P3NK-3352-04Z0

Fujitsu Network Si-R
Si-R brinシリーズ

コマンド設定事例集　V2

FUJITSU

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

2009年 2月初版
2014 年 3月第2版
2016年12月第3版
2023年 5月第4版

目次

はじめに 2
本書の構成と使いかた 6
本書の読者と前提知識 6
本書の構成 6
本書における商標の表記について 7
本装置のマニュアルの構成 8

第 1 章 導入例 9

1.1 プライベート LAN を構築する 10
1.2 CATV インターネットに接続する 13
1.3 LAN をネットワーク間接続する 15
1.4 IPv4 のネットワークに IPv6 ネットワークを追加する 17
1.5 インターネットへ PPPoE で接続する 18
1.6 複数の事業所 LAN を IP-VPN 網を利用して接続する 20
1.6.1 ADSL モデムを使用して IP-VPN 網と接続する 20
1.7 複数の事業所 LAN を VPN（IPsec）で接続する 24
1.7.1 NAT と併用しない固定 IP アドレスでの VPN（自動鍵交換） 24
1.7.2 NAT と併用した固定 IP アドレスでの VPN（自動鍵交換） 29
1.7.3 NAT と併用した可変 IP アドレスでの VPN（自動鍵交換） 34
1.8 IPv6 の事業所 LAN を IPv4 トンネルで接続する 40

第 2 章 活用例 44

2.1 RIP の経路を制御する（IPv4） 47
2.1.1 特定の経路情報の送信を許可する 49
2.1.2 特定の経路情報のメトリック値を変更して送信する 50
2.1.3 特定の経路情報の受信を許可する 51
2.1.4 特定の経路情報のメトリック値を変更して受信する 52
2.1.5 特定の経路情報の送信を禁止する 53
2.1.6 特定の経路情報の受信を禁止する 54
2.2 RIP の経路を制御する（IPv6） 55
2.2.1 特定の経路情報の送信を許可する 57
2.2.2 特定の経路情報のメトリック値を変更して送信する 58
2.2.3 特定の経路情報の受信を許可する 59
2.2.4 特定の経路情報のメトリック値を変更して受信する 60
2.2.5 特定の経路情報の送信を禁止する 61
2.2.6 特定の経路情報の受信を禁止する 62
2.3 OSPFv2 を使用したネットワークを構築する（IPv4） 63
2.3.1 バーチャルリンクを使う 67
2.3.2 スタブエリアを使う 71
2.4 OSPF の経路を制御する（IPv4） 74
2.4.1 OSPF ネットワークでエリアの経路情報（LSA）を集約する 74
2.4.2 AS 外部経路を集約して OSPF ネットワークに広報する 75
2.4.3 エリア境界ルータで不要な経路情報（LSA）を遮断する 77
2.5 BGP の経路を制御する（IPv4） 78
2.5.1 特定の経路情報の受信を透過させる 78
2.5.2 特定の AS からの経路情報の受信を遮断する 79
2.5.3 IP-VPN 網からの受信情報の他 IP-VPN 網への送信を遮断する 80
2.5.4 冗長構成の通信経路を使用する 81

2.6 マルチキャスト機能を使う 83
2.6.1 マルチキャスト機能（PIM-DM）を使う 83
2.6.2 マルチキャスト機能（PIM-SM）を使う 87
2.6.3 マルチキャスト機能（スタティックルーティング）を使う 93
2.7 VLAN 機能を使う 96
2.8 IP フィルタリング機能を使う 98
2.8.1 外部の特定サービスへのアクセスだけを許可する 102
2.8.2 外部から特定サーバへのアクセスだけを許可する 106
2.8.3 外部から特定サーバへのアクセスだけを許可して SPI を併用する 110
2.8.4 外部の特定サービスへのアクセスだけを許可する（IPv6 フィルタリング） 114
2.8.5 外部の特定サーバへのアクセスだけを禁止する 118
2.8.6 利用者が意図しない発信を防ぐ 120
2.8.7 回線が接続しているときだけを許可する 121
2.8.8 外部から特定サーバへの ping だけを禁止する 122
2.9 IPsec 機能を使う 124
2.9.1 IPv4 over IPv4 で固定 IP アドレスでの VPN（手動鍵交換） 129
2.9.2 IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換） 133
2.9.3 IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換） 137
2.9.4 IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換） 141
2.9.5 IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換） 145
2.9.6 IPv4 over IPv4 で 1 つの IKE セッションに複数の IPsec トンネル構成での VPN（自動鍵交換） 149
2.9.7 IPsec 機能と他機能との併用 153
2.9.8 テンプレート着信機能（AAA 認証）を使用した固定 IP アドレスでの VPN 158
2.9.9 テンプレート着信機能（AAA 認証）を使用した可変 IP アドレスでの VPN 162
2.9.10 テンプレート着信機能（RADIUS 認証）を使用した固定 IP アドレスでの VPN 167
2.9.11 テンプレート着信機能（RADIUS 認証）を使用した可変 IP アドレスでの VPN 172
2.9.12 テンプレート着信機能（動的 VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN 177
2.9.13 テンプレート着信機能（動的 VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN（冗長構成） 186
2.9.14 テンプレート着信機能（動的 VPN）を使用した IPv6 over IPv6 で固定 IP アドレスでの VPN 189
2.9.15 NAT トラバーサルを使用した可変 IP アドレスでの VPN 198
2.9.16 テンプレート着信機能（AAA 認証）および NAT トラバーサルを使用した可変 IP アドレスでの VPN 202
2.9.17 接続先情報（動的 VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN 206
2.10 システムログを採取する 217
2.11 マルチ NAT 機能（アドレス変換機能）を使う 219
2.11.1 プライベート LAN 接続でサーバを公開する 220
2.11.2 PPPoE 接続でサーバを公開する 221
2.11.3 サーバ以外のアドレス変換をしないで、プライベート LAN 接続でサーバを公開する 223
2.11.4 複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する 224
2.11.5 NAT あて先変換で双方向のアドレスを変換する 225
2.11.6 NAT 変換テーブル数を拡張する 226
2.12 VoIP NAT トラバーサル機能を使う 227
2.13 TOS/Traffic Class 値書き換え機能を使う 229
2.14 VLAN プライオリティマッピング機能を使う 231
2.15 シェーピング機能を使う 232
2.15.1 特定のインタフェースでシェーピング機能を使う 232
2.15.2 送信先ごとにシェーピング機能を使う 233
2.16 ヘッダ圧縮機能を使う 234
2.17 帯域制御（WFQ）機能を使う 235

2.18 DHCP 機能を使う 237
2.18.1 DHCP サーバ機能を使う 238
2.18.2 DHCP スタティック機能を使う 240
2.18.3 DHCP クライアント機能を使う 242
2.18.4 DHCP リレーエージェント機能を使う 243
2.18.5 IPv6 DHCP クライアント機能を使う 244
2.18.6 IPv6 DHCP サーバ機能を使う 246
2.18.7 IPv6 DHCP クライアント機能で取得した情報を IPv6 DHCP サーバ機能で配布する 248
2.19 DNS サーバ機能を使う（ProxyDNS） 250
2.19.1 DNS サーバの自動切り替え機能（順引き）を使う 250
2.19.2 DNS サーバの自動切り替え機能（逆引き）を使う 252
2.19.3 DNS サーバアドレスの自動取得機能を使う 253
2.19.4 DNS サーバアドレスを DHCP サーバから取得して使う 255
2.19.5 DNS 問い合わせタイプフィルタ機能を使う 257
2.19.6 DNS サーバ機能を使う 258
2.20 特定の URL へのアクセスを禁止する（URL フィルタ機能） 259
2.21 SNMP エージェント機能を使う 261
2.22 ECMP 機能を使う 264
2.23 VRRP 機能を使う 269
2.23.1 簡易ホットスタンバイ機能を使う 270
2.23.2 クラスタリング機能を使う 273
2.24 遠隔地のパソコンを起動させる（リモートパワーオン機能） 276
2.24.1 リモートパワーオン情報を設定する 277
2.24.2 リモートパワーオン機能を使う 277
2.25 スケジュール機能を使う 278
2.25.1 スケジュールを予約する 278
2.25.2 構成定義情報の切り替えを予約する 279
2.26 ブリッジ／ STP 機能を使う 280
2.26.1 ブリッジで FNA をつないで STP 機能を使う 280
2.26.2 IP トンネルで事業所間をブリッジ接続する（Ethernet over IP ブリッジ） 282
2.27 スイッチポートを使う 285
2.27.1 スイッチポートを HUB として使用する 286
2.27.2 スイッチポートを単独ポートとして使用する（Si-R80brin） 288
2.28 アプリケーションフィルタ機能を使う 289
2.29 不正端末アクセス防止機能（MAC アドレス認証）を使う 291
2.30 装置を保護する 294
2.30.1 設定例 294
索引 296

本書の構成と使いかた

本書では、ネットワークを構築するために、代表的な接続形態や本装置の機能を活用した接続形態について説明しています。

また、CD-ROMの中のREADMEファイルには大切な情報が記載されていますので、併せてお読みください。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

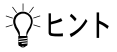
本書の構成

以下に、本書の構成と各章の内容を示します。

章タイトル	内　容
第1章　導入例	この章では、本装置の代表的な接続形態を紹介します。
第2章　活用例	この章では、本装置の便利な機能の活用方法について説明します。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。



本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。

こんな事に気をつけて　本装置をご使用になる際に、注意していただきたいことを説明しています。

操作手順で説明しているもののほかに、補足情報を説明しています。

操作方法など関連事項を説明している箇所を示します。

製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。

製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

設定例の記述について

設定はSi-R80brinを例に記述しています。

Si-R90brinの場合は、説明の中で物理ポートを指す“LAN1ポート”といった記述は“SW1ポート”へ読み替えてください。

コマンド例ではconfigureコマンドを実行して、構成定義モードに入ったあとのコマンドを記述しています。

また、プロンプトは設定や機種によって変化するため、“#”に統一しています。

マニュアル「コマンドユーザーズガイド」

本書における商標の表記について

Microsoft、Windows、Windows NT、Windows Server およびWindows Vista は、米国Microsoft Corporation の米国およびその他の国における登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

なお、本文中では®を省略しています。

製品名称	本文中の表記
Microsoft® Windows® XP Professional operating system	Windows XP
Microsoft® Windows® XP Home Edition operating system	
Microsoft® Windows® 2000 Server Network operating system	Windows 2000
Microsoft® Windows® 2000 Professional operating system	
Microsoft® Windows NT® Server network operating system Version 4.0	Windows NT 4.0
Microsoft® Windows NT® Workstation operating system Version 4.0	
Microsoft® Windows Server® 2003, Standard Edition	Windows Server 2003
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise Edition	
Microsoft® Windows Server® 2003 R2, Enterprise Edition	
Microsoft® Windows Server® 2003, Datacenter Edition	
Microsoft® Windows Server® 2003 R2, Datacenter Edition	
Microsoft® Windows Server® 2003, Web Edition	
Microsoft® Windows Server® 2003, Standard x64 Edition	
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise x64 Edition	
Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based systems	
Microsoft® Windows Server® 2003, Datacenter x64 Edition	
Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition	
Microsoft® Windows Vista® Ultimate operating system	Windows Vista
Microsoft® Windows Vista® Business operating system	
Microsoft® Windows Vista® Home Premium operating system	
Microsoft® Windows Vista® Home Basic operating system	
Microsoft® Windows Vista® Enterprise operating system	
Microsoft® Windows® 7 64bit Home Premium	Windows 7
Microsoft® Windows® 7 32bit Professional	

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
Si-R効率化運用ツール使用手引書	Si-R効率化運用ツールを使用する方法を説明しています。
Si-R80brin　ご利用にあたって	Si-R80brinの設置方法やソフトウェアのインストール方法を説明しています。
Si-R90brin　ご利用にあたって	Si-R90brinの設置方法やソフトウェアのインストール方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様とMIB/Trap一覧を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンド設定事例集（本書）	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
コマンドリファレンス-構成定義編-	構成定義コマンドの項目やパラメタの詳細な情報を説明しています。
コマンドリファレンス-運用管理編-	運用管理コマンド、その他のコマンドの項目やパラメタの詳細な情報を説明しています。
Webユーザーズガイド	Web画面を使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
Web設定事例集	Web画面を使用した、基本的な接続形態または機能の活用方法を説明しています。
Webリファレンス	Web画面の項目の詳細な情報を説明しています。

第1章　導入例

この章では、本装置の代表的な接続形態を紹介します。

1.1　プライベートLANを構築する 10
1.2　CATVインターネットに接続する 13
1.3　LANをネットワーク間接続する 15
1.4　IPv4のネットワークにIPv6ネットワークを追加する 17
1.5　インターネットへPPPoEで接続する 18
1.6　複数の事業所LANをIP-VPN網を利用して接続する 20
1.6.1　ADSLモデムを使用してIP-VPN網と接続する 20
1.7　複数の事業所LANをVPN（IPsec）で接続する 24
1.7.1　NATと併用しない固定IPアドレスでのVPN（自動鍵交換） 24
1.7.2　NATと併用した固定IPアドレスでのVPN（自動鍵交換） 29
1.7.3　NATと併用した可変IPアドレスでのVPN（自動鍵交換） 34
1.8　IPv6の事業所LANをIPv4トンネルで接続する 40

1.1　プライベートLANを構築する

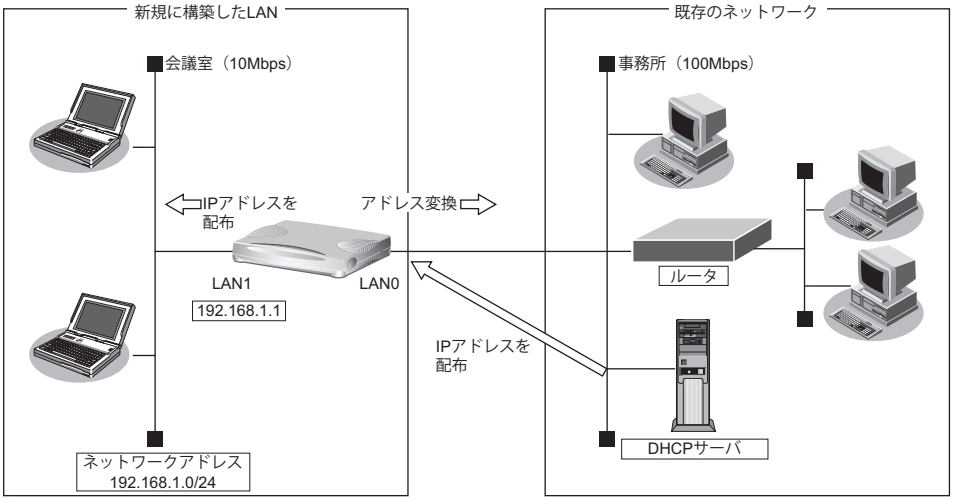
プライベートLANでは、マルチNAT機能を使用することで、割り当てられた1つのグローバルアドレスを使って、複数台のパソコンからネットワークにアクセスすることができます。

また、DHCPサーバ機能が動作しているため、パソコンのIPアドレス管理が必要ありません。そのため、簡単にLANを構築することができます。

ここでは、以下の条件で会議室LANを一時的に構築し、事務所ネットワークと接続する場合を例に説明します。

本装置のIPアドレスを変更しない場合

本装置がご購入時の状態の場合、本装置の電源を投入するだけで通信できます。



● 設定条件

[事務所側]

- 転送レートは自動認識
- IPアドレスはDHCPサーバから自動的に取得する

[会議室側]

- 転送レートは自動認識
- 本装置のIPアドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24

[その他の条件]

- パスワードを設定する
  パスワード　：himitu

☛参照 マニュアル「コマンドユーザーズガイド」

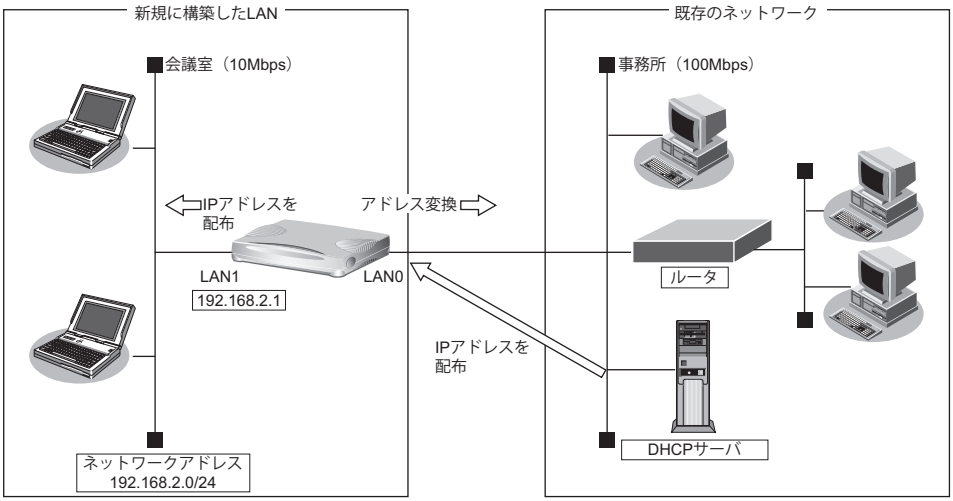
こんな事に気をつけて

- パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。
- 「プライベートLAN構築」でDHCPサーバを使用すると設定した場合は、DHCPサーバが広報する情報（デフォルトルータ、DNSサーバ、ドメイン名）に、DHCPサーバが動作するインタフェース側のネットワーク構成に応じた情報を設定してください。
- スイッチポート（SW1～4）を利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

本装置のIPアドレスを変更する場合

「プライベートLAN構築」では、プライベートLAN側のネットワークアドレスを変更することができます。

以下に、プライベートLAN側（LAN1側）のネットワークアドレスを192.168.2.0/24に変更する手順を示します。



こんな事に気をつけて

- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

  参照 マニュアル「コマンドユーザーズガイド」

- 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

● 設定条件

[プライベート側ネットワーク]

- IPアドレス　：192.168.2.1
- ネットマスク　：24
- DHCPサーバ　：192.168.2.1
- デフォルトルータ広報　：192.168.2.1

● コマンド

```
プライベート側LAN情報を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info address 192.168.2.2/24 253
# lan 1 ip dhcp info gateway 192.168.2.1

設定終了
# save

再起動
# reset
```

こんな事に気をつけて

- 本装置のIPアドレスを変更した場合、以下に示す２つの操作が必要です。
  - 本装置に接続しているパソコンのIPアドレスも変わります。再度、DHCPサーバから割り当ててもらう必要があります。
  - 再起動後に本装置にアクセスするためには、telnetで指定するIPアドレスに変更後のIPアドレスを指定する必要があります。
- 本装置に接続するネットワーク上のパソコンは、IPアドレスを自動的に取得する設定にしてください。IPアドレスを固定的に設定していると、本装置が配布するIPアドレスと重なり、矛盾が生じる場合があります。なお、常時同じIPアドレスを取得する場合は、「2.18.2 DHCPスタティック機能を使う」（P.240）でIPアドレスとMACアドレスを設定してください。
- ご購入時は、LAN1ポートからだけ設定できます。

1.2　CATVインターネットに接続する

CATVインターネット接続とは、CATV事業者が提供するインターネット接続サービスです。CATVインターネット接続には、ケーブルモデム接続とダイヤルアップ接続の２つの接続形態があります。ケーブルモデム接続は、ケーブルテレビ網を利用したもので、CATV事業者が提供するケーブルモデムに接続する形態です。ダイヤルアップ接続とは、CATV電話サービスを利用したもので、パソコンにモデムを接続する形態です。本装置を使用してCATVインターネット接続する場合は、「ケーブルモデム接続」の形態となり、CATV事業者との契約が必要です。接続にあたっては、CATV事業者の指示に従ってください。

ヒント

◆ ケーブルモデムとは？

ケーブルテレビ網に接続するための専用モデムで、CATVインターネット接続サービスに必要な機器です。パソコン（LANボード）とはLANケーブルで接続します。通常、CATVサービス加入時にCATV事業者より貸し出され、宅内工事の際に設置されます。

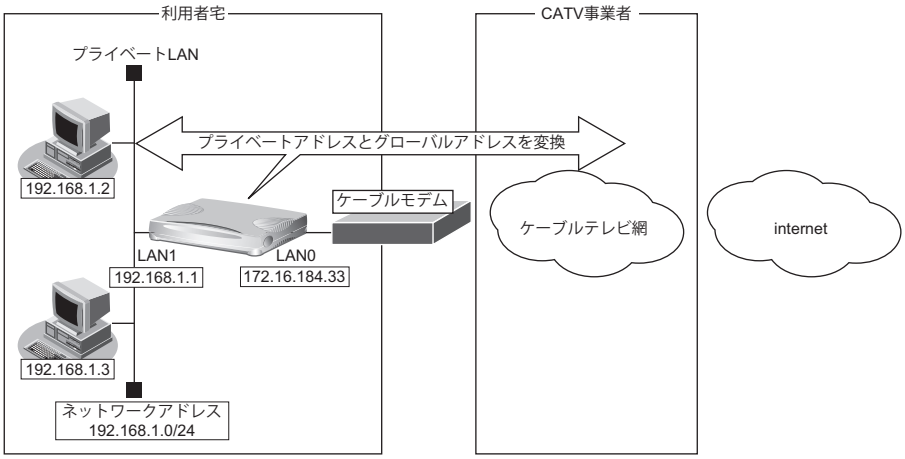
本装置を使ったCATVインターネット接続は、CATV事業者が提供するインターネット接続サービスをプライベートLAN上の複数のパソコンから利用するための接続形態です。本装置とCATV事業者が提供するケーブルモデムを接続することで、プライベートLAN上のパソコンからインターネット接続サービスを利用できます。

本装置のアドレス変換機能がCATV事業者側のネットワークと利用者側のプライベートLANとの間で動作し、プライベートLAN側のIPアドレスを外部から隠すため、セキュリティが確保できます。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照　マニュアル「トラブルシューティング」



● 設定条件

[CATV事業者側]

- LAN0ポートを使用する
- IPアドレス　：172.16.184.33
- ネットワークアドレス／ネットマスク　：172.16.184.0/24
- デフォルトルータ　：172.16.184.100
- DNSサーバ　：192.10.10.10

[プライベートLAN側]

- IPアドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24
- DHCPサーバ機能を使用する

こんな事に気をつけて

- 契約したCATV事業者によって設定方法が異なります。実際の設定は、CATV事業者の指示に従ってください。
- 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- スイッチポートを利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

● コマンド

```
CATV事業者側を設定する
# delete lan
# lan 0 ip address 172.16.184.33/24 3
# lan 0 ip dhcp info time 1d
# lan 0 ip route 0 default 172.16.184.100 1 0
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1 5m

プライベートLAN側を設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.10.10.10
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off

ProxyDNSを設定する
# proxydns domain 0 any * any static 192.10.10.10
# proxydns address 0 any static 192.10.10.10

設定終了
# save

再起動
# reset
```

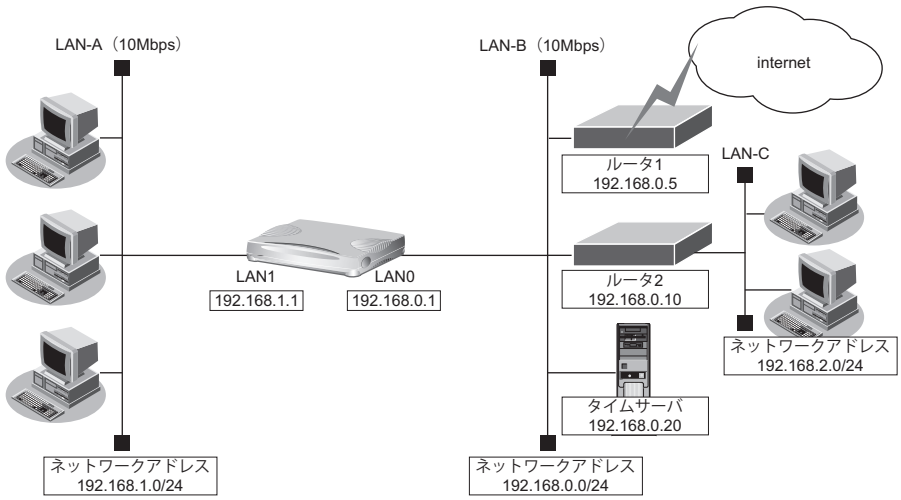
1.3　LANをネットワーク間接続する

ここでは、既存のLAN-Bに新規のLAN-Aをネットワーク間接続し、静的に経路情報を設定する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛参照　マニュアル「トラブルシューティング」



● 設定条件

[LAN-A側]

- 転送レートは自動認識
- 本装置のLAN1側のIPアドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24
- DHCP機能を使用する
- NATを使用しない

[LAN-B側]

- 転送レートは自動認識
- 本装置のLAN0側のIPアドレス　：192.168.0.1
- ネットワークアドレス／ネットマスク　：192.168.0.0/24
- DHCP機能を使用しない
- ルーティングプロトコルとしてRIP-V1を使用する
- インターネットにつながるルータ１と、事業所内のその他のネットワークにつながるルータ２が存在し、静的に経路情報を登録する
  ルータ１のIPアドレス　：192.168.0.5
  ルータ２のIPアドレス　：192.168.0.10
- LAN-Cのネットワークアドレス／ネットマスク　：192.168.2.0/24
- NATは使用しない

[その他の条件]

- 自動時刻設定にする

タイムサーバ	：使用する
サーバ設定	：設定する
プロトコル	：TIME プロトコル
タイムサーバのアドレス	：192.168.0.20

ヒント

◆ TIME プロトコル、SNTP とは？

TIME プロトコル（RFC868）はネットワーク上で時刻情報を配布するプロトコルです。SNTP（Simple Network Time Protocol、RFC1361、RFC1769）は NTP（Network Time Protocol）のサブセットで、パソコンなど末端のクライアントマシンの時刻を同期させるのに適しています。

こんな事に気をつけて

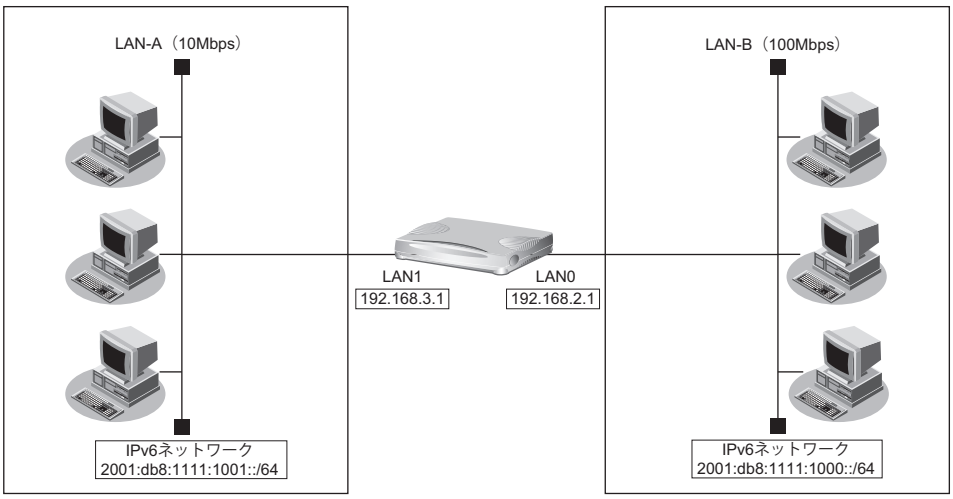
- 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- スイッチポートを利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

● コマンド

```
LAN0 情報を設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 0 ip dhcp service off
# lan 0 ip route 0 192.168.2.0/24 192.168.0.10 1 0
# lan 0 ip route 0 default 192.168.0.5 1 0
# lan 0 ip rip use v1 v1 0 off

LAN1 情報を設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off

自動時刻を設定する
# time auto server 192.168.0.20 time
# time auto interval start

ProxyDNS を設定する
# proxydns domain 0 any * any static 192.168.0.30
# proxydns address 0 any static 192.168.0.30

設定終了
# save

再起動
# reset
```

1.4　IPv4 のネットワークに IPv6 ネットワークを追加する

ここでは、IPv4 で通信しているネットワーク環境に IPv6 通信設定を追加する例について説明します。



● 設定条件

[LAN-A 側]

- プレフィックス／プレフィックス長　：2001:db8:1111:1001::/64

[LAN-B 側]

- プレフィックス／プレフィックス長　：2001:db8:1111:1000::/64

こんな事に気をつけて

スイッチポートを利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

● コマンド

```
LAN0 情報を設定する
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:1000::/64 30d 7d c0
# lan 0 ip6 ra mode send
# lan 0 ip6 rip use on on 0
# lan 0 ip6 rip site-local on

LAN1 情報を設定する
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:1001::/64 30d 7d c0
# lan 1 ip6 ra mode send
# lan 1 ip6 rip use on on 0
# lan 1 ip6 rip site-local on

設定終了
# save
# commit
```

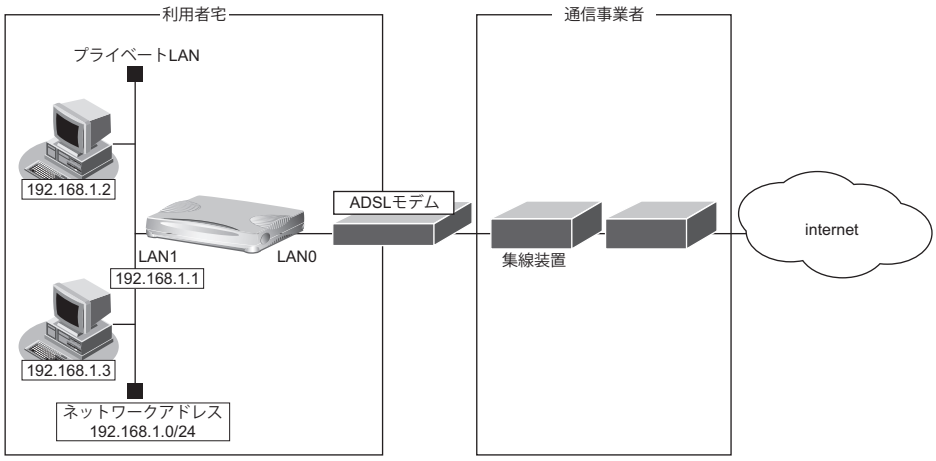
1.5　インターネットへ PPPoE で接続する

ここでは、PPPoE 接続を使ってフレッツ・ADSL などのサービスを利用し、インターネットへ接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照　マニュアル「トラブルシューティング」



● 設定条件

[通信事業者側]

- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- LAN0 ポートを使用する

[プライベート LAN 側]

- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24

こんな事に気をつけて

- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「”」、「<」、「>」、「&」、「%」は入力しないでください。

  ☛ 参照　マニュアル「コマンドユーザーズガイド」

- 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- PPPoE で利用する相手情報の MTU 値は、接続先から指定された MTU 値を設定します。一般的には、1454 を設定すれば問題ありません。
- PPPoE を利用する物理インタフェースの LAN 情報設定では、lan mode コマンドで動作モードを必ず設定してください。lan mode コマンドで動作モードの設定がなく、その他の lan 情報で設定する値もすべて初期値とした場合、その LAN 情報は保存されないため、通信できなくなります。

● コマンド

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.1/24 3

DHCP サーバを設定する
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip dhcp service server
# lan 1 ip nat mode off

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 autodial enable
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1
# remote 0 ip rip use off off 0 off
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect

ProxyDNS を設定する
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0

設定終了
# save

再起動
# reset
```

1.6　複数の事業所LANをIP-VPN網を利用して接続する

ここでは、プロトコルBGP4 を使用して、IP-VPN網で複数の事業所を接続する場合の設定方法を説明します。

こんな事に気をつけて

- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

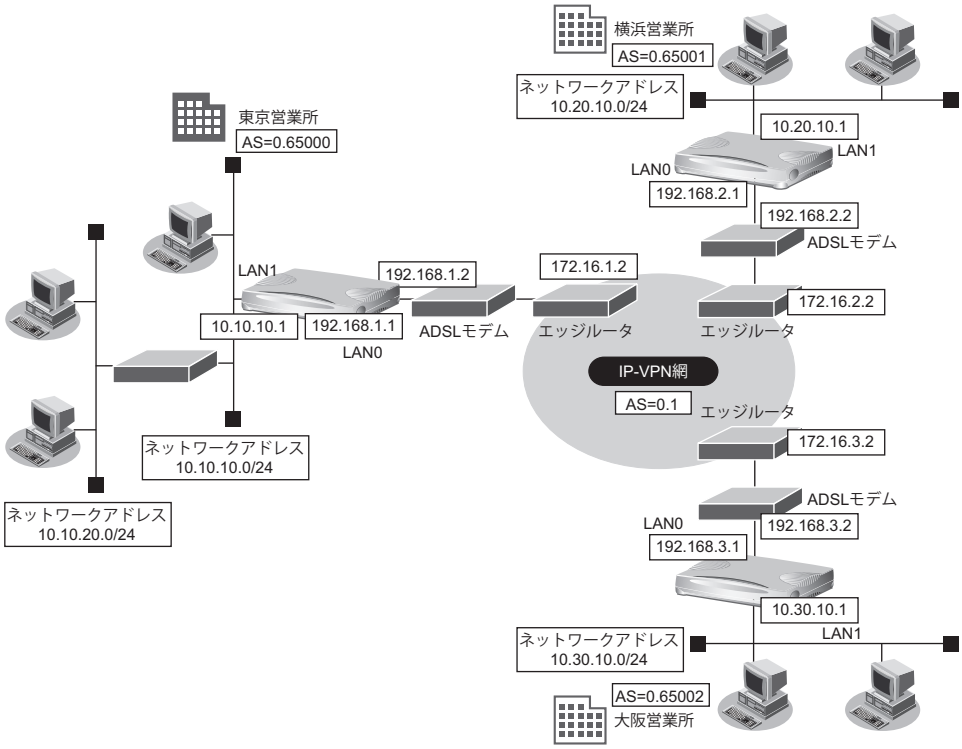
  ☛参照　マニュアル「トラブルシューティング」

- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「”」、「<」、「>」、「&」、「%」は入力しないでください。

  ☛参照　マニュアル「コマンドユーザーズガイド」

- NAT 機能と併用することはできません。
- バージョン4だけをサポートしています。
- 本装置のグレースフルリスタート機能のサポート範囲は、以下のとおりです。
  - レシーブルータ機能のみ（リスタート機能は、サポートしていません。）
  - アドレスファミリはIPv4のみ
- 経路情報を最大値まで保持している状態では、受信したBGPパケットは破棄されます。破棄したBGPパケットの経路情報は、その後、経路情報に空きができた場合でも反映されません。
- BGP使用中にcommitコマンドを実行した場合、接続中のセッションが一度切断されることがあります。

1.6.1　ADSLモデムを使用してIP-VPN網と接続する



● 設定条件

- LAN0 ポートを ADSL モデムに接続する

[IP-VPN 網]

- 東京営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。また、グレースフルリスタートを使用する。
- 横浜営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 大阪営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 東京営業所向け IP アドレス　：172.16.1.2
- 横浜営業所向け IP アドレス　：172.16.2.2
- 大阪営業所向け IP アドレス　：172.16.3.2
- AS 番号　：0.1

[東京営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.1.1
- LAN0 側ネットワークアドレス／ネットマスク　：192.168.1.0/24
- LAN1 側 IP アドレス　：10.10.10.1
- LAN1 側ネットワークアドレス／ネットマスク　：10.10.10.0/24
- AS 番号　：0.65000
- BGP グレースフルリスタート　：使用する
- 営業所内のルーティングプロトコル　：RIPv2

[横浜営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.2.1
- LAN0 側ネットワークアドレス／ネットマスク　：192.168.2.0/24
- LAN1 側 IP アドレス　：10.20.10.1
- LAN1 側ネットワークアドレス／ネットマスク　：10.20.10.0/24
- AS 番号　：0.65001
- BGP グレースフルリスタート　：使用しない

[大阪営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.3.1
- LAN0 側ネットワークアドレス／ネットマスク　：192.168.3.0/24
- LAN1 側 IP アドレス　：10.30.10.1
- LAN1 側ネットワークアドレス／ネットマスク　：10.30.10.0/24
- AS 番号　：0.65002
- BGP グレースフルリスタート　：使用しない

こんな事に気をつけて

スイッチポートを利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

東京営業所を設定する

● コマンド

```
LAN ポートを削除する
# delete lan

LAN 情報を設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip route 0 172.16.1.0/24 192.168.1.2 1
# lan 1 ip address 10.10.10.1/24 3
# lan 1 ip rip use v2m v2 0 off

ルーティングプロトコル情報を設定する
# routemanage ip redist rip bgp on
# routemanage ip redist bgp rip on
# bgp as 0.65000
# bgp ip network route 0 10.10.10.0/24
# bgp neighbor 0 address 172.16.1.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2
# bgp neighbor 0 graceful-restart family ipv4

設定終了
# save
# commit
```

横浜営業所を設定する

● コマンド

```
LAN ポートを削除する
# delete lan

LAN 情報を設定する
# lan 0 ip address 192.168.2.1/24 3
# lan 0 ip route 0 172.16.2.0/24  192.168.2.2 1
# lan 1 ip address 10.20.10.1/24 3

ルーティングプロトコル情報を設定する
# bgp as 0.65001
# bgp ip network route 0 10.20.10.0/24
# bgp neighbor 0 address 172.16.2.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

大阪営業所を設定する

● コマンド

```
LAN ポートを削除する
# delete lan

LAN 情報を設定する
# lan 0 ip address 192.168.3.1/24 3
# lan 0 ip route 0 172.16.3.0/24 192.168.3.2 1
# lan 1 ip address 10.30.10.1/24 3

ルーティングプロトコル情報を設定する
# bgp as 0.65002
# bgp ip network route 0 10.30.10.0/24
# bgp neighbor 0 address 172.16.3.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

1.7　複数の事業所LANをVPN（IPsec）で接続する

ここでは、VPN（IPsec）で複数の事業所を接続する場合を例に説明します。

1.7.1　NATと併用しない固定IPアドレスでのVPN（自動鍵交換）

IPsec機能を使って自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは、以下のコマンドによって、支社Aおよび支社BはPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE常時接続）]

- ローカルネットワークIPアドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定IPアドレス　：202.168.1.66/24
- PPPoE ユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[支社B（PPPoE常時接続）]

- ローカルネットワークIPアドレス　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定IPアドレス　：202.168.3.66/24
- PPPoE ユーザ認証ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPアドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定IPアドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPアドレス　：202.168.2.65

こんな事に気をつけて

スイッチポートを利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

● 設定コマンド

[支社A（PPPoE常時接続）]

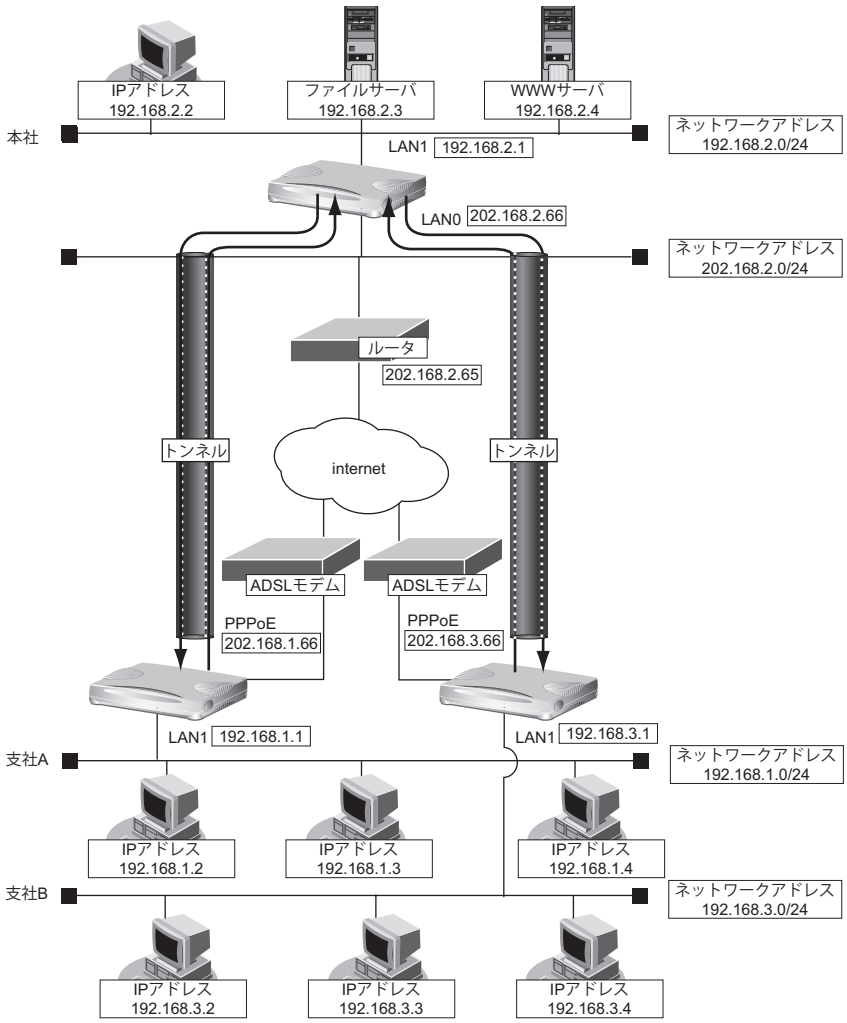
```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
```

[支社Ｂ（PPPoE常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.3.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid3 userpass3
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.3.66
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：202.168.1.66 - 202.168.2.66
- IPsec対象範囲　：192.168.1.0/24-any4

[支社B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：202.168.3.66 - 202.168.2.66
- IPsec対象範囲　：192.168.3.0/24-any4

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE区間　：202.168.2.66 - 202.168.1.66
- IPsec対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE区間　：202.168.2.66 - 202.168.3.66
- IPsec対象範囲　：any4-192.168.3.0/24

[共通A]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

[共通B]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：3des-cbc
- IPsec認証アルゴリズム　：hmac-sha1
- IPsec DHグループ　：なし
- IKE認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE認証方法　：shared
- IKE暗号アルゴリズム　：3des-cbc
- IKE認証アルゴリズム　：hmac-sha1
- IKE DHグループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社 A を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
```

```
設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 0
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.3.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

1.7.2　NATと併用した固定IPアドレスでのVPN（自動鍵交換）

IPsec機能を使って自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは、以下のコマンドによって、支社Aおよび支社BはPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE常時接続）]

- ローカルネットワークIPアドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定IPアドレス　：202.168.1.66/24
- グローバルネットワークIPアドレス　：10.0.1.1/24
- PPPoE ユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[支社B（PPPoE常時接続）]

- ローカルネットワークIPアドレス　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定IPアドレス　：202.168.3.66/24
- グローバルネットワークIPアドレス　：10.0.3.1/24
- PPPoE ユーザ認証ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPアドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定IPアドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPアドレス　：202.168.2.65

こんな事に気をつけて

スイッチポートを利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

● 設定コマンド

[支社A（PPPoE常時接続）]

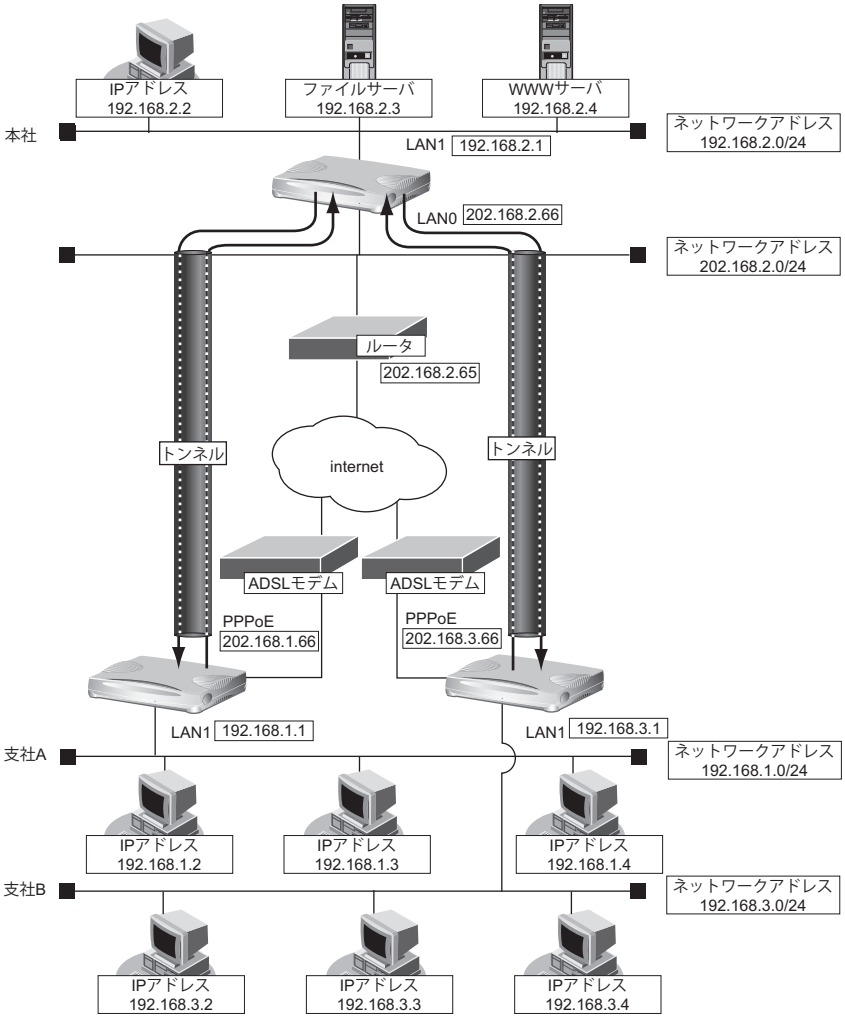
```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi 10.0.1.1 1 5m
# remote 0 ip msschange 1414
```

[支社Ｂ（PPPoE常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.3.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid3 userpass3
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.3.66
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi 202.168.3.66 1 5m
# remote 0 ip msschange 1414
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：10.0.1.1 - 202.168.2.66
- IPsec対象範囲　：192.168.1.0/24-any4

[支社B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：10.0.3.1 - 202.168.2.66
- IPsec対象範囲　：192.168.3.0/24-any4

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE区間　：202.168.2.66 - 10.0.1.1
- IPsec対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE区間　：202.168.2.66 - 10.0.3.1
- IPsec対象範囲　：any4-192.168.3.0/24

[共通A]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

[共通B]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：3des-cbc
- IPsec認証アルゴリズム　：hmac-sha1
- IPsec DHグループ　：なし
- IKE認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE認証方法　：shared
- IKE暗号アルゴリズム　：3des-cbc
- IKE認証アルゴリズム　：hmac-sha1
- IKE DHグループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社 A を設定する

● コマンド

```
インターネットへ IPsec/IKE パケットを送信する設定をする
# remote 0 ip nat static 0 202.168.1.66 500 10.0.1.1 500 17
# remote 0 ip nat static 1 202.168.1.66 any 10.0.1.1 any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B を設定する

● コマンド

```
インターネットへ IPsec/IKE パケットを送信する設定をする
# remote 0 ip nat static 0 202.168.3.66 500 10.0.3.1 500 17
# remote 0 ip nat static 1 202.168.3.66 any 10.0.3.1 any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
```

```
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 10.0.1.1
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 0
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 10.0.3.1
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

1.7.3　NATと併用した可変IPアドレスでのVPN（自動鍵交換）

接続するたびにIPアドレスが変わる環境でVPNを構築する場合の設定方法を説明します。

ここでは、以下のコマンドによって、支社Aおよび支社BはPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE接続）]

- ローカルネットワークIPアドレス　：192.168.1.1/24
- PPPoE ユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[支社B（PPPoE接続）]

- ローカルネットワークIPアドレス　：192.168.3.1/24
- PPPoE ユーザ認証ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPアドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定IPアドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPアドレス　：202.168.2.65

こんな事に気をつけて

スイッチポートを利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

● 設定コマンド

[支社A（PPPoE接続）]

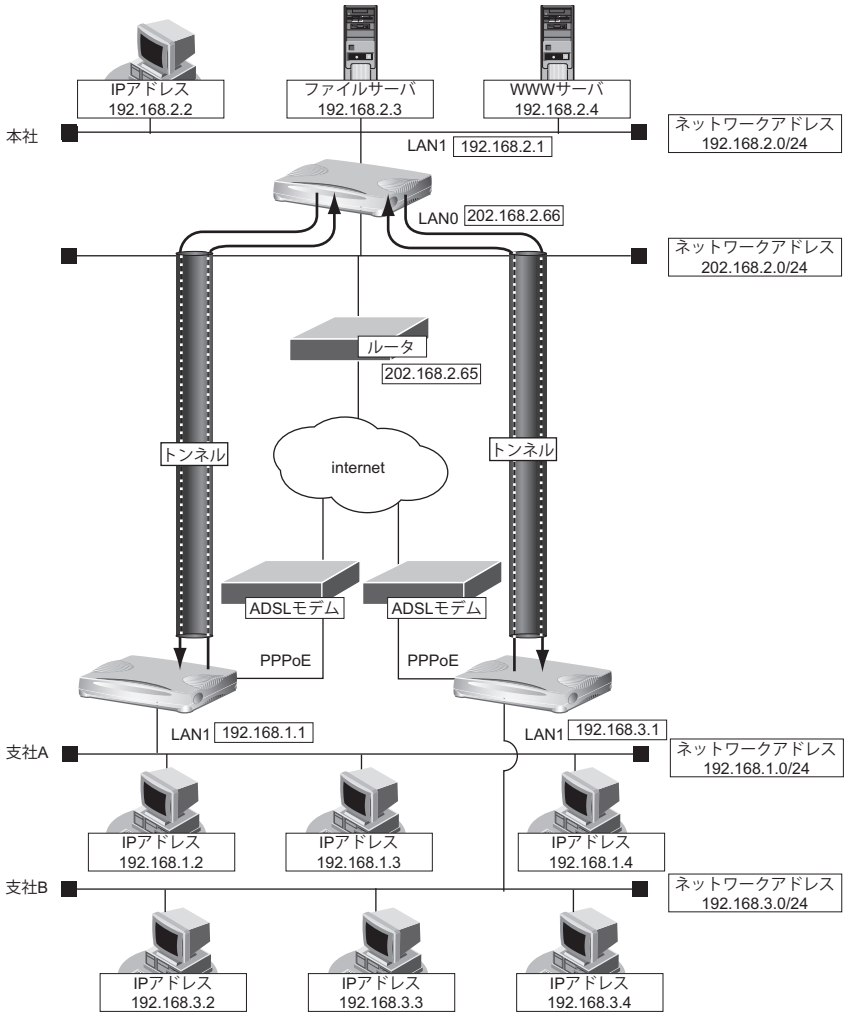
```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
```

[支社Ｂ（PPPoE接続)]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.3.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid3 userpass3
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社A（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：支社A - 202.168.2.66
- IPsec対象範囲　：192.168.1.0/24-any4
- IKE（UDP：500番ポート）のプライベートアドレス　：192.168.1.1
- ESPのプライベートアドレス　：192.168.1.1

[支社B（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：支社B - 202.168.2.66
- IPsec対象範囲　：192.168.3.0/24-any4
- IKE（UDP：500番ポート）のプライベートアドレス　：192.168.3.1
- ESPのプライベートアドレス　：192.168.3.1

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE区間　：202.168.2.66 - 支社A
- IPsec対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE区間　：202.168.2.66 - 支社B
- IPsec対象範囲　：any4-192.168.3.0/24

[共通A]

- 鍵交換タイプ　：Aggressive Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE支社A ID/IDタイプ　：shisyaA（自装置名）/FQDN
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

[共通 B]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：3des-cbc
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：なし
- IKE 支社 B ID/ID タイプ　：shisyaB（自装置名）/FQDN
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：3des-cbc
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

こんな事に気をつけて

可変 IP アドレスでの VPN 接続を行うときは、インターネットプロバイダから割り当てられる IP アドレスが不定であるため、ローカルネットワーク IP アドレスで IKE ネゴシエーションを行う場合があります。このような運用では、送出インタフェースで NAT 機能を使用してください。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社 A（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.3.1 500 any 500 17
# remote 0 ip nat static 1 192.168.3.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

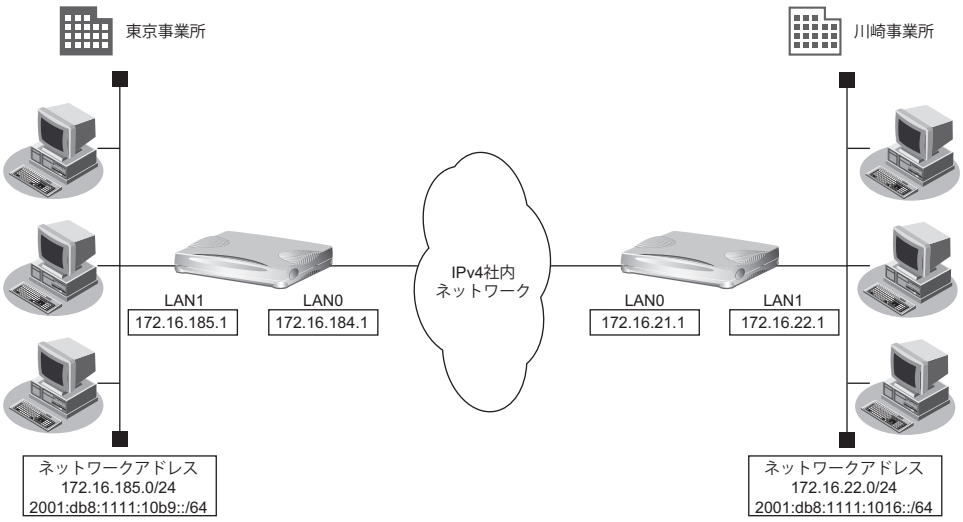
本社（**Responder**）を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 0
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

1.8　IPv6の事業所LANをIPv4トンネルで接続する

ここでは、IPv4で構築されたイントラネットを介して、2つの事業所（東京、川崎）のIPv6ネットワークどうしを接続（トンネリング）する場合を例に説明します。



● 設定条件

[東京事業所]

- ダイナミックルーティングを使用する
- LAN0側のIPv4アドレス　：172.16.184.1
- LAN1側のIPv4アドレス　：172.16.185.1
- LAN1側のIPv6プレフィックス／プレフィックス長　：2001:db8:1111:10b9::/64（※）

[川崎事業所]

- ダイナミックルーティングを使用する
- LAN0側のIPv4アドレス　：172.16.21.1
- LAN1側のIPv4アドレス　：172.16.22.1
- LAN1側のIPv6プレフィックス／プレフィックス長　：2001:db8:1111:1016::/64（※）

※）　この例では、プライベートアドレス（IPv4）／ドキュメント記述用アドレス（IPv6）を使用しています。

こんな事に気をつけて

- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

  ☛参照　マニュアル「コマンドユーザーズガイド」

- IPv6 over IPv4トンネルを利用する場合は、カプセル化されたIPv4パケットのフラグメントを防ぐため、トンネルに利用する相手情報のMTUに1280を設定してください。
- 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- スイッチポートを利用する場合は、「2.27 スイッチポートを使う」（P.285）を参照してください。

東京事業所を設定する

● コマンド

```
IPv4 で事業所間を接続する
# lan 0 ip address 172.16.184.1/24 3
# lan 0 ip rip use v1 v1 0
# lan 0 ip dhcp service off
# lan 0 ip nat mode off
# lan 1 ip address 172.16.185.1/24 3
# lan 1 ip rip use v1 v1 0
# lan 1 ip dhcp service off
# lan 1 ip nat mode off

IPv6 情報を設定する
# lan 1 ip6 use on
# lan 1 ip6 ifid auto
# lan 1 ip6 address 0 2001:db8:1111:10b9::/64 30d 7d c0
# lan 1 ip6 ra mode send

IP トンネル接続（川崎事業所）の情報を設定する
# remote 0 name v6kawasa
# remote 0 mtu 1280
# remote 0 ap 0 name tn-kawa
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 172.16.184.1
# remote 0 ap 0 tunnel remote 172.16.21.1
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:1016::/64 1

設定終了
# save

再起動
# reset
```

川崎事業所を設定する

● コマンド

```
IPv4 で事業所間を接続する
# lan 0 ip address 172.16.21.1/24 3
# lan 0 ip rip use v1 v1 0 off
# lan 0 ip dhcp service off
# lan 0 ip nat mode off
# lan 1 ip address 172.16.22.1/24 3
# lan 1 ip rip use v1 v1 0
# lan 1 ip dhcp service off
# lan 1 ip nat mode off

IPv6 情報を設定する
# lan 1 ip6 use on
# lan 1 ip6 ifid auto
# lan 1 ip6 address 0 2001:db8:1111:1016::/64 30d 7d c0
# lan 1 ip6 ra mode send

IP トンネル接続（東京事業所）の情報を設定する
# remote 0 name v6tokyo
# remote 0 mtu 1280
# remote 0 ap 0 name tn-tkyo
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 172.16.21.1
# remote 0 ap 0 tunnel remote 172.16.184.1
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:10b9::/64 1

設定終了
# save

再起動
# reset
```

ヒント

◆ NAT と IPv6 over IPv4 トンネルを併用する

IPv4 環境の NAT と、IPv6 over IPv4 トンネルを利用した IPv6 通信環境を併用する場合は、IPv4 環境の NAT の処理によって、IPv4 アドレスがどのように変換処理されるかを判断して IPv6 over IPv4 トンネル通信の設定を行う必要があります。

本装置では、トンネル処理は NAT 処理の内側（プライベートアドレス側）で行われますので、以下のように設定します。

設定項目	設定内容
自側エンドポイント	以下の IP アドレスのどちらかを設定します。 • LAN に設定された IP アドレスまたはセカンダリ IP アドレス • remote ip address local コマンドで設定した自側 IP アドレス ※）PPP で割り当てられる IP アドレスは利用できません。
相手側エンドポイント	相手トンネル GW の IP アドレス
静的 NAT	IPv6 over IPv4 トンネル通信が相手トンネル GW 側から開始されることがある場合は、静的 NAT の設定が必要となります。 • プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　すべて • グローバル IP 情報 IP アドレス　相手トンネル GW に設定された、本装置側のアドレス ポート番号　すべて • プロトコル　IPv6 over IPv4

具体例を以下に示します。

条件：

- 本装置の NAT 変換で利用するグローバルアドレスに 172.16.0.1 を利用
- 本装置のプライベート LAN 側に 192.168.1.1 を利用
- 相手トンネル GW の IP アドレスに 172.31.0.1 を利用

IPv6 over IPv4 トンネル接続：

- 本装置のトンネル通信の設定：
  192.168.1.1 と 172.31.0.1 の間でトンネル通信を行うことを前提に、以下のとおり設定します。
  remote 0 ap 0 tunnel local 192.168.1.1
  remote 0 ap 0 tunnel remote 172.31.0.1

  静的 NAT 設定：

- lan 0 ip nat static 0 192.168.1.1 any 172.16.0.1 any 41

  なお、この具体例で、相手トンネル GW の設定は、以下のとおりです。

  172.16.0.1 と 172.31.0.1 の間でトンネル通信を行うことを前提とします。

  相手トンネル GW に Si-R brin シリーズ（NAT 未使用）を利用する場合は、相手側の Si-R brin に以下を設定します。

  remote 0 ap 0 tunnel local 172.31.0.1
  remote 0 ap 0 tunnel remote 172.16.0.1

第２章　活用例

この章では、本装置の便利な機能の活用方法について説明します。

2.1 RIP の経路を制御する（IPv4）. 47
2.1.1 特定の経路情報の送信を許可する 49
2.1.2 特定の経路情報のメトリック値を変更して送信する 50
2.1.3 特定の経路情報の受信を許可する 51
2.1.4 特定の経路情報のメトリック値を変更して受信する 52
2.1.5 特定の経路情報の送信を禁止する 53
2.1.6 特定の経路情報の受信を禁止する 54
2.2 RIP の経路を制御する（IPv6）. 55
2.2.1 特定の経路情報の送信を許可する 57
2.2.2 特定の経路情報のメトリック値を変更して送信する 58
2.2.3 特定の経路情報の受信を許可する 59
2.2.4 特定の経路情報のメトリック値を変更して受信する 60
2.2.5 特定の経路情報の送信を禁止する 61
2.2.6 特定の経路情報の受信を禁止する 62
2.3 OSPFv2 を使用したネットワークを構築する（IPv4）. 63
2.3.1 バーチャルリンクを使う 67
2.3.2 スタブエリアを使う 71
2.4 OSPF の経路を制御する（IPv4）. 74
2.4.1 OSPF ネットワークでエリアの経路情報（LSA）を集約する 74
2.4.2 AS 外部経路を集約して OSPF ネットワークに広報する 75
2.4.3 エリア境界ルータで不要な経路情報（LSA）を遮断する 77
2.5 BGP の経路を制御する（IPv4）. 78
2.5.1 特定の経路情報の受信を透過させる 78
2.5.2 特定の AS からの経路情報の受信を遮断する. 79
2.5.3 IP-VPN 網からの受信情報の他 IP-VPN 網への送信を遮断する 80
2.5.4 冗長構成の通信経路を使用する. 81
2.6 マルチキャスト機能を使う 83
2.6.1 マルチキャスト機能（PIM-DM）を使う 83
2.6.2 マルチキャスト機能（PIM-SM）を使う 87
2.6.3 マルチキャスト機能（スタティックルーティング）を使う. 93
2.7 VLAN 機能を使う 96
2.8 IP フィルタリング機能を使う 98
2.8.1 外部の特定サービスへのアクセスだけを許可する. 102
2.8.2 外部から特定サーバへのアクセスだけを許可する. 106
2.8.3 外部から特定サーバへのアクセスだけを許可して SPI を併用する 110
2.8.4 外部の特定サービスへのアクセスだけを許可する（IPv6 フィルタリング）. 114
2.8.5 外部の特定サーバへのアクセスだけを禁止する 118

2.8.6 利用者が意図しない発信を防ぐ . . . 120
2.8.7 回線が接続しているときだけを許可する . . . 121
2.8.8 外部から特定サーバへのpingだけを禁止する . . . 122
2.9 IPsec機能を使う . . . 124
2.9.1 IPv4 over IPv4で固定IPアドレスでのVPN（手動鍵交換） . . . 129
2.9.2 IPv4 over IPv6で固定IPアドレスでのVPN（自動鍵交換） . . . 133
2.9.3 IPv6 over IPv4で固定IPアドレスでのVPN（自動鍵交換） . . . 137
2.9.4 IPv6 over IPv4で可変IPアドレスでのVPN（自動鍵交換） . . . 141
2.9.5 IPv6 over IPv6で固定IPアドレスでのVPN（自動鍵交換） . . . 145
2.9.6 IPv4 over IPv4で1つのIKEセッションに複数のIPsecトンネル構成でのVPN（自動鍵交換） . . . 149
2.9.7 IPsec機能と他機能との併用 . . . 153
2.9.8 テンプレート着信機能（AAA認証）を使用した固定IPアドレスでのVPN . . . 158
2.9.9 テンプレート着信機能（AAA認証）を使用した可変IPアドレスでのVPN . . . 162
2.9.10 テンプレート着信機能（RADIUS認証）を使用した固定IPアドレスでのVPN . . . 167
2.9.11 テンプレート着信機能（RADIUS認証）を使用した可変IPアドレスでのVPN . . . 172
2.9.12 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN . . . 177
2.9.13 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN（冗長構成） . . . 186
2.9.14 テンプレート着信機能（動的VPN）を使用したIPv6 over IPv6で固定IPアドレスでのVPN . . . 189
2.9.15 NATトラバーサルを使用した可変IPアドレスでのVPN . . . 198
2.9.16 テンプレート着信機能（AAA認証）およびNATトラバーサルを使用した可変IPアドレスでのVPN . . . 202
2.9.17 接続先情報（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN . . . 206
2.10 システムログを採取する . . . 217
2.11 マルチNAT機能（アドレス変換機能）を使う . . . 219
2.11.1 プライベートLAN接続でサーバを公開する . . . 220
2.11.2 PPPoE接続でサーバを公開する . . . 221
2.11.3 サーバ以外のアドレス変換をしないで、プライベートLAN接続でサーバを公開する . . . 223
2.11.4 複数のNATトラバーサル機能を使用したIPsecクライアントを同じIPsecサーバに接続する . . . 224
2.11.5 NATあて先変換で双方向のアドレスを変換する . . . 225
2.11.6 NAT変換テーブル数を拡張する . . . 226
2.12 VoIP NATトラバーサル機能を使う . . . 227
2.13 TOS/Traffic Class値書き換え機能を使う . . . 229
2.14 VLANプライオリティマッピング機能を使う . . . 231
2.15 シェーピング機能を使う . . . 232
2.15.1 特定のインタフェースでシェーピング機能を使う . . . 232
2.15.2 送信先ごとにシェーピング機能を使う . . . 233
2.16 ヘッダ圧縮機能を使う . . . 234
2.17 帯域制御（WFQ）機能を使う . . . 235
2.18 DHCP機能を使う . . . 237
2.18.1 DHCPサーバ機能を使う . . . 238
2.18.2 DHCPスタティック機能を使う . . . 240
2.18.3 DHCPクライアント機能を使う . . . 242
2.18.4 DHCPリレーエージェント機能を使う . . . 243
2.18.5 IPv6 DHCPクライアント機能を使う . . . 244
2.18.6 IPv6 DHCPサーバ機能を使う . . . 246
2.18.7 IPv6 DHCPクライアント機能で取得した情報をIPv6 DHCPサーバ機能で配布する . . . 248
2.19 DNSサーバ機能を使う（ProxyDNS） . . . 250
2.19.1 DNSサーバの自動切り替え機能（順引き）を使う . . . 250
2.19.2 DNSサーバの自動切り替え機能（逆引き）を使う . . . 252
2.19.3 DNSサーバアドレスの自動取得機能を使う . . . 253
2.19.4 DNSサーバアドレスをDHCPサーバから取得して使う . . . 255
2.19.5 DNS問い合わせタイプフィルタ機能を使う . . . 257
2.19.6 DNSサーバ機能を使う . . . 258
2.20 特定のURLへのアクセスを禁止する（URLフィルタ機能） . . . 259
2.21 SNMPエージェント機能を使う . . . 261
2.22 ECMP機能を使う . . . 264
2.23 VRRP機能を使う . . . 269

2.23.1 簡易ホットスタンバイ機能を使う 270
2.23.2 クラスタリング機能を使う 273
2.24 遠隔地のパソコンを起動させる（リモートパワーオン機能） 276
2.24.1 リモートパワーオン情報を設定する 277
2.24.2 リモートパワーオン機能を使う 277
2.25 スケジュール機能を使う 278
2.25.1 スケジュールを予約する 278
2.25.2 構成定義情報の切り替えを予約する 279
2.26 ブリッジ／STP 機能を使う 280
2.26.1 ブリッジでFNA をつないでSTP 機能を使う 280
2.26.2 IP トンネルで事業所間をブリッジ接続する（Ethernet over IP ブリッジ） 282
2.27 スイッチポートを使う 285
2.27.1 スイッチポートをHUB として使用する 286
2.27.2 スイッチポートを単独ポートとして使用する（Si-R80brin） 288
2.28 アプリケーションフィルタ機能を使う 289
2.29 不正端末アクセス防止機能（MAC アドレス認証）を使う 291
2.30 装置を保護する 294
2.30.1 設定例 294

2.1　RIP の経路を制御する（IPv4）

本装置を経由して、ほかのルータに送受信する経路情報に対して、IP アドレスや方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

- RIP による経路情報

指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件（IP アドレス／アドレスマスク）
- メトリック値

補足 メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0 を指定すると変更は行いません。経路情報のフィルタリング条件に any 以外を指定した場合に有効です。送信方向のメトリック値に 1 ～ 16 を指定した場合、インタフェースに設定した RIP の加算メトリック値は加算されません。

ヒント

◆ IP アドレスとアドレスマスクの決め方

フィルタリング条件の要素には、「IP アドレス」と「アドレスマスク」があります。制御対象となる経路情報は、経路情報の IP アドレスとアドレスマスクが指定した IP アドレスとアドレスマスクと一致したものだけです。

例）　指定値　　：172.21.0.0/16 の場合
　　経路情報　　：172.21.0.0/16 は制御対象となる
　　　　172.21.0.0/24 は制御対象とならない

また、フィルタリング条件の IP アドレスと指定した IP アドレスが、指定したアドレスマスクまで一致した場合に制御対象とすることもできます。

　　指定値　　：172.21.0.0/16 の場合
　　経路情報　　：172.21.0.0/24 は制御対象となる
　　　　172.21.10.0/24 は制御対象となる

こんな事に気をつけて

RIPv1 を使用している場合もアドレスマスクの設定が必要です。この場合、インタフェースのアドレスマスクを指定してください。また、アドレスクラスが異なる経路情報を制御する場合は、ナチュラルマスク値を指定してください。
例）lan 0 ip address 192.168.1.1/24 に 10.0.0.0 の経路情報を制御する場合は、10.0.0.0/8 を指定します。

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の２つがあります。

A. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する。

B. 特定の条件の経路情報だけを遮断し、その他はすべて透過させる。

ここでは、設計方針Ａの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

また、設計方針Ｂの例として、以下の設定例について説明します。

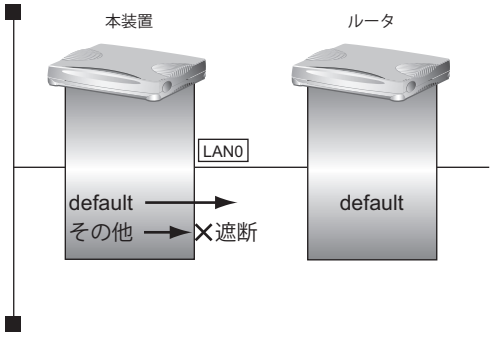
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

こんな事に気をつけて

- フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、より高い優先度を示します。
- RIP 受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しない RIP 経路情報は遮断されます。
- RIP 送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しない RIP 経路情報は遮断されます。

2.1.1　特定の経路情報の送信を許可する

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明します。



● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

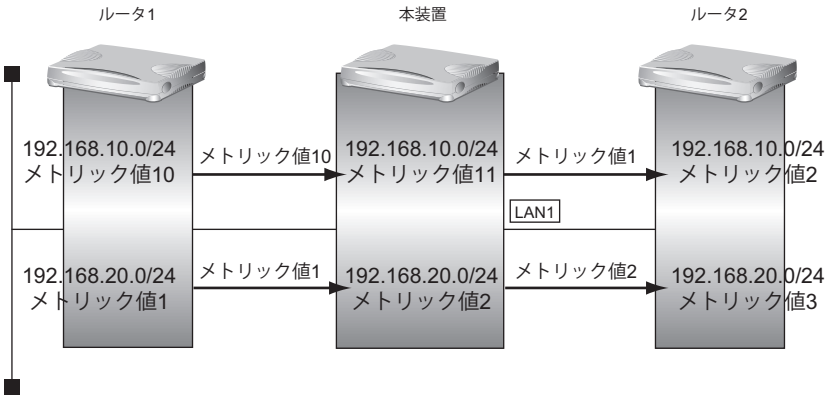
● コマンド

```
デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass out
# lan 0 ip rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ip rip filter 1 act reject out
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```

2.1.2　特定の経路情報のメトリック値を変更して送信する

ここでは、本装置がルータ 2 へ 192.168.10.0/24、メトリック値 1 の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ 1 から 192.168.10.0/24 のメトリック値 10 と 192.168.20.0/24 のメトリック値 1 の経路情報を受信するものとします。



● フィルタリング設計

- 本装置から 192.168.10.0/24 の送信を許可する場合、メトリック値 1 に変更
- 192.168.10.0/24 以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

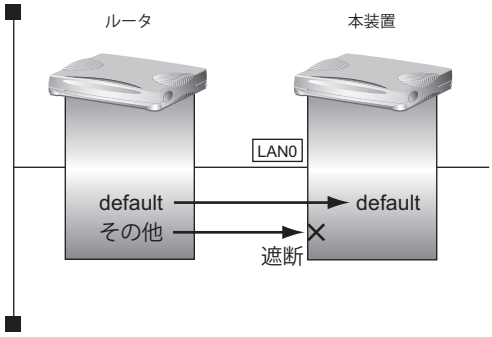
```
192.168.10.0/24 をメトリック値 1 で送信する
# lan 1 ip rip filter 0 act pass out
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 1

その他の経路情報はメトリック値を変更しないで送信する
# lan 1 ip rip filter 1 act pass out
# lan 1 ip rip filter 1 route any

設定終了
# save
# commit
```

こんな事に気をつけて

- 送信方向でメトリック値が設定されている場合、インタフェースの RIP 加算メトリック値の加算は行われません。
- 送信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。

2.1.3　特定の経路情報の受信を許可する

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

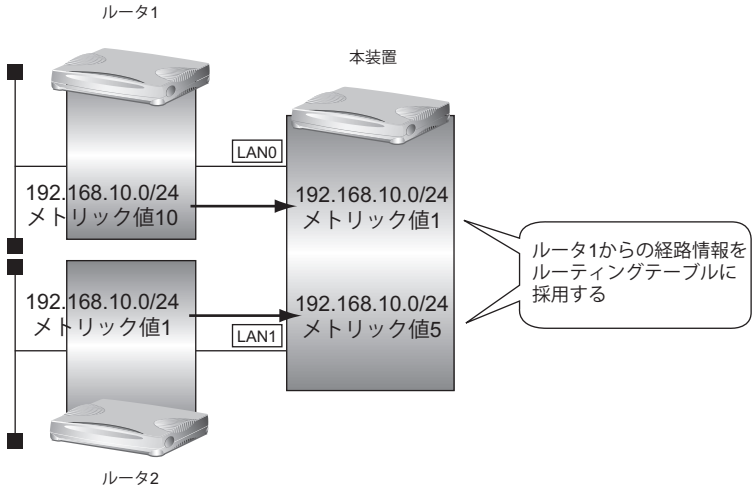
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ip rip filter 1 act reject in
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```

2.1.4　特定の経路情報のメトリック値を変更して受信する

ここでは、本装置が、ルータ１とルータ２から同じあて先への経路情報 192.168.10.0/24 を受信した場合に、ルータ１から受信した経路情報を採用する場合の設定方法を説明します。



● フィルタリング設計

- ルータ１から、192.168.10.0/24 の経路情報を受信した場合、メトリック値１に変更
- ルータ２から、192.168.10.0/24 の経路情報を受信した場合、メトリック値５に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

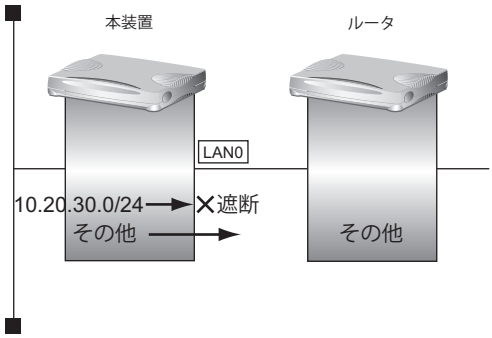
```
LAN0 から 192.168.10.0/24 を受信した場合、メトリック値１で受信する
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route 192.168.10.0/24
# lan 0 ip rip filter 0 set metric 1

LAN0 からのその他の経路情報はすべて受信する
# lan 0 ip rip filter 1 act pass in
# lan 0 ip rip filter 1 route any

lan1 から 192.168.10.0/24 を受信した場合、メトリック値５で受信する
# lan 1 ip rip filter 0 act pass in
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 5

lan1 からのその他の経路情報はすべて受信する
# lan 1 ip rip filter 1 act pass in
# lan 1 ip rip filter 1 route any

設定終了
# save
# commit
```

こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。

2.1.5　特定の経路情報の送信を禁止する

ここでは、本装置からルータへの 10.20.30.0/24 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● フィルタリング設計

- 本装置からルータへの 10.20.30.0/24 の送信を禁止
- その他はすべて透過

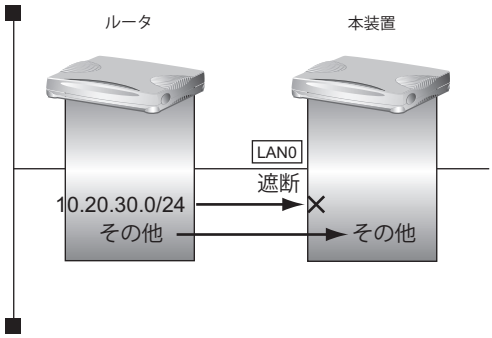
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
10.20.30.0/24 を遮断する
# lan 0 ip rip filter 0 act reject out
# lan 0 ip rip filter 0 route 10.20.30.0/24

その他の経路情報はすべて透過させる
# lan 0 ip rip filter 1 act pass out
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```

2.1.6　特定の経路情報の受信を禁止する

ここでは、本装置は、ルータから 10.20.30.0/24 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



● フィルタリング設計

- 本装置は 10.20.30.0/24 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
10.20.30.0/24 を遮断する
# lan 0 ip rip filter 0 act reject in
# lan 0 ip rip filter 0 route 10.20.30.0/24

その他の経路情報はすべて透過させる
# lan 0 ip rip filter 1 act pass in
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```

2.2　RIPの経路を制御する（IPv6）

本装置を経由して、ほかのルータに送信する経路情報や、ほかのルータから受信する経路情報に対して、経路情報や方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または、不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

- RIPによる経路情報（IPv6）

指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件（プレフィックス／プレフィックス長）
- メトリック値

補足　メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にany以外を指定した場合に有効です。送信方向のメトリック値に1～16を指定した場合、インタフェースに設定したRIPの加算メトリック値は加算されません。

ヒント

◆ プレフィックスとプレフィックス長の決め方

フィルタリング条件の要素には、「プレフィックス」と「プレフィックス長」があります。制御対象となる経路情報は、経路情報のプレフィックスとプレフィックス長が指定したプレフィックスとプレフィックス長と一致したものだけです。

例）　指定値　：2001:db8:1111::/32の場合

　　経路情報　：2001:db8:1111::/32は制御対象となる

　　2001:db8:1111::/64は制御対象とはならない

また、経路情報のプレフィックスと指定したプレフィックスが、指定したプレフィックス長まで一致した場合に制御対象とすることもできます。

　　指定値　：2001:db8::/16の場合

　　経路情報　：2001:db8::/32は制御対象となる

　　2001:db8:1111::/32は制御対象となる

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の２つがあります。

A. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する。

B. 特定の条件の経路情報だけを遮断し、その他はすべて透過させる。

ここでは、設計方針Ａの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

また、設計方針Ｂの例として、以下の設定例について説明します。

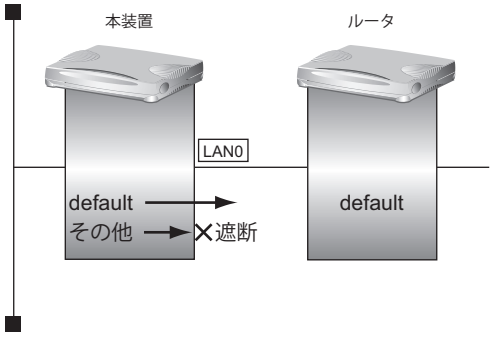
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

こんな事に気をつけて

- フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、より高い優先度を示します。
- RIP 受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しない RIP 経路情報は遮断されます。
- RIP 送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しない RIP 経路情報は遮断されます。

2.2.1　特定の経路情報の送信を許可する

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明しています。



● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

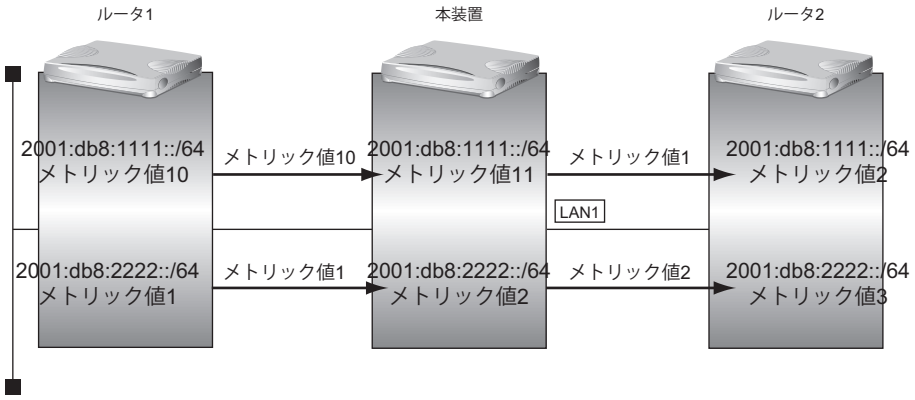
● コマンド

```
デフォルトルートを透過させる
# lan 0 ip6 rip filter 0 act pass out
# lan 0 ip6 rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ip6 rip filter 1 act reject out
# lan 0 ip6 rip filter 1 route any

設定終了
# save
# commit
```

2.2.2　特定の経路情報のメトリック値を変更して送信する

ここでは、本装置がルータ２へ2001:db8:1111::/64、メトリック値１の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ１から2001:db8:1111::/64のメトリック値10と2001:db8:2222::/64のメトリック値１の経路情報を受信するものとします。



● フィルタリング設計

- 本装置から2001:db8:1111::/64の送信を許可する場合、メトリック値１に変更
- 2001:db8:1111::/64以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

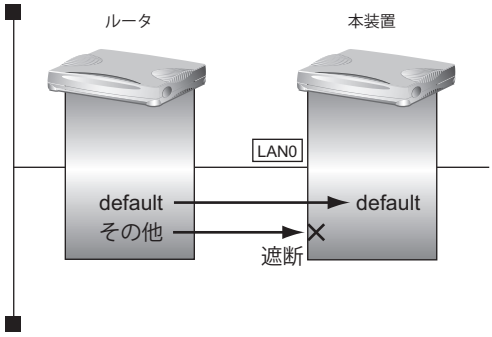
```
2001:db8:1111::/64 をメトリック値１で送信する
# lan 1 ip6 rip filter 0 act pass out
# lan 1 ip6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ip6 rip filter 0 set metric 1

その他の経路情報はメトリック値を変更しないで送信する
# lan 1 ip6 rip filter 1 act pass out
# lan 1 ip6 rip filter 1 route any

設定終了
# save
# commit
```

こんな事に気をつけて

- 送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。
- 送信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

2.2.3　特定の経路情報の受信を許可する

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

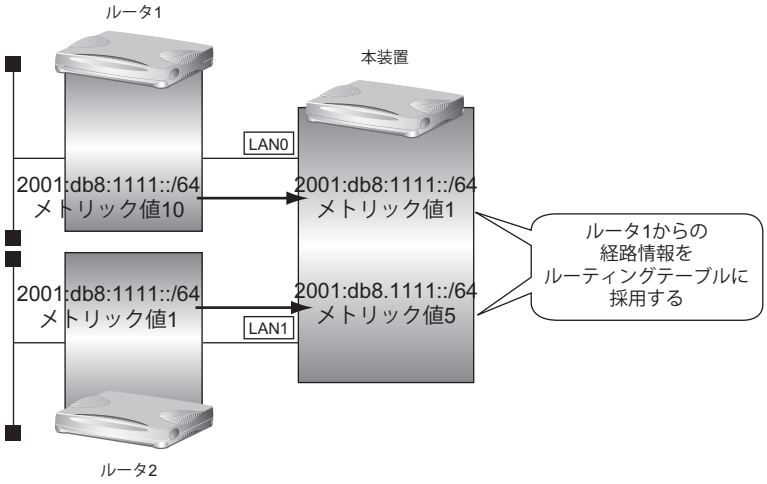
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
デフォルトルートを透過させる
# lan 0 ip6 rip filter 0 act pass in
# lan 0 ip6 rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ip6 rip filter 1 act reject in
# lan 0 ip6 rip filter 1 route any

設定終了
# save
# commit
```

2.2.4　特定の経路情報のメトリック値を変更して受信する

ここでは、本装置が、ルータ１とルータ２から同じあて先への経路情報2001:db8:1111::/64を受信した場合に、ルータ１から受信した経路情報を採用する場合の設定方法を説明します。



● フィルタリング設計

- ルータ１から、2001:db8:1111::/64の経路情報を受信した場合、メトリック値１に変更
- ルータ２から、2001:db8:1111::/64の経路情報を受信した場合、メトリック値５に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

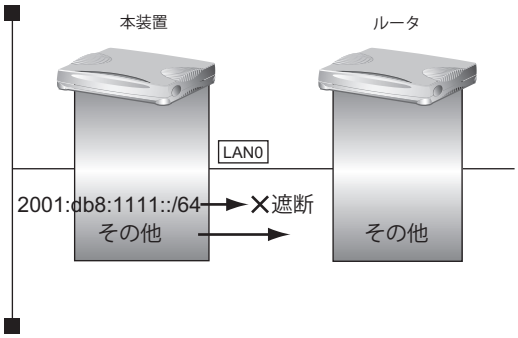
```
LAN0から2001:db8:1111::/64を受信した場合、メトリック値１で受信する
# lan 0 ip6 rip filter 0 act pass in
# lan 0 ip6 rip filter 0 route 2001:db8:1111::/64
# lan 0 ip6 rip filter 0 set metric 1

LAN0からのその他の経路情報はすべて受信する
# lan 0 ip6 rip filter 1 act pass in
# lan 0 ip6 rip filter 1 route any

lan1から2001:db8:1111::/64を受信した場合、メトリック値５で受信する
# lan 1 ip6 rip filter 0 act pass in
# lan 1 ip6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ip6 rip filter 0 set metric 5

lan1からのその他の経路情報はすべて受信する
# lan 1 ip6 rip filter 1 act pass in
# lan 1 ip6 rip filter 1 route any

設定終了
# save
# commit
```

こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

2.2.5　特定の経路情報の送信を禁止する

ここでは、本装置からルータへの 2001:db8:1111::/64 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● フィルタリング設計

- 本装置からルータへの 2001:db8:1111::/64 の送信を禁止
- その他はすべて透過

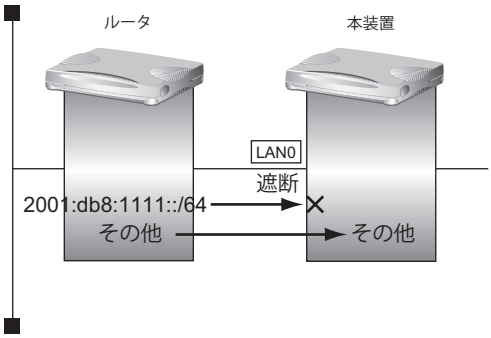
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
2001:db8:1111::/64 を遮断する
# lan 0 ip6 rip filter 0 act reject out
# lan 0 ip6 rip filter 0 route 2001:db8:1111::/64

その他の経路情報はすべて透過させる
# lan 0 ip6 rip filter 1 act pass out
# lan 0 ip6 rip filter 1 route any

設定終了
# save
# commit
```

2.2.6　特定の経路情報の受信を禁止する

ここでは、本装置は、ルータから 2001:db8:1111::/64 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



● フィルタリング設計

- 本装置は 2001:db8:1111::/64 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
2001:db8:1111::/64 を遮断する
# lan 0 ip6 rip filter 0 act reject in
# lan 0 ip6 rip filter 0 route 2001:db8:1111::/64

その他の経路情報はすべて透過させる
# lan 0 ip6 rip filter 1 act pass in
# lan 0 ip6 rip filter 1 route any

設定終了
# save
# commit
```

2.3 OSPFv2を使用したネットワークを構築する（IPv4）

ここでは、OSPFv2を使用したダイナミックルーティングのネットワークの設定方法について説明します。

OSPFを使用するネットワークは、バックボーンエリアとその他のエリアに分割して管理します。

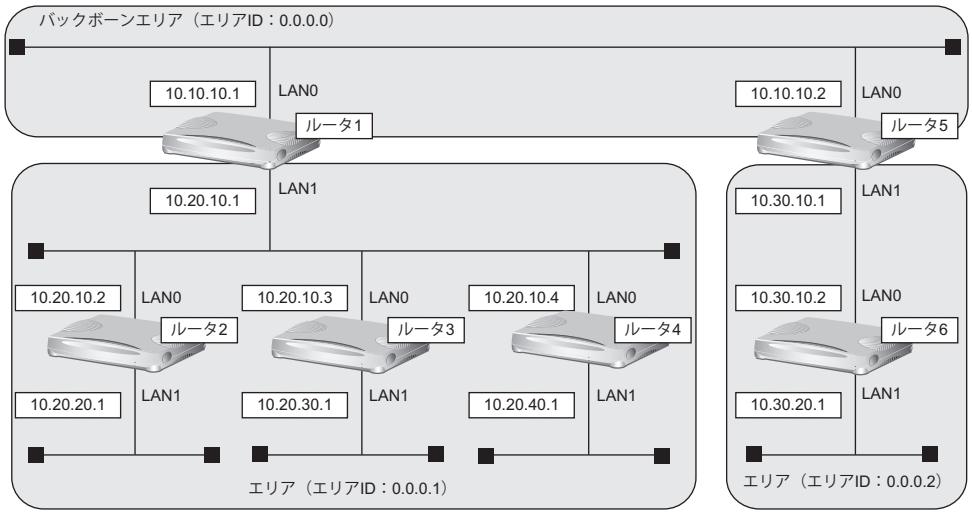
エリアには、エリアごとにエリアIDを設定します。バックボーンエリアには必ず0.0.0.0のエリアIDを設定し、ほかのエリアには重複しないように0.0.0.0以外のエリアIDを設定します。

エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

参照 マニュアル「機能説明書」

こんな事に気をつけて

- NAT機能と併用することはできません。
- OSPFを使用するインタフェースは、それぞれ異なったネットワークに属するIPアドレスを設定する必要があります。同じネットワークに属するIPアドレスを設定した場合、OSPFを使用しないと判断されます。
- ルータは、各エリアに50台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2つ以上のエリアの指定ルータ（Designated Router）とならないように設定してください。
- 隣接するOSPFルータどうしは、同じMTU値を設定してください。
- 経路情報を最大値まで保持した場合、OSPF以外の経路情報の減少によって経路情報に空きができても、OSPFの経路は、経路情報に反映されません。
- 本装置で保有できるLSA数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません（LSDBオーバフロー）。
  また、LSA生成元のルータの停止などによって、LSA数が本装置の上限値以下まで減少した場合、本装置の電源再投入、commit/resetコマンド実行にかかわらず、正常に通信ができるまでに最大60分かかることがあります。
- OSPF使用中にcommitコマンドを実行した場合、自装置が広報したすべてのLSAに対してMaxAgeで再広報を行ったあとに、OSPFネットワークへの経路情報が再作成されることがあります。



● 前提条件

- ルータ1からルータ6のすべてのインタフェースにIPアドレスを設定する
- ルータ1からルータ6のすべてのインタフェースでNAT機能およびDHCPクライアント機能を使用しない

● 設定条件

[ルータ 1 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN1 でのルータ優先度　：0
- エリア 0.0.0.1 への集約経路設定　：10.20.0.0/16

[ルータ 2 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN0 でのルータ優先度　：1
- LAN1 での passive-interface 設定　：設定する

[ルータ 3 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN0 でのルータ優先度　：255
- LAN1 での passive-interface 設定　：設定する

[ルータ 4 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN1 での passive-interface 設定　：設定する
- LAN0 でのルータ優先度　：1

[ルータ 5 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.2
- エリア 0.0.0.2 への集約経路設定　：10.30.0.0/16

[ルータ 6 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- LAN1 での OSPF エリア ID　：0.0.0.2
- LAN1 での passive-interface 設定　：設定する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

ルータ 1 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1
# lan 1 ip ospf priority 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1
# ospf ip area 1 range 0 10.20.0.0/16

設定終了
# save
# commit
```

ルータ 2 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 1
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

ルータ 3 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 255
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

ルータ 4 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 1
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

ルータ 5 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2
# ospf ip area 1 range 0 10.30.0.0/16

設定終了
# save
# commit
```

ルータ 6 を設定する

● コマンド

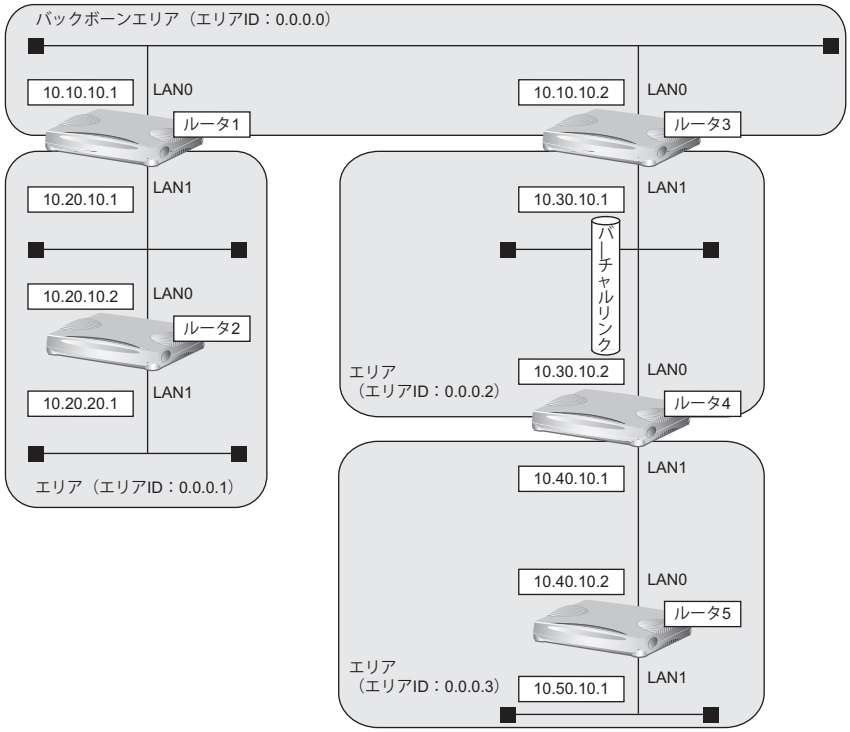
```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.2

設定終了
# save
# commit
```

2.3.1　バーチャルリンクを使う

バックボーンエリアと直接接続できないエリアを、バーチャルリンクを使用して接続する設定方法について説明します。

こんな事に気をつけて

- バーチャルリンクは、スタブエリア、準スタブエリアを経由して使用することはできません。
- バーチャルリンクを使用する場合は、OSPF ルータ ID を設定する必要があります。設定する際は、OSPF ルータ ID が重複しないように設定してください。



● 前提条件

- ルータ１からルータ５のすべてのインタフェースに IP アドレスを設定する
- ルータ１からルータ５のすべてのインタフェースで NAT 機能および DHCP クライアント機能を使用しない

● 設定条件

[ルータ１でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1

[ルータ２でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1

[ルータ 3 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.2
- OSPF ルータ ID　：10.30.10.1
- バーチャルリンク接続先 OSPF ルータ ID　：10.40.10.1

[ルータ 4 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- LAN1 での OSPF エリア ID　：0.0.0.3
- OSPF ルータ ID　：10.40.10.1
- バーチャルリンク接続先 OSPF ルータ ID　：10.30.10.1

[ルータ 5 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.3
- LAN1 での OSPF エリア ID　：0.0.0.3

上記の設定条件に従って設定を行う場合のコマンド例を示します。

ルータ 1 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1

設定終了
# save
# commit
```

ルータ 2 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

ルータ 3 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip id 10.30.10.1
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2
# ospf ip area 1 vlink 0 id 10.40.10.1

設定終了
# save
# commit
```

ルータ 4 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip id 10.40.10.1
# ospf ip area 0 id 0.0.0.2
# ospf ip area 0 vlink 0 id 10.30.10.1
# ospf ip area 1 id 0.0.0.3

設定終了
# save
# commit
```

ルータ **5** を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.3

設定終了
# save
# commit
```

2.3.2　スタブエリアを使う

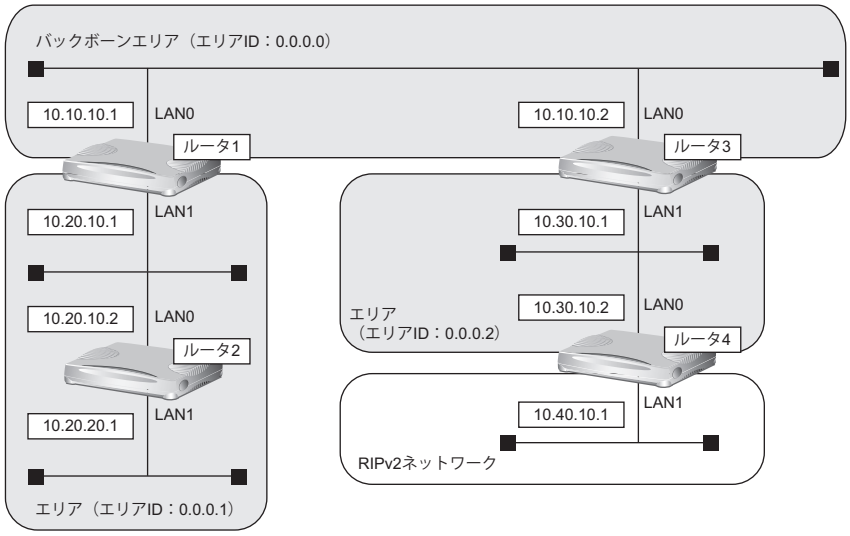
OSPF 以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

OSPF は、RIP または BGP で受信した経路情報、スタティック経路情報およびインタフェース経路情報を OSPF ネットワークに取り入れることができます。また、OSPFの経路情報をRIPおよびBGPで広報することができます。

OSPF 以外のネットワークと接続する場合、スタブエリアとして運用すると、OSPF ネットワーク外の経路としてデフォルトルートを使用するため、エリア内の経路情報を少なくすることができます。スタブエリアから OSPF 以外のネットワークに直接接続することはできません。直接、接続する場合は、準スタブエリア（NSSA）として運用します。

こんな事に気をつけて

OSPF 以外のネットワークと接続する場合、OSPF 以外のネットワークで使用するインタフェース経路情報を OSPF ネットワークに取り入れるように設定する必要があります。



● 前提条件

- ルータ１からルータ４のすべてのインタフェースに IP アドレスを設定する
- ルータ１からルータ４のすべてのインタフェースで NAT 機能および DHCP クライアント機能を使用しない

● 設定条件

[東京営業所]

[ルータ１でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1
- エリア ID 0.0.0.1 のエリアタイプ　：stub

[ルータ２でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- エリア ID 0.0.0.1 のエリアタイプ　：stub

[ルータ 3 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.2
- エリア ID 0.0.0.2 のエリアタイプ　：nssa

[ルータ 4 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：RIP V2,OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- LAN1 での passive-interface 設定　：設定する
- エリア ID0.0.0.2 のエリアタイプ　：nssa
- OSPF 経路の RIP での広報　：再配布する
- RIP 経路の OSPF での広報　：再配布する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

ルータ 1 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1
# ospf ip area 1 type stub

設定終了
# save
# commit
```

ルータ 2 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1
# ospf ip area 0 type stub

設定終了
# save
# commit
```

ルータ 3 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2
# ospf ip area 1 type nssa

設定終了
# save
# commit
```

ルータ 4 を設定する

● コマンド

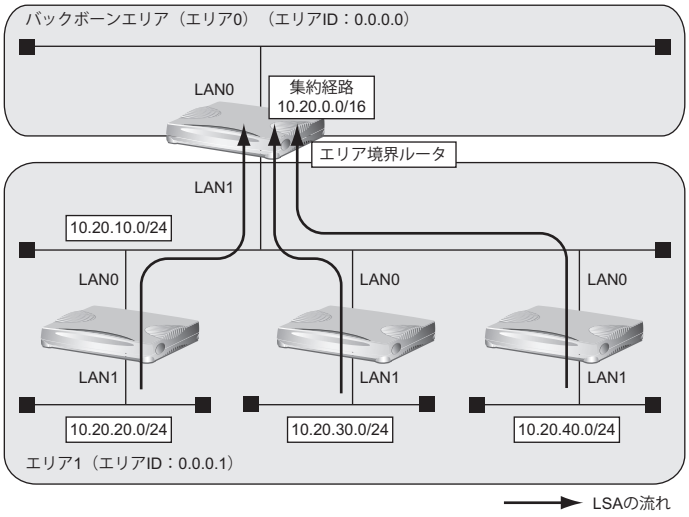
```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip rip use v2m v2 0 off
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

ルーティングマネージャ情報を設定する
# routemanage ip redist ospf rip on
# routemanage ip redist rip ospf on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.2
# ospf ip area 0 type nssa

設定終了
# save
# commit
```

2.4　OSPF の経路を制御する（IPv4）

本装置で、ほかのルータから受信する経路情報（LSA）に変更を加えることで、本装置で保有する経路情報や広報する経路情報の数を制御することができます。

2.4.1　OSPF ネットワークでエリアの経路情報（LSA）を集約する

エリア内の LSA を、本装置（エリア境界ルータ）で集約して、バックボーンエリアへ取り込む場合の設定方法を説明します。



● 経路情報の設計

- エリア内の LSA を、本装置（エリア境界ルータ）で集約してバックボーンエリアに取り込む

● 設定条件

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 でのエリア ID　：0.0.0.0
- LAN1 でのエリア ID　：0.0.0.1
- バックボーンエリアへの集約経路設定　：10.20.0.0/16

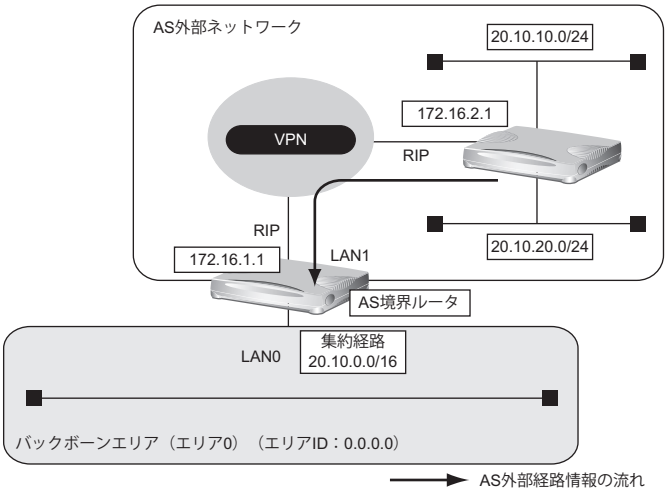
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
OSPF で使用するインタフェースを設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1

集約経路を設定する
# ospf ip area 1 range 0 10.20.0.0/16

設定終了
# save
# commit
```

2.4.2　AS外部経路を集約してOSPFネットワークに広報する

AS外部（OSPF以外）のネットワークの経路情報を本装置（AS境界ルータ）で集約して、バックボーンエリアに広報する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスの設定がされている
- LAN1インタフェースにRIPv2を使用する設定がされている

● 経路情報の設計

- AS外部経路情報を本装置（AS境界ルータ）でOSPFネットワーク（バックボーンエリア）に広報する

● 設定条件

- LAN0でのルーティングプロトコル　：OSPF
- LAN0でのエリアID　：0.0.0.0
- バックボーンエリアへの集約経路設定　：20.10.0.0/16
- OSPFに再配布するRIP経路　：20.10.0.0/16でマスクした結果が一致する経路だけを再配布

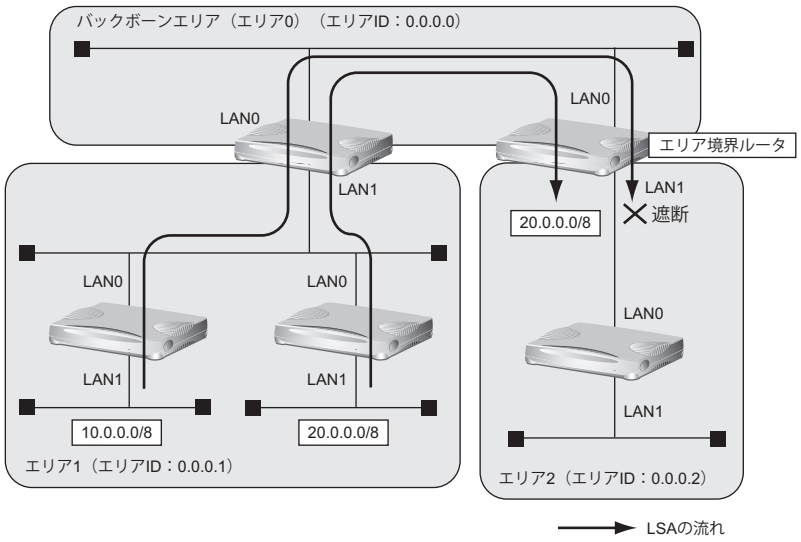
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
OSPF で使用するインタフェースを設定する
# lan 0 ip ospf use on 0

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0

OSPF に広報する AS 外部経路を設定する
# routemanage ip redist ospf rip on

集約経路を設定する
# ospf ip summary 0 20.10.0.0/16

不要な AS 外部経路情報を遮断する
# ospf ip redist 0 pass 20.10.0.0/16 inexact
# ospf ip redist 1 reject any

設定終了
# save
# commit
```

2.4.3　エリア境界ルータで不要な経路情報（LSA）を遮断する

エリア境界ルータで、通信に使用しないTYPE3サマリLSAの経路情報を遮断する設定方法を説明します。



● 経路情報の設計

- エリア１の10.0.0.0/8のネットワークとエリア２のネットワークでは通信を行わないため、10.0.0.0/8の経路情報を遮断する
- その他はすべて透過させる

● 設定条件

- LAN0でのルーティングプロトコル　：OSPF
- LAN1でのルーティングプロトコル　：OSPF
- LAN0でのエリアID　：0.0.0.0
- LAN1でのエリアID　：0.0.0.2
- 10.0.0.0/8のLSAを遮断

上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
OSPFで使用するインタフェースを設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2

エリア２に注入する経路情報を制限する
# ospf ip area 1 type3-lsa 0 reject 10.0.0.0/8 in exact
# ospf ip area 1 type3-lsa 1 pass any in

設定終了
# save
# commit
```

2.5　BGP の経路を制御する（IPv4）

本装置を経由して、ほかのルータに送受信する経路情報に変更を加えることで、意図的にトラフィックを制御することができます。

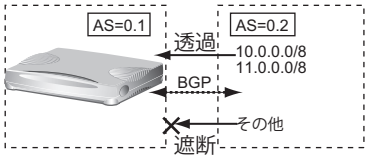
☛参照 マニュアル「機能説明書」

こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- 送信時のフィルタを設定した場合、相手装置に広報する MED メトリック値、AS パスプリペンドはフィルタの設定値が使用されます。
- MED メトリック値の設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- AS パスプリペンドの設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- BGP 使用中に commit コマンドを実行した場合、接続中のセッションが一度切断されることがあります。
- 動的定義反映で BGP IPv4 フィルタを設定した場合、動的定義反映後に送受信する経路情報に対してフィルタリングを実施します。動的定義反映前に送受信した経路情報に対してフィルタリングを実施する場合は、BGP IPv4 セッションのクリア機能を使用してください。

2.5.1　特定の経路情報の受信を透過させる

通信が必要なネットワークに限定して経路を透過させる場合の設定方法を説明します。



● 経路情報の設計

- 10.0.0.0/8 のネットワークの経路情報を透過
- 11.0.0.0/8 のネットワークの経路情報を透過
- その他はすべてを遮断

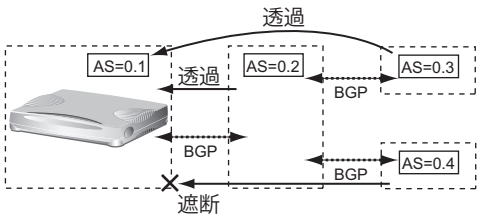
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
フィルタリング条件を設定する
# bgp neighbor 0 ip filter 0 act pass in
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 1 act pass in
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 2 act reject in
# bgp neighbor 0 ip filter 2 route any

設定終了
# save
# commit
```

2.5.2　特定の AS からの経路情報の受信を遮断する

フルルートを受信するネットワーク（トランジット）に接続されている場合、特定の経路情報を遮断する場合の設定方法を説明します。



● 経路情報の設計

- AS0.4 からの経路情報を遮断
- その他はすべて透過

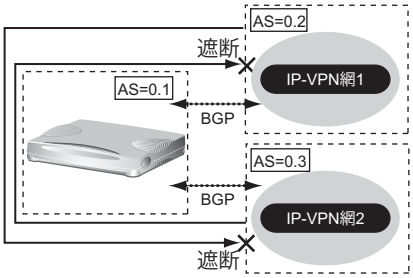
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
フィルタリング条件を設定する
# bgp neighbor 0 ip filter 0 act reject in
# bgp neighbor 0 ip filter 0 as 0.4
# bgp neighbor 0 ip filter 1 act pass in
# bgp neighbor 0 ip filter 1 route any

設定終了
# save
# commit
```

2.5.3　IP-VPN網からの受信情報の他IP-VPN網への送信を遮断する

異なるIP-VPN網を使用し、冗長化ネットワークを構成する場合、IP-VPN網１から受信した経路情報のIP-VPN網２への送信を遮断、およびIP-VPN網２から受信した経路情報のIP-VPN網１への送信を遮断する場合の設定方法を説明します。



● 経路情報の設計

- AS0.2からAS0.3への経路情報を遮断
- AS0.3からAS0.2への経路情報を遮断

上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

フィルタリング条件を設定する

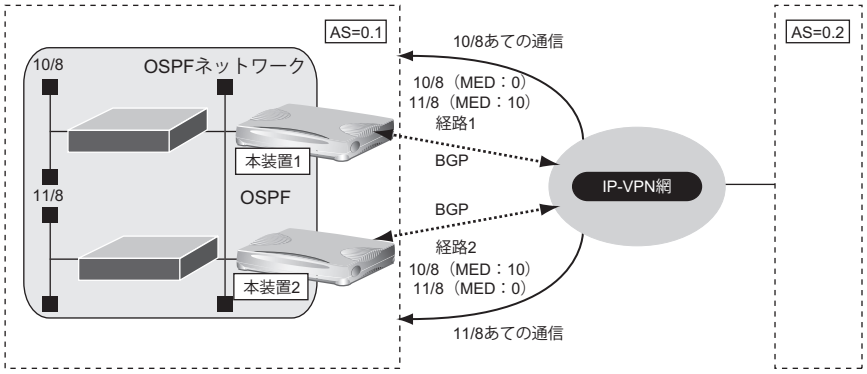
IP-VPN網１への送信を遮断する
```
# bgp neighbor 0 ip filter 0 act reject out
# bgp neighbor 0 ip filter 0 as 0.3
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route any
```

IP-VPN網２への送信を遮断する
```
# bgp neighbor 1 ip filter 0 act reject out
# bgp neighbor 1 ip filter 0 as 0.2
# bgp neighbor 1 ip filter 1 act pass out
# bgp neighbor 1 ip filter 1 route any
```

設定終了
```
# save
# commit
```

2.5.4　冗長構成の通信経路を使用する

IP-VPN 網に接続する経路を 2 つ使用した冗長構成で、通信の負荷分散および通信網異常による経路切り替えを行う場合の設定方法を説明します。



● 経路情報の設計

- OSPF ネットワークである AS0.1 で IP-VPN 網を経由した AS0.2 への通信経路を冗長化する
- 10/8 への通信は経路 1 を優先経路とし、11/8 への通信経路は経路 2 を優先経路とする。それぞれの経路で異常が発生した場合、異常が発生していない経路に切り替わる。優先順位を設定するときは MED メトリック値を使用する
- AS0.1 内の OSPF ネットワークでの経路変更は BGP で AS0.2 に広報する

上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

[本装置 1]

```
経路情報に MED メトリック値を付加する
# bgp neighbor 0 ip filter 0 act pass out
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 0 set medmetric 0
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 1 set medmetric 10

その他のすべての経路は透過する
# bgp neighbor 0 ip filter 2 act pass out
# bgp neighbor 0 ip filter 2 route any

BGP で OSPF 経路を広報する
# routemanage ip redist bgp ospf on

設定終了
# save
# commit
```

[本装置 2]

```
経路情報に MED メトリック値を付加する
# bgp neighbor 0 ip filter 0 act pass out
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 0 set medmetric 10
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 1 set medmetric 0

その他のすべての経路は透過する
# bgp neighbor 0 ip filter 2 act pass out
# bgp neighbor 0 ip filter 2 route any

BGP で OSPF 経路を広報する
# routemanage ip redist bgp ospf on

設定終了
# save
# commit
```

2.6　マルチキャスト機能を使う

本装置には、マルチキャスト機能を動作させるために以下の２種類のプロトコルがあります。

- PIM-DM プロトコル
- PIM-SM プロトコル

また、本装置では、ルーティングプロトコルは使用しないで、スタティックにマルチキャスト経路を設定することもできます。

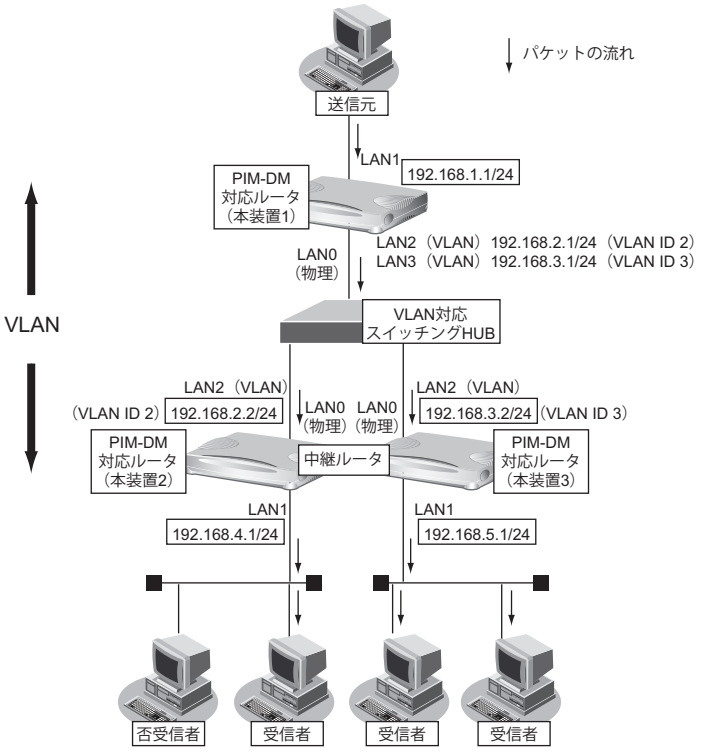
☛参照 マニュアル「機能説明書」

2.6.1　マルチキャスト機能（PIM-DM）を使う

マルチキャスト機能（PIM-DM）を使用すると、会社などのLAN内で、動画や音声などを配送することができます。

こんな事に気をつけて

- マルチキャストでパケットを配送するルータは、すべてPIM-DMに対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。
- IPアドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側IPアドレスと相手側IPアドレスの両方を正しく設定する必要があります。



ここでは、PIM-DMを利用してマルチキャスト・パケットを転送する場合の設定方法を説明します。

● 設定条件

- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：2　ネットワークアドレス：192.168.2.0/24
  VLAN ID：3　ネットワークアドレス：192.168.3.0/24
- マルチキャスト・ルーティングプロトコルには PIM-DM を利用する

[本装置 1]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2、LAN3 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1 の IP アドレス　：192.168.1.1/24
- LAN2 の IP アドレス　：192.168.2.1/24
- LAN3 の IP アドレス　：192.168.3.1/24

[本装置 2]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1 の IP アドレス　：192.168.4.1/24
- LAN2 の IP アドレス　：192.168.2.2/24

[本装置 3]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1 の IP アドレス　：192.168.5.1/24
- LAN2 の IP アドレス　：192.168.3.2/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
LANポートを削除する
# delete lan

LAN 0ポートを設定する
# lan 0 mode auto

192.168.1.0/24のネットワークを設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip multicast mode pimdm

192.168.2.0/24のネットワークを設定する
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 2

192.168.3.0/24のネットワークを設定する
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimdm
# lan 3 vlan bind 0
# lan 3 vlan tag vid 3

設定終了
# save
# commit
```

[本装置2]

```
LANポートを削除する
# delete lan

LAN 0ポートを設定する
# lan 0 mode auto

192.168.4.0/24のネットワークを設定する
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode pimdm

192.168.2.0/24のネットワークを設定する
# lan 2 ip address 192.168.2.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 2

設定終了
# save
# commit
```

[本装置 3]

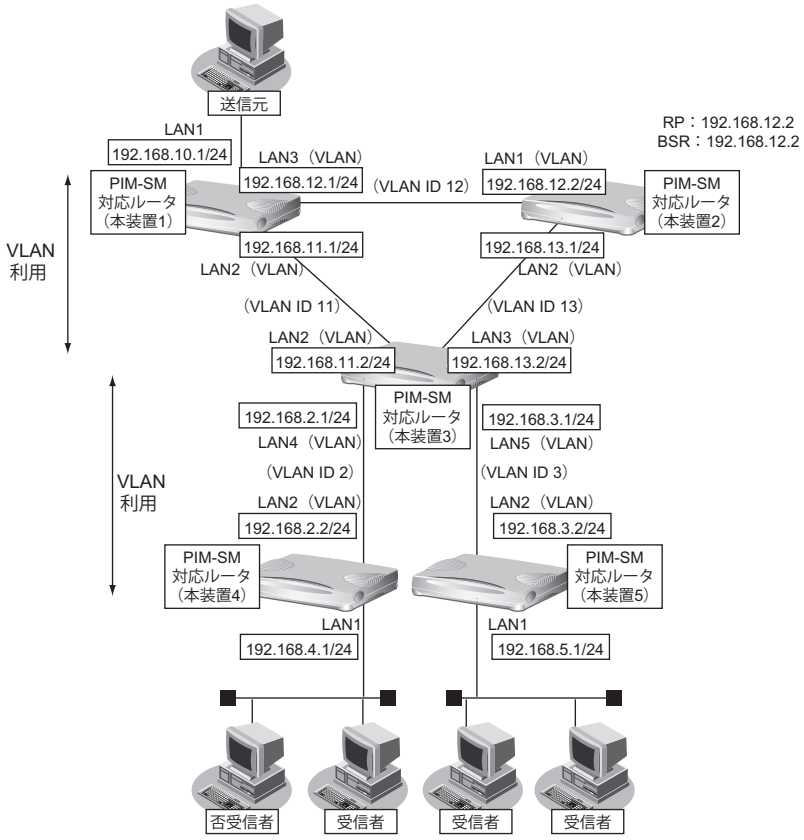
```
LAN ポートを削除する
# delete lan

LAN 0 ポートを設定する
# lan 0 mode auto

192.168.5.0/24 のネットワークを設定する
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode pimdm

192.168.3.0/24 のネットワークを設定する
# lan 2 ip address 192.168.3.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 3

設定終了
# save
# commit
```

2.6.2　マルチキャスト機能（PIM-SM）を使う

マルチキャスト機能（PIM-SM）を使用すると、インターネットなど、十分な帯域を保証されないネットワーク上で、マルチキャスト・パケットを配送することができます。

こんな事に気をつけて

- マルチキャスト・パケットを配送するルータは、すべて PIM-SM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。
- IPアドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側IPアドレスと相手側IPアドレスの両方を正しく設定する必要があります。
- ネットワーク内にBSR（Bootstrap Router：ブートストラップルータ）として動作するルータを１台以上置く必要があります。BSRはRP（Rendezvous Point：ランデブーポイント）の情報を広報します。
- ネットワーク内にRPとして動作するルータを１台以上置く必要があります。パケットの配送は、RPを配送樹の頂点として開始され、その後、最短経路（SPT：Shortest Path Tree）に切り替わります。
- PIM-SMではマルチキャスト・パケットの配送をRPを配送樹の頂点として開始するため、RPはネットワークの中心付近に置くことをお勧めします。
- SPTへの切り替えは、マルチキャスト・パケットの受信者の直前のルータ（lasthop router）が行います。lasthop routerで設定することでSPTへの切り替えを無効にすることができます。



ここでは、PIM-SMを利用してマルチキャスト・パケットを転送する場合の設定方法を説明します。

この設定例では、VLANを利用して、上図のネットワークを仮想的に構築します。

マルチキャスト・パケットは、はじめはRPである本装置２を経由して、本装置１→本装置２→本装置３→本装置４の順に配送されます（一度、本装置１から本装置２に送られ、本装置２を配送樹の頂点として配送されます）。本装置４へのパケット転送開始直後に、本装置４はSPTへの切り替えを開始します。切り替えが行われると、本装置１→本装置３→本装置４のように、最短経路を利用して配送されます（本装置１を配送樹の頂点として配送されます）。同様の切り替えが本装置５でも行われます。

● 設定条件

- VLAN IDとネットワークアドレスを以下のように対応付ける
  VLAN ID：2　ネットワークアドレス：192.168.2.0/24
  VLAN ID：3　ネットワークアドレス：192.168.3.0/24
  VLAN ID：11　ネットワークアドレス：192.168.11.0/24
  VLAN ID：12　ネットワークアドレス：192.168.12.0/24
  VLAN ID：13　ネットワークアドレス：192.168.13.0/24
- マルチキャスト・ルーティングプロトコルにはPIM-SMを利用する
  ユニキャストのルーティングテーブルの作成にRIPを使用する
  RP　：本装置2（192.168.12.2）
  BSR　：本装置2（192.168.12.2）
- SPTへの切り替えを行う（初期値）

[本装置1]

- マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2、LAN3を使用する
- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス　：192.168.10.1/24
- LAN2のIPアドレス　：192.168.11.1/24
- LAN3のIPアドレス　：192.168.12.1/24

[本装置2]

- マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する
- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN1、LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス　：192.168.12.2/24
- LAN2のIPアドレス　：192.168.13.1/24
- RP　：192.168.12.2
- BSR　：192.168.12.2

[本装置3]

- マルチキャスト・パケットを転送するインタフェースとしてLAN2、LAN3、LAN4、LAN5を使用する
- LAN0、LAN1はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN4、LAN5はVLANとし、出力先の物理インタフェースはLAN1とする
- LAN2のIPアドレス　：192.168.11.2/24
- LAN3のIPアドレス　：192.168.13.2/24
- LAN4のIPアドレス　：192.168.2.1/24
- LAN5のIPアドレス　：192.168.3.1/24

[本装置4]

- マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する
- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス　：192.168.4.1/24
- LAN2のIPアドレス　：192.168.2.2/24

[本装置 5]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.5.1/24
- LAN2 の IP アドレス　：192.168.3.2/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置 1]

```
LAN ポートを削除する
# delete lan

LAN 0 ポートを設定する
# lan 0 mode auto

192.168.10.0/24 のネットワークを設定する
# lan 1 ip address 192.168.10.1/24 3
# lan 1 ip multicast mode pimsm

192.168.11.0/24 のネットワークを設定する
# lan 2 ip address 192.168.11.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 11

192.168.12.0/24 のネットワークを設定する
# lan 3 ip address 192.168.12.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan bind 0
# lan 3 vlan tag vid 12

設定終了
# save
# commit
```

[本装置 2]

```
LAN ポートを削除する
# delete lan

LAN 0 ポートを設定する
# lan 0 mode auto

192.168.12.0/24 のネットワークを設定する
# lan 1 ip address 192.168.12.2/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimsm
# lan 1 vlan bind 0
# lan 1 vlan tag vid 12

192.168.13.0/24 のネットワークを設定する
# lan 2 ip address 192.168.13.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 13

マルチキャストを設定する
# multicast ip pimsm candrp mode on
# multicast ip pimsm candrp address 192.168.12.2
# multicast ip pimsm candbsr mode on
# multicast ip pimsm candbsr address 192.168.12.2

設定終了
# save
# commit
```

[本装置 3]

```
LAN ポートを削除する
# delete lan

LAN 0、LAN 1 ポートを設定する
# lan 0 mode auto
# lan 1 mode auto

192.168.11.0/24 のネットワークを設定する
# lan 2 ip address 192.168.11.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 11

192.168.13.0/24 のネットワークを設定する
# lan 3 ip address 192.168.13.2/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan bind 0
# lan 3 vlan tag vid 13

192.168.2.0/24 のネットワークを設定する
# lan 4 ip address 192.168.2.1/24 3
# lan 4 ip rip use v2 v2 0 on
# lan 4 ip multicast mode pimsm
# lan 4 vlan bind 1
# lan 4 vlan tag vid 2

192.168.2.0/24 のネットワークを設定する
# lan 5 ip address 192.168.3.1/24 3
# lan 5 ip rip use v2 v2 0 on
# lan 5 ip multicast mode pimsm
# lan 5 vlan bind 1
# lan 5 vlan tag vid 3

設定終了
# save
# commit
```

[本装置4]

```
LANポートを削除する
# delete lan

LAN 0ポートを設定する
# lan 0 mode auto

192.168.4.0/24のネットワークを設定する
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode pimsm

192.168.2.0/24のネットワークを設定する
# lan 2 ip address 192.168.2.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 2

設定終了
# save
# commit
```

[本装置5]

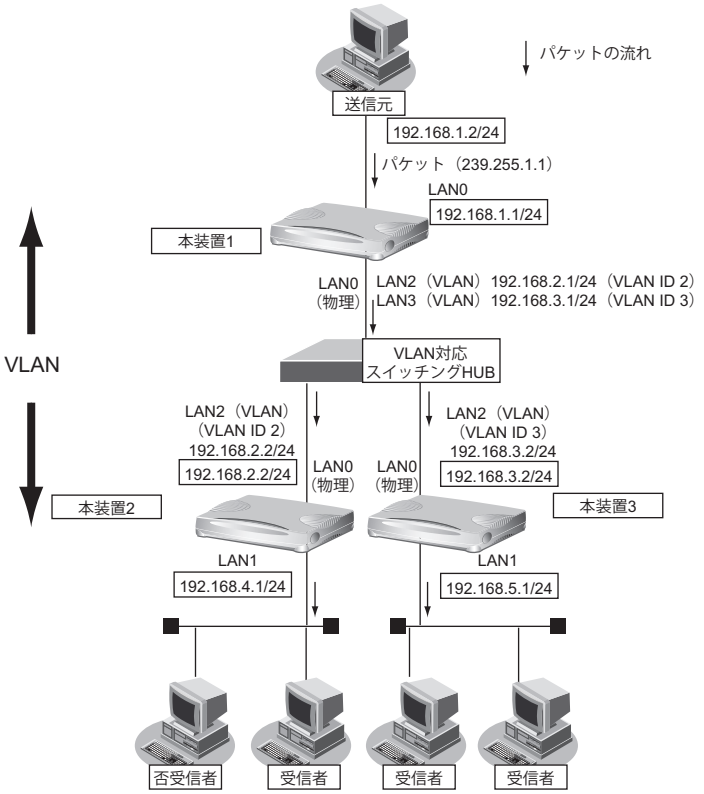
```
LANポートを削除する
# delete lan

LAN 0ポートを設定する
# lan 0 mode auto

192.168.5.0/24のネットワークを設定する
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode pimsm

192.168.3.0/24のネットワークを設定する
# lan 2 ip address 192.168.3.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 3

設定終了
# save
# commit
```

2.6.3　マルチキャスト機能（スタティックルーティング）を使う

マルチキャスト機能（スタティックルーティング）を利用すると、マルチキャストパケットが配送される経路を静的に設定することができます。

こんな事に気をつけて

マルチキャスト・スタティックルーティングでは、入力インタフェースでのIGMPグループ参加を指定することができます。
上流側にPIM-DMなどのIGMP参加要求を受け付けるマルチキャスト・ルータが存在する場合は、入力インタフェースでIGMPグループ参加を行うこと、パケットを強制的に転送させることができます。



ここでは、スタティックルーティングを利用してマルチキャストパケットの転送を行う場合を例に説明します。

● 設定条件

- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける
  VLAN ID：2　　ネットワークアドレス：192.168.2.0/24
  VLAN ID：3　　ネットワークアドレス：192.168.3.0/24
- マルチキャスト・スタティックルーティングを利用する
- マルチキャストパケットの送信元アドレスは 192.168.1.2 とする
- マルチキャストパケットのグループアドレスは 239.255.1.1 とする
- 入力インタフェースでのIGMPグループ参加は行わない

[本装置 1]

- マルチキャストパケットを転送するインタフェースとして LAN1、LAN2、LAN3 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.1.1/24
- LAN2 の IP アドレス　：192.168.2.1/24
- LAN3 の IP アドレス　：192.168.3.1/24

[本装置 2]

- マルチキャストパケットを転送するインタフェースとして LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.4.1/24
- LAN2 の IP アドレス　：192.168.2.2/24

[本装置 3]

- マルチキャストパケットを転送するインタフェースとして LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.5.1/24
- LAN2 の IP アドレス　：192.168.3.2/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置 1]

```
LAN ポートを削除する
# delete lan

LAN0 ポートを設定する
# lan 0 mode auto

192.168.1.0/24 のネットワークの設定をする
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip multicast mode static

192.168.2.0/24 のネットワークの設定をする
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip multicast mode static
# lan 2 vlan bind 0
# lan 2 vlan tag vid 2

192.168.3.0/24 のネットワークの設定をする
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip multicast mode static
# lan 3 vlan bind 0
# lan 3 vlan tag vid 3

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan1 lan2-lan3 off

設定終了
# save
# commit
```

[本装置 2]

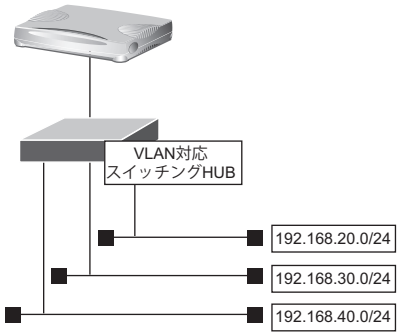
```
LAN ポートを削除する
# delete lan

LAN0 ポートを設定する
# lan 0 mode auto

192.168.4.0/24 のネットワークの設定をする
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode static

192.168.2.0/24 のネットワークの設定をする
# lan 2 ip address 192.168.2.2/24 3
# lan 2 ip multicast mode static
# lan 2 vlan bind 0
# lan 2 vlan tag vid 2

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan2 lan1

設定終了
# save
# commit
```

[本装置 3]

```
LAN ポートを削除する
# delete lan

LAN0 ポートを設定する
# lan 0 mode auto

192.168.5.0/24 のネットワークの設定をする
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode static

192.168.3.0/24 のネットワークの設定をする
# lan 2 ip address 192.168.3.2/24 3
# lan 2 ip multicast mode static
# lan 2 vlan bind 0
# lan 2 vlan tag vid 3

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan2 lan1

設定終了
# save
# commit
```

2.7　VLAN 機能を使う

ここでは、VLAN 機能を利用して、１つの物理ポートで３つのネットワークを組む場合を例に説明します。



☛参照 マニュアル「機能説明書」

● 設定条件

- LAN0 ポートを使用する
- VLAN ID として 2、3、4 を使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：2　　ネットワークアドレス：192.168.20.0/24
  VLAN ID：3　　ネットワークアドレス：192.168.30.0/24
  VLAN ID：4　　ネットワークアドレス：192.168.40.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
LAN0 ポートを設定する
# delete lan
# lan 0 mode auto

VLAN ID 2 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 ip rip use v1 v1 0 off
# lan 1 vlan bind 0
# lan 1 vlan tag vid 2

VLAN ID 3 のネットワークを設定する
# lan 2 ip address 192.168.30.1/24 3
# lan 2 ip rip use v1 v1 0 off
# lan 2 vlan bind 0
# lan 2 vlan tag vid 3

VLAN ID 4 のネットワークを設定する
# lan 3 ip address 192.168.40.1/24 3
# lan 3 ip rip use v1 v1 0 off
# lan 3 vlan bind 0
# lan 3 vlan tag vid 4

設定終了
# save
```

再起動
reset

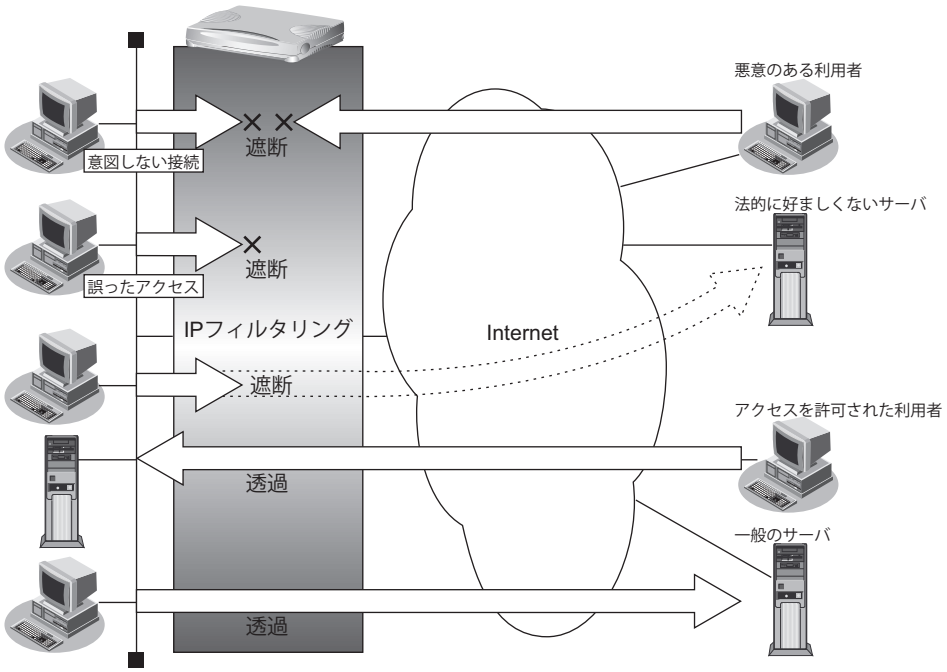
こんな事に気をつけて

- VLAN 機能を利用すると、Ethernet フレームに 4 バイトの VLAN タグが付加され、最大 1522 バイトの Ethernet フレームが送出されることになります。通常の Ethernet フレームの最大サイズは 1518 バイトです。そのため、その状態では 1522 バイトのフレームに対応していない機器とは接続することはできません。1522 バイトのフレームに対応していない機器と接続する場合は、VLAN インタフェースの MTU サイズを 1496 に変更してください。
- VLAN インタフェース上では、シェーピングおよび帯域制御（WFQ）の機能を利用することはできません。
- VLAN の物理インタフェースに、VLAN インタフェースを使用することはできません。
- 同じ物理インタフェースを使用する複数の VLAN インタフェース上で、重複する VLAN ID を使用することはできません。
- VLAN 対応スイッチング HUB やルータ製品の中には、VLAN が設定されていない LAN ポートで、VLAN タグ付きフレームを受信してしまう装置があります。
  このような装置と接続する際には、スイッチング HUB（またはルータ）の設定を「VLAN あり」から「VLAN なし」に設定を変更してください。
  また、フレームを送信する PC の arp エントリが本装置に残っていると、arp エントリの生存時間中だけ通信するという現象が発生する場合があります。これを防ぐために、設定後に本装置で commit コマンドを実行してください。
- VLAN を利用する物理インタフェースの LAN 情報では、lan mode コマンドで動作モードを必ず設定してください。
  lan mode コマンドで動作モードの設定がなく、その他の LAN 情報で設定する値もすべて初期値とした場合、その LAN 情報は保存されないため、通信ができなくなります。

2.8　IP フィルタリング機能を使う

参照 マニュアル「機能説明書」

本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットをIPアドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、回線への超過課金を防止することができます。



IP フィルタリングの条件

本装置では、以下の条件を指定することによって、データの流れを制御できます。

- 動作
- プロトコル
- 送信元情報（IPアドレス／アドレスマスク／ポート番号）
- あて先情報（IPアドレス／アドレスマスク／ポート番号）
- TCP 接続要求
- TOS 値
- 方向

ヒント

◆ TCP 接続要求とは

TCP プロトコルでのコネクション確立要求を、フィルタリングの対象にするかどうか指定するものです。フィルタリングの動作に透過、プロトコルに TCP を指定した場合に有効です。TCP プロトコルはコネクション型であるため、コネクション確立要求を発行し、それに対する応答を受信することによって、コネクションを開設します。したがって、一方からのコネクションを禁止する場合でも、コネクション確立要求だけを遮断し、その他の応答や通常データなどを透過させるように設定しないと通信できません。

次に、TCP パケットとフラグ設定について説明します。TCP パケット内には SYN フラグと ACK フラグの２つの制御フラグがあります。このフラグの組み合わせによって、TCP パケットの内容が分かります。以下に、対応表を示します。

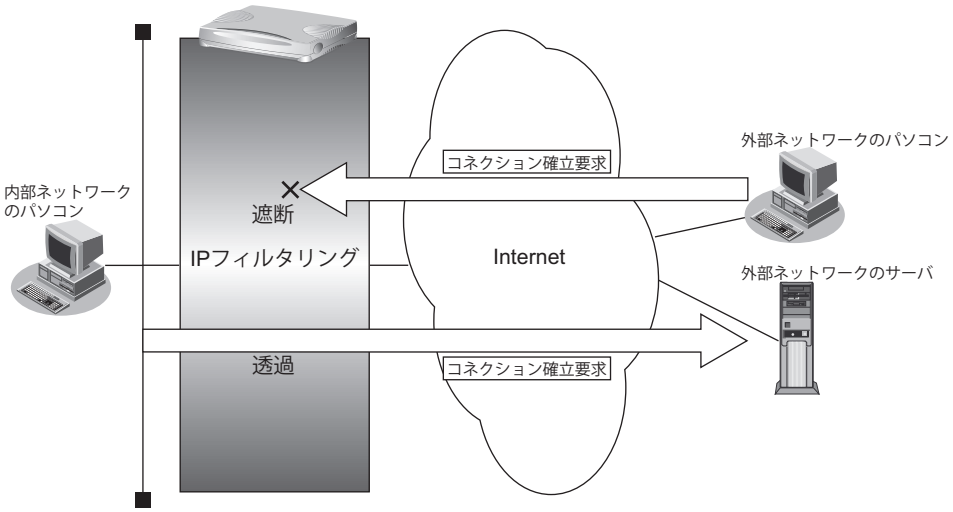
制御フラグ		TCP パケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

この表から、制御フラグの組み合わせが SYN ＝ 1、ACK ＝ 0 の場合に、TCP パケットがコネクションの確立要求を行うことが分かります。つまり、IP パケットが禁止されている IP アドレスからの送信を禁止すれば、TCP/IP サービスのフィルタリングを行えます。

以下に、telnet（ポート番号 23）を例に説明します。

・外部ネットワークからのコネクション確立要求は遮断

・内部ネットワークからのコネクション確立要求は透過



◆ IP アドレスとアドレスマスクの決め方

IP フィルタリング条件の要素には「IP アドレス」と「アドレスマスク」があります。制御対象となるパケットは、本装置に届いたパケットの IP アドレスとアドレスマスクの論理積の結果が、指定した IP アドレスと一致したものに限ります。

◆ IP フィルタリングの方向

IP フィルタリングの方向に「リバース（reverse)」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象になります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

- 送信元 IP アドレス／アドレスマスクとあて先 IP アドレス／アドレスマスク
- 送信元ポート番号とあて先ポート番号

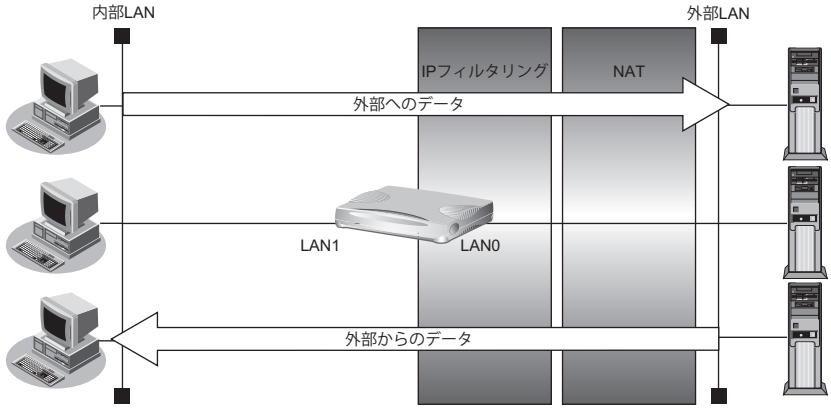
補足 IP フィルタリング機能と NAT 機能を併用する場合、回線切断時に NAT 機能の情報が消えてしまうため、回線切断後に再度接続しても、サーバからの応答が正しくアドレス変換されず、IP フィルタリング機能によってパケットは破棄されてしまいます。

ヒント

◆ アドレス変換（NAT）機能利用時の IP フィルタリングのかかるタイミング

内部 LAN から外部 LAN に向かう場合は、アドレス変換でアドレスが変更される前に IP フィルタリング処理を通過します。また、外部 LAN から内部 LAN に向かう場合は、アドレス変換でアドレスが変更されたあとで、IP フィルタリング処理を通過します。つまり、IP フィルタリングは「プライベートアドレス」を対象に行います。

本装置の IP フィルタリングとアドレス変換の位置付けは以下のとおりです。



IP フィルタリングの設計方針

IP フィルタリングの設計方針には大きく分類して以下の２つがあります。

A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる。

B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する。

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけ許可して SPI を併用する
- 外部の特定サービスへのアクセスだけを許可する（IPv6 フィルタリング）

また、設計方針Bの例として、以下の設定例について説明します。

- 外部の特定サーバへのアクセスだけを禁止する
- 利用者が意図しない発信を防ぐ
- 回線が接続しているときだけ許可する

補足 TCP 接続要求の設定は、プロトコルに TCP またはすべてを指定した場合にだけ有効です。それ以外のプロトコルを指定した場合は無効となります。

こんな事に気をつけて

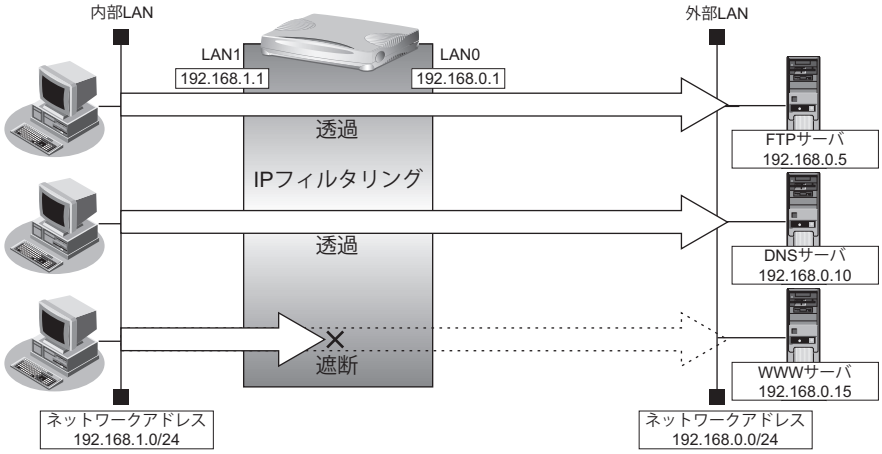
- IP フィルタリングで WWW（ポート番号 80）でのアクセスを制限する設定を行った場合、外部の WWW ブラウザからアクセスができなくなる場合があります。
- IP フィルタリングで DHCP（ポート番号 67、68）でのアクセスを制限する設定を行った場合、DHCP 機能が使用できなくなる場合があります。
- IP フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。PPPoE の場合は、remote 側にフィルタをかけるようにしてください。
- IP フィルタリングの方向に「reverse」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象になります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス／アドレスマスクとあて先 IP アドレス／アドレスマスク
  - 送信元ポート番号とあて先ポート番号

2.8.1　外部の特定サービスへのアクセスだけを許可する

LAN 定義の場合

ここでは、一時的に LAN を作成し、外部 LAN のすべての FTP サーバに対してアクセスすることだけを許可し、ほかのサーバ（WWW サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために、DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でドメイン名を指定した場合も DNS サーバへの発信が発生します。あらかじめ接続する FTP サーバが決まっている場合は、本装置の DNS サーバ機能を利用することによって、DNS サーバへの発信を抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.0/24）から外部 LAN の FTP サーバへのアクセスを許可
- 内部 LAN のホスト（192.168.1.0/24）から外部 LAN への DNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには

  (1) 192.168.1.0/24 の任意のポートから、任意の FTP サーバのポート 21（ftp）への TCP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには

  (1) 192.168.1.0/24 の任意のポートから、DNS サーバのポート 53（domain）への UDP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- ICMP の通信を許可するためには

  (1) ICMP パケットを透過させる

- その他をすべて遮断するには
  (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

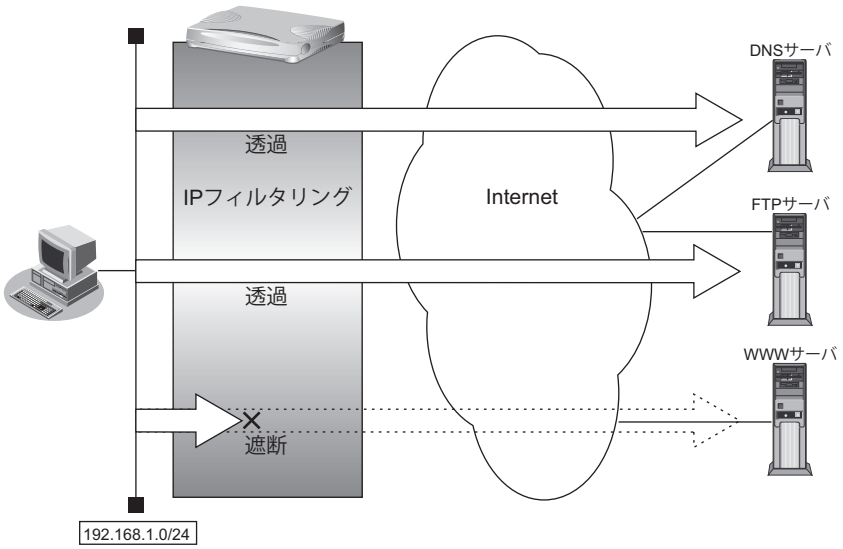
● コマンド

```
任意のFTPサーバのポート21へのTCPパケットを透過させる
# acl 0 ip 192.168.1.0/24 any 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

FTPサーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ip 192.168.1.0/24 192.168.0.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNSサーバからの応答パケットを透過させる
# acl 3 ip 192.168.0.10/32 192.168.1.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMPのパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# lan 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

リモート定義の場合

ここでは、LAN 上のパソコンからインターネット上のすべての FTP サーバに対してアクセスすることだけを許可し、ほかのサーバ（WWW サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために、DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でドメイン名を指定した場合も DNS サーバへの発信が発生します。あらかじめ接続する FTP サーバが決まっている場合は、本装置の DNS サーバ機能を利用することによって、DNS サーバへの発信を抑止することができます。
- 本装置は、ftp-data の転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- LAN 上のホスト（192.168.1.0/24）から任意の FTP サーバへのアクセスを許可
- LAN 上のホスト（192.168.1.0/24）から WAN の先の DNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには

  (1) 192.168.1.0/24 の任意のポートから、任意の FTP サーバのポート 21（ftp）への TCP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには

  (1) 192.168.1.0/24 の任意のポートから、DNS サーバのポート 53（domain）への UDP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- ICMP の通信を許可するためには

  (1) ICMP パケットを透過させる
- その他をすべて遮断するには

  (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

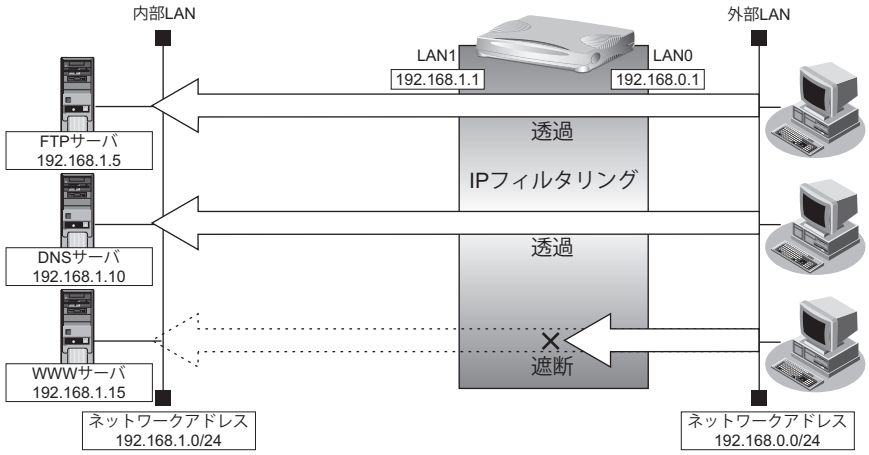
```
任意のFTPサーバのポート21へのTCPパケットを透過させる
# acl 0 ip 192.168.1.0/24 any 6
# acl 0 tcp any 21 yes
# remote 0 ip filter 0 pass acl 0 any

FTPサーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6
# acl 1 tcp 21 any no
# remote 0 ip filter 1 pass acl 1 any

DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ip 192.168.1.0/24 any 17
# acl 2 udp any 53
# remote 0 ip filter 2 pass acl 2 any

DNSサーバからの応答パケットを透過させる
# acl 3 ip any 192.168.1.0/24 17
# acl 3 udp 53 any
# remote 0 ip filter 3 pass acl 3 any

ICMPのパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# remote 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# remote 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

2.8.2　外部から特定サーバへのアクセスだけを許可する

LAN 定義の場合

ここでは、内部 LAN の特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でもドメイン名で指定されると DNS サーバへの問い合わせが発生します。あらかじめ接続する ftp サーバが決まっている場合は、本装置の DNS サーバ機能を利用することで、DNS サーバへの問い合わせを抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.5/32）を FTP サーバとして利用を許可
- 内部 LAN のネットワークへの DNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- 内部 LAN のホストの FTP サーバとしての利用を許可するには
  (1) 192.168.1.5/32 のポート 21（ftp）への TCP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  (1) 192.168.0.0/24 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- ICMP の通信を許可するためには
  (1) ICMP パケットを透過させる
- その他をすべて遮断するには
  (1) すべてのパケットを遮断する

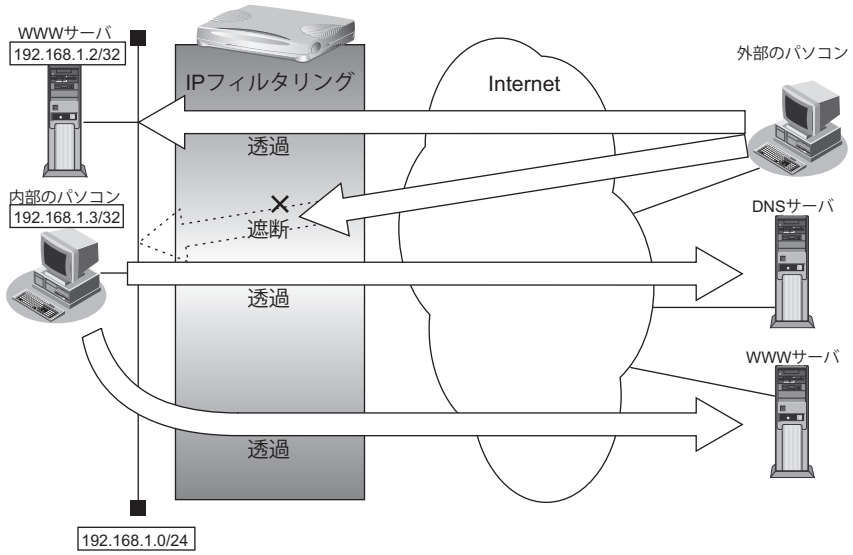
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
LAN 上のホストのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.0.0/24 192.168.1.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.5/32 192.168.0.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# lan 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

リモート定義の場合

ここでは、LAN上のWWWサーバに対する外部のパソコンからのアクセスを許可し、LAN上のほかのパソコンへのアクセスは禁止する場合の設定方法を説明します。また、LAN上のほかのパソコンはインターネット上のWWWサーバに対してアクセスすると想定されるため、そのアクセスには制限をつけません。



● フィルタリング設計

- LAN上のホスト（192.168.1.2/32）をWWWサーバとして利用することを許可
- LAN上のホスト（192.168.1.3/32）から任意のWWWサーバへのアクセスを許可
- LAN上のホスト（192.168.1.0/24）からWANの先のDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- LAN上のホストのWWWサーバとしての利用を許可するには
  (1) 192.168.1.2/32のポート80（www-http）へのパケットを透過させる
  (2) (1) の応答パケットを透過させる
- 任意のWWWサーバへのアクセスを許可するには
  (1) 192.168.1.3/32の任意のポートから任意のWWWサーバのポート80（www-http）へのパケットを透過させる
  (2) (1) の応答パケットを透過させる
- DNSサーバへのアクセスを許可するには
  (1) 192.168.1.0/24の任意のポートからDNSサーバのポート53（domain）へのUDPパケットを透過させる
  (2) (1) の応答パケットを透過させる
- ICMPの通信を許可するためには
  (1) ICMPパケットを透過させる
- その他をすべて遮断するには
  (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

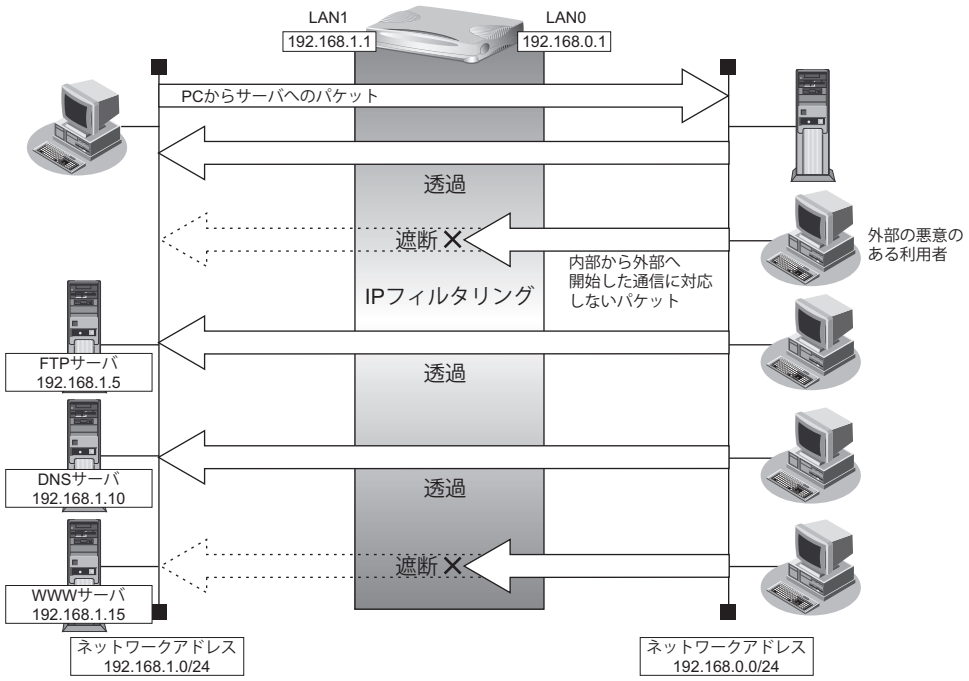
```
LAN 上のホストのポート 80 へのパケットを透過させる
# acl 0 ip any 192.168.1.2/32 6
# acl 0 tcp any 80 yes
# remote 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.2/32 any 6
# acl 1 tcp 80 any no
# remote 0 ip filter 1 pass acl 1 any

任意の WWW サーバのポート 80 へのパケットを透過させる
# acl 2 ip 192.168.1.3/32 any 6
# acl 2 tcp any 80 yes
# remote 0 ip filter 2 pass acl 2 any

任意の WWW サーバからの応答パケットを透過させる
# acl 3 ip any 192.168.1.3/32 6
# acl 3 tcp 80 any no
# remote 0 ip filter 3 pass acl 3 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 4 ip 192.168.1.0/24 any 17
# acl 4 udp any 53
# remote 0 ip filter 4 pass acl 4 any

DNS サーバからの応答パケットを透過させる
# acl 5 ip any 192.168.1.0/24 17
# acl 5 udp 53 any
# remote 0 ip filter 5 pass acl 5 any

ICMP のパケットを透過させる
# acl 6 ip any any 1
# acl 6 icmp any any
# remote 0 ip filter 6 pass acl 6 any

残りのパケットをすべて遮断する
# acl 7 ip any any any
# remote 0 ip filter 7 reject acl 7 any

設定終了
# save
# commit
```

2.8.3 外部から特定サーバへのアクセスだけを許可して SPI を併用する

LAN 定義の場合

ここでは、内部 LAN の特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止し、SPI を利用して外部へアクセスする場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でもドメイン名で指定されると DNS サーバへの問い合わせが発生します。あらかじめ接続する ftp サーバが決まっている場合は、本装置の DNS サーバ機能を利用することで、DNS サーバへの問い合わせを抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.5/32）を FTP サーバとして利用を許可
- 内部 LAN のネットワークへの DNS サーバへのアクセスを許可
- ICMP の通信を許可
- 内部 LAN から外部へ開始するアクセスを許可し、その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- 内部 LAN のホストの FTP サーバとしての利用を許可するには
  (1) 192.168.1.5/32 のポート 21（ftp）への TCP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  (1) 192.168.0.0/24 の任意ポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- ICMP の通信を許可するためには
  (1) ICMP パケットを透過させる
- 内部 LAN から外部へ開始するアクセスは許可し、その他をすべて遮断するには
  (1) 残りのパケットに SPI を利用して IP フィルタリングを行う

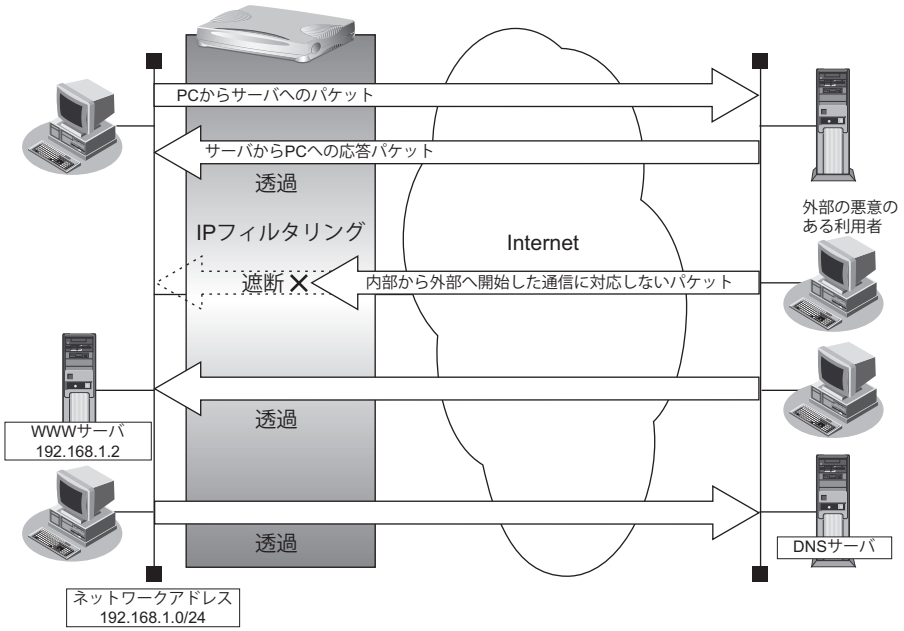
上記のフィルタリングルールに従って設定する場合のコマンド例を示します。

● コマンド

```
LAN 上のホストのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.0.0/24 192.168.1.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.5/32 192.168.0.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットに SPI を利用して IP フィルタリングを行う
# lan 0 ip filter default spi

設定終了
# save
# commit
```

リモート定義の場合

ここでは、外部から LAN 上の WWW サーバに対するアクセスを許可し、ほかの LAN 上のパソコンへのアクセスを禁止する場合の設定方法を説明します。また、LAN 上のほかのパソコンはインターネット上のサーバに対してアクセスしますが、これらのアクセスに対しては SPI による IP フィルタリングの対象とします。



● フィルタリング設計

- LAN 上のホスト（192.168.1.2/32）を WWW サーバとして利用を許可
- ICMP の通信を許可
- 内部 LAN から外部へ開始するアクセスは許可し、その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- 内部 LAN のホストの WWW サーバとしての利用を許可するには
  (1) 192.168.1.2/32 のポート 80（www-http）への TCP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- ICMP の通信を許可するためには
  (1) ICMP パケットを透過させる
- 内部 LAN から外部へ開始するアクセスは許可し、その他をすべて遮断するには
  (1) 残りのパケットに SPI を利用して IP フィルタリングを行う

上記のフィルタリングルールに従って設定する場合のコマンド例を示します。

● コマンド

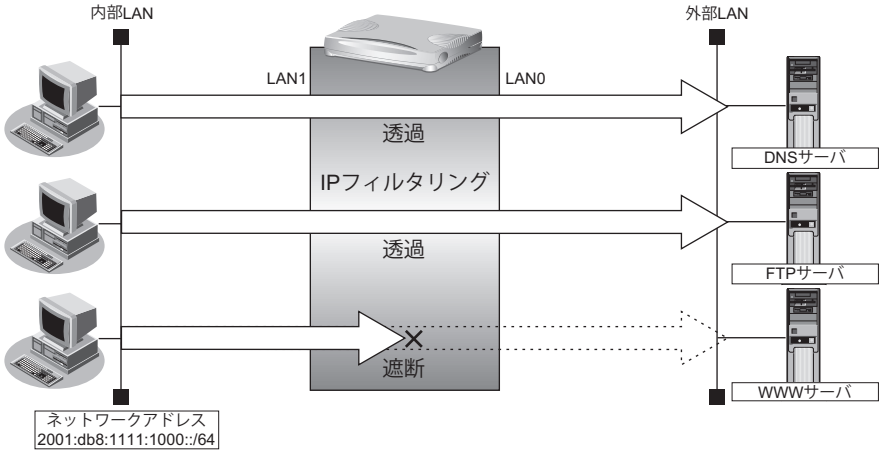
```
LAN 上のホストのポート 80 へのパケットを透過させる
# acl 0 ip any 192.168.1.2/32 6
# acl 0 tcp any 80 yes
# remote 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.2/32 any 6
# acl 1 tcp 80 any no
# remote 0 ip filter 1 pass acl 1 any

ICMP のパケットを透過させる
# acl 2 ip any any 1
# acl 2 icmp any any
# remote 0 ip filter 2 pass acl 2 any

残りのパケットに SPI を利用して IP フィルタリングを行う
# remote 0 ip filter default spi

設定終了
# save
# commit
```

2.8.4　外部の特定サービスへのアクセスだけを許可する（IPv6 フィルタリング）

LAN 定義の場合

ここでは、IPv6 フィルタリングを使って、内部 LAN 上のパソコンから外部 LAN 上のすべての FTP サーバに対してアクセスすることだけを許可し、ほかのサーバ（WWW サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスを許可する設定にします。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でもドメイン名で指定されると DNS サーバへの通信が発生します。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN 上のホスト（2001:db8:1111:1000::/64）から任意の FTP サーバへのアクセスを許可
- 内部 LAN 上のホスト（2001:db8:1111:1000::/64）から外部 LAN の DNS サーバへのアクセスを許可
- ICMPv6 の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6 は、IPv6 通信を行う際にさまざまな制御メッセージを交換します。ICMPv6 の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6 の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには
  (1) 2001:db8:1111:1000::/64 の任意のポートから、任意のアドレスのポート 21（ftp）への TCP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  (1) 2001:db8:1111:1000::/64 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  (2) (1) の応答パケットを透過させる

- ICMPv6 の通信を許可するためには
  (1) ICMPv6 パケットを透過させる
- その他をすべて遮断するには
  (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

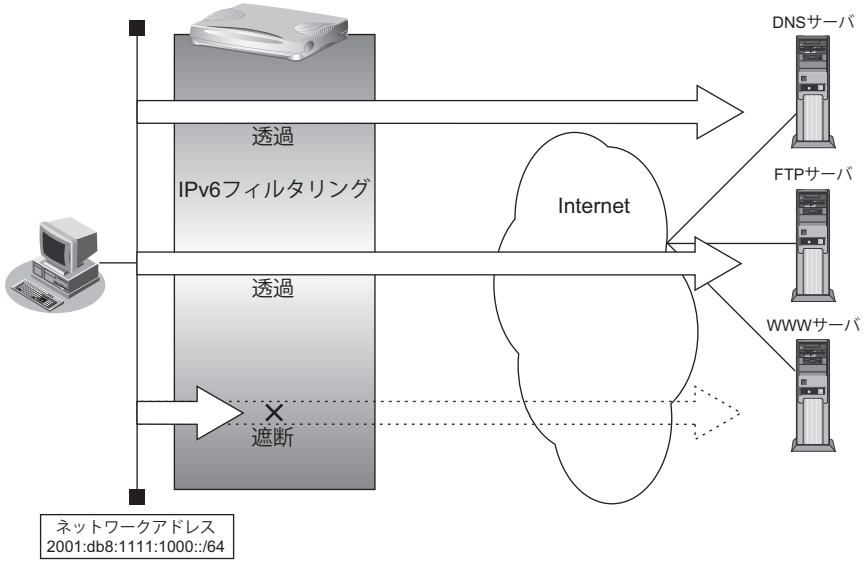
● コマンド

```
任意の FTP サーバのポート 21 への TCP パケットを透過させる
# acl 0 ip6 2001:db8:1111:1000::/64 any 6
# acl 0 tcp any 21 yes
# lan 0 ip6 filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ip6 any 2001:db8:1111:1000::/64 6
# acl 1 tcp 21 any no
# lan 0 ip6 filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip6 2001:db8:1111:1000::/64 any 17
# acl 2 udp any 53
# lan 0 ip6 filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip6 any 2001:db8:1111:1000::/64 17
# acl 3 udp 53 any
# lan 0 ip6 filter 3 pass acl 3 any

ICMPv6 のパケットを透過させる
# acl 4 ip6 any any 58
# acl 4 icmp any any
# lan 0 ip6 filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip6 any any any
# lan 0 ip6 filter 5 reject acl 5 any

設定終了
# save
# commit
```

リモート定義の場合

ここでは、IPv6フィルタリングを使って、LAN上のパソコンからイントラネット上のすべてのFTPサーバに対してアクセスすることだけを許可し、ほかのサーバ（WWWサーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ名を解決するためにDNSサーバへのアクセスを許可する設定にします。

補足
- ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でドメイン名を指定する場合もDNSサーバへの発信が発生します。
- 本装置はftp-data転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- LAN上のホスト（2001:db8:1111:1000::/64）から任意のFTPサーバへのアクセスを許可
- LAN上のホスト（2001:db8:1111:1000::/64）からWANの先のDNSサーバへのアクセスを許可
- ICMPv6の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6は、IPv6通信を行う際にさまざまな制御メッセージを交換します。ICMPv6の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTPサーバへのアクセスを許可するには
  (1) 2001:db8:1111:1000::/64の任意のポートから、任意のFTPサーバのポート21（ftp）へのTCPパケットを透過させる
  (2) (1) の応答パケットを透過させる
- DNSサーバへのアクセスを許可するには
  (1) 2001:db8:1111:1000::/64の任意のポートからDNSサーバのポート53（domain）へのUDPパケットを透過させる
  (2) (1) の応答パケットを透過させる
- ICMPv6の通信を許可するためには
  (1) ICMPv6パケットを透過させる

- その他をすべて遮断するには
  (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

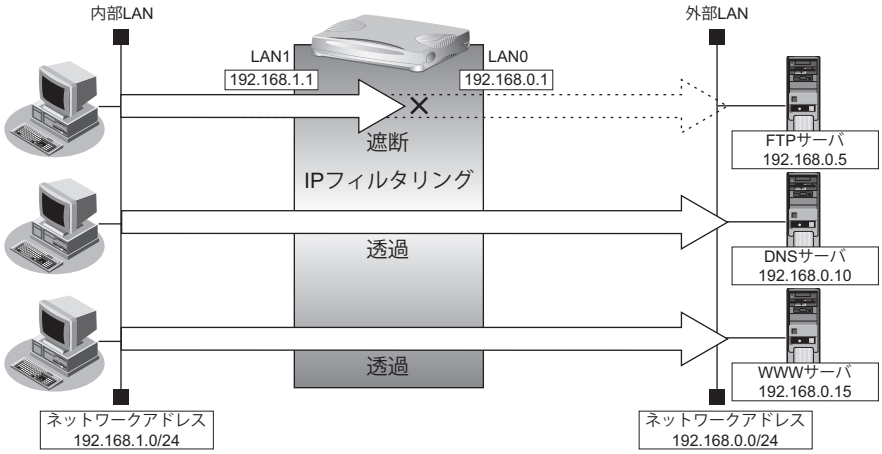
● コマンド

```
任意のFTPサーバのポート21へのTCPパケットを透過させる
# acl 0 ip6 2001:db8:1111:1000::/64 any 6
# acl 0 tcp any 21 yes
# remote 0 ip6 filter 0 pass acl 0 any

FTPサーバからの応答パケットを透過させる
# acl 1 ip6 any 2001:db8:1111:1000::/64 6
# acl 1 tcp 21 any no
# remote 0 ip6 filter 1 pass acl 1 any

DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ip6 2001:db8:1111:1000::/64 any 17
# acl 2 udp any 53
# remote 0 ip6 filter 2 pass acl 2 any

DNSサーバからの応答パケットを透過させる
# acl 3 ip6 any 2001:db8:1111:1000::/64 17
# acl 3 udp 53 any
# remote 0 ip6 filter 3 pass acl 3 any

ICMPv6のパケットを透過させる
# acl 4 ip6 any any 58
# acl 4 icmp any any
# remote 0 ip6 filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip6 any any any
# remote 0 ip6 filter 5 reject acl 5 any

設定終了
# save
# commit
```

2.8.5　外部の特定サーバへのアクセスだけを禁止する

LAN 定義の場合

ここでは、外部 LAN の FTP サーバに対するアクセスを禁止する場合の設定方法を説明します。



● フィルタリング設定

- 内部 LAN のホスト（192.168.1.0/24）から外部 LAN の FTP サーバ（192.168.0.5）へのアクセスを禁止

● フィルタリングルール

- FTP サーバへのアクセスを禁止するには

  (1) 192.168.1.0/24 から 192.168.0.5 のポート 21（ftp）への TCP パケットを遮断する

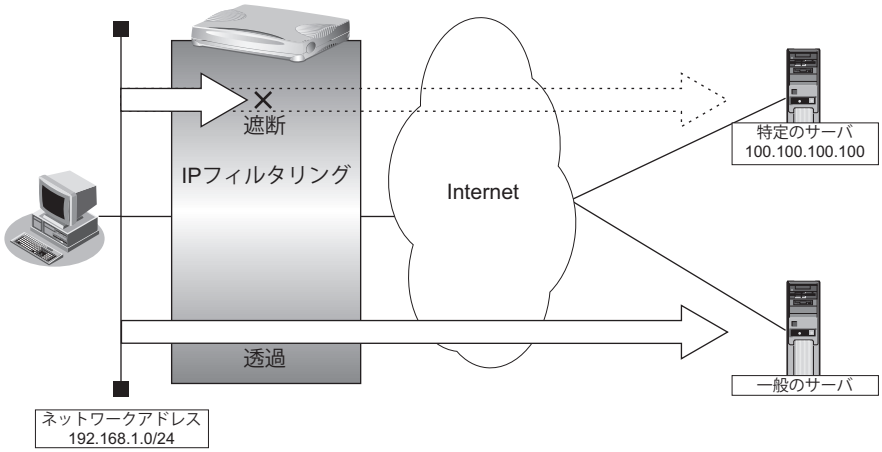
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
内部の LAN から 192.168.0.5 への FTP パケットを遮断する
# acl 0 ip 192.168.1.0/24 192.168.0.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 reject acl 0 any

設定終了
# save
# commit
```

リモート定義の場合

ここでは、インターネット上の特定のサーバに対するアクセスを禁止する場合の設定方法を説明します。



● フィルタリング設計

- LAN 上のホスト（192.168.1.0/24）からアドレス 100.100.100.100 へのアクセスを禁止

● フィルタリングルール

- 特定アドレスへのアクセスを禁止するには
  (1) 192.168.1.0/24 から 100.100.100.100 の任意のポートへのすべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

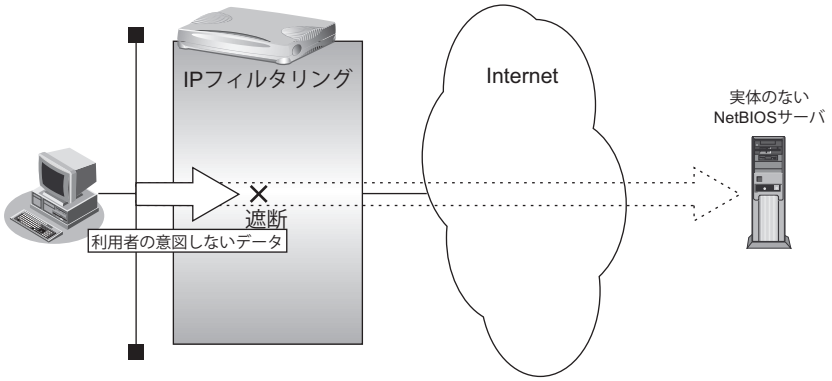
● コマンド

```
アドレス 100.100.100.100 へのすべてのパケットを遮断する
# acl 0 ip 192.168.1.0/24 100.100.100.100/32 any
# remote 0 ip filter 0 reject acl 0 any

設定終了
# save
# commit
```

2.8.6　利用者が意図しない発信を防ぐ

LAN上のパソコンは、利用者の意志とは無関係に、実体のないNetBIOSサーバにアクセスすることがあります。その際、回線が接続され、利用者が意識しないところで通信料金がかかってしまいます。

ここでは、上記のような、回線に対するむだな発信を抑止する場合のフィルタリング設定方法を説明します。



● フィルタリング設計

- ポート137～139（NetBIOSサービス）へのアクセスを禁止

● フィルタリングルール

- ポート137～139へのアクセスを禁止するには

  (1) ポート137～139へのすべてのパケットを遮断する

  (2) ポート137～139からのすべてのパケットを遮断する

補足　Windows（TCP上のNetBIOS）環境のネットワークでは、セキュリティ上の問題とむだな課金を抑えるために、ポート番号137～139の外向きの転送経路をふさいでおく必要があります。

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

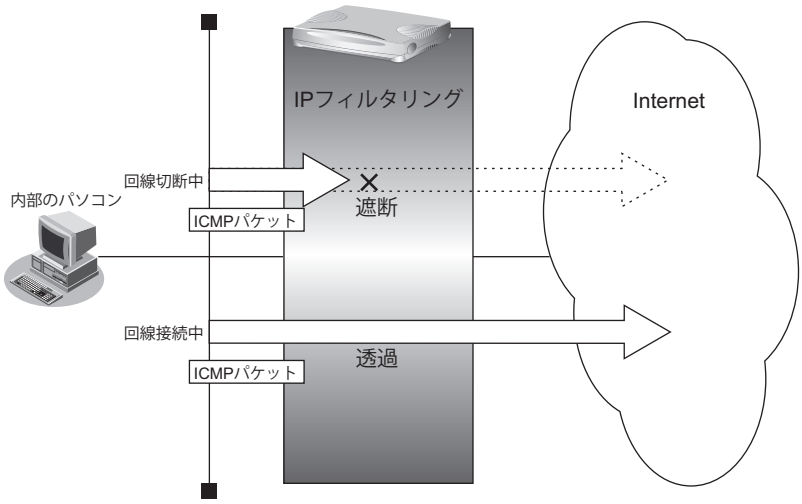
● コマンド

```
ポート137～139へのすべてのTCPパケットを遮断する
# acl 0 ip any any 6
# acl 0 tcp any 137-139 yes
# remote 0 ip filter 0 reject acl 0 any

ポート137～139からのすべてのTCPパケットを遮断する
# acl 1 ip any any 6
# acl 1 tcp 137-139 any yes
# remote 0 ip filter 1 reject acl 1 any

ポート137～139へのすべてのUDPパケットを遮断する
# acl 2 ip any any 17
# acl 2 udp any 137-139
# remote 0 ip filter 2 reject acl 2 any

ポート137～139からのすべてのUDPパケットを遮断する
# acl 3 ip any any 17
# acl 3 udp 137-139 any
# remote 0 ip filter 3 reject acl 3 any

設定終了
# save
# commit
```

2.8.7　回線が接続しているときだけを許可する

一部のパソコンでは、ネットワークの設定によって、ログイン時に自動的に PING を発行して PPPoE を接続してしまうものがあります。回線接続を必要とする ICMP パケットを遮断することによって、意図しない PING によるむだな発信を抑止することができます。ここでは、回線が接続されているときにだけ ICMP パケットを透過させる場合の設定方法を説明します。

補足 IP アドレスを直接指定せず、DNS による名前アドレス変換を利用した場合、発信を抑止することはできません。



● フィルタリング設計

- すでに回線が接続している場合にだけ PING を許可

● フィルタリングルール

- すでに回線が接続している場合にだけ PING を許可するには
  (1) 回線接続中だけ ICMP パケットを透過させる

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

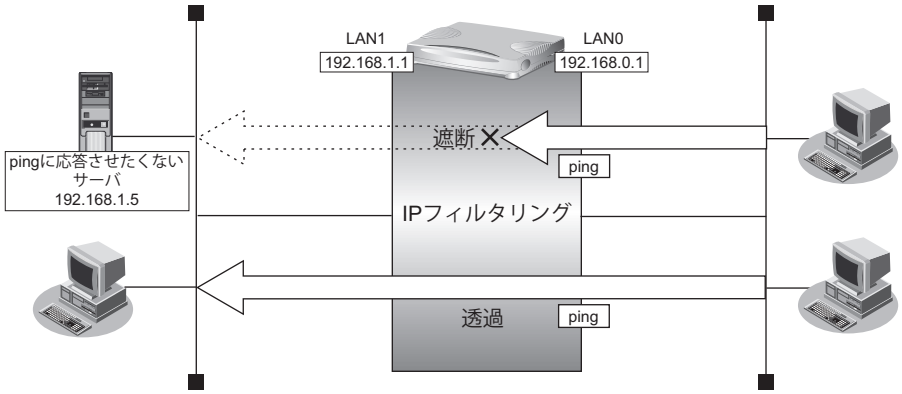
● コマンド

```
回線が接続しているときだけICMPパケットを透過させる
# acl 0 ip any any 1
# acl 0 icmp any any
# remote 0 ip filter 0 restrict acl 0 any

設定終了
# save
# commit
```

2.8.8　外部から特定サーバへの ping だけを禁止する

LAN 定義の場合

ここでは、内部 LAN の特定のサーバに対する ping（ICMP ECHO）を禁止し、この特定のサーバに対するほかの ICMP パケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。



● フィルタリング設定

- 内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止
- その他はすべて通過

● フィルタリングルール

- 内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止するには
  (1) 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
- その他のパケットを許可する
  (1) すべてのパケットを透過させる

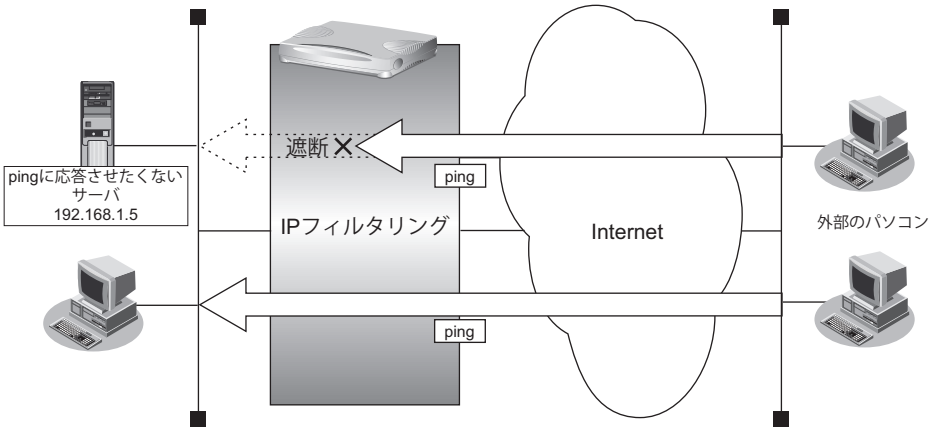
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
アドレス 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
# acl 0 ip any 192.168.1.5/32 1
# acl 0 icmp 8 any
# lan 0 ip filter 0 reject acl 0 any

残りのパケットをすべて透過させる
# acl 1 ip any any any
# lan 0 ip filter 1 pass acl 1 any

設定終了
# save
# commit
```

リモート定義の場合

ここでは、LAN 上の特定のサーバに対する ping（ICMP ECHO）を禁止し、この特定のサーバに対するほかの ICMP パケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。



● フィルタリング設計

- LAN 上のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止
- その他はすべて通過

● フィルタリングルール

- LAN 上のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止するには
  (1) 192.168.1.5/32 の ICMP TYPE 8 の ICMP パケットを遮断する
- その他のパケットを許可する
  (1) すべてのパケットを透過させる

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
アドレス 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
# acl 0 ip any 192.168.1.5/32 1
# acl 0 icmp 8 any
# remote 0 ip filter 0 reject acl 0 any

残りのパケットをすべて透過させる
# acl 1 ip any any any
# remote 0 ip filter 1 pass acl 1 any

設定終了
# save
# commit
```

2.9　IPsec 機能を使う

VPN（Virtual Private Network）は、インターネットを利用して遠隔地の LAN をつなぐと、遠隔地の LAN 上のアプリケーションやデータが、あたかも同じオフィスの LAN のように利用できる機能です。また、認証情報や暗号情報を設定することにより、インターネット上を流れるデータのセキュリティを確保することができます。

本装置では、VPN を実現するために IPsec というプロトコルを使用して、以下の接続形態が利用できます。

- IPv4 over IPv4 で固定 IP アドレスでの VPN（手動鍵交換）（P.129）
  自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は手動で設定します。
- IPv4 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換）
  自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。構成例は、「第 1 章 導入例」（P.9）を参照してください。
- IPv4 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）
  自装置または相手装置のどちらかが IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。構成例は、「第 1 章 導入例」（P.9）を参照してください。
- IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）（P.133）
  自装置および相手装置の IPv6 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換）（P.137）
  自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）（P.141）
  自装置または相手装置のどちらかが IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）（P.145）
  自装置および相手装置の IPv6 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- IPv4 over IPv4 で 1 つの IKE セッションに複数の IPsec トンネル構成での VPN（自動鍵交換）（P.149）
  複数の IPsec 対象範囲が存在し、IPsec 対象範囲をすべて（any）とすることができない環境で、IKE セッション（トンネル）を 1 つとして VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode、Aggressive Mode が使用できます。ただし、設定例では Main Mode のみで説明します。

- IPsec 機能と他機能との併用（P.153）
  IPsec 機能と他機能を併用する場合のいくつかの設定例を説明します。
- テンプレート着信機能（AAA 認証）を使用した固定 IP アドレスでの VPN（P.158）
  IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能を使用して VPN 通信を行います。
  認証情報および暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- テンプレート着信機能（AAA 認証）を使用した可変 IP アドレスでの VPN（P.162）
  相手装置の IP アドレスが動的に割り当てられる環境で、IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能を使用して VPN 通信を行います。
  認証情報および暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- テンプレート着信機能（RADIUS 認証）を使用した固定 IP アドレスでの VPN（P.167）
  IKE 不特定着信の IKE 認証鍵取得に RADIUS 認証機能を使用して VPN 通信を行います。
  認証情報および暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- テンプレート着信機能（RADIUS 認証）を使用した可変 IP アドレスでの VPN（P.172）
  相手装置の IP アドレスが動的に割り当てられる環境で、IKE 不特定着信の IKE 認証鍵取得に RADIUS 認証機能を使用して VPN 通信を行います。
  認証情報および暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- テンプレート着信機能（動的 VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN（P.177）
  不特定着信の環境で、動的 VPN 接続契機パケットを監視して動的に VPN 通信を行います。
  自装置の IPv4 トンネルエンドポイントアドレス、IPsec 対象範囲、IPsec 経路情報および接続先監視アドレスは、動的 VPN 情報交換機能で自動的に交換されます。
- テンプレート着信機能（動的 VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN（冗長構成）（P.186）
  VRRP 機能を使用した冗長構成環境で、動的 VPN 機能を使用した構成を説明します。
- テンプレート着信機能（動的 VPN）を使用した IPv6 over IPv6 で固定 IP アドレスでの VPN（P.189）
  不特定着信の環境で、動的 VPN 接続契機パケットを監視して動的に VPN 通信を行います。
  自装置の IPv6 トンネルエンドポイントアドレス、IPsec 対象範囲、IPsec 経路情報および接続先監視アドレスは、動的 VPN 情報交換機能で自動的に交換されます。
- NAT トラバーサルを使用した可変 IP アドレスでの VPN（P.198）
  自装置側の IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、IKE 区間にある NAT を介した IPsec 通信を可能にするために、NAT トラバーサル機能を使用して VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode、Aggressive Mode が使用できます。ただし、設定例では Aggressive Mode のみで説明します。
- テンプレート着信機能（AAA 認証）および NAT トラバーサルを使用した可変 IP アドレスでの VPN（P.202）
  相手装置の IP アドレスが動的に割り当てられ、IKE 区間にある NAT を介した環境で、IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能と NAT トラバーサル機能を使用して VPN 通信を行います。
  認証情報および暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- 接続先情報（動的 VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN（P.206）
  動的 VPN 機能で、送出インタフェースを固定にした場合の構成を説明します。
  また、設定例にはテンプレート着信機能の動的 VPN との併用動作で記載されています。

☛参照 マニュアル「機能説明書」

こんな事に気をつけて

- IPsec は IPv4、IPv6 で使用できます。
- NAT 変換には、IPsec の前の変換と IPsec のあとの変換があります。IPsec 前に変換する場合は IPsec 用の remote ip nat コマンドで設定します。IPsec 後に変換する場合は、プロバイダ接続用の remote ip nat コマンドで設定します。
- インターネット VPN では、VPN 装置どうしがインターネットを介して通信する必要があるため、VPN 装置にはインターネット上で使用可能なグローバルな IP アドレスを使用してください（NAT を使用している場合は、マルチ NAT（静的 NAT）で IP アドレスを割り当てます）。
- VPN 相互接続するアドレスがプライベートアドレスの場合、重複しないように設計してください。
- IPsec では、IPv4、IPv6 パケット通信だけをサポートしています。IPv4、IPv6 パケット以外は VPN の対象とならないため中継されません。
- 暗号パケットが多重に暗号化される形態で使用しないでください。暗号パケットが二重に暗号化され、復号処理が正常に行えないため通信異常となります。
- IPsec と NAT 機能を併用する場合は、マルチ NAT を使用してください。
- IPsec とマルチ NAT を併用する場合は、静的 NAT の設定が必要となることがあります。
- 経路情報を設定する場合、IPsec/IKE ネゴシエーションパケットが VPN のトンネルに入らないように設定してください。
- 複数の接続先情報定義に同じ IPsec トンネルアドレスを定義しないでください。
- IKE セッションに対して複数の IPsec トンネル構成を使用する場合は、同じ IPsec 対象範囲がないように設定してください。
- IPsec 対象範囲が複数ネットワーク存在し、IPsec 対象範囲にすべて（any）を設定できない環境の場合だけ、“IKE セッションに対して複数の IPsec トンネル構成”を使用することをお勧めします。ネットワークごとに IPsec SA を作成する構成や IPsec 対象範囲にすべて（any）を定義できない装置と接続する場合は、“IKE セッションに対して複数の IPsec トンネル構成”を使用してください。
- テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、以下の点に注意してください。
  - IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
  - 初回 IKE ネゴシエーションは Responder でのみ動作します。
  - 自側トンネルエンドポイントアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。
  - テンプレート定義の接続先監視アドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。
  - AAA 設定または RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。
- RADIUS および AAA の登録情報を変更して IPsec が接続できない場合は、手動切断を行い、再度テンプレート着信機能で接続してください。
- 動的 VPN 情報交換機能を使用する場合、システム全体で一意となるユーザ ID を設定してください。
- テンプレート着信機能（動的 VPN）を使用した IPsec では、以下の点に注意してください。
  - IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
  - IKE モードは Main Mode で動作します。
  - 動的 VPN で作成されたインタフェースにスタティック経路情報が設定されるように動的 VPN 接続契機パケットを監視するインタフェースの経路情報を設定してください。
- 動的 VPN 機能を使用する場合に経路情報再登録（clear ip route コマンドまたは clear ipv6 route コマンド）を行うと、経路削除により動的 VPN のセッションが切断されることがあります。
- 動的 VPN で接続する自側ネットワークを異なるアドレスファミリで設定した場合、拡張 IPsec 対象範囲が 1 定義分追加されます。
- 拡張 IPsec 対象範囲機能を使用して IPsec パケットを通過させた場合、IPsec 対象範囲をチェックする相手装置の場合は IPsec が遮断されます。この場合は、拡張 IPsec 対象範囲機能を使用することはできません。
- 拡張 IPsec 対象範囲を使用して双方向通信を行う場合、相手装置側にも同様の設定が必要です。相手装置側に、自側装置と同様の設定が存在しない場合、片側通信のみ暗号化し、折り返しの通信は暗号化されない場合があります。

- NATトラバーサル機能を利用するときは、以下の点に注意してください。
  - IKEを行う双方の装置で設定してください。片方の装置での利用やNATトラバーサルのバージョンが異なると、NATトラバーサルはできません。
    NATトラバーサルは、以下のRFC、Internet Draftのバージョンをサポートします。
    “Negotiation of NAT-Traversal in the IKE”
    RFC3947
    draft-ietf-ipsec-nat-t-ike-03
    draft-ietf-ipsec-nat-t-ike-02
    “UDP Encapsulation of IPsec ESP Packets”
    RFC3948
  - IPsecトンネルに存在するNAT装置の変換テーブルが解放されると、NATトラバーサルは動作できなくなります。変換テーブルを保持するために、接続先監視機能と併用することを推奨します。
  - IPsec通信プロトコルは暗号（ESP）を使用するように設定してください。IPsec通信プロトコルが認証（AH）の場合は動作しません。
  - 自側および相手側トンネルエンドポイントアドレスにIPv6アドレスを設定した場合は動作しません。
  - IKEモードがAggressive Mode設定で、自側および相手側トンネルエンドポイントアドレスにIPv4アドレスを設定した場合は動作しません。
  - IKEを使用する設定をしてください。動的VPN（dvpn）および手動鍵（manual）を設定した場合は動作しません。
  - 初回IKEネゴシエーションが、initiator装置側でNATされる環境でのみ動作します。
  - テンプレート着信機能（AAA認証およびRADIUS認証）を使用したIPsecでは、IKEモードをAggressive Modeで設定してください。Main Modeで設定した場合は動作しません。
- 接続優先制御の設定は、IKEネゴシエーションのすれ違いが頻発する場合にそれぞれ異なる優先方法を設定してください。同じ優先制御を行うと、競合した場合にIKEネゴシエーションが失敗します。この機能を利用する場合は、以下の設定を奨励します。
  - 一方の装置でInitiatorを優先し、一方の装置でResponderを優先する。
- IDタイプがx501_sbjの場合は、Aggressiveモードを使用することはできません。
- 接続先情報の動的VPN接続を使用する場合、相手装置の自側ネットワーク設定（dvpn client localnet）と自装置の相手側ネットワーク設定（remote ap dvpn remotenet）が異なる場合は、以下に注意してください。
  - 双方の装置で自装置ID設定（dvpn client localid）を設定してください。
  - 接続先情報の動的VPN接続を使用する場合は、相手装置ID設定（remote ap dvpn remoteid）に相手装置の自装置ID（dvpn client localid）を設定してください。
  - 自装置の相手側ネットワーク設定（remote ap dvpn remotenet）に存在しないネットワーク情報を相手装置の自側ネットワーク設定（dvpn client localnet）に追加する場合は、必ず後ろの番号に追加してください。
  - 対向装置がテンプレート情報の動的VPN接続の場合、自装置の相手側ネットワーク設定（remote ap dvpn remotenet）に存在しないネットワークからの接続はできません。
- 接続先情報の動的VPN接続でINVITE自動ignore機能を使用する場合は、以下に注意してください。
  - 相手装置側のネットワーク情報にall-0（0.0.0.0/0または::/0）が含まれている場合は、INVITE自動ignoreルール適用の対象外となります。
  - 動的VPNが設定されている接続先情報にセッション監視定義があった場合は、セッション監視パケットもINVITE自動ignore対象となります。
  - INVITE自動ignore機能により作成されたignoreルールの自側アドレス範囲は、any（0.0.0.0/0または::/0）となります。

ヒント

◆ VPNとは？

暗号化技術や認証技術を使って、インターネットを仮想的な専用線として利用する技術です。また、VPNを使ってつないだルータ間の通信経路のことをトンネルと言います。

◆ 自動鍵交換とは？

IPsecの通信に使用される暗号化・認証用の鍵素材を、自動で作成・更新します。鍵素材を定期的に自動更新させることにより、セキュリティの強度を高めることができます。自動鍵交換を使用しない場合は、手動で鍵を設定する必要があります。

◆ NAT と IPsec を併用する

IPsec で使用するグローバルアドレスで NAT を使用している場合（IPsec 後の NAT 変換後）は、IPsec パケットが NAT を通過できるように、実回線の LAN または remote 定義で、以下の静的 NAT を設定します。

利用形態	設定内容
固定 IP アドレスでの VPN（手動鍵交換）	ESP パケットの受信を設定します。 • プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　すべて • グローバル IP 情報 IP アドレス　相手 VPN 装置に設定された本装置側の IP アドレス ポート番号　すべて • プロトコル　ESP
固定 IP アドレスでの VPN（自動鍵交換）	IKE パケットの受信を設定します。 • プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　500 • グローバル IP 情報 IP アドレス　相手 VPN 装置に設定された本装置側の IP アドレス ポート番号　500 • プロトコル　UDP ESP パケットの受信を設定します。 • プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　すべて • グローバル IP 情報 IP アドレス　相手 VPN 装置に設定された本装置側の IP アドレス ポート番号　すべて • プロトコル　ESP 例） 本装置のネットワーク情報の自側 IP アドレスが 202.168.1.66（固定）であり、202.168.1.66（自側）と 202.168.2.66（相手側）の間で IPsec/IKE 通信を行う場合、IPsec/IKE 通信の自側エンドポイントに 202.168.1.66 を設定します。このとき静的 NAT のプライベートアドレスおよびグローバルアドレスには、202.168.1.66 を設定します。
可変 IP アドレスでの VPN（Initiator）	IKE パケットの受信を設定します。 • プライベート IP 情報 IP アドレス　本装置の LAN 側 IP アドレス ポート番号　500 • グローバル IP 情報 IP アドレス　指定しない ポート番号　500 • プロトコル　UDP
可変 IP アドレスでの VPN（Initiator）	ESP パケットの受信を設定します。 • プライベート IP 情報 IP アドレス　本装置の LAN 側 IP アドレス ポート番号　すべて • グローバル IP 情報 IP アドレス　指定しない ポート番号　すべて • プロトコル　ESP

2.9.1　IPv4 over IPv4 で固定 IP アドレスでの VPN（手動鍵交換）

IPsec 機能を使って手動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IP アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65

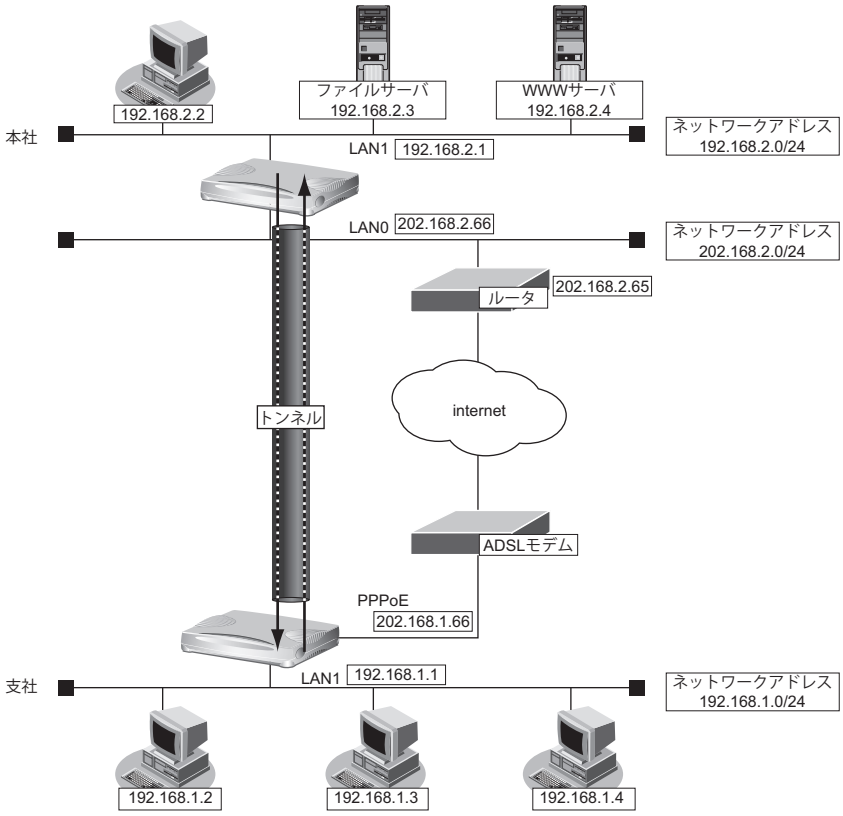
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip address local 202.168.1.66
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- IPsec区間　：202.168.1.66 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IPsecプロトコル　：esp
- IPsec送信用SPI　：100（16進数）
- IPsec送信用SA暗号アルゴリズムと暗号秘密鍵　：des-cbc、0123456789（16進数）
- IPsec送信用SA認証アルゴリズムと認証秘密鍵　：hmac-md5、123456789a（16進数）
- IPsec受信用SPI　：101（16進数）
- IPsec受信用SA暗号アルゴリズムと暗号秘密鍵　：des-cbc、23456789ab（16進数）
- IPsec受信用SA認証アルゴリズムと認証秘密鍵　：hmac-md5、3456789abc（16進数）

[本社]

- IPsec区間　：202.168.2.66 - 202.168.1.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IPsecプロトコル　：esp
- IPsec送信用SPI　：101（16進数）
- IPsec送信用SA暗号アルゴリズムと暗号秘密鍵　：des-cbc、23456789ab（16進数）
- IPsec送信用SA認証アルゴリズムと認証秘密鍵　：hmac-md5、3456789abc（16進数）
- IPsec受信用SPI　：100（16進数）
- IPsec受信用SA暗号アルゴリズムと暗号秘密鍵　：des-cbc、0123456789（16進数）
- IPsec受信用SA認証アルゴリズムと認証秘密鍵　：hmac-md5、123456789a（16進数）

ヒント

◆ SPI とは？

トンネルの識別子です。SPI はトンネルの往路と復路でそれぞれ異なる値を設定します。トンネルをつなぐ本装置を設定するときには、同じ方向のトンネルには同じ SPI を設定します。

こんな事に気をつけて

- 暗号アルゴリズムに des-cbc を選択する場合、鍵に単純な文字列（同じ文字だけ、文字列の繰り返しなど）を指定すると、暗号強度が低下するおそれがあるので指定しないでください。暗号アルゴリズムに 3des-cbc を選択する場合は、鍵を 16 桁ごとに 3 つに分割した、それぞれ 3 つの暗号強度が低下する鍵（弱い鍵）にならないように指定してください。des-cbc で弱い鍵として具体的に知られているものには以下のようなものがあります。本装置は、これらの文字列で始まる鍵で通信できないようにしています。
  0101 0101 0101 0101、1F1F 1F1F E0E0 E0E0、E0E0 E0E0 1F1F 1F1F、FEFE FEFE FEFE FEFE、
  01FE 01FE 01FE 01FE、1FE0 1FE0 0EF1 0EF1、01E0 01E0 01F1 01F1、FE01 FE01 FE01 FE01、
  E01F E01F F10E F10E、E001 E001 F101 F101、1FFE 1FFE 0EFE 0EFE、011F 011F 010E 010E、
  E0FE E0FE F1FE F1FE、FE1F FE1F FE0E FE0E、1F01 1F01 0E01 0E01、FEE0 FEE0 FEF1 FEF1
- 暗号アルゴリズムに 3des を選択する場合は、以下のように鍵を 16 桁ごとに 3 つに分割し、鍵１≠鍵２≠鍵３となるように鍵を設定してください。
  鍵:　1122334455667788　9900aabbccddeeff　1122334455667788
  　　鍵１（16 桁）　鍵２（16 桁）　鍵３（16 桁）
  鍵１＝鍵３のように鍵を設定すると、16 バイトの鍵で暗号化するのと同じ結果になります。また、鍵１＝鍵２、鍵２＝鍵３のように鍵を設定すると、それぞれ鍵３、鍵１の des-cbc 暗号と同じ結果になります（鍵１＝鍵２＝鍵３の場合も同様です）。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honten
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type manual

送信用 SA を設定する
# remote 1 ap 0 ipsec send protocol esp
# remote 1 ap 0 ipsec send spi 100
# remote 1 ap 0 ipsec send encrypt des-cbc hex 0123456789
# remote 1 ap 0 ipsec send auth hmac-md5 hex 123456789a

受信用 SA を設定する
# remote 1 ap 0 ipsec receive protocol esp
# remote 1 ap 0 ipsec receive spi 101
# remote 1 ap 0 ipsec receive encrypt des-cbc hex 23456789ab
# remote 1 ap 0 ipsec receive auth hmac-md5 hex 3456789abc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPNを設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shiten
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type manual

送信用SAを設定する
# remote 0 ap 0 ipsec send protocol esp
# remote 0 ap 0 ipsec send spi 101
# remote 0 ap 0 ipsec send encrypt des-cbc hex 23456789ab
# remote 0 ap 0 ipsec send auth hmac-md5 hex 3456789abc

受信用SAを設定する
# remote 0 ap 0 ipsec receive protocol esp
# remote 0 ap 0 ipsec receive spi 100
# remote 0 ap 0 ipsec receive encrypt des-cbc hex 0123456789
# remote 0 ap 0 ipsec receive auth hmac-md5 hex 123456789a

設定終了
# save
# commit
```

2.9.2　IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）

IPsec 機能を使って IPv4 ローカルネットワーク間を IPv6 インターネットで結び、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス
  ：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス
  ：2001:db8:1111:1::66/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65

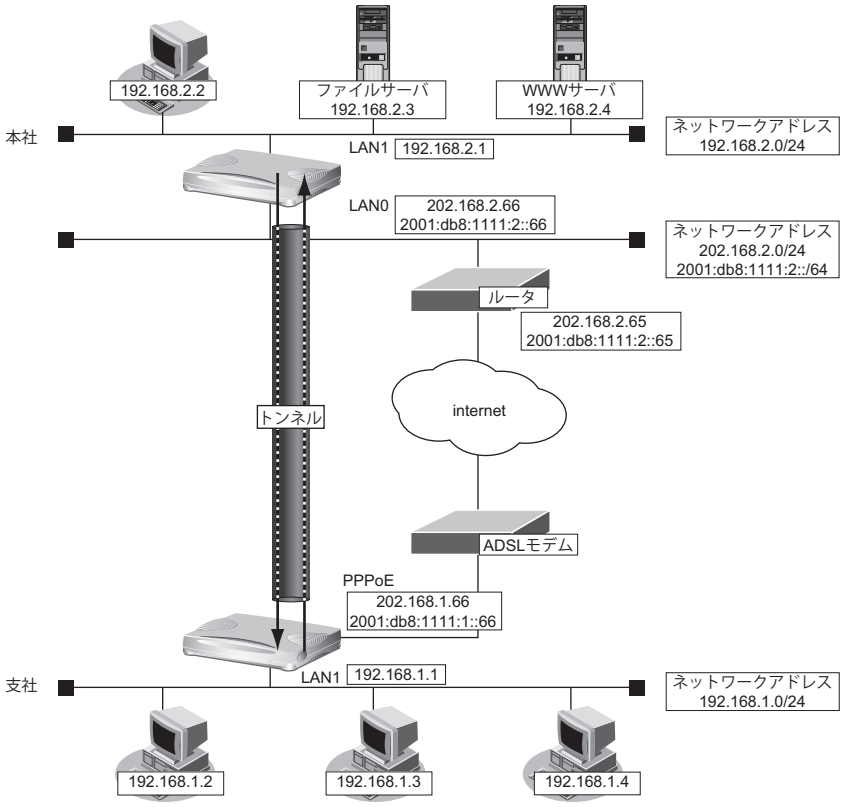
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip6 use on
# remote 0 ip6 address 0 2001:db8:1111:1::66/64 infinity infinity c0
# remote 0 ip6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:2::66/64 infinity infinity c0
# lan 0 ip6 route 0 default 2001:db8:1111:2::65 1
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：2001:db8:1111:1::66-2001:db8:1111:2::66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE区間　：2001:db8:1111:2::66-2001:db8:1111:1::66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし

- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.9.3　IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換）

IPsec 機能を使って IPv6 ローカルネットワーク間を IPv4 インターネットで結び、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:1::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:2::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

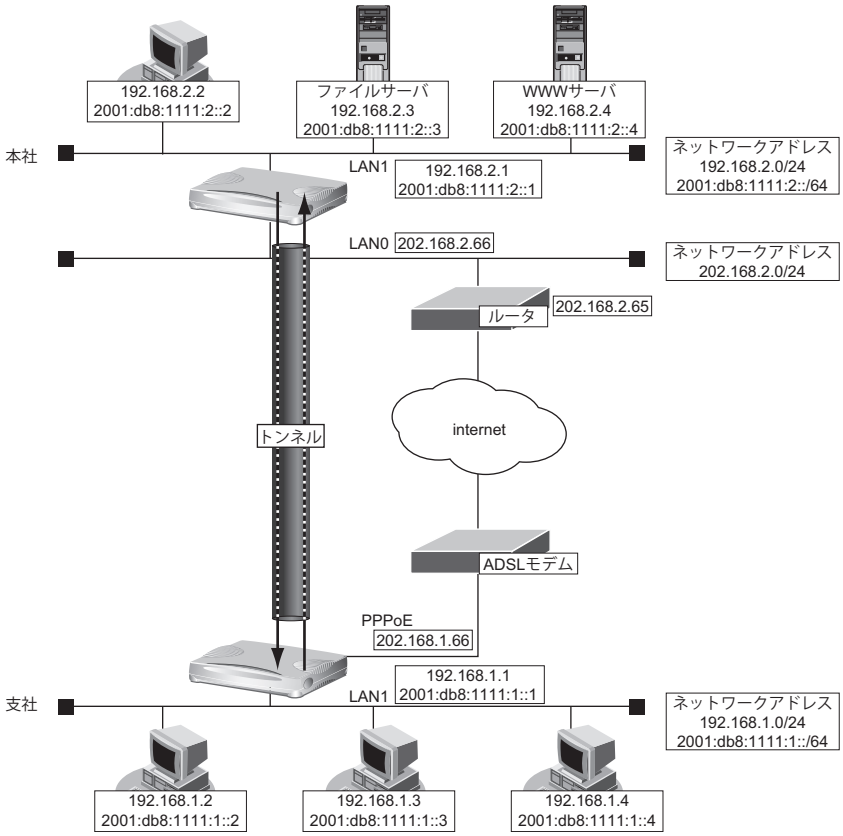
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:1::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:2::1/64 infinity infinity c0
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：202.168.1.66-202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE区間　：202.168.2.66-202.168.1.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.9.4　IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）

接続するたびに IP アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

IPv6 ローカルネットワーク間を IPv4 インターネットで結んで IPsec を行います。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:1::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:2::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

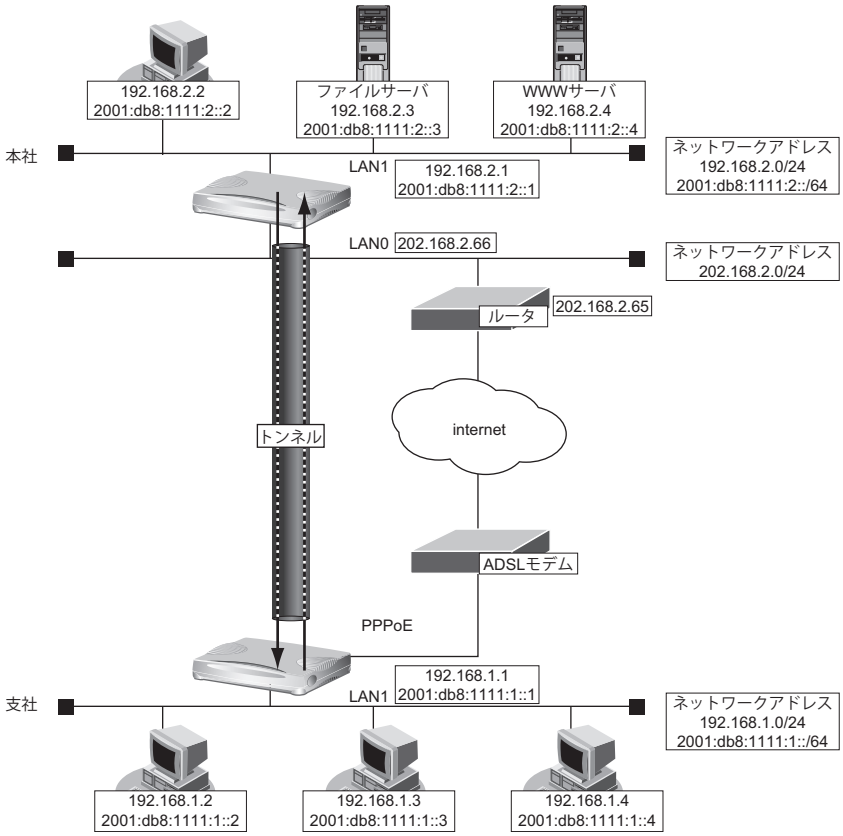
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:1::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
```

[本社]

```
# delete lan
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:2::1/64 infinity infinity c0
```



● 設定条件

[支社（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 -202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP:500 番ポート）のプライベートアドレス：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：202.168.2.66- 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）

- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社（**Responder**）を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.9.5　IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）

IPsec 機能を使って IPv6 で自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:1::66/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65

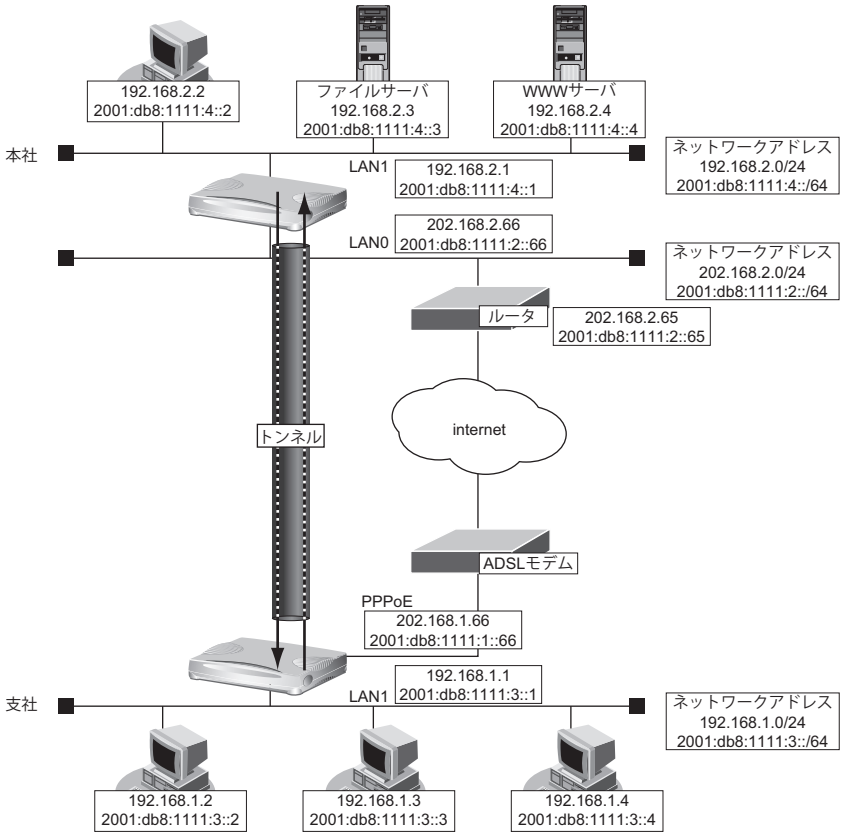
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:3::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip6 use on
# remote 0 ip6 address 0 2001:db8:1111:1::66/64
# remote 0 ip6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:2::66/64 infinity infinity c0
# lan 0 ip6 route 0 default 2001:db8:1111:2::65 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:4::1/64 infinity infinity c0
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：2001:db8:1111:1::66-2001:db8:1111:2::66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE区間　：2001:db8:1111:2::66-2001:db8:1111:1::66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc

- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:4::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:3::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.9.6 IPv4 over IPv4で1つのIKEセッションに複数のIPsecトンネル構成でのVPN（自動鍵交換）

IPsec機能を使って複数のネットワークにそれぞれのIPsec SAを作成する環境を構築する場合を例に説明します（自動鍵交換の固定IPアドレスを使用した構成です）。

ここでは以下のコマンドにより、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE常時接続）]

- ローカルネットワークIPアドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス　：202.168.1.66/24
- PPPoEユーザ認証ID　：userid（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPアドレス1　：LAN0ポート使用
- ローカルネットワークIPアドレス2　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPアドレス　：202.168.2.65

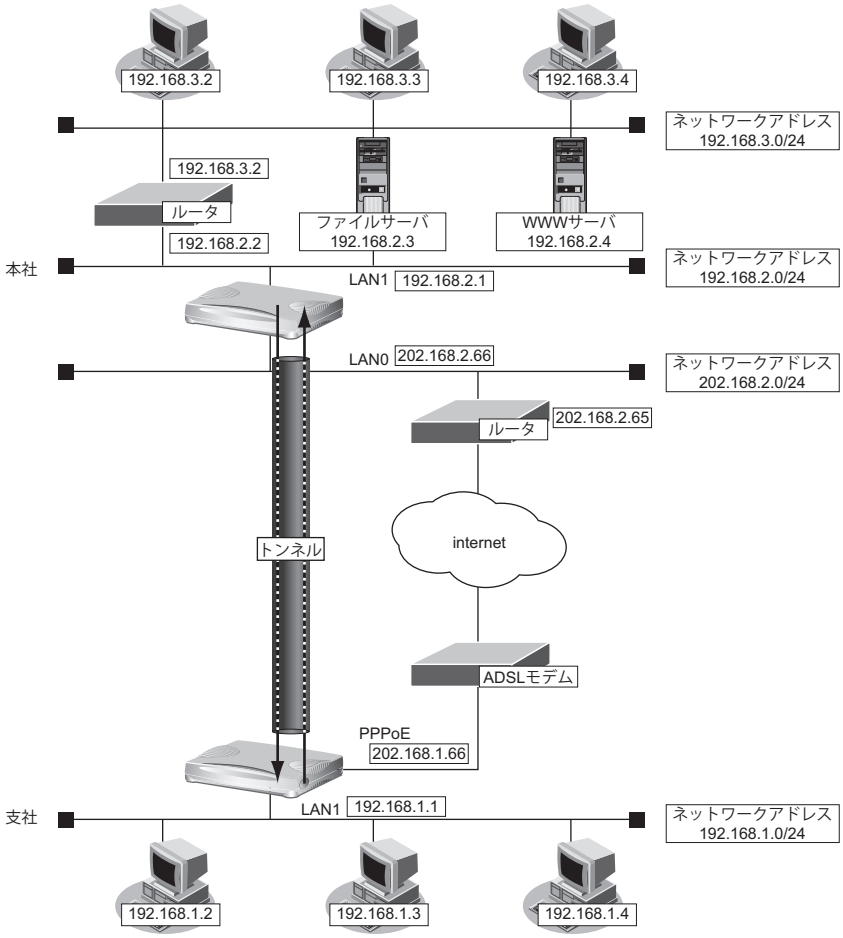
● 設定コマンド

[支社（PPPoE接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip address local 202.168.1.66
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip route 0 192.168.3.0/24 192.168.2.2 1
```



● 設定条件

[支社]

- IPsec/IKE区間　：202.168.1.66 - 202.168.2.66
- IPsec対象範囲（1）　：any - 192.168.2.0/24（マルチルーティングにも定義する）
- IPsec対象範囲（2）　：any - 192.168.3.0/24

[本社]

- IPsec/IKE区間　：202.168.2.66 - 202.168.1.66
- IPsec対象範囲（1）　：192.168.2.0/24 - any（マルチルーティングにも定義する）
- IPsec対象範囲（2）　：192.168.3.0/24 - any

[共通]

- 鍵交換モード　：Main Mode
- IPsecプトロコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec PFS時のDHグループ　：なし
- IKE共有鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方式　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証（ハッシュ）アルゴリズム：hmac-md5
- IKE DHグループ　：modp768（グループ1）

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ip route 1 192.168.3.0/24 1 0
# remote 1 ap 0 name honten1
# remote 1 ap 0 multiroute pattern 0 use any any 192.168.2.0/24 any 0 any
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.2.0/24
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 1 datalink type ipsec
# remote 1 ap 1 ipsec type ike
# remote 1 ap 1 ipsec ike protocol esp
# remote 1 ap 1 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 1 ipsec ike encrypt des-cbc
# remote 1 ap 1 ipsec ike auth hmac-md5
# remote 1 ap 1 ike bind ap 0

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shiten
# remote 0 ap 0 multiroute pattern 0 use 192.168.2.0/24 any any any 0 any
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range 192.168.2.0/24 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 1 datalink type ipsec
# remote 0 ap 1 ipsec type ike
# remote 0 ap 1 ipsec ike protocol esp
# remote 0 ap 1 ipsec ike range 192.168.3.0/24 any4
# remote 0 ap 1 ipsec ike encrypt des-cbc
# remote 0 ap 1 ipsec ike auth hmac-md5
# remote 0 ap 1 ike bind ap 0

設定終了
# save
# commit
```

2.9.7　IPsec 機能と他機能との併用

IPsec 機能と他機能を併用する場合のいくつかの設定例を、以下に説明します。

ここでは、「1.7 複数の事業所 LAN を VPN（IPsec）で接続する」（P.24）相当の設定が行われていることを前提とします。

- IPsec 変換前のマルチ NAT ／ IP フィルタリング／ TOS 値書き換え機能
- IPsec 変換前のシェーピング機能と帯域制御（WFQ）機能
- IPsec 変換前の MSS 書き換え機能
- IPsec 変換前の MTU 分割機能
- 接続先監視機能
- IKE セッション監視機能
- 動的経路（RIP）機能

補足　以下の機能については、IPv6 アドレスで使用することはできません。
- IPsec 変換前のマルチ NAT 機能
- IKE セッション監視機能

IPsec 変換前のマルチ NAT ／ IP フィルタリング／ TOS 値書き換え機能との併用例

● 設定条件

[支社]

- NAT の使用　：マルチ NAT を使用する
  グローバルアドレス　：192.168.1.1
  アドレス個数　：1
  アドレス割当てタイマ　：5 分
- IP フィルタリング　：支社 - 本社間の telnet ／ ftp 通信以外遮断
- TOS 値書き換え　：ftp 通信を 0xa0 に変換

[本社]

- IP フィルタリング　：支社 - 本社間の telnet ／ ftp 通信以外遮断
- TOS 値書き換え　：ftp 通信を 0xa0 に変換

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 ip nat mode multi 192.168.1.1 1

# acl 0 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 0 tcp any 21,23 yes
# acl 1 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 1 tcp 21,23 any no
# acl 2 ip any any any any
# acl 3 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 3 tcp any 20,21 yes

# remote 1 ip filter 0 pass acl 0 out
# remote 1 ip filter 1 pass acl 1 in
# remote 1 ip filter 2 reject acl 2 any
# remote 1 ip tos 0 acl 3 a0
```

本社を設定する

● コマンド

```
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 0 tcp any 21,23 yes
# acl 1 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 1 tcp 21,23 any no
# acl 2 ip any any any any
# acl 3 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 3 tcp any 20,21 yes

# remote 0 ip filter 0 pass acl 0 in
# remote 0 ip filter 1 pass acl 1 out
# remote 0 ip filter 2 reject acl 2 any
# remote 0 ip tos 0 acl 3 a0
```

IPsec 変換前のシェーピング機能と帯域制御（WFQ）機能の併用例

● 設定条件

[本社]

- シェーピングレート　：2Mbps
- 帯域制御対象送信元 IP アドレス　：192.168.2.0/24
- 帯域制御対象送信元ポート番号　：すべて
- 帯域制御対象あて先 IP アドレス　：192.168.1.0/24
- 帯域制御対象あて先ポート番号　：すべて
- 帯域制御対象プロトコル　：TCP
- 帯域制御対象 TOS 値　：すべて
- 割り当て帯域　：最優先

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本社を設定する

● コマンド

```
# remote 0 shaping on 2m
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 6 any
# remote 0 ip priority 0 acl 0 express
```

こんな事に気をつけて

IPsec 機能と帯域制御（WFQ）機能を併用する場合、IPsec 前のパケットに対して帯域制御を行うときには、IPsec 用の remote で設定します。この場合、IPsec 用の remote でシェーピングを行うか、または、実回線の remote で IPsec 後のパケットに対して帯域制御を設定する必要があります。

IPsec 変換前の MSS 書き換え機能との併用例

● 設定条件

[共通]

- MSS 書き換え値　：1414Byte

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 ip msschange 1414
```

本社を設定する

● コマンド

```
# remote 0 ip msschange 1414
```

IPsec変換前のMTU分割機能との併用例

● 設定条件

[共通]

- MTU長　：1460Byte

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 mtu 1460
```

本社を設定する

● コマンド

```
# remote 0 mtu 1460
```

接続先監視機能との併用例

● 設定条件

[支社]

- 送信元IPアドレス　：192.168.1.1
- あて先IPアドレス　：192.168.2.1
- タイムアウト時間　：5秒
- 正常時送信間隔　：10秒
- 異常時送信間隔　：1分

補足 監視対象装置は、本社側VPN装置を指定します。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 ap 0 sessionwatch address 192.168.1.1 192.168.2.1
```

IKEセッション監視機能との併用例

● 設定条件

[支社]

- あて先IPアドレス　：192.168.2.1
- タイムアウト時間　：5秒
- 正常時送信間隔　：10秒
- 異常時送信間隔　：1分

補足 監視対象装置は、本社側VPN装置を指定します。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 ap 0 ike sessionwatch 192.168.2.1 10s 1m 5s
```

こんな事に気をつけて

- 接続先監視／IKEセッション監視のあて先IPアドレスは、remote ap ipsec ike rangeコマンドで設定するIPsec対象パケット範囲に含まれるIPアドレスを指定してください。
- 接続先監視／IKEセッション監視のあて先IPアドレスに、常時運転しているIPsec対象の装置を指定してください。あて先IPアドレスに相手IKEサーバとは異なる装置を指定した場合、あて先IPアドレスからの応答が受信できなくなります。その場合、相手IKEサーバが生存していてもIPsec/IKE SAは解放されます。そのため通信が不安定にあることがあります。

動的経路（RIP）機能との併用例

● 設定条件

[共通]

- RIP送信　：v1
- RIP受信　：v1
- RIP送信時加算メトリック値　：0

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
# delete remote 1 ip route
# remote 1 ip rip use v1 v1 0 off
```

本社を設定する

● コマンド

```
# delete remote 0 ip route
# remote 0 ip rip use v1 v1 0 off
```

2.9.8 テンプレート着信機能（AAA 認証）を使用した固定 IP アドレスでの VPN

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

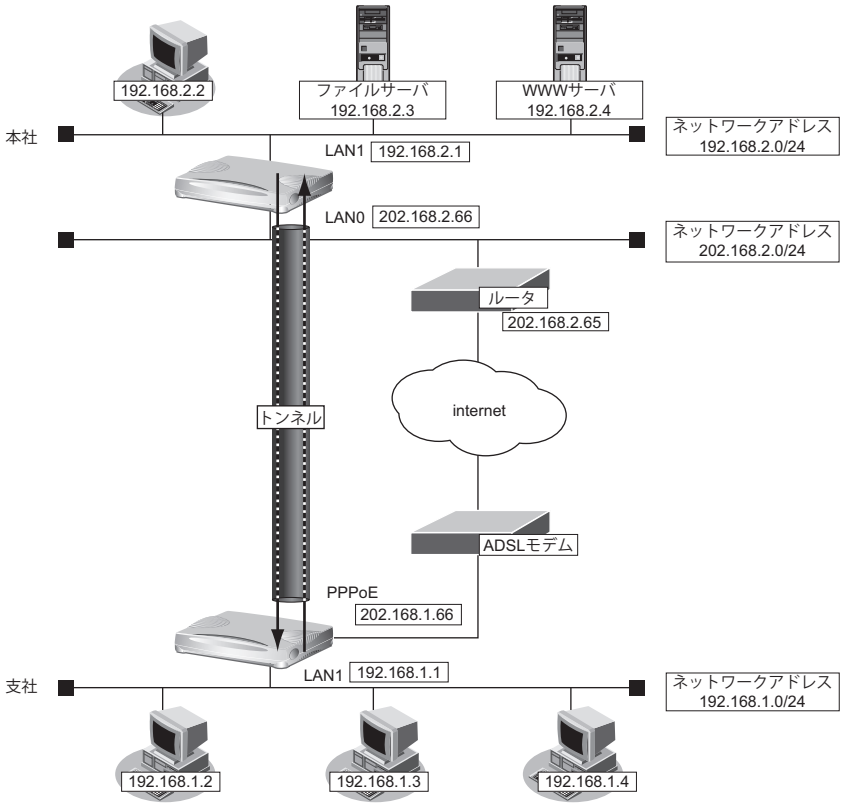
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：202.168.1.66 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE区間　：202.168.2.66 - 202.168.1.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

こんな事に気をつけて

- テンプレート着信機能（AAA 認証）を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。
  Main Mode の場合　　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合 ：相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0 の設定を推奨します。

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する（Initiator）

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 0

設定終了
# save
# reset
```

本社を設定する（Responder）

● コマンド

```
VPN（テンプレート）を設定する
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode main
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name shisya
# aaa 0 user 0 id 202.168.1.66
# aaa 0 user 0 password 202.168.1.66
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# reset
```

2.9.9 テンプレート着信機能（AAA 認証）を使用した可変 IP アドレスでの VPN

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

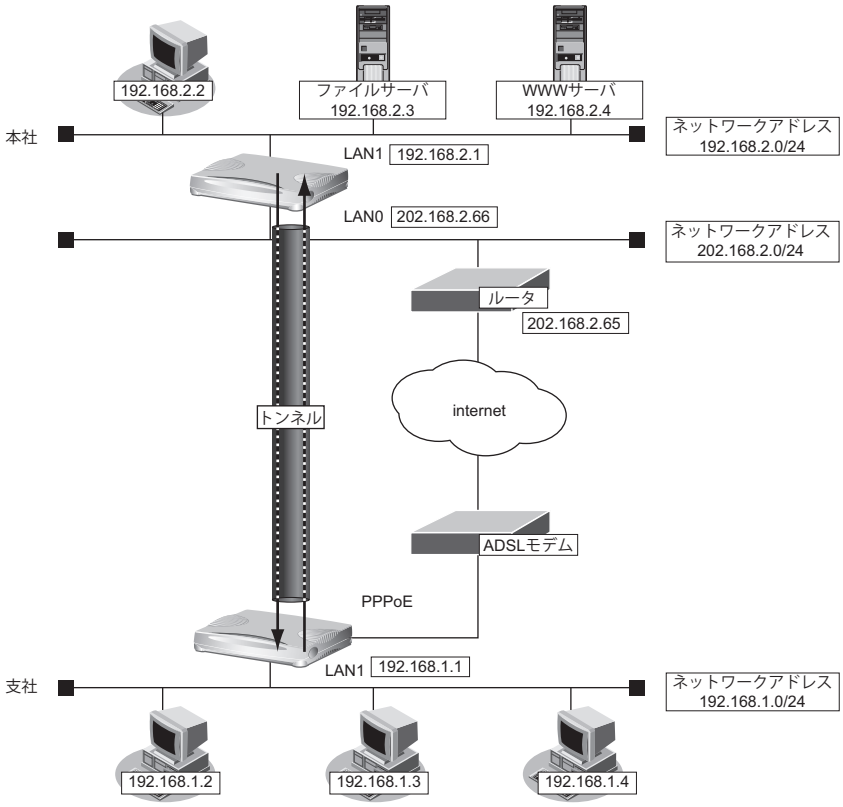
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：支社 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE区間　：202.168.2.66 - 支社
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE支社ID/IDタイプ　：shisya（自装置名）/FQDN
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

こんな事に気をつけて

- テンプレート着信機能（AAA 認証）を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。
  Main Mode の場合　　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合 ：相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0 の設定を推奨します。

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する（Initiator）

● コマンド

```
インターネットからIPsec/IKEパケットを受信するように設定する
 # remote 0 ip nat static 0 192.168.1.1 500 any 500 17
 # remote 0 ip nat static 1 192.168.1.1 any any any 50
 # remote 0 ip nat static default reject

VPNを設定する
 # remote 1 name vpn-hon
 # remote 1 ap 0 name honsya
 # remote 1 ap 0 datalink type ipsec
 # remote 1 ap 0 ipsec type ike
 # remote 1 ap 0 ipsec ike protocol esp
 # remote 1 ap 0 ipsec ike range any4 any4
 # remote 1 ap 0 ipsec ike encrypt des-cbc
 # remote 1 ap 0 ipsec ike auth hmac-md5
 # remote 1 ap 0 ipsec ike pfs off
 # remote 1 ap 0 ipsec ike lifetime 8h
 # remote 1 ap 0 ipsec ike lifebyte 0
 # remote 1 ap 0 ipsec ike newsa initiator 90s 0
 # remote 1 ap 0 ipsec ike newsa responder 30s 0
 # remote 1 ap 0 ike mode aggressive
 # remote 1 ap 0 ike bind self
 # remote 1 ap 0 ike idtype fqdn
 # remote 1 ap 0 ike name local shisya
 # remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
 # remote 1 ap 0 ike proposal 0 encrypt des-cbc
 # remote 1 ap 0 ike proposal 0 hash hmac-md5
 # remote 1 ap 0 ike proposal 0 pfs modp768
 # remote 1 ap 0 ike proposal 0 lifetime 1d
 # remote 1 ap 0 ike retry 10s 3
 # remote 1 ap 0 ike release on
 # remote 1 ap 0 ike initial forward
 # remote 1 ap 0 tunnel remote 202.168.2.66
 # remote 1 ip route 0 192.168.2.0/24 1 0

設定終了
 # save
 # reset
```

本社を設定する（**Responder**）

● コマンド

```
VPN（テンプレート）を設定する
 # template 0 name vpn-hon
 # template 0 combine use aaa
 # template 0 datalink type ipsec
 # template 0 interface pool 1 1
 # template 0 aaa 0
 # template 0 ipsec ike protocol esp
 # template 0 ipsec ike encrypt des-cbc
 # template 0 ipsec ike auth hmac-md5
 # template 0 ipsec ike pfs off
 # template 0 ipsec ike lifetime 8h
 # template 0 ipsec ike lifebyte 0
 # template 0 ipsec ike newsa initiator 90s 0
 # template 0 ipsec ike newsa responder off 0
 # template 0 ike mode aggressive
 # template 0 ike idtype fqdn
 # template 0 ike proposal 0 encrypt des-cbc
 # template 0 ike proposal 0 hash hmac-md5
 # template 0 ike proposal 0 pfs modp768
 # template 0 ike proposal 0 lifetime 1d
 # template 0 ike retry 10s 3
 # template 0 ike release on
 # template 0 tunnel local 202.168.2.66

AAA情報を設定する
 # aaa 0 name shisya
 # aaa 0 user 0 id shisya
 # aaa 0 user 0 password shisya
 # aaa 0 user 0 ipsec ike range any4 any4
 # aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
 # aaa 0 user 0 ip route 0 192.168.1.0/24 1 1

設定終了
 # save
 # reset
```

2.9.10 テンプレート着信機能（RADIUS 認証）を使用した固定 IP アドレスでの VPN

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

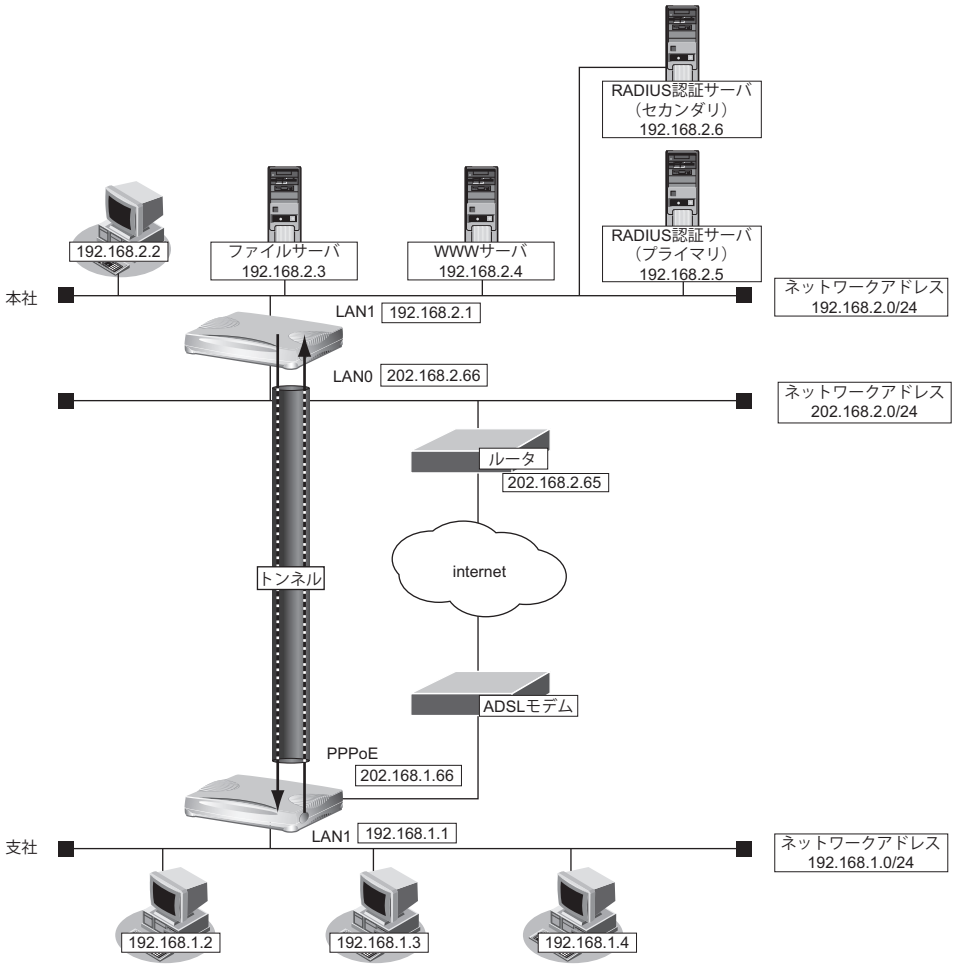
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：202.168.1.66 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE区間　：202.168.2.66 - 202.168.1.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- RADIUSサービス　：クライアント機能
  ：認証、アカウンティング
- 自側認証IPアドレス　：192.168.2.1
- 自側アカウンティングIPアドレス　：192.168.2.1
- 認証情報1（プライマリ）
  共有鍵　：192.168.2.1
  サーバIPアドレス　：192.168.2.5
  復旧待機時間　：30分
  優先度　：0

- 認証情報２（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30分
  優先度　：100
- アカウンティング情報１（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30分
  優先度　：0
- アカウンティング情報２（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30分
  優先度　：100

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

こんな事に気をつけて

- テンプレート着信機能（RADIUS 認証）を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0 の設定を推奨します。

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する（**Initiator**）

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 0

設定終了
# save
# reset
```

本社を設定する（**Responder**）

● コマンド

```
VPN（テンプレート）を設定する
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode main
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name shisya

RADIUS クライアントに関する情報を設定する
# aaa 0 radius service client both
# aaa 0 radius auth source 192.168.2.1
# aaa 0 radius accounting source 192.168.2.1
# aaa 0 radius client server-info auth 0 secret 192.168.2.1
# aaa 0 radius client server-info auth 0 address 192.168.2.5
# aaa 0 radius client server-info auth 0 deadtime 30m
# aaa 0 radius client server-info auth 0 priority 0
# aaa 0 radius client server-info auth 1 secret 192.168.2.1
# aaa 0 radius client server-info auth 1 address 192.168.2.6
# aaa 0 radius client server-info auth 1 deadtime 30m
# aaa 0 radius client server-info auth 1 priority 100
# aaa 0 radius client server-info accounting 0 secret 192.168.2.1
# aaa 0 radius client server-info accounting 0 address 192.168.2.5
# aaa 0 radius client server-info accounting 0 deadtime 30m
# aaa 0 radius client server-info accounting 0 priority 0
# aaa 0 radius client server-info accounting 1 secret 192.168.2.1
# aaa 0 radius client server-info accounting 1 address 192.168.2.6
# aaa 0 radius client server-info accounting 1 deadtime 30m
# aaa 0 radius client server-info accounting 1 priority 100

設定終了
# save
# reset
```

2.9.11 テンプレート着信機能（RADIUS 認証）を使用した可変 IP アドレスでの VPN

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

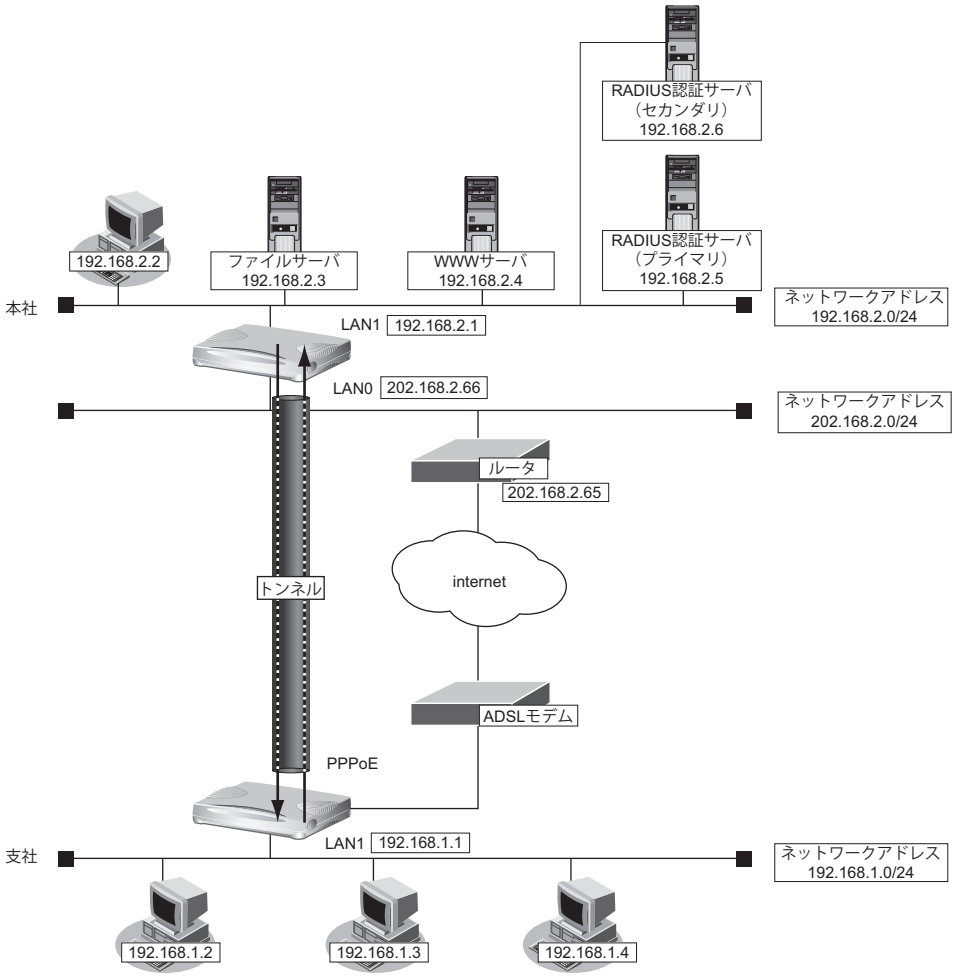
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：支社 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE区間　：202.168.2.66 - 支社
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- RADIUSサービス　：クライアント機能
  ：認証、アカウンティング
- 自側認証IPアドレス　：192.168.2.1
- 自側アカウンティングIPアドレス　：192.168.2.1
- 認証情報1（プライマリ）
  共有鍵　：192.168.2.1
  サーバIPアドレス　：192.168.2.5
  復旧待機時間　：30分
  優先度　：0

- 認証情報２（セカンダリ）
  共有鍵　：192.168.2.1
  サーバIPアドレス　：192.168.2.6
  復旧待機時間　：30分
  優先度　：100
- アカウンティング情報１（プライマリ）
  共有鍵　：192.168.2.1
  サーバIPアドレス　：192.168.2.5
  復旧待機時間　：30分
  優先度　：0
- アカウンティング情報２（セカンダリ）
  共有鍵　：192.168.2.1
  サーバIPアドレス　：192.168.2.6
  復旧待機時間　：30分
  優先度　：100

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE支社ID/IDタイプ　：shisya（自装置名）/FQDN
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

こんな事に気をつけて

- テンプレート着信機能（RADIUS認証）を使用したIPsecでは、RADIUS認証サーバ側のユーザIDとユーザ認証パスワードを同じに設定してください。
- ユーザIDとユーザ認証パスワードは、テンプレート情報のIKE情報の交換モードにより以下のように設定します。
  Main Modeの場合　：相手側IPsecトンネルアドレス
  Aggressive Modeの場合　：相手側の装置識別情報
- テンプレート着信側からIKEネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0の設定を推奨します。

ヒント

◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する（Initiator）

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike idtype fqdn
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 0

設定終了
# save
# reset
```

本社を設定する（**Responder**）

● コマンド

```
VPN（テンプレート）を設定する
# template 0 name vpn-hon
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name shisya

RADIUS クライアントに関する情報を設定する
# aaa 0 radius service client both
# aaa 0 radius auth source 192.168.2.1
# aaa 0 radius accounting source 192.168.2.1
# aaa 0 radius client server-info auth 0 secret 192.168.2.1
# aaa 0 radius client server-info auth 0 address 192.168.2.5
# aaa 0 radius client server-info auth 0 deadtime 30m
# aaa 0 radius client server-info auth 0 priority 0
# aaa 0 radius client server-info auth 1 secret 192.168.2.1
# aaa 0 radius client server-info auth 1 address 192.168.2.6
# aaa 0 radius client server-info auth 1 deadtime 30m
# aaa 0 radius client server-info auth 1 priority 100
# aaa 0 radius client server-info accounting 0 secret 192.168.2.1
# aaa 0 radius client server-info accounting 0 address 192.168.2.5
# aaa 0 radius client server-info accounting 0 deadtime 30m
# aaa 0 radius client server-info accounting 0 priority 0
# aaa 0 radius client server-info accounting 1 secret 192.168.2.1
# aaa 0 radius client server-info accounting 1 address 192.168.2.6
# aaa 0 radius client server-info accounting 1 deadtime 30m
# aaa 0 radius client server-info accounting 1 priority 100

設定終了
# save
# reset
```

2.9.12 テンプレート着信機能（動的VPN）を使用した IPv4 over IPv4で固定IPアドレスでのVPN

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.1.1/24
- PPPoEユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社B（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.2.1/24
- PPPoEユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[本社]

- ローカルネットワークIPv4アドレス　：192.168.0.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス：202.168.2.65

● 設定コマンド

[支社A（PPPoE常時接続）]

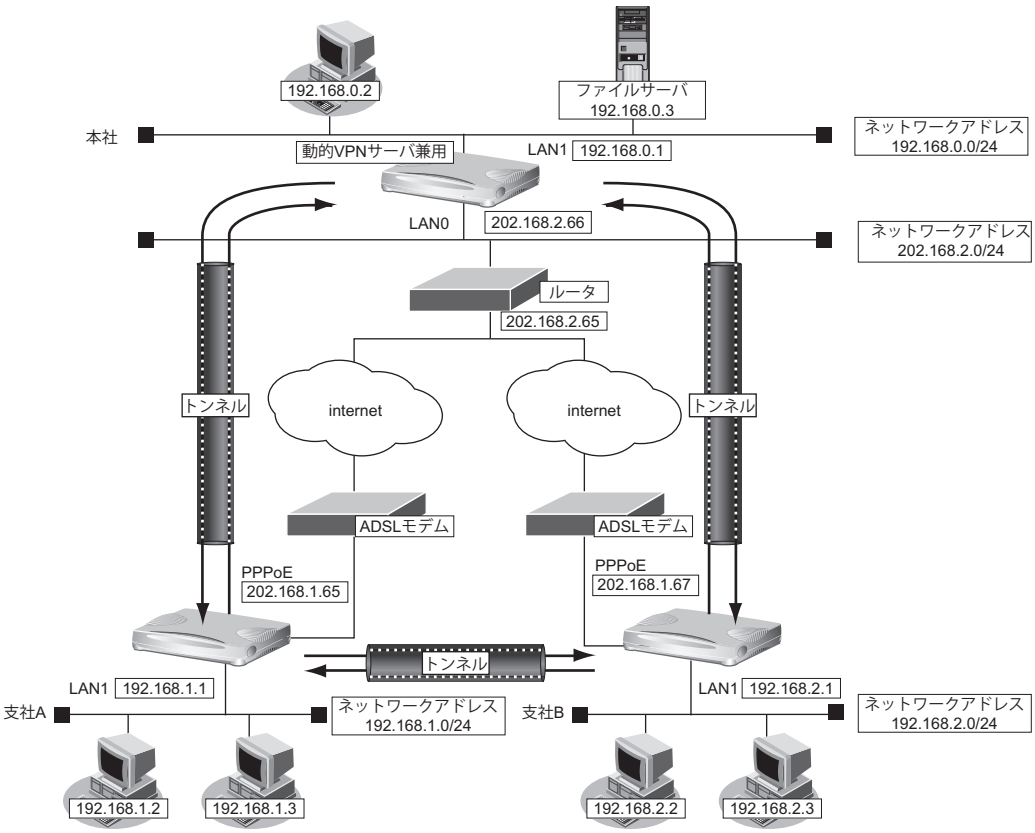
```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社B（PPPoE常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.2.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.0.1/24 3
```



● 設定条件（VPN接続）

[支社A（Initiator）]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：支社A - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.1.1
- ESPのプライベートアドレス　：192.168.1.1

- テンプレート名　：vpn-shiB
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた IPv4 アドレスを使用する
- 接続先監視アドレス　：192.168.1.1

[支社 B（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 B - 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.2.1
- ESP のプライベートアドレス　：192.168.2.1
- テンプレート名　：vpn-shiA
- IPsec/IKE 始点　:インターネットプロバイダから割り当てられた IPv4 アドレス を使用する
- 接続先監視アドレス　：192.168.2.1

[本社（Responder)]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 - 支社 A
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：202.168.2.66 - 支社 B
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通（本社 - 支社 A、B)]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 A ID/ID タイプ　：shisyaA（自装置識別情報）/FQDN
- IKE 支社 B ID/ID タイプ　：shisyaB（自装置識別情報）/FQDN
- IKE 支社 A IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社 B IKE 認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

● 設定条件（動的VPN接続）

[支社A]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.0.1
  ポート番号　：5070
  認証ID　：shisyaAid
  認証パスワード　：shisyaApass
- 有効期間　：1時間
- セッション更新間隔　：5分
- クライアントIPアドレス　：192.168.1.1
- ドメイン名　：example.com
- VPN通信
  利用インタフェース　：rmt0
- 動的VPNクライアントの優先度　：10
- 動的VPN IPv4経路情報の優先度　：1

[支社B]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.0.1
  ポート番号　：5070
  認証ID　：shisyaBid
  認証パスワード　：shisyaBpass
- 有効期間　：1時間
- セッション更新間隔　：5分
- クライアントIPアドレス　：192.168.2.1
- ドメイン名　：example.com
- VPN通信
  利用インタフェース　：rmt0
- 動的VPNクライアントの優先度　：10
- 動的VPN IPv4経路情報の優先度　：1

[本社]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAAグループID　：0
- AAAユーザ情報（支社A認証情報）
  ユーザID　：shisyaAid
  認証パスワード　：shisyaApass
- AAAユーザ情報（支社B認証情報）
  ユーザID　：shisyaBid
  認証パスワード　：shisyaBpass

[共通（支社 A-支社 B)]

- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-128
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：modp768
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：aes-cbc-128
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社 A を設定する（Initiator）

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
```

```
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.0.0/24 1 0
# remote 1 ip route 1 192.168.2.0/24 1 2
# remote 1 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any

動的VPN情報を定義する
# dvpn client 0 server 0 address 192.168.0.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiB
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1

設定終了
# save
# reset
```

支社 B を設定する（Initiator）

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.0.0/24 1 0
# remote 1 ip route 1 192.168.1.0/24 1 2
# remote 1 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any

動的 VPN 情報を設定する
# dvpn client 0 server 0 address 192.168.0.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiA
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
```

```
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

設定終了
# save
# reset
```

本社を設定する（**Responder**）

● コマンド

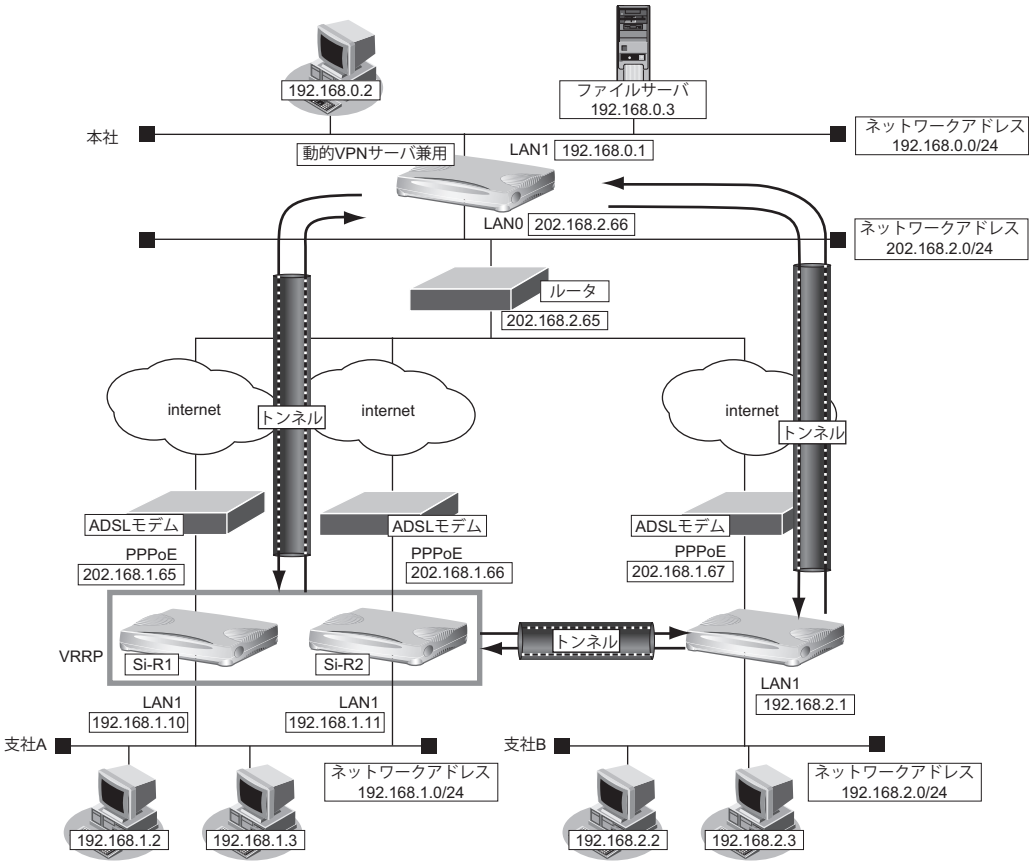
```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs off
# remote 0 ap 0 ipsec ike lifetime 8h
# remote 0 ap 0 ipsec ike lifebyte 0
# remote 0 ap 0 ipsec ike newsa initiator 90s 0
# remote 0 ap 0 ipsec ike newsa responder 30s 0
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike proposal 0 hash hmac-md5
# remote 0 ap 0 ike proposal 0 pfs modp768
# remote 0 ap 0 ike proposal 0 lifetime 1d
# remote 0 ap 0 ike retry 10s 3
# remote 0 ap 0 ike release on
# remote 0 ap 0 ike initial forward
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 1 name vpn-shiB
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
```

```
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 0

動的VPNサーバを設定する
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# dvpn server auth aaa 0
# aaa name dvpnserver
# aaa user 0 id shisyaAid
# aaa user 0 password shisyaApass
# aaa user 1 id shisyaBid
# aaa user 1 password shisyaBpass

設定終了
# save
# reset
```

2.9.13 テンプレート着信機能（動的VPN）を使用した IPv4 over IPv4で固定IPアドレスでのVPN（冗長構成）

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを冗長構成で構築する場合の設定方法を説明します。

ここでは「2.9.12 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN」（P.177）で説明したネットワーク構成で、支社と本社が動的VPNによって接続されていることを前提とします。ただし、支社AはVRRPによる冗長構成の設定を行います。



● 設定コマンド

[支社A（Si-R1）]

「2.9.12 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN」（P.177）で説明した支社Aの設定を事前に行います。

[支社A（Si-R2）]

「2.9.12 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN」（P.177）で説明した支社Aの設定を事前に行います。

● 設定条件（冗長構成）

[支社 A（Si-R1)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.10/24
- VRRP 優先度　：254
- 動的 VPN クライアントの優先度　：1
- ノードダウントリガ　：202.168.2.66

[支社 A（Si-R2)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.11/24
- VRRP 優先度　：100
- 動的 VPN クライアントの優先度　：2

[支社 A（共通)]

- VRRP 仮想 IP アドレス　：192.168.1.1/24
- VRRP グループ ID　：10

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社 A を設定する（Si-R1）

● コマンド

```
# lan 1 ip address 192.168.1.10/24 3
# remote 0 ip nat static 0 192.168.1.10 500 any 500 17
# remote 0 ip nat static 1 192.168.1.10 any any any 50
# remote 1 ip route 1 192.168.2.0/24 1 200

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 node 202.168.2.66 any

動的 VPN を設定する
# template 0 tunnel local 192.168.1.10
# template 0 sessionwatch address 192.168.1.10
# dvpn client 0 ua 192.168.1.10
# dvpn client priority 1

設定終了
# save
# reset
```

支社 A を設定する（Si-R2）

● コマンド

```
# lan 1 ip address 192.168.1.11/24 3
# remote 0 ip nat static 0 192.168.1.11 500 any 500 17
# remote 0 ip nat static 1 192.168.1.11 any any any 50
# remote 1 ip route 1 192.168.2.0/24 1 200
# remote 1 ap 0 ike name local shisyaa

VRRP を設定する
```

```
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1

動的VPNを設定する
# template 0 tunnel local 192.168.1.11
# template 0 sessionwatch address 192.168.1.11
# dvpn client 0 ua 192.168.1.11
# dvpn client priority 2

設定終了
# save
# reset
```

本社を設定する

● コマンド

```
# remote 0 ip route 0 192.168.1.0/24 1 10
# remote 2 name vpn-shia
# remote 2 ap 0 name shisyaa
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaa
# remote 2 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.1.0/24 1 254

設定終了
# save
# reset
```

2.9.14 テンプレート着信機能（動的VPN）を使用した IPv6 over IPv6で固定IPアドレスでのVPN

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.1.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:1::66/64
- PPPoEユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[支社B（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.2.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:5::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.1.67/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:1::67/64
- PPPoEユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPv4アドレス　：192.168.0.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス　：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートのIPv6アドレス　：2001:db8:1111:2::65

● 設定コマンド

[支社Ａ（PPPoE常時接続）]

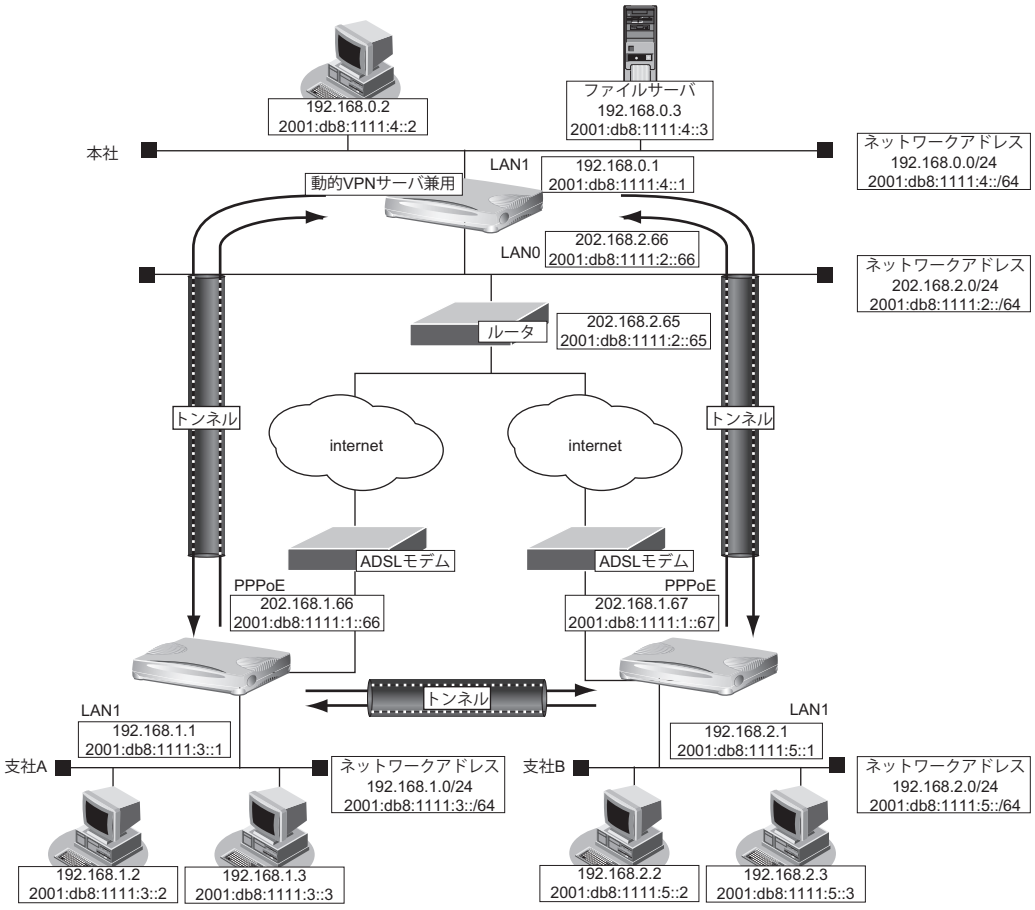
```
# delete lan
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:3::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip6 use on
# remote 0 ip6 address 0 2001:db8:1111:1::66/64 infinity infinity c0
# remote 0 ip6 route 0 default 1 0
```

[支社Ｂ（PPPoE常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:5::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip6 use on
# remote 0 ip6 address 0 2001:db8:1111:1::67/64 infinity infinity c0
# remote 0 ip6 route 0 default 1 0
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:2::66/64 infinity infinity c0
# lan 0 ip6 route 0 default 2001:db8:1111:2::65 1 0
# lan 1 ip address 192.168.0.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:4::1/64 infinity infinity c0
```



● 設定条件（VPN 接続）

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::66 - 2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- テンプレート名　：vpn-shiB
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた固定 IPv6 アドレスを使用する
- 接続先監視アドレス　：2001:db8:1111:3::1

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::67 - 2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- テンプレート名　：vpn-shiA
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた固定 IPv6 アドレスを使用する
- 接続先監視アドレス　：2001:db8:1111:5::1

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE区間　：2001:db8:1111:2::66 - 2001:db8:1111:1::66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE区間　：2001:db8:1111:2::66 - 2001:db8:1111:1::67
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通（本社-支社A、B)]

- 鍵交換タイプ　：Main Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE支社A IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE支社B IKE認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

● 設定条件（動的VPN接続）

[支社A]

- クライアント情報　：0
- サーバ情報
  アドレス　：2001:db8:1111:4::1
  ポート番号　：5070
  認証ID　：shisyaAid
  認証パスワード　：shisyaApass
- 有効期間　：1時間
- セッション更新間隔　：5分
- クライアントIPアドレス　：2001:db8:1111:3::1
- ドメイン名　：example.com
- VPN通信
  利用インタフェース　：rmt0
- 動的VPNクライアントの優先度　：10
- 動的VPN IPv6経路情報の優先度　：1

[支社 B]

- クライアント情報　：0
- サーバ情報
  アドレス　：2001:db8:1111:4::1
  ポート番号　：5070
  認証 ID　：shisyaBid
  認証パスワード　：shisyaBpass
- 有効期間　：1 時間
- セッション更新間隔　：5 分
- クライアント IP アドレス　：2001:db8:1111:5::1
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv6 経路情報の優先度　：1

[本社]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAA グループ ID　：0
- AAA ユーザ情報（支社 A 認証情報）
  ユーザ ID　：shisyaAid
  認証パスワード　：shisyaApass
- AAA ユーザ情報（支社 B 認証情報）
  ユーザ ID　：shisyaBid
  認証パスワード　：shisyaBpass

[共通（支社 A-支社 B）]

- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-128
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：modp768
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：aes-cbc-128
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社 A を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:4::/64 1 0
# remote 1 ip6 route 1 2001:db8:1111:5::/64 1 2
# remote 1 ip6 dvpn 0 invite acl 0 64 0
# acl 0 ip6 2001:db8:1111:3::/64 2001:db8:1111:5::/64 any any

動的 VPN 情報を設定する
# dvpn client 0 server 0 address 2001:db8:1111:4::1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 2001:db8:1111:3::1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 2001:db8:1111:3::/64
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
```

```
# dvpn client 0 ip6 route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiB
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ip6 use on
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 2001:db8:1111:1::66
# template 0 sessionwatch address 2001:db8:1111:3::1

設定終了
# save
# reset
```

支社 B を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:1::67
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ip6 use on
```

```
# remote 1 ip6 route 0 2001:db8:1111:4::/64 1 0
# remote 1 ip6 route 1 2001:db8:1111:3::/64 1 2
# remote 1 ip6 dvpn 0 invite acl 0 64 0
# acl 0 ip6 2001:db8:1111:5::/64 2001:db8:1111:3::/64 any any

動的VPN情報を設定する
# dvpn client 0 server 0 address 2001:db8:1111:4::1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 2001:db8:1111:5::1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 2001:db8:1111:5::/64
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip6 route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiA
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ip6 use on
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 2001:db8:1111:1::67
# template 0 sessionwatch address 2001:db8:1111:5::1

設定終了
# save
# reset
```

本社を設定する

● コマンド

```
VPNを設定する
# remote 0 name vpn-shiA
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs off
# remote 0 ap 0 ipsec ike lifetime 8h
# remote 0 ap 0 ipsec ike lifebyte 0
```

```
# remote 0 ap 0 ipsec ike newsa initiator 90s 0
# remote 0 ap 0 ipsec ike newsa responder 30s 0
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike proposal 0 hash hmac-md5
# remote 0 ap 0 ike proposal 0 pfs modp768
# remote 0 ap 0 ike proposal 0 lifetime 1d
# remote 0 ap 0 ike retry 10s 3
# remote 0 ap 0 ike release on
# remote 0 ap 0 ike initial forward
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:3::/64 1 0
# remote 1 name vpn-shiB
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:2::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:1::67
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:5::/64 1 0

動的VPNサーバを設定する
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# dvpn server auth aaa 0
# aaa name dvpnserver
# aaa user 0 id shisyaAid
# aaa user 0 password shisyaApass
# aaa user 1 id shisyaBid
# aaa user 1 password shisyaBpass

設定終了
# save
# reset
```

2.9.15　NAT トラバーサルを使用した可変 IP アドレスでの VPN

接続するたびに IP アドレスが変わる環境で NAT トラバーサルを使って、VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

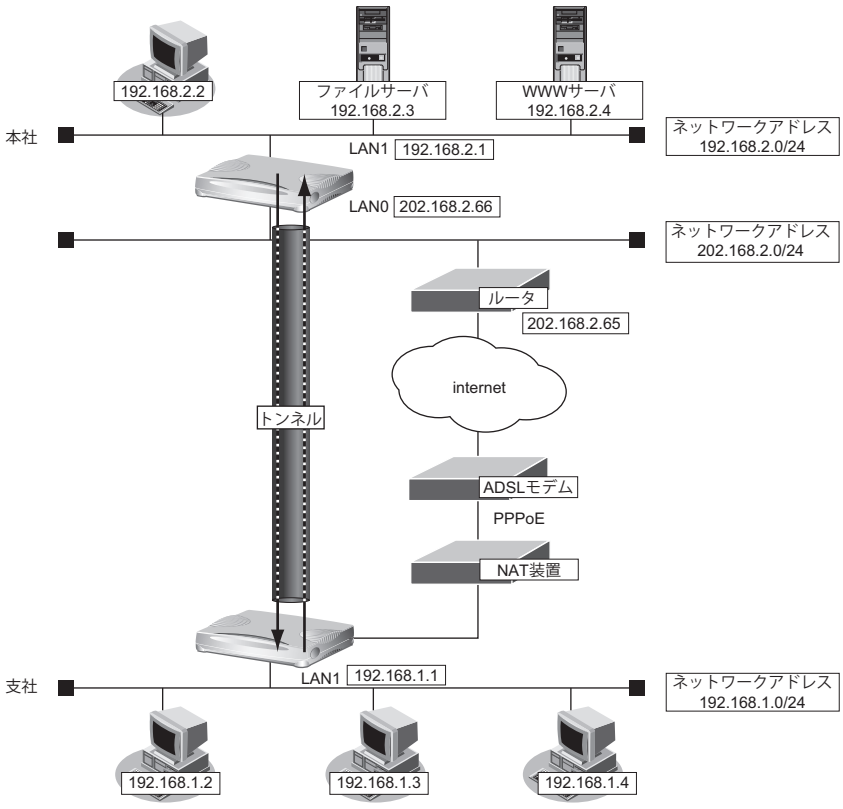
● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：支社 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE区間　：202.168.2.66 - 支社
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE支社ID/IDタイプ　：shisya（自装置名）/FQDN
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768
- IKE NATトラバーサル機能　：使用する

ヒント

◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

◆ IDタイプとは？

Aggressive Modeの場合に、ネゴシエーションで使用する自装置を識別するIDの種別です。相手VPN装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する（**Initiator**）

● コマンド

```
PPPoE を設定する
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike nat-traversal use on

設定終了
# save
# commit
```

本社を設定する（**Responder**）

● コマンド

```
LAN を設定する
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3

VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike nat-traversal use on

設定終了
# save
# commit
```

2.9.16 テンプレート着信機能（AAA 認証）および NAT トラバーサルを使用した可変 IP アドレスでの VPN

IPsec 機能、テンプレート機能および NAT トラバーサルを使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

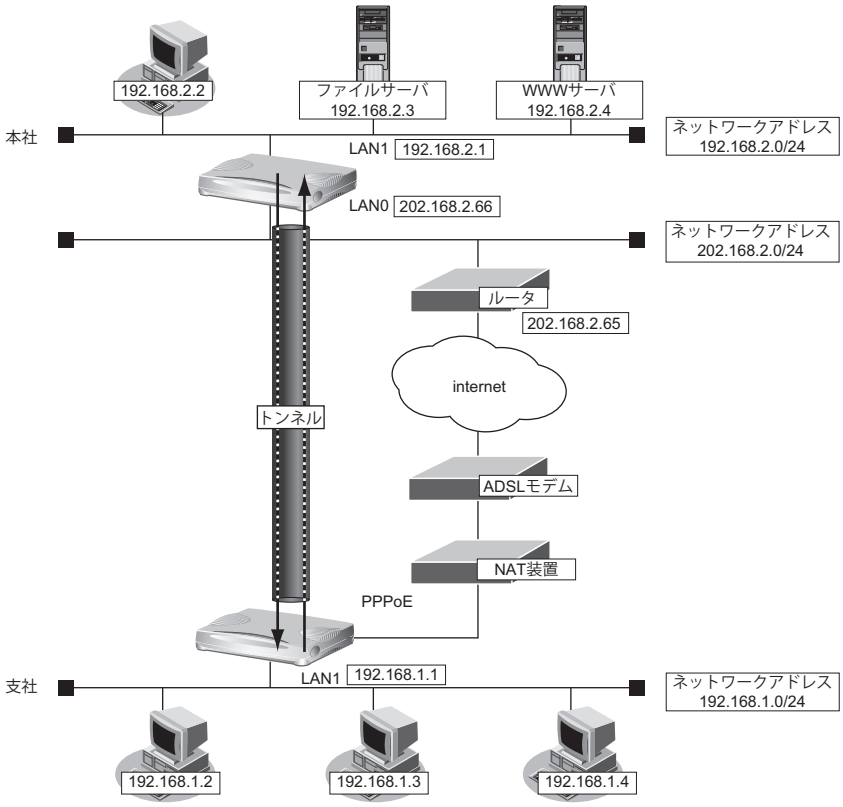
● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：支社 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE区間　：202.168.2.66 - 支社
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE支社ID/IDタイプ　：shisya（自装置名）/FQDN
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768
- IKE NATトラバーサル機能　：使用する

こんな事に気をつけて

- テンプレート着信機能（AAA認証）を使用したIPsecでは、AAA設定のユーザIDとユーザ認証パスワードを同じに設定してください。
- ユーザIDとユーザ認証パスワードは、テンプレート情報のIKE情報の交換モードにより以下のように設定します。
  Main Modeの場合　：相手側IPsecトンネルアドレス
  Aggressive Modeの場合　：相手側の装置識別情報

ヒント

◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

◆ IDタイプとは？

Aggressive Modeの場合に、ネゴシエーションで使用する自装置を識別するIDの種別です。相手VPN装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する（Initiator）

● コマンド

```
PPPoE を設定する
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike nat-traversal use on

設定終了
# save
# commit
```

本社を設定する（Responder）

● コマンド

```
LAN を設定する
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3

VPN（テンプレート）を設定する
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 ike nat-traversal use on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name vpn-shi
# aaa 0 user 0 id shisya
# aaa 0 user 0 password shisya
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# commit
```

2.9.17 接続先情報（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN

IPsec機能、動的VPN情報交換機能、接続先およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社および本社はPPPoEでインターネットに接続され、動的VPNサーバはグローバルアドレス空間の終端装置として本装置が接続されていることを前提とします。

● 前提条件

[本社（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.0.1/24
- PPPoEユーザ認証ID　：userid0（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass0（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社A（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.1.1/24
- PPPoEユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社B（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.2.1/24
- PPPoEユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[動的VPNサーバ]

- ローカルネットワークIPv4アドレス　：192.168.10.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス　：202.168.2.65

● 設定コマンド

[本社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.0.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid0 userpass0
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社 A（PPPoE 常時接続）]

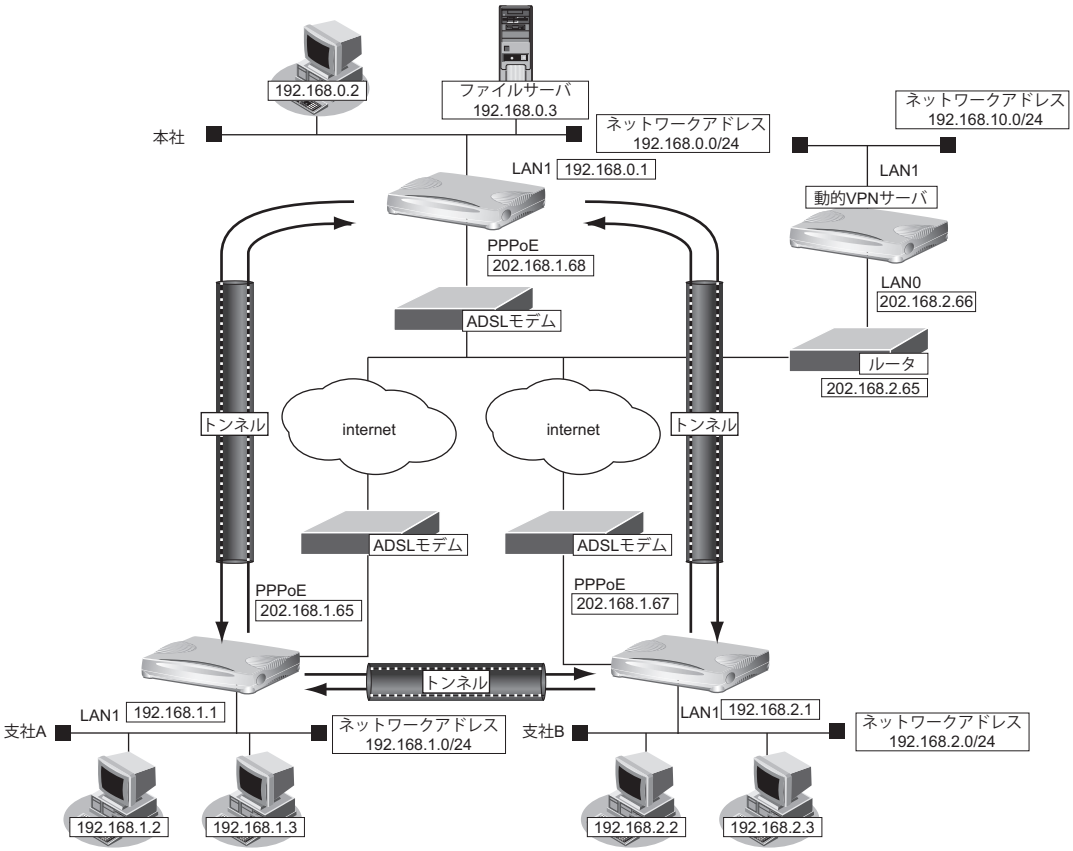
```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社 B（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.2.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[動的 VPN サーバ]

```
# delete lan
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.10.1/24 3
```



● 設定条件（動的VPNサーバ-本社、支社A、B）

[本社（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE 区間　：本社 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.0.1
- ESPのプライベートアドレス　：192.168.0.1

[支社A（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE区間　：支社A - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.1.1
- ESPのプライベートアドレス　：192.168.1.1

[支社B（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE区間　：支社B - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

- IKE（UDP：500 番ポート）のプライベートアドレス
  ：192.168.2.1
- ESP のプライベートアドレス　：192.168.2.1

[動的 VPN サーバ（Responder）]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.2.66 - 本社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 - 支社 A
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：202.168.2.66 - 支社 B
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通（本社、支社 A、B-動的 VPN サーバ）]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 本社 ID/ID タイプ　：honsya （自装置識別情報）/FQDN
- IKE 支社 A ID/ID タイプ　：shisyaA（自装置識別情報）/FQDN
- IKE 支社 B ID/ID タイプ　：shisyaB（自装置識別情報）/FQDN
- IKE 本社 IKE 認証鍵　：1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
- IKE 支社 A IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社 B IKE 認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

● 設定条件（本社 - 支社 A、B）

[本社]

- テンプレート名　：vpn-shi
- IKE（UDP：500 番ポート）のプライベートアドレス
  ：192.168.0.1
- ESP のプライベートアドレス　：192.168.0.1
- テンプレート接続先監視アドレス　：192.168.0.1

[支社A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- テンプレート名　：vpn-shiB
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.1.1
- ESPのプライベートアドレス　：192.168.1.1
- 接続先監視アドレス　：192.168.1.1-192.168.0.1
- テンプレート接続先監視アドレス　：192.168.1.1

[支社B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- テンプレート名　：vpn-shiA
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.2.1
- ESPのプライベートアドレス　：192.168.2.1
- 接続先監視アドレス　：192.168.2.1-192.168.0.1
- テンプレート接続先監視アドレス　：192.168.2.1

● 設定条件（動的VPN接続）

[本社-支社A/B間の動的VPN共通設定]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.10.1
  ポート番号　：5070
- INVITE自動ignore機能　：使用する
- 有効期間　：1時間
- セッション更新間隔　：5分
- ドメイン名　：example.com
- VPN通信
  利用インタフェース　：rmt0
- 動的VPNクライアントの優先度　：10
- 動的VPN IPv4経路情報の優先度　：1
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：aes-cbc-128
- IPsec認証アルゴリズム　：hmac-sha1
- IPsecDHグループ　：modp768
- IKE認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：aes-cbc-128
- IKE認証アルゴリズム　：hmac-sha1
- IKE DHグループ　：modp768

[本社の動的 VPN 設定]

- サーバ情報
  認証 ID　：honsyaid
  認証パスワード　：honsyapass
- クライアントの IP アドレス（本社）　：192.168.0.1
- ローカル ID　：honsya

[支社 A の動的 VPN 設定]

- サーバ情報
  認証 ID　：shisyaAid
  認証パスワード　：shisyaApass
- クライアントの IP アドレス（支社 A）　：192.168.1.1

[支社 B の動的 VPN 設定]

- サーバ情報
  認証 ID　：shisyaBid
  認証パスワード　：shisyaBpass
- クライアントの IP アドレス（支社 B）　：192.168.2.1

[動的 VPN サーバ設定]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAA グループ ID　：0
- AAA ユーザ情報（本社認証情報）
  ユーザ ID　：honsyaid
  認証パスワード　：honsyapass
- AAA ユーザ情報（支社 A 認証情報）
  ユーザ ID　：shisyaAid
  認証パスワード　：shisyaApass
- AAA ユーザ情報（支社 B 認証情報）
  ユーザ ID　：shisyaBid
  認証パスワード　：shisyaBpass

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本社を設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信するように設定する
# remote 0 ip nat static 0 192.168.0.1 500 any 500 17
# remote 0 ip nat static 1 192.168.0.1 any any any 50
# remote 0 ip nat static default reject

本社-動的VPNサーバ間のVPNを設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local honsya
# remote 1 ap 0 ike shared key text 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 0

本社-支社A/B間の動的VPNを設定する
# remote 0 ip dvpn 0 invite acl 0 24 0
# remote 0 ip dvpn 1 invite acl 1 24 0
# acl 0 ip 192.168.0.0/24 192.168.1.0/24 any any
# acl 1 ip 192.168.0.0/24 192.168.2.0/24 any any
# template 0 name vpn-shi
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 tunnel local 192.168.0.1
# template 0 sessionwatch address 192.168.0.1
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth honsyaid honsyapass
# dvpn client 0 ua 192.168.0.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.0.0/24 on
# dvpn client 0 localid honsya
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

支社 A を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

支社 A- 動的 VPN サーバ間の VPN を設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 0

本社 - 支社 A 間の動的 VPN を設定する
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 tunnel local 192.168.1.1
# remote 2 ap 0 sessionwatch address 192.168.1.1 192.168.0.1
# remote 2 ip route 0 192.168.0.0/24 1 0
# remote 2 ip route 1 192.168.2.0/24 1 2

支社間の動的 VPN を設定する
# remote 2 ip dvpn 0 autoignore
# remote 2 ip dvpn 1 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any
# template 0 name vpn-shiB
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
```

```
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

支社 B を設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信するように設定する
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject

支社B-動的VPNサーバ間のVPNを設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 0

本社-支社B間の動的VPNを設定する
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 tunnel local 192.168.2.1
# remote 2 ap 0 sessionwatch address 192.168.2.1 192.168.0.1
```

```
# remote 2 ip route 0 192.168.0.0/24 1 0
# remote 2 ip route 1 192.168.1.0/24 1 2

支社間の動的VPN を設定する
# remote 2 ip dvpn 0 autoignore
# remote 2 ip dvpn 1 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any
# template 0 name vpn-shiA
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

動的 **VPN** サーバを設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-hon
# remote 0 ap 0 name honsya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote honsya
# remote 0 ap 0 ike shared key text 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.0.0/24 1 0
# remote 1 name vpn-shi
# remote 1 ap 0 name shisyaA
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
```

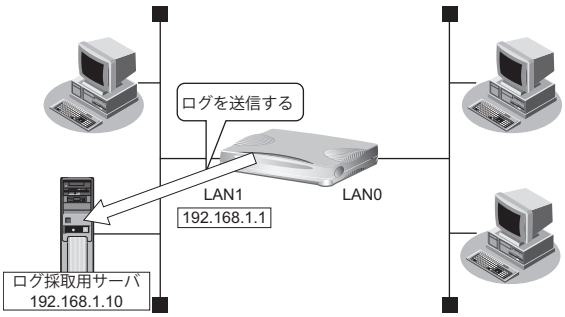
```
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 0
# remote 2 name vpn-shiB
# remote 2 ap 0 name shisyaB
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaB
# remote 2 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.2.0/24 1 0

動的VPNサーバを設定する
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# aaa 0 name dvpnserver
# aaa 0 user 0 id honsyaid
# aaa 0 user 0 password honsyapass
# aaa 0 user 1 id shisyaAid
# aaa 0 user 1 password shisyaApass
# aaa 0 user 2 id shisyaBid
# aaa 0 user 2 password shisyaBpass

設定終了
# save
# reset
```

2.10 システムログを採取する

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上のシステムログサーバに送信することができます。また、セキュリティログとして以下のログを採取することができます。

- PPP（着信拒否）
- IP フィルタ（遮断したパケット）
- URL フィルタ（遮断したパケット）
- NAT（遮断したパケット、変換テーブル作成）
- DHCP（配布した IPv4 アドレス、IPv6 プレフィックス）
- IDS（検出されたパケット）
- MAC アドレス認証（不正端末の MAC アドレス）

ここでは、システムログを採取する場合の設定方法を説明します。



● 設定条件

- 以下のプライオリティを設定する
  - プライオリティ LOG_ERROR
  - プライオリティ LOG_WARNING
  - プライオリティ LOG_NOTICE
  - プライオリティ LOG_INFO
- 以下のセキュリティログを採取する
  - IP フィルタ
  - NAT
  - PPP
  - DHCP
  - Proxy DNS
  - IDS
  - MAC アドレス認証
- ログ受信用サーバの IP アドレス　：192.168.1.10

上記の設定条件に従ってシステムログを採取する場合のコマンド例を示します。

● コマンド

```
# syslog server 192.168.1.10

システムログを設定する
# syslog pri error,warn,notice,info
# syslog security ipfilter,nat,ppp,dhcp,proxydns,ids,macauth

設定終了
# save
# commit
```

採取したシステムログを確認する

採取したシステムログの確認方法は、お使いのサーバによって異なります。

2.11 マルチ NAT 機能（アドレス変換機能）を使う

本装置のマルチ NAT 機能を使用すると、通信発生のたびにあいているグローバルアドレスを割り当てるので、限られた数のグローバルアドレスでそれ以上のパソコンを接続できます。

ここでは、静的 NAT を使って、サーバを公開する場合を例に説明します。静的 NAT は、特定のパソコンやアプリケーションに同じ IP アドレス、ポート番号を割り当てます。そのために Web を公開するような場合に適しています。

☛ 参照　マニュアル「機能説明書」

ヒント

◆ 同時に接続できる台数

機能	同時接続台数およびセッション数	備考
基本 NAT	グローバルアドレス数 セッション数制限なし	割り当て時間内は外部からの通信もできる 基本 NAT と静的 NAT で同一グローバルアドレスを使用しないでください
動的 NAT	最大 1024 セッションまで	外部からの通信はできない
静的 NAT	最大 64 個まで割り当て可能	プライベートアドレスとポートをグローバルアドレスとポートに割り当てできる 割り当てたアドレスとポートに関しては外部からの通信もできる
あて先変換	最大 64 個まで割り当て可能	グローバルアドレスをプライベートアドレスに割り当てできる

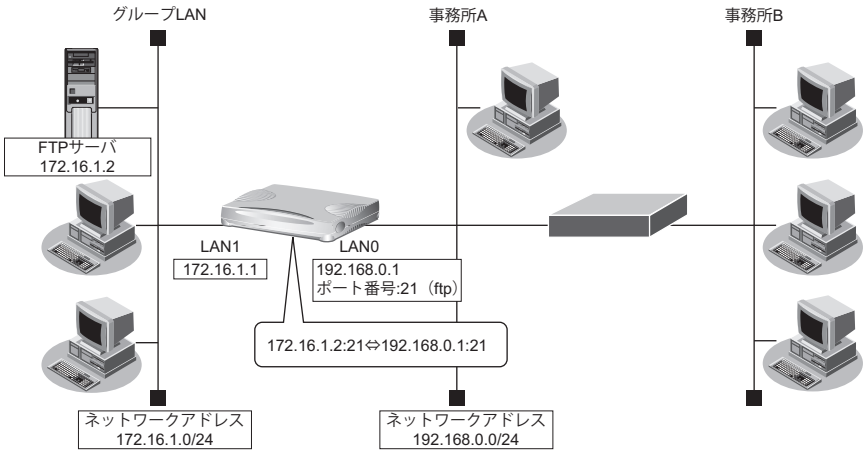
こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　マニュアル「コマンドユーザーズガイド」

2.11.1　プライベート LAN 接続でサーバを公開する

ここでは、静的 NAT を使って、FTP サーバを公開する場合の設定方法を説明します。



● 設定条件

[事務所 A 側]

- LAN0 ポートを使用する
- 静的 NAT を使用する

[グループ LAN 側]

- IP アドレス　：172.16.1.1
- ネットワークアドレス／ネットマスク　：172.16.1.0/24
- FTP サーバの IP アドレス　：172.16.1.2

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT 情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat static 0 172.16.1.2 21 192.168.0.1 21 6

設定終了
# save
# commit
```

こんな事に気をつけて

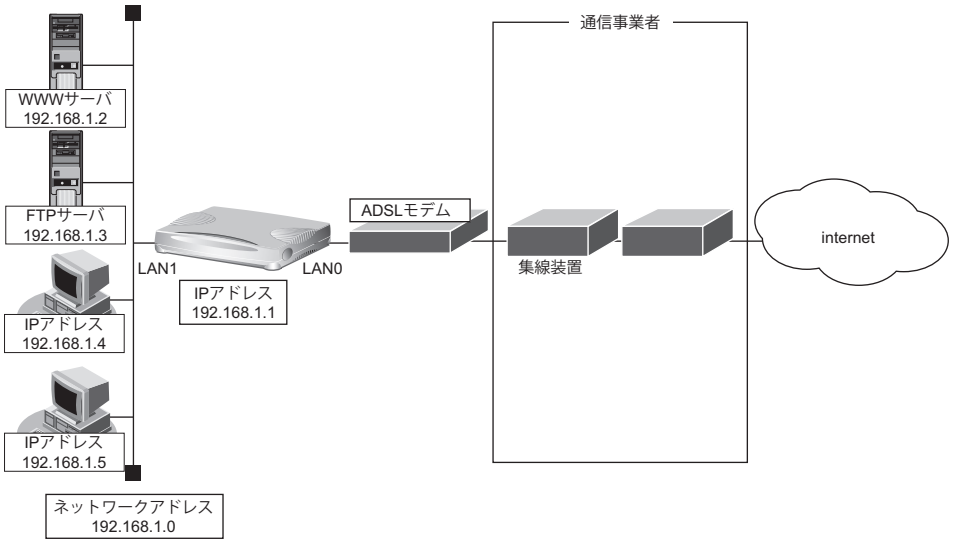
NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.11.2　PPPoE 接続でサーバを公開する

PPPoE を使ってインターネットへ接続している場合の例です。

ここでは、PPPoE 接続時に静的NAT を使ってサーバを公開する場合の設定方法を説明します。



● 設定条件

- 既存の LAN を使用する
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- ネットワークアドレス／ネットマスク　：192.168.1.0/24
- ブロードキャストアドレス　：192.168.1.255

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
PPPoE でインターネットへ接続する環境を設定する
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0

NAT 情報を設定する
# remote 0 ip nat static 0 192.168.1.2 80 any 80 any
# remote 0 ip nat static 1 192.168.1.3 21 any 21 any

設定終了
# save

再起動
# reset
```

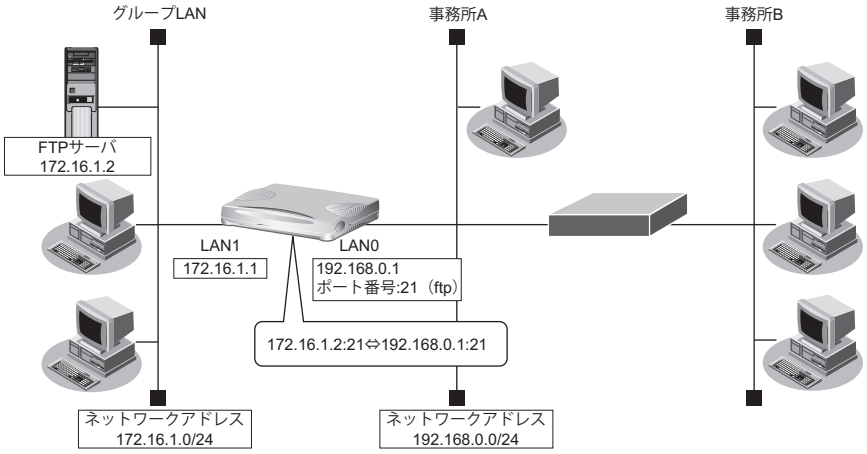
こんな事に気をつけて

- ネットワーク型接続でマルチ NAT を使用する際、グローバルアドレスの設定が必須となります。なお、端末型接続では、接続時にグローバルアドレスが割り当てられるため、設定は不要です。
- 動的 NAT と静的 NAT が混在する場合、動的 NAT で使用する IP アドレスと静的 NAT で使用する IP アドレスは重複しないようにしてください。
- NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# remote 0 ip nat rule 0 ftp any 21 off
# remote 0 ip nat rule 1 dns global 53 off
```

2.11.3 サーバ以外のアドレス変換をしないで、プライベート LAN 接続でサーバを公開する

ここでは、静的 NAT だけを使って、サーバ以外のアドレス変換をしないで、FTP サーバを公開する場合の設定方法を説明します。



● 設定条件

[事務所 A 側]

- LAN0 ポートを使用する
- 静的 NAT だけを使用する

[グループ LAN 側]

- IP アドレス　：172.16.1.1
- ネットワークアドレス／ネットマスク　：172.16.1.0/24
- FTP サーバの IP アドレス　：172.16.1.2

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT 情報を設定する
# lan 0 ip nat mode static any 1 5m
# lan 0 ip nat static 0 172.16.1.2 21 192.168.0.1 21 6

設定終了
# save
# commit
```

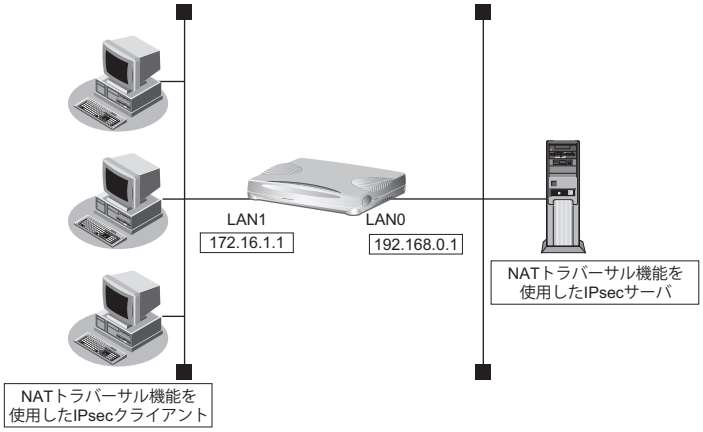
こんな事に気をつけて

NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.11.4 複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する

ここでは、静的 NAT を使って、複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する場合の設定方法を説明します。



● 設定条件

[IPsec サーバ側]

- LAN0 ポートを使用する
- マルチ NAT を使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT 情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat wellknown 0 500 off

設定終了
# save
# commit
```

こんな事に気をつけて

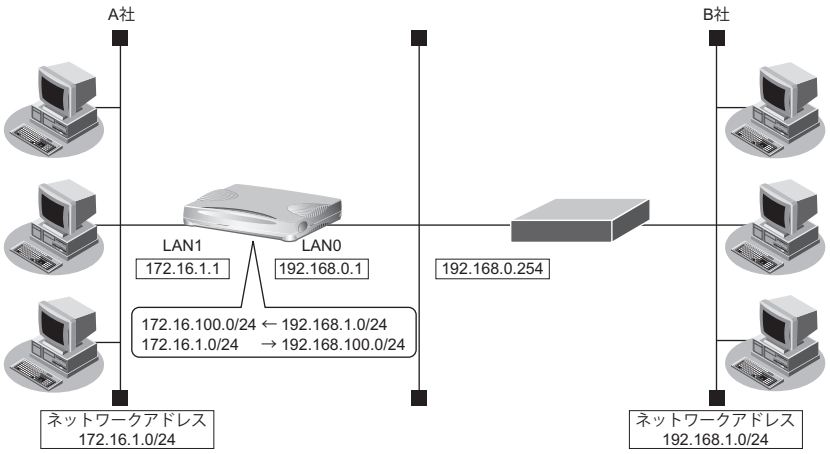
NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.11.5　NAT あて先変換で双方向のアドレスを変換する

ここでは、NAT あて先変換を使って、双方向の IP アドレスを変換する場合の設定方法を説明します。

この機能を使用して異なるアドレス体系を持つＡ社とＢ社を接続した場合、同じアドレス体系であるかのように見せることができます。



● 設定条件

[A 社]

- IP アドレス　：172.16.1.1
- ネットワークアドレス／ネットマスク　：172.16.1.0/24

[B 社]

- LAN0 ポートを使用する
- マルチ NAT を使用する
- NAT あて先変換を使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

B 社 への経路を設定する
# lan 0 ip route 0 192.168.1.0/24 192.168.0.254

NAT 情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat static 0 172.16.1.2 any 192.168.100.2-192.168.100.254 any any
# lan 0 ip nat destination 0 172.16.100.2 192.168.1.2-192.168.1.254

設定終了
# save
# commit
```

2.11.6　NAT 変換テーブル数を拡張する

ここでは、NAT 変換テーブル数を拡張する場合の設定方法を説明します。
本装置の NAT 変換テーブル数については、マニュアル「仕様一覧」を参照してください。

以下にコマンド例を示します。

● コマンド

```
本装置の NAT 変換テーブル数を拡張する
# ip nat table extension

設定終了
# save
# commit
```

こんな事に気をつけて

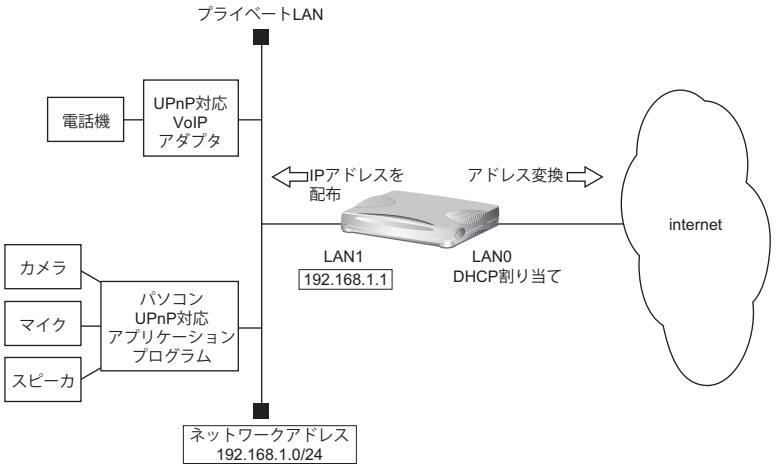
OSPF または BGP を使用する場合、NAT 変換テーブル数の設定は無効であり NAT 変換テーブル数は通常とみなされます。
OSPF または BGP を使用していたが、使用しない設定に変更したあと、NAT 変換テーブル数を拡張する場合は commit コマンドによる構成定義情報の動的反映は行えません。save コマンドを実行後に reset コマンドを実行して本装置を再起動してください。
NAT 変換テーブル数の設定変更を行った場合、NAT が有効なすべてのインタフェースの NAT 変換テーブルがいったん解放されます。

2.12 VoIP NAT トラバーサル機能を使う

マルチ NAT 機能を使用すると動作しない VoIP アダプタが UPnP に対応している場合、本装置の VoIP NAT トラバーサル機能を使用することによって動作できるようになることがあります。同様に、UPnP に対応した装置やアプリケーションプログラムもマルチ NAT 機能を使用しても動作できるようになることがあります。

☛ 参照 マニュアル「機能説明書」

ここでは、UPnP 対応 VoIP アダプタや UPnP 対応アプリケーションプログラムを使用する設定方法を説明します。



● 設定条件

[インターネット側 LAN]

- LAN0 ポートを使用する
- 転送レート　：自動認識
- IP アドレス　：DHCP サーバから自動的に取得
- マルチ NAT を使用する
  グローバルアドレス　：インターネットプロバイダから割り当てられた IP アドレスを使用する
  アドレス個数　：1
  アドレス割り当てタイマ　：5 分
- NAT での SIP アプリ対応を無効にする

[UPnP 対応装置（プライベート LAN）側]

- LAN1 ポートを使用する
- 転送レート　：自動認識
- IP アドレス　：192.168.1.1/24
- DHCP サーバ機能を使用する
  割り当て先頭アドレス　：192.168.1.2
  割り当てアドレス数　：253
  リース期間　：1 日
  デフォルトルータ広報　：192.168.1.1

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
インターネット側のLAN情報を設定する
# delete lan 0
# lan 0 mode auto
# lan 0 ip dhcp service client
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1
# lan 0 ip nat appli sip off

UPnP対応装置側のLAN情報を設定する
# delete lan 1
# lan 1 mode auto
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off

UPnP機能を設定する
# upnp use on

設定終了
# save

再起動
# reset
```

本装置の設定が終了したら、設定を有効にするためにパソコンのシステムを終了し、パソコンおよび本装置の電源を切断します。各装置をLANケーブルで正しく接続したあと、本装置、UPnP対応装置やパソコンの順に電源を投入します。

2.13 TOS/Traffic Class値書き換え機能を使う

本装置を経由してネットワークに送信される、またはネットワークから受信したパケットをIPアドレスとポート番号の組み合わせでTOS/Traffic Class値を変更することにより、ポリシーベースネットワークのポリシーに合わせることができます。

参照 マニュアル「機能説明書」

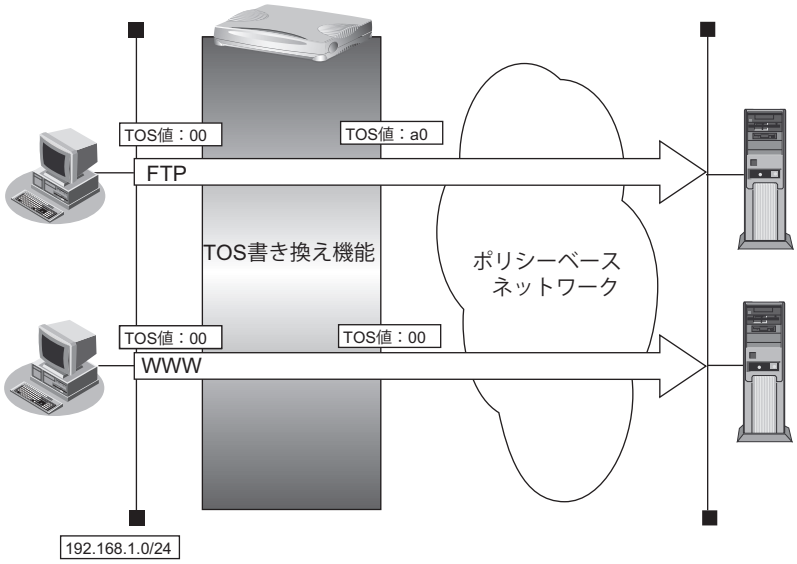
TOS/Traffic Class値書き換え機能の条件

本装置では、コマンドで以下の条件を指定することによって、ポリシーベースネットワークのポリシーに合ったTOS/Traffic Class値に書き換えることができます。

- プロトコル
- 送信元情報（IPアドレス／アドレスマスク／ポート番号）
- あて先情報（IPアドレス／アドレスマスク／ポート番号）
- IPパケットのTOS値またはIPv6パケットのTraffic Class値
- 新TOSまたはTraffic Class

ここではネットワークが以下のポリシーを持つ場合の設定方法を説明します。

- FTP（TOS値a0）を最優先とする
- その他はなし



● 設定条件

- 送信元IPアドレス／アドレスマスク　：192.168.1.0/24
- 送信元ポート番号　：指定しない
- あて先IPアドレス／アドレスマスク　：指定しない
- あて先ポート番号　：20（ftp-dataのポート番号）、21（ftpのポート番号）
- プロトコル　：TCP
- TOS値　：00
- 新TOS値　：a0

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
FTP サーバのアクセスで TOS 値を 00 から a0 に書き換える
# acl 0 ip 192.168.1.0/24 any 6 tos 0
# acl 0 tcp any 20,21 yes
# remote 0 ip tos 0 acl 0 a0

設定終了
# save
# commit
```

2.14 VLANプライオリティマッピング機能を使う

VLANプライオリティマッピング機能を使用して、レイヤ2スイッチなどでQoS制御を行うことができます。

本装置から送信されるVLANパケットのVLANのプライオリティ値を、IPパケットのTOSフィールドおよびIPv6パケットのトラフィッククラスフィールドの値から設定します。

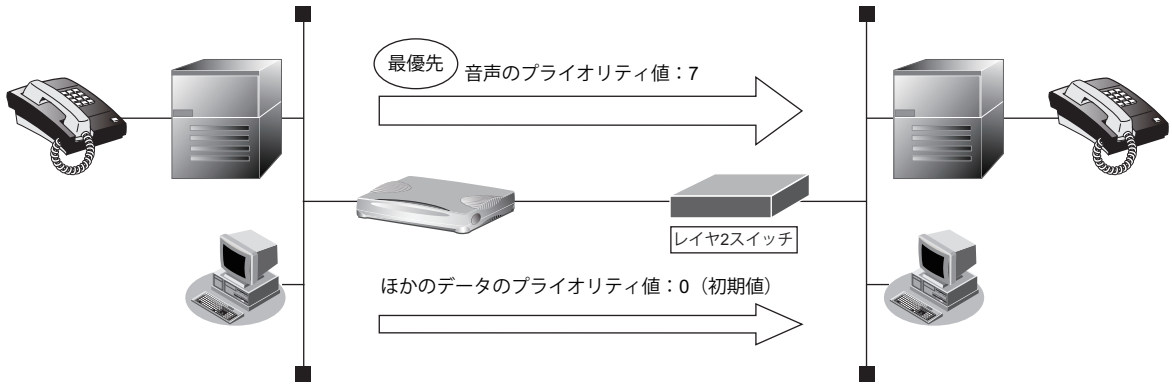
参照 マニュアル「機能説明書」

本装置では、コマンドで以下の条件を指定することによって、VLANのプライオリティフィールドを設定することができます。

- プロトコル
- TOS/Traffic Class
- プライオリティ

ここでは、本装置が以下の音声データを転送する場合の設定方法を説明します。

- 音声（IPでTOS値がa0）を最優先とする（プライオリティ値が7）
- その他は初期値（プライオリティ値が0）



● 設定条件

- プロトコル　：IPv4
- TOS値　：a0
- プライオリティ値　：7

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

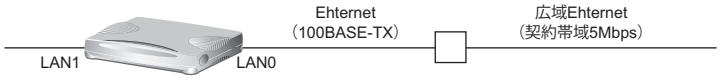
```
TOS値a0のパケットのプライオリティ値を7に設定する
# lan 0 vlan tag primap 0 ip a0 7

設定終了
# save
# commit
```

2.15 シェーピング機能を使う

シェーピング機能を使用すると、LANおよびWAN回線に送出するデータ量を制限することができます。

2.15.1 特定のインタフェースでシェーピング機能を使う

ここでは、Ethernet回線の送出するデータ量を制限する場合の設定方法を説明します。



● 設定条件

- 広域Ethernetを利用する通信環境が設定済み
- 広域Ethernetの契約帯域は5Mbps

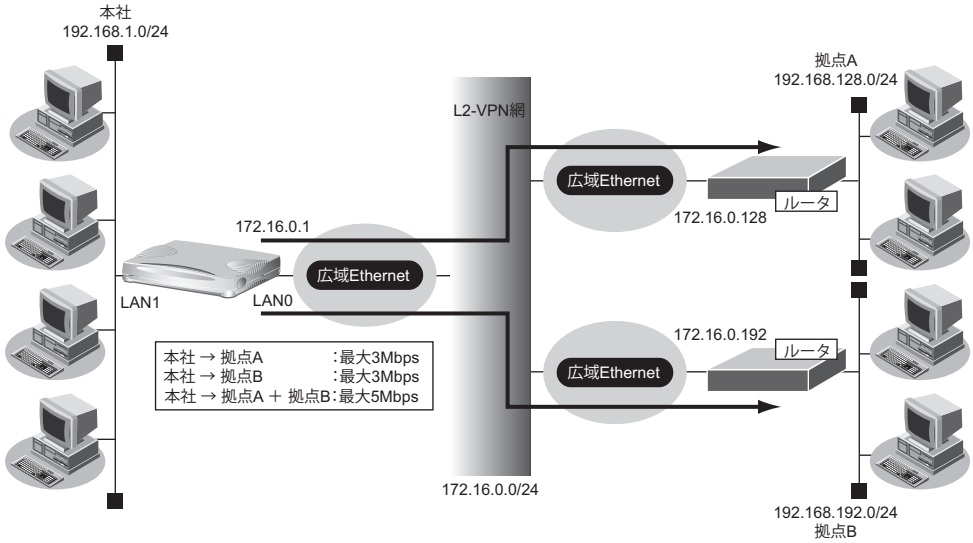
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
LAN0の送出するデータ量を5Mbpsに制限する
# lan 0 shaping on 5m

設定終了
# save
# commit
```

2.15.2　送信先ごとにシェーピング機能を使う

ここでは、各拠点に送出するデータ量を制限する場合の設定方法を説明します。



● 設定条件

- 広域 Ethernet をアクセスラインとする。L2-VPN 網を利用して本社と各拠点を接続する
- 本社から拠点 A への送信データは、最大 3Mbps に制限する
- 本社から拠点 B への送信データは、最大 3Mbps に制限する
- 本社から拠点 A と拠点 B への送信データの合計は、最大 5Mbps に制限する
- 本社の本装置は LAN ポートのアドレス設定ができた状態から設定を始める

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
シェーピング機能を設定する
# lan 0 shaping on 5m

拠点Aの情報を設定する
# remote 0 name kyotenA
# remote 0 ip route 0 192.168.128.0/24 1 1
# remote 0 shaping on 3m
# remote 0 ap 0 name OV-A
# remote 0 ap 0 datalink type overlap
# remote 0 ap 0 overlap to lan 0
# remote 0 ap 0 overlap nexthop 172.16.0.128

拠点Bの情報を設定する
# remote 1 name kyotenB
# remote 1 ip route 0 192.168.192.0/24 1 1
# remote 1 shaping on 3m
# remote 1 ap 0 name OV-B
# remote 1 ap 0 datalink type overlap
# remote 1 ap 0 overlap to lan 0
# remote 1 ap 0 overlap nexthop 172.16.0.192

設定終了
# save
# commit
```

2.16 ヘッダ圧縮機能を使う

PPP を使った相手装置との接続時に、ヘッダ圧縮機能によって回線の利用効率を高めることができます。

ヘッダ圧縮機能を利用する場合、接続する相手装置側でも同じ圧縮機能をサポートしている必要があります。以下に、サポートしている圧縮機能を示します。

- ヘッダ圧縮
  - VJ　：VJ ヘッダ圧縮（RFC1144 に準拠）の利用
  - IPHC　：IP ヘッダ圧縮（圧縮方法：RFC2507/RFC2508、ネゴシエーション方法：RFC2509 に準拠）の利用

ここでは、PPPoE 接続をネットワーク 0（remote 0）で定義している環境に対して、ヘッダ圧縮を行う場合の設定方法を説明します。

● 設定条件

- ネットワーク 0（remote 0）で PPPoE による通信環境が設定済み
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってヘッダ圧縮を行う場合のコマンド例を示します。

● コマンド

```
ヘッダ圧縮機能を設定する
# remote 0 ppp ipcp vjcomp enable
# remote 0 ppp ipcp iphc enable

設定終了
# save
# commit
```

こんな事に気をつけて

ヘッダ圧縮機能は、シェーピングによって通信速度が低速の場合に効果があります。高速回線で使用した場合は、処理のオーバーヘッドによって回線の利用効率が低くなることがあります。

2.17 帯域制御（WFQ）機能を使う

本装置の帯域制御（WFQ）機能では、IP アドレスやポート番号の組み合わせで帯域を割り当てることによって、特定のデータを優先的に通すことができます。

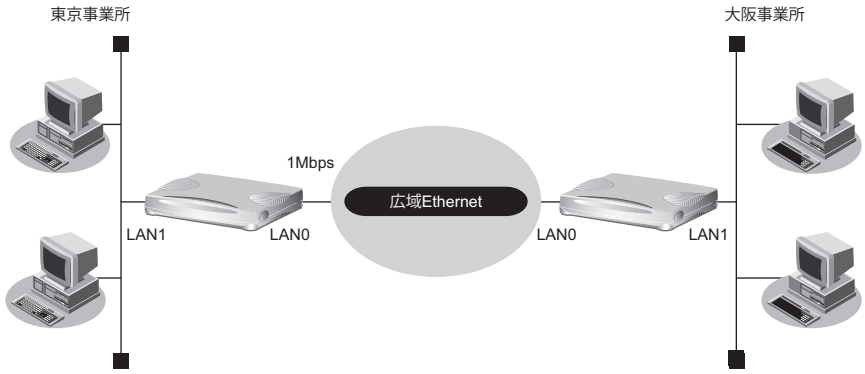
参照 マニュアル「機能説明書」

帯域制御（WFQ）機能の条件

本装置では、以下の条件を指定することによって、優先的にデータを通すように帯域を割り当てることができます。

- プロトコル
- IP アドレス
- ポート番号
- IP パケットの TOS 値または IPv6 パケットの Traffic Class 値

ここでは、広域 Ethernet による拠点間の接続がすでに設定されている場合を例に帯域制御を利用する設定方法を説明します。



● 設定条件

- LAN0 インタフェースで広域 Ethernet を利用する通信環境が設定済み
- 広域 Ethernet の契約速度は 1Mbps
- 音声データ（TOS 値：a0）を最優先で透過させる

上記の設定条件に従って帯域制御する場合のコマンド例を示します。

東京事業所を設定する

● コマンド

```
シェーピングを設定する
# lan 0 shaping on 1m

帯域制御（WFQ）を設定する
# acl 0 ip any any any tos a0
# lan 0 ip priority 0 acl 0 express

設定終了
# save
# commit
```

大阪事業所を設定する

● コマンド

```
シェーピングを設定する
# lan 0 shaping on 1m

帯域制御（WFQ）を設定する
# acl 0 ip any any any tos a0
# lan 0 ip priority 0 acl 0 express

設定終了
# save
# commit
```

2.18 DHCP機能を使う

本装置のIPv4 DHCPには、以下の機能があります。

- DHCPサーバ機能
- DHCPスタティック機能
- DHCPクライアント機能
- DHCPリレーエージェント機能

☛参照 マニュアル「機能説明書」

本装置では、それぞれのインタフェースでDHCP機能が使用できます。

こんな事に気をつけて

- 1つのインタフェースでは、1つの機能だけ動作します。同時に複数の機能を動作することはできません。
- 本装置のDHCPサーバは、リレーエージェントを経由して運用することはできません。

本装置のIPv6 DHCPには、以下の機能があります。

- IPv6 DHCPサーバ機能
- IPv6 DHCPクライアント機能

☛参照 マニュアル「機能説明書」

2.18.1　DHCP サーバ機能を使う

DHCP サーバ機能は、ネットワークに接続されているパソコンに対して、IP アドレスの自動割り当てを行う機能です。管理者はパソコンが増えるたびに IP アドレスが重複しないように設定する必要があります。

この機能を利用すると、DHCP クライアント機能を持つパソコンは IP アドレスの設定が不要になり、管理者の手間を大幅に省くことができます。

本装置の DHCP サーバ機能は、以下の情報を広報することができます。

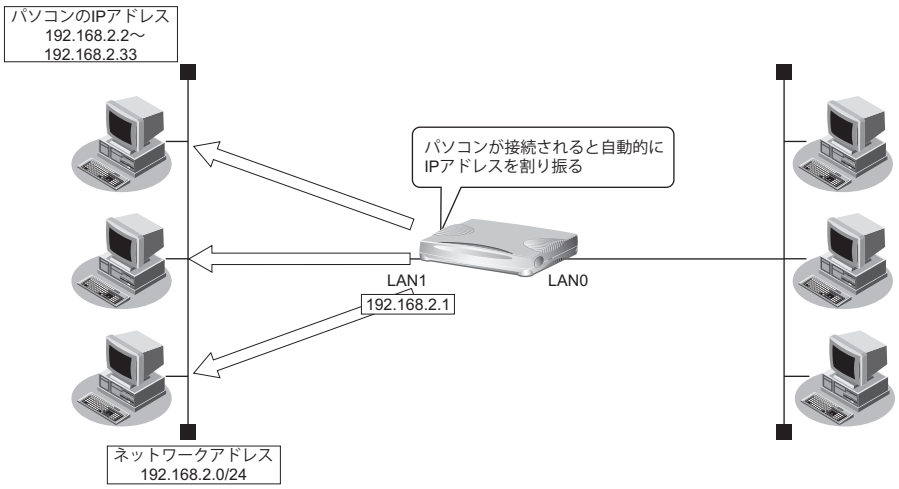
- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- DNS サーバの IP アドレス
- ドメイン名
- NTP サーバの IP アドレス
- TIME サーバの IP アドレス
- WINS サーバの IP アドレス
- SIP サーバのドメイン名または IP アドレス

こんな事に気をつけて

本装置の DHCP サーバ機能は、DHCP リレーエージェントのサーバにはなれません。

ここでは、DHCP サーバ機能を使用する場合の設定方法を説明します。

補足　DHCP サーバ機能で割り当てることのできる IP アドレスの最大数は 253 個です。



● 設定条件

- 本装置の IP アドレス　：192.168.2.1
- ブロードキャストアドレス　：3（ネットワークアドレス＋オール 1）
- パソコンに割り当てる IP アドレス　：192.168.2.2 ～ 192.168.2.33
- パソコンに割り当て可能 IP アドレス数　：32
- ネットワークアドレス／ネットマスク　：192.168.2.0/24
- デフォルトルータの IP アドレス　：192.168.2.1
- リース期間　：1 日
- DHCP サーバ機能を使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DHCP サーバ機能を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp info address 192.168.2.2/24 32
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.2.1
# lan 1 ip dhcp service server

設定終了
# save
# commit
```

2.18.2　DHCP スタティック機能を使う

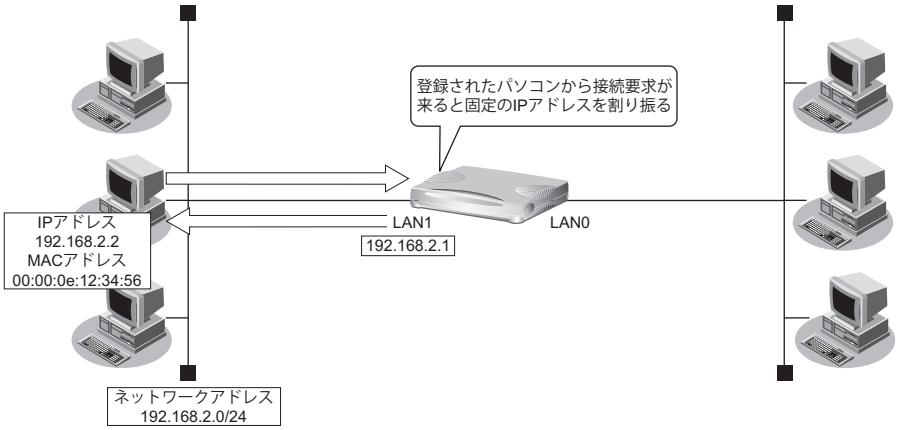
DHCP サーバは、使用していない IP アドレスを一定期間（またはパソコンが IP アドレスを返却するまで）割り当てます。不要になった IP アドレスは自動的に再利用されるため、パソコンの IP アドレスが変わることがあります。本装置では、IP アドレスと MAC アドレスを対応付けることによって、登録されたパソコンから DHCP 要求が発行されると、常に同じ IP アドレスを割り当てることができます。これを DHCP スタティック機能と言います。

DHCP スタティック機能を利用する場合は、ホストデータベース情報に IP アドレスと MAC アドレスを設定してください。

補足
- MAC アドレスとは、LAN 機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。
- 本装置がサポートしている「IP フィルタリング機能」、「マルチルーティング機能」などはパソコンの IP アドレスが固定されていないと使いにくい場合があります。これらの機能と DHCP サーバ機能の併用を実現するために、本装置では「DHCP スタティック機能」をサポートしています。

ここでは、DHCP スタティック機能を使用する場合の設定方法を説明します。

補足
- ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。
- DHCP スタティック機能で設定できるホストの最大数は 64 個です。



● 設定条件

- ネットワークアドレス／ネットマスク　：192.168.2.0/24
- IP アドレスを固定するパソコンの MAC アドレス：00:00:0e:12:34:56
- 割り当て IP アドレス　：192.168.2.2
- DHCP サーバ機能を使用する

こんな事に気をつけて

DHCP サーバ機能を使用するコマンドを実行していない場合、DHCP スタティック機能の設定は無効となります。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DHCP サーバ機能を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp info address 192.168.2.2/24 32
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.2.1
# lan 1 ip dhcp service server

DHCP スタティック機能を設定する
# host 0 ip address 192.168.2.2
# host 0 mac 00:00:0e:12:34:56

設定終了
# save
# commit
```

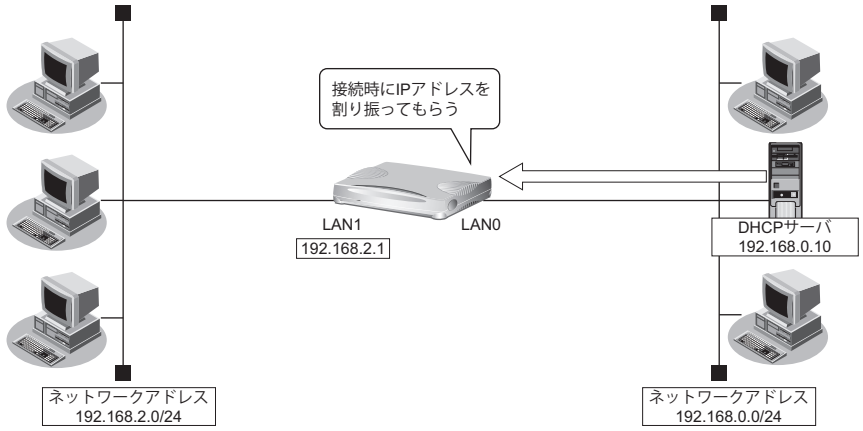
2.18.3　DHCP クライアント機能を使う

DHCP クライアント機能は、DHCP サーバから IP アドレスなどの情報を取得する機能です。使用する場合は、DHCP サーバが動作している LAN に接続する必要があります。利用者は、IP アドレスを意識することなくネットワークを利用できます。

本装置の DHCP クライアント機能は、以下の情報を受け取って動作します。

- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- DNS サーバの IP アドレス
- TIME サーバの IP アドレス
- NTP サーバの IP アドレス
- ドメイン名
- リース更新時間

ここでは、DHCP クライアント機能を使用する場合の設定方法を説明します。



● 設定条件

- 本装置の IP アドレス　　：DHCP サーバから取得する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

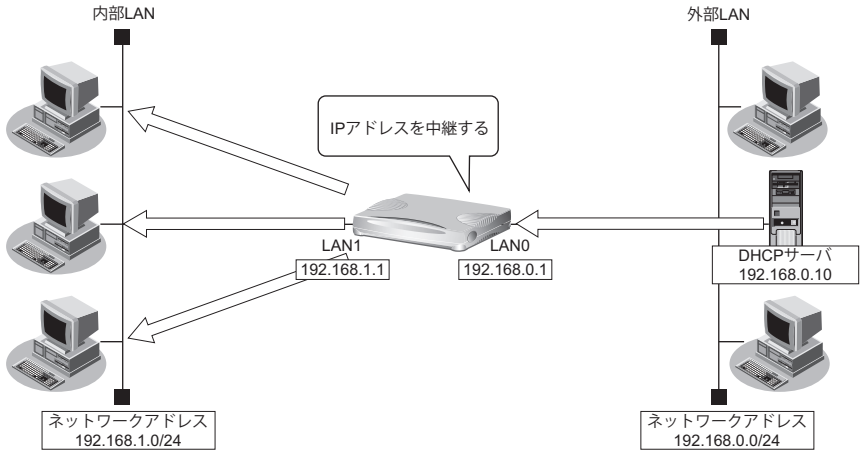
```
DHCP クライアント機能を設定する
# lan 0 ip dhcp service client

マルチ NAT 機能を設定する
# lan 0 ip nat mode multi any 1

LAN1 インタフェースを設定する
# lan 1 ip address 192.168.2.1/24 3

設定終了
# save
# commit
```

2.18.4　DHCP リレーエージェント機能を使う

DHCPクライアントは､同じネットワーク上にあるサーバから､IPアドレスなどの情報を獲得することができます。

DHCP リレーエージェントは、遠隔地にある DHCP クライアントの要求を DHCP サーバが配布する情報を中継する機能です。この機能を利用することで、遠隔地の別のネットワークに DHCP サーバが存在する場合も同様に情報を獲得することができます。

ここでは、DHCP リレーエージェント機能を使用する場合の設定方法を説明します。



● 設定条件

[内部 LAN 側]

- 本装置の IP アドレス　：192.168.1.1
- DHCP リレーエージェント機能を使用する

[外部 LAN 側]

- 本装置の IP アドレス　：192.168.0.1
- DHCP サーバ　：192.168.0.10

補足 DHCP リレーエージェント機能を使用するときは、NAT 機能を使用できません。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

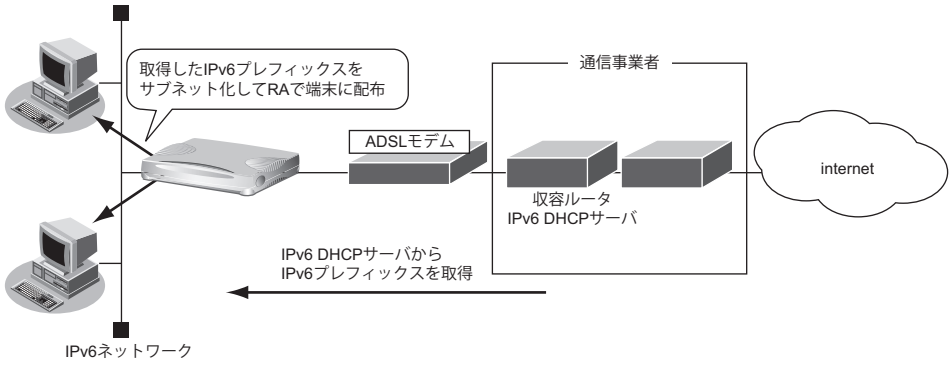
● コマンド

```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 192.168.1.1/24 3

DHCP リレーエージェント機能を設定する
# lan 1 ip dhcp service relay 192.168.0.10

設定終了
# save
# commit
```

2.18.5　IPv6 DHCP クライアント機能を使う

IPv6 DHCP クライアント機能は、プロバイダの IPv6 DHCP サーバから IPv6 プレフィックスなどの情報を取得する機能です。この機能を利用すると、プロバイダから取得した IPv6 プレフィックスをサブネット化して、Router Advertisement Message（RA）で下流ネットワークに 64 ビットの IPv6 プレフィックスを配布することができます。

ここでは、PPPoE でインターネットに接続して、IPv6 DHCP クライアント機能を使用する場合の設定方法を説明します。



● 設定条件

- PPPoE で使用する LAN ポート　：LAN0 ポート
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- IPv6 DHCP サーバから取得する IPv6 プレフィックス長　：48 ビット
- IPv6 プレフィックスを配布する LAN ポート　：LAN1 ポート
- RA で配布する IPv6 プレフィックスのサブネット ID　：0001

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 mode auto

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip6 use on

IPv6 DHCP クライアントを設定する
# remote 0 ip6 dhcp service client

ProxyDNS を設定する
# proxydns domain 0 any * any on 0
# proxydns address 0 any on 0

LAN 情報を設定する
# lan 1 ip6 use on
# lan 1 ip6 address 0 dhcp@rmt0:1::/64 infinity infinity
# lan 1 ip6 ra mode send

設定終了
# save

再起動
# reset
```

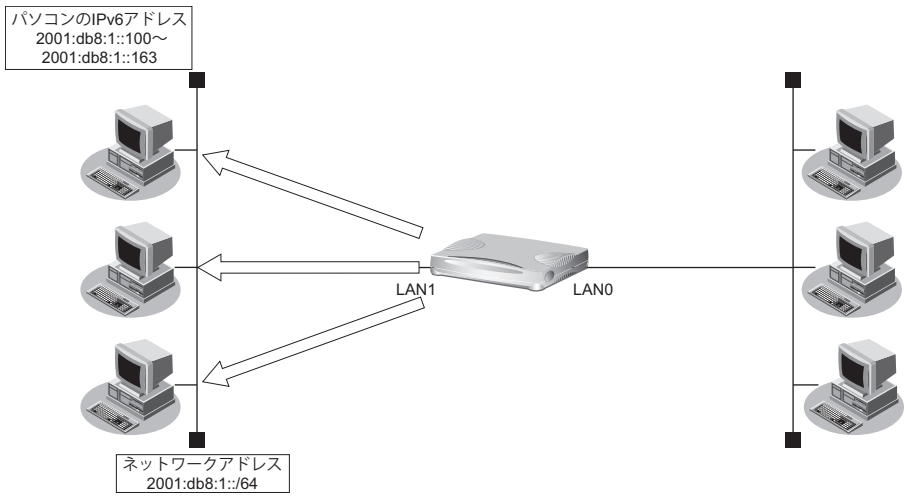
2.18.6　IPv6 DHCP サーバ機能を使う

本装置の IPv6 DHCP サーバ機能は、以下の情報を広報することができます。

- IPv6 アドレス
- IPv6 プレフィックス
- DNS サーバの IPv6 アドレス
- DNS ドメイン名
- SIP サーバの IPv6 アドレス
- SIP ドメイン名
- SNTP サーバの IPv6 アドレス

ここでは、IPv6 DHCP サーバ機能を使用する場合の設定方法を説明します。

補足　IPv6 DHCP サーバ機能で割り当てることのできる IP アドレスの最大数は 300 個です。



● 設定条件

- 本装置の IP アドレス　：2001:db8:1::1
- パソコンに割り当てる IPv6 アドレス　：2001:db8:1::100～2001:db8:1::163
- パソコンに割り当て可能 IPv6 アドレス数　：100
- ネットワークアドレス／プレフィックス長　：2001:db8:1::/64
- Valid Lifetime　：30 日
- Preferred Lifetime　：7 日
- DNS サーバの IPv6 アドレス　：2001:db8:1::53
- IPv6 DHCP サーバ機能を使用する

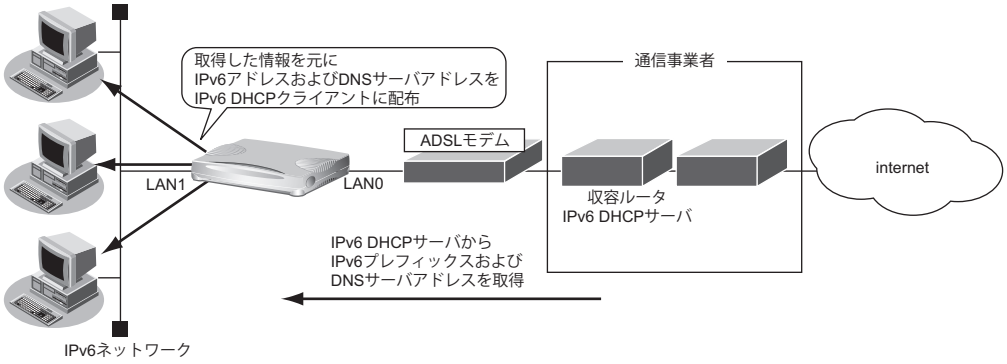
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
IPv6 DHCPサーバの動作するインタフェースを設定する
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1::1/64 infinity infinity c0
# lan 1 ip6 ra mode send
# lan 1 ip6 ra flags c0

IPv6 DHCPサーバ機能を設定する
# lan 1 ip6 dhcp service server
# lan 1 ip6 dhcp server info address 2001:db8:1::100 100 30d 7d
# lan 1 ip6 dhcp server info dns 2001:db8:1::53

設定終了
# save
# commit
```

2.18.7 IPv6 DHCP クライアント機能で取得した情報を IPv6 DHCP サーバ機能で配布する

ここでは、IPv6 DHCP クライアント機能と IPv6 DHCP サーバ機能を併用し、クライアントが取得した情報をサーバが配布する場合の設定方法を説明します。



● 設定条件

- PPPoE で使用する LAN ポート　：LAN0 ポート
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- IPv6 DHCP サーバから取得する IPv6 プレフィックス長　：48 ビット
- IPv6 アドレスを配布する LAN ポート　：LAN1 ポート
- パソコンに割り当てる IPv6 アドレスのサブネット ID　：0001
- パソコンに割り当てる IPv6 アドレスのインタフェース ID　：::100 ～ ::163
- パソコンに割り当て可能 IPv6 アドレス数　：100
- パソコンに配布する DNS サーバの IPv6 アドレス　：IPv6 DHCP クライアントが取得した DNS サーバアドレス

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 mode auto

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip6 use on

IPv6 DHCP クライアントを設定する
# remote 0 ip6 dhcp service client

LAN 情報を設定する
# lan 1 ip6 use on
# lan 1 ip6 address 0 dhcp@rmt0:1::/64 infinity infinity
# lan 1 ip6 ra mode send
# lan 1 ip6 ra flags c0

IPv6 DHCP サーバを設定する
# lan 1 ip6 dhcp service server
# lan 1 ip6 dhcp server info address dhcp@rmt0:1::100 100 30d 7d
# lan 1 ip6 dhcp server info dns dhcp@rmt0

設定終了
# save
# commit
```

2.19 DNS サーバ機能を使う（ProxyDNS）

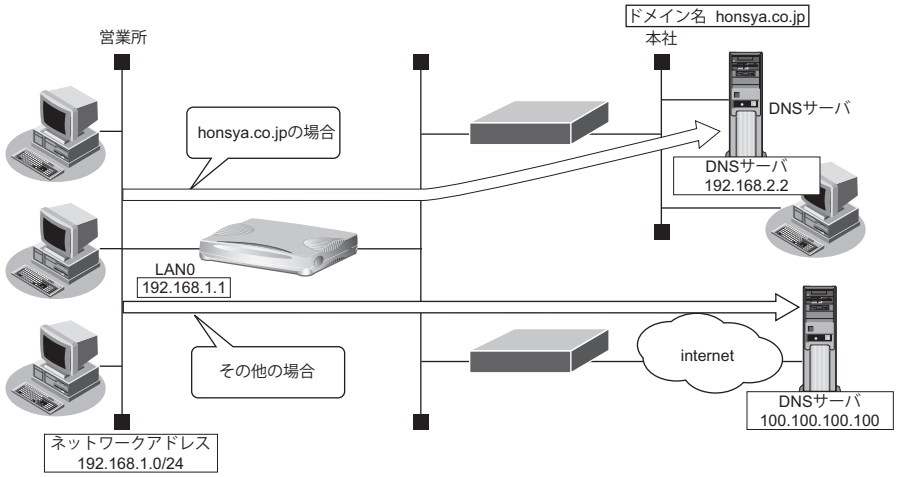
本装置の ProxyDNS には、以下の機能があります。

- DNS サーバの自動切り替え機能
- DNS サーバアドレスの自動取得機能
- DNS 問い合わせタイプフィルタ機能
- DNS サーバ機能

参照 マニュアル「機能説明書」

2.19.1 DNS サーバの自動切り替え機能（順引き）を使う

ProxyDNS は、パソコン側で本装置の IP アドレスを DNS サーバの IP アドレスとして登録するだけで、ドメインごとに使用する DNS サーバを切り替えて中継できます。ここでは、順引きの場合の設定方法を説明します。



● 設定条件

- 会社の DNS サーバを使用する場合
  使用するドメイン　：honsya.co.jp
  DNS サーバの IP アドレス　：192.168.2.2
- インターネット上の DNS サーバを使用する場合
  使用するドメイン　：honsya.co.jp 以外
  DNS サーバの IP アドレス　：100.100.100.100

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DNS サーバ自動切り替え機能（順引き）を設定する
# proxydns domain 0 any *.honsya.co.jp any static 192.168.2.2
# proxydns domain 1 any * any static 100.100.100.100

設定終了
# save
# commit
```

パソコン側の設定を確認する

1. パソコン側が DHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。

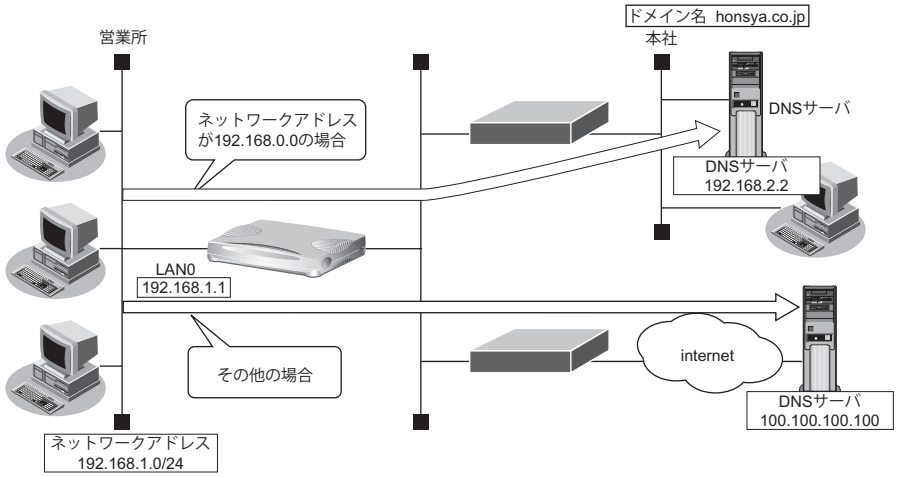
こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザーズガイド」

2.19.2　DNS サーバの自動切り替え機能（逆引き）を使う

ProxyDNS は、先に説明した順引きとは逆に、IP アドレスごとに使用する DNS サーバを切り替えて中継できます。ここでは、逆引きの場合の設定方法を説明します。



● 設定条件

- 会社の DNS サーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0
  DNS サーバの IP アドレス　：192.168.2.2
- インターネット上の DNS サーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0 以外
  DNS サーバの IP アドレス　：100.100.100.100

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛参照 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DNS サーバ自動切り替え機能（逆引き）を設定する
# proxydns address 0 192.168.0.0/24 static 192.168.2.2
# proxydns address 1 any static 100.100.100.100

設定終了
# save
# commit
```

パソコン側の設定を確認する

1.　パソコン側が DHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。

2.19.3　DNS サーバアドレスの自動取得機能を使う

この機能を利用すると、ProxyDNS が DNS サーバのアドレスを、回線接続時に接続先から自動的に取得します。そのため、DNS サーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、接続先が DNS サーバアドレスの配布機能（RFC1877）に対応している場合にだけ利用できます。

● 設定条件

- ドメイン名　：＊
- 動作　：接続先の DNS サーバへ指定ネットワークを経由して問い合わせる

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
DNS サーバアドレスの自動取得機能を設定する
# proxydns domain 0 any * any on 0 off

設定終了
# save
# commit
```

パソコン側の設定を行う

ここでは、Windows 7の場合を例に説明します。

1. ［スタート］－［コントロールパネル］をクリックします。
2. ［ネットワークとインターネット］をクリックします。
3. ［ネットワークと共有センター］をクリックします。
4. ［アダプターの設定の変更］をクリックします。
5. ［ローカルエリア接続］アイコンを右クリックし、［プロパティ］ボタンをクリックします。
   ［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。
6. 一覧から「インターネットプロトコルバージョン4（TCP/IPv4）」を選択します。
7. ［プロパティ］ボタンをクリックします。
   ［インターネットプロトコルバージョン4（TCP/IPv4）のプロパティ］ダイアログボックスが表示されます。
8. 「次のDNSサーバーのアドレスを使う」を選択します。
9. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。
10. ［OK］ボタンをクリックします。
    ［ローカルエリア接続のプロパティ］ダイアログボックスに戻ります。
11. ［閉じる］ボタンをクリックします。
    設定した内容が有効になります。

ヒント

◆ 本装置の「DHCPサーバ機能」を使わない場合の設定は？

パソコン側の「DNS設定」で本装置のIPアドレスを指定すると、ProxyDNS機能だけ使用できます。また、本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとして本装置のIPアドレスを指定するとProxyDNS機能を使用できます。

◆ DNS解決したホストへのホスト経路を自動で作成する設定は？

以下のコマンドを設定することにより、DNS解決したホストへのホスト経路を自動で作成することができます。

```
# proxydns domain 0 any * any on 0 on
```

◆「接続先のDNSサーバへ問い合わせる」と「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」の違いは？

「接続先のDNSサーバへ問い合わせる」は、経路情報に従って、接続先から取得したDNSサーバへ問い合わせるのに対して、「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視して指定ネットワークを経由して、接続先から取得したDNSサーバへ問い合わせます。

2.19.4　DNS サーバアドレスを DHCP サーバから取得して使う

この機能を利用すると、ProxyDNS が DNS サーバのアドレスを、DHCP サーバから自動的に取得します。そのため、DNS サーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、DHCP サーバが DNS サーバのアドレスを広報している場合にだけ利用できます。

● 設定条件

- ドメイン名　：＊
- 動作　：lan0 の DNS サーバへ問い合わせる

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛参照 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
DNS サーバアドレスの自動取得機能を設定する
# proxydns domain 0 any * any dhcp lan0

設定終了
# save
# commit
```

パソコン側の設定を行う

ここでは、Windows 7の場合を例に説明します。

1. ［スタート］－［コントロールパネル］をクリックします。
2. ［ネットワークとインターネット］をクリックします。
3. ［ネットワークと共有センター］をクリックします。
4. ［アダプターの設定の変更］をクリックします。
5. ［ローカルエリア接続］アイコンを右クリックし、［プロパティ］ボタンをクリックします。
   ［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。
6. 一覧から「インターネットプロトコルバージョン4（TCP/IPv4）」を選択します。
7. ［プロパティ］ボタンをクリックします。
   ［インターネットプロトコルバージョン4（TCP/IPv4）のプロパティ］ダイアログボックスが表示されます。
8. 「次のDNSサーバーのアドレスを使う」を選択します。
9. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。
10. ［OK］ボタンをクリックします。
    ［ローカルエリア接続のプロパティ］ダイアログボックスに戻ります。
11. ［閉じる］ボタンをクリックします。
    設定した内容が有効になります。

ヒント

◆ 本装置の「DHCPサーバ機能」を使わない場合の設定は？

パソコン側の「DNS設定」で本装置のIPアドレスを指定すると、ProxyDNS機能だけ使用できます。また、本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとして本装置のIPアドレスを指定するとProxyDNS機能を使用できます。

◆ DNS解決したホストへのホスト経路を自動で作成する設定は？

以下のコマンドを設定することにより、DNS解決したホストへのホスト経路を自動で作成することができます。

```
# proxydns domain 0 any * any on 0 on
```

◆「接続先のDNSサーバへ問い合わせる」と「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」の違いは？

「接続先のDNSサーバへ問い合わせる」は、経路情報に従って、接続先から取得したDNSサーバへ問い合わせるのに対して、「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視して指定ネットワークを経由して、接続先から取得したDNSサーバへ問い合わせます。

2.19.5　DNS 問い合わせタイプフィルタ機能を使う

端末が送信する DNS パケットのうち、特定の問い合わせタイプ（QTYPE）のパケットを破棄することができます。たとえば、パソコンからの予期しない DNS パケット送信によって、自動発信する問題を回避するために、かんたん設定のかんたんフィルタを「使用する」に設定します。このとき、問い合わせタイプが SOA（6）と SRV（33）のパケットを破棄する場合の設定方法を説明します。

こんな事に気をつけて

ProxyDNS 機能を使用する場合、問い合わせタイプが A（1）の DNS 問い合わせパケットを破棄するように指定にすると、正常な通信が行えなくなります。

● 設定条件

- ドメイン名　：＊
- 問い合わせタイプ　：SOA（6）
- 動作　：破棄する

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
DNS 問い合わせパケット破棄を設定する
# proxydns domain 0 6 * any reject

設定終了
# save
# commit
```

パソコン側の設定を行う

パソコン側の設定を行います。

設定方法は、「2.19.3 DNS サーバアドレスの自動取得機能を使う」（P.253）の「 パソコン側の設定を行う」（P.254）を参照してください。

2.19.6　DNS サーバ機能を使う

本装置のホストデータベースにホスト名と IP アドレスを登録します。登録したホストに対して DNS 要求があった場合は、ProxyDNS が DNS サーバの代わりに応答します。LAN 内の情報をホストデータベースにあらかじめ登録しておくと、LAN 内のホストの DNS 要求によって回線が接続されるといったトラブルを防止できます。

● 設定条件

- ホスト名　：host.com
- IPv4 アドレス　：192.168.1.2
- IPv6 アドレス　：2001:db8::2

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
ホストデータベース情報を設定する
# host 0 name host.com
# host 0 ip address 192.168.1.2
# host 0 ip6 address 2001:db8::2

設定終了
# save
# commit
```

補足　ホストデータベース情報は「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。

パソコン側の設定を行う

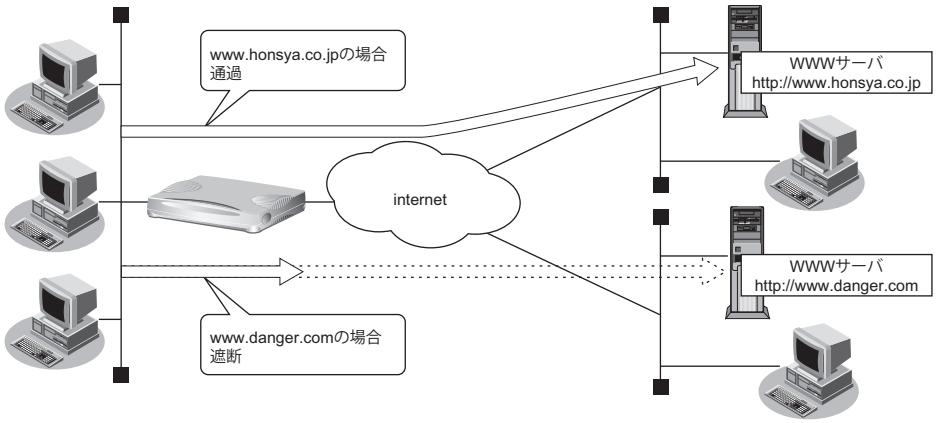
パソコン側の設定を行います。

設定方法は、「2.19.3 DNS サーバアドレスの自動取得機能を使う」(P.253) の「 パソコン側の設定を行う」(P.254) を参照してください。

2.20 特定のURLへのアクセスを禁止する（URLフィルタ機能）

URLフィルタ機能は、特定のURLへのアクセスを禁止することができます。本機能を使用する場合は、ProxyDNS情報で設定します。

以下にURLフィルタを行う場合の設定方法を説明します。



☛参照 マニュアル「機能説明書」

ここでは、会社のネットワークとプロバイダがすでに接続されていることを前提とします。また、ProxyDNS情報は何も設定されていないものとします。

● 設定条件

- アクセスを禁止するドメイン名　：www.danger.com

こんな事に気をつけて

- URLフィルタ機能を使用する場合は、LAN内のパソコンが本装置のIPアドレスをDNSサーバのIPアドレスとして登録する必要があります。
- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛参照 マニュアル「コマンドユーザーズガイド」

ヒント

◆「＊」は使えるの？

たとえば「www.danger.com」と「XXX.danger.com」の両方をURLフィルタの対象とする場合は「＊.danger.com」と指定することで両方を対象にできます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

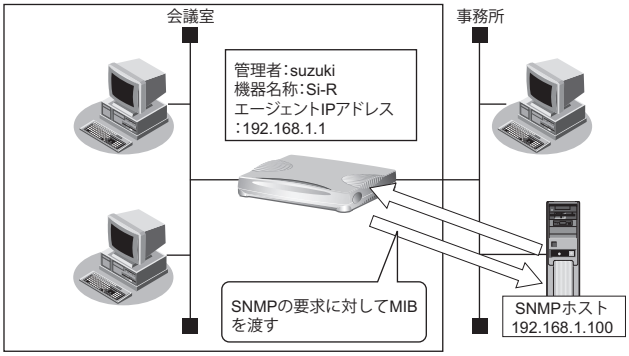
● コマンド

```
URL の情報を設定する
# proxydns domain 0 any www.danger.com any reject
# proxydns domain 1 any * any on 0

設定終了
# save
# commit
```

2.21 SNMP エージェント機能を使う

本装置は、SNMP（Simple Network Management Protocol）エージェント機能をサポートしています。

ここでは、本装置が SNMP ホストに対して MIB 情報を通知する場合の設定方法を説明します。



☛参照 マニュアル「機能説明書」

ヒント

◆ SNMP とは？

SNMP（Simple Network Management Protocol）は、ネットワーク管理用のプロトコルです。SNMP ホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMP エージェントは、SNMP ホストの要求に対して MIB（Management Information Base）という管理情報を返します。

また、特定の情報についてはトラップという機能を用いて、SNMP エージェントから SNMP ホストに対して非同期通知を行うことができます。

☛参照 マニュアル「仕様一覧」

こんな事に気をつけて

- エージェントアドレスには、本装置に設定されたどれかのインタフェースの IP アドレスを設定します。誤った IP アドレスを設定した場合は、SNMP ホストとの通信ができなくなります。
- 認証プロトコルとパスワード、暗号プロトコルとパスワードは、SNMP ホストの設定と同じにしてください。誤ったプロトコルとパスワードを設定した場合は、SNMP ホストとの通信ができなくなります。
- SNMPv3 で認証／暗号プロトコルを使用する場合、snmp 設定反映時の認証／暗号鍵生成に時間がかかります。このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。
- SNMPv3 で使用される snmpEngineBoots 値は、装置再起動時に初期化（初期値：1）されます。そのため、MIB 情報取得中に装置が再起動されると、SNMP ホストによっては継続した MIB 情報の取得ができないことがあります。

☛参照 マニュアル「コマンドリファレンス - 構成定義編」の「snmp service」

SNMPv1 または SNMPv2c でアクセスする場合の情報を設定する

SNMPv1 または SNMPv2c でアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMP エージェント機能を使用する
- 管理者　：suzuki
- 機器名称　：Si-R
- 機器設置場所　：1F（1 階）
- エージェントアドレス　：192.168.1.1（自装置 IP アドレス）
- SNMP ホストアドレス　：192.168.1.100
- コミュニティ名　：public00

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname Si-R
# snmp agent location 1F
# snmp agent address 192.168.1.1

SNMP ホスト情報を設定する
# snmp manager 0 192.168.1.100 public00 off disable

SNMP エージェント機能を使用する
# snmp service enable

設定終了
# save
# commit
```

SNMPv3 でアクセスする場合の情報を設定する

SNMPv3 でアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMP エージェント機能を使用する
- 管理者　：suzuki
- 機器名称　：Si-R
- 機器設置場所　：1F（1 階）
- エージェントアドレス　：192.168.1.1（自装置 IP アドレス）
- SNMP ホストアドレス　：192.168.1.100
- トラップ通知ホストアドレス　：192.168.1.100
- ユーザ名　：user00
- 認証プロトコル　：MD5
- 認証パスワード　：auth_password
- 暗号プロトコル　：DES
- 暗号パスワード　：priv_password
- MIB ビュー　：MIB 読み出しは system、interfaces グループのみ許可。
  トラップ通知は linkDown、linkUp トラップのみ許可。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

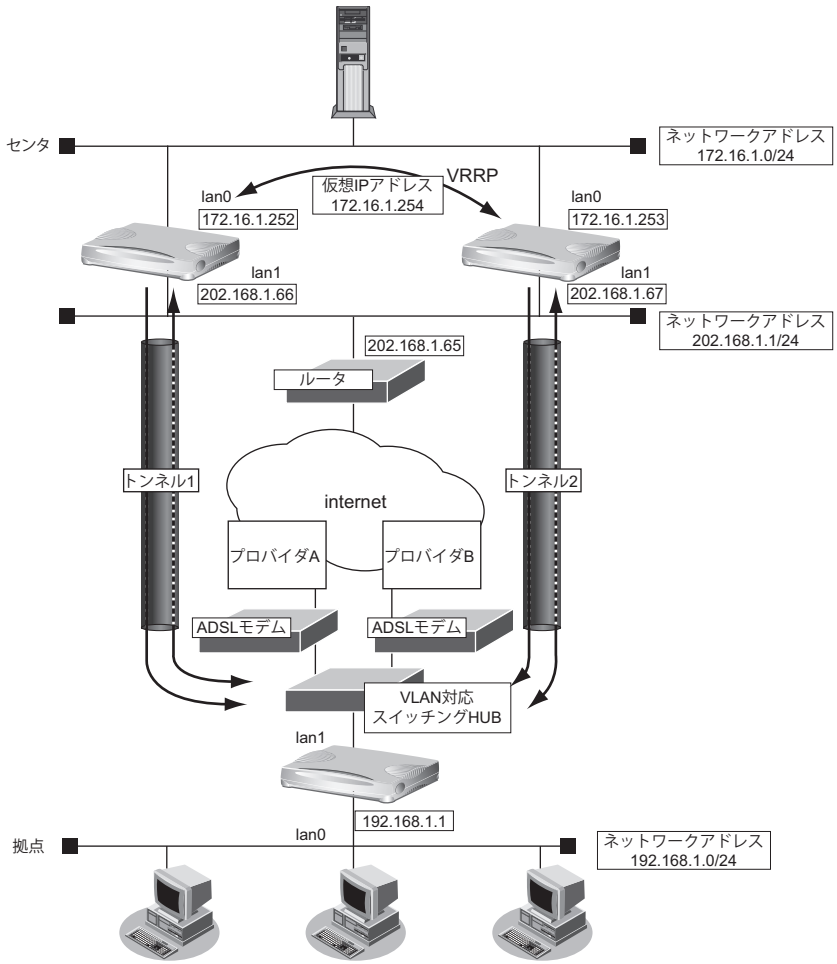
● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname Si-R
# snmp agent location 1F
# snmp agent address 192.168.1.1

SNMPv3 情報を設定する
# snmp user 0 name user00
# snmp user 0 address 0 192.168.1.100
# snmp user 0 notification 0 192.168.1.100

認証・暗号プロトコルを設定する
# snmp user 0 auth md5 auth_password
# snmp user 0 priv des priv_password

MIB ビュー情報を設定する
# snmp user 0 read view 0
# snmp user 0 notify view 0
# snmp view 0 subtree 0 include system
# snmp view 0 subtree 1 include interfaces
# snmp view 0 subtree 2 include linkdown
# snmp view 0 subtree 3 include linkup

SNMP エージェント機能を使用する
# snmp service enable

設定終了
# save
# commit
```

2.22 ECMP機能を使う

ここでは、ECMP機能を利用した負荷分散通信を行う場合の設定方法を説明します。

ADSLでは、受信速度は高速ですが、送信速度はそれほど高速ではありません。この例では、ADSLを２本利用して負荷を分散することで、送信速度の向上をはかります。さらに、片方のトンネルに障害が発生した場合に、通信可能なトンネルを利用して通信のバックアップを実現します。



参照 マニュアル「機能説明書」

● 設定条件

- 拠点では、センタへの通信は、トンネル１とトンネル２を利用して負荷分散して送信します。どちらかのトンネルで通信障害が発生した場合は、通信可能なトンネルだけを利用して送信します。
- センタでは、拠点への通信は、トンネル１だけを利用して送信します。トンネル１で通信障害が発生した場合は、トンネル２を利用して送信します。
- トンネル１の通信障害は、両端の本装置が接続先監視で検出します。
  この監視は、ISP Aの通信障害およびセンタ側本装置（左）の故障を検出します。
- トンネル２の通信障害は、両端の本装置が接続先監視で検出します。
  この監視は、ISP Bの通信障害およびセンタ側本装置（右）の故障を検出します。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[センタ側本装置（左）]

```
LAN ポートを削除する
# delete lan

LAN0 側を設定する
# lan 0 ip address 172.16.1.252/24 3
# lan 0 vrrp use on
# lan 0 vrrp group 0 id 10 254 172.16.1.254
# lan 0 vrrp group 0 trigger 0 ifdown rmt0

IPsec に関する ACL を設定する
# acl 0 ip 202.168.1.66/32 any 17 any
# acl 0 udp 500 500
# acl 1 ip 202.168.1.66/32 any 50 any

LAN1 側を設定する
# lan 1 ip address 202.168.1.66/24 3
# lan 1 ip route 0 default 202.168.1.65 1 0
# lan 1 ip filter 0 pass acl 0 reverse
# lan 1 ip filter 1 pass acl 1 reverse
# lan 1 ip filter default reject

トンネルを設定する
# remote 0 name RMTbyA
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ip msschange 1360
# remote 0 mtu 1400
# remote 0 ap 0 name IPsecbyA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs modp768
# remote 0 ap 0 ike name remote RMTbyA
# remote 0 ap 0 ike shared key text 12345678-A
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 sessionwatch address 172.16.1.252 192.168.1.1
# remote 0 ap 0 sessionwatch interval 5s 1m 5s

設定終了
# save
# commit
```

［センタ側本装置（右）］

```
LAN ポートを削除する
# delete lan

LAN0 側を設定する
# lan 0 ip address 172.16.1.253/24 3
# lan 0 vrrp use on
# lan 0 vrrp group 0 id 10 100 172.16.1.254
# lan 0 vrrp group 0 trigger 0 ifdown rmt0

IPsec に関する ACL を設定する
# acl 0 ip 202.168.1.67/32 any 17 any
# acl 0 udp 500 500
# acl 1 ip 202.168.1.67/32 any 50 any

LAN1 側を設定する
# lan 1 ip address 202.168.1.67/24 3
# lan 1 ip route 0 default 202.168.1.65 1 0
# lan 1 ip filter 0 pass acl 0 reverse
# lan 1 ip filter 1 pass acl 1 reverse
# lan 1 ip filter default reject

トンネルを設定する
# remote 0 name RMTbyB
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ip msschange 1360
# remote 0 mtu 1400
# remote 0 ap 0 name IPsecbyB
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.1.67
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs modp768
# remote 0 ap 0 ike name remote RMTbyB
# remote 0 ap 0 ike shared key text 12345678-B
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 sessionwatch address 172.16.1.253 192.168.1.1
# remote 0 ap 0 sessionwatch interval 5s 1m 5s

設定終了
# save
# commit
```

[拠点側本装置]

```
LAN ポートを削除する
# delete lan

LAN のアドレスを設定する
# lan 0 ip address 192.168.1.1/24 3

PPPoE で利用する LAN を設定する
# lan 1 mode auto
# lan 2 vlan bind 1
# lan 2 vlan tag vid 10
# lan 3 vlan bind 1
# lan 3 vlan tag vid 20

IPsec に関する ACL を設定する
# acl 0 ip any 202.168.1.66/32 17 any
# acl 0 udp 500 500
# acl 1 ip any 202.168.1.66/32 50 any
# acl 2 ip any 202.168.1.67/32 17 any
# acl 2 udp 500 500
# acl 3 ip any 202.168.1.67/32 50 any

プロバイダ A を利用する PPPoE 接続を設定する
# remote 0 name INTER-A
# remote 0 ip route 0 202.168.1.66/32 1 0
# remote 0 ip filter 0 pass acl 0 reverse
# remote 0 ip filter 1 pass acl 1 reverse
# remote 0 ip filter default reject
# remote 0 ip msschange 1414
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-A
# remote 0 ap 0 datalink bind lan 2
# remote 0 ap 0 ppp auth send UIDtoA PASStoA
# remote 0 ap 0 keep connect
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

プロバイダ B を利用する PPPoE 接続を設定する
# remote 1 name INTER-B
# remote 1 ip route 0 202.168.1.67/32 1 0
# remote 1 ip filter 0 pass acl 2 reverse
# remote 1 ip filter 1 pass acl 3 reverse
# remote 1 ip filter default reject
# remote 1 ip msschange 1414
# remote 1 mtu 1454
# remote 1 ap 0 name ISP-B
# remote 1 ap 0 datalink bind lan 3
# remote 1 ap 0 ppp auth send UIDtoB PASStoB
# remote 1 ap 0 keep connect
# remote 1 ip nat mode multi any 1 5m
# remote 1 ip nat static 0 192.168.1.1 500 any 500 17
# remote 1 ip nat static 1 192.168.1.1 any any any 50
```

センタ側本装置（左）とのトンネルを設定する
remote 2 name CENTER-A
remote 2 ip route 0 172.16.1.0/24 1 1
remote 2 ip msschange 1360
remote 2 mtu 1400
remote 2 ap 0 name IPsecbyA
remote 2 ap 0 datalink type ipsec
remote 2 ap 0 tunnel remote 202.168.1.66
remote 2 ap 0 ipsec type ike
remote 2 ap 0 ipsec ike protocol esp
remote 2 ap 0 ipsec ike range any4 any4
remote 2 ap 0 ipsec ike encrypt des-cbc
remote 2 ap 0 ipsec ike auth hmac-md5
remote 2 ap 0 ipsec ike pfs modp768
remote 2 ap 0 ike name local RMTbyA
remote 2 ap 0 ike shared key text 12345678-A
remote 2 ap 0 ike proposal 0 encrypt des-cbc
remote 2 ap 0 sessionwatch address 192.168.1.1 172.16.1.252
remote 2 ap 0 sessionwatch interval 5s 1m 5s

センタ側本装置（右）とのトンネルを設定する
remote 3 name CENTER-B
remote 3 ip route 0 172.16.1.0/24 1 1
remote 3 ip msschange 1360
remote 3 mtu 1400
remote 3 ap 0 name IPsecbyB
remote 3 ap 0 datalink type ipsec
remote 3 ap 0 tunnel remote 202.168.1.67
remote 3 ap 0 ipsec type ike
remote 3 ap 0 ipsec ike protocol esp
remote 3 ap 0 ipsec ike range any4 any4
remote 3 ap 0 ipsec ike encrypt des-cbc
remote 3 ap 0 ipsec ike auth hmac-md5
remote 3 ap 0 ipsec ike pfs modp768
remote 3 ap 0 ike name local RMTbyB
remote 3 ap 0 ike shared key text 12345678-B
remote 3 ap 0 ike proposal 0 encrypt des-cbc
remote 3 ap 0 sessionwatch address 192.168.1.1 172.16.1.253
remote 3 ap 0 sessionwatch interval 5s 1m 5s

ECMP を設定する
routemanage ip ecmp mode hash

設定終了
save
commit

2.23 VRRP機能を使う

VRRP機能は２つ以上のルータがグループを形成し、１台のルータ（仮想ルータ）のように動作します。グループ内の各ルータには優先度が設定されており、その優先度に従ってマスタルータ（実際に経路情報を処理する装置）とバックアップルータ（マスタルータで異常を検出したときに経路情報の処理を引き継ぐ装置）を決定します。

本装置には、以下のVRRP機能があります。

- 簡易ホットスタンバイ機能
  動的に経路制御（RIPなど）できない端末から、別のネットワークへの通信に使用しているルータがなんらかの理由で中継できなくなった場合、自動でほかのルータが通信をバックアップします。
- クラスタリング機能
  VRRPのグループを複数設定することで、通信の負荷分散と冗長構成を実現します。本装置では、２台のルータを組み合わせることで簡易ホットスタンバイによる信頼性の高い通信を実現できます。

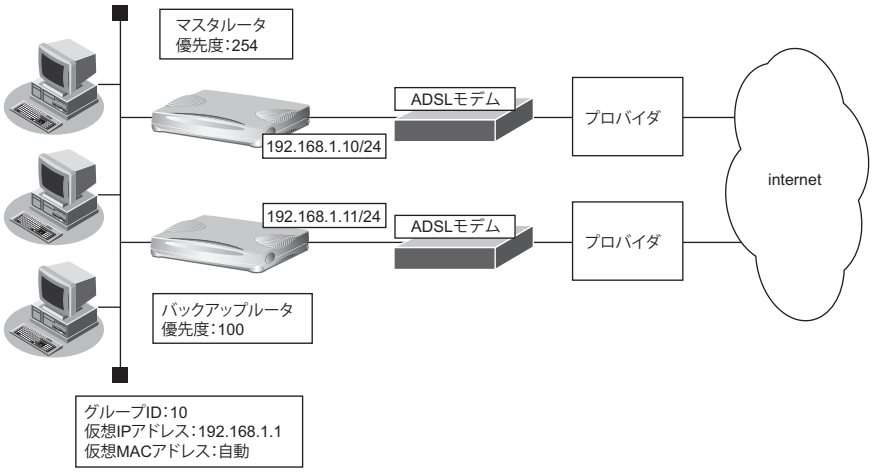
☛参照 マニュアル「機能説明書」

こんな事に気をつけて

- 本装置の電源の投入、マスタルータでの設定反映、または装置リセットを実行した場合、バックアップルータがマスタルータとなることがあります。プリエンプトモードがonの場合は自動で切り戻りますが、プリエンプトモードがoffの場合は、vrrp preempt-permitコマンドで切り戻しを行う必要があります。
- 優先度の値が大きい方が優先的にマスタルータとなります。
- LANに接続される装置はデフォルトルートとして仮想IPアドレスを設定してください。
- ルータに設定するIPアドレスと仮想IPアドレスには、異なるIPアドレスを設定することをお勧めします。同じIPアドレスを設定した場合、そのIPアドレスで装置にアクセスすることはできなくなります。同じにした場合、必ず、VRRPグループのVRRPルータの優先度を“master”に設定してください（VRRPルータの優先度として“master”を設定した場合、仮想IPアドレスは設定できません）。
- VRRP機能では、VRRP-ADメッセージに以下のパケットを使用します。IPフィルタ設定時には、このパケットを遮断しないように設定する必要があります。
  あて先IPアドレス　：224.0.0.18
  プロトコル番号　　：112

2.23.1　簡易ホットスタンバイ機能を使う

本装置では、2台のルータを組み合わせることで簡易ホットスタンバイ機能による信頼性の高い通信を実現できます。2台のルータをPPPoEでインターネットに接続して、ホットスタンバイを構成する場合の設定方法を説明します。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータはPPPoE側経路をノードダウントリガによって監視する

[マスタルータ]

- PPPoEで使用するLANポート　：LAN0ポート
- 本装置のIPアドレス／ネットマスク　：192.168.1.10/24
- ユーザ認証ID　：userid
- ユーザ認証パスワード　：userpass
- ノードダウントリガの監視IPアドレス　：202.168.2.1（プロバイダ側のDNSサーバアドレスなど）

[バックアップルータ]

- PPPoEで使用するLANポート　：LAN0ポート
- 本装置のIPアドレス／ネットマスク　：192.168.1.11/24
- ユーザ認証ID　：userid2
- ユーザ認証パスワード　：userpass2

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[マスタルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 ip address 0.0.0.0/0 3
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.10/24 3

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass

VRRP を設定する（ノードダウントリガを使用する）
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 node 202.168.2.1 any

設定終了
# save

再起動
# reset
```

[バックアップルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 ip address 0.0.0.0/0 3
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.11/24 3

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1
# lan 1 vrrp group 0 preempt on

設定終了
# save

再起動
# reset
```

上の設定例で、インタフェースダウントリガを使用して PPPoE インタフェース状態を監視する場合は、以下の設定を追加します。

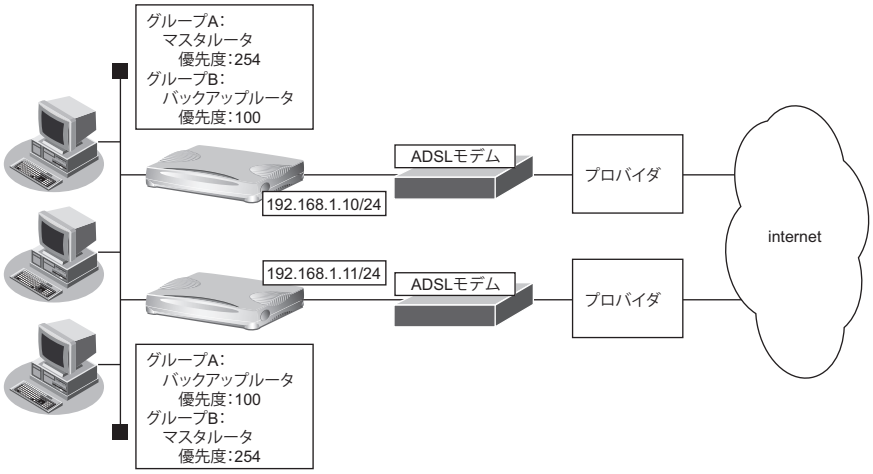
● コマンド

[マスタルータの設定]

```
# lan 1 vrrp group 0 trigger 0 ifdown rmt0
```

2.23.2　クラスタリング機能を使う

本装置では、2台のルータに複数のグループ ID を設定することで、信頼性を高めると同時に通信の負荷分散を実現できます。2台のルータを PPPoE でインターネットに接続する場合の設定方法を説明します。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータは PPPoE 側のインタフェースをインタフェースダウントリガにより監視する

[グループ A]

- グループ ID　：10
- 仮想 IP アドレス　：192.168.1.1

[グループ B]

- グループ ID　：11
- 仮想 IP アドレス　：192.168.1.2

[マスタルータ]

- PPPoE で使用する LAN ポート　：LAN0 ポート
- 本装置の IP アドレス／ネットマスク　：192.168.1.10/24
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass

[バックアップルータ]

- PPPoE で使用する LAN ポート　：LAN0 ポート
- 本装置の IP アドレス／ネットマスク　：192.168.1.11/24
- ユーザ認証 ID　：userid2
- ユーザ認証パスワード　：userpass2

こんな事に気をつけて

クラスタリング機能を有効に利用するには、PC からのトラフィック量に応じて、PC 側で設定するデフォルトルートの定義を適切に分散する必要があります。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[マスタルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 ip address 0.0.0.0/0 3
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.10/24 3

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass

VRRP を設定する（インタフェースダウントリガを使用する）
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 ifdown rmt0 254
# lan 1 vrrp group 1 id 11 100 192.168.1.2

設定終了
# save

再起動
# reset
```

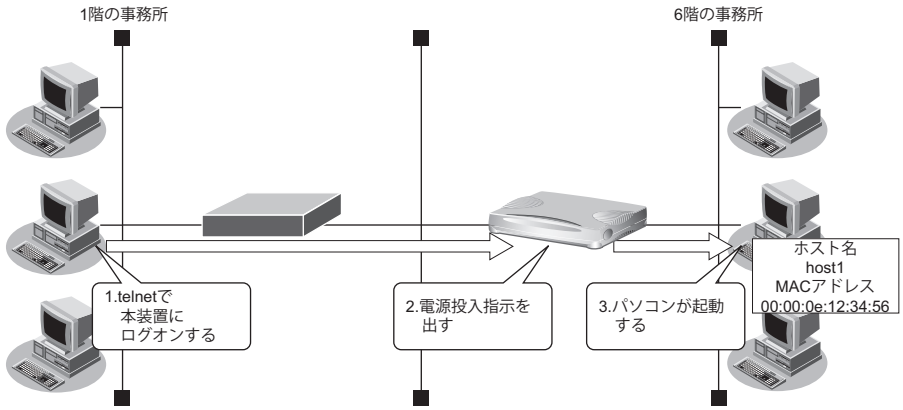
[バックアップルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 ip address 0.0.0.0/0 3
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.11/24 3

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1
# lan 1 vrrp group 1 id 11 254 192.168.1.2
# lan 1 vrrp group 1 preempt off
# lan 1 vrrp group 1 trigger 0 ifdown rmt0 254

設定終了
# save

再起動
# reset
```

2.24 遠隔地のパソコンを起動させる（リモートパワーオン機能）

リモートパワーオン機能は、本装置につながっている離れた所にあるパソコンを、本装置からWakeup on LAN機能を使用して起動させることができます。

ここでは、１階の事務所のパソコンから６階の事務所のパソコンを起動する場合の設定方法を説明します。



● 設定条件

[本社側]

- 起動するパソコンのホスト名　：host1
- 起動するパソコンのMACアドレス　：00:00:0e:12:34:56

ヒント

◆ Wakeup on LAN機能とは？

AMD社が開発したネットワーク上の電源OFF状態のパソコンを遠隔操作で起動する機能です。起動はMagic Packetと呼ばれるパケットを送付して行います。なお、Wakeup on LAN機能はパソコンを起動するだけで電源OFFは行いません。

電源OFFする場合は、別途、電源制御用ソフトウェアが必要になります。

こんな事に気をつけて

- 本機能は、Wakeup on LANに対応したパソコンだけで利用できます。Wakeup on LAN対応機種については、パソコンのメーカーにお問い合わせください。
- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「”」、「<」、「>」、「&」、「%」は入力しないでください。

☛参照 マニュアル「コマンドユーザーズガイド」

補足 ホストデータベース情報は「リモートパワーオン機能」、「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だけを設定します。

2.24.1　リモートパワーオン情報を設定する

● 設定コマンド

```
ホストデータベースへ登録する
# host 0 name host1
# host 0 mac 00:00:0e:12:34:56

設定終了
# save
# commit
```

2.24.2　リモートパワーオン機能を使う

1. パソコン上のtelnetクライアントから本装置にログオンします。

2. 本装置からコマンドによって、Wakeup on LAN機能を使用します。

● コマンド

```
# rpon all
```

補足 パソコンがMagic Packetを受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種やOSによって異なります）。

2.25 スケジュール機能を使う

本装置のスケジュール機能には、以下のとおりです。

- スケジュール予約
  特定の動作とそれを行う時間をスケジュール予約情報として登録できます。スケジュール予約情報を登録しておくと、定期的に特定のパソコンを起動させる作業を本装置が自動的に行います。
  スケジュール予約情報は、最大16件まで登録できます。
- 構成定義情報切り替え予約
  本装置は、内部に２つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情報を用意し、指定した日時に新しい構成定義に切り替えることができます。

こんな事に気をつけて

設定前に本装置の内部時刻を正しくセットしてください。

☛参照 マニュアル「コマンドユーザーズガイド」

2.25.1 スケジュールを予約する

リモートパワーオンを予約する

ここでは、毎朝8時に特定のパソコンを起動する場合の設定方法を説明します。

こんな事に気をつけて

リモートパワーオン機能を利用する場合は、あらかじめ対象とするパソコンの情報を本装置のホストデータベース情報に登録しておく必要があります。スケジュール機能を使ってリモートパワーオンを行うと、host rponコマンドでoffが指定されていないすべてのパソコンが起動します。

☛参照 「2.24 遠隔地のパソコンを起動させる（リモートパワーオン機能）」（P.276）

● 設定条件

- 動作　：リモートパワーオン
- 予約時刻　：08:00
  ：毎日

上記の設定条件に従ってリモートパワーオンを予約する場合のコマンド例を示します。

● コマンド

```
スケジュールを予約する
# schedule 0 at any 0800 rpon all

設定終了
# save
# commit
```

2.25.2　構成定義情報の切り替えを予約する

本装置は、構成定義情報を内部に２つ持つことができます。

ここでは、2009年1月1日6時30分に構成定義情報を１から２に切り替える場合の設定方法を説明します。

● 設定条件

- 実行日時　：2009年1月1日　6時30分
- 構成定義情報切り替え　：構成定義情報１→構成定義情報２

上記の設定条件に従って構成定義情報を切り替える場合のコマンド例を示します。

● コマンド

```
構成定義を切り替える
# addact 0 0901010630 reset config2

設定終了
# save
# commit
```

2.26 ブリッジ／STP 機能を使う

ここでは、ブリッジで FNA をつないで STP 機能を使用する場合、および IP トンネルでブリッジ通信を行う場合の設定方法を説明します。

こんな事に気をつけて

- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「”」、「<」、「>」、「&」、「%」は入力しないでください。

  ☛参照 マニュアル「コマンドユーザーズガイド」

- STP 機能は、グループ 0 でだけ動作します。VLAN インタフェースでは、STP を使用できません。
- WAN インタフェースでブリッジを利用する場合は、1 つの相手情報（remote）に対して、1 つの接続先情報（ap）となるように設計してください。
- 本装置では、ファームウェアの更新や SNMP での監視などの目的で IPv4 の IP アドレスを使用します。そのため、IPv4 の IP アドレスを設定しないで運用することはできません。IPv6 およびブリッジだけを使用しているネットワークで運用する場合でも、どれかの LAN インタフェースに必ず IPv4 の IP アドレスを設定してください。
- VLAN でバインドされたインタフェースでブリッジを行うことはできません。
- 本装置のブリッジ MAC 学習は、異なる VLAN 上で同一の MAC アドレスを学習することはできません。本装置は、唯一装置が持つ学習テーブルを各 VLAN が共有する SVL（Shared VLAN Learning）と呼ばれる方式で学習を行っています。VLAN インタフェースでブリッジを行う場合は、異なる VLAN 上に同一の MAC アドレスを持つネットワークと接続しないでください。
- 設定を間違えてループ構成を構成し、ブロードキャストストームが発生してコンソールなどが反応しなくなった場合は、ブリッジが有効な LAN のケーブルを抜くとブロードキャストストームが収まります。ブロードキャストストームが収まったところで設定を修正してください。

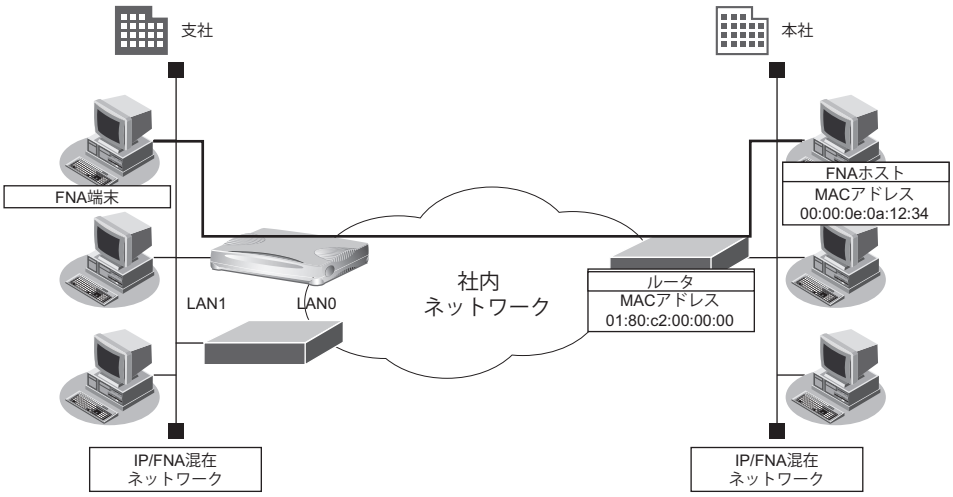
2.26.1 ブリッジで FNA をつないで STP 機能を使う

ブリッジ機能を使用すると、離れた LAN どうしを 1 つのサブネットワークとして使用することができます。また、STP 機能を使用すると、物理的にループしているネットワークでも、論理的にループしないようにすることができます。これによって、ネットワーク内のデータを円滑に流すことができます。

☛参照 マニュアル「機能説明書」

LAN接続の場合

ここでは、離れたLAN（FNA）をブリッジでつなぐ場合を例に説明します。



● 設定条件

- 本社へFNAのデータだけをブリッジする
- STP機能を使用する

こんな事に気をつけて

ブリッジ機能によりネットワークを接続する場合は、ブリッジ通信をするパケット以外をフィルタリングする設定にしてください。フィルタリングしないと不要なトラフィックが発生するだけでなく、IP通信できなくなる場合があります。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ブリッジ情報を設定する
# lan 0 bridge use on
# lan 0 bridge stp use on
# lan 1 bridge use on
# lan 1 bridge stp use on

フィルタリング情報でFNAを透過させる
# acl 0 mac any 00:00:0e:0a:12:34 llc 8080
# lan 0 bridge filter 0 pass acl 0 reverse

フィルタリング情報でSTPを透過させる
# acl 1 mac any 01:80:c2:00:00:00 llc 4242
# lan 0 bridge filter 1 pass acl 1 reverse

残りの通信をすべて遮断する
# acl 2 mac any any any
# lan 0 bridge filter 2 reject acl 2 any

設定終了
# save
# commit
```

2.26.2 IP トンネルで事業所間をブリッジ接続する（Ethernet over IP ブリッジ）

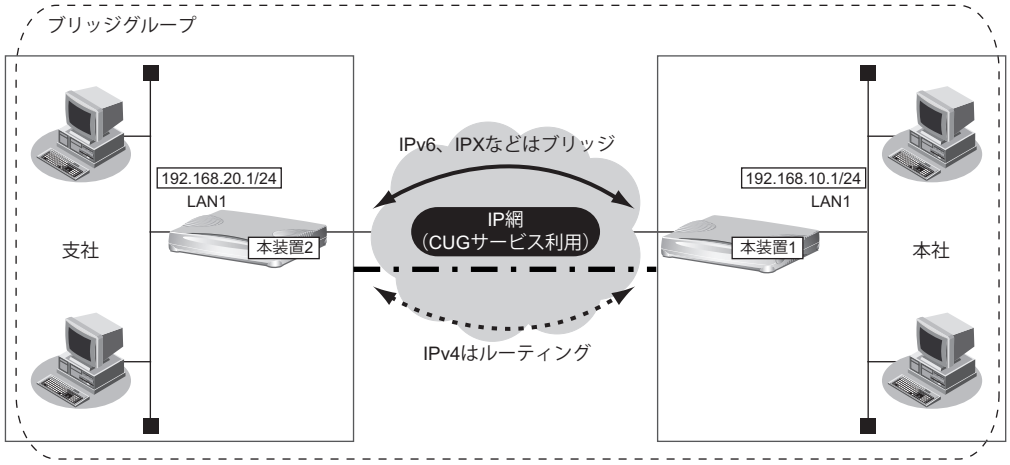
IP トンネル上でブリッジ機能を使用することにより、IP 通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。

こんな事に気をつけて

- ブリッジ学習テーブル生存時間は、グループ 0 に設定した値がすべてのグループで使用されます。
- VLAN インタフェースをブリッジグループに含める場合は、1 つまたは複数のリモートインタフェースと VLAN インタフェースでだけグルーピングできます。
- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数の LAN インタフェースを同じグループに含めて IP ブリッジをする場合は、同じグループ内で定義番号がもっとも小さい LAN インタフェースでだけ以下の機能を利用できます。
  - FTP（ファームアップデートなど）
  - telnet
  - WWW ブラウザによる設定
  - syslog の送信
  - SNMP エージェント、Trap 送信
  - ダイナミックルーティング

  IP フレームをブリッジする場合に、転送ポリシを loose に設定したときだけ、ブリッジグループ外とブリッジ転送が行われます。また、ブリッジドメイン内は唯一の IP セグメントであることに注意してダイナミックルーティングを使用してください。
- STP はグループ 0 でだけ動作するため、グループ 0 以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ 0 でループを構成するブリッジ構成を行う場合は、必ず STP を有効にしてください。
- IP をブリッジする場合、WAN 側にはブリッジで中継されるフレームだけが転送され、直接 WAN 側に Ethernet フレームではない IP パケットを送受信することはできません。よって、IP をブリッジする運用形態では、IP に関するすべての設定は LAN インタフェース側で定義します。リモートインタフェースでは、IP に関する設定は定義しないでください。
- WAN 経由で IP をブリッジし、ブリッジ転送を許す場合（転送ポリシが Loose）、たとえ WAN の先に存在するネットワークに対する経路であっても、すべての静的経路の設定は LAN インタフェース側で定義してください。ブリッジによって相手装置の LAN と本装置の LAN が WAN 経由で接続されているため、LAN 側に経路設定を定義すれば、問題なく WAN の先に存在するあて先ネットワークにブリッジで転送されて到達します。
- Ethernet over IP ブリッジの接続先に対して接続先監視を行うことができません。接続先監視の設定は行わないでください。

ここでは、本社と特定の支社との間で、IP 網を経由し、IPv4 以外のフレームに対してブリッジ通信を行う場合の設定方法を説明します。



● 前提条件

- IP 網は、PPPoE 接続で LAN 型払い出しによりアドレス割り当てを行う CUG（Closed Users Group）サービスを利用する

[本社（PPPoE 常時接続）]

- 払い出される IPv4 アドレス（LAN1 ポートに設定）
  ：192.168.10.1/24
- PPPoE ユーザ認証 ID　：userid1@groupname
- PPPoE ユーザ認証パスワード　：userpass1
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

[支社（PPPoE 常時接続）]

- 払い出される IPv4 アドレス（LAN1 ポートに設定）
  ：192.168.20.1/24
- PPPoE ユーザ認証 ID　：userid2@groupname
- PPPoE ユーザ認証パスワード　：userpass2
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

● 設定条件

[本社]

- 自側エンドポイントアドレス　：192.168.10.1
- 相手側エンドポイントアドレス　：192.168.20.1

[支社]

- 自側エンドポイントアドレス　：192.168.20.1
- 相手側エンドポイントアドレス　：192.168.10.1

[本社、支社共通]

- ブリッジ対象インタフェース　：LAN1 ポートと IP トンネル
- IPv4 の転送方式　：ルーティングで転送
- IPv6 の転送方式　：ブリッジで転送

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置 1（本社側）]

```
# delete lan

CUG サービスに接続する PPPoE の接続情報を設定する
# lan 0 mode auto
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1@groupname userpass1
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
```

```
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414

LAN1 の IP アドレスを設定する
# lan 1 ip address 192.168.10.1/24 3

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.10.1
# remote 1 ap 0 tunnel remote 192.168.20.1

ブリッジを行うインタフェースを設定する
# remote 1 bridge use on
# lan 1 bridge use on

ブリッジグループを設定する
# bridge 0 ip routing on
# bridge 0 ip6 routing off

設定終了
# save
# commit
```

[本装置 2（支社側）]

```
# delete lan

CUG サービスに接続する PPPoE の接続情報を設定する
# lan 0 mode auto
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user2
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2@groupname userpass2
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414

LAN1 の IP アドレスを設定する
# lan 1 ip address 192.168.20.1/24 3

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.20.1
# remote 1 ap 0 tunnel remote 192.168.10.1

ブリッジを行うインタフェースを設定する
# remote 1 bridge use on
# lan 1 bridge use on

ブリッジグループを設定する
# bridge 0 ip routing on
# bridge 0 ip6 routing off

設定終了
# save
# commit
```

2.27 スイッチポートを使う

本装置は、ご購入時の状態や未設定の状態ではスイッチング HUB として動作します。
Si-R80brin では LAN1 側のポートをスイッチング HUB として使用するか、従来の単独ポートとして使用するかを構成定義により選択できます。

本装置のスイッチポートでは以下のような形態が利用できます。

- スイッチポートを HUB として使用する

☛ 参照 「2.27.1 スイッチポートを HUB として使用する」（P.286）

- スイッチポートを単独ポートとして使用する（Si-R80brin）

☛ 参照 「2.27.2 スイッチポートを単独ポートとして使用する（Si-R80brin）」（P.288）

こんな事に気をつけて

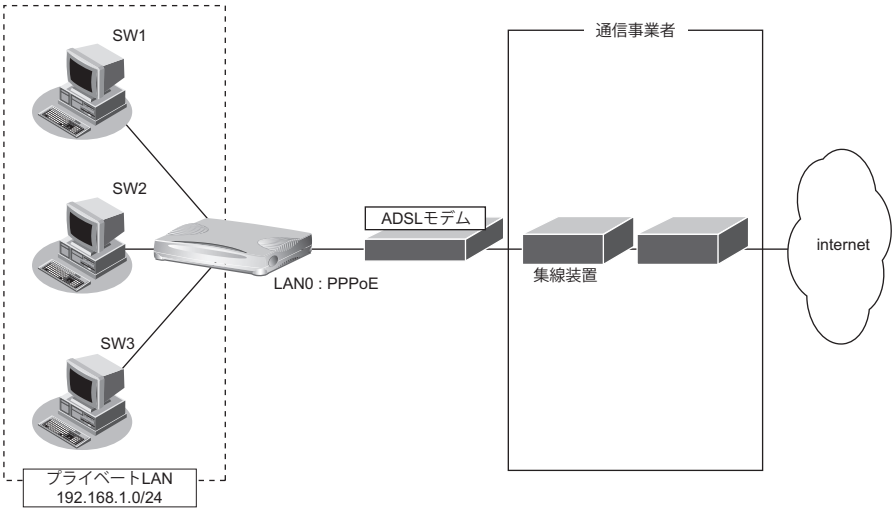
- 本装置のスイッチポートの MTU は 1532 バイトです。トンネルプロトコルを利用する場合は MTU をスイッチポートの MTU サイズ以下になるように設定するか、スイッチポートを無効にし、使用するパケットの最大長の転送が可能な外付けのスイッチを使用してください。
- スイッチポートを HUB として使用した場合、VLAN ヘッダに依存しないで、MAC アドレスのみでスイッチポート間の転送を行います（VLAN ヘッダごと転送）。
  スイッチポートで VLAN ヘッダに応じた転送を行う場合は、LAN1 ポートに対して VLAN の定義を行ってください。その際、VLAN を使用した場合と同じ注意事項が適用されますので、スイッチポートを使用する前に必ず「VLAN 機能」に関する記述を確認してください。

☛ 参照 「2.7 VLAN 機能を使う」（P.96）

2.27.1　スイッチポートを HUB として使用する

接続するスイッチポートを HUB としてインターネットに接続する場合の設定方法を説明します。

☛ 参照 「1.5 インターネットへ PPPoE で接続する」（P.18）



● 設定条件

[通信事業者側]

- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- LAN0 ポートを使用する

[プライベート LAN 側]

- LAN1 側をスイッチポートとして使用する
- ローカルネットワークでは VLAN は使用しない
- ローカルネットワークでは DHCP サーバを使用し、パソコンに割り当てるアドレスは 192.168.1.2 から 64 個用意する
- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ADSLモデムに接続するインタフェースを設定する
# delete lan 0
# lan 0 mode auto

本装置のIPアドレスを設定する
# lan 1 ip address 192.168.1.1/24 3

DHCPサーバを設定する
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 64
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip dhcp service server
# lan 1 ip nat mode off

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 autodial enable
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1
# remote 0 ip rip use off off 0 off
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass

ProxyDNSを設定する
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0

設定終了
# save

再起動
# reset
```

上の設定例で、LAN1側を単独ポートとして使用していた場合は、以下の設定を追加します（Si-R90brinでは設定は不要です）。

● コマンド

```
# switch use on
```

2.27.2　スイッチポートを単独ポートとして使用する（Si-R80brin）

トンネルプロトコル利用時やブリッジでのSTP機能利用時など、スイッチポートを無効にして単独ポートとして使用する場合の設定方法を説明します。

● 設定条件

- スイッチポートを無効にし、単独ポートとして使用する。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
スイッチポートを無効にする
# switch 0 use off

設定終了
# save
# reset
```

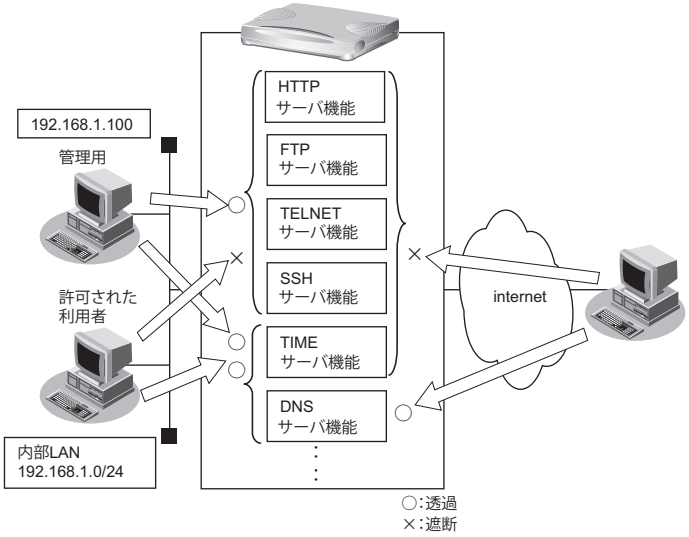
こんな事に気をつけて

switch use コマンド未設定時は、スイッチングHUBとして動作します。
そのため delete コマンドでスイッチ情報を削除した場合は、スイッチポートは無効にはなりません。
スイッチポートを無効にする場合は、本手順を実施してください。

2.28 アプリケーションフィルタ機能を使う

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。

これにより、装置をメンテナンスまたは装置のサーバ機能を使用する端末を限定し、セキュリティを向上させることができます。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明します。

● 設定条件

- 管理用のホスト（192.168.1.100）からのみHTTP/TELNET/FTP/SSHサーバ機能へのアクセスを許可する。
- 内部LANのホスト（192.168.1.0/24）からのみTIMEサーバ機能へのアクセスを許可する。
- その他のサーバ機能は制限しない。

こんな事に気をつけて

IPフィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行っていてもアクセスはできません。

上記の設定条件に従ってアプリケーションフィルタを設定する場合のコマンド例を示します。

● コマンド

```
制限するサーバ機能に対し、デフォルトのアクセスを遮断する
# serverinfo http filter default reject
# serverinfo ftp filter default reject
# serverinfo telnet filter default reject
# serverinfo ssh filter default reject
# serverinfo time filter default reject

管理用のホストからのFTP/TELNET/SSHサーバ機能へのアクセスを許可する
# acl 0 ip 192.168.1.100/32 any any any
# serverinfo http filter 0 accept acl 0
# serverinfo ftp filter 0 accept acl 0
# serverinfo telnet filter 0 accept acl 0
# serverinfo ssh filter 0 accept acl 0

内部LANのホストからのTIMEサーバ機能へのアクセスを許可する
# acl 1 ip 192.168.1.0/24 any any any
# serverinfo time filter 0 accept acl 1

設定終了
# save
# commit
```

2.29 不正端末アクセス防止機能（MACアドレス認証）を使う

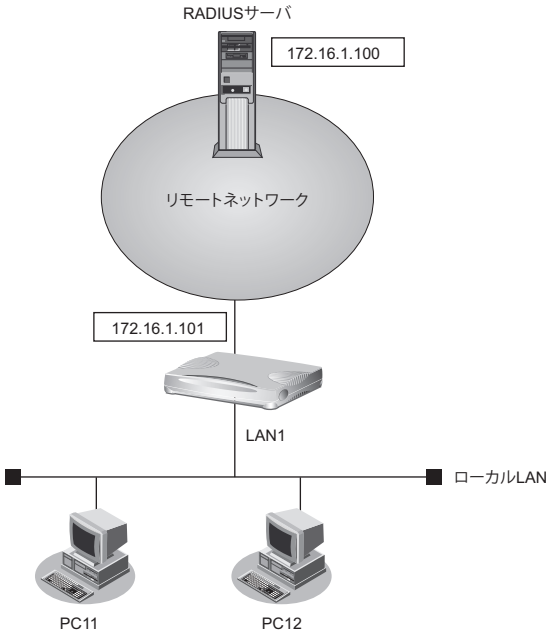
不正端末アクセス防止機能（MACアドレス認証）を使用すると、本装置のローカルLANに接続する端末がリモートネットワークへのアクセス権限を持っているかを認証することができます。

ここでは、リモートネットワークへの接続がすでに設定されている場合を例にMACアドレス認証機能を利用する設定方法を説明します。

こんな事に気をつけて

MACアドレス認証で利用するAAAのグループIDを正しく設定してください。

外部の RADIUS サーバによるリモート認証の場合



● 設定条件

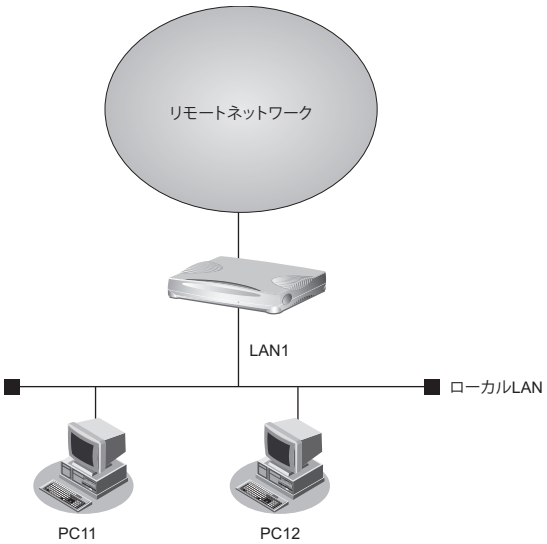
- LAN1ポートでMACアドレス認証を使用する
- LAN1ポートで利用する認証データベース　：RADIUSサーバ
- AAAグループID　：0
- リモートネットワークへの接続定義は設定済み
- RADIUSサーバはリモートネットワークに接続
- RADIUSサーバのIPアドレス　：172.16.1.100
- RADIUSサーバのシークレット　：radius-secret

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
MACアドレス認証で使用するパスワードを設定する
# macauth password macauth-pass

MACアドレス認証を使用する
# lan 1 macauth use on
# lan 1 macauth aaa 0

RADIUSサーバを利用するAAAグループ情報を設定する
# aaa 0 name radiusAuth
# aaa 0 radius service client auth
# aaa 0 radius auth source 172.16.1.101
# aaa 0 radius client server-info auth secret radius-secret
# aaa 0 radius client server-info auth address 172.16.1.100

設定終了
# save
# commit
```

自装置内の AAA 機能を用いたローカル認証の場合



● 設定条件

- LAN1 ポートで MAC アドレス認証を使用する
- LAN1 ポートで利用する認証データベース　：ローカルで設定した認証情報
- AAA グループ ID　：0
- ローカル LAN で利用可能なユーザは以下のとおり

ユーザ	MAC アドレス
PC11	00:11:11:00:00:01
PC12	00:22:22:00:00:02

- リモートネットワークへの接続定義は設定済み

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
MACアドレス認証で使用するパスワードを設定する
# macauth password macauth-pass

MACアドレス認証を使用する
# lan 1 macauth use on
# lan 1 macauth aaa 0

ローカル認証情報を利用するAAAグループ情報を設定する
# aaa 0 name localAuth
# aaa 0 user 0 id 001111000001
# aaa 0 user 0 password macauth-pass
# aaa 0 user 1 id 002222000002
# aaa 0 user 1 password macauth-pass

設定終了
# save
# commit
```

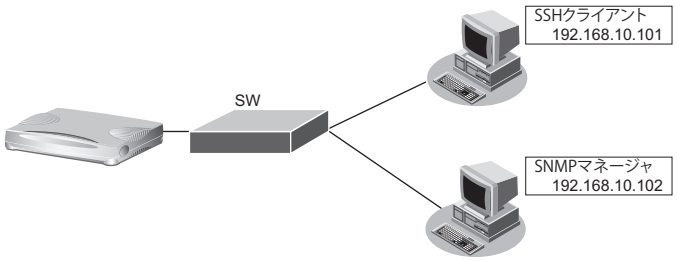
2.30 装置を保護する

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者(admin)用パスワードの設定
- オートログアウトの設定
- Telnet/SSHおよびSNMP接続に対するアクセス制限
- 不要なサービスの停止

2.30.1 設定例

以下にそれぞれの設定を行う場合の例を示します。



● 設定条件

- 管理者(admin) パスワード　：sir_admin-2022
- IPアドレス　：192.168.10.100/24
- オートログアウトの設定（ログインしたままの状態で指定時間無操作だった際に自動切断を行う）
  コンソールのオートログアウト時間　：5分
  SSHのオートログアウト時間　：5分
  ※SSH のオートログアウト時間は ”telnetinfo autologout” と共通
- SNMP設定
  アクセス許可するSNMPマネージャ　：192.168.10.102
  コミュニティ名　：private
  マネージャからの書き込み　：許可しない
- SSH接続を許可するホストのIPアドレス　：192.168.10.101
- Telnet接続　：禁止
- 不要なサーバ機能はすべて停止
  ＃ serverinfo <サーバ機能名> ip off
- IPv6アドレスをSi-Rに付与した際には、IPv6に関する不要なサーバ機能はすべて停止
  ＃ serverinfo <サーバ機能名> ip6 off

```
adminパスワードをsir_admin-2022に設定
# password admin set sir_admin-2022

コンソール接続のオートログアウト時間を5分に設定
# consoleinfo autologout 5m

Telnet/SSHのオートログアウトまでの無操作時間を5分に設定
# telnetinfo autologout 5m
```

```
自装置IPアドレスの設定
# lan 0 ip address 192.168.10.100/24 3

SNMPを有効、コミュニティ名をprivate、書き込み許可しない
# snmp service enable
# snmp manager 0 192.168.10.102 private v1 disable

許可するホストからのSSH接続のみ許可する
# acl 0 ip 192.168.10.101/32 any any any
# serverinfo ssh filter 0 accept acl 0
# serverinfo ssh filter default reject

Telnetサーバ機能を停止
# serverinfo telnet ip off

不要なサーバ機能はすべて停止
# serverinfo ftp ip off
# serverinfo sftp ip off
# serverinfo http ip off
# serverinfo dns ip off
# serverinfo sntp ip off
# serverinfo time ip tcp off
# serverinfo time ip udp off

設定終了
# save
# commit
```

索引

A

AAA 認証 125, 158
ADSL モデム 20
arp エントリ 97
AS 外部経路 75
AS 境界ルータ 75

B

BGP4 20
BGP 経路の制御（IPv4） 78
BSR（ブートストラップルータ） 87

C

CATV インターネット接続 13
CUG（Closed Users Group） 283

D

DHCP 機能 237
DHCP クライアント機能 242
DHCP サーバ機能 238
DHCP スタティック機能 240
DHCP リレーエージェント機能 243
DH グループ 27, 32
DNS サーバ 104
DNS サーバアドレスの自動取得機能 253
DNS サーバ機能 258
DNS サーバの自動切り替え機能（逆引き） 252
DNS サーバの自動切り替え機能（順引き） 250
DNS 問い合わせタイプフィルタ機能 257

E

ECMP 機能 264
Ethernet over IP ブリッジ 282
Ethernet フレーム 97

F

FNA 280

I

ID タイプ 37
IKE 27, 32
IKE セッション監視機能 157
IPsec 機能 124
IPsec クライアント 224
IPsec サーバ 224
IPv4 トンネル 40
IPv6 40
IPv6 DHCP クライアント機能 244, 248
IPv6 DHCP サーバ機能 246
IPv6 over IPv4 トンネル 43
IPv6 ネットワークの追加 17
IPv6 フィルタリング 114
IP-VPN 接続 20
IP アドレス 47, 99, 235
IP アドレスの自動割り当て 238
IP トンネル 282
IP フィルタリング機能 98, 153
IP フィルタリングの条件 98
IP フィルタリングの設計方針 101

L

LAN のネットワーク間接続 15
LSA 74

M

MAC アドレス認証 291
MAC アドレス 240
MED メトリック値 81
MIB 261
MSS 書き換え機能 155
MTU サイズ 97
MTU 分割機能 156

N

NAT 43
NAT トラバーサル機能 224
NetBIOS サーバ 120

O

OSPFv2（IPv4） 63
OSPF 経路の制御（IPv4） 74

P

PIM-DM 83
PIM-SM 87
PING 121
PPPoE 接続 18
ProxyDNS 250

R

RADIUS 認証 125, 167
RFC1877 253

RIP 経路の制御（IPv4）.....47
RIP 経路の制御（IPv6）.....55
RP（ランデブーポイント）.....87

S

SNMP 261
SNMP エージェント機能 261
SNTP 16
SPI 110, 131
SPT（最短経路）.....87
STP 280

T

TCP 接続要求 98, 99, 101
TIME プロトコル 16
TOS 229, 235
TOS/Traffic Class 231
TOS/Traffic Class 値書き換え機能 229
TOS 値 98
TOS 値書き換え機能 153
Traffic Class 値 229, 235

U

URL フィルタ機能 259

V

VLAN ID 96
VLAN インタフェース 97
VLAN 機能 96
VLAN パケット 231
VLAN プライオリティマッピング機能 231
VoIP NAT トラバーサル機能 227
VPN 124, 127
VRRP 機能 269

W

Wakeup on LAN 機能 276
WFQ 機能 235

あ

あて先情報 98, 229
あて先変換 219
アドレス変換機能 219
アドレスマスク 47, 99
アプリケーションフィルタ機能 289
暗号情報 124

え

エリア ID 63
エリア境界ルータ 74

か

可変 IP アドレス 34
簡易ホットスタンバイ機能 269, 270

き

基本 NAT 219
逆引き 252

く

クラスタリング機能 269, 273
グループ ID 273

け

ケーブルモデム 13
ケーブルモデム接続 13

こ

構成定義情報切り替え予約 278, 279
固定 IP アドレス 24, 29, 129
コネクション確立要求 99

さ

サーバの公開（PPPoE 接続）.....221
サーバの公開（プライベート LAN 接続） 220, 223

し

シェーピング機能 155, 232
システムログ 217
システムログの確認 218
自動鍵交換 24, 29, 124, 127
手動鍵交換 124, 129
準スタブエリア 71
順引き 250
冗長化ネットワーク 80
冗長構成の通信経路 81
新 TOS 229

す

スイッチポート 285
スイッチング HUB 96, 285
スケジュール機能 278
スケジュール予約 278

スタティックルーティング 93
スタブエリア 71

せ

制御 98
静的 NAT 219
セキュリティ 98
接続先監視機能 156

そ

送信元情報 98, 229

た

帯域制御機能 155, 235
ダイヤルアップ接続 13

ち

超過課金 98

つ

通信の負荷分散 81

て

テンプレート着信機能 158

と

動画・音声 83
動的 NAT 219
動的 VPN 125, 177, 186, 189
動的経路（RIP）機能 157
ドメイン 250
トラフィックの制御 78
トランジット 79
トンネリング 40

に

認証情報 124

は

バックアップルータ 269
バックボーンエリア 63, 74

ふ

フィルタリング条件（ルーティング）.....47
フィルタリングの設計方針（ルーティング）48, 56
負荷分散通信 264
不正端末アクセス防止機能 291
プライオリティ 231
プライベートアドレス 100
ブリッジ 280
フレッツ・ADSL 18
プロトコル 98, 229, 231, 235

へ

ヘッダ圧縮機能 234

ほ

ポート番号 235
方向 47, 55, 98
ホストデータベース 258
ホストデータベース情報 240
ポリシーベースネットワーク 229

ま

マスタルータ 269
マニュアル構成 8
マルチ NAT 機能 153, 219
マルチキャスト機能 83
マルチキャスト・パケット 87

め

メトリック値 47, 55

ゆ

優先順位 101
ユニキャスト 83

り

リモートパワーオン機能 276
リモートパワーオン予約 278

Si-R brin シリーズ　コマンド設定事例集

P3NK-3352-04Z0

発行日　　2023年5月

発行責任　　富士通株式会社