

BROADBAND GATE

L2TPv3 搭載プロードバンドルータ

FutureNet XR-410/TX2-L2

ユーザーズガイド

Ver1.3.3 対応版

センチュリー・システムズ 株式会社

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 XR-410/TX2-L2 の概要	11
I. XR-410/TX2-L2 の特長	12
II. 各部の名称と機能	13
III. 動作環境	14
第2章 XR-410/TX2-L2 の設置	15
XR-410/TX2-L2 の設置	16
第3章 コンピューターのネットワーク設定	17
I. Windows 95/98/Me のネットワーク設定	18
II. Windows 2000 のネットワーク設定	19
III. Windows XP のネットワーク設定	20
IV. Macintosh のネットワーク設定	21
V. IP アドレスの確認と再取得	22
第4章 設定画面へのログイン	23
設定画面へのログイン方法	24
第5章 インターフェース設定	25
I. Ethernet ポートの設定	26
II. Ethernet ポートの設定について	27
III. VLAN タギングの設定	28
第6章 PPPoE 設定	29
I. PPPoE の接続先設定	30
II. PPPoE の接続設定と回線の接続 / 切断	32
III. 副回線とバックアップ回線	33
IV. PPPoE 特殊オプション設定	36
第7章 RS-232 ポートを使った接続(リモートアクセス機能)	37
I. XR-410/TX2-L2 とアナログモデム /TA の接続	38
アナログモデム /TA の接続	38
II. リモートアクセス回線の接続先設定	39
III. リモートアクセス回線の接続と切断	41
IV. 副回線接続とバックアップ回線接続	42
第8章 複数アカウント同時接続設定	43
複数アカウント同時接続の設定	44
第9章 各種サービスの設定	48
各種サービス設定	49
第10章 DNS リレー / キャッシュ機能	50
DNS リレー機能	51
DNS キャッシュ機能	51
DNS のキャッシュについて	51
第11章 IPsec 機能	52
I. 本装置の IPsec 機能について	53
II. IPsec 設定の流れ	54
III. IPsec 設定	55
IV. IPsec Keep-Alive 機能	62
V. 「X.509 デジタル証明書」を用いた電子認証	64
VI. IPsec 通信時のパケットフィルタ設定	66

VII. IPsec 設定例 1 (センター / 拠点間の 1 対 1 接続)	67
VIII. IPsec 設定例 2 (センター / 拠点間の 2 対 1 接続)	71
IX. IPsec がつながらないとき	78
第 12 章 ダイナミックルーティング(RIP と OSPF の設定)	81
I. ダイナミックルーティング機能	82
設定の開始	82
II. RIP の設定	83
RIP の設定	83
RIP フィルターの設定	84
III. OSPF の設定	85
インターフェースへの OSPF エリア設定	85
OSPF エリア設定	86
OSPF VirtualLink 設定	87
OSPF 機能設定	88
インターフェース設定	90
ステータス表示	91
第 13 章 L2TPv3 機能	92
I. L2TPv3 機能概要	93
II. L2TPv3 機能設定	94
III. L2TPv3 Tunnel 設定	96
IV. L2TPv3 Xconnect(クロスコネクト)設定	97
V. L2TPv3 Group 設定	99
VI. 起動 / 停止設定	100
VII. L2TPv3 ステータス表示	101
VIII. 制御メッセージ一覧	102
IX. L2TPv3 設定例 1	103
X. L2TPv3 設定例 2 (L2TP トンネル二重化)	105
第 14 章 SYSLOG 機能	109
syslog 機能の設定	110
第 15 章 SNMP エージェント機能	111
SNMP エージェント機能の設定	112
第 16 章 NTP サービス	113
NTP サービスの設定方法	114
第 17 章 アクセスサーバ機能	115
I. XR-410/TX2-L2 とアナログモデム /TA の接続	116
アナログモデム /TA の接続	116
II. アクセスサーバ機能の設定	117
第 18 章 スタティックルート設定	118
スタティックルート設定	119
第 19 章 ソースルート設定	121
ソースルート設定	122
第 20 章 NAT 機能	123
I. XR-410/TX2-L2 の NAT 機能について	124
II. バーチャルサーバ設定	125
III. 送信元 NAT 設定	126
IV. バーチャルサーバの設定例	127
WWW サーバを公開する際の NAT 設定例	127
FTP サーバを公開する際の NAT 設定例	127

PPTP サーバを公開する際の NAT 設定例	128
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)	129
V. 送信元 NAT の設定例	130
補足：ポート番号について	131
第21章 パケットフィルタリング機能	132
I. 機能の概要	133
II.XR-410/TX2-L2 のフィルタリング機能について	134
III. パケットフィルタリングの設定	135
IV. パケットフィルタリングの設定例	137
インターネットから LAN へのアクセスを破棄する設定	137
WWW サーバを公開する際のフィルタ設定例	138
FTP サーバを公開する際のフィルタ設定例	138
WWW、FTP、メール、DNS サーバを公開する際のフィルタ設定例	139
NetBIOS パケットが外部へ出るのを防止するフィルタ設定	140
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)	140
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)	141
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	141
PPTP を通すためのフィルタ設定	142
V. 外部から設定画面にアクセスさせる設定	143
補足：NAT とフィルタの処理順序について	144
補足：ポート番号について	145
補足：フィルタのログ出力内容について	146
第22章 仮想インターフェース機能	147
仮想インターフェースの設定	148
第23章 GRE 機能	149
GRE の設定	150
第24章 QoS 設定	152
I.QoS について	153
II.QoS 機能の各設定画面について	157
III. 各キューイング方式の設定手順について	158
IV. 各設定画面での設定方法について	159
V. ステータスの表示	166
VI. 設定の編集・削除方法	167
VII. ステータス情報の表示例	168
VIII. クラスの階層構造について	172
IX.TOS について	173
第25章 ゲートウェイ認証機能	175
ゲートウェイ認証機能の設定	176
基本設定	176
ユーザー設定	177
RADIUS 設定	178
フィルタ設定	179
ログ設定	179
ゲートウェイ認証下のアクセス方法	180
ホストからのアクセス方法	180
設定画面へのアクセスについて	180
RADIUS 設定について	180
認証について	180

ゲートウェイ認証の制御方法について	181
第26章 ネットワークテスト	182
ネットワークテスト	183
第27章 各種システム設定	186
時計の設定	187
ログの表示	188
ログの削除	188
パスワードの設定	189
ファームウェアのアップデート	189
設定の保存と復帰	190
設定のリセット	191
本体再起動	192
セッションライフタイムの設定	192
設定画面の設定	193
ARP filter 設定	193
第28章 情報表示	194
本体情報の表示	195
第29章 運用管理設定	196
一時的に工場出荷設定に戻す方法	197
付録 A インタフェース名一覧	198
インターフェース名について	199
付録 B 工場出荷設定一覧	200
付録 C 製品仕様	202
付録 D サポートについて	205
サポートについて	206

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粋経済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下さい。
- 2 通信情報が漏洩した事による経済的、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下さい。
- 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、外観の内容について、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下さい。

商標の表示

「BROADBAND GATE」はセンチュリー・システムズ株式会社の登録商標です。
「XR-410/TX2-L2」はセンチュリー・システムズ株式会社の商標です。
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 NT4.0
Windows 2000、Windows XP
Macintosh は、アップルコンピュータ社の登録商標です。
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下さい。

絵表示について

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。



製品の隙間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下さい。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下さい。
 -  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の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。火災の原因になります。
 - !
 - 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下さい。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、ACアダプタをコンセントから抜いて、ご使用をお控え下さい。落雷が火災・感電・故障の原因となることがあります。
-  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本体	1台
はじめにお読み下さい	1部
製品マニュアル PDF形式(CD-ROM)	1枚
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

第1章

XR-410/TX2-L2 の概要

I. XR-410/TX2-L2 の特長

XR-410/TX2-L2(以下、本製品)は次のような特長を持っています。

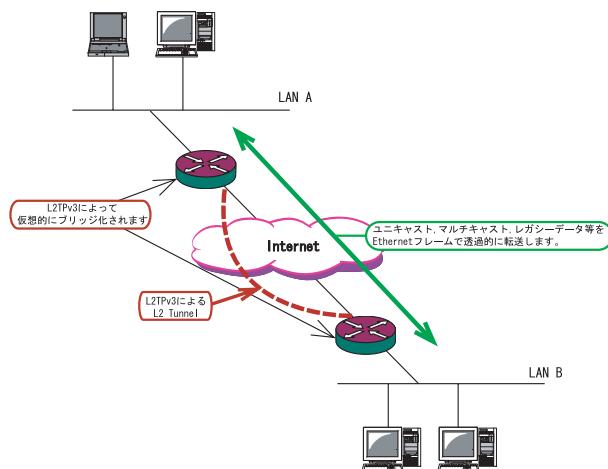
L2TPv3 機能を搭載

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](#)をご参照下さい。

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を組み合わせて使うことで、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回線や予備のブ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。インター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

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

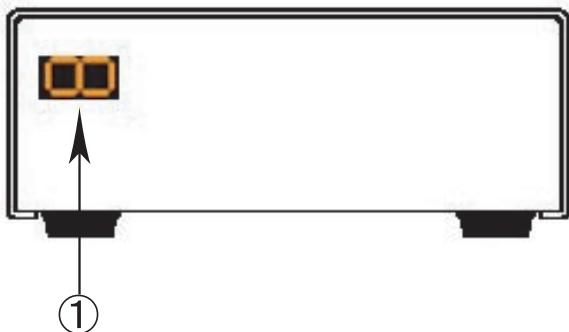
GREトンネリング機能

ゲートウェイ認証機能

各種システムログの記録

II. 各部の名称と機能

製品前面



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。

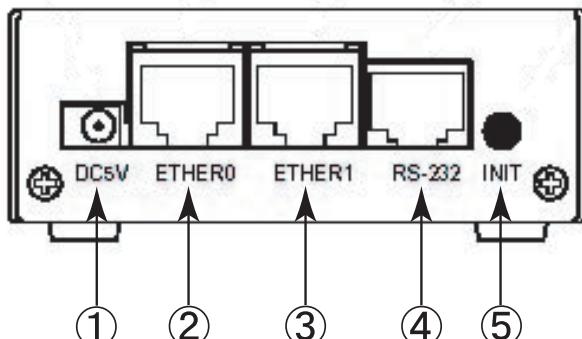


ケーブルを接続して
動作している状態の表示例。

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下さい。

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押します。操作方法については第28章をごらんください。

III. 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ーの全てに、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ー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ー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ーの中で少なくとも 1 台に、Internet Explorer4.0 以降か Netscape Navigator4.0 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係する 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、あらかじめご了承下さい。

第2章

XR-410/TX2-L2 の設置

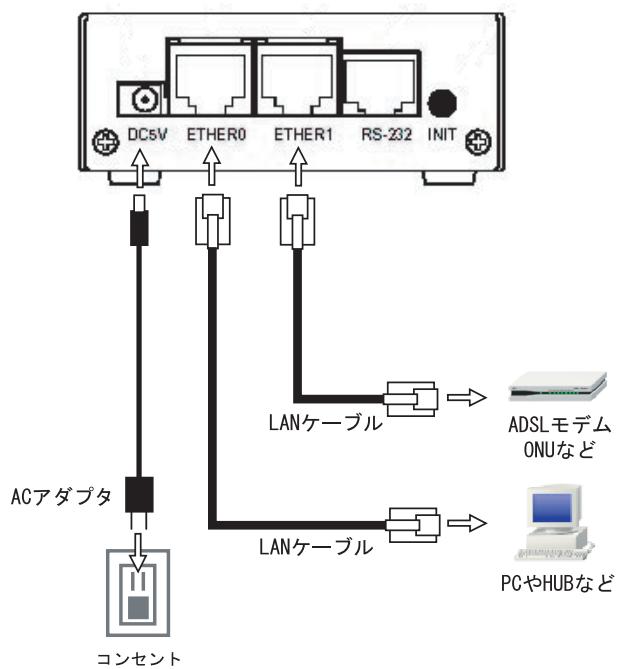
第2章 XR-410/TX2-L2 の設置

XR-410/TX2-L2 の設置

XR-410/TX2-L2 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。
- 4 本装置とACアダプタ、ACアダプタとコンセン
トを接続して下さい。
- 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アダプターのプラグを本体に差し込んだ後に
ACアダプター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下さい。
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アダプター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

コンピューターのネットワーク設定

第3章 コンピューターのネットワーク設定

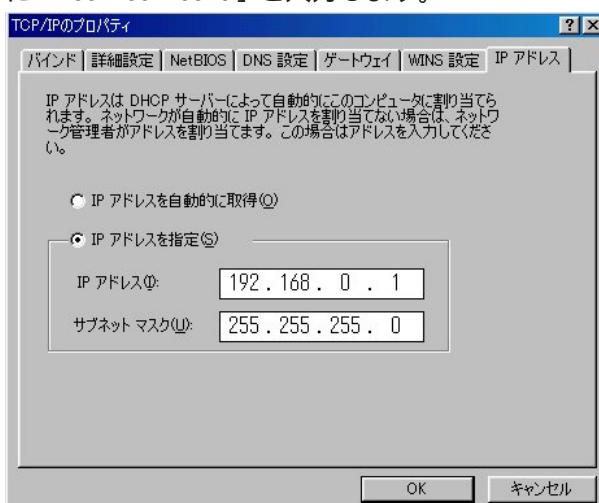
I. Windows 95/98/Me のネットワーク設定

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

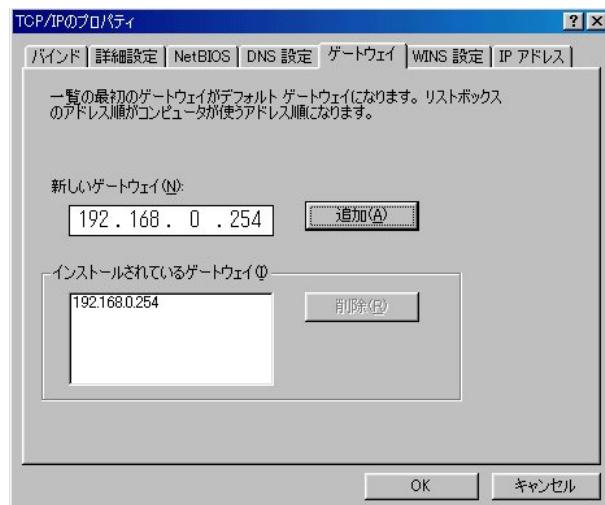
1 「コントロールパネル」 「ネットワーク」 の順で開き、「ネットワークの設定」タブの「現在のネットワーク構成」から、コンピューターに装着された LAN ボード(カード)のプロパティを開きます。



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ーが再起動します。再起動後に、XR-410/TX2-L2 の設定画面へのログインが可能になります。

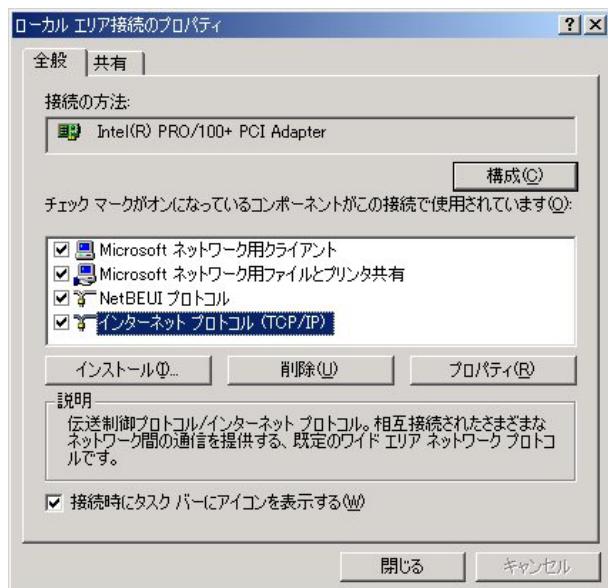
第3章 コンピューターのネットワーク設定

II. Windows 2000 のネットワーク設定

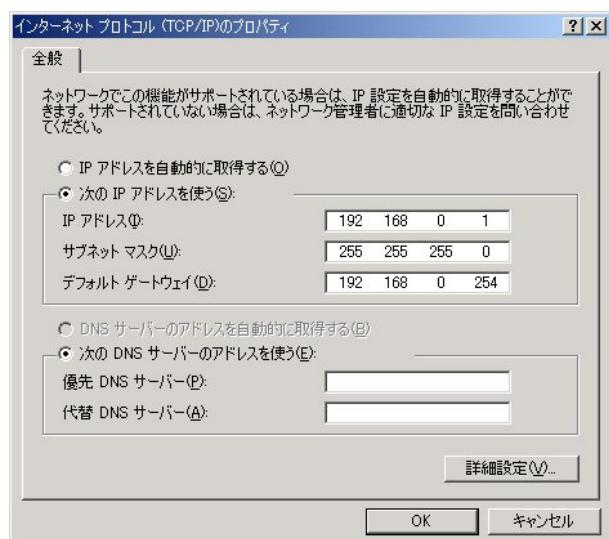
ここではWindows2000が搭載されたコンピューターのネットワーク設定について説明します。

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XR-410/TX2-L2へのログインの準備が整
いました。

第3章 コンピューターのネットワーク設定

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ー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。

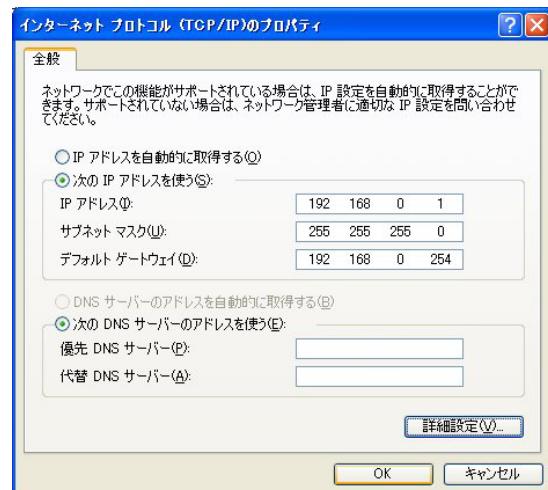


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコル(TCP/IP)」を選択して「プロパティ」ボタンをクリックします。



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XR-410/TX2-L2へのログインの準備が整いました。

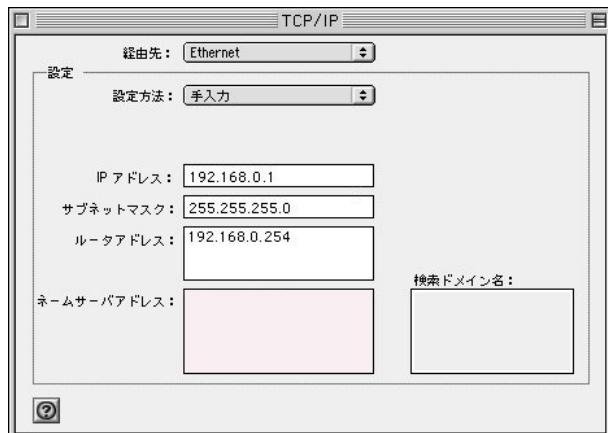
第3章 コンピューターのネットワーク設定

IV. 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 XR-410/TX2-L2 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

V. 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「全て開放」をクリックすると、現在の IP 設定がクリアされます。引き続いて「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 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。

第4章

設定画面へのログイン

第4章 設定画面へのアクセス

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、それにあわせてユーザー名・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

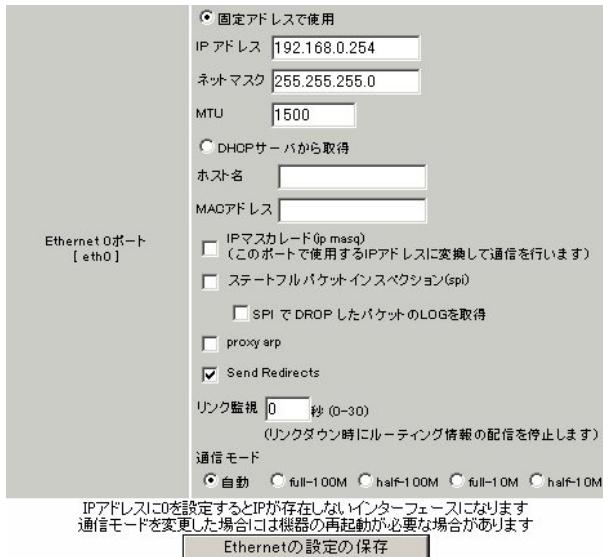
インターフェース設定

第5章 インターフェース設定

I.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「インターフェース設定」->「Ethernet0 (または1)の設定」をクリックして設定します。



各インターフェースについて、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、そのインターフェースは 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ー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 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 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」をご覧下さい。

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、そのインターフェースにおいて 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、そのインター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、そのインター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

XR-410/TX2-L2 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。

<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。

XR-410/TX2-L2 のインター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

II. 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、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21章参照)。

[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。

XR-410/TX2-L2 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ていますので、「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]

XR-410/TX2-L2 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 XR-410/TX2-L2 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、XR-410/TX2-L2 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 XR-410/TX2-L2 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)の設定」をクリックして、以下の画面で設定します。

VLANの設定の保存								
No.	dev.Tag ID	enable	IPアドレス	ネットマスク	MTU	ip masq	spi	drop log
1	eth0.	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

(Ether0 ポートの表示例です)

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>」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インスペクションが有効となります。

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。

第 6 章

PPPoE 設定

第6章 PPPoE 設定

I. 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あります）。

プロバイダ名	<input type="text"/>
ユーザーID	<input type="text"/>
パスワード	<input type="password"/>
DNS サーバ	<input checked="" 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る <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"/> 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 checked="" type="radio"/> 無効 <input checked="" type="radio"/> 有効(獎勵) 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。)

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、「」「」「（」「）」「|」「¥」等の特殊記号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。1～63 文字まで入力可能です。

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る」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た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。

I. 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。

II. 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。

回線状態	回線は接続されていません
接続先の選択	<input type="radio"/> 接続先1 <input checked="" 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 type="radio"/> 手動接続 <input checked="" 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

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。

RS232C 接続タイプ

PPPoE 接続では「通常」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 25 章「補足：フィルタのログ出力内容について」をご覧下さい。

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。「インターフェース設定」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。「インターフェース設定」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。

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 22 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下さい」欄で設定します。

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

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ーフェースを選択します。

RS232C/BRI 接続タイプ

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。**

III. 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下さい」欄で設定します。

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 type="radio"/> 無効 <input checked="" 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 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
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	[入力欄]
Ping使用時の送信元アドレス	[入力欄]
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 [入力欄]
IPSEC+Ping使用時のIPSECポリシーのNO	[入力欄]
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ーフェースを選択します。

RS232C/BRI 接続タイプ

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25章「補足：フィルタのログ出力内容について」をご覧下さい。

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。

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 が返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。

III. 副回線とバックアップ回線

Ping 使用時の device

ping を使用する際の、ping を発行する回線(インターフェース)を選択します。「その他」を選択して、インター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 12 章 IPsec 設定」や IPsec 設定ガイドをご覧下さい。

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、「接続接定」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。**

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。

これはユーザー側が 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)	<input type="checkbox"/> 回線接続時に前回の PPPoE セッションの PADT を強制送出
	<input type="checkbox"/> 非接続 Session の IPv4Packet 受信時に PADT を強制送出
	<input type="checkbox"/> 非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出

回線接続時に前回の PPPoE セッションの PADT を強制送出する。

非接続 Session の IPv4Packet 受信時に PADT を強制送出する。

非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出する。

の動作について

XR 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、XR 側から強制的に PADT を送出してセッションの終了を網側に認識させます。その後、XR 側から再接続を行います。

、 の動作について

XR が LCP キープアライブ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 XR が受信すると、XR が PADT を送出してセッションの終了を網側に認識させます。その後、XR 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 接続ができなってしまった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-232 ポートを使った接続
(リモートアクセス機能)

第7章 RS-232 ポートを使った接続(リモートアクセス機能)

I. XR-410/TX2-L2 とアナログモデム /TA の接続

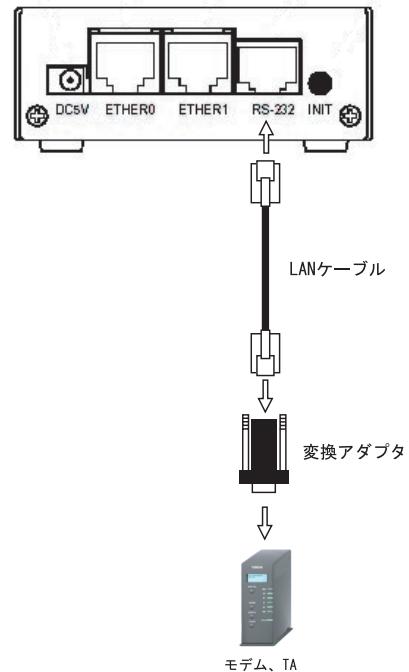
XR-410/TX2-L2 は、RS-232 ポートを搭載しています。これらの各ポートにアナログモデムやターミナルアダプタを接続し、XR-410/TX2-L2 の PPP 接続機能を使うことでリモートアクセスが可能となります。

また XR-410/TX2-L2 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

- 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たら、モデムの電源を投入してください。

接続図



第7章 RS-232ポートを使った接続(リモートアクセス機能)

II. 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ないます。

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 checked="" 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"/> 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PnP-Gatewayに発行します
Un Numbered-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
ダイアルタイムアウト	60 <input type="text"/> 秒
初期化用ATコマンド	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	180 <input type="text"/> 秒
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

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。1～63文字まで入力可能です。

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。

II. リモートアクセス回線の接続先設定

ダイアルタイムアウト

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、発信するときに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

回線のダイアル方法を選択します。

ON-DEMAND 接続用切断タイマー

PPP 接続設定の RS232C 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、
PPP 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 の接続設定を行ないます。

第7章 RS-232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。

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

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「RS232」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接続タイプ

「通常」は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を有効にするかどうかを選択します。

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。「インターフェース設定」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。「インターフェース設定」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。

IV. 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(注)
- ・フレッツ ADSL での接続と、ISDN 接続(リモートアクセス)を同時におこなう

(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」と呼ばれることがあります。

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すが、マルチ接続 (#2 ~ #4) では設定できませんので、ご注意下さい。

- ・デフォルトルートとして指定する
- ・接続 IP アドレス変更のお知らせメールを送る
- ・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・スクエアやフレッツ・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。したがいまして、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。

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。

この機能を利用する場合は以下のステップに従つて設定して下さい。

STEP 1 主接続の接続先設定

1 つ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 章または第 7 章をご覧ください。

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 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。設定方法については、第6章をご参照ください。

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、主接続を使うことになります。

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。

回線状態	回線は接続されていません
接続先の選択	<input type="radio"/> 接続先1 <input checked="" 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 type="radio"/> 手動接続 <input checked="" 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

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、本装置のインター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。

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。

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

デフォルトルート

「有効」を選択します。

接続 IP 変更お知らせメール

任意で設定します。

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]

以下の部分で設定します。

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

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、本装置のインター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ーフェースを選択します。

RS232C 接続タイプ

RS232C 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。

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

複数アカウント同時接続の設定

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」に赤文字で表示されます。

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。

などと表示されます。

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 キャッシュ機能」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

Web設定画面「各種サービスの起動・停止・設定」をクリックすると、以下の画面が表示されます。

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	
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	

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、以下のページを参照してください。

[DNSサーバ機能](#)

[IPsec機能](#)

[ダイナミックルーティング機能](#)

[L2TPv3機能](#)

[SYSLOG機能](#)

[SNMPエージェント機能](#)

[NTPサービス](#)

[アクセスサーバ機能](#)

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」を選択して画面最下部にある「動作変更」ボタンをクリックすることで、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、各項目の右側に表示されます。

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

各種サービス設定画面の「DNS サーバ」を起動させてください。

DNS サーバが「停止」のときは、DNS リレー機能も停止します。

DNS キャッシュ機能

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

<input type="checkbox"/> DNS キャッシュを使用する	<input checked="" type="radio"/> 使用しない	<input type="radio"/> 使用する
以下は DNS キャッシュを使用する際に設定して下さい。		
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"/>	

DNS キャッシュ機能の ON/OFF を選択します。
また DNS キャッシュ機能を使う場合は、ISP から指定されたもの、もしくは任意の DNS サーバの IP アドレスを指定してください。

DNS のキャッシュについて

本装置は、DNS リレー・DNS キャッシュのどちらでも DNS の結果をキャッシュします。

設定によるキャッシュの動作は以下のようになります。

- ・「(DNS キャッシュを)使用する、(DNS)サーバ指定あり」の設定の場合。
指定 DNS が解決した情報を XR がキャッシュします。
- ・「使用する、サーバ指定なし」の組み合わせでは設定できません。
- ・「使用しない、サーバ指定あり」の設定の場合。
XR がキャッシュオンリーサーバとなります。
XR 自身が名前解決した情報のみキャッシュします。
- ・「使用しない、サーバ指定なし」の設定の場合。
XR がキャッシュオンリーサーバとなります。
XR 自身が名前解決した情報のみキャッシュします。

設定後に「設定の保存」をクリックして設定完了です。

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

第11章 IPsec機能

I. 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。

他の機器との接続実績について

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

認証方式について

XR-410/TX2-L2 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。XR-410/TX2-L2 暗号化はソフト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

XR-410/TX2-L2 は ESP の認証機能を利用していますので、AH での認証はおこなっていません。

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 抱点まで 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。

FutureNet XR VPN Client との接続において、NAT トラバーサルに対応しています。

III. 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

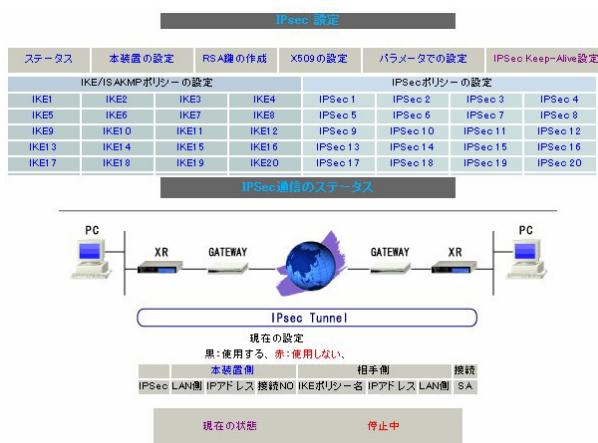
IPsec起動後に、正常にIPsec通信ができるかどうかを確認します。「情報表示」画面でのインターフェースとルーティングテーブル、ログで確認します。

第11章 IPsec機能

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

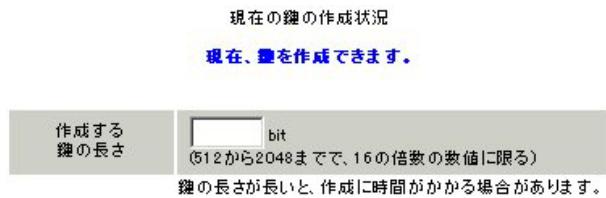
IPsec に関する設定・確認は、全てこの設定画面からおこなえます。

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。

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。

インターフェース	MTU値
主回線 使用時の ipsec インターフェイスの MTU 値	1500
マルチ#1回線 使用時の ipsec インターフェイスの MTU 値	1500
マルチ#2回線 使用時の ipsec インターフェイスの MTU 値	1500
マルチ#3回線 使用時の ipsec インターフェイスの MTU 値	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	1500
Ether0 ポート 使用時の ipsec インターフェイスの MTU 値	1500
Ether1 ポート 使用時の ipsec インターフェイスの MTU 値	1500

機能	状態
NAT Traversal	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
Virtual Private 設定	（空欄）

表示	内容
本装置の RSA 鍵 (PSK を使用する場合は 必要ありません)	（空欄）

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 トランザ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 トランザ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 トランザ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	（空欄）
上位ルータの IP アドレス	（空欄）
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

[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。

上位ルータの IP アドレス

本装置から見て 1 つ上位のルータ(ゲートウェイ)の IP アドレスを入力します。

[固定アドレスの場合]

上位ルータの IP アドレスをそのまま入力します。PPP/PPPoE 接続の場合は「%ppp0」と入力してください。

[動的アドレスの場合]

空欄のままにします。

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(aggressive モードで接続する場合)は、インターフェースの ID を設定します(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。

III. IPsec設定

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:@vr.centurysys)
モードの設定	main モード
transformの設定	1番目:すべてを送信する 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 (0.081~28800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	Certificate: Data: Version: 3 (0x2) Serial Number: 8 (0x8) Signature Algorithm:

(画面は表示例です)

IKE/ISAKMP ポリシー名

設定名を任意で設定します。(省略可)

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。

上位ルータの IP アドレス

相手側装置から見て1つ上位のルータ(主にゲートウェイ)IPアドレスを入力します。
本装置への 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]

上位ルータの IP アドレスをそのまま入力します。

相手側装置が PPP、PPPoE 接続の場合は、空欄にしておきます。

[相手側装置が動的アドレスの場合]

空欄のままにします。

インターフェースの 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る場合に限り、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。

(次ページに続きます)

III. IPsec設定

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。

[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、相手側の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」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			
<input type="text"/> (例: 192.168.0.0/24)			
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			
<input type="button" 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"/> 秒 (1081~86400秒まで)			
SAのライフタイム			
<input type="text"/> (1~255まで)			
DISTANCE			

(画面は表示例です)

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。XR-410/TX2-L2 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は、本値を選択して下さい。
 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下さい。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 XR-410/TX2-L2 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。

但し、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(PerfectForwardSecrecy)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。

(次ページに続きます)

第11章 IPsec機能

III. IPsec設定

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 を接続相手に送ります。

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 XR-410/TX2-L2 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、XR-410/TX2-L2 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 XR-410/TX2-L2 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。

サービス名	停止	起動	動作中	動作変更
DNS サーバ	<input type="radio"/>	<input checked="" type="radio"/>	動作中	動作変更
IPsec サーバ	<input checked="" type="radio"/>	<input type="radio"/>	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	
L2TPv2	<input checked="" type="radio"/>	<input type="radio"/>	停止中	動作変更
SYSLOG サービス	<input type="radio"/>	<input checked="" type="radio"/>	動作中	動作変更
SNMP サービス	<input checked="" type="radio"/>	<input type="radio"/>	停止中	動作変更
NTP サービス	<input checked="" type="radio"/>	<input type="radio"/>	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

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。

起動する IKE/ISAKMP ポリシー、IPsec ポリシーが増えるほど、IPsec の起動に時間がかかります。起動が完了するまで数十分かかる場合もあります。

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 "xriplsec1" #1: STATE_MAIN_I4: ISAKMP SA  
established . . .(1)
```

及び

```
Aug 1 12:00:20 localhost ipsec_plutorun:  
004 "xriplsec1" #2: STATE_QUICK_I2: sent QI2,  
IPsec SA established . . .(2)
```

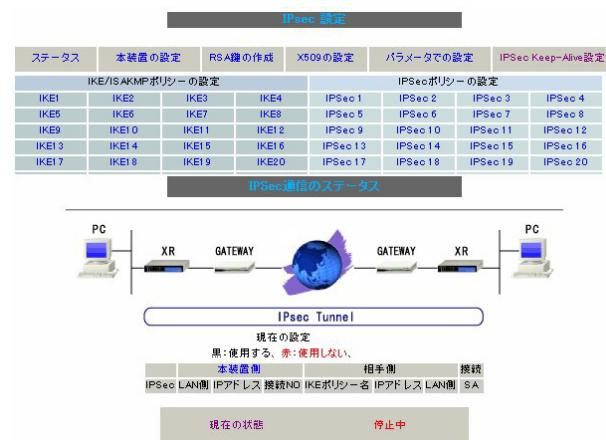
上記2つのメッセージが表示されていれば、IPsecが正常に接続されています。

(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見ています。

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。



(画面は表示例です)

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。

IV. IPsec Keep-Alive機能

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	interface	slave SA	remove?
1	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>			30	6	180	<input type="checkbox"/>	ipsec0	<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による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。IPsecが最初に確立する前にpingが失敗してもなにもしません。またdelayは初回のみ発生します。

interface

Keep-Alive機能を使う、本装置のIPsec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」をご参照下さい。

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、ここで指定したIPsecポリシー設定をbackup SAとして起動させます。

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。

複数のIPsecポリシーを設定することも可能です。その場合は、”_”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

(次ページに続きます)

IV. IPsec Keep-Alive機能

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Keep-AliveのPolicy 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下さい。

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="text"/>

X509の設定

X.509の使用 / 不使用を選択します。

証明書のパスワード

証明書のパスワードを入力します。

第11章 IPsec機能

V. 「X.509 デジタル証明書」を用いた電子認証

[CAの設定]

ここには、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('cacert.pem'ファイル等)。

[本装置側の証明書の設定]

ここには、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]

ここにはデジタル証明書と一緒に発行された、本装置の秘密鍵の内容をコピーして貼り付けます('cakey.pem'ファイル等)。

[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('crl.pem'ファイル等)。

[その他の設定について]

「IKE/ISAKMP ポリシーの設定」画面内の「鍵の設定」項目は「RSAを使用する」にチェックします。さらにその下の「X.509」設定で、IPsec通信をおこなう場合は、相手側のデジタル証明書をテキストボックス内に貼り付けます。

その他の設定については、通常のIPsec設定と同様にしてください。

以上でX.509の設定は完了です。

[設定のバックアップ保存について]

設定のバックアップを作成しても、X.509関連の設定は含まれません。またパラメータによる設定にも反映されません。

バックアップファイルから設定を復帰させる場合でも、X.509関連の設定は再度おこなってください。

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>

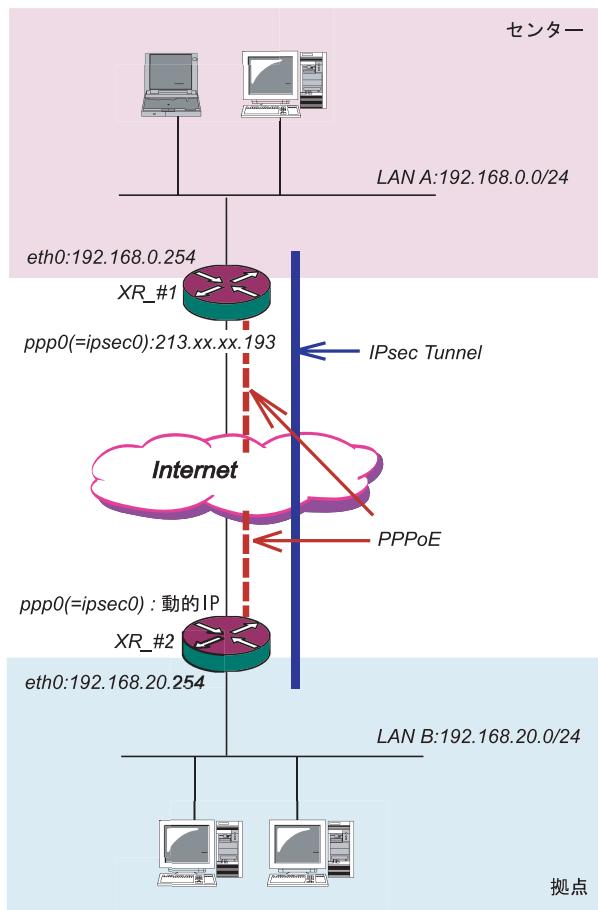
No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG	削除
1	ppp0	パケット受信時	許可	udp				500	<input type="checkbox"/>	<input type="checkbox"/>
2	ppp0	パケット受信時	許可	esp					<input type="checkbox"/>	<input type="checkbox"/>

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)

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>



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。

<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。

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	
<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)

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下さい。

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。

「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		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		(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」
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。

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	%ppp0
上位ルータのIPアドレス	[空欄]
インターフェースのID	@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
にして下さい。

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」

「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	213.xx.xx.193
上位ルータのIPアドレス	[空欄]
インターフェースのID	[空欄] (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
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

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。

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)

「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="button" 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="button" 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="button" 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"/> (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」

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。

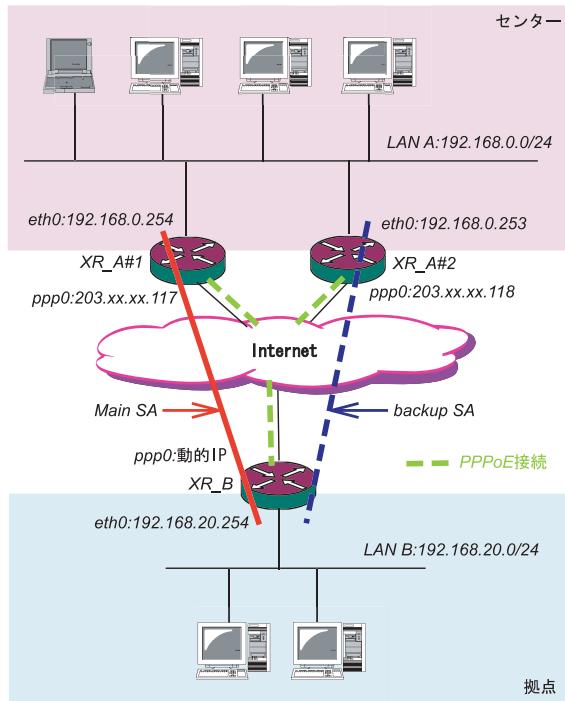
backupSA 「空欄」

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	
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	

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。

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	(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」

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)

「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下さい。

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
ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.254			

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。

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下さい。

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
ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.254			

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。

「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。

XR_A#1のスタティックルート設定

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>
192.168.20.0	255.255.255.0		192.168.0.253 20

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。

XR_A#2のスタティックルート設定

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>
192.168.20.0	255.255.255.0		192.168.0.254 20

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。

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 とも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	%ppp0
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)

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
にして下さい。

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。

メインSA用のIKE/ISAKMPポリシーの設定を行
います。

「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	203.xx.xx.117
上位ルータのIPアドレス	
インターフェースのID	
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

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。

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)

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 ポリシーの設定」

「IKE2」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	203.xx.xx.118
上位ルータのIPアドレス	
インターフェースのID	(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

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。

メイン SA 用の IPsec ポリシーの設定を行います。

「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 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。

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)

バックアップ SA用のIPsecポリシーの設定を行います。

「IPSecポリシーの設定」

「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
使用的 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」を選択して下さい。

使用的 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。

「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	30	3	60	<input checked="" type="checkbox"/>	ipsec0	2	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	192.168.20.254	192.168.0.253	30	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。

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」

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下さい。

IX. IPsecがつながらないとき

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。

これらのログやメッセージ内に

- ISAKMP SA established
- IPsec SA established

[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
```

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

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 通信のパケット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 のパケットを通すフィルタ設定は、「IV. 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しました。

固定 IP - 動的 IP 間での main モード接続と aggressive モード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 アドレスが分からぬいために、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 XR-410/TX2-L2 には IPsec のログが出ているのに、こちらの XR-410/TX2-L2 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 XR-410/TX2-L2 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」をクリックして下さい。ここに現在の IPsec の状況が表示されます。

第 12 章

ダイナミックルーティング
(RIP と OSPF の設定)

第12章 ダイナミックルーティング

I. ダイナミックルーティング機能

XR-410/TX2-L2シリーズのダイナミックルーティング機能は、RIP および OSPF 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

- 1 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。

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

- 2 「RIP」、「OSPF」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。

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。

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	120 (1-255) デフォルト120
OSPFルートの再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
再配信時のメトリック設定	<input type="text" value=""/> (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" value=""/> (0-16) 指定しない場合は空白
default-information の送信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

Ether0、Ether1ポート

XR-410/TX2-L2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。

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.	インターフェース	方向	ネットワーク	編集 削除
現在設定はありません				

フィルターの追加

<input type="checkbox"/>	-----	-----	<input type="text"/> (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。

インターフェース

RIP フィルタを実行するインター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.	インターフェース	方向	ネットワーク	編集 削除
1	Ether0ポート	in-coming	192.168.1.0/24	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。

III. 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。

インターフェースへの OSPF エリア設定

どのインターフェースで OSPF 機能を動作させるかを設定します。

設定画面上部の「インターフェースへの 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		
2		
3		
4		
5		
6		
7		
8		
9		
10		

ネットワークアドレス

XR-410/TX2-L2 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	(0-4294967295)
スタブ設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
トータリースタブ設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
default-cost	(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	

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。

トータリースタブ設定

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していします。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	192.168.1.0/29	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	(0-4294967295)
Remote-ABR Router-ID設定	(例:192.168.0.1)
Helloインターバル設定	10 (0-65535)
Deadインターバル設定	40 (0-65535)
Retransmitインターバル設定	5 (0-65535)
transmit delay設定	1 (0-65535)
認証パスワード設定	(英数字で最大8文字)
MD5 KEY-ID設定(1)	(0-255)
MD5 パスワード設定(1)	(英数字で最大16文字)
MD5 KEY-ID設定(2)	(0-255)
MD5 パスワード設定(2)	(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。

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。

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	Simple Password	MD5 KEY-ID	MD5 Password	Configure
1	192.168.0.1	10	40	5	1	aaa	111	bbb	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。

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およびIPSec接続先ルート再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 メトリックタイプ <input type="checkbox"/> 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="checkbox"/> 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="checkbox"/> 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 (1~255)"/>
Inter-areaルート Distance設定	<input type="text" value="1 (1~255)"/>
Intra-areaルート Distance設定	<input type="text" value="1 (1~255)"/>
Default-information	<input type="button" value="送信しない"/> メトリックタイプ <input type="checkbox"/> 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。

III. OSPF の設定

Default-information

デフォルトルートを 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った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を向けるように、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

各インターフェースごとのOSPF設定を行ないます。

設定画面上部の「インターフェース設定」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。

インターフェース名	eth0	gre No.	(1~64)
Passive-Interface設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効		
コスト値設定	[] (1~65535)		
帯域設定	[] (0~10000000kbps)		
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	[] (英数字で最大8文字)		
MDキ-ID設定(1)	[] (1~255)		
MD5パスワード設定(1)	[] (英数字で最大16文字)		
MDキ-ID設定(2)	[] (1~255)		
MD5パスワード設定(2)	[] (英数字で最大16文字)		
Priority設定	[] (0~255)		
MTU-Ignore設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効		

インターフェース名

設定するインターフェースを選択します。

Passive-Interface設定

インター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の送出間隔を設定します。

Transmit Delay設定

LSUを送出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)

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。

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。

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

設定後は「インターフェース設定」画面に、設定内容が一覧で表示されます。

インターフェース名	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)	<input type="button" value="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)	<input type="button" value="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)	<input type="button" value="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)	<input type="button" value="表示する"/>
インターフェース情報の表示 (表示したいインターフェースを指定して下さい)	<input type="button" value="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。

インターフェース情報の表示

現在のインターフェースの状態が表示されます。

第 13 章

L2TPv3 機能

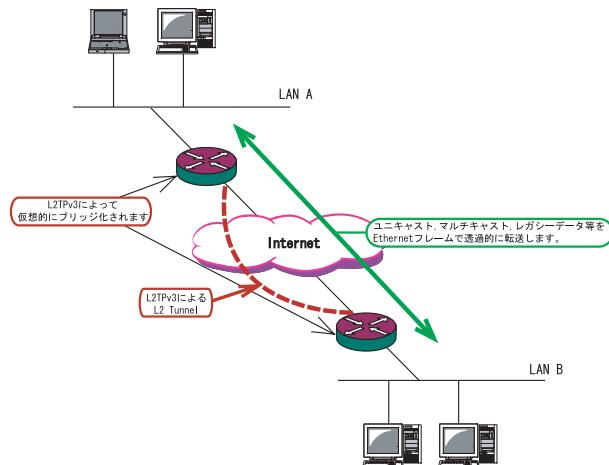
第13章 L2TPv3 機能

I. 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出来ます。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ます。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できます。

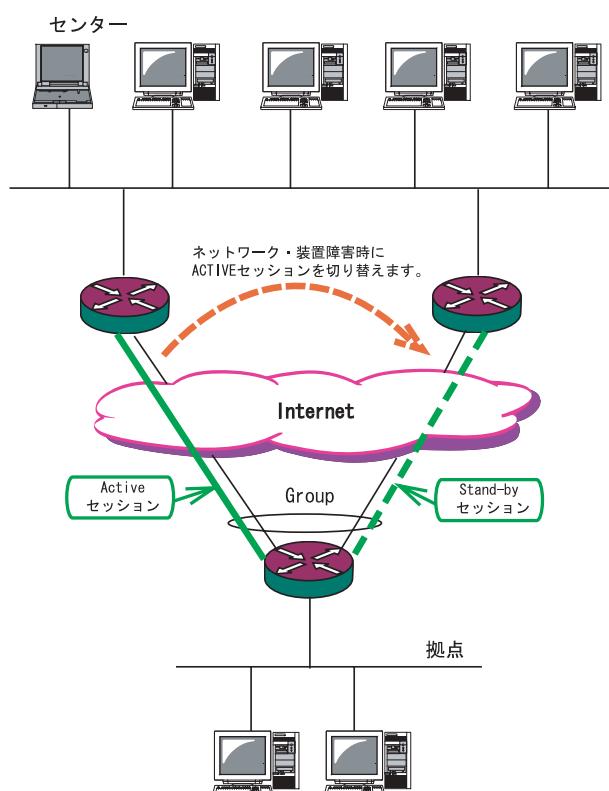
L2TPv3 セッションの二重化機能

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。



II.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。

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
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

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下さい。
(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。

Path MTU Discovery 設定

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、本装置が送信する 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。

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。

第13章 L2TPv3機能

III. L2TPv3 機能設定

(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、不要なトライ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。新規に設定を行うときは「New Entry」をクリックします。

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96文字まで)
AVP Hiding設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Digest Type設定	無効 <input type="button" value="▼"/>
Hello Interval設定	60 [0-1000s] (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	0 IETF 9:Cisco
Bind Interface設定	<input type="text"/>

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()

AVP Hidingを有効にするかを選択します。

Digest Type

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下さい。

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

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

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。

Vendor ID 設定

対向 LCCE のベンダー ID を設定します。「0」は IETF 機器(XR-410/TX2-L2、XR-640/CD-L2)、「9」は Cisco Router となります。

Bind Interface 設定

バインドさせる本装置のインターフェースを設定します。指定可能なインターフェースは「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。

()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 の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に使用するパラメータの設定を行います。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel 設定選択	---
L2Frame 受信インターフェース 設定	(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	[1-4294967295]
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
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

Tunnel 設定

「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 受信インターフェース 設定

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

Point to Multi-point 接続を行う場合は、1つのインターフェースに対し、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インターフェースとVLANインター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。

VLAN ID

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

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下さい。

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か対向 LCCE からのネゴシエーションによって再接続します。

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設定して下さい。

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下さい。

(次ページに続きます)

第13章 L2TPv3機能

IV. L2TPv3 Xconnect(クロスコネクト)設定

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。

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。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。

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。

Group ID	<input type="text" value="1~4095"/>
Primary Xconnect設定選択	---
Secondary Xconnect設定選択	---
Preempt設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Primary active時のSecondary Session強制切断設定	<input checked="" type="radio"/> 有効 <input 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下さい。設定可能な値は、1～4095の任意の整数値です。

Primary Xconnect設定

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

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。「有効」にする場合、「Preempt設定」も「有効」に設定して下さい。

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。

第13章 L2TPv3機能

VI. 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。



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」で設定したインター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

停止したいトンネル / セッションの ID または Remote Router ID を指定することで、該当するトンネル / セッションを終了します。

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。

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 を指定して下さい。

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ーフェースを選択して下さい。プルダウンには、「L2TPv3 Xconnect 設定」で設定したインターフェースが表示されます。

第13章 L2TPv3 機能

VII.L2TPv3 ステータス表示

L2TPv3の各種ステータスを表示します。

Xconnect Interface情報表示	---	表示する
MAC Table/FDB情報表示	---	表示する
	<input checked="" type="checkbox"/> local MAC Table表示 <input checked="" type="checkbox"/> FDB表示	
Tunnelステータス表示		表示する
Sessionステータス表示	Session ID	表示する
	<input checked="" type="checkbox"/> detail表示	
Groupステータス表示	Group ID ---	表示する
すべてのステータス情報表示		表示する

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。

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ーフェースを選択して下さい。

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下さい。

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。

Tunnel ステータス表示

L2TPv3 トンネルの情報のみを表示します。

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 を指定して下さい。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。

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下さい。選択しない場合は全てのグループの情報を表示します。

VIII. 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、下記を参照して下さい。

[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。

SCCRQ : 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示します。

SCCCN : Start-Control-Connection-Connected

SCCRQ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

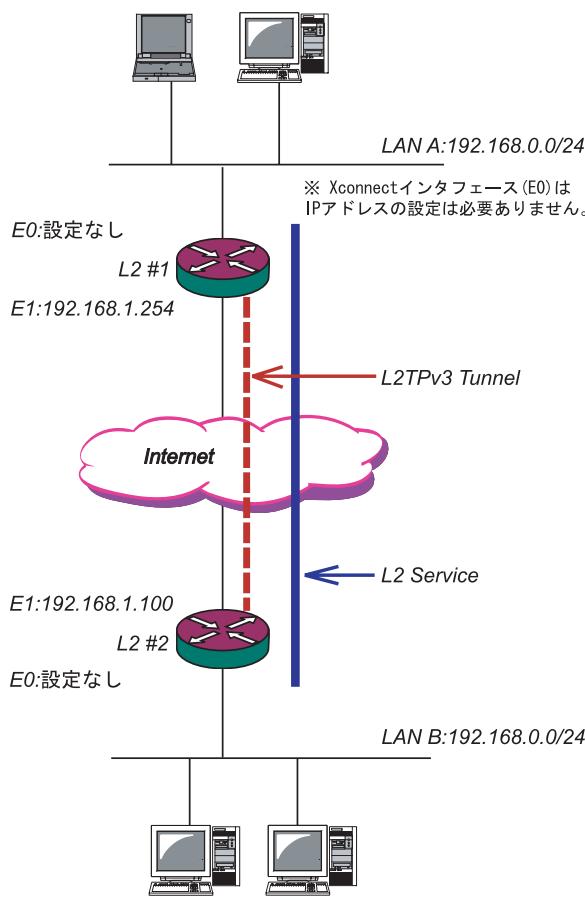
L2TPセッションの切断を要求するメッセージ。

第13章 L2TPv3機能

IX. L2TPv3 設定例1

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)



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 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 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	
			動作変更

L2 #1の設定

[L2TPv3機能設定]

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
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

- 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)。

[L2TPv3 Tunnel の設定]

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 [0-1000s] (default 60s)
Remote Hostname設定	L2-2
Remote RouterID設定	192.168.1.100
Vendor ID設定	0 0:IETF 9:Cisco
Bind Interface設定	

- 「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ときは、「Bind Interface」にPPPインターフェース名を設定します。

[L2TPv3 Xconnect Interface の設定]

Tunnel設定選択	192.168.1.100
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 [0-1000s] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="checkbox"/> 有効 <input type="radio"/> 無効

第13章 L2TPv3機能

IX.L2TPv3 設定例1

L2 #2 の設定

[L2TPv3 機能設定]

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
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 Tunnel の設定]

Description	sample
Peerアドレス	192.168.1.254 (例192.168.0.1)
パスワード	(英数字96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 [0-1000s] (default 60s)
Remote Hostname設定	L2-1
Remote RouterID設定	192.168.1.254
Vendor ID設定	0 IETF 9:Cisco
Bind Interface設定	

[L2TPv3 Xconnect Interfaceの設定]

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 [0-1000s] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

L2TPv3TunnelSetup の起動

設定後は「起動 / 停止設定」画面に移ります。

L2TPv3接続を開始するときは「起動」にチェックを入れ、Xconnect Interfaceを選択します。そして「実行」ボタンをクリックしてください。

The screenshot shows the 'Tunnel Setup' section of the configuration interface. The '起動' (Start) button is checked. The 'Xconnect Interface' dropdown is set to 'eth0'. The 'Remote-ID選択' (Remote-ID Selection) dropdown is set to '192.168.1.254'. There are several other options available but are not selected.

Xconnect Interfaceは、L2TPv3接続に関連付けるインターフェースを選択します。

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。

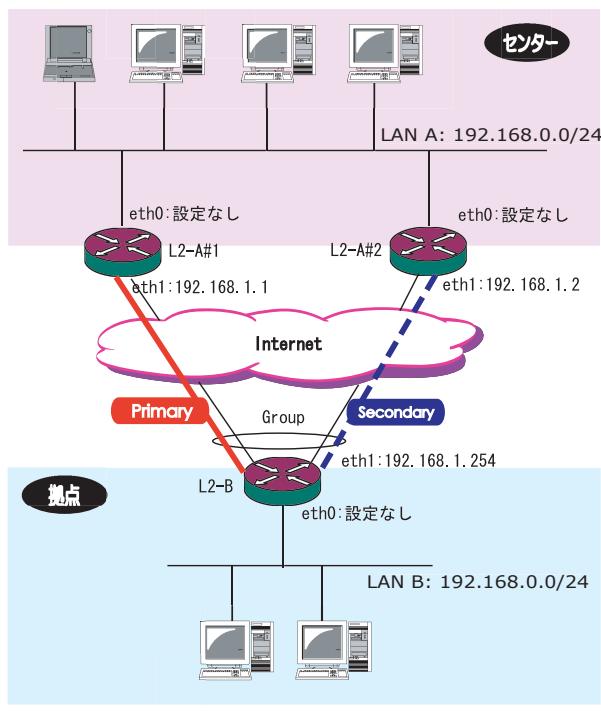
第13章 L2TPv3機能

X. 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)



L2-A#1/L2-A#2(センター側)の設定

[L2TPv3機能設定](Primaryルータ L2-A#1)

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
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

- 「Local HostName」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。

[L2TPv3機能設定](Secondaryルータ L2-A#2)

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
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ルータと同じ要領で設定して下さい。

第13章 L2TPv3 機能

X.L2TPv3 設定例2 (L2TP トンネル二重化)

[L2TPv3 Tunnel 設定](Primary ルータ L2-A#1)

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 [0-1000s] (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	0 IETF 9:Cisco
Bind Interface設定	

- 「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。

[L2TPv3 Tunnel 設定](Secondary ルータ L2-A#2)

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 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 [0-1000s] (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	0 IETF 9:Cisco
Bind Interface設定	

- Primary ルータと同じ要領で設定して下さい。本例の場合、Primary ルータと同じ設定になります。

[L2TPv3 Xconnect 設定](Primary セッション側)

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
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

- 「Xconnect ID 設定」は Group 設定を行わないでの設定不要です。
- 「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下さい。

[L2TPv3 Xconnect 設定](Secondary セッション側)

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	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
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

- Primary ルータと同じ要領で設定して下さい。
- 「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]

- Primary、Secondary ルータともに、L2TP セッションの Group 化は行ないので、設定の必要はありません。

第13章 L2TPv3機能

X.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]

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
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

- 「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。

[L2TPv3 Tunnel 設定](Primaryセッション側)

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 [0-1000s] (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	0 0:IETF 9:Cisco
Bind Interface設定	

- 「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。

[L2TPv3 Tunnel 設定](Secondaryセッション側)

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 checked="" type="radio"/> 有効 <input type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000s] (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	0 0:IETF 9:Cisco
Bind Interface設定	

- Primary セッションと同じ要領で設定して下さい。

第13章 L2TPv3機能

X.L2TPv3 設定例2 (L2TP トンネル二重化)

[L2TPv3 Xconnect 設定](Primary セッション側)

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	60 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
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

- 「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下さい。
- 「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 時間を設定して下さい。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。

[L2TPv3 Xconnect 設定](Secondary セッション側)

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 Hidne設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000s] (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	0 IETF 9.Cisco
Bind Interface設定	

- Primary セッションと同じ要領で設定して下さい。

[L2TPv3 Group 設定]

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

- 「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 セッションを同時に Active 化します。

L2TPv3 Tunnel Setup の起動

設定後は「起動 / 停止設定」画面に移ります。

L2TPv3 接続を開始するときは「起動」にチェックを入れ、Xconnect Interface を選択します。そして「実行」ボタンをクリックしてください。

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。

第 14 章

SYSLOG 機能

第14章 syslog機能

syslog機能の設定

XR-410/TX2-L2は、syslogを出力・表示することができます。また、他のsyslogサーバに送出することもできます。

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。



<syslog機能設定>

「ログの取得」項目で設定します。

「取得する」

XR-410/TX2-L2でsyslogを取得する場合に選択します。

「他のsyslogサーバに送信する」

syslogを他のサーバに送信するときに選択します。このとき、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以下のようになります。

- ・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。

初期設定は20分です。

XR-410/TX2-L2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。

ファシリティと監視レベルについて

XR-410/TX2-L2シリーズで設定されているsyslogのファシリティ・監視レベル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

第 15 章

SNMP エージェント機能

第15章 SNMPエージェント機能

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XR-410/TX2-L2のMIB Ver.2(RFC1213)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。

SNMPマネージャ	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ください。
コミュニティ名	community
SNMP TRAP	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
SNMP TRAPの送信先IPアドレス	
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"/>

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。

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。

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。

SNMP TRAPの送信元

「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。

「インターフェース」を選択した場合

SNMP TRAPの送信元アドレスとなるインターフェース名を指定します。指定可能なインターフェースは、本装置のイーサネットポートとPPPインターフェースのみです。

入力が終わったら「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。

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)

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インターフェースの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

第 16 章

NTP サービス

NTPサービスの設定方法

XR-410/TX2-L2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。

問合せ先NTPサーバ(IPアドレス, URL)	設定1 <input type="text"/>
	設定2 <input type="text"/>

NTPサーバのIPアドレスもしくはURLを「設定「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、XR-410/TX2-L2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URLを入力しない場合は、XR-410/TX2-L2はNTPサーバとしてのみ動作します。

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。**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。**

基準NTPサーバについて

基準となるNTPサーバには以下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) サーバをドメイン名で指定するときは、各種サービス設定の「DNSサーバ」を起動しておきます。

NTPサービスの動作について

NTPサービスが起動したときは64秒間隔でNTPサーバとポーリングをおこないます。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補正していきます。

NTPクライアントの設定方法

各ホスト／サーバーをNTPクライアントとしてXR-410/TX2-L2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下さい。

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社にお問い合わせ下さい。

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下さい。

第 17 章

アクセスサーバ機能

第17章 アクセスサーバ機能

I. XR-410/TX2-L2 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。

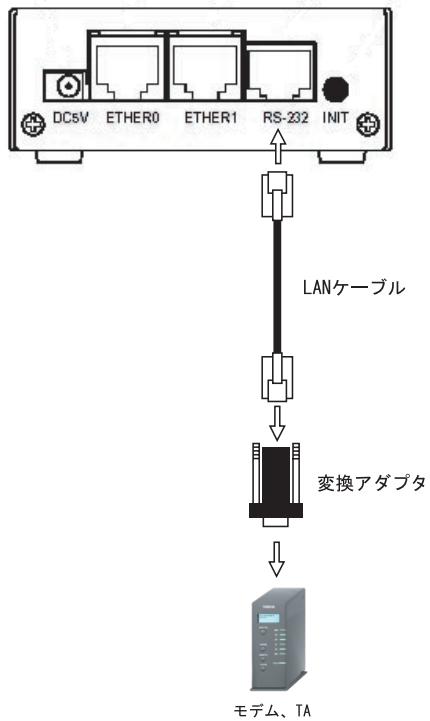
アナログモデム /TA の接続

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たら、モデム /TA の電源を投入してください。

接続図



第17章 アクセスサーバ機能

II. アクセスサーバ機能の設定

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	192.168.253.254
クライアントのIPアドレス	192.168.253.170
モデムの速度	<input type="radio"/> 9600 <input checked="" 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	[]

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

XR-410/TX2-L2 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。

モデムの速度

XR-410/TX2-L2 とモデムの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。

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	削除
1	[]	[]	<input type="checkbox"/>
2	[]	[]	<input type="checkbox"/>
3	[]	[]	<input type="checkbox"/>
4	[]	[]	<input type="checkbox"/>
5	[]	[]	<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。5アカウントまで登録しておけます。

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。

アカウント設定観の「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。設定後は、外部からダイヤルアップ接続を行なってください。

外部からダイヤルアップ接続されていないときには、「各種サービスの設定」画面の「アクセスサーバ」が「待機中」の表示となります。

アカウント設定上の注意

ユーザーアカウント設定のユーザー名と、PPP/PPPoE 設定の接続先設定で設定してあるユーザー名に同じユーザ名を登録した場合、そのユーザは**着信できません**。

ユーザー名が重複しないように設定して下さい。

第 18 章

スタティックルート設定

第18章 スタティックルート設定

スタティックルート設定

XR-410/TX2-L2 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 checked="" type="checkbox"/>
2	192.168.20.1	255.255.255.0	gre1		<input checked="" 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、あて先アドレスを单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。

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」をご参照下さい。

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ルー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つずつ設定番号がズ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。

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。

スタティックルート設定

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 19 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すが、ソースルート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」をご参照下さい。

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。FQDN での設定も可能です。

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XR-410/TX2-L2のインターフェースが含まれていると、設定後はXR-410/TX2-L2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XR-410/TX2-L2の設定画面にアクセスできなくなります。

第 20 章

NAT 機能

I. XR-410/TX2-L2 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。

XR-410/TX2-L2 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XR-410/TX2-L2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になります。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な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。

II. 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			全て			<input type="checkbox"/>
2			全て			<input type="checkbox"/>
3			全て			<input type="checkbox"/>
4			全て			<input type="checkbox"/>
5			全て			<input type="checkbox"/>
6			全て			<input type="checkbox"/>
7			全て			<input type="checkbox"/>
8			全て			<input type="checkbox"/>
9			全て			<input type="checkbox"/>
10			全て			<input type="checkbox"/>
11			全て			<input type="checkbox"/>
12			全て			<input type="checkbox"/>
13			全て			<input type="checkbox"/>
14			全て			<input type="checkbox"/>
15			全て			<input type="checkbox"/>
16			全て			<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。						
			全て			

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。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」をご参照下さい。

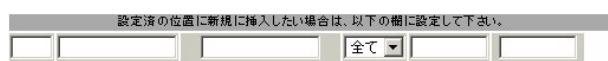
入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

"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。



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="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"/>
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="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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 側コンピューターのプライベート 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」をご参照下さい。

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。



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。

第20章 NAT機能

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側のコンピューター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
192.168.0.0/24	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 192.168.0.0/24 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下さい。

<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21章

パケットフィルタリング機能

第21章 パケットフィルタリング機能

I. 機能の概要

XR-410/TX2-L2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。
- ・XR-410/TX2-L2 自身が受信するパケットを制限する。
- ・XR-410/TX2-L2 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)
- ・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)、ポート番号に基づいてパケットを通過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、コンピューター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ー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。

第21章 パケットフィルタリング機能

II.XR-410/TX2-L2 のフィルタリング機能について

XR-410/TX2-L2は、以下の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。

- ・転送(forward)
- ・入力(input)
- ・出力(output)
- ・ゲートウェイ認証フィルタ

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、XR-410/TX2-L2で内部転送する(XR-410/TX2-L2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。

入力(input)フィルタ

外部からXR-410/TX2-L2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XR-410/TX2-L2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。

出力(output)フィルタ

XR-410/TX2-L2内部からインターネットやLANなど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「XR-410/TX2-L2自身へのアクセス」か「XR-410/TX2-L2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おこないます。

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。

本製品の工場出荷設定では、Ether0ポート以外はステートフルパケットインスペクション機能が有効になっています。この機能により、Ether0ポート以外からXR-410/TX2-L2自身、またLAN内へのアクセスは一切できないようになっています。

unnumbered接続やバーチャルサーバ機能によるサーバ公開を運用される場合は、ステートフルパケットインスペクション機能を無効にするかパケットフィルタリングの設定を行い、外部からLANへのアクセスを許可する設定を行ってください。

第21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・出力フィルタの3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」のいずれかをクリックして、以下の画面から設定します。

No.	インターフェース	方向	動作	プロトコル	通信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG	削除
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				
5	eth1	パケット受信時	破棄	udp				1900		
6	ppp0	パケット受信時	破棄	tcp				1900		
7	eth1	パケット受信時	破棄	tcp				5000		
8	ppp0	パケット受信時	破棄	tcp				5000		
9	eth1	パケット受信時	破棄	tcp				2869		
10	ppp0	パケット受信時	破棄	tcp				2869		
11		パケット受信時	許可	全て						
12		パケット受信時	許可	全て						
13		パケット受信時	許可	全て						
14		パケット受信時	許可	全て						
15		パケット受信時	許可	全て						
16		パケット受信時	許可	全て						

(画面は「転送フィルタ」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」をご参照下さい。

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。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>

单一のIPアドレスを指定する：

192.168.253.19/32 ("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)

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、FQDNでの指定が可能です。

入力方法は、送信元IP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。

(次ページに続きます)

III. パケットフィルタリングの設定

入力が終わったら「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。

送信元 / あて先アドレスを FQDN で設定したときは、本装置の DNS サーバ機能が「起動」している必要があります。
また本装置がインターネットに接続できるようになっている必要があります。
いずれも本装置が名前解決をおこなうためです。本装置を再起動したときなど、タイミングによっては名前解決ができずに FQDN での設定が正しく動作しない場合には、本装置がインターネットに接続していることを確認し、「設定の保存」ボタンを再度クリックしてください。

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。



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21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。
- XR-410/TX2-L2 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。
- ステートフルインスペクションは無効とする。

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 「192.168.0.1」

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。

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
eth1	パケット受信時	許可	tcp				1024:65535
eth1	パケット受信時	許可	udp				1024:65535
eth1	パケット受信時	破棄	全て				

「入力フィルタ」で以下のように設定します。

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
eth1	パケット受信時	許可	tcp				1024:65535
eth1	パケット受信時	許可	udp				1024:65535
eth1	パケット受信時	破棄	全て				

フィルタの解説

「転送フィルタ」「入力フィルタ」

No.1 :

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.2 :

上記の条件に合致しないパケットを全て破棄する。

第21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。

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」
- ステートフルインスペクションは無効とする。

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。

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
eth1	パケット受信時	許可	tcp			192.168.0.1/32	80
eth1	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
eth1	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
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 :

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 :

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。

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」
- ステートフルインスペクションは無効とする。

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。

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
ppp0	パケット受信時	許可	tcp			192.168.0.2/32	21
ppp0	パケット受信時	許可	tcp			192.168.0.2/32	20
ppp0	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
ppp0	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
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、あて先ポートが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下さい。

第21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 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。
- ステートフルインスペクションは無効とする。

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」
- 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。

インターフェース	方向	動作	プロトコル	通信元アドレス	通信元ポート	あて先アドレス	あて先ポート
ppp0	パケット受信時	許可	tcp			192.168.0.1/32	80
ppp0	パケット受信時	許可	tcp			192.168.0.2/32	25
ppp0	パケット受信時	許可	tcp			192.168.0.2/32	110
ppp0	パケット受信時	許可	tcp			192.168.0.3/32	21
ppp0	パケット受信時	許可	tcp			192.168.0.3/32	20
ppp0	パケット受信時	許可	tcp			192.168.0.4/32	53
ppp0	パケット受信時	許可	udp			192.168.0.4/32	53
ppp0	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
ppp0	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
ppp0	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 :

192.168.0.2 のサーバに SMTP と POP3 のパケットを通す。

No.4,5 :

192.168.0.3 のサーバに ftp と 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、あて先ポートが 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証するものではありませんのでご注意下さい。

第21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」

eth0	パケット受信時	破棄	tcp				137:139
eth0	パケット受信時	破棄	udp				137:139
eth0	パケット受信時	破棄	tcp		137		
eth0	パケット受信時	破棄	udp		137		

「転送フィルタ」

eth0	パケット受信時	破棄	tcp				137:139
eth0	パケット受信時	破棄	udp				137:139
eth0	パケット受信時	破棄	tcp		137		
eth0	パケット受信時	破棄	udp		137		

フィルタの解説

No.1 :

あて先ポートがtcpの137から139のパケットをEther0ポートで破棄する。

No.2 :

あて先ポートが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.2 :

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。

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
ppp0	パケット受信時	破棄	全			210.xxx.xxx.32/32	
ppp0	パケット受信時	破棄	全			210.xxx.xxx.47/32	

フィルタの解説

No.1 :

210.xxx.xxx.32(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.32のネットワークのブロードキャスト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下さい。

第21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。

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
ppp0	パケット受信時	破棄	全て	10.0.0.8			
ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
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。

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。

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
ppp0	パケット受信時	破棄	全て	10.0.0.8			
ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
ppp0	パケット受信時	破棄	全て	192.168.0.0/16			
ppp0	パケット受信時	破棄	全て			202.xxx.xxx.112/3	
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。

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
ppp0	パケット受信時	破棄	全て			10.0.0.8	
ppp0	パケット受信時	破棄	全て			172.16.0.0/16	
ppp0	パケット受信時	破棄	全て			192.168.0.0/16	

フィルタの解説

入力フィルタの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。

入力フィルタのNo.4,5 :

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

出力フィルタの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上にプライベートネットワーク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証するものではありませんのでご注意下さい。

第21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。

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
ppp0	パケット受信時	許可	tcp				1723
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」

したがいまして、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21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

ステートフルパケットインスペクションが有効となっていても、遠隔地から XR-410/TX2-L2 にログインして設定・制御をおこなうことができます。その場合は「入力フィルタ」で必要な設定をおこないます。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。

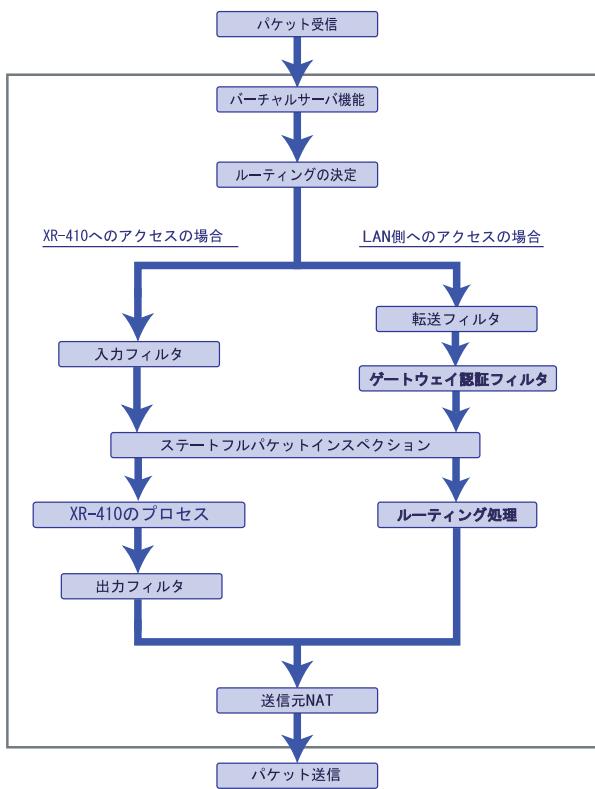
インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
ppp0	パケット受信時	許可	tcp	xxx.xxx.xxx.xxx			880

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 XR-410/TX2-L2 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、XR-410/TX2-L2 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)。

補足：NATとフィルタの処理順序について

XR-410/TX2-L2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。
- XR-410/TX2-L2 自身へのアクセスをフィルタするときは「入力フィルタ」、XR-410/TX2-L2 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)。
- 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 XR-410/TX2-L2 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「転送フィルタ」「入力フィルタ」を設定している場合は、先に「転送フィルタ」「入力フィルタ」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る)。

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

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。出力内容は以下のようになります。

<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: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イスが記されます。
OUT=	パケットを送出したインターフェイスが記されます。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。

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 22 章

仮想インターフェース機能

仮想インターフェースの設定

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。

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。
自由に設定できます。

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 23 章

GRE 機能

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。

インターフェースアドレス	<input type="text"/> (例192.168.0.1/30)
リモート(宛先)アドレス	<input type="text"/> (例192.168.1.1)
ローカル(送信元)アドレス	<input type="text"/> (例192.168.2.1)
PEERアドレス	<input type="text"/> (例192.168.0.2/30)
TTL	255 (1-255)
MTU	1476 (最大値1500)
Path MTU Discovery	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
TOS設定 (ECN Field設定不可)	<input checked="" type="radio"/> TOS値の指定 <input type="text"/> (0x0-0xfc) <input type="radio"/> inherit(TOS値のコピー)
GREoverIPSec	<input type="radio"/> 使用する <input type="text"/> ipsec0 <input checked="" type="radio"/> Routing Tableに依存
IDキーの設定	<input type="text"/> (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0 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。)

インターフェースアドレス

GREトンネルを生成するインター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ーフェースの仮想アドレスを設定します。「インターフェースアドレス」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。本機能を有効にした場合は、本装置が送信するGRE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。

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に依存」はGREトンネルを暗号化して使わないときに選択してください。

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

GREパケットの識別用のIDを設定します。

GRE の設定

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。



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 Addressee	Local Address	Peer Address	MTU	ID Key	Check sum	PMTU	Link State
gre1	192.168.0.1/30	192.168.1.1	192.168.2.1	192.168.0.2/30	1478	無効	有効		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 24 章

QoS 設定

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つのキューリング方式で、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リング

キューリングには、クラスフルなものとクラスレスなものがあります。

クラスレスなキューリングは、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リングです。

クラスフルなキューリングでは、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。またキューリ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リ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リングです。

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です。

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。トーカンバケツにトーカンを、ある一定の速度(トーカン速度)で収納していきます。このトーカン1個ずつがパケットを1個ずつつかみ、トーカン速度を超えない範囲でパケットを送信していきます(送信後はトーカンは削除されます)。

またバケツに溜まっている余分なトーカンは、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カンを使ってパケットを送信しますので、溜まった分のトーカンを使い切らないような短期的なバーストであれば、トーカン速度(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カンがすぐになくなってしま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になります。

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おこないません。

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リングを定義し、クラス内でのキューリングをおこなうこともできます(クラスキューリング)。

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。

II.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

すべてのキューリ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)	<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"/> byte
CBO Parameter設定	
回線帯域	<input type="text"/> Kbit/s
平均パケットサイズ	<input type="text"/> byte
PQ Parameter設定	
最大Band数設定	<input type="text"/> 3 default 3 (2~5)
Priority-map設定	<input type="text"/> 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"/>
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"/>

Interface名

キューリ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」をご参照ください。

Queueing Discipline

キューリング方式を選択します。

[pfifoの設定]

pfifo queue limit

パケットをキューリ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 Paramater 設定」について設定します。

制限 Rate

パケットにトーカ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。これは瞬間に利用できるトーカ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

トーカンを待っている状態でキューリングするときの、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10000kbit/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. [] 2. [] 3. [] 4. [] 5. [] 6. [] 7. [] 8. [] 9. [] 10. []

(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」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。

第24章 QoS機能

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 queuing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	<table border="1"><tr><td>1</td><td>2</td><td>2</td><td>2</td><td>1</td><td>2</td><td>0</td></tr></table>	1	2	2	2	1	2	0
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"/>							
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」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	2 (hex.0-fe)
<input type="checkbox"/> Marking情報によるフィルタ	
Mark値	(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。单一ホストを指定するときは<ホストIPアドレス>/32の形式で指定します。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24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。

設定番号	1
パケット分類条件	
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	1024-65535 (ポート番号/範囲指定:で番号連結)
宛先アドレス	10.10.10.10/32
宛先ポート	80 (ポート番号/範囲指定:で番号連結)
インターフェース	ppp1
TOS/MARK 値	<input checked="" type="radio"/> TOS <input type="radio"/> MARK <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)
TOS/MARK 値の設定	
設定対象	<input checked="" type="radio"/> TOS/Precedence <input type="radio"/> MARK
設定値	<ul style="list-style-type: none">・ MARK 設定 (1-999) <input type="text"/>・ TOS/Precedence 設定 選択して下さい <input type="button"/> TOS Bit 選択して下さい <input type="button"/> Precedence Bit

(画面は表示例です)

「ローカルパケット出力時の設定」か「パケット入力時の設定」をクリックして選択します。

[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。単一ホストを指定するときは<ホスト IP アドレス>/32の形式で指定します。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

インターフェースを選択します。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」を参照してください。

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。**

TOS/MARK 値

マッチングする TOS/MARK 値を指定します。TOS、MARK 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 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 値を設定します。

設定対象

TOS/Precedence、MARK のいずれかを選択します。

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 については章末をご参照下さい。

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。

Filter Type	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	Packet Head	host_1	1	6	192.168.0.1/32	10.10.10.10/32	80	0x2		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
 20: -> 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 -> 過負荷の状態で届いたパケット数

```
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 -> プライオリティ(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 -> EMWA 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、過負荷の状態では "0" 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/fffffff00 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/fffffff00 at 16
  match 00060000/00ff0000 at 8

  protocol -> マッチするプロトコル
  pref -> 優先度
  u32 -> パケットフィルタを参照してフィルタすることの宣言
  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ります。
                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 -> TOSまたはMARK値

classid -> マッチパケットを送るクラスID

クラスID 1:(n) のとき、100(n):に送られます。

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
 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。

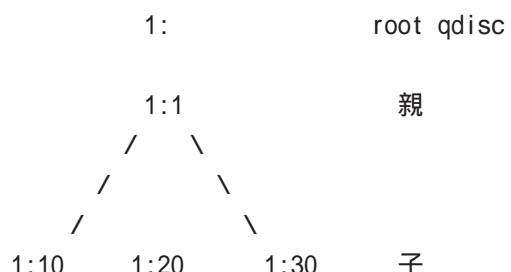
[クラス IDについて]

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)>



10: leaf

30: qdisc / \\"
 1001: 1002: leaf

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 Paramater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 Paramater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 25 章

ゲートウェイ認証機能

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

「はい」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

「はい」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」XR-410/TX2-L2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25章 ゲートウェイ認証機能

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)
○ 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

認証したからの、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.	ユーザーID	パスワード	削除
1			<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"/>

ユーザーID・パスワード

ユーザーID・パスワードを登録します。

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。

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="button" value="指定しない"/>
セッションタイムアウト	<input type="button" 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。RADUIS 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 XR-410/TX2-L2 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です。

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。フィルタ設定によって認証を必要とせずに通信可能になります。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 にて設定して下さい。**」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。

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
	パケット受信時	許可	全て				
	パケット受信時	許可	全て				

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21章 パケットフィルタリング機能**」をご参照下さい)。

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	<input checked="" type="radio"/> 使用しない	<input type="radio"/> syslogに取る
アクセスログ	<input checked="" type="radio"/> 使用しない	<input type="radio"/> 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
```

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くても、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、XR-410/TX2-L2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」の場合、HTTP Basic認証を使って認証されます。

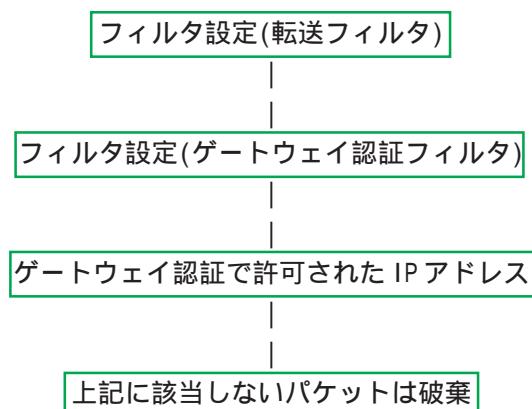
「RADIUSサーバ」の場合は、PAPで認証要求を送信します。

第25章 ゲートウェイ認証機能

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 26 章

ネットワークテスト

第26章 ネットワークテスト

ネットワークテスト

XR-410/TX2-L2 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。

Ping	<p>FQDNまたはIPアドレス</p> <input type="text"/> <p>インターフェースの指定(省略可)</p> <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 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</p> <input type="text"/> <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 checked="" 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"/> 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 高帯域下での使用は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>

ping テスト

指定した相手に XR-410/TX2-L2 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。

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 2.253 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 21.188 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下さい。

第26章 ネットワークテスト

ネットワークテスト

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。その他を選択し、直接インターフェース名を指定することもできます。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

「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。

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本書「付録A インタフェース名について」をご参照下さい。

「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」: ここに文字列を指定して、それに合致するダンプ内容のみを取得できます。空白・大小文字も判別します。一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したパケットダンプ内容のみ抽出して記録します。

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

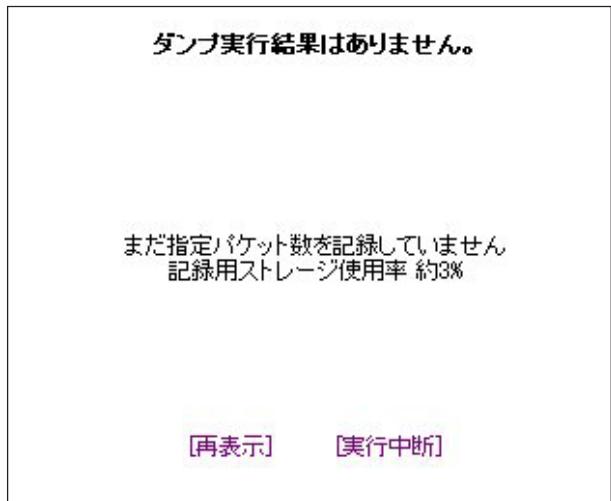
実行結果は即時出力できない場合があります。
[再表示]で確認して下さい

[再表示] [実行中断]

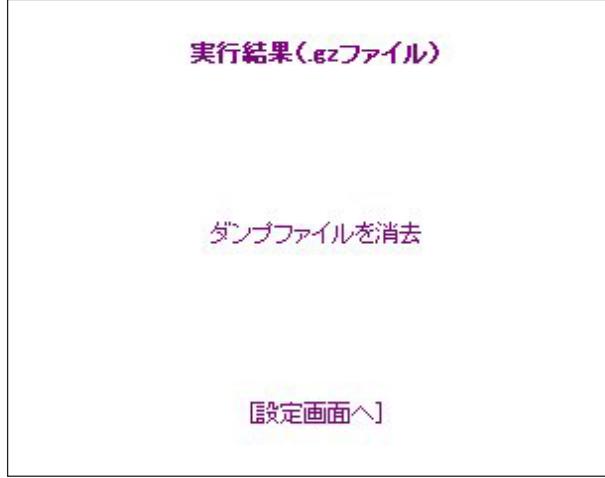
第26章 ネットワークテスト

ネットワークテスト

また、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、上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。

[PacketDump TypePcap の注意点]

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」をご参照下さい。

第 27 章

各種システム設定

各種システム設定

「システム設定」ページでは、XR-410/TX2-L2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
- ・ARP filter 設定

時計の設定

XR-410/TX2-L2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。



24時間単位で時刻を設定してください。

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。

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。

各種システム設定

ログの表示

「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 RNKD=0
RFwdR=0 RDupR=0 RFail=0 RErrr=0 RXFR=0 RLame=0 RPorts=0 SSys=0 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RO=3 RIO=0 RFwdQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNAns=0 SNKD=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 RNKD=0
RFwdR=0 RDupR=0 RFail=0 RErrr=0 RXFR=0 RLame=0 RPorts=0 SSys=0 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RO=3 RIO=0 RFwdQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNAns=0 SNKD=0
Apr 26 02:07:06 localhost -- MARK --
Apr 26 02:27:06 localhost -- MARK --
Apr 26 02:39:54 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 02:39:54 localhost named[436]: USAGE 1019756394 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 02:39:54 localhost named[436]: NSTATS 1019756394 1019556843 A=3
Apr 26 02:39:54 localhost named[436]: XSTATS 1019756394 1019556843 RR=0 RNKD=0
RFwdR=0 RDupR=0 RFail=0 RErrr=0 RXFR=0 RLame=0 RPorts=0 SSys=0 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RO=3 RIO=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNAns=0 SNKD=0
```

XR-410/TX2-L2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。

「ログの削除」をクリックして画面を開きます。

すべてのログメッセージを削除します。

実行する

「削除実行」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。

各種システム設定

パスワードの設定

XR-410/TX2-L2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。

「パスワードの設定」をクリックして設定画面を開きます。

新しいユーザー名	<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下さい。

入力が終わったら「設定」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。

ファームウェアのアップデート

XR-410/TX2-L2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。

- 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。

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	<input type="text"/> <input type="button" value="参照..."/>

- 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-410/TX2-L2 ver 1.0.3
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-410/TX2-L2 ver 1.0.3
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	
<input type="button" value="実行する"/>	<input type="button" value="中止する"/>

(次のページに続きます)

各種システム設定

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。

アップデート中は、本体のLEDが”8”を表示します。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。

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"/> EUO(LF) <input checked="" type="radio"/> SJIS(OR+LF) <input type="radio"/> SJIS(OR)	
形式の指定	<input type="radio"/> 全設定(gzip) <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下さい。

「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。

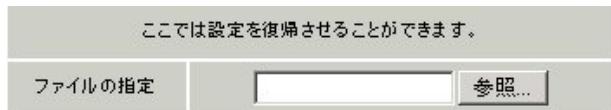
(次のページに続きます)

各種システム設定

「全設定」を選択すると、本装置のすべての設定を 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。



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。

設定のリセット

XR-410/TX2-L2 の設定を全てリセットし、工場出荷時の設定に戻します(ハードウェアリセット)。

「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。

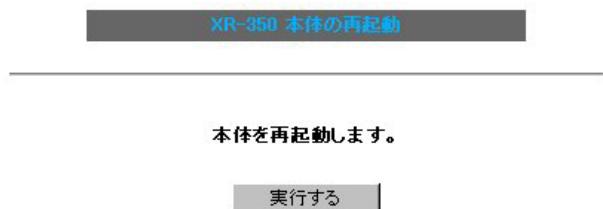
「実行する」ボタンをクリックするとリセットが実行され、本体の全設定が工場出荷設定に戻ります。

各種システム設定

本体再起動

XR-410/TX2-L2 を再起動します。設定内容は変更されません。

「再起動」をクリックして画面を開きます。



「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。

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。

「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。

UDP	<input type="text" value="30"/>	秒 (0 ~ 8640000)
UDP stream	<input type="text" value="180"/>	秒 (0 ~ 8640000)
TCP	<input type="text" value="432000"/>	秒 (0 ~ 8640000)
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 432000 秒です。

「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。

各種システム設定

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

を取得するかどうかを指定して、「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。

ARP filter 設定

ARP filter設定をおこないます。

実行方法

「ARP filter設定」をクリックして画面を開きます。

ARP filter設定

ARP filter	<input checked="" type="radio"/> 無効	<input type="radio"/> 有効
------------	-------------------------------------	--------------------------

「有効」を選択して保存すると、ARP filterが動作します。

ARP filterを有効にすることで、同一IPアドレスのARPを複数のインター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ーフェースからARP応答を出さないようにできます。

第 28 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 論理インター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およびリンク速度が表示されます。

・ルーティング情報

直接接続、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。

・DHCP クライアント情報

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「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。



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 29 章

運用管理設定

一時的に工場出荷設定に戻す方法

XR-410/TX2-L2 の背面にある「INITボタン」を使用して、XR-410/TX2-L2 の設定を一時的に工場出荷設定に戻すことができます(ソフトウェアリセット)。

INITボタンを押したまま電源切斷　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と、本装置は工場出荷時の設定で再起動します。

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。

付録 A

インターフェース名一覧

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
- ・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
- ・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。

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)

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

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

DHCPクライアント機能	無効
デフォルトゲートウェイ	設定なし
IPマスカレード機能	無効
NAT機能	設定なし
パケットフィルタ機能	ステートフルパケットインスペクション機能 (Ether0ポート以外) NetBIOS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)
DNSリレー機能	有効
DNSキャッシュ機能	無効
スタティックルート設定	設定なし
ダイナミックルーティング	無効
L2TPv3機能	無効
IPsec機能	無効
GRE機能	無効
UPnP機能	無効
ログ機能	有効
仮想インターフェース機能	設定なし
アクセスサーバ機能	無効
リモートアクセス機能	無効
SNMPエージェント機能	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

製品仕様

ハードウェア仕様

製品名	FutureNet XR-410/TX2-L2
CPU	400MHz
暗号化処理	ソフトウェア
OS	Linux Kernel 2.4.18
通信インターフェース	<p>Ether0 100/10 x 1ポート (LAN側) IEEE802.3u(100Base-TX)/IEEE802.3(10Base-T) コネクタ RJ-45 (Auto MDI/MDIX)</p> <p>Ether1 100/10 x 1ポート (WAN側) IEEE802.3u(100Base-TX)/IEEE802.3(10Base-T) コネクタ RJ-45 (Auto MDI/MDIX)</p> <p>RS-232 RS-232ポート(PPP接続用) x 1 9,600bps~230.4kbps コネクタ RJ-45 RJ-45↔D-sub9ピン 変換コネクタ付属</p>
本体LED	ステータス (7セグメントLED)
本体設定方法	Webブラウザ、設定ファイル 工場出荷値設定上のリセットボタン Webブラウザからのファームウェア更新機能
環境条件	温度 0°C~+40°C、湿度 25%~85% (結露なきこと)
電波障害防止	VCCI クラスA 準拠
JATE認定	D03-0229JP
電源	DC5V 1A(最大)
消費電力	5W(最大)
外形寸法	81mm(W) x 117mm(D) x 32.5mm(H)
重量	約350g
付属品	リリースノート、製品マニュアル PDF形式(CD-ROMに収録) RJ-45/D-sub9ピン変換アダプタ(ストレート仕様) UTPケーブル(ストレート)、AC電源ケーブル、保証書
保障	購入日から1年間 センドバックによる対応

ソフトウェア仕様

対応する接続形態	FTTH、ADSL、CATV、ローカルルータ PPPoE Unnumbered接続に対応
主な対応プロトコル	L2TPv3、IP(IPv4)、IPsec(IPv4)、TCP、UDP、ICMP ARP、PPPoE、SMTP、HTTP、SNMP、GRE
IPルーティング方式	RIP、RIPv2、静态ルート、デフォルトルート、OSPF
トンネリング機能	GRE64対地までサポート
NAT方式	1対1アドレス変換、IPマスカレード機能
静的NAT変換	バーチャルサーバ機能(最大128 IP、256エントリ) 送信元NAT機能
ホスト名	CATV接続設定において設定可能
マルチPPPoEセッション	同時に最大4セッション
VPN機能(IPsec)	1対128拠点(最大)の構成、aggressiveモード対応 3DES/DES/AESでの暗号化処理
セキュリティ機能	パケットフィルタ、ステートフルパケットインスペクション DoS検出、パケット記録
パケットフィルタ機能	入力、転送、出力ごとに256ずつ設定可能 インターフェース、IN/OUT、制御方法、IPアドレス プロトコル、ポートによる設定が可能
MACアドレスの変更	インターフェースをDHCPクライアントとした場合に 設定可能
高速化・チューニング	DNSキャッシュ機能、Proxy ARP、MTU設定
ログ機能	ブラウザ上の表示、自動トリミング機能
運用管理機能	設定ファイルによる一括設定 SNMPエージェント機能
リモートアクセス	リモートアクセス機能、アクセスサーバ機能
設定	WWWブラウザ上から実施
設定のバックアップ リストア	ブラウザ上から可能
バージョンアップ	ブラウザ上から可能
シリアルポート	インターネット接続機能、インターネットVPN機能、 アクセスサーバ機能 ※ PPPoEのバックアップ回線としても使用可能
その他	ゲートウェイ認証機能、パケットダンプ、ルータping発行

付録 D

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、お願ひいたします。

サポートに関する技術的なお問い合わせやご質問は、下記へご連絡下さい。

- ・サポートデスク

電話 0422-37-8926

受付時間 10:00 ~ 16:30 (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下さい。事前のご連絡なしに弊社までご送付いただきましても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、お願ひいたします。

- ・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28章 情報表示」をご覧下さい)

- ・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、差し支えのない範囲でお知らせ下さい。

- ・不具合の内容または、不具合の再現手順

何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせ下さい。

- ・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。

- ・XR-410/TX2-L2の設定内容、およびコンピューターのIP設定

- ・可能であれば、「設定のバックアップファイル」をお送りください。

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、是非ご覧下さい。

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下さい。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 ユーザーズガイド v1.3.3対応版

2005年11月版

発行 センチュリー・システムズ株式会社

2005 CENTURYSYSTEMS, INC. All rights reserved.
