コンピュータネットワークの概要



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- コンピュータネットワークは、私たちの生活、娯楽、ビジネスのやり方を大きく変えました。
- この章では、初心者を対象に、コンピュータネットワークの世界について説明します。
- 本章は今後の学習の基礎となります。

学習の目標

このレッスンを修了すると、次のことができるようになります：

- コンピュータネットワークの基本機能を説明する
- コンピュータネットワーク開発の背後にある要因の特定
- コンピュータネットワークのタイプと主要なパフォーマンス仕様の特定
- コンピュータネットワークのプロトコル、標準、標準化機関の特定

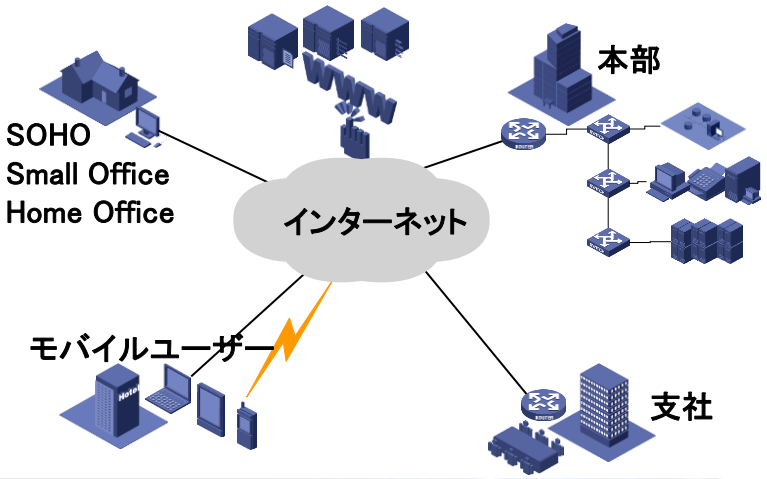


アジェンダ

- **コンピュータネットワークの定義と基本的機能**
- コンピュータネットワークの進化
- コンピュータネットワークのタイプ
- コンピュータネットワークの主要な性能仕様
- ネットワーク標準化組織

コンピュータネットワーク定義

- コンピュータネットワークは、相互接続されたコンピュータのグループです。



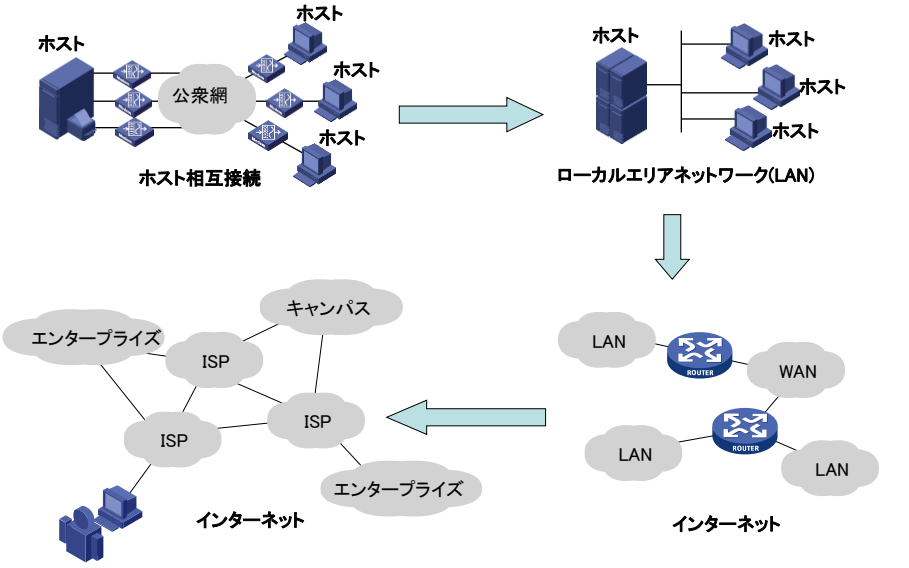
コンピュータネットワークの基本機能

- サーバー、データベース等をつないでリソースの共有
- ネットワークリソースの有効利用のための分散処理とロードバランシング
- ネットワークを活用した情報の提供

アジェンダ

- コンピュータネットワークの定義と基本的機能
- コンピュータネットワークの進化
- コンピュータネットワークのタイプ
- コンピュータネットワークの主要な性能仕様
- ネットワーク標準化組織

コンピュータネットワークの進化



アジェンダ

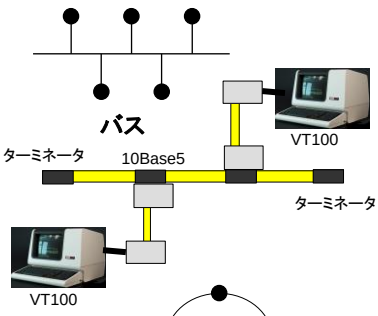
- コンピュータネットワークの定義と基本的機能
- コンピュータネットワークの進化
- コンピュータネットワークのタイプ
- コンピュータネットワークの主要な性能仕様
- ネットワーク標準化組織

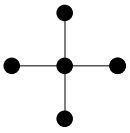
LAN、MAN、およびWANの概要

H3C

- **ローカルエリアネットワーク(LAN)**
  - → LANは、小さな物理領域(数キロメートル以内)をカバーし、コンピュータ、プリンタ、モデム、またはその他のデバイスを特定のメディアと相互接続するコンピュータネットワークです。
- **メトロポリタンエリアネットワーク(MAN)**
  - → MANは、LANよりも大きく、WANよりも小さく、数ブロックから都市全体(約10km)に及ぶコンピュータネットワークです。NTT東日本は、超高速イーサネットMANを実現する通信網サービス「メトロイーサ」を平成13年3月より提供しておりますが、新たなサービスとして10Gビットのサービスも提供しています。
- **ワイドエリアネットワーク(WAN)**
  - → WANは、広域をカバーするコンピュータネットワークであり、様々なタイプのシリアル接続を使用して、大都市、地域、または国の境界を越えてアクセスを実装します。

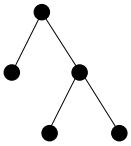
ネットワークトポロジ構造





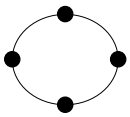
スター型

スター型の典型はハブ



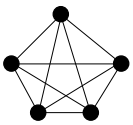
ツリー

ツリー型はスター型をつないだ形



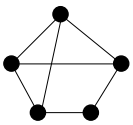
リング

トークンリングとよばれるリングトポロジーを持つネットワーク



フルメッシュ

全てのノードが接続されている障害対策が考えられたネットワーク



部分メッシュ

重要なコンピュータ同士がネットワークに障害が発生したときにも影響の無いように部分的にノードが接続されている

回線交換およびパケット交換の概要

- **回線交換: PSTN(公衆電話網)ベースの回線スイッチング**
  - → 利点: 短い遅延とリアルタイムな伝送
  - → 短所: ・帯域幅が固定されている
    ・ネットワークのスピードが遅い
    ・電話のように相手に接続要求をだして、相手が受け付けてから通信が始まるので、始まりが遅い
- **パケット交換: パケット単位(例えばMPLS,X.25)での保存と転送**
  - → 利点: ネットワークリソースの使用率が高い
  - → 短所: 長い遅延と非リアルタイムな伝送

アジェンダ

- コンピュータネットワークの定義と基本的機能
- コンピュータネットワークの進化
- コンピュータネットワークのタイプ
- コンピュータネットワークの主要な性能仕様
- ネットワーク標準化組織

コンピュータネットワークの主要な性能仕様

H3C

- **帯域幅**
  - → 指定された期間内にノードから別のノードに転送できるデータ量を示します。
  - → bps単位(1秒間に移動するビット数)で測定
  - → たとえば、イーサネット帯域幅は10Mbpsで、ファストイーサネット帯域幅は100Mbpsです。現在では1000Mbps(1G)以上が普通に使われます。
- **遅延**
  - → ノードから別のノードにデータユニットを転送するために使用される時間を示します。

アジェンダ

- ■ コンピュータネットワークの定義と基本的機能
- ■ コンピュータネットワークの進化
- ■ コンピュータネットワークのタイプ
- ■ コンピュータネットワークの主要な性能仕様
- ■ ネットワーク標準化組織

ネットワーク標準化組織

H3C

- 国際標準化機構(ISO)
- 米国電気電子技術者協会(IEEE)
- 米国規格協会(ANSI)
- 国際電気通信連合(ITU)
- インターネットアーキテクチャボード(IAB)

復習

- コンピュータネットワークでは、リソース共有、統合情報サービス、ロードバランシング、分散データ処理を実装できます。
- コンピュータネットワークは、地理的範囲、トポロジ、スイッチング方法などに基づいて分類することができます。
- 帯域幅と遅延は、コンピュータネットワークを測定する重要なパフォーマンス仕様です。

コンピュータネットワーク概要

次の記述のうち、回線交換とパケット交換について正しいものはどれか？

パケット交換はネットワークリソースの使用効率が低いことが特徴です

回線交換は短い遅延とリアルタイム伝送を特徴としています

回線交換はネットワークリソースの使用効率が高いことが特徴です

パケット交換は長い遅延と非リアルタイム伝送を特徴としています

H3C

IToIP Solutions Expert



IP基礎

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- IPは広く使用されているネットワーク層プロトコルです。
- IPは、パケットのエンドツーエンド配信を実装するために、データをカプセル化し、ネットワークノードを識別する方法を定義します。

学習の目標

このレッスンを修了すると、次のことができるようになります：

- IPアドレスの形式、クラス、およびマスクについて説明する
- IPルーティングの一般的な手順について説明し、主要なルーティングプロトコルの名前を列記する
- ARP/RARPの仕組みについて説明する
- IPアドレッシングの仕組みについて説明する



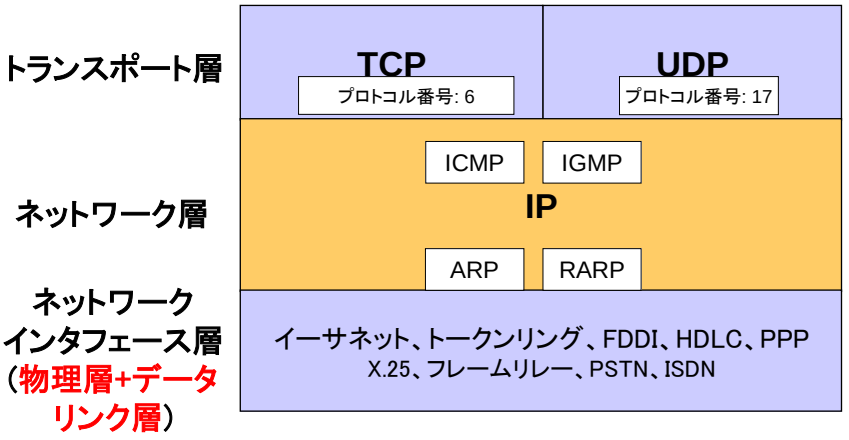
アジェンダ

- IP概要
- IPアドレス指定とアドレスマッピング
- IPパケットの配信
- 他の関連プロトコルの紹介

IPおよび関連プロトコル

H3C

OSI参照モデルの一部をサポート



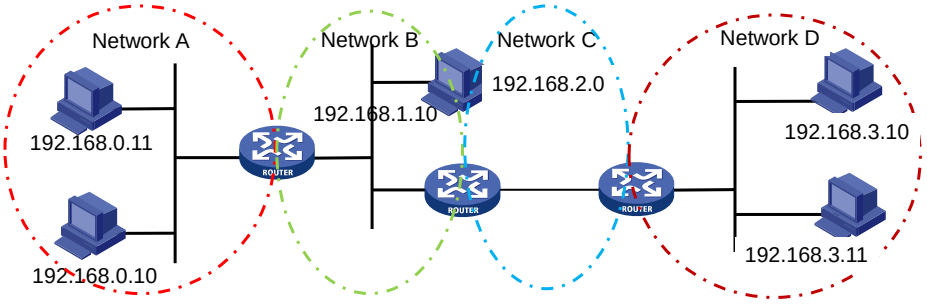
IPの主な機能

H3C

- ノードとセグメントの識別
  - 固有のIPアドレスを持つすべてのノード(装置)の識別
  - 固有のIPネットワーク番号を持つすべてのセグメントの識別
- アドレス指定と転送
  - ターゲットノードが存在するネットワークを特定し、ターゲットノードの位置を特定する
  - IPルータは、IPパケットを宛先に転送するための適切なルートを選択します。
- 各種データリンクへの対応(物理媒体ごとの転送サイズの違いに対応させる)
  - リンク上のMTU(Maximum Transmission Unit:1回の通信で転送できる最大データサイズ)に従ったIPパケットのフラグメント化と再構築

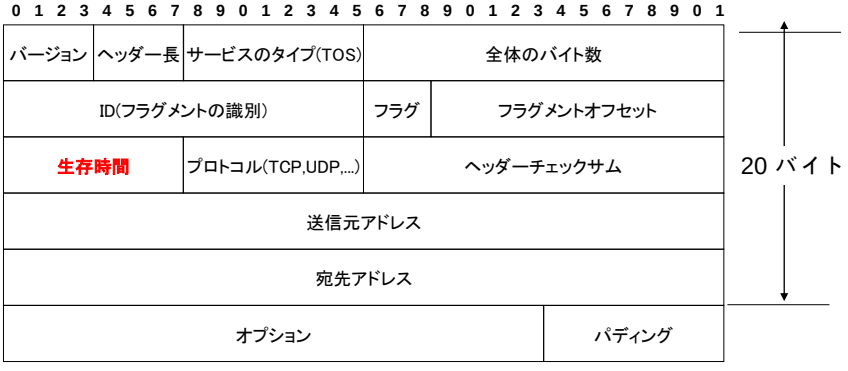
    ※イーサネットでは標準1,500バイトで最大は8,896バイト
  - パケットを配信するためのIPアドレスとデータリンク層アドレス(MAC)間のマッピングの作成(ARP / RARP)

IPネットワーク構造



- IPインターネットは、複数のネットワークセグメントから成り、各ネットワークセグメントはリンクでつながっています。
- ルータは、別々のネットワークセグメントを接続し、さまざまなデータリンク層プロトコルをサポートし、ネットワーク間でパケットを転送する。

IPヘッダのフォーマット

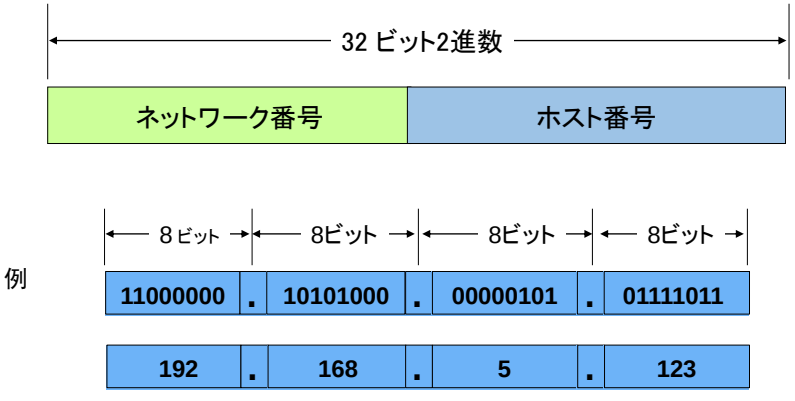


※生存時間とはルータを超えるたびに1づつマイナスされ0になったらこのパケットは破棄されます。これはループを防ぐためのものです。ホストが最初にパケットを送信するとき、255に設定する。現実にはルーターを255台超えるような状況はありえない。

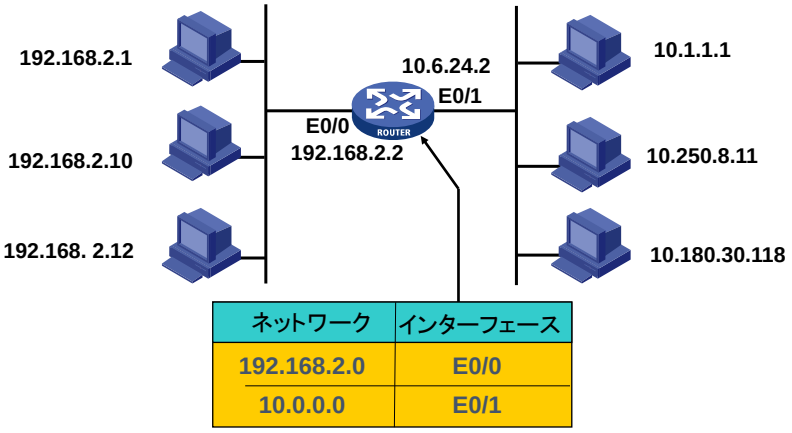
アジェンダ

- IP概要
- IPアドレス指定とアドレスマッピング
- IPパケットの配信
- 他の関連プロトコルの紹介

IPアドレスの形式と表現

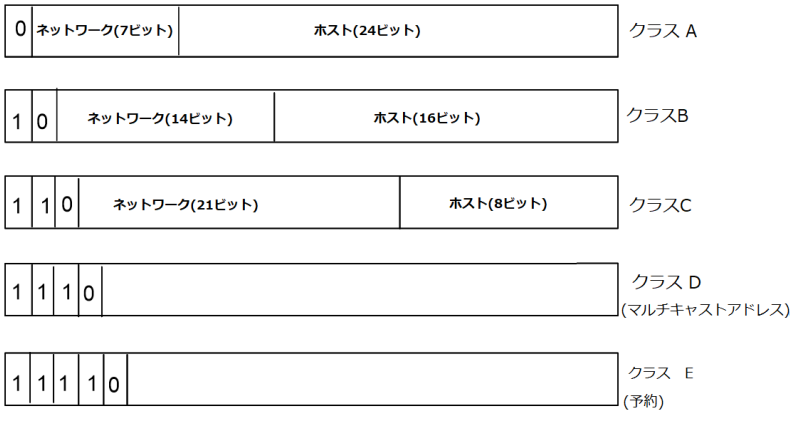


ネットワーク番号とホスト番号



- ネットワーク番号は、IPネットワークを一意に識別します。
- ホスト番号は、ネットワーク上のIPノードを一意に識別します。

IPアドレスの分類

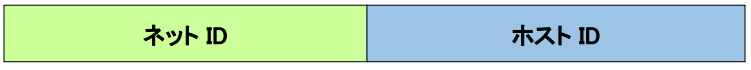


特殊なIPアドレス

ネットワーク番号	ホスト番号	アドレスの種類と機能
任意	すべて0	ネットワークセグメントを識別するネットワークアドレス 例えば、192.168.10.0
任意	全て1	ネットワークセグメントのブロードキャストアドレス。ネットワークセグメント上のすべてのノードを識別します。 例えば、192.168.10.255
127	任意	ループテスト用のループバックアドレス 例えば、127.0.0.1
全て0		全て0、すべてのネットワークを識別し、デフォルトルートの設定に使用されます 例えば、0.0.0.0
全て1		全ノードを識別する全ネットワークのブロードキャストアドレス 例えば、255.255.255.255

IPサブネット化

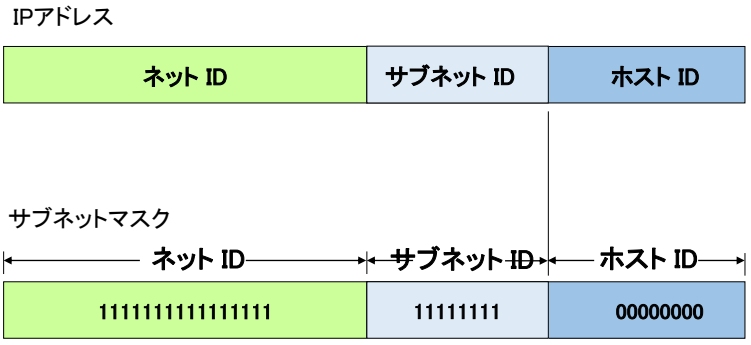
サブネット化のない2つのコンポーネントで構成されるIPアドレス



サブネット化された3レベルのIPアドレス



IPアドレスとサブネットマスク



IPアドレスの分類

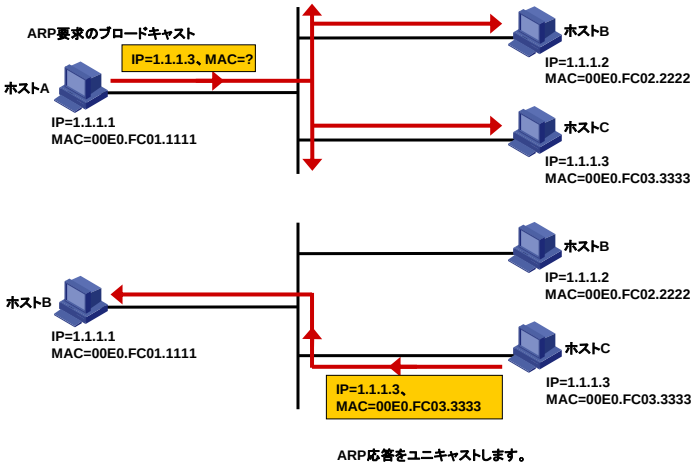
クラス	アドレス
クラスA	1.0.0.0 ～ 9.255.255.255
	10.0.0.0～10.255.255.255(プライベートアドレス)
	11.0.0.0 ～ 126.255.255.255
クラスB	128.0.0.0 ～ 172.15.255.255
	172.16.0.0～172.31.255.255(プライベートアドレス)
	172.32.0.0 ～ 191.255.255.255
クラスC	192.0.0.0 ～ 192.167.255.255
	192.168.0.0～192.168.255.255(プライベートアドレス)
	192.169.0.0 ～ 223.255.255.255
クラスD	224.0.0.0～239.255.255.255(**IPマルチキャスト使用**)
クラスE	240.0.0.0～255.255.255.255(**予約済み、未使用**)

グローバルIPアドレスとは、インターネットに接続された機器に一意に割り当てられるIPアドレスであり、世界的にはICANN、日本ではJPNICという機関で管理しています。
プライベートIPアドレスはJPNICなどの機関に申請する必要はなく自由に使えますがインターネットに接続するにはNATなどでグローバルIPアドレスに変換する必要があります。

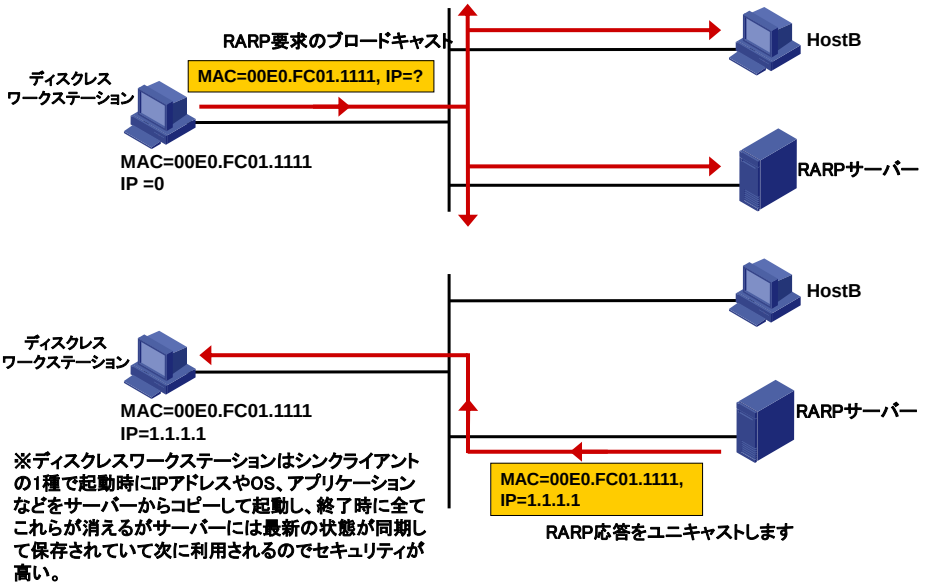
デフォルトのサブネットマスク

- クラスAアドレスのデフォルトのサブネットマスクは255.0.0.0です。
- クラスBアドレスのデフォルトのサブネットマスクは255.255.0.0です。
- クラスCアドレスのデフォルトのサブネットマスクは255.255.255.0です。

ARP



RARP

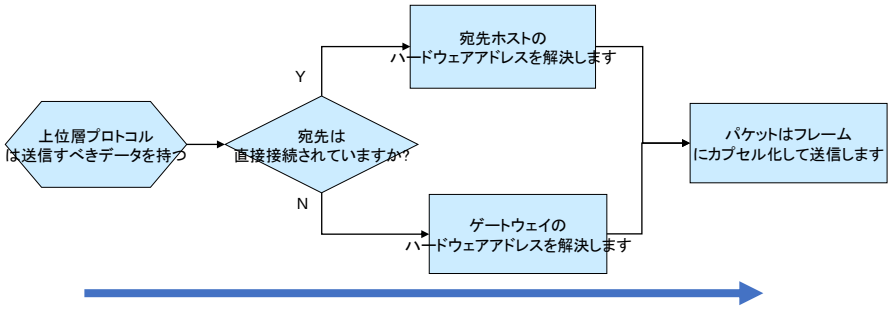


※ディスクレスワークステーションはシンクライアントの1種で起動時にIPアドレスやOS、アプリケーションなどをサーバーからコピーして起動し、終了時に全てこれらが消えるがサーバーには最新の状態が同期して保存されていて次に利用されるのでセキュリティが高い。

アジェンダ

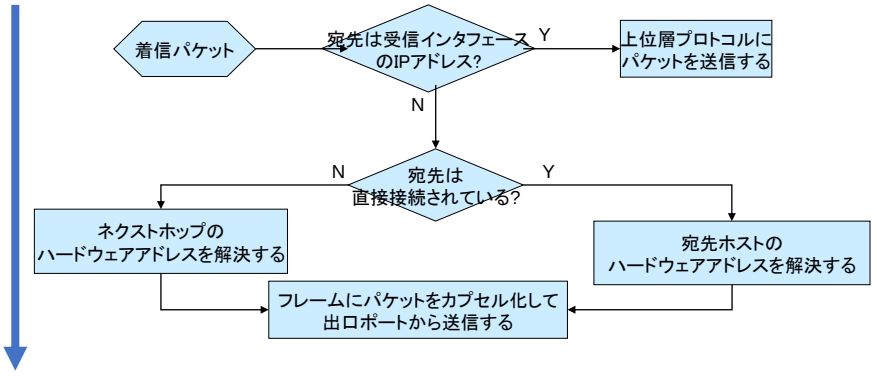
- IP概要
- IPアドレス指定とアドレスマッピング
- IPパケットの配信
- 他の関連プロトコルの紹介

ホストがユニキャストパケットを送信する



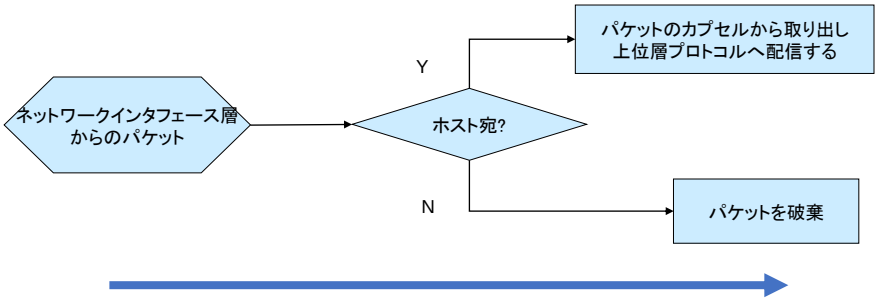
- 宛先アドレスのネットワーク番号が送信ホストのネットワーク番号と同じ場合、宛先は直接接続されたネットワーク上にあります。

ルータがユニキャストIPパケットを配信する



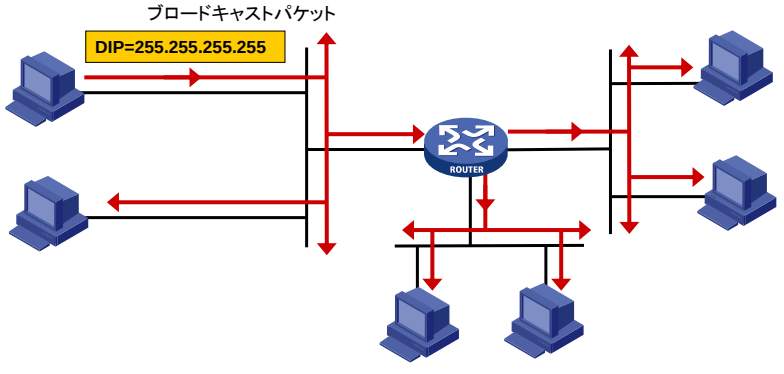
- 宛先アドレスのネットワーク番号がルータのインターフェイスのネットワーク番号と同じ場合、宛先は直接接続されていると見なされます。
- ルータはルーティングテーブルを検索してネクストホップを見つけます。

ホストがIPパケットを受信する



- ホストは、パケットが次のいずれかの要件を満たす場合にパケットを受け入れます。
  - 宛先IPアドレスは、ホストのIPアドレスです。
  - 宛先IPアドレスはブロードキャストアドレスです。
  - 宛先IPアドレスはマルチキャストアドレスであり、ホストのサービスはマルチキャストグループに属しています。
- そうでない場合、ホストのネットワーク層はIPパケットを廃棄します。

ブロードキャストストーム



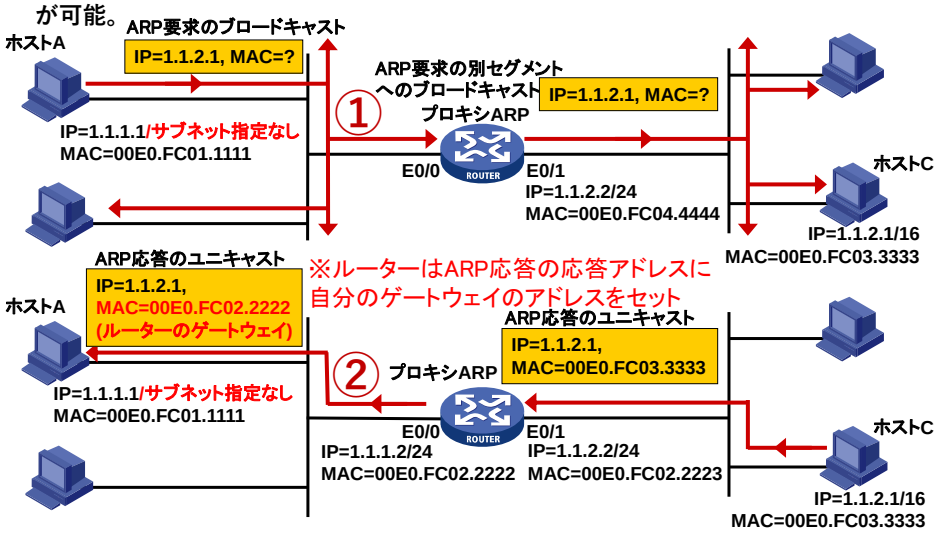
- ルータがブロードキャストパケットを転送すると、ブロードキャストストームが発生し、ネットワークが過負荷状態になります。
- デフォルトでは、ルータはブロードキャストパケットを転送しません。

アジェンダ

- IP概要
- IPアドレス指定とアドレスマッピング
- IPパケットの配信
- 他の関連プロトコルの紹介

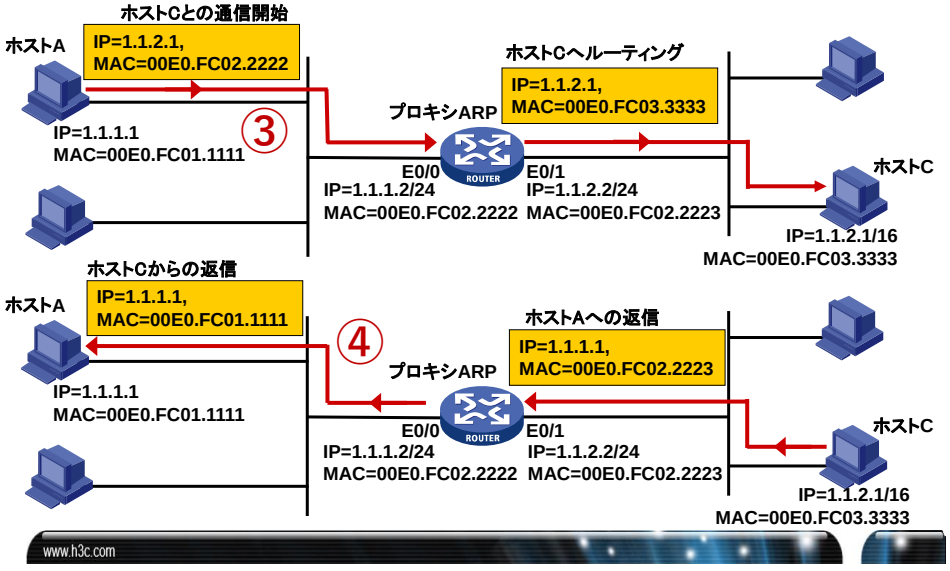
プロキシARP

ホストのIP設定にサブネットやゲートウェイが定義されていないと別セグメントのホストとは通信できないが、ルーターやL3スイッチにProxy ARPの設定があれば通信が可能。



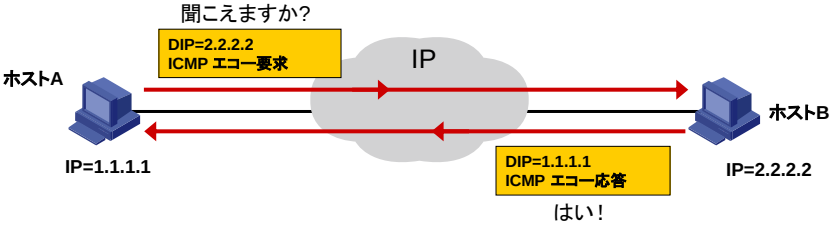
プロキシARP

※H3C L3スイッチではデフォルトでプロキシARP機能は無効です。Ciscoはデフォルトで有効なので気を付けましょう



ICMP

Ping(ICMP到達可能性テスト)



- ICMPは、IPデータを処理するためのエラーレポートとその他のメッセージを定義します。
- ICMPは、データの送信中のエラーと障害を報告し、到達可能性診断を提供します。
- ICMPメッセージは、ICMPエラーメッセージとクエリーメッセージに分けられます。

復習

- 32ビットIPアドレスは、ネットワークとネットワーク上のホストを識別するためのネットIDとホストIDで構成されます。
- ホストは、別のネットワーク宛てのIPパケットをデフォルトゲートウェイに配信します。ルータは、ネットワーク間でパケットを転送する役割を持ちます。
- ARPは、IPアドレスをMACアドレスにマッピングします。
- RARPは、データリンク層アドレスをIPアドレスにマッピングします。
- ICMPはエラー制御と診断機能を提供します。

IPアドレスは … で表されます。

- ドット付き16進表記
- コロン16進表記
- コロン10進表記
- ドット付き10進表記

IP基礎

以下のIPアドレスに関する説明で正しいものを選びなさい

IPアドレスは、ネットワーク番号とホスト番号の2つの部分で構成されます

クラスAのIPアドレスのネットワーク番号は8ビットで、実際の可変桁数は7ビットです。

クラスDのIPアドレスは通常マルチキャストアドレスとして使用されます

アドレス変換（NAT）テクノロジは通常、クラスAアドレスからクラスCアドレスへの変換を解決するために使用されます。

IP基礎

IPアドレスに関する次の記述のうち正しいものは？

一般に、IP アドレスは 10.110.168.121 のようにドット付き 10 進数形式で表されます

タイプ A アドレスの場合、ネットワーク アドレスは最初のオクテットです。タイプ A アドレスの最初のバイトは 0 ～ 126 です（127 は他の目的のために予約済）誤り:タイプAアドレスは1.0.0.0～126.255.255.255

ホスト ID 部分のバイナリ ビットがすべて 1 の場合、IP アドレスはネットワーク アドレスと呼ばれ、ネットワークのすべてのホストを識別するために使用されます

IP アドレスは、ネットワーク ID とホスト ID の 2 つの部分で構成されます。

IP基礎

サブネット化は自然なクラスフルIPアドレッシングに基づいて … を導入することによって実装されます

- ホストID
- ネットID
- サブネットID

IP基礎

pingはどのプロトコルを利用したアプリケーションですか？

- ICMP
- IP
- TCP
- UDP

IP基礎

図に示すように、ルータRTAはPCAおよびPCBに接続されています。RTAでProxy ARPエージェントを有効にする必要がある場合次の設定のどれが正しいですか？



A. [RTA] proxy-arp enable

B. [RTA-GigabitEthernet0/0] proxy-arp enable

C. [RTA-GigabitEthernet0/1] proxy-arp enable

D. [RTA] proxy-arp enable port G1/0/1

IP基礎

IPアドレス172.30.123.45、サブネットマスク255.255.252.0のネットワーク番号を求めなさい。

172.30.120.0

IP基礎

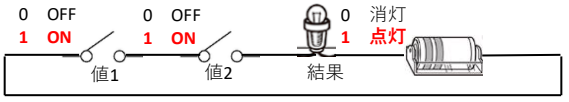
H3C

解説:

IP	172		30		123		45	
2進数	1010	1100	0001	1110	0111	1011	0010	1101
マスク	255		255		252		0	
2進数	1111	1111	1111	1111	1111	1100	0000	0000
	ネットワーク部						ホスト部	
論理積	1010	1100	0001	1110	0111	1000	0000	0000
セグメント	**172**		**30**		**120**		**0**	

値1	値2	結果
1(ON)	1(ON)	1(点灯)
1(ON)	0(OFF)	0(消灯)
0(OFF)	1(ON)	0(消灯)
0(OFF)	0(OFF)	0(消灯)

IPアドレスとサブネットマスクのそれぞれの桁に論理積の演算を行った結果が求めるものです。論理積(**AND**)は両方が1の場合のみ1となる。



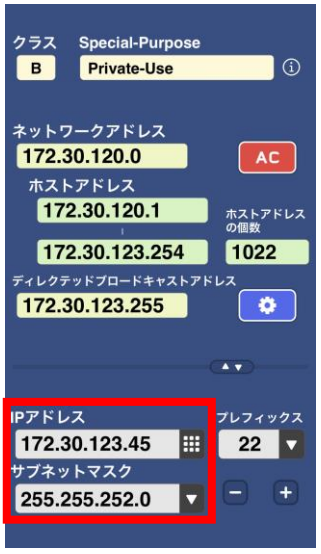
IP基礎

H3C

解説:

IP	**172**		**30**		**123**		**45**	
2進数	1010	1100	0001	1110	0111	1011	0010	1101
マスク	255		255		252		0	
2進数	1111	1111	1111	1111	1111	1100	0000	0000
	ネットワーク部						ホスト部	
開始アドレス	1010	1100	0001	1110	0111	1000	0000	0001
開始アドレス	**172**		**30**		**120**		**1**	
終了アドレス	1010	1100	0001	1110	0111	1011	1111	1110
終了アドレス	**172**		**30**		**123**		**254**	

ネットワークセグメント172.30.120.0のIPアドレス範囲は
172.30.120.1～172.20.123.254



アドレス計算はスマホのアプリが便利です。

答えのネットワークアドレスは
172.30.120.0

また、このサブネットマスクでのIPアドレスの範囲は
172.30.120.1 ～ 172.30.123.254

従って、このサブネットマスクでのIPアドレスの個数は　**1022台**

IPアドレス192.168.0.94、192.168.0.116が同じセグメントになるためのサブネットマスクの値はどれですか。

- **255.255.255.192**
- **255.255.255.224**
- **255.255.255.240**
- **255.255.255.248**

解説:

IP	192		168		0		94	
2進数	1100	0000	1010	1000	0000	0000	0101	1110
IP	192		168		0		116	
2進数	1100	0000	1010	1000	0000	0000	0111	0100
				⇩				
論理積	1111	1111	1111	1111	1111	1111	1100	0000
セグメント	255		255		255		192	

H3C
IToIP Solutions Expert

DHCP

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- LAN上の多数のホストのIPアドレス、サブネットマスク、ゲートウェイアドレス、およびその他のパラメータを手動で設定すると、時間がかかり、エラーが発生しやすくなります。
- DHCPは、LAN上のホストのTCP/IP設定を自動的に完了します。
- DHCPは、IPアドレスの競合を防ぎます。

学習の目標

このレッスンを修了すると、次のことができるようになります：

- DHCPのメカニズムと機能
- DHCPアドレス割り当て方法の説明
- DHCPアドレス割り当てプロセスの説明
- DHCPリレーエージェントの動作の説明
- ルータでのDHCPの設定



DHCPの紹介

H3C

- DHCPはDynamic Host Configuration Protocolの略です。
- Bootstrap Protocol(BOOTP)の拡張として設計されたDHCPは、IPアドレスおよびその他の構成情報をTCP/IPネットワーク上のホストに動的に割り当てます。
- DHCPはクライアント/サーバモデルとして構築されます。クライアントは、サーバにコンフィグレーションパラメータを要求します。IPコンフィグレーション情報を集中管理するサーバは、要求されたコンフィグレーション情報で応答します。
- DHCPメッセージはUDPデータ内にカプセル化されます。DHCPサーバはポート67を使用し、DHCPクライアントはポート68を使用します。

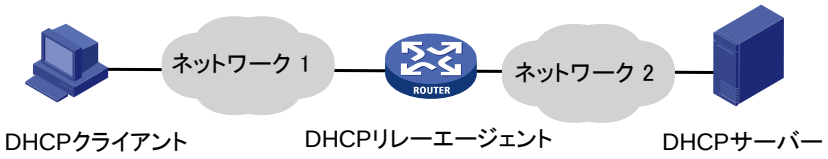
DHCP機能

- DHCPサーバーが提供する情報
  - IPアドレス
  - サブネットマスク
  - デフォルトゲートウェイ
  - DNSサーバのIPアドレス
  - IPアドレスの有効期限（IPアドレスのリース期間）
  - 割り当てから除外するIPアドレス
  - その他オプション

DHCP機能

- プラグアンドプレイ
  - DHCPを使用すると、クライアントは手動で設定することなくIPアドレスと関連する設定パラメータを取得できるため、ネットワーク設定が簡略化され、メンテナンスコストが削減されます。
- 統合管理
  - DHCPサーバは、すべてのIPアドレスと関連する設定パラメータを集中的に管理し、割り当てます。
- 高効率
  - IPアドレスリース管理により、IPアドレスの利用効率が向上します。
- サブネット間での実装
  - DHCPリレーエージェントは、異なるサブネット上のDHCPクライアントとDHCPサーバー間でDHCPメッセージを渡すことができます。

DHCPシステムコンポーネント



- DHCPサーバー
  - DHCP対応サーバー
- DHCPリレーエージェント
  - 一般に、ルータやレイヤ3スイッチなどのネットワークデバイス
- DHCPクライアント
  - DHCPを使用してIPアドレスを動的に取得するホスト

DHCPアドレス割り当て方法

- 手動割り当て(固定IP)
  - ネットワーク管理者は、特定のIPアドレスをDNSサーバーやプリンタなどの少数のホストに設定します。設定されたIPアドレスは期限切れになりません。
- 自動割り当て
  - DHCPは、ネットワークに接続されているホストに永続的なIPアドレスを割り当てます。
- ダイナミック割り当て
  - これは、最もよく使用されるアドレス割り当て方法です。DHCPサーバーは、DHCPクライアントにIPアドレスを一定期間(リース期間)割り当てます。リース期間が終了した後、クライアントは再度IPアドレスを要求する必要があります。

ダイナミックIPアドレス割り当て



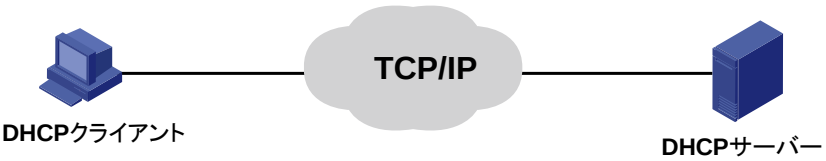
DISCOVER（発見）：IPアドレスが割り当てられますか？

OFFER（提示）：10.0.0.2/24を提供することができます。

REQUEST（要求）：提案された10.0.0.2/24を使用します。

ACK（承認）：許可します

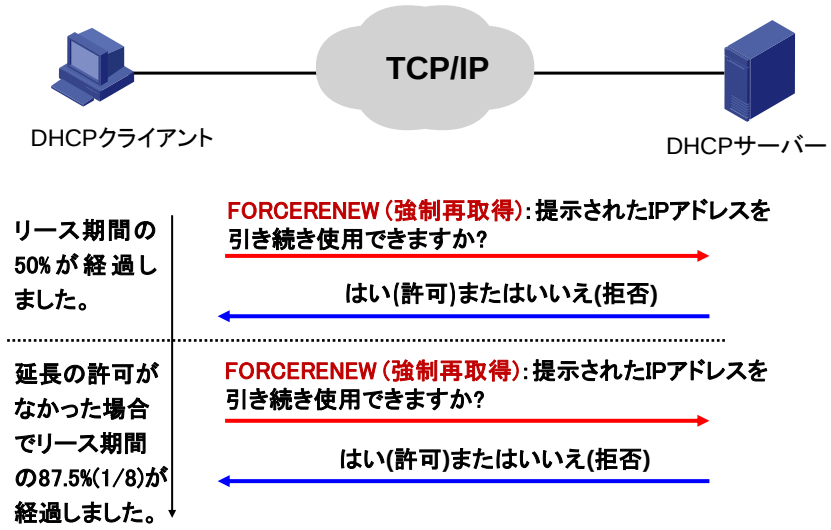
アドレスの拒否と解放



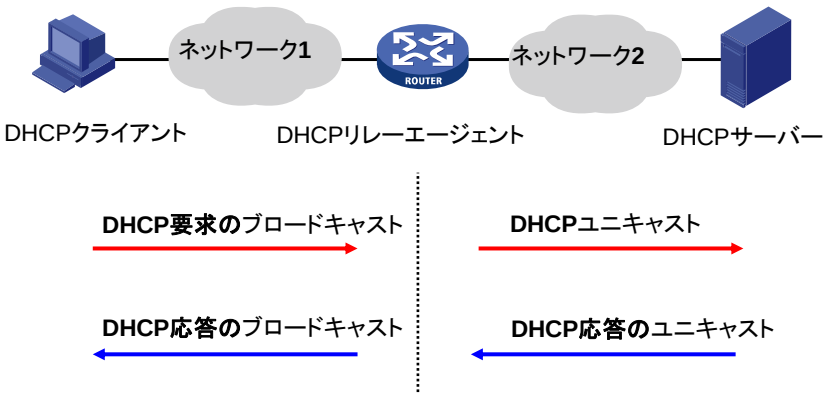
DECLINE（辞退）：10.0.0.2/24はすでに使用されています。
使用できません。

RELEASE（解放）：アドレスはもう必要ないので、返却します。

DHCPリース期間の更新(延長)



DHCPリレーエージェントの動作



DHCPサーバの基本設定コマンド

- DHCPを有効にする。

[Router] dhcp enable

- DHCPアドレスプールを作成します。

[Router] dhcp server ip-pool *pool-name*

- ダイナミック割り当てのIPアドレスの領域を指定します。

[Router] dhcp server ip-pool 0
[Router-dhcp-pool-0] network *network-address*
[*mask-length* | **mask** *mask*]

- DHCPクライアントのゲートウェイIPアドレスを指定します。

[Router-dhcp-pool-0] gateway-list *ip-address*&<1-8>

DHCPサーバのオプション設定コマンド

- DHCPクライアントのためのDNSサーバアドレスを指定します。

[Router-dhcp-pool-0] dns-list *ip-address*&<1-8>

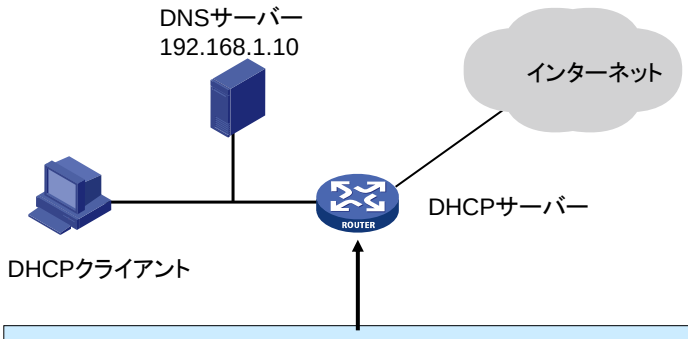
- ダイナミック割り当てから特定IPアドレスを除外します。

[Router] dhcp server forbidden-ip *start-ip-address*
[*end-ip-address*]

- ダイナミックに割り当てられるIPアドレスのリース期間を指定します。

[Router] dhcp server ip-pool 0
[Router-dhcp-pool-0] expired { **day** *day* [**hour** *hour*
[**minute** *minute* [**second***second*]] | **unlimited** }

DHCPサーバの設定例




```
[Router] dhcp enable
[Router] dhcp server forbidden-ip 192.168.1.10
[Router] dhcp server forbidden-ip 192.168.1.254
[Router] dhcp server ip-pool 0
[Router-dhcp-pool-0] network 192.168.1.0 mask 255.255.255.0
[Router-dhcp-pool-0] gateway-list 192.168.1.254
[Router-dhcp-pool-0] dns-list 192.168.1.10
[Router-dhcp-pool-0] expired day 5
[Router-dhcp-pool-0] quit
```


DHCPサーバの表示とメンテナンスコマンド

- DHCPアドレスプール情報を表示します。

[Router] display dhcp server pool [*pool-name*]

- DHCPアドレスプール内の割り当て可能なIPアドレスに関する情報を表示します。

[Router] display dhcp server free-ip

- DHCPサーバの統計情報を表示します。

[Router] display dhcp server statistics

DHCPリレーエージェントの基本設定コマンド

- DHCPを有効にする。

[Router] dhcp enable

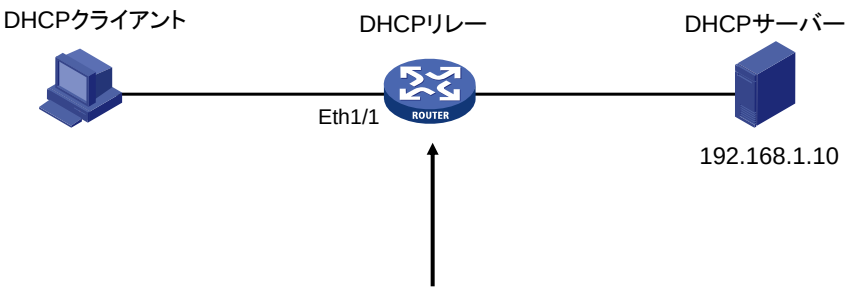
- DHCPサーバーのIPアドレスを指定します。

[Router] interface Ethernet1/1
[Router-Ethernet1/1] dhcp relay server-address *ip-address*

- インターフェイス上でDHCPリレーエージェントを有効にします。

[Router-Ethernet1/1] dhcp select relay

DHCPリレーエージェントの設定例




```
[Router] dhcp enable
[Router] interface ethernet 1/1
[Router-Ethernet1/1] dhcp select relay
[Router-Ethernet1/1] dhcp relay server-address 192.168.1.10
[Router-Ethernet1/1] quit
```

DHCPリレーエージェントの表示と保守コマンド

- DHCPリレー情報を表示します。

[Router] display dhcp relay server-address [**interface** *interface-type interface-number*]

- DHCPリレークライアント情報を表示します。

[Router] display dhcp relay client-information[**interface** *interface-type interface-number* | **ip** *ip-address* [**vpn-instance***vpn-instance-name*]]

- DHCPリレーパケット統計情報を表示します。

[Router] display dhcp relay statistics [**interface** *interface-type interface-number*]

復習

- DHCPはクライアント/サーバモデル上に構築されます。
- DHCPは自動的にIPアドレスをDHCPクライアントに割り当てます。
- DHCPはリース管理を通じてIPアドレスの利用効率を向上させます。
- DHCPリレーエージェントを使用すると、サブネット間でDHCPを動作させることができます。
- ルータは、DHCPサーバーまたはDHCPリレーエージェントとして設定できます。


H3C
ITOIP Solutions Expert

コマンドライン操作の基本

バージョン 1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- コンソールポート、AUXポート、Telnet、およびSSHを使用して、ネットワークデバイスの設定環境を設定できます。
- H3C Comwareでは、これらの設定方法で使用されるコマンドラインの設定を階層的に制御しています。

学習の目標

このレッスンを修了すると、次のことができるようになります:

- ネットワークデバイスの設定
- 階層コマンドラインを使用する
- 基本コマンドでデバイスを管理する



アジェンダ

- ネットワークデバイスの設定
- コマンドライン操作ガイド
- よく使用するコマンド
- リモートログインの設定
- 基本的なVLAN設定

コマンドラインインタフェースへのアクセス

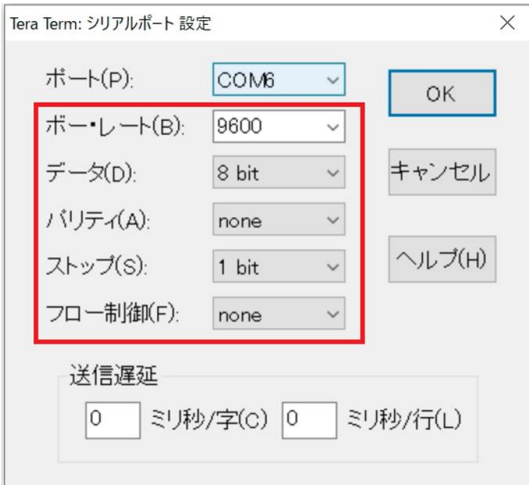
- コンソールポートを介したローカルでのログイン
- AUXポートを介したリモートからのモデムでのログイン
- telnetを介したログイン
- SSHを介したログイン

コンソールポートを介した接続の設定

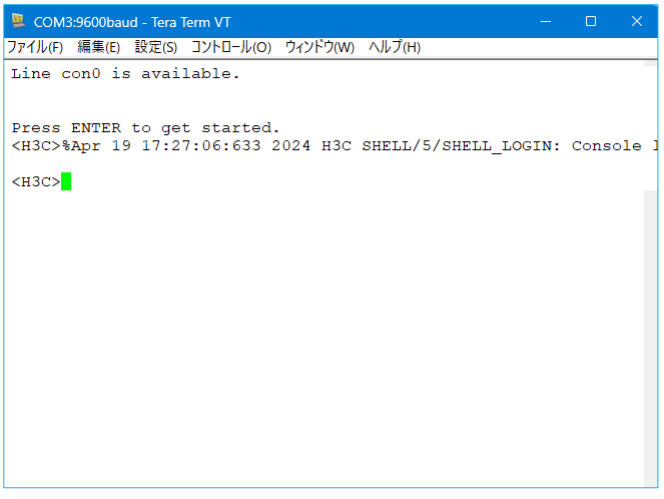


USBシリアル変換
ケーブル

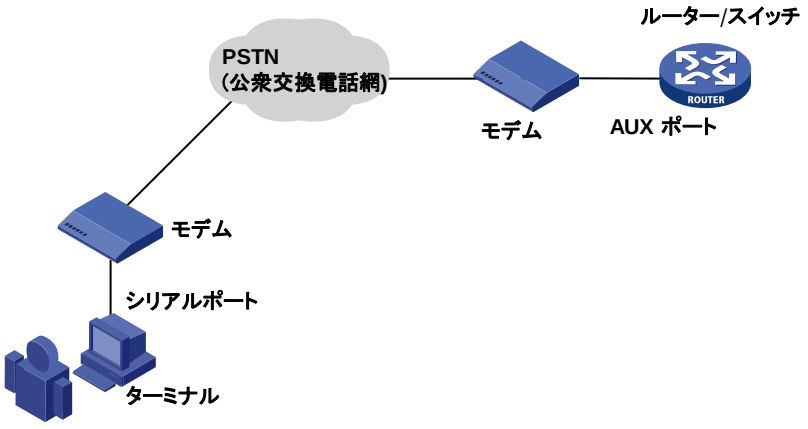
COMポートを選択する



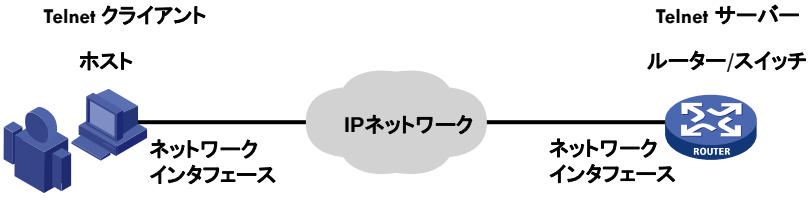
デバイス設定インターフェイスに入る



AUXポート経由の接続の設定



Telnetを介した接続の設定



SSH概要

H3C

•Secure Shell(SSH)はリモートデバイスに安全にログインするためのアプローチを提供します。

•SSHは、転送プロトコル、認証プロトコル、および接続プロトコルで構成されます。

•TCPポート22を使用して、パスワード認証方式と公開キー認証方式を提供します。



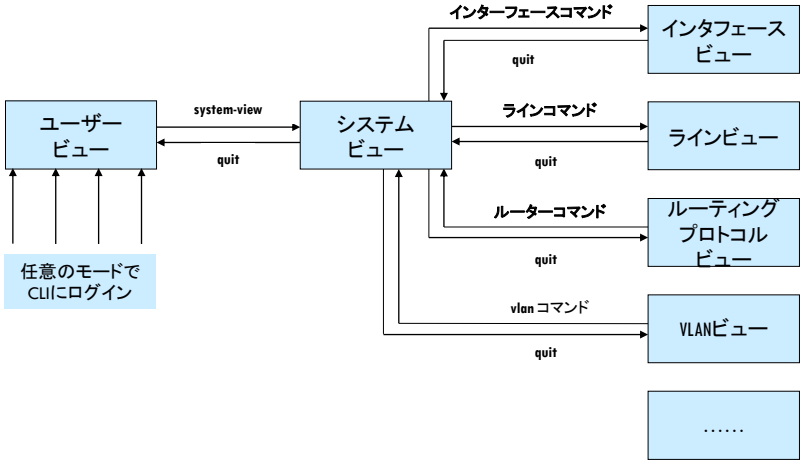
アジェンダ

- ネットワークデバイスの設定
- コマンドライン操作ガイド
- よく使用するコマンド
- リモートログインの設定
- 基本的なVLAN設定

コマンドビュー

- ユーザービュー
  - デバイス起動後のデフォルトビュー。
    実行ステータスと統計情報を表示できます。
- システムビュー
  - システムグローバルパラメータが構成されているビュー
- ルーティングプロトコルビュー
  - ルーティングプロトコルパラメータを構成するためのビュー
- インタフェースビュー
  - インタフェースパラメータを構成するためのビュー
- ラインビュー
  - デバイスにログインするユーザーの属性を設定するための
    ビュー

ビューの関係



- 任意のビューからユーザービューに戻るには、Ctrl+Zを押します。

コマンドビューを使用する

```
******************************************************************************
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Line aux0 is available.


Press ENTER to get started.
<H3C>%Oct 13 09:16:14:706 2013 H3C SHELL/5/SHELL_LOGIN: TTY logged in
from aux0.

<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0]description to_MyPC
[H3C-GigabitEthernet0/0]ip add 192.168.0.1 255.255.255.0
[H3C-GigabitEthernet0/0]quit
[H3C]user-interface vty 0 63
[H3C-line-vty0-63]authentication-mode scheme
```


コマンドタイプ

- 読み出しタイプ
  - **display**コマンドや**dir**コマンド(ファイル情報表示用)など、システム構成情報や保守情報を表示するために使用します。
- 書込タイプ
  - **info-center enable**コマンド(情報センター機能を有効にする)やdebuggingコマンド(デバッグ情報を設定する)など、システムの設定に使用します。
- 実行タイプ
  - **ping**コマンドや**FTP**コマンド(FTPサーバとの接続を確立するため)などの特定の機能を実行するために使用します。

ユーザーロール

H3C

ユーザーロール	ユーザー権限
network-admin	システムの全ての機能及び資源を設定する権利
network-operator	全ての機能および資源を表示する権限(**display history-command all**を除く)

ユーザーロール

H3C

ユーザーロール	ユーザー権限
レベル-n(n=0～15)	**Level-0** - **ping**、**tracert**、**ssh2**、**telnet**、**mtrace**、**super**などのコマンドにアクセスできます。レベル0のアクセス権は設定可能です。 **level-1** - システム内の機能およびリソースの**display**コマンドにアクセスできます。**level-1**ユーザーロールには、level-0ユーザーロールのすべてのアクセス権も付与されます。level-1アクセス権は設定可能です。 **level-2**から**level-8**、および**level-10**から**level-14** - デフォルトでは、アクセス権はありません。アクセス権は構成可能です。 **level-9** - システムのほとんどの機能およびリソースにアクセスできます。レベル9のユーザーロールを持つローカルユーザーアカウントでログインしている場合は、ローカルユーザーアカウントのパスワードを変更できます。 次に、レベル9ユーザーロールがアクセスできない主な機能とコマンドを示します。 RBAC non-debuggingコマンド。 ローカルユーザー。 ファイル管理。 デバイス管理。 **display history-command all**コマンド。 **level-15** - network-adminと同じ権限を持ちます。

コマンドラインヘルプ (I)

```
<Sysname>?
User view commands:
  backup            Backup next startup-configuration file to TFTP
server
  boot-loader       Set boot loader
  bootrom           Update/read/backup/restore bootrom
  cd                Change current directory
  clock             Specify the system clock
  copy              Copy from one file to another
  debugging         Enable system debugging functions
  delete            Delete a file
  dialer            Dialer disconnect
  dir               List files on a file system
  display           Show running system information
  fixdisk           Recover lost chains in storage device
  format            Format the device
  free              Clear user terminal interface
  ftp               Open FTP connection
  graceful-restart  Restart LDP protocol
  language-mode     Specify the language environment
  license           Software license information
---- More ----
```

```
[Sysname] interface vlan ?
  <1-4094>  VLAN interface number
[Sysname] interface vlan 1 ?
  <cr>
```


コマンドラインヘルプ (II)

```
<Sysname> di?
   dialer
   dir
   display

<Sysname> dis?
   display

<Sysname> dis
<Sysname> display
<Sysname> display v?
   version
   virtual-access
   vlan
   voice
   voiceboard
   vrrp

<Sysname> display ver?
   version

<Sysname> display ver ?
  <cr>
```

Tabを押すと、コマンドを補完できます。

エラープロンプト情報

```
[Router] di
         ^
 % Ambiguous command found at '^' position.

[Router] dispaly
         ^
 % Unrecognized command found at '^' position.

[Router] display
                ^
 % Incomplete command found at '^' position.

[Router] display interface gigabitethernet 0/0 0
                                               ^
 % Too many parameters found at '^' position.

[Router] display interface gigabitethernet 0/0/0
                                             ^
 % Wrong parameter found at '^' position.

[Router]
```


コマンドラインヒストリー

- コマンドヒストリーを表示する

  display history-command

- ヒストリーバッファの中を表示する
  - ↑またはCtrl+Pを押すと、前のコマンドが表示されます。
  - ↓またはCtrl+Nを押すと、次のコマンドが表示されます。

編集機能

キー	機能
共通キー	編集バッファがいっぱいでない場合は、カーソル位置に文字を挿入し、カーソルを右に移動します。
Backspace	カーソルの左側の文字を削除し、カーソルを1文字分戻します。
← or Ctrl+B	カーソルを左に1文字分移動します。
→ or Ctrl+F	カーソルを右に1文字分移動します。
Ctrl+A	カーソルを現在の行の先頭に移動します。
Ctrl+E	カーソルを現在の行の末尾に移動します。
Ctrl+D	現在のカーソル位置の文字を削除します。
Ctrl+W	カーソルの左側にある連続した文字列内のすべての文字を削除します。
Esc+D	現在のカーソル位置とカーソルの右側にある連続文字列のすべての文字を削除します。
Esc+B	カーソルを左の連続文字列の先頭文字に移動します。
Esc+F	カーソルを右隣の連続した文字列の前に移動します。
Ctrl+X	カーソルの左側にあるすべての文字を削除します。
Ctrl+Y	カーソルの右側にあるすべての文字を削除します。

アイテムのページごとの表示

```
<H3C>display interface
Aux0 current state: DOWN
Line protocol current state: DOWN
Description: Aux0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Physical layer is asynchronous, Baudrate is 9600 bps
Phy-mru is 1700
Last clearing of counters: Never
    Last 300 seconds input rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
    Last 300 seconds output rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
    Input: 0 packets, 0 bytes
           0 broadcasts, 0 multicasts
           0 errors, 0 runts, 0 giants
---- More ----
```

情報が完全に表示されません。次のページに移動してください。

- Space:次の画面ページの情報を表示します。
- Enter:次の画面行の情報を表示します。
- Ctrl+C:表示とコマンドの実行を停止します。

アジェンダ

- ■ ネットワークデバイスの設定
- ■ コマンドライン操作ガイド
- ■ よく使用するコマンド
- ■ リモートログインの設定
- ■ 基本的なVLAN設定

一般的に使用されるデバイス管理コマンド

H3C

- 装置名の設定

```
[H3C] sysname ?
  TEXT  Host name (1 to 30 characters)
```

- システム時間の設定

```
<H3C> clock datetime ?
  TIME  Specify the time (HH:MM:SS)
```

- システム時間の表示

```
<H3C> display clock
```

- バナー/プロンプト情報の設定

```
[H3C] header ?
  incoming  Specify the banner of the terminal user-interface
  legal     Specify the legal banner
  login     Specify the login authentication banner
  motd      Specify the banner of today
  shell     Specify the session banner
```

一般的に使用されるdisplayコマンド

H3C

- バージョン情報の表示

```
<H3C>display version
```

- 現在のコンフィグレーションの表示

```
<H3C>display current-configuration
```

- インタフェース情報の表示

```
<H3C>display interface
```

- インタフェースIPステータスとコンフィグレーション情報の表示

```
<H3C>display ip interface brief
```

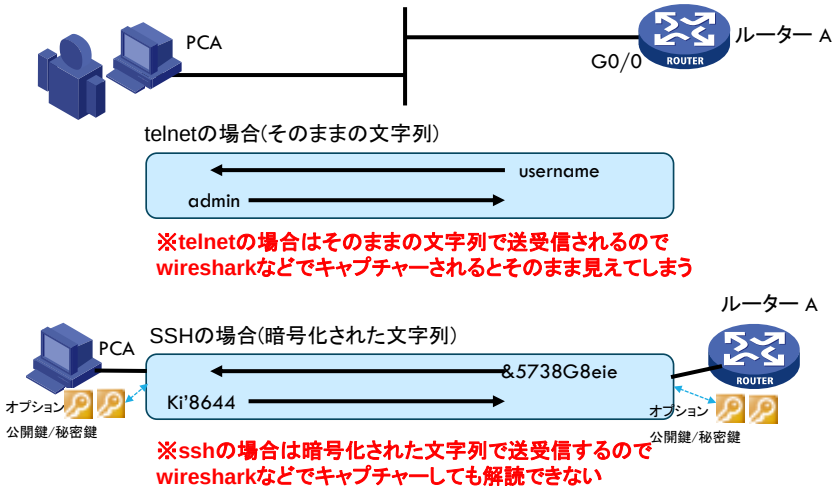
- システム実行統計情報の表示

```
<H3C>display diagnostic-information
```


アジェンダ

- ネットワークデバイスの設定
- コマンドライン操作ガイド
- よく使用するコマンド
- リモートログインの設定
- 基本的なVLAN設定

telnetとSSHの違い



ルータでのTelnetサービスコンフィギュレーションコマンド(I)

- ネットワークに接続するインターフェイスのIPアドレスの設定

```
[H3C]interface ethernet0/0
[H3C-ethernet0/0]ip address ip-address { mask | mask-length }
```

- Telnetサーバ機能のイネーブル化

```
[H3C]telnet server enable
```

- VTYユーザインターフェイスビューに入り、認証方式を設定します。

```
[H3C]user-interface vty first-num2 [ last-num2 ]
[H3C-ui-vty0]authentication-mode { none | password |
scheme }
```

ルータでのTelnetサービスコンフィギュレーションコマンド (II)

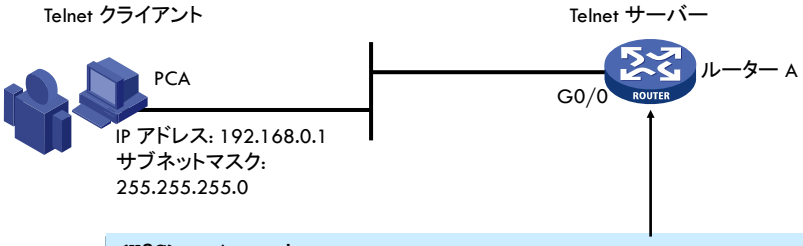
- ログインパスワードとユーザロールの設定

```
[H3C] line vty 0 63
[H3C-line-vty0-63] set authentication password {hash | simple } password
[H3C-line-vty0-63] user-role role-name
```

- ユーザの作成、パスワードの設定、サービスタイプの設定、ユーザロールの設定

```
[H3C] local-user username
[H3C-luser-manage-xxx] password { hash | simple } password
[H3C-luser-manage-xxx] service-type telnet
[H3C-luser-manage-xxx] authorization-attribute user-role role-name
```


Telnetの設定例




```
<H3C>system-view
[H3C]telnet server enable
[H3C]interface GigabitEthernet 0/0
[H3C-GigabitEthernet0/0]ip address 192.168.0.254 24
[H3C]line vty 0
[H3C-line-vty0]set authentication password simple 123456
[H3C-line-vty0]user-role network-admin
```

Telnetによるログイン

```
Microsoft Windows XP [ Version 5.1.2600]
(C) All Rights Reserved1985-2001 Microsoft Corp.

C:¥Documents and Settings¥user>telnet 192.168.0.254

******************************************************************************
* Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.  *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Login authentication

Password:
<H3C>
```

パスワードを入力します。

ルータでのSSHサービスコンフィギュレーションコマンド

- SSHサーバ機能のイネーブル化

```
[H3C] ssh server enable
```

- SSHクライアントのログイン時のユーザインターフェイスの設定

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4]authentication-mode scheme
[H3C-ui-vty0-4]protocol inbound ssh
```

- SSHユーザの設定

```
[H3C] local-user username
[H3C-luser-manage-xxx] password { hash | simple } password
[H3C-luser-manage-xxx] service-type ssh
[H3C-luser-manage-xxx] authorization-attribute user-role role-name
```

- SSHユーザーの登録

```
[H3C] ssh user username service-type stelnet authentication-type
publickey assign publickey filename
```

ルータでのSSHサービスコンフィギュレーションコマンド(II)

- RSAキーの生成

```
[H3C] public-key local create rsa
```

- RSAキーのエクスポート

```
[H3C] public-key local export rsa ssh2 name
```

- ホスト側で生成された公開鍵をインポートする

```
[H3C] public-key peer keyname import sshkey filename
```

- RSAキーの破棄

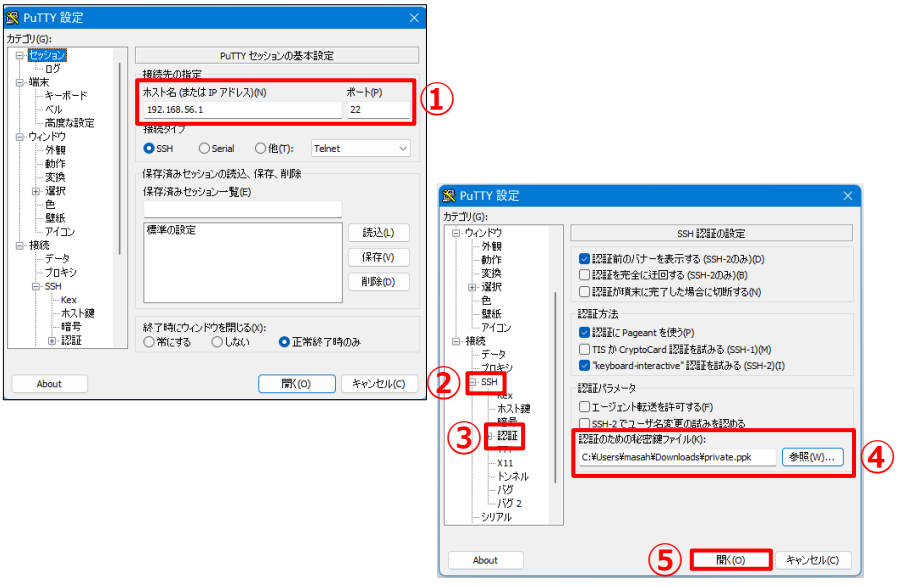
```
[H3C] public-key local destroy rsa
Confirm to destroy the key pair? [Y/N]:y
```


SSHの設定例

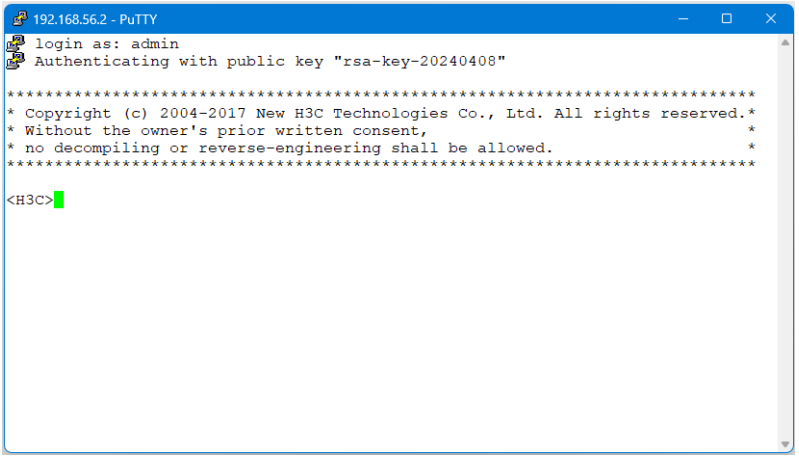



```
[H3C]interface GigabitEthernet0/0
[H3C-GigabitEthernet0/0]ip address 192.168.0.254
255.255.255.0
[H3C]ssh server enable
[H3C]line vty 0 4
[H3C-line-vty0-4]authentication-mode scheme
[H3C-line-vty0-4]protocol inbound ssh
[H3C]local-user sshclient
[H3C-luser-manage-sshclient]password simple abc
[H3C-luser-manage-sshclient]service-type ssh
[H3C-luser-manage-sshclient]authorization-attribute user-role
network-admin
[H3C-luser-manage-sshclient]quit
[H3C]ssh user admin service-type stelnet authentication-type
publickey assign publickey host.pub
```

SSHクライアントの起動



ネットワークデバイスへのログイン



アジェンダ

- ■ ネットワークデバイスの設定
- ■ コマンドライン操作ガイド
- ■ よく使用するコマンド
- ■ リモートログインの設定
- ■ 基本的なVLAN設定

基本的なVLAN設定

H3C

- VLANを作成し、VLANビューを開始します。

```
[Switch]vlan vlan-id
```

- ポートをVLANに割り当てます。

```
[Switch] vlan 10
[Switch-vlan10]port interface-list
```

ポートの設定

パケットの向かう方向	Access	Trunk	Hybrid
タグなしフレームのインバウンド方向	フレームにPVIDタグを付けます。	・ポートでPVIDが許可されている場合は、フレームにPVIDタグを付けます。 ・そうでない場合は、フレームをドロップします。	
タグ付きフレームのインバウンド方向	・ VLAN IDがPVIDと同じであれば、フレームを受信します。 ・ VLAN IDがPVIDと異なる場合は、フレームをドロップします。	・VLANがポートで許可されている場合は、フレームを受信します。 ・VLANがポートで許可されていない場合は、フレームをドロップします。	
アウトバウンド方向	VLANタグを削除し、フレームを送信します。	**・フレームがPVIDタグを持ち、ポートがPVIDに属している場合は、タグを削除**してフレームを送信します。 ・VLANがポート上で伝送されているがPVIDと異なる場合、タグを削除せずにフレームを送信します。	VLANがポートで許可されている場合にフレームを送信します。**フレームにタグをつけるかどうか**は、port hybrid *vlanvlan-id-list* { tagged | untagged } **コマンドの設定によって異なります**。デフォルトはuntaggedです。
		送信するパケットにタグを付けるか、付けないかの判断 ・Trunk: PVIDと同じなら付けない ・Hybrid: 付けるか、付けないかはコマンドで指定(tagged, untagged)	

トランクポートの設定

- ポートのリンクタイプをトランクとして設定します。

```
[Switch] interface Ethernet1/0/1
[Switch-Ethernet1/0/1]port link-type trunk
```

- トランクポートをVLANに割り当てます。

```
[Switch-Ethernet1/0/1]port trunk permit vlan {vlan-id-list all}
```

- トランクポートのデフォルトVLANを設定します。

```
[Switch-Ethernet1/0/1]port trunk pvid vlan vlan-id
```

ハイブリッドポートの設定

- ポートのリンクタイプをハイブリッドとして設定します。

```
[Switch] interface Ethernet1/0/1
[Switch-Ethernet1/0/1] port link-type hybrid
```

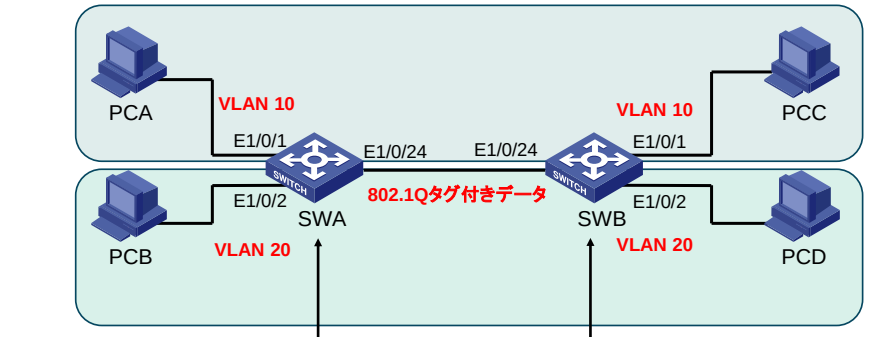
- ハイブリッドポートをVLANに割り当てます。

```
[Switch-Ethernet1/0/1] port hybrid vlan vlan-id-list
{tagged untagged}
```

- ハイブリッドポートのデフォルトVLANを設定します。

```
[Switch-Ethernet1/0/1] port hybrid pvid vlan vlan-id
```


VLANの設定例




```
[SWA]vlan 10
[SWA-vlan10]port Ethernet1/0/1
[SWA]vlan 20
[SWA-vlan20]port Ethernet1/0/2
[SWA]interface Ethernet1/0/24
[SWA-Ethernet1/0/24]port link-type
trunk
[SWA-Ethernet1/0/24]port trunk
permit vlan 10 20
```

```
[SWB]vlan 10
[SWB-vlan10]port Ethernet1/0/1
[SWB]vlan 20
[SWB-vlan20]port Ethernet1/0/2
[SWB]interface Ethernet1/0/24
[SWB-Ethernet1/0/24]port link-type trunk
[SWB-Ethernet1/0/24]port trunk permit vlan
10 20
```

復習

- 複数の構成方法:コンソールポートを介したローカル構成、AUXポート/ Telnet / SSHを介したローカル/リモート構成。
- コマンドラインは、コマンドビューで管理されます。
- コマンドラインは階層的に保護されています。

コマンド操作基礎

H3C

MSR ルーターのイーサネット ポートに IP アドレスを割り当てる場合は、... で操作を実行します？

- ユーザービュー
- システム ビュー
- インターフェイス ビュー
- ルーティング プロトコル ビュー

コマンド操作基礎

MSR では、コマンドの特定のキーワードの最初の数文字を入力してから … キーを押すことができます。システムはコマンドを補完します。

- <Ebter>
- <Tab>
- <Space>
- <Esc>

コマンド操作基礎

スイッチのEthernet1/0/1ポートをトランクポート(タグポート)とするには以下のどのコマンドが適切ですか？

- [SWA] undo port link-type access
- [SWA] undo port link-type trunk
- [SWA-Ethernet1/0/1] undo port link-type access
- [SWA-Ethernet1/0/1] port link-type trunk


H3C
ITOIP Solutions Expert

イーサネットスイッチの基本

v1.0



New H3C Technologies Co., Ltd. All rights reserved

学習の目標

このレッスンを修了すると、次のことができるようになります：

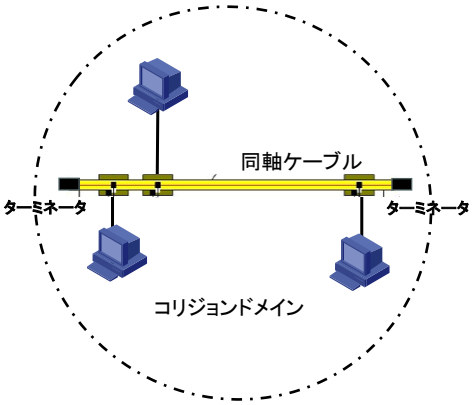
- 共有イーサネットとスイッチドイーサネットの違いを説明
- スイッチがMACアドレステーブルを確立する方法の説明
- スイッチがデータフレームを転送する方法
- 競合ドメインとブロードキャストドメインの特定

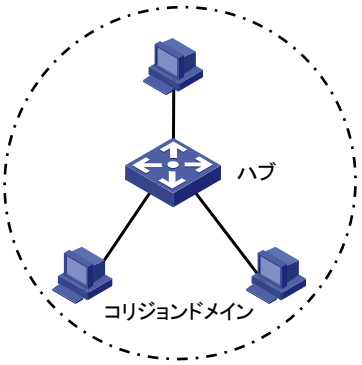


アジェンダ

- 共有イーサネットおよびスイッチドイーサネット
- MACアドレス学習プロセス
- データフレームの転送とフィルタリング
- ブロードキャストドメイン

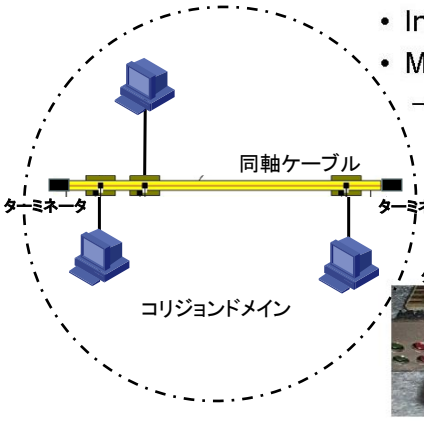
共有イーサネット



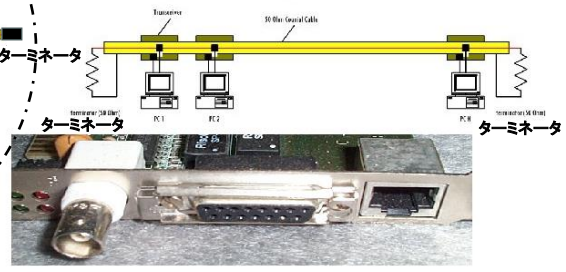


共有イーサネットでは、すべてのホストが同じコリジョンドメインに属し、ネットワーク全体の帯域幅を共有します。

共有イーサネット

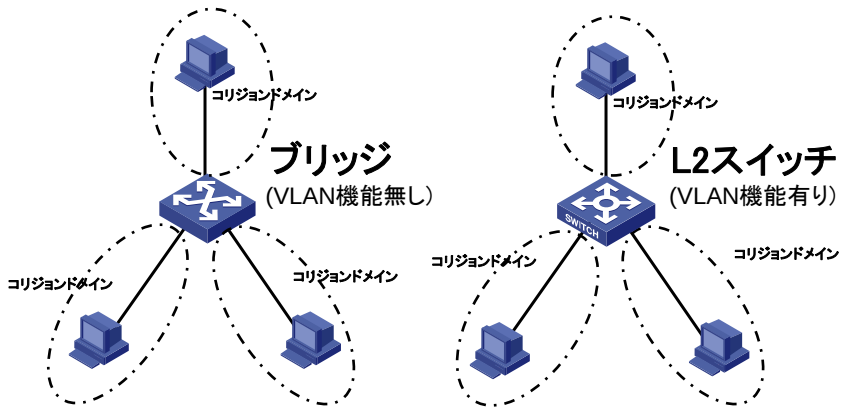


- In 1972, the first bus based Ethernet
- Medium Access Control
  - Carrier Sense Multiple Access with Collision Detection(CSMA/CD)



10base-2　10base-5　10base-T

スイッチドイーサネット

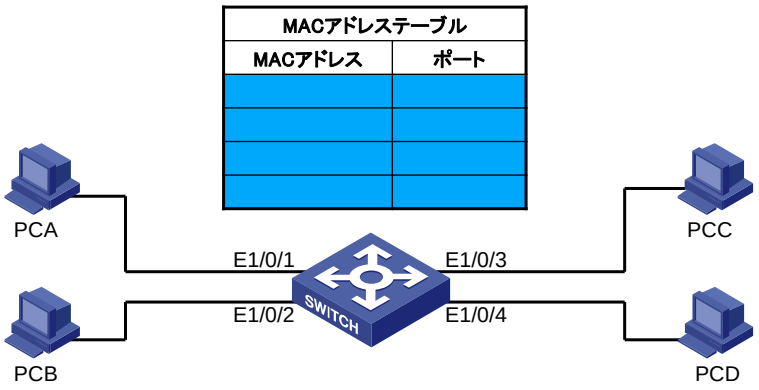


スイッチドイーサネットでは、スイッチのポートはコリジョンドメイン間の境界を形成します。同じポートに接続されたすべてのホストは、ポートの帯域幅を共有します。

アジェンダ

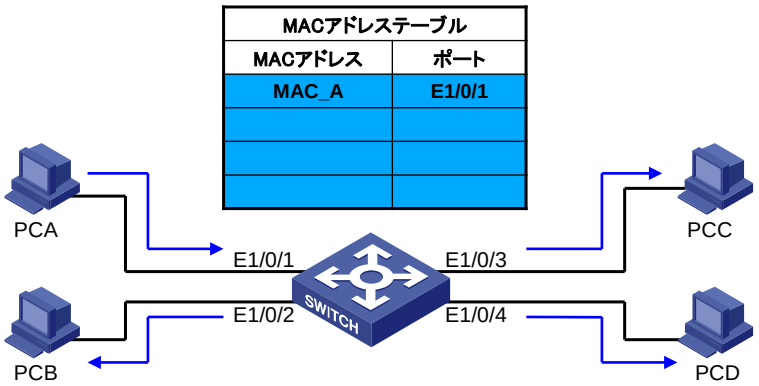
- 共有イーサネットおよびスイッチドイーサネット
- MACアドレス学習プロセス
- データフレームの転送とフィルタリング
- ブロードキャストドメイン

初期MACアドレステーブル



スイッチの起動時には、最初のMACアドレステーブルは空です。

MACアドレス学習プロセス(1)

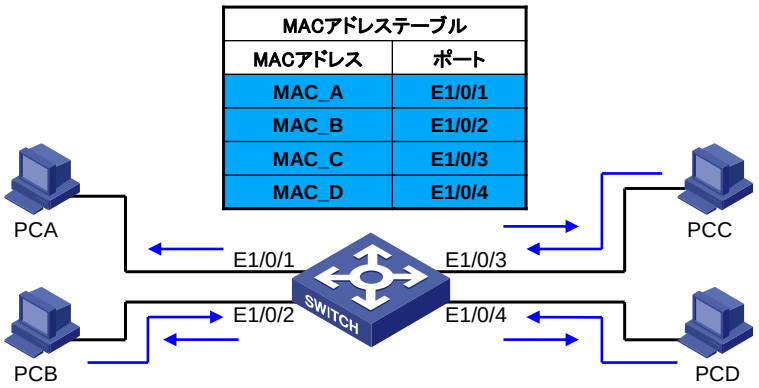


1) PCAはデータフレームを送信します。

2) スイッチは、データフレームの送信元MACアドレスを着信ポートに関連付けます。

3) スイッチは、データフレームをその他のポートへ転送します。

MACアドレス学習プロセス(2)



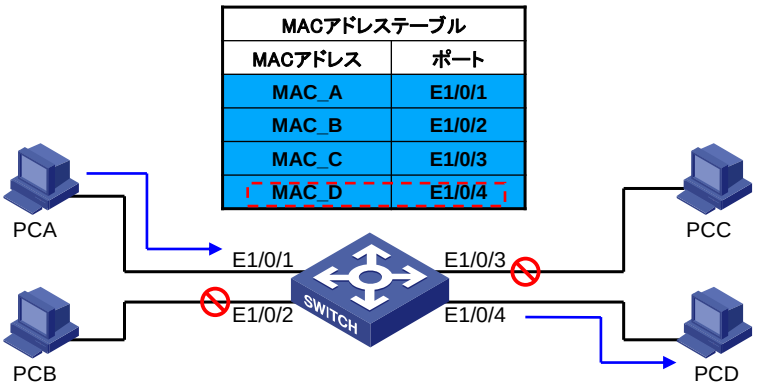
4) PCB, PCC, PCDはデータフレームを送信する。

5) スイッチは、各受信データフレームの送信元MACアドレスを着信ポートに関連付けます。

アジェンダ

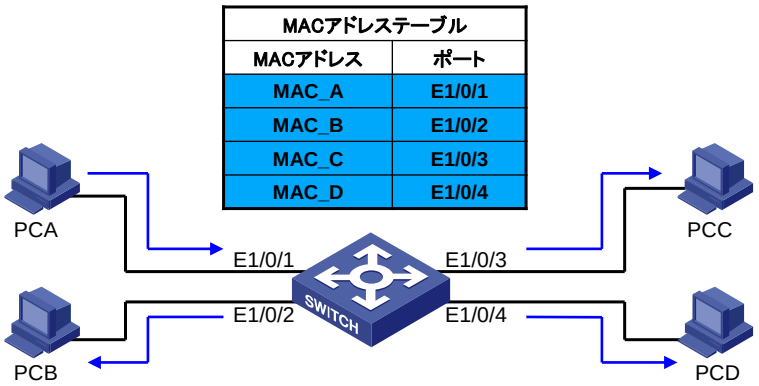
- 共有イーサネットおよびスイッチドイーサネット
- MACアドレス学習プロセス
- データフレームの転送とフィルタリング
- ブロードキャストドメイン

ユニキャストデータフレームの転送



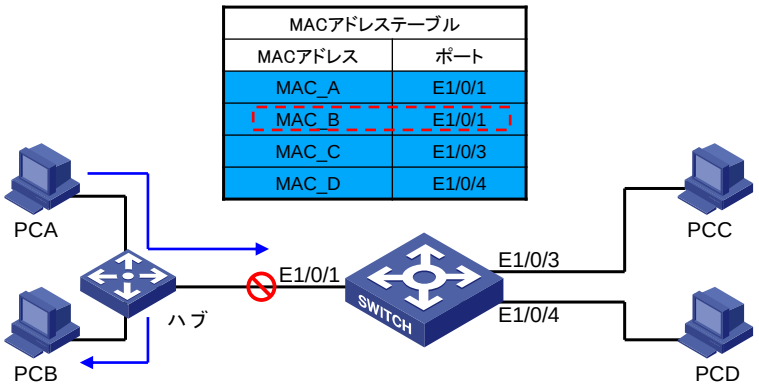
- PC AはPCD宛てのユニキャストフレームを送信します。
- スイッチはMACアドレステーブルに基づいて、フレームをポートEthernet1/0/4に転送します。
- スイッチはフレームを他のポートに転送しません。

ブロードキャスト、マルチキャスト、および不明なユニキャストフレームの転送



スイッチは、着信ポート以外のすべてのポートからブロードキャスト、マルチキャスト、または不明なユニキャストフレームを送信します。

データフレームのフィルタ処理

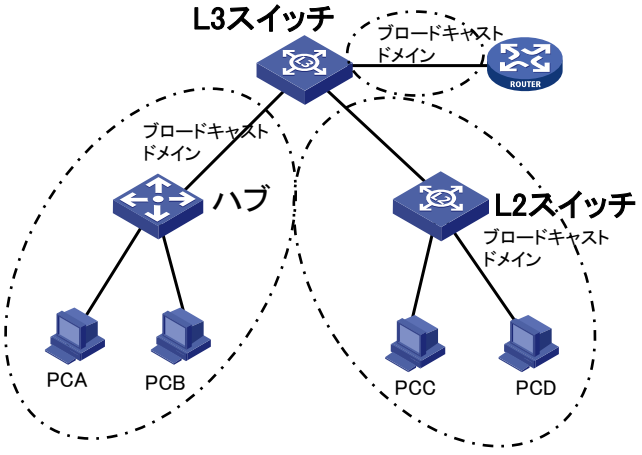


- PCAは、PCB宛てのデータフレームを送信します。
- フレームがポートEthernet1/0/1に到達すると、スイッチは宛先アドレスに基づいてMACアドレステーブルを検索します。エントリが検出され、発信ポートがEthernet1/0/1の場合、スイッチはフレームを廃棄します。

アジェンダ

- 共有イーサネットおよびスイッチドイーサネット
- MACアドレス学習プロセス
- データフレームの転送とフィルタリング
- ブロードキャストドメイン

ブロードキャストドメイン



ルータまたはレイヤ3スイッチの各レイヤ3ポートは、個別のブロードキャストドメインの境界を形成します。

復習

- 共有イーサネット上のすべてのホストはコリジョンドメインを形成しますが、スイッチドイーサネット上のレイヤ2スイッチの異なるポートに接続されたホストは、個別のコリジョンドメインに存在します。
- スイッチは、着信フレームの送信元MACアドレスに基づいてMACアドレステーブルにこの情報を記録します。
- スイッチは、MACアドレステーブルに基づいてデータフレームを転送します。
- ルータ/レイヤ3スイッチのレイヤ3ポートは、ブロードキャストドメイン間の境界を形成します。

H3C

IToIP Solutions Expert

スパニングツリーの設定

v1.0



New H3C Technologies Co., Ltd. All rights reserved

学習の目標

このレッスンを修了すると、次のことができるようになります:

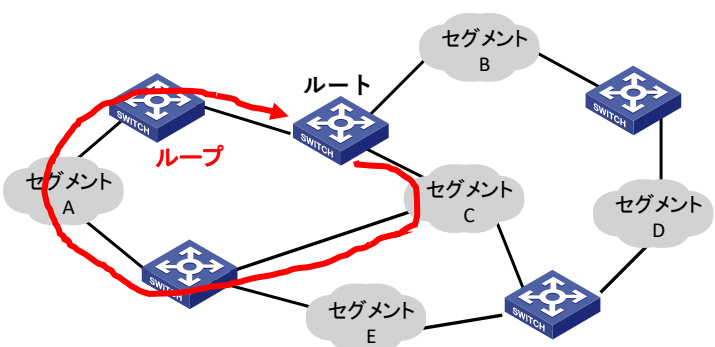
- STPが対処する問題の特定
- STPの動作の説明
- RSTP、PVST、MSTPの動作の説明
- スパニングツリーの設定



アジェンダ

- **STPの背景**
- **STP** (Spanning Tree Protocol)
- **RSTP** (Rapid Spanning Tree Protocol)
- **PVST** (Per VLAN Spanning Tree)
- **MSTP** (Multiple Spanning Tree Protocol)
- **基本的なスパニングツリー設定**

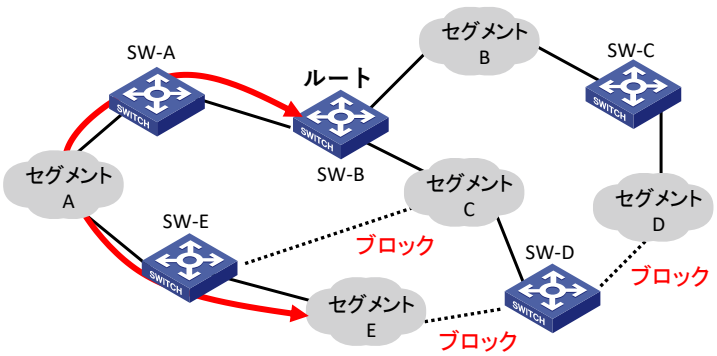
STPでできること?



手順1

- 冗長リンクがあるとループが発生します。

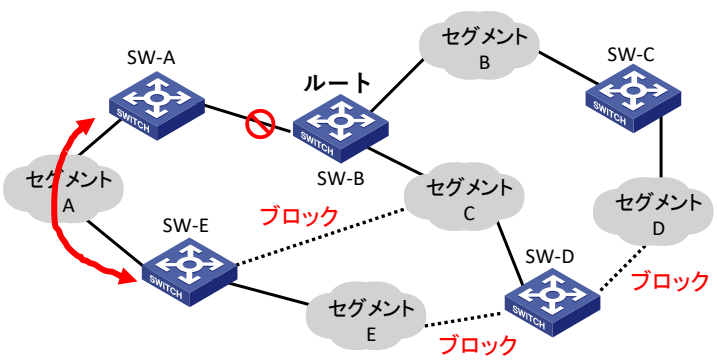
STPでできること?



手順2

- 冗長リンクをブロック(ポートをdisableにする)することで ループを防ぐことができます。

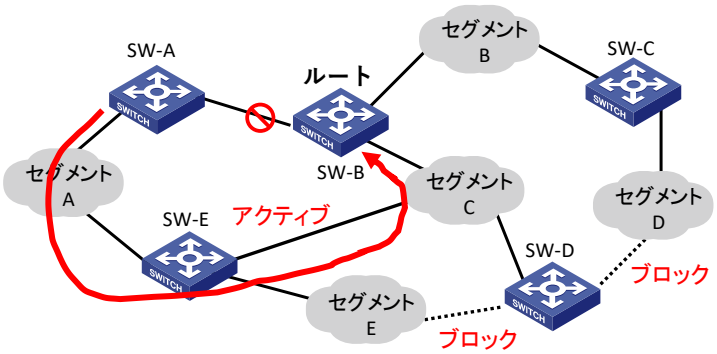
STPでできること?



手順3

- SW-AとSW-B間のリンクに障害が発生すると、SW-Aと SW-B間の通信が遮断されます。

STPでできること?



手順4

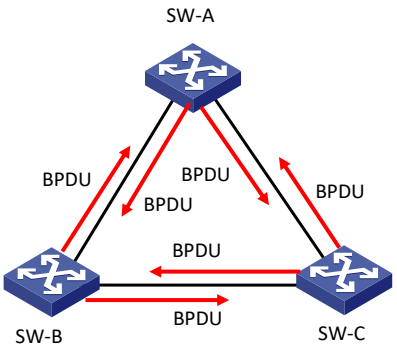
- 障害が発生したリンクの冗長リンクをアクティブにすることでSW-AとSW-B間のネットワーク接続が回復します。

アジェンダ

- **STPの背景**
- **STP (**Spanning Tree Protocol**)**
- **RSTP (**Rapid Spanning Tree Protocol**)**
- **PVST (**Per VLAN Spanning Tree**)**
- **MSTP (**Multiple Spanning Tree Protocol**)**
- **基本的なスパニングツリー設定**

スパニングツリープロトコル

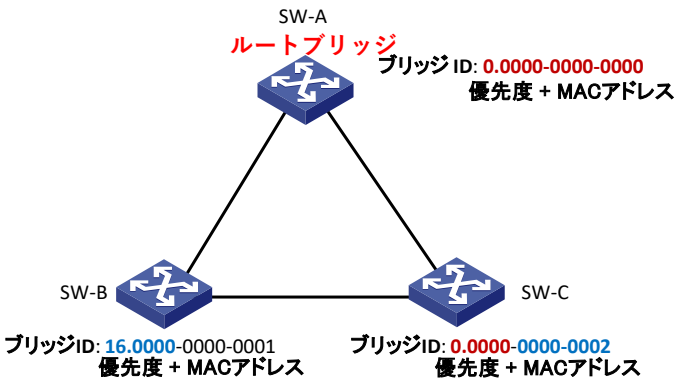
- Spanning Tree Protocol(STP)は、スイッチ接続されたLANのLayer2(データリンク層)でのループを解消します。
- STP対応のスイッチは、Bridge Protocol Data Unit(BPDU)を交換することで、スパニングツリーの計算を完了します。



コンフィギュレーションBPDU

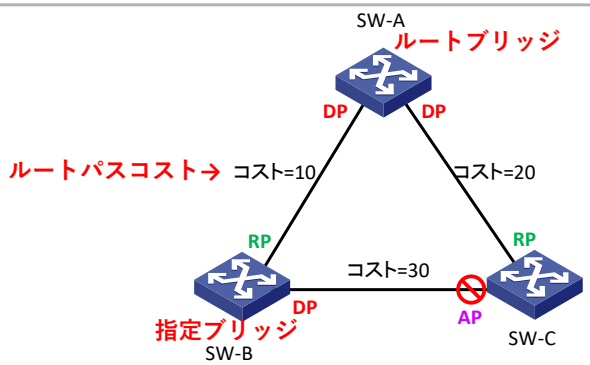
- コンフィグレーションBPDUは次のものを伝送します。
  - **ルートID (重要性により設定した優先度 + MACアドレス)**
  - **ルートパスコスト (回線速度により決まっている)**
  - **指定(Designated)ブリッジID**
  - **指定(Designated)ポートID (物理ポート番号の小さいものを優先)**
- 最初に、各ポートは現在のスイッチをルートブリッジとしてコンフィギュレーションBPDUを生成します。
- トポロジが収束した後、ルートブリッジはコンフィギュレーションBPDUを定期的に送信し、他のブリッジはこれらのBPDUを転送します。これはネットワークに障害が発生していないかを監視するためです。

ルートブリッジの選定



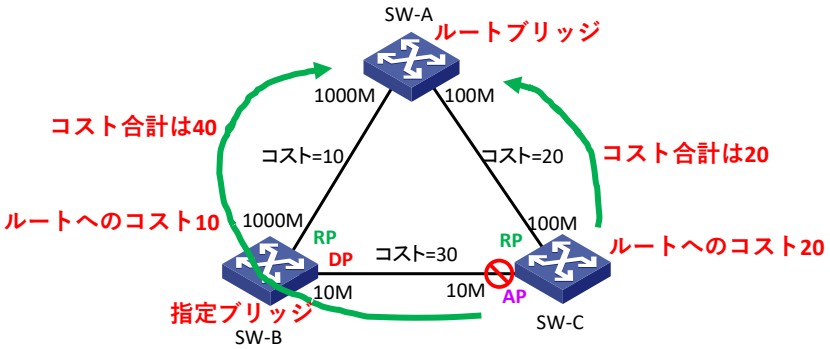
- ブリッジIDは、ブリッジ優先度とMACアドレスで構成されます。ルートIDは、送信側ブリッジがルートブリッジであると見なすブリッジのIDです。
- ブリッジIDが最も小さいブリッジが**ルートブリッジ**として選択されます。

ポートの役割



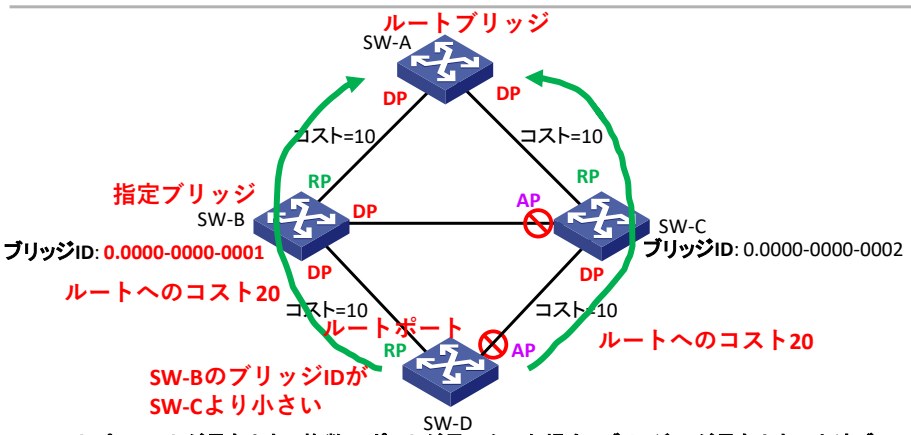
- ルートブリッジ上のすべてのポートが指定ポート(**DP**)です。
- 非ルートブリッジでは、ルートパスコストが最小のポートがルートポート(**RP**)です。
- 各物理セグメントでは、ルートパスコストが最小のブリッジが**指定ブリッジ**になり、指定ブリッジを物理セグメントに接続するポートが指定ポート(**DP**)になります。
- 指定ポートでもルートポートでもないポート代替ポート(**AP:Alternate Port**)はブロックされます。

ルートパスコスト



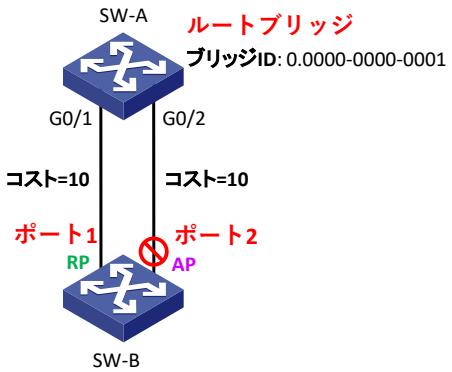
- 非ルートブリッジの場合、ルートパスコストは、ルートブリッジへの最小コストパス上のすべてのポートパスコストの合計です。
- 非ルートブリッジでは、パスコストが最小のポートがRP(ルートポート)として選択されます。
- 物理セグメントでは、ルートパスコストが最小の**指定ブリッジ** (Designated Bridge) として選択されます。

ポートの役割が同条件の時、勝者を決めるブリッジID



- **ルートパスコストが最も小さい複数のポートが見つかった場合、ブリッジIDが最も小さい上流ブリッジに接続されているポートがRP(ルートポート)として選択されます。**
- **ルートパスコストが最も小さい物理セグメントに複数のブリッジが接続されている場合、ブリッジIDが最も小さいブリッジが物理セグメントの指定ブリッジとして選択されます。ルートブリッジの物理セグメントに接続するポートには、DP(指定ポート)のロールが割り当てられます。**

ポートの役割が同条件の時、勝者を決めるポートID



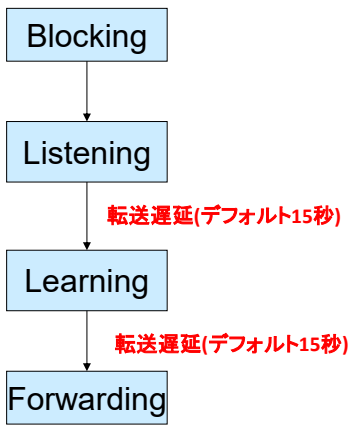
同じ上流のブリッジに接続されているポートが、同じルートパスコストである場合、上流のポートに接続されたポートのうち、**最も小さいポート番号**(ID)を持つポートが、**RP**(ルートポート)になります。

ポートのステータス

状態	ポートの動作
Disable	BPDUの送受信は行われず、データの送受信も行われません。
Blocking	BPDUを受信しますが送信しません。データを受信または転送しません。
Listening	BPDUを送受信しますが、データの送受信は行いません。
Learning	BPDUを送受信して、データの送信元MACアドレスは学習しますが、データの送信は行いません。
Forwarding	BPDUを送受信し、データを送受信します。

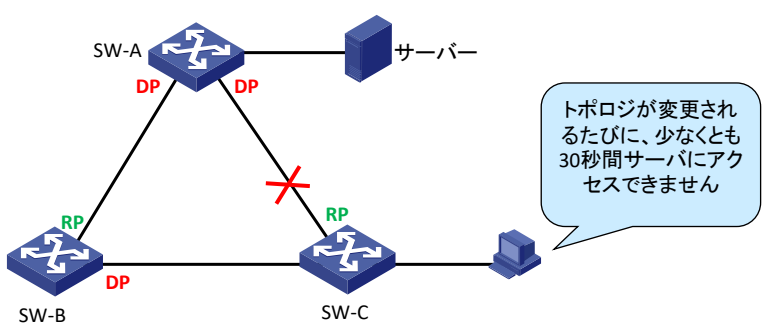
ポート状態遷移

- ルートポートまたは指定ポートが初期ブロッキング状態からフォワーディング状態に移行する前に、リスニング状態とラーニング状態を通過する必要があります。
- デフォルトの**転送遅延は15秒**です。



STPの欠点

- **RP(ルートポート)またはDP(指定ポート)では、ブロッキングからフォワーディングへの移行に2倍の転送遅延(30秒)が発生する必要があります。**
- **トポロジが頻繁に変更されると、ネットワークの接続が常に失われます。**



アジェンダ

- **STPの背景**
- **STP (**Spanning Tree Protocol**)**
- **RSTP (**Rapid Spanning Tree Protocol**)**
- **PVST (**Per VLAN Spanning Tree**)**
- **MSTP (**Multiple Spanning Tree Protocol**)**
- **基本的なスパニングツリー設定**

RSTP

H3C

- Rapid Spanning Tree Protocol(RSTP)は、IEEE802.1D-1998STPを拡張したものです。
- RSTPは、STPのすべての機能を提供します。
- RSTPは、高速なネットワークコンバージェンスを実現します。
- RSTPは、**RP**(ルートポート)または**DP**(指定ポート)がブロッキング状態からフォワーディング状態に移行する際に発生する遅延を短縮します。

RSTPの改良点

イベント	STPの動作	RSTPの動作
ポートはルートポートとして選択されます。	デフォルトでは、状態遷移遅延は転送遅延の2倍です。	ブロックされた代替ポートが存在する場合、遅延はわずか数ミリ秒です。
ポートは指定ポートとして選択されます。	デフォルトでは、状態遷移遅延は転送遅延の2倍です。	指定ポートが非エッジポートの場合、状態遷移遅延は複数の要因に依存します。
		指定ポートがエッジポートの場合、遅延なしにフォワーディング状態に移行します。

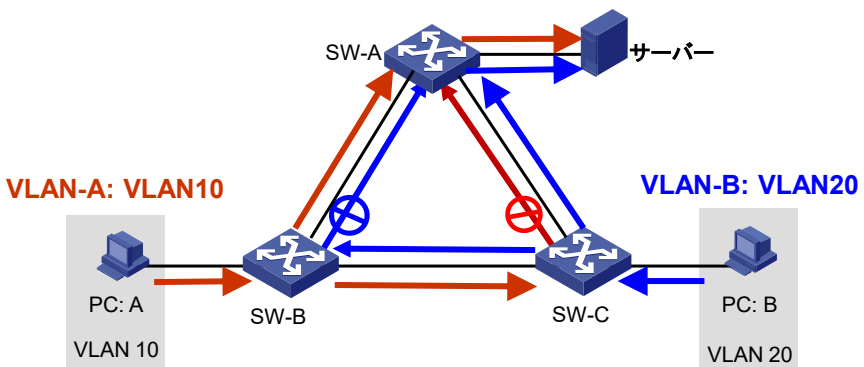
www.h3c.com

アジェンダ

- **STPの背景**
- **STP** (Spanning Tree Protocol)
- **RSTP** (Rapid Spanning Tree Protocol)
- **PVST** (Per VLAN Spanning Tree)
- **MSTP** (Multiple Spanning Tree Protocol)
- **基本的なスパニングツリー設定**

PVST

- PVSTは、Per VLAN Spanning Tree(VLAN単位のスパニングツリー)の略です。
- 各VLANはSTPまたはRSTPを実行します。異なるVLAN間のスパニングツリーは完全に独立しています。

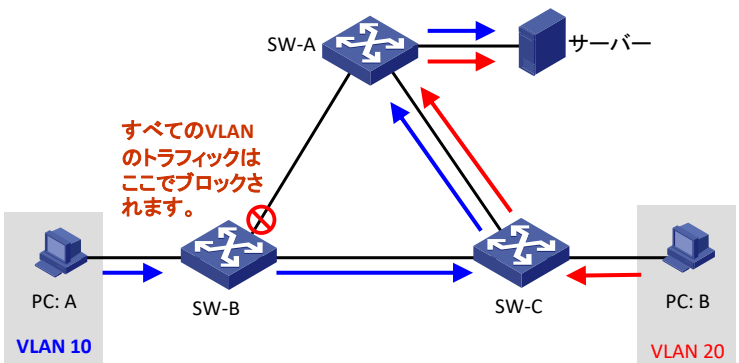


アジェンダ

- STPの背景
- STP (Spanning Tree Protocol)
- RSTP (Rapid Spanning Tree Protocol)
- PVST (Per VLAN Spanning Tree)
- MSTP (Multiple Spanning Tree Protocol)
- 基本的なスパニングツリー設定

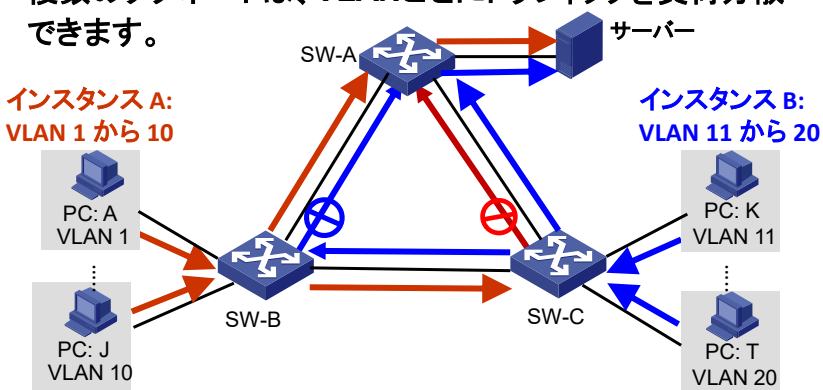
STPとRSTPの欠点

- タグポートは、複数のVLANのトラフィックを伝送します。
- すべてのVLANが同じスパニングツリーを共有します。



MSTP

- **Multiple Spanning Tree Protocol(MSTP)は、1つまたは複数のVLANを1つのインスタンスとして扱い、各インスタンスは独立したスパニングツリーを維持します。従って、インスタンス毎にブロッキングされます。**
- **複数のタグポートは、VLANごとにトラフィックを負荷分散できます。**

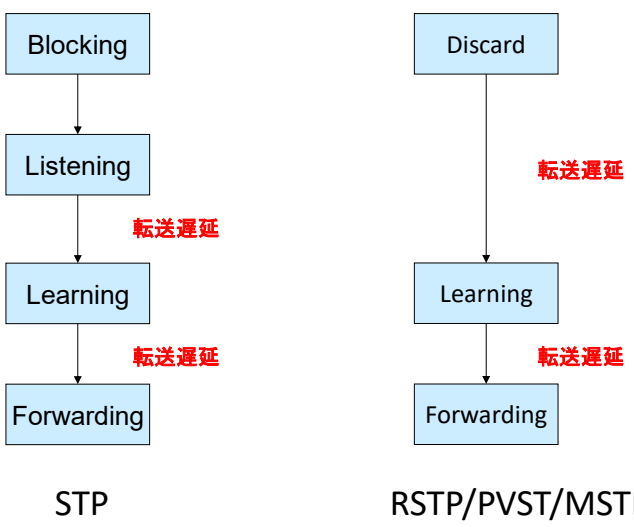


4つのスパニングツリープロトコルの機能比較

機能	STP	RSTP	PVST	MSTP
ループ障害の解決と冗長性の実現	Y	Y	Y	Y
高速収束	N	Y	Y	Y
多重スパニングツリー間の負荷分散	N	N	Y	Y

- MSTPとPVSTは、RSTPおよびロードバランシングとしての高速コンバージェンスをサポートします。
- MSTPは、STPおよびRSTPと互換性があるので、PVSTよりMSTPの方が、汎用性があります。

RSTP/PVST/MSTPとSTP間のポート状態の比較



アジェンダ

- **STPの背景**
- **STP (**Spanning Tree Protocol**)**
- **RSTP (**Rapid Spanning Tree Protocol**)**
- **PVST (**Per VLAN Spanning Tree**)**
- **MSTP (**Multiple Spanning Tree Protocol**)**
- **基本的なスパニングツリー設定**

基本的なスパニングツリー設定

H3C

- スパニングツリー機能をグローバルに有効にします。

```
[Switch] stp global enable
```

- ポート上でスパニングツリー機能をディセーブルにします。

```
[Switch-Ethernet1/0/1] undo stp enable
```

- スパニングツリー機能の動作モードを設定します。

```
[Switch] stp mode { stp | rstp | pvst | mstp }
```

オプションのスパニングツリー設定

- スイッチのブリッジプライオリティを設定します。

[Switch] stp [**instance** *instance-id*] **priority** *priority*
注：*priority*は0-61440で4096刻み

- ポートをエッジポートとして設定します。

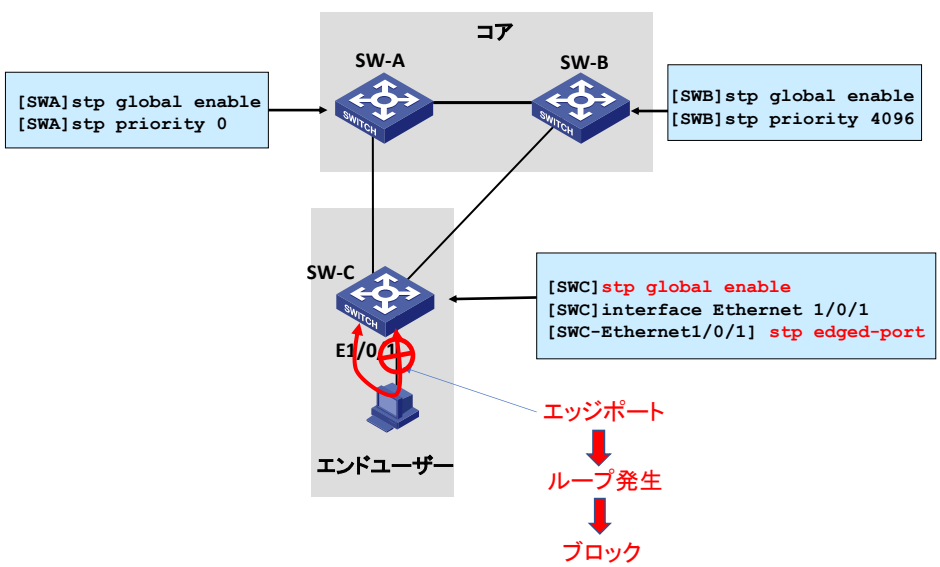
[Switch-Ethernet1/0/1] stp edged-port

エッジポート：ループの発生が起こらないようなポートに設定するので、ツリートポロジーの計算の対象外です。
従って、BPDUは送信しませんが、BPDUを受信した場合、ループが発生していると判断できるため、STPの対象として動作します。

- ポートのコスト

[Switch-Ethernet1/0/1] stp cost *cost*
注：*cost*は1-200000

スパニングツリーの設定例



スパニングツリー機能の表示と保守

```
[SWA]display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge           :32768.000f-e23e-f9b0
Bridge Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :32768.000f-e23e-f9b0 / 0
CIST RegRoot/IRPC     :32768.000f-e23e-f9b0 / 0
CIST RootPortId       :0.0
BPDU-Protection       :disabled
Bridge Config-
Digest-Snooping       :disabled
TC or TCN received    :0
......
```

動作モード

ブリッジID

```
[SWA]display stp brief
 MSTID   Port                Role   STP State     Protection
   0     Ethernet1/0/1       DESI   FORWARDING    NONE
   0     Ethernet1/0/2       DESI   FORWARDING    NONE
......
```

インスタンスID　　ポートロール　　ポートの状態

復習

- STPは、経路の冗長性を確保しながらループを排除します。
- STPの概念は、ブリッジされたネットワークをルートブリッジから広がるツリーにするために不要な部分を削除することです。
- STPに基づいて、RSTPはトポロジの収束を高速化し、MSTPはさらに負荷分散のための多重スパニングツリーの使用を可能にします。

STP

SWAのブリッジプライオリティを0にするのはどのコマンドでしょうか？

- [SWA] stp priority 0
- [SWA-Ethernet1/0/1] stp priority 0
- [SWA] stp root priority 0
- [SWA-Ethernet1/0/1] stp root priority 0

STP

STPプロトコルについての正しい説明はどれでしょうか？

- Bridge IDはBridgeプライオリティとMACアドレスを組み合わせたものです
- H3Cイーサネットスイッチのデフォルトの優先度値は32768です
- 優先度の値が小さいほど、優先度は低くなります。
- 優先度が同じ場合、MACアドレスが小さいほど優先度が高くなります。
- ブリッジID値が大きいほうがルートブリッジとして選択されます

STP

BPDUを受信、処理、送信し、受信したデータのMACアドレスを学習するが、データを転送しない場合、STP 対応ポートは ... 状態です？

- Forwarding
- Listening
- Learning
- Waiting
- Blocking
- Disable

STP

MSTPにはいくつかの特徴があります。正しいものを選択してください（1つまたは、それ以上を選択してください）

- MSTPはSTPおよびRSTPと互換性があります。
- MSTPは、スイッチングネットワークを複数のドメインに分割し、各ドメインは複数のスパニングツリーを形成し、それぞれのスパニングツリーは互いに独立しています。
- MSTPは、ループネットワーク内のパケットの急増と無限のループを回避するために、ループネットワークをループのないツリーネットワークに整えます。
- 以上のどれも正しくない。

STP

STP、RSTP とMSTPについての説明で正しいものはどれでしょうか ？

MSTPはSTPおよびRSTPと互換性があります。

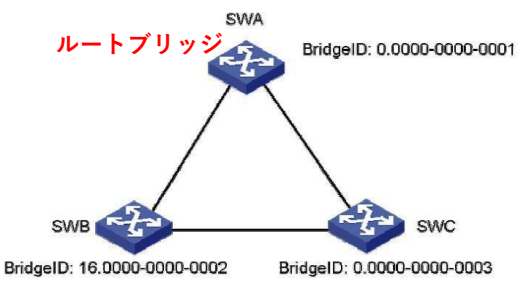
STPはすぐに収束できません。ネットワークトポロジが変更されると、元のブロックされたポートは、転送状態になるまで一定時間待機する必要があります。

RSTPは、STPの最適化されたバージョンです。状況によっては、ポートが転送状態に入るまでの遅延が大幅に短縮されるため、トポロジが安定するために必要なネットワークの最終到達時間が短縮されます。

RSTPとMSTPは異なる経路に設定されて共存できるので、それらのトラフィックの違いを補うことができます

STP

図に示すスイッチングネットワークでは、すべてのスイッチでSTPが有効になっています。図の情報によると、ルートブリッジとしてどのスイッチが選択されますか？

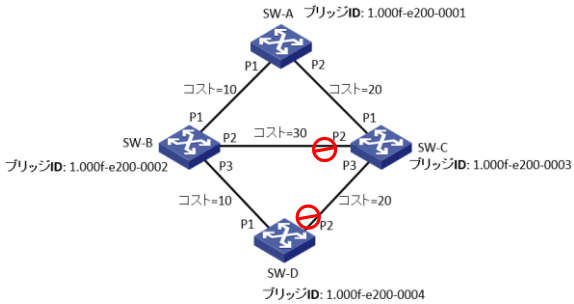


SWA

SWB

SWC

図に示すスイッチングネットワークでは、すべてのスイッチでSTPプロトコルが有効になっています。SWAがルートブリッジとして選択されました。図の情報によると、どのポートがブロッキング状態になるでしょうか？



- SWCのP1
- SWCのP2
- SWDのP1
- SWDのP2

H3C
IToIP Solutions Expert

リンクアグリゲーションの基本と設定

v1.0



New H3C Technologies Co., Ltd. All rights reserved

学習の目標

このレッスンを修了すると、次のことができるようになります:

- リンクアグリゲーションのメリット
- リンクアグリゲーションのアプローチ
- 静的リンクアグリゲーショングループの作成



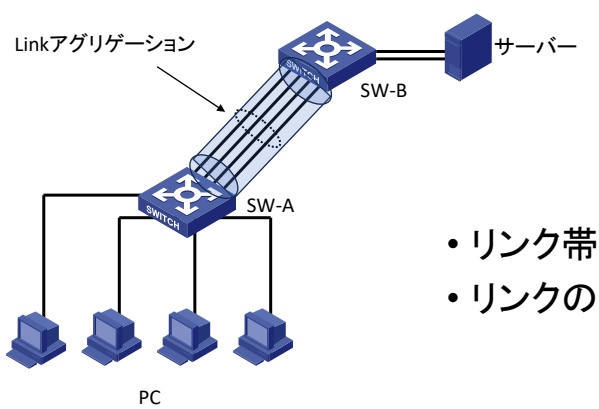
アジェンダ

- リンクアグリゲーションの概要
- リンクアグリゲーションのアプローチ
- 静的リンクアグリゲーショングループの作成

リンクアグリゲーションのメリット

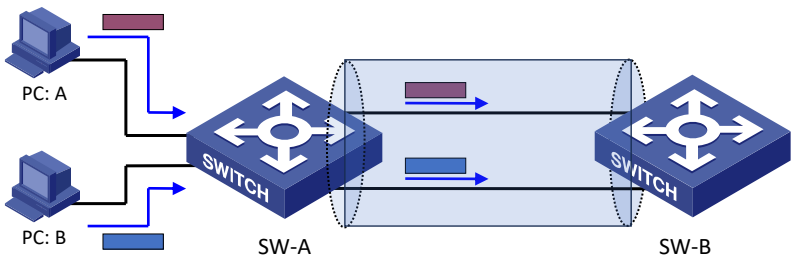
H3C

リンクアグリゲーションは複数の物理ポートを論理的に1つのポートとして扱う技術です。



- リンク帯域幅の増加
- リンクの信頼性の向上

アグリゲーショングループでの負荷分散



リンクアグリゲーショングループ内で、フローベース（パケットが相手に伝わる順番が入れ替わらないようにするためラウンドロビンは行わない）負荷分散が実行されます。

アジェンダ

- リンクアグリゲーションの概要
- リンクアグリゲーションのアプローチ
- スタティックリンクアグリゲーショングループの作成

リンクアグリゲーションのアプローチ

- 静的リンクアグリゲーション
  - **両端のシステムはポートステータスをネゴシエートしません。**
- ダイナミックリンクアグリゲーション
  - **両端のシステムは、LACPを使用してポートステータスをネゴシエートします。**
  - **Link Aggregation Control Protocol(LACP)は、ダイナミックリンクアグリゲーションのIEEE802.3adに記載されています。**

リンクアグリゲーションのアプローチ

静的リンクアグリゲーションの例
<Sysname> system-view
[Sysname] link-aggregation global load-sharing mode destination-mac

link-aggregation global load-sharing mode
{ { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **ip-protocol** | **mpls-label1** | **mpls-label2** | **mpls-label3** | **source-ip** | **source-mac** | **source-port** | **vlan-id** } * | **flexible** | **per-packet** }

※ ingress-port : スイッチ上のどのポートから入ってきたパケットを出力しようとしているか
※ flexible : パケットタイプ(L2, IPv4, IPv6, MPLS)により振り分ける

リンクアグリゲーションのアプローチ

動的リンクアグリゲーションの例

```
<Sysname> system-view
[H3C]int Bridge-Aggregation 1
[H3C-Bridge-Aggregation1]link-aggregation mode dynamic
[H3C-Bridge-Aggregation1]quit
```

リンクアグリゲーションのデフォルト

```
<H3C>display link-aggregation load-sharing mode
Link-aggregation load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```


アジェンダ

- リンクアグリゲーションの概要
- リンクアグリゲーションのアプローチ
- 静的リンクアグリゲーショングループの作成

静的リンクアグリゲーショングループの作成

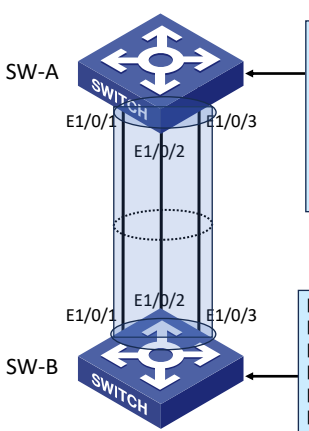
- レイヤー2アグリゲーションインターフェイスを作成する

[Switch] interface bridge-aggregation *interface-number*

- リンクアグリゲーショングループへのイーサネットポートの割り当て

[Switch] interface Ethernet1/0/1
[Switch-Ethernet1/0/1] port link-aggregation group *number*

リンクアグリゲーションの設定例

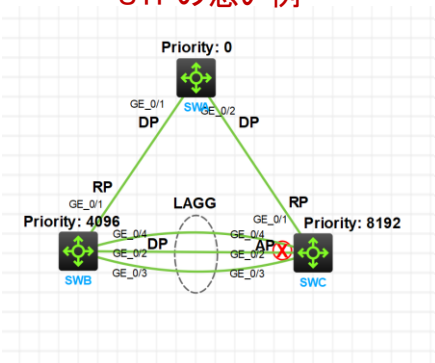



```
[SWA] interface bridge-aggregation 1
[SWA-Bridge-Aggregation1] quit
[SWA]int Ethernet 1/0/1
[SWA-Ethernet1/0/1] port link-aggregation group 1
[SWA]int Ethernet 1/0/2
[SWA-Ethernet1/0/2] port link-aggregation group 1
[SWA]int Ethernet 1/0/3
[SWA-Ethernet1/0/3] port link-aggregation group 1
```

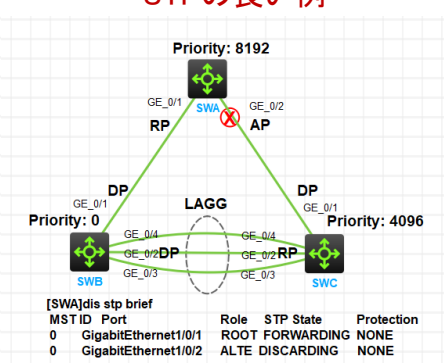
```
[SWB] interface bridge-aggregation 1
[SWB-Bridge-Aggregation1] quit
[SWB]int Ethernet 1/0/1
[SWB-Ethernet1/0/1] port link-aggregation group 1
[SWB]int Ethernet 1/0/2
[SWB-Ethernet1/0/2] port link-aggregation group 1
[SWB]int Ethernet 1/0/3
[SWB-Ethernet1/0/3] port link-aggregation group 1
```

リンクアグリゲーションの設定例

STPの悪い例



STPの良い例




```
[SWA]dis stp brief
 MST ID  Port                    Role  STP State     Protection
 0       GigabitEthernet1/0/1    ROOT  FORWARDING    NONE
 0       GigabitEthernet1/0/2    ALTE  DISCARDING    NONE

<SWB>dis stp brief
 MST ID  Port                    Role  STP State     Protection
 0       Bridge-Aggregation1     DESI  FORWARDING    NONE
 0       GigabitEthernet1/0/1    DESI  FORWARDING    NONE
```


リンクアグリゲーションの表示と保守

```
<Switch>display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e267-6c6a

AGG             AGG     Partner ID      Select      Unselect        Share
Interface       Mode                    Ports       Ports           Type
--------------------------------------------------------------------------
BAGG1           S       none            3           0               Shar
```

アグリゲートIDは 1

アグリゲーション モードはstaticで す。

アグリゲーショングループに3つのメンバーポートが含まれる

メンバーポートは負荷分散されます。

復習

- リンクアグリゲーションは、リンクバックアップの実現、リンク帯域幅の増加、負荷分散の実行に役立ちます。
- リンクアグリゲーションは、静的アグリゲーションとダイナミックアグリゲーションに分類されます。

LAGG

H3C

以下のうちリンクアグリゲーションの機能を選んでください

リンク帯域幅が増加します。

データのロードバランシングの実現

スイッチ間のリンクの信頼性が向上

スイッチングネットワークのループを回避できる

LAGG

ある企業が、異なるベンダーのスイッチを購入しました。装置間をリンクアグリゲーションで接続する必要がありました。1つのベンダーのスイッチがLACPプロトコルをサポートしていないことがわかりました。この場合、以下の構成方法で合理的なものはどれですか?

一方は静的リンクアグリゲーションを設定し、他方はダイナミックリンクアグリゲーションを設定します

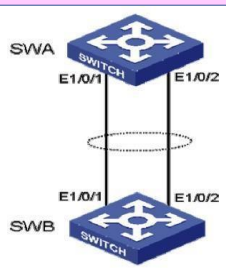
両方の側がダイナミックリンクアグリゲーションを構成します

両方の側が静的リンクアグリゲーションを構成します

リンクアグリゲーションは構成できません

LAGG

スイッチSWAはポートE1/0/1およびE1/0/2を使用して別のスイッチSWBに接続します。帯域幅を増やすには、スイッチで静的リンクアグリゲーションを構成する必要があります。次の構成のうち正しいものはどれですか。



[SWA] interface bridge-aggregation 1
[SWA-Ethernet1/0/1] port link-aggregation group 1

[SWA-Ethernet1/0/2] interface bridge-aggregation 1
[SWA]interface bridge-aggregation 1 port Ethernet1/0/1 Ethernet1/0/2


H3C
IToIP Solutions Expert

TCPおよびUDPの基礎

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- TCPおよびUDPは、TCP/IPスイートにおける2つの主要なトランスポート層プロトコルです。
- TCPはコネクション型であり、信頼性の高いデータ転送を提供します。
- UDPはコネクションレス型です。信頼性の低いデータ転送を提供し、通常は遅延に影響されやすいアプリケーションに使用されます。

学習の目標

このレッスンを修了すると、次のことができるようになります：

- TCP/UDPによって提供されるサービスが識別できる
- TCP/UDPパケット構造の説明
- TCP接続の確立と終了に精通していること
- TCPのスライディングウィンドウを説明する
- TCPの信頼性の高いメカニズムを説明する



アジェンダ

- トランスポート層機能
- TCPの基礎
- UDPの基礎

トランスポート層機能

- コネクション型サービス、またはコネクションレス型サービスを提供する
- 接続ステータスを維持する
- アプリケーションレイヤーデータをセグメントに分割してカプセル化
- ポート番号を利用した多重化の実装
- データを確実に転送
- データ長の長いフレームを分割するフロー制御の実装

アジェンダ

■ トランスポート層機能

■ TCPの基礎

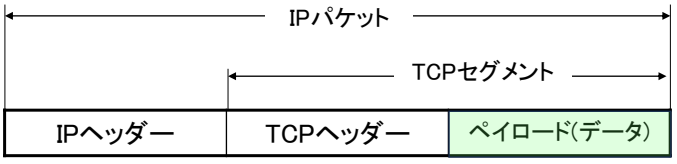
■ UDPの基礎

TCP機能

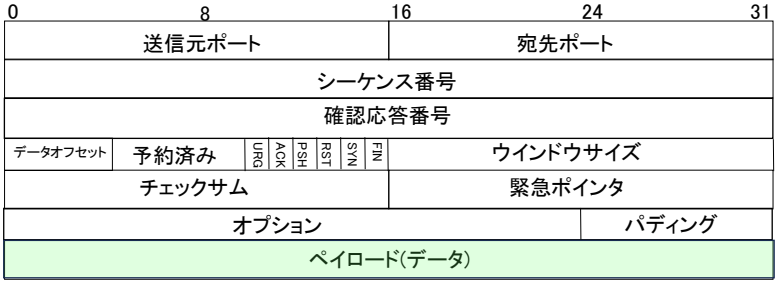
- スリーウェイハンドシェイク
  - 信頼性の高い接続確立
- ポート番号の利用
  - 異なるアプリケーションで利用可能となる
- シーケンス番号
  - セグメント損失検出、送出の順番通りでなく受信したパケットの再配置
- アクノレッジメント
  - 受信確認
- スライドウインドウ
  - フロー制御
- チェックサム
  - エラー検出

TCPカプセル化

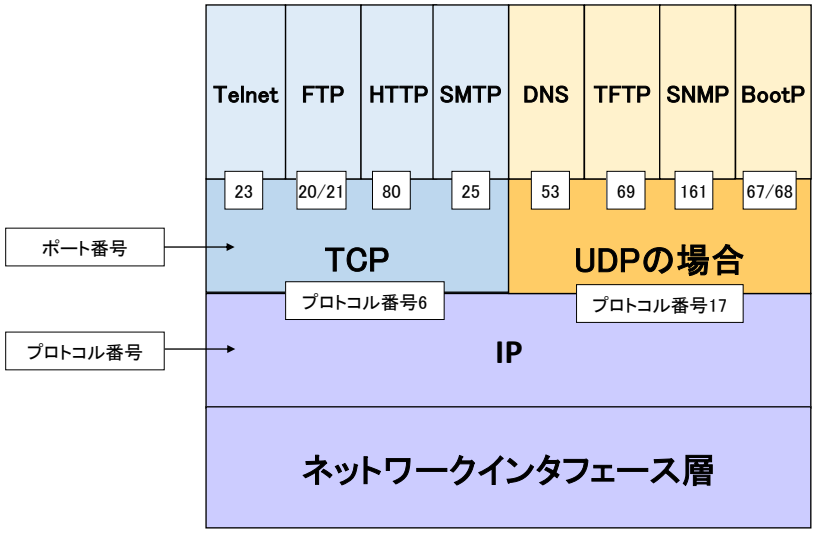
TCPカプセル化



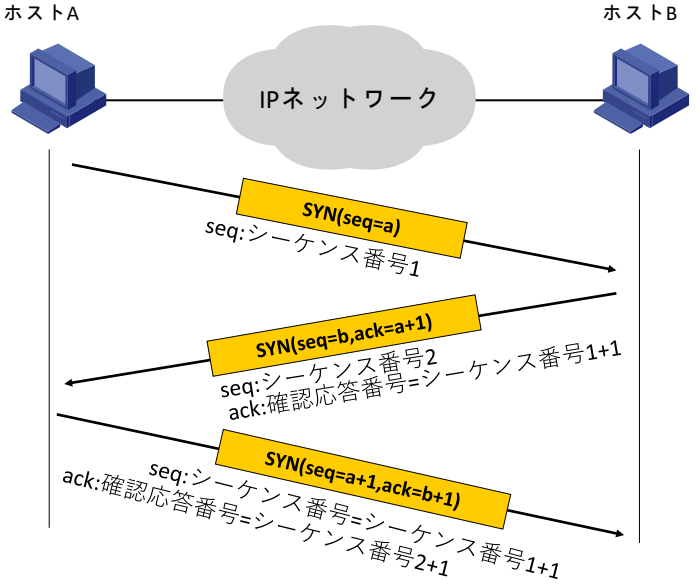
TCPヘッダー形式



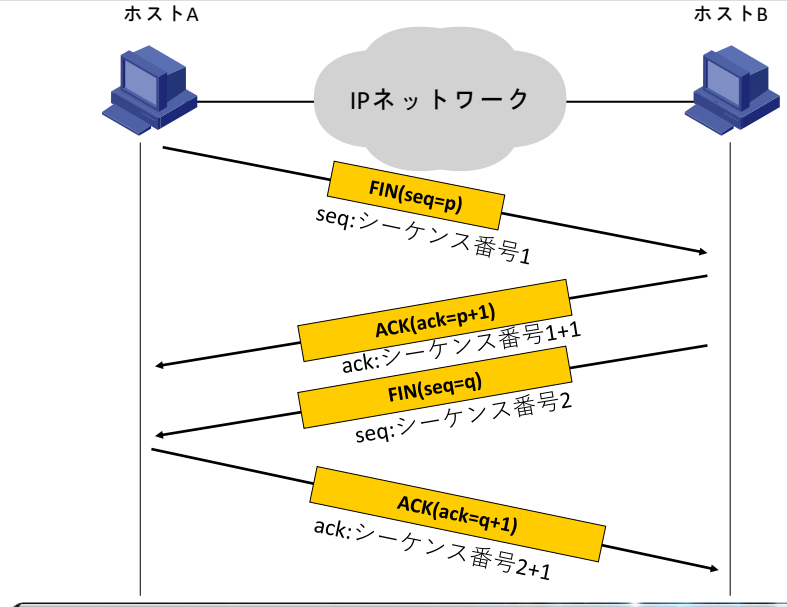
TCP/UDPポート番号



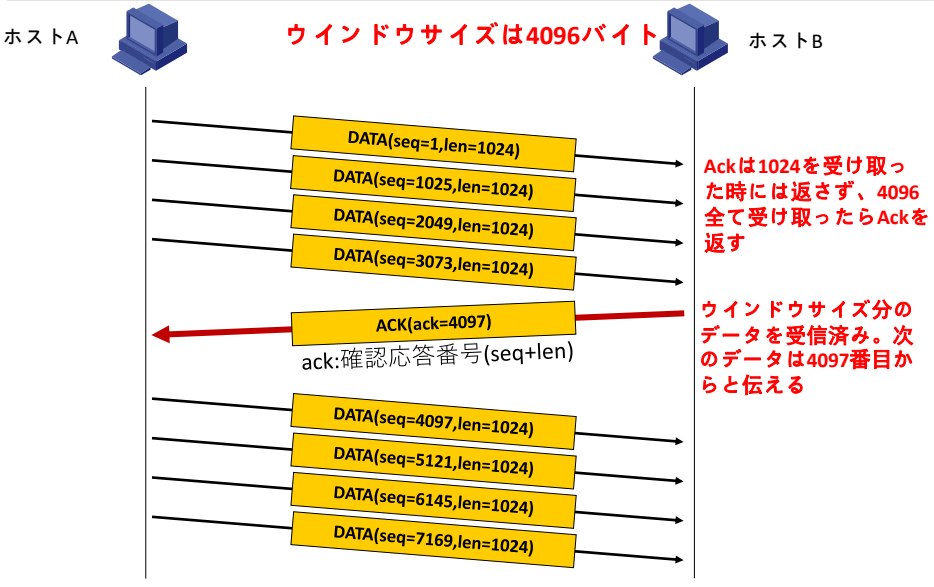
TCP接続の確立(3ウェイハンドシェーク)



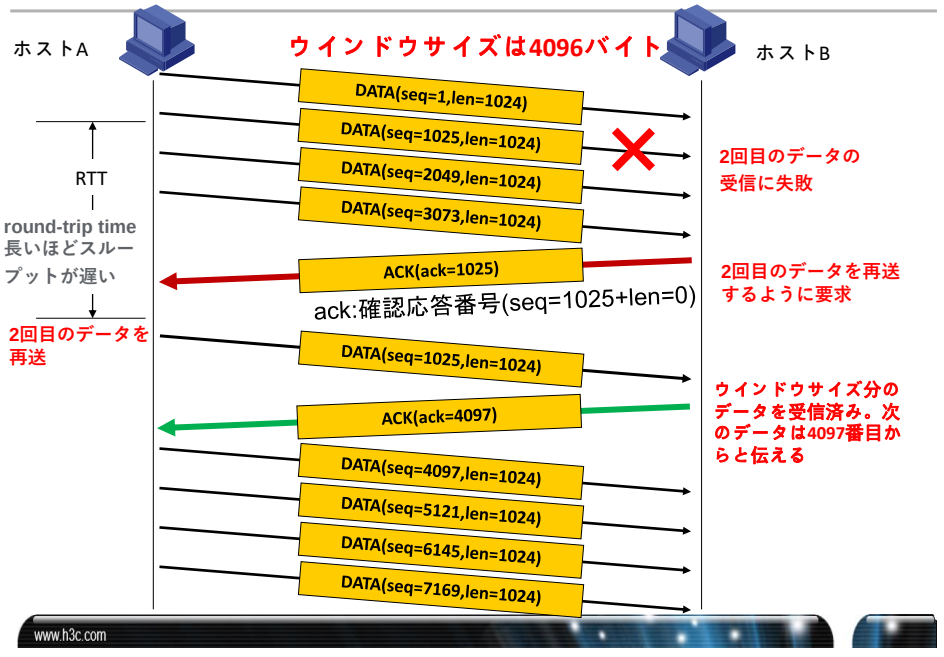
TCP接続の終了



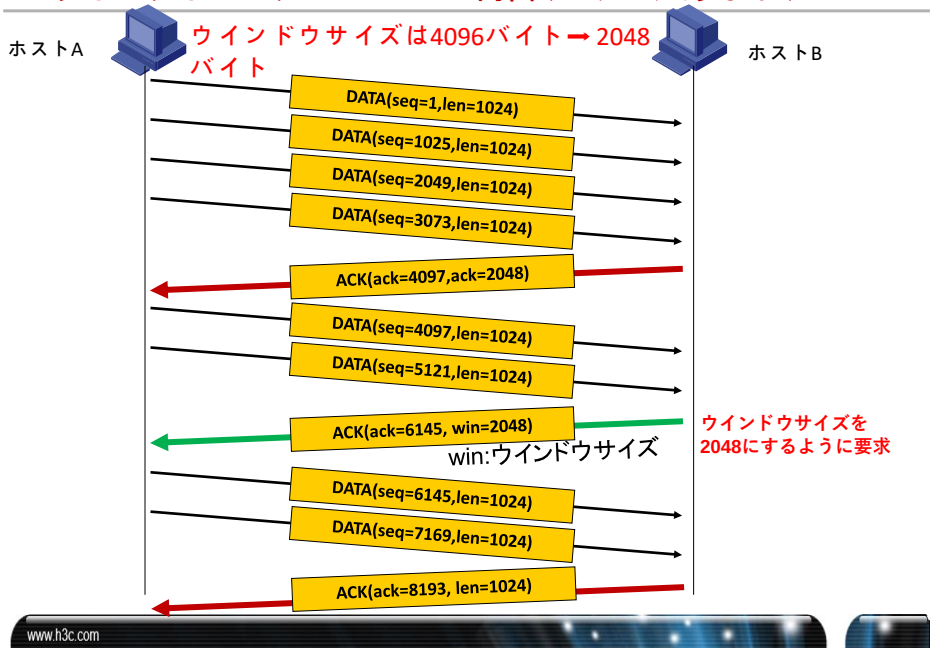
送信確認応答



タイムアウトによる再送信



スライドウインドウでのフロー制御(バッファあふれ)



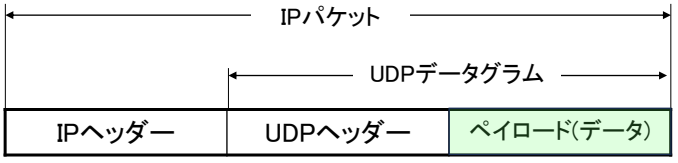
アジェンダ

- トランスポート層機能
- TCPの基礎
- UDPの基礎

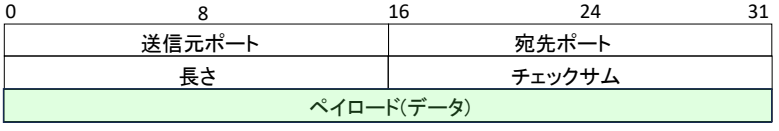
UDPカプセル化

H3C

UDPカプセル化



UDPヘッダーフォーマット



TCPとUDPの比較

項目	TCP	UDPの場合
接続タイプ	コネクション型	コネクションレス
接続ステータスのメンテナンス	エンドツーエンド(受信確認/再送)	該当なし(垂れ流し)
アプリケーション層データのカプセル化	アプリケーション層データをセグメントに分割してカプセル化し、 ポート番号でアプリケーション層プログラムを識別する	アプリケーション層データをデータグラムにカプセル化し、 ポート番号でアプリケーション層プログラムを識別する
データ転送	シーケンス番号と転送確認応答の使用による信頼できるデータ転送	信頼性が低いデータ転送
フロー制御	ウィンドウをスライドすることによるフロー制御	該当なし

TCPの例 – FTP

- FTPは、インターネット上で一般的に使用されるファイル転送プロトコルです。TCPに基づいており、クライアント/サーバモードを使用します。
- FTPはデュアルTCP接続モードを採用しています。
  - → 接続の認証や応答信号の受信は、TCPポート21を使用します。
  - → データの送受信にはTCPポート20が使用されます。
- FTPは2つのモードでファイルを転送します。
  - → アクティブモード
    - FTPサーバーからFTPクライアントに接続
  - → パッシブモード
    - FTPクライアントからFTPサーバーに接続し、データの転送用のポート番号はランダムに決めます

UDPの例 – TFTP

- Trivial File Transfer Protocol(TFTP)もクライアント/サーバモードを採用しています。
- TFTPは、クライアントとサーバ間の複雑な相互作用が不要な環境に適しています。
- TFTPはUDP上で伝送され、データ伝送にポート69を使用します。
- TFTPは、単純なファイル転送機能(アップロードおよびダウンロード)を提供します。
- TFTPは認可および認証メカニズムを提供せず、ディレクトリリスト機能も提供しません。
- TFTPでは、ファイル転送はクライアントによって開始されます。

復習

■TCPおよびUDPはポート番号を使用して、アプリケーション層のプログラムおよびサービスを識別します。

■TCPは、3方向ハンドシェークを使用して信頼性の高い接続を確立します。

■TCPはチェックサムを使用してエラー検出を実装し、シーケンス番号、転送確認および再送信を使用して信頼性のあるデータ転送を提供し、スライディングウィンドウを使用してフロー制御を実装します。

■UDPは実装が容易で、必要なリソースが少なく、よりタイムリーです。これは、信頼性の高いネットワークで伝送される遅延の影響を受けやすいアプリケーションに適用できます。

TCPとUDP基礎

H3C

TCPはOSI参照モデルの … 層に属します？

- 物理層
- トランスポート層
- セッション層
- 表現層(representation Layer)

TCPとUDP基礎

H3C

次のフィールドのうちUDPヘッダーとTCPヘッダーの両方にあるのはどれか？

- シーケンス番号
- 送信元IPアドレス
- 宛先ポート
- 送信元ポート
- チェックサム
- フロー制御

TCPとUDP基礎

TFTPは …. に基づいています。

- UDP
- IPX
- SSH
- TCP

H3C
ITolP Solutions Expert

IP ルーティング

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- ルータは論理ネットワークセグメント間でパケットを転送します。
- ルータは、ルートが一致するパケットを転送するための経路情報を提供します。
- 各ルータは、ルートエントリを格納するルーティングテーブルを保持します。

学習の目標

このレッスンを修了すると、次のことができるようになります:

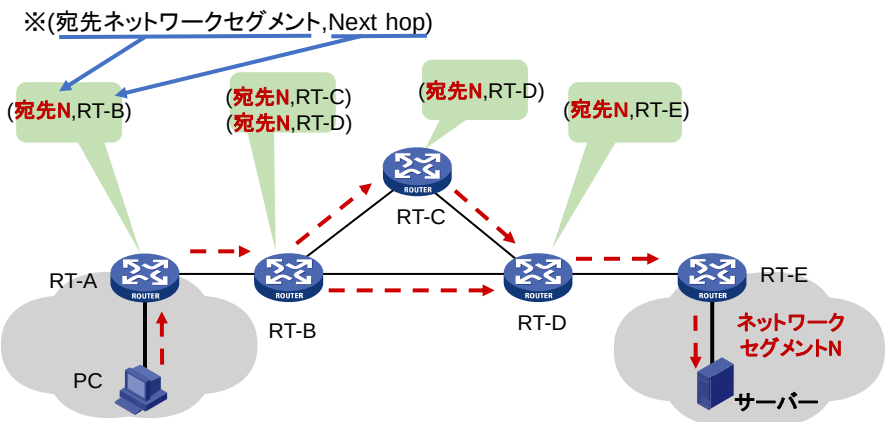
- ルーティング機能について説明する
- ルーティングの基本について説明する
- ルーティングエントリについて説明する
- デバイス上のルーティングテーブルを表示する



ルーティングとは?

H3C

- ルーティングは、IPパケットの転送をガイドする経路情報(ルーティングテーブル)を提供します。



ルーターとL3スイッチの違い

H3C

ルーター:
・WANのインタフェース(ISDN, FR, etc)を持つ
・LANのセグメントを**WANへ**NATでルーティングする
・ポート毎にIPアドレスを割り当てる

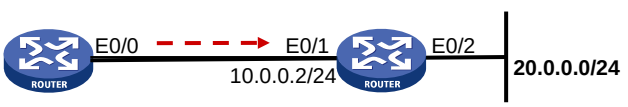
L3スイッチ:
・WANのインタフェースを持たない
・LAN内の異なるセグメント間をルーティングする
・VLAN毎にIPアドレスを割り当てる

L2スイッチ:
・同一セグメント内のスイッチング

ルーティングテーブル項目

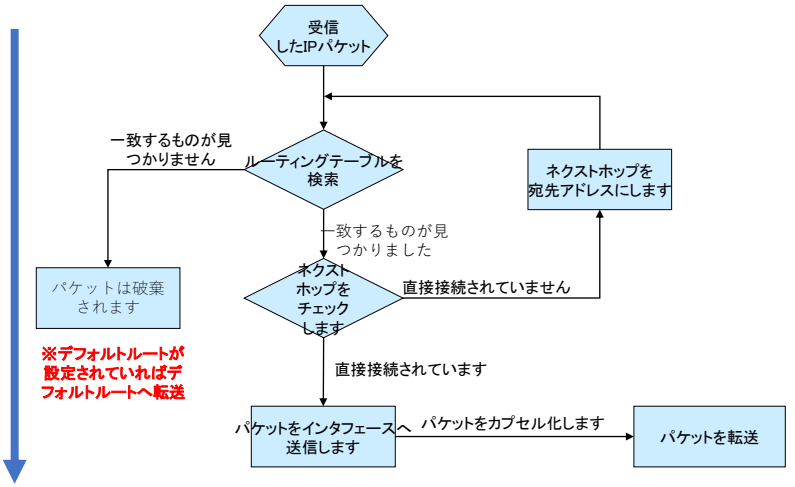
H3C

- **ルータはルーティングテーブルに基づいてパケットを転送します。**

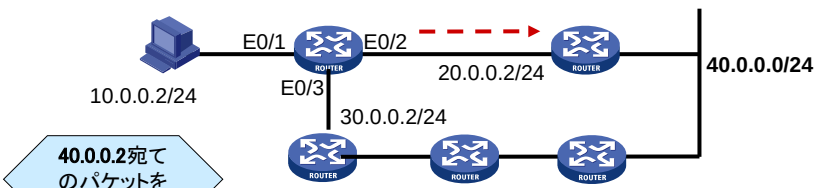


宛先/マスク	ネクストホップ	アウトバウンドインターフェイス	メトリック(コスト)
0.0.0.0/0	20.0.0.2	E0/2	10
10.0.0.0/24	10.0.0.1	E0/1	0
20.0.0.0/24	20.0.0.1	E0/2	0
20.0.0.1/32	127.0.0.1	InLoop0	0
40.0.0.0/24	20.0.0.2	E0/2	1
40.0.0.0/8	30.0.0.2	E0/3	3
50.0.0.0/24	40.0.0.2	E0/2	0

ルータ上でのシングルホップ動作



ルートの検索 – 例1

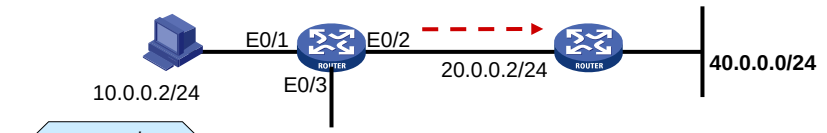


40.0.0.2宛てのパケットを受信します。

宛先/マスク	ネクストホップ	アウトバウンドインターフェイス	メトリック(コスト)
10.0.0.0/24	10.0.0.1	E0/1	0
20.0.0.0/24	20.0.0.1	E0/2	0
20.0.0.1/32	127.0.0.1	InLoop0	0
40.0.0.0/24	20.0.0.2	E0/2	1
40.0.0.0/8	30.0.0.2	E0/3	3
50.0.0.0/24	40.0.0.2	E0/2	0

最も長いマスクを持つエントリが転送に使用されます。

ルートの検索 – 例2



30.0.0.2宛てのパケットを受信します。

宛先/マスク	ネクストホップ	アウトバウンドインターフェイス	メトリック(コスト)
0.0.0.0/0	20.0.0.2	E0/2	10
10.0.0.0/24	10.0.0.1	E0/1	0
20.0.0.0/24	20.0.0.1	E0/2	0
20.0.0.1/32	127.0.0.1	InLoop0	0
40.0.0.0/24	20.0.0.2	E0/2	1
40.0.0.0/8	30.0.0.2	E0/3	3
50.0.0.0/24	40.0.0.2	E0/2	0

デフォルトルートを使用してパケットを転送します。

ルートの発信元

- **ダイレクトルート(ルータのインタフェースそのもの)**
  - → 低コストで構成が容易で、手作業によるメンテナンスが不要。インターフェイスは、直接接続されたネットワークへのルートだけを検出できます。
- **スタティックルート(マニュアルで設定)**
  - → コストがかからず、設定が簡単で、シンプルなネットワークに適しています。
- **ダイナミックルート(他のルータから得たルート)**
  - → ルーティングプロトコルによって動的に検出されます。コストが高く、設定が複雑です。手動によるメンテナンスが不要で、複雑なネットワークに適しています。

メトリック

- **ルートのメトリックは、ローカルデバイスから宛先ルート内までのコストを示します。コストの小さいほうが優先される。**
- **メトリックの計算に使用される基準:**

  → 遅延、帯域幅、リンク使用率、リンク信頼性、ホップカウント、およびPMTU

- **メトリックの計算に使用する基準は、ルーティングプロトコルによって異なります。**

プロトコル	メトリック（コスト）
スタティックルーティング	固定値0
OSPF	帯域幅より算出
RIPv1/RIPv2	ホップカウント

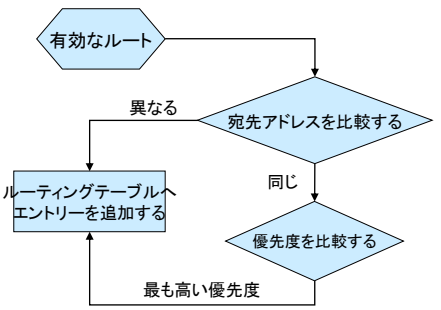
メトリック

OSPFのコスト設計された当時は100Mが最高だったので、100Mを最高を表す1としたが、現状では高速となったデータセンター内のL3スイッチでは最適なルートを見つけられないので、マニュアルでルートのコストを変更することも必要。

帯域幅	OSPFコスト
100Gbps	1
40Gbps	1
10Gbps	1
1Gbps	1
100Mbps	1
10Mbps	10
1.544Mbps	64
768Kbps	133
384Kbps	266
128Kbps	781

ルートの優先度

- 同じ宛先への複数のルートが使用可能な場合
  - ルートを検出したルーティングプロトコルの優先度が比較されます。
  - **優先度値が小さいほど、優先度が高くなります。**
  - 最も高い優先度を持つルーティングプロトコルによって検出されたルートがルーティングテーブルに追加されます。



ルーティングプロトコルのデフォルトの優先度

ルートの決定順はまずは優先度値が小さい(優先度が高い)ルートが優先されます。同じ優先度であれば、次にコストにより比較します。

ルートタイプ	デフォルト設定
ダイレクトルート	0
OSPF内部ルート	10
スタティックルート	60
RIPルート	100
OSPF外部ルート	150
BGPルート	256

ルーティングテーブルの表示

- ルーティングテーブルの要約情報を表示します:

[Router] display ip routing-table

- 特定のルートに関する情報を表示します:

[Router] display ip routing-table *ip-address* [*mask-length* | *mask*]

- ルーティングテーブルのルート統計情報を表示します:

[Router] display ip routing-table statistics

ルーティングテーブルの要約情報

```
[Router]display ip routing-table

Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      NextHop         Interface
0.0.0.0/32          Direct  0    0         127.0.0.1       InLoop0
2.2.2.2/32          Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0         127.0.0.1       InLoop0
224.0.0.0/4         Direct  0    0         0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0         0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0         127.0.0.1       InLoop0
```

ルートメトリック

ルーティングプロトコルの優先度

復習

- ルーティングはIPパケットの転送をガイドします。
- ルートエントリには、宛先アドレス/ネットワークマスク、ネクストホップ、インターフェイスなどが含まれます。
- ルートの発信源(ダイレクト、スタティック、ダイナミック)
- ルートメトリックとルーティングプロトコルの設定
- デバイス上のルーティングテーブルの表示

次のルーティングプロトコルのうち、宛先ネットワークまでの距離と方向のみを反映するのはどれですか？

- RIPv2
- OSPF
- IGP
- RIPv1

MSR ルーターがネットワーク 100.120.10.0/24 への 2 つのルートを取得し、2 つのルートのコストがそれぞれ 120 と 10、優先度が 10 と 150 であるとします。その後、ネットワーク宛てのデータ パケットは…？

優先度が 150 のルートを採用。

コストが 120 のルートを採用

優先度が 10 のルートを採用。

コストが 10 のルートを採用

ITofIP Solutions Expert

ダイレクトルートおよびスタティックルート

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- ルータは、手動で設定することなく、直接接続されたネットワークへのルートを取得できます。
- ダイレクトルーティングとVLAN間ルーティングの機能は、さまざまな複雑なルーティング機能を理解し、小規模なネットワークを構築するための基礎となります。
- スタティックルートは手動で設定され、単純なネットワークに適用されます。

学習の目標

このレッスンを修了すると、次のことができるようになります:

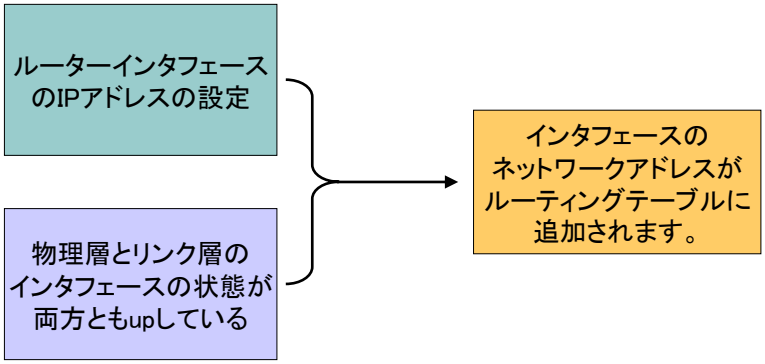
- ダイレクトルートとスタティックルートを設定する
- VLAN間ルーティングを設定する
- デフォルトルートとブラックホールルートを設定する
- スタティックルート間のロードシェアリングとルートバックアップを実装する



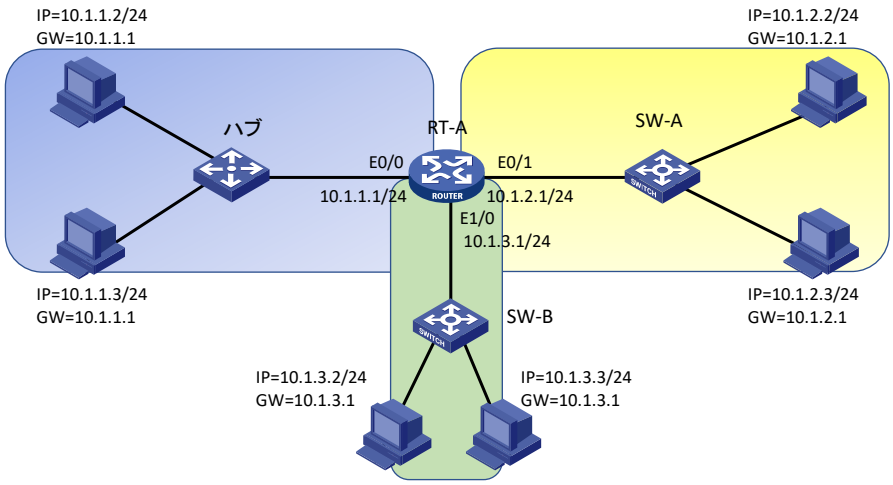
アジェンダ

- ダイレクトルート
- VLAN間のルート
- スタティックルート

ダイレクトルート生成



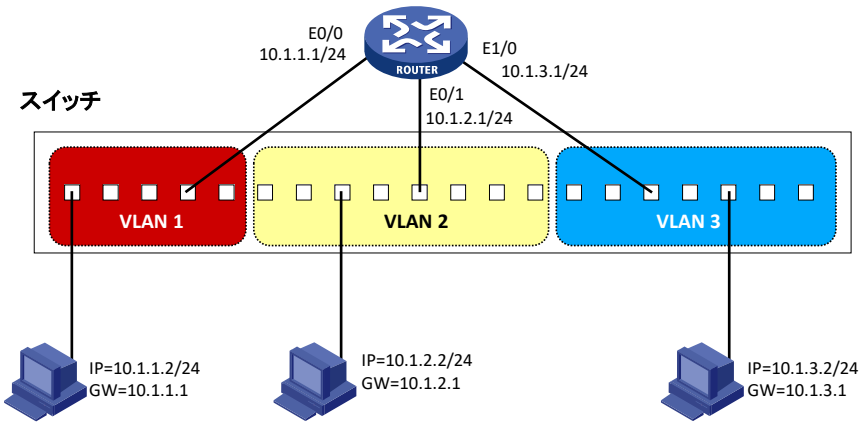
LAN間ルーティング



アジェンダ

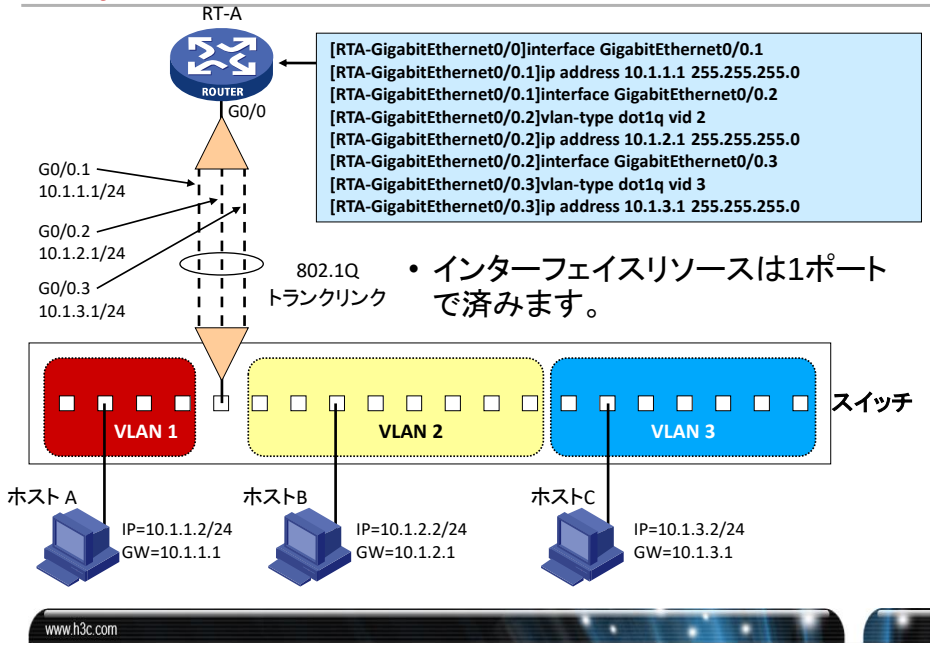
- ダイレクトルート
- VLAN間のルート
- スタティックルート

不適切なVLAN間ルーティング

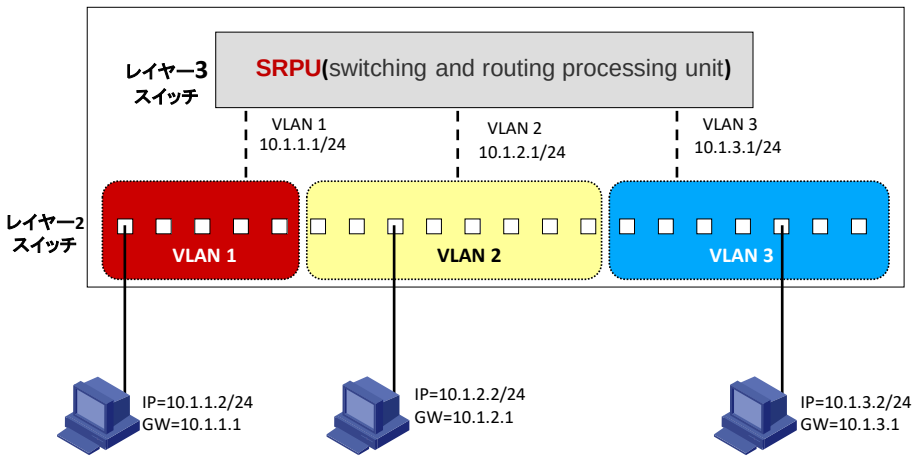


- ルータは物理リンクを介して各VLANに接続し、インターフェイスリソースを浪費します（3ポートも使ってしまいます）。

802.1Qおよびサブインターフェイスを使用したVLAN間ルーティング



レイヤー3スイッチを使用したVLAN間ルーティング



• レイヤー3スイッチは、組み込みルーティングエンジンを使用してVLAN間ルーティングを実装します。

アジェンダ

■ ダイレクトルート

■ VLAN間のルート

■ スタティックルート

スタティックルート設定

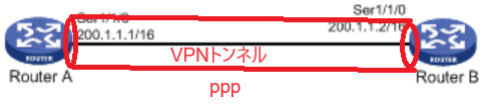
H3C

●スタティックルート設定コマンド

[Router]**ip route-static** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* } [***preference*** *preference-value*]

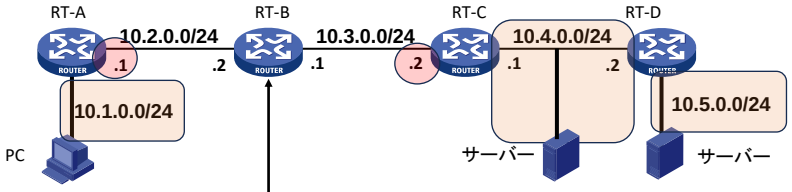
●キーポイント

→出力インターフェイスがポイントツーポイント(PPP)インターフェイスの場合は、interface-type interface-name引数だけを指定できます。それ以外の場合は、*next-hop-address*引数も指定する必要があります。



→宛先IPアドレスとマスクの両方が0.0.0.0の場合、設定されたルートはデフォルトルートになります。

スタティックルートの設定例



●RT-Bのルーティングテーブル

```
[RTB]ip route-static 10.1.0.0 255.255.255.0 10.2.0.1
[RTB]ip route-static 10.4.0.0 255.255.255.0 10.3.0.2
[RTB]ip route-static 10.5.0.0 255.255.255.0 10.3.0.2
```

●次の作業が必要です。

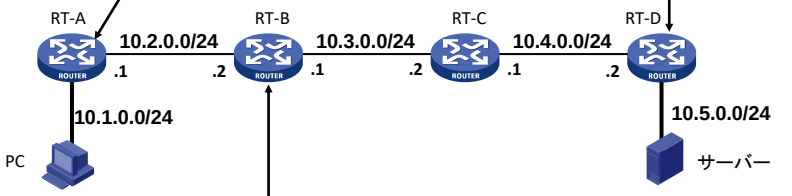
→各ルータ上のすべてのネットワークセグメントへのスタティックルートの設定

→ネクストホップが直接接続され、到達可能であることを確認します。

デフォルトルートの設定

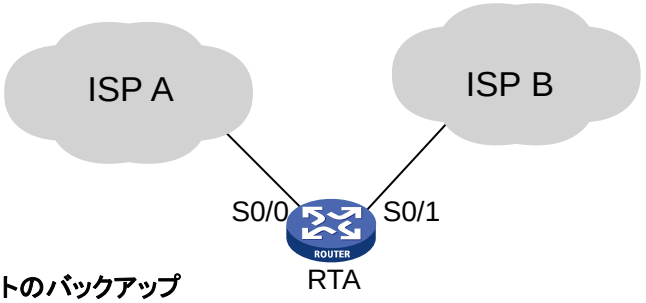
```
[RTA]ip route-static 0.0.0.0 0.0.0.0 10.2.0.2
```

```
[RTD]ip route-static 0.0.0.0 0.0.0.0 10.4.0.1
```




```
[RTB]ip route-static 10.1.0.0 255.255.255.0 10.2.0.1
[RTB]ip route-static 0.0.0.0 0.0.0.0 10.3.0.2
```

スタティックルート間のロードシェアリングとルートバックアップ



●ルートのバックアップ

→同じ宛先へのルートのネクストホップと優先度が異なる

→優先度が高いルートがプライマリルート、優先度が低いルートがバックアップルート

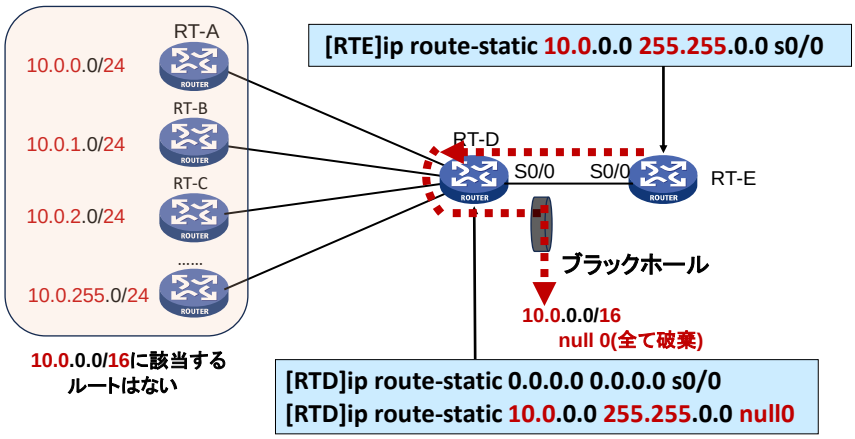
●ロードシェアリング

→同じ宛先へのルートが異なるネクストホップを持つが、優先度は同じ

→宛先へのルート間でトラフィックが共有される

ブラックホールルート

●ブラックホールルートを使用すると、ルーティングループを回避できます。



復習

- ダイレクトルートおよびVLAN間ルーティングの設定
- スタティックルートの設定
- デフォルトルートの設定
- スタティックルート間でのロードシェアリングとルートバックアップの実装
- ブラックホールルート

ダイレクトルートとスタティックルート

H3C

MSR では、... コマンドを実行して静的ルートを構成します。

- static-route
- ip static-route
- ip route-static
- route-static

ダイレクトルートとスタティックルート

お客様のネットワーク接続は次のとおりです。

HostA----GE0/0--MSR-1--S1/0-----WAN-----S1/0--MSR-2--GE0/0----HostB

どちらのルーターも工場出荷時のデフォルト構成です。ルータの4つのインターフェイスに正しいIPアドレスが設定され、2つのホストのHostAとHostBにIPアドレスとゲートウェイが正しく設定されています。すべての物理的な接続が正常であると仮定すると、正しい説明を選択しなさい。

HostAとHostBの間のインターワーキングを実現するには、各ルーターに少なくとも1つの静的ルートが必要です。

HostAとHostBの間のインターワーキングを実現するには、各ルーターで少なくとも2つの静的ルートを構成する必要があります。

ルータにルートが設定されておらず、HostAはmsr-2のインターフェイスS1/0のIPアドレスにpingを実行できます。

ルータにルートが設定されておらず、HostAはMSR-1のインターフェイスS1/0のIPアドレスにpingを実行できます。

ダイレクトルートとスタティックルート

ルータに静的ルートを設定します。宛先アドレスが192.168.1.0、マスクが20ビット、送信元インターフェイスがgigabitethernet0/0、送信元インターフェイスのIPアドレスが10.10.202.1であるとすると、次のコンフィグのどれが正しいですか。

ip route-static 192.168.1.0 255.255.240.0 GigabitEthernet0/0

ip route-static 192.168.1.0 255.255.248.0 10.10.202.1

ip route-static 192.168.1.0 255.255.240.0 10.10.202.1

ip route-static 192.168.1.0 255.255.248.0 GigabitEthernet0/0


H3C
ITOIP Solutions Expert

RIP基礎

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- ダイナミックルーティングプロトコルでは、他のルーターとの情報交換でルートを計算します。
- 最も初期のダイナミックルーティングプロトコルは、Routing Information Protocol(RIP)です。これは設定が容易です。

学習の目標

このレッスンを修了すると、次のことができるようになります：

- RIP機能の説明
- RIPがルートを作成および維持する方法
- ルーティングループを回避する方法の説明
- RIPv2がRIPv1より優れている理由の説明



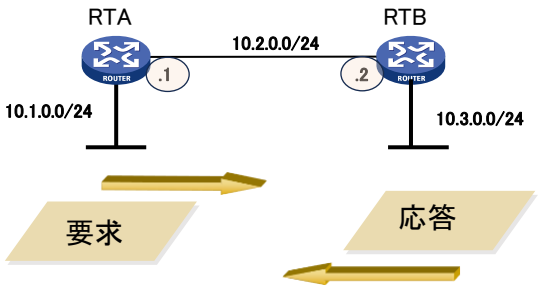
RIPの概要

- Routing Information Protocol(RIP)には、RIPv1とRIPv2の2つのバージョンがあります。
- RIPは目的地までに経由するルーターの数(Distance-Vectorアルゴリズム)に基づいて経路を決定します。
- RIPは、中小規模のネットワークに適しています。
- RIPは、スプリットホライズン、ポイズンリバース、およびトリガーされたアップデートをサポートし、ルーティングループを防止します。
- RIPはUDPデータグラムを使用して、ポート520を介して情報を交換します。

RIPルーティングテーブルの初期化

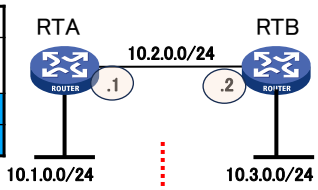
ルーティングテーブル		
送信先	ネクストホップ	メトリック
10.1.0.0	–	0
10.2.0.0	–	0

ルーティングテーブル		
送信先	ネクストホップ	メトリック
10.2.0.0	–	0
10.3.0.0	–	0



RIPルーティングテーブルの更新

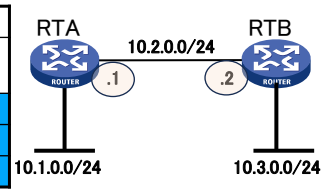
ルーティングテーブル		
送信先	ネクストホップ	メトリック
10.1.0.0	–	0
10.2.0.0	–	0



ルーティングテーブル		
送信先	ネクストホップ	メトリック
10.2.0.0	–	0
10.3.0.0	–	0

ルーティング情報を交換することで
ルーティングテーブルを更新する

ルーティングテーブル		
送信先	ネクストホップ	メトリック
10.1.0.0	–	0
10.2.0.0	–	0
10.3.0.0	10.2.0.2	1

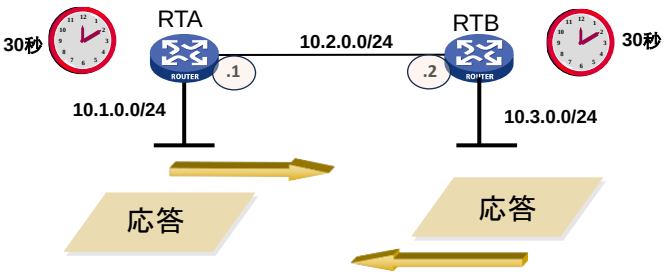


ルーティングテーブル		
送信先	ネクストホップ	メトリック
10.1.0.0	10.2.0.1	1
10.2.0.0	–	0
10.3.0.0	–	0

RIPルーティングテーブルを最新に保つ

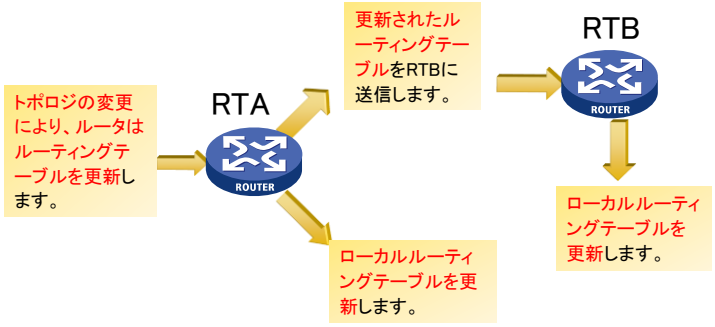
ルーティングテーブル		
送信先	ネクストホップ	メトリック
10.1.0.0	–	0
10.2.0.0	–	0
10.3.0.0	10.2.0.2	1

ルーティングテーブル		
送信先	ネクストホップ	メトリック
10.1.0.0	10.2.0.1	1
10.2.0.0	–	0
10.3.0.0	–	0

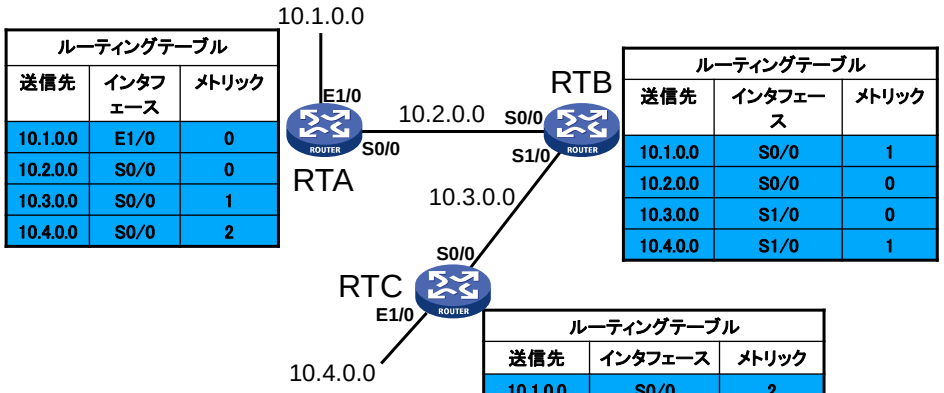


- 応答メッセージは定期的(デフォルトでは30秒間隔:1～3600秒設定可)に送信されます

ネットワーク内でのトポロジ変更の伝播



経路が1つのネットワークでのルーティングループ①



ルーティングテーブル

送信先	インタフェース	メトリック
10.1.0.0	E1/0	0
10.2.0.0	S0/0	0
10.3.0.0	S0/0	1
10.4.0.0	S0/0	2

ルーティングテーブル

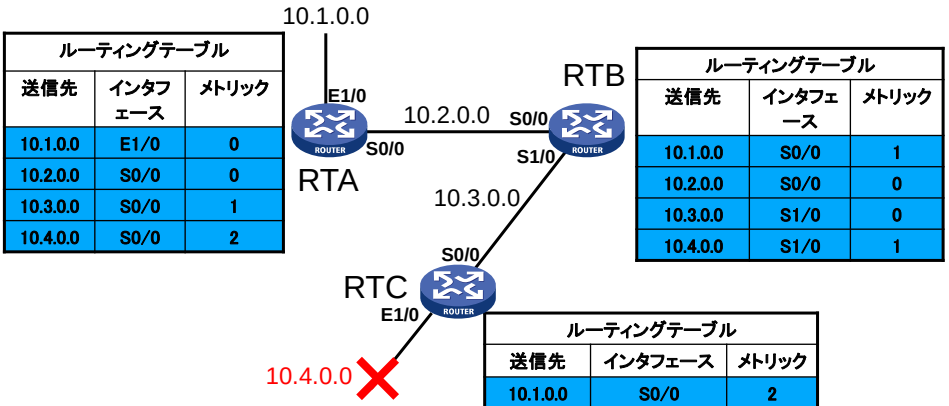
送信先	インタフェース	メトリック
10.1.0.0	S0/0	1
10.2.0.0	S0/0	0
10.3.0.0	S1/0	0
10.4.0.0	S1/0	1

ルーティングテーブル

送信先	インタフェース	メトリック
10.1.0.0	S0/0	2
10.2.0.0	S0/0	1
10.3.0.0	S0/0	0
10.4.0.0	E1/0	0

- ネットワークが安定し、ルーティングテーブルエントリが正しい状態である。

経路が1つのネットワークでのルーティングループ②



ルーティングテーブル

送信先	インタフェース	メトリック
10.1.0.0	E1/0	0
10.2.0.0	S0/0	0
10.3.0.0	S0/0	1
10.4.0.0	S0/0	2

ルーティングテーブル

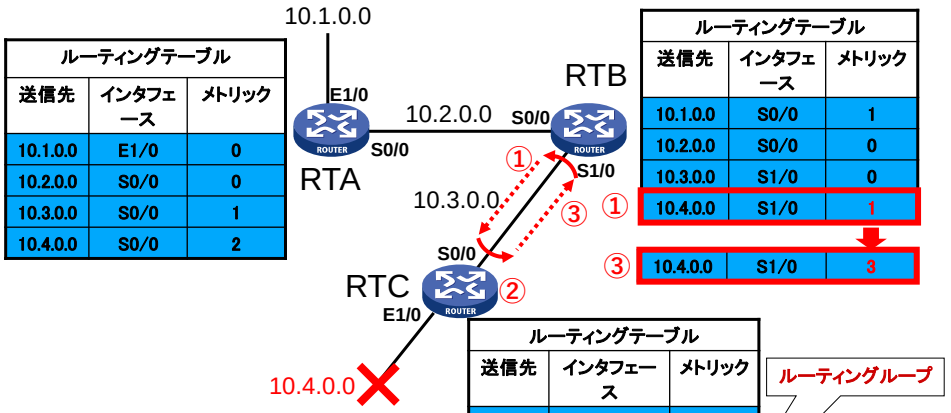
送信先	インタフェース	メトリック
10.1.0.0	S0/0	1
10.2.0.0	S0/0	0
10.3.0.0	S1/0	0
10.4.0.0	S1/0	1

ルーティングテーブル

送信先	インタフェース	メトリック
10.1.0.0	S0/0	2
10.2.0.0	S0/0	1
10.3.0.0	S0/0	0
10.4.0.0	E1/0	0

- 10.4.0.0のリンクがダウンし、関連するルートエントリを削除します。

経路が1つのネットワークでのルーティングループ③



ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	E1/0	0
10.2.0.0	S0/0	0
10.3.0.0	S0/0	1
10.4.0.0	S0/0	2

ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	S0/0	1
10.2.0.0	S0/0	0
10.3.0.0	S1/0	0
10.4.0.0	S1/0	1
10.4.0.0	S1/0	3

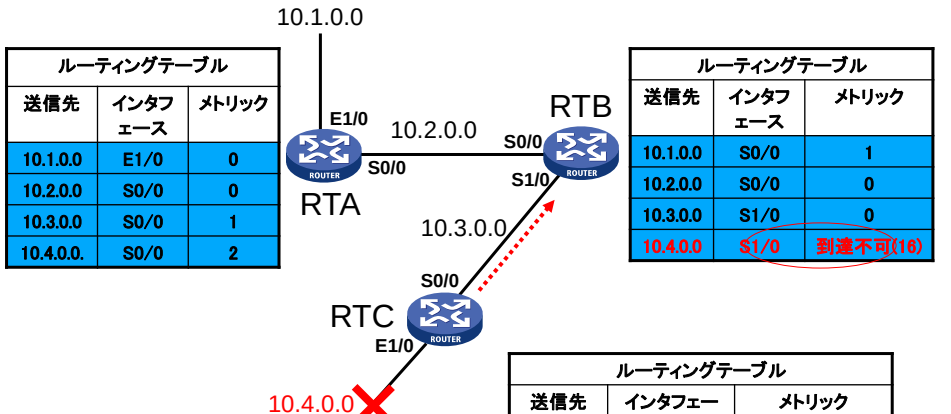
ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	S0/0	2
10.2.0.0	S0/0	1
10.3.0.0	S0/0	0
10.4.0.0	S0/0	2

ルーティングループ

RTBからの情報で10.4.0.0を追加

- RTBから10.4.0.0のルート情報がもたらされたのでルートを追加。この情報が正しくないためループが発生します。

ループ回避メカニズム - ルートポイズニング①



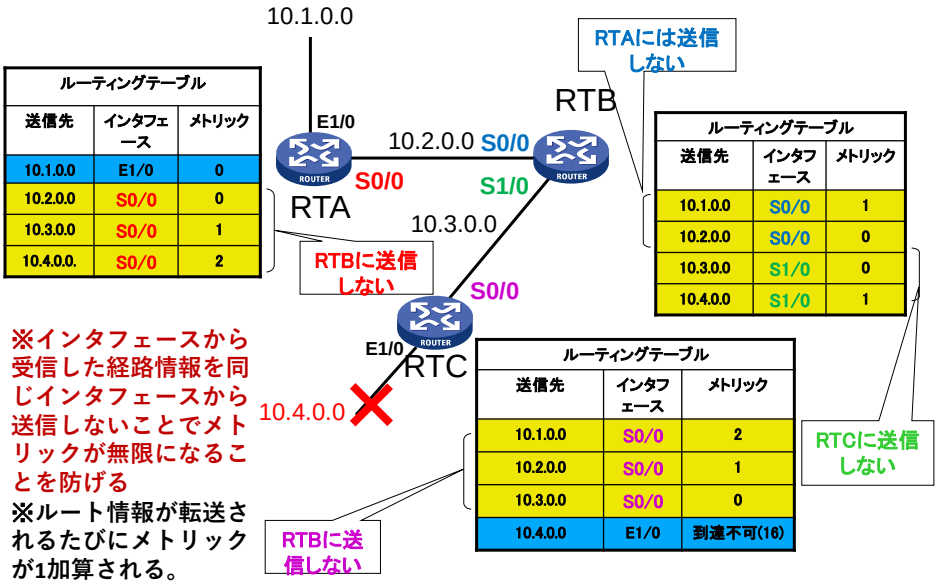
ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	E1/0	0
10.2.0.0	S0/0	0
10.3.0.0	S0/0	1
10.4.0.0.	S0/0	2

ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	S0/0	1
10.2.0.0	S0/0	0
10.3.0.0	S1/0	0
10.4.0.0	S1/0	到達不可(16)

ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	S0/0	2
10.2.0.0	S0/0	1
10.3.0.0	S0/0	0
10.4.0.0	E1/0	到達不可(16)

ルートポイズニングとはリンクダウンを明示的に通知するためにメトリックを16に設定する

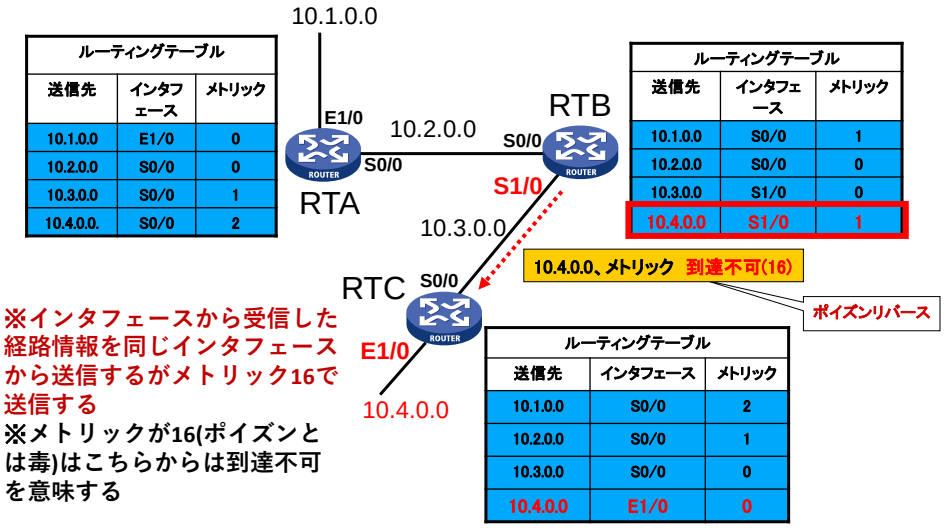
ループ回避メカニズム – スプリットホライズン②



※インタフェースから受信した経路情報を同じインタフェースから送信しないことでメトリックが無限になることを防げる

※ルート情報が転送されるたびにメトリックが1加算される。

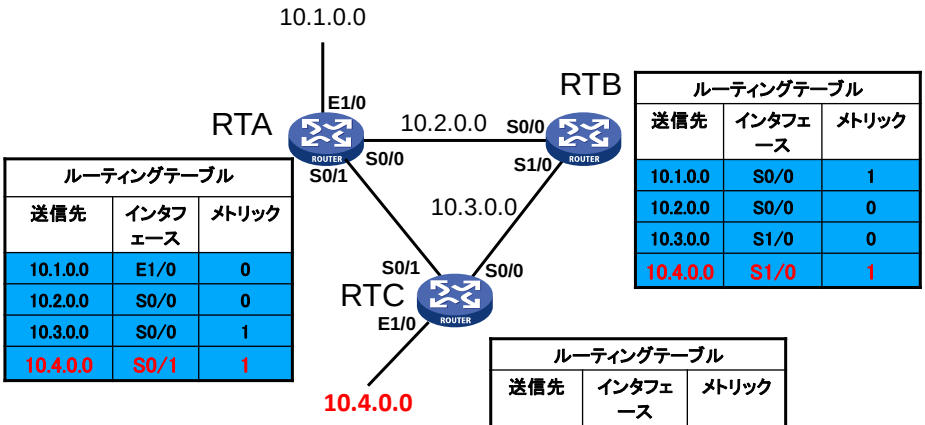
ループ回避メカニズム – ポイズンリバース(毒を返す)③



※インタフェースから受信した経路情報を同じインタフェースから送信するがメトリック16で送信する

※メトリックが16(ポイズンとは毒)はこちらからは到達不可を意味する

マルチパスネットワーク内のルーティングループ①



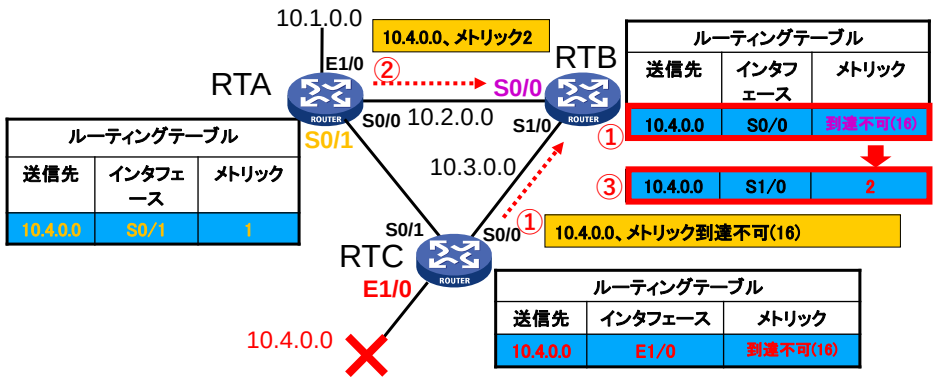
ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	E1/0	0
10.2.0.0	S0/0	0
10.3.0.0	S0/0	1
10.4.0.0	S0/1	1

ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	S0/0	1
10.2.0.0	S0/0	0
10.3.0.0	S1/0	0
10.4.0.0	S1/0	1

ルーティングテーブル		
送信先	インタフェース	メトリック
10.1.0.0	S0/1	1
10.2.0.0	S0/0	1
10.3.0.0	S0/0	0
10.4.0.0	E1/0	0

- ネットワークが収束され、ルーティングテーブルエントリが正しい。

マルチパスネットワークでのルーティングループ②



ルーティングテーブル		
送信先	インタフェース	メトリック
10.4.0.0	S0/1	1

ルーティングテーブル		
送信先	インタフェース	メトリック
10.4.0.0	S0/0	到達不可(16)
10.4.0.0	S1/0	2

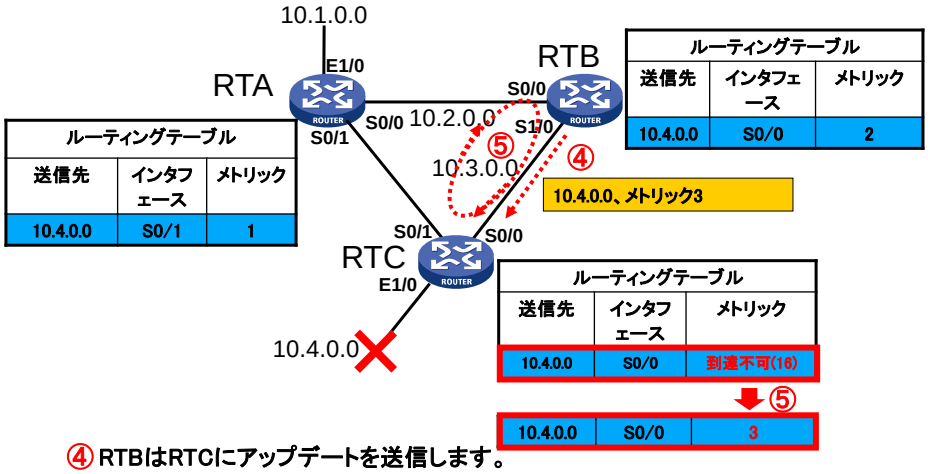
ルーティングテーブル		
送信先	インタフェース	メトリック
10.4.0.0	E1/0	到達不可(16)

① ネットワーク10.4.0.0に障害が発生すると、RTCはエントリ10.4.0.0のメトリックを無限大(16)に設定し、ルーティングアップデートを送信します。

② RTAはRTBにアップデートを送信します。

③ RTBはルーティングテーブルのエントリ10.4.0.0をアップデートします。

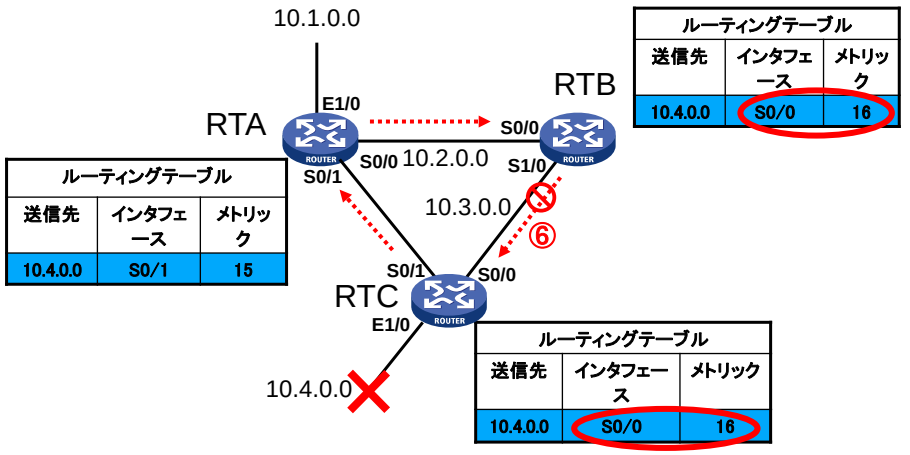
マルチパスネットワークのルーティングループ③



④ RTBはRTCにアップデートを送信します。

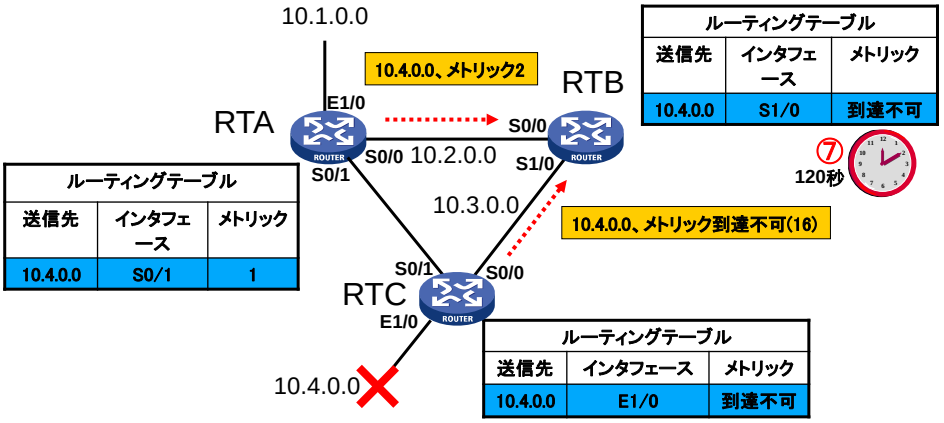
⑤ RTCはルーティングテーブルのエントリ10.4.0.0をアップデートします。このため、ルーティングループが発生します。

ループ回避メカニズム – 最大メトリックの定義④



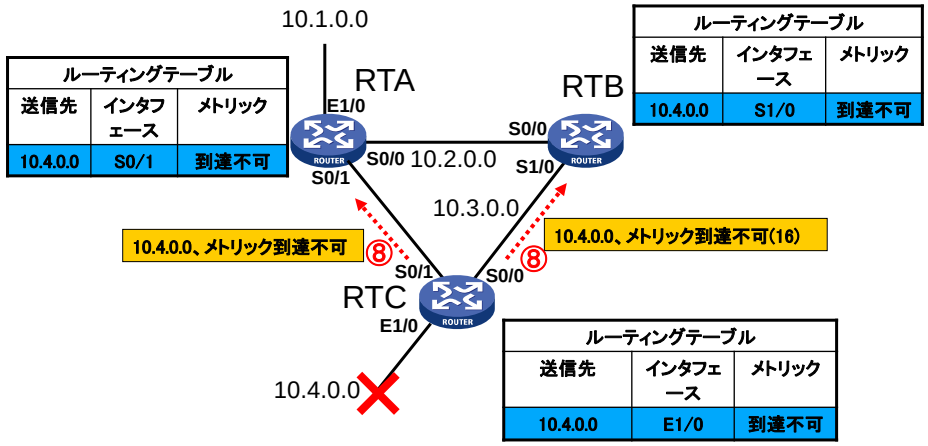
⑥ エントリの最大有効メトリックに到達すると、ルータは10.4.0.0宛てのパケットの転送を停止します。

ループ回避メカニズム– 抑制タイマ⑤



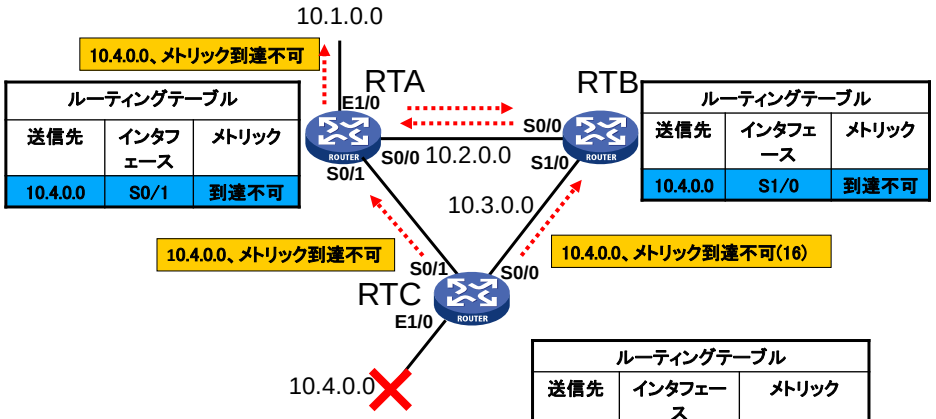
⑦ RTBでは、エントリ10.4.0.0の更新が中断状態に入ります。
RTBはRTCからのメトリックが16未満のみを受け入れます

ループ回避メカニズムによってトリガーされる更新⑥



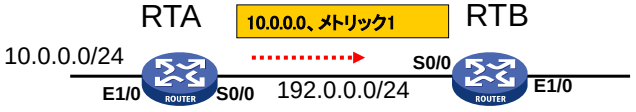
⑧RTCは、アップデートタイマーが期限切れになった後ではなく、すぐに
ルート10.4.0.0の到達不能に関するアップデートを送信します。

マルチパスネットワークでループを回避する例



- **ルートポイズニング**
- **タイマーによる更新の中断**
- **トリガーされた更新**

RIPv1の短所



ルーティングテーブル

宛先ネットワーク/マスク	インタフェース	メトリック
10.0.0.0/8	S0/0	1

- **RIPv1プロトコルメッセージはサブネットマスク情報を伝達しません。これにより、サブネットアドレス指定でエラーが発生する可能性があります。**
- **その他**
  - → RIPv1は認証をサポートしていません。
  - → RIPv1は、ブロードキャストによるメッセージアドバタイズメントだけをサポートします。

RIPv2で導入された改善点

- **RIPv2はクラスレス(IPアドレスにサブネットマスク情報を含める)ルーティングプロトコルです。**
- **RIPv2プロトコルメッセージはマスク情報を伝送し、Variable-Length Subnet Mask(VLSM)およびClassless Inter-Domain Routing(CIDR)をサポートします。**
  - → VLSM（サブネットマスクを変更可能）
  - → CIDR（可変長サブネットマスキング（VLSM）を使用して、IP アドレスのネットワークアドレスビットとホストアドレスビットの比率を変更します。）
- **RIPv2では、マルチキャストアドレス224.0.0.9を定期的な更新に使用して、リソースの消費を削減します。**
- **RIPv2では、セキュリティを強化するために、プロトコルメッセージのプレーンテキスト認証とMD5認証がサポートされています。**

RIPの基本設定

- RIPプロセスをイネーブルにし、RIPビューに入ります。

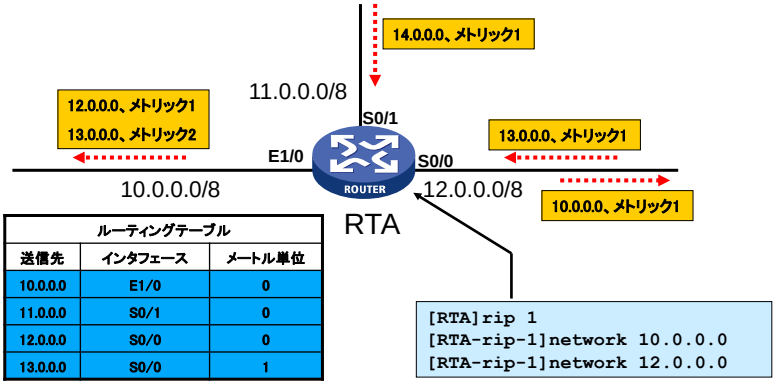
[Router] rip [*process-id*]

- 指定したネットワークに接続されているインターフェイスでRIPをイネーブルにします。

[Router] rip 1
[Router-rip-1] network *network-address* [*wildcard-mask*]

networkコマンドの意味

- networkコマンドには2つの意味があります。
  - RIPルーティングテーブルに追加するインターフェイスルートを指定します。
  - RIPパケットを送受信できるインターフェイスを指定します。



ルーティングテーブル

送信先	インタフェース	メートル単位
10.0.0.0	E1/0	0
11.0.0.0	S0/1	0
12.0.0.0	S0/0	0
13.0.0.0	S0/0	1

オプションのRIP設定

- インターフェイスによるRIPパケットの送信をディセーブルにします。

[Router] rip 1
[Router-rip-1] silent-interface { **all** | *interface-type interface-number* }

- スプリットホライズンの有効化:

[Router] interface Ethernet1/0
[Router-Ethernet1/0] rip split-horizon

- ポイズンリバースを有効にする:

[Router] interface Ethernet1/0
[Router-Ethernet1/0] rip poison-reverse

オプションのRIP設定

- グローバルRIPバージョンを指定します。

```
[Router] rip 1
[Router-rip-1] version { 1 | 2 }
```

- RIPv2のルート自動サマライズをディセーブルにします。

```
[Router-rip-1] undo summary
```

宛先ネットワークが多いとルーティングテーブルのサイズが大きくなりすぎるので自動的に共通にできるネットワークアドレスまでサブネットマスクを調整してエントリーを削減する手法をサマライズと呼びます。

- RIPv2認証モードとパラメータを設定します。

```
[Router-Ethernet1/0] rip authentication-mode { md5
{ rfc2082 { cipher cipher-string | plain plain-string } key-
id | rfc2453 { cipher cipher-string | plain plain-string } } |
simple { cipher cipher-string | plain plain-string } }
```


オプションのRIP設定

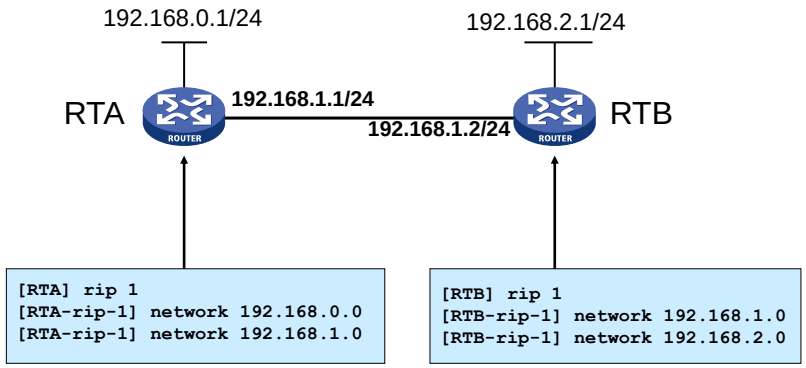
- RIPのタイマー値を指定します。

```
[Router] timers { garbage-collect garbage-collect-value
| suppress suppress-value | timeout timeout-value |
update update-value }
```

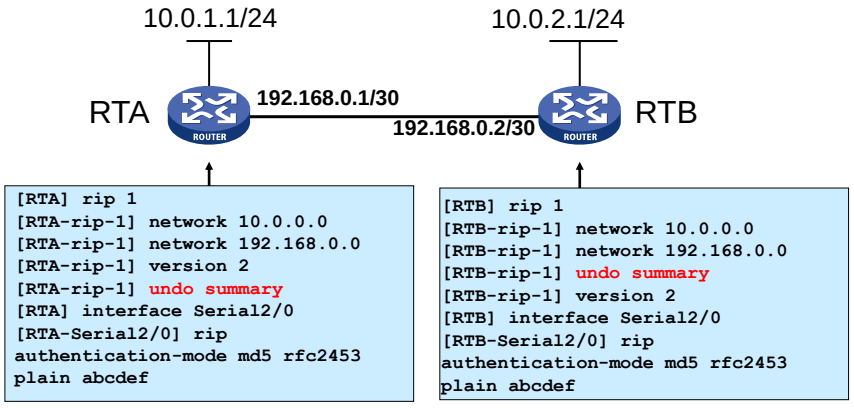
パラメータ:
garbage-collect-value:ガベージ コレクト タイマーを1 ～ 3600 秒の範囲で指定。
suppress-value:抑制タイマーを0～3600秒の範囲で指定。
timeout-value:タイムアウトタイマーを1～3600秒の範囲で指定。
update-value:更新タイマーを 1 ～ 3600 秒の範囲で指定。

デフォルト値:
ガベージ コレクション タイマーは 120 秒。
抑制タイマーは 120 秒。
タイムアウトタイマーは180秒。
アップデートタイマーは30秒。

基本的なRIPの設定例



RIPv2の設定例



※summaryはデフォルトで有効ですが、大規模でネットワークセグメントが連続している場合には効果がありますが、不連続の場合は処理の負荷がかかりますので、無効(undo summary)にします。

復習

- RIPはディスタンスベクトルルーティングプロトコルです。
- RIPはルーティング情報をホップバイホップ(通過するルーター毎)に更新します。
- RIPルーティングループの原因
- RIPは、スプリットホライズン、ルートポイズニング、およびその他のメカニズムを使用して、ルーティングループを回避します。
- RIPv2はVLSMをサポートします。

インタフェースでルートを学習した後、RIPはルートのメトリックを無限大(16)に設定し、インタフェースを介してルートを隣接ルートへ送り返す。この方式を何と呼びますか？

- スプリットホライズン
- トリガーされた更新
- ルートポイズニング
- ポイズンリバース

OSPFの基礎

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- RIPは、その特性上、主に中小規模のネットワークで使用されています。
- RIPは、急速に拡大するネットワークの要件を満たすことができません。
- OSPFは、RIPの多くの問題を解決し、普及しています。

学習の目標

このレッスンを修了すると、次のことができるようになります:

- OSPFの基本概念を理解する
- OSPFエリアの設定
- OSPFの問題をトラブルシュートする

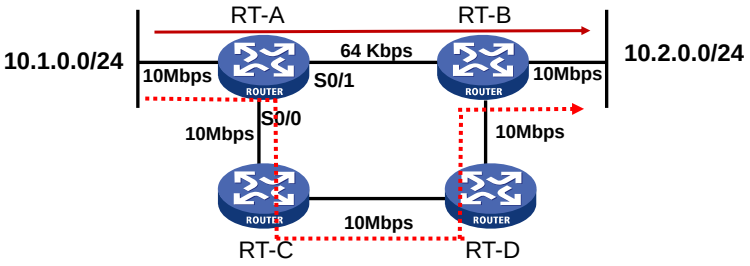


アジェンダ

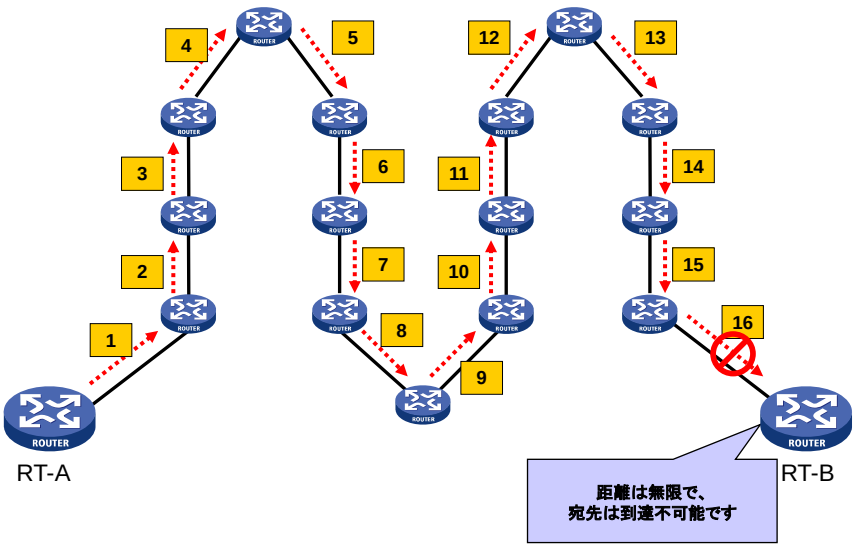
- RIPの短所
- OSPFの基本
- OSPFの設定
- OSPFの表示とデバッグ

ルートはホップカウントで計算されると最適でない場合がある

RT-Aルーティングテーブル		
宛先	インターフェース	メトリック
10.2.0.0	S0/1	1

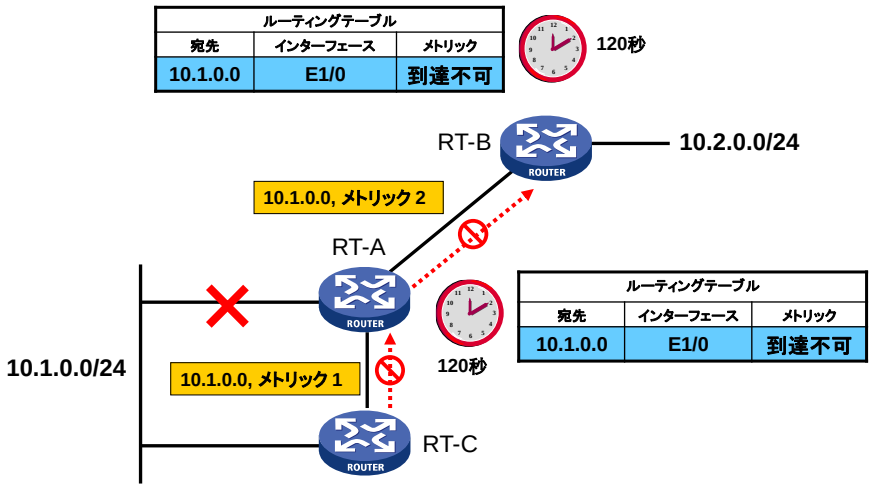


ホップ数制限による小規模ネットワーク



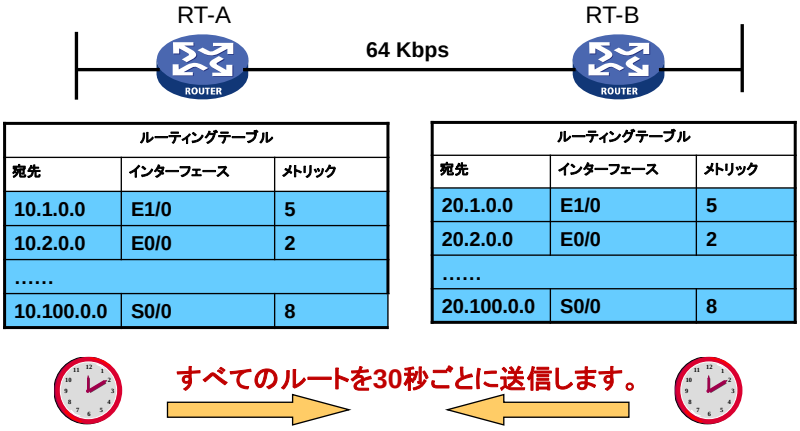
- RIPのネットワークホップは16ホップを超えることはできません。

ネットワークに障害が発生した場合、収束が遅い



- RT-AとRT-Bは到達不可ルート(16)の更新中断タイマーを設定します。
- 中断時間内に、RT-AとRT-Bは、ルートのルーティングアップデートを受信しても、ルートをアップデートしません。

すべてのルートをアップデートすると、ネットワークリソースが浪費される



- RT-AとRT-Bがそれぞれ1000のルートを持ち、各RIPルートエントリがRIPメッセージの20バイトを占有するとします。RT-AとRT-B間の一方向のルーティングアップデートプロセスでは、160KBの帯域幅が使用されます。

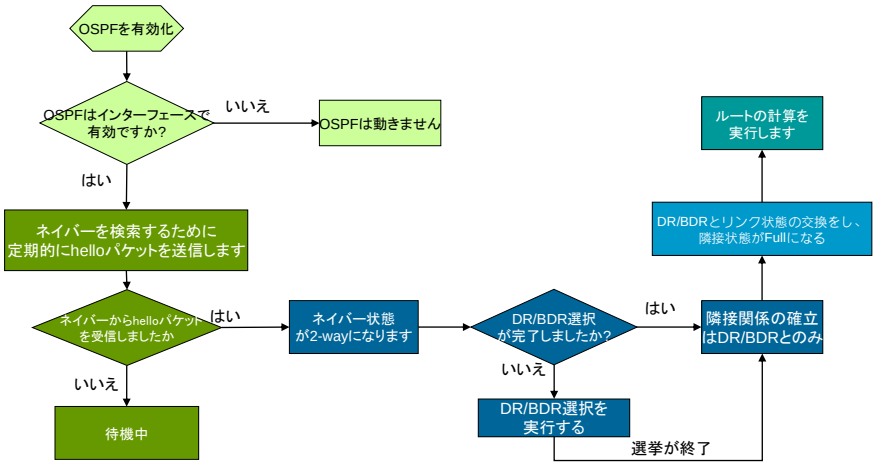
アジェンダ

- RIPの短所
- OSPFの基本
- OSPFの設定
- OSPFの表示とデバッグ

OSPFとは

- Open Shortest Path First(OSPF)は、Internet Engineering Task Force(IETF)によって開発されたリンクステート内部ゲートウェイプロトコル(経由ルーターの数ではなく、到達時間で判断)です。
- OSPFルータは、ネットワークコンバージェンスを高速化し、ネットワークリソースの浪費を回避するために、隣接ルーターから要求されたルート情報だけを隣接ルーターに送信します。
- OSPFパケットは直接IPパケットにカプセル化されます。OSPFのIPプロトコル番号は89です。
- OSPFはマルチキャストアドレスでパケットを送信できます。

OSPFの動作

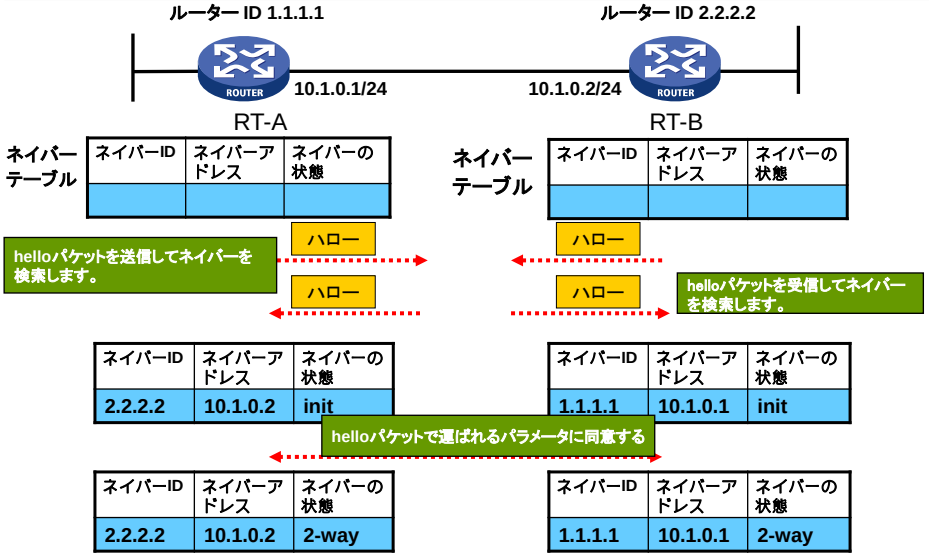


- OSPFには、次の4つの主要な操作手順があります。

  ネイバーの検出、隣接関係の確立、リンクステート情報の交換、ルート計算の実行

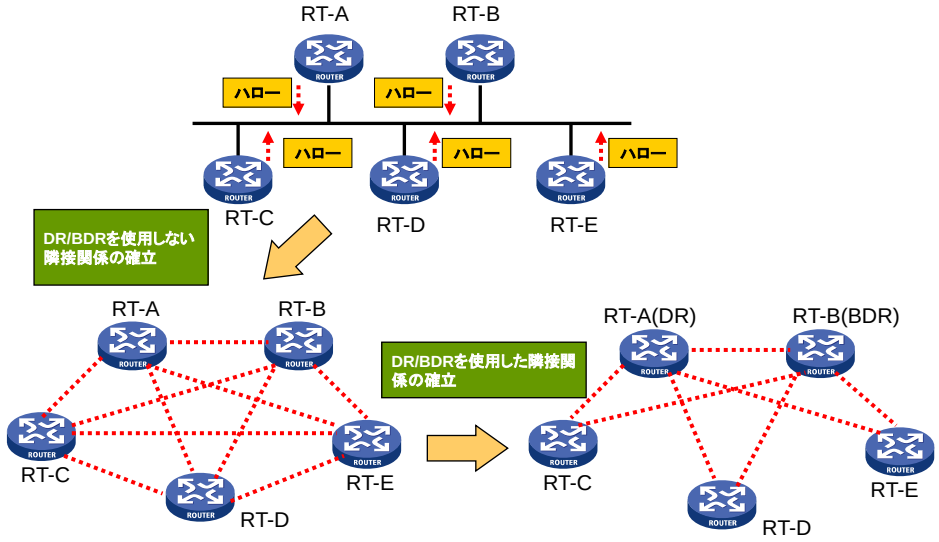
※DR (Designated Router) 代表ルータと、BDR (Backup Designated Router) バックアップ代表ルータ

ネイバーの検出

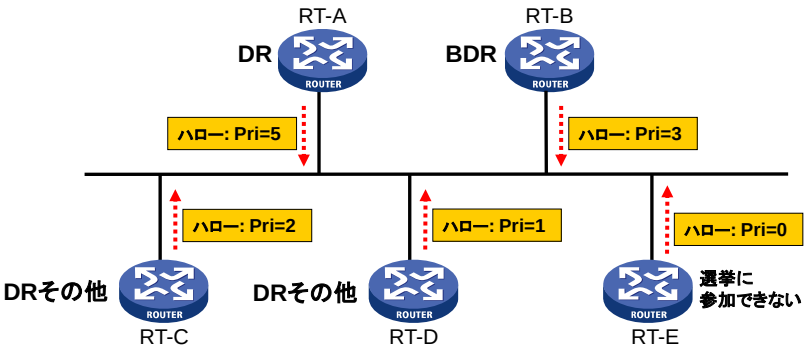


- ネイバー状態が2-wayになると、RT-AとRT-Bは隣接関係の確立を開始します。

隣接関係の確立

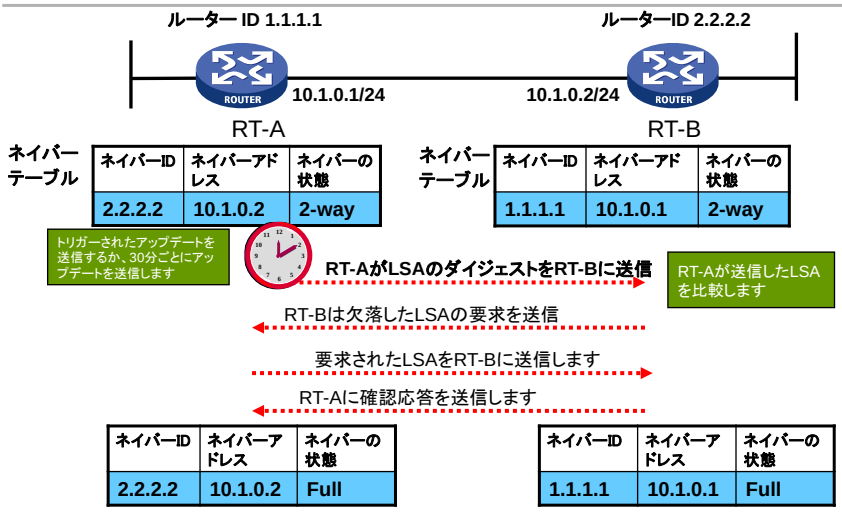


DR と BDR の選挙



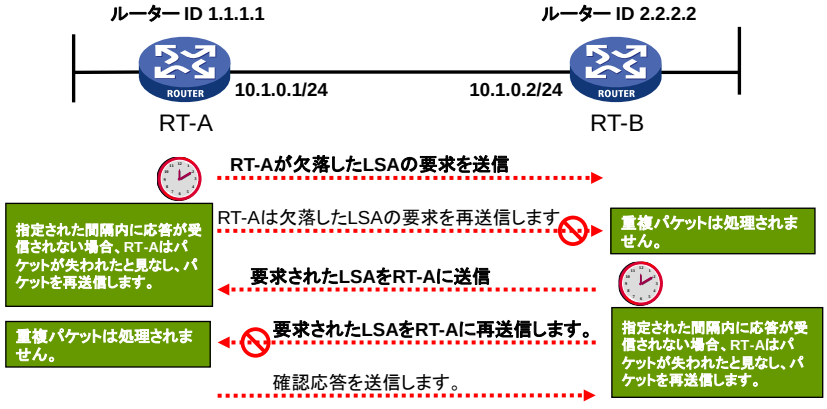
- helloパケットは、アドバタイジングルータのプライオリティを伝送します。プライオリティが0のルータは選出に適格ではありません。
- 最初にBDRが選出され、次にDRが選出されます。
- DRとBDRが選出されると、プライオリティの高いルータがエリアに追加されても、DRとBDRが無効にならない限り、選出は実行されません。

ルート情報交換①



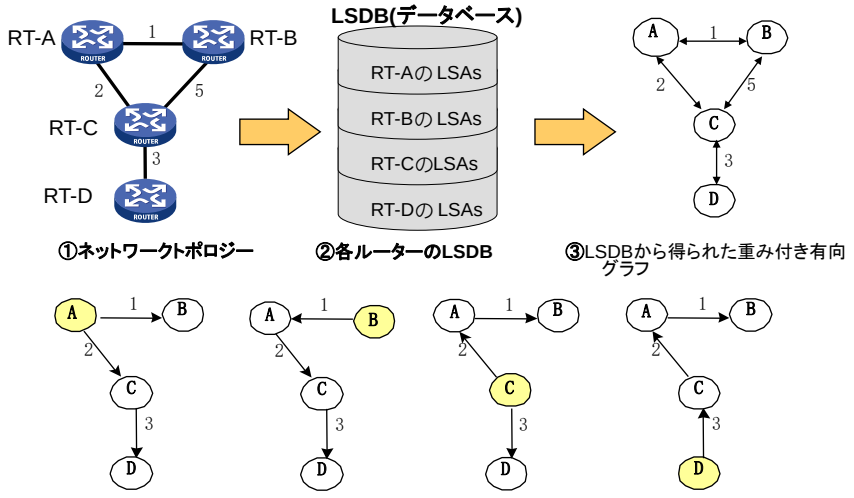
- RTAは同様に、RTBから欠落しているLSA(ルート情報)を取得します。
- RTBがLSAをRTAと同期させると、RTBのネイバーテーブル内のRTAのネイバー状態がフルになります。

ルート情報交換②



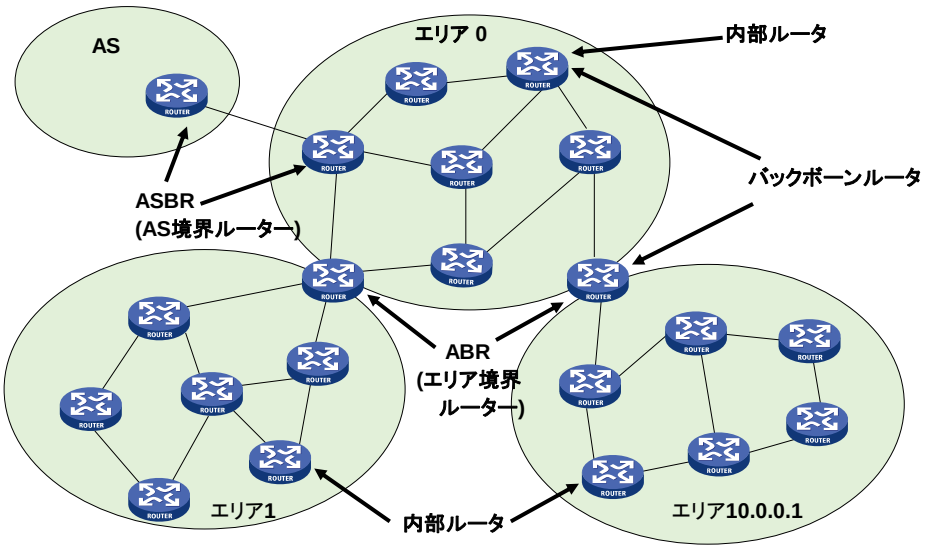
- OSPFはパケット再送信メカニズムを提供します。
- 各OSPFパケットにはシーケンス番号があるため、重複パケットは処理されません。
- LSAはマスク情報を伝送し、VLSMをサポートします。

ルート計算



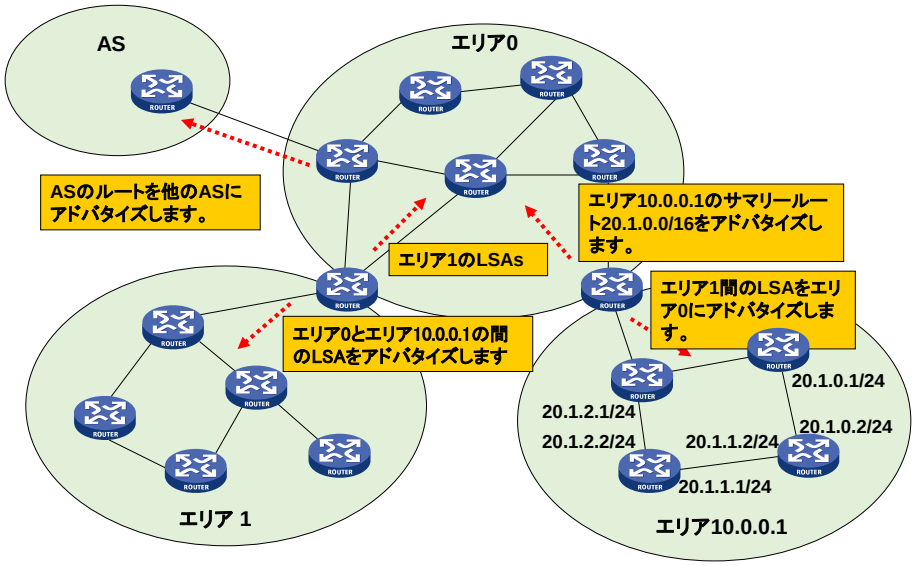
④各ルータは、自身をルートノードとしてSPTを計算します

エリアベースのOSPFネットワークパーティション



※ASとはAutonomous Systemの略でASはISPである場合が多い

LSAアドバタイズ



アジェンダ

- RIPの短所
- OSPFの基本
- OSPFの設定
- OSPFの表示とデバッグ

基本的なOSPFコンフィギュレーションコマンド

- ルータIDを設定する

[Router]router id *router-id*

- OSPFプロセスを有効にする

[Router]ospf [*process-id*]

- OSPFプロセスをリセットする

<Router>reset ospf [*process-id*] **process**

- OSPFエリアを作成する

[Router-ospf-100]area *area-id*

- エリア内の指定されたネットワークに接続されたインターフェイス上でOSPFを有効にする

[Router-ospf-1-area-0.0.0.0] network *ip-address wildcard-mask*

オプションのOSPFコンフィギュレーションコマンド

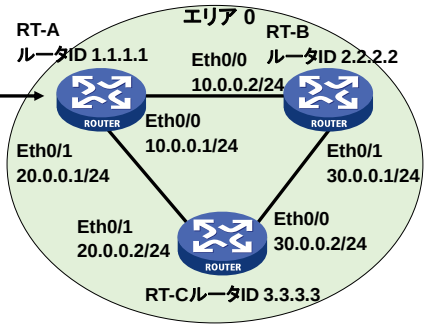
- インターフェイスのDRプライオリティを設定する

[Router] interface Ethernet0/0
[Router-Ethernet0/0] ospf dr-priority *priority*

- インターフェイスのOSPFコストを設定する

[Router-Ethernet0/0] ospf cost *value*

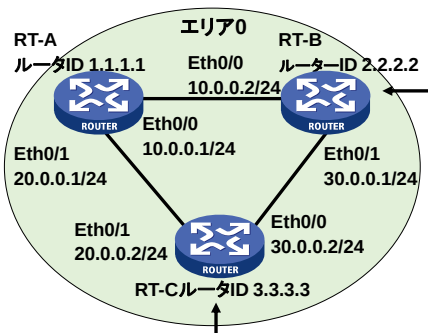
OSPFシングルエリアコンフィギュレーションの例① (A)



※ルーターIDはトポロジーを保つために重要なIDなので、ルーターIDが依存するインタフェースは物理的なインターフェイスの状態に依存することなく、ルーターが正常に稼働している限りダウンしないことが条件となる。そのためにデバイス上に仮想的にLoopback Interfaceというものが作成された。

```
[RTA] interface loopback 0
[RTA-loopback-0]ip address 1.1.1.1 255.255.255.255
[RTA-loopback-0]quit
[RTA] router id 1.1.1.1
[RTA] ospf 1
[RTA-ospf-1] area 0
[RTA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0] network 20.0.0.0 0.0.0.255
```


OSPFシングルエリアコンフィギュレーションの例① (B)




```
[RTB]interface loopback 0
[RTB-loopback-0]ip address 2.2.2.2
255.255.255.255
[RTB-loopback-0]quit
[RTB]route id 2.2.2.2
[RTB]ospf 1
[RTB-ospf-1]area 0
[RTB-ospf-1-area-0.0.0.0]network
2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network
10.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]network
30.0.0.0 0.0.0.255
```

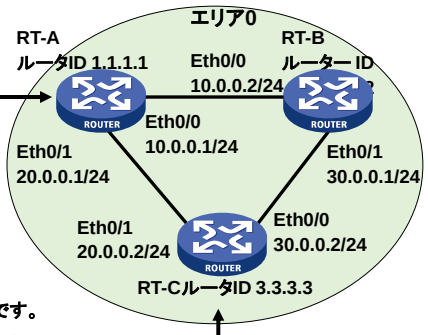
```
[RTC]interface loopback 0
[RTC-loopback-0]ip address 3.3.3.3 255.255.255.255
[RTC-loopback-0]quit
[RTC]router id 3.3.3.3
[RTC]ospf 1
[RTC-ospf-1]area 0
[RTC-ospf-1-area-0.0.0.0]network 3.3.3.3 0.0.0.0
[RTC-ospf-1-area-0.0.0.0]network 20.0.0.0
0.0.0.255
[RTC-ospf-1-area-0.0.0.0]network 30.0.0.0
0.0.0.255
```

- **RT-A上のEth0/0およびRT-B上のEth0/0はネイバーです。**
- **RT-A上のEth0/1およびRT-C上のEth0/1はネイバーです。**
- **RT-B上のEth0/1およびRT-C上のEth0/0はネイバーです。**
- RT-A、RT-B、およびRT-Cには、互いに到達する最短パスがあります

OSPFシングルエリアコンフィギュレーションの例②

- ルータインターフェイスのプライオリティとコストを変更します

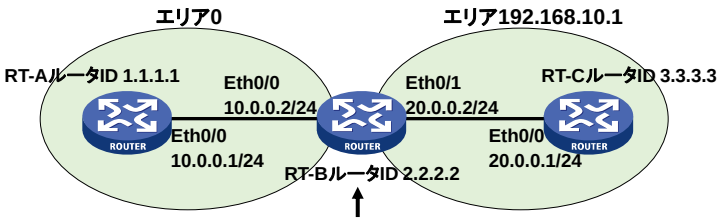
```
[RTA] interface ethernet0/0
[RTA-ethernet-0/0] ospf dr-priority 0
[RTA-ethernet-0/0] ospf cost 50
[RTA-ethernet-0/0] quit
[RTA] interface ethernet0/1
[RTA-ethernet-0/1] ospf dr-priority 0
[RTA-ethernet-0/1] ospf cost 10
```



- RT-A上のEth0/0およびRT-B上のEth0/0はネイバーです。
- RT-A上のEth0/1およびRT-C上のEth0/1はネイバーです。
- RT-B上のEth0/1およびRT-C上のEth0/0はネイバーです。
- RT-Cのルーティングテーブルが変更されます。

```
[RTC] interface ethernet0/0
[RTC-ethernet-0/0] ospf cost 100
[RTC-ethernet-0/0] quit
[RTC] interface ethernet0/1
[RTC-ethernet-0/1] ospf cost 10
```


OSPFマルチエリアコンフィギュレーションの例②



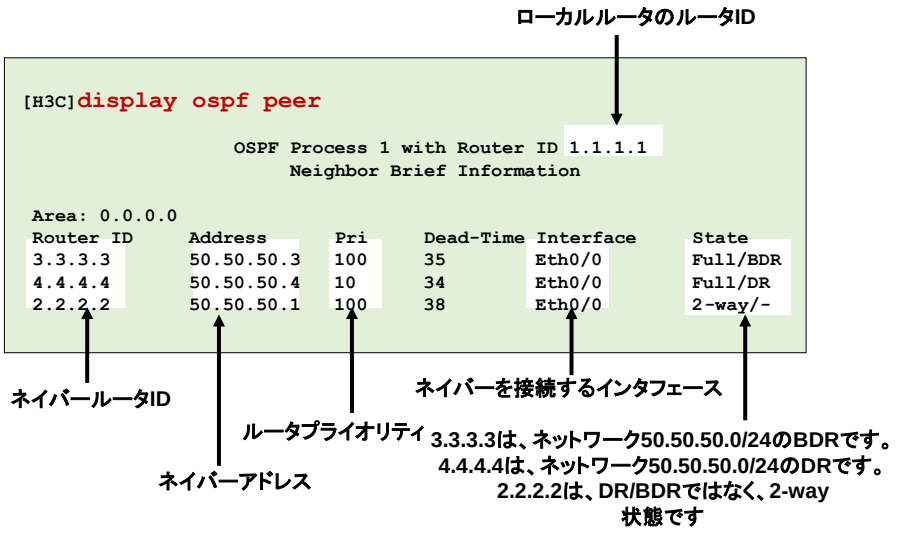

```
[RTB] interface loopback 0
[RTB-loopback-0] ip address 2.2.2.2 255.255.255.255
[RTB-loopback-0] quit
[RTB] route id 2.2.2.2
[RTB] ospf 100
[RTB-ospf-100] area 0
[RTB-ospf-100-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[RTB-ospf-100-area-0.0.0.0] network 10.0.0.0 0.0.0.255
[RTB-ospf-100-area-0.0.0.0] quit
[RTB-ospf-100] area 192.168.10.1
[RTB-ospf-100-area-192.168.10.1] network 20.0.0.0 0.0.0.255
```

- RT-AおよびRT-Cの設定は、OSPFシングルエリアの設定例と同じです。
- RT-Bは2つのエリアに追加する必要があります。RT-AとRT-Cは互いに到達可能です

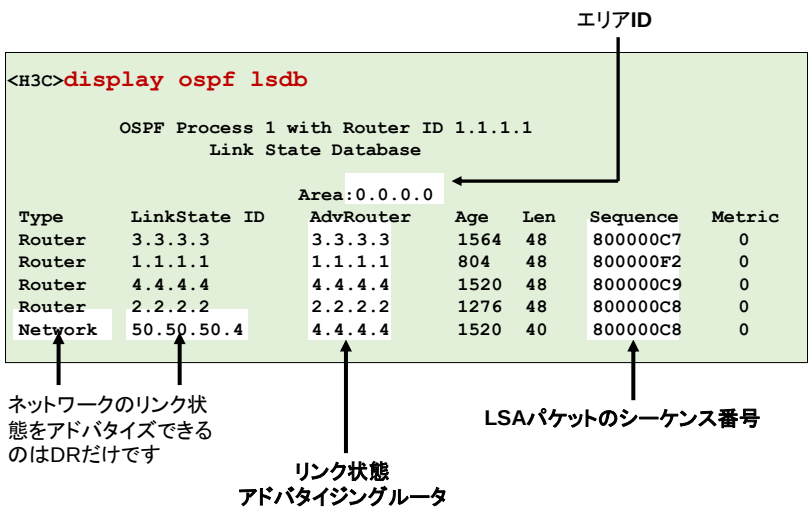
アジェンダ

- RIPの短所
- OSPFの基本
- OSPFの設定
- OSPFの表示とデバッグ

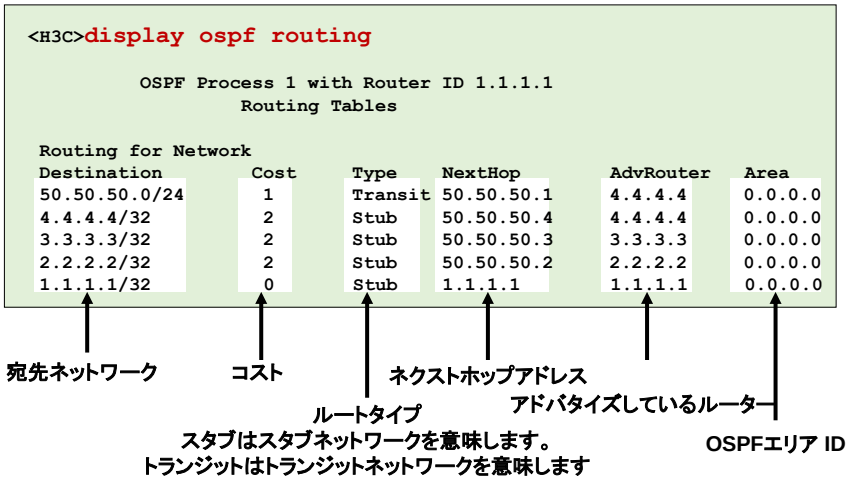
OSPFネイバーに関する情報の表示



LSDB情報の表示



OSPFルーティング情報の表示



その他のOSPF情報の表示

- OSPF情報の表示

[Router] display ospf [*process-id* **] [verbose]**

- OSPFインターフェイス情報を表示します

[Router] display ospf [*process-id* **] interface**
[*interface-type interface-number* **| verbose]**

OSPFのデバッグ

- OSPFイベントのデバッグを有効にします。

<Router> debugging ospf event
<Router> Terminal debugging ※コンソールにデバッグログを表示

- OSPF LSAのデバッグを有効にします。

<Router> debugging ospf lsa

- OSPFパケットのデバッグを有効にします。

<Router> debugging ospf packet

- OSPF SPFデバッグを有効にします。

<Router> debugging ospf spf

- OSPFプロセスデバッグを有効にします。

<Router> debugging ospf *process-id*

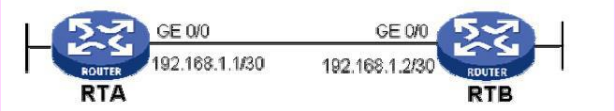
- デバッグをやめる

<Router> undo debugging all

復習

- OSPFはリンク状態ルーティングプロトコルです。SPFアルゴリズムを使用してルート計算を実行し、ルーティングループを回避します。
- OSPFはDR/BDR選定を導入して隣接の数を減らします。リンク状態情報の同期はDR/BDRによって管理されます。
- OSPFはエリアベースのOSPFネットワークパーティションを介して動作を最適化します。
- OSPFは、高速ネットワークコンバージェンスと信頼性の高い情報配信を特徴とし、ネットワークリソースを節約し、VLSMをサポートするため、適切な計画によって中小規模のネットワークや大規模なネットワークにも適用可能です。

設定がされていない2つのMSRルータは、図に示す方法で接続されています。IPアドレスを設定することにより、2つのルータのge0/0インターフェイスは相互に通信できます。



現在、次の設定が2つのルータに追加されています。
RTA:
[RTA]ospf 1
[RTA-ospf-1]area 0
[RTA-ospf-1-area-0.0.0.0]network 192.168.1.1 0.0.0.3
[RTA]interface GigabitEthernet0/0
[RTA-GigabitEthernet0/0]ospf dr-priority 2
RTB:
[RTB]ospf 1
[RTB-ospf-1] ares 0
[RTB-ospf-1-area-0.0.0.0]network192.168.1.1 0.0.0.3
[RTB]interface GigabitEthernet0/0
[RTB-gigabitethernet0/0]ospf dr priority

現在はOSPFネイバーが安定した状態になっています。次のうち正しい説明はどれでしょうか？

OSPF基礎

OSPFインターフェイスのプライオリティは同じであり、192.168.1.0/30ネットワークセグメントではOSPF DRの選択は行われません

2つのルータのうち、1つはDRであり、もう1つはBDRです

2つのルータのうち、1つはDRで、もう1つはDRotherです

2つのルータのネイバー状態は、それぞれfullと2-wayです

OSPF基礎

ネットワーク内のOSPFエリアに関する次の説明で正しいものを選びなさい

ネットワーク内のルータはいくつかの異なる領域に属している可能性がありますが、それらの1つがバックボーンエリアである必要があります。

ネットワーク内のルータは複数の異なるリージョンに属している場合がありますが、これらのエリアはバックボーンではない場合があります。

同じエリア内のOSPFルーターのみがネイバーと隣接関係を確立できます

同じ内の複数のOSPFエリアのルータは同じLSDBを共有し、各エリアのルータは同じLSDBを維持します。

OSPF情報表示およびデバッグコマンドに関する正しいステートメントはどれですか。

ルータのOSPFネイバー関係はdisplay OSPF peerコマンドを使用して表示できます

display OSPF LSDBコマンドを使用すると、ルータのリンクステートデータベースを表示できます。ネットワーク内のすべてのOSPFルータのデータベースは同じである必要があります。

display OSPF routingコマンドを使用すると、ルータのOSPFルーティングを表示できます。すべてのOSPFルートがグローバルルーティングテーブルに追加されるわけではありません

display OSPF faultを使用してOSPFエラー情報を表示します。



ACLベースのパケットフィルタリング

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- ネットワークセキュリティを強化するには、ネットワークデバイスがネットワークトラフィックを制御できる必要があります。
- ACLベースのパケットフィルタリングは、一般的に使用されるネットワークセキュリティ技術です。アクセスコントロールリスト(ACL)を使用してトラフィックを識別し、パケットを転送またはドロップするかどうかを決定します。
- ACLルールは、トラフィック分類が必要な他の技術で使用できます。

学習の目標

このレッスンを修了すると、次のことができるようになります:



- ACLを作成して適用する
- ACLベースのパケットフィルタリングについて説明する。
- ACLの分類
- ACLベースのパケットフィルタリングの設定
- ACLベースのパケットフィルタリングの設定ガイドラインを使用します。

アジェンダ

- ACLの概要
- ACLパケットフィルタリングの基本
- ACL分類
- ACLパケットフィルタリング設定
- ACLパケットフィルタリングのガイドライン

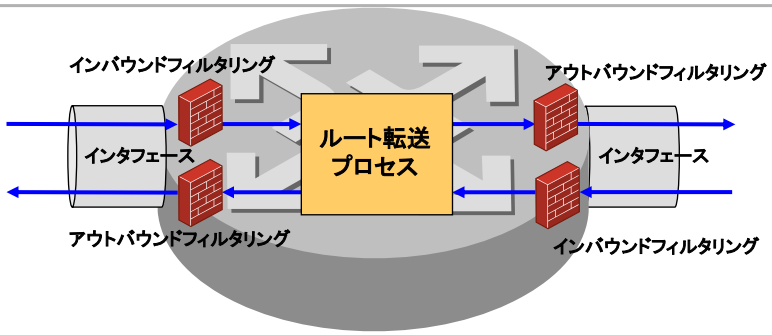
ACLの概要

- ACLは主にトラフィックフローを識別するために使用されます。
- ACLは、次のようなアプリケーションで広く使用されています。
  - パケットフィルタリング
  - ネットワークアドレス変換(NAT)
  - データのQuality of Service(QoS)分類
  - ルーターのルートポリシーとフィルタリング
  - ダイヤルオンデマンド(アクセス要求に応じた電話回線を通じたネットワーク接続)

アジェンダ

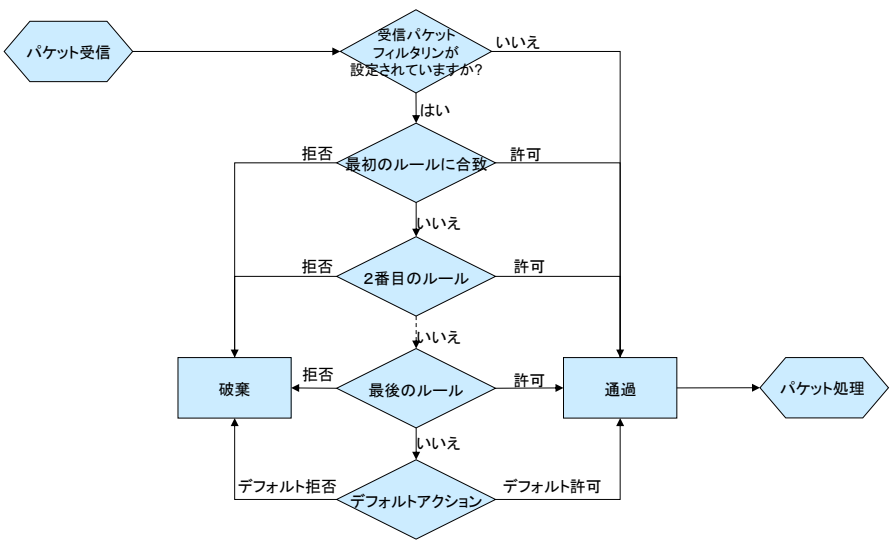
- ■ **ACLの概要**
- ■ **ACLパケットフィルタリングの基本**
- ■ ACL分類
- ■ **ACLパケットフィルタリング設定**
- ■ **ACLパケットフィルタリングのガイドライン**

ACLベースのパケットフィルタリング

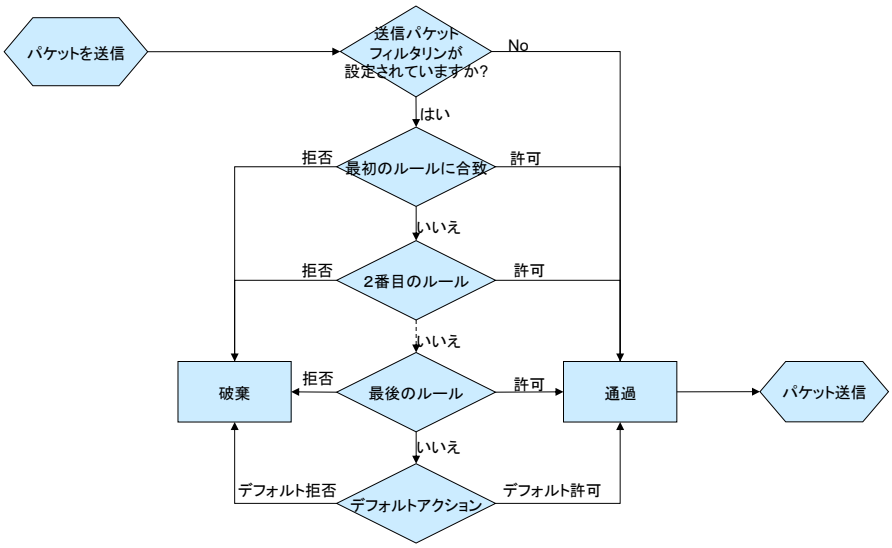


- ACLは、インターフェイスのインバウンドまたはアウトバウンド方向に適用されます。
- インターフェイスがパケットを送受信するとき、インターフェイスに適用されるインバウンド/アウトバウンドACLはパケットをフィルタリングします。
- インバウンドパケットとアウトバウンドパケットを1つずつフィルタリングして、パケットを破棄するか許可するかを決定します。

インバウンドパケットフィルタリング作業手順



アウトバウンドパケットフィルタリング作業手順



ワイルドカードマスク

- IPアドレスとワイルドカードマスクは、アドレス範囲を決定します。
- ワイルドカードは、フォーマットがサブネットマスクに似ていますが、意味が異なります。
  - **ワイルドカードマスクの0のビットは、IPアドレスの対応するビットが正確に一致する必要があることを意味します。**
  - **ワイルドカードマスクの1のビットは、ビットが一致する必要がないことを意味し、無視することができます。**

ワイルドカードマスク	意味
0.0.0.255	アドレスの最初の24ビットと一致する
0.0.3.255	アドレスの最初の22ビットに一致する
0.255.255.255	アドレスの最初の8ビットと一致する

ワイルドカードマスク応用例

IPアドレス	ワイルドカード	アドレスとワイルドカードで指定されたアドレス範囲
192.168.0.1	0.0.0.255	192.168.0.0/24
192.168.0.1	0.0.3.255	192.168.0.0/22
192.168.0.1	0.255.255.255	192.0.0.0/8
192.168.0.1	0.0.0.0	192.168.0.1
192.168.0.1	255.255.255.255	0.0.0.0/0
192.168.0.1	0.0.2.255	192.168.0.0/24 および 192.168.2.0/24

アジェンダ

- ACLの概要
- ACLパケットフィルタリングの基本
- ACL 分類
- ACLパケットフィルタリング設定
- ACLパケットフィルタリングのガイドライン

ACLの識別

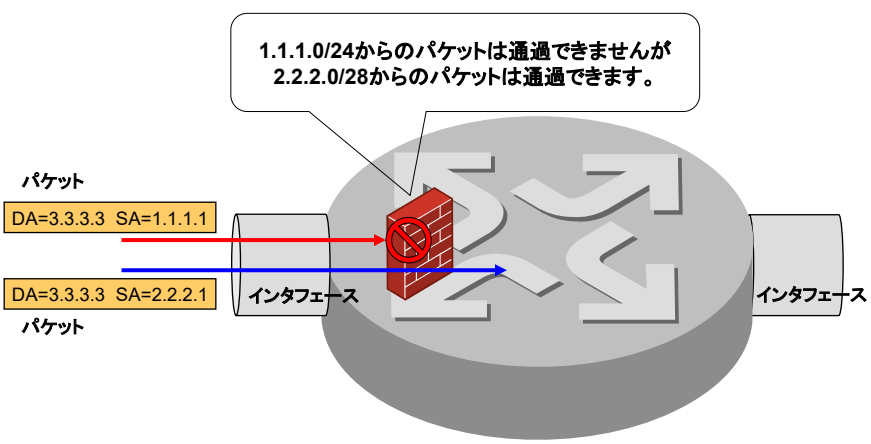
- ACLはACL番号で識別されます

タイプ	ACL 番号
基本ACL	2000 から 2999
拡張ACL	3000から3999
イーサネットフレームヘッダーACL	4000から4999

- ACLの名前を指定して、メンテナンスを容易にすることもできます

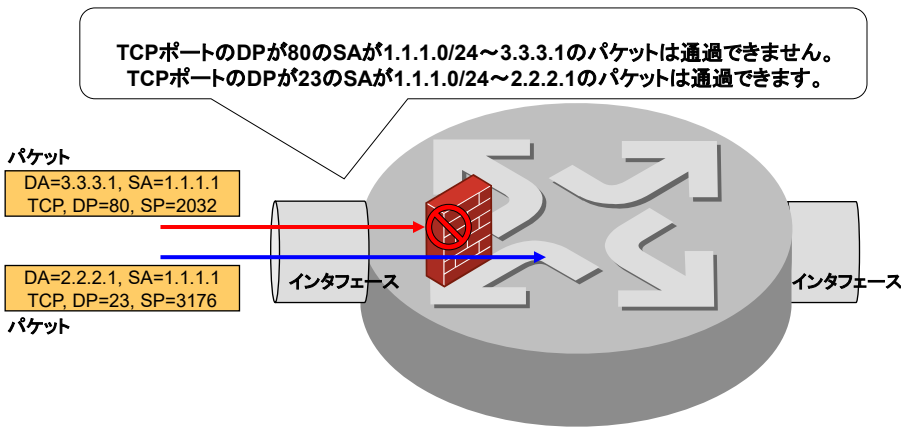
基本ACL

- 基本ACLは、送信元IPアドレスのみに基づいてフィルタリング基準を定義します。



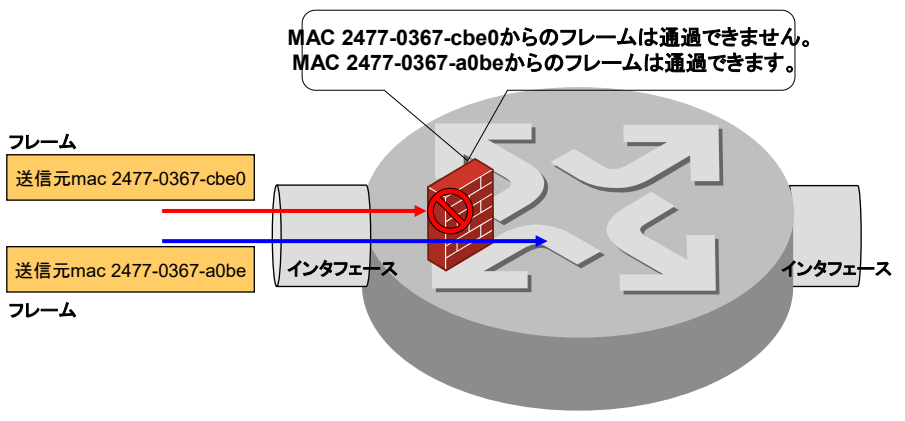
拡張ACL

- 拡張ACLは、送信元IPアドレス、宛先IPアドレス、IP上で伝送されるプロトコル、およびその他のレイヤー3またはレイヤー4プロトコルヘッダー情報に基づいてパケットを照合します



イーサネットフレームヘッダーACL

- イーサネットフレームヘッダーACLは、送信元MACアドレス、宛先MACアドレス、802.1pプライオリティ(VLANプライオリティ)、リンクレイヤプロトコルタイプなどのレイヤー2プロトコルヘッダーフィールドに基づいてパケットを照合します。



アジェンダ

- ■ ACLの概要
- ■ ACLパケットフィルタリングの基本
- ■ ACL分類
- ■ ACLパケットフィルタリング設定
- ■ ACLパケットフィルタリングのガイドライン

ACLパケットフィルタリングの設定作業

H3C

- パケットフィルタリングのデフォルトのフィルタリングアクションを設定します。
- 適切なACLタイプを選択します。
- 適切なACLルールを作成します。
  - 一致基準を指定します。
  - フィルタリングアクション(許可/拒否)を設定します。
- ルータのインターフェイスにACLを適用し、フィルタリング方向(インバウンド/アウトバウンド)を指定します。

デフォルトのフィルタリングアクションを設定

- **システムのデフォルトのフィルタリングアクションを指定します。**
  →デフォルトは、スイッチ、ルーター、ファイアウォールとも許可(permit)です。

```
[H3C] firewall default deny
```


基本ACLの設定

- 基本ACLを設定し、ACL番号を指定する
  - 基本ACLのACL番号の範囲は2000～2999です。

```
[H3C] acl basic acl-number
```

- **ルールを作成する**
  → 照合する送信元IPアドレス範囲の指定
  → フィルタリングアクションを許可(**permit**)または拒否(**deny**)に指定する

```
[H3C-acl-basic-2000] rule [ rule-id ] { deny | permit } [ counting
| fragment | logging | source { sour-addr sour-wildcard | any } |
time-range time-range-name ]
```

拡張ACLの設定

- **拡張ACLの設定とACL番号の指定**
  → 拡張ACLのACL番号の範囲は3000～3999です。

[H3C] acl advanced *acl-number*

- **ルールを作成する**
  → 照合する送信元IPアドレス、宛先IPアドレス、IPで運ばれるプロトコル、ポート番号
  → 許可または拒否のフィルタリングアクション

[H3C-acl-adv-3000] rule [*rule-id*] **{ deny | permit }** *protocol* **[destination** { *dest-addr dest-wildcard* **| any } | destination-port** *operator port1* [*port2*] **established | fragment | source {** *sour-addr sour-wildcard* | **any } | source-port** *operator port1* [*port2*] | **time-range** *time-range-name* **]**

イーサネットフレームヘッダーACLの設定

- **イーサネットフレームヘッダーACLを設定後、ACL番号を指定します**
  → イーサネットフレームヘッダーACL番号は4000から4999です。

[H3C] acl mac *acl-number*

- **ルールを作成する**
  → 送信元 MAC アドレス、宛先 MAC アドレス、802.1p 優先度、レイヤー 2 プロトコルなど、照合するヘッダー情報を指定します。
  → フィルタリング アクションをpermitまたはdenyとして指定します

[H3C-acl-mac-4000] rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-addr dest-mask* | **lsap** *lsap-type lsap-type-mask* | **source-mac** *sour-addr source-mask* | **time-range** *time-range-name*]

インターフェイスへのACLの適用

- ACLがインターフェイスに適用された後にのみ、ACLベースのパケットフィルタリングが有効になります。
- インターフェイスのフィルタリング方向をアウトバウンドまたはインバウンドに指定します。

[H3C-Serial2/0] packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

ACLパケットフィルタリングの表示とデバッグ

やるべきこと	使用するコマンド
パケットフィルタリングに関する統計情報を表示する	**display packet-filter statistics** { **interface** *[interface-type interface-number]* { **inbound** | **outbound** } { *acl-number* | **name** *acl-name* } }
パケットフィルタ統計情報をクリアする	**reset packet-filter statistics** { **interface** *[interface-type interface-number]* { **inbound** | **outbound** } { *acl-number* | **name** *acl-name* } }
1つまたはすべてのIPv4ACLに関する情報を表示します。	**display acl** { *acl-number* | **all** }
ACLの統計情報をクリアします。	**reset acl counter** { *acl-number* | **all** | **name** *acl-name* }

アジェンダ

- ■ ACLの概要
- ■ ACLパケットフィルタリングの基本
- ■ ACL分類
- ■ ACLパケットフィルタリング設定
- ■ ACLパケットフィルタリングのガイドライン

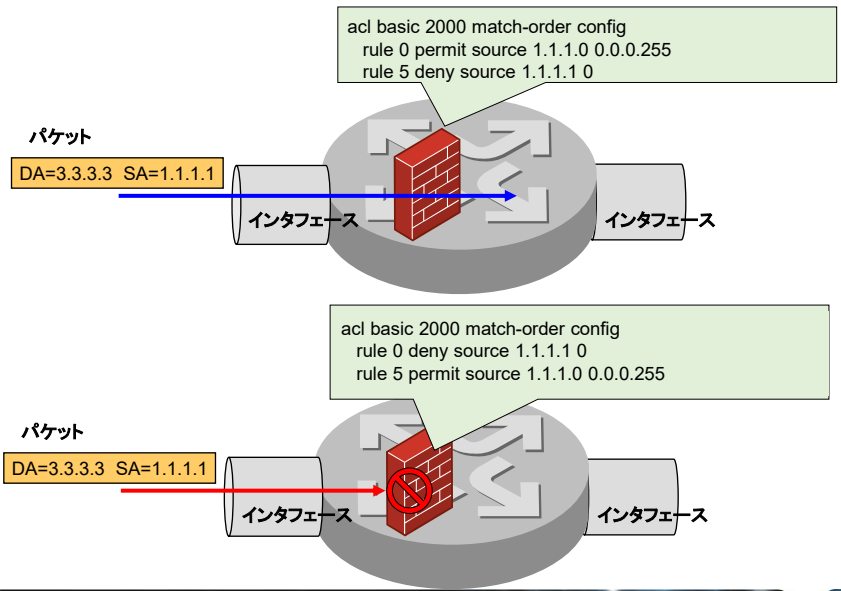
ACLルールの適用順

H3C

- match-orderは、ACL内のルールの優先順位を示します
- ACLでは、次の2つのルールの順序を使用できます。
  - Config:ACLルールはルールIDの昇順でソートされます。ID番号が小さいルールは、優先順位が高くなります。
  - auto:ACLルールは深さ順でソートされます。システムは他のルールよりも最小のIPアドレス範囲のルール優先して採用します。
- ACLルールの順序を設定します:

[H3C] acl basic *acl-number* [**match-order** { **auto** | **config** }]

ルールの順番が異なると異なる結果を得る

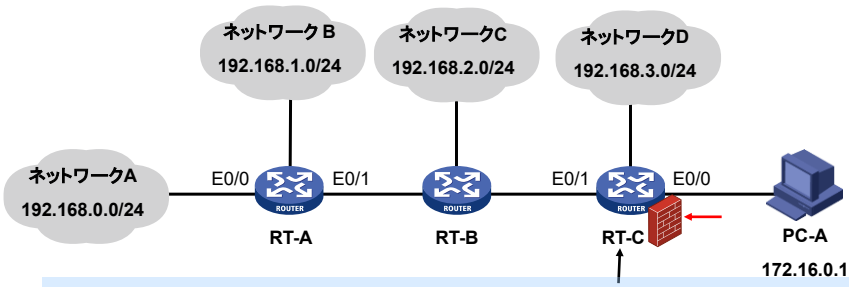


適切なインタフェースへのACLの適用

- 送信元に可能な限り近いルータインタフェースにACLを適用し、不要なトラフィック転送を削減します。
- 基本ACL
  - 基本ACLを送信元に近すぎるインターフェイスに適用すると送信元から一部のネットワークへの合法的なアクセスが停止する可能性があります。
  - 有効なトラフィックをブロックしない限り、基本ACLを送信元にできるだけ近いインターフェイスに適用してください。
- 拡張ACL
  - 拡張ACLを使用すると、ネットワークトラフィックをより詳細にアクセス制御できます。不要なトラフィックがネットワークに入らないように、できるだけ送信元の近くに配置してください。

拡張ACLの設置例

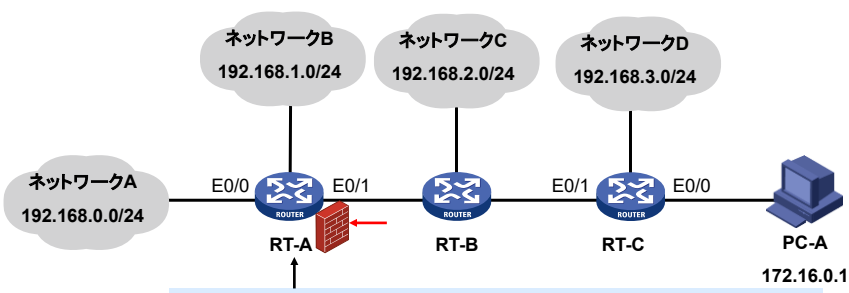
- PC-AがネットワークAとネットワークBにアクセスすることを禁止しますが、他のネットワークにはアクセスできます。




```
[RTC]acl advanced 3000
[RTC-acl-adv-3000]rule deny ip source 172.16.0.1 0 destination 192.168.0.0 0.0.1.255
[RTC-acl-adv-3000] quit
[RTC]interface GigabitEthernet0/0
[RTC-GigabitEthernet0/0]packet-filter 3000 inbound
```


基本ACLの設置例

- PC-AがネットワークAとネットワークBにアクセスすることを禁止し、他のネットワークにアクセスすることを許可する




```
[RTA]acl basic 2000
[RTA-acl-basic-2000]rule deny source 172.16.0.1 0
[RTA-acl-basic-2000] quit
[RTA] interface GigabitEthernet0/1
[RTA-GigabitEthernet0/1]packet-filter 2000 inbound
```

ACLパケットフィルタリングの限界

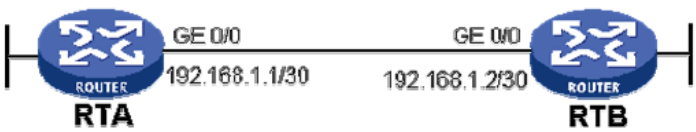
- ACLベースのパケットファイアウォールは、パケットヘッダー内のレイヤー2、3、4情報に従ってパケットをフィルタリングします。アプリケーションレイヤ情報を識別することはできません。
  - ユーザ名によってユーザからのパケットを許可または拒否することはできません。
  - ユーザを認可することはできません。
- ACLベースのパケットフィルタリングファイアウォールは、スタティックファイアウォールです。アプリケーション層プロトコルを動的に検出することはできません。

復習

- **パケットフィルタリングは、ACLルールを使用してパケットをフィルタリングします。ACLは、NAT、QoS、ルーティングポリシー、ダイヤルオンデマンド、およびトラフィック分類が必要な他のアプリケーションでも使用できます。**
- **基本ACLは、送信元IPアドレスに基づいてパケットをフィルタリングします。拡張ACLは、送信元/宛先IPアドレス、プロトコル番号、およびポート番号に基づいてパケットをフィルタリングします。**
- **ACL内のルールの一致順は、ACLフィルタリング結果に影響を与えます。**
- **ACLベースのパケットフィルタリングファイアウォールを適切なインターフェイスに適用して、不要なトラフィックがネットワークに入らないようにします。**

ACLベースのパケットフィルタリング

ルーターが接続されています。OSPFは現在、2つのルーター間で実行されています。ここで、RTAとRTBの間にOSPFネイバー関係が確立されないように、RTAでACLを設定する場合、RTAのge0/0インターフェイスのアウトバウンド方向に適用できるACLはどれですか。



ACLベースのパケットフィルタリング

acl number 3000
rule 0 deny ip destination 224.0.0.5 0
rule 5 permit ip

acl number 3000
rule 0 deny ip destination 224.0.0.5 0 destination-port eq 89
rule 5 permit ip

acl number 3000
rule 0 deny udp destination-port eq 89
rule 5 permit ip

acl number 3000
rule 0 deny ospf
rule 5 permit ip

ACLベースのパケットフィルタリング

顧客の1つのMSRルートは、WANインターフェイスS1/0を介してインターネットに接続し、LANインターフェイスge0/0を介してオフィスネットワークに接続します。現在、オフィスネットワークのユーザーは通常どおりインターネットにアクセスできます。次のACL構成をルーターに追加します。

```
[RTA] firewall enable
[RTA] firewall default deny
[RTA] acl number 3000
[RTA-acl-3000] rule 0 deny icmp
[RTA-acl-3000] rule 5 permit tcp destination-port eq 20
[RTA-acl-3000] quit
[RTA] interface GigabitEthernet0/0
[RTA- GigabitEthernet0/0] Firewall packet filter 3000 inbound
[RTA- GigabitEthernet0/0] firewall packet-filter 3000 outbound
```



正しい説明を選びなさい。

ACLベースのパケットフィルタリング

オフィスネットワークユーザーによって開始されたインターネットへのICMPメッセージは、ルーターによって禁止されています

オフィスネットワークユーザーによって開始されたルーターへのFTP(port:20)トラフィックは、正常に通過できます。

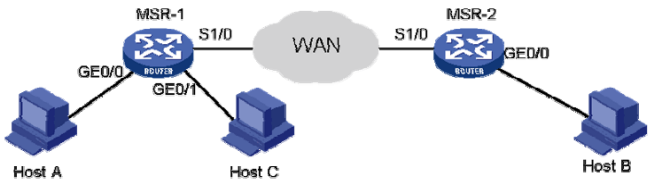
オフィスネットワークユーザーからルーターge0/0に送信されたTelnet(port:23)メッセージは正常に通過できます

オフィスネットワークユーザーによって開始されたインターネットへのFTP(port:20)トラフィックはルーターを正常に通過でき、他のすべてのメッセージはルーターを通過できません。

※TCPとUDPの講義を思い出してください。FTPは接続の認証や応答信号の受信は、TCPポート21を使用します。データの送受信にはTCPポート20が使用されます。

ACLベースのパケットフィルタリング

顧客のネットワーク構造を図に示します。以下の要件を達成するために正しいものを選びなさい。
ホストCとホストBがお互いにアクセスできます。
ホストAとホストBはお互いにアクセスできません。
ホストAとホストCはお互いにアクセスできません。



この要件は、拡張ACLでのみ実装できます。

MSR-1のインターフェイスge0/0にACLを適用するだけでは、要件を満たすことはできません。

この要件は、2台のルーターのインターフェースge0/0に拡張ACLを適用することで実現できます。

この要件は、MSR-1のS1/0およびge0/0に拡張ACLを適用することで実現できます。

H3C
IToIP Solutions Expert

スイッチのポートセキュリティ

v1.0



New SWA Technologies Co., Ltd. All rights reserved

学習の目標

このレッスンを修了すると、次のことができるようになります：

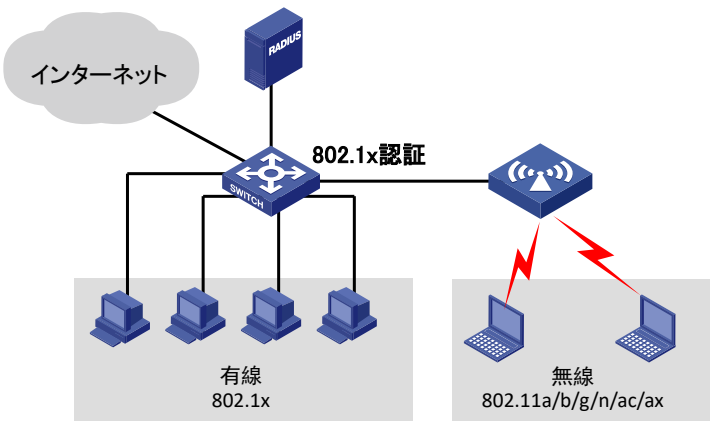
- 802.1x認証の設定
- MAC認証の設定
- ポートアイソレーションの設定



アジェンダ

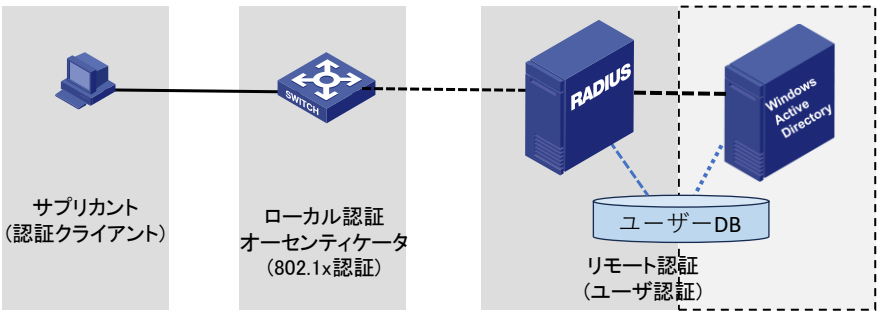
- **802.1x認証の概要と設定**
- **MAC認証の概要と設定**
- **ポートアイソレーションの概要と設定**

802.1x 認証概要



- IEEE802.11無線LAN(WLAN)のセキュリティのために開発された802.1xプロトコルは、ユーザアクセス認証のためにLANで広く使用されています。

802.1x アーキテクチャ



- ローカル認証
  - オーセンティケータシステムのローカルサーバーがサプリカントを認証する
- リモート認証
  - リモート認証サーバーがユーザを認証する

基本的な802.1xコンフィグレーション

- **802.1xをスイッチ全体で有効にする**

```
[Switch] dot1x
```

- **802.1xのポート方式を指定する(ポート毎、又はMACアドレスに基づいて)**

```
[Switch-Ten-GigabitEthernet1/0/1] dot1x port-method
{ macbased | portbased }
```

- **802.1xをインタフェースで有効にする**

```
[Switch-Ten-GigabitEthernet1/0/1] dot1x
```

- **ローカルユーザーを作成し、関連するパラメーターを設定する**

```
[Switch] local-user user-name class network
[Switch- luser-network-localuser] service-type lan-access
[Switch- luser-network-localuser] password { cipher | simple
} password
```

基本的な802.1xコンフィグレーション

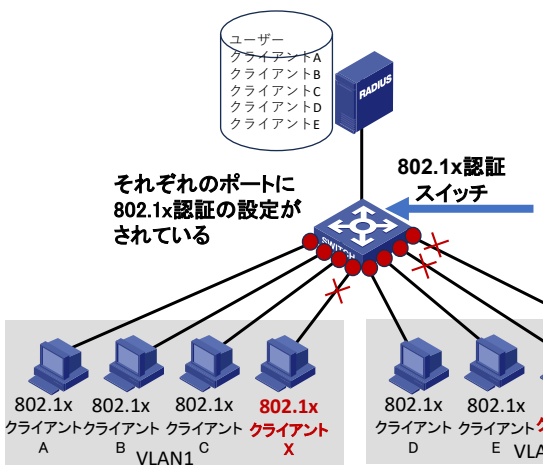
- **local-userのnetworkクラスのユーザーが提供するサービス**

```
[Switch-luser-network-localuser] service-type ?
  advpn          ADVPN service
  ike            IKE service
  ipoe           IPOE service
  lan-access     LAN access service(802.1xのサービス)
  portal         Portal service
  ppp            PPP service
  sslvpn         SSL VPN service
```

- **local-userのmanageクラスのユーザーが提供するサービス**

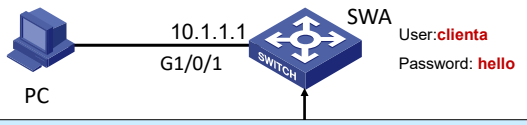
```
[Switch-luser-manage-localuser] service-type ?
  ftp            FTP service
  http           HTTP service type
  https          HTTPS service type
  pad            X.25 PAD service
  ssh            Secure Shell service
  telnet         Telnet service
  terminal       Terminal access service
```


アクセス制御方式(ポートベースの802.1x認証)



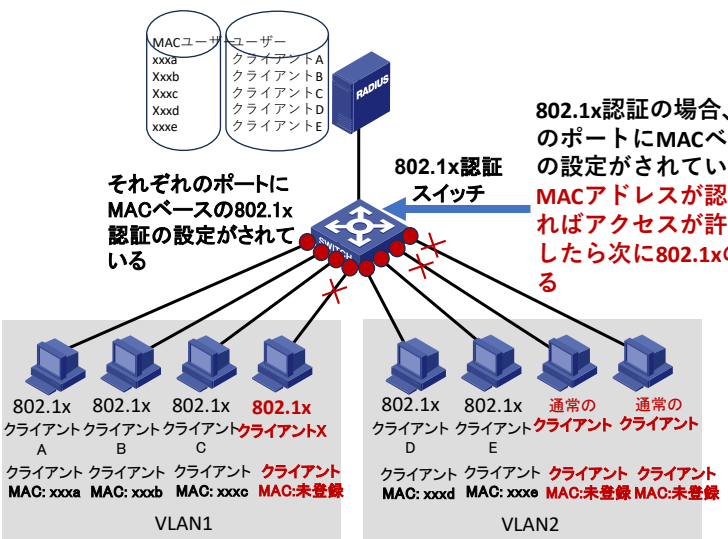
802.1x認証の場合、認証スイッチのポートに802.1x認証の設定がされていれば、個別にクライアントが認証されます。認証合格すれば、ポートにアクセス可能となり、その後の認証はありません。
このポートにスイッチがカスケードされていて他のPCがあれば1台のPCが802.1x認証に合格すれば、他のPCは認証無しでアクセス可能です。認証されたPCがオフラインになれば他のPCはアクセスできなくなります。

ポートベースの802.1x認証の設定例

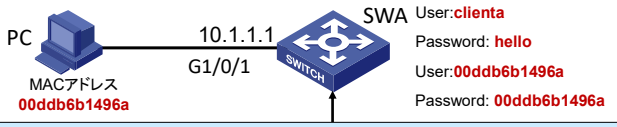



```
[SWA]dot1x
[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1]dot1x
[SWA-GigabitEthernet1/0/1]dot1x port-method portbased
[SWA-GigabitEthernet1/0/1]dot1x mandatory-domain local
[SWA-GigabitEthernet1/0/1]dot1x port-control auto
#
[SWA]radius scheme radius-local
[SWA-radius-radius1]primary authentication 10.1.1.1
[SWA-radius-radius1]primary accounting 10.1.1.1
[SWA-radius-radius1]key authentication simple name
[SWA-radius-radius1]user-name-format without-domain
#
[SWA]domain local
[SWA-isp-bbb]authentication lan-access radius-scheme radius-local local
[SWA-isp-bbb]authorization lan-access radius-scheme radius-local local
[SWA-isp-bbb]accounting lan-access radius-scheme radius-local local
#
[SWA]local-user clienta class network
[SWA-luser-network-localuser]password simple hello
[SWA-luser-network-localuser]service-type lan-access
```


アクセス制御方式(MACベースの802.1x認証)



MACベースの802.1x認証の設定例




```
[SWA]dot1x
[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1]dot1x
[SWA-GigabitEthernet1/0/1]dot1x port-method macbased
[SWA-GigabitEthernet1/0/1]dot1x mandatory-domain local
#
[SWA]radius scheme radius-local
[SWA-radius-radius1]primary authentication 10.1.1.1
[SWA-radius-radius1]primary accounting 10.1.1.1
[SWA-radius-radius1]key authentication simple name
[SWA-radius-radius1]user-name-format without-domain
#
[SWA]domain local
[SWA-isp-bbb]authentication lan-access radius-scheme radius-local local
[SWA-isp-bbb]authorization lan-access radius-scheme radius-local local
[SWA-isp-bbb]accounting lan-access radius-scheme radius-local local
```

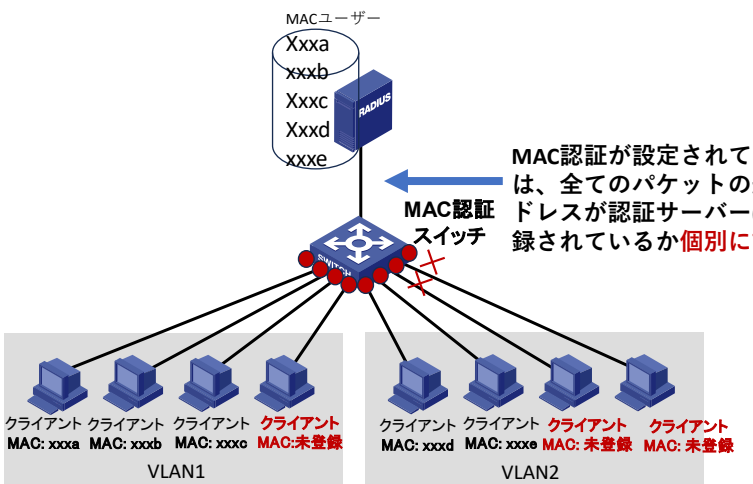

802.1x認証の設定例(続き)

```
#
[SWA]local-user clienta class network
[SWA-luser-network-localuser]password simple hello
[SWA-luser-network-localuser]service-type lan-access
#
[SWA]local-user 00ddb6b1496a class network
[SWA-luser-network-localuser]password simple 00ddb6b1496a
[SWA-luser-network-localuser]service-type lan-access
```

アジェンダ

- 802.1xの概要と設定
- MAC認証の概要と設定
- ポートアイソレーションの概要と設定

アクセス制御方式(MAC認証)



基本的なMAC認証コンフィグレーション

- MAC認証をスイッチ全体で有効にする

```
[Switch] mac-authentication
```

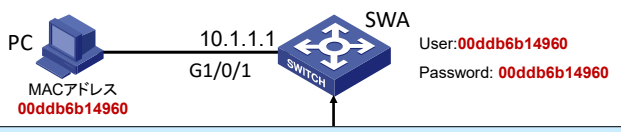
- MAC認証をポート毎に有効化

```
[Switch-Ten-GigabitEthernet1/0/1] mac-authentication
```

- ローカルユーザーを作成し、関連するパラメーターを設定する

```
[Switch] local-user user-name class network
[Switch- luser-network-localuser] service-type lan-access
[Switch- luser-network-localuser] password { cipher | simple
} password
```


MAC認証の設定例

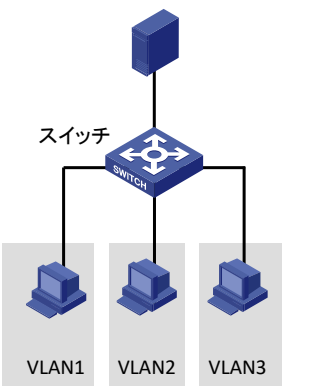



```
[SWA]mac-authentication
[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1]mac-authentication
#
[SWA]radius scheme radius-local
[SWA-radius-radius1]primary authentication 10.1.1.1
[SWA-radius-radius1]primary accounting 10.1.1.1
[SWA-radius-radius1]key authentication simple name
[SWA-radius-radius1]user-name-format without-domain
#
[SWA]domain local
[SWA-isp-bbb]authentication lan-access radius-scheme radius-local local
[SWA-isp-bbb]authorization lan-access radius-scheme radius-local local
[SWA-isp-bbb]accounting lan-access radius-scheme radius-local local
[SWA]domain default enable local
#
[SWA]local-user 00ddb6b14960 class network
[SWA-luser-network-localuser]password simple 00ddb6b14960
[SWA-luser-network-localuser]service-type lan-access
```

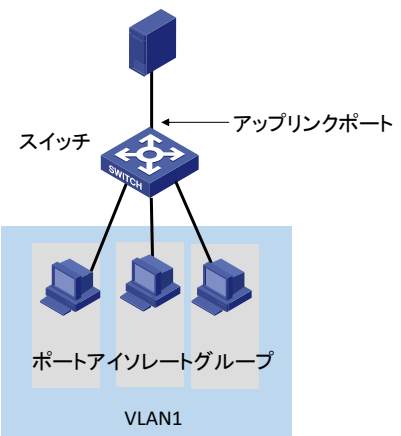
アジェンダ

- 802.1xの概要と設定
- MAC認証の概要と設定
- ポートアイソレーションの概要と設定

ポートアイソレーション概要



VLAN間のポートを分離



VLAN内のポートを分離

ポートアイソレーションの基本設定

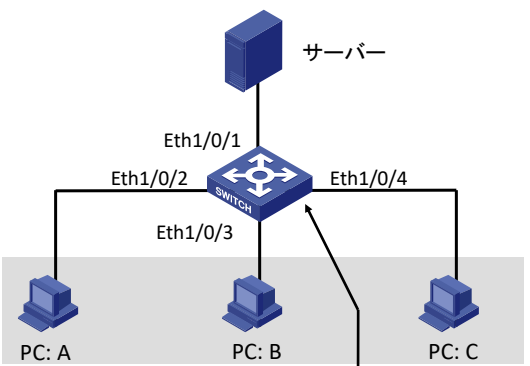
- アイソレーショングループを作成します

```
[switch]port-isolate group 1
```

- 指定したポートをアイソレーショングループに追加し、アイソレーショングループの共通ポートとして構成します。

```
[Switch-Ethernet1/0/1] port-isolate enable group 1
```


アイソレーションポートの設定例




```
[SWA] port-isolate group 1
[SWA]interface ethernet1/0/2
[SWA-Ethernet1/0/2] port-isolate enable group 1
[SWA]interface ethernet1/0/3
[SWA-Ethernet1/0/3] port-isolate enable group 1
[SWA]interface ethernet1/0/4
[SWA-Ethernet1/0/4] port-isolate enable group 1
```

復習

- 802.1Xは、ポートベースのネットワークアクセス制御プロトコルであり、ユーザの認証を実行します。
- MAC認証は、ポートベースのネットワークアクセス制御プロトコルであり、クライアントのMACアドレス認証を実行します。
- ポートアイソレーションは、VLAN内のそれぞれのポートを孤立させます。

ポートベースの802.1x認証の特徴は次のうちどれですか？

ポート内のすべてのアクセスユーザーを個別に確認する必要があります

ポートの下の最初のユーザーがオフラインの場合、同じポートの他のユーザーもネットワークの使用を拒否されます

ユーザーがオフラインの場合、そのユーザーのみがネットワークを使用できません

ポートの下の最初のユーザーが正常に検証される限り、同じポートの他のアクセスユーザーは認証なしでネットワークリソースを使用できます

スイッチのポートセキュリティ

MACベースの802.1x認証の機能は次のうちどれですか？

ポート内のすべてのアクセスユーザーを個別に確認する必要があります

ポートの下の最初のユーザーがオフラインの場合、他のユーザーもネットワークの使用を拒否されます

ユーザーがオフラインの場合、そのユーザーのみがネットワークを使用できません

ポートの下の最初のユーザーが正常に検証される限り、他のアクセスユーザーは認証なしでネットワークリソースを使用できます



H3C

ITolP Solutions Expert

NAT

v1.0



New H3C Technologies Co., Ltd. All rights reserved

はじめに

- ネットワークの爆発的な成長に伴い、IPv4アドレスは不足しています。
- プライベートアドレスを持つユーザはインターネットにアクセスしようとします。
- NATはプライベートアドレスをパブリックアドレスに変換します。

学習の目標

このレッスンを修了すると、次のことができるようになります:

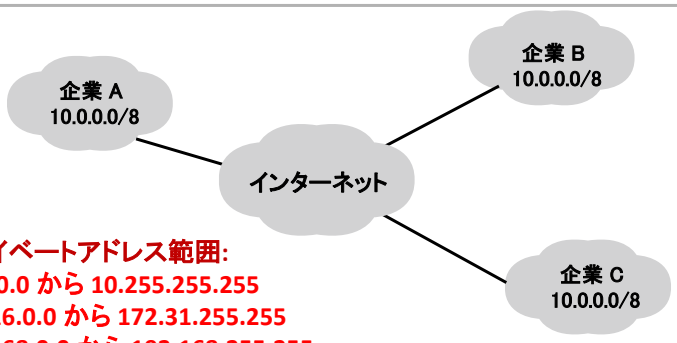
- NATの必要性について説明する
- NATの仕組みについて説明する
- 一般的なNATアプリケーションを設定する
- NATのトラブルシューティング
- 異なるネットワークへのNATの適用



アジェンダ

- NATの概要
- 基本的なNAT
- NAPT (Network Address Port Translation)
- Easy IP
- 外部公開用内部サーバ
- NAT ALG (Application Layer Gateway)
- NATの表示とデバッグ

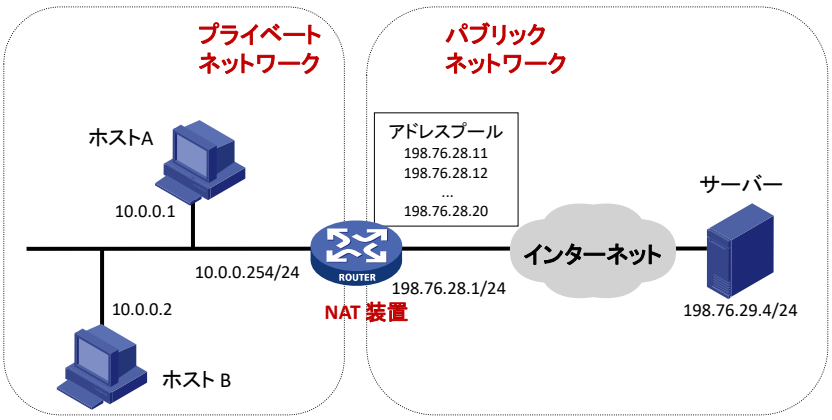
パブリックアドレスとプライベートアドレス



プライベートアドレス範囲:
10.0.0.0 から 10.255.255.255
172.16.0.0 から 172.31.255.255
192.168.0.0 から 192.168.255.255

- 任意の組織がプライベートアドレスを自由に使用できます。
- プライベートアドレスを持つパケットは、インターネット上でルーティングできません。
- プライベートユーザがインターネットにアクセスできるように、出力側にNATデバイスを配置する必要があります。

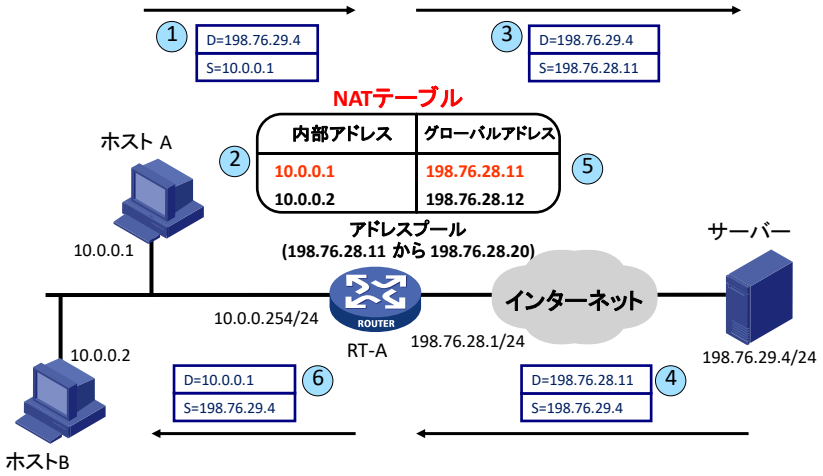
NAT アプリケーション



アジェンダ

- NATの概要
- 基本的なNAT
- NAPT (Network Address Port Translation)
- Easy IP
- 内部サーバ
- NAT ALG(Application Layer Gateway)
- NATの表示とデバッグ

基本的なNAT

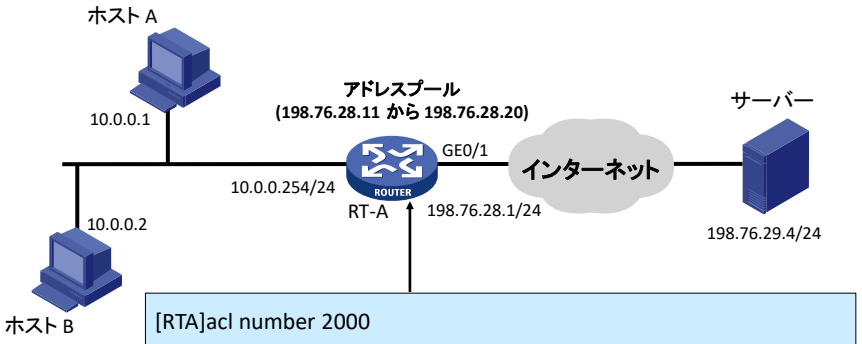


基本的なNATの設定

- ACLの定義
  - 変換されるパケットを照合するには、ACLによって許可されたパケットは変換されますが、ACLによって拒否されたパケットは変換されません。
- アドレスプールの作成
  - **nat address-group** *group-number*
  - **address** *start-address end-address*
- NATの設定
  - **nat outbound** *acl-number* **address-group** *group-number* **no-pat**

※no-pat (Not Port Address Translation)はアドレス変換において変換後のアドレスは同じで、ポート番号を変えて区別することは行わず、あくまでも異なるアドレスへ変換する

基本的なNAT設定例

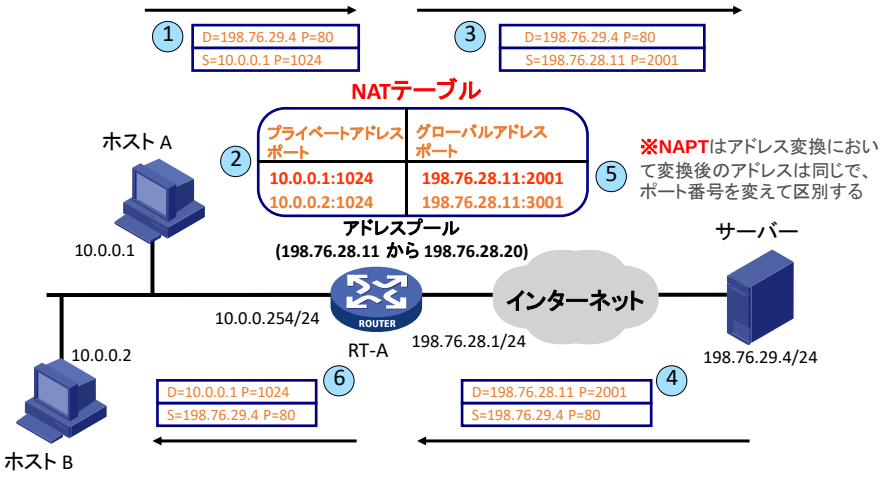



```
[RTA]acl number 2000
[RTA-acl-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255
[RTA]nat address-group 1
[RTA-address-group-1]address 198.76.28.11 198.76.28.20
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]nat outbound 2000 address-group 1 no-pat
```

アジェンダ

- NATの概要
- 基本的なNAT
- **NAPT(**Network Address Port Translation **)**
- Easy IP
- 外部公開用内部サーバ
- NAT ALG(Application Layer Gateway)
- NATの表示とデバッグ

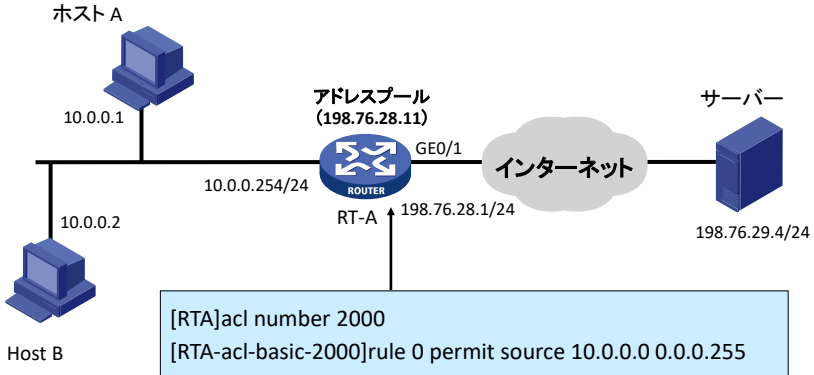
NAPT



NAPTの設定

- ACLの定義
  - 変換するパケットを決定する
  - ACLによって許可されたパケットは変換されますが、ACLによって拒否されたパケットは変換されません。
- アドレスプールの作成
  - **nat address-group** *group-number*
  - **address** *start-address end-address*
- NATの有効化
  - **nat outbound** *acl-number* **address-group** *group-number*

NAPTの設定例




```
[RTA]acl number 2000
[RTA-acl-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255
[RTA]nat address-group 1
[RTA-address-group-1]address 198.76.28.11 198.76.28.11
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]nat outbound 2000 address-group 1
```

アジェンダ

- NATの概要
- 基本的なNAT
- NAPT (Network Address Port Translation)
- Easy IP
- 外部公開用内部サーバ
- NAT ALG(Application Layer Gateway)
- NATの表示とデバッグ

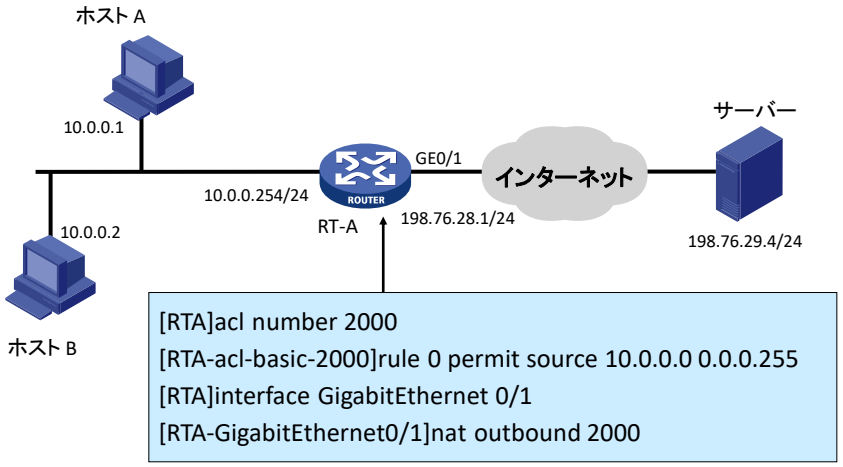
Easy IP

- 変換されるグローバルIPアドレスが一つなのでアドレスプールを設定する必要はありません。
- Easy IPはNAPTの一つの形態で複数のプライベートアドレスを1つのグローバルアドレスに変換し、ポート番号のみをダイナミックに割り当ててインターネットにアクセスします。

Easy IPの設定

- ACLの定義
  変換するパケットを決定するには
  ACLによって許可されたパケットは変換されますが、
  ACLによって拒否されたパケットは変換されません。
- NATの有効化
  - **nat outbound** *acl-number*

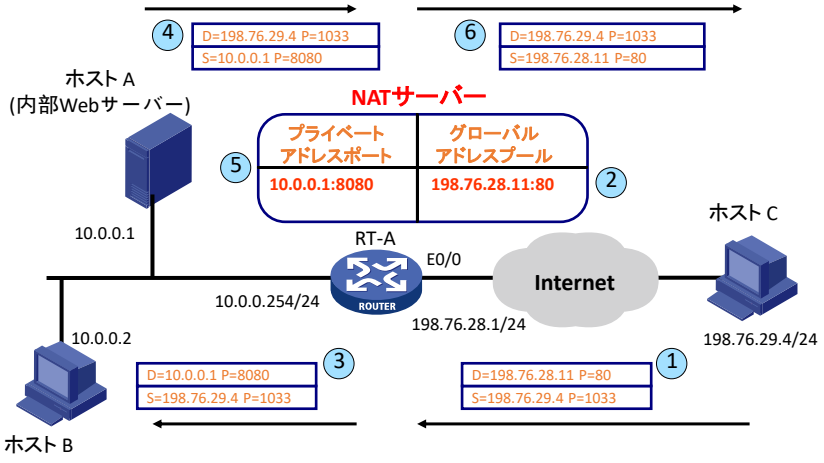
Easy IPの設定例



アジェンダ

- NATの概要
- 基本的なNAT
- NAPT (Network Address Port Translation)
- Easy IP
- 外部公開用内部サーバ
- NAT ALG(Application Layer Gateway)
- NATの表示とデバッグ

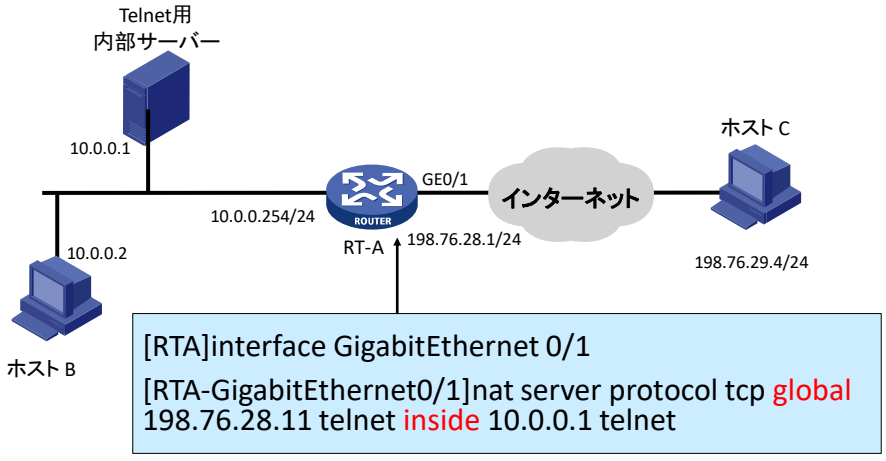
外部公開用内部サーバ



外部公開用内部サーバの設定

- 内部サーバを設定するには、次のコマンドを使用します。
  - **nat server protocol** *pro-type* **global** *global-addr* **[** *global-port* **]** **inside** *host-addr* **[** *host-port* **]**

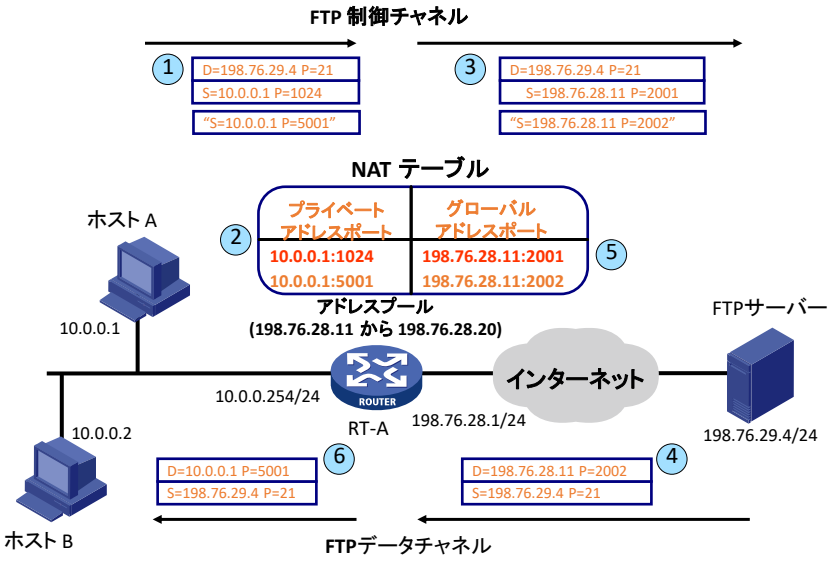
外部公開用内部サーバの設定例



アジェンダ

- NATの概要
- 基本的なNAT
- NAPT (Network Address Port Translation)
- Easy IP
- 外部公開用内部サーバ
- NAT ALG(Application Layer Gateway)
- NATの表示とデバッグ

NAT ALG



NAT ALG

- NAT ALGを設定するには、次のコマンドを使用します。
  - **nat alg { all | dns | ftp | h323 | icmp-error | ils | mgcp | nbt | pptp | rsh | rtsp | sccp | sip | sqlnet | tftp | xdmcp }**

※デフォルトでは、NAT ALG は DNS、FTP、ICMP-ERROR、PPTP、および RTSP に対して有効になっており、その他のサポートされているプロトコルに対しては無効になっています。

※PPTP(Point to Point Tunneling Protocol)は、VPN用の様々なリモートネットワーク接続の実装方式の一つ。

※RTSP(Real Time Streaming Protocol)は、オーディオやビデオなどのマルチメディア・データを含むサーバを、遠隔操作するためのプロトコル

アジェンダ

- NATの概要
- 基本的なNAT
- NAPT
- Easy IP
- 外部公開用内部サーバ
- NAT ALG(Application Layer Gateway)
- NATの表示とデバッグ

NATの表示とデバッグ

- アドレス変換ステータスを表示するには、次のコマンドを使用します。
  - **display nat { address-group** *group-number* **all outbound** *port-block-group* **server statistics session }**
- NATデバッグをイネーブルにするには、次のコマンドを使用します。
  - **<H3C>debugging nat { alg config event packet acl number }**
- NAT接続をクリアするには、次のコマンドを使用します。
  - **<H3C>reset nat session**

復習

- NATは、IPv4アドレスの枯渇を効果的に遅らせ、セキュリティを向上させます。
- 基本的なNATでは、プライベートアドレスとパブリックアドレスの間で1対1の変換が可能です。
- NAPTでは、プライベートアドレスとパブリックアドレスの間で多対1の変換が可能ですが、Easy IPはIPアドレスが動的に取得されるシナリオに適用できます。
- 内部サーバでは、パブリックホストがプライベートネットワーク上のサーバにアクセスできます。
- NAT ALGを使用すると、FTPなどの上位層プロトコルのメッセージのアドレス情報を変換できます。

Easy IP関する次の説明で正しいものを選びなさい

Easy IPを設定するには、インタフェースビューでnat outbound acl-numberコマンドを実行します。

Easy IPは、インタフェースのIPアドレスがアドレス変換後に送信元アドレスとして直接使用されることを示します。

Easy IPはダイヤル時またはインタフェースのIPアドレスが固定されている場合に使用できます。

インタフェースビューでは、ACLはデフォルトでインタフェースに関連付けられています。

ITofIP Solutions Expert