ルーター基礎セミナー

オンラインセミナー
ウェビナー

Allied Telesis

V2.2

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

目次

① ルーティングの役割・種類 (3P)

② RIP (9P)

③ NAT (16P)

④ PPPoE (22P)

⑤ 設定・管理機能 (26P)

⑥ 製品紹介 (31P)

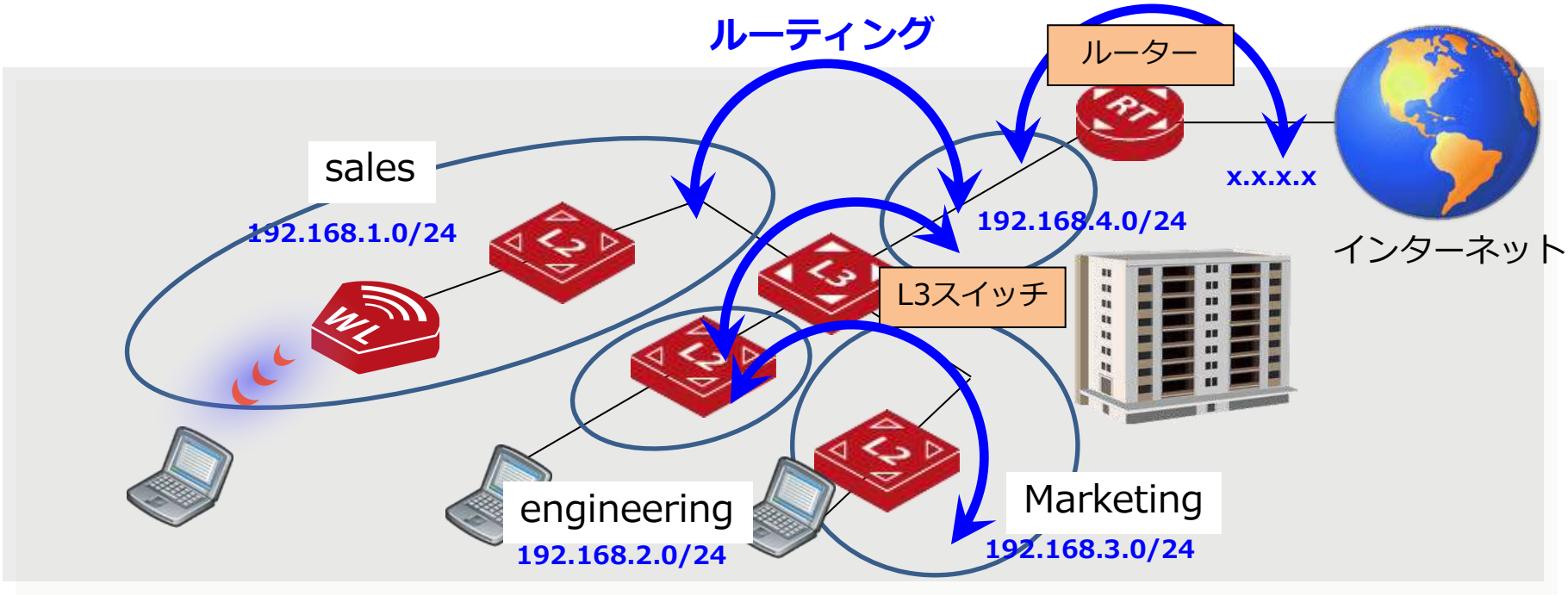
Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

①ルーティングの役割・種類

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ルーティングとは

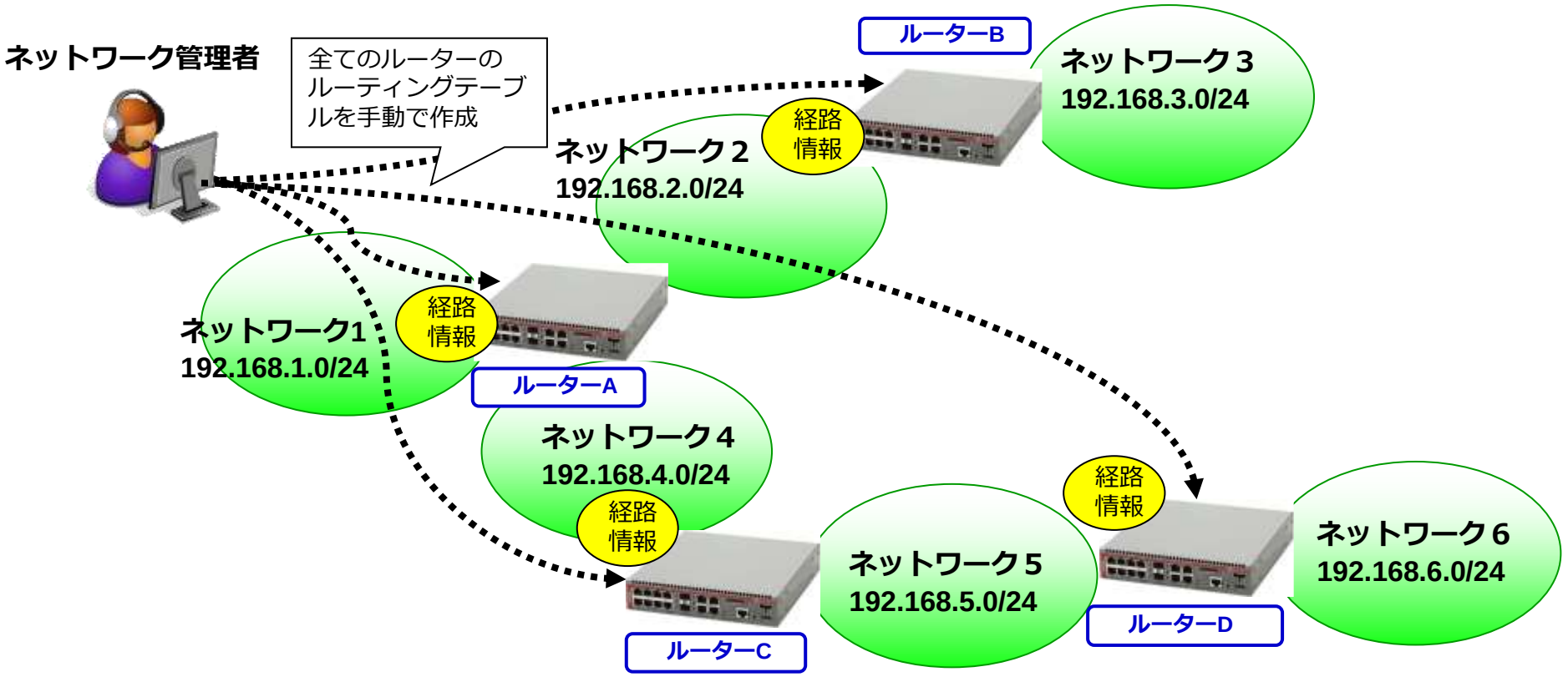
- ルーターやレイヤー3スイッチがパケットをネットワークを越えて目的地に正しく届けるための経路を選定・転送する機能です。
- スイッチがMACアドレスの情報に基づきブロードキャストドメイン内（サブネット）での通信を実現にするのに対し、ルーターやレイヤー3スイッチはIPアドレスを理解することにより異なるネットワーク間の通信を実現します。



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

スタティックルーティング

- ルーティングテーブルの内容をネットワーク管理者が構築する方法です。ネットワーク上の全ルーター（L3スイッチ）に経路情報を1つずつ登録します。
- 「経路情報の管理がしやすい」、「ルーティング機器への負担が少なくダイナミックルーティングに比べネットワークトラフィックが低くなる」、というメリットはありますが、全ルーターに経路情報を手動で設定する必要があるため、「手間がかかる」、「障害発生時には経路の再設定が必要」、などのデメリットもあります。



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

スタティックルーティングによる構築

- 下記ネットワーク構成における各ルーターのルーティングテーブル登録情報を示します。登録するネットワーク情報は、直接接続されていない（=他ルーターへの転送が必要な）ネットワーク情報（青字の部分）で、通常1つのコマンドで1つのネットワーク情報を登録します。
- NextHopとは、ルーターが目的ネットワークにパケットを送るために次に渡すルーターのインターフェースアドレスです。なお、インターフェースアドレスでなく、パケットを転送するルーターのインターフェース名を指定する場合もあります。

ルーターAのルーティングテーブル

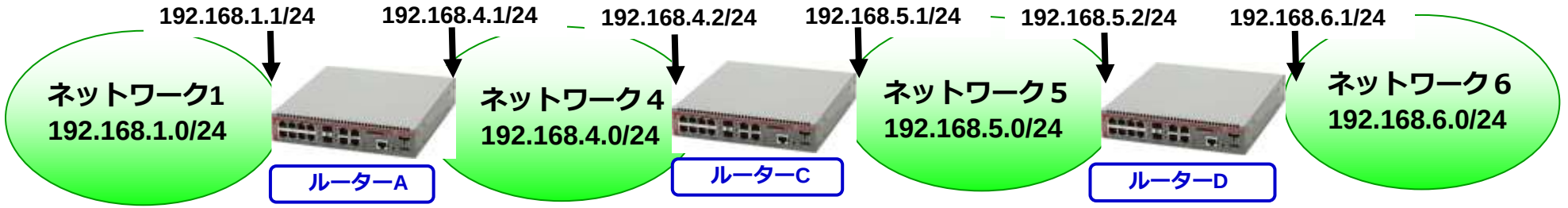
Network	NextHop
192.168.1.0/24	無
192.168.4.0/24	無
192.168.5.0/24	192.168.4.2
192.168.6.0/24	192.168.4.2

ルーターCのルーティングテーブル

Network	NextHop
192.168.1.0/24	192.168.4.1
192.168.4.0/24	無
192.168.5.0/24	無
192.168.6.0/24	192.168.5.2

ルーターDのルーティングテーブル

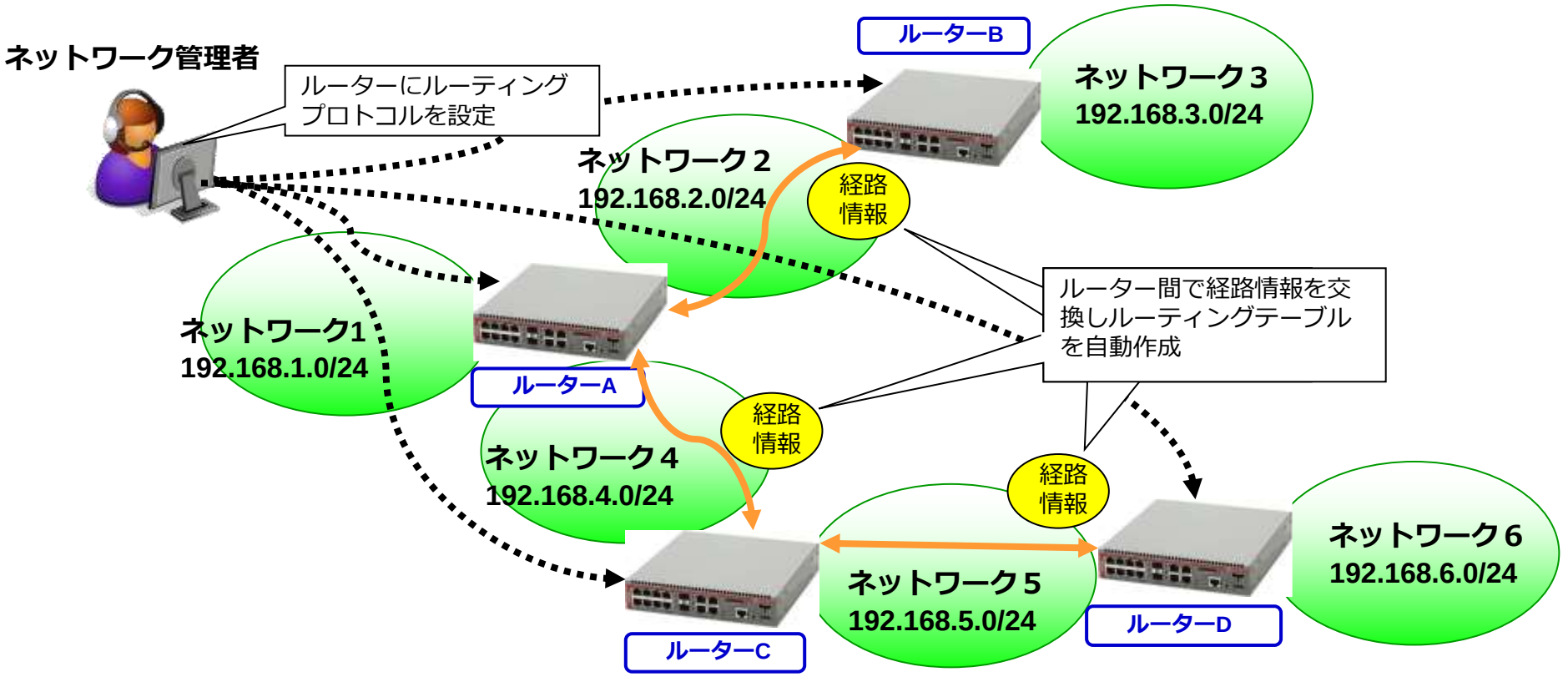
Network	NextHop
192.168.1.0/24	192.168.5.1
192.168.4.0/24	192.168.5.1
192.168.5.0/24	無
192.168.6.0/24	無



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ダイナミックルーティング

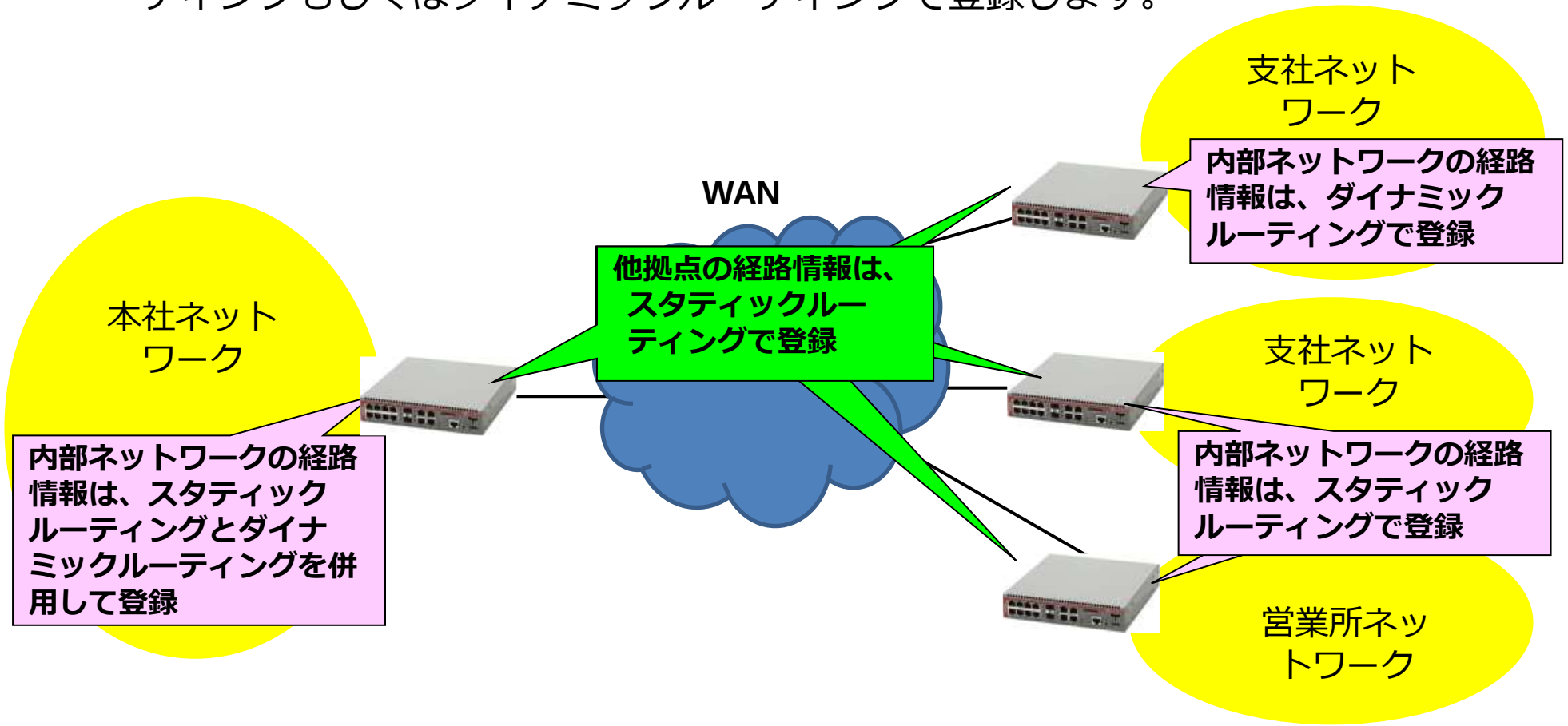
- 連結されるネットワークの数が多い大規模ネットワークでは、手動でネットワーク情報を設定するのは工数がかかります。
- そこで、ルーター（L3スイッチ）でルーティングプロトコルを動作させて自動的にルーティングテーブルを作成します。この方法をダイナミックルーティングと呼びます。



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ルーターにおける経路情報の登録方法

– ネットワーク構築において、主に外部ネットワークと内部ネットワークを接続する位置に設置されるルーターでは、外部ネットワーク及び他拠点の経路情報はスタティックルーティングで登録し、内部ネットワークの経路情報はスタティックルーティングもしくはダイナミックルーティングで登録します。



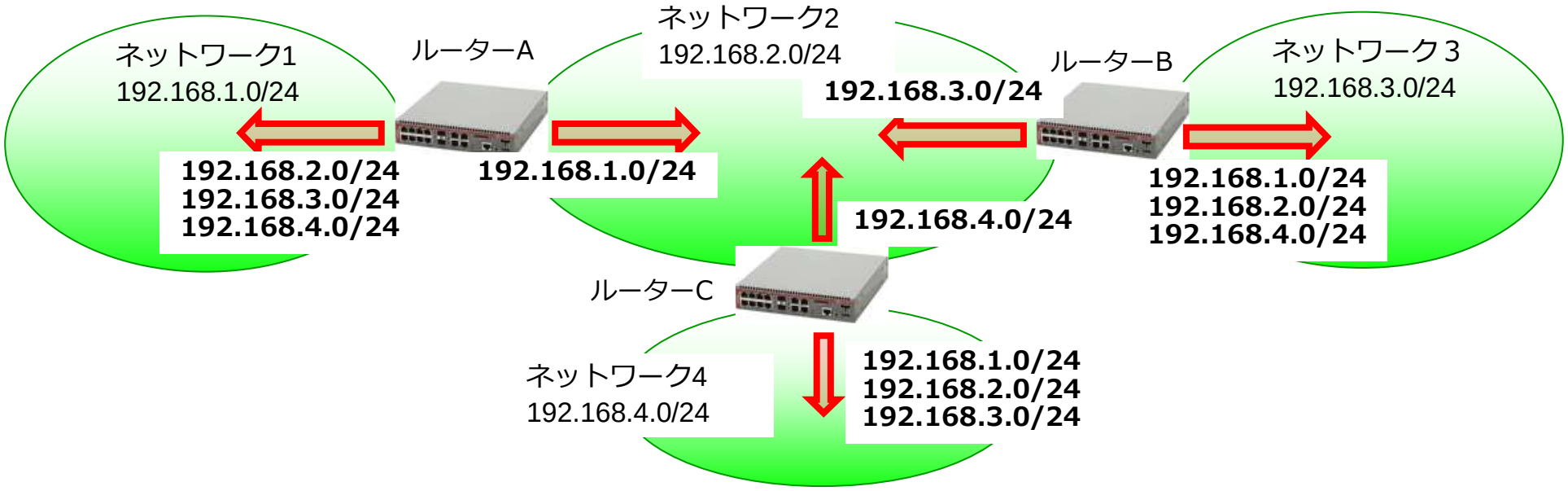
Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

②RIP

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

RIP(Routing Information Protocol)

- ルーティングテーブルの情報を定期的（30秒に1回）に隣接ルーターに通知します。RIPv1ではブロードキャストアドレスを使用し、RIPv2ではマルチキャストアドレス（224.0.0.9）を使用します（現在の主流はRIPv2のため、以降RIPv2の内容をベースに記載します）。
- Metric（経路選択の指標）はホップ数（経由するルーティング機器の数）を使用。ホップ数の上限は15のため、小・中規模のネットワーク向けルーティングプロトコル
- 経路計算アルゴリズムが簡素なためルーターにかかる負荷が少なく、処理能力の低いルーターにも実装可能です。また、設定も容易です。



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ルーティングテーブル作成の流れ（1）

- 自身のインターフェースアドレスのネットワークアドレスをルーティングテーブルに登録し、その情報を配信します。

ルーターAのルーティングテーブル

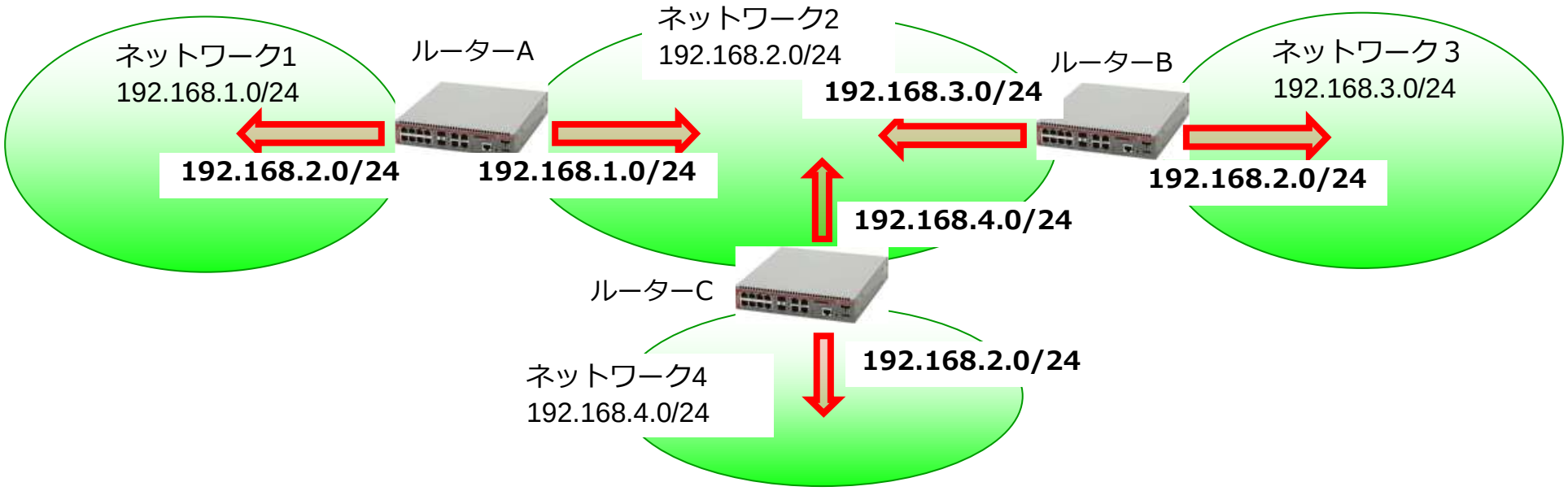
Network	Metric	NextHop
192.168.1.0/24	直接	無
192.168.2.0/24	直接	無

ルーターCのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.4.0/24	直接	無

ルーターBのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.3.0/24	直接	無



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ルーティングテーブル作成の流れ（2）

- ルーティングテーブル未登録の経路情報を他ルーターから受信した場合、ホップ数を1プラスしその経路情報をルーティングテーブルに登録します。
- ルーターが直接接続のネットワーク情報をホップ数0（ゼロ）で配信するか、ホップ数1で配信するかはベンダー機器により異なります。ここでは、ホップ数1で配信した場合の流れを記載します。※1

ルーターAのルーティングテーブル

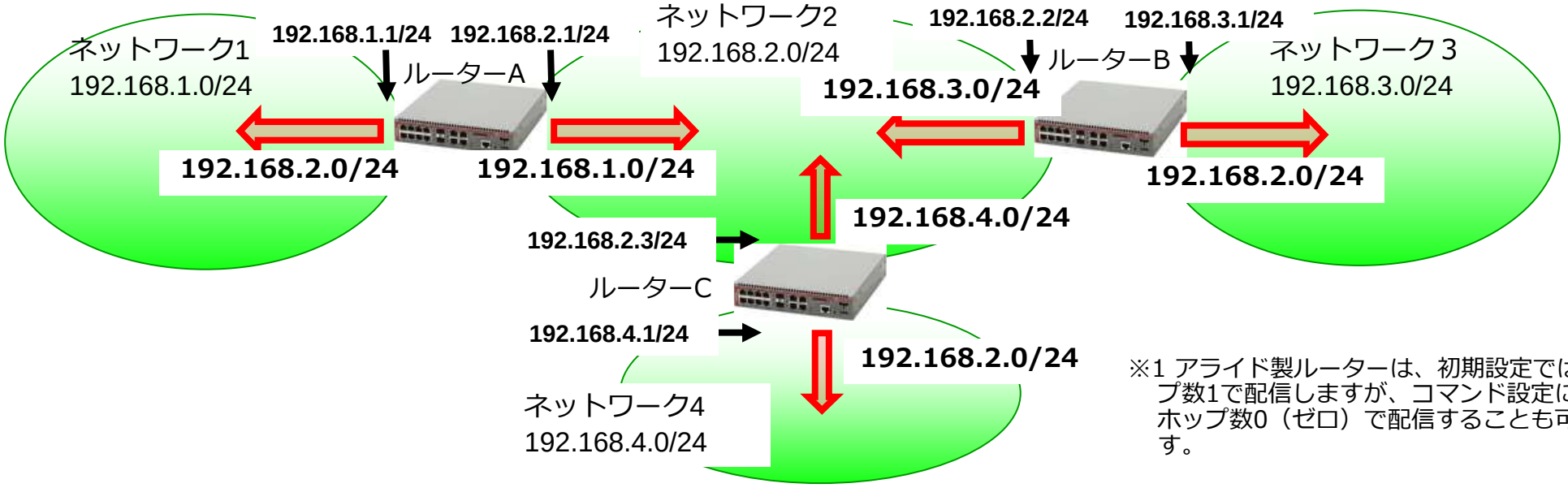
Network	Metric	NextHop
192.168.1.0/24	直接	無
192.168.2.0/24	直接	無
192.168.3.0/24	2	192.168.2.2
192.168.4.0/24	2	192.168.2.3

ルーターCのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.4.0/24	直接	無
192.168.1.0/24	2	192.168.2.1
192.168.3.0/24	2	192.168.2.2

ルーターBのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.3.0/24	直接	無
192.168.1.0/24	2	192.168.2.1
192.168.4.0/24	2	192.168.2.3



※1 アライド製ルーターは、初期設定ではホップ数1で配信しますが、コマンド設定によりホップ数0（ゼロ）で配信することも可能です。

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ルーティングテーブル作成の流れ（3）

- 各ルーターは、新しく登録した経路情報を追加して経路情報を配信します。RIPの各ルーターは隣接ルーターからの経路情報のみでルーティングテーブルを作成します。そのため、スプリットホライズンなどのルーティングループ防止機能があります。
  - スプリットホライズンとは、隣接ルーターから受信した経路情報は受信したインターフェースに送信しない機能です。

ルーターAのルーティングテーブル

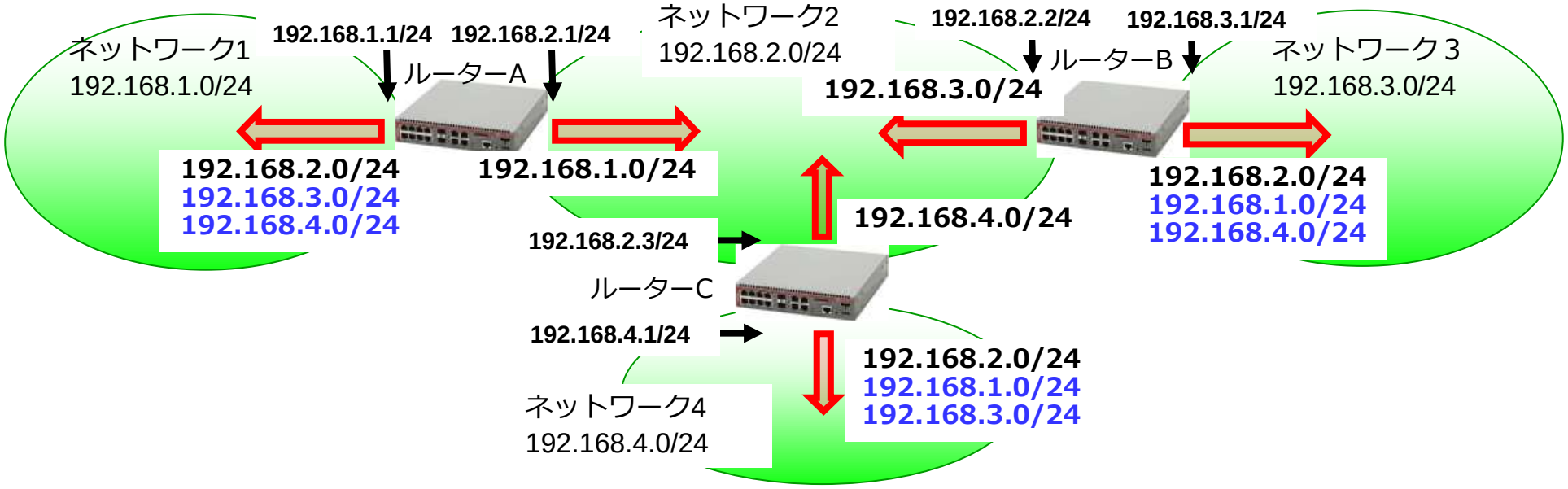
Network	Metric	NextHop
192.168.1.0/24	直接	無
192.168.2.0/24	直接	無
192.168.3.0/24	2	192.168.2.2
192.168.4.0/24	2	192.168.2.3

ルーターCのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.4.0/24	直接	無
192.168.1.0/24	2	192.168.2.1
192.168.3.0/24	2	192.168.2.2

ルーターBのルーティングテーブル

Network	Metric	NextHop
192.168.2.0/24	直接	無
192.168.3.0/24	直接	無
192.168.1.0/24	2	192.168.2.1
192.168.4.0/24	2	192.168.2.3



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

RIPルーティングテーブル（例）

- RIPのルーティングテーブルは以下になります。各項目の意味は以下の通りです。

R 10.10.10.0/24 172.17.10.2 3 172.17.10.2 vlan20 02:56

① ② ③ ④ ⑤ ⑥ ⑦

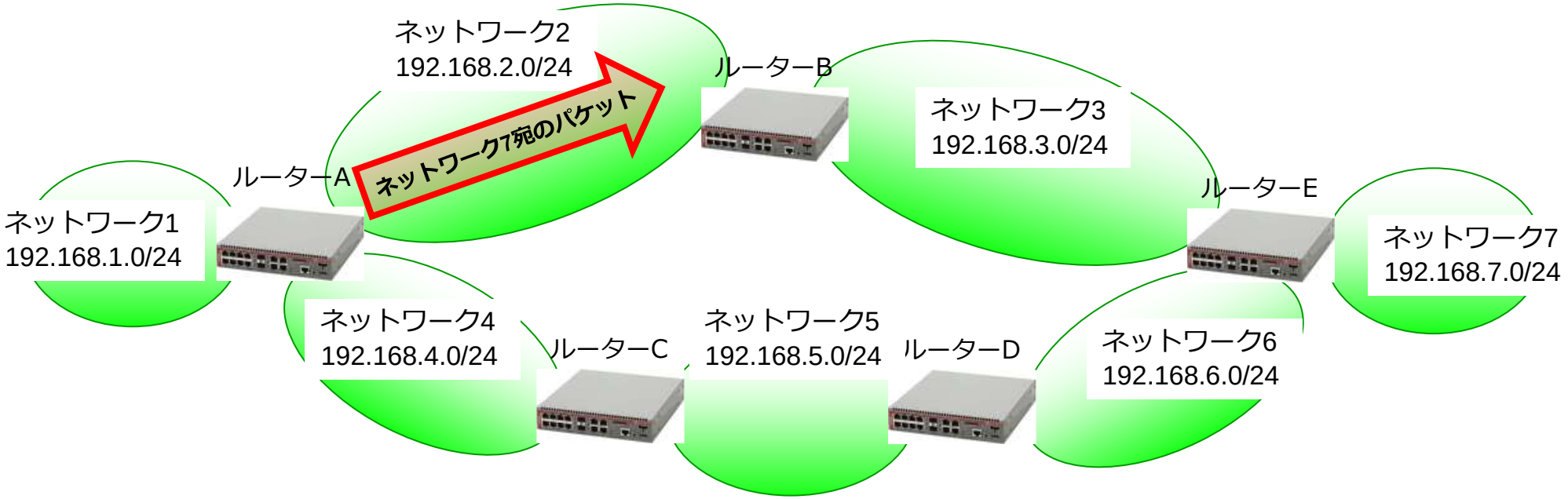
①経路情報の取得方法： RIPはRです。RcはRIPが動作している直接接続のネットワークアドレス
②ネットワークアドレス及びサブネットマスク長
③NextHop： 次に転送するルーターのアドレス
④Metric： RIPはホップ数
⑤経路情報を送ってきたネットワーク機器のIPアドレス
⑥出力インターフェース： パケットを出力するインターフェース
⑦経路情報が登録されてからの経過時間

```
awplus> show ip rip ↓

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

   Network          Next Hop        Metric From            If      Time
R  10.10.10.0/24    172.17.10.2          3 172.17.10.2     vlan20  02:56
R  10.10.20.0/24    192.168.10.2         4 192.168.10.2    vlan10  02:47
                    172.17.10.2          4 172.17.10.2     vlan20  02:56
R  172.16.10.0/24   192.168.10.3         2 192.168.10.3    vlan10  02:50
R  172.16.20.0/24   192.168.10.3         3 192.168.10.3    vlan10  02:50
Rc 172.17.10.0/24                        1                 vlan20
R  172.17.20.0/24   192.168.10.2         2 192.168.10.2    vlan10  02:47
R  172.17.30.0/24   172.17.10.2          2 172.17.10.2     vlan20  02:56
R  172.17.40.0/24   192.168.10.2         3 192.168.10.2    vlan10  02:47
                    172.17.10.2          3 172.17.10.2     vlan20  02:56
R  172.17.50.0/24   172.17.10.2          2 172.17.10.2     vlan20  02:56
Rc 192.168.10.0/24                       1                 vlan10
```

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

複数経路時の選択

- 目的ネットワークへの経路が複数存在する場合の判断基準は以下になります。
  - Metric（ホップ数）が異なる経路が複数存在する場合、Metricの小さい経路を選択（回線速度は考慮されない）
  - Metricが同じ経路が複数存在する場合はベンダー機器によって動作が異なります。RFC1058に準拠している機器では先に受信した経路情報を使用しますが、複数経路に交互にパケットを転送するベンダー機器もあります。
- 以下の図はルーターAから見て、ネットワーク7宛の経路が2つ存在します。この場合、ルーターAはネットワーク7宛のパケットをMetric(経由するルーターの数)が少ないネットワーク2の経路に転送します。



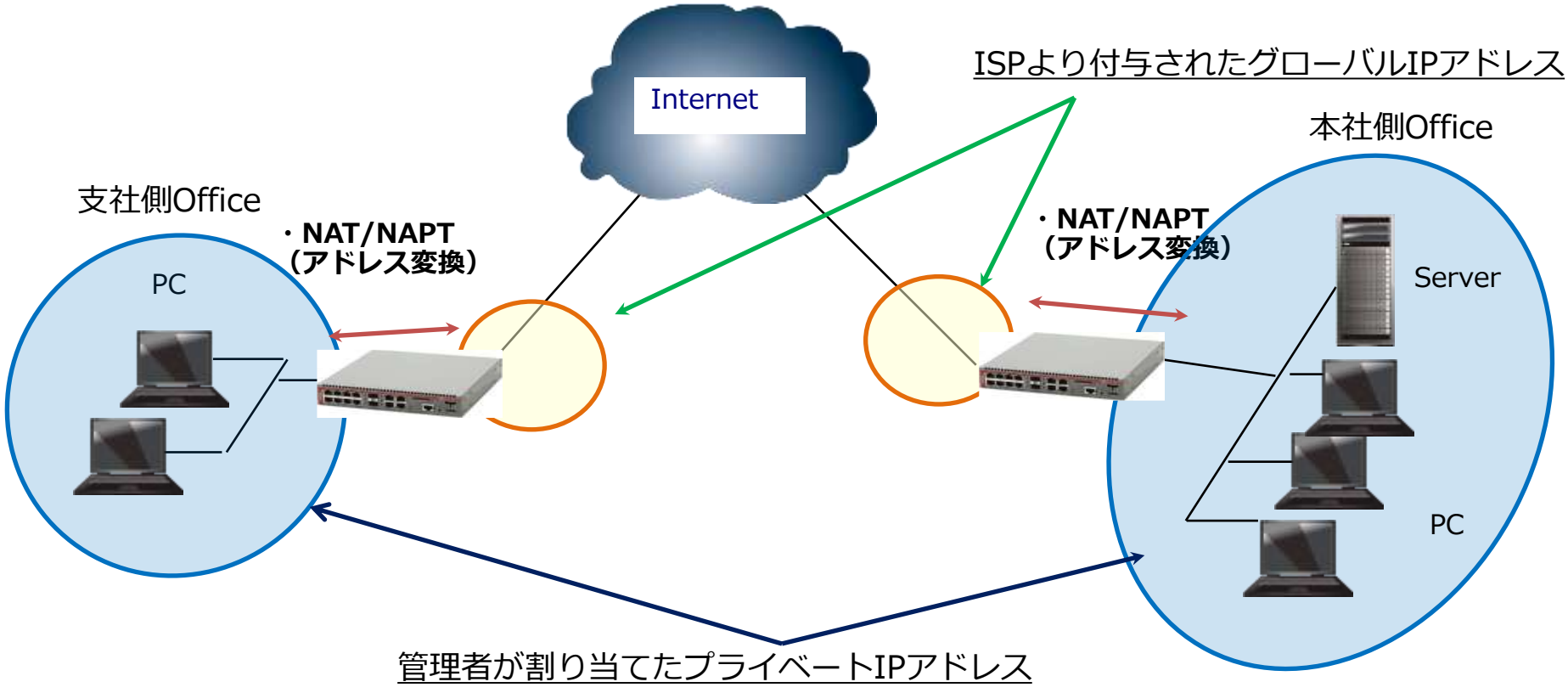
Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

③NAT

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

NAT(Network Address Translation)とは

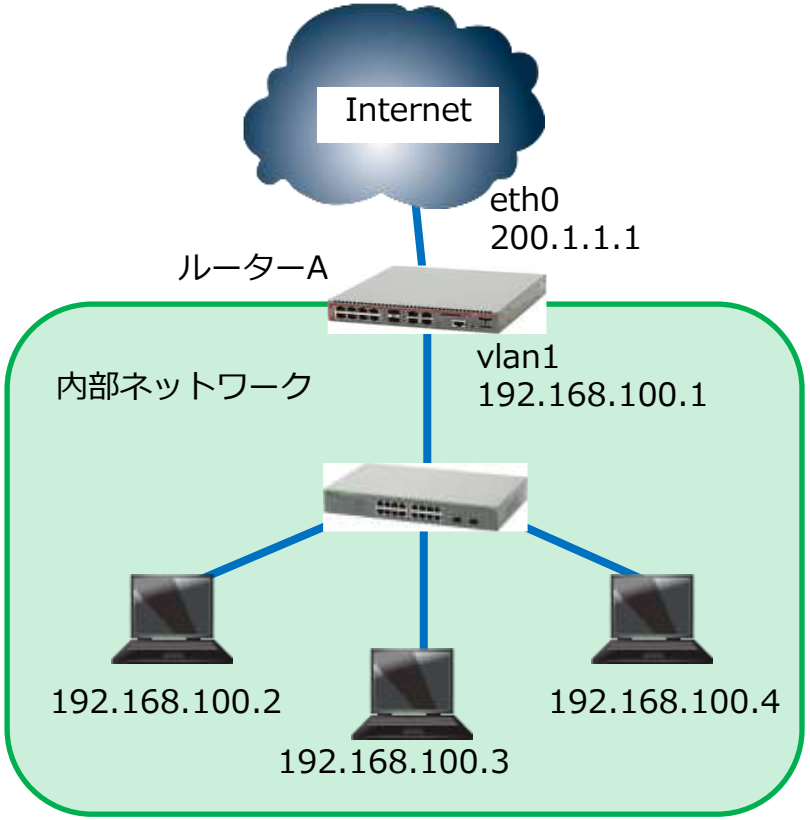
- 外部アドレス(グローバルIPアドレス)と内部アドレス(プライベートIPアドレス)のアドレス変換技術です。
- プライベートIPアドレスを使用している内部ネットワーク環境のホストから、インターネットのような外部ネットワークにアクセスするために利用します。
- 内部ネットワーク上のホストのIPアドレスを外部ネットワークに公開しないため、不正アクセスのリスクを低減するメリットもあります。



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

スタティックNAT

- プライベートIPアドレスとグローバルIPアドレスの1対1の変換を、ネットワーク管理者が手動設定で行います。
- 常にプライベートIPアドレスをグローバルIPアドレスに1対1で変換するため管理が容易というメリットはありますが、複数の端末から外部ホストに同時接続する場合は複数のグローバルIPアドレスが必要になるというデメリットあります。



管理が容易な半面、同時接続には
複数のグローバルIPアドレスが必要

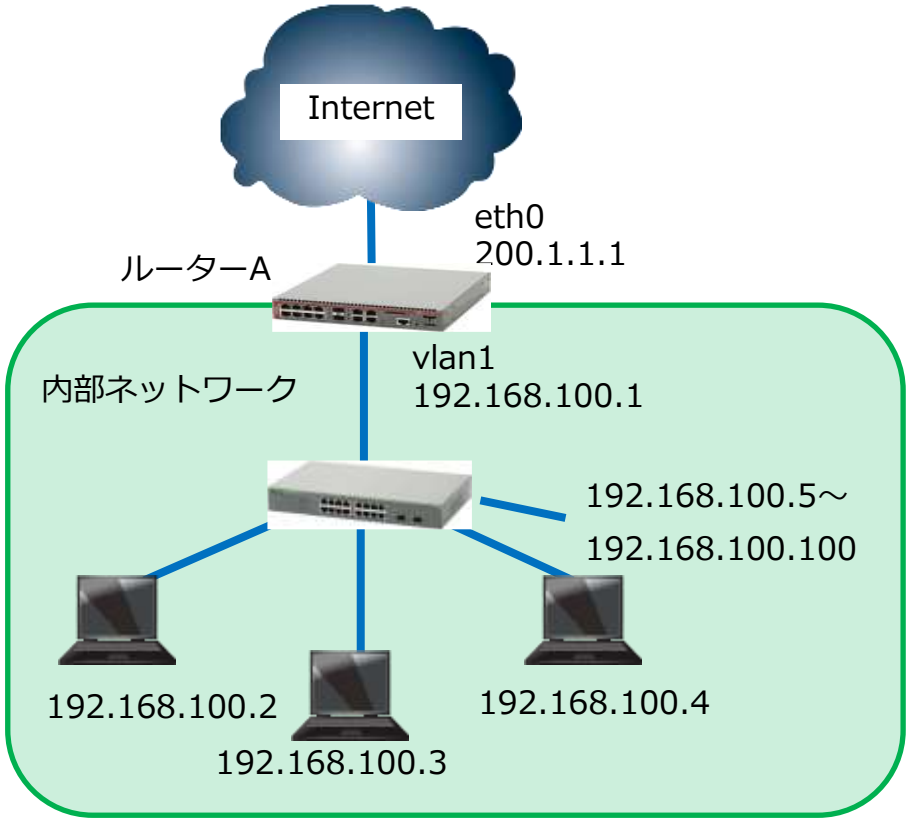
ルーターAのNATテーブル

プライベートIPアドレス	グローバルIPアドレス
192.168.100.2	200.1.1.2
192.168.100.3	200.1.1.3
192.168.100.4	200.1.1.4

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ダイナミックNAT

- 複数のプライベートIPアドレスから、複数のグローバルIPアドレスへの多対多の変換を行います。
- 予め「どの範囲のプライベートIPアドレスをどの範囲のグローバルIPアドレスに変換する」という設定を行うことで、ルーターは指定されたプライベートIPアドレスのホストから送られてきたパケットを、空いているグローバルIPアドレスに変換して外部ネットワークへ転送します。



内部アドレス遮蔽によるセキュリティ向上が期待できる
IPアドレスは固定されない

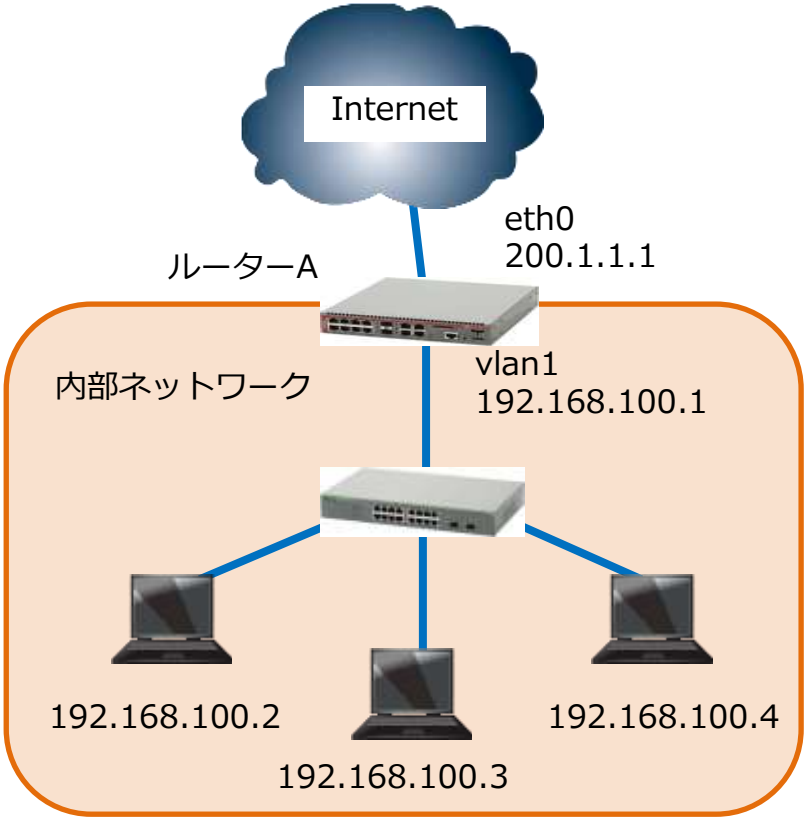
ルーターAのNATテーブル

プライベートIPアドレス	グローバルIPアドレス
（変換対象アドレス） 192.168.100.2 ～192.168.100.100	（変換先アドレス） 200.1.1.2 ～ 200.1.1.100

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

スタティックNAPT

- グローバルIPアドレス＋TCP/UDPポート番号とプライベートIPアドレス＋TCP/UDPポート番号の1対1の変換を、ネットワーク管理者が手動設定で行います。
- 端末数分のグローバルIPアドレスを用意する必要がないというメリットはありますが、ポートとIPアドレスの組み合わせを固定的に行うため、アプリケーションによっては対応できなかったり、ポートの衝突が発生しやすいというデメリットがあります。



ルーターAのNATテーブル

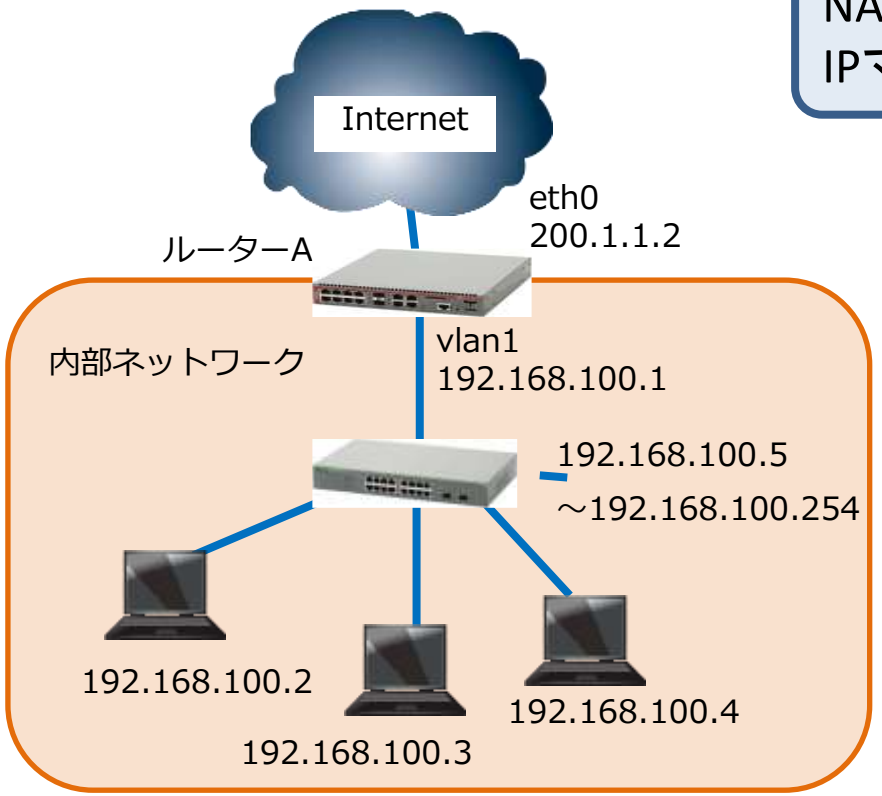
プライベートIPアドレス	ポート	グローバルIPアドレス	ポート
192.168.100.2	80	200.1.1.3	1200
192.168.100.3	21	200.1.1.3	1500
192.168.100.4	25	200.1.1.3	2010

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ダイナミックNAPT

- 複数のプライベートIPアドレス＋TCP/UDPポート番号から、1つのグローバルIPアドレス＋複数のTCP/UDPポート番号への変換を自動的に行います。
- ダイナミックNAPTは動的にプライベートIPアドレスのポート番号が変化することから、セキュリティ面で非常に有効なため、多くのブロードバンドルーターで利用されているアドレス変換方式となります。

NAPTは、NATオーバーロード、オーバーロード変換、IPマスカレードとも呼びます。



ルーターAのNATテーブル

プライベート IPアドレス	ポート	グローバル IPアドレス	ポート
192.168.100.2	1030	200.1.1.3	11030
192.168.100.3	1200	200.1.1.3	11200
192.168.100.4	1354	200.1.1.3	11354

※グローバルアドレス変換時のポートは
空きポートが割り当てられます。

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

④PPPoE

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

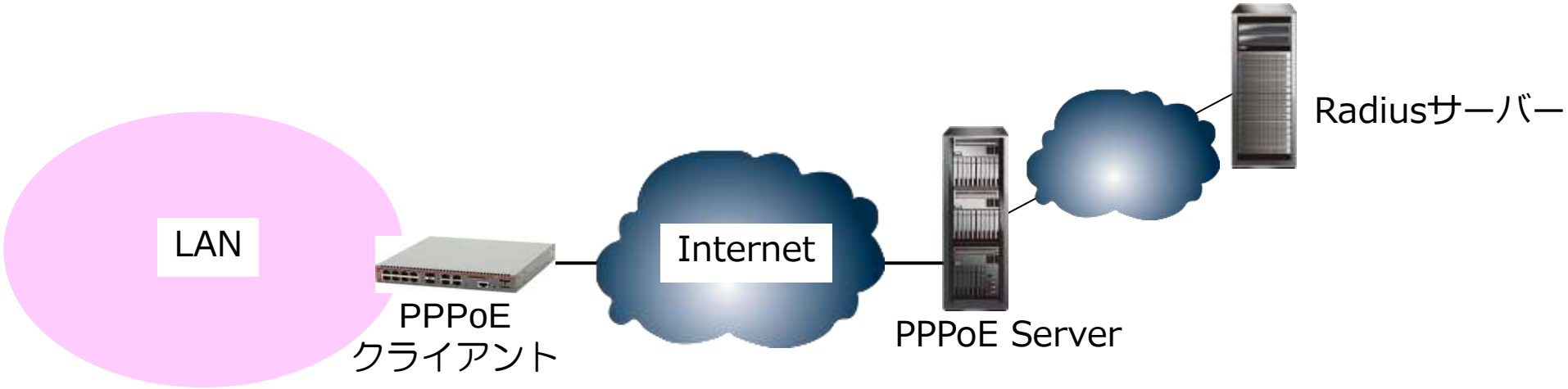
PPP(Point to Point Protocol)の概要

- PPPは、２点間で複数のプロトコルのデータを運ぶための手段で、いくつかのプロトコル群から構成されています。
  - LCP（Link Control Protocol）：LCPによってパスワード認証機能を提供して、リンクを確立します。
  - NCP（Network Control Protocol）：それぞれの通信プロトコルに必要な設定を行って接続を確立します。
- PPPのメリット
  - 複数のセッションを並行して確立できる
  - セッション単位の課金ができる（RADIUS Server等が必要）
  - 認証の仕組みが簡単で、ユーザー名とパスワードによるシンプルな認証方式
  - セッション単位での認証、暗号化と圧縮が可能
  - ネットワーク層プロトコルに依存しない。TCP/IP以外の通信プロトコルも利用できる
  - 標準化されているので、様々なベンダー機器で利用が可能（RFC1661で標準化）

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

PPPoE(PPP over Ethernet)の機能

- PPPoEとは、イーサネットフレーム上にPPPをカプセル化する通信プロトコルで、RFC2516で定義されています。
- PPPの持つ認証機能が利用できますし、複数回線との同時接続も可能（マルチセッション）です。
- PPPoE使用時の注意点
  - PPPoEクライアントの明確化：最近ではルーターを利用することが主流
  - 認証におけるユーザー名とパスワードの設定
  - パケットサイズの設定（MTU）
  - 最低限のファイアウォール、ウイルス対策ソフトを導入してから接続する

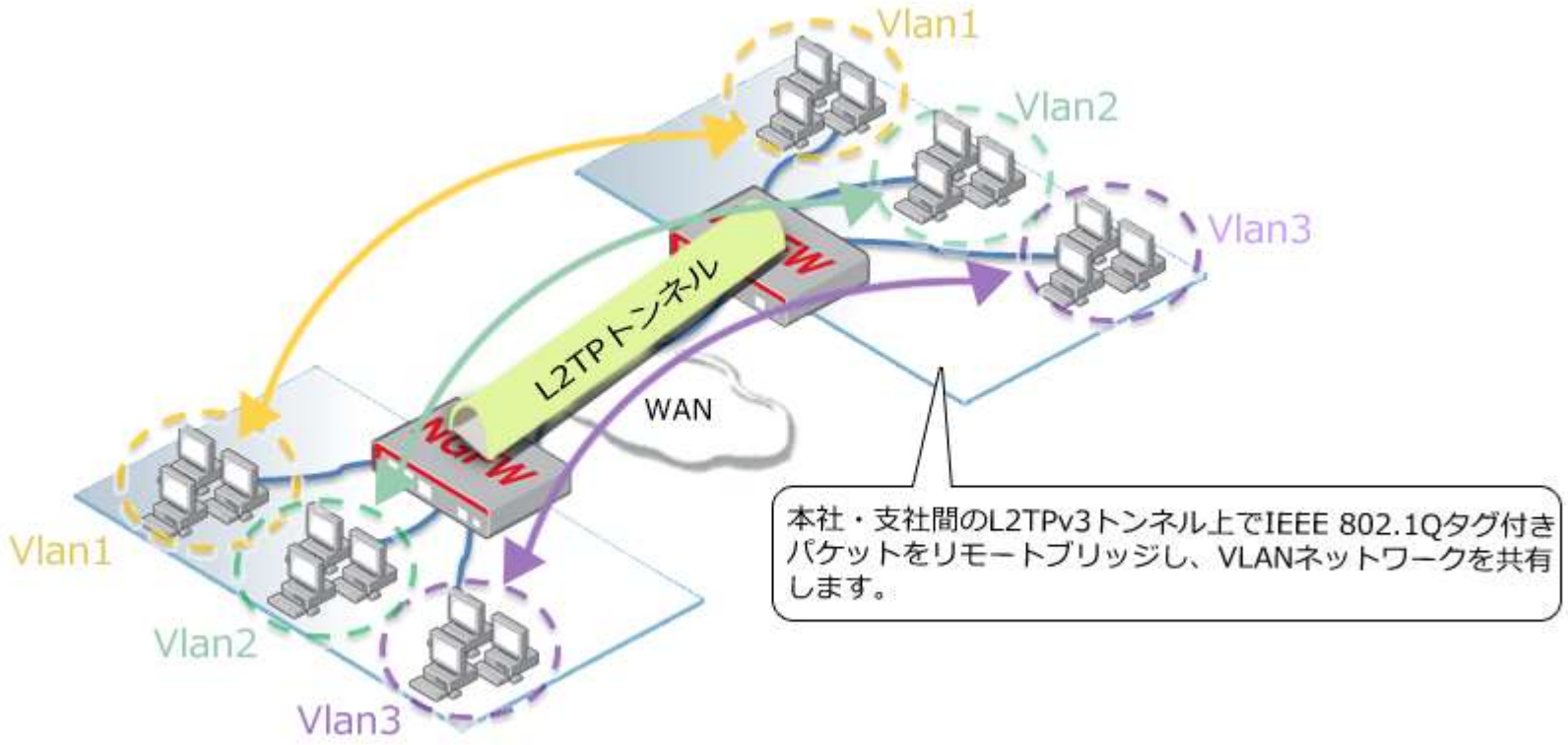


Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

PPPoEの用途

- PPPoEは、接続先との接続開始時にユーザー認証を行うことが可能なため、インターネット接続サービスに利用されます。（PPPoEの利用無しでEthernetを直接インターネットに接続することも可能です（IPoE）。）
- 企業においては、VPNのプロトコル（トンネリングプロトコル）と連携して拠点間を接続する際に利用することが可能です。

※VPNについては「ルーター応用セミナー」で説明しています。



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

⑤設定・管理機能

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

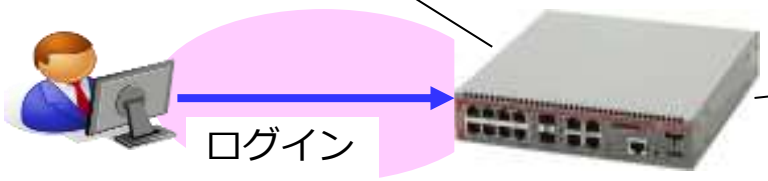
設定方法

- ルーターの設定方法には、「コンソール接続やtelnet接続によるコマンド(CLI)での設定」と「WebGUIインターフェースによるブラウザ画面での設定」があります。
- 基本的な設定はWebGUIインターフェースで行えますが、詳細な機能の場合はコマンド設定が必要になります。

【コマンド(CLI)によるIPアドレス設定】

```
awplus(config)# interface vlan10
awplus(config-if)# ip address 192.168.10.1/24
awplus(config-if)# ip address 192.168.11.1/24 secondary
awplus(config-if)# ip address 192.168.12.1/24 secondary
```

【WebGUIによるインターフェース設定画面】



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

AMFマスター機能

- ルーター「AT-AR4050S」は、AMFマスターライセンスの導入によりAMFマスター機能が利用できるようになり、xシリーズスイッチ（AMFメンバー）を最大20メンバー管理できます。リモートサイトの統合管理や小規模オフィスに最適です。
- 以下はAMFマスターが管理しているAMF機器の一覧になります。

AT-AR4050S

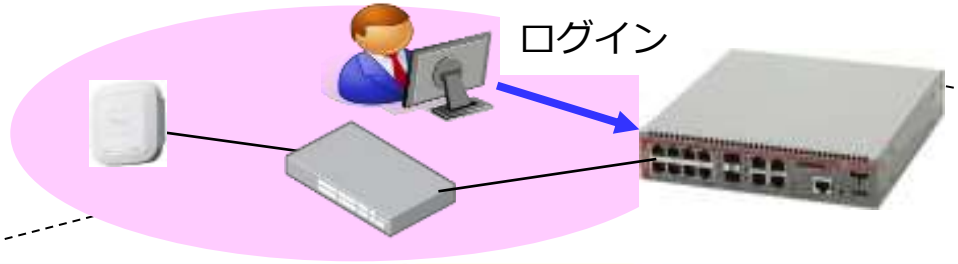
【AMFノード管理】

```
SBx81# show atmf nodes

Node Information:

  * = Local device

 SC = Switch Configuration:
  C = Chassis    S = Stackable    N = Standalone

  Node                 Device             ATMF                          Node
  Name                 Type               Master  SC  Parent            Depth
-------------------------------------------------------------------------------
* SBx81                AT-SBx81CFC960       Y     C   none               0
  FSW242               x510-28GTX           N     S   SBx81              1
  FSW241               x510-28GTX           N     S   SBx81              1
  ESW231               x510-52GTX           N     S   FSW242             2

 Current ATMF node count 4
```

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

無線コントローラー機能

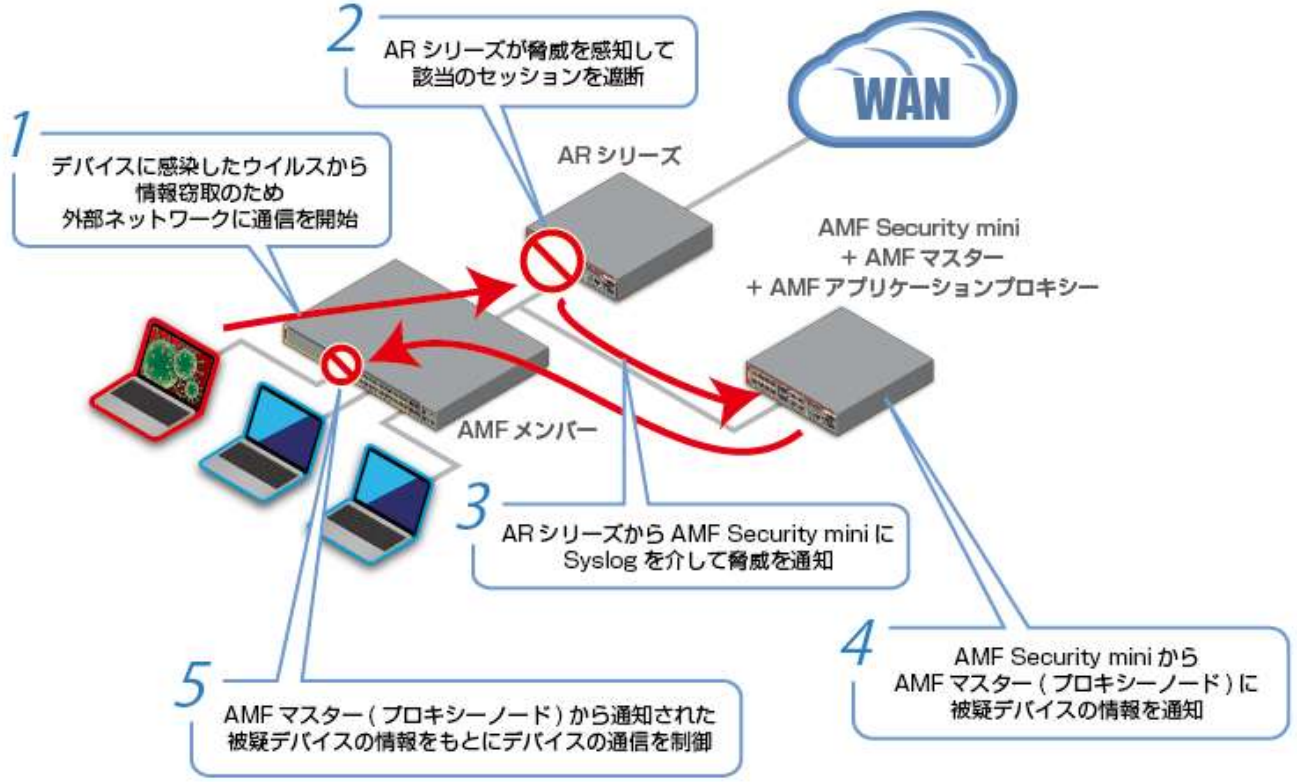
- ルーター「AT-AR4050S、AT-AR3050S、AT-AR2050V、AT-AR2010V」は無線コントローラー機能を持ち、標準5台の無線アクセスポイントを管理可能です。なおAT-AR4050Sは、ライセンスの追加により最大25台まで無線アクセスポイントを管理できます。
- 小規模オフィスでも容易に無線コントローラーを導入でき、外来波による影響を最小限にとどめ、最適な無線LANネットワークを維持します。
- 以下は、ルーターが管理している無線アクセスポイントの一覧画面です。



Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

AMF-SECコントローラー機能

- ルーター「AT-AR4050S」は、AMF-SECurityコントローラーminiライセンスの導入によりAMF-SECコントローラーとして動作します。これにより、AT-AR4050S 1台でAMF-SECコントローラー機能とAMFマスター機能を提供します。※1
- AMF-SECurityは、セキュリティ・IT資産管理・人事などのアプリケーションをAMF-SECコントローラーと連携させることで、セキュリティリスクのある端末を自動で隔離する機能です。



※1 AMFマスターとして動作するためにはAMFマスターライセンスが必要です。また、UTM関連機能（ファイアウォールとNATは除く）とは併用不可となります。
なお、ルーターのAMF-SECコントローラー機能はOpenFlowに対応していないため、OpenFlowによる制御はできません。

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

⑥製品紹介

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.

ご清聴ありがとうございました。

Allied Telesis

今回ご紹介しましたネットワーク製品に関して、
別途個別に相談がございましたら、お気軽に弊社
営業までお問い合わせください。

Copyright© 2022 Allied Telesis K.K. All Rights Reserved.