet Name Service
WLAN	–	Wireless Local Area Network
WMS	–	Warehouse Management System
WPA	–	WiFi Protected Access
WPS	–	WiFi Protected Setup
www	–	World Wide Web
XDSL	–	Extended Digital Subscriber Line
XML	–	eXtensible Markup Language
Zeroconf	–	Zero Configuration

CompTIA Network+ ハードウェアとソフトウェアの一覧

** CompTIA では、CompTIA Network+の受験の学習を進める上で必要となるハードウェアとソフトウェアの一覧を提示しています。本リストは、ラボトレーニングなどを提供されるトレーニング企業にもご活用いただけます。
各項目の箇条書きにされているリストは、出題範囲の全ての項目を網羅しているものではありません。

機器

- パッチパネル
- パンチダウンブロック（Punch downs blocks）
- レイヤー3 スイッチ/ルーター
- レイヤー2 スイッチ
- ファイアウォール
- VPN コンセントレーター
- DHCP サーバー
- DNS サーバー
- IDS/IPS
- ワイヤレスアクセスポイント
- 2 台以上の PC
- メディアコンバーター
- Configuration terminal（telnet/SSH）
- VoIP システム（電話を含む）
- KVM スイッチ

予備のハードウェア

- NIC
- 電源設備
- GBIC
- SFP
- スイッチ
- ハブ
- ワイヤレスアクセスポイント
- UPS

予備のパーツ

- パッチケーブル
- RJ-45 コネクタ、モジューラージャック
- RJ-11 コネクタ
- 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

ツール

- 電話/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
- 同軸ストリッパー
- ワイヤーカッター
- トナージェネレーター
- ファイバーターミナルキット
- スニップ
- バットセット
- 光パワーメーター

ソフトウェア

- パケットスニッファー（Packet Sniffer）
- プロトコルアナライザー
- ターミナルエミュレーションソフトウェア
- Linux/Windows OS
- ソフトウェアファイアウォール
- ソフトウェア IDS / IPS
- ネットワークマッパー
- バーチャルネットワーク環境（Virtual network environment）
- WiFi アナライザー
- スペクトラムアナライザー
- アンチマルウェアソフトウェア
- ネットワーク監視ソフトウェア

その他

- ネットワーク関連文書のサンプル
- サンプルログ
- 不良ケーブル
- マルウェア/ウイルスのサンプル