

FIBER GATE

L2TPv3 対応 FiberGate

FutureNet XR-410/TX2-L2

XR-640/CD-L2

ユーザースガイド

v 1.6.1 対応版



目次

はじめに	6
ご使用にあたって	7
パッケージの内容物の確認	10
第1章 本装置の概要	11
I. 本装置の特長	12
II. 各部の名称と機能 (XR-410L2)	13
III. 各部の名称と機能 (XR-640L2)	14
IV. 動作環境	17
第2章 本装置の設置	18
I. XR-410L2 の設置	19
II. XR-640L2 の設置	20
第3章 コンピュータのネットワーク設定	21
I. Windows 95/98/Me のネットワーク設定	22
II. Windows 2000 のネットワーク設定	23
III. Windows XP のネットワーク設定	24
IV. Windows Vista のネットワーク設定	25
V. Macintosh のネットワーク設定	26
VI. IP アドレスの確認と再取得	27
第4章 設定画面へのログイン	28
設定画面へのログイン方法	29
第5章 インターフェース設定	30
I. Ethernet ポートの設定	31
II. Ethernet ポートの設定について	32
III. VLAN タギングの設定	33
IV. デフォルトゲートウェイの設定	34
V. ポートベース VLAN の設定 (XR-640L2 のみ)	35
VI. ARP エントリの設定 (XR-640L2 のみ)	36
第6章 PPPoE 設定	37
I. PPPoE の接続先設定	38
II. PPPoE の接続設定と回線の接続 / 切断	40
III. 副回線とバックアップ回線	41
IV. PPPoE 特殊オプション設定	44
第7章 RS-232C、RS-232C/BRI ポートを使った接続(リモートアクセス機能)	45
I. 本装置とアナログモデム / TA の接続	46
II. BRI ポートを使った TA / DSU との接続 (XR-640L2 のみ)	47
III. リモートアクセス回線の接続先設定	48
IV. リモートアクセス回線の接続と切断	50
V. 回線への自動発信の防止について	51
VI. 副回線接続とバックアップ回線接続	52
第8章 複数アカウント同時接続設定	53
複数アカウント同時接続の設定	54
第9章 各種サービスの設定	58
各種サービス設定	59
第10章 DNS リレー / キャッシュ機能	60
DNS 機能の設定	61

第 11 章 IPsec 機能	62
I. 本装置の IPsec 機能について	63
II. IPsec 設定の流れ	64
III. IPsec 設定	65
IV. IPSec Keep-Alive 設定	72
V. 「X.509 デジタル証明書」を用いた電子認証	74
VI. IPsec 通信時のパケットフィルタ設定	75
VII. IPsec 設定例 1 (センター / 拠点間の 1 対 1 接続)	76
VIII. IPsec 設定例 2 (センター / 拠点間の 2 対 1 接続)	80
IX. IPsec がつながらないとき	87
第 12 章 ダイナミックルーティング	90
I. ダイナミックルーティング機能	91
II. RIP の設定	92
III. OSPF の設定	94
IV. DVMRP の設定 (XR-640L2 のみ)	101
第 13 章 L2TPv3 機能	103
I. L2TPv3 機能概要	104
II. L2TPv3 機能設定	105
III. L2TPv3 Tunnel 設定	107
IV. L2TPv3 Xconnect (クロスコネク) 設定	109
V. L2TPv3 Group 設定	111
VI. Layer2 Redundancy 設定	112
VII. L2TPv3 Filter 設定	114
VIII. 起動 / 停止設定	115
IX. L2TPv3 ステータス表示	117
X. 制御メッセージ一覧	118
XI. L2TPv3 設定例 1 (2 拠点間の L2TP トンネル)	119
XII. L2TPv3 設定例 2 (L2TP トンネル二重化)	123
第 14 章 L2TPv3 フィルタ機能	131
I. L2TPv3 フィルタ 機能概要	132
II. 設定順序について	135
III. 機能設定	136
IV. L2TPv3 Filter 設定	137
V. Root Filter 設定	139
VI. Layer2 ACL 設定	141
VII. IPv4 Extend ACL 設定	143
VIII. ARP Extend ACL 設定	145
IX. 802.1Q Extend ACL 設定	146
X. 802.3 Extend ACL 設定	148
XI. 情報表示	149
第 15 章 SYSLOG 機能	151
syslog 機能の設定	152
第 16 章 SNMP エージェント機能	154
I. SNMP エージェント機能の設定	155
II. Century Systems プライベート MIB について	158
第 17 章 NTP サービス	159
NTP サービスの設定方法	160

第 18 章 アクセスサーバ機能	162
I. アクセスサーバ機能について	163
II. 本装置とアナログモデム /TA の接続	164
III. BRI ポートを使った TA/DSU との接続 (XR-640L2 のみ)	165
IV. アクセスサーバ機能の設定	166
第 19 章 スタティックルート設定	169
スタティックルート設定	170
第 20 章 ソースルート設定	172
ソースルート設定	173
第 21 章 NAT 機能	174
I. 本装置の NAT 機能について	175
II. バーチャルサーバ設定	176
III. 送信元 NAT 設定	177
IV. バーチャルサーバの設定例	178
V. 送信元 NAT の設定例	181
補足：ポート番号について	182
第 22 章 パケットフィルタリング機能	183
I. パケットフィルタリング機能の概要	184
II. 本装置のフィルタリング機能について	185
III. パケットフィルタリングの設定	186
IV. パケットフィルタリングの設定例	188
V. 外部から設定画面にアクセスさせる設定	194
補足：NAT とフィルタの処理順序について	195
補足：ポート番号について	196
補足：フィルタのログ出力内容について	197
第 23 章 スケジュール設定 (XR-640L2 のみ)	198
スケジュール機能の設定方法	199
第 24 章 ネットワークイベント機能	201
I. 機能の概要	202
II. 各トリガテーブルの設定	204
III. 実行イベントテーブルの設定	206
IV. 実行イベントのオプション設定	207
V. ステータスの表示	208
第 25 章 仮想インターフェース機能	209
仮想インターフェース機能の設定	210
第 26 章 GRE 設定	211
GRE の設定	212
第 27 章 QoS 機能	214
I. QoS について	215
II. QoS 機能の各設定画面について	219
III. 各キューイング方式の設定手順について	220
IV. 各設定画面での設定方法について	221
V. ステータスの表示	229
VI. 設定の編集・削除方法	230
VII. ステータス情報の表示例	231
VIII. クラスの階層構造について	235
IX. TOS について	236

第 28 章 ゲートウェイ認証機能	238
I. ゲートウェイ認証機能の設定	239
II. ゲートウェイ認証下のアクセス方法	243
III. ゲートウェイ認証の制御方法について	244
第 29 章 ネットワークテスト	245
ネットワークテスト	246
第 30 章 簡易 CLI 機能 (XR-640L2 のみ)	250
I. 簡易 CLI 機能の概要	251
II. 簡易 CLI 機能のアクセス設定	252
1. ユーザアカウントの作成	252
2. アクセスリストの設定	253
3. CLI 接続の受付開始	254
第 31 章 システム設定	256
システム設定	257
時計の設定	257
ログの表示	258
ログの削除	258
パスワードの設定	259
ファームウェアのアップデート	260
設定の保存と復帰	261
設定のリセット	262
再起動	262
セッションライフタイムの設定	263
設定画面の設定	264
ISDN 設定 (XR-640L2 のみ)	264
オプション CF カード (XR-640L2 のみ)	265
CLI 設定 (XR-640L2 のみ)	266
ARP filter 設定	266
第 32 章 情報表示	267
本体情報の表示	268
第 33 章 詳細情報表示 (XR-640L2 のみ)	270
各種情報の表示	271
第 34 章 テクニカルサポート	272
テクニカルサポート	273
第 35 章 運用管理設定	274
I. INIT ボタンの操作	275
II. 携帯電話による制御 (XR-640L2 のみ)	277
付録 A インターフェース名について	279
付録 B 工場出荷設定一覧	281
付録 C サポートについて	283

はじめに

ご注意

- 1 本装置の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信の機会を逸したために生じた損害などの純粹經濟損失につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。
- 2 通信情報が漏洩した事による經濟的、精神的損害につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。
- 3 本書の内容の一部または全部を無断で転載、複写することを禁じます。
- 4 本書およびソフトウェア、ハードウェア、外觀の内容について、将来予告なしに変更することがあります。
- 5 本書の内容については万全を期しておりますが、万一ご不審な点や誤り、記載漏れなどお気づきの点がありましたらご連絡ください。

商標の表示

「FIBER GATE」はセンチュリー・システムズ株式会社の登録商標です。

「FutureNet」はセンチュリー・システムズ株式会社の登録商標です。

下記製品名等は米国Microsoft Corporationの登録商標です。

Microsoft、Windows、Windows 95、Windows 98、Windows NT3.51、Windows NT4.0

Windows 2000、Windows Me、Windows XP、Windows Vista

Macintosh、Mac OS Xは、アップル社の登録商標です。

その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

ご使用にあたって

本製品を安全にお使いいただくために、まず以下の注意事項を必ずお読みください。

この取扱説明書では、製品を安全に正しくお使いいただき、あなたや他の人々への危害や財産への損害を未然に防止するために、いろいろな絵表示をしています。その表示と意味は次のようになっています。内容をよく理解してから本文をお読みください。

次の表示の区分は、表示内容を守らず、誤った使用をした場合に生じる「危害や損害の程度」を説明しています。



危険

この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う危険が差し迫って生じることが想定される内容を示しています。



警告

この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。



注意

この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容および物的損害のみの発生が想定される内容を示しています。

次の絵表示の区分は、お守りいただく内容を説明しています。



このような絵表示は、してはいけない「禁止」を意味するものです。それぞれに具体的な禁止内容が書かれています。



このような絵表示は、必ず実行していただく「強制」を指示するものです。それぞれに具体的な指示内容が書かれています。

危険



必ず本体に付属している電源ケーブルをご使用ください。



使用温度範囲は0 ~ 40 です。この温度範囲以外では使用しないでください。



ストーブのそばなど高温の場所で使用したり、放置しないでください。











火の中に投入したり、加熱したりしないでください。



製品の間隙から針金などの異物を挿入しないでください。










ご使用にあたって

警告

-  万一、異物(金属片・水・液体)が製品の内部に入った場合は、まず電源を外し、お買い上げの販売店にご連絡ください。そのまま使用すると火災の原因となります。
-  万一、発熱していたり、煙が出ている、変な臭いがするなどの異常状態のまま使用すると、火災の原因となります。すぐに電源を外し、お買い上げの販売店にご連絡ください。
-  本体を分解、改造しないでください。けがや感電などの事故の原因となります。
-  本体または電源ケーブルを直射日光の当たる場所や、調理場や風呂場など湿気が多い場所では絶対に使用しないでください。火災・感電・故障の原因となります。
-  電源ケーブルの電源プラグについたほこりはふき取ってください。火災の原因となります。
-  濡れた手で電源ケーブル、コンセントに触れないでください。感電の原因となります。
-  電源ケーブルのプラグにドライバなどの金属が触れないようにしてください。火災・感電・故障の原因となります。
-  AC100V の家庭用電源以外では絶対に使用しないでください。火災・感電・故障の原因となります。

ご使用にあたって

注意

-  湿気やほこりの多いところ、または高温となるところには保管しないでください。故障の原因となります。
-  乳幼児の手の届かないところに保管してください。けがなどの原因となります。
-  長期間使用しないときには、電源ケーブルをコンセントおよび本体から外してください。
-  電源ケーブルの上に重いものを乗せたり、ケーブルを改造したりしないでください。また、電源ケーブルを無理に曲げたりしないでください。火災・感電・故障の原因となることがあります。
-  電源ケーブルは必ず電源プラグを持って抜いてください。ケーブルを引っ張ると、ケーブルに傷が付き、火災・感電・故障の原因となることがあります。
-  近くに雷が発生したときには、電源ケーブルをコンセントから抜いて、ご使用をお控えください。落雷が火災・感電・故障の原因となることがあります。
-  電源ケーブルのプラグを本体に差し込んだ後に電源ケーブルを左右および上下に引っ張ったり、ねじったり、曲げたりしないでください。緩みがある状態にしてください。
-  本製品に乗らないでください。本体が壊れて、けがの原因となることがあります。
-  高出力のアンテナや高圧線などが近くにある環境下では、正常な通信ができない場合があります。

パッケージの内容物の確認

本製品のパッケージには以下のものが同梱されております。本製品をお使いいただく前に、内容物がすべて揃っているかご確認ください。
万が一、不足がありましたら、お買いあげいただいた店舗または弊社サポートデスクまでご連絡ください。

< XR-410/TX2-L2 をお買い上げの方 >

XR-410/TX2-L2本体	1台
はじめにお読みください	1部
安全にお使いいただくために	1部
RJ-45/D-sub9ピン変換アダプタ(ストレート)	1個
UTPケーブル(ストレート)	1本
ACアダプタ	1個
保証書	1部
海外使用禁止シート	1部

< XR-640/CD-L2 をお買い上げの方 >

XR-640/CD-L2本体	1台
はじめにお読みください	1部
安全にお使いいただくために	1部
UTPケーブル(1m、ストレート)	1本
AC電源ケーブル	1本
保証書	1部
海外使用禁止シート	1部

第1章

本装置の概要

第1章 本装置の概要

1. 本装置の特長

XR-410/TX2-L2 と XR-640/CD-L2(以下 本装置または XR-410L2、XR-640L2)は次のような特長を持っています。

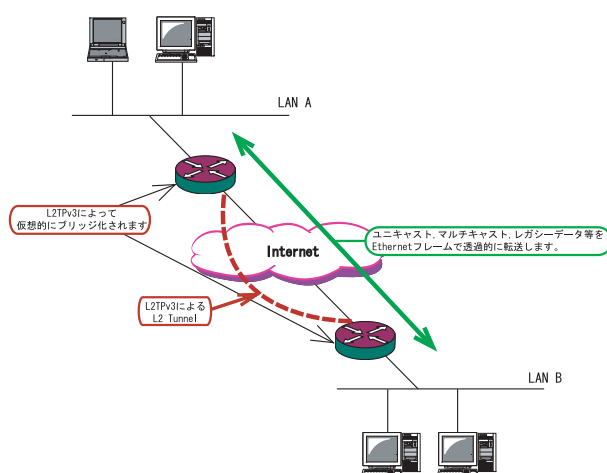
L2TPv3 機能を搭載

本製品は次世代ネットワークのトンネリング及びVPNにおける主要技術になりつつあるL2TPv3機能を搭載しています。

L2TPv3 機能は、IP ネットワーク上のルータ間でL2TP トンネルを構築します。これにより本製品が仮想的なブリッジとなり、遠隔のネットワーク間でレイヤ2通信が可能となります。

レイヤ2でトンネリングするため、2つのネットワークはHUBで繋がった1つのEthernetネットワークとして使うことができます。また上位プロトコルに依存せずにネットワーク通信ができ、TCP/IPだけでなく、任意の上位プロトコル(IPX、AppleTalk、SNA等)を透過的に転送することができます。

またL2TPv3 機能は、従来の専用線やフレームリレー網ではなくIP網で利用できますので、低コストな運用が可能です。



L2TPv3 機能につきましては、第13章「L2TPv3 機能」をご参照ください。

IPsec 機能を搭載

本製品のIPsec機能を使うことで、インターネット上で複数の拠点をつなぐIP仮想専用線(インターネットVPN)の構築に利用できます。

またL2TPv3とIPsecを組み合わせることで、セキュアなL2トンネリング通信を実現できるようになります。

障害時のバックアップ回線接続機能

PingやOSPFによるインターネットVPNのエンド～エンドの監視を実現し、ネットワークの障害時にISDN回線や予備のプロードバンド回線を用いてバックアップ接続する機能を搭載しています。

ルーティング機能

RIP v1/v2、OSPFを用いたダイナミックルーティングが可能です。スタティックルートも設定できます。

802.1q VLANに対応

本製品の各EthernetポートでVLAN IDが最大64個までの802.1qマルチプルVLANを構築できます。インタフェース毎に複数のVLANセグメントを設定し、LAN内でのセキュリティを強化することができます。

その他、以下のような各機能を搭載しています。

PPPoEに対応したブロードバンド接続が利用可

DHCPクライアント機能

NAT/IPマスカレード機能を搭載

パケットフィルタリング機能

DNSリレー機能

GREトンネリング機能

QoS機能

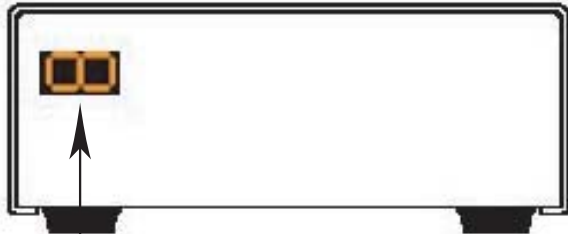
ゲートウェイ認証機能

ISDN BRI 接続機能 (XR-640L2のみ)

各種システムログの記録

II. 各部の名称と機能 (XR-410L2)

製品前面



①

7セグメント LED

本装置の状態を表します。

本装置の起動中は 2 3 4 5 6 7 の順に LED が表示されます。

本装置の起動後は、本装置の各インターフェースのリンク状態を表示します。以下に各状態について説明します。



Ether0 ポートが Linkup している状態。



Ether1 ポートが Linkup している状態。



RS-232 ポートが Linkup している状態。



システムが動作している状態。
右上にある「。」が点滅します。

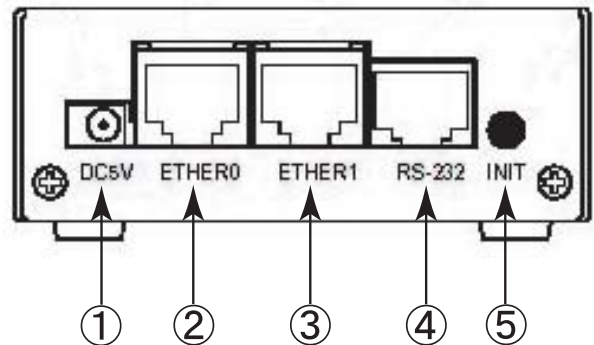


ケーブルを接続して動作している状態の表示例。

ファームウェアのアップデート中は「8」が表示されます。

「2」「6」「8」等の数字を表示したまま止まっているときは、システム故障により本装置が正常に起動できない状態となっています。弊社にてシステムの復旧が必要となりますので、この状態になったときは弊社までご連絡ください。

製品背面



電源コネクタ

製品付属の AC アダプタを接続します。

Ether0 ポート

主に LAN との接続に使用します。イーサネット規格の UTP 100Base-TX ケーブルを接続します。ケーブルの極性は自動判別します。

Ether1 ポート

WAN 側ポートとして、また、Ether0 ポートとは別セグメントを接続するポートとして使います。イーサネット規格の UTP 100Base-TX ケーブルを接続します。ケーブルの極性は自動判別します。

RS-232 ポート

リモートアクセスやアクセスサーバー機能を使用するときにモデムを接続します。ストレートタイプの LAN ケーブルと製品添付の変換アダプタを用いてモデムと接続してください。

INIT ボタン

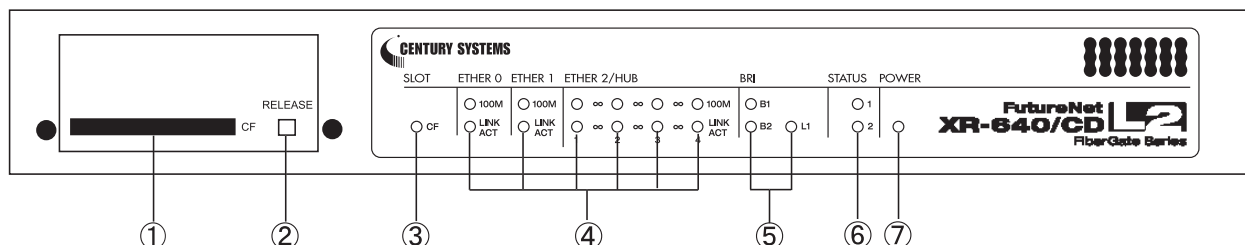
本装置を工場出荷時の設定に戻して起動するときには押します。操作方法については第 29 章「システム設定」をごらんください。

XR-410L2 には Ether 2 ポートはありません。文中の "eth2" の記述は XR-640L2 のものです。

第1章 本装置の概要

III. 各部の名称と機能 (XR-640L2)

製品前面



CFカードスロット

オプションで用意されているCFカードを挿入します。

RELEASE ボタン

CFカードを取り外すときに押します。RELEASE ボタンを数秒押し続けると、の「CF」LEDが消灯します。この状態になったら、CFカードを安全に取り外せます。

SLOT CF LED

CFカードが挿入され動作しているときに、CF(緑)が点灯します。

CFカードをスロットに挿入しカードが使用可能状態になるまでの間は、CF(緑)は点滅します。

CFカードが挿入されていないとき、またの操作をおこないCFカードを安全に取り外せる状態になったときは、CF(緑)は消灯します。

Ethernet ポート LED

各Ethernetポートの状態を表示します。

LANケーブルが正常に接続されているときに

「LINK/ACT」(緑)ランプが点灯します。

「100M」(緑)ランプは、10Base-Tで接続した場合に消灯、100Base-TXで接続した場合に点灯します。データ通信時は「LINK/ACT」ランプが消灯します。

BRI LED

「L1」(緑)ランプは、本装置のBRI U点・S/T点ポートがリンクアップしているときに点灯します。

「B1」「B2」(緑)ランプは、本装置のBRIポートを使って回線接続しているときに点灯します。回線接続していないときは消灯しています。

STATUS LED

本装置の全てのサービスが動作開始状態になっているときに、STATUS1(赤)は消灯します。

PPP/PPPoE主回線で接続しているときに、STATUS2(緑)は点灯します。PPP/PPPoE主回線で接続していない時は消灯しています。

ファームウェアのアップデート作業中は、STATUS1(赤)が点滅します。

ファームウェアのアップデートに失敗した場合など、本装置が正常に起動できない状態になったときは、STATUS1(赤)とSTATUS2(緑)のどちらも点滅します。

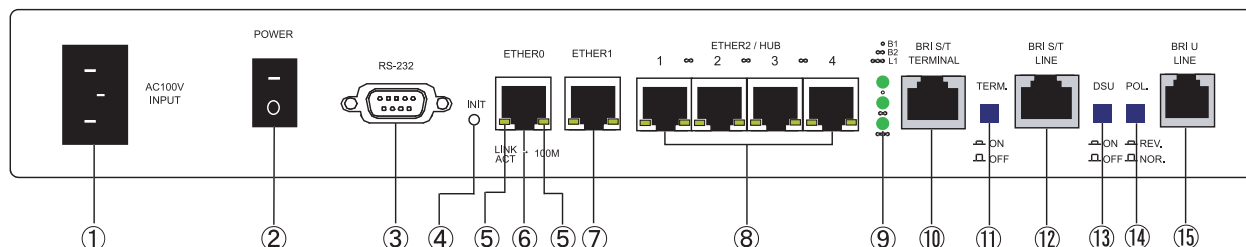
POWER LED

本装置に電源が投入されているときに点灯(緑)します。

第1章 本装置の概要

III. 各部の名称と機能 (XR-640L2)

製品背面



電源ケーブル差込口

製品付属の電源ケーブルを接続するコネクタです。ケーブルは必ず付属のものをご使用ください。

電源スイッチ

電源をオン/オフするためのスイッチです。

RS-232ポート

リモートアクセスやアクセスサーバ機能を使用するときにモデムを接続します。接続には別途シリアルケーブルをご用意ください。

INITボタン

本装置を工場出荷時の設定に戻して起動するとき、およびオプションCFカードの設定から起動するときに使用します。

LINK/ACT LED

Ethernetポートの状態を表示します。LANケーブルが正常に接続されているときに「LINK/ACT」(緑)ランプが点灯します。「100M」(黄)ランプは、10Base-Tで接続した場合に消灯、100Base-TXで接続した場合に点灯します。データ通信時は「LINK/ACT」ランプが消灯します。本装置のすべてのEthernetポートに実装されています。

Ether0ポート

主にDMZポートとして、また、Ether1、Ether2ポートとは別セグメントを接続するポートとして使います。イーサネット規格のUTPケーブル(LANケーブル)を接続します。極性は自動判別します。

Ether1ポート

主にWAN側ポートとして、また、Ether0、Ether2ポートとは別セグメントを接続するポートとして使います。イーサネット規格のUTPケーブル(LANケーブル)を接続します。極性は自動判別します。

Ether2ポート

4ポートのスイッチングHUBです。主にLANとの接続に使用します。イーサネット規格のUTPケーブル(LANケーブル)を接続します。極性は自動判別します。

BRI LED

「L1」(緑)ランプは、本装置のBRIポートと回線・機器が正常に接続されているときに点灯します。「B1」「B2」(緑)ランプは、Bチャンネルで通信時に点灯します。MP接続時は「B1」「B2」ランプの両方が点灯します。

BRI S/T TERMINALポート

外部ISDN端末機器を接続する際にISDNケーブルを用いて、このポートと他のISDN機器のBRI S/T点ポートを接続します。

TERM. スイッチ

「ISDN S/T点ポート」接続時の終端抵抗のON/OFFを切替えます。BRI S/T点ポートを使って他のISDN機器のDSU機器を接続している場合は、本装置を含めていずれか1つの機器の終端抵抗をONにしてください。

第1章 本装置の概要

III. 各部の名称と機能 (XR-640L2)

BRI S/T LINE ポート

本装置の DSU 機能を使わずに外部の DSU を使う場合に、ISDN ケーブルでこのポートと外部 DSU の BRI S/T 点ポートを接続します。

DSU スイッチ

本装置の内蔵 DSU を使用する際は「ON」(ボタンを押した状態)に、外部 DSU を使用する際は「OFF」(ボタンを押していない状態)にしてください。

本装置の内蔵 DSU を使用して ISDN 接続する場合は、本装置の「BRI S/T LINE」ポートは使用しません。

POL. スイッチ

BRI U 点で ISDN 接続する場合の、回線の極性を切り替えます。極性がリバースの場合は「REV.」(ボタンを押した状態)に、ノーマルの場合は「NOR.」(ボタンを押していない状態)にしてください。

BRI U ポート

本装置の内蔵 DSU を使用して ISDN 接続するときは、回線をこのポートに接続します。また回線の極性に合わせて「POL. スイッチ」を切り替えてください。

IV. 動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

ハードウェア環境

- ・本製品に接続するコンピュータの全てに、10Base-Tまたは100Base-TXのLANボード/カードがインストールされていること。
- ・ADSLモデムまたはCATVモデムに、10Base-Tまたは100Base-TXのインターフェースが搭載されていること。
- ・本製品と全てのコンピュータを接続するためのハブやスイッチングハブが用意されていること。
- ・本製品と全てのコンピュータを接続するために必要な種類のネットワークケーブルが用意されていること。
- ・シリアルポートを使う場合は、接続に必要なシリアルケーブルが用意されていること。

ソフトウェア環境

- ・TCP/IPを利用できるOSがインストールされていること。
- ・接続されている全てのコンピュータの中で少なくとも1台に、Internet Explorer 5.0以降か Netscape Navigator 6.0以降がインストールされていること。

なおサポートにつきましては、本製品固有の設定項目と本製品の設定に関するOS上の設定に限らせていただきます。OS上の一般的な設定やパソコンにインストールされたLANボード/カードの設定、各種アプリケーションの固有の設定等のお問い合わせについてはサポート対象外とさせていただきますので、あらかじめご了承ください。

第2章

本装置の設置

第2章 本装置の設置

1. XR-410L2 の設置

XR-410L2 と xDSL/ ケーブルモデムやコンピューターは、以下の手順で接続してください。

1 本装置と xDSL/ ケーブルモデムやパソコン・HUB など、接続する全ての機器の電源が OFF になっていることを確認してください。

2 本装置の背面にある Ether1 ポートと xDSL/ ケーブルモデムや ONU を、LAN ケーブルで接続してください。

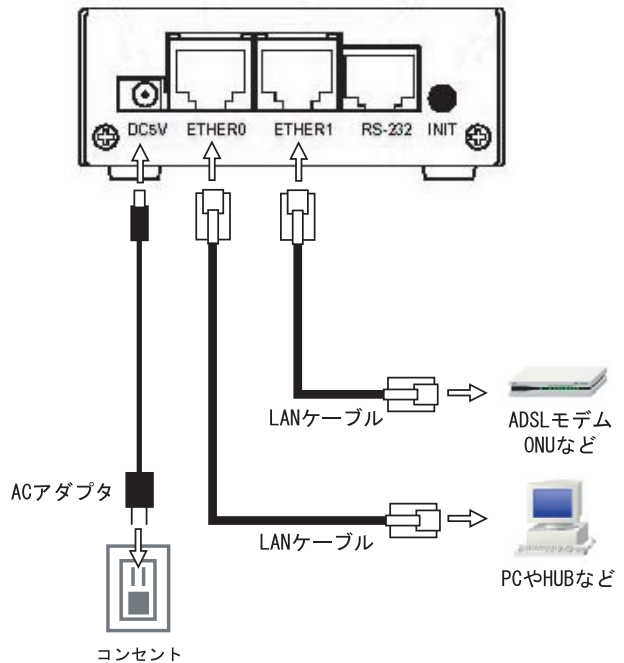
3 本装置の背面にある Ether0 ポートと HUB や PC を、LAN ケーブルで接続してください。

各 Ethernet ポートは LAN ケーブルの極性を自動判別します。

4 本装置と AC アダプタ、AC アダプタとコンセントを接続してください。

5 全ての接続が完了しましたら、本装置と各機器の電源を投入してください。

接続図(例)



⚠ 注意！

本装置は直射日光が当たる場所や、温度の高い場所には設置しないようにしてください。内部温度が上がり、動作が不安定になる場合があります。

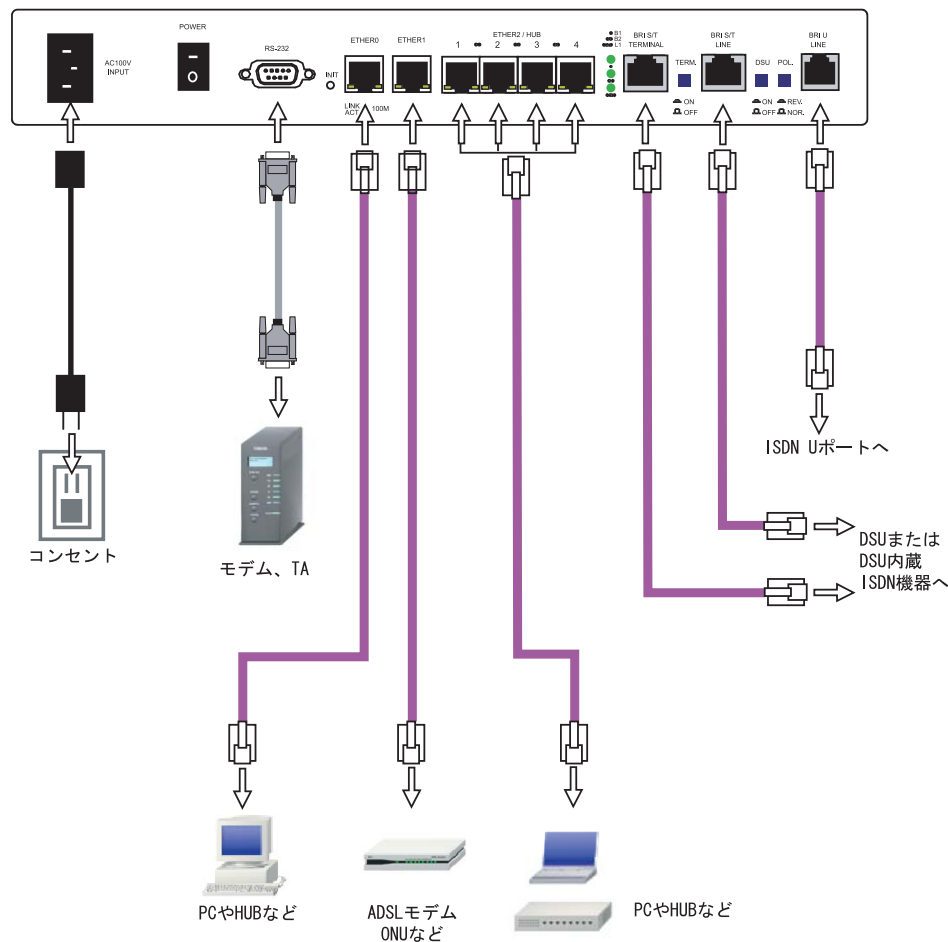
⚠ 注意！

AC アダプタのプラグを本体に差し込んだ後に、AC アダプタのケーブルを左右及び上下に引っ張らず、緩みがある状態にしてください。抜き差しもケーブルを引っ張らず、コネクタを持っておこなってください。また、AC アダプタのケーブルを足などで引っ掛けてプラグ部に異常な力が掛からないように配線にご注意ください。

第2章 本装置の設置

11. XR-640L2 の設置

XR-640L2 と xDSL/ ケーブルモデムやコンピュータは、以下の手順で接続してください。



1 本装置と xDSL/ ケーブルモデムやパソコン・HUB など、接続する全ての機器の電源が OFF になっていることを確認してください。

2 本装置の背面にある Ether1 ポートと xDSL/ ケーブルモデムや ONU を、LAN ケーブルで接続してください。接続に使うケーブルの種類は、各機器の説明書等をご覧ください。

3 本装置の設定が工場出荷状態の場合、Ether0 ポートと PC を LAN ケーブルで接続してください。ケーブルの極性は自動判別します。

4 本装置の背面にある Ether2(HUB)ポート(1 ~ 4 のいずれかのポート)と PC を LAN ケーブルで接続してください。ケーブルの極性は自動判別します。

5 本装置と電源ケーブル、電源ケーブルとコンセントを接続してください。

6 全ての接続が完了しましたら、本装置と各機器の電源を投入してください。

注意！

本装置は直射日光が当たるところや、温度の高いところには設置しないようにしてください。内部温度が上がり、動作が不安定になる場合があります。

注意！

AC 電源ケーブルのプラグを本体に差し込んだ後に AC 電源ケーブルのケーブルを左右及び上下に引っ張らず、緩みがある状態にしてください。抜き差しもケーブルを引っ張らず、コネクタを持っておこなってください。

20 また、AC 電源ケーブルのケーブルを足などで引っ掛けてプラグ部に異常な力が掛からないように配線にご注意ください。

第3章

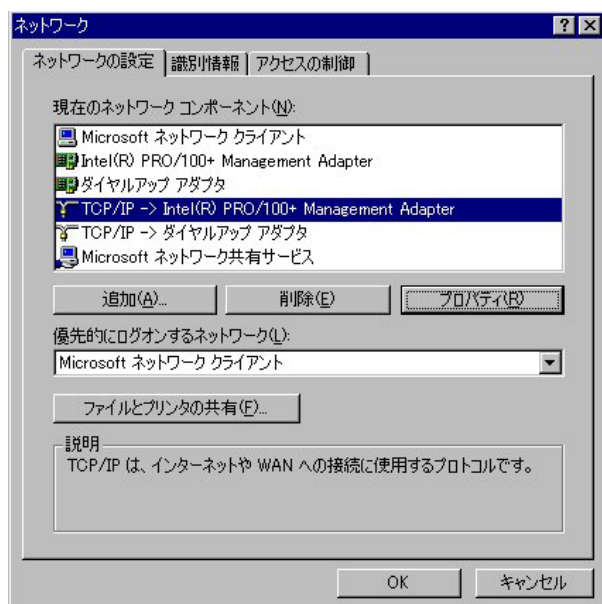
コンピュータのネットワーク設定

第3章 コンピュータのネットワーク設定

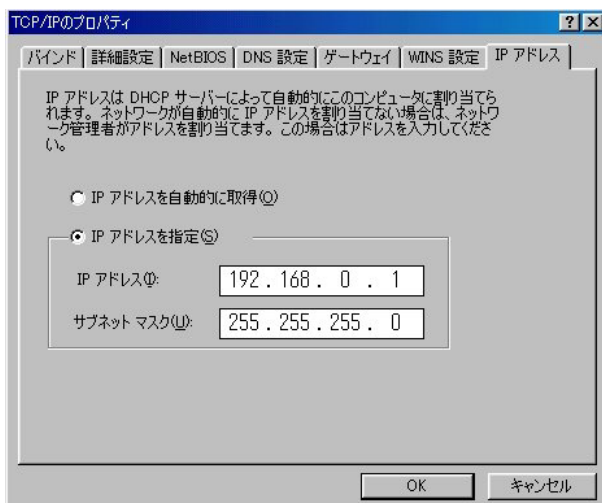
1. Windows 95/98/Me のネットワーク設定

ここではWindows95/98/Meが搭載されたコンピュータのネットワーク設定について説明します。

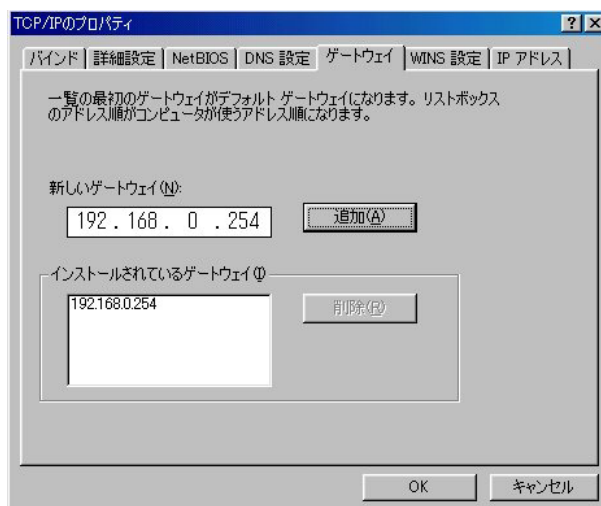
1 「コントロールパネル」 「ネットワーク」の順で開き、「ネットワークの設定」タブの「現在のネットワーク構成」から、コンピュータに装着されたLANボード(カード)のプロパティを開きます。



2 「TCP/IPのプロパティ」が開いたら、「IPアドレス」タブをクリックしてIP設定をおこないます。「IPアドレスを指定」にチェックを入れて、
IPアドレスに「192.168.0.1」
サブネットマスクに「255.255.255.0」
と入力します。



3 続いて「ゲートウェイ」タブをクリックして、新しいゲートウェイに「192.168.0.254」と入力して追加ボタンをクリックしてください。



4 最後にOKボタンをクリックするとコンピュータが再起動します。再起動後に、本装置の設定画面へのログインが可能になります。

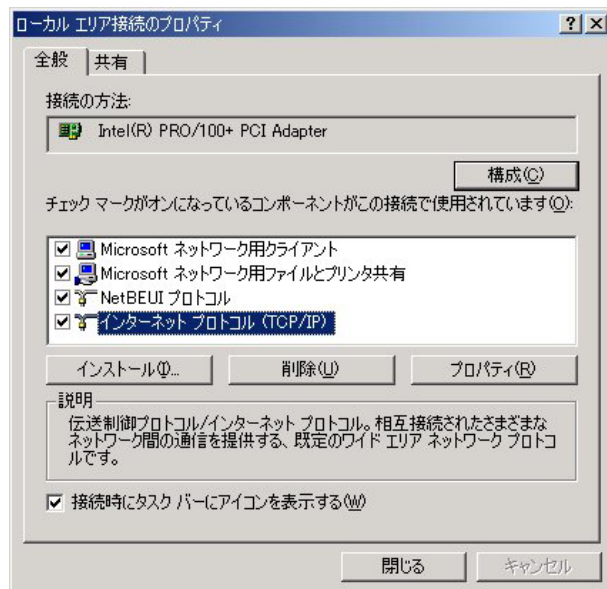
第3章 コンピュータのネットワーク設定

11. Windows 2000 のネットワーク設定

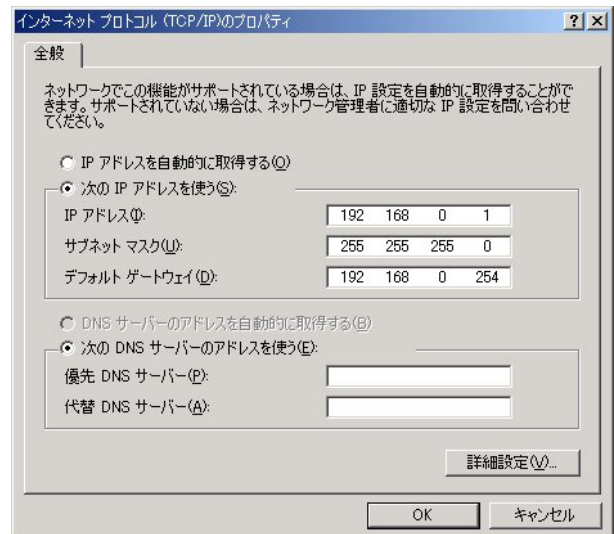
ここではWindows2000が搭載されたコンピュータのネットワーク設定について説明します。

1 「コントロールパネル」 「ネットワークとダイヤルアップ接続」から、「ローカル接続」を開きます。

2 画面が開いたら、「インターネットプロトコル(TCP/IP)」のプロパティを開きます。



3 「全般」の画面では、「次の IP アドレスを使う」にチェックを入れて以下のように入力します。
IP アドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」



4 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

第3章 コンピュータのネットワーク設定

III. Windows XPのネットワーク設定

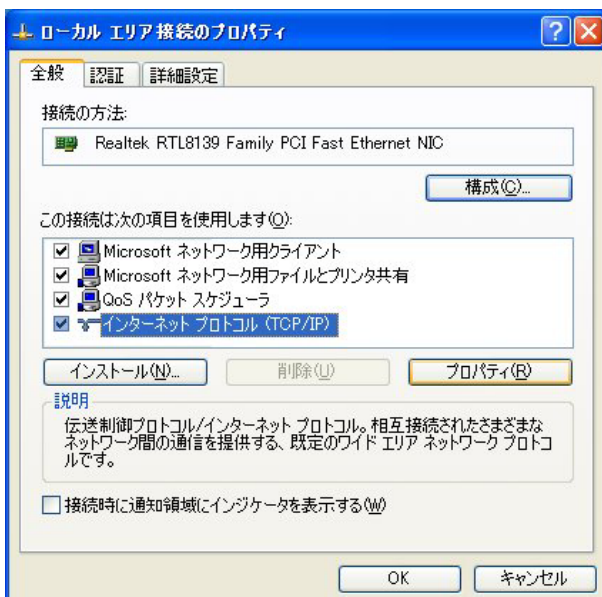
ここではWindowsXPが搭載されたコンピュータのネットワーク設定について説明します。

1 「コントロールパネル」 「ネットワーク接続」から、「ローカル接続」を開きます。

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。



3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコル(TCP/IP)」を選択して「プロパティ」ボタンをクリックします。

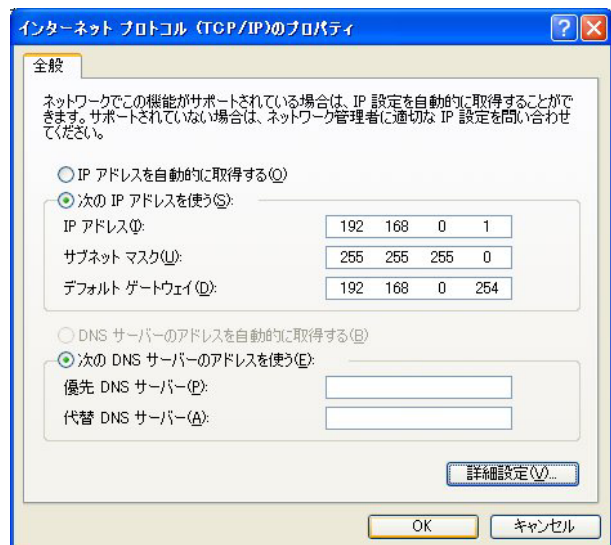


4 「インターネットプロトコル(TCP/IP)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.1」

サブネットマスク「255.255.255.0」

デフォルトゲートウェイ「192.168.0.254」



5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

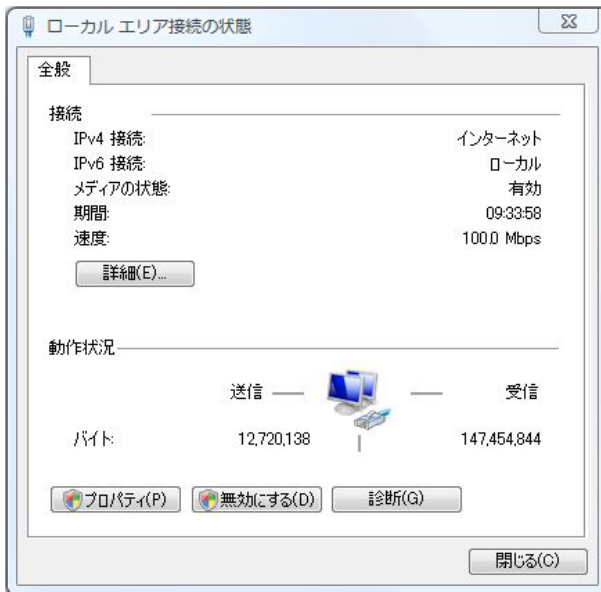
第3章 コンピュータのネットワーク設定

IV. Windows Vistaのネットワーク設定

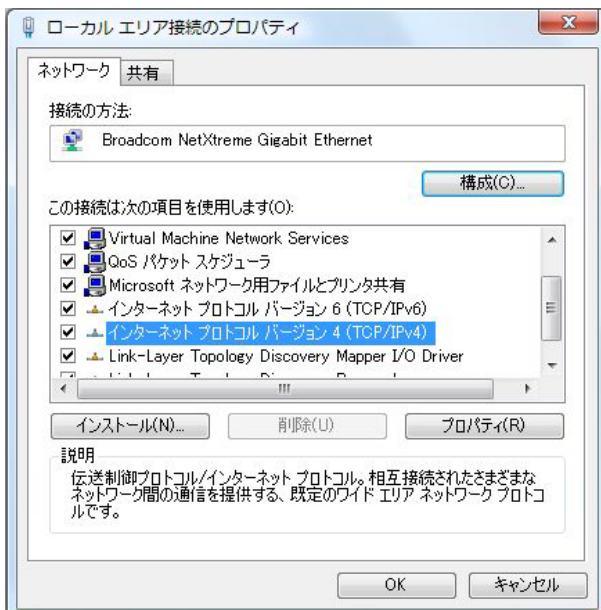
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

1 「コントロールパネル」 「ネットワークと共有センター」 「ネットワーク接続の管理」から、「ローカル接続」を開きます。

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。



3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。

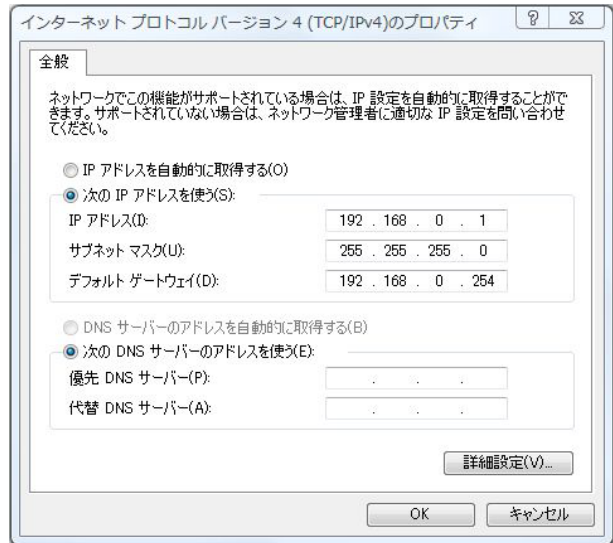


4 「インターネットプロトコルバージョン4(TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.1」

サブネットマスク「255.255.255.0」

デフォルトゲートウェイ「192.168.0.254」



5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

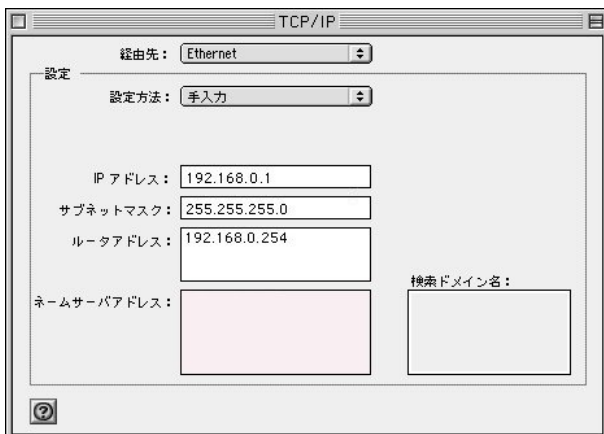
第3章 コンピュータのネットワーク設定

V. Macintosh のネットワーク設定

ここではMacintoshのネットワーク設定について説明します。

1 「アップルメニュー」から「コントロールパネル」 「TCP/IP」を開きます。

2 経由先を「Ethernet」、設定方法を「手入力」にして、以下のように入力してください。
IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」

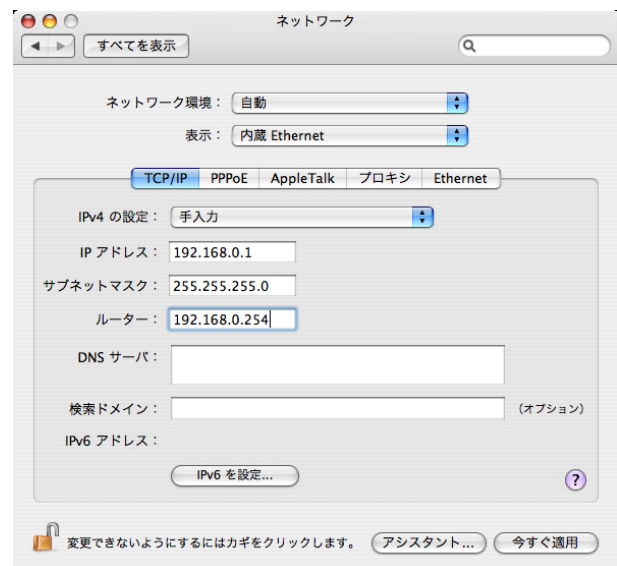


3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これで本装置へログインする準備が整いました。

ここでは、Mac OS Xのネットワーク設定について説明します。

1 「システム環境設定」から「ネットワーク」を開きます。

2 ネットワーク環境を「自動」、表示を「内蔵 Ethernet」、IPv4の設定を「手入力」にして、以下のように入力してください。
IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
ルーター「192.168.0.254」



3 ウィンドウを閉じて設定の変更を適用します。これで、本装置へログインする準備が整いました。

第3章 コンピューターのネットワーク設定

VI. IPアドレスの確認と再取得

Windows95/98/Me の場合

1 「スタート」 「ファイル名を指定して実行」を開きます。

2 名前欄に、"winipcfg" というコマンドを入力して「OK」をクリックしてください。

3 「IP設定」画面が開きます。リストから、パソコンに装着されているLANボード等を選び、「詳細」をクリックしてください。そのLANボードに割り当てられたIPアドレス等の情報が表示されます。



4 「IP設定」画面で「全て解放」をクリックすると、現在のIP設定がクリアされます。引き続き「すべて書き換え」をクリックすると、IP設定を再取得します。

WindowsNT3.51/4.0/2000/XP の場合

1 「スタート」 「プログラム」 「アクセサリ」 「コマンドプロンプト」を開きます。

2 以下のコマンドを入力すると、現在のIP設定がウィンドウ内に表示されます。

```
c:*\>ipconfig /all
```

3 IP設定のクリアと再取得をするには以下のコマンドを入力してください。

```
c:*\>ipconfig /release (IP設定のクリア)
```

```
c:*\>ipconfig /renew (IP設定の再取得)
```

Macintosh の場合

IP設定のクリア/再取得をコマンド等でおこなうことはできませんので、Macintosh本体を再起動してください。

本装置のIPアドレス・DHCPサーバ設定を変更したときは、必ずIP設定の再取得をするようにしてください。

第4章

設定画面へのログイン

第4章 設定画面へのログイン

設定画面へのログイン方法

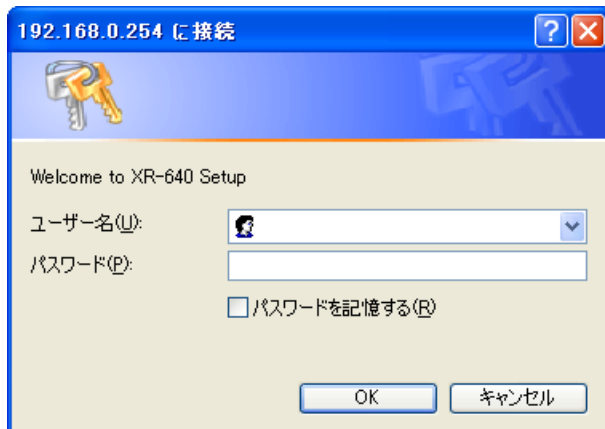
- 1 各種ブラウザを開きます。
- 2 ブラウザから設定画面にアクセスします。
ブラウザのアドレス欄に、以下の IP アドレスとポート番号を入力してください。

http://192.168.0.254:880/

「192.168.0.254」は、Ether0 ポートの工場出荷時のアドレスです。アドレスを変更した場合は、そのアドレスを指定してください。

設定画面のポート番号 880 は変更することができません。

- 3 次のような認証ダイアログが表示されます。



- 4 ダイアログ画面にパスワードを入力します。
工場出荷設定のユーザー名とパスワードはともに「admin」です。ユーザー名・パスワードを変更している場合は、それに合わせてユーザー名・パスワードを入力します。



- 5 ブラウザ設定画面が表示されます。



第5章

インターフェース設定

第5章 インターフェイス設定

1. Ethernet ポートの設定

本装置の各 Ethernet ポートの設定を行います。

Web 設定画面「インターフェイス設定」->「Ethernet0 (または1、2)の設定」をクリックして設定します。

Ethernet0ポート [eth0]

固定アドレスで使用
IPアドレス 192.168.0.254
ネットマスク 255.255.255.0
MTU 1500

DHCPサーバから取得
ホスト名
MACアドレス

IPマスカレード (p masq)
(このポートで使用するIPアドレスに変換して通信を行います)

ステートフルパケットインスペクション (spi)

SPIでDROPしたパケットのLOGを取得

proxy arp

Send Redirects

リンク監視 0 秒 (0-30)
(リンクダウン時にルーティング情報の配信を停止します)

通信モード
 自動 full-100M half-100M full-10M half-10M

IPアドレスに0を設定するとIPが存在しないインターフェイスになります。
通信モードを変更した場合には機器の再起動が必要な場合があります。

Ethernetの設定の保存

各インターフェイスについて、それぞれ必要な情報を入力します。

IPアドレスが固定割り当ての場合は「固定アドレスで使用」にチェックして、IPアドレスとネットマスクを入力します。

IPアドレスに「0」を設定すると、そのインタフェースはIPアドレス等が設定されず、ルーティング・テーブルに載らなくなります。OSPFなどで使用していないインタフェースの情報を配信したくないときなどに「0」を設定してください。

IPアドレスがDHCPで割り当ての場合は「DHCPサーバから取得」にチェックして、必要であればホストネームとMACアドレスを設定します。

MTU

「Path-MTU-Black-HOLE」現象が発生した場合等は、この値を変更することで回避できます。通常は初期設定の1500byteのままでもかまいません。

IPマスカレード
チェックを入れると、そのEthernetポートでIPマスカレードされます。

ステートフルパケットインスペクション
チェックを入れると、そのEthernetポートでステートフルパケットインスペクション(SPI)が適用されます。

SPIでDROPしたパケットのLOGを取得
チェックを入れると、SPIにより破棄(DROP)されたパケットの情報をsyslogに出力します。SPIが有効のときだけ設定可能です。ログの出力内容については、第22章「パケットフィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

Proxy ARP
Proxy ARPを使う場合にチェックを入れます。

Send Redirects
チェックを入れると、そのインタフェースにおいてICMP Redirectsを送出します。

ICMP Redirects

他に適切な経路があることを通知するICMPパケットのことです。

リンク監視
チェックを入れると、Ethernetポートのリンク状態の監視を定期的に行います。OSPFの使用時にリンクのダウンを検知した場合、そのインタフェースに関連付けられたルーティング情報の配信を停止します。再度リンク状態がアップした場合には、そのインタフェースに関連付けられたルーティング情報の配信を再開します。監視間隔は1～30秒の間で設定できます。また、0を設定するとリンク監視を行いません。

ポートの通信モード
本装置のEthernetポートの通信速度・方式を選択します。工場出荷設定では「自動」(オートネゴシエーション)となっていますが、必要に応じて通信速度・方式を選択してください。
Ether2ポートは自動設定のみとなります。

<デフォルトゲートウェイの設定>

デフォルトゲートウェイは「その他の設定」画面で設定します。「デフォルトゲートウェイの設定」欄にIPアドレスを設定します(PPPoE接続時は設定の必要はありません)。

入力が終わりましたら「設定の保存」をクリックして設定完了です。設定はすぐに反映されます。

本装置のインタフェースのアドレスを変更した後は設定が直ちに反映されます。設定画面にアクセスしているホストやその他クライアントのIPアドレス等もXRの設定にあわせて変更し、変更後のIPアドレスで設定画面に再ログインしてください。

第5章 インターフェース設定

11. Ethernet ポートの設定について

[ステートフルパケットインスペクション]

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能とも言えるものです。

通常はWANからのアクセスを全て遮断し、WAN方向へのパケットに対応するLAN方向へのパケット(WANからの戻りパケット)に対してのみポートを開放します。これにより、自動的にWANからの不要なアクセスを制御でき、簡単な設定でより高度な安全性を保つことができます。

ステートフルパケットインスペクション機能を有効にすると、原則としてそのインターフェースへのアクセスは一切不可能となります。ステートフルパケットインスペクション機能とバーチャルサーバ機能を同時に使う場合等は、パケットフィルタリングの設定をおこなって、外部からアクセスできるように設定する必要があります(第22章「パケットフィルタリング機能」参照)。

[PPPoE 接続時の Ethernet ポート設定]

PPPoE 回線に接続する Ethernet ポートの設定については、実際には使用しない、ダミーのプライベート IP アドレスを設定しておきます。

本装置が PPPoE で接続する場合には " ppp " という論理インターフェースを自動的に生成し、この ppp 論理インターフェースを使って PPPoE 接続をおこなうためです。

物理的な Ethernet ポートとは独立して動作しますので、「DHCP サーバから取得」の設定やグローバル IP アドレスの設定はしません。PPPoE に接続しているインターフェースでこれらの設定をおこなうと、正常に動作しなくなる場合があります。

[IPsec 通信時の Ethernet ポート設定]

本装置を IPsec ゲートウェイとして使う場合は、Ethernet ポートの設定に注意してください。

IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが本装置の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。

たとえば、IPsec 通信をおこなう相手側のネットワークが 192.168.1.0/24 で、且つ、本装置の Ether1 ポートに 192.168.1.254 が設定されていると、正常に IPsec 通信がおこなえません。

このような場合は本装置の Ethernet ポートの IP アドレスを、別のネットワークに属する IP アドレスに設定し直してください。

第5章 インターフェース設定

III. VLAN タギングの設定

本装置の各 Ethernet ポートで、VLAN タギング (IEEE802.1Q 準拠) 設定ができます。

Web 設定画面「インターフェース設定」-> 「Ethernet0(または1、2)の設定」をクリックして、以下の画面で設定します。

No.	dev.Tag ID	enable	IPアドレス	ネットマスク	MTU	ip masq	spi	drop log	proxy arp
1	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	eth0	<input checked="" type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VLAN-インターフェースの名称は[eth0.TagID]になります。
64個まで登録できます。
Tag IDに0を登録するとその設定を削除します。
設定は有効なTagIDをもったものから上方につめられます。

devTag ID.

VLAN のタグ ID を設定します。1 から 4094 の間で設定します。各 Ethernet ポートごとに 64 個までの設定ができます。

設定後の VLAN インタフェース名は「eth0.<ID>」「eth1.<ID>」「eth2.<ID>」となります。

enable

チェックを入れることで設定を有効にします。

IP アドレス、サブネットマスク

VLAN インタフェースの IP アドレスとサブネットマスクを設定します。

MTU

VLAN インタフェースの MTU 値を設定します。

ip masq.

チェックを入れることで、VLAN インタフェースでの IP マスカレードが有効となります。

spi

チェックを入れることで、VLAN インタフェースでステートフルパケットインスペクション(SPI)が有効となります。

drop log

チェックを入れると、SPI により破棄(DROP)されたパケットの情報を syslog に出力します。SPI が有効の場合のみ設定可能です。

proxy arp

チェックを入れることで、VLAN インタフェースで proxy arp が有効となります。

入力が終わりましたら「VLAN の設定の保存」をクリックして設定完了です。設定はすぐに反映されます。

また、VLAN 設定を削除する場合は、dev.Tag ID 欄に「0」を入力して「VLAN の設定の保存」をクリックしてください。

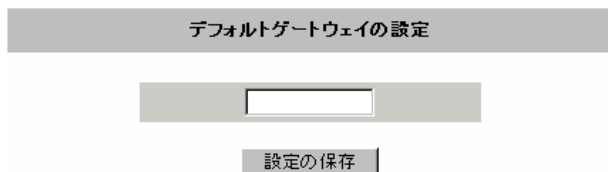
設定情報の表示

VLAN 設定項目にある「設定情報」リンクをクリックすると、現在の VLAN 設定情報が表示されます。

IV. デフォルトゲートウェイの設定

デフォルトゲートウェイの設定

WEB 設定画面「インターフェース設定」「その他の設定」リンクをクリックして以下の画面で設定します。



デフォルトゲートウェイの設定

設定の保存

本装置のデフォルトルートとなる IP アドレスを入力してください。(PPPoE 接続時は設定の必要はありません。)

入力が終わりましたら、「設定の保存」をクリックして設定完了です。

第5章 インターフェース設定

V. ポートベース VLAN の設定 (XR-640L2 のみ)

Ethernet2 ポートで、ポートベース VLAN 設定ができます。

設定できる VLAN グループは A ~ D の 4 つとなります。

Web 設定画面「インターフェース設定」->「その他の設定」をクリックして、以下の画面で設定します。

Ether2 HUB の設定

Port VLAN 機能を使用しない
 Port VLAN 機能を使用する

各ポートとVLANメンバの組み合わせ

	Port 1	Port 2	Port 3	Port 4
VLAN A	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
VLAN B	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VLAN C	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VLAN D	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

ポートベース VLAN 機能を使う場合「Port VLAN 機能を使用する」にチェックします。

「各ポートと VLAN メンバの組み合わせ」で、Ether2 の各ポートと所属する VLAN グループの組み合わせを設定します。

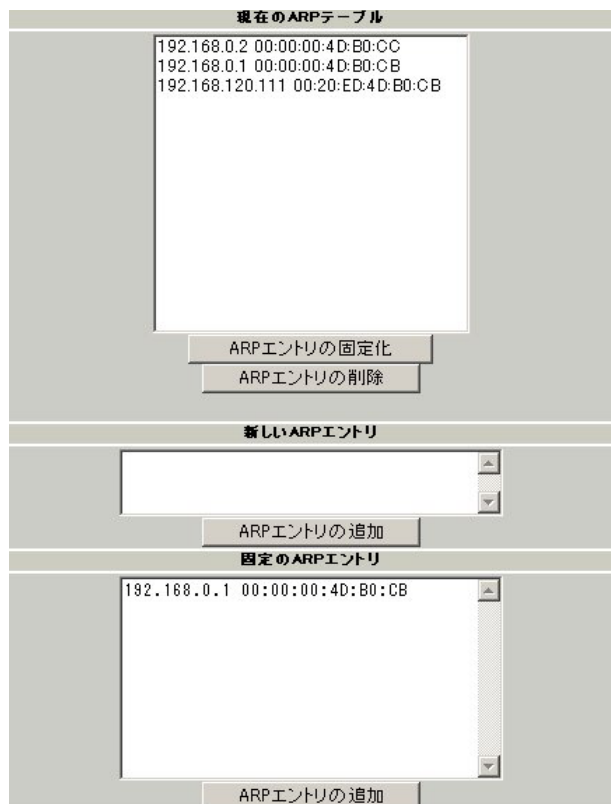
入力が終わりましたら「設定の保存」をクリックして設定完了です。

第5章 インターフェース設定

VI. ARP エントリの設定 (Xr-640L2 のみ)

ARP エントリの設定

「その他の設定」画面中央にある「ARP テーブル」をクリックすると、本装置の ARP テーブルについて設定することができます。



(画面は表示例です)

現在の ARP テーブル

本装置に登録されている ARP テーブルの内容を表示します。

初期状態では動的な ARP エントリが表示されています。

ARP エントリをクリックして「ARP エントリの固定化」ボタンをクリックすると、そのエントリは固定エントリとして登録されます。

ARP エントリをクリックして「ARP エントリの削除」ボタンをクリックすると、そのエントリがテーブルから削除されます。

新しい ARP エントリ

ARP エントリを手動で登録するときは、ここから登録します。

入力欄に IP アドレスと MAC アドレスを入力し「ARP エントリの追加」ボタンをクリックして登録します。

エントリの入力例：

192.168.0.1 00:11:22:33:44:55

固定の ARP エントリ

ARP エントリを固定するときは、ここから登録します。

入力欄に IP アドレスと MAC アドレスを入力し「ARP エントリの追加」ボタンをクリックして登録します。

エントリの入力方法は「新しい ARP エントリ」と同様です。

ARP テーブルの確認

「その他の設定」画面中央で、現在の ARP テーブルの内容を確認できます。

IP address	HW type	Flags	HW address	Mask	Device
192.168.0.1	0x1	0x2	00:20:ED:00:00:00	*	eth0
192.168.0.2	0x1	0x2	00:20:ED:00:00:00	*	eth0

(画面は表示例です)

第 6 章

PPPoE 設定

第6章 PPPoE 設定

1. PPPoE の接続先設定

Web 設定画面「PPP/PPPoE 設定」をクリックします。

はじめに、接続先の設定（ISP のアカウント設定）をおこないます。「接続先設定」1～5のいずれかをクリックします（5つまで設定を保存しておくことができます）。

プロバイダ名	<input type="text"/>
ユーザID	<input type="text"/>
パスワード	<input type="password"/>
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手動で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>
LCPキープアライブ	チェック間隔 <input type="text" value="30"/> 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はP-t-P Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	<input type="text"/> 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効(奨励) MSS値 <input type="text"/> Byte (有効時にMSS値が0の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1492。ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

プロバイダ名

任意で設定名を付けることができます。半角英数字のみ使用できます。

ユーザー ID

プロバイダから指定されたユーザー IDを入力してください。

パスワード

プロバイダから指定された接続パスワードを入力してください。

原則として「'」「(」「)」「|」「¥」等の特殊記号については使用できませんが、入力が必要な場合は該当文字の直前に「¥」を付けて入力してください。

<例>

abc(def)g'h abc¥(def¥)g¥'h

DNSサーバ

特に指定のない場合は「プロバイダから自動割り当て」をチェックします。

指定されている場合は「手動で設定」をチェックして、DNSサーバのアドレスを入力します。

プロバイダから DNS アドレスを自動割り当てされてもそのアドレスを使わない場合は「割り当てられたDNSを使わない」をチェックします。この場合は、LAN側の各ホストにDNSサーバのアドレスをそれぞれ設定しておく必要があります。

LCPキープアライブ

キープアライブのためのLCP echoパケットを送出する間隔を指定します。設定した間隔でLCP echoパケットを3回送出してreplyを検出しなかったときに、本装置がPPPoEセッションをクローズします。「0」を指定すると、LCPキープアライブ機能は無効となります。

Pingによる接続確認

回線によっては、LCP echoを使ったキープアライブを使うことができないことがあります。その場合は、Pingを使ったキープアライブを使用します。「使用するホスト」欄には、Pingの宛先ホストを指定します。空欄にした場合はP-t-P Gateway宛にPingを送出します。**通常は空欄にしておきます。**

第6章 PPPoE 設定

1. PPPoE の接続先設定

IP アドレス

固定 IP アドレスを割り当てられる接続の場合 (unnumbered 接続を含む)、ここにプロバイダから割り当てられた IP アドレスを設定します。IP アドレスを自動的に割り当てられる形態での接続の場合は、ここにはなにも入力しないでください。

MSS 設定

「有効」を選択すると、本装置が MSS 値を自動的に調整します。「MSS 値」は任意に設定できます。最大値は 1452 バイトです。

「0」にすると最大 1414byte に自動調整します。特に必要のない限り、この機能を有効にして、かつ MSS 値を 0 にしておくことを推奨いたします (それ以外では正常にアクセスできなくなる場合があります)。

MSS 設定項目以下は設定しません。

最後に「設定」ボタンをクリックして、設定完了です。設定はすぐに反映されます。

LAN 側の設定 (IP アドレスや DHCP サーバ機能など) を変更する場合は、それぞれの設定ページで変更してください。

第6章 PPPoE 設定

11. PPPoE の接続設定と回線の接続 / 切断

Web 設定画面「PPP/PPPoE 接続設定」をクリックし、右画面の「接続設定」をクリックして、以下の画面から設定します。

XR-410L2

回線状態	回線は接続されていません
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続
RS232C接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

XR-640L2

回線状態	回線は接続されていません
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI64K <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続 <input type="radio"/> スケジューラ接続
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

接続設定

回線状態

現在の回線状態を表示します。

接続先の選択

どの接続先設定を使って接続するかを選択します。

接続ポート

どのポートを使って接続するかを選択します。
PPPoE 接続では、いずれかの Ethernet ポートを選択します。

接続形態

「手動接続」 PPPoE(PPP)の接続 / 切断を手動で切り替えます。
「常時接続」本装置が起動すると自動的に PPPoE 接続を開始します。また PPPoE セッションが切断しても、自動的に再接続します。

「スケジューラ接続」 BRI ポートでの接続をする時に選択できます。

RS232C、RS232C/BRI 接続タイプ

PPPoE 接続では「通常接続」を選択します。

IP マスカレード

PPPoE 接続時に IP マスカレードを有効にするかどうかを選択します。

ステートフルパケットインスペクション

PPPoE 接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、第22章「パケットフィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

デフォルトルートの設定

「有効」を選択すると、PPPoE 接続時に IP アドレスとともに ISP から通知されるデフォルトルートを自動的に設定します。「インタフェース設定」でデフォルトルートが設定されていても、PPPoE 接続で通知されるものに置き換えられます。

「無効」を選択すると、ISP から通知されるデフォルトルートを無視し、自動設定しません。「インタフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。**特に必要のない限り「有効」設定にしておきます。**

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。

「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

第6章 PPPoE 設定

III. 副回線とバックアップ回線

PPPoE 接続では、「副回線接続」設定と「バックアップ回線接続」設定ができます。

[副回線接続]

主回線が何らかの理由で切断されてしまったときに、自動的に副回線設定での接続に切り替えて、接続を維持することができます。また主回線が再度接続されると、自動的に副回線から主回線の接続に戻ります。

主回線から副回線の接続に切り替わっても、NAT 設定やパケットフィルタ設定、ルーティング設定等の全ての設定が、そのまま副回線接続にも引き継がれます。

回線状態の確認は、セッションキープアライブ機能を用います。

[バックアップ回線接続]

副回線接続と同様に、主回線がダウンしたときに、自動的に回線を切り替えて接続を維持しようとします。

ただし副回線接続と異なり、NAT 設定やパケットフィルタ設定等は、主回線用の設定とは別に設定しなければなりません。

これにより、主回線接続時とバックアップ回線接続時とでセキュリティレベルを変更したり、回線品質にあった帯域制御などを個別に設定する、といったことができるようになります。

回線状態の確認は、ping または OSPF を用います。OSPF については、**第12章「ダイナミックルーティング」**をご覧ください。

副回線設定

PPPoE 接続設定画面の「副回線使用時に設定してください」欄で設定します。

XR-410L2

副回線使用時に設定して下さい	
副回線の使用	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
RS232C接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続

XR-640L2

副回線使用時に設定して下さい	
副回線の使用	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続

副回線の使用

副回線を利用する場合は「有効」を選択します。

接続先の選択

副回線接続で利用する接続先設定を選択します。

接続ポート

副回線を接続しているインタフェースを選択します。

RS232C、RS232C/BRI 接続タイプ

RS232C または RS232C/BRI インターフェースを使って副回線接続するときの接続タイプを選択します。「通常」を選択すると常時接続となります。「On-Demand 接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

上記3項目以外の接続設定は、すべてそのまま引き継がれます。

副回線での自動接続機能は、「接続設定」で「常時接続」に設定してある場合のみ有効です。また「接続設定」を変更した場合には、回線を一度切断して再接続した際に変更が反映されます。

第6章 PPPoE 設定

111. 副回線とバックアップ回線

バックアップ回線設定

PPPoE 接続設定画面の「バックアップ回線使用時に設定してください」欄で設定します。

XR-410L2

バックアップ回線使用時に設定して下さい	
バックアップ回線の使用	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input checked="" type="radio"/> RS232C <input type="radio"/> Ether0 <input type="radio"/> Ether1
RS232C接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得
主回線接続確認のインターバル	30 秒
主回線の回線断の確認方法	<input type="radio"/> PING <input checked="" type="radio"/> OSPF <input type="radio"/> IPSEC+PING
Ping使用時の宛先アドレス	<input type="text"/>
Ping使用時の送信元アドレス	<input type="text"/>
Ping fail時のリトライ回数	0
Ping使用時のdevice	<input type="radio"/> 主回線#1 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input checked="" type="radio"/> その他 <input type="text"/>
IPSEC+Ping使用時のIPSECポリシーのNO	<input type="text"/>
復旧時のバックアップ回線の強制切断	<input checked="" type="radio"/> する <input type="radio"/> しない

XR-640L2

バックアップ回線使用時に設定して下さい	
バックアップ回線の使用	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input checked="" type="radio"/> RS232C
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得
主回線接続確認のインターバル	30 秒
主回線の回線断の確認方法	<input type="radio"/> PING <input checked="" type="radio"/> OSPF <input type="radio"/> IPSEC+PING
Ping使用時の宛先アドレス	<input type="text"/>
Ping使用時の送信元アドレス	<input type="text"/>
Ping fail時のリトライ回数	0
Ping使用時のdevice	<input type="radio"/> 主回線#1 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input checked="" type="radio"/> その他 <input type="text"/>
IPSEC+Ping使用時のIPSECポリシーのNO	<input type="text"/>
復旧時のバックアップ回線の強制切断	<input checked="" type="radio"/> する <input type="radio"/> しない

バックアップ回線 の使用

バックアップ回線を利用する場合は「有効」を選択します。

接続先の選択

バックアップ回線接続で利用する接続先設定を選択します。

接続ポート

副回線を接続しているインタフェースを選択します。

RS232C、RS232C/BRI 接続タイプ

RS232CまたはRS232C/BRI インターフェースを使ってバックアップ回線接続するときの接続タイプを選択します。

「通常」を選択すると常時接続となります。

「On-Demand接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

IPマスカレード

バックアップ回線接続時のIPマスカレードの動作を選択します。

ステートフルパケットインスペクション

バックアップ回線接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。SPIを有効にして「DROPしたパケットのLOGを取得」にチェックを入れると、SPIが適用され破棄(DROP)したパケットの情報をsyslogに出力します。SPIが有効のときだけ動作可能です。ログの出力内容については、**第21章「補足：フィルタのログ出力内容について」**をご覧ください。

第6章 PPPoE 設定

III. 副回線とバックアップ回線

主回線接続確認のインターバル

主回線接続の確認のためにパケットを送出する間隔を設定します。30 ~ 999(秒)の間で設定できます。

主回線の回線断の確認方法

主回線の回線断を確認する方法を選択します。

「PING」は ping パケットにより、「OSPF」は OSPF の Hello パケットにより、「IPSEC+PING」は IPSEC 上での ping により、回線の切断を確認します。

Ping 使用時の宛先アドレス

回線断の確認方法で ping を選択したときの、ping パケットのあて先 IP アドレスを設定します。ここから ping の Reply が帰ってこなかった場合に、バックアップ回線接続に切り替わります。

OSPF の場合は、OSPF 設定画面「OSPF 機能設定」の「バックアップ切り替え監視対象 Remote Router-ID 設定」で設定した IP アドレスに対して接続確認をおこないます。

Ping 使用時の送信元アドレス

回線断の確認方法で「IPSEC+PING」を選択したときの、ping パケットの送信元 IP アドレスを設定できます。

Ping fail 時のリトライ回数

ping のリプライがないときに何回リトライするかを指定します。

Ping 使用時の device

ping を使用する際に ping を発行する、本装置のインタフェースを選択します。「その他」を選択して、インタフェース名を直接指定もできます。

IPSEC + PING 使用時の IPSEC ポリシーの NO

IPSEC+PING で回線断を確認するときは必ず、使用する IPsec ポリシーの設定番号を指定します。IPsec 設定については「第 11 章 IPsec 機能」や IPsec 設定ガイドをご覧ください。

復旧時のバックアップ回線の強制切断

主回線の接続が復帰したときに、バックアップ回線を強制切断させるときに「する」を選択します。「しない」を選択すると、主回線の接続が復帰しても、バックアップ回線接続の設定に従ってバックアップ回線の接続を維持します。

このほか、NAT 設定・パケットフィルタ設定・ルーティング設定など、バックアップ回線接続時のための各種設定を別途行なってください。

バックアップ回線接続機能は、「接続設定」で「常時接続」に設定してある場合のみ有効です。また「接続設定」を変更した場合には、回線を一度切断して再接続した際に変更が反映されます。

第6章 PPPoE 設定

IV. PPPoE 特殊オプション設定

地域 IP 網での工事や不具合・ADSL 回線の不安定な状態によって、正常に PPPoE 接続が行えなくなることがあります。

これはユーザー側は PPPoE セッションが確立していないことを検知していても地域 IP 網側はそれを検知していないために、ユーザー側からの新規接続要求を受け入れることができない状態になっていることが原因です。

ここで PPPoE 特殊オプション機能を使うことにより、本装置が PPPoE セッションを確立していないことを検知し、強制的に PADT パケットを地域 IP 網側へ送信して、地域 IP 網側に PPPoE セッションの終了を通知します。

本装置から PADT パケットを送信することで地域 IP 網側の PPPoE セッション情報がクリアされ、PPPoE の再接続性を高めることができます。

PADT = PPPoE Active Discovery Terminate の略。PPPoE セッションが終了したことを示すパケットです。これにより、PADT を受信した側で該当する PPPoE セッションを終了させます。

PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。

PPPoE 特殊オプション
(全回線共通)

- 回線接続時に前回の PPPoE セッションの PADT を強制送す
- 非接続 Session の IPv4 Packet 受信時に PADT を強制送す
- 非接続 Session の LCP-EchoRequest 受信時に PADT を強制送す

回線接続時に前回の PPPoE セッションの PADT を強制送す。

非接続 Session の IPv4 Packet 受信時に PADT を強制送す。

非接続 Session の LCP-EchoRequest 受信時に PADT を強制送す。

の動作について

本装置側が回線断と判断していても網側が回線断と判断していない状況下において、本装置側から強制的に PADT を送ってセッションの終了を網側に認識させます。その後、本装置側から再接続を行います。

の動作について

本装置が LCP キープアラートにより断を検知しても網側が断と判断していない状況下において、網側から

- ・ IPv4 パケット
- ・ LCP エコーリクエスト

のいずれかを本装置が受信すると、本装置が PADT を送ってセッションの終了を網側に認識させます。

その後、本装置側から再接続を行います。

使用したい特殊オプションごとに、チェックボックスにチェックを付けてください。PPPoE 回線接続中に設定を変更したときは、PPPoE を再接続する必要があります。

地域 IP 網の工事後に PPPoE 接続ができなくなってしまう事象を回避するためにも、PPPoE 特殊オプション機能を有効にした上で PPPoE 接続をしていただくことを推奨します。

第7章

RS-232C、RS-232C/BRI ポートを使った接続
(リモートアクセス機能)

1. 本装置とアナログモデム /TAの接続

本装置はRS-232Cポート・ISDN U点ポート（XR-640L2のみ）・ISDN S/T点ポート（BRIポート）（XR-640L2のみ）を搭載しています。これらの各ポートにアナログモデムやターミナルアダプタを接続し、本装置のPPP接続機能を使うことでリモートアクセスが可能となります。

また本装置の副回線接続機能で、PPP接続を副回線として設定しておくこと、リモートアクセスを障害時のバックアップ回線として使うこともできます。

アナログモデム /TAの接続

<XR-410L2>

1 XR-410L2本体背面の「RS-232C」ポートと製品付属の変換アダプタとを、ストレートタイプのLANケーブルで接続してください。

2 変換アダプタのコネクタを、アナログモデムのシリアルポートに接続してください。モデムのコネクタが25ピンタイプの場合は別途、変換コネクタをご用意ください。

3 全ての接続が完了しましたら、モデムの電源を投入してください。

アナログモデム /TAのシリアル接続

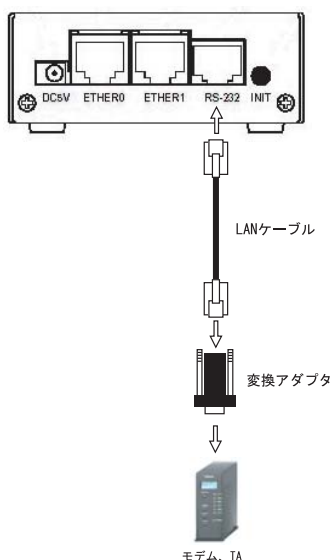
<XR-640L2>

1 XR-640L2の電源をオフにします。

2 本装置の「RS-232C」ポートとモデム /TAのシリアルポートをシリアルケーブルで接続します。シリアルケーブルは別途ご用意ください。

3 全ての接続が完了しましたら、モデムの電源を投入してください。

接続図



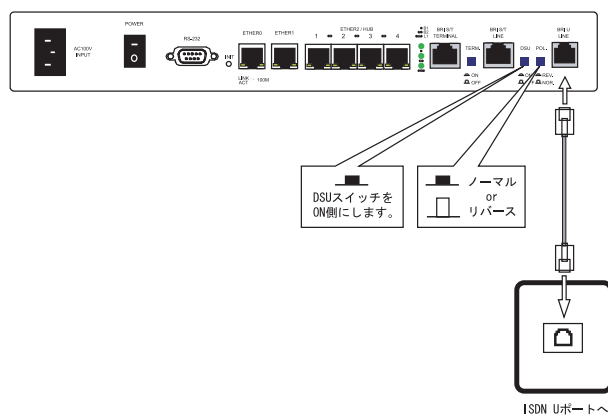
第7章 RS-232C、RS-232C/BRI ポートを使った接続（リモートアクセス機能）

II. BRI ポートを使った TA/DSU との接続(XR-640L2 のみ)

本装置内蔵の DSU を使う場合

- 1 本装置の電源をオフにします。
- 2 ISDN U点ジャックと本装置の「BRI U」ポートをモジュラーケーブルで接続します。モジュラーケーブルは別途ご用意ください。
- 3 本体背面の「DSU」スイッチを「ON」側にします。
- 4 本体背面の「POL.」スイッチを、ISDN 回線の極性に合わせます。
- 5 全ての接続が完了しましたら、本装置と TA の電源を投入してください。

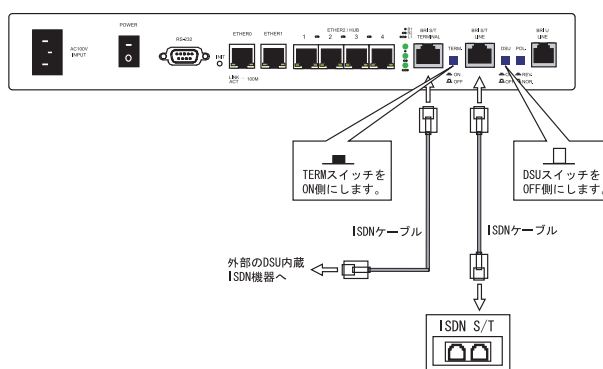
接続図



外付け TA に内蔵の DSU を使う場合

- 1 本装置の電源をオフにします。
- 2 外部の DSU と本装置の「BRI S/T LINE」ポートを ISDN 回線ケーブルで接続します。ISDN ケーブルは別途ご用意ください。
- 3 本体背面の「DSU」スイッチを「OFF」側にします。
- 4 本体背面の「TERM.」スイッチを「ON」側にします。
- 5 別の ISDN 機器を接続する場合は「BRI S/T TERMINAL」ポートと接続してください。

接続図



第7章 RS-232C、RS-232C/BRIポートを使った接続（リモートアクセス機能）

III. リモートアクセス回線の接続先設定

PPP(リモートアクセス)接続の接続先設定を行いません。

Web 設定画面「PPP/PPPoE 設定」をクリックし、接続先の設定をおこないます。右画面上部「接続先設定」1～5のいずれかをクリックします(5つまで設定を保存しておくことができます)。

XR-410L2

プロバイダ名	<input type="text"/>
ユーザID	<input type="text"/>
パスワード	<input type="text"/>
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手動で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>
LCPキープアライブ	チェック間隔 <input type="text" value="30"/> 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はPtP-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	<input type="text"/> 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効(奨励) MSS値 <input type="text" value="0"/> Byte (有効時にMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1452。ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)
PPPシリアル回線使用時に設定して下さい	
電話番号	<input type="text"/>
シリアルDTE	<input type="radio"/> 9600 <input type="radio"/> 19200 <input type="radio"/> 38400 <input type="radio"/> 57600 <input checked="" type="radio"/> 115200 <input type="radio"/> 230400
ダイヤルタイムアウト	<input type="text" value="60"/> 秒
初期化用ATコマンド	<input type="text" value="ATQ0V1"/>
回線種別	<input checked="" type="radio"/> 無指定 <input type="radio"/> トーン <input type="radio"/> パルス
ON-DEMAND接続用切断タイマー	<input type="text" value="180"/> 秒

XR-640L2

プロバイダ名	<input type="text"/>
ユーザID	<input type="text"/>
パスワード	<input type="text"/>
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手動で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>
LCPキープアライブ	チェック間隔 <input type="text" value="30"/> 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はPtP-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	<input type="text"/> 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効(奨励) MSS値 <input type="text" value="0"/> Byte (有効時にMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1452。ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)
BRI/PPPシリアル回線使用時に設定して下さい	
電話番号	<input type="text"/>
ダイヤルタイムアウト	<input type="text" value="60"/> 秒
PPPシリアル回線使用時に設定して下さい	
シリアルDTE	<input type="radio"/> 9600 <input type="radio"/> 19200 <input type="radio"/> 38400 <input type="radio"/> 57600 <input checked="" type="radio"/> 115200 <input type="radio"/> 230400
初期化用ATコマンド	<input type="text" value="ATQ0V1"/>
回線種別	<input checked="" type="radio"/> 無指定 <input type="radio"/> トーン <input type="radio"/> パルス
BRI/PPPシリアル回線使用時に設定して下さい	
ON-DEMAND接続用切断タイマー	<input type="text" value="180"/> 秒

第7章 RS-232C、RS-232C/BR1ポートを使った接続（リモートアクセス機能）

III. リモートアクセス回線の接続先設定

プロバイダ名

接続するプロバイダ名を入力します。任意に入力できますが、「'」「(」「)」「|」「¥」等の特殊文字については使用できません。

ユーザー ID

プロバイダから指定されたユーザー IDを入力してください。

パスワード

プロバイダから指定された接続パスワードを入力してください。

原則として「'」「(」「)」「|」「¥」等の特殊文字については使用できませんが、入力が必要な場合は該当文字の直前に「¥」を付けて入力してください。

<例> abc(def)g'h abc¥(def¥)g¥'h

DNS サーバ

特に指定のない場合は「プロバイダから自動割り当て」をチェックします。指定されている場合は「手動で設定」をチェックして、DNS サーバのアドレスを入力します。

プロバイダから DNS アドレスを自動割り当てされてもそのアドレスを使わない場合は「割り当てられた DNS を使わない」をチェックします。この場合は、LAN 側の各ホストに DNS サーバのアドレスをそれぞれ設定しておく必要があります。

LCP キープアライブ

ping による接続確認

IP アドレス

MSS 設定

上記項目は、リモートアクセス接続の場合は設定のしません。

電話番号

アクセス先の電話番号を入力します。市外局番から入力してください。

ダイヤルタイムアウト

アクセス先にログインするときのタイムアウト時間を設定します。単位は秒です。

シリアル DTE

本装置とモデム /TA 間の DTE 速度を選択します。工場出荷値は 115200bps です。

初期化用 AT コマンド

モデム /TA によっては、発信するとき初期化が必要なものもあります。その際のコマンドをここに入力します。

回線種別

回線のダイヤル方法を選択します。

ON-DEMAND 接続用切断タイマー

PPPoE 接続設定の RS232C、RS232C/BR1 接続タイプを On-Demand 接続にした場合の、自動切断タイマーを設定します。ここで設定した時間を過ぎて無通信状態のときに、接続を切断します。

最後に「設定の保存」ボタンをクリックして、設定完了です。設定はすぐに反映されます。

続いて PPP の接続設定を行いません。

第7章 RS-232C、RS-232C/BRI ポートを使った接続（リモートアクセス機能）

IV. リモートアクセス回線の接続と切断

接続先設定に続いて、リモートアクセス接続のために接続設定をおこないます。

Web 設定画面「PPP/PPPoE 接続設定」をクリックします。右画面の「接続設定」をクリックして、以下の画面から設定します。

XR-410L2

回線状態	回線は接続されていません
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続
RS232C接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

XR-640L2

回線状態	回線は接続されていません
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続 <input type="radio"/> スケジューラ接続
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

接続設定

回線状態

現在の回線状態を表示します。

接続先の選択

どの接続先設定を使って接続するかを選択します。

接続ポート

どのポートを使って接続するかを選択します。リモートアクセス接続では「BRI」または「RS232C」ポートを選択します。

接続形態

「手動接続」リモートアクセスの接続 / 切断を手動で切り替えます。

「常時接続」本装置が起動すると自動的にリモートアクセス接続を開始します。

RS232C、RS232C/BRI 接続タイプ

「通常接続」接続形態設定にあわせて接続します。「On-Demand接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

IPマスカレード

リモートアクセス接続時に IP マスカレードを有効にするかどうかを選択します。unnumbered 接続時以外は、「有効」を選択してください。

ステートフルパケットインスペクション

リモートアクセス接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、第22章「パケットフィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

デフォルトルートの設定

「有効」を選択すると、リモートアクセス接続時に IP アドレスとともに ISP から通知されるデフォルトルートを自動的に設定します。「インタフェース設定」でデフォルトルートが設定されていても、リモートアクセス接続で通知されるものに置き換えられます。

「無効」を選択すると、ISP から通知されるデフォルトルートを無視し、自動設定しません。「インタフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。**特に必要のない限り「有効」設定にしておきます。**

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

第7章 RS-232C、RS-232C/BRI ポートを使った接続（リモートアクセス機能）

V. 回線への自動発信の防止について

Windows OSはNetBIOSで利用する名前からアドレス情報を得るために、自動的にDNSサーバへ問い合わせをかけるようになっています。

そのため「On-Demand接続」機能を使っている場合には、アナログ/ISDN回線に自動接続してしまう問題が起こります。

この意図しない発信を防止するために、本装置ではあらかじめ以下のフィルタリングを設定しています。

(入力フィルタ)

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	eth0	バケット受信時	破棄	tcp				137:139
2	eth0	バケット受信時	破棄	udp				137:139
3	eth0	バケット受信時	破棄	tcp		137		
4	eth0	バケット受信時	破棄	udp		137		

(転送フィルタ)

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	eth0	バケット受信時	破棄	tcp				137:139
2	eth0	バケット受信時	破棄	udp				137:139
3	eth0	バケット受信時	破棄	tcp		137		
4	eth0	バケット受信時	破棄	udp		137		

第7章 RS-232C、RS-232C/BRI ポートを使った接続（リモートアクセス機能）

VI. 副回線接続とバックアップ回線接続

リモートアクセス接続についても、PPPoE 接続と同様に、副回線接続設定とバックアップ回線接続設定が可能です。

設定方法については、**第6章「PPPoE 設定」**をご覧ください。

第8章

複数アカウント同時接続設定

第8章 複数アカウント同時接続設定

複数アカウント同時接続の設定

本装置シリーズは、同時に複数の PPPoE 接続をおこなうことができます。以下のような運用が可能です。

- ・NTT 東西が提供している B フレッツサービスで、インターネットとフレッツ・スクエアに同時に接続する
- ・フレッツ ADSL での接続と、ISDN 接続(リモートアクセス)を同時にこなう

(注)NTT 西日本の提供するフレッツスクエアはNTT 東日本提供のものとはネットワーク構造がことなるため、B フレッツとの同時接続運用はできません。

この接続形態は「マルチ PPPoE セッション」と呼ばれることもあります。

本装置のマルチ PPPoE セッション機能は、主回線 1 セッションと、マルチ接続 3 セッションの合計 4 セッションまでの同時接続をサポートしています。なお、以下の項目については主回線では設定できませんが、マルチ接続(#2 ~ #4)では設定できませんので、ご注意ください。

- ・デフォルトルートとして指定する
- ・副回線を指定する
- ・IPsec を設定する

マルチ PPPoE セッションを利用する場合のルーティングは宛先ネットワークアドレスによって切り替えます。したがって、フレッツ・スクウェアやフレッツ・オフィスのように特定の IP アドレス体系で提供されるサービスをインターネット接続と同時に利用する場合でも、アクセスする PC 側の設定を変更する必要はありません。

ただし、マルチリンクには対応していませんので、帯域を広げる目的で利用することはできません。

また本装置のマルチ PPPoE セッション機能は、PPPoE で接続しているすべてのインターフェースがルーティングの対象となります。したがって、それぞれのインターフェースにステートフルパケットインスペクション、又はフィルタリング設定をしてください。

この機能を利用する場合は以下のステップに従って設定してください。

またマルチ接続側(主回線ではない側)は**フレッツスクエアのように閉じた空間を想定している**ので、工場出荷設定ではステートフルパケットインスペクションは無効となっています。必要に応じてステートフルパケットインスペクション等の設定をして使用してください。

第8章 複数アカウント同時接続設定

複数アカウント同時接続の設定

STEP 1 主接続の接続先設定

1つ目のプロバイダの接続設定をおこないます。
ここで設定した接続を主接続とします。

最初にWeb設定画面「PPP/PPPoE設定」をクリックし、「接続先設定」のいずれかをクリックして設定します。詳しい設定方法は、第6章「PPPoE設定」または第7章「RS-232C、RS-232C/BRIポートを使った接続」をご覧ください。

STEP 2 マルチ接続用の接続先設定

マルチ接続(同時接続)用の接続先設定をおこないます。

Web設定画面「PPP/PPPoE設定」をクリックし、「接続先設定」のいずれかをクリックして設定します。

さらに設定画面最下部にある下図の部分で、マルチ接続を使ってアクセスしたい先のネットワークアドレスとネットマスクを指定します。

マルチPPP/PPPoEセッション回線利用時に指定可能です	
ネットワーク	<input type="text"/> 接続するネットワークを指定して下さい
ネットマスク	<input type="text"/> 上記のネットワークのネットマスクを指定して下さい

例えば

ネットワークアドレスに「172.26.0.0」

ネットマスクに「255.255.0.0」

と指定すると、172.26.0.0/16のネットワークにアクセスするときはマルチ接続を使ってアクセスするようになります。

別途「スタティックルート設定」でマルチ接続を使う経路を登録することもできます。

このどちらも設定しない場合はすべてのアクセスが、主接続を使うこととなります。

最後に「設定の保存」をクリックして接続先設定は完了です。

STEP 3 PPPoE 接続の設定

複数同時接続のための接続設定をおこないます。
主接続とマルチ接続それぞれについて接続設定をおこないます。

「PPP/PPPoE設定」->「接続設定」を開きます。

[主接続用の接続設定]

以下の部分で設定します。

XR-410L2

回線状態	回線は接続されていません
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続
RS232C接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
ステータフルバケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたバケットのLOGを取得
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

XR-640L2

回線状態	回線は接続されていません
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(G4K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続 <input type="radio"/> スケジューラ接続
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
ステータフルバケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたバケットのLOGを取得
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

接続先の選択

主接続用の設定を選択します。

接続先ポート

主接続で使用する、本装置のインタフェースを選択します。

接続形態

常時接続の回線を利用する場合は通常、「常時接続」を選択します。手動接続を選択した場合は、同画面最下部のボタンで接続・切断の操作をおこなってください。

第8章 複数アカウント同時接続設定

複数アカウント同時接続の設定

RS232C、RS232C/BRI 接続タイプ

主接続が PPPoE 接続の場合は、「通常」を選択します。

主接続が RS232C または RS232C/BRI インターフェースで接続する場合は、「通常」を選択すると、接続形態に合わせて接続します。

「On-Demand 接続」を選択すると、オンデマンド接続となります。オンデマンド接続における接続タイマーは「接続先設定」で設定します。

IP マスカレード

通常は「有効」を選択します。

LAN 側をグローバル IP で運用している場合は「無効」を選択します。

ステートフルパケットインスペクション

任意で選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。

ログの出力内容については、第 22 章「パケット i フィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

デフォルトルート

「有効」を選択します。

続いてマルチ接続用の接続設定をおこないます。

[マルチ接続用の設定]

次の画面で設定します。

XR-410L2

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい

マルチ接続 #2	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
RS232C接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得

マルチ接続 #3	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
RS232C接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得

マルチ接続 #4	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
RS232C接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得

XR-640L2

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい

マルチ接続 #2	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得

マルチ接続 #3	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得

マルチ接続 #4	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得

第 8 章 複数アカウント同時接続設定

複数アカウント同時接続の設定

マルチ接続 #2 ~ #4

マルチ PPPoE セッション用の回線として使うものに「有効」を選択します。

接続先の選択

マルチ接続用の接続先設定を選択します。

接続ポート

マルチ接続で使用する、本装置のインタフェースを選択します。B フレッツ回線で複数の同時接続をおこなう場合は、主接続の設定と同じインタフェースを選択します。

RS232C、RS232C/BRI 接続タイプ

RS232C または BRI インターフェースを使って複数アカウント同時接続するときの接続タイプを選択します。

「通常」を選択すると常時接続となります。

「On-Demand 接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

IP マスカレード

任意で選択します。通常は「有効」にします。

ステートフルパケットインスペクション

任意で選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。

ログの出力内容については、第 22 章「パケットフィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

マルチ接続設定は 3 つまで設定可能です(最大 4 セッションの同時接続が可能)。

STEP 4 PPPoE 接続の開始

すべて設定した後、「接続」をクリックして PPPoE 接続を開始します。

PPPoE の接続状態は、接続設定画面上部の「回線状態」に赤字で表示されます。

接続に成功した場合：

主回線で接続しています。

マルチセッション回線 1 で接続しています。

接続できていない場合：

主回線で接続を試みています。

マルチセッション回線 1 で接続を試みています。

など表示されます。

PPPoE 接続に成功したあとは、STEP 2 の設定、「スタティックルート設定」、もしくは「ソースルート設定」にしたがって接続を振り分けられてアクセスできます。

複数アカウント同時接続時の注意点

通常の ISP とフレッツスクエアへの同時接続をするには、本装置の「DNS サーバ機能」を「有効」にし、各 PC の DNS サーバ設定を本装置の IP アドレスに設定してください。

本装置に名前解決要求をリレーさせないと、同時接続ができません。

第9章

各種サービスの設定

第9章 各種サービスの設定

各種サービス設定

本装置の設定画面「各種サービスの設定」をクリックすると、以下の画面が表示されます。

サービスの起動・停止・設定

現在のサービス稼働状況を反映しています
各種設定はサービス項目名をクリックして下さい

DNSキャッシュ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい		停止中
L2TPv3	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい		停止中

動作変更

ここでは

- ・各種サービスの設定
- ・各種サービスの起動と停止
- ・サービスの稼働状況の確認

をおこないます。

サービスの設定

それぞれのサービスの設定をおこなうには、画面中の各サービス名をクリックしてください。そのサービスの設定画面が表示されます。

それぞれの設定方法については、各機能についてのページを参照してください。

DNS キャッシュ

IPsec サーバ

ダイナミックルーティング

L2TPv3

SYSLOG サービス

SNMP サービス

NTP サービス

アクセスサーバ

サービスの起動と停止

それぞれのサービスを起動・停止するときは、それぞれのサービス項目で「停止」か「起動」を選択し、「動作変更」ボタンをクリックしてください。これにより、サービスの稼働状態が変更されます。またサービスの稼働状態は、各項目ごとに表示されます。

第 10 章

DNS リレー / キャッシュ機能

第10章 DNS リレー / キャッシュ機能

DNS 機能の設定

DNS リレー機能

本装置では LAN 内の各ホストの DNS サーバを本装置に指定して、ISP から指定された DNS サーバや任意の DNS サーバへリレーすることができます。

DNS リレー機能を使う場合は、各種サービス設定画面の「DNS キャッシュ」を起動させてください。

任意の DNS を指定する場合は、Web 設定画面「各種サービスの設定」->「DNS キャッシュ」をクリックして以下の画面で設定します。

DNSキャッシュの設定

プライマリDNS IPアドレス	<input type="text"/>
セカンダリDNS IPアドレス	<input type="text"/>
root server	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない

プライマリ DNS IPアドレス

セカンダリ DNS IPアドレス

任意の DNS サーバの IP アドレスを入力してください。ISP から指定された DNS サーバへリレーする場合は本設定の必要はありません。

root server

上記プライマリ DNS IPアドレス、セカンダリ DNS IPアドレスで設定した DNS サーバへの問い合わせに失敗した場合や、DNS サーバの指定が無い場合に、ルートサーバへの問い合わせを行うかどうかを指定します。

設定後に「設定の保存」をクリックして設定完了です。

DNS キャッシュ機能

また「DNS キャッシュ」を起動した場合、本装置がリレーして名前解決された情報は、自動的にキャッシュされます。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを起動させてください。また設定を変更した場合は、サービスの再起動（「停止」「起動」）をおこなってください。

第 11 章

IPsec 機能

1. 本装置のIPsec機能について

鍵交換について

IKEを使用しています。IKEフェーズ1ではメインモード、アグレッシブモードの両方をサポートしています。フェーズ2ではクイックモードをサポートしています。

固定IPアドレス同士の接続はメインモード、固定IPアドレスと動的IPアドレスの接続はアグレッシブモードで設定してください。

認証方式について

本装置は「共通鍵方式」「RSA公開鍵方式」「X.509」による認証に対応しています。

ただしアグレッシブモードは「共通鍵方式」にのみ対応、「X.509」はメインモードにのみ対応しています。

暗号化アルゴリズム

シングルDESとトリプルDES、AES128bitをサポートしています。暗号化はハードウェア処理で行ないます。

ハッシュアルゴリズム

SHA1とMD-5を使用しています。

認証ヘッダ

本装置はESPの認証機能を利用しています。AHでの認証はサポートしていません。

DH鍵共有アルゴリズムで使用するグループgroup1、group2、group5をサポートしています。

IPsec使用時の通信可能対地数

128拠点とIPsec接続が可能です。

IPsecとインターネット接続

IPsec通信をおこなっている場合でも、その設定以外のネットワークへは、通常通りインターネットアクセスが可能です。

NATトラバーサル機能に対応しています。

他の機器との接続実績について

- FutureNet XRシリーズ
- FutureNet XR VPN Clinet (SSH Sentinel)
- Linuxサーバ (FreeS/WAN)

11. IPsec 設定の流れ

PreShared(共通鍵)方式での IPsec 通信

STEP 1 共通鍵の決定

IPsec 通信をおこなうホスト同士の認証と、データの暗号化・復号化で使う共通秘密鍵の生成に必要な鍵を任意で決定します。IPsec 通信をおこなう双方で共通の鍵を使います。半角英数字であればどんな文字列でもかまいません。

STEP 2 共通鍵の交換

決定した共通鍵は、第三者に知られないように十分注意して交換してください。共通鍵が第三者に渡ると、その鍵を利用して不正な IPsec 接続が確立されるおそれがあります。

STEP 3 本装置側の設定

自分側の本装置の設定をおこないます。

STEP 4 IKE/ISAKMP ポリシーの設定

データの暗号化と復号に必要な共通の秘密鍵を交換するための IKE/ISAKMP ポリシー設定をおこないます。ここで共通鍵の設定、IKE の動作設定、相手側の IPsec ゲートウェイの設定や IKE の有効期間の設定をおこないます。

STEP 5 IPsec ポリシー設定

IPsec 通信を行う相手側セグメントの設定をおこないます。このとき、どの IKE 設定を使用するかを指定します。

STEP 6 IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7 IPsec 接続の確認

IPsec 起動後に、正常に IPsec 通信ができるかどうかを確認します。「情報表示」画面でのインターフェースとルーティングテーブル、ログで確認します。

RSA(公開鍵)方式での IPsec 通信

STEP 1 公開鍵・暗号鍵の生成

IPsec 通信をおこなうホスト同士の認証とデータの暗号化に必要な公開鍵と、復号化に必要な秘密鍵を生成します。公開鍵は IPsec の通信相手に渡しておきます。鍵の長さを指定するだけで、自動的に生成されます。

STEP 2 公開鍵の交換

鍵を生成すると、設定画面上では公開鍵が表示されます。この鍵を IPsec 通信をおこなう相手側に通知してください。また同様に、相手側が生成した公開鍵を入手してください。公開鍵は第三者に知られても問題ありません。

STEP 3 本装置側の設定

自分側の本装置の設定をおこないます。

STEP 4 IKE/ISAKMP ポリシーの設定

データの暗号化と復号に必要な共通の秘密鍵を交換するための IKE/ISAKMP ポリシーの設定をおこないます。ここで公開鍵の設定、IKE の動作設定、相手側の IPsec ゲートウェイの設定や IKE の有効期間の設定をおこないます。

STEP 5 IPsec ポリシー設定

IPsec 通信をおこなう相手側セグメントの設定をおこないます。このとき、どの IKE 設定を使用するかを指定します。

STEP 6 IPsec の起動

本装置の IPsec 機能を起動します。

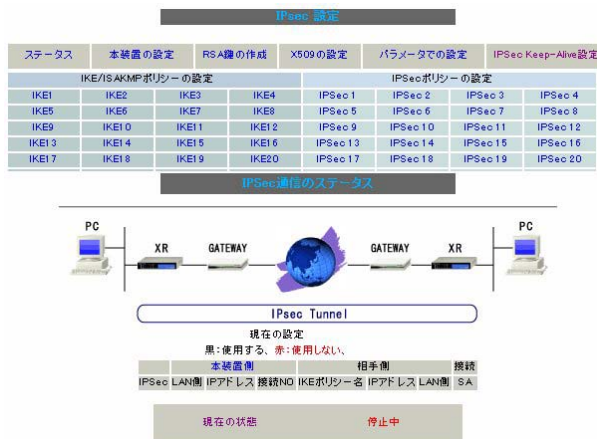
STEP 7 IPsec 接続の確認

IPsec 起動後に、正常に IPsec 通信ができるかどうかを確認します。「情報表示」画面でのインターフェースとルーティングテーブル、ログで確認します。

III. IPsec設定

STEP 0 設定画面を開く

- 1 Web設定画面にログインします。
- 2 「各種サービスの設定」 「IPsecサーバ」をクリックして、以下の画面から設定します。



(画面は表示例です)

- 鍵の作成
- X.509設定
- IPsec Keep-Alive設定
- 本装置の設定
- IKE/ISAKMPポリシーの設定
- IPsecポリシーの設定
- ステータスの確認
- パラメータでの設定

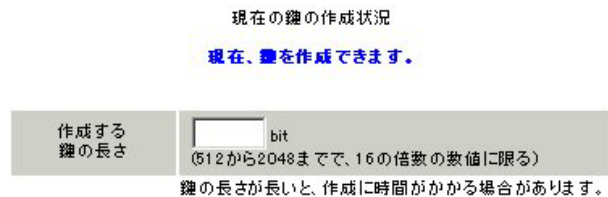
IPsecに関する設定・確認は、全てこの設定画面からおこなえます。

STEP 1,2 鍵の作成・交換

RSA公開鍵方式を用いてIPsec通信をおこなう場合は、最初に鍵を自動生成します。

PSK共通鍵方式を用いてIPsec通信をおこなう場合は、「鍵の作成」は不要です。相手側と任意で共通鍵を決定し、交換しておきます。

- 1 IPsec設定画面上部の「RSA鍵の作成」をクリックして、以下の画面を開きます。



- 2 作成する鍵の長さを指定して「公開鍵の作成」をクリックします。
鍵の長さは512bitから2048bitまでで、16の倍数となる数値が指定可能です。
現在の鍵の作成状況が「鍵を作成できます」の表示の時に限り、作成可能です。

- 3 鍵を生成します。「鍵を作成しました。」のメッセージが表示されると、鍵の生成が完了です。生成した鍵は、後述する「本装置側の設定」に自動的に反映されます。
またこの鍵は公開鍵となりますので、相手側にも通知してください。

第11章 IPsec機能

III. IPsec設定

STEP 3 本装置側の設定をおこなう

IPsec設定画面上部の「本装置の設定」をクリックして設定します。

[本装置の設定]

「本装置の設定」をクリックします。

XR-410L2

MTUの設定	
主回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
マルチ#2回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
マルチ#3回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
マルチ#4回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
バックアップ回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
Ether 0ポート使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
Ether 1ポート使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>

NAT Traversalの設定	
NAT Traversal	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
Virtual Private設定	<input type="text"/>

鍵の表示	
本装置のRSA鍵 (PSKを使用する場合は必要ありません)	<input type="text"/>

XR-640L2

MTUの設定	
主回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
マルチ#2回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
マルチ#3回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
マルチ#4回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
バックアップ回線使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
Ether 0ポート使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
Ether 1ポート使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>
Ether 2ポート使用時のipsecインターフェイスのMTU値	<input type="text" value="1500"/>

NAT Traversalの設定	
NAT Traversal	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
Virtual Private設定	<input type="text"/>
Virtual Private設定2	<input type="text"/>
Virtual Private設定3	<input type="text"/>
Virtual Private設定4	<input type="text"/>

鍵の表示	
本装置のRSA鍵 (PSKを使用する場合は必要ありません)	<input type="text"/>

MTUの設定

IPsec接続時のMTU値を設定します。各インターフェースごとに設定できます。通常は初期設定のままでかまいません。

NAT Traversalの設定

NATトラバーサル機能を使うことで、NAT環境下にあるクライアントとIPsec通信を行えるようになります。

「NAT Traversal」

NATトラバーサル機能を使うかどうかを選択します。

「Virtual Private設定」

接続相手のクライアントが属しているネットワークと同じネットワークアドレスを入力します。以下のような書式で入力してください。

%v4:<ネットワーク>/<マスクビット値>

本装置をNATトラバーサルのホストとして使用する場合に設定します。クライアントとして使用する場合は空欄のままにします。

鍵の表示

RSA鍵の作成をおこなった場合ここに、作成したRSA鍵の公開鍵が表示されます。

PSK方式やX.509電子証明を使う場合はなにも表示されません。

[本装置側の設定]

「本装置側の設定」の1～8のいずれかをクリックします。ここで本装置自身のIPアドレスやインターフェースIDを設定します。

インターフェースのIPアドレス	<input type="text"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text" value="0x.centurysys"/> (例: 0x.centurysys)

インターフェースのIPアドレス

[固定アドレスの場合]

本装置に設定されているIPアドレスをそのまま入力します。

[動的アドレスの場合]

PPP/PPPoE主回線接続の場合は「%ppp0」と入力します。Ether0(Ether1)ポートで接続している場合は「%eth0(%eth1)」と入力します。

III. IPsec 設定

上位ルータの IP アドレス
空欄にしておきます。

インターフェースの ID
本装置への IP アドレスの割り当てが動的割り当て
の場合(agressive モードで接続する場合)は、イン
タフェースの ID を設定しません(必須)。

<入力形式> @ <任意の文字列>

<入力例> @centurysystems

(@の後は、任意の文字列でかまいません。)

固定アドレスの場合は、設定を省略できます。省
略した場合は、自動的に「インターフェースの IP
アドレス」を ID として使用します。

最後に「設定の保存」をクリックして設定完了で
す。続いて IKE/ISAKMP ポリシーの設定をおこな
います。

STEP 4 IKE/ISAKMP ポリシーの設定

IPsec 設定画面上部の「IKE/ISAKMP ポリシーの設
定」1 ~ 128 のいずれかをクリックして、以下の画
面から設定します。

IKE/ISAKMPポリシー名	<input type="text"/>
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	<input type="text"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text"/> (例: @x.centurysys)
モードの設定	main モード
transformの設定	1番目 <input type="text"/> すべてを送信する
	2番目 <input type="text"/> 使用しない
	3番目 <input type="text"/> 使用しない
	4番目 <input type="text"/> 使用しない
IKEのライフタイム	3600 秒 (1081 ~ 28800秒まで)
鍵の設定	<input type="radio"/> PSKを使用する <input checked="" type="radio"/> RSAを使用する <small>(X509を使用する場合は RSAに設定してください)</small>
X509の設定	
接続先の証明書の設定	<small>(X509を使用しない場合は 必要ありません)</small>

IKE/ISAKMP ポリシー名
設定名を任意で設定します。(省略可)

接続する本装置側の設定
接続で使用する「本装置側の設定」を選択します。

インターフェースの IP アドレス
相手側 IPsec 装置の IP アドレスを設定します。相
手側装置への IP アドレスの割り当てが固定か動的
かで、入力が異なります。

[相手側装置が固定アドレスの場合]

IP アドレスをそのまま入力します。

[相手側装置が動的アドレスの場合]

「0.0.0.0」を入力します。

III. IPsec 設定

上位ルータの IP アドレス
空欄にしておきます。

インタフェースの ID
対向側装置への IP アドレスの割り当てが動的割り
当ての場合に限り、IP アドレスの代わりに ID を設
定します。

<入力形式> @ <任意の文字列>
<入力例> @centurysystems
(@の後は、任意の文字列でかまいません)

**対向側装置への割り当てが固定アドレスの場合は
設定の必要はありません。**

モードの設定
IKE のフェーズ1 モードを「main モード」と
「aggressive モード」のどちらかから選択します。

transform の選択
ISAKMP SA の折衝で必要な暗号化アルゴリズム等の
組み合わせを選択します。本装置は、以下のもの
の組み合わせが選択できます。

- ・DH group 値 (group1、group2、group5)
- ・暗号化アルゴリズム (des、3des、aes)
- ・認証アルゴリズム (md5、sha1)

「aggressive モード」の場合、接続相手の機器に合
わせて transform を選択する必要があります。
aggressive モードでは transform を1つだけ選択し
てください(2番目～4番目は「使用しない」を選
択しておきます)。

「main モード」の場合も transform を選択できま
すが、基本的には「すべてを送信する」の設定で構
いません。

IKE のライフタイム

ISAKMP SA のライフタイムを設定します。ISAKMP
SA のライフタイムとは、双方のホスト認証と秘密
鍵を交換するトンネルの有効期間のことです。
1081 ~ 28800 秒の間で設定します。

鍵の設定

[PSK 方式の場合]

「PSK を使用する」にチェックして、相手側と任意
に決定した共通鍵を入力してください。
半角英数字のみ使用可能です。最大 2047 文字まで
設定できます。

[RSA 公開鍵方式の場合]

「RSA を使用する」にチェックして、相手側から通
知された公開鍵を入力してください。「X.509」設
定の場合も「RSA を使用する」にチェックします。

X509 の設定

「X.509」設定で IPsec 通信をおこなう場合は、相
手側装置に対して発行されたデジタル証明書をテ
キストボックス内に貼り付けます。

最後に「設定の保存」をクリックして設定完了で
す。

続いて、IPsec ポリシーの設定をおこないます。

III. IPsec 設定

STEP 5 IPsec ポリシーの設定

IPsec 設定画面上部の「IPsec ポリシーの設定」のいずれかをクリックして、以下の画面から設定します。

<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない <input type="radio"/> Responderとして使用する <input type="radio"/> On-Demandで使用する	
使用するIKEポリシー名の選択	----- ▾
本装置側のLAN側のネットワークアドレス	<input type="text"/> (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	<input type="text"/> (例:192.168.0.0/24)
PH2のTransformの選択	すべてを送信する ▾
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択 (PFS使用時に有効)	指定しない ▾
SAのライフタイム	<input type="text"/> 秒 (1081 ~ 86400秒まで)
DISTANCE	<input type="text"/> (1 ~ 255まで)

32 個以上の IPsec ポリシーを設定する場合は、画面上部の「パラメータの設定」をクリックして、パラメータでの設定を行なってください。

最初に IPsec の起動状態を選択します。

「使用する」は initiator にも responder にもなります。

「使用しない」は、その IPsec ポリシーを使用しません。

「Responder として使用する」はサービス起動時や起動中の IPsec ポリシー追加時に、responder として IPsec 接続を待ちます。本装置が固定 IP アドレス設定で接続相手が動的 IP アドレス設定の場合に選択します。

また、後述する IPsec KeepAlive 機能において、backupSA として使用する場合もこの選択にしてください。メイン側の IPsecSA で障害を検知した場合に、Initiator として接続を開始します。

「On-Demand で使用する」は、IPsec をオンデマンド接続します。切断タイマーは SA のライフタイムとなります。

使用する IKE ポリシー名の選択

STEP 4 で設定した IKE/ISAKMP ポリシーのうち、どのポリシーを使うかを選択します。

本装置側の LAN 側のネットワークアドレス
自分側の本装置に接続している LAN のネットワークアドレスを入力します。ネットワークアドレス / マスクビット値の形式で入力します。

[入力例] **192.168.0.0/24**

相手側の LAN 側のネットワークアドレス
相手側の IPsec 装置に接続されている LAN のネットワークアドレスを入力します。ネットワークアドレス / マスクビット値の形式で入力します。設定の要領は「本装置側の LAN 側のネットワークアドレス」と同様です。

また NAT Traversal 機能を使用している場合に限っては、"**vhost:%priv**" と設定します。

PH2 の Transform の選択

IPsec SA の折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。

- ・暗号化アルゴリズム (des, 3des, aes)
- ・認証アルゴリズム (md5, sha1)

通常は「すべてを送信する」の選択で構いません。

PFS

PFS(Perfect Forward Secrecy) を「使用する」か「使用しない」かを選択します。

PFS とは、パケットを暗号化している秘密鍵が解読されても、その鍵ではその後に生成された鍵を解読できないようにするものです。装置への負荷が増加しますが、より高いセキュリティを保つためには PFS を使用することを推奨します。

DH Group の選択 (PFS 使用時に有効)

「PFS を使用する」場合に使用する DH group を選択します。ただし「指定しない」を選択しても構いません。その場合は、PH1 の結果、選択された DH Group 条件と同じ DH Group 条件を接続相手に送ります。

III. IPsec 設定

SA のライフタイム

IPsec SA の有効期間を設定します。IPsecSA とはデータを暗号化して通信するためのトラフィックのことです。1081 ~ 86400 秒の間で設定します。

DISTANCE

IPsec ルートの DISTANCE 値を設定します。同じ内容でかつ DISTANCE 値の小さい IPsec ポリシーが起動したときには、DISTANCE 値の大きいポリシーは自動的に切断されます。

なお、本設定は省略可能です。省略した場合は「1」として扱います。

IPsec ルートを OSPF で再配信する場合は、「OSPF 機能設定」の「static ルートの再配信」を「有効」にする必要があります。

最後に「設定の保存」をクリックして設定完了です。続いて、IPsec 機能の起動をおこないます。

[IPsec 通信時の Ethernet ポート設定について]

IPsec 設定をおこなう場合は、Ethernet ポートの設定に注意してください。

IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが本装置の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。

たとえば、IPsec 通信をおこなう相手側のネットワークが 192.168.1.0/24 の設定で、且つ、本装置の Ether1 ポートに 192.168.1.254 が設定されていると、正常に IPsec 通信がおこなえません。

このような場合は本装置の Ethernet ポートの IP アドレスを、別のネットワークに属する IP アドレスに設定し直してください。

STEP 6 IPsec 機能を起動する

「各種サービスの設定」をクリックして、以下の画面を開きます。

DNSサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい		停止中
I2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	動作変更
SYNLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
SNMPサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	動作変更
NTPサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	動作変更
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい		停止中

動作状態の制御

IPsec サーバ項目、「起動」にチェックして「動作変更」をクリックすると、IPsec 機能が起動します。以降は、本装置を起動するたびに IPsec 機能が自動起動します。

IPsec 機能を止める場合は「停止」にチェックして「動作変更」をクリックしてください。

IPsec 機能を起動した後は、現在のサービス稼働状況が「動作中」と表示されます。

III. IPsec 設定

STEP 7 IPsec 接続を確認する

IPsec が正常に接続したかどうかは、「システム設定」の「ログの表示」でログを確認します。

ログの中で、以下のメッセージが含まれているかを確認してください（ログメッセージは「メインモード」で通信した場合の表示例です）

```
Aug 1 12:00:20 localhost ipsec_plutorun:
004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP SA
established . . .(1)
```

及び

```
Aug 1 12:00:20 localhost ipsec_plutorun:
004 "xripsec1" #2: STATE_QUICK_I2: sent Q12,
IPsec SA established . . .(2)
```

上記 2 つのメッセージが表示されていれば、IPsec が正常に接続されています。

(1)のメッセージは、IKE 鍵交換が正常に完了し、ISAKMP SA が確立したことを示しています。

(2)のメッセージは、IPsec SA が正常に確立したことを示しています。

STEP 8 IPsec ステータス確認の確認

IPsec の簡単なステータスを確認できます。「各種サービスの設定」「IPsec サーバ」「ステータス」をクリックして、画面を開きます。

The screenshot shows the 'IPsec 設定' (IPsec Settings) page. It features a table with columns for 'ステータス' (Status), '本装置の設定' (Local Device Settings), 'RSA鍵の作成' (RSA Key Creation), 'X509の設定' (X509 Settings), 'パラメータでの設定' (Settings by Parameter), and 'IPsec Keep-Alive設定' (IPsec Keep-Alive Settings). The table lists IKE/ISAKMP policies (IKE1-IKE18) and IPsec policies (IPSec 1-IPSec 20). Below the table is a diagram titled 'IPsec 通信のステータス' (IPsec Communication Status) showing two PCs connected via XR routers and gateways through an IPsec Tunnel. A legend indicates '黒: 使用する、赤: 使用しない' (Black: Use, Red: Do not use) for '本装置側' (Local Device Side) and '相手側' (Peer Side) for '接続' (Connection). The current status is shown as '現在の状態' (Current Status) and '停止中' (Stopped).

それぞれの対向側設定でおこなった内容から、本装置・相手側の LAN アドレス・IP アドレス・上位ルータアドレスの一覧や、現在の動作状況が表示されます。

「現在の状態」リンクをクリックすると、現在の IPsec の状況が表示されます。

また、それぞれの設定番号をクリックすると、設定画面に移ることができます。

第11章 IPsec 機能

IV. IPsec Keep-Alive 設定

IPsec Keep-Alive 機能は、IPsec トンネルの障害を検出する機能です。

指定した宛先へ IPsec トンネル経由で ping パケットを発行して応答がない場合に IPsec トンネルに障害が発生したと判断し、その IPsec トンネルを自動的に削除します。不要な IPsec トンネルを自動的に削除することで、IPsec の再接続性を高めます。

IPsec 設定画面上部の「IPsecKeep-Alive 設定」をクリックして設定します。

Policy No.	enable	source address	destination address	interval(sec)	watch count	delay(sec)	flag	slave SA	remove?
1	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>			30	5	180	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

enable

設定を有効にする時にチェックします。IPsec Keep-Alive 機能を使いたい IPsec ポリシーと同じ番号にチェックを入れます。

source address

IPsec 通信を行う際の、XR の LAN 側インターフェースの IP アドレスを入力します。

destination address

IPsec 通信を行う際の、XR の対向側装置の LAN 側のインターフェースの IP アドレスを入力します。

interval(sec)

watch count

ping を発行する間隔を設定します。

「『interval(sec)』間に『watch count』回 ping を発行する」という設定になります。

delay(sec)

IPsec が起動してから ping を発行するまでの待ち時間を設定します。IPsec が確立するまでの時間を考慮して設定します。

flag

チェックを入れると、delay 後に ping を発行して、ping が失敗したら即座に指定された IPsec トンネルの削除、再折衝を開始します。また Keep-Alive によって SA 削除後は、毎回 delay 時間待ってから Keep-Alive が開始されます。

チェックをはずすと、delay 後に最初に ping が成功 (IPsec が確立) し、その後に ping が失敗してはじめて指定された IPsec トンネルの削除、再折衝を開始します。最初から ping に失敗してしまうときは、IPsec SA を削除しません。また delay は初回のみ発生します。

通常はチェックを外した設定で運用してください。

backup SA

ここに IPsec ポリシーの設定番号を指定しておくと、IPsec Keep-Alive 機能で IPsec トンネルを削除した時に、Slave SA で指定した IPsec ポリシー設定を起動させます。

注) backup SA として使用する IPsec ポリシーの起動状態は必ず「Responder として使用する」を選択してください。

IV. IPsec Keep-Alive 設定

複数のポリシーを指定することもできます。その際は、"_" でポリシー番号を区切って設定します。これにより、指定した複数の IPsec ポリシーがネゴシエーションを開始します。

<入力例>

1_2_3

またここに、以下のような設定もできます。

ike<n> <n> は 1-128 の整数

この設定の場合、バックアップ SA 動作時には、「IPsec ポリシー設定の <n> 番」が使用しているものと同じ IKE/ISAKMP ポリシー設定を使う他の IPsec ポリシーが、同時にネゴシエーションをおこないます。

<例>

使用する IKE ポリシー IKE/ISAKMP2 番

IPsec ポリシー IPsec2 IPsec4 IPsec5

上図の設定で backupSA に「ike2」と設定すると、「IPsec2」が使用している IKE/ISAKMP ポリシー設定 2 番を使う、他の IPsec ポリシー (IPsec4 と IPsec5) も同時にネゴシエーションを開始します。

remove

設定を削除したいときにチェックします。

最後に「設定の保存」ボタンをクリックします。

設定番号について

IPsec Keep-Alive 機能を使う際は、監視する IPsec のポリシー No. と Keepalive の No. は一致させてください。

IPsec トンネルの障害を検知する条件

IPsec Keep-Alive 機能によって障害を検知するのは、「interval/watch count」に従って ping を発行して、一度も応答がなかったときです。このとき本装置は、ping の応答がなかった IPsec トンネルを自動的に削除します。反対に一度でも応答があったときは、本装置は IPsec トンネルを保持します。

動的アドレスの場合の本機能の利用について

拠点側に動的 IP アドレスを用いた構成で、センター側からの通信があるようなケースについては SA の不一致が起こりうるため、IPsec Keep-Alive 機能を動作させることを推奨します。

第 11 章 IPsec 機能

V. 「X.509 デジタル証明書」を用いた電子認証

本装置は X.509 デジタル証明書を用いた電子認証方式に対応しています。

ただし本装置は証明書署名要求の発行や証明書の発行ができませんので、あらかじめ CA 局から証明書の発行を受けておく必要があります。

電子証明の仕組みや証明書発行の詳しい手順につきましては関連書籍等をご参考ください。

情報処理振興事業協会セキュリティセンター
<http://www.ipa.go.jp/security/pki/>

設定は、IPsec 設定画面内の「X.509 の設定」から行えます。

[X.509 の設定]

「X.509 の設定」画面 「X.509 の設定」を開きます。

X509 の設定	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
設定した接続先の証明書のみを使用する	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
証明書のパスワード	<input type="password"/>

X509 の設定

X.509 の使用 / 不使用を選択します。

設定した接続先の証明書のみを使用する

「IKE/ISAKMP の設定」で X.509 の設定を行った接続先のみ X.509 を使用します。

証明書のパスワード

証明書のパスワードを入力します。

[CA の設定]

ここでは、CA 局自身のデジタル証明書の内容をコピーして貼り付けます。

[本装置側の証明書の設定]

ここでは、本装置に対して発行されたデジタル証明書の内容をコピーして貼り付けます。

[本装置側の鍵の設定]

ここではデジタル証明書と同時に発行された、本装置の秘密鍵の内容をコピーして貼り付けます。

[失効リストの設定]

失効リストを作成している場合は、その内容をコピーして貼り付けます。

以上で X.509 の設定は完了です。

第11章 IPsec機能

VI. IPsec通信時のパケットフィルタ設定

ステートフルパケットインスペクション機能を使っていたり、パケットフィルタの設定によっては、IPsec通信ができない場合があります。このような場合はIPsec通信でのデータをやりとりできるように、パケットフィルタの設定を追加する必要があります。

IPsecでは、以下の2種類のプロトコル・ポートを使用します。

- ・プロトコル「UDP」のポート「500」番
->IKE(IPsecの鍵交換)のトラフィックに必要です
- ・プロトコル「ESP」
->ESP(暗号化ペイロード)のトラフィックに必要です

これらのパケットを通せるように、「入力フィルタ」に設定を追加してください。なお、「ESP」については、ポート番号の指定はしません。

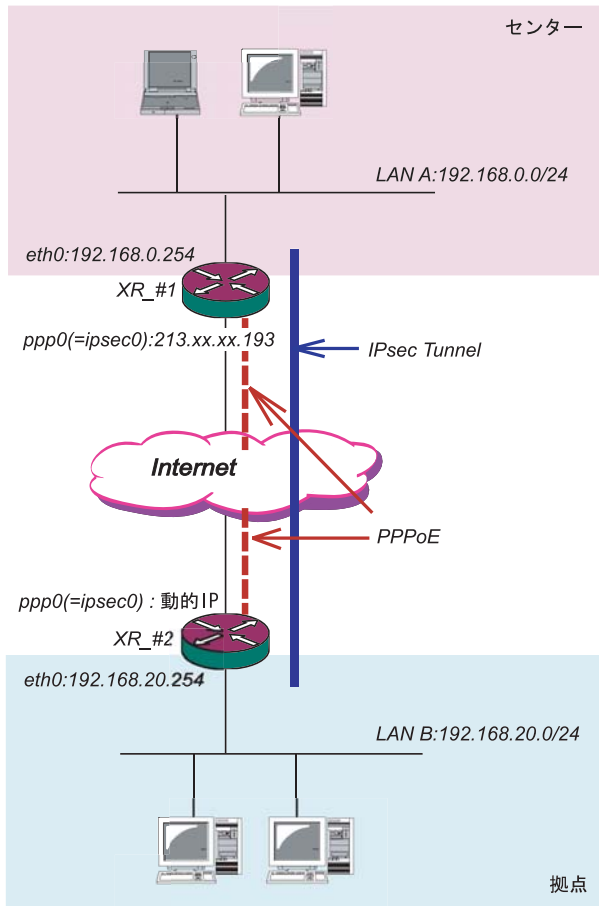
<設定例>

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	udp				500
2	ppp0	パケット受信時	許可	esp				

VII. IPsec 設定例 1 (センター / 拠点間の 1 対 1 接続)

センター / 拠点間で IPsec トンネルを 1 対 1 で構築する場合の設定例です。

< 設定例 1 >



< 接続条件 >

- ・センター側 / 拠点側ともに PPPoE 接続とします。
- ・但し、センター側は固定アドレス、拠点側は動的アドレスとします。
- ・IPsec 接続の再接続性を高めるため、IPsec Keep-Alive を用います。
- ・IP アドレス、ネットワークアドレス、インターフェース名は図中の表記を使用するものとします。
- ・拠点側を Initiator、センター側を Responder とします。
- ・拠点側が動的アドレスのため、aggressive モードで接続します。
- ・PSK 共通鍵を用い、鍵は「test_key」とします。

XR_#1(センター側 XR)の設定

各設定画面で下記のように設定します。

「本装置の設定」

「本装置側の設定 1」を選択します。

インターフェースの IP アドレス	213.xx.xx.193
上位ルータの IP アドレス	%ppp0
インターフェースの ID	(例: @xr.centurysys)

インターフェースの IP アドレス

「213.xx.xx.193」

上位ルータの IP アドレス「%ppp0」

PPPoE 接続かつ固定 IP アドレスの場合は、必ずこの設定にします。

インターフェースの ID「空欄」

固定アドレスの場合は、「インターフェースの ID」は省略できます。省略した場合は、自動的に「インターフェースの IP アドレス」を ID として使用します。

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	
接続する本装置側の設定	本装置側の設定 1
インターフェースの IP アドレス	0.0.0.0
上位ルータの IP アドレス	
インターフェースの ID	@host (例: @xr.centurysys)
モードの設定	aggressive モード
transform の設定	1 番目 group2-3des-sha1
	2 番目 使用しない
	3 番目 使用しない
	4 番目 使用しない
IKE のライフタイム	3600 秒 (1081 ~ 28800 秒まで)
鍵の設定	
<input checked="" type="radio"/> PSK を使用する	test_key
<input type="radio"/> RSA を使用する (X509 を使用する場合は RSA に設定してください)	
X509 の設定	
接続先の証明書の設定 (X509 を使用しない場合は必要ありません)	

第 11 章 IPsec 機能

VII. IPsec 設定例 1 (センター / 拠点間の 1 対 1 接続)

IKE/ISAKMP ポリシー名 「(任意で設定します)」
接続する本装置側の設定 「本装置側の設定 1」

インターフェースの IP アドレス 「0.0.0.0」
対向装置が動的アドレスの場合は必ずこの設定
にしてください。

上位ルータの IP アドレス 「空欄」
インターフェースの ID 「@host」
(@以降は任意の文字列)

上記の 2 項目は、対向装置の「本装置の設定」
と同じものを設定します。

モードの設定 「aggressive モード」
transform の設定 「group2-3des-sha1」
(任意の設定を選択)
IKE のライフタイム 「3600」(任意の設定値)

鍵の設定 「PSK を使用する」を選択し、対向装
置との共通鍵 「test_key」を入力します。

PH2 の Transform の選択 「すべてを送信する」
PFS 「使用する」(推奨)
DH Group の選択 「指定しない」
SA のライフタイム 「28800」(任意の設定値)

DISTANCE 「空欄」
省略した場合は、自動的にディスタンス値を
「1」として扱います。

「IPsec Keep-Alive の設定」

対向装置が動的アドレスの場合は、固定アドレス
側からの再接続ができないため、通常、IPsec
Keep-Alive は動的アドレス側 (Initiator 側) で設
定します。よって、本装置では設定しません。

「IPsec ポリシーの設定」

「IPsec1」を選択します。

<input type="radio"/> 使用する <input type="radio"/> 使用しない <input checked="" type="radio"/> Responderとして使用する <input type="radio"/> On-Demandで使用する	
使用するIKEポリシー名の選択	<input type="text" value="IKE1"/>
本装置側のLAN側のネットワークアドレス	<input type="text" value="192.168.0.0/24"/> (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	<input type="text" value="192.168.20.0/24"/> (例:192.168.0.0/24)
PH2のTransformの選択	<input type="text" value="すべてを送信する"/>
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	<input type="text" value="指定しない"/>
SAのライフタイム	<input type="text" value="28800"/> 秒 (1081~86400秒まで)
DISTANCE	<input type="text" value=""/> (1~255まで)

「Responder として使用する」を選択します。
対向が動的アドレスの場合は、固定アドレス
側は Initiator にはなれません。

使用する IKE ポリシー名の選択 「IKE1」
本装置側の LAN 側のネットワークアドレス
「192.168.0.0/24」
相手側の LAN 側のネットワークアドレス
「192.168.20.0/24」

第11章 IPsec 機能

VII. IPsec 設定例 1 (センター / 拠点間の1対1接続)

XR_#2(拠点側 XR)の設定

各設定画面で下記のように設定します。

「本装置の設定」

「本装置側の設定 1」を選択します。

インターフェースのIPアドレス	<input type="text" value="%ppp"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text" value="@host"/> (例: @xr.centurysys)

インターフェースの IP アドレス「%ppp0」
PPPoE 接続かつ動的アドレスの場合は、必ずこの設定にします。

上位ルータの IP アドレス「空欄」
PPPoE 接続かつ動的アドレスの場合は、空欄にしてください。

インターフェースの ID「@host」
(@以降は任意の文字列)

動的アドレスの場合は、必ず任意の ID を設定します。

IKE/ISAKMP ポリシー名「(任意で設定します)」
接続する本装置側の設定「本装置側の設定 1」

インターフェースの IP アドレス「213.xx.xx.193」
対向装置の IP アドレスを設定します。

上位ルータの IP アドレス「空欄」
対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

インターフェースの ID「空欄」
対向装置が固定アドレスなので、設定不要です。

モードの設定「aggressive モード」
transform の設定「group2-3des-sha1」
(任意の設定を選択)

IKE のライフタイム「3600」(任意の設定値)

鍵の設定「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	<input type="text"/>
接続する本装置側の設定	<input type="text" value="本装置側の設定1"/>
インターフェースのIPアドレス	<input type="text" value="213.xx.xx.193"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text"/> (例: @xr.centurysys)
モードの設定	<input type="text" value="aggressive モード"/>
transform の設定	1 番目 <input type="text" value="group2-3des-sha1"/>
	2 番目 <input type="text" value="使用しない"/>
	3 番目 <input type="text" value="使用しない"/>
	4 番目 <input type="text" value="使用しない"/>
IKE のライフタイム	<input type="text" value="3600"/> 秒 (1081~28800秒まで)
鍵の設定	
<input checked="" type="radio"/> PSK を使用する <input type="radio"/> RSA を使用する (X509 を使用する場合は RSAI に設定してください)	<input type="text" value="test_key"/>
X509 の設定	
接続先の証明書の設定 (X509 を使用しない場合は必要ありません)	<input type="text"/>

「IPSec ポリシーの設定」

「IPSec1」を選択します。

<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない <input type="radio"/> Responder として使用する <input type="radio"/> On-Demand で使用する	
使用するIKEポリシー名の選択	<input type="text" value="IKE1"/>
本装置側のLAN側のネットワークアドレス	<input type="text" value="192.168.20.0/24"/> (例: 192.168.0.0/24)
相手側のLAN側のネットワークアドレス	<input type="text" value="192.168.0.0/24"/> (例: 192.168.0.0/24)
PH2のTransFormの選択	<input type="text" value="すべてを送信する"/>
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	<input type="text" value="指定しない"/>
SAのライフタイム	<input type="text" value="28800"/> 秒 (1081~86400秒まで)
DISTANCE	<input type="text"/> (1~255まで)

「使用する」を選択します。
動的アドレスの場合は、必ず initiator として動作させます。

使用する IKE ポリシー名の選択「IKE1」
本装置側の LAN 側のネットワークアドレス
「192.168.20.0/24」

第11章 IPsec 機能

VII. IPsec 設定例 1 (センター / 拠点間の1対1接続)

相手側のLAN側のネットワークアドレス

「192.168.0.0/24」

PH2のTransformの選択 「すべてを送信する」

PFS 「使用する」(推奨)

DH Groupの選択 「指定しない」

SAのライフタイム 「28800」(任意の設定値)

DISTANCE 「空欄」

省略した場合は、自動的にディスタンス値を「1」として扱います。

「IPsec Keep-Aliveの設定」

PolicyNo.1の行に設定します。

Policy No.	enable	source address	destination address	interval(sec)	watch count	delay(sec)	flag	interface	backup SA	remove?
1	<input checked="" type="checkbox"/>	192.168.20.254	192.168.0.254	30	3	60	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>

enableにチェックを入れます。

source address 「192.168.20.254」

destination address 「192.168.0.254」

source addressには本装置側LANのインターフェースアドレスを、destination addressには相手側LANのインターフェースアドレスを設定することを推奨します。

interval 「30」(任意の設定値)

watch count 「3」(任意の設定値)

delay 「60」(任意の設定値)

flag 「チェック」(推奨)

interface 「ipsec0」

ppp0上のデフォルトのIPsecインターフェース名は「ipsec0」です。

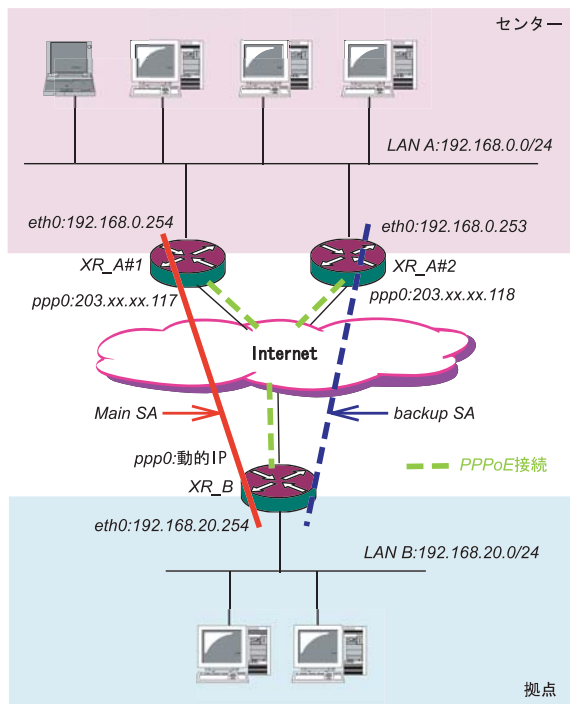
backupSA 「空欄」

第 11 章 IPsec 機能

VIII. IPsec 設定例 2 (センター / 拠点間の 2 対 1 接続)

センター側を 2 台の冗長構成とし、センター側の装置障害やネットワーク障害に備えて、センター / 拠点間の IPsec トンネルを二重化する場合の設定例です。

< 設定例 2 >



< 接続条件 >

- ・センター側は XR2 台の冗長構成とします。メインの IPsec トンネルは XR_A#1 側で、バックアップの IPsec トンネルは XR_A#2 側で接続するものとします。
- ・センター側 / 拠点側ともに PPPoE 接続とします。
- ・但し、センター側は固定アドレス、拠点側は動的アドレスとします。
- ・障害の検出および IPsec トンネルの切り替えは、拠点側の IPsec Keep-Alive を用いて行います。
- ・IP アドレス、ネットワークアドレス、インターフェース名は図中の表記を使用するものとします。
- ・拠点側を Initiator、センター側を Responder とします。
- ・拠点側が動的アドレスのため、aggressive モードで接続します。
- ・PSK 共通鍵を用い、鍵は「test_key」とします。
- ・センター側 LAN では、拠点方向のルートをアクティブの SA にフローティングさせるため、スタティックルートをを用います。

「本装置の設定」

XR_A#1(センター側 XR#1)の設定

「本装置側の設定 1」を選択します。

インターフェースの IP アドレス	<input type="text" value="203.xx.xx.117"/>
上位ルータの IP アドレス	<input type="text" value="%ppp0"/>
インターフェースの ID	<input type="text" value=""/> (例: @xr.centurysys)

インターフェースの IP アドレス「203.xx.xx.117」
上位ルータの IP アドレス「%ppp0」
PPPoE 接続かつ固定 IP アドレスの場合は、必ずこの設定にします。

インターフェースの ID「空欄」

固定アドレスの場合は、「インターフェースの ID」は省略できます。省略した場合は、自動的に「インターフェースの IP アドレス」を ID として使用します。

XR_A#2(センター側 XR#2)の設定

「本装置側の設定 1」を選択します。

インターフェースの IP アドレス	<input type="text" value="203.xx.xx.118"/>
上位ルータの IP アドレス	<input type="text" value="%ppp0"/>
インターフェースの ID	<input type="text" value=""/> (例: @xr.centurysys)

インターフェースの IP アドレス「203.xx.xx.118」
上位ルータの IP アドレス「%ppp0」
PPPoE 接続かつ固定 IP アドレスの場合は、必ずこの設定にします。

インターフェースの ID「空欄」

固定アドレスの場合は、「インターフェースの ID」は省略できます。省略した場合は、自動的に「インターフェースの IP アドレス」を ID として使用します。

第 11 章 IPsec 機能

VIII. IPsec 設定例 2 (センター / 拠点間の 2 対 1 接続)

「IKE/ISAKMP ポリシーの設定」

XR_A#1, XR_A#2 の IKE/ISAKMP ポリシーの設定
IKE/ISAKMP ポリシーの設定は、鍵の設定を除いて、
センター側 XR#1, XR#2 共に同じ設定で構いません。

「IKE1」を選択します。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	<input type="text"/>
接続する本装置側の設定	本装置側の設定1
インターフェースの IP アドレス	0.0.0.0
上位ルータの IP アドレス	<input type="text"/>
インターフェースの ID	@host (例:@xr.centurysys)
モードの設定	aggressive モード
transform の設定	1 番目 group2-3des-sha1
	2 番目 使用しない
	3 番目 使用しない
	4 番目 使用しない
IKE のライフタイム	3600 秒 (1081~28800 秒まで)
鍵の設定	
<input checked="" type="radio"/> PSK を使用する <input type="radio"/> RSA を使用する (X509 を使用する場合は RSA に設定してください)	test_key
X509 の設定	
接続先の証明書の設定 (X509 を使用しない場合は必要ありません)	<input type="text"/>

IKE/ISAKMP ポリシー名 「(任意で設定します)」
接続する本装置側の設定 「本装置側の設定1」

インターフェースの IP アドレス 「0.0.0.0」
対向装置が動的アドレスの場合は必ずこの設定
にします。

上位ルータの IP アドレス 「空欄」
インターフェースの ID 「@host」
(@以降は任意の文字列)

上記の2項目は、対向装置の「本装置の設定」
と同じものを設定します。

モードの設定 「aggressive モード」
transform の設定 「group2-3des-sha1」
(任意の設定を選択)
IKE のライフタイム 「3600」(任意の設定値)

鍵の設定 「PSK を使用する」を選択し、対向装
置との共通鍵 「test_key」を入力します。

「IPSec ポリシーの設定」

XR_A#1, XR_A#2 の IPsec ポリシーの設定
IPsec ポリシーの設定は、センター側 XR#1, XR#2 共
に同じ設定で構いません。

「IPSec1」を選択します。

<input type="radio"/> 使用する <input type="radio"/> 使用しない <input checked="" type="radio"/> Responder として使用する <input type="radio"/> On-Demand で使用する	
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransformの選択	すべてを送信する
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081~86400 秒まで)
DISTANCE	<input type="text"/> (1~255まで)

「Responder として使用する」を選択します。
使用する IKE ポリシー名の選択 「IKE1」
本装置側の LAN 側のネットワークアドレス
「192.168.0.0/24」
相手側の LAN 側のネットワークアドレス
「192.168.20.0/24」
PH2 の Transform の選択 「すべてを送信する」
PFS 「使用する」(推奨)
DH Group の選択 「指定しない」
SA のライフタイム 「28800」(任意の設定値)
DISTANCE 「空欄」

「転送フィルタ」の設定

メイン側 XR と WAN とのネットワーク断により、
バックアップ SA へ切り替えた際、メイン SA への
KeepAlive 要求がバックアップ XR からセンター側
LAN を経由してメイン側 XR に届いてしまいます。
これにより、IPsec 接続が復旧したと誤認し、再び
メイン SA へ切り戻しようとするため、バック
アップ接続が不安定な状態になります。

これを防ぐために、バックアップ側 XR (XR_A#2) に
下記のような転送フィルタを設定してください。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.254	

第11章 IPsec機能

VIII. IPsec 設定例 2 (センター / 拠点間の2対1接続)

インターフェース 「ipsec0」
ppp0のデフォルトのIPsecインターフェース
の「ipsec0」を設定します。

動作 「破棄」

送信元アドレス 「192.168.20.254」

拠点側メインSAのKeepAliveの送信元アドレス
を設定します。

あて先アドレス 「192.168.0.254」

拠点側メインSAのKeepAliveの送信先アドレス
を設定します。

XR_A#1のスタティックルート設定

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>	削除	
1	192.168.20.0	255.255.255.0		192.168.0.253	20	<input type="checkbox"/>

アドレス 「192.168.20.0」

ネットマスク 「255.255.255.0」

ゲートウェイ 「192.168.0.253」

XR_A#2のアドレスを設定します。

ディスタンス 「20」

IPsecルートのディスタンス(=1)より大きい任
意の値を設定します。

また同じ理由から、メインSAで接続中にIPsec接
続が不安定になるのを防ぐために、**メイン側XR
(XR_A#1)**にも下記のような転送フィルタを設定し
てください。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.253	

インターフェース 「ipsec0」

ppp0のデフォルトのIPsecインターフェース
の「ipsec0」を設定します。

動作 「破棄」

送信元アドレス 「192.168.20.254」

拠点側バックアップSAのKeepAliveの送信元
アドレスを設定します。

あて先アドレス 「192.168.0.253」

拠点側バックアップSAのKeepAliveの送信先
アドレスを設定します。

XR_A#2のスタティックルート設定

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>	削除	
1	192.168.20.0	255.255.255.0		192.168.0.254	20	<input type="checkbox"/>

アドレス 「192.168.20.0」

ネットマスク 「255.255.255.0」

ゲートウェイ 「192.168.0.254」

XR_A#1のアドレスを設定します。

ディスタンス 「20」

IPsecルートのディスタンス(=1)より大きい任
意の値を設定します。

「スタティックルート」の設定

センター側のXRでは自分がIPsec接続していない
ときに、拠点方向のルートをIPsec接続中のXRへ
フローティングさせるために、スタティックルー
トの設定を行います。

自分がIPsec接続しているときは、IPsecルートの
ディスタンス値(=1)の方が小さいため、このスタ
ティックルートは無効の状態となっています。

第11章 IPsec 機能

VIII. IPsec 設定例 2 (センター / 拠点間の2対1接続)

「IPsec Keep-Alive 設定」

さらに、障害時にすぐにフローティングスタティックルートへ切り替えるために、IPsec Keep-Alive を設定します。(KeepAlive 機能を使用しない場合は、Rekey のタイミングまでフローティングできない場合があります。)

XR_A#1 の IPsec Keep-Alive 設定

Policy No.	enable	source address	destination address	interval(sec)	watch count	delay(sec)	flag	interface	backup SA	remove?
1	<input checked="" type="checkbox"/>	192.168.0.254	192.168.20.254	30	3	60	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>

enable にチェックを入れます。
source address 「192.168.0.254」
destination address 「192.168.20.254」
interval 「30」(任意の設定値) 注)
watch count 「3」(任意の設定値)
delay 「60」(任意の設定値)
flag 「チェック」(推奨)
interface 「ipsec0」
backupSA 「空欄」

XR_A#2 の IPsec Keep-Alive 設定

Policy No.	enable	source address	destination address	interval(sec)	watch count	delay(sec)	flag	interface	backup SA	remove?
1	<input checked="" type="checkbox"/>	192.168.0.253	192.168.20.254	30	3	60	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>

enable にチェックを入れます。
source address 「192.168.0.253」
destination address 「192.168.20.254」
interval 「30」(任意の設定値) 注)
watch count 「3」(任意の設定値)
delay 「60」(任意の設定値)
flag 「チェック」(推奨)
interface 「ipsec0」
backupSA 「空欄」

注)

センター側と拠点側の interval が同じ値の場合、Keep-Alive の周期が同期してしまい、障害時の IPsec 切り替え直後に、切り替えた先でもすぐに障害を検出して、IPsec 通信が不安定になることがあります。
これを防ぐために、センター側の interval は拠点側のメイン SA、バックアップ SA のいずれの interval と異なる値を設定することを推奨します。
但し、センター内の XR 同士は同じ interval 値でも構いません。

第 11 章 IPsec 機能

VIII. IPsec 設定例 2 (センター / 拠点間の 2 対 1 接続)

XR_B(拠点側 XR)の設定

「本装置の設定」

「本装置側の設定 1」を選択します。

インターフェースの IP アドレス	<input type="text" value="%ppp"/>
上位ルータの IP アドレス	<input type="text"/>
インターフェースの ID	<input type="text" value="@host"/> (例: @xr.centurysys)

インターフェースの IP アドレス「%ppp0」
PPPoE 接続かつ動的アドレスの場合は、必ずこの設定にします。

上位ルータの IP アドレス「空欄」
PPPoE 接続かつ動的アドレスの場合は、空欄にしてください。

インターフェースの ID「@host」
(@以降は任意の文字列)
動的アドレスの場合は、必ず任意の ID を設定します。

「IKE/ISAKMP ポリシーの設定」

メイン SA 用の IKE/ISAKMP ポリシーの設定を行います。

「IKE1」を選択します。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	<input type="text"/>
接続する本装置側の設定	本装置側の設定1
インターフェースの IP アドレス	203.xx.xx.117
上位ルータの IP アドレス	<input type="text"/>
インターフェースの ID	<input type="text"/> (例: @xr.centurysys)
モードの設定	aggressive モード
transform の設定	1 番目 group2-3des-sha1
	2 番目 使用しない
	3 番目 使用しない
	4 番目 使用しない
IKE のライフタイム	3600 秒 (1081~28800 秒まで)
鍵の設定	
<input checked="" type="radio"/> PSK を使用する <input type="radio"/> RSA を使用する (X509 を使用する場合は RSA に設定してください)	<input type="text" value="test_key"/>
X509 の設定	
接続先の証明書の設定 (X509 を使用しない場合は必要ありません)	<input type="text"/>

IKE/ISAKMP ポリシー名「(任意で設定します)」
接続する本装置側の設定「本装置側の設定 1」
インターフェースの IP アドレス「203.xx.xx.117」
対向装置が固定アドレスなので、その IP アドレスを設定します。

上位ルータの IP アドレス「空欄」
対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

インターフェースの ID「空欄」
対向装置が固定アドレスなので、設定不要です。

モードの設定「aggressive モード」
transform の設定
1 番目「group2-3des-sha1」(任意の設定を選択)
2 ~ 4 番目「使用しない」
IKE のライフタイム「3600」(任意の設定値)

鍵の設定「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

「IKE/ISAKMP ポリシーの設定」

「IKE2」を選択します。

バックアップ SA 用の IKE/ISAKMP ポリシーの設定を行います。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	<input type="text"/>
接続する本装置側の設定	本装置側の設定1
インターフェースの IP アドレス	203.xx.xx.118
上位ルータの IP アドレス	<input type="text"/>
インターフェースの ID	<input type="text"/> (例: @xr.centurysys)
モードの設定	aggressive モード
transform の設定	1 番目 group2-3des-sha1
	2 番目 使用しない
	3 番目 使用しない
	4 番目 使用しない
IKE のライフタイム	3600 秒 (1081~28800 秒まで)
鍵の設定	
<input checked="" type="radio"/> PSK を使用する <input type="radio"/> RSA を使用する (X509 を使用する場合は RSA に設定してください)	<input type="text" value="test_key"/>
X509 の設定	
接続先の証明書の設定 (X509 を使用しない場合は必要ありません)	<input type="text"/>

第11章 IPsec機能

VIII. IPsec設定例2 (センター/拠点間の2対1接続)

IKE/ISAKMPポリシー名「(任意で設定します)」
接続する本装置側の設定「本装置側の設定1」
インターフェースのIPアドレス「203.xx.xx.118」
対向装置が固定アドレスなので、そのIPアドレスを設定します。

上位ルータのIPアドレス「空欄」
対向装置がPPPoE接続かつ固定アドレスなので、設定不要です。

インターフェースのID「空欄」
対向装置が固定アドレスなので、設定不要です。

モードの設定「aggressiveモード」
transformの設定
1番目「group2-3des-sha1」(任意の設定を選択)
2～4番目「使用しない」
IKEのライフタイム「3600」(任意の設定値)

鍵の設定「PSKを使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

「IPsecポリシーの設定」

メインSA用のIPsecポリシーの設定を行います。
「IPsec1」を選択します。

<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない <input type="radio"/> Responderとして使用する <input type="radio"/> On-Demandで使用する	
使用するIKEポリシー名の選択	[IKE1]
本装置側のLAN側のネットワークアドレス	[192.168.20.0/24] (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	[192.168.0.0/24] (例:192.168.0.0/24)
PH2のTransformの選択	[すべてを送信する]
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	[指定しない]
SAのライフタイム	[28800] 秒 (1081～86400秒まで)
DISTANCE	[1] (1～255まで)

「使用する」を選択します。

本装置はInitiatorとして動作し、かつメインSA用のIPsecポリシーであるため、「使用する」を選択します。

使用するIKEポリシー名の選択「IKE1」
本装置側のLAN側のネットワークアドレス
「192.168.20.0/24」

相手側のLAN側のネットワークアドレス
「192.168.0.0/24」

PH2のTransformの選択「すべてを送信する」
PFS「使用する」(推奨)

DH Groupの選択「指定しない」

SAのライフタイム「28800」(任意の設定値)

DISTANCE「1」

メイン側のディスタンス値は最小値(=1)を設定します。

「IPsecポリシーの設定」

バックアップSA用のIPsecポリシーの設定を行います。

「IPsec2」を選択します。

<input type="radio"/> 使用する <input type="radio"/> 使用しない <input checked="" type="radio"/> Responderとして使用する <input type="radio"/> On-Demandで使用する	
使用するIKEポリシー名の選択	[IKE2]
本装置側のLAN側のネットワークアドレス	[192.168.20.0/24] (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	[192.168.0.0/24] (例:192.168.0.0/24)
PH2のTransformの選択	[すべてを送信する]
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	[指定しない]
SAのライフタイム	[28800] 秒 (1081～86400秒まで)
DISTANCE	[2] (1～255まで)

「Responderとして使用する」を選択します。
バックアップSA用のIPsecポリシーであるため、「Responderとして使用する」を選択してください。

使用するIKEポリシー名の選択「IKE2」
本装置側のLAN側のネットワークアドレス

「192.168.20.0/24」

相手側のLAN側のネットワークアドレス

「192.168.0.0/24」

PH2のTransformの選択「すべてを送信する」
PFS「使用する」(推奨)

DH Groupの選択「指定しない」

SAのライフタイム「28800」(任意の設定値)

DISTANCE「2」

バックアップ側のディスタンス値は、メイン側のディスタンス値より大きな値を設定します。

第 11 章 IPsec 機能

VIII. IPsec 設定例 2 (センター / 拠点間の 2 対 1 接続)

「IPsec Keep-Alive の設定」

拠点側が動的 IP アドレスを用いた構成で、センター側からの通信があるようなケースでは SA の不一致が起こりうるため、メイン側、バックアップ側の両方で Keep-Alive を動作させることを推奨します。

Policy No.	enable	source address	destination address	interval(sec)	watch count	delay(sec)	flag	interface	backup SA	remove?
1	<input checked="" type="checkbox"/>	192.168.20.254	192.168.0.254	45	3	60	<input checked="" type="checkbox"/>	ipsec0	2	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	192.168.20.254	192.168.0.253	60	3	60	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>

メイン SA 用の KeepAlive の設定

PolicyNo.1 の行に設定します。

source address 「192.168.20.254」
destination address 「192.168.0.254」
interval 「45」(任意の設定値) **注)**
watch count 「3」(任意の設定値)
delay 「60」(任意の設定値)
flag 「チェック」(推奨)
interface 「ipsec0」
backupSA 「2」
Keep-Alive により障害検知した場合に、IPSec2 のポリシーに切り替えるため、「2」を設定します。

注)

メイン SA とバックアップ SA、または拠点側とセンター側の interval が同じ値の場合、Keep-Alive の周期が同期してしまい、障害時の IPsec 切り替え直後に、切り替えた先でもすぐに障害を検出して、IPsec 通信が不安定になることがあります。

これを防ぐために、拠点側の XR 同士の interval は、それぞれ異なる値を設定することを推奨します。さらにそれぞれの値はセンター側とも異なる値を設定してください。

バックアップ SA 用の KeepAlive の設定

PolicyNo.2 の行に設定します。

source address 「192.168.20.254」
destination address 「192.168.0.253」
interval 「60」(任意の設定値) **注)**
watch count 「3」(任意の設定値)
delay 「60」(任意の設定値)
flag 「チェック」(推奨)
interface 「ipsec0」
backupSA 「空欄」

IX. IPsecが繋がらないとき

IPsecで正常に通信できないときは本体ログを確認することで、どの段階で接続に失敗しているかを把握することができます。

本体ログは、「システム設定」内の「ログ表示」で確認します。

[正常にIPsec接続できたときのログメッセージ]

メインモードの場合

```
Aug 3 12:00:14 localhost ipsec_setup:
...FreeS/WAN IPsec started
```

```
Aug 3 12:00:20 localhost ipsec__plutorun:
104 "xripsec1" #1: STATE_MAIN_I1: initiate
```

```
Aug 3 12:00:20 localhost ipsec__plutorun:
106 "xripsec1" #1: STATE_MAIN_I2: from
STATE_MAIN_I1; sent MI2, expecting MR2
```

```
Aug 3 12:00:20 localhost ipsec__plutorun:
108 "xripsec1" #1: STATE_MAIN_I3: from
STATE_MAIN_I2; sent MI3, expecting MR3
```

```
Aug 3 12:00:20 localhost ipsec__plutorun:
004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP SA
established
```

```
Aug 3 12:00:20 localhost ipsec__plutorun:
112 "xripsec1" #2: STATE_QUICK_I1: initiate
```

```
Aug 3 12:00:20 localhost ipsec__plutorun:
004 "xripsec1" #2: STATE_QUICK_I2: sent QI2,
IPsec SA established
```

アグレッシブモードの場合

```
Apr 25 11:14:27 localhost ipsec_setup:
...FreeS/WAN IPsec started
```

```
Aug 3 11:14:34 localhost ipsec__plutorun: whack:
ph1_mode=aggressive whack:CD_ID=@home
whack:ID_FQDN=@home 112 "xripsec1" #1:
STATE_AGGR_I1: initiate
```

```
Aug 3 11:14:34 localhost ipsec__plutorun: 004
"xripsec1" #1: SAEST(e)=STATE_AGGR_I2: sent AI2,
ISAKMP SA established
```

```
Aug 3 12:14:34 localhost ipsec__plutorun: 117
"xripsec1" #2: STATE_QUICK_I1: initiate
```

```
Aug 3 12:14:34 localhost ipsec__plutorun: 004
"xripsec1" #2: SAEST(13)=STATE_QUICK_I2: sent QI2,
IPsec SA established
```

IX. IPsec がつながらないとき

「現在の状態」は IPsec 設定画面の「ステータス」から、画面中央下の「現在の状態」をクリックして表示します。

[正常に IPsec が確立したときの表示例]

```
000 interface ipsec0/eth1 218.xxx.xxx.xxx
000
000 "xripsec1": 192.168.xxx.xxx/24
===218.xxx.xxx.xxx[<id>]---218.xxx.xxx.xxx...
000 "xripsec1": ...219.xxx.xxx.xxx
===192.168.xxx.xxx.xxx/24
000 "xripsec1":  ike_life: 3600s; ipsec_life:
28800s; rekey_margin: 540s; rekey_fuzz: 100%;
keyingtries: 0
000 "xripsec1":  policy: PSK+ENCRYPT+TUNNEL+PFS;
interface: eth1; erouted
000 "xripsec1":  newest ISAKMP SA: #1; newest
IPsec SA: #2; eroute owner: #2
000
000 #2: "xripsec1" STATE_QUICK_I2 (sent QI2, IPsec
SA established); EVENT_SA_REPLACE in 27931s;
newest IPSEC; eroute owner
000 #2: "xripsec1" esp.32a406c4@219.xxx.xxx.xxx
esp.1be9611c@218.xxx.xxx.xxx
tun.1002@219.xxx.xxx.xxx tun.1001@218.xxx.xxx.xxx
000 #1: "xripsec1" STATE_MAIN_I4 (ISAKMP SA
established); EVENT_SA_REPLACE in 2489s; newest
ISAKMP
```

これらのログやメッセージ内に

- ISAKMP SA established
- IPsec SA established

のメッセージがない場合は IPsec が確立していません。設定を再確認してください。

IX. IPsec がつながらないとき

「...FreeS/WAN IPsec started」でメッセージが止まっています。

この場合は、接続相手との IKE 鍵交換が正常に行えていません。

IPsec 設定の「IKE/ISAKMP ポリシーの設定」項目で相手側機器についての設定を確認してください。

また、ステートフルパケットインスペクションを有効にしている場合、IPsec 通信の packets を受信できるようにフィルタ設定を施す必要があります。IPsec の packets を通すフィルタ設定は、「VI. IPsec 通信時のパケットフィルタ設定」をご覧ください。

「ISAKMP SA established」メッセージは表示されていますが「IPsec SA established」メッセージが表示されていません。

この場合は、IPsec SA が正常に確立できていません。IPsec 設定の「IPsec ポリシー設定」項目で、自分側と相手側のネットワークアドレスが正しいか、設定を確認してください。

新規に設定を追加したのですが、追加した設定については IPsec がつながりません。

設定を追加し、その設定を有効にする場合には IPsec 機能を再起動(本体の再起動)を行ってください。設定を追加しただけでは設定が有効になりません。

IPsec は確立していますが、Windows でファイル共有ができません。

XR シリーズは工場出荷設定において、NetBIOS を通さないフィルタリングが設定されています。Windows ファイル共有をする場合はこのフィルタ設定を削除もしくは変更してください。

aggressive モードで接続しようとしたら、今までつながっていた IPsec がつながらなくなってしまいました。

固定 IP - 動的 IP 間での main モード接続と aggressive モード接続を共存させることはできません。このようなトラブルを避けるために、固定 IP - 動的 IP 間で IPsec 接続する場合は aggressive モードで接続するようにしてください。

XR シリーズは工場出荷設定において、NetBIOS を通さないフィルタリングが設定されています。Windows ファイル共有をする場合はこのフィルタ設定を削除もしくは変更してください。

IPsec 通信中に回線が一時的に切断してしまうと、回線が回復しても IPsec 接続がなかなか復帰しません。

固定 IP アドレスと動的 IP アドレス間の IPsec 通信で、固定 IP アドレス側装置の IPsec 通信が意図しない切断をしてしまったときに起こりえる現象です。

相手が動的 IP アドレスの場合は相手側の IP アドレスが分からないために、固定 IP アドレス側からは IPsec 通信を開始することが出来ず、動的 IP アドレス側から IPsec 通信の再要求を受けるまでは IPsec 通信が復帰しなくなります。また動的側 IP アドレス側が IPsec 通信の再要求を出すのは IPsec SA のライフタイムが過ぎてからとなります。

これらの理由によって、IPsec 通信がなかなか復帰しない現象となります。

すぐに IPsec 通信を復帰させたいときは、動的 IP アドレス側の IPsec サービスも再起動する必要があります。

また、「IPsec Keep-Alive 機能」を使うことで IPsec の再接続性を高めることができます。

相手の装置には IPsec のログが出ているのに、こちらの装置にはログが出ていません。IPsec は確立しているようなのですが、確認方法はありますか？

固定 IP - 動的 IP 間での IPsec 接続をおこなう場合、固定 IP 側(受信者側)の本装置ではログが表示されないことがあります。その場合は「各種サービスの設定」 「IPsec サーバ」 「ステータス」を開き、「現在の状態」をクリックしてください。ここに現在の IPsec の状態が表示されます。

第 12 章

ダイナミックルーティング
(RIP、OSPF、DVMRP)

第12章 ダイナミックルーティング

1. ダイナミックルーティング機能

本装置のダイナミックルーティング機能は、RIP、OSPF および DVMRP (XR-640L2 のみ) をサポートしています。

RIP 機能のみで運用することはもちろん、RIP で学習した経路情報を OSPF で配布することなどもできます。

設定の開始

Web 設定画面「各種サービスの設定」画面左「ダイナミックルーティング」をクリックします。

DNSサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい	停止中	
I2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	動作変更
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
SNMPサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	動作変更
NTPサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	動作変更
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい	停止中	

「RIP」、「OSPF」、「DVMRP」(XR-640L2 のみ) をクリックして、それぞれの機能の設定画面を開いて設定をおこないます。

XR-410L2

RIP	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	再起動
OSPF	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	再起動

XR-640L2

RIP	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	再起動
OSPF	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	再起動
DVMRP	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	停止中	再起動

第12章 ダイナミックルーティング

II. RIPの設定

RIPの設定

Web 設定画面「各種サービスの設定」画面左「ダイナミックルーティング設定」 「RIP」をクリックして、以下の画面から設定します。

XR-410L2

Ether0ポート	<input type="button" value="使用しない"/>
	<input type="button" value="バージョン1"/>
Ether1ポート	<input type="button" value="使用しない"/>
	<input type="button" value="バージョン1"/>
Administrative Distance設定	<input type="text" value="120"/> (1-255) デフォルト120
OSPFルートの再配信	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
再配信時のメトリック設定	<input type="text"/> (0-16) 指定しない場合は空白
staticルートの再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
staticルート再配信時のメトリック設定	<input type="text"/> (0-16) 指定しない場合は空白
default-informationの送信	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR-640L2

Ether0ポート	<input type="button" value="使用しない"/>
	<input type="button" value="バージョン1"/>
Ether1ポート	<input type="button" value="使用しない"/>
	<input type="button" value="バージョン1"/>
Ether2ポート	<input type="button" value="使用しない"/>
	<input type="button" value="バージョン1"/>
Administrative Distance設定	<input type="text" value="120"/> (1-255) デフォルト120
OSPFルートの再配信	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
再配信時のメトリック設定	<input type="text"/> (0-16) 指定しない場合は空白
staticルートの再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
staticルート再配信時のメトリック設定	<input type="text"/> (0-16) 指定しない場合は空白
default-informationの送信	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

Ether0、Ether1、Ether2ポート
本装置の各Ethernetポートで、RIPの使用/不使用、また使用する場合のRIPバージョンを選択します。

Administrative Distance 設定

RIPとOSPFを併用していて全く同じ経路を学習する場合がありますが、その際はこの値の小さい方を経路として採用します。

OSPF ルートの再配信

RIPとOSPFを併用していて、OSPFで学習したルーティング情報をRIPで配信したいときに「有効」にしてください。RIPのみを使う場合は「無効」にします。

再配信時のメトリック設定

OSPFルートをRIPで配信するときのメトリック値を設定します。

staticルートの再配信

staticルーティング情報もRIPで配信したいときに「有効」にしてください。RIPのみを使う場合は「無効」にします。

staticルート再配信時のメトリック設定

staticルートをRIPで配信するときのメトリック値を設定します。

default-informationの送信

デフォルトルート情報をRIPで配信したいときに「有効」にしてください。
選択、入力後は「設定」をクリックして設定完了です。

設定後は「ダイナミックルーティング設定」画面に戻り、「起動」を選択して「動作変更」をクリックしてください。

また設定を変更した場合には、「再起動」をクリックしてください。

なお、RIPの動作状況およびルーティング情報は、「RIP情報の表示」をクリックすることで確認できます。

第12章 ダイナミックルーティング

II. RIPの設定

RIPフィルターの設定

RIPによる route 情報の送信または受信をしたくないときに設定します。

Web 設定画面「各種サービスの設定」画面左「ダイナミックルーティング設定」「RIPフィルタ設定」をクリックして、以下の画面から設定します。

NO.	インタフェース	方向	ネットワーク	編集 削除
既定設定はありません。				
フィルタの追加				
<input type="checkbox"/>	<input type="text" value="-----"/>	<input type="text" value="-----"/>	<input type="text" value="(例:192.168.0.0/16)"/>	

NO.

設定番号を指定します。1～64の間で指定します。

インタフェース

RIPフィルタを実行するインタフェースを選択します。

方向

「in-coming」は本装置がRIP情報を受信する際にRIPフィルタリングします(受信しない)。

「out-going」は本装置からRIP情報を送信する際にRIPフィルタリングします(送信しない)。

ネットワーク

RIPフィルタリングの対象となるネットワークアドレスを指定します。

<入力形式>

ネットワークアドレス/サブネットマスク値

入力後は「保存」をクリックしてください。

「取消」をクリックすると、入力内容がクリアされます。

RIPフィルタ設定後は、ただちに設定が有効となります。

設定後は、画面上部に設定内容が一覧表示されます。

NO.	インタフェース	方向	ネットワーク	編集 削除
1	Ether0ポート	in-coming	192.168.100.0/24	編集 削除
2	Ether1ポート	out-going	192.168.0.0/24	編集 削除

「削除」をクリックすると、設定が削除されます。

「編集」をクリックすると、その設定について内容を編集できます。

第12章 ダイナミックルーティング

111. OSPF の設定

OSPFはリンクステート型経路制御プロトコルです。

OSPFでは各ルータがリンクステートを交換しあい、そのリンクステートをもとに、他のルータがどこに存在するか、どのように接続されているか、というデータベースを生成し、ネットワークトポロジを学習します。

またOSPFは主に帯域幅からコストを求め、コストがもっとも低いものを最適な経路として採用します。これにより、トラフィックのロードバランシングが可能となっています。

その他、ホップ数に制限がない、リンクステートの更新にIPマルチキャストを利用する、RIPより収束が早いなど、大規模なネットワークでの利用に向いています。

OSPFの具体的な設定方法に関しましては、弊社サポートデスクでは対応しておりません。専門のコンサルティング部門にて対応いたしますので、その際は弊社までご連絡ください。

OSPF設定は、Web設定画面「各種サービスの設定」画面左「ダイナミックルーティング設定」 「OSPF」をクリックします。

インタフェースへのOSPFエリア設定

どのインタフェースでOSPF機能を動作させるかを設定します。

設定画面上部の「インタフェースへのOSPFエリア設定」をクリックします。

	ネットワークアドレス (例192.168.0.0/24)	AREA番号 (0-4294967295)
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

ネットワークアドレス
本装置に接続しているネットワークのネットワークアドレスを指定します。**ネットワークアドレス/マスクビット値**の形式で入力します。

AREA番号
そのネットワークのエリア番号を指定します。

AREA：リンクステートアップデートを送信する範囲を制限するための論理的な範囲

入力後は「設定」をクリックして設定完了です。

第12章 ダイナミックルーティング

III. OSPFの設定

OSPF エリア設定

各AREA(エリア)ごとの機能設定をおこないます。

設定画面上部の「OSPF エリア設定」をクリックします。

初めて設定するとき、もしくは設定を追加するときは「New Entry」をクリックします。

AREA番号	<input type="text" value="0-4294967295"/>
スタブ設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
トータル スタブ設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
default-cost	<input type="text" value="0-16777215"/>
認証設定	使用しない
エリア間ルートの経路集約設定	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

AREA 番号

機能設定をおこなうエリアの番号を指定します。

スタブ設定

外部に通じる経路がひとつしかない場合や最適な経路を通る必要がない場合にはスタブエリアに指定します。スタブエリアに指定するときは「有効」を選択します。スタブエリアにはLSA type5を送信しません。

トータルスタブ設定

LSA type5に加え、type3、4も送信しないエリアに指定するときに「有効」にします。

default-cost 設定

スタブエリアに対してデフォルトルート情報を送信する際のコスト値を指定します。指定しない場合は1です。

認証設定

該当エリアでパスワード認証かMD5認証をおこなうかどうかを選択します。デフォルト設定は「使用しない」です。

エリア間ルートの経路集約設定

経路情報を集約して送信したいときに設定します。

Ex:128.213.64.0 ~ 128.213.95.0のレンジのサブネットを渡すときに1つずつ渡すのではなく、128.213.64.0/19に集約して渡す、といったときに使用します。ただし、連続したサブネットでなければなりません(レンジ内に存在しないサブネットがあってはなりません)。

入力後は「設定」をクリックしてください。

設定後は「OSPF エリア設定」画面に、設定内容が一覧で表示されます。

	AREA番号	STUB	Totally STUB	Default-cost	Authentication	経路集約	Configure
1	1	有効	無効	10	無効	192.168.10.1/29	Edit,Remove

「Configure」項目の「Edit」「Remove」をクリックすることで、それぞれ設定内容の「編集」と設定の「削除」をおこなえます。(画面は表示例です)

第12章 ダイナミックルーティング

III. OSPF の設定

OSPF VirtualLink 設定

OSPFにおいて、すべてのエリアはバックボーンエリア(エリア0)に接続している必要があります。もし接続していなければ、他のエリアの経路情報は伝達されません。

しかし物理的にバックボーンエリアに接続できない場合にはVirtualLinkを設定して、論理的にバックボーンエリアに接続させます。

設定画面上部の「VirtualLink 設定」をクリックして設定します。

初めて設定するとき、もしくは設定を追加するときは「New Entry」をクリックします。

Transit AREA番号	<input type="text" value=""/>	(0-4294967295)
Remote-ABR Router-ID設定	<input type="text" value=""/>	(例:192.168.0.1)
Hello-インターバル設定	<input type="text" value="10"/>	(1-65535)
Dead-インターバル設定	<input type="text" value="40"/>	(1-65535)
Retransmit-インターバル設定	<input type="text" value="5"/>	(3-65535)
transmit delay設定	<input type="text" value="1"/>	(1-65535)
認証パスワード設定	<input type="text" value=""/>	(英数字で最大8文字)
MD5 KEY-ID設定(1)	<input type="text" value=""/>	(1-255)
MD5 パスワード設定(1)	<input type="text" value=""/>	(英数字で最大16文字)
MD5 KEY-ID設定(2)	<input type="text" value=""/>	(1-255)
MD5 パスワード設定(2)	<input type="text" value=""/>	(英数字で最大16文字)

Transit AREA 番号

VirtualLinkを設定する際に、バックボーンと設定するルータのエリアが接続している共通のエリアの番号を指定します。このエリアが「Transit AREA」となります。

Remote-ABR Router-ID 設定

VirtualLinkを設定する際のバックボーン側のルータIDを設定します。

Hello インターバル設定

Helloパケットの送出間隔を設定します。

Dead インターバル設定

Deadタイムを設定します。

Retransmit インターバル設定

LSAを送出する間隔を設定します。

transmit delay 設定

LSUを送出する際の遅延間隔(delay)を設定します。

認証パスワード設定

VirtualLink上でsimpleパスワード認証を使用する際のパスワードを設定します。半角英数字のみ使用できます。

MD5 KEY-ID 設定(1)

MD5 認証使用時のKEY IDを設定します。

MD5 パスワード設定(1)

エリア内でMD5 認証を使用する際のMD5 パスワードを設定します。

MD5 KEY-ID 設定(2)

MD5 パスワード設定(2)

MD5 KEY-IDとパスワードは2つ同時に設定可能です。その場合は(2)に設定します。半角英数字のみ使用できます。

VirtualLink 設定では、スタブエリアおよびバックボーンエリアをTransit AREAとして設定することはできません。

入力後は「設定」をクリックしてください。

設定後は「VirtualLink 設定」画面に、設定内容が一覧で表示されます。

AREA番号	Remote-ABR ID	Hello	Dead	Retransmit	Transmit Delay	認証 Password	MD5 KEY-ID	MD5 Password	Configure
1	192.168.0.1	10	40	5	1	aaa	111 112	bbb ccc	Edit/Remove

「Configure」項目の「Edit」「Remove」をクリックすることで、それぞれ設定内容の「編集」と設定の「削除」をおこなえます。

第12章 ダイナミックルーティング

III. OSPF の設定

OSPF 機能設定

OSPF の動作について設定します。設定画面上部の「OSPF 機能設定」をクリックして設定します。

Router-ID設定	<input type="text" value=""/> (例:192.168.0.1)
Connected再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 メトリックタイプ <input type="text" value="2"/> メトリック値設定 <input type="text" value=""/> (0-16777214)
staticルート再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 メトリックタイプ <input type="text" value="2"/> メトリック値設定 <input type="text" value=""/> (0-16777214)
RIPルートの再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 メトリックタイプ <input type="text" value="2"/> メトリック値設定 <input type="text" value=""/> (0-16777214)
Administrative Distance設定	<input type="text" value="110"/> (1-255)デフォルト110
Externalルート Distance設定	<input type="text" value=""/> (1-255)
Inter-areaルート Distance設定	<input type="text" value=""/> (1-255)
Intra-areaルート Distance設定	<input type="text" value=""/> (1-255)
Default-information	<input type="text" value="送信しない"/> メトリックタイプ <input type="text" value="2"/> メトリック値設定 <input type="text" value=""/> (0-16777214)
SPF計算Delay設定	<input type="text" value="5"/> (0-4294967295) デフォルト5s
2つのSPF計算の最小間隔設定	<input type="text" value="10"/> (0-4294967295) デフォルト10s
バックアップ切替え監視対象 Remote Router-ID設定	<input type="text" value=""/> (例:192.168.0.2)

Router-ID 設定

neighbor を確立した際に、ルータの ID として使用されたり、DR、BDR の選定の際にも使用されます。指定しない場合は、ルータが持っている IP アドレスの中でもっとも大きい IP アドレスを Router-ID として採用します。

Connected の再配信

connected ルートを OSPF で配信するかどうかを選択します。「有効」にした場合は以下の2項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

static ルートの再配信

static ルートを OSPF で配信するかどうかを選択します。**IPsec ルートを再配信する場合も、この設定を「有効」にする必要があります。**

「有効」にした場合は以下の2項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

RIP ルートの再配信

RIP が学習したルート情報を OSPF で配信するかどうかを選択します。「有効」にした場合は以下の2項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

Administrative Distance 設定

ディスタンス値を設定します。OSPF と他のダイナミックルーティングを併用していて同じサブネットを学習した際に、この値の小さい方のダイナミックルートを経路として採用します。

External ルート Distance 設定

OSPF 以外のプロトコルで学習した経路のディスタンス値を設定します。

Inter-area ルート Distance 設定

エリア間の経路のディスタンス値を設定します。

intra-area ルート Distance 設定

エリア内の経路のディスタンス値を設定します。

第12章 ダイナミックルーティング

III. OSPF の設定

Default-information

デフォルトルート OSPF で配信するかどうかを選択します。

「送信する」の場合、ルータがデフォルトルートを持っていれば送信されますが、たとえば PPPoE セッションが切断してデフォルトルート情報がなくなってしまうときは配信されなくなります。「常に送信」の場合、デフォルトルートの有無にかかわらず、自分にデフォルトルートに向けるように、OSPF で配信します。

「送信する」「常に送信する」の場合は、以下の2項目についても設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

SPF 計算 Delay 設定

LSU を受け取ってから SPF 計算をする際の遅延 (delay) 時間を設定します。

2つの SPF 計算の最小間隔設定

連続して SPF 計算をおこなう際の間隔を設定します。

バックアップ切替え監視対象 Remote Router-ID 設定

OSPF Hello によるバックアップ回線切り替え機能を使用する際に、Neighbor が切れたかどうかをチェックする対象のルータを判別するために、対象のルータの IP アドレスを設定します。

バックアップ機能を使用しない場合は、設定する必要はありません。

入力後は「設定」をクリックしてください。

第12章 ダイナミックルーティング

III. OSPF の設定

インタフェース設定

各インタフェースごとの OSPF 設定を行ないます。

設定画面上部の「インタフェース設定」をクリックして設定します。

初めて設定するとき、もしくは設定を追加するときは「New Entry」をクリックします。

インタフェース名	eth0
Passive-Interface設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
コスト値設定	<input type="text"/> (1-65535)
帯域設定	<input type="text"/> (1-10000000kbps)
Hello-インターバル設定	10 (1-65535s)
Dead-インターバル設定	40 (1-65535s)
Retransmit-インターバル設定	5 (3-65535s)
Transmit Delay設定	1 (1-65535s)
認証キー設定	<input type="text"/> (英数字で最大8文字)
MD5 KEY-ID設定(1)	<input type="text"/> (1-255)
MD5 パスワード設定(1)	<input type="text"/> (英数字で最大16文字)
MD5 KEY-ID設定(2)	<input type="text"/> (1-255)
MD5 パスワード設定(2)	<input type="text"/> (英数字で最大16文字)
Priority設定	<input type="text"/> (0-255)
MTU-Ignore設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

インタフェース名

設定するインタフェース名を入力します。本装置のインタフェース名については、本マニュアルの「付録A インターフェース名について」をご参照ください。

Passive-Interface 設定

インタフェースが該当するサブネット情報を OSPF で配信し、かつ、このサブネットには OSPF 情報を配信したくないという場合に「有効」を選択します。

コスト値設定

コスト値を設定します。

帯域設定

帯域設定をおこないます。この値をもとにコスト値を計算します。コスト値 = 100Mbps / 帯域 kbps です。コスト値と両方設定した場合は、コスト値設定が優先されます。

Hello インターバル設定

Hello パケットを送出する間隔を設定します。

Dead インターバル設定

Dead タイムを設定します。

Retransmit インターバル設定

LSA の送付間隔を設定します。

Transmit Delay 設定

LSU を送付する際の遅延間隔を設定します。

認証パスワード設定

simple パスワード認証を使用する際のパスワードを設定します。

MD5 KEY-ID 設定(1)

MD5 認証使用時の KEY ID を設定します。

MD5 パスワード設定(1)

VirtualLink 上で MD5 認証を使用する際の MD5 パスワードを設定します。半角英数字のみ使用できます。

MD5 KEY-ID 設定(2)

MD5 パスワード設定(2)

MD5 KEY-ID とパスワードは 2 つ同時に設定可能です。その場合は(2)に設定します。

Priority 設定

DR、BDR の設定の際に使用する priority を設定します。priority 値が高いものが DR に、次に高いものが BDR に選ばれます。0 を設定した場合は DR、BDR の選定には関係しなくなります。

DR、BDR の選定は、priority が同じであれば、IP アドレスの大きいものが DR、BDR になります。

MTU-Ignore 設定

DBD 内の MTU 値が異なる場合、Full の状態になることはできません(Exstart になる)。

どうしても MTU を合わせることができないときには、この MTU 値の不一致を無視して Neighbor (Full) を確立させるための MTU-Ignore を「有効」にしてください。

第12章 ダイナミックルーティング

III. OSPF の設定

入力後は「設定」をクリックしてください。
設定後は「インタフェース設定」画面に、設定内容が一覧で表示されます。

インタフェース名	Passive	Cost	帯域	Hello	Dead	Retransmit	Transmit Delay	認証 Password	MD5 KEY-ID	MD5 Password	Priority	MTU ignore	Configure
eth0	on	10	1000000	10	40	5	1	century	150	centurysystems	50	off	Edit,Remove

「Configure」項目の「Edit」「Remove」をクリックすることで、それぞれ設定内容の「編集」と設定の「削除」をおこなえます。

ステータス表示

OSPFの各種ステータスを表示します。

設定画面上部の「ステータス表示」をクリックして設定します。

OSPFデータベースの表示 (各Link state情報が表示されます)	表示する	
ネイバーリスト情報の表示 (現在のネイバー状態を確認できます)	表示する	
OSPFルーティングテーブル情報の表示 (OSPFルーティング情報が表示されます)	表示する	
OSPF統計情報の表示 (SPF計算回数などの情報を表示します)	表示する	
インタフェース情報の表示 (表示したいインタフェースを指定して下さい)	表示する	eth0

OSPF データベース表示

LinkState 情報が表示されます。

ネイバーリスト情報の表示

現在のネイバー状態が表示されます。

OSPF ルーティングテーブル情報の表示

OSPF ルーティング情報が表示されます。

OSPF 統計情報の表示

SPF の計算回数やRouter IDなどが表示されます。

インタフェース情報の表示

現在のインタフェースの状態が表示されます。

第12章 ダイナミックルーティング

IV. DVMRP の設定 (XR-640L2 のみ)

DVMRP はルータ間で使用される、マルチキャストデータグラムの経路を制御するプロトコルです。

DVMRP も他のダイナミックルーティングプロトコル同様にルータ間で経路情報を交換して、自動的にマルチキャストパケットの最適なルーティングを実現します。

ユニキャスト・ブロードキャストデータグラムについては DVMRP は経路制御しません。RIP や OSPF を利用してください。

インターフェース設定

設定画面上部の「インターフェース設定」をクリックして設定します。

No.	Interface	Metric	Threshold	Disable	Del
1	eth0	1	1	<input type="checkbox"/>	<input type="checkbox"/>
2				<input type="checkbox"/>	<input type="checkbox"/>
3				<input type="checkbox"/>	<input type="checkbox"/>
4				<input type="checkbox"/>	<input type="checkbox"/>
5				<input type="checkbox"/>	<input type="checkbox"/>
6				<input type="checkbox"/>	<input type="checkbox"/>
7				<input type="checkbox"/>	<input type="checkbox"/>
8				<input type="checkbox"/>	<input type="checkbox"/>
9				<input type="checkbox"/>	<input type="checkbox"/>
10				<input type="checkbox"/>	<input type="checkbox"/>
11				<input type="checkbox"/>	<input type="checkbox"/>
12				<input type="checkbox"/>	<input type="checkbox"/>
13				<input type="checkbox"/>	<input type="checkbox"/>
14				<input type="checkbox"/>	<input type="checkbox"/>
15				<input type="checkbox"/>	<input type="checkbox"/>
16				<input type="checkbox"/>	<input type="checkbox"/>

(画面は表示例です)

Interface

DVMRP を実行する、本装置のインターフェース名を指定します。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名について」をご参照ください。

Metric

メトリックを指定します。経路選択時のコストとなり、Metric 値が大きいほどコストが高くなります。

Threshold

TTL の ”しきい値” を設定します。この値とデータグラム内の TTL 値とを比較して、そのデータグラムを転送または破棄します。

「Threshold > データグラムの TTL」のときはデータグラムを破棄、「Threshold ≤ データグラムの TTL」のときはデータグラムをルーティングします。

Disable

チェックを入れて設定を保存すると、その設定は無効となります。

Del

チェックを入れて設定を保存すると、その設定は削除されます。

IV. DVMRP の設定 (XR-640L2 のみ)

全体設定

設定画面上部の「全体設定」をクリックして設定します。

インターフェイスのデフォルト	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Cache Lifetime (sec) (300s - 86400s)	<input type="text" value="300"/>

(画面は表示例です)

インターフェイスのデフォルト
インターフェイスのデフォルトの送信 / 非送信を設定します。

Cache Lifetime

マルチキャスト・ルーティングテーブルのキャッシュ保持時間を指定します。300 秒 ~ 86400 秒の間で指定します。

ステータス表示

設定画面上部の「ステータス表示」をクリックして表示します。

DVMRP ステータス表示								
UP TIME: 29024:44								
Neighbors: 0								
DVMRP Interface 表示								
Virtual Interface Table								
Vif	Name	Local-Address	M	Thr	Rate	Flags		
0	eth0	192.168.120.237 subnet: 192.168.120/24	1	1	0	leaf		
1	eth2	192.168.2.254 subnet: 192.168.2/24	1	1	0	querier leaf		
DVMRP Routing 表示								
Multicast Routing Table (2 entries)								
Origin-Subnet	From-Gateway	Metric	Tmr	Fl	In-Vif	Out-Vifs		
192.168.120/24		1	145	..	0	1*		
192.168.2/24		1	145	..	1	0*		
DVMRP Cache 表示								
Multicast Routing Cache Table (2 entries)								
1	Origin	Mcast-group	OTmr	Age	Ptmr	Rx	IVif	ForwVifs
2	(prunesrc:vif[id:]/tmr)	prunebitmap						
3	Source	Lifetime	SavPkt	Pkts	Bytes	RPFf		
1	192.168.120/24	239.255.2.2	0:04:52	0:02:22	-	-	0	
3	192.168.120.161	0:02:22	0	1	47	0		
1	192.168.120/24	239.255.255.250	0:02:43	0:04:36	-	-	0	
3	192.168.120.101	0:04:36	0	36	13710	0		

(画面は表示例です)

「ステータス表示」画面では、DVMRP が動作しているインターフェイスの状態、マルチキャストルーティングテーブルの内容、ルーティングテーブルキャッシュの内容が表示されます。

第 13 章

L2TPv3 機能

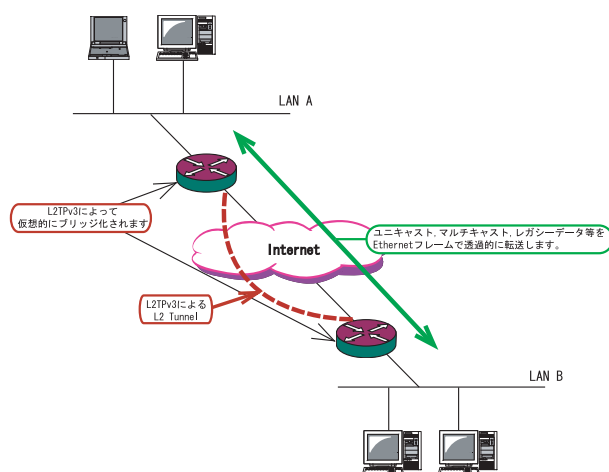
第13章 L2TPv3 機能

1. L2TPv3 機能概要

L2TPv3 機能は、IP ネットワーク上のルータ間で L2TPv3 トンネルを構築します。これにより本製品が仮想的なブリッジとなり、遠隔のネットワーク間でレイヤ2通信が可能となります。

レイヤ2レベルでトンネリングするため、2つのネットワークはHUBで繋がった1つのEthernetネットワークのように使うことができます。また上位プロトコルに依存せずにネットワーク通信ができ、TCP/IPだけでなく、任意の上位プロトコル(IPX、AppleTalk、SNA等)を透過的に転送することができます。

また L2TPv3 機能は、従来の専用線やフレームリレー網ではなく IP 網で利用できますので、低コストな運用が可能です。



- End to EndでEthernetフレームを転送したい
- FNAやSNAなどのレガシーデータを転送したい
- ブロードキャスト/マルチキャストパケットを転送したい
- IPXやAppleTalk等のデータを転送したい

このような、従来のIP-VPNやインターネットVPNでは通信させることができなかったものも、L2TPv3を使うことで通信ができるようになります。

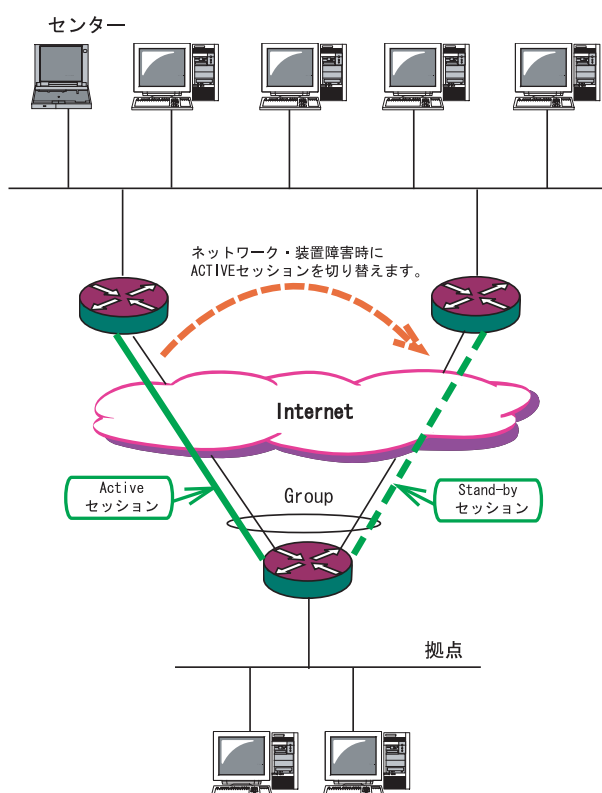
またPoint to Multi-Pointに対応しており、1つのXconnect Interfaceに対して複数のL2TP sessionを関連づけすることが可能です。

L2TPv3セッションの二重化機能

本装置では、L2TPv3 Group機能(L2TPv3セッションの二重化機能)を具備しています。ネットワーク障害や対向機器の障害時に二重化されたL2TPv3セッションのActiveセッションを切り替えることによって、レイヤ2通信の冗長性を高めることができます。

・L2TPv3セッション二重化の例

センター側を2台の冗長構成にし、拠点側のXRで、センター側へのL2TPv3セッションを二重化します。



第13章 L2TPv3 機能

11. L2TPv3 機能設定

本装置の ID やホスト名、MAC アドレスに関する設定を行います。

Web 設定画面「各種サービスの設定」->「L2TPv3」をクリックして、以下の画面で設定します。

XR-410L2

L2TPv3 機能設定

Local hostname	Router
Local Router-ID	
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Debug設定 (Syslogメッセージ出力設定)	<input type="checkbox"/> Tunnel Debug出力 <input type="checkbox"/> Session Debug出力 <input checked="" type="checkbox"/> L2TPエラーメッセージ出力

設定

各種サービスの設定画面へ

XR-640L2

L2TPv3 機能設定

Local hostname	Router
Local Router-ID	
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Debug設定 (Syslogメッセージ出力設定)	<input type="checkbox"/> Tunnel Debug出力 <input type="checkbox"/> Session Debug出力 <input checked="" type="checkbox"/> L2TPエラーメッセージ出力

設定

各種サービスの設定画面へ

Local hostname

本装置のホスト名を設定します。半角英数字のみ使用可能です。対向LCCE(1)の”リモートホスト名”設定と同じものにします。設定は必須ですが、後述の「L2TPv3 Tunnel 設定」で設定した場合はそちらが優先されます。

Local Router-ID

本装置のルータ ID を設定します。LCCE のルータ ID の識別に使用します。対向 LCCE の ”リモートルータ ID ” 設定と同じものにします。

ルータ ID は IP アドレス形式で設定してください。
(ex. 192.168.0.1 など)

設定は必須ですが、後述の「L2TPv3 Tunnel 設定」で設定した場合はそちらが優先されます。

MAC Address 学習機能(2)

MAC アドレス学習機能を有効にするかを選択します。

MAC Address Aging Time

本装置が学習した MAC アドレスの保持時間を設定します。30 ~ 1000(秒)で設定します。

Loop Detection 設定(3)

LoopDetect 機能を有効にするかを選択します。

Known Unicast 設定(4)

Known Unicast 送信機能を有効にするかを選択します。

PMTU Discovery

Path MTU Discovery機能を有効にするかを選択します。本機能を有効にした場合は、送信するL2TPv3パケットのDF(Don't Fragment)ビットを1にします。無効にした場合は、DFビットを常に0にして送信します。但し、カプセリングしたフレーム長が送信インターフェースのMTU値を超過する場合は、この設定に関係なく、フラグメントされ、DFビットを0にして送信します。

11. L2TPv3 機能設定

受信ポート番号 (over UDP)

L2TPv3 over UDP 使用時の L2TP パケットの受信ポートを指定します。

PMTU Discovery 設定 (over UDP)

L2TPv3 over UDP 使用時に Path MTU Discovery 機能を有効にするかを選択します。

SNMP 機能設定 (XR-640L2 のみ)

L2TPv3 用の SNMP エージェント機能を有効にするかを選択します。L2TPv3 に関する MIB の取得が可能になります。

SNMP Trap 機能設定 (XR-640L2 のみ)

L2TPv3 用の SNMP Trap 機能を有効にするかを選択します。L2TPv3 に関する Trap 通知が可能になります。

これらの SNMP 機能を使用する場合は、SNMP サービスを起動させてください。

また、MIB や Trap に関する詳細は第 16 章「SNMP エージェント機能」を参照してください。

Debug 設定

syslog に出力するデバッグ情報の種類を選択します。トンネルのデバッグ情報、セッションのデバッグ情報、L2TP エラーメッセージの 3 種類を選択できます。

(1) LCCE (L2TP Control Connection Endpoint)
L2TP コネクションの末端にある装置を指す言葉。

(2) MAC Address 学習機能

本装置が受信したフレームの MAC アドレスを学習し、不要なトラフィックの転送を抑制する機能です。ブロードキャスト、マルチキャストについては MAC アドレスに関係なく、すべて転送されます。

Xconnect インターフェースで受信した MAC アドレスはローカル側 MAC テーブル(以下、Local MAC テーブル)に、L2TP セッション側で受信した MAC アドレスはセッション側 MAC テーブル(以下、FDB)にてそれぞれ保存されます。

さらに本装置は Xconnect インターフェース毎に Local MAC テーブル / FDB を持ち、それぞれの Local MAC テーブル / FDB につき、最大 65535 個の MAC アドレスを学習することができます。学習した MAC テーブルは手動でクリアすることができます。

(3) Loop Detection 機能

フレームの転送がループしてしまうことを防ぐ機能です。この機能が有効になっているときは、以下の 2 つの場合にフレームの転送を行いません。

- ・ Xconnect インターフェースより受信したフレームの送信元 MAC アドレスが FDB に存在するとき
- ・ L2TP セッションより受信したフレームの送信元 MAC アドレスが Local MAC テーブルに存在するとき

(4) Known Unicast 送信機能

Known Unicast とは、既に MAC アドレス学習済みの Unicast フレームのことを言います。この機能を「無効」にしたときは、以下の場合に Unicast フレームの転送を行いません。

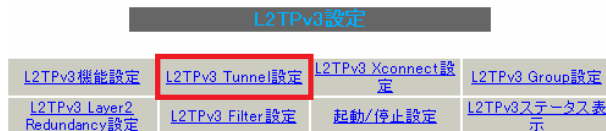
- ・ Xconnect インターフェースより受信した Unicast フレームの送信先 MAC アドレスが Local MAC テーブルに存在するとき

第13章 L2TPv3 機能

III. L2TPv3 Tunnel 設定

L2TPv3のトンネル(制御コネクション)のための設定を行います。

「各種サービスの設定」->「L2TPv3」の「L2TPv3 Tunnel 設定」をクリックします。



新規に設定を行うときは「New Entry」をクリックして、以下の画面で設定します。

L2TPv3 Tunnel設定

Description	<input type="text"/>
Peerアドレス	<input type="text"/> (例:192.168.0.1)
パスワード	<input type="password"/> (英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	<input type="text"/>
Local RouterID設定	<input type="text"/>
Remote Hostname設定	<input type="text"/>
Remote RouterID設定	<input type="text"/>
Vendor ID設定	20376:CENTURY
Bind Interface設定	<input type="text"/>
送信プロトコル	<input checked="" type="radio"/> over IP <input type="radio"/> over UDP
送信ポート番号	1701 (default 1701)

Description

このトンネル設定についてのコメントや説明を付記します。この設定はL2TPv3の動作には影響しません。

Peer アドレス

対向 LCCE の IP アドレスを設定します。但し、対向 LCCE が動的 IP アドレスの場合には空欄にしてください。

パスワード

CHAP 認証やメッセージダイジェスト、AVP Hiding で利用する共有鍵を設定します。パスワードは設定しなくてもかまいません。

パスワードは、制御コネクションの確立時における対向 LCCE の識別、認証に使われます。

AVP Hiding 設定()

AVP Hiding を有効にするかを選択します。

Digest Type 設定

メッセージダイジェストを使用する場合に設定します。

Hello Interval 設定

Hello パケットの送信間隔を設定します。「0」を設定すると Hello パケットを送信しません。

Hello パケットは、L2TPv3 の制御コネクションの状態を確認するために送信されます。

L2TPv3 二重化機能で、ネットワークや機器障害を自動的に検出したい場合は必ず設定してください。

Local Hostname 設定

本装置のホスト名を設定します。LCCE の識別に使用します。設定しない場合は「L2TPv3 機能設定」での設定が有効になります。

Local Router ID 設定

対向 LCCE のルータ ID を設定します。LCCE のルータ ID の識別に使用します。設定しない場合は「L2TPv3 機能設定」での設定が有効になります。

Remote Hostname 設定

対向 LCCE のホスト名を設定します。LCCE の識別に使用します。設定は必須となります。

Remote Router ID 設定

対向 LCCE のルータ ID を設定します。LCCE のルータ ID の識別に使用します。設定は必須となります。

III. L2TPv3 Tunnel 設定

Vender ID 設定

対向 LCCE のベンダー ID を設定します。

「0」は RFC3931 対応機器、「9」は Cisco Router、「20376」は XR シリーズとなります。

Bind Interface 設定

バインドさせる本装置のインタフェースを設定します。指定可能なインタフェースは「PPP インタフェース」のみです。

この設定により、PPP/PPPoE の接続 / 切断に伴って、L2TP トンネルとセッションの自動確立 / 解放がおこなわれます。

送信プロトコル

L2TP パケット送信時のプロトコルを「over IP」「over UDP」から選択します。接続する対向装置と同じプロトコルを指定する必要があります。「over UDP」を選択した場合、PPPoE to L2TP 機能を同時に動作させることはできません。

送信ポート番号

L2TPv3 over UDP 使用時（上記「送信プロトコル」で「over UDP」を選択した場合）に、対向装置のポート番号を指定します。

()AVP Hiding

L2TPv3 では、AVP (Attribute Value Pair) と呼ばれる、属性と値のペアでトンネルの確立や解放、維持などの制御メッセージをやりとりします。AVP は通常、平文で送受信されますが、AVP Hiding 機能を使うことで AVP 中のデータを暗号化します。

第13章 L2TPv3 機能

IV. L2TPv3 Xconnect (クロスコネクト) 設定

主にL2TPセッションを確立するときを使用するパラメータの設定を行います。

「各種サービスの設定」->「L2TPv3」の「L2TPv3 Xconnect 設定」をクリックします。

L2TPv3設定			
L2TPv3機能設定	L2TPv3 Tunnel設定	L2TPv3 Xconnect設定	L2TPv3 Group設定
L2TPv3 Layer2 Redundancy設定	L2TPv3 Filter設定	起動/停止設定	L2TPv3ステータス表示

新規に設定を行うときは「New Entry」をクリックして、以下の画面で設定します。

L2TPv3 Xconnect Interface設定	
Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	---
L2Frame受信インタフェース設定	<input type="text" value=""/> (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	<input type="text" value="0"/> [0-4094] (0の場合付与しない)
Remote END ID設定	<input type="text" value=""/> [1-4294967295]
Reschedule Interval設定	<input type="text" value="0"/> [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	<input type="text" value="0"/> [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

Xconnect ID 設定

「L2TPv3 Group 設定」で使用する ID を任意で設定します。

Tunnel 設定選択

「L2TPv3 Tunnel 設定」で設定したトンネル設定を選択して、トンネルの設定とセッションの設定を関連づけます。

プルダウンメニューには、「L2TPv3 Tunnel 設定」の「Remote Router ID」で設定された値が表示されます。

L2Frame 受信インタフェース設定

レイヤー2フレーム(Ethernet フレーム)を受信するインタフェース名を設定します。設定可能なインタフェースは、本装置のイーサネットポートとVLANインタフェースのみです。

Point to Multi-point 接続を行う場合は、1つのインタフェースに対し、複数のL2TPv3セッションの関連付けが可能です。

但し、本装置のEthernet インタフェースとVLAN インタフェースを同時に設定することはできません。

2つ(以上)のXconnect 設定を行うときの例 :

「eth0.10」と「eth0.20」・・・設定可能
「eth0.10」と「eth0.10」・・・設定可能()
「eth0」と「eth0.10」・・・設定不可

Point to Multi-point 接続、もしくはL2TPv3二重化の場合のみ設定可能です。

VLAN ID 設定

本装置でVLAN タギング機能を使用する場合に設定します。本装置の配下にVLANに対応していないL2スイッチが存在するときに使用できます。0 ~ 4094まで設定でき、「0」のときはVLAN タグを付与しません。

Remote END ID 設定

対向LCCEのEND IDを設定します。END IDは1 ~ 4294967295の任意の整数値です。対向LCCEのEND ID設定と同じものにします。但し、L2TPv3セッション毎に異なる値を設定してください。

Reschedule Interval 設定

L2TPトンネル/セッションが切断したときにreschedule(自動再接続)することができます。自動再接続するときはここで、自動再接続を開始するまでの間隔を設定します。0 ~ 1000(秒)で設定します。

また、「0」を設定したときは自動再接続は行われません。このときは手動による接続が対向LCCEからのネゴシエーションによって再接続します。

第 13 章 L2TPv3 機能

IV. L2TPv3 Xconnect (クロスコネクト) 設定

L2TPv3 二重化機能で、ネットワークや機器の復旧時に自動的にセッション再接続させたい場合は必ず Reschedule Interval を設定してください。

Auto Negotiation 設定

この設定が有効になっているときは、L2TPv3 機能が起動後に自動的に L2TPv3 トンネルの接続が開始されます。

この設定は Ethernet 接続時に有効です。PPP/PPPoE 環境での自動接続は、「L2TPv3 Tunnel 設定」の「Bind Interface 設定」で ppp インタフェースを設定してください。

MSS 設定

MSS 値の調整機能を有効にするかどうかを選択します。

MSS 値 (byte)

MSS 設定を「有効」に選択した場合、MSS 値を指定することができます (指定可能範囲 0-1460)。0 を指定した場合、自動的に計算された値を設定します。

特に必要のない限り、この機能を有効にして、かつ MSS 値を 0 にしておくことを推奨いたします (それ以外では正常にアクセスできなくなる場合があります)。

LoopDetection 設定

この Xconnect において、LoopDetection 機能を有効にするかを選択します。

Known Unicast 設定

この Xconnect において、Known Unicast 送信機能を有効にするかを選択します。

注) LoopDetect 設定、Known Unicast 設定は、「L2TPv3 機能設定」でそれぞれ有効にしていない場合、ここでの設定は無効となります。

Circuit Down 時 Frame 転送設定

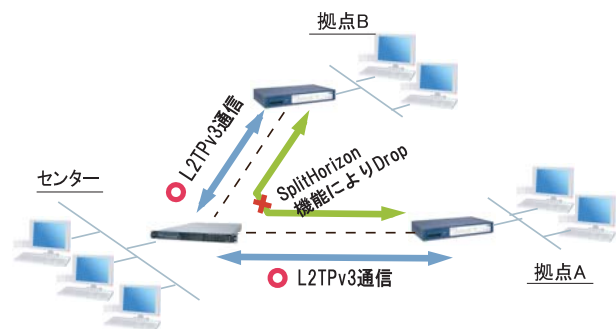
Circuit Status が Down 状態の時に、対向 LCCE に対して Non-Unicast Frame を送信するかを選択します。

Split Horizon 設定

Point-to-Multi-Point 機能によって、センターと 2 拠点間を接続しているような構成において、センターと拠点間の L2TPv3 通信は行すが、拠点同士間の通信は必要ない場合に、センター側でこの機能を有効にします。

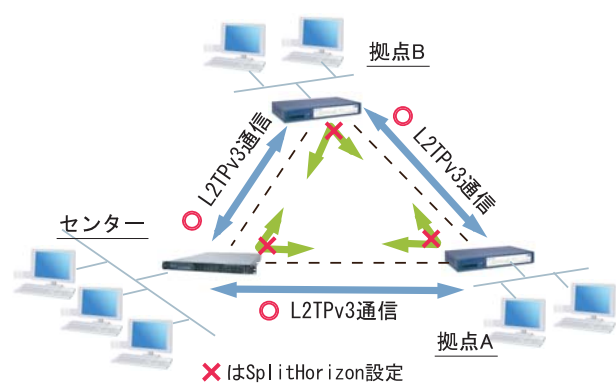
センター側では、Split Horizon 機能が有効の場合、一方の拠点から受信したフレームをもう一方のセッションへは転送せず、Local Interface に対してのみ転送します。

Split Horizon の使用例 1



また、この機能は、拠点間でフルメッシュの構成をとる様な場合に、フレームの Loop の発生を防ぐための設定としても有効です。この場合、全ての拠点において Split Horizon 機能を有効に設定します。LoopDetect 機能を有効にする必要はありません。

Split Horizon の使用例 2



V. L2TPv3 Group 設定

L2TPv3セッション二重化機能を使用する場合に、二重化グループのための設定を行います。

二重化機能を使用しない場合は、設定する必要はありません。

「各種サービスの設定」->「L2TPv3」の「L2TPv3 Group 設定」をクリックします。



新規のグループ設定を行うときは、「New Entry」をクリックします。



Group ID	<input type="text" value=""/> [1-4095]
Primary Xconnect設定選択	---
Secondary Xconnect設定選択	---
Preempt設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Primary active時のSecondary Session強制切断設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Active Hold設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

Group ID 設定

Groupを識別する番号を設定します。他のGroupと重複しない値を設定してください。

設定可能な値は、1 ~ 4095の任意の整数値です。

Primary Xconnect 設定選択

Primaryとして使用したいXconnectをプルダウンから選択します。プルダウンには「L2TPv3 Xconnect設定」の「Xconnect ID設定」で設定した値が表示されます。

既に他のGroupで使用されているXconnectを指定することはできません。

Secondary Xconnect 設定選択

Secondaryとして使用したいXconnectをプルダウンから選択します。プルダウンには「L2TPv3 Xconnect設定」の「Xconnect ID設定」で設定した値が表示されます。既に他のGroupで使用されているXconnectを指定することはできません。

Preempt 設定

GroupのPreemptモード()を有効にするかどうかを設定します。

Preempt モード

SecondaryセッションがActiveとなっている状態で、Primaryセッションが確立したときに、通常SecondaryセッションがActiveな状態を維持し続けますが、Preemptモードが「有効」の場合は、PrimaryセッションがActiveになり、SecondaryセッションはStand-byとなります。

Primary active時のSecondary Session強制切断設定

この設定が「有効」となっている場合、PrimaryセッションがActiveに移行した際に、Secondaryセッションを強制的に切断します。本機能を「有効」にする場合、「Preempt設定」も「有効」に設定してください。

SecondaryセッションをISDNなどの従量回線で接続する場合には「有効」にすることを推奨します。

Active Hold 設定

GroupのActive Hold機能()を有効にするかどうかを設定します。

Active Hold機能

対向のLCCEからLink Downを受信した際に、Secondaryセッションへの切り替えを行わず、PrimaryセッションをActiveのまま維持する機能のことを言います。

1vs1の二重化構成の場合、対向LCCEでLink Downが発生した際に、PrimaryからSecondaryへActiveセッションを切り替えたとしても、通信できない状態は変わりません。よってこの構成においては、不要なセッションの切り替えを抑制するために本機能を有効に設定することを推奨します。

第13章 L2TPv3 機能

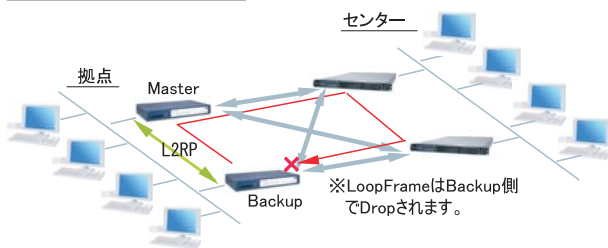
VI. Layer2 Redundancy 設定

Layer2 Redundancy Protocol 機能 (以下、L2TP 機能)とは、装置の冗長化を行い、Frame の Loop を抑止するための機能です。

L2RP 機能では、2 台の LCCE で Master/Backup 構成を取り、Backup 側は受信 Frame を全て Drop させることによって、Loop の発生を防ぐことができます。また機器や回線の障害発生時には、Master/Backup を切り替えることによって拠点間の接続を維持することができます。

下図のようなネットワーク構成では、フレームの Loop が発生し得るため、本機能を有効にしてください。

L2RP 機能の使用例



L2RP の設定方法

「各種サービスの設定」->「L2TPv3」の「L2TPv3 Layer2 Redundancy 設定」をクリックします。

L2TPv3設定

L2TPv3機能設定	L2TPv3 Tunnel設定	L2TPv3 Xconnect設定	L2TPv3 Group設定
L2TPv3 Layer2 Redundancy設定	L2TPv3 Filter設定	起動/停止設定	L2TPv3ステータス表示

「New Entry」をクリックすると以下の設定画面が開きます。

L2RP ID

L2RP の ID です。対になる LCCE の L2RP と同じ値を設定します。

Type 設定

Master/Backup を決定する判定方法を選択します。「Priority」は Priority 値の高い方が Master となります。「Active Session」は Active Session 数の多い方が Master となります。

XR-410L2

L2TPv3 Layer2 Redundancy設定

L2RP ID	<input type="text" value=""/> [1-255]
Type設定	<input checked="" type="radio"/> Priority <input type="radio"/> Active Session
Priority設定	<input type="text" value="100"/> [1-255] (default 100)
Advertisement Interval設定	<input type="text" value="1"/> [1-60] (default 1)
Preempt設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Xconnectインタフェース設定	<input type="text" value=""/> (interface名指定)
Forward Delay設定	<input type="text" value="0"/> [0-60] (default 0s)
Port Down Time設定	<input type="text" value="0"/> [0-10] (default 0s)
Block Reset設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR-640L2

L2TPv3 Layer2 Redundancy設定

L2RP ID	<input type="text" value=""/> [1-255]
Type設定	<input checked="" type="radio"/> Priority <input type="radio"/> Active Session
Priority設定	<input type="text" value="100"/> [1-255] (default 100)
Advertisement Interval設定	<input type="text" value="1"/> [1-60] (default 1)
Preempt設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Xconnectインタフェース設定	<input type="text" value=""/> (interface名指定)
Forward Delay設定	<input type="text" value="0"/> [0-60] (default 0s)
Port Down Time設定	<input type="text" value="0"/> [0-10] (default 0s)
FDB Reset設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Block Reset設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

Priority 設定

Master の選定に使用する Priority 値です。1 ~ 255 の間で設定します。

Advertisement Interval 設定

Advertise Frame を送信する間隔です。1 ~ 60 (秒) の間で設定します。

VI. Layer2 Redundancy 設定

Advertise Frame

Master側が定期的を送出する情報フレームです。Backup側ではこれを監視し、一定時間受信しない場合にMaster側の障害と判断し、自身がMasterへ遷移します。

Preempt 設定

Priority値が低いものがMasterで高いものがBackupとなることを許可するかどうかの設定です。

Xconnect インターフェース設定

Xconnect インターフェース名を指定してください。Advertise FrameはXconnect上で送受信されます。

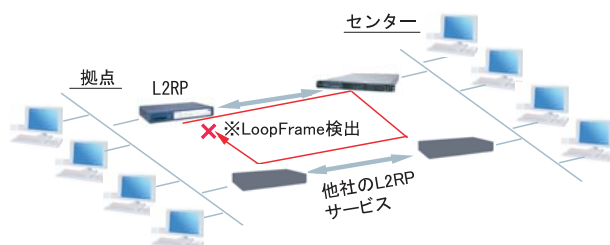
Forward Delay 設定

Forward Delayとは、L2TPセッション確立後、指定されたDelay Timeの間、Frameの転送を行わない機能のことです。

例えば、他のL2サービスと併用し、L2RPの対向が存在しないような構成において、L2RP機能では自身が送出したAdvertiseフレームを受信することでLoopを検出しますが、Advertiseフレームを受信するまでは一時的にLoopが発生する可能性があります。このような場合にForward Delayを有効にすることによって、Loopの発生を抑止することができます。

delay Timeの設定値はAdvertisement Intervalより長い時間を設定することを推奨します。

他のL2RPサービスとの併用例



Port Down Time 設定

L2RP機能によって、Activeセッションの切り替えが発生した際、配下のスイッチにおけるMACアドレスのエントリが、以前Masterだった機器のPortを向いているために最大約5分間通信ができなくなる場合があります。

これを回避するために、MasterからBackupの切り替え時に自身のPortのリンク状態を一時的にダウンさせることによって配下のスイッチのMACテーブルをフラッシュさせることができます。

設定値は、切り替え時にPortをダウンさせる時間です。0を指定すると本機能は無効になります。

L2RP Group Blocking状態について

他のL2サービスと併用している場合に、自身が送出したAdvertise Frameを受信したことによって、Frameの転送を停止している状態をGroup Blocking状態と言います。このGroup Blocking状態に変化があった場合にも、以下の設定で、機器のMACテーブルをフラッシュすることができます。

FDB Reset 設定 (XR-640L2のみ)

XRがHUBポートを持っている場合に、自身のHUBポートのMACテーブルをフラッシュします。

Block Reset 設定

自身のPortのリンク状態を一時的にDownさせ、配下のスイッチのMACテーブルをフラッシュします。Group Blocking状態に遷移した場合のみ動作します。

L2RP 機能使用時の注意

L2RP機能を使用する場合は、Xconnect設定において以下のオプション設定を行ってください。

- Loop Detect 機能 「無効」
- known-unicast 機能 「送信する」
- Circuit Down時Frame転送設定「送信する」

第 13 章 L2TPv3 機能

VII. L2TPv3 Filter 設定

L2TPv3 Filter 設定については、第 14 章「L2TPv3 フィルタ機能」で説明します。

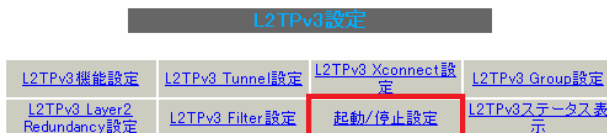
L2TPv3 設定

L2TPv3 機能設定	L2TPv3 Tunnel 設定	L2TPv3 Xconnect 設定	L2TPv3 Group 設定
L2TPv3 Layer2 Redundancy 設定	L2TPv3 Filter 設定	起動/停止設定	L2TPv3 ステータス表示

VIII. 起動 / 停止設定

L2TPv3 トンネル / セッションの起動や停止、MAC テーブルのクリア等を行います。

「各種サービスの設定」->「L2TPv3」の「起動 / 停止設定」をクリックします。



起動

トンネル / セッション接続を実行したい Xconnect インタフェースを選択します。プルダウンには、「L2TPv3 Xconnect 設定」で設定したインタフェースが表示されます。

また、Point to Multi-point 接続や L2TPv3 二重化の場合に、1セッションずつ接続したい場合は、接続したい Remote-ID をプルダウンから選択してください。

画面下部の「実行」ボタンを押下すると、接続を開始します。

停止

トンネル / セッションの停止を行います。停止したい方法を以下から選択してください。

- Local Tunnel/SessionID 指定
1セッションのみ切断したい場合は、切断するセッションの Tunnel ID/SessionID を指定してください。
- Remote-ID 指定
ある LCCE に対するセッションを全て切断したい場合は、対向 LCCE の Remote-ID を選択してください。
- Group-ID 指定
グループ内のセッションを全て停止したい場合は、停止するグループ ID を指定してください。

Local MAC テーブルクリア

L2TPv3 機能で保持しているローカル側の MAC テーブル(Local MAC テーブル)をクリアします。クリアしたい Xconnect Interface をプルダウンから選択してください。

FDB クリア

L2TPv3 機能で保持している L2TP セッション側の MAC テーブル(FDB)をクリアします。Group ID を選択した場合は、そのグループで持つ FDB のみクリアします。Xconnect Interface をプルダウンから選択した場合は、その Interface で持つ全てのセッション ID の FDB をクリアします。

なお、Local MAC テーブル / FDB における MAC テーブルは、本装置の「情報表示」で表示される ARP テーブルとは別です。

VIII. 起動 / 停止設定

Peer counter クリア

「L2TPv3 ステータス表示」で表示される「Peer ステータス表示」のカウンタをクリアします。プルダウンからクリアしたいRemote-IDを選択してください。プルダウンには、「L2TPv3 Xconnect 設定」で設定したPeer IDが表示されます。

Tunnel Counter クリア

「L2TPv3 ステータス表示」で表示される「Tunnel ステータス表示」のカウンタをクリアします。クリアしたいTunnel IDを指定してください。

Session counter クリア

「L2TPv3 ステータス表示」で表示される「Session ステータス」のカウンタをクリアします。クリアしたいセッションIDを指定してください。

Interface counter クリア

「L2TPv3 ステータス表示」で表示される「Xconnect Interface 情報表示」のカウンタをクリアします。プルダウンからクリアしたいインタフェースを選択してください。プルダウンには、「L2TPv3 Xconnect 設定」で設定したインタフェースが表示されます。

第13章 L2TPv3 機能

IX. L2TPv3 ステータス表示

L2TPv3の各種ステータスを表示します。

「各種サービスの設定」->「L2TPv3」の
「L2TPv3 ステータス表示」をクリックします。

L2TPv3設定			
L2TPv3機能設定	L2TPv3 Tunnel設定	L2TPv3 Xconnect設定	L2TPv3 Group設定
L2TPv3 Layer2 Redundancy設定	L2TPv3 Filter設定	起動/停止設定	L2TPv3ステータス表示

L2TPv3 ステータス表示		
Xconnect Interface情報表示	--- <input checked="" type="checkbox"/> detail表示	表示する
MAC Table/FDB情報表示	--- <input checked="" type="checkbox"/> local MAC Table表示 <input checked="" type="checkbox"/> FDB表示	表示する
Peerステータス表示	Router-ID <input type="text"/>	表示する
Tunnelステータス表示	Tunnel ID <input type="text"/> <input checked="" type="checkbox"/> detail表示	表示する
Sessionステータス表示	Session ID <input type="text"/> <input checked="" type="checkbox"/> detail表示	表示する
Groupステータス表示	Group ID <input type="text"/>	表示する
すべてのステータス情報表示		表示する

[各種サービスの設定画面へ](#)

Xconnect Interface 情報表示

Xconnect インタフェースのカウンタ情報を表示します。プルダウンから表示したいインタフェースを選択してください。

「detail 表示」にチェックを入れると詳細情報を表示することができます。

MAC Table/FDB 情報表示

L2TPv3 機能が保持している MAC アドレステーブルの内容を表示します。プルダウンから表示したい Xconnect インタフェースを選択してください。

なお、ローカル側で保持する MAC テーブルを表示したい場合は、「local MAC Table 表示」にチェックを入れ、L2TP セッション側で保持する MAC テーブルを表示したい場合は、「FDB 表示」にチェックを入れてください。両方にチェックを入れることもできます。

Peer ステータス表示

Peer ステータス情報を表示します。表示したい Router-ID を指定してください。

Tunnel ステータス表示

L2TPv3 トネルの情報のみを表示します。

「detail 表示」にチェックを入れると詳細情報を表示することができます。

Session ステータス表示

L2TPv3 セッションの情報とカウンタ情報を表示します。表示したいセッション ID を指定してください。指定しない場合は全てのセッションの情報を表示します。

「detail 表示」にチェックを入れると詳細情報を表示することができます。

Group ステータス表示

L2TPv3 グループの情報を表示します。プライマリ・セカンダリの Xconnect / セッション情報と現在 Active のセッション ID が表示されます。表示したいグループ ID をプルダウンから選択してください。選択しない場合は全てのグループの情報を表示します。

すべてのステータス情報表示

上記5つの情報を一覧表示します。

X. 制御メッセージ一覧

L2TPのログには各種制御メッセージが表示されます。メッセージの内容については、下記を参照してください。

[制御コネクション関連メッセージ]

SCCRQ : Start-Control-Connection-Request

制御コネクション(トンネル)の確立を要求するメッセージ。

SCCRP : Start-Control-Connection-Reply

SCCRQ に対する応答メッセージ。トンネルの確立に同意したことを示します。

SCCCN : Start-Control-Connection-Connected

SCCRP に対する応答メッセージ。このメッセージにより、トンネルが確立したことを示します。

StopCCN : Stop-Control-Connection-Notification

トンネルを切断するメッセージ。これにより、トンネル内のセッションも切断されます。

HELLO : Hello

トンネルの状態を確認するために使われるメッセージ。

[呼管理関連メッセージ]

ICRQ : Incoming-Call-Request

リモートクライアントから送られる着呼要求メッセージ。

ICRP : Incoming-Call-Reply

ICRQ に対する応答メッセージ。

ICCN : Incoming-Call-Connected

ICRP に対する応答メッセージ。このメッセージにより、L2TPセッションが確立した状態になったことを示します。

CDN : Call-Disconnect-Notify

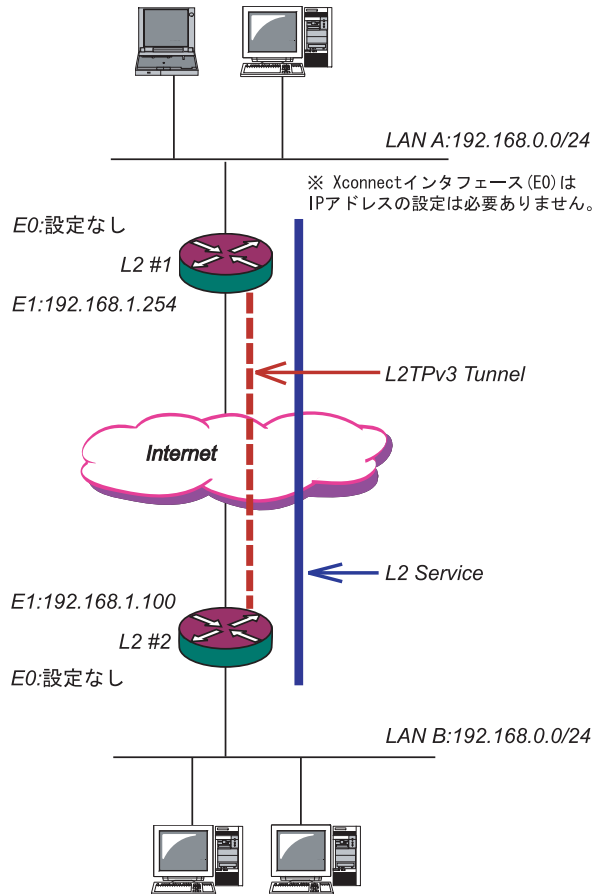
L2TPセッションの切断を要求するメッセージ。

第13章 L2TPv3 機能

XI. L2TPv3 設定例 1(2拠点間のL2TPトンネル)

2拠点間でL2TPトンネルを構築し、End to EndでEthernetフレームを透過的に転送する設定例です。

構成図(例)



注：画像は全て XR-640L2 で設定を行っています。

L2TPv3 サービスの起動

L2TPv3 機能を設定するときは、はじめに「各種サービス」の「L2TPv3」を起動してください。

DNSサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい		停止中
L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい		停止中

第13章 L2TPv3 機能

XI. L2TPv3 設定例 1(2 拠点間の L2TP トンネル)

L2 #1 ルータの設定

L2TPv3 機能設定をします。

・Local Router-IDはIPアドレス形式で設定します(この設定例ではEther1ポートのIPアドレスとしています)。

Local hostname	L2-1
Local Router-ID	192.168.1.254
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Debug設定 (Syslogメッセージ出力設定)	<input type="checkbox"/> Tunnel Debug出力 <input type="checkbox"/> Session Debug出力 <input checked="" type="checkbox"/> L2TPエラーメッセージ出力

L2TPv3 Xconnect Interface設定をします。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.100
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

L2TPv3 Tunnel 設定をします。

・「AVP Hiding」「Digest type」を使用するときは、「パスワード」を設定する必要があります。
 ・PPPoE接続とL2TPv3接続を連動させるときは、「Bind Interface」にPPPインタフェース名を設定します。
 ・XR-410L2で設定をする場合は、「Vendor ID」を0に設定してください。

Description	sample
Peerアドレス	192.168.1.100 (例192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-2
Remote RouterID設定	192.168.1.100
Vendor ID設定	20376:CENTURY
Bind Interface設定	

第13章 L2TPv3 機能

XI. L2TPv3 設定例1 (2拠点間のL2TPトンネル)

L2 #2 ルータの設定

L2TPv3 機能設定をします。

Local hostname	L2-2
Local Router-ID	192.168.1.100
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Debug設定 (Syslogメッセージ出力設定)	<input type="checkbox"/> Tunnel Debug出力 <input type="checkbox"/> Session Debug出力 <input checked="" type="checkbox"/> L2TPエラーメッセージ出力

L2TPv3 Xconnect Interfaceの設定をします。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.254
L2Frame受信インターフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合は付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

L2TPv3 Tunnel 設定をします。

・XR-410L2で設定をする場合は、「Vendor ID」を0に設定してください。

Description	sample
Peerアドレス	192.168.1.254 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-1
Remote RouterID設定	192.168.1.254
Vendor ID設定	20376-CENTURY
Bind Interface設定	

XI. L2TPv3 設定例 1 (2 拠点間の L2TP トンネル)

L2TPv3TunnelSetup の起動

ルータの設定後、「起動 / 停止設定」画面で L2TPv3 接続を開始させます。

下の画面で「起動」にチェックを入れ、Xconnect Interface と Remote-ID を選択します。

画面下の「実行」ボタンをクリックすると L2TPv3 接続を開始します。

Tunnel Setup 起動/停止
MAC テーブルクリア
カウンタクリア

起動
Xconnect Interface 選択 eth0
Remote-ID 選択 192.168.1.254

停止(下記を選択してください)
 Local Tunnel/Session ID 指定
 Tunnel ID
 Session ID
 Remote-ID 指定
 Remote-ID 選択 ---
 Group-ID 指定
 Group ID 選択
 Local MAC テーブルクリア
 Interface 選択 ---
 FDB クリア
 Interface 選択 ---
 Group ID 選択
 Peer counter クリア
 Remote-ID 選択 ---
 Tunnel counter クリア
 Local Tunnel ID
 Session counter クリア
 Local Session ID
 Interface counter クリア
 Interface 選択 ---

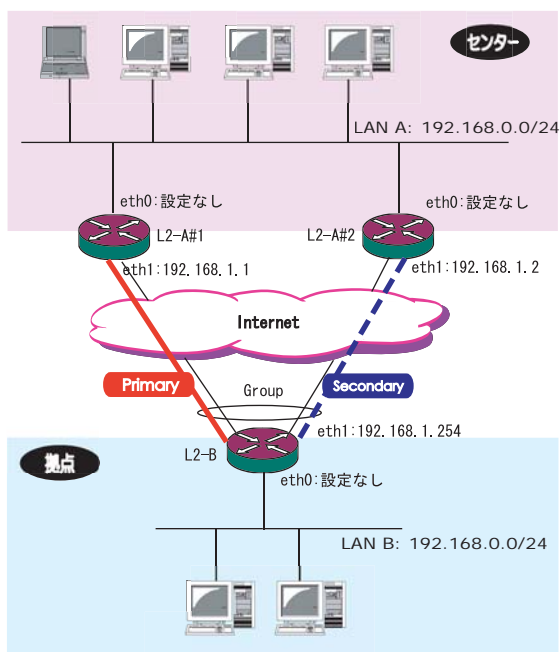
L2TPv3 接続を停止するときは、「起動 / 停止設定」画面で停止するか、各種サービス設定画面で L2TPv3 を停止します。

XII. L2TPv3 設定例 2 (L2TP トンネル二重化)

次に、センター側を 2 台の冗長構成にし、拠点 / センター間の L2TP トンネルを二重化する場合の設定例です。

本例では、センター側の 2 台の XR のそれぞれに対し、拠点側 XR から L2TPv3 セッションを張り、Secondary 側セッションは STAND-BY セッションとして待機させるような設定を行います。

構成図 (例)



第 13 章 L2TPv3 機能

XII. L2TPv3 設定例 2 (L2TP トンネル二重化)

L2-A#1/L2-A#1(センター側)ルータの設定

L2-A#1 (Primary) ルータの L2TPv3 機能設定をします。

- ・「LocalHostName」には任意のホスト名を設定します。
- ・「Local Router-ID」にはWAN側のIPアドレスを設定します。

Local hostname	L2-A1
Local Router-ID	192.168.1.1
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Debug設定 (Syslogメッセージ出力設定)	<input type="checkbox"/> Tunnel Debug出力 <input type="checkbox"/> Session Debug出力 <input checked="" type="checkbox"/> L2TPエラーメッセージ出力

XR-640L2

L2-A#2 (Secondary) ルータの L2TPv3 機能設定をします。

- ・Primaryルータと同じ要領で設定してください。

Local hostname	L2-A2
Local Router-ID	192.168.1.2
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Debug設定 (Syslogメッセージ出力設定)	<input type="checkbox"/> Tunnel Debug出力 <input type="checkbox"/> Session Debug出力 <input checked="" type="checkbox"/> L2TPエラーメッセージ出力

L2-A#1 (Primary) ルータの Tunnel 設定をします。

- ・「Peer アドレス」には拠点側ルータのWAN側のIPアドレスを設定します。
- ・「LocalHostName」「Local Router-ID」が未設定の場合は、機能設定で設定した値が使用されます。
- ・「Local Router-ID」にはWAN側のIPアドレスを設定します。
- ・「RemoteHostName」「Remote Router-ID」は、それぞれ拠点側ルータで設定する「LocalHostName」「Local Router-ID」と同じものを設定します。
- ・XR-410L2で設定をする場合は、「Vendor ID」を0に設定してください。

Description	primary
Peerアドレス	192.168.1.254 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-B
Remote RouterID設定	192.168.1.254
Vendor ID設定	20376:CENTURY
Bind Interface設定	

XII. L2TPv3 設定例 2 (L2TP トンネル二重化)

L2-A#2 (Secondary) ルータの Tunnel 設定をします。

- Primary ルータと同じ要領で設定してください。本例の場合、Primary ルータと同じ設定になります。

Description	secondary
Peer アドレス	192.168.1.254 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type 設定	無効
Hello Interval 設定	60 [0-1000] (default 60s)
Local Hostname 設定	
Local RouterID 設定	
Remote Hostname 設定	L2-B
Remote RouterID 設定	192.168.1.254
Vendor ID 設定	20376:CENTURY
Bind Interface 設定	

L2-A#1 (Primary) ルータの Xconnect Interface 設定をします。

- 「Xconnect ID 設定」は Group 設定を行わないので設定不要です。
- 「Tunnel 設定選択」はプルダウンから拠点側ルータの Peer アドレスを選択します。
- 「L2Frame 受信インターフェース」は LAN 側のインターフェースを指定します。**LAN 側インターフェースには IP アドレスを設定する必要はありません。**
- 「Remote End ID 設定」は任意の END ID を設定します。必ず拠点側ルータの Primary セッションと同じ値を設定してください。

Xconnect ID 設定 (Group 設定を行う場合は指定)	[1-4294967295]
Tunnel 設定選択	192.168.1.254
L2Frame 受信インターフェース 設定	eth0 (interface 名指定)
VLAN ID 設定 (VLAN Tag 付与する場合指定)	0 [0-4094] (0 の場合付与しない)
Remote END ID 設定	1 [1-4294967295]
Reschedule Interval 設定	0 [0-1000] (default 0s)
Auto Negotiation 設定 (Service 起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS 設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS 値 (byte)	0 [0-1460] (0 の場合は自動設定)
Loop Detect 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast 設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down 時 Frame 転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

第 13 章 L2TPv3 機能

XII. L2TPv3 設定例 2 (L2TP トンネル二重化)

L2-A#2 (Secondary) ルータの Xconnect Interface 設定をします。

- Primary ルータと同じ要領で設定してください。
- 「Remote End ID 設定」は、拠点側ルータの Secondary セッションと同じ値を設定します。

L2TPv3 Group 設定について

- Primary、Secondary ルータともに、L2TP セッションの Group 化は行わないので、設定の必要はありません。

Xconnect ID 設定 (Group 設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel 設定選択	192.168.1.254
L2Frame 受信インターフェース設定	eth0 (interface 名指定)
VLAN ID 設定 (VLAN Tag 付与する場合指定)	0 [0-4094] (0 の場合付与しない)
Remote END ID 設定	2 [1-4294967295]
Reschedule Interval 設定	0 [0-1000] (default 0s)
Auto Negotiation 設定 (Service 起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS 設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS 値(byte)	0 [0-1460] (0 の場合は自動設定)
Loop Detect 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast 設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down 時 Frame 転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

第 13 章 L2TPv3 機能

XII. L2TPv3 設定例 2 (L2TP トンネル二重化)

L2-B(拠点側ルータ)の設定

L2TPv3 機能設定をします。

- ・「LocalHostName」には任意のホスト名を設定します。
- ・「Local Router-ID」にはWAN側のIPアドレスを設定します。

Local hostname	L2-B
Local Router-ID	192.168.1.254
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP 機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Debug設定 (Syslogメッセージ出力設定)	<input type="checkbox"/> Tunnel Debug出力 <input type="checkbox"/> Session Debug出力 <input checked="" type="checkbox"/> L2TPエラーメッセージ出力

Primaryセッション側のL2TPv3 Tunnel設定をします。

- ・「Peerアドレス」にはセンター側PrimaryルータのWAN側のIPアドレスを設定します。
- ・「Hello Interval設定」を設定した場合、L2TPセッションのKeep-Aliveを行います。回線または対向LCCEの障害を検出し、ACTIVEセッションをSecondary側へ自動的に切り替えることができます。
- ・「LocalHostName」「Local Router-ID」が未設定の場合は、機能設定で設定した値が使用されます。
- ・「Local Router-ID」にはWAN側のIPアドレスを設定します。
- ・「RemoteHostName」「Remote Router-ID」は、それぞれセンター側Primaryルータで設定する「LocalHostName」「Local Router-ID」と同じものを設定します。
- ・XR-410L2で設定をする場合は、「Vendor ID」を0に設定してください。

Description	primary
Peerアドレス	192.168.1.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-A1
Remote RouterID設定	192.168.1.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	

XII. L2TPv3 設定例 2 (L2TP トンネル二重化)

Primary セッション側の L2TPv3 Tunnel 設定をします。

- Primary セッションと同じ要領で設定してください。

Description	secondary
Peerアドレス	192.168.1.2 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-A2
Remote RouterID設定	192.168.1.2
Vendor ID設定	20376:CENTURY
Bind Interface設定	

Primary セッション側の L2TPv3 Xconnect 設定をします。

- 「Xconnect ID 設定」は任意の Xconnect ID を設定します。必ず Secondary 側と異なる値を設定してください。
- 「Tunnel 設定選択」はプルダウンから Primary セッションの Peer アドレスを選択します。
- 「L2Frame 受信インターフェース」は LAN 側のインターフェースを指定します。**LAN 側インターフェースには IP アドレスを設定する必要はありません。**
- 「Remote End ID 設定」は任意の END ID を設定します。必ずセンター側 Primary ルータで設定する End ID と同じ値を設定します。但し、Secondary 側と同じ値は設定できません。
- 「Reschedule Interval 設定」に任意の Interval 時間を設定してください。この場合、L2TP セッションの切断検出時に自動的に再接続を行います。

Xconnect ID 設定 (Group 設定を行う場合は指定)	1 [1-4294967295]
Tunnel 設定選択	192.168.1.1
L2Frame 受信インターフェース設定	eth0 (interface 名指定)
VLAN ID 設定 (VLAN Tag 付与する場合指定)	0 [0-4094] (0 の場合付与しない)
Remote END ID 設定	1 [1-4294967295]
Reschedule Interval 設定	0 [0-1000] (default 0s)
Auto Negotiation 設定 (Service 起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS 設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS 値 (byte)	0 [0-1460] (0 の場合は自動設定)
Loop Detect 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast 設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down 時 Frame 転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

X11. L2TPv3 設定例 2 (L2TP トンネル二重化)

Secondary セッション側の L2TPv3 Xconnect 設定をします。

- Primary セッションと同じ要領で設定してください。

Xconnect ID設定 (Group設定を行う場合は指定)	2 [1-4294967295]
Tunnel設定選択	192.168.1.2
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	2 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

L2TPv3 Group 設定をします。

- 「Group ID」は任意のグループ ID を設定します。
- 「Primary Xconnect 設定選択」はプルダウンから Primary セッションの Xconnect ID を選択します。
- 「Secondary Xconnect 設定選択」はプルダウンから Secondary セッションの Xconnect ID を選択します。
- 本例では「Preempt 設定」「Primary active 時の Secondary Session 強制切断設定」をそれぞれ「無効」に設定しています。常に Primary/Secondary セッションの両方が接続された状態となり、Secondary セッション側は Stand-by 状態として待機しています。Primary セッションの障害時には、Secondary セッションを即時に Active 化します。

Group ID	1 [1-4095]
Primary Xconnect 設定選択	1
Secondary Xconnect 設定選択	2
Preempt 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Primary active 時の Secondary Session 強制切断設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Active Hold 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XII. L2TPv3 設定例 2 (L2TP トンネル二重化)

L2TPv3 Tunnel Setup の起動

設定後が終わりましたら L2TPv3 機能の起動 / 停止設定を行います。

「起動 / 停止」画面で Xconnect Interface と Remote-ID を選択し、画面下の「実行」ボタンをクリックすると L2TPv3 接続を開始します。

本例では、拠点側から Primary/Secondary の両方の L2TPv3 接続を開始し、Primary 側が ACTIVE セッション、Secondary 側は STAND-BY セッションとして確立します。

L2TPv3 接続を停止するときは、「起動 / 停止設定」画面で停止するか、各種サービス設定画面で L2TPv3 を停止します。

第 14 章

L2TPv3 フィルタ機能

I. L2TPv3 フィルタ 機能概要

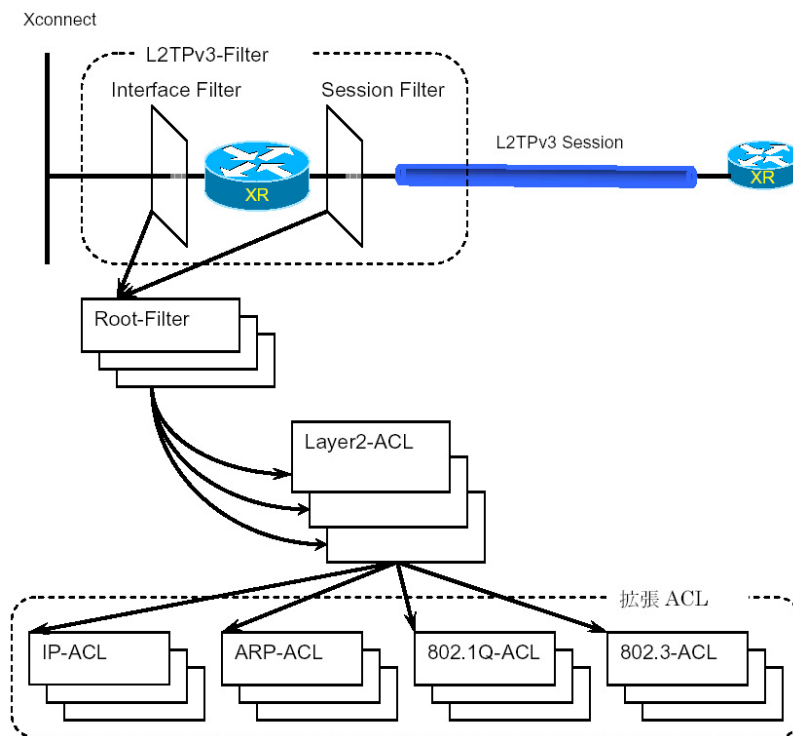
L2TPv3 フィルタ概要

XR の L2TPv3 フィルタ機能は、ユーザが設定したフィルタリングルールに従い、Xconnect Interface 上もしくは Session 上でアクセス制御を行ないます。

アクセス制御は、MAC アドレスや IPv4、ARP、802.1Q、TCP/UDP など L2-L4 での詳細な指定が可能です。

L2TPv3 フィルタ設定概要

L2TPv3 フィルタは以下の要素で構成されています。



(1) Access Control List (ACL)

Layer2 レベルでルールを記述する「Layer2 ACL」およびプロトコル毎に詳細なルールを記述する拡張 ACL として IP-ACL、ARP-ACL、802.1Q-ACL、802.3-ACL があります。

(2) Root-Filter

Root-Filter では Layer2 ACL を検索する順にリストします。各 Root Filter にはユーザによりシステムでユニークな名前を付与し、識別します。

Root Filter では、配下に設定された全ての Layer2 ACL に一致しなかった場合の動作を Default ポリシーとします。Default ポリシーとして定義可能な動作は、deny (破棄) / permit (許可) です。

(3) L2TPv3-Filter

Xconnect Interface、Session それぞれに適用する Root-Filter を設定します。Xconnect Interface に関しては Interface Filter、Session に関しては Session Filter で設定します。

1. L2TPv3 フィルタ 機能概要

L2TPv3 フィルタの動作 (ポリシー)

設定条件に一致した場合、L2TPv3 フィルタは以下の動作を行います。

1) 許可 (permit)

フィルタルールに一致した場合、検索を中止してフレームを転送します。

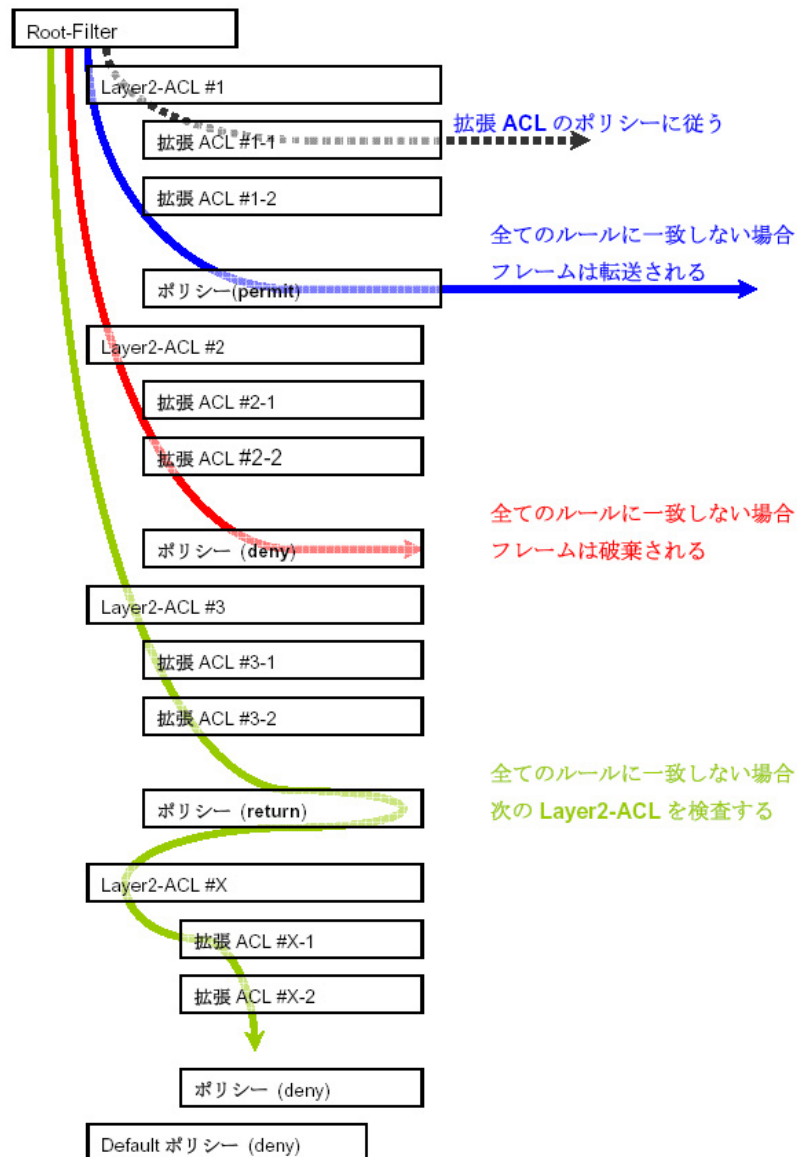
2) 破棄 (deny)

フィルタルールに一致した場合、検索を中止してフレームを破棄します。

3) 復帰 (return)

Layer2 ACL でのみ指定可能です。フィルタルールに一致しない場合、該当 Layer2 ACL での検索を中止して呼び出し元の次の Layer2 ACL から検索を再開します。

フィルタ評価のモデル図



第 14 章 L2TPv3 フィルタ機能

1. L2TPv3 フィルタ 機能概要

フィルタの評価

Root-Filter の配下に設定された Layer2 ACL の検索は、定義された上位から順番に行い、最初に条件に一致したもの (1st match) に対して以下の評価を行います。

- ・ 拡張 ACL がない場合
該当 Layer2 ACL のポリシーに従い、deny/permit/return を行います。
- ・ 拡張 ACL がある場合
Layer2 ACL の配下に設定された拡張 ACL の検索は、1st match にて検索を行い、以下の評価を行います。
 - 1) 拡張 ACL に一致する場合、拡張 ACL の policy に従い deny/permit を行います。
 - 2) 全ての拡張 ACL に一致しない場合、該当 Layer2 ACL のポリシーに従い、deny/permit/return を行います。

フレームが配下に設定された全ての Layer2 ACL に一致しなかった場合は、Default ポリシーによりフレームを deny または permit します。

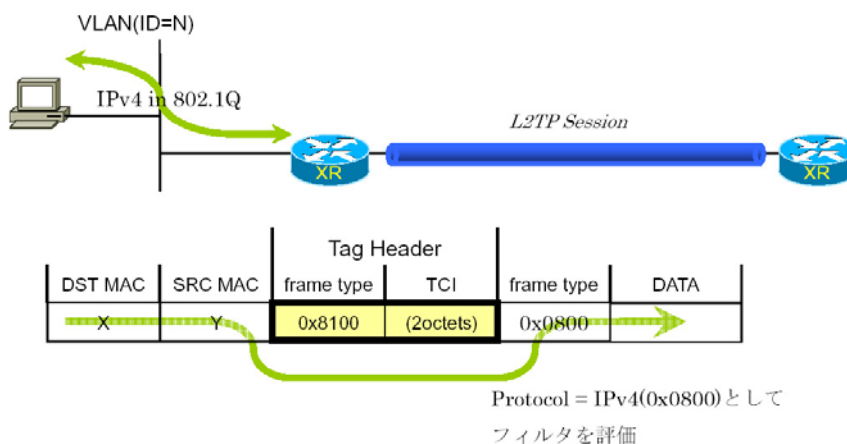
フィルタ処理順序

L2TPv3 フィルタにおける処理順序は、IN 側フィルタでは送信元 / 宛先 MAC アドレスのチェックを行ったあとになります。

「Known Unicast 設定」や「Circuit Down 時の Frame 転送」によりフレームの転送が禁止されている状態で permit 条件に一致するフレームを受信しても、フレームの転送は行われませんのでご注意ください。

802.1Q タグヘッダ

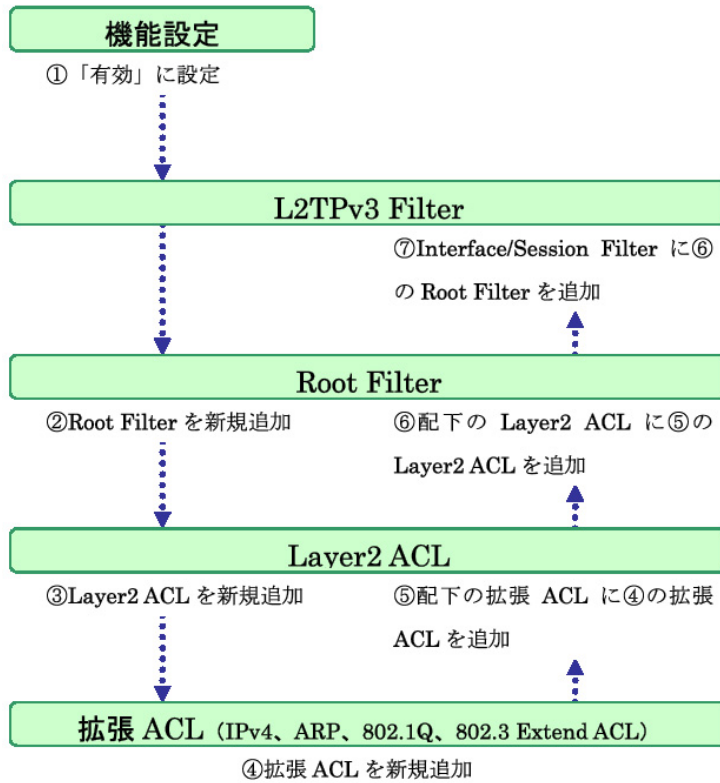
Xconnect Interface が VLAN(802.1Q) であるフレームをフィルタリングする場合、タグヘッダについては、フィルタの評価対象から除外し、タグヘッダに続くフィールドから再開します(下図参照)。



II. 設定順序について

L2TPv3 Filter の設定順序は、下の表を参考にしてください。

【L2TPv3 Filter の設定順序】



第 14 章 L2TPv3 フィルタ機能

III. 機能設定

「各種サービスの設定」 「[L2TPv3](#)」をクリックして、画面上部の「L2TPv3 Filter 設定」をクリックします。

L2TPv3設定			
L2TPv3機能設定	L2TPv3 Tunnel設定	L2TPv3 Xconnect設定	L2TPv3 Group設定
L2TPv3 Layer2 Redundancy設定	L2TPv3 Filter設定	起動/停止設定	L2TPv3ステータス表示

L2TPv3 フィルタは以下の画面で設定を行います。

L2TPv3 Filter設定				
機能設定	L2TPv3 Filter設定	Root Filter設定	Layer2 ACL設定	IPv4 Extend ACL設定
ARP Extend ACL設定	802.1Q Extend ACL設定	802.3 Extend ACL設定	情報表示	

機能設定

L2TPv3 フィルタ設定画面の「機能設定」をクリックします。

機能設定	
本機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
リセット 設定 戻る	

本機能

L2TPv3 Filter 機能の有効 / 無効を選択し、設定ボタンを押します。

* 設定で可能な文字について

Root Filter・ACL 名で使用可能な文字は英数字、ハイフン(-)、アンダースコア(_)、ピリオド(.)です。1 ~ 64文字の間で設定できます。ただし、1文字目は英数字に限ります。

IV. L2TPv3 Filter 設定

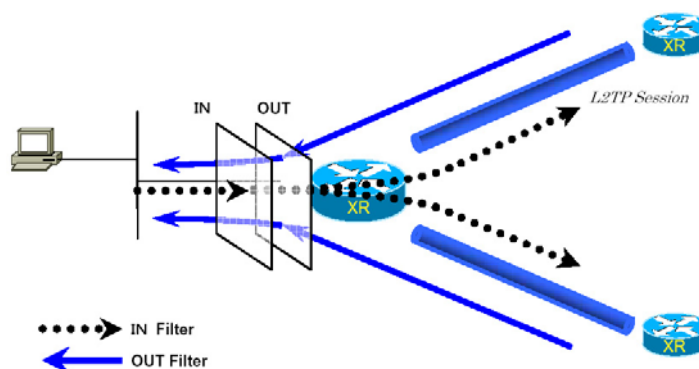
L2TPv3 Filter 設定画面の「L2TPv3 Filter 設定」をクリックします。
 現在設定されている Interface Filter と Session Filter が一覧表示されます。

Interface Filter

Interface Filter

Index	Interface	IN Filter	OUT Filter	edit
1	eth0	Root-1	Root-2	edit

Interface Filter は、Root Filter を Xconnect Interface に対応づけてフィルタリングを行います。
 IN Filter は外側のネットワークから Xconnect Interface を通して XR が受信するフレームをフィルタリングします。OUT Filter は XR が Xconnect Interface を通して送信するフレームをフィルタリングします。



Interface Filter のモデル図

Interface Filter を編集する

Interface Filter 一覧表示内の「edit」ボタンをクリックします。

L2TPv3 Filter 適用設定

Interface	eth0
ACL(in)	Root-1
ACL(out)	Root-2

Interface

Xconnect Interface に設定したインターフェース名が表示されます。

ACL(in)

IN 方向に設定する Root Filter 名を選択します。

ACL(out)

OUT 方向に設定する Root Filter 名を選択します。

第 14 章 L2TPv3 フィルタ機能

IV. L2TPv3 Filter 設定

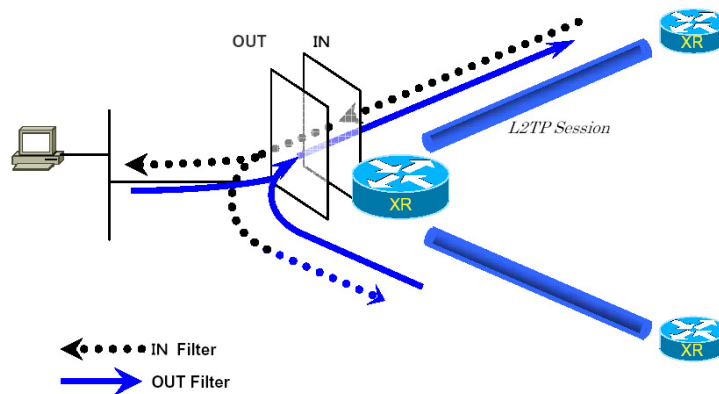
Session Filter

Session Filter

Index	Peer ID	RemoteEND ID	IN Filter	OUT Filter	edit
1	192.168.0.1	1	Root-2	Root-3	edit
2	192.168.0.2	2	Root-3	Root-4	edit

Session Filter は、Root Filter を Session に関連づけてフィルタリングを行いますので、Session から Session への通信を制御することが出来ます。

下の図で、IN Filter は XR が L2TP Session A から受信するフレームをフィルタリングしています。OUT Filter は XR が L2TP Session A へ送信するフレームをフィルタリングしています。



Session Filter のモデル図

Session Filter を編集する

Session Filter 一覧表示内の「edit」ボタンをクリックします。

L2TPv3 Filter適用設定

PeerID : RemoteEndID	192.168.0.1:1
ACL(in)	Root-2
ACL(out)	Root-3

PeerID : RemoteEndID

対向側の Xconnect Interface ID と Remote End ID が表示されます。

ACL(in)

IN 方向に設定したい Root Filter 名を選択します。

ACL(out)

OUT 方向に設定したい Root Filter 名を選択します。

V. Root Filter 設定

L2TPv3 Filter 設定画面の「Root Filter 設定」をクリックします。
現在設定されている Root Filter が一覧表示されます。

L2TPv3 Filter 一覧表示

Index	Root Filter Name	edit	layer2	del
1	Root-1	edit	layer2	<input type="checkbox"/>
2	Root-2	edit	layer2	<input type="checkbox"/>
3	Root-3	edit	layer2	<input type="checkbox"/>
4	Root-4	edit	layer2	<input type="checkbox"/>

(最大512個まで設定できます)

[リセット](#) [追加](#) [削除](#) [戻る](#)

Root Filter を追加する

画面下の「追加」ボタンをクリックします。

L2TPv3 Filter 設定

Root Filter Name	<input type="text"/>
Default Policy	deny <input type="button" value="v"/>

[リセット](#) [設定](#) [戻る](#)

Root Filter Name

Root Filter を識別するための名前を入力します (*).

Default Policy

受け取ったフレームが、その Root Filter の配下にある Layer2 ACL のすべてに一致しなかった場合の動作を設定します。Permit/Deny のどちらかを選択してください。

Root Filter を編集する

一覧表示内の「edit」をクリックします。

L2TPv3 Filter 設定

Index	1
Root Filter Name	Root-1 <input type="text"/>
Default Policy	deny <input type="button" value="v"/>

[リセット](#) [設定](#) [戻る](#)

追加画面と同様に設定してください。

Root Filter を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

V. Root Filter 設定

配下に Layer2 ACL を設定する

一覧表示内の「layer2」をクリックします。

現在設定されている配下の Layer2 ACL が一覧表示されます。

Seq.No.	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length	edit	del
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4	edit	<input type="checkbox"/>
*	default	deny					

配下の Layer2 ACL を追加する

画面下の「追加」ボタンをクリックします。

Seq.No.	<input type="text"/>
Layer2 ACL Name	---- <input type="button" value="v"/>

Seq.No.

配下の Layer2 ACL を検索する際の順番（シーケンス番号）を指定します。無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

Layer2 ACL Name

その Root Filter の配下に設定したい Layer2 ACL を選択します。同一 Root Filter 内で重複する Layer2 ACL を設定することはできません。

配下の Layer2 ACL を編集する

一覧表示内の「edit」をクリックします。

Seq.No.	1
Layer2 ACL Name	L2ACL-1 <input type="button" value="v"/>

追加画面と同様に設定してください。

配下の Layer2 ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

第 14 章 L2TPv3 フィルタ機能

VI. Layer2 ACL 設定

L2TPv3 Filter 設定画面の「Layer2 ACL 設定」をクリックします。
現在設定されている Layer2 ACL が一覧表示されます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length	edit	extend	del
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4	edit	extend	<input type="checkbox"/>

Layer2 ACL を追加する

画面下の「追加」ボタンをクリックします。

Layer2 ACL Name	<input type="text"/>
Policy	---- <input type="button" value="v"/>
Source MAC	<input type="text"/>
Destination MAC	<input type="text"/>
Type/Length	---- <input type="button" value="v"/> or <input type="text"/> [0x0600-0xffff]

Layer2 ACL Name

ACLを識別するための名前を入力します(*)。

Policy

deny (破棄) / permit (許可) / return (復帰) のいずれかを選択します。

Source MAC

送信元 MAC アドレスを指定します (マスクによるフィルタリングも可能です)。

<フォーマット>

XX:XX:XX:XX:XX:XX

XX:XX:XX:XX:XX:XX/MM:MM:MM:MM:MM:MM

Destination MAC

あて先 MAC アドレスを指定します。Source MAC 設定と同様に設定してください。

Type/Length

IPv4、IPv6、ARP、802.1Q、length または 16 進数指定の中から選択します (無指定でも可)。16 進数指定の場合は右側の入力欄に指定値を入力します。(指定可能な範囲 : 0600-ffff)。

IPv4、ARP、802.1Q を指定すると配下の拡張 ACL に IPv4 Extend ACL、ARP Extend ACL、802.1Q Extend ACL を指定することが出来ます。16 進数で length を指定すると、802.3 Extend ACL を指定することが出来ます。

Layer2 ACL を編集する

一覧表示内の「edit」をクリックします。

Layer2 ACL Name	L2ACL-1
Policy	permit <input type="button" value="v"/>
Source MAC	00:11:22:33:44:55
Destination MAC	<input type="text"/>
Type/Length	IPv4 <input type="button" value="v"/> or <input type="text"/> [0x0600-0xffff]

追加画面と同様に設定してください。

Layer2 ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

VI. Layer2 ACL 設定

配下に拡張 ACL を設定する

一覧表示内の「extend」をクリックします。

現在設定されている配下の拡張 ACL が一覧表示されます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4

Seq.No.	Extend ACL Name	edit	del
1	IPv4-1	edit	<input type="checkbox"/>

配下の拡張 ACL を追加する

画面下の「追加」ボタンをクリックします。

Seq.No.	<input type="text"/>
Name	----- <input type="button" value="v"/>

Seq.NO.

配下の拡張 ACL を検索する際の順番（シーケンス番号）を指定します。無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

Name

設定可能な拡張 ACL 名を選択します。同一 Layer2 ACL 内で重複する拡張 ACL を設定することはできません。

配下の拡張 ACL を編集する

一覧表示内の「edit」をクリックします。

Seq.No.	1
Name	IPv4acl_sample <input type="button" value="v"/>

追加画面と同様に設定してください。

配下の拡張 ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

第14章 L2TPv3 フィルタ機能

VII. IPv4 Extend ACL 設定

L2TPv3 Filter 設定画面の「IPv4 Extend ACL 設定」をクリックします。
現在設定されている IPv4 Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	Source IP	Destination IP	TOS	Protocol	option	edit	del
1	IPv4-1	permit	192.168.0.100	192.168.0.200		tcp		edit	<input type="checkbox"/>

オプション欄表示の意味は次の通りです。

- ・src-port=X 送信元ポート番号が X
- ・dst-port=X:Y あて先ポート番号の範囲が X ~ Y

IPv4 Extend ACL を追加する

画面下の「追加」ボタンをクリックします。

Extend ACL Name	<input type="text"/>
Policy	---- <input type="button" value="v"/>
Source IP	<input type="text"/>
Destination IP	<input type="text"/>
TOS	<input type="text"/> [0-0xff]
IP Protocol	---- <input type="button" value="v"/> or <input type="text"/> [0-255]
Source Port	<input type="text"/> [1-65535]
Destination Port	<input type="text"/> [1-65535]
ICMP Type	<input type="text"/> [0-255]
ICMP Code	<input type="text"/> [0-255]

Extend ACL Name
拡張 ACL を識別するための名前を入力します(*)。

Policy
deny (破棄) / permit (許可) を選択します。

Source IP
送信元 IP アドレスを指定します (マスクによる指定も可)。
<フォーマット>
A.B.C.D
A.B.C.D/M

Destination IP
あて先 IP アドレスを指定します。Source IP と同様に設定してください。

TOS
TOS 値を 16 進数で指定します。
(指定可能な範囲 : 00-ff)

IP Protocol

TCP/UDP/ICMP または 10 進数指定の中から選択します (無指定でも可)。
10 進数指定の場合は右側の入力欄に指定値を入力してください (指定可能な範囲 : 0-255)。

Source Port

送信元ポートを指定します。IP Protocol に TCP/UDP を指定した時のみ設定可能です。
範囲設定が可能です。

<フォーマット>

xxx (ポート番号 xx)
xxx:yyy (xxx 以上、yyy 以下のポート番号)

Destination Port

あて先ポートを指定します。設定方法は Source Port と同様です。

ICMP Type

ICMP Type の指定が可能です。IP Protocol に ICMP を指定した場合のみ設定可能です。
(指定可能な範囲 : 0-255)

ICMP Code

ICMP Code の指定が可能です。ICMP Type が指定されていないと設定できません。
(指定可能な範囲 : 0-255)

VII. IPv4 Extend ACL 設定

IPv4 Extend ACL を編集する

一覧表示内の「edit」をクリックします。

Extend ACL Name	<input type="text" value="IPv4-1"/>
Policy	<input type="text" value="permit"/>
Source IP	<input type="text" value="192.168.0.100"/>
Destination IP	<input type="text" value="192.168.0.200"/>
TOS	<input type="text"/> [0-0xff]
IP Protocol	<input type="text" value="TCP"/> or <input type="text"/> [0-255]
Source Port	<input type="text"/> [1-65535]
Destination Port	<input type="text"/> [1-65535]
ICMP Type	<input type="text"/> [0-255]
ICMP Code	<input type="text"/> [0-255]

追加画面と同様に設定してください。

IPv4 Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

第14章 L2TPv3 フィルタ機能

VIII. ARP Extend ACL 設定

L2TPv3 Filter 設定画面の「ARP Extend ACL 設定」をクリックします。
現在設定されている ARP Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	OPCODE	Source MAC	Destination MAC	Source IP	Destination IP	edit	del
1	ARP-1	permit		00:11:22:33:44:55			192.168.0.200	edit	<input type="checkbox"/>

ARP Extend ACL を追加する

画面下の「追加」ボタンをクリックします。

Extend ACL Name	<input type="text"/>
Policy	---- <input type="button" value="v"/>
OPCODE	---- <input type="button" value="v"/> or <input type="text"/> [0-65535]
Source MAC	<input type="text"/>
Destination MAC	<input type="text"/>
Source IP	<input type="text"/>
Destination IP	<input type="text"/>

Extend ACL Name
拡張 ACL を識別するための名前を入力します(*)。

Policy
deny (破棄) / permit (許可) を選択します。

OPCODE
Request、Reply、Request_Reverse、
Reply_Reverse、DRARP_Request、DRARP_Reply、
DRARP_Error、InARP_Request、ARP_NAK または 10
進数指定の中から選択します (無指定でも可)。

10進数指定の場合は右側の入力欄に指定値を入力してください (指定可能な範囲 : 0-65535)。

Source MAC
送信元 MAC アドレスを指定します (マスクによる
フィルタリングも可)。

<フォーマット>
XX:XX:XX:XX:XX:XX
XX:XX:XX:XX:XX/MM:MM:MM:MM:MM

Destination MAC
あて先 MAC アドレスを指定します。Source MAC 設
定と同様に設定してください。

Source IP
送信元 IP アドレスを指定します (マスクによる
フィルタリングも可)。

<フォーマット>
A.B.C.D
A.B.C.D/M

Destination IP
あて先 IP アドレスを指定します。Source IP 設定
と同様に設定してください。

ARP Extend ACL を編集する

一覧表示内の「edit」をクリックします。

Extend ACL Name	ARP-1
Policy	permit <input type="button" value="v"/>
OPCODE	---- <input type="button" value="v"/> or <input type="text"/> [0-65535]
Source MAC	00:11:22:33:44:55
Destination MAC	<input type="text"/>
Source IP	<input type="text"/>
Destination IP	192.168.0.200

追加画面と同様に設定してください。

ARP Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の
「削除」ボタンをクリックします。

IX. 802.1Q Extend ACL 設定

L2TPv3 Filter 設定画面の「802.1Q Extend ACL 設定」をクリックします。
現在設定されている 802.1Q Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	VLAN ID	Priority	Ethernet Type	edit	extend	del
1	802.1Q-1	permit	10		IPv4	edit	extend	<input type="checkbox"/>

802.1Q Extend ACL を追加する

画面下の「追加」ボタンをクリックします。

Name	<input type="text"/>
Policy	---- <input type="button" value="v"/>
VLAN ID	<input type="text"/> [0-4095]
Priority	<input type="text"/> [0-7]
Ethernet Type	---- <input type="button" value="v"/> or <input type="text"/> [0x0600-0xffff]

Name

拡張 ACL を識別するための名前を入力します (*).

Policy

deny (破棄) / permit (許可) のいずれかを選択します。

VLAN ID

VLAN ID を指定します。

範囲設定が可能です (指定可能な範囲 : 0-4095)。

<フォーマット>

xxx (VLAN ID : xx)

xxx:yyy (xxx 以上、yyy 以下の VLAN ID)

Priority

IEEE 802.1P で規定されている Priority Field を判定します (指定可能な範囲 : 0 - 7)。

Ethernet Type

カプセル化されたフレームの Ethernet Type を指定します。IPv4、IPv6、ARP または 16 進数指定の中から選択します (無指定でも設定可)。16 進数指定の場合は右側の入力欄に指定値を入力してください (指定可能な範囲 : 0600-ffff)。

IPv4、ARP、802.1Q を指定すると配下の拡張 ACL に IPv4 Extend ACL、ARP Extend ACL、802.1Q Extend ACL を指定することが出来ます。16 進数で length を指定すると、802.3 Extend ACL を指定することが出来ます。

802.1Q Extend ACL を編集する

一覧表示内の「edit」をクリックします。

Name	802.1Q-1
Policy	permit <input type="button" value="v"/>
VLAN ID	10 [0-4095]
Priority	<input type="text"/> [0-7]
Ethernet Type	IPv4 <input type="button" value="v"/> or <input type="text"/> [0x0600-0xffff]

追加画面と同様に設定してください。

802.1Q Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

IX. 802.1Q Extend ACL 設定

配下に拡張 ACL を設定する

一覧表示内の「extend」をクリックします。

現在設定されている配下の拡張 ACL の一覧が表示されます。

Index	Extend ACL Name	Policy	VLAN ID	Priority	Ethernet Type
1	802.1Q-1	deny	10		ARP

Seq.No.	Extend ACL Name	edit	del
1	ARP-1	edit	<input type="checkbox"/>

配下の拡張 ACL を追加する

画面下の「追加」ボタンをクリックします。

Seq.No.	<input type="text"/>
Name	---- <input type="button" value="v"/>

Seq.No.

配下の拡張 ACL を検索する際の順番（シーケンス番号）を指定します。無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

Name

設定可能な拡張 ACL 名を選択します。同一 802.1Q Extend ACL 内で重複する拡張 ACL を設定することはできません。

配下の拡張 ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

配下の拡張 ACL を編集する

一覧表示内の「edit」をクリックします。

Seq.No.	1
Name	ARP-1 <input type="button" value="v"/>

追加画面と同様に設定してください。

X. 802.3 Extend ACL 設定

L2TPV3 Filter 設定画面の「802.3 Extend ACL 設定」をクリックします。
現在設定されている 802.3 Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	DSAP/SSAP	type	edit	del
1	802.3-1	permit	0xaa		edit	<input type="checkbox"/>

802.3 Extend ACL を追加する

画面下の「追加」ボタンをクリックします。

Name	<input type="text"/>
Policy	---- ▾
DSAP/SSAP	0x <input type="text"/> [0x00-0xff]
Type	0x <input type="text"/> [0x0600-0xffff]

Name

拡張 ACL を識別するための名前を入力します(*)。

Policy

deny (破棄) / permit (許可) のいずれかを選択します。

DSAP/SSAP

16進数で DSAP/SSAP を指定します (指定可能な範囲: 00-ff)。DSAP/SSAP は等値なので 1byte で指定します。

Type

16進数で 802.3 with SNAP の type field を指定します (指定可能な範囲: 0600-ffff)。DSAP/SSAP を指定した場合は設定できません。
この入力欄で Type を指定した場合の DSAP/SSAP は 0xaa/0xaa として判定されます。

802.3 Extend ACL を編集する

一覧表示内の「edit」をクリックします。

Name	ACL-802_3-1
Policy	permit ▾
DSAP/SSAP	0x aa [0x00-0xff]
Type	0x <input type="text"/> [0x0600-0xffff]

追加画面と同様に設定してください。

802.3 Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

XI. 情報表示

L2TPv3 Filter 設定画面の「情報表示」をクリックします。

root ACL情報表示	---- <input type="checkbox"/> detail表示/リセット	表示する	カウンタリセット
layer2 ACL情報表示	---- <input type="checkbox"/> detail表示/リセット	表示する	カウンタリセット
ipv4 ACL情報表示	----	表示する	カウンタリセット
arp ACL情報表示	----	表示する	カウンタリセット
802_1q ACL情報表示	---- <input type="checkbox"/> detail表示/リセット	表示する	カウンタリセット
802_3 ACL情報表示	----	表示する	カウンタリセット
interface Filter情報表示	----	表示する	カウンタリセット
session Filter情報表示	----	表示する	カウンタリセット
すべてのACL情報表示		表示する	カウンタリセット

表示する

「表示する」ボタンをクリックすると ACL 情報を表示します。プルダウンから ACL 名を選択して個別に表示することもできます。

「detail 表示 / リセット」にチェックを入れてクリックすると、設定した全ての ACL 情報が表示されます。

カウンタリセット

「カウンタリセット」ボタンをクリックすると ACL のカウンタをリセットします。プルダウンから ACL 名を選択して個別にリセットすることもできます。

「detail 表示 / リセット」にチェックを入れてクリックすると、配下に設定されている ACL のカウンタも同時にリセットできます。

「表示する」ボタンで表示される情報は以下の通りです。
(は detail 表示にチェックを入れた時に表示されます。)

Root ACL 情報表示

Root Filter 名 総カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数) Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
(+ 拡張 ACL 名)

(カウンタ (frame 数、 byte 数)、 Policy)

+Default Policy カウンタ (frame 数、 byte 数) Default Policy

layer2 ACL 情報表示

Layer2 ACL 名

カウンタ (frame 数、 byte 数) Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
(+ 拡張 ACL 名)

(カウンタ (frame 数、 byte 数)、 Policy)

ipv4 ACL 情報表示

IPv4 ACL 名

カウンタ (frame 数、 byte 数) Policy、送信元 IP アドレス、あて先 IP アドレス、TOS、Protocol、オプション

XI. 情報表示

arp ACL 情報表示

ARP ACL 名

カウンタ (frame 数、 byte 数)、 Policy、 Code、 送信元 MAC アドレス、 あて先 MAC アドレス、 送信元 IP アドレス、 あて先 IP アドレス

802_1q ACL 情報表示

802.1Q ACL 名

カウンタ (frame 数、 byte 数)、 Policy、 VLAN-ID、 Priority、 encap-type
(+ 拡張 ACL 名)
(カウンタ (frame 数、 byte 数)、 Policy)

802_3 ACL 情報表示

802.3 ACL 名

カウンタ (frame 数、 byte 数)、 Policy、 DSAP/SSAP、 type

interface Filter 情報表示

interface、 in : カウンタ (frame 数、 byte 数) : Root Filter 名

Root Filter 名、 カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数)、 Policy、 送信元 MAC アドレス、 あて先 MAC アドレス、 Protocol
+Default Policy カウンタ (frame 数、 byte 数) Default Policy

interface、 out : カウンタ (frame 数、 byte 数) : Root Filter 名

Root Filter 名、 カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数)、 Policy、 送信元 MAC アドレス、 あて先 MAC アドレス、 Protocol
+Default Policy カウンタ (frame 数、 byte 数) Default Policy

session Filter 情報表示

Peer ID、 RemoteEND-ID、 in : カウンタ (frame 数、 byte 数) : Root Filter 名

Root Filter 名、 カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数)、 Policy、 送信元 MAC アドレス、 あて先 MAC アドレス、 Protocol
+Default Policy カウンタ (frame 数、 byte 数) Default Policy

Peer ID、 RemoteEND-ID、 out : カウンタ (frame 数、 byte 数) : Root Filter 名

Root Filter 名、 カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数)、 Policy、 送信元 MAC アドレス、 あて先 MAC アドレス、 Protocol
+Default Policy カウンタ (frame 数、 byte 数) Default Policy

第 15 章

SYSLOG 機能

syslog 機能の設定

本装置は、syslog を出力・表示することが可能です。また、他の syslog サーバに送出することもできます。さらに、ログの内容を電子メールで送ることもできます。

Web 設定画面「各種サービスの設定」->「SYSLOG サービス」をクリックして、以下の画面から設定をおこないます。

ログ機能の設定

ログの取得	出力先 <input type="text" value="本装置"/>
	送信先IPアドレス <input type="text"/>
	取得プライオリティ <input type="radio"/> Debug <input checked="" type="radio"/> Info <input type="radio"/> Notice
	--MARK--を出力する時間間隔 <input type="text" value="20"/> 分 <small>(0を設定すると--MARK--の出力を停止します。) <small>(MARKを使用する場合は取得プライオリティを Debug か Info にしてください。)</small> </small>
<input type="button" value="入力のやり直し"/> <input type="button" value="設定の保存"/>	

ログの取得

出力先

ログの出力先を「本装置」「SYSLOG サーバ」「本装置とSYSLOG サーバ」から選択します。

送信先 IP アドレス

出力先で「SYSLOG サーバ」または「本装置とSYSLOG サーバ」を指定した場合に、SYSLOG サーバの IP アドレスを指定します。

取得プライオリティ

ログ内容の出力レベルを指定します。プライオリティの内容は右の通りです。

- ・ Debug : デバッグ時に有益な情報
- ・ Info : システムからの情報
- ・ Notice : システムからの通知

--MARK-- を出力する時間間隔

syslog が動作していることを表す「--MARK--」ログを送出する間隔を指定します。取得プライオリティを Info または Debug に設定したときのみ MARK が出力されます。初期設定は 20 分です。

本体に記録しておけるログの容量には制限があります。継続的にログを取得される場合は外部の syslog サーバにログを送出するようにしてください。

「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを起動させてください。また設定を変更した場合は、サービスの再起動(「停止」「起動」)をおこなってください。

ファシリティと監視レベルについて

本装置で設定されている syslog のファシリティ・監視レベルおよび出力先は以下のようになっています。

[ファシリティ：監視レベル]

*.info;mail.none;news.none;authpriv.none

[出力先]

/var/log/messages

オプション CF カード装着時の syslog 機能 について (XR-640L2 のみ)

オプション CF カードを装着している場合は、システムログは自動的に CF カードに記録されます。

ログはローテーションして CF カードに記録されていきます。記録のタイミングは

- ・1週間ごと
- ・CF カードの空き容量が 20% に達したとき

のいずれか早い方です。

ローテーションで記録されたログは圧縮して保存されます。保存されるファイルは最大で4つです。以降は古いログファイルから順に削除されていきます。

ログファイルが作成されたときは画面上にリンクが生成され、各端末にダウンロードして利用できます。

第 16 章

SNMP エージェント機能

第16章 SNMP エージェント機能

1. SNMP エージェント機能の設定

SNMP エージェントを起動すると、SNMP マネージャから本装置の MIB Ver.2(RFC1213)およびプライベート MIB の情報を取得することができます。

Web 設定画面「各種サービス設定」 「SNMP サービス」をクリックして、以下の画面で設定します。

XR-410L2

SNMP機能の設定

SNMP マネージャ	<input type="text" value="192.168.0.0/24"/> SNMP マネージャを使いたいネットワーク範囲(ネットワーク番号/サブネット長) 又は SNMP マネージャの IP アドレスを指定して下さい。
コミュニティ名	<input type="text" value="community"/>
SNMP TRAP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
SNMP TRAP の送信先 IP アドレス	<input type="text"/>
SNMP TRAP の送信元	<input checked="" type="radio"/> 指定しない <input type="radio"/> IP アドレス <input type="radio"/> インターフェース <input type="text"/>
送信元	<input checked="" type="radio"/> 指定しない <input type="radio"/> IP アドレス <input type="text"/>

入力のやり直し

設定の保存

XR-640L2

SNMP機能の設定

SNMP マネージャ	<input type="text" value="192.168.0.0/24"/> <input type="text"/> <input type="text"/> SNMP マネージャを使いたいネットワーク範囲(ネットワーク番号/サブネット長) 又は SNMP マネージャの IP アドレスを指定して下さい。
コミュニティ名	<input type="text" value="community"/> <input type="text"/> (SNMP TRAP 用)
ロケーション	<input type="text"/>
コンタクト	<input type="text"/>
SNMP TRAP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
SNMP TRAP の送信先 IP アドレス	<input type="text"/> <input type="text"/> <input type="text"/>
SNMP TRAP の送信元	<input checked="" type="radio"/> 指定しない <input type="radio"/> IP アドレス <input type="radio"/> インターフェース <input type="text"/>
送信元	<input checked="" type="radio"/> 指定しない <input type="radio"/> IP アドレス <input type="text"/>

入力のやり直し

設定の保存

第 16 章 SNMP エージェント機能

1. SNMP エージェント機能の設定

SNMP マネージャ

SNMP マネージャを使いたいネットワーク範囲（ネットワーク番号 / サブネット長）又は、SNMP マネージャの IP アドレスを指定します。
XR-640L2 では、最大 3 つまで指定することができます。

コミュニティ名

任意のコミュニティ名を指定します。ご使用の SNMP マネージャの設定に合わせて入力してください。
XR-640L2 では、Get / Response 用と SNMP TRAP 用とそれぞれ異なるコミュニティ名が設定可能です。

ロケーション（ XR-640L2 のみ）

装置の設置場所を表す標準 MIB “ sysLocation ” (oid=.1.3.6.1.2.1.1.6.0) に、任意のロケーション名を設定することができます。

コンタクト（ XR-640L2 のみ）

装置管理者の連絡先を表す標準 MIB “ sysContact ” (oid=.1.3.6.1.2.1.1.4.0) に、任意の連絡先情報を設定することができます。

SNMP TRAP

「使用する」を選択すると、SNMP TRAP を送信できるようになります。

SNMP TRAP の送信先 IP アドレス

SNMP TRAP を送信する先 (SNMP マネージャ) の IP アドレスを指定します。
XR-640L2 では、最大 3 つまで指定することができます。

SNMP TRAP の送信元

SNMP パケット内の “ Agent Address ” に、任意のインターフェースアドレスを指定することができます。

「指定しない」を選択した場合

SNMP TRAP の送信元アドレスが自動的に設定されます。

「IP アドレス」を選択した場合

SNMP TRAP の送信元アドレスを指定します。

「インタフェース」を選択した場合

SNMP TRAP の送信元アドレスとなるインタフェース名を指定します。
指定可能なインタフェースは、本装置のイーサネットポートと PPP インタフェースのみです。

送信元

SNMP RESPONSE パケットの送信元アドレスを設定できます。
IPsec 接続を通して、リモート拠点のマネージャから SNMP を取得したい場合は、ここに IPsecSA の LAN 側アドレスを指定してください。
通常の LAN 内でマネージャを使用する場合には設定の必要はありません。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを起動させてください。
なお、設定を変更した場合は、即時設定が反映されませんが、「SNMP TRAP の送信元」を変更した場合のみ、サービスの再起動(「停止」「起動」)をおこなってください。

第 16 章 SNMP エージェント機能

I. SNMP エージェント機能の設定

MIB 項目について

以下の MIB に対応しております。

- MIB II (RFC 1213)
- UCD-SNMP MIB
- SNMPv3 MIB (RFC2571 ~ 2976)
- RFC2011 (IP-MIB)
- RFC2012 (TCP-MIB)
- RFC2013 (UDP-MIB)
- RFC2863 (IF-MIB)

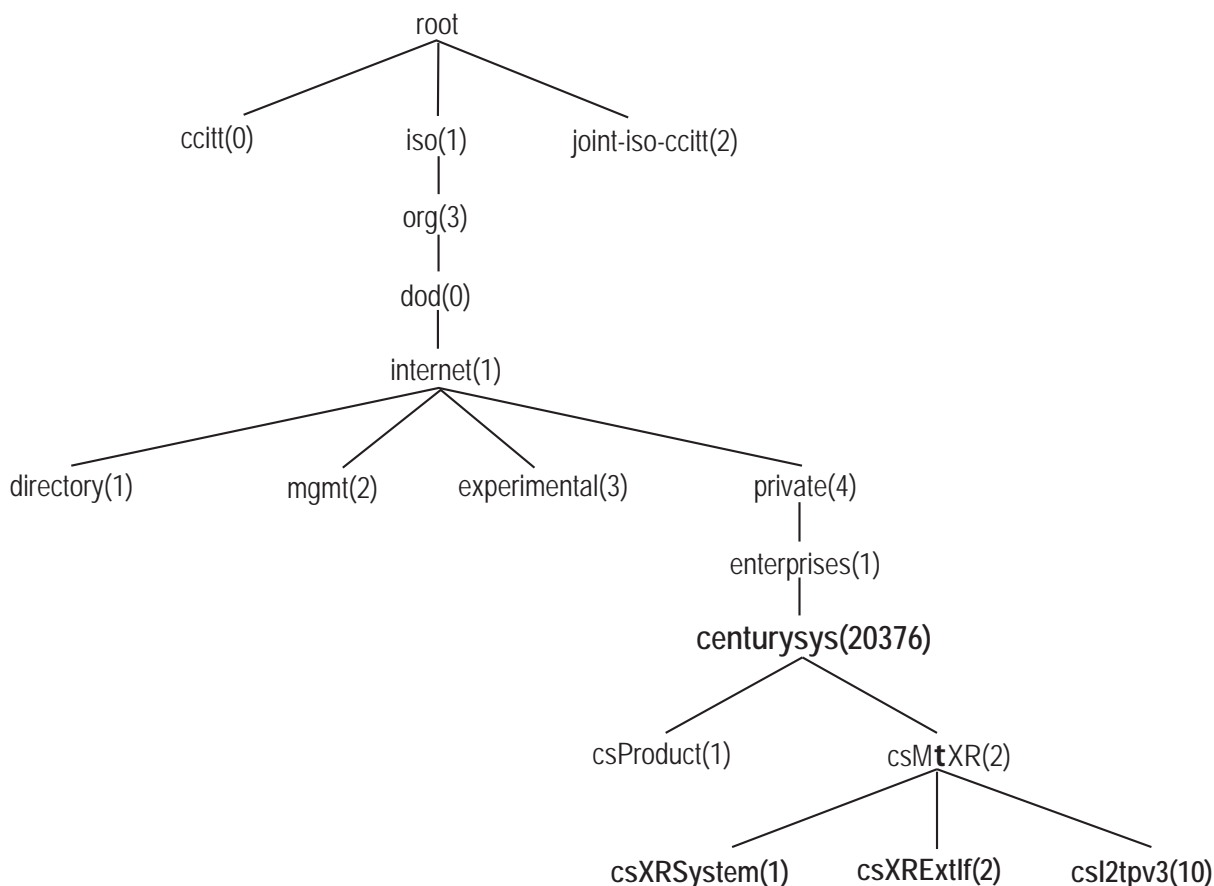
SNMP TRAP を送信するトリガーについて

以下のものに関して、SNMP TRAP を送信します。

- Ethernet インターフェースの up、down
- PPP インタフェースの up、down
- 下記の各機能の up、down
 - DNS
 - PLUTO (IPSec の鍵交換を行う IKE 機能)
 - RIP
 - OSPF
 - SYSLOG
 - NTP
 - LCP キープアライブ
 - L2TPv3
- SNMP TRAP 自身の起動、停止

II. Century Systems プライベート MIB について

本装置では保守性を高めるために以下のようなプライベート MIB (centurysys) を実装しています。この MIB 定義の階層下には、XR システム用 MIB (csXRSystem)、XR インターフェース用 MIB (csXRExtIf)、L2TPv3 用 MIB (csL2tpv3) の 3 つがあります。



csXRSystem

システム情報に関する XR 独自の定義 MIB です。CPU 使用率、空きメモリ量、コネクショントラッキング数、ファンステータスのシステム情報や、サービスの状態に関する情報を定義しています。また、これらに関する Trap 通知用の MIB 定義も含まれます。なお、主なシステム情報 Trap の通知条件は下記の通りです。

- ・CPU 使用率：90% 超過時
- ・空きメモリ量：2MB 低下時
- ・コネクショントラッキング：総数の 90% 超過時

csXRExtIf

インターフェースに関する XR 独自の定義 MIB です。各インターフェースの状態や IP アドレス情報などを定義しています。また、UP/DOWN やアドレス変更時などの Trap 通知用の MIB 定義も含まれます。

csL2tpv3

L2TPv3 サービスに関する定義 MIB です。Tunnel / Session の状態や、送受信フレームのカウント情報などを定義しています。また、Tunnel / Session の Establish や Down 時などの Trap 通知用の MIB 定義も含まれます。

これらの MIB 定義の詳細については、MIB 定義ファイルを参照してください。

注) システム、インターフェース、サービスに関する情報は標準 MIB-II でも取得できますが、Trap については全て独自 MIB によって通知されます。

第 17 章

NTP サービス

第17章 NTP サービス

NTP サービスの設定方法

本装置は、NTP クライアント / サーバ機能を持っています。インターネットを使った時刻同期の手法の一つであるNTP(Network Time Protocol)を用いてNTPサーバと通信を行い、時刻を同期させることができます。

Web 設定画面「各種サービスの設定」 「NTP サービス」をクリックして以下の画面でNTP機能の設定をします。

XR-640L2

NTP機能の設定	
情報表示	
問合せ先NTPサーバ (IPアドレス/FQDN)	1. <input type="text"/> Polling間隔 (Min) <input type="text" value="6"/> (Max) <input type="text" value="10"/>
	2. <input type="text"/> Polling間隔 (Min) <input type="text" value="6"/> (Max) <input type="text" value="10"/>
Polling間隔にX(sec)を指定すると、 指定したNTPサーバへのポーリング間隔は2 ^X 秒となります。 ex. (4: 16sec, 6: 64sec,... 10: 1024sec)	
時刻同期タイムアウト時間	<input type="text" value="1"/> (秒:1-10) NTPサービス起動時に適用されます

問合せ先NTPサーバ

NTPサーバのIPアドレスもしくはFQDNを「設定1」もしくは「設定2」に入力します（NTPサーバの場所は2箇所設定できます）。

これにより、本装置がNTPクライアント/サーバとして動作できます。

NTPサーバのIPアドレスもしくはFQDNを入力しない場合は、本装置はNTPサーバとしてのみ動作します。

Polling 間隔

NTPサーバと通信を行う間隔を設定します。サーバとの接続状態により、指定した最小値と最大値の範囲でポーリングの間隔を調整します。

Polling 間隔 X を指定した場合、秒単位での間隔は2のX乗(秒)となります。

指定可能な範囲は4 ~ 17(16 ~ 131072 秒)です。

例 X=4 : 16 秒、X=6 : 64 秒、... X=10 : 1024 秒

初期設定は(Min)6 (64 秒) (Max)10 (1024 秒)です。

初期設定のままNTPサービスを起動させると、はじめは64秒間隔でNTPサーバとポーリングをおこない、その後は64秒から1024秒の間でNTPサーバとポーリングをおこない、時刻のずれを徐々に修正していきます。

時刻同期タイムアウト時間

サーバ応答の最大待ち時間を設定できます。

1 ~ 10 秒の間で設定できます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。

情報表示 (XR-640L2 のみ)

クリックすると、現在のNTPサービスの動作状況を確認できます。

NTP機能の設定

情報表示

NTP サービスの設定方法

基準 NTP サーバについて

基準となる NTP サーバには次のようなものがあります。

- ntp1.jst.mfeed.ad.jp (210.173.160.27)
- ntp2.jst.mfeed.ad.jp (210.173.160.57)
- ntp3.jst.mfeed.ad.jp (210.173.160.87)

(注) サーバを FQDN で指定するときは、各種サービス設定の「DNS サーバ」を起動しておきます。

NTP クライアントの設定方法

各ホスト / サーバを NTP クライアントとして本装置と時刻同期させる方法は、OS により異なります。

Windows 9x/Me/NT の場合

これらの OS では NTP プロトコルを直接扱うことができません。フリーウェアの NTP クライアント・アプリケーション等を入手してご利用ください。

Windows 2000 の場合

「net time」コマンドを実行することにより時刻の同期を取ることができます。コマンドの詳細については Microsoft 社にお問い合わせください。

Windows XP の場合

Windows 2000 と同様のコマンドによるか、「日付と時刻のプロパティ」で NTP クライアントの設定ができます。詳細については Microsoft 社にお問い合わせください。

Macintosh の場合

コントロールパネル内の NTP クライアント機能で設定してください。詳細は Apple 社にお問い合わせください。

Linux の場合

Linux 用 NTP サーバをインストールして設定してください。詳細は NTP サーバの関連ドキュメント等をご覧ください。

第 18 章

アクセスサーバ機能

第18章 アクセスサーバ機能

1. アクセスサーバ機能について

アクセスサーバとは、電話回線などを使った外部からの接続要求を受けて、LANに接続する機能です。例えば、アクセスサーバとして設定した本装置を会社に設置すると、モデムを接続した外出先のコンピュータから会社のLANに接続できます。これは、モバイルコンピューティングや在宅勤務を可能にします。クライアントはモデムによるPPP接続を利用できるものであれば、どのようなPCでもかまいません。この機能を使って接続したクライアントは、接続先のネットワークにハブで接続した場合と同じようにネットワークを利用できます。

セキュリティは、ユーザーID・パスワード認証によって確保します。ユーザーID・パスワードは、最大5アカウント分を登録できます。



II. 本装置とアナログモデム / TA の接続

アクセスサーバ機能を設定する前に、XR-410/TX2-L2とアナログモデムやTAを接続します。以下のように接続してください。

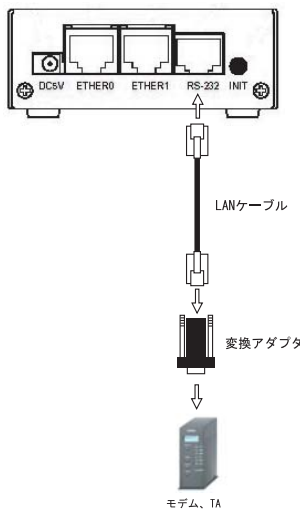
アナログモデム / TA の接続 (XR-410L2)

1 XR-410/TX2-L2 本体背面の「RS-232」ポートと製品付属の変換アダプタとを、ストレートタイプのLANケーブルで接続してください。

2 変換アダプタのコネクタを、アナログモデム / TAのシリアルポートに接続してください。シリアルポートのコネクタが25ピンタイプの場合は別途、変換コネクタをご用意ください。

3 全ての接続が完了しましたら、モデム / TAの電源を投入してください。

接続図



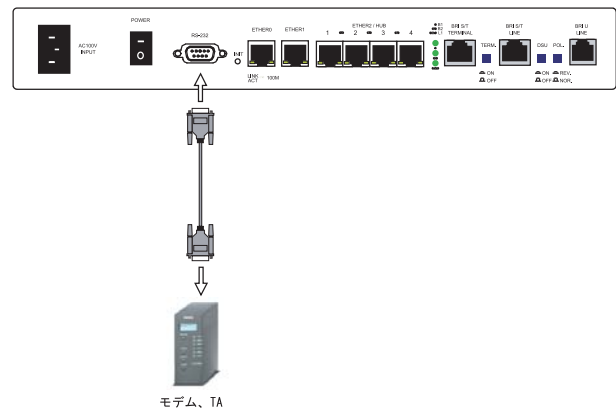
アナログモデム / TA の接続 (XR-640L2)

1 XR-640L2の電源をオフにします。

2 XR-640L2の「RS-232C/BR1」ポートとモデム / TAのシリアルポートをシリアルケーブルで接続します。シリアルケーブルは別途ご用意ください。

3 全ての接続が完了しましたら、モデムの電源を投入してください。

接続図



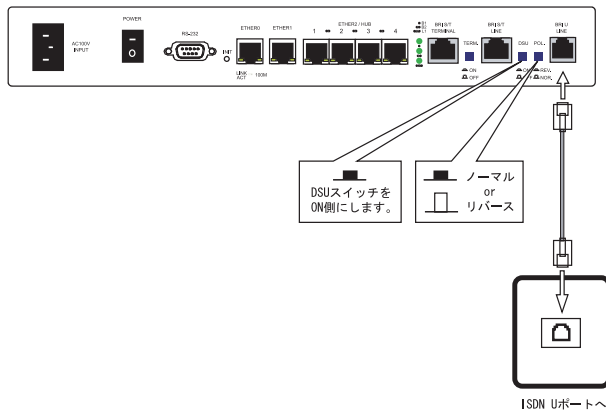
第18章 アクセスサーバ機能

III. BRIポートを使ったTA/DSUとの接続 (XR-640L2のみ)

XR-640/CD-L2内蔵のDSUを使う場合

- 1 本装置の電源をオフにします。
- 2 ISDN U点ジャックと本装置の「BRI U」ポートをモジュラーケーブルで接続します。モジュラーケーブルは別途ご用意ください。
- 3 本体背面の「DSU」スイッチを「ON」側にします。
- 4 本体背面の「POL.」スイッチを、ISDN回線の極性に合わせます。
- 5 全ての接続が完了しましたら、本装置とTAの電源を投入してください。

接続図

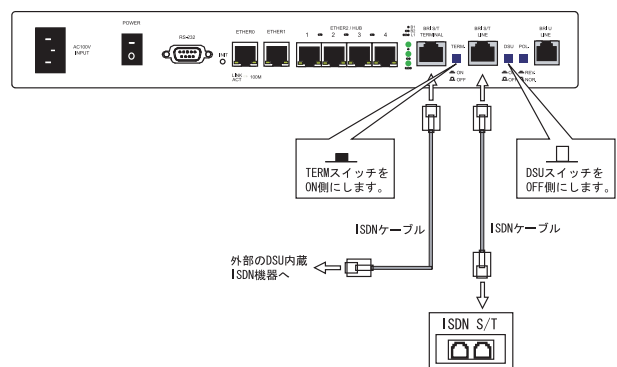


外付けTAに内蔵のDSUを使う場合

- 1 本装置の電源をオフにします。
- 2 外部のDSUと本装置の「BRI S/T LINE」ポートをISDN回線ケーブルで接続します。ISDNケーブルは別途ご用意ください。
- 3 本体背面の「DSU」スイッチを「OFF」側にします。
- 4 本体背面の「TERM.」スイッチを「ON」側にします。
- 5 別のISDN機器を接続する場合は「BRI S/T TERMINAL」ポートと接続してください。

- 6 全ての接続が完了しましたら、本装置とTAの電源を投入します。

接続図



第18章 アクセスサーバ機能

IV. アクセスサーバ機能の設定

< XR-410L2 >

Web 設定画面「各種サービスの設定」 「アクセスサーバ」をクリックして設定します。

アクセスサーバ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
アクセスサーバ(本装置)の IP アドレス	<input type="text" value="192.168.253.254"/>
クライアントの IP アドレス	<input type="text" value="192.168.253.170"/>
モデムの速度	<input type="radio"/> 9600 <input type="radio"/> 19200 <input type="radio"/> 38400 <input checked="" type="radio"/> 57600 <input type="radio"/> 115200 <input type="radio"/> 230400
受信のための AT コマンド	<input type="text"/>

アクセスサーバ

アクセスサーバ機能の使用 / 不使用を選択します。

アクセスサーバ(本装置)の IP アドレス
リモートアクセスされた時の XR-410/TX2-L2 自身の IP アドレスを入力します。各 Ethernet ポートのアドレスとは異なるプライベートアドレスを設定してください。**なお、サブネットのマスクビット値は 24 ビット(255.255.255.0)に設定されています。**

クライアントの IP アドレス

本装置にリモートアクセスしてきたホストに割り当てる IP アドレスを入力します。上記の「アクセスサーバの IP アドレス」で設定したものと同一ネットワークとなるアドレスを設定してください。

モデムの速度

本装置とモデム間の通信速度を選択します。

着信のための AT コマンド

モデムが外部から着信する場合、AT コマンドが必要な場合があります。その場合は、ここで AT コマンドを入力してください。コマンドについては、各モデムの説明書をご確認ください。

< XR-640L2 >

Web 設定画面「各種サービスの設定」 「アクセスサーバ」をクリックして設定します。

シリアル回線で着信する場合(XR-640L2のみ)

「シリアル回線」欄で設定します。

シリアル回線	
着信	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
アクセスサーバ(本装置)の IP アドレス	<input type="text" value="192.168.253.254"/>
クライアントの IP アドレス	<input type="text" value="192.168.253.170"/>
モデムの速度	<input type="radio"/> 9600 <input type="radio"/> 19200 <input type="radio"/> 38400 <input checked="" type="radio"/> 57600 <input type="radio"/> 115200 <input type="radio"/> 230400
受信のための AT コマンド	<input type="text"/>

着信

シリアル回線で着信したい場合は「許可する」を選択します。

アクセスサーバ(本装置)の IP アドレス
リモートアクセスされた時の本装置自身の IP アドレスを入力します。各 Ethernet ポートのアドレスとは異なるプライベートアドレスを設定してください。**なお、サブネットマスクビット値は 24 ビット(255.255.255.0)に設定されています。**

クライアントの IP アドレス

本装置にリモートアクセスしてきたホストに割り当てる IP アドレスを入力します。上記の「アクセスサーバの IP アドレス」で設定したものと同一ネットワークとなるアドレスを設定してください。

モデムの速度

本装置とモデム間の通信速度を選択します。

着信のための AT コマンド

モデムが外部から着信する場合、AT コマンドが必要な場合があります。その場合は、ここで AT コマンドを入力してください。コマンドについては、各モデムの説明書をご確認ください。

第18章 アクセスサーバ機能

IV. アクセスサーバ機能の設定

BRI 回線で着信する場合(XR-640L2のみ)

「BRI 回線」欄で設定します。2チャンネル分の設定が可能です。

BRI 回線	
回線1 着信	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
アクセスサーバ(本装置)のIPアドレス	<input type="text" value="192.168.251.254"/>
クライアントのIPアドレス	<input type="text" value="192.168.251.171"/>
回線2 着信	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
アクセスサーバ(本装置)のIPアドレス	<input type="text" value="192.168.252.254"/>
クライアントのIPアドレス	<input type="text" value="192.168.252.172"/>
発信者番号認証	<input checked="" type="radio"/> しない <input type="radio"/> する
本装置のホスト名	<input type="text" value="localhost"/>

回線1、回線2 着信

BRI 回線で着信したい場合は、「許可する」を選択します。

アクセスサーバ(本装置)のIPアドレス
リモートアクセスされた時の本装置自身のIPアドレスを入力します。各Ethernetポートのアドレスとは異なるプライベートアドレスを設定してください。なお、サブネットマスクビット値は24ビット(255.255.255.0)に設定されています。

クライアントのIPアドレス

本装置にリモートアクセスしてきたホストに割り当てるIPアドレスを入力します。上記の「アクセスサーバのIPアドレス」で設定したものと同じネットワークとなるアドレスを設定してください。

発信者番号認証

発信者番号で認証する場合は「する」を選択します。

本装置のホスト名

本装置のホスト名を任意で設定可能です。

続けてユーザーアカウントの設定をおこないます。

ユーザーアカウントの設定

設定画面の下側でユーザーアカウントの設定をおこないます。

No.	アカウント	パスワード	アカウント毎に別IPを割り当てる場合		削除
			本装置のIP	クライアントのIP	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

外部からリモートアクセスする場合の、ユーザーアカウントとパスワードを登録してください。そのまま、リモートアクセス時のユーザーアカウント・パスワードとなります。XR-410L2は5アカウントまで、XR-640L2は50アカウントまで登録しておけます。

またアカウントごとに、割り当てるIPアドレスを個別に指定することも可能です。その場合は「本装置のIP」と「クライアントのIP」のどちらか、もしくは両方を設定します。

また BRI 回線(XR-640L2のみ)の設定で発信者番号認証を「する」にしている場合は、「許可する着信番号」欄に、発信者の電話番号を入力し、着信する回線(回線1か回線2)を選択してください。

No.	許可する着信番号	着信する回線	削除
1	<input type="text"/>	<input type="text" value="すべて"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text" value="すべて"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text" value="すべて"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text" value="すべて"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text" value="すべて"/>	<input type="checkbox"/>

入力後、「設定の保存」をクリックしてください。設定が反映されます。

アカウント設定覧の「削除」ラジオボックスにチェックして「設定 / 削除の実行」をクリックすると、その設定が削除されます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

IV. アクセスサーバ機能の設定

スタティックルートを設定する場合

通常のスタティックルート設定では「インターフェイス / ゲートウェイ」のどちらかひとつの項目のみ設定可能ですが、アクセスサーバ機能で着信するインターフェイス向けにスタティックルート設定を行う場合は、以下の両項目ともに設定が必要になりますのでご注意ください。

インターフェイス : ppp6 (固定)

ゲートウェイ : アクセスサーバ設定画面にて指定した着信時のクライアントの IP アドレス

設定例

前ページ「BRI 回線で着信する場合 (XR-640L2 のみ)」のスタティックルート設定例です。

No.	アドレス	ネットマスク	インターフェイス/ゲートウェイ	ディスタンス <1-255>	
1	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	ppp6	192.168.251.171	1
2	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	ppp6	192.168.252.172	2

第 19 章

スタティックルート設定

第19章 スタティックルート設定

スタティックルート設定

本装置は、最大256エントリのスタティックルートを登録できます。

Web 設定画面「スタティックルート設定」をクリックして、以下の画面から設定します。

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>	削除
1	192.168.10.0	255.255.255.0		192.168.120.15	<input type="checkbox"/>
2	192.168.20.1	255.255.255.0	gre1		<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>
11					<input type="checkbox"/>
12					<input type="checkbox"/>
13					<input type="checkbox"/>
14					<input type="checkbox"/>
15					<input type="checkbox"/>
16					<input type="checkbox"/>

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

(画面は設定例です)

入力方法

アドレス

あて先ホストのアドレス、またはネットワークアドレスを入力します。

ネットマスク

あて先ネットワークのサブネットマスクを入力します。IPアドレス形式で入力してください。

入力例 : **255.255.255.248**

また、あて先アドレスを単一ホストで指定した場合には、「255.255.255.255」と入力します。

インターフェース/ゲートウェイ

ルーティングをおこなうインターフェース名、もしくは上位ルータのIPアドレスのどちらかを設定します。

PPP/PPPoE や GRE インターフェースを設定するときはインターフェース名だけの設定となります。

ディスタンス

経路選択の優先順位を指定します。1 ~ 255 の間で指定します。値が低いほど優先度が高くなります。**スタティックルートのデフォルトディスタンス値は1です。**

ディスタンス値を変更することで、フローティングスタティックルート設定とすることも可能です。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

設定を挿入する

ルーティング設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

その番号以降に設定がある場合は、1つずつ設定番号がずれて設定が更新されます。

設定を削除する

ルーティング設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

スタティックルート設定

デフォルトルートを設定する

スタティックルート設定でデフォルトルートを設定するときは、「アドレス」と「ネットマスク」項目をいずれも「0.0.0.0」として設定してください。

アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>
0.0.0.0	0.0.0.0	gre1	1

(画面は設定例です)

ルーティング情報を確認する

現在のルーティング情報を確認するには、設定画面上部にある「経路情報表示」をクリックします。ウィンドウがポップアップし、経路情報が確認できます。

”inactive”と表示されている経路は、その時点では有効な経路ではなく、無視されます。

表示されていないものに関しては、正しい設定ではありません。設定をご確認のうえ、再度設定してください。

第 20 章

ソースルート設定

ソースルート設定

通常のダイナミックルーティングおよびスタティックルーティングでは、パケットのあて先アドレスごとにルーティングを行ないませんが、ソースルーティングはパケットの送信元アドレスをもとにルーティングをおこないます。

このソースルート機能を使うことで、外部へアクセスするホスト/ネットワークごとにアクセス回線を選択することができますので、複数のインターネット接続をおこなって負荷分散が可能となります。

ソースルート設定は、設定画面「ソースルート設定」でおこないます。

1 はじめに、ソースルートのテーブル設定をおこないます。「ソースルートのテーブル設定へ」をクリックしてください。

テーブルNO	IP	DEVICE
1		
2		
3		
4		
5		
6		
7		
8		

IP

デフォルトゲートウェイ(上位ルータ)のIPアドレスを設定します。必ず明示的に設定しなければなりません。

DEVICE

デフォルトゲートウェイが存在する回線に接続しているインターフェースのインターフェース名を設定します。本装置のインターフェース名については、本マニュアルの「付録 A インターフェース名について」をご参照ください。

設定後は「設定の保存」をクリックします。

2 画面右上の「ソースルートのルール設定へ」をクリックします。

ルールNO	送信元ネットワークアドレス	送信先ネットワークアドレス	ソースルートのテーブルNO
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

送信元ネットワークアドレス

送信元のネットワークアドレスもしくはホストのIPアドレスを設定します。ネットワークアドレスで設定する場合は、

ネットワークアドレス/マスクビット値

の形式で設定してください。

送信先ネットワークアドレス

送信先のネットワークアドレスもしくはホストのIPアドレスを設定します。ネットワークアドレスで設定する場合は、

ネットワークアドレス/マスクビット値

の形式で設定してください。

ソースルートのテーブルNo.

使用するソースルートテーブルの番号(1 ~ 8)を設定します。

最後に「設定の保存」をクリックして設定完了です。

送信元ネットワークアドレスをネットワークアドレスで指定した場合、そのネットワークに本装置のインターフェースが含まれていると、設定後は本装置の設定画面にアクセスできなくなります。

<例>Ether0 ポートの IP アドレスが 192.168.0.254 で、送信元ネットワークアドレスを 192.168.0.0/24 と設定すると、192.168.0.0/24 内のホストは本装置の設定画面にアクセスできなくなります。

第 21 章

NAT 機能

1. 本装置のNAT機能について

NAT(Network Address Translation)は、プライベートアドレスをグローバルアドレスに変換してインターネットにアクセスできるようにする機能です。また1つのプライベートアドレス・ポートと、1つのグローバルアドレス・ポートを対応させて、インターネット側からLANのサーバへアクセスさせることもできます。

本装置は以下の3つのNAT機能をサポートしています。

IPマスカレード機能

複数のプライベートアドレスを、ある1つのグローバルアドレスに変換する機能です。グローバルアドレスは本装置のインターネット側ポートに設定されたものを使います。またLANのプライベートアドレス全てが変換されることとなります。この機能を使うと、グローバルアドレスを1つしか持っていないくても複数のコンピュータからインターネットにアクセスすることができるようになります。

なおIPマスカレード(NAT機能)では、プライベートアドレスからグローバルアドレスだけではなく、プライベートアドレスからプライベートアドレス、グローバルアドレスからグローバルアドレスの変換も可能です。IPマスカレード機能については、「インターフェース設定」もしくは「PPP/PPPoE接続」の接続設定画面で設定します。

送信元NAT機能

IPマスカレードとは異なり、プライベートアドレスをどのグローバルIPアドレスに変換するかをそれぞれ設定できるのが送信元NAT機能です。例えば、プライベートアドレスAをグローバルアドレスXに、プライベートアドレスBをグローバルアドレスYに、プライベートアドレスCからFをグローバルアドレスZに変換する、といった設定が可能になります。IPマスカレード機能を設定せずに送信元NAT機能だけを設定した場合は、送信元NAT機能で設定されたアドレスを持つコンピュータしかインターネットにアクセスできません。

バーチャルサーバ機能

インターネット上からLAN上のサーバ等にアクセスさせることができる機能です。通常はインターネット側からLANへアクセスする事はできませんが、送信先グローバルアドレスをプライベートアドレスへ変換する設定をおこなうことで、見かけ上はインターネット上のサーバへアクセスできているかのようにすることができます。設定上ではプライベートアドレスとグローバルアドレスを1対1で関連づけます。また同時に、プロトコルとTCP/UDPポート番号も指定しておきます。ここで指定したプロトコル・TCP/UDPポート番号でアクセスされた時にグローバルアドレスからプライベートアドレスへ変換され、LAN上のサーバに転送されます。

これらのNAT機能は同時に設定・運用が可能です。

NetMeetingや各種IM、ネットワークゲームなど、独自のプロトコル・ポートを使用しているアプリケーションについては、NAT機能を使用すると正常に動作しない場合があります。原則として、NATを介しての個々のアプリケーションの動作についてはサポート対象外とさせていただきます。

11. バーチャルサーバ設定

NAT環境下において、LANからサーバを公開するときなどの設定をおこないます。

設定方法

Web設定画面「NAT設定」「バーチャルサーバ」をクリックして、以下の画面から設定します。

No.	サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	削除
1	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。						
<input type="text"/>	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

サーバのアドレス

インターネットに公開するサーバの、プライベートIPアドレスを入力します。

公開するグローバルアドレス

サーバのプライベートIPアドレスに対応させるグローバルIPアドレスを入力します。インターネットからはここで入力したグローバルIPアドレスでアクセスします。

プロバイダから割り当てられているIPアドレスが一つだけの場合は、ここは空欄にします。

プロトコル

サーバのプロトコルを選択します。

ポート

サーバが公開するポート番号を入力します。範囲で指定することも可能です。範囲で指定するときは、ポート番号を ":" で結びます。

<例> ポート20番から21番を指定する **20:21**

インターフェース

外部からのアクセスを受信するインターフェース名を設定します。外部に接続しているインターフェース名を設定してください。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名について」をご参照ください。

入力が終わりましたら「設定/削除の実行」をクリックして設定完了です。

"No."項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

設定情報の確認

「情報表示」をクリックすると、現在のバーチャルサーバ設定の情報が一覧表示されます。

設定を挿入する

バーチャルサーバ設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。						
<input type="text"/>	<input type="text"/>	<input type="text"/>	全て▼	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

その番号以降に設定がある場合は、1つずつ設定番号がずれて設定が更新されます。

設定を削除する

バーチャルサーバ設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定/削除の実行」ボタンをクリックすると削除されます。

ポート番号を指定して設定するときは、必ずプロトコルも選択してください。「全て」の選択ではポートを指定することはできません。

III. 送信元 NAT 設定

設定方法

Web 設定画面「NAT 設定」 「送信元 NAT」をクリックして、以下の画面から設定します。

No.	送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース	削除
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
----------------------	----------------------	----------------------	----------------------	--------------------------

送信元のプライベートアドレス

NATの対象となるLAN側コンピュータのプライベートIPアドレスを入力します。ネットワーク単位での指定も可能です。

変換後のグローバルアドレス

プライベートIPアドレスの変換後のグローバルIPアドレスを入力します。送信元アドレスをここで入力したアドレスに書き換えてインターネット(WAN)へアクセスします。

インターフェース

外部につながっているインターフェース名を設定してください。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名について」をご参照ください。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

”No.”項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

設定情報の確認

「情報表示」をクリックすると、現在の送信元 NAT 設定の情報が一覧表示されます。

設定を挿入する

送信元 NAT 設定を追加する場合、任意の場所に挿入することができます。

挿入は、設定テーブルの一番下にある行からおこないます。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
----------------------	----------------------	----------------------	----------------------	--------------------------

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

その番号以降に設定がある場合は、1つずつ設定番号がずれて設定が更新されます。

設定を削除する

送信元 NAT 設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

IV. バーチャルサーバの設定例

WWWサーバを公開する際のNAT設定例

NATの条件

- WAN側のグローバルアドレスにTCPのポート80番(http)でのアクセスを通す。
- WANはEther1、LANはEther0ポートに接続。

LAN構成

- LAN側ポートのIPアドレス「192.168.0.254」
- WWWサーバのアドレス「192.168.0.1」
- 割り当てられるグローバルアドレスは1つのみ。

設定画面での入力方法

- あらかじめIPマスカレードを有効にします。
- 「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.1		tcp	80	eth1

設定の解説

No.1 :

WAN側から本装置のIPアドレスへポート80番(http)でアクセスがあれば、LAN内のサーバ192.168.0.1へ通す。(WAN側からTCPのポート80番以外でアクセスがあっても破棄される)

FTPサーバを公開する際のNAT設定例

NATの条件

- WAN側のグローバルアドレスにTCPのポート20番(ftpdata)、21番(ftp)でのアクセスを通す。
- WANはEther1、LANはEther0ポートに接続する。
- Ether1ポートはPPPoEでADSL接続する。

LAN構成

- LAN側ポートのIPアドレス「192.168.0.254」
- FTPサーバのアドレス「192.168.0.2」
- 割り当てられるグローバルアドレスは1つのみ。

設定画面での入力方法

- あらかじめIPマスカレードを有効にします。
- 「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.2		tcp	20	ppp0
192.168.0.2		tcp	21	ppp0

設定の解説

No.1 :

WAN側から本装置のIPアドレスへポート21番(ftp)でアクセスがあれば、LAN内のサーバ192.168.0.2へ通す。

No.2 :

WAN側から本装置のIPアドレスへポート20番(ftpdata)でアクセスがあれば、LAN内のサーバ192.168.0.2へ通す。

バーチャルサーバ設定以外に、適宜パケットフィルタ設定を行ってください。とくにステートフルパケットインスペクション機能を使っている場合には、「転送フィルタ」で明示的に、使用ポートを開放する必要があります。

IV. バーチャルサーバの設定例

PPTP サーバを公開する際の NAT 設定例

NAT の条件

- ・WAN 側のグローバルアドレスにプロトコル「gre」と TCP のポート番号 1723 を通す。
- ・WAN は Ether1、LAN は Ether0 ポートに接続する。
- ・WAN 側ポートは PPPoE で ADSL 接続する。

LAN 構成

- ・LAN 側ポートの IP アドレス「192.168.0.254」
- ・PPTP サーバのアドレス「192.168.0.3」
- ・割り当てられるグローバルアドレスは1つのみ。

設定画面での入力方法

- ・あらかじめ IP マスカレードを有効にします。
- ・「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.3		tcp	1723	ppp0
192.168.0.3		gre		ppp0

バーチャルサーバ設定以外に、適宜パケットフィルタ設定を行ってください。とくにステートフルパケットインスペクション機能を使っている場合には、「転送フィルタ」で明示的に、使用ポートを開放する必要があります。

IV. バーチャルサーバの設定例

DNS、メール、WWW、FTPサーバを公開する際の NAT設定例(複数グローバルアドレスを利用)

NATの条件

- WAN側からは、LAN側のメール、WWW、FTPサーバへアクセスできるようにする。
- LAN内のDNSサーバがWANと通信できるようにする。
- LANからWANへのアクセスは自由にできる。
- WANはEther1、LANはEther0ポートに接続。
- グローバルアドレスは複数使用する。
- WAN側はPPPoE接続する。

LAN構成

- LAN側ポートのIPアドレス「192.168.0.254」
- WWWサーバのアドレス「192.168.0.1」
- 送受信メールサーバのアドレス「192.168.0.2」
- FTPサーバのアドレス「192.168.0.3」
- DNSサーバのアドレス「192.168.0.4」
- WWWサーバに対応させるグローバルIPアドレスは「211.xxx.xxx.104」
- 送受信メールサーバに対応させるグローバルIPアドレスは「211.xxx.xxx.105」
- FTPサーバに対応させるグローバルIPアドレスは「211.xxx.xxx.106」
- DNSサーバに対応させるグローバルIPアドレスは「211.xxx.xxx.107」

設定画面での入力方法

1 まず最初に、使用する複数のグローバルアドレスを、仮想インターフェースとして登録します。メニューにある「仮想インターフェース設定」を開き、以下のように設定しておきます。

インターフェース	仮想I/F番号	IPアドレス	ネットマスク
ppp0	1	211.xxx.xxx.104	255.255.255.248
ppp0	2	211.xxx.xxx.105	255.255.255.248
ppp0	3	211.xxx.xxx.106	255.255.255.248
ppp0	4	211.xxx.xxx.107	255.255.255.248

2 「バーチャルサーバ設定」で以下の様に設定してください。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.1	211.xxx.xxx.104	tcp	80	ppp0
192.168.0.2	211.xxx.xxx.105	tcp	25	ppp0
192.168.0.2	211.xxx.xxx.105	tcp	110	ppp0
192.168.0.3	211.xxx.xxx.106	tcp	21	ppp0
192.168.0.3	211.xxx.xxx.106	tcp	20	ppp0
192.168.0.4	211.xxx.xxx.107	tcp	53	ppp0
192.168.0.4	211.xxx.xxx.107	udp	53	ppp0

設定の解説

No.1

WAN側から211.xxx.xxx.104へポート80番(http)でアクセスがあれば、LAN内のサーバ192.168.0.1へ通す。

No.2、3

WAN側から211.xxx.xxx.105へポート25番(smtp)か110番(pop3)でアクセスがあれば、LAN内のサーバ192.168.0.2へ通す。

No.4、5

WAN側から211.xxx.xxx.106へポート20番(ftpdata)か21番(ftp)でアクセスがあれば、LAN内のサーバ192.168.0.3へ通す。

No.6、7

WAN側から211.xxx.xxx.107へ、tcpポート53番(domain)かudpポート53番(domain)でアクセスがあればLAN内のサーバ192.168.0.4へ通す。

複数のグローバルアドレスを使ってバーチャルサーバ設定をおこなうときは、必ず「仮想インターフェース機能」において使用するグローバルアドレスを設定しておく必要があります。

V. 送信元 NAT の設定例

送信元 NAT 設定では、LAN 側のコンピュータのアドレスをどのグローバルアドレスに変換するかを個々に設定することができます。

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
192.168.0.1	61.xxx.xxx.101	ppp0
192.168.0.2	61.xxx.xxx.102	ppp0
192.168.10.0/24	61.xxx.xxx.103	ppp0

例えば上記のような送信元 NAT 設定をおこなうと、

- ・送信元アドレス 192.168.0.1 を 61.xxx.xxx.101 に変換して WAN へアクセスする
- ・送信元アドレス 192.168.0.2 を 61.xxx.xxx.102 に変換して WAN へアクセスする
- ・送信元アドレスとして 192.168.10.0/24 からのアクセスを 61.xxx.xxx.103 に変換して WAN へアクセスする

という設定になります。

送信元のアドレスは、ホスト単位かネットワーク単位で指定できます。範囲指定はできません。ネットワークで指定するときは、以下のように設定してください。

<設定例> **192.168.254.0/24**

複数のグローバルアドレスを使って送信元 NAT 設定をおこなうときは、必ず「仮想インターフェース機能」で使用する IP アドレスを設定しておく必要があります。

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細はRFC1700(Oct. 1994)を参照してください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137~139
snmp	161
snmptrap	162
route	520

第 22 章

パケットフィルタリング機能

第22章 パケットフィルタリング機能

1. パケットフィルタリング機能の概要

本装置はパケットフィルタリング機能を搭載しています。パケットフィルタリング機能を使うと、以下のようなことができます。

- ・外部からLANに入ってくるパケットを制限する。
- ・LANから外部に出ていくパケットを制限する。
- ・本装置自身が受信するパケットを制限する。
- ・本装置自身から送信するパケットを制限する。
- ・ゲートウェイ認証機能を使用しているときにアクセス可能にする。

またフィルタリングは以下の情報に基づいて条件を設定することができます。

- ・送信元 / あて先 IP アドレス
- ・プロトコル(TCP/UDP/ICMP/ など)・番号
- ・送信元 / あて先ポート番号
- ・入出力方向(入力 / 転送 / 出力)
- ・インターフェース

パケットフィルタリング機能を有効にすると、パケットを単にルーティングするだけでなく、パケットのヘッダ情報を調べて、送信元やあて先のIPアドレス、プロトコルの種類(TCP/UDP/ICMPなど)・プロトコル番号、ポート番号に基づいてパケットを通過させたり破棄させることができます。

このようなパケットフィルタリング機能は、コンピュータやアプリケーション側の設定を変更する必要がないために、個々のコンピュータでパケットフィルタの存在を意識することなく、簡単に利用できます。

Xconnect Interfaceに指定されたインターフェースは、フィルタ設定を適用することができません。L2TPセッション間でのフィルタリングを設定するには、第14章「L2TPv3 フィルタ機能」を参考にしてください。

第22章 パケットフィルタリング機能

II. 本装置のフィルタリング機能について

本装置は、4つの基本ルールについてフィルタリングの設定をおこないます。この4つの項目は以下の通りです。

- ・入力(input)
- ・転送(forward)
- ・出力(output)
- ・ゲートウェイ認証フィルタ

入力(input)フィルタ

外部から本装置自身に入ってくるパケットに対して制御します。インターネットやLANから本装置へのアクセスについて制御したい場合には、この入力ルールにフィルタ設定をおこないます。

転送(forward)フィルタ

LANからインターネットへのアクセスや、インターネットからLAN内サーバへのアクセス、LANからLANへのアクセスなど、本装置で内部転送する(本装置がルーティングする)アクセスを制御するという場合には、この転送ルールにフィルタ設定をおこないます。

出力(output)フィルタ

本装置内部からインターネットやLANなどへのアクセスを制御したい場合には、この出力ルールにフィルタ設定をおこないます。

パケットが「転送されるもの」か「本装置自身へのアクセス」か「本装置自身からのアクセス」かをチェックしてそれぞれのルールにあるフィルタ設定を実行します。

ゲートウェイ認証フィルタ

「ゲートウェイ認証機能」を使用しているときに設定するフィルタです。ゲートウェイ認証を必要とせずに外部と通信可能にするフィルタ設定を行います。ゲートウェイ認証機能については第26章「ゲートウェイ認証機能」をご覧ください。

各ルール内のフィルタ設定は先頭から順番にマッチングされ、最初にマッチした設定がフィルタとして動作することになります。逆に、マッチするフィルタ設定が見つからなければそのパケットはフィルタリングされません。

フィルタの初期設定について

工場出荷設定では、「入力フィルタ」と「転送フィルタ」において、以下のフィルタ設定がセットされています。

- ・NetBIOSを外部に送出不いフィルタ設定
- ・外部からUPnPで接続されないようにするフィルタ設定

Windows ファイル共有をする場合は、NetBIOS用のフィルタを削除してお使いください。

第22章 パケットフィルタリング機能

III. パケットフィルタリングの設定

入力・転送・出力・ゲートウェイ認証フィルタの4種類ありますが、設定方法はすべて同様となります。

設定方法

Web 設定画面にログインします。「フィルタ設定」「入力フィルタ」「転送フィルタ」「出力フィルタ」「ゲートウェイ認証フィルタ」のいずれかをクリックして、以下の画面から設定します。

フィルタ設定 No.1~16まで

[情報表示](#)

※No.赤色の設定は現在無効です

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG	削除	No.
1	eth0	パケット受信時	破棄	tcp				137:139	<input type="checkbox"/>	<input type="checkbox"/>	1
2	eth0	パケット受信時	破棄	udp				137:139	<input type="checkbox"/>	<input type="checkbox"/>	2
3	eth0	パケット受信時	破棄	tcp		137			<input type="checkbox"/>	<input type="checkbox"/>	3
4	eth0	パケット受信時	破棄	udp		137			<input type="checkbox"/>	<input type="checkbox"/>	4
5	eth1	パケット受信時	破棄	udp				1900	<input type="checkbox"/>	<input type="checkbox"/>	5
6	ppp0	パケット受信時	破棄	udp				1900	<input type="checkbox"/>	<input type="checkbox"/>	6
7	eth1	パケット受信時	破棄	tcp				5000	<input type="checkbox"/>	<input type="checkbox"/>	7
8	ppp0	パケット受信時	破棄	tcp				5000	<input type="checkbox"/>	<input type="checkbox"/>	8
9	eth1	パケット受信時	破棄	tcp				2869	<input type="checkbox"/>	<input type="checkbox"/>	9
10	ppp0	パケット受信時	破棄	tcp				2869	<input type="checkbox"/>	<input type="checkbox"/>	10
11		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	11
12		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	12
13		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	13
14		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	14
15		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	15
16		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	16
設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。											
		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	

(画面は「入力フィルタ」です)

インターフェース

フィルタリングをおこなうインターフェース名を指定します。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名について」をご参照ください。

方向

ポートがパケットを受信するときにフィルタリングするか、送信するときにフィルタリングするかを選択します。

入力フィルタでは「パケット受信時」、出力フィルタでは「パケット送信時」のみとなります。

動作

フィルタリング設定にマッチしたときにパケットを破棄するか通過させるかを選択します。

プロトコル

フィルタリング対象とするプロトコルを選択します。右側の空欄でプロトコル番号による指定もできます。ポート番号も指定する場合は、ここで必ずプロトコルを選択しておいてください。

送信元アドレス

フィルタリング対象とする、送信元の IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレス、ドメイン名での指定が可能です。

<入力例>

単一の IP アドレスを指定する：

192.168.253.19 (" アドレス /32 " の書式)

ネットワーク単位で指定する：

192.168.253.0/24

(" ネットワークアドレス / マスクビット値 " の書式)

第22章 パケットフィルタリング機能

III. パケットフィルタリングの設定

送信元ポート

フィルタリング対象とする、送信元のポート番号を入力します。範囲での指定も可能です。範囲で指定するときは”:”でポート番号を結びます。

<入力例> ポート 1024 番から 65535 番を指定する場合。 **1024:65535**

ポート番号を指定するときは、プロトコルもあわせて選択しておかなければなりません(「全て」のプロトコルを選択して、ポート番号を指定することはできません)

あて先アドレス

フィルタリング対象とする、送信元の IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。入力方法は、送信元アドレスと同様です。

あて先ポート

フィルタリング対象とする、送信先のポート番号を入力します。範囲での指定も可能です。指定方法は送信元ポート同様です。

LOG

チェックを入れると、そのフィルタ設定に合致したパケットがあったとき、そのパケットの情報を syslog に出力します。許可 / 破棄いずれの場合も出力します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

”No.”項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

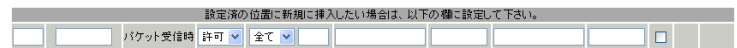
設定情報の確認

「情報表示」をクリックすると、現在のフィルタ設定の情報が一覧表示されます。

設定を挿入する

フィルタ設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。



最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

その番号以降に設定がある場合は、1つずつ設定番号がずれて設定が更新されます。

設定を削除する

フィルタ設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

第 22 章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

インターネットから LAN へのアクセスを破棄する設定

フィルタの条件

- WAN 側からは LAN 側へアクセス不可にする。
- LAN から WAN へのアクセスは自由にできる。
- 本装置から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続する。
- LAN から WAN へ IP マスカレードをおこなう。
- ステートフルパケットインスペクションは有効。

LAN 構成

- LAN のネットワークアドレス「192.168.0.0/24」
- LAN 側ポートの IP アドレス「192.168.0.1」

設定画面での入力方法

「入力フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット受信時	許可	tcp				1024-65535
2	eth1	パケット受信時	許可	udp				1024-65535
3	eth1	パケット受信時	許可	---	1			
4	eth1	パケット受信時	破棄	全て				

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット受信時	許可	tcp				1024-65535
2	eth1	パケット受信時	許可	udp				1024-65535
3	eth1	パケット受信時	許可	---	1			
4	eth1	パケット受信時	破棄	全て				

フィルタの解説

「入力フィルタ」「転送フィルタ」

No.1、2：

WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.3：

WAN から来る、ICMP パケットを通す。

No.4：

上記の条件に合致しないパケットを全て破棄する。

第22章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

WWWサーバを公開する際のフィルタ設定例

フィルタの条件

- WAN側からはLAN側のWWWサーバにだけアクセス可能にする。
- LANからWANへのアクセスは自由にできる。
- WANはEther1、LANはEther0ポートに接続。
- ステートフルパケットインスペクションは有効。

LAN構成

- LANのネットワークアドレス「192.168.0.0/24」
- LAN側ポートのIPアドレス「192.168.0.254」
- WWWサーバのアドレス「192.168.0.1」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	eth1	パケット受信時	許可	tcp			192.168.0.1	80
2	eth1	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
3	eth1	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
4	eth1	パケット受信時	破棄	全て				

フィルタの解説

No.1:

192.168.0.1のサーバにHTTPのパケットを通す。

No.2、3:

WANから来る、宛て先ポートが1024から65535のパケットを通す。

No.4:

上記の条件に合致しないパケットを全て破棄する。

FTPサーバを公開する際のフィルタ設定例

フィルタの条件

- WAN側からはLAN側のFTPサーバにだけアクセスが可能にする。
- LANからWANへのアクセスは自由にできる。
- WANはEther1、LANはEther0ポートに接続する。
- NATは有効。
- Ether1ポートはPPPoE回線に接続する。
- ステートフルパケットインスペクションは有効。

LAN構成

- LANのネットワークアドレス「192.168.0.0/24」
- LAN側ポートのIPアドレス「192.168.0.254」
- FTPサーバのアドレス「192.168.0.2」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット受信時	許可	tcp			192.168.0.2/32	21
2	ppp0	パケット受信時	許可	tcp			192.168.0.2/32	20
3	ppp0	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
4	ppp0	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
5	ppp0	パケット受信時	破棄	全て				

フィルタの解説

No.1:

192.168.0.2のサーバにftpのパケットを通す。

No.2:

192.168.0.2のサーバにftpdataのパケットを通す。

No.3、4:

WANから来る、宛て先ポートが1024から65535のパケットを通す。

No.5:

上記の条件に合致しないパケットを全て破棄する。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

第22章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

WWW、FTP、メール、DNSサーバを公開する際の フィルタ設定例

フィルタの条件

- ・WAN側からはLAN側のWWW、FTP、メールサーバにだけアクセスが可能にする。
- ・DNSサーバがWANと通信できるようにする。
- ・LANからWANへのアクセスは自由にできる。
- ・WANはEther1、LANはEther0ポートに接続する。
- ・PPPoEでADSLに接続する。
- ・NATは有効。
- ・ステートフルパケットインスペクションは有効。

LAN構成

- ・LANのネットワークアドレス 「192.168.0.0/24」
- ・LAN側ポートのIPアドレス 「192.168.0.254」
- ・WWWサーバのアドレス 「192.168.0.1」
- ・メールサーバのアドレス 「192.168.0.2」
- ・FTPサーバのアドレス 「192.168.0.3」
- ・DNSサーバのアドレス 「192.168.0.4」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット受信時	許可	tcp			192.168.0.1	80
2	ppp0	パケット受信時	許可	tcp			192.168.0.2	25
3	ppp0	パケット受信時	許可	tcp			192.168.0.2	110
4	ppp0	パケット受信時	許可	tcp			192.168.0.3	21
5	ppp0	パケット受信時	許可	tcp			192.168.0.3	20
6	ppp0	パケット受信時	許可	tcp			192.168.0.4	53
7	ppp0	パケット受信時	許可	udp			192.168.0.4	53
8	ppp0	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
9	ppp0	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
10	ppp0	パケット受信時	継承	全て				

フィルタの解説

- No.1 :
192.168.0.1のサーバにHTTPのパケットを通す。
- No.2 :
192.168.0.2のサーバにSMTPのパケットを通す。
- No.3 :
192.168.0.2のサーバにPOP3のパケットを通す。
- No.4 :
192.168.0.3のサーバにftpのパケットを通す。
- No.5 :
192.168.0.3のサーバにftpdataのパケットを通す。
- No.6、7 :
192.168.0.4のサーバに、domainのパケット(tcp,udp)を通す。
- No.8、9 :
WANから来る、宛て先ポートが1024から65535のパケットを通す。
- No.10 :
上記の条件に合致しないパケットを全て破棄する。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

第22章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

NetBIOSパケットが外部へ出るのを防止する フィルタ設定

フィルタの条件

- LAN側から送出されたNetBIOSパケットをWANへ出さない。(Windowsでの自動接続を防止する)

LAN構成

- LANのネットワークアドレス「192.168.0.0/24」
- LAN側ポートのIPアドレス「192.168.0.254」

設定画面での入力方法

「入力フィルタ」

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	eth0	パケット受信時	破棄	tcp				137:139
2	eth0	パケット受信時	破棄	udp				137:139
3	eth0	パケット受信時	破棄	tcp		137		
4	eth0	パケット受信時	破棄	udp		137		

「転送フィルタ」

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	eth0	パケット受信時	破棄	tcp				137:139
2	eth0	パケット受信時	破棄	udp				137:139
3	eth0	パケット受信時	破棄	tcp		137		
4	eth0	パケット受信時	破棄	udp		137		

フィルタの解説

「入力フィルタ」「転送フィルタ」

No.1 :

宛て先ポートがtcpの137から139のパケットをEther0ポートで破棄する。

No.2 :

宛て先ポートがudpの137から139のパケットをEther0ポートで破棄する。

No.3 :

送信先ポートがtcpの137のパケットをEther0ポートで破棄する。

No.4 :

送信先ポートがudpの137のパケットをEther0ポートで破棄する。

WANからのブロードキャストパケットを破棄する フィルタ設定(smurf攻撃の防御)

フィルタの条件

- WAN側からのブロードキャストパケットを受け取らないようにする。 smurf攻撃を防御する

LAN構成

- プロバイダから割り当てられたネットワーク空間「210.xxx.xxx.32/28」
- WAN側はPPPoE回線に接続する。
- WAN側ポートのIPアドレス「210.xxx.xxx.33」

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット受信時	破棄	全て			210.xxx.xxx.32/32	
2	ppp0	パケット受信時	破棄	全て			210.xxx.xxx.47/32	

フィルタの解説

No.1 :

210.xxx.xxx.32/32 (210.xxx.xxx.32/28のネットワークアドレス)宛てのパケットを受け取らない。

No.2 :

210.xxx.xxx.47/32 (210.xxx.xxx.32/28のネットワークのブロードキャストアドレス)宛てのパケットを受け取らない。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

第22章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

WANからのパケットを破棄するフィルタ設定 (IP spoofing 攻撃の防御)

フィルタの条件

- ・WAN側からの不正な送信元IPアドレスを持つパケットを受け取らないようにする。
IP spoofing 攻撃を受けないようにする。

LAN構成

- ・LAN側のネットワークアドレス
「192.168.0.0/24」
- ・WAN側はPPPoE回線に接続する。

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
2	ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
3	ppp0	パケット受信時	破棄	全て	192.168.0.0/16			

フィルタの解説

No.1、2、3：

- WANから来る、送信元IPアドレスがプライベートアドレスのパケットを受け取らない。
WAN上にプライベートアドレスは存在しない。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

外部からの攻撃を防止する総合的なフィルタリング設定

フィルタの条件

- ・WAN側からの不正な送信元・送信先IPアドレスを持つパケットを受け取らないようにする。
WANからの攻撃を受けない・攻撃の踏み台にされないようにする。

LAN構成

- ・プロバイダから割り当てられたアドレス空間
「202.xxx.xxx.112/28」
- ・LAN側のネットワークアドレス
「192.168.0.0/24」
- ・WAN側はPPPoE回線に接続する。

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
2	ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
3	ppp0	パケット受信時	破棄	全て	192.168.0.0/16			
4	ppp0	パケット受信時	破棄	全て			202.xxx.xxx.127/3	

「出力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット送信時	許可	全て	10.0.0.0/8			
2	ppp0	パケット送信時	許可	全て	172.16.0.0/16			
3	ppp0	パケット送信時	許可	全て	192.168.0.0/16			

フィルタの解説

「入力フィルタ」

No.1、2、3：

- WANから来る、送信元IPアドレスがプライベートアドレスのパケットを受け取らない。
WAN上にプライベートアドレスは存在しない。

No.4：

- WANからのブロードキャストパケットを受け取らない。
smurf 攻撃の防御

「出力フィルタ」

No.1、2、3：

- 送信元IPアドレスが不正なパケットを送出しない。
WAN上にプライベートアドレスは存在しない。

第22章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

PPTPを通すためのフィルタ設定

フィルタの条件

- ・WAN側からのPPTPアクセスを許可する。

LAN構成

- ・WAN側はPPPoE回線に接続する。

設定画面での入力方法

「転送フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛先アドレス	宛先ポート
1	ppp0	パケット受信時	許可	tcp				1723
2	ppp0	パケット受信時	許可	gre				

フィルタの解説

PPTPでは以下のプロトコル・ポートを使って通信します。

- ・プロトコル「GRE」
- ・プロトコル「tcp」のポート「1723」

したがって、フィルタ設定では上記2つの条件に合致するパケットを通す設定をおこなっています。

第 22 章 パケットフィルタリング機能

V. 外部から設定画面にアクセスさせる設定

以下は、PPPoE で接続した場合の設定方法です。

1 まず設定画面にログインし、パケットフィルタ設定の「入力フィルタ」画面を開きます。

2 「入力フィルタ」設定の中で、以下のような設定を追加してください。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛先アドレス	宛先ポート
1	ppp0	パケット受信時	許可	tcp	xxx.xxx.xxx.xxx			880

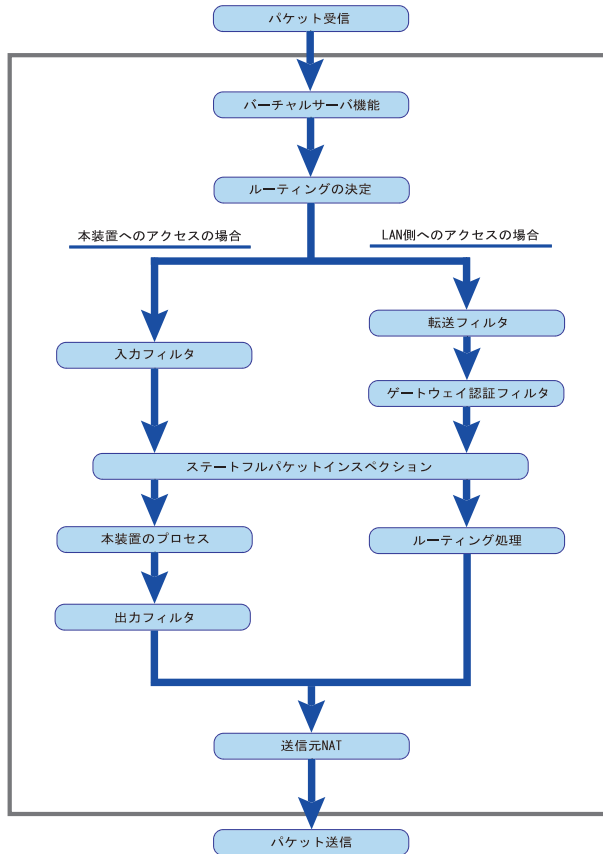
上記設定では、xxx.xxx.xxx.xxx の IP アドレスを持つホストだけが、外部から本装置の設定画面へのアクセスが可能になります。

また「送信元アドレス」を空欄にすると、すべてのインターネット上のホストから、本装置にアクセス可能になります(**セキュリティ上たいへん危険** **ですので、この設定は推奨いたしません**)。

第22章 パケットフィルタリング機能

補足：NATとフィルタの処理順序について

本装置における、NATとフィルタリングの処理方法は以下のようになっています。



(図の上部をWAN側、下部をLAN側とします。またLAN → WANへNATをおこなうとします。)

- WAN側からパケットを受信したとき、最初に「バーチャルサーバ設定」が参照されます。
- 「バーチャルサーバ設定」で静的NAT変換したあとに、パケットがルーティングされます。
- 本装置自身へのアクセスをフィルタするときは「入力フィルタ」、本装置自身からのアクセスをフィルタするときは「出力フィルタ」で設定します。
- WAN側からLAN側へのアクセスをフィルタするときは「転送フィルタ」で設定します。その場合のあて先アドレスは「(LAN側の)プライベートアドレス」になります(NATの後の処理となるためです)。
- ステートフルパケットインスペクションだけを有効にしている場合、WANからLAN、また本装置自身へのアクセスはすべて破棄されます。
- ステートフルパケットインスペクションと同時に「入力フィルタ」「転送フィルタ」を設定している場合は、先に「入力フィルタ」「転送フィルタ」にある設定が優先して処理されます。
- 「送信元NAT設定」は、一番最後に参照されます。
- LAN側からWAN側へのアクセスの場合も、処理の順序は同様です。
(最初にバーチャルサーバ設定が参照されます。)

第22章 パケットフィルタリング機能

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細はRFC1700(Oct. 1994)を参照してください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137~139
snmp	161
snmptrap	162
route	520

第22章 パケットフィルタリング機能

補足：フィルタのログ出力内容について

フィルタ設定画面で「LOG」にチェックを入れると、その設定に合致したパケットの情報を syslog に出力します。出力内容は以下ようになります。

<入力パケットを破棄したときのログ出力例>

```
Jan 25 14:14:07 localhost XR-Filter: FILTER_INPUT_1 IN=eth0 OUT= MAC=00:80:6d:xx:xx:xx:00:20:ed:yy:yy:yy:80:00 SRC=192.168.xxx.xxx DST=xxx.xxx.xxx.xxx LEN=40 TOS=00 PREC=0x00 TTL=128 ID=43951 CE DF PROTO=TCP SPT=2526 DPT=880 SEQ=4098235374 ACK=1758964579 WINDOW=48000 ACK URGP=0
```

Jan 25 14:14:07	syslog がログを取得した日時です。
XR-Filter:	フィルタのログであることを表します。
FILTER_INPUT_1	入力フィルタの1番目のフィルタで取得されたものです。 FILTER_FORWARD は転送フィルタを意味します。
IN=	パケットを受信したインターフェースが記されます。
OUT=	パケットを送出したインターフェースが記されます。なにも記載されていないときは、XRのどのインターフェースからもパケットを送出していないことを表わしています。
MAC=	送信元・あて先のMACアドレスが記されます。
SRC=	送信元IPアドレスが記されます。
DST=	送信先IPアドレスが記されます。
LEN=	パケット長が記されます。
TOS=	TOS bitの状態が記されます。
TTL=	TTLの値が記されます。
ID=	IPのIDが記されます。
PROTO=	プロトコルが記されます。
SPT=	送信元ポートが記されます。
DPT=	送信先ポートが記されます。

プロトコルが ICMP の時は、以下のような ICMP 用のメッセージも記されます。

TYPE=0	ICMP のタイプが記されます。
CODE=0	ICMP のコードが記されます。
ID=3961	ICMP の ID が記されます。
SEQ=6656	ICMP のシーケンス番号が記されます。

第 23 章

スケジュール設定
(XR-640L2 のみ)

第23章 スケジュール設定 (XR-640L2のみ)

スケジュール機能の設定方法

XR-640L2には、主回線を接続または切断する時間を管理するスケジュール機能があります。

スケジュールの設定は10個まで設定できます

Web 設定画面の「スケジュール設定」をクリックします。

スケジュール設定

時間	動作	実行	有効期限	スケジュール
1	スケジュールは設定されていません			
2	スケジュールは設定されていません			
3	スケジュールは設定されていません			
4	スケジュールは設定されていません			
5	スケジュールは設定されていません			
6	スケジュールは設定されていません			
7	スケジュールは設定されていません			
8	スケジュールは設定されていません			
9	スケジュールは設定されていません			
10	スケジュールは設定されていません			

1～10のいずれかをクリックし、以下の画面でスケジュール機能の詳細を設定します。

スケジュール No.1

時刻 動作

実行日

毎日

毎週

毎月

有効期限

なし

1月 1日 ~ 1月 1日 の期間

2007年 1月 1日 以降

2007年 1月 1日 まで

2007年 1月 1日 に実行

スケジュールを

スケジュール
実行させる「時刻」「動作」を設定します。

「時刻」
実行させる時刻を設定します。

「動作」
動作内容を設定します。
「時刻」項目で設定した時間に主回線を接続する場合は「主回線接続」、切断する場合は「主回線切断」を選択します。

実行日
実行する日を「毎日」「毎週」「毎月」の中から選択します。

「毎日」
毎日同じ時間に接続 / 切断するように設定する場合に選択します。

「毎週」
毎週同じ曜日の同じ時間に接続 / 切断するように設定する場合に選択します。
なお、複数の曜日を選択することができます。

「毎月」
毎月同じ日の同じ時間に接続 / 切断するように設定する場合に選択します。
なお、複数の日を選択することができます。

複数選択する場合

【Windows の場合】

Control キーを押しながらクリックします。

【Macintosh の場合】

Command キーを押しながらクリックします。

第23章 スケジュール設定 (XR-640L2のみ)

スケジュール機能の設定方法

有効期限

実行有効期限を設定します。有効期限は、常に設定する年から10年分まで設定できます。

有効期限で「xxxx年xx月xx日に実行」を選択した場合、実行日は「毎日」のみ選択できます。

「なし」

特に実行する期限を定めない場合に選択します。

「xx月xx日～x月x日の期間」

実行する期間を定める場合に選択し、有効期限を設定します。

「xxxx年xx月xx日以降」

実行する期間の開始日を設定したい場合に選択します。

「xxxx年xx月xx日まで」

実行する期間の終了日を設定したい場合に選択します。

「xxxx年xx月xx日に実行」

実行する日時を設定したい場合に選択します。

設定したスケジュール内容の実行・削除・保存を決定します。

「スケジュールを有効にする」

設定したスケジュールを起動する場合に選択します。

「スケジュールを無効にする」

スケジュールの設定内容を残しておきたい場合に選択します(スケジュールは起動しません)。

「スケジュールを削除する」

スケジュールの設定内容を削除する場合に選択します。

入力が終わりましたら、「設定 / 削除の実行」をクリックします。

設定内容は画面上のスケジュール設定欄に反映されます。

スケジュール設定欄の項目について

スケジュール設定欄にある項目(「時間」「動作」「実行」「有効期間」「スケジュール」)のリンクをクリックすると、クリックした項目を基準にしたソートがかかります。

<例>

スケジュール設定

時間	動作	実行	有効期限	スケジュール
1 15:51	主回線接続	毎日	なし	無効
2 08:00	主回線切断	毎週月水曜日	2007年9月1日以降	有効
3 18:10	主回線切断	毎日	なし	無効
4 23:00	主回線接続	毎週日火曜日	2007年9月30日以降	有効
5	スケジュールは設定されていません			
6	スケジュールは設定されていません			
7	スケジュールは設定されていません			
8	スケジュールは設定されていません			
9	スケジュールは設定されていません			
10	スケジュールは設定されていません			

上の画面で「時間」項目をクリックします。

下の画面のように、「時間」の早い順番に並べ替えられます。

スケジュール設定

時間	動作	実行	有効期限	スケジュール
1 08:00	主回線切断	毎週月水曜日	2007年9月1日以降	有効
2 15:51	主回線接続	毎日	なし	無効
3 18:10	主回線切断	毎日	なし	無効
4 23:00	主回線接続	毎週日火曜日	2007年9月30日以降	有効
5	スケジュールは設定されていません			
6	スケジュールは設定されていません			
7	スケジュールは設定されていません			
8	スケジュールは設定されていません			
9	スケジュールは設定されていません			
10	スケジュールは設定されていません			

第24章

ネットワークイベント機能

第24章 ネットワークイベント機能

1. 機能の概要

ネットワークイベントは、回線障害などのネットワーク状態の変化を検知し、それをトリガとして特定のイベントを実行する機能です。

本装置では、以下のネットワーク状態の変化をトリガとして検知することができます。

- ・ ping 監視の状態
- ・ link 監視の状態
- ・ vrrp 監視の状態

ping 監視

本装置から任意の宛先へ ping を送信し、その応答の有無を監視します。一定時間応答がなかった時にトリガとして検知します。また、再び応答を受信した時は、復旧トリガとして検知します。

link 監視

Ethernet インタフェースや ppp インタフェースのリンク状態を監視します。監視するインタフェースのリンクがダウンした時にトリガとして検知します。また再びリンクがアップした時は復旧トリガとして検知します。

vrrp 監視

本装置の VRRP ルータ状態を監視します。指定したルータ ID の VRRP ルータがバックアップルータへ切り替わった時にトリガとして検知します。また、再びマスタールータへ切り替わった時は復旧トリガとして検知します。

またこれらのトリガを検知した際に実行可能なイベントとして以下の2つがあります。

- ・ VRRP 優先度変更
- ・ IPsec 接続切断

VRRP 優先度変更

トリガ検知時に、指定した VRRP ルータの優先度を変更します。またトリガ復旧時には、元の VRRP 優先度に変更します。

例えば、ping 監視と連動して、PPPoE 接続先がダウンした時に、自身は VRRP バックアップルータに移行し、新マスタールータ側の接続へ切り替える、といった使い方ができます。

IPsec 接続 / 切断

トリガ検知時に、指定した IPsec ポリシーを切断します。またトリガ復旧時には、IPsec ポリシーを再び接続します。

例えば、vrrp 監視と連動して、2台の VRRP ルータのマスタールータの切り替わりに応じて、IPsec 接続を繋ぎかえる、といった使い方ができます。

第 24 章 ネットワークイベント機能

1. 機能の概要

本機能で使用する各種テーブルについて

本機能は複数のテーブル定義を連携させることによって実現しています。



ping監視テーブル / link監視テーブル / vrrp監視テーブル

これらのテーブルでは、監視対象、監視周期、障害検出した場合のトリガー番号を設定します。

ここで設定を有効(enable)にしたトリガー番号は、次の「ネットワークイベント設定テーブル」のインデックス番号になります。

ネットワークイベント設定テーブル

このテーブルでは、トリガー番号とイベント番号の関連付けを定義します。

ここで設定したイベント番号は、次の「イベント実行テーブル」のインデックス番号になります。

イベント実行テーブル

このテーブルでは、イベント番号と実行イベント種別 / オプション番号の関連付けを定義します。

イベントの実行種別を「VRRP優先度」に設定した場合は、次に「VRRP優先度テーブル」を索引します。設定したオプション番号は、テーブルのインデックス番号になります。

また、イベントの実行種別を「IPSECポリシー」に設定した場合は、次に「IPsec接続切断テーブル」を索引します。設定したオプション番号は、テーブルのインデックス番号になります。

VRRP優先度テーブル

このテーブルでは、VRRP優先度を変更するルータIDとその優先度を定義します。

IPsec接続切断テーブル

このテーブルでは、IPsec接続 / 切断を行うIPsecポリシー番号、またはIPsecインタフェース名を定義します。

第24章 ネットワークイベント機能

II. 各トリガテーブルの設定

ping 監視の設定方法

設定画面上部の「ping 監視の設定」をクリックして、以下の画面から設定します。

ネットワークping設定

NO	enable	トリガー番号	インターバル	リトライ	送信先アドレス
1	<input type="checkbox"/>	1	10	3	
2	<input type="checkbox"/>	2	10	3	
3	<input type="checkbox"/>	3	10	3	
4	<input type="checkbox"/>	4	10	3	
5	<input type="checkbox"/>	5	10	3	
6	<input type="checkbox"/>	6	10	3	
7	<input type="checkbox"/>	7	10	3	
8	<input type="checkbox"/>	8	10	3	
9	<input type="checkbox"/>	9	10	3	
10	<input type="checkbox"/>	10	10	3	
11	<input type="checkbox"/>	11	10	3	
12	<input type="checkbox"/>	12	10	3	
13	<input type="checkbox"/>	13	10	3	
14	<input type="checkbox"/>	14	10	3	
15	<input type="checkbox"/>	15	10	3	
16	<input type="checkbox"/>	16	10	3	

enable

チェックを入れることで設定を有効にします。

トリガー番号

ping送信先から応答が無かった場合に検知するトリガーの番号(1 ~ 16)を指定します。本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

インターバル(秒)

リトライ

pingを発行する間隔を設定します。

「『インターバル』秒間に、『リトライ』回pingを発行する」という設定になります。この間、一度も応答が無かった場合にトリガとして検知されません。

送信先アドレス

pingを送信する先のIPアドレスを指定します。

最後に「設定の保存」をクリックして設定完了です。

link 監視の設定方法

設定画面上部の「link 監視の設定」をクリックして、以下の画面から設定します。

デバイス監視設定

NO	enable	トリガー番号	インターバル	リトライ	監視するデバイス名
1	<input type="checkbox"/>	1	10	3	
2	<input type="checkbox"/>	2	10	3	
3	<input type="checkbox"/>	3	10	3	
4	<input type="checkbox"/>	4	10	3	
5	<input type="checkbox"/>	5	10	3	
6	<input type="checkbox"/>	6	10	3	
7	<input type="checkbox"/>	7	10	3	
8	<input type="checkbox"/>	8	10	3	
9	<input type="checkbox"/>	9	10	3	
10	<input type="checkbox"/>	10	10	3	
11	<input type="checkbox"/>	11	10	3	
12	<input type="checkbox"/>	12	10	3	
13	<input type="checkbox"/>	13	10	3	
14	<input type="checkbox"/>	14	10	3	
15	<input type="checkbox"/>	15	10	3	
16	<input type="checkbox"/>	16	10	3	

enable

チェックを入れることで設定を有効にします。

トリガー番号

監視するインターフェースのリンクがダウンした場合に検知するトリガーの番号(1 ~ 16)を指定します。本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

インターバル(秒)

リトライ

インターフェースのリンク状態を監視する間隔を設定します。

「『インターバル』秒間に、『リトライ』回、インターフェースのリンク状態をチェックする」という設定になります。この間、リンク状態が全てダウンだった場合にトリガとして検知されます。

監視するデバイス名

リンク状態を監視するデバイスのインターフェース名を指定します。Ethernet インターフェース名、またはPPP インターフェース名を入力してください。

最後に「設定の保存」をクリックして設定完了です。

第24章 ネットワークイベント機能

II. 各トリガテーブルの設定

vrrip 監視の設定方法

設定画面上部の「vrrip 監視の設定」をクリックして、以下の画面から設定します。

vrrip監視設定

NO	enable	トリガー番号	インターバル	リトライ	VRRP ルータID
1	<input type="checkbox"/>	1	10	3	
2	<input type="checkbox"/>	2	10	3	
3	<input type="checkbox"/>	3	10	3	
4	<input type="checkbox"/>	4	10	3	
5	<input type="checkbox"/>	5	10	3	
6	<input type="checkbox"/>	6	10	3	
7	<input type="checkbox"/>	7	10	3	
8	<input type="checkbox"/>	8	10	3	
9	<input type="checkbox"/>	9	10	3	
10	<input type="checkbox"/>	10	10	3	
11	<input type="checkbox"/>	11	10	3	
12	<input type="checkbox"/>	12	10	3	
13	<input type="checkbox"/>	13	10	3	
14	<input type="checkbox"/>	14	10	3	
15	<input type="checkbox"/>	15	10	3	
16	<input type="checkbox"/>	16	10	3	

enable

チェックを入れることで設定を有効にします。

トリガー番号

監視する VRRP ルータがバックアップへ切り替わった場合に検知するトリガーの番号(1 ~ 16)を指定します。本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

インターバル(秒)

リトライ

VRRP ルータの状態を監視する間隔を設定します。「『インターバル』秒間に、『リトライ』回、VRRP のルータ状態を監視する」という設定になります。この間、監視した状態が全てバックアップ状態であった場合にトリガとして検知されます。

VRRP ルータ ID

VRRP ルータ状態を監視するルータ ID を指定します。

最後に「設定の保存」をクリックして設定完了です。

各監視機能を有効にするにはネットワークイベントサービス設定画面で、「起動」ボタンにチェックを入れ、「動作変更」をクリックしてサービスを起動してください。

また設定の変更、追加、削除を行った場合は、サービスの再起動を行ってください。

(注) 各監視設定で指定したトリガー番号は、「ネットワークイベント設定」テーブルでのインデックス番号となるため、それぞれの監視設定の間で同じトリガー番号が有効にならないように設定してください。

第24章 ネットワークイベント機能

III. 実行イベントテーブルの設定

ネットワークイベント設定テーブルの設定

設定画面上部の「ネットワークイベント設定」をクリックして、以下の画面から設定します。

ネットワークイベント設定

イベント実行テーブル設定

NO	トリガー番号	実行イベントテーブル番号
1	<input type="text" value="1"/>	<input type="text" value="1"/>
2	<input type="text" value="2"/>	<input type="text" value="2"/>
3	<input type="text" value="3"/>	<input type="text" value="3"/>
4	<input type="text" value="4"/>	<input type="text" value="4"/>
5	<input type="text" value="5"/>	<input type="text" value="5"/>
6	<input type="text" value="6"/>	<input type="text" value="6"/>
7	<input type="text" value="7"/>	<input type="text" value="7"/>
8	<input type="text" value="8"/>	<input type="text" value="8"/>
9	<input type="text" value="9"/>	<input type="text" value="9"/>
10	<input type="text" value="10"/>	<input type="text" value="10"/>
11	<input type="text" value="11"/>	<input type="text" value="11"/>
12	<input type="text" value="12"/>	<input type="text" value="12"/>
13	<input type="text" value="13"/>	<input type="text" value="13"/>
14	<input type="text" value="14"/>	<input type="text" value="14"/>
15	<input type="text" value="15"/>	<input type="text" value="15"/>
16	<input type="text" value="16"/>	<input type="text" value="16"/>

トリガー番号

「ping 監視の設定」、「link 監視の設定」、「vrrp 監視の設定」で設定したトリガー番号を指定します。なお、複数のトリガー検知の組み合わせによって、イベントを実行させることも可能です。

<例>

- ・トリガー番号1とトリガー番号2のどちらかを検知した時にイベントを実行させる場合
1&2
- ・トリガー番号1とトリガー番号2の両方を検知した時、またはトリガー番号3を検知した時にイベントを実行させる場合
[1|2]&3

実行イベントテーブル番号

そのトリガー番号を検知した時に実行されるイベント番号(1～16)を指定します。本値は、イベント実行テーブルでのインデックス番号となります。なお、複数のイベントを同時に実行させることも可能です。その場合は「_」でイベント番号を繋ぎます。

<例> イベント番号1,2,3を同時に実行させる場合
1_2_3

最後に「設定の保存」をクリックして設定完了です。

イベント実行テーブルの設定

設定画面上部の「イベント実行テーブル設定」をクリックして、以下の画面から設定します。

イベント実行テーブル設定

ネットワークイベント設定

NO	実行イベント設定	オプション設定
1	IPsecポリシー	<input type="text" value="1"/>
2	VRRP 優先度	<input type="text" value="2"/>
3	VRRP 優先度	<input type="text" value="3"/>
4	VRRP 優先度	<input type="text" value="4"/>
5	VRRP 優先度	<input type="text" value="5"/>
6	VRRP 優先度	<input type="text" value="6"/>
7	VRRP 優先度	<input type="text" value="7"/>
8	VRRP 優先度	<input type="text" value="8"/>
9	VRRP 優先度	<input type="text" value="9"/>
10	VRRP 優先度	<input type="text" value="10"/>
11	VRRP 優先度	<input type="text" value="11"/>
12	VRRP 優先度	<input type="text" value="12"/>
13	VRRP 優先度	<input type="text" value="13"/>
14	VRRP 優先度	<input type="text" value="14"/>
15	VRRP 優先度	<input type="text" value="15"/>
16	VRRP 優先度	<input type="text" value="16"/>

実行イベント設定

実行されるイベントの種類を選択します。

「IPsec ポリシー」は、IPsec ポリシーの切断を行います。

「VRRP 優先度」は、VRRP ルータの優先度を変更します。

オプション設定

実行イベントのオプション番号です。本値は、「VRRP 優先度変更設定」テーブル、または「IPSEC 接続切断設定」テーブルでのインデックス番号となります。

最後に「設定の保存」をクリックして設定完了です。

IV. 実行イベントのオプション設定

VRRP 優先度変更設定テーブルの設定

設定画面上部の「VRRP 優先度」をクリックして、以下の画面から設定します。

VRRP 優先度変更設定
現在のVRRPの状態

NO	ルータID	優先度
1	51	50
2	52	50
3	53	50
4	54	50
5	55	50
6	56	50
7	57	50
8	58	50
9	59	50
10	60	50
11	61	50
12	62	50
13	63	50
14	64	50
15	65	50
16	66	50

ルータ ID

トリガ検知時に VRRP 優先度を変更する VRRP ルータ ID を指定します。

優先度

トリガ検知時に変更する VRRP 優先度を指定します。1 ~ 255 の間で設定してください。
なお、トリガ復旧時には「VRRP サービス」で設定されている元の値に戻ります。

最後に「設定の保存」をクリックして設定完了です。

IPSEC 接続切断設定 テーブルの設定

設定画面上部の「IPSEC ポリシー」をクリックして、次の画面から設定します。

IPSEC 接続切断設定
現在のIPSECの状態

NO	IPSECポリシー番号、 又はインターフェース名	使用IKE連動機能	使用interface連動機能
1		使用しない	使用する
2		使用しない	使用する
3		使用しない	使用する
4		使用しない	使用する
5		使用しない	使用する
6		使用しない	使用する
7		使用しない	使用する
8		使用しない	使用する
9		使用しない	使用する
10		使用しない	使用する
11		使用しない	使用する
12		使用しない	使用する
13		使用しない	使用する
14		使用しない	使用する
15		使用しない	使用する
16		使用しない	使用する

IPSEC ポリシー番号、又はインターフェース名 トリガ検知時に切断する IPsec ポリシーの番号、又は IPsec インターフェース名を指定します。ポリシー番号は、範囲で指定することもできます。

例) IPsec ポリシー 1 から 20 を切断する **1:20**

インターフェース名を指定した場合は、そのインターフェースで接続する IPsec は全て切断されます。トリガ復旧時には再度 IPsec 接続されます。

使用 IKE 連動機能

切断する IPsec ポリシーが使用する IKE と同じ IKE を使用する IPsec ポリシーが設定されている場合において、トリガ検知時にその IKE を使用する全ての IPsec ポリシーを切断する場合は、「使用する」を選択します。ここで設定した IPsec ポリシーのみを切断する場合は「使用しない」を選択します。

使用 interface 連動機能

本装置では、PPPoE 上で IPsec 接続している場合、PPPoE 接続時に自動的に IPsec 接続も開始されます。ネットワークイベント機能を使った IPsec 二重化において、バックアップ側の PPPoE 接続時に IPsec を自動接続させたくない場合には「使用しない」を選択します。

最後に「設定の保存」をクリックして設定完了です。

ステータスの表示

設定画面上部の「ステータス」をクリックして表示します。



トリガー情報

設定が有効なトリガー番号とその状態を表示します。

“ON”と表示されている場合は、トリガを検知していない、またはトリガが復旧している状態を表します。

“OFF”と表示されている場合は、トリガ検知している状態を表します。

イベント情報

・No.

イベント番号とその状態を表します。

“x”の表示は、トリガ検知し、イベントを実行している状態を表します。

“o”の表示は、トリガ検知がなく、イベントが実行されていない状態を表します。

“-”の表示は、無効なイベントです。

・トリガー

イベント実行の条件となるトリガ番号とその状態を表します。

・イベントテーブル

左からイベント実行テーブルのインデックス番号、実行イベント種別、オプションテーブル番号を表します。

第 25 章

仮想インターフェース機能

第 25 章 仮想インターフェース機能

仮想インターフェース機能の設定

主にバーチャルサーバ機能を利用する場合に、仮想インターフェースを設定します。

設定方法

Web 設定画面「仮想インターフェース」をクリックして、以下の画面から設定します。

No.	インターフェース	仮想 I/F 番号	IP アドレス	ネットマスク	削除
1	ppp0	1	192.168.0.254	255.255.255.0	<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>
11					<input type="checkbox"/>
12					<input type="checkbox"/>
13					<input type="checkbox"/>
14					<input type="checkbox"/>
15					<input type="checkbox"/>
16					<input type="checkbox"/>

(画面は設定例です)

インターフェース

仮想インターフェースを作成するインターフェース名を指定します。本装置のインターフェース名については、本マニュアルの「付録 A インターフェース名について」をご参照ください。

仮想 I/F 番号

作成するインターフェースの番号を指定します。
0 ~ 127 の間で設定できます。

IP アドレス

作成するインターフェースの IP アドレスを指定します。

ネットマスク

作成するインターフェースのネットマスクを指定します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

”No.” 項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

設定を削除する

仮想インターフェース設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

第 26 章

GRE 設定

GRE の設定

GRE は Generic Routing Encapsulation の略で、リモート側にあるルータまで仮想的なポイントツーポイント リンクを張って、多種プロトコルのパケットを IP トンネルにカプセル化するプロトコルです。

また IPsec トンネル内に GRE トンネルを生成することもできますので、GRE を使用する場合でもセキュアな通信を確立することができます。

設定は設定画面左「GRE 設定」でおこないます。

インタフェースアドレス	<input type="text" value="172.10.10.1/30"/> (例:192.168.0.1/30)
リモート(宛先)アドレス	<input type="text" value="192.168.121.1"/> (例:192.168.1.1)
ローカル(送信元)アドレス	<input type="text" value="192.168.121.2"/> (例:192.168.2.1)
PEERアドレス	<input type="text" value="172.10.10.2/30"/> (例:192.168.0.2/30)
TTL	<input type="text" value="255"/> (1-255)
MTU	<input type="text" value="1476"/> (最大値 1476)
TOS設定	<input checked="" type="radio"/> TOS 値の指定 <input type="text" value=""/> (0x0-0xff) <input type="radio"/> inherit(TOS 値のコピー)
GREoverIPsec	<input type="radio"/> 使用する <input type="text" value="IPsec0"/> <input checked="" type="radio"/> Routing Table に依存
IDキーの設定	<input type="text" value=""/> (0-4294967295)
End-to-End Checksumming	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 MSS 値 <input type="text" value="0"/> Byte <small>(有効時にMSS値が0の場合は、MSS値を自動設定(Clamp MSS to MTU)します。)</small>

インタフェースアドレス

GRE トンネルを生成するインタフェースの仮想アドレスを設定します。任意で指定します。

例) 192.168.90.1/30

リモート(宛先)アドレス

GRE トンネルのエンドポイントの IP アドレス(対向側装置の WAN 側 IP アドレス)を設定します。

ローカル(送信元)アドレス

本装置の WAN 側 IP アドレスを設定します。

PEER アドレス

GRE トンネルを生成する対向側装置のインタフェースの仮想アドレスを設定します。「インタフェースアドレス」と同じネットワークに属するアドレスを指定してください。

例) 192.168.90.2/30

TTL

GRE パケットの TTL 値を設定します。

MTU

MTU 値を設定します。最大値は 1500byte です。

Path MTU Discovery

Path MTU Discovery 機能を有効にするかを選択します。

機能を有効にした場合は、常に IP ヘッダの DF ビットを ON にして転送します。転送パケットの DF ビットが 1 でパケットサイズが MTU を超えている場合は、送信元に ICMP Fragment Needed を返送します。

PathMTU Discovery を無効にした場合、TTL は常にカプセル化されたパケットの TTL 値がコピーされます。従って、GRE 上で OSPF を動かす場合には、TTL が 1 に設定されてしまうため、PathMTU Discovery を有効にしてください。

ToS

GRE パケットの ToS 値を設定します。

GREoverIPsec

IPsec を使用して GRE パケットを暗号化する場合に「使用する」を選択します。またこの場合には別途、IPsec の設定が必要です。

Routing Table に合わせて暗号化したい場合には「Routing Table に依存」を選択します。ルートが IPsec の時は暗号化、IPsec でない時は暗号化しません。

(次ページにつづく)

第26章 GRE 設定

GRE の設定

GRE トンネルを暗号化するときの IPsec 設定は以下のようにしてください。

- ・本装置側設定 **通常通り**
- ・IKE/ISAKMP ポリシー設定 **通常通り**
- ・IPsec ポリシー設定
本装置側の LAN 側のネットワークアドレス：
GRE 設定のローカルアドレス /32

相手側の LAN 側のネットワークアドレス：
GRE 設定のリモートアドレス /32

ID キーの設定

この機能を有効にすると、KEY Field の 4byte が GRE ヘッダに付与されます。

End-to-End Checksumming

チェックサム機能の有効 / 無効を選択します。
この機能を有効にすると、
checksum field (2byte) + offset (2byte)
の計 4byte が GRE パケットに追加されます。

MSS 設定

GRE トンネルに対して、clamp to MSS 機能を有効にしたり、MSS 値の設定が可能です。

入力後は「追加 / 変更」ボタンをクリックします。
直ちに設定が反映され、GRE トンネルが生成されます。

「削除」をクリックすると、その設定に該当する GRE トンネルが無効化されます(設定自体は保存されています)。再度有効とするときは「追加 / 変更」ボタンをクリックしてください。

「現在の状態」では GRE の動作状況が表示されます。

現在の状態 **Tunnel is down, Link is down**

GRE 設定を行うと、設定内容が一覧表示されます。

Interface名	Interface Address	Remote Address	Local Address	Peer Address	MTU	ID Key	Check sum	Link State
gre1	172.10.10.1/30	192.168.121.1	192.168.121.2	172.10.10.2/30	1476		無効	down

設定の編集は「Interface 名」をクリックしてください。また GRE トンネルのリンク状態は「Link State」に表示されます。「UP」が GRE トンネルがリンクアップしている状態です。

第 27 章

QoS 機能

1. QoS について

本装置の優先制御・帯域制御機能(以下、QoS 機能)は以下の5つのキューイング方式で、トラフィック制御をおこないます。

1. PFIFO
2. TBF
3. SFQ
4. PQ
5. CBQ

クラスフル/クラスレスなキューイング

キューイングには、クラスフルなものと同様にクラスレスなものがあります。

クラスレスなキューイングは、内部に設定可能なトラフィック分割用のバンド(クラス)を持たず、到着するすべてのトラフィックを同等に取り扱います。PFIFO、TBF、SFQ がクラスレスなキューイングです。

クラスフルなキューイングでは、内部に複数のクラスを持ち、選別器(クラス分けフィルタ)によって、パケットを送り込むクラスを決定します。各クラスはそれぞれに帯域を持つため、クラス分けすることで帯域制御ができるようになります。またキューイング方式によっては、あるクラスがさらに自分の配下にクラスを持つこともできます。さらに、各クラス内でそれぞれキューイング方式を決めることもできます。PQ と CBQ がクラスフルなキューイングです。

1. QoS について

1. PFIFO

もっとも単純なキューイング方式です。あらかじめキューのサイズを決定しておき、どのパケットも区別なくキューに収納していきます。キューからパケットを送信するとき、送信するパケットはFIFOにしたがって選別されます。

キューのサイズを超えてパケットが到着したとき、超えた分のパケットは全て破棄されてしまいます。

キューのサイズが大きすぎると、キューイングによる遅延が発生する可能性があります。

キューとは、データの入り口と出口を一つだけ持つバッファのことを指します。

FIFOとは「First In First Out」の略で、「最初に入ったものが最初に出る」、つまり最も古いものが最初に取り出されることを指します。

2. TBF

帯域制御方法の1つです。

トークンバケツにトークンを、ある一定の速度(トークン速度)で収納していきます。このトークン1個ずつがパケットを1個ずつつかみ、トークン速度を超えない範囲でパケットを送信していきます(送信後はトークンは削除されます)。

またバケツに溜まっている余分なトークンは、突発的なバースト状態(パケットが大量に届く状態)でパケットが到着しているときに使われます。バーストが起きているときはすでにバケツに溜まっている分のトークンを使ってパケットを送信しますので、溜まった分のトークンを使い切らないような短期的なバーストであれば、トークン速度(制限Rate)を超えたパケット送信が可能です。

バースト状態が続くとバケツのトークンがすぐになくなってしまいうため遅延が発生していき、最終的にはパケットが破棄されてしまうこととなります。

1. QoS について

3. SFQ

SFQはパケットの流れ(トラフィック)を整形しません。パケットを送り出す順番を決めるだけです。

SFQでは、トラフィックを多数の内部キューに分割して収納します。そして各キューをラウンドロビンで回り、各キューからパケットをFIFOで順番に送信していきます。

ラウンドロビンで順番にトラフィックが送信されることから、ある特定のトラフィックが他のトラフィックを圧迫してしまうことがなくなり、どのトラフィックも公平に送信されるようになります(複数のトラフィックを平均化できる)。

整形とは、トラフィック量が一定以上にならないように転送速度を調節することを指します。「シェーピング」とも呼ばれます。

4. PQ

PQは優先制御の1つです。トラフィックのシェーピングは起こりません。

PQでは、パケットを分類して送り込むクラスに優先順位をつけておきます。そしてフィルタによってパケットをそれぞれのクラスに分類したあと、優先度の高いクラスから優先的にパケットを送信します。なお、クラス内のパケットはFIFOで取り出されます。

優先度の高いクラスに常にパケットがキューイングされているときには、より優先度の低いクラスからはパケットが送信されなくなります。

1. QoSについて

5. CBQ

CBQは帯域制御の1つです。複数のクラスを作成しクラスごとに帯域幅を設定することで、パケットの種類に応じて使用できる帯域を割り当てる方式です。

CBQにおけるクラスは、階層的に管理されます。最上位にはrootクラスが置かれ、利用できる総帯域幅を定義しておきます。rootクラスの下に子クラスが置かれ、それぞれの子クラスにはrootで定義した総帯域幅の一部を利用可能帯域として割り当てます。子クラスの下には、さらにクラスを置くこともできます。

各クラスへのパケットの振り分けは、フィルタ(クラス分けフィルタ)の定義に従っておこなわれます。

各クラスには帯域幅を割り当てます。兄弟クラス間で割り当てている帯域幅の合計が、上位クラスで定義している帯域幅を超えないように設計しなければなりません。

また、それぞれのクラスには優先度を割り振り、優先度に従ってパケットを送信していきます。

<クラス構成図(例)>

root クラス (1Mbps)

 クラス 1 (500kbps、優先度 2)

 HTTP (優先度 1)

 FTP (優先度 5)

 クラス 2 (500kbps、優先度 1)

 HTTP (優先度 1)

 FTP (優先度 5)

子クラスからはFIFOでパケットが送信されますが、子クラスの下にキューイングを定義し、クラス内でのキューイングをおこなうこともできます(クラスキューイング)。

CBQの特徴として、各クラス内において、あるクラスが兄弟クラスから帯域幅を借りることができます。たとえば図のクラス1において、トラフィックが500kbpsを超えていて、且つ、クラス2の使用帯域幅が500kbps以下の場合に、クラス1はクラス2で余っている帯域幅を借りてパケットを送信することができます。

11. QoS 機能の各設定画面について

Interface Queuing 設定画面

本装置の各インターフェースでおこなうキューイング方式を定義します。すべてのキューイング方式で設定が必要です。

CLASS 設定

CBQ をおこなう場合の、各クラスについて設定します。

CLASS Queuing 設定

各クラスにおけるキューイング方式を定義します。CBQ 以外のキューイング方式について定義できます。

CLASS 分けフィルタ設定

パケットを各クラスに振り分けるためのフィルタ設定を定義します。PQ、CBQ をおこなう場合に設定が必要です。

パケット分類設定

各パケットに TOS 値や MARK 値を付加するための設定です。PQ をおこなう場合に設定します。PQ では IP ヘッダによる CLASS 分けフィルタリングができないため、TOS 値または MARK 値によってフィルタリングをおこないます。

III. 各キューイング方式の設定手順について

各キューイング方式の基本的な設定手順は以下の通りです。

pfifoの設定手順

「Interface Queueing 設定」でキューのサイズを設定します。

TBFの設定手順

「Interface Queueing 設定」で、トークンのレート、パケットサイズ、キューのサイズを設定します。

SFQの設定手順

「Interface Queueing 設定」で設定します。

PQの設定手順

1. インターフェースの設定

「Interface Queueing 設定」で、Band 数、Priority-map、Marking Filter を設定します。

2. CLASS 分けのためのフィルタ設定

「CLASS 分けフィルタ設定」で、Mark 値によるフィルタを設定します。

3. パケット分類のための設定

「パケット分類設定」で、TOS 値または MARK 値の付与設定をおこないます。

CBQの設定手順

1. ルートクラスの設定

「Interface Queueing 設定」で、ルートクラスの設定をおこないます。

2. 各クラスの設定

・「CLASS 設定」で、全てのクラスの親となる親クラスについて設定します。

・「CLASS 設定」で、親クラスの下に置く子クラスについて設定します。

・「CLASS 設定」で、子クラスの下に置くリーフクラスを設定します。

3. クラス分けの設定

「CLASS 分けフィルタ設定」で、CLASS 分けのマッチ条件を設定します。

4. クラスキューイングの設定

クラス内でさらにキューイングをおこなうときには「CLASS Queueing 設定」でキューイング設定をおこないます。

IV. 各設定画面での設定方法について

Interface Queueing 設定

すべてのキューイング方式において設定が必要です。設定を追加するときは「New Entry」をクリックします。

Interface名	eth0
Queueing Discipline	---
pfifo queue limit (pfifo選択時有効)	
TBF Parameter設定	
制限Rate	Kbit/s
Buffer Size	byte
Limit Byte (tokenが利用できるようになるまで Queueing可能なbyte数)	byte
CBQ Parameter設定	
回線帯域	Kbit/s
平均パケットサイズ	byte
PQ Parameter設定	
最大Band数設定	3 default 3 (2-5)
Priority-map設定	1 2 2 2 1 2 0
Marking Filter選択 (PacketヘッダによるFilter設定は選択できません)	FilterNo. Class No. 1. <input type="checkbox"/> <input type="checkbox"/> 2. <input type="checkbox"/> <input type="checkbox"/> 3. <input type="checkbox"/> <input type="checkbox"/> 4. <input type="checkbox"/> <input type="checkbox"/> 5. <input type="checkbox"/> <input type="checkbox"/> 6. <input type="checkbox"/> <input type="checkbox"/> 7. <input type="checkbox"/> <input type="checkbox"/> 8. <input type="checkbox"/> <input type="checkbox"/> 9. <input type="checkbox"/> <input type="checkbox"/> 10. <input type="checkbox"/> <input type="checkbox"/>

Interface名

キューイングをおこなうインターフェース名を入力します。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名について」をご参照ください。

Queueing Discipline

キューイング方式を選択します。

[pfifoの設定]

pfifo queue limit

パケットをキューイングするキューの長さを設定します。**パケットの数**で指定します。1 ~ 999 の範囲で設定してください。

[TBF の設定]

「TBF Parameter 設定」について設定します。

制限 Rate

パケットにトークンを入れていく速度を設定します。

回線の実効速度を上限に設定してください。

Buffer Size

パケットのサイズを設定します。これは瞬間的に利用できるトークンの最大値となります。帯域の制限幅を大きくするときは、Buffer Size を大きく設定しておきます。

Limit Byte

トークンを待っている状態でキューイングするときの、キューのサイズを設定します。

[SFQ の設定]

Queueing Discipline で「SFQ」を選択するだけです。

IV. 各設定画面での設定方法について

[PQの設定]

「PQ Parameter 設定」について設定します。

最大 Band 数設定

生成するバンド数を設定します。ここでいう band 数はクラス数のことです。

本装置で設定されるクラス ID は 1001:、1002:、1003:、1004:、1005: となります。バンド番号は 1001: が 1、1002: が 2、1003: が 3、1004: が 4、1005: が 5 となります。

Band 数の初期設定は 3 です (クラス ID 1001: ~ 1003:)。設定可能な band 数は 2 ~ 5 です。初期設定外の数値に設定した場合は、Priority-map 設定を変更します。

Priority-map 設定

Priority-map には 7 つの入れ物が用意されています (左から 0、1、2、3、4、5、6 という番号が付けられています)。そしてそれぞれに Band を設定します。最大 Band 数で設定した範囲で、それぞれに Band を設定できます。

Marking Filter 設定

パケットの Marking 情報によって振り分けを決定するときに設定します。

Filter No. には Class 分けフィルタの設定番号を指定します。

Class No. には、パケットをおくるクラス番号 (= Band 番号) を指定します。1001: が 1、1002: が 2、1003: が 3、1004: が 4、1005: が 5 となります。

Priority-map の箱に付けられている番号は、TOS 値の「Linux における扱い番号 (パケットの優先度)」とリンクしています。「TOS 値について」を参照ください)

インターフェースに届いたパケットは、2 つの方法でクラス分けされます。

- ・TOS フィールドの「Linux における扱い番号 (パケットの優先度)」を参照し、同じ番号の Priority-map の箱にパケットを送ります。

- ・Marking Filter 設定に従って、各クラスにパケットを送る

Prioritymap の箱に付けられる Band はクラスのことです。箱に設定されている値のクラスに属することを意味します。Band 数が小さい方が、より優先度が高くなります。

クラス分けされたあとのパケットは、優先度の高いクラスから FIFO で送信されていきます。**各クラスの優先度は 1001: > 1002: > 1003: > 1004: > 1005: となります。**

より優先度の高いクラスにパケットがあると、その間は優先度の低いクラスからはパケットが送信されなくなります。

IV. 各設定画面での設定方法について

[CBQの設定]

「CBQ Parameter 設定」について設定します。

回線帯域

root クラスの帯域幅を設定します。接続回線の物理的な帯域幅を設定します(10Base-TXで接続しているときは10000kbits/s)。

平均パケットサイズ設定

パケットの平均サイズを設定します。バイト単位で設定します。

IV. 各設定画面での設定方法について

CLASS 設定

設定を追加するときは「New Entry」をクリックします。

Description	user_1
Interface名	eth0
Class ID	10
親class ID	1
Priority	1
Rate設定	1000 Kbit/s
Class内Average Packet Size設定	1000 byte
Maximum Burst設定	20
Bounded設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Filter設定 (Filter番号を入力してください)	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/> 5. <input type="text"/> 6. <input type="text"/> 7. <input type="text"/> 8. <input type="text"/> 9. <input type="text"/> 10. <input type="text"/>

(画面は表示例です)

Description

設定名を付けることができます。半角英数字のみ使用可能です。

Interface 名

キューイングをおこなうインターフェース名を入力します。本装置のインターフェース名については、本マニュアルの「付録 A インターフェース名について」をご参照ください。

Class ID

クラス ID を設定します。クラスの階層構造における <minor 番号> となります。

親 Class ID

親クラスの ID を指定します。クラスの階層構造における <major 番号> となります。

Rate 設定

クラスの帯域幅を設定します。設定は kbit/s 単位となります。

Class 内 Average Packet Size 設定

クラス内のパケットの平均サイズを指定します。設定はバイト単位となります。

Maximum Burst 設定

一度に送信できる最大パケット数を指定します。

bounded 設定

「有効」を選択すると、兄弟クラスから余っている帯域幅を借りようとはしなくなります (Rate 設定値を超えて通信しません)。

「無効」を選択すると、その逆の動作となります。

Filter 設定

CLASS 分けフィルタの設定番号を指定します。ここで指定したフィルタにマッチングしたパケットが、このクラスに送られてきます。

設定後は「設定」ボタンをクリックします。

IV. 各設定画面での設定方法について

「CLASS Queueing 設定」

設定を追加するときは「New Entry」をクリックします。

Description	<input type="text"/>
Interface名	eth0
QDISC番号	<input type="text"/>
MAJOR ID	1
class ID	<input type="text"/>
Queueing Discipline	---
pfifo limit (PFIFO選択時有効)	<input type="text"/>
TBF Parameter設定	
制限Rate	<input type="text"/> Kbit/s
Buffer Size	<input type="text"/> byte
Limit Byte (tokenが利用できるようになるまで queueing可能なbyte数)	<input type="text"/>
PQ Parameter設定	
最大Band数設定	3 default 3 (2-5)
priority-map設定	1 2 2 2 1 2 0
Marking Filterの選択 (PacketヘッダによるFilter設定は選択できません)	FilterNo. Class No.
	1. <input type="text"/> <input type="text"/>
	2. <input type="text"/> <input type="text"/>
	3. <input type="text"/> <input type="text"/>
	4. <input type="text"/> <input type="text"/>
	5. <input type="text"/> <input type="text"/>
	6. <input type="text"/> <input type="text"/>
	7. <input type="text"/> <input type="text"/>
	8. <input type="text"/> <input type="text"/>
	9. <input type="text"/> <input type="text"/>
10. <input type="text"/> <input type="text"/>	

(画面は表示例です)

Description

設定名を付けることができます。半角英数字のみ使用可能です。

Interface名

キューイングをおこなうインターフェース名を選択します。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名について」をご参照ください。

QDISC 番号

このクラスが属しているQDISC番号を指定します。

MAJOR ID

親のクラスIDを指定します。クラスの階層構造における <major 番号> となります。

Class ID

自身のクラスIDを指定します。クラスの階層構造における <minor 番号> となります。

Queueing Discipline 以下は、Interface Queueing 設定と同様に設定します。

IV. 各設定画面での設定方法について

「CLASS分けフィルタ設定」

設定を追加するときには「New Entry」をクリックします。

設定番号	1
Description	host_1
Priority	1 (1-999)
<input checked="" type="checkbox"/> パケットヘッダ情報によるフィルタ	
プロトコル	6 (Protocol番号)
送信元アドレス	192.168.0.1/32
送信元ポート	(ポート番号)
宛先アドレス	10.10.10.10/32
宛先ポート	80 (ポート番号)
TOS値	02 (hex0-fe)
<input type="checkbox"/> Marking情報によるフィルタ	
Mark値	100 (1-999)

(画面は表示例です)

Description

設定名を付けることができます。半角英数字のみ使用可能です。

Priority

複数のCLASS分けフィルタ間での優先度を設定します。値が小さいものほど優先度が高くなります。

パケットヘッダによるフィルタ

パケットヘッダ情報でCLASS分けをおこなうときにチェックします。以下、マッチ条件を設定していきます。ただしPQをおこなうときは、パケットヘッダによるフィルタはできません。

プロトコル

プロトコルを指定します。プロトコル番号で指定してください。

送信元アドレス

送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。範囲での指定はできません。

送信元ポート

対象とする送信元ポート番号を指定します。範囲での指定はできません。

宛先アドレス

宛先 IP アドレスを指定します。指定方法は送信元 IP アドレスと同様です。

宛先ポート

対象とする宛先ポート番号を指定します。範囲での指定はできません。

TOS 値

TOS 値を指定します。16進数で指定します。

Marking情報によるフィルタ

MARK 値によってCLASS分けをおこなうときにチェックします。以下、「Mark 値」欄にマッチ条件となるMark 値を指定します。PQでフィルタをおこなうときはMarking情報によるもののみ有効です。

設定後は「設定」ボタンをクリックします。

第27章 QoS機能

IV. 各設定画面での設定方法について

「パケット分類設定」

設定を追加するときは「New Entry」をクリックします。

XR-410L2

設定番号	1	
パケット分類条件		
プロトコル	6 (Protocol番号)	<input type="checkbox"/> Not条件
送信元アドレス	192.168.0.1/32	<input type="checkbox"/> Not条件
送信元ポート	1024:65535 (ポート番号/範囲指定で番号連結)	<input type="checkbox"/> Not条件
宛先アドレス	10.10.10.10/32	<input type="checkbox"/> Not条件
宛先ポート	80 (ポート番号/範囲指定まで番号連結)	<input type="checkbox"/> Not条件
インターフェース	eth1	<input type="checkbox"/> Not条件
TOS/DSCP値	<input checked="" type="radio"/> TOS <input type="radio"/> DSCP <input type="radio"/> マッチ条件無効 8 上記で選択したマッチ条件に対応する設定値	TOS Bit値 hex 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay DSCP Bit値 hex(0-3f)
TOS/DSCP値の設定		
設定対象	<input checked="" type="radio"/> TOS/Precedence <input type="radio"/> DSCP	
設定値	・TOS/Precedence設定 選択して下さい TOS Bit 選択して下さい Precedence Bit ・DSCP設定 選択して下さい DSCP Bit	

XR-640L2

設定番号	1	
パケット分類条件		
プロトコル	6 (Protocol番号)	<input type="checkbox"/> Not条件
送信元アドレス	192.168.1.1/32	<input type="checkbox"/> Not条件
送信元ポート	1024:65535 (ポート番号/範囲指定で番号連結)	<input type="checkbox"/> Not条件
宛先アドレス	10.10.10.10/32	<input type="checkbox"/> Not条件
宛先ポート	80 (ポート番号/範囲指定まで番号連結)	<input type="checkbox"/> Not条件
インターフェース	eth1	<input type="checkbox"/> Not条件
TOS/MARK/DSCP値	<input checked="" type="radio"/> TOS <input type="radio"/> MARK <input type="radio"/> DSCP <input type="radio"/> マッチ条件無効 8 上記で選択したマッチ条件に対応する設定値	TOS Bit値 hex 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay MARK値 (1-999) DSCP Bit値 hex(0-3f)
TOS/MARK/DSCP値の設定		
設定対象	<input checked="" type="radio"/> TOS/Precedence <input type="radio"/> MARK <input type="radio"/> DSCP	
設定値	・MARK設定 (1-999) [] ・TOS/Precedence設定 Minimize cost(1) TOS Bit Internetwork Control(6) Precedence Bit ・DSCP設定 BE(0x0) DSCP Bit	

[パケット分類条件]

パケット選別のマッチ条件を定義します。

プロトコル

プロトコルを指定します。プロトコル番号で指定してください。

送信元アドレス

送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。範囲での指定はできません。

送信元ポート

送信元ポート番号を指定します。範囲で指定するときは、**始点ポート：終点ポート**の形式で指定します。

宛先アドレス

宛先 IP アドレスを指定します。指定方法は送信元 IP アドレスと同様です。

宛先ポート

宛先ポート番号を指定します。指定方法は送信元ポートと同様です。

インターフェース

インターフェース名を入力します。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名について」をご参照ください。

各項目について「Not 条件」にチェックを付けると、**その項目で指定した値以外のものがマッチ条件**となります。

IV. 各設定画面での設定方法について

TOS/MARK/DSCP 値 (MASK 値は XR-640L2 のみ)

マッチングする TOS/MARK/DSCP 値を指定します。

TOS、MARK または DSCP のいずれかを選択し、その値を指定します。これらをマッチ条件としないときは「マッチ条件無効」を選択します。

[TOS/MARK/DSCP 値]

パケット分類条件で選別したパケットに、あらたに TOS 値、MARK 値または DSCP 値を設定します。

設定対象

TOS/Precedence、MARK (XR-640L2 のみ) または DSCP を選択します。

設定値

設定対象で選択したものについて、設定値を指定します。

設定後は「設定」ボタンをクリックします。

TOS/Precedence については巻末をご参照ください。

V. ステータスの表示

「ステータス表示」をクリックすると、以下の画面に移ります。

Queueing Discipline ステータス表示	<input type="button" value="表示する"/>
CLASS設定 ステータス表示	<input type="button" value="表示する"/>
CLASS分けルール ステータス表示	<input type="button" value="表示する"/>
各インターフェースの上記ステータスをすべて表示	<input type="button" value="表示する"/>
Packet分類設定ステータス表示	<input type="button" value="表示する"/>
Interfaceの指定	<input type="text" value="eth0"/>

QoS機能の各種ステータスを表示します。

「Packet 分類設定ステータス表示」以外では、必ず Interface 名を「Interfaceの指定」に入力してから「表示する」ボタンをクリックしてください。

VI. 設定の編集・削除方法

設定をおこなうと、設定内容が一覧で表示されます。

	FilterType	Description	Priority	プロトコル	送信元アドレス	送信元ポート	宛先アドレス	宛先ポート	TOS値	MARK値	Configure
1	Mark		1							1	Edit,Remove
2	Mark		2							2	Edit,Remove
3	Mark		3							3	Edit,Remove

(「クラス分けフィルタ設定」画面の表示例)

Configureの「Edit」をクリックすると設定画面に遷移し、その設定を修正できます。

「Remove」をクリックすると、その設定が削除されます。

VII. ステータス情報の表示例

[Queueing 設定情報]表示例

各クラスで設定したキューイング方式や設定パラメータの他、送信したパケット数・送信データサイズ等の情報を表示します。

```
qdisc pfifo 1: limit 300p
Sent 9386 bytes 82 pkts (dropped 0, overlimits 0)
```

qdisc -> キューイング方式
 1: -> キューイングを設定しているクラス ID
 limit -> キューイングできる最大パケット数
 Sent (nnn) byte (mmm)pkts -> 送信したデータ量とパケット数
 dropped -> 破棄したパケット数
 overlimits -> 過負荷の状態が届いたパケット数

```
qdisc sfq 20: limit 128p quantum 1500b flows 128/1024 perturb 10sec
Sent 140878 bytes 206 pkts (dropped 0, overlimits 0)
```

limit (nnn)p -> キューに待機できるパケット数
 quantum -> パケットのサイズ
 flows (nnn)/(mmm) -> mmm 個のバケツが用意され、同時にアクティブになるのは nnn 個まで
 perturb (n)sec -> ハッシュの更新間隔

```
qdisc tbf 1: rate 500Kbit burst 1499b/8 mpu 0b lat 4295.0s
Sent 73050 bytes 568 pkts (dropped 2, overlimits 17)
```

rate -> 設定している帯域幅
 burst -> バケツのサイズ
 mpu -> 最小パケットサイズ
 lat -> パケットが tbf に留まっていられる時間

```
qdisc cbq 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8 weight
1000Kbit allot 1514b
```

```
level 2 ewma 5 avpkt 1000b maxidle 242us
Sent 2420755 bytes 3945 pkts (dropped 0, overlimits 0)
borrowed 0 overactions 0 avgidle 6399 undertime 0
```

bounded,isolated -> bounded,isolated 設定がされている
 (bounded は帯域を借りない、isolated は帯域を貸さない)
 prio -> 優先度(上記では root クラスなので、prio 値はありません)
 weight -> ラウンドロビンプロセスの重み
 allot -> 送信できるデータサイズ
 ewma -> 指数重み付け移動平均
 avpkt -> 平均パケットサイズ
 maxidle -> パケット送信時の最大アイドル時間
 borrowed -> 帯域幅を借りて送信したパケット数
 avgidle -> EMMA で測定した値から、計算したアイドル時間を差し引いた数値。通常は数字が
 カウントされていますが、負荷で一杯の接続の状態では "0"、過負荷の状態では
 マイナスの値になります

VII. ステータス情報の表示例

[CLASS 設定情報]表示例

設定している各クラスの情報を表示します。

その 1(CBQ での表示例)

```
class cbq 1: root rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8
weight 1000Kbit allot 1514b
level 2 ewma 5 avpkt 1000b maxidle 242us
  Sent 33382 bytes 108 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 6399 undertime 0
class cbq 1:10 parent 1:1 rate 500Kbit cell 8b mpu 64b prio 1/1 weight 50Kbit allot 1500b
level 0 ewma 5 avpkt 1000b maxidle 6928us offtime 15876us
  Sent 0 bytes 0 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 181651 undertime 0
class cbq 1:1 parent 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio 3/3 weight
100Kbit allot 1500b
level 1 ewma 5 avpkt 1000b maxidle 242us
  Sent 2388712 bytes 3843 pkts (dropped 0, overlimits 0)
  borrowed 2004 overactions 0 avgidle 6399 undertime 0
class cbq 1:20 parent 1:1 leaf 20: rate 500Kbit cell 8b mpu 64b (bounded) prio 2/2 weight
50Kbit allot 1500b
level 0 ewma 5 avpkt 1000b maxidle 6928us offtime 15876us
  Sent 142217 bytes 212 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 174789 undertime 0
```

parent -> 親クラス ID

その 2(PQ での表示例)

```
class prio 1: parent 1: leaf 1001:
class prio 1: parent 1: leaf 1002:
class prio 1: parent 1: leaf 1003:
```

prio -> 優先度

parent -> 親クラス ID

leaf -> leaf クラス ID

VII. ステータス情報の表示例

[CLASS分けフィルタ設定情報]表示例

クラス分けフィルタの設定情報を表示します。

その 1 (CBQ での表示例)

```
[ PARENT 1: ]
filter protocol ip pref 1 u32
filter protocol ip pref 1 u32 fh 805: ht divisor 1
filter protocol ip pref 1 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 1 u32 fh 804: ht divisor 1
filter protocol ip pref 1 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32
filter protocol ip pref 3 u32 fh 805: ht divisor 1
filter protocol ip pref 3 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32 fh 804: ht divisor 1
filter protocol ip pref 3 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
```

protocol -> マッチするプロトコル

pref -> 優先度

u32 -> パケット内部のフィールド (発信元 IP アドレスなど) に基づいて処理すべきクラスの決定を行います

at 8、at16 -> マッチの開始は、指定した数値分のオフセットからであることを示します。
at 8であれば、ヘッダの9バイトめからマッチします。

flowid -> マッチしたパケットを送るクラス

その 2 (PQ での表示例)

```
[ PARENT 1: ]
filter protocol ip pref 1 fw
filter protocol ip pref 1 fw handle 0x1 classid 1:3
filter protocol ip pref 2 fw
filter protocol ip pref 2 fw handle 0x2 classid 1:2
filter protocol ip pref 3 fw
filter protocol ip pref 3 fw handle 0x3 classid 1:1
```

pref -> 優先度

handle -> MARK 値

classid -> マッチパケットを送るクラス ID

VII. ステータス情報の表示例

[Packet 分類設定情報]表示例

パケット分類設定の情報を表示します。

```
pkts bytes target  prot opt in   out  source          destination      MARK set
272 39111 MARK    all  -- eth0 any  192.168.120.111 anywhere        MARK set 0x1
 83  5439 MARK    all  -- eth0 any  192.168.120.113 anywhere        MARK set 0x2
447 48695 MARK    all  -- eth0 any  192.168.0.0/24  anywhere        MARK set 0x3
 0    0 FTOS    tcp  -- eth0 any  192.168.0.1    111.111.111.111 tcp spts:1024:
65535 dpt:450 Type of Service set 0x62
```

pkts -> 入力(出力)されたパケット数

bytes -> 入力(出力)されたバイト数

target -> 分類の対象(MARK か TOS か)

prot -> プロトコル

in -> パケット入力インターフェース

out -> パケット出力インターフェース

source -> 送信元 IP アドレス

destination -> あて先 IP アドレス

MARK set -> セットする MARK 値

spts -> 送信元ポート番号

dpt -> あて先ポート番号

Type of Service set -> セットする TOS ビット値

VIII. クラスの階層構造について

CBQにおけるクラスの階層構造は以下のようになります。

root クラス

ネットワークデバイス上のキューイングです。本装置のシステムが直接的に対話するのはこのクラスです。

親クラス

すべてのクラスのベースとなるクラスです。帯域幅を 100%として定義します。

子クラス

親クラスから分岐するクラスです。親クラスの持つ帯域幅を分割して、それぞれの子クラスの帯域幅として持ちます。

leaf (葉)クラス

leaf クラスは自分から分岐するクラスがないクラスです。

qdisc

キューイングです。ここでキューを管理・制御します。

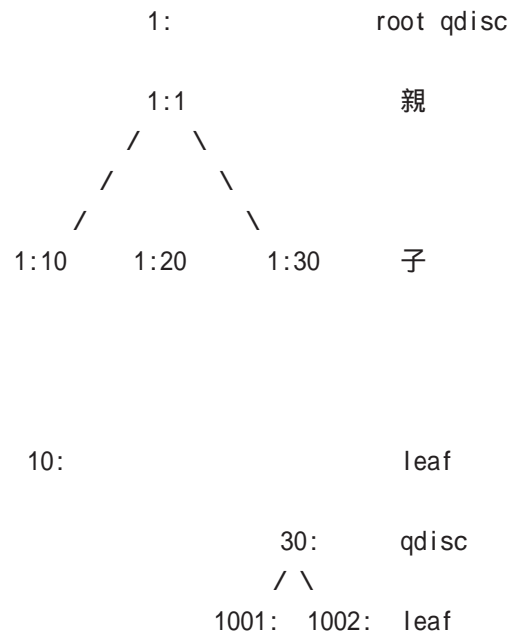
[クラス ID について]

各クラスはクラス ID を持ちます。クラス ID は MAJOR 番号と MINOR 番号の 2 つからなります。表記は以下のようになります。

<MAJOR 番号> : <MINOR 番号>

- ・ root クラスは「1:0」というクラス ID を持ちます。
- ・ 子クラスは、親と同じ MAJOR 番号を持つ必要があります。
- ・ MINOR 番号は、他のクラスと qdisc 内で重複しないように定義する必要があります。

<クラス構成図(例)>



IX. TOS について

IP パケットヘッダには TOS フィールドが設けられています。ここにパケットの優先度情報を付与しておくことで、優先度にあわせて機器がパケットを適切に扱えることを期待します。

IP ヘッダ内の TOS フィールドの各ビットは、以下のように定義されています。<表 1>

バイナリ 10進数 意味

バイナリ	10進数	意味
1000	8	Minimize delay (md)
0100	4	Maximize throughput (mt)
0010	2	Maximize reliability (mr)
0001	1	Minimize monetary cost (mmc)
0000	0	Normal Service

md は最小の遅延、mt は最高のスループット、mr は高い信頼性、mmc は低い通信コスト、を期待するパケットであることを示します。

各ビットの組み合わせによる TOS 値は以下のように定義されます。<表 2>

TOS	ビット	意味	Linux での扱い	バンド
0x0	0	Normal Service	0 Best Effort	1
0x2	1	Minimize Monetary Cost	1 Filler	2
0x4	2	Maximize Reliability	0 Best Effort	1
0x6	3	mmc+mr	0 Best Effort	1
0x8	4	Maximize Throughput	2 Bulk	2
0xa	5	mmc+mt	2 Bulk	2
0xc	6	mr+mt	2 Bulk	2
0xe	7	mmc+mr+mt	2 Bulk	2
0x10	8	Minimize Delay	6 Interactive	0
0x12	9	mmc+md	6 Interactive	0
0x14	10	mr+md	6 Interactive	0
0x16	11	mmc+mr+md	6 Interactive	0
0x18	12	mt+md	4 Int. Bulk	1
0x1a	13	mmc+mt+md	4 Int. Bulk	1
0x1c	14	mr+mt+md	4 Int. Bulk	1
0x1e	15	mmc+mr+mt+md	4 Int. Bulk	1

バンドは優先度です。0 が最も優先度が高いものです。初期値ではバンド数は 3(優先度は 3 段階)です。本装置では、PQ Parameter 設定の「最大 Band 数設定」でバンド数を変更できます(0 ~ 4)。

Linux での扱いの数値は、Linux での TOS ビット列の解釈です。これは PQ Parameter 設定の「Priority-map 設定」の箱にリンクしており、対応する Priority-map の箱に送られます。

IX. TOS について

またアプリケーションごとのパケットの取り扱い方法も定義されています(RFC1349)。アプリケーションのTOS値は以下のようになっています。<表3>

アプリケーション	TOSビット値	定義
TELNET	1000	(minimize delay)
FTP		
Control	1000	(minimize delay)
Data	0100	(maximize throughput)
TFTP	1000	(minimize delay)
SMTp		
Command phase	1000	(minimize delay)
DATA phase	0100	(maximize throughput)
Domain Name Service		
UDP Query	1000	(minimize delay)
TCP Query	0000	
Zone Transfer	0100	(maximize throughput)
NNTP	0001	(minimize monetary cost)
ICMP		
Errors	0000	
Requests	0000 (mostly)	
Responses	<same as request>	(mostly)

表中のTOSビット値(2進数表記)が、<表2>のビットに対応しています。

TOS値は定義があいまいで相互運用できない、正しい値が設定されている保証がない、悪用される可能性があるなどの要因により、現在までほとんど使われていません。

第 28 章

ゲートウェイ認証機能

第28章 ゲートウェイ認証機能

1. ゲートウェイ認証機能の設定

「ゲートウェイ認証機能」は、本装置を経由して外部にアクセスをする場合に、本装置での認証を必要とする機能です。

この機能を使うことで、外部へアクセスできるユーザーを管理できるようになります。

基本設定

[基本設定]

基本設定		
本機能	<input checked="" type="radio"/> 使用しない	<input type="radio"/> 使用する
認証	<input type="radio"/> しない (URL転送のみ)	<input checked="" type="radio"/> する
80/tcp 監視	<input checked="" type="radio"/> 行わない	<input type="radio"/> 行う

本機能

ゲートウェイ認証機能を使う場合は「使用する」を選択します。

認証

当機能を使用していて、かつ認証をおこなうときは「する」を選択します(初期設定)。認証を行わないときは「しない」を選択します。このときは、外部へのアクセスをリダイレクトするだけの動作となります。

80/tcp 監視

認証を受けていないIPアドレスからのTCPポート80番のコネクションを監視し、**このコネクションがあったときに、強制的にゲートウェイ認証をおこないます。**

初期設定は監視を「行わない」設定となります。

[URL 転送]

URL転送		
URL	<input type="text"/>	
通常認証後	<input checked="" type="radio"/> 行わない (デフォルト)	<input type="radio"/> 行う
強制認証後	<input checked="" type="radio"/> 行わない (エンドユーザ要求URL)	<input type="radio"/> 行う

URL

転送先のURLを設定します。

通常認証後

「行う」を選択すると、ゲートウェイ認証後に「URL」で指定したサイトに転送させることができます。初期設定ではURL転送を行いません。

強制認証後

「行う」を選択すると、強制認証後に「URL」で指定したサイトに転送させることができます。初期設定ではURL転送を行いません。この機能を使う場合は「80/tcp 監視」を有効にしてください。

[認証方法]

認証方法	
<input checked="" type="radio"/> ローカル	<input type="radio"/> RADIUSサーバ

認証方法

「ローカル」本装置でアカウントを管理 / 認証します。

「RADIUSサーバ」外部のRADIUSサーバでアカウントを管理 / 認証します。

第28章 ゲートウェイ認証機能

1. ゲートウェイ認証機能の設定

[接続許可時間]

接続許可時間	
<input checked="" type="radio"/> アイドルタイムアウト	30 分 (1~43200)
<input type="radio"/> セッションタイムアウト	分 (1~43200)
<input type="radio"/> 認証を受けたWebブラウザのウィンドウを閉じるまで	

接続許可時間

認証したあとの、ユーザーの接続形態を選択できます。

「アイドルタイムアウト」

認証で許可された通信が無通信状態となってから切断するまでの時間を設定します。

「セッションタイムアウト」

認証で許可された通信を強制的に切断するまでの時間を設定します。認証してからこの時間が経過すると、通信状態にかかわらず通信を切断します。

「認証を受けたWebブラウザのウィンドウを閉じるまで」

認証を受けた後にブラウザに表示された画面を閉じたときに、通信を切断します。通信可能な状態を保つには、認証後の画面を開いたままにしなければなりません。webブラウジングをする場合は、別のブラウザを開く必要があります。

上記設定にしたがって通信が切断した場合は、各ユーザーは再度ゲートウェイ認証を実行する必要があります。

最後に「設定変更」をクリックしてください。

ゲートウェイ認証機能を「使用する」にした場合はただちに機能が有効となりますので、ユーザー設定等から設定をおこなってください。

ユーザー設定

No.	ユーザID	パスワード	削除
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

ユーザー ID・パスワード

ユーザーアカウントを登録します。

ユーザー ID・パスワードには半角英数字が使用できます。空白やコロン(:)は含めることができません。

「削除」をチェックすると、その設定が削除対象となります。

最後に「設定 / 削除の実行」をクリックしてください。

1. ゲートウェイ認証機能の設定

RADIUS 設定

「基本設定」において、認証方法を「RADIUS サーバ」に選択した場合にのみ設定します。

プライマリサーバ設定	
IPアドレス	<input type="text"/>
ポート番号	<input checked="" type="radio"/> 1645 <input type="radio"/> 1812 <input type="radio"/> 手動設定 <input type="text"/>
secret	<input type="text"/>
セカンダリサーバ設定	
IPアドレス	<input type="text"/>
ポート番号	<input checked="" type="radio"/> 1645 <input type="radio"/> 1812 <input type="radio"/> 手動設定 <input type="text"/>
secret	<input type="text"/>
サーバ共通設定	
NAS-IP-Address	<input type="text"/>
NAS-Identifier	<input type="text"/>
接続許可時間 (RADIUSサーバから送信されるアトリビュートの指定)	
アイドルタイムアウト	<input type="text" value="指定しない"/>
セッションタイムアウト	<input type="text" value="指定しない"/>

プライマリ / セカンダリサーバ設定

RADIUSサーバのIPアドレス、ポート番号、secretを設定します。プライマリ項目の設定は必須です。セカンダリ項目の設定はなくてもかまいません。

サーバ共通設定

RADIUSサーバへ問い合わせをする際に送信するNASの情報を設定します。RADIUSサーバが、どのNASかを識別するために使います。どちらかの設定が必須です。

”NAS-IP-Address”はIPアドレスです。通常は本装置のIPアドレスを設定します。

”NAS-Identifier”は任意の文字列を設定します。半角英数字が使用できます。

アイドルタイムアウト

セッションタイムアウト

RADIUSサーバからの認証応答に該当のアトリビュートがあればその値を使います。該当のアトリビュートがなければ「基本設定」で設定した値を使用します。それぞれ、基本設定で選択されているものが有効となります。

Idle-Timeout : アイドルタイムアウト

Ascend-Maximum-Time : セッションタイムアウト

Ascend-Idle-Limit : アイドルタイムアウト

アトリビュートとは、RADIUSで設定されるパラメータのことを指します。

最後に「設定変更」をクリックしてください。

第28章 ゲートウェイ認証機能

1. ゲートウェイ認証機能の設定

フィルタ設定

ゲートウェイ認証機能を有効にすると外部との通信は認証が必要となりますが、フィルタ設定によって認証を必要とせずに通信可能にできます。特定のポートだけはつねに通信できるようにしたいといった場合に設定します。

設定画面「フィルタ設定」をクリックします。
「**フィルタ設定**」の**ゲートウェイ認証設定フィルタ設定画面**にて**設定してください。**というメッセージが表示されたらリンクをクリックしてフィルタ設定画面に移ります。

フィルタ設定 No.1~16まで
入力フィルタ 転送フィルタ 出力フィルタ **ゲートウェイ認証フィルタ**
情報表示

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート	LOG	削除	No.
1		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	1
2		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	2

ここで設定したIPアドレスやポートについては、ゲートウェイ認証機能によらず、通信可能になります(設定方法については第22章「パケットフィルタリング機能」をご参照ください)。

ログ設定

ゲートウェイ認証機能のログを本装置のシステムログに出力できます。

エラーログ 使用しない syslogに取る
アクセスログ 使用しない syslogに取る

ログを取得するかどうかを選択します。

- ・エラーログ : ゲートウェイ認証時のログインエラーを出力します。
- ・アクセスログ : ゲートウェイ認証時のアクセスログを出力します。

<エラーログの表示例>

```
Apr 7 17:04:45 localhost httpd[21529]:  
[error] [client 192.168.0.1] user abc: authentication failure for "/": password mismatch
```

<アクセスログの表示例>

```
Apr 7 17:04:49 localhost authgw: 192.168.0.1  
- abc [07/Apr/2003:17:04:49 +0900] "GET /  
HTTP/1.1" 200 353
```

11. ゲートウェイ認証下のアクセス方法

ホストからのアクセス方法

ホストから本装置にアクセスします。以下の形式でアドレスを指定してアクセスします。

`http://<本装置の IP アドレス>/login.cgi`

認証画面がポップアップしますので、通知されているユーザー ID とパスワードを入力します。

認証に成功すると以下のメッセージが表示され、本装置を経由して外部にアクセスできるようになります。

<認証成功時の表示例>

You can connect to the External Network
(abc@192.168.0.1).

Date: Mon Apr 7 10:06:51 2003

設定画面へのアクセスについて

ゲートウェイ認証機能を使用していて認証をおこなっていない場合でも、本装置の設定画面にはアクセスすることができます。アクセス方法は、通常と同じです。

RADIUS 設定について

認証方法を「RADIUS サーバ」に選択した場合、本装置は RADIUS サーバに対して認証要求のみを送信します。

RADIUS サーバへの要求はタイムアウトが 5 秒、リトライが最大 3 回です。プライマリサーバから応答がない場合は、セカンダリサーバに要求を送信します。

認証について

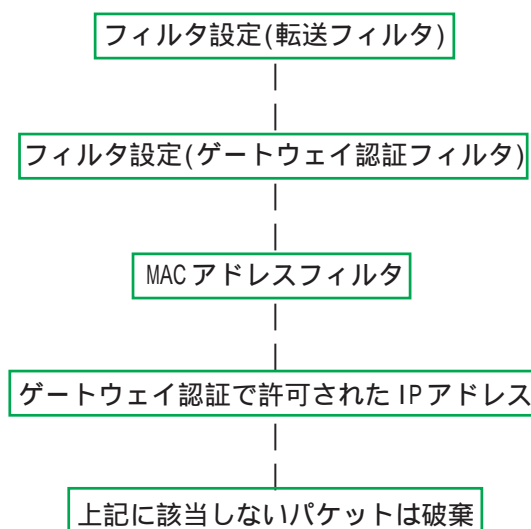
認証方法が「ローカル」、「RADIUS サーバ」のどちらの場合でも、クライアント - 本装置間の認証には、HTTP Basic 認証が用いられます。

また、「RADIUS サーバ」を使用する場合、本装置 - RADIUS サーバ間は User-Password を用いた認証 (PAP) が行われます。

III. ゲートウェイ認証の制御方法について

ゲートウェイ認証機能はパケットフィルタの一種で、認証で許可されたユーザー(ホスト)のIPアドレスを送信元/あて先に持つ転送パケットのみを通過させます。制御は、転送フィルタ設定の最後でおこなわれます。

フィルタリング制御の順番は以下の通りです。



ゲートウェイ認証機能を使わない場合は、通常の「転送フィルタ」のみ有効となります。

「転送フィルタ」に設定をしてしまうと、ゲートウェイ認証よりも優先してそのフィルタが参照されてしまい、ゲートウェイ認証が有効に機能しなくなる恐れがあります。

ゲートウェイ認証機能を使用する場合は、「転送フィルタ」には何も設定せずに運用してください。

第 29 章

ネットワークテスト

第29章 ネットワークテスト

ネットワークテスト

本装置の運用時において、ネットワークテストをおこなうことができます。ネットワークのトラブルシューティングに有効です。以下の3つのテストができます。

- pingテスト
- tracerouteテスト
- パケットダンプの取得

実行方法

Web 設定画面「ネットワークテスト」をクリックして、以下の画面でテストを実行します。

XR-410L2

Ping	<p>FQDNまたはIPアドレス <input type="text"/></p> <p>インターフェースの指定(省略可)</p> <p><input type="radio"/> 主回線 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input type="radio"/> Ether0 <input type="radio"/> Ether1 <input checked="" type="radio"/> その他 <input type="text"/></p> <p><input type="button" value="実行"/></p>
Trace Route	<p>FQDNまたはIPアドレス <input type="text"/></p> <p><input type="button" value="実行"/></p>
パケットダンプ	<p><input checked="" type="radio"/> 主回線 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> その他 <input type="text"/></p> <p><input type="button" value="実行"/> <input type="button" value="結果表示"/></p>
PacketDump TypePcap	<p>Device <input type="text"/> CapCount <input type="text"/> CapSize <input type="text"/></p> <p>Dump Filter <input type="text"/></p> <p>生成ファイルの最大サイズは圧縮後で約4Mbyteです 高帯域下での使用によりパケットロスを生じる場合があります</p> <p><input type="button" value="実行"/> <input type="button" value="結果表示"/></p>

XR-640L2

Ping	<p>FQDNまたはIPアドレス <input type="text"/></p> <p>インターフェースの指定(省略可)</p> <p><input type="radio"/> 主回線 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input checked="" type="radio"/> その他 <input type="text"/></p> <p><input type="button" value="実行"/></p>
Trace Route	<p>FQDNまたはIPアドレス <input type="text"/></p> <p><input type="button" value="実行"/></p>
パケットダンプ	<p><input checked="" type="radio"/> 主回線 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> その他 <input type="text"/></p> <p><input type="button" value="実行"/> <input type="button" value="結果表示"/></p>
PacketDump TypePcap	<p>Device <input type="text"/> CapCount <input type="text"/> CapSize <input type="text"/></p> <p>Dump Filter <input type="text"/></p> <p>生成ファイルの最大サイズは圧縮後で約4Mbyteです 高帯域下での使用によりパケットロスを生じる場合があります</p> <p><input type="button" value="実行"/> <input type="button" value="結果表示"/></p>

第29章 ネットワークテスト

ネットワークテスト

pingテスト

指定した相手に本装置からPingを発信します。FQDN (www.xxx.co.jpなどのドメイン名) もしくはIPアドレスを入力して「実行」をクリックします。またpingを送出するインターフェースを指定することもできます(省略可)。

実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=49.5 ms
64 bytes from 211.14.13.66: icmp_seq=1 ttl=52 time=65.7 ms
64 bytes from 211.14.13.66: icmp_seq=2 ttl=52 time=11.7 ms
64 bytes from 211.14.13.66: icmp_seq=3 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=4 ttl=52 time=69.0 ms
64 bytes from 211.14.13.66: icmp_seq=5 ttl=52 time=58.3 ms
64 bytes from 211.14.13.66: icmp_seq=6 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=7 ttl=52 time=71.4 ms
64 bytes from 211.14.13.66: icmp_seq=8 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=9 ttl=52 time=11.8 ms

--- 211.14.13.66 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 11.7/37.3/71.4 ms
```

tracerouteテスト

指定した宛先までに経由するルータの情報を表示します。pingと同様にFQDNもしくはIPアドレスを入力して「実行」をクリックします。

実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=12.4 ms

--- 211.14.13.66 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.4/12.4/12.4 ms
traceroute to 211.14.13.66 (211.14.13.66), 30 hops max, 40 byte packets
 1 192.168.120.15 (192.168.120.15) 1.545 ms 2.258 ms 1.607 ms
 2 192.168.100.50 (192.168.100.50) 2.210 ms 4.955 ms 2.309 ms
 3 172.17.254.1 (172.17.254.1) 8.777 ms 21.189 ms 13.946 ms
 4 210.135.192.108 (210.135.192.108) 9.205 ms 8.953 ms 9.310 ms
 5 210.135.208.34 (210.135.208.34) 35.538 ms 19.923 ms 14.744 ms
 6 210.135.208.10 (210.135.208.10) 41.641 ms 40.476 ms 63.293 ms
 7 210.171.224.115 (210.171.224.115) 43.948 ms 27.255 ms 36.767 ms
 8 211.14.3.233 (211.14.3.233) 36.861 ms 33.890 ms 37.679 ms
 9 211.14.3.148 (211.14.3.148) 36.865 ms 47.151 ms 18.491 ms
10 211.14.3.105 (211.14.3.105) 53.573 ms 13.889 ms 50.057 ms
11 211.14.2.193 (211.14.2.193) 33.777 ms 11.380 ms 17.282 ms
12 * * *
13 211.14.12.249 (211.14.12.249) 19.692 ms !X * 15.213 ms !X
```

ping・tracerouteテストで応答メッセージが表示されない場合は、DNSで名前解決ができていない可能性があります。その場合はまず、IPアドレスを直接指定してご確認ください。

パケットダンプ

パケットのダンプを取得できます。ダンプを取得したいインターフェースを選択して「実行」をクリックします。その後、「結果表示」をクリックすると、ダンプ内容が表示されます。

実行結果例

実行結果

```
19:08:26.587225 192.168.120.111.4937 > 192.168.120.118.880: [Etop sum ok] 207161989:207161989(0) sok.168562927 win 16550 (DF) (ttl 128, id 8212, len 40)
19:08:26.759367 192.168.120.118.1079 > 201.168.120.129.53: [Etop sum ok] 74: 74 www.velox.jp [Etop sum ok] 1422298:1422298(0) sok.1422298 win 3250 (DF) (ttl 110, id 65023, len 69)
19:08:32.774688 203.140.123.3.53 > 192.168.254.1.1073: 74: 74 www.velox.jp [Etop sum ok] 1422298:1422298(0) sok.1422298 win 3250 (DF) (ttl 246, id 25223, len 108)
19:08:32.780338 192.168.120.118.1074 > 210.173.173.17.80: S [Etop sum ok] 1422298:1422298(0) sok.1422298 win 3250 (DF) (ttl 121, id 65049, len 48)
19:08:32.784830 210.173.173.17.80 > 192.168.254.1.1074: S [Etop sum ok] 207110954:207110954(0) sok.1422298 win 3250 (DF) (ttl 110, id 25347, len 40)
19:08:32.796099 192.168.120.118.1074 > 210.173.173.17.80: S [Etop sum ok] 1422299:1422299(0) sok.207110955 win 3250 (DF) (ttl 121, id 64001, len 40)
19:08:32.803535 192.168.120.118.1074 > 210.173.173.17.80: P 0:329329(0) sok.1 win 3250 (DF) (ttl 121, id 64257, len 368)
19:08:32.821350 210.173.173.17.80 > 192.168.254.1.1074: P 1:109110(0) sok.329 win 7952 (DF) (ttl 110, id 32259, len 148)
19:08:32.834442 210.173.173.17.80 > 192.168.254.1.1074: 109:1489(1380) sok.329 win 7952 (DF) (ttl 110, id 32315, len 1420)
19:08:32.836906 192.168.120.118.1074 > 210.173.173.17.80: 1489:298(1272) sok.329 win 7952 (DF) (ttl 110, id 32371, len 1212)
19:08:32.849487 210.173.173.17.80 > 192.168.254.1.1074: 298:414(1350) sok.329 win 7952 (DF) (ttl 110, id 42243, len 1420)
19:08:32.859512 210.173.173.17.80 > 192.168.254.1.1074: 592:1629(108) sok.329 win 7952 (DF) (ttl 110, id 42356, len 148)
19:08:32.868802 210.173.173.17.80 > 192.168.254.1.1074: 414:592(1350) sok.329 win 7952 (DF) (ttl 110, id 42429, len 1420)
19:08:32.884591 192.168.120.118.1074 > 210.173.173.17.80: 8 [Etop sum ok] 1422297:1422297(0) win 0 (DF) (ttl 121, id 795, len 40)
19:08:32.886197 192.168.120.118.1074 > 210.173.173.17.80: S [Etop sum ok] 329:329(0) sok.414 win 8280 (DF) (ttl 121, id 2, len 40)
19:08:32.893442 192.168.120.118.1074 > 210.173.173.17.80: S [Etop sum ok] 329:329(0) sok.414 win 8280 (DF) (ttl 121, id 254, len 40)
19:08:32.876961 210.173.173.17.80 > 192.168.254.1.1074: FP 5629:6294(495) sok.329 win 7952 (DF) (ttl 110, id 45059, len 509)
19:08:32.879442 192.168.120.118.1074 > 210.173.173.17.80: [Etop sum ok] 329:329(0) sok.6296 win 7616 (DF) (ttl 121, id 514, len 40)
19:08:32.886906 192.168.120.118.1074 > 210.173.173.17.80: 8 [Etop sum ok] 1422297:1422297(0) win 0 (DF) (ttl 121, id 795, len 40)
19:08:32.901492 192.168.120.118.1074 > 210.173.173.17.80: S [Etop sum ok] 1422450:1422450(0) win 8192 (DF) (ttl 121, id 1026, len 48)
19:08:32.904895 192.168.120.118.1074 > 210.173.173.17.80: S [Etop sum ok] 1422451:1422451(0) win 8192 (DF) (ttl 121, id 1534, len 48)
19:08:32.919673 210.173.173.17.80 > 192.168.254.1.1074: S [Etop sum ok] 1102297913:1102297913(0) sok.1422451 win 8280 (DF) (ttl 110, id 20733, len 44)
19:08:32.927212 192.168.120.118.1074 > 210.173.173.17.80: S [Etop sum ok] 1422451:1422451(0) sok.1102297914 win 8280 (DF) (ttl 121, id 1794, len 40)
19:08:32.962244 210.173.173.17.80 > 192.168.254.1.1074: S [Etop sum ok] 20711070:20711070(0) sok.1422451 win 8280 (DF) (ttl 110, id 12546, len 40)
19:08:32.962817 192.168.120.118.1074 > 210.173.173.17.80: [Etop sum ok] 1422453:1422453(0) sok.20711071 win 8280 (DF) (ttl 121, id 2050, len 40)
19:08:32.011934 192.168.120.118.1074 > 210.173.173.17.80: P 0:444644(0) sok.1 win 8280 (DF) (ttl 121, id 2098, len 444)
19:08:32.012222 192.168.120.118.1074 > 210.173.173.17.80: P 0:374(274) sok.1 win 8280 (DF) (ttl 121, id 2818, len 414)
19:08:32.023646 210.173.173.17.80 > 192.168.254.1.1074: P 1:168(160) sok.445 win 7950 (DF) (ttl 110, id 40045, len 200)
19:08:32.043097 192.168.120.118.1074 > 210.173.173.17.80: P 444:820(376) sok.194 win 8117 (DF) (ttl 121, id 3074, len 416)
19:08:32.042348 210.173.173.17.80 > 192.168.254.1.1074: P 1:252(251) sok.375 win 7906 (DF) (ttl 110, id 35583, len 291)
19:08:32.049797 210.173.173.17.80 > 192.168.254.1.1074: 252:1032(1380) sok.375 win 7906 (DF) (ttl 110, id 35544, len 1420)
19:08:32.050238 192.168.120.118.1074 > 210.173.173.17.80: [Etop sum ok] 374:374(0) sok.1632 win 8280 (DF) (ttl 121, id 35586, len 40)
19:08:32.064106 210.173.173.17.80 > 192.168.254.1.1074: P 164:414(250) sok.821 win 7460 (DF) (ttl 110, id 51309, len 230)
19:08:32.070964 210.173.173.17.80 > 192.168.254.1.1074: 414:1794(1380) sok.821 win 7460 (DF) (ttl 110, id 51595, len 1420)
19:08:32.072131 210.173.173.17.80 > 192.168.254.1.1074: 1794:3174(1380) sok.821 win 7460 (DF) (ttl 110, id 51511, len 1420)
19:08:32.079809 210.173.173.17.80 > 192.168.254.1.1074: 1032:3012(1380) sok.375 win 7906 (DF) (ttl 110, id 44548, len 1420)
19:08:32.078376 210.173.173.17.80 > 192.168.254.1.1074: 3012:4392(1380) sok.375 win 7906 (DF) (ttl 110, id 44504, len 1420)
19:08:32.077659 210.173.173.17.80 > 192.168.254.1.1074: 4392:5772(1380) sok.375 win 7906 (DF) (ttl 110, id 45009, len 1420)
19:08:32.077344 192.168.120.118.1074 > 210.173.173.17.80: [Etop sum ok] 820:820(0) sok.3174 win 8280 (DF) (ttl 121, id 3842, len 40)
19:08:32.099122 210.173.173.17.80 > 192.168.254.1.1074: 3174:4954(1380) sok.821 win 7460 (DF) (ttl 110, id 59173, len 1420)
19:08:32.100225 210.173.173.17.80 > 192.168.254.1.1074: 4954:5904(1380) sok.821 win 7460 (DF) (ttl 110, id 59159, len 1420)
19:08:32.101217 210.173.173.17.80 > 192.168.254.1.1074: P 5904:8814(884) sok.821 win 7460 (DF) (ttl 110, id 59985, len 224)
19:08:32.100897 192.168.120.118.1074 > 210.173.173.17.80: [Etop sum ok] 3174:3174(0) sok.3772 win 8280 (DF) (ttl 121, id 40294, len 40)
19:08:32.109581 192.168.120.118.1074 > 210.173.173.17.80: [Etop sum ok] 820:820(0) sok.5904 win 8280 (DF) (ttl 121, id 4554, len 40)
19:08:32.128899 210.173.173.17.80 > 192.168.254.1.1074: 5772:7152(1380) sok.375 win 7906 (DF) (ttl 110, id 64916, len 1420)
19:08:32.129851 210.173.173.17.80 > 192.168.254.1.1074: P 7152:8932(1380) sok.375 win 7906 (DF) (ttl 110, id 64972, len 1420)
19:08:32.131170 210.173.173.17.80 > 192.168.254.1.1074: 8932:9912(1380) sok.375 win 7906 (DF) (ttl 110, id 65023, len 1420)
```

「結果表示」をクリックするたびに、表示結果が更新されます。

パケットダンプの表示は、最大で100パケット分までです。100パケット分を超えると、古いものから順に表示されなくなります。

インターフェースについては「その他」を選択し、直接インターフェースを指定することもできます。その場合はインターフェース名を指定してください(「gre1」や「ipsec0」など)

ネットワークテスト

PacketDump TypePcap

拡張版パケットダンプ取得機能です。
指定したインターフェースで、指定した数のパケットダンプを取得できます。

「Device」: パケットダンプを実行する、本装置のインターフェース名を設定します。インターフェース名は「付録A インターフェース名について」をご参照ください。

「CapCount」: パケットダンプの取得数を指定します。1 ~ 99999 の間で指定します。

「CapSize」

1パケットごとのダンプデータの最大サイズを指定できます。単位は "byte" です。
たとえば 128 と設定すると、128 バイト以上の長さのパケットでも 128 バイト分だけをダンプします。

大きなサイズでダンプするときは、本装置への負荷が増加することがあります。また記録できるダンプ数も減少します。

「Dump Filter」

ここに条件式を記述することで、条件に合致したパケットについてのパケットダンプを取得することができます。条件式の記述方法の例を以下に記します。

(例) IP アドレスを指定して取得する

```
host 192.168.1.1
```

(例) ポート番号を指定して取得する

```
port 80
```

(例) 送信元ネットワークを指定して取得する

```
src net 192.168.1.0/24
```

(例) プロトコルを指定して取得する

```
tcp
```

条件式は、" or " " and " " not " といった論理条件も指定できます。

(例) 192.168.0.0/24 の外から中に入っているパケットを取得する

```
src net not 192.168.0.0/24 and dst net 192.168.0.0/24
```

複数の条件を指定したいときは上記のように、論理条件によって一連の条件式として設定してください。

条件式の記述方法が正しくない場合は、「tcpdump は異常終了しました。filter 等を確認してください」と表示され、パケットダンプが取得できません。DumpFilter の設定を見直してください。

上記項目を入力後、「実行」ボタンでパケットダンプを開始します。

パケットダンプを開始したときの画面表示

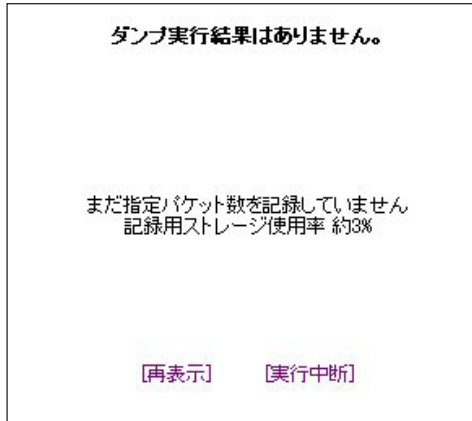
実行結果は即時出力できない場合があります。
[再表示]で確認して下さい

[再表示]

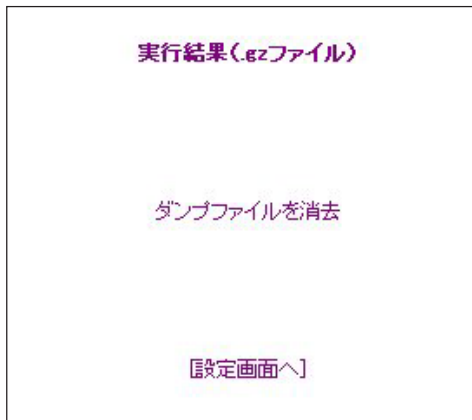
[実行中断]

ネットワークテスト

パケットダンプ結果を表示できないときの画面
パケットダンプ実行中に「再表示」ボタンをクリックすると、下記のような画面が表示されます。



パケットダンプが実行終了したときの画面
「Count」で指定した数のパケットダンプを取得したとき、「実行中断」ボタンをクリックしたとき、またはパケットダンプ取得終了後に「結果表示」をクリックしたとき、下記の画面が表示されます。



「実行結果(.gz ファイル)」リンクから、パケットダンプ結果を圧縮したファイルをローカルホストに保存してください。

ローカルホスト上で解凍してできたファイルは、Ethereal で閲覧することができます。

「ダンプファイルを消去」をクリックすると、本装置に記録されているダンプファイルを消去します。

[PacketDump TypePcapの注意点]

- ・取得したパケットダンプ結果は、libcap形式でgzip圧縮して保存されます。
- ・取得できるデータサイズは、gzip圧縮された状態で最大約1MBです。
- ・本装置上にはパケットダンプ結果を1つだけ記録しておけます。パケットダンプ結果を消去せずにPacketDump TypePcapを再実行して実行結果ファイルを作成したときは、それまでに記録されていたパケットダンプ結果に上書きされます。
- ・本装置のインターフェース名については「付録A インターフェース名について」をご参照ください。

第 30 章

簡易 CLI 機能
(XR-640L2 のみ)

第30章 簡易CLI機能 (XR-640L2のみ)

1. 簡易CLI機能の概要

本装置では、表示コマンドを中心とした簡易CLI (Command Line Interface)機能を実装しています。ブラウザベースのGUIに比べ、よりスピーディな運用監視が可能になります。

簡易CLIでは以下のようなコマンド群を実装しています。

- ・システム情報の表示
- ・インターフェース情報の表示
- ・システム内部情報の表示
- ・各種サービス情報の表示
- ・ステートフルパケットインスペクション情報の表示
- ・L2TPv3セッションの開始 / 停止
- ・L2TPv3カウンタ情報のクリア
- ・L2TPv3フィルタ情報の表示 / クリア
- ・テクニカルサポート機能(情報一括表示)

各コマンドの実行方法などの詳細については、別紙「CLIコマンドリファレンス」を参照してください。

CLIに関する設定

CLIを使用するための本装置へのアクセスはtelnetで行いますが、初期状態では全てのアクセスが禁止されています。CLIへアクセスするための設定は以下の画面から行います。

「システム設定」 「CLI設定」をクリックして設定画面を開きます。

CLI設定		
機能設定	ユーザ設定	ACL設定
本機能	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> telnet <input type="checkbox"/> ssh	
ホスト名	<input type="text" value="xr640l2"/>	
Enableパスワード	<input type="text"/>	

CLIへのアクセス設定は以下の手順で行います。

- 1)ユーザ設定
ユーザアカウントの作成
- 2)ACL設定
アクセスリストの設定
- 3)機能設定
CLI接続の受付開始

II. 簡易CLI機能のアクセス設定

1. ユーザアカウントの作成

まずCLIにアクセスするためのユーザアカウントを作成します。
アカウントは最大64アカウントまで設定可能です。

ユーザアカウントの作成は、「ユーザ設定」をクリックして、以下の設定画面から行います。

No.	ユーザ	パスワード	無効	削除
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

ユーザ

任意のユーザ名を設定してください。使用可能な文字は、半角英数字、"-"(ハイフン)、“_”(アンダースコア)、“.”(ピリオド)です。最大64文字まで入力可能です。

入力が終わりましたら「設定」をクリックして設定完了です。

パスワード

任意のパスワードを設定してください。使用可能な文字は、半角英数字、“-”(ハイフン)、“_”(アンダースコア)、“.”(ピリオド)です。最大64文字まで入力可能です。

無効

設定したアカウントを一時的に使用不可にしたい場合は、このボックスにチェックを入れてください。GUI上の設定は残りますが、このアカウントからのアクセスはできません。

II. 簡易CLI機能のアクセス設定

2. アクセスリストの設定

次にCLIへのアクセス可能なホスト、ネットワークを制限するために、アクセスリストを設定します。

アクセスリストが未設定の状態では全てのホストからの接続が可能になっています。必ずアクセスリストを設定してください。

アクセスリストの設定は、「ACL設定」をクリックして、以下の設定画面から行います。

No.	パーミッション	送信元アドレス	宛先アドレス	無効	削除
1	----	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	----	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	----	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

パーミッション

このリストエントリの条件にマッチしたアクセスに対して、許可(permit)または拒否(deny)を選択します。

送信元アドレス

アクセス元のホストアドレスまたはネットワークアドレスを指定します。

宛先アドレス

アクセス先(つまり本装置)のホストアドレスまたはネットワークアドレスを指定します。

送信元アドレス、宛先アドレスの指定はホストアドレス形式(xx.xx.xx.xx)、ネットワーク形式(xx.xx.xx.xx/yy)のいずれの形式でも可能です。

すべてのネットワークを指定する場合は、「0.0.0.0/0」と入力してください。

無効

設定したアクセスリストを一時的に無効にしたい場合は、このボックスにチェックを入れてください。GUI上の設定は残りますが、このアクセスリストは無効になります。

入力が終わりましたら「設定」をクリックして設定完了です。

アクセスリストの評価順について

CLIアクセス時のアクセス条件の比較は、アクセスリストの上から順に行われます。条件にマッチするアクセスリストが見つかった場合は、そのパーミッション動作に従ってアクセスの許可/拒否を決定し、以降のアクセスリストは評価されません。例えば、192.168.0.100のホストを除く192.168.0.0/24のネットワークからのアクセスを禁止したい場合は、以下の並びでアクセスリストを設定します。

No.	パーミッション	送信元アドレス	宛先アドレス
1	permit	192.168.0.100	192.168.0.254
2	deny	192.168.0.0/24	192.168.0.254

暗黙のdenyについて

アクセスリストを設定した場合、アクセスリストの最後には全てのアクセスを禁止する暗黙のdenyが設定されています。つまり、全てのアクセスリストに対してマッチしないアクセスは禁止されることになります。

II. 簡易CLI機能のアクセス設定

3. CLI接続の受付開始

最後にCLI機能を有効にすることで、CLIへのアクセスの受け付けを開始します。

CLI機能の有効は、「機能設定」をクリックして、以下の設定画面から行います。

本機能	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> telnet <input type="checkbox"/> ssh
ホスト名	<input type="text" value="xr640l2"/>
Enableパスワード	<input type="text"/>

本機能

「telnet」「ssh」のチェック欄で、CLIへのアクセスを受け付けるポートを選択し、「有効」にチェックを入れます。

ホスト名

任意のホスト名を設定してください。CLIのプロンプトとして表示されます。

ENABLE パスワード

特権ユーザ用の「Enableパスワード」を設定します。

CLIには一般ユーザ用の「VIEWモード」と、特権ユーザ用の「ENABLEモード」があり、内部システム情報の表示や実行系のコマンドはENABLEモードでのみ実行可能です。このEnableパスワードを設定すると、ENABLEモードへ以降する際に、パスワード認証を行います。

詳細は、「CLIコマンドリファレンス」を参照してください。

入力が終わりましたら「設定」ボタンをクリックして設定完了です。チェックを入れたtelnet/sshポートをリッスンし、CLIへのアクセスを受け付けます。

II. 簡易CLI機能のアクセス設定

- - 注意 - -

telnet, sshポートのフィルタリング

CLI機能を有効にした場合、全てのインターフェースのtelnetポート(23番)またはsshポート(22番)でリッスンしている状態になります。CLIへのアクセスはアクセスリストで制限できますが、telnet, sshポートは攻撃の対象とされやすいので、WAN側のtelnet, sshポートは入力パケットのフィルタリングを設定することを推奨します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	破棄	tcp				22
2	ppp0	パケット受信時	破棄	tcp				23

フィルタリングの設定例です

telnet 接続クライアントについて

telnet 接続クライアントは、Windows「MS-DOS プロンプト」や端末エミュレータソフト、UNIXのtelnetコマンドなど任意のクライアントが使用できます。

これらのクライアントの使い方については、個々のマニュアル等を参照してください。

sshの対応バージョンについて

ssh接続はversion1, version2の両方に対応しています。常に両方のバージョンでの接続が可能です。但し、RSA鍵認証には対応しておりません。パスワード認証による接続のみ可能です。

telnet, sshセッションのキープアライブ

telnet, sshクライアントから突然に切断された場合に備え、TCPが無通信の状態でも120分を経過すると、自動的にTCP Keepaliveを開始します。

Keepaliveの応答がない場合は、TCPセッション断と判断し、内部のTCPセッションを解放します。

第31章

システム設定

システム設定

「システム設定」ページでは、本装置の運用に関する制御をおこないます。下記の項目に関して設定・制御が可能です。

- ・時計の設定
- ・ログの表示 / 削除
- ・パスワード設定
- ・ファームウェアアップデート
- ・設定の保存・復帰
- ・設定のリセット
- ・本体の再起動
- ・セッションライフタイムの設定
- ・設定画面の設定
- ・ISDN設定(XR-640L2のみ)
- ・オプションCFカードの操作(XR-640L2のみ)
- ・CLI設定(XR-640L2のみ)
- ・ARP Filterの設定

実行方法

Web 設定画面「システム設定」をクリックします。各項目のページへは、設定画面上部のリンクをクリックして移動します。

時計の設定

本装置内蔵時計の設定をおこないます。

「時計の設定」をクリックして設定画面を開きます。

内蔵時計の設定

2007年 08月 28日 火曜日

19時 08分 28秒

※時刻は24時間形式で入力してください。

設定の保存

24時間単位で時刻を設定してください。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。設定はすぐに反映されます。

第31章 システム設定

システム設定

ログの表示

実行方法

「ログの表示」をクリックして表示画面を開きます。



```
Apr 26 00:05:11 localhost -- MARK --
Apr 26 00:25:11 localhost -- MARK --
Apr 26 00:37:59 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 00:37:59 localhost named[436]: USAGE 1019749079 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 00:37:59 localhost named[436]: NSTATS 1019749079 1019556843 A=3
Apr 26 00:37:59 localhost named[436]: XSTATS 1019749079 1019556843 RR=0 RNXD=0
RFwdr=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SsysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdr=0 SFail=0
SFErr=0 SNaAns=0 SNXD=0
Apr 26 01:06:09 localhost -- MARK --
Apr 26 01:26:09 localhost -- MARK --
Apr 26 01:38:57 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 01:38:57 localhost named[436]: USAGE 1019752737 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 01:38:57 localhost named[436]: NSTATS 1019752737 1019556843 A=3
Apr 26 01:38:57 localhost named[436]: XSTATS 1019752737 1019556843 RR=0 RNXD=0
RFwdr=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SsysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdr=0 SFail=0
SFErr=0 SNaAns=0 SNXD=0
Apr 26 02:07:08 localhost -- MARK --
Apr 26 02:27:08 localhost -- MARK --
Apr 26 02:38:54 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 02:38:54 localhost named[436]: USAGE 1019756394 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 02:38:54 localhost named[436]: NSTATS 1019756394 1019556843 A=3
Apr 26 02:38:54 localhost named[436]: XSTATS 1019756394 1019556843 RR=0 RNXD=0
RFwdr=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SsysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdr=0 SFail=0
SFErr=0 SNaAns=0 SNXD=0
```

最大1000行まで表示できます

表示の更新

ログファイルの取得

ブラウザの「リンクを保存する」を使用して取得して下さい
[最新ログ](#)

本装置のログが全てここで表示されます。

「表示の更新」ボタンをクリックすると表示が更新されます。

ログの削除

ログ情報は最大2MBまでのサイズで保存されます。また再起動時にログ情報は削除されます。手動で削除する場合は次のようにしてください。

実行方法

「ログの削除」をクリックして画面を開きます。

ログの削除

すべてのログメッセージを削除します。

実行する

「実行する」ボタンをクリックすると、保存されているログが**全て削除**されます。

パスワードの設定

本装置の設定画面にログインする際のユーザー名、パスワードを変更します。ルータ自身のセキュリティのためにパスワードを変更されることを推奨します。

実行方法

「パスワードの設定」をクリックして設定画面を開きます。

パスワード設定

新しいユーザ名	<input type="text"/>
新しいパスワード	<input type="password"/>
もう一度入力してください	<input type="password"/>

新しいユーザー名とパスワードを設定します。
半角英数字で1から8文字まで設定可能です。
大文字・小文字も判別しますのでご注意ください。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。
次回のログインからは、新しく設定したユーザー名とパスワードを使います。

システム設定

ファームウェアのアップデート

本装置は、ブラウザ上からファームウェアのアップデートをおこないます。

実行方法

1 「ファームウェアのアップデート」をクリックして画面を開きます。

ファームウェアのアップデート

ここではファームウェアのアップデートをおこなうことができます。

ファイルの指定

参照...

アップデート実行

2 「参照」ボタンを押して、弊社ホームページからダウンロードしてきたファームウェアファイルを選択し、「アップデート実行」ボタンを押してください。

3 その後、ファームウェアを本装置に転送します(転送が終わるまではしばらく時間がかかります)。転送完了後に、以下のようなアップデートの確認画面が表示されますので、バージョン等が正しければ「実行する」をクリックしてください。

ファームウェアのアップデート

ファームウェアのダウンロードが完了しました

現在のファームウェアのバージョン

Century Systems XR-640/CD-L2 Series ver 1.4.4

ダウンロードされたファームウェアのバージョン

Century Systems XR-640/CD-L2 Series ver 1.6.1

このファームウェアでアップデートしますか？

注意:3分以内にアップデートが実行されない場合はダウンロードしたファームウェアを破棄します

実行する

中止する

注：上記画面が表示されたままで3分間経過すると、以下の画面が表示され、アップデートが実行されません。

アップロード完了から3分以上経過したため
ファームウェアは破棄されました

4 アップデートを実行した場合は以下の画面が表示され、ファームウェアの書き換えが始まります。

ファームウェアのアップデートを実行します。
作業には数分かかりますので電源を切らずにお待ち下さい。
作業が終了しますと自動的に再起動します。

アップデート中、XR-410L2は本体のLEDに"8"が表示され、XR-640L2は本体のLEDが時計回りに回転します。この間は、アクセスをおこなわずにそのままお待ちください。

ファームウェアの書き換え後に本装置が自動的に再起動されて、アップデートの完了です。

システム設定

設定の保存と復帰

本装置の設定の保存および、保存した設定の復帰をおこないます。

実行方法

「設定の保存・復帰」をクリックして画面を開きます。

- - 注意 - -

「設定の保存復帰画面」にて設定情報を表示・更新する際、ご利用のプロバイダ登録情報や本装置のRSAの秘密鍵を含む設定情報等がネットワーク上に平文で流れます。

設定の保存・復帰は、ローカル環境もしくはVPN環境等、セキュリティが確保された環境下で行う事をお勧めします。

上記のような注メッセージが表示されてから、「設定の保存・復帰」のリンクをクリックします。

【設定の保存】

設定を保存するときは、テキストのエンコード形式と保存形式を選択して「設定ファイルの作成」をクリックします。

現在の設定を保存することができます。	
コードの指定	<input type="radio"/> EUC(LF) <input checked="" type="radio"/> SJIS(CR+LF) <input type="radio"/> SJIS(CR)
形式の指定	<input type="radio"/> 全設定(zip) <input checked="" type="radio"/> 初期値との差分(text)

クリックすると以下のメッセージが表示されます。

設定をバックアップしました。
バックアップファイルのダウンロード

ブラウザのリンクを保存する等で保存してください。

「バックアップファイルのダウンロード」リンクから、設定をテキストファイルで保存しておきます。

(次のページに続きます)

「全設定」を選択すると、すべての本装置の設定をgzip形式で圧縮して保存します。

「初期値との差分」を選択すると、初期値と異なる設定のみを抽出して、テキスト形式で保存します。このテキストファイルの内容を直接書き換えて設定を変更することもできます。

【設定の復帰】

上記項目から「参照」をクリックして、保存しておいた設定ファイルを選択します。全設定の保存ファイルはgzip圧縮形式のまま、復帰させることができます。

ここでは設定を復帰させることができます。	
ファイルの指定	<input type="text"/> <input type="button" value="参照..."/>

その後「設定の復帰」をクリックすると、設定の復帰がおこなわれます。

設定が正常に復帰できたときは、本装置が自動的に再起動されます。

- - 注意 - -

「設定の保存復帰画面」にて設定情報を表示・更新する際、ご利用のプロバイダ登録情報や本装置のRSAの秘密鍵を含む設定情報等がネットワーク上に平文で流れます。設定の保存・復帰は、ローカル環境もしくはVPN環境等、セキュリティが確保された環境下で行う事をおすすめします。

システム設定

設定のリセット

本装置の設定を全てリセットし、工場出荷時の設定に戻します。

実行方法

「設定のリセット」をクリックして画面を開きます。

現在の本体設定内容を全てクリアして工場出荷設定に戻します。

実行する

「実行する」ボタンをクリックするとリセットが実行され、本体の全設定が工場出荷設定に戻ります。

再起動

本装置を再起動します。設定内容は変更されません。

実行方法

「再起動」をクリックして画面を開きます。

本体の再起動

本体を再起動します。

実行する

「実行する」ボタンをクリックすると、リセットが実行されます。

システム設定

セッションライフタイムの設定

NAT/IPマスカレードのセッションライフタイムを設定します。

「設定の保存」ボタンをクリックすると、設定が保存されます。設定内容はすぐに反映されます。

「セッションライフタイムの設定」をクリックして画面を開きます。

XR-410L2

UDP	<input type="text" value="30"/>	秒 (0 - 8640000)
UDP stream	<input type="text" value="180"/>	秒 (0 - 8640000)
TCP	<input type="text" value="3600"/>	秒 (0 - 8640000)
0を入力した場合、デフォルト値を設定します。		

XR-640L2

UDP	<input type="text" value="30"/>	秒 (0 - 8640000)
UDP stream	<input type="text" value="180"/>	秒 (0 - 8640000)
TCP	<input type="text" value="3600"/>	秒 (0 - 8640000)
セッション最大数	<input type="text" value="8192"/>	セッション (0, 4096 - 16384)
0を入力した場合、デフォルト値を設定します。		

UDP

UDPセッションのライフタイムを設定します。単位は秒です。0 ~ 8640000の間で設定します。初期設定は30秒です。

UDP stream

UDP streamセッションのライフタイムを設定します。単位は秒です。0 ~ 8640000の間で設定します。初期設定は180秒です。

TCP

TCPセッションのライフタイムを設定します。単位は秒です。0 ~ 8640000の間で設定します。初期設定は3600秒です。

セッション最大数 (XR-640L2のみ)

XRで保持できるNAT/IPマスカレードのセッション情報の最大数を設定します。UDP/UDPstream/TCPのセッション情報を合計した最大数になります。4096 ~ 16384の間で設定します。初期設定は8192です。

なお、XR内部で保持しているセッション数は、定期的にsyslogに表示することができます。詳しくは第15章「SYSLOG機能」を参照してください。

システム設定

設定画面の設定

WEB設定画面へのアクセスログについての設定をします。

実行方法

「設定画面の設定」をクリックして画面を開きます。

設定画面の設定	
アクセスログ	<input checked="" type="radio"/> 使用しない <input type="radio"/> syslogに取る
エラーログ	<input checked="" type="radio"/> 使用しない <input type="radio"/> syslogに取る

設定画面の

アクセスログ

(アクセス時の)エラーログ

取得するかどうかを指定します。

最後に「設定の保存」をクリックします。

アクセスログ・エラーログは、「syslog」サービスの設定にしたがって出力されます。

ISDN設定 (XR-640L2のみ)

BRIを使ったISDN回線接続を行なうときの「ISDN発信者番号」を設定します。

実行方法

「ISDNの設定」をクリックして画面を開きます。

ISDN番号	<input type="text"/>
サブアドレス	<input type="text"/>

ISDN番号

ISDN発信者番号を入力します。

サブアドレス

サブアドレスを指定します。

「設定の保存」をクリックします。

システム設定

オプションCFカード (XR-640L2のみ)

本装置にオプションで用意されているコンパクトフラッシュ(CF)カードを装着している場合の、CFカードの操作を行います。

ここでは以下の設定を行うことができます。

- ・CFカードの初期化
- ・CFカードへの設定のバックアップ

実行方法

コンパクトフラッシュ(CF)カードを装着してから「オプションCFカード」をクリックして画面を開きます。

画面には、装着したCFカードの情報が表示されます。

CFカードの初期化

はじめてCFカードを装着したときは、必ずCFカードを初期化する必要があります。初期化を行わないとCFカードを使用できません。

CFカードを初期化するときは「オプションCFカードの初期化」をクリックします。

オプションCFカード

このオプションCFカードは初期化しないと使用出来ません

オプションCFカードを初期化します

オプションCFカードの初期化

CFカードへの設定のバックアップ

設定のバックアップをCFカードにコピーするときは「設定ファイルをコピーする」をクリックしてコピーを実行します。

オプションCFカード

オプションCFカードの状況

総容量 [124906 kbyte] 空容量 [121898 kbyte] 使用率 [2%]

機器設定のバックアップはありません

オプションCFカードに現在の設定をコピーします

設定ファイルをコピーする

オプションCFカードを初期化します

オプションCFカードの初期化

設定のバックアップがある場合は、画面上部に、装着したCFカードの状況とバックアップ情報が表示されます。

オプションCFカード

オプションCFカードの状況

総容量 [124906 kbyte] 空容量 [121822 kbyte] 使用率 [2%]

機器設定のバックアップ日時

Sep 4 15:27

[CFカードの取り扱いについて]

オプションCFカードは、本装置前面パネルのCFカードスロットに挿入してください。

CFカードを挿入すると、本体前面のCF(緑)ランプが点滅します。その後CFランプが点灯すると、CFカードが使用できる状態となります。

CFカードを本装置から取り外すときは、必ず本体前面のCFカードスロット横にあるRELEASEボタンを数秒押し続けてください。その後CFランプが消灯状態になりましたら、CFカードを安全に取り外せます。

上記の手順以外でCFカードを取り扱った場合、本装置および、CFカードが故障する場合がありますのでご注意ください。

システム設定

CLI 設定 (XR-640L2 のみ)

CLI 設定については、第 28 章「簡易 CLI 機能 (XR-640L2 のみ)」で説明します。

ARP filter 設定

ARP filter の設定をおこないます。

ARP filter を有効にすることで、同一 IP アドレスの ARP を複数のインタフェースで受信したときに、当該 MAC アドレス以外のインタフェースから ARP 応答を出さないようにできます。

「ARP filter 設定」をクリックして設定画面を開きます。



「無効」または「有効」を選択して「設定の保存」をクリックします。

第 32 章

情報表示

本体情報の表示

本体の機器情報を表示します。
以下の項目を表示します。

- ファームウェアバージョン情報**
現在のファームウェアバージョンを確認できます。
- インターフェース情報**
各インターフェースの IP アドレスや MAC アドレスなどです。
PPP/PPPoE や IPsec 論理インタフェースもここに表示されます。
- リンク情報**
本装置の各 Ethernet ポートのリンク状態、リンク速度が表示されます。
- ルーティング情報**
インターフェースルート、スタティックルート、ダイナミックルートに関するルーティング情報です。
- Default Gateway 情報**
デフォルトルート情報です。
- ARP テーブル情報**
XR が保持している ARP テーブルです。
- DHCP クライアント取得情報**
DHCP クライアントとして設定しているインターフェースがサーバから取得した IP アドレス等の情報を表示します。

実行方法

Web 設定画面の「情報表示」をクリックすると、新しいウィンドウが開いて本体情報表示されます。

XR-410L2



第32章 情報表示

本体情報の表示

XR-640L2

```
http://192.168.0.254:880 - 機器情報 - Microsoft Internet Explorer
ファームウェアバージョン
Century Systems XR-640/CD-L2 IRI ver 1.4.2 (build 16/Mar 9 16:53 2006)
更新
インターフェース情報
eth0 Link encap:Ethernet HWaddr 00:80:6D:77:04:06
inet addr:192.168.0.254 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:532 errors:0 dropped:0 overruns:0 frame:0
TX packets:335 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:84348 (82.9 Kb) TX bytes:134049 (130.9 Kb)
Interrupt:60
eth1 Link encap:Ethernet HWaddr 00:80:6D:77:04:07
inet addr:192.168.1.254 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:62
eth2 Link encap:Ethernet HWaddr 00:80:6D:77:04:08
inet addr:192.168.2.254 Bcast:192.168.2.255 Mask:255.255.255.0
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:26 Base address:0xaf00
リンク情報
eth0 Link:up AutoNegotiation:on Speed: 100M Duplex:full
eth1 Link:down
eth2 Port1 Link:down
Port2 Link:down
Port3 Link:down
Port4 Link:down
ルーティング情報
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth2
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
Default Gateway情報
ARPテーブル情報
IP address HW type Flags HW address Mask Device
192.168.0.10 0x1 0x2 00:01:80:6D:A7 * eth0
更新
anchor for reload-button
```

画面中の「更新」をクリックすると、表示内容が更新されます。

第 33 章

詳細情報表示
(XR-640L2 のみ)

各種情報の表示

ここではルーティング情報や各種サービス情報をまとめて表示することができます。

以下の項目を表示します。

・ルーティング情報

XR のルーティングテーブル、ルーティングテーブルの内部情報、ルートキャッシュの情報、デフォルトゲートウェイ情報が表示できます。

このうち、ルーティングテーブルの内部情報とルートキャッシュの情報はここでのみ表示できます。

- ・ OSPF 情報
- ・ RIP 情報
- ・ IPsec 情報
- ・ NTP 情報
- ・ QoS 情報

実行方法

Web 設定画面「詳細情報表示」をクリックすると、次の画面が表示されます。

ルーティング	ルーティング詳細情報
	ルーティングキャッシュ情報
	デフォルトゲートウェイ情報
OSPF	データベース情報
	ネイバー情報
	ルート情報
	統計情報
	インターフェース情報 <input type="text"/>
RIP	RIP 情報
IPsecサーバ	IPsec 情報
NTPサービス	NTP 情報
QoS	Queueing 設定情報
	CLASS 設定情報
	CLASS 分けフィルタ設定情報
	Packet 分類設定情報
	Interface の指定 <input type="text"/>
全ての詳細情報を表示する	

左列の機能名をクリックすると、新しいウィンドウが開いて、その機能に関する情報がまとめて表示されます。

右列の小項目名をクリックした場合は、その小項目のみの情報が表示されます。なお、「OSPF のインターフェース情報」および QoS の各情報については、ボックス内に表示したいインターフェース名を入力してください。

一番下の「全ての詳細情報を表示する」をクリックすると、全ての機能の全ての項目についての情報が一括表示されます。

第 34 章

テクニカルサポート

第 34 章 テクニカルサポート

テクニカルサポート

テクニカルサポートを利用することによって、本体の情報を一括して取得することができます。

機器情報の取得を行います

情報取得

「情報取得」をクリックします。下記の 3 つの情報を一括して取得することができます。

syslog

設定ファイル

本体の機器情報

第 35 章

運用管理設定

1. INIT ボタンの操作

本装置の背面にある「INIT ボタン」を使用することで、以下操作ができます。

- ・本装置の設定を一時的に初期化する
(ソフトウェアリセット)
- ・オプション CF カードに保存された設定で起動する (XR-640L2 のみ)

本装置の設定を初期化する

XR-410L2

1. INIT ボタンを押したまま電源切断
2. 電源投入し、電源投入後も 5 秒ほど INIT ボタンを押しつづける

その後、工場出荷設定で起動します。

XR-640L2

1. 本装置が停止状態になっていることを確認します。
2. 本体背面にある「INIT」ボタンを押しながら、電源スイッチをオンにします。INIT ボタンは押し続けたままにしておきます。
3. 本体前面の STATUS1 ランプが点灯、他の STATUS ランプが消灯するまで INIT ボタンを押し続けます。
4. 3. の状態になったら INIT ボタンを放します。

その後、工場出荷設定で起動します。

注： ただしこのとき、工場出荷時の設定での再起動前の設定は別の領域に残っています。

この操作後にもう一度再起動すると、それまでの設定が復帰します。工場出荷時の設定で戻したあとに設定を変更していれば、変更した設定が反映された上で復帰します。

設定を完全にリセットする場合は、「システム設定」「設定のリセット」でリセットを実行してください。

CF カードの設定で起動する (XR-640L2 のみ)

- 1 本装置にオプション CF カードが挿入されていることを確認します。
- 2 本体背面にある「INIT」ボタンを押しながら、電源スイッチをオンにします。INIT ボタンは押し続けたままにしておきます。
- 3 本体前面の「CF」ランプの点滅が止まるまで INIT ボタンを押し続けます。
- 4 点滅が止まったら INIT ボタンを放します。その後、本装置が CF カードに保存されている設定内容で起動します。

1. INIT ボタンの操作

補足：バージョンアップ後の設定内容について

本装置をバージョンアップしたとき、CF カード内の設定ファイルは旧バージョンの形式で保存されたままです。

ただしバージョンアップ後に本装置を電源 OFF
CF カードの設定内容で起動しても、旧バージョンの設定内容を自動的に新バージョン用に変換して起動できません。

CF カード内の設定を新バージョン用にするためには、新バージョンで CF カードの設定から起動し、あらためて CF カードへ設定の保存を行ってください。

11. 携帯電話による制御(XR-640L2のみ)

本装置にグローバルアドレスが割り当てられていて、インターネットに接続している状態ならば、iモードおよびEZウェブに対応した携帯電話から以下のような操作が可能です。

- ・ルータとしてのサービスを停止する
- ・ルータとしてのサービスを再開する
- ・本装置を再起動する

この機能を利用する際は、パケットフィルタリング設定によってWAN側からの設定変更を許す設定になっていることが必要になります。WAN側から本装置の設定変更を許すフィルタ設定については「パケットフィルタ機能」項目をご覧ください。

実際に操作画面にアクセスするためには、iモード端末から次のURLをしてしてください。

<iモード端末からアクセスする場合>

http:// 装置の IP アドレス:880/i/

<EZウェブ端末からアクセスする場合>

**http:// 装置の IP アドレス:880/ez/
index.html**

アクセスすると認証画面が表示されますので、ユーザー名とパスワードを入力してください。

「iフィルタ起動」を実行すると、ルータとしてのサービスが停止します。

この状態では、WANからLANへのアクセスはできません。WAN側からは本装置自身の設定画面もしくはiモード画面にしかアクセスできなくなります。

またLAN側からインターネット側へアクセスしても、アクセス先からの応答を受け取ることができなくなります。

「iフィルタ停止」を実行すると、以前の設定状態に戻り、ルータ機能が再開されます。

iモードからアクセスするには、パケットフィルタの「入力フィルタ設定」で、インターネット側から本装置の設定画面にログインできるように設定しておく必要があります。

IPアドレス自動割り当ての契約でインターネットに接続されている場合、本装置に割り当てられたグローバルアドレスが変わってしまう場合があります。もしアドレスが変わってしまったときはiモードからの制御ができなくなってしまうことが考えられますので(アドレスが分からなくなるため)、運用には十分ご注意ください。

II. 携帯電話による制御(XR-640L2 のみ)

操作方法

1 携帯電話端末から本装置の WAN 側に割り当てられたグローバルアドレスを指定してアクセスします。



3 操作メニューが表示されます。



操作したい項目を選択して実行してください。

2 ユーザー名とパスワードを入力して「OK」を選択します。



4 「フィルタ状態」を選択すると以下のような画面が表示されて、現在の状態を確認できます。



付録 A

インターフェース名について

付録 A

インターフェース名について

本装置は、以下の設定においてインターフェース名を直接指定する必要があります。

- ・ OSPF 機能
- ・ IPsec 機能
- ・ SNMP エージェント機能
- ・ スタティックルート設定
- ・ ソースルート設定
- ・ NAT 機能
- ・ パケットフィルタリング機能
- ・ 仮想インターフェース機能
- ・ QoS 機能
- ・ ネットワークテスト

本装置のインターフェース名と実際の接続インターフェースの対応づけは次の表の通りとなります。

XR-410L2

eth0	Ether0ポート
eth1	Ether1ポート
ppp0	PPP/PPPoE主回線
ppp2	PPP/PPPoEマルチ接続 2
ppp3	PPP/PPPoEマルチ接続 3
ppp4	PPP/PPPoEマルチ接続 4
ppp5	バックアップ回線
ppp6	アクセスサーバ(シリアル接続)
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
ipsec7	eth2上のipsec
gre<n>	gre(<n>は設定番号)
eth0.<n>	eth0上のVLAN(<n>はタグID)
eth1.<n>	eth1上のVLAN(<n>はタグID)

XR-640L2

eth0	Ether0ポート
eth1	Ether1ポート
eth2	Ether2ポート
ppp0	PPP/PPPoE主回線
ppp2	PPP/PPPoEマルチ接続 2
ppp3	PPP/PPPoEマルチ接続 3
ppp4	PPP/PPPoEマルチ接続 4
ppp5	バックアップ回線
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
ipsec7	eth2上のipsec
gre<n>	gre(<n>は設定番号)
eth0.<n>	eth0上のVLANインターフェース(<n>はタグID)
eth1.<n>	eth1上のVLANインターフェース(<n>はタグID)
eth2.<n>	eth2上のVLANインターフェース(<n>はタグID)
eth0:<n>	eth0上の仮想インターフェース(<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インターフェース(<n>は仮想IF番号)
eth2:<n>	eth2上の仮想インターフェース(<n>は仮想IF番号)

表左：インターフェース名
表右：実際の接続デバイス

付録 B

工場出荷設定一覧

工場出荷設定一覧

IPアドレス設定	IPアドレス/サブネットマスク値
ETHER0ポート	192.168.0.254/255.255.255.0
ETHER1ポート	192.168.1.254/255.255.255.0
ETHER2ポート (XR-640L2のみ)	192.168.2.254/255.255.255.0
DHCPクライアント機能	無効
IPマスカレード機能	無効
ステートフルパケットインスペクション機能	無効
デフォルトゲートウェイ設定	設定なし
リモートアクセス接続	無効
DNSリレー/キャッシュ機能	有効
IPsec機能	無効
ダイナミックルーティング機能	無効
L2TPv3機能	無効
SYSLOG機能	有効
SNMPエージェント機能	無効
NTP機能	無効
アクセスサーバ機能	無効
スタティックルート設定	設定なし
ソースルート設定	設定なし
NAT機能	設定なし
パケットフィルタリング機能	NetBIOSからの漏洩を防止するフィルタ設定 (入力・転送フィルタ設定) 外部からのUPnPパケットを遮断する設定 (入力・転送フィルタ設定)
スケジュール機能 (XR-640L2のみ)	設定なし
ネットワークイベント機能	無効
仮想インターフェース機能	設定なし
GRE機能	無効
QoS機能	設定なし
パケット分類機能	設定なし
ゲートウェイ認証機能	無効
設定画面ログインID	admin
設定画面ログインパスワード	admin

付録 C

サポートについて

サポートについて

本製品に関するサポートは、ユーザー登録をされたお客様に限らせていただきます。必ずユーザー登録していただきますよう、お願いいたします。

サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。

- ・サポートデスク
電話 0422-37-8926
受付時間 10:00 ~ 17:00
(土日祝祭日、及び弊社の定める休日を除きます)
- ・FAX 0422-55-3373
- ・e-mail support@centurysys.co.jp
- ・ホームページ <http://www.centurysys.co.jp/>

故障と思われる場合は

製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡ください。事前のご連絡なしに弊社までご送付いただきますとサポートをお受けすることはできません。

ご連絡をいただく前に

スムーズなユーザーサポートをご提供するために、サポートデスクにご連絡いただく場合は以下の内容をお知らせいただきますよう、お願いいたします。

- ・ファームウェアのバージョンと MAC アドレス
(バージョンの確認方法は「第 32 章 情報表示」をご覧ください)
- ・ネットワークの構成(図)
どのようなネットワークで運用されているかを、差し支えない範囲でお知らせください。
- ・不具合の内容または、不具合の再現手順
何をしたときにどのような問題が発生するのか、できるだけ具体的にお知らせください。
- ・エラーメッセージ
エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
- ・本装置の設定内容、およびコンピュータの IP 設定
- ・**「設定のバックアップファイル」を電子メール等でお送りください。**

サポート情報

弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。また製品の FAQ も掲載しておりますので、是非ご覧ください。

XR-410/TX2-L2 製品サポートページ

<http://www.centurysys.co.jp/support/XR410TX2L2.html>

XR-640/CD-L2 製品サポートページ

<http://www.centurysys.co.jp/support/xr640cdl2.html>

製品の保証について

本製品の保証期間は、お買い上げ日より1年間です。保証期間をすぎたもの、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承ください。保証規定については、同梱の保証書をご覧ください。

XR-410/TX2-L2 XR-640/CD-L2 ユーザーズガイド v1.6.1対応版

2007年09月版

発行 センチュリー・システムズ株式会社

Copyright (c) 2002-2007 Century Systems Co., Ltd. All rights reserved.
