Ciscoネットワーク演習１　第9週　　 クラス　　　　番号　　　　氏名

• 8 - ネットワーク層

8.0 - 概要

8.0.1 - このモジュールを学ぶ理由

ローカルネットワーク上にいない人に電子メール（ビデオやファイルなど）を送信するには、ルータにアクセスできる必要があります。ルータにアクセスするには、ネットワーク層のプロトコルを使用する必要があります。

8.0.2 - このモジュールで学ぶこと

**モジュールの目標:** ルータがネットワーク層のプロトコルとサービスを使用して、エンドツーエンド接続を実現する方法について説明します。

8.1 - ネットワーク層の特性

8.1.1 - ネットワーク層

ネットワーク層（OSIレイヤ3）は、エンドデバイスがネットワーク間でデータを交換できるようにするサービスを提供します。IPバージョン4（IPv4）とIPバージョン6（IPv6）は、ネットワーク層の主要な通信プロトコルです。

ネットワーク境界を越えてエンドツーエンドの通信を実現するために、ネットワーク層プロトコルは4つの基本的な操作を行います。

* **エンドデバイスのアドレッシング**:エンドデバイスは、ネットワーク上で識別するための一意の IP アドレスを設定される必要があります。
* **カプセル化**:ネットワーク層は、トランスポート層からのプロトコルデータユニット（PDU）をパケットに**[** ① **カプセル化 ]**します。
* **ルーティング**:ネットワーク層は、別のネットワーク上の宛先ホストにパケットを転送するサービスを提供します。
* **カプセル化解除**:パケットが宛先ホストのネットワーク層に到着すると、ホストはパケットの IP ヘッダーをチェックします。カプセル化解除の処理は、IP パケットの宛先ホストによって実行されます。

8.1.2 - IPのカプセル化

IP は、IP ヘッダーを追加することによって、トランスポート層（ネットワーク層のすぐ上の層）のセグメントまたはその他のデータをカプセル化します。IP ヘッダーは、宛先ホストにパケットを配送するために使用されます。

8.1.3 - IPの特性

IP は、オーバーヘッドの少ないプロトコルとして設計されました。このプロトコルは、パケットのフローを追跡および管理するようには設計されていません。

IP の基本特性は次のとおりです。

* **コネクションレス型：**データパケットを送信する前に確立された宛先との接続はありません。
* **ベストエフォート：**パケット配信が保証されないため、IPは本質的に信頼性がありません。
* **メディア非依存：**データ配信に使われるメディア（例えば、銅線や光ファイバ、無線など）に依存しません。

8.1.4 - コネクションレス

IP はコネクションレスです。つまり、 データが送信される前に IP によって専用のエンドツーエンド接続は作成されません。

8.1.5 - ベストエフォート

IP プロトコルは、配信されるすべてのパケットが実際に受信されることを保証しません。この図は、IP プロトコルの配送特性が、信頼性がないこと、すなわち**[** ② **ベストエフォート ]**であることを説明しています。

8.1.6 - メディア非依存

TCP/IPプロトコルスイートにおいて、信頼性はトランスポート層のTCPプロトコルの役割です。IPは、プロトコルスタックの下位層に位置するデータ伝送メディアから切り離されたものとして動作します。IP パケットは銅ケーブルでは電子信号として、光ファイバでは光信号として、ワイヤレスでは無線信号として送信できます

IPパケットを受け取り、通信メディア上で送信できるように準備することは、OSI**[** ③ **データリンク ]**層の責任です。つまり、IP パケットの配信は特定のメディアに限定されません。

8.1.7 - 理解の確認-IP特性

8.2 - IPv4 パケット

8.2.1 - IPv4 パケット ヘッダー

IPv4パケットヘッダーは、このパケットが宛先エンドデバイスに向かう途中で次の中継点に配信されるようにするために使用されます。 IPv4パケットヘッダーは、パケットに関する重要な情報が含まれるフィールドで構成されます。

8.2.2 - IPv4 パケットヘッダーのフィールド

ダイアグラム

中程度の精度で自動的に生成された説明

**バージョン**　バイナリ値0100(4)、IPパケットのバージョン(この場合はIPv4)を示す

**DS**　パケットの優先順位を決定するために使用され、DSCPとECNに分けられる。１バイト

・**DSCP**(Differentiated Services Code Point)　6 ビット。QoSメカニズムによって使用される値を示す。

・**ECN**(Explicit Congestion Notification)・・・最後の2ビットは、ネットワーク輻輳時にパケットのドロップを防止できる明示的輻輳通知の値を示す。

**TTL**(Time to Live)　パケット生存時間、ルータを通過するたびに1減算され0になるとパケットを破棄する。

**プロトコル**　上位層(トランスポート層)を示すプロトコル番号がある。TCP(6)、UDP(17)、ICMP(1)など

**ヘッダーチェックサム**　IPv4ヘッダーの破損のチェックに使用、ルータ転送ごとに再計算される。

**送信元IPアドレス**　送信元IPアドレスを示す32ビットの値、常にユニキャスト

**宛先IPアドレス**　宛先IPアドレスを示す32ビットの値、常にユニキャストとは限らない

（ユニキャスト、マルチキャスト、ブロードキャストのいずれか）

8.2.3 - ビデオ - Wireshark におけるIPv4ヘッダーのサンプル

8.2.4 - 理解の確認 - IPv4パケット

8.3 - IPv6 パケット

8.3.1 - IPv4 の制限

IPv4は現在でも使用されています。このトピックでは、IPv4を最終的に置き換えるIPv6を扱います。

IPv4 には 3 つの大きな問題があります。

* **IPv4アドレスの枯渇：**IPv4では、使用可能な一意の**[** ④ **パブリックアドレス ]**の数が限られています。
* **エンドツーエンド接続の欠如**：ネットワークアドレス変換（NAT）は、IPv4ネットワーク内で一般的に実装される技術です。ただし、パブリック IPv4 アドレスが共有されるため、内部ネットワークホストの IPv4 アドレスは隠れてしまいます。これは、エンドツーエンド接続を必要とするテクノロジでは問題になる可能性があります。
* **ネットワークの複雑さの増大：**NAT のさまざまな実装では、ネットワークがさらに**[** ⑤ **複雑 ]**になり、レイテンシーが生み出され、トラブルシューティングが難しくなります。

8.3.2 - IPv6 の概要

IPv6 がもたらす改善点は、次のものです。

* **アドレス空間の増加：**IPv6アドレスは、32ビットのIPv4に対し、**[** ⑥ **128 ]**ビットの階層アドレッシングに基づいています。
* **パケット処理の改善：**IPv6 ヘッダーは簡素化され、フィールドが少なくなっています。
* **NAT の必要性の排除：**膨大な数のパブリック IPv6 アドレスでは、プライベート IPv4 アドレスとパブリック IPv4 の間の NAT は不要です。これにより、エンドツーエンド接続を必要とするアプリケーションで発生する、いくつかあった NAT の問題を回避できます。

8.3.3 - IPv6 パケットヘッダーにおける IPv4 パケットヘッダーフィールド

IPv4 ヘッダーは、20 オクテット (Options フィールドが使用されている場合は最大 60 バイト) の可変長ヘッダーと 12 の基本ヘッダーフィールドで構成されます

IPv6 ヘッダーは、**[** ⑦ **40 ]**オクテットの固定長ヘッダーで構成されています（送信元と宛先 IPv6 アドレスの長さによるものがほとんどです）。（８の基本ヘッダーフィールドで構成される）

タイムライン

中程度の精度で自動的に生成された説明

8.3.4 - IPv6 パケットヘッダー

**バージョン**　4ビット、バイナリ値0110(6)がセットされている

**トラフィッククラス**　8ビット、IPv4のDSフィールドに相当。パケットの優先度を付ける

**フローラベル**　20ビット、同じフローラベルを持つすべてのパケットが、同じ扱いを受ける

**ペイロード長**　16ビット、データ部分の長さを示す。ヘッダーの長さは含まれない

**ネクストヘッダ**ー　8ビット、IPv4のプロトコルフィールド相当。上位層プロトコルのタイプを示す

**ホップリミット**　8ビット、IPv4でのTTLに相当するフィールド　ルータ転送ごとに1ずつ減算

**送信元IPアドレス**　128ビット

**宛先IPアドレス**　128ビット

8.3.5 - ビデオ - Wireshark におけるIPv6ヘッダのサンプル

8.3.6 - 理解の確認 - IPv6パケット

8.4 - ホストのルーティング方法

8.4.1 - ホストの転送決定

このトピックでは、エンドデバイスがどのようにルーティングテーブルを使用するかについて説明します。

* **Itself**(自身)**：**特別なIPv4アドレス **127.0.0.1**、またはIPv6アドレス **::1** へping を実行できます。これは、ループバックインターフェイスと呼ばれます。ループバループバックインターフェイスにpingを実行すると、ホストの TCP/IP プロトコルスタックがテストされます。
* **ローカルホスト：**これは、送信側ホストと**[** ⑧ **同じ ]**ローカルネットワーク上にある宛先ホストです。送信元ホストと宛先ホストは同じネットワークアドレスを共有します。
* **リモートホスト：**リモートネットワーク上の宛先ホストです。送信元ホストと宛先ホストは異なるネットワークアドレス持ちます。

パケットがローカルホストかリモートホストのどちらに送信されるかは、送信元エンドデバイスによって決定されます。

* **IPv4 の場合：**送信元デバイスは、自身の IPv4 アドレスと宛先 IPv4 アドレスとともに、自身のサブネットマスクを使用して、この決定を行います。
* **IPv6 の場合：**ローカルルータは、ネットワーク上のすべてのデバイスにローカルネットワークアドレス（プレフィックス）を広告します。

送信元デバイスがリモート宛先デバイスにパケットを送信するとき、ルータとルーティングの助けが必要です。ルーティングは、宛先への最適パスを決定する処理です。ローカルネットワークセグメントに接続されたルータはデフォルトゲートウェイと呼ばれます。

8.4.2 - デフォルトゲートウェイ

デフォルトゲートウェイは、他のネットワークにトラフィックをルーティングできるネットワークデバイス (すなわち、ルータやレイヤー3スイッチ)です。

8.4.3 - ホストのデフォルトゲートウェイへのルート

ホストのルーティングテーブルは、通常デフォルトゲートウェイを含みます。IPv4の場合、ホストはデフォルトゲートウェイのIPv4アドレスを **[** ⑨ **DHCP ]** (Dynamic Host Configuration Protocol)で動的に取得するか、手動で設定します。IPv6の場合、ルータがデフォルトゲートウェイのアドレスを広告するか、ホストを手動で設定します。

8.4.4 - ホストのルーティングテーブル

Windowsホストでは、 **route print** または **netstat -r** コマンドを使用してホストのルーティングテーブルを表示できます。

8.4.5 - 理解を確認する-ホストのルーティング方法

8.5 - ルーティングの概要

8.5.1 - ルータのパケット転送決定

このトピックでは、ネットワーク層におけるルータの動作について説明します。ホストが別のホストにパケットを送信するとき、自身のルーティングテーブルを参照して、パケットの送信先を決定します。宛先ホストがリモートネットワーク上にある場合、パケットはデフォルトゲートウェイ（通常はローカルルータ）に転送されます。

8.5.2 - IP ルータのルーティングテーブル

ルーティングテーブルには、次の 3 種類のルートエントリが格納されます。

* **直接接続ネットワーク：**これらのネットワークルートエントリは、アクティブなルータインターフェイスです。IP アドレスが設定されたインターフェイスがアクティブになると、ルータは直接接続ルートを追加します。各ルータインターフェイスは、異なるネットワークセグメントに接続されています。
* **リモートネットワーク：**これらのネットワークルートエントリは、他のルータへ接続されています。ルータは、管理者の明示的な設定か、ダイナミックルーティングプロトコルの使用による情報交換によって、リモートネットワークについて学習します。
* **デフォルトルート**：ホストと同様に、ほとんどのルータはデフォルトルートエントリ、**[** ⑩ **ラストリゾート ]**ゲートウェイを含んでいます。デフォルトルートは、IP ルーティングテーブルに最適（最長）一致がない場合に使用されます。

ルータは、次の 2 つの方法のいずれかでリモートネットワークについて学習できます。

* **手動：**リモートネットワークは、スタティックルートを使用して手動でルートテーブルに入力されます。
* **動的：**リモートルートは、ダイナミックルーティングプロトコルを使用して自動的に学習されます。

8.5.3 - スタティック ルーティング

スタティックルーティングには、次のような特性があります。

* スタティックルートは**[** ⑪ **手動 ]**で設定する必要があります。
* トポロジに変更があり、スタティックルートが使用できなくなった場合、管理者はスタティックルートを再設定する必要があります。
* スタティックルートは、小規模なネットワークや、冗長なリンクがほとんどない場合やまったく存在しない場合に適しています。
* スタティックルートは、通常、デフォルトルートを設定するためにダイナミックルーティングプロトコルとともに使用されます。

8.5.4 - ダイナミックルーティング

ダイナミックルーティングプロトコルは、ルータが、デフォルトルートを含むリモートネットワークについて、他のルータから自動的に学習するようにします。ネットワークトポロジに変更がある場合、ルータはダイナミックルーティングプロトコルを使用してこの情報を共有し、ルーティングテーブルを自動的に更新します。

8.5.5 - ビデオ IPv4 ルータのルーティングテーブル

8.5.6 - IPv4 ルーティングテーブルの概要

特権 EXEC モードコマンド **show ip route** は、Cisco IOS ルータ上の IPv4 ルーティングテーブルを表示するために使用します。各ルーティングテーブルエントリの先頭には、ルートのタイプまたはルートの学習方法を識別するために使用される記号があります。一般的なルートソース（記号）には、次のものがあります。

* **L :** 直接接続されたローカルインターフェイス IP アドレス
* **C :** 直接接続ネットワーク
* **S :** 管理者によって手動設定されたスタティックルート
* **O :** OSPF(ダイナミックルーティングプロトコル)
* **D :** EIGRP(ダイナミックルーティングプロトコル)

8.5.7 - 理解の確認-ルーティングの概要

8.6 - モジュール演習とクイズ

8.6.1 - このモジュールで学んだこと

8.6.2 - モジュールクイズ-ネットワーク層