Ciscoネットワーク演習2　第9週　　 クラス　　　　番号　　　　氏名

• 17 - 小規模ネットワークの構築

17.0 - 概要

17.0.1 - このモジュールを学ぶ理由

独自のネットワークをセットアップするために必要な基礎知識のほとんどがあります。次のステップとしてネットワークを構築します。

17.0.2 - このモジュールで学ぶこと

**モジュールの目標:** 小規模ネットワーク用にルータ、スイッチ、およびエンドデバイスを含むネットワーク設計を実装します。

17.1 - 小規模ネットワークのデバイス

17.1.1 - 小規模ネットワークトポロジ

小規模なネットワーク設計は、通常は簡単です。含まれるデバイスの数と種類は、大規模なネットワークに比べて大幅に削減されます。

17.1.2 - 小規模ネットワークのデバイスの選択

大規模なネットワークと同様に、小規模なネットワークでは、ユーザーの要件を満たすための計画と設計が必要です。計画により、すべての要件、コスト要因、および導入オプションが十分に考慮されます。

最初の設計上の考慮事項の 1 つは、ネットワークをサポートするために使用する中間デバイスのタイプです。

**コスト：** スイッチまたはルータの**[** ① **コスト ]**は、その容量と機能によって決まります。

**スピードとタイプ：**ルータまたはスイッチのポートの数とタイプを選択することは、重要な決定です。

**拡張性：**ネットワーキングデバイスは、固定およびモジュラー物理構成で利用できます。

**OSの機能とサービス：**ネットワークデバイスには、次のような組織の要件をサポートできるオペレーティングシステムが必要です。

* レイヤ 3 スイッチング
* ネットワーク アドレス変換（NAT）
* Dynamic Host Configuration Protocol（DHCP）
* セキュリティ
* Quality of Service（QoS）
* Voice over IP（VoIP）

17.1.3 - 小規模ネットワークの IP アドレッシング

ネットワークを実装する場合は、**[** ② **IPアドレッシング方式 ]**を作成して使用します。IP アドレッシング方式の要素となるデバイスには、次のものがあります。

* エンドユーザーデバイス-接続の数とタイプ（有線、無線、リモートアクセスなど）
* サーバーおよび周辺機器（プリンタや防犯カメラなど）
* スイッチおよびアクセスポイントを含む中間デバイス

デバイスタイプに基づいて IP アドレス指定スキームを計画、文書化、保守することをお勧めします

17.1.4 - 小規模ネットワークでの冗長性

ネットワーク設計のもう一つの重要な部分は、信頼性です。ネットワークの障害は、非常にコストがかかる可能性があります。

高い信頼性を維持するために、ネットワーク設計では**[** ③ **冗長性 ]**が必要です。冗長性は、単一の障害点を排除するのに役立ちます。

17.1.5 - トラフィック管理

ネットワーク管理者は、さまざまなタイプのトラフィックと、ネットワーク設計におけるそれらの処理を考慮する必要があります。

小規模ネットワークのルータおよびスイッチは、音声やビデオなどのリアルタイムトラフィックを、他のデータトラフィックと比較して適切な方法でサポートするように設定する必要があります。

17.1.6 - 理解の確認-小規模ネットワーク内のデバイス

17.2 - 小規模ネットワークアプリケーションとプロトコル

17.2.1 - 共通アプリケーション

セットアップ後、ネットワークが機能するためには、特定の種類のアプリケーションとプロトコルが必要です。

ネットワークは、ネットワーク上のアプリケーションと同じくらい有用です。ネットワークへのアクセスを提供するソフトウェアプログラムまたはプロセスには、ネットワークアプリケーションとアプリケーションレイヤサービスの 2 つの形式があります。

**ネットワークアプリケーション：**アプリケーションは、ネットワークを介して通信するために使用されるソフトウェアプログラムです。この種のアプリケーションの例としては、電子メールクライアントと Web ブラウザがあります．

**Application Layer Services　：**他のプログラムでは、ファイル転送やネットワーク印刷スプールなどのネットワークリソースを使用するには、**[** ④ **アプリケーション層サービス ]**の支援が必要な場合があります。

17.2.2 - 一般に使用されるプロトコル

ネットワークプロトコルは、小規模ネットワーク内の従業員が使用するアプリケーションとサービスをサポートします。

ネットワーク管理者は、通常、ネットワークデバイスおよびサーバへのアクセスを必要とします。最も一般的なリモートアクセスソリューションは、Telnet と**[** ⑤ **セキュアシェル (SSH) ]**の 2 つです。SSH の方が Telnet よりも安全な方式です。

17.2.3 - 音声およびビデオアプリケーション

今日の企業は、顧客やビジネスパートナーとのコミュニケーションに IP テレフォニーやストリーミングメディアを使用するようになっています。多くの組織は、従業員がリモートで作業できるようにしています。

ネットワーク管理者は、適切な装置がネットワークに設置されていること、およびネットワークデバイスが優先配信されるように設定されていることを確認する必要があります。

17.2.4 - 理解の確認-小規模ネットワークアプリケーションとプロトコル

17.3 - 大規模なネットワークへの拡張

17.3.1 - 小規模ネットワークの増加

ネットワークが小規模企業向けである場合、おそらくそのビジネスを成長させ、ネットワークも成長させたいと考えています。これはネットワークのスケーリングと呼ばれ、これを行うためのベストプラクティスがいくつかあります。

ネットワークを拡張するには、いくつかの要素が必要です。

* デバイスインベントリ -ネットワークを使用または構成するデバイスのリスト
* 予算 -IT予算の項目別（会計年度の設備購入予算を含む）
* トラフィック分析 -プロトコル、アプリケーション、サービス、およびそれぞれのトラフィック要件を文書化する必要があります。

17.3.2 - プロトコル分析

ネットワークが拡大するにつれて、ネットワークトラフィックの管理方法を決定することが重要になります。ネットワークを通過するトラフィックのタイプと、現在のトラフィックフローを理解することが重要です。この目的に使用できるネットワーク管理ツールはいくつかあります。ただし、**[** ⑥ **Wireshark ]**などの単純なプロトコルアナライザを使用することもできます。

17.3.3 - 従業員のネットワーク使用率

ネットワーク管理者は、変化するトラフィックの傾向を理解するだけでなく、ネットワークの使用状況の変化にも注意する必要があります。多くのオペレーティングシステムは、そのような情報を表示するための組み込みツールを提供しています。

17.3.4 - 理解の確認-大規模なネットワークへの拡張

17.4 - 接続の確認

17.4.1 - ping を使用した接続の確認

ping このコマンドは、送信元と宛先 IP アドレス間のレイヤ 3 接続を迅速にテストする最も効果的な方法です。このコマンドは、さまざまなラウンドトリップ時間の統計情報も表示します。

17.4.2 - 拡張 ping

Cisco IOS には、 ping コマンドの「拡張」モードがあります。このモードでは、コマンド操作に関連するパラメータを調整して、特殊なタイプの ping を作成できます。

拡張 ping は、宛先 IP アドレスを指定 せずにping 入力することで特権 EXEC モードで開始されます。その後、拡張 ping をカスタマイズするためのプロンプトがいくつか表示されます。

17.4.3 - トレースルートでの接続の確認

traceroute は、ネットワーク内の**[** ⑦ **レイヤ 3 ]**の問題エリアを特定するのに役立ちます。トレースは、パケットがネットワーク経由でルーティングされる場合にホップのリストを返します。このパスを使用して、問題が見つかるパス上のポイントを特定できます。

17.4.4 - traceroute の拡張

拡張 ping コマンドと同様に、拡張 traceroute コマンドもあります。これにより、管理者はコマンド操作に関連するパラメータを調整できます。

17.4.5 - ネットワーク ベースライン

ネットワークパフォーマンスを監視およびトラブルシューティングするための最も効果的なツールの 1 つは、ネットワークベースラインを確立することです。効果的なネットワークパフォーマンスベースラインの作成は、一定期間にわたって行われます。

17.4.6 - ラボ-ping および traceroute を使用したネットワーク遅延のテスト

17.5 - ホストおよび IOS コマンド

17.5.1 - WindowsホストでのIP構成

ネットワーク管理者は、通常、出力例に示すように、Windowsコンピュータの **ipconfig** コマンドラインでコマンドを発行して、Windowsホスト上のIPアドレス情報を表示します。

17.5.2 - LinuxホストでのIP構成

ネットワーク管理者は、コマンドラインで**[** ⑧ **ifconfig ]**コマンドを使用して、出力に示されているように、現在アクティブなインターフェイスのステータスと IP 設定を表示します。

17.5.3 - macOS ホストでの IP 設定

ifconfig このコマンドを使用して、出力に示されているインターフェイス IP 設定を確認することもできます。

17.5.4 - arp コマンド

arp コマンドは、Windows、Linux、または Mac のコマンドプロンプトから実行されます。このコマンドは、ホストの ARP キャッシュに現在含まれているすべてのデバイスを一覧表示します。

17.5.5 - 一般的な show コマンドの再表示

|  |  |
| --- | --- |
| コマンド | 確認項目 |
| show running-config | 現在の構成と設定を確認します |
| show interfaces | インターフェイスステータスを確認し、エラーメッセージを表示 |
| show ip interface | インターフェイスのレイヤ3情報を確認 |
| show arp | ローカルイーサネットLAN上の既知のホストのリストを確認 |
| show ip route | レイヤ3ルーティング情報を確認 |
| show protocols | どのプロトコルが動作しているかを確認 |
| show version | デバイスのメモリ、インターフェイス、およびライセンスを確認 |

17.5.6 - **show cdp neighbors** コマンド

Cisco Discovery Protocol（CDP）は、データリンク層でネットワーク検出を行うためのシスコ独自のプロトコルです。

17.5.7 - show ip interface brief コマンド

最も頻繁に使用されるコマンドの 1 つは、**[** ⑨ **show ip interface brief ]**コマンドです。ルータ上のすべてのネットワークインターフェイスに関する重要な情報の要約を提供します

17.5.8 - ビデオ－show versionコマンド

省略

17.5.9 - Packet Tracer-show コマンドの出力を解釈する

省略

17.6 - トラブルシューティング方法論

17.6.1 - 基本的なトラブルシューティング

前の 2 つのトピックでは、ネットワーク内の問題領域を特定するために使用できるユーティリティとコマンドについて学習しました。

この表は、トラブルシューティングプロセスの 6 つの主な手順を示しています。

|  |  |
| --- | --- |
| ステップ | 説明 |
| ステップ 1：問題の特定 | トラブルシューティング プロセスの最初のステップ このステップではツールを使用できますが、 ユーザーとの会話も非常に役立ちます。 |
| ステップ 2：可能性のある原因の理論を確立する | 問題が特定された後、考えられる原因の仮説を立ててみる 多くの場合、この手順によって可能性のある原因が複数見つかります。 |
| ステップ 3：原因を特定するための理論をテストする | 可能性のある原因に基づき、どれが問題の原因かを決めるために、**[** ⑩ **仮説を検証 ]**します。 多くの場合、技術者は簡単な手順を使用してテストを行い、問題が解決されたかどうかを確認します。 簡単な手順で問題が解決しない場合は、 正確な原因を確立するためにさらに問題を研究する。 |
| ステップ 4：問題を解決するための行動計画を立案し実行する | 問題の正確な原因を特定したら、 問題を解明し解決策を実行するための計画を策定する。 |
| ステップ 5：システム全体の機能を確認し、予防手段を実装する。 | 問題を修正したら、すべての機能を確認します。 該当する場合は、予防措置を実施します。 |
| ステップ 6：所見、処置、結果を文書化する | トラブルシューティング プロセスの最後のステップは、 所見、処置、および結果を文書化します。 これは今後の参照用に非常に重要です。 |

17.6.2 - 自ら解決しますか、エスカレーションしますか?

状況によっては、問題を迅速に解決できない場合があります。マネージャの判断、特定の専門知識、またはトラブルシューティングの技術者が対応できないネットワーク アクセス レベルが必要な場合、問題をエスカレーションする必要があります。

17.6.3 - debug コマンド

OS のプロセス、プロトコル、メカニズム、およびイベントでは、ステータスを伝えるためのメッセージが生成されます。これらのメッセージでは、システム動作のトラブルシューティングまたは確認に有益な情報が提供される場合があります。IOS の debug コマンドを使用すると、管理者は分析用にリアルタイムでメッセージを表示することができます。

17.6.4 - terminal monitor コマンド

特定の IOS メッセージは、コンソール接続では自動的に表示されますが、リモート接続では表示されません。たとえば、 debug 出力はデフォルトでコンソール接続に表示されます。

端末（仮想コンソール）にログ メッセージを表示するには、terminal monitor コマンドを使用します。

17.6.5 - 理解の確認-トラブルシューティング方法

17.7 - トラブルシューティング シナリオ

17.7.1 - デュプレックスの動作とミスマッチの問題

このトピックでは、ネットワーク管理者として見つけられる可能性のある一般的なネットワークの問題について説明します。

デュプレックスの不一致は、通常、インターフェイスの設定ミスや、まれに自動ネゴシエーションの失敗によって発生します。

17.7.2 - IOS デバイスの IP アドレス問題

誤って割り当てられた IP アドレスによって、IP アドレスの競合やルーティング問題など、さまざまな問題が発生します。

17.7.3 - エンド デバイスの IP アドレス問題

Windows ベースのマシンでは、デバイスが DHCP サーバに接続できない場合、Windows は 169.254.0.0/16 の範囲に属しているアドレスを自動的に割り当てます。

しばしば、169.254.0.0/16 のコンピュータは、ネットワーク内の他のデバイスが 169.254.0.0/16 ネットワークに属していない可能性が高いため、それらのデバイスと通信できません。

17.7.4 - デフォルト ゲートウェイの問題

デバイスに正しくないまたは存在しないデフォルト ゲートウェイ アドレスがある場合、リモート ネットワークのデバイスと通信することができません。デフォルト ゲートウェイはリモート ネットワークへのパスであるため、そのアドレスはエンド デバイスと同じネットワークに属する必要があります。

17.7.5 - DNS 問題のトラブルシューティング

「ネットワークがダウンした」や「インターネットがダウンした」などのユーザのクレームは、多くの場合、到達不能な**[** ⑪ **DNS サーバ ]**が原因です。

17.7.6 - ラボ - 接続の問題のトラブルシューティング

省略

17.7.7 - Packet Tracer - 接続問題のトラブルシューティング

17.8 - モジュール練習とクイズ

17.8.1 - ラボ-スモールビジネスネットワークの設計と構築

17.8.2 - Packet Tracer：統合課題

17.8.3 - Packet Tracer - トラブルシューティング

17.8.4 - このモジュールで学んだこと

17.8.5 - モジュールクイズ-小規模ネットワークの構築記