

FutureNet XR シリーズ

設定例集

Ver 1.1.0



※上記写真は XR-540/C です。

センチュリー・システムズ株式会社



目次

目次	2
はじめに	5
改版履歴	6
1. インタフェース設定	7
1-1. ローカルルータ設定	7
1-1-1. 構成図	7
1-1-2. 設定例	8
1-2. DHCP クライアント設定	9
1-2-1. 構成図	9
1-2-2. 設定例	10
1-3. ブリッジ設定	11
1-3-1. 構成図	11
1-3-2. 設定例	12
2. PPPoE 設定	13
2-1. 端末型接続設定	13
2-1-1. 構成図	13
2-1-2. 設定例	14
2-2. LAN 型接続設定	16
2-2-1. 構成図	16
2-2-2. 設定例	17
2-3. マルチセッション接続設定	19
2-3-1. 構成図	19
2-3-2. 設定例	20
2-4. マルチホーミング設定	23
2-4-1. 構成図	23
2-4-2. 設定例	24
3. NAT 設定	28
3-1. IP マスカレード設定	28
3-1-1. 構成図	28
3-1-2. 設定例	29
3-2. 送信元 NAT 設定	30
3-2-1. 構成図	30
3-2-2. 設定例	31
3-3. バーチャルサーバ設定	33
3-3-1. 構成図	33

3-3-2. 設定例	34
4. フィルタ設定	36
4-1. 入力フィルタ設定	36
4-1-1. 構成図	36
4-1-2. 設定例	37
4-2. 転送フィルタ設定	39
4-2-1. 構成図	39
4-2-2. 設定例	40
4-3. ステートフルパケットインスペクション	42
4-3-1. 構成図	42
4-3-2. 設定例	43
5. NAT/フィルタ応用設定	44
5-1. NAT でのサーバ公開 1（ポートマッピング）	44
5-1-1. 構成図	44
5-1-2. 設定例	45
5-2. NAT でのサーバ公開 2（複数 IP+PPPoE）	48
5-2-1. 構成図	48
5-2-2. 設定例	49
5-3. NAT でのサーバ公開 3（複数 IP+Ether）	52
5-3-1. 構成図	52
5-3-2. 設定例	53
5-4. DMZ 構築例（PPPoE）	55
5-4-1. 構成図	55
5-4-2. 設定例	56
5-4-3. 設定例補足	59
6. ブリッジフィルタ設定	60
6-1. 同一 LAN 内でのアクセス制御	60
6-1-1. 構成図	60
6-1-2. 設定例	61
7. DHCP 設定	65
7-1. DHCP サーバ設定	65
7-1-1. 構成図	65
7-1-2. 設定例	66
7-2. DHCP リレー設定	68
7-2-1. 構成図	68
7-2-2. 設定例	69

8. 攻撃検出設定	71
8-1. アクティブファイアウォールの利用	71
8-1-1. 構成図	71
8-1-2. 設定例	72
8-1-3. 設定例補足（メール送信設定）	76
9. Web 認証設定（ゲートウェイ認証設定）	78
9-1. ユーザ認証	78
9-1-1. 構成図	78
9-1-2. 設定例	79
9-1-3. 設定例補足（ユーザ認証方法）	83
9-2. URL 転送	84
9-2-1. 構成図	84
9-2-2. 設定例	85
9-3. ユーザ強制認証＋URL 転送＋RADIUS 連携	88
9-3-1. 構成図	88
9-3-2. 設定例	89
9-4. Web 認証機能ソリューション例（NS-430 との併用）	96
9-4-1. 構成図	96
9-4-2. 設定例	97
10. QoS 設定	112
10-1. 帯域制限	112
10-1-1. 構成図	112
10-1-2. 設定例	113
10-2. 帯域制御（簡易 QoS 設定と詳細 QoS 設定の利用）	115
10-2-1. 構成図	115
10-2-2. 設定例	116
10-2-3. 設定例補足（クラス階層図）	124
10-3. PPPoE での帯域制御＋優先制御	125
10-3-1. 構成図	125
10-3-2. 設定例	126
10-3-3. 設定例補足（クラス階層図）	142
11. サポートデスクへのお問い合わせ	143
11-1. サポートデスクへのお問い合わせに関して	143
11-2. サポートデスクのご利用に関して	143

はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- 本書に記載されている会社名、製品名は、各社の商標および登録商標です。
- 本ガイドは、以下の FutureNet XR 製品に対応しております。
 - ・ XR-510/C
 - ・ XR-540/C
 - ・ XR-730/C
 - ・ XR-1100 シリーズ

※一部設定内容によっては上記機種以外での設定も可能です。詳しくは各製品のユーザーズガイドをご参照下さい。

- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書は FutureNet XR シリーズ XR-540/C Ver3.5.2 をベースに作成しております。各種機能において、ご使用されている製品およびファームウェアのバージョンによっては、一部機能および設定画面が異なっている場合もありますので、その場合は各製品のユーザーズガイドを参考に、適宜読みかえてご参照および設定を行って下さい。
- 本書を利用し運用した結果発生した問題に関しましては、責任を負いかねますのでご了承下さい。

改版履歴

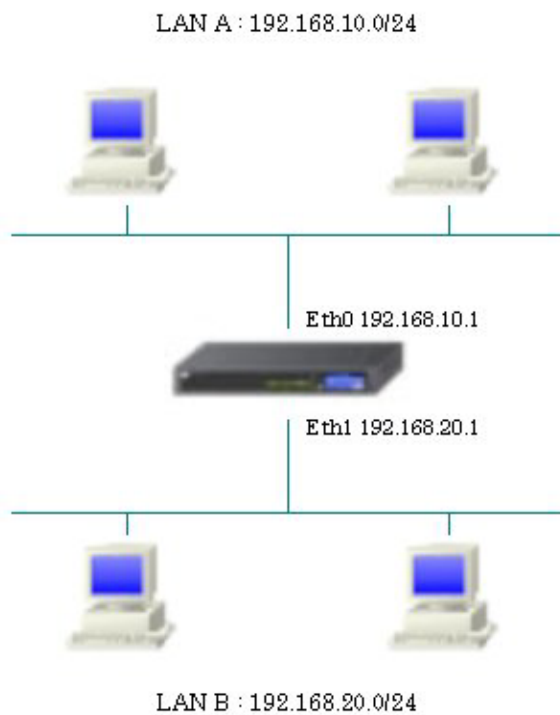
Version	更新内容
1.0.0	初版
1.1.0	ブリッジフィルタ, DHCP, 攻撃検出, Web 認証, QoS 設定例追加

1. インタフェース設定

1-1. ローカルルータ設定

LAN A「192.168.10.0/24」とLAN B「192.168.20.0/24」のネットワークを接続し、通信するための設定をします。

1-1-1. 構成図



1-1-2. 設定例

インタフェース設定でそれぞれのネットワークに属する IP アドレスをルータに設定します。
IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

The screenshot shows the configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. Below these, there are checkboxes for 'IP Masquerade (ip masq)', 'Stateful Packet Inspection (spi)', 'SPI Log Drop', 'proxy arp', and 'Directed Broadcast', all of which are currently unchecked.

[Ethernet1 の設定]

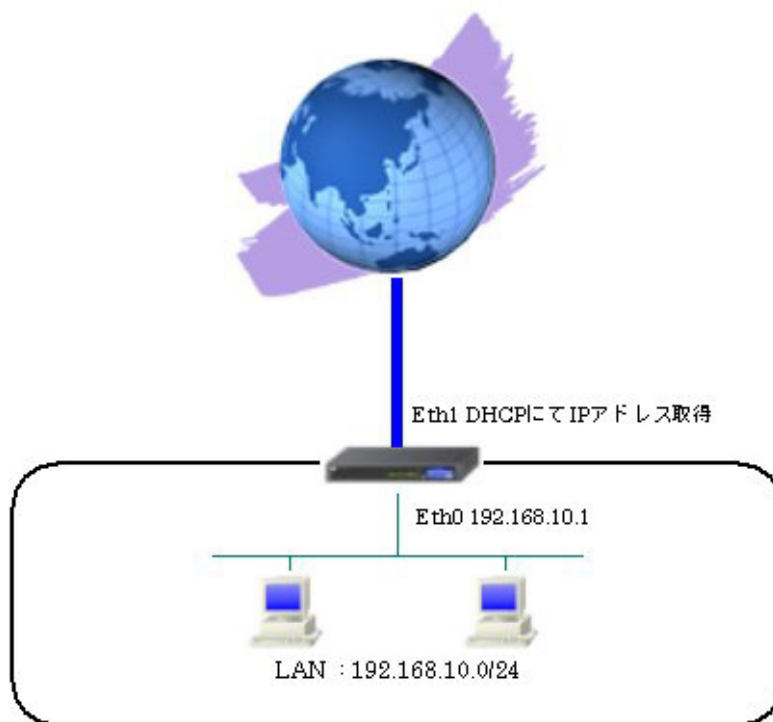
IP アドレスに「192.168.20.1」を設定します。

The screenshot shows the configuration window for Ethernet1. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.20.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. Below these, there are checkboxes for 'IP Masquerade (ip masq)', 'Stateful Packet Inspection (spi)', 'SPI Log Drop', 'proxy arp', and 'Directed Broadcast', all of which are currently unchecked.

1-2. DHCP クライアント設定

CATV など IP アドレスを DHCP にて払い出される場合には、DHCP クライアントの設定を行います。

1-2-1. 構成図



1-2-2. 設定例

本設定例では Ether1 インタフェースを DHCP クライアントとして利用するための設定を行っています。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

The screenshot shows the configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Several checkboxes are present: 'IP Masquerade (ip masq)' is unchecked, 'Stateful Packet Inspection (spi)' is unchecked, 'SPI Log' is unchecked, 'proxy arp' is unchecked, and 'Directed Broadcast' is unchecked.

[Ethernet1 の設定]

「DHCP サーバから取得」を選択します。

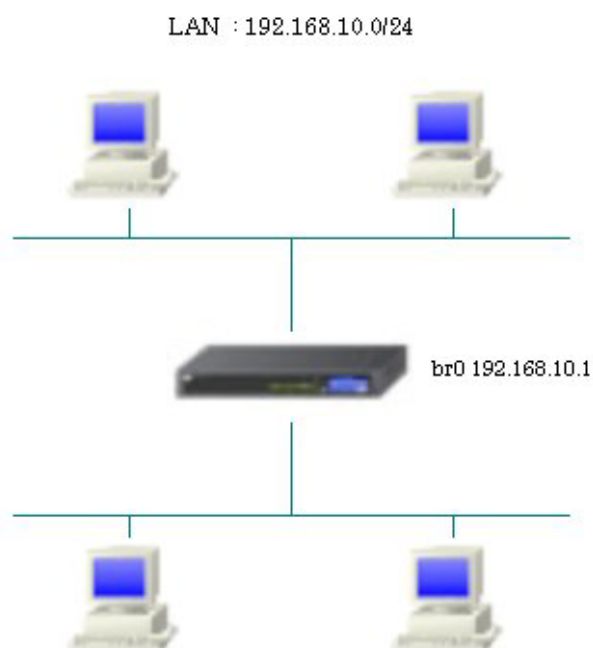
※ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定しています。

The screenshot shows the configuration window for Ethernet1. The 'DHCP Server Acquisition' radio button is selected. The IP address is set to 0, the netmask to 255.255.255.0, and the MTU to 1500. The host name and MAC address fields are empty. Several checkboxes are present: 'IP Masquerade (ip masq)' is checked, 'Stateful Packet Inspection (spi)' is checked, 'SPI Log' is unchecked, 'proxy arp' is unchecked, and 'Directed Broadcast' is unchecked.

1-3. ブリッジ設定

2 つ以上の Ethernet インタフェース, また VLAN インタフェースをブリッジ設定することが可能です。ブリッジフィルタ設定と組み合わせることで、同一 LAN の特定エリアを分離し、フィルタリングによる制御を行うことも可能です。

1-3-1. 構成図



1-3-2. 設定例

本設定例では二つの同一ネットワークを接続するための設定を行っています。

<<インタフェース設定>>

[Bridge の設定]

ブリッジインタフェースのインタフェース番号を設定します。

本設定例では、Ethernet0 と Ethernet1 でブリッジを設定します。

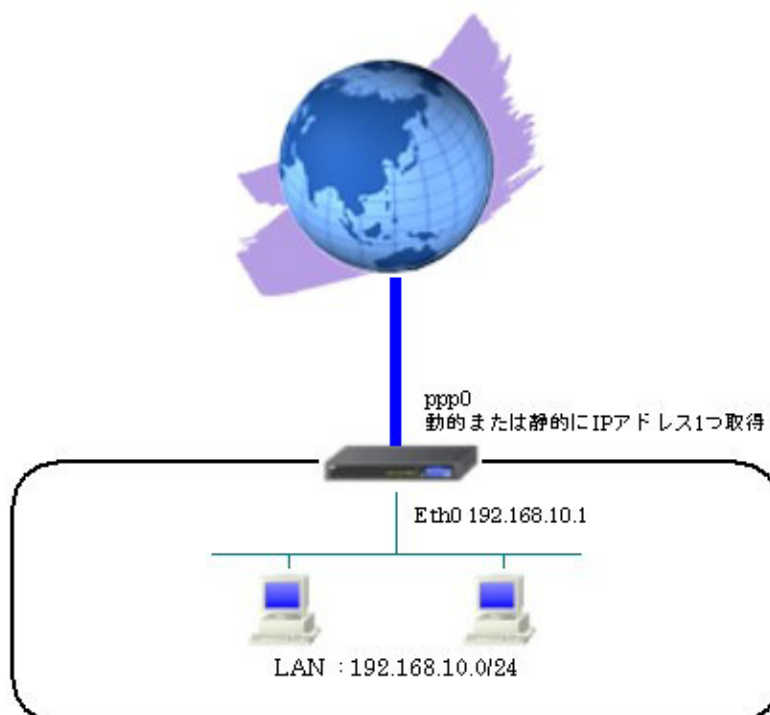
IP アドレスに「192.168.10.1」、ネットマスクに「255.255.255.0」を設定します。

2. PPPoE 設定

2-1. 端末型接続設定

フレッツ ADSL や B フレッツ など PPPoE 接続を必要とする環境で、IP アドレスを 1 つ利用できるサービスで利用可能な設定です。

2-1-1. 構成図



2-1-2. 設定例

PPPoE 接続に必要な設定を行います。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

The screenshot shows the configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Several checkboxes are present: 'IP Masquerade (ip masq)' (unchecked), 'Stateful Packet Inspection (spi)' (unchecked), 'SPI Log' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

The screenshot shows the configuration window for Ethernet1. The 'Fixed IP Address' radio button is selected. The IP address is set to 0, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Several checkboxes are present: 'IP Masquerade (ip masq)' (unchecked), 'Stateful Packet Inspection (spi)' (unchecked), 'SPI Log' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時 PADTを強制送出 ☒ 非接続SessionのLDP-EchoRequest受信時 PADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

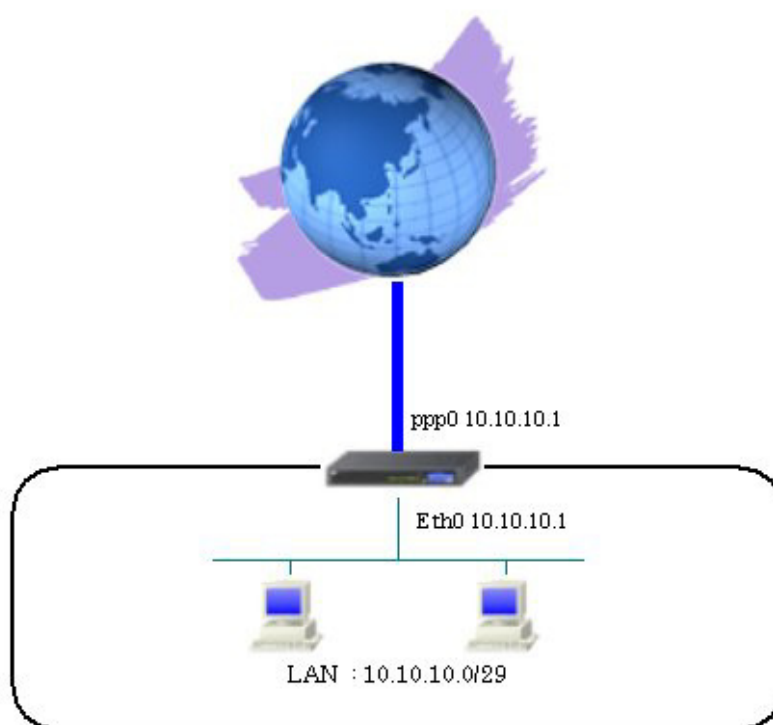
回線状態	主回線で接続しています
------	-------------

2-2. LAN 型接続設定

フレッツ ADSL や B フレッツ など PPPoE 接続を必要とする環境で、IP アドレスを複数利用可能な場合、ルータの LAN 側にもグローバル IP アドレスを割り当てることができます。

またこの接続は Unnumbered 接続とも呼ばれています。

2-2-1. 構成図



2-2-2. 設定例

PPPoE 接続に必要な設定を行い、LAN 側にもグローバル IP アドレス “10.10.10.0/29” を利用可能にするための設定を行います。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「10.10.10.1」、ネットマスクに「255.255.255.248」を設定します。

☒ 固定アドレスで使用
IP アドレス 10.10.10.1
ネットマスク 255.255.255.248
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

☒ 固定アドレスで使用
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

ppp インタフェースに割り当てる IP アドレス「10.10.10.1」を設定します。

UnNumbered-PPP回線使用時に設定できます	
IPアドレス	10.10.10.1 回線接続時に割り付けるグローバルIPアドレスです

[接続設定]

本設定例では、IP マスカレードを「無効」にし、WAN からのパケットをフィルタリングしないためにステートフルパケットインスペクションを「無効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケットインスペクション	☒ 無効 ☐ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

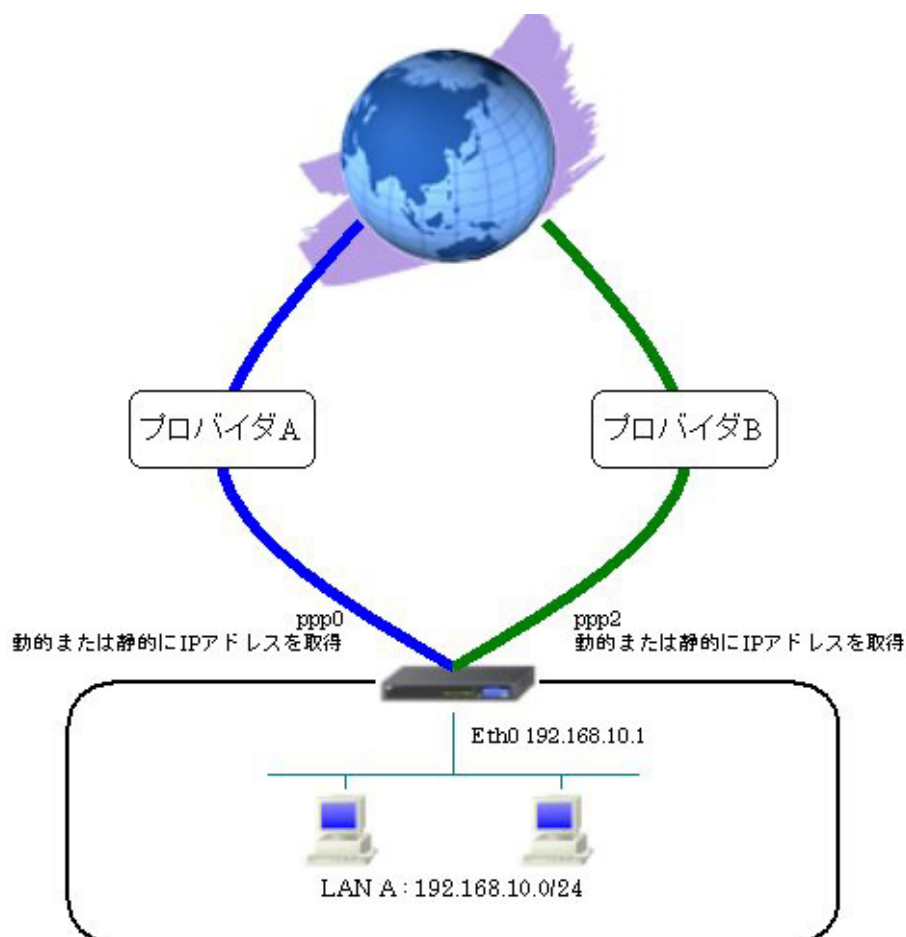
接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

2-3. マルチセッション接続設定

B フレッツなどでは同時に複数の PPPoE 接続を行うことが可能です。これにより複数のプロバイダに接続して利用することも可能です。

2-3-1. 構成図



2-3-2. 設定例

PPPoE 接続（主回線，マルチ回線）に必要な設定を行います。

また宛先 IP アドレスが「10.100.0.0/24」の時には、マルチ回線を利用し、それ以外の宛先 IP アドレスに対しては主回線を利用するように設定しています。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

固定アドレスで使用

IP アドレス 192.168.10.1

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルバケットインスペクション(spi)

☐ SPI で DROP したバケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

固定アドレスで使用

IP アドレス 0

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルバケットインスペクション(spi)

☐ SPI で DROP したバケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定 1]

PPPoE 接続（主回線）で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続先設定 2]

PPPoE 接続（マルチ回線#2）で使用するユーザ ID とパスワードを設定します。

ユーザID	test@example.com
パスワード	testpass

[接続設定]

PPPoE（主回線）に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE（マルチ接続#2）に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLDP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています マルチ接続 #2で接続しています
------	---

<<スタティックルート設定>>

宛先 IP アドレスが「10.100.0.0/24」の時には、マルチ回線を利用するための設定をします。

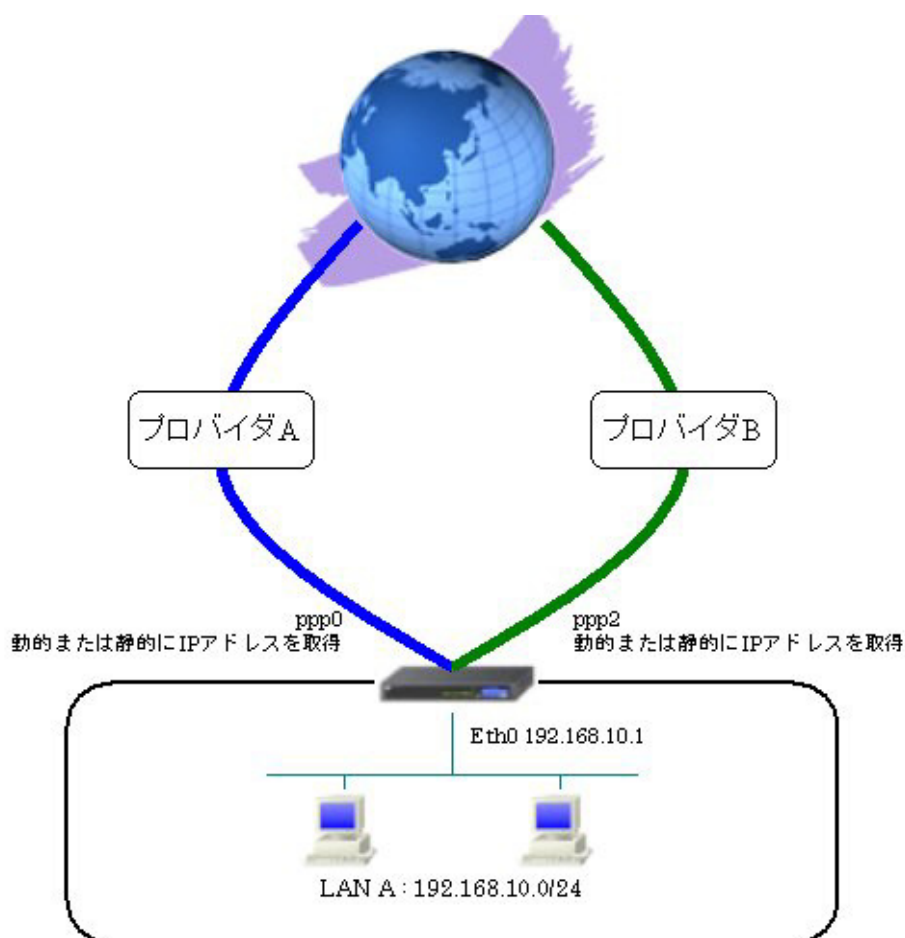
アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>
10.100.0.0	255.255.255.0	ppp2	1

2-4. マルチホーミング設定

PPP/PPPoE 接続の主回線とマルチ回線によるロードバランシング（マルチホーミング）を行うことが可能です。通信のストリーム毎に使用する回線を振り分けます。（ストリームは送信元 IP アドレスと宛先 IP アドレスにより識別します）

※マルチホーミング機能は XR-510/C Ver3. 5. 0, XR-540/C Ver3. 5. 0 以降でのみ対応しております。

2-4-1. 構成図



2-4-2. 設定例

マルチホーミング機能を有効にし、PPPoE 接続（主回線，マルチ回線）に必要な設定を行います。
またスタティックルート設定でデフォルトルート为主回線（ppp0）とマルチ回線（ppp2）で設定します。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

固定アドレスで使用
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

固定アドレスで使用
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

<<システム設定>>

[マルチホーミング設定]

マルチホーミングを機能させるために「有効」を選択します。

マルチホーミング	☒ 有効	☐ 無効
----------	-------------------------------------	--------------------------

<<スタティックルート設定>>

主回線（ppp0）とマルチ回線（ppp2）をデフォルトルートとして設定します。

アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>
0.0.0.0	0.0.0.0	ppp0	1
0.0.0.0	0.0.0.0	ppp2	1

<<PPP/PPPoE 設定>>

[接続先設定 1]

PPPoE 接続（主回線）で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続先設定 2]

PPPoE 接続（マルチ回線#2）で使用するユーザ ID とパスワードを設定します。

ユーザID	test@example.com
パスワード	testpass

[接続設定]

PPPoE（主回線）に関する設定をします。

デフォルトルートは「無効」を選択します。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☒ 無効 ☐ 有効

PPPoE（マルチ接続#2）に関する設定をします。

本設定例では、ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

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

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時 PADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

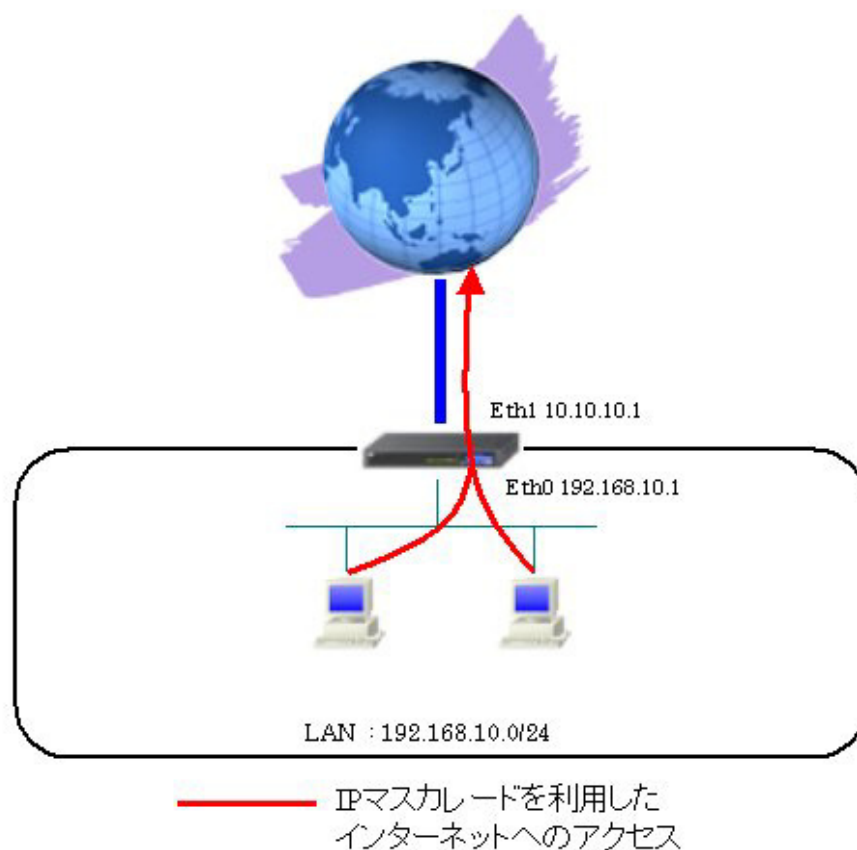
回線状態	主回線で接続しています マルチ接続 #2 で接続しています
------	----------------------------------

3. NAT 設定

3-1. IP マスカレード設定

プライベート IP アドレスのネットワーク内にある端末がインターネットへアクセスする際など、送信元 IP アドレスを IP マスカレードの設定を有効にしたインタフェースの IP アドレスに変換して通信することができます。

3-1-1. 構成図



3-1-2. 設定例

送信元 IP アドレスを変換するインタフェースで IP マスカレードの設定を有効にしています。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

固定アドレスで使用
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション spi
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

IP アドレスに「10.10.10.1」, ネットマスクに「255.255.255.252」を設定します。

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にします。

※WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

固定アドレスで使用
IP アドレス 10.10.10.1
ネットマスク 255.255.255.252
MTU 1500
DHCPサーバから取得
ホスト名
MACアドレス
☒ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☒ ステートフルパケットインスペクション spi
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

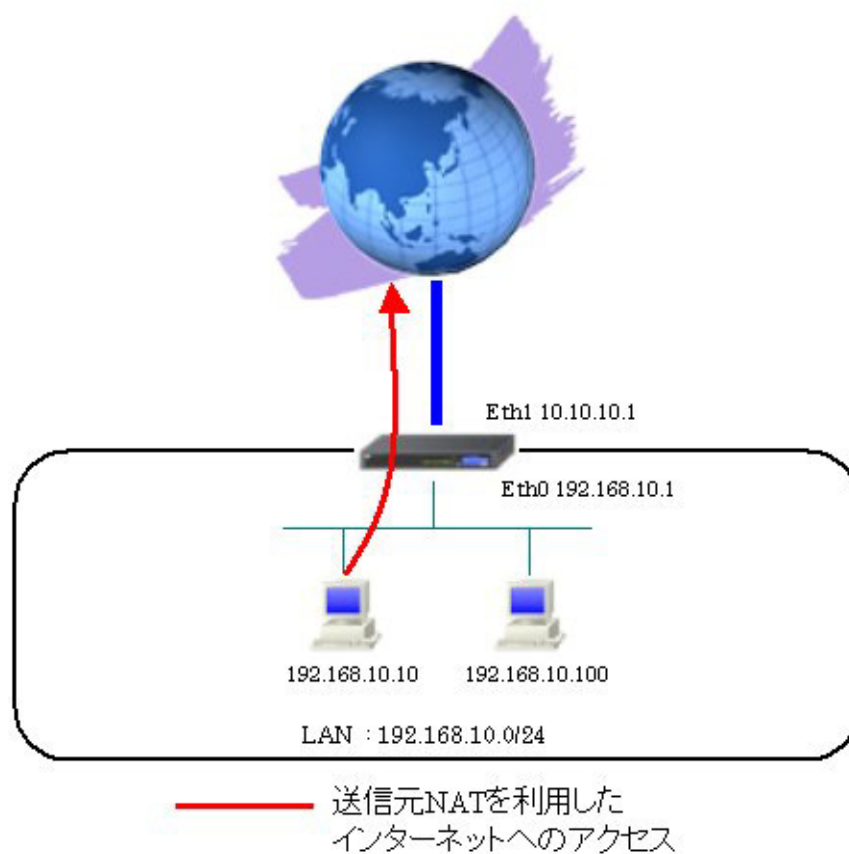
[その他の設定]

デフォルトゲートウェイの設定
10.10.10.2

3-2. 送信元 NAT 設定

ある特定のネットワークやホストを指定し、送信元 IP アドレスの変換を行うことができます。例えばプライベート IP アドレスのある特定の端末のみ送信元 IP アドレスを変換するといった場合に利用します。

3-2-1. 構成図



3-2-2. 設定例

ある特定の端末のみ送信元 IP アドレスを変換するための設定をします。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

☒ 固定アドレスで使用する
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

IP アドレスに「10.10.10.1」, ネットマスクに「255.255.255.252」を設定します。

※WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

☒ 固定アドレスで使用する
IP アドレス 10.10.10.1
ネットマスク 255.255.255.252
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☒ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
	10.10.10.2

<<NAT 設定>>

[送信元 NAT]

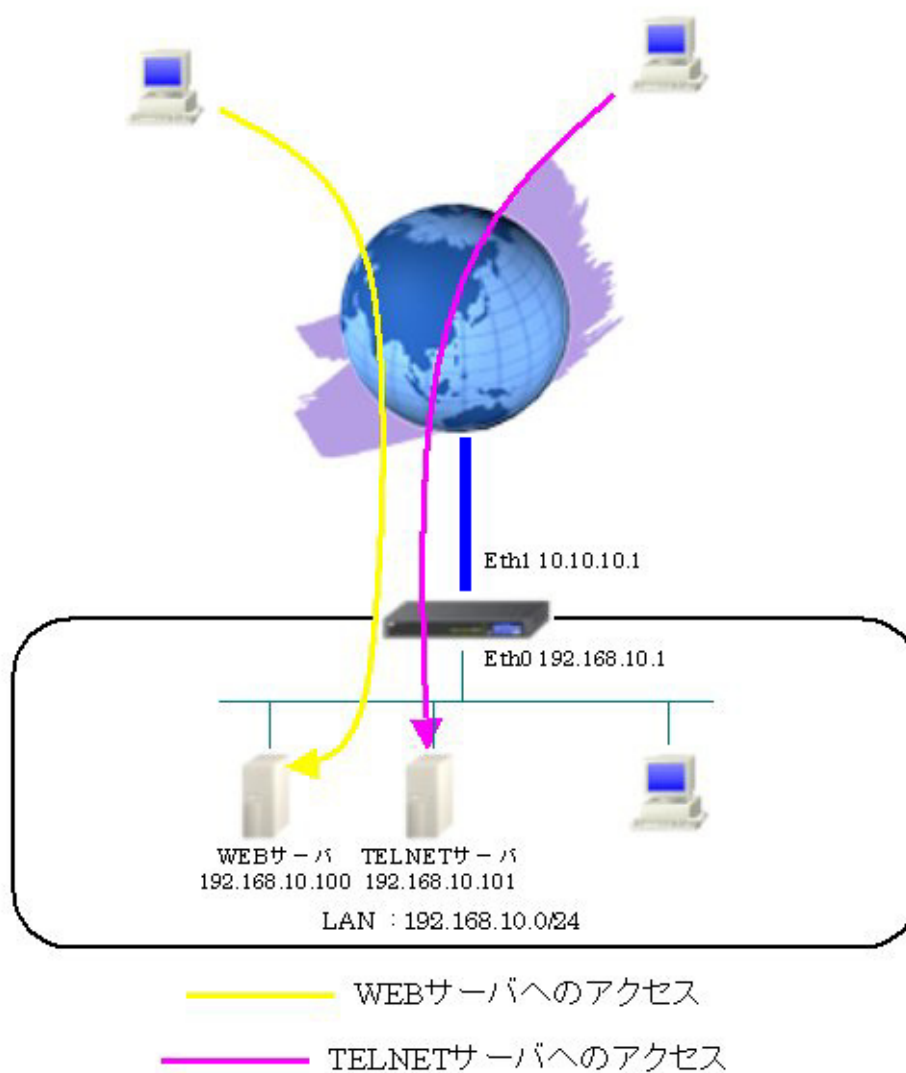
LAN 上にある「192.168.10.10」の端末の送信元 IP アドレスを eth1 からのパケット送信時に「10.10.10.1」に変換する設定をします。

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
192.168.10.10	10.10.10.1	eth1

3-3. バーチャルサーバ設定

プライベート IP アドレスのネットワーク内にあるサーバをインターネット経由でアクセスさせる場合、バーチャルサーバ機能によりルータ経由でのアクセスが可能になります。

3-3-1. 構成図



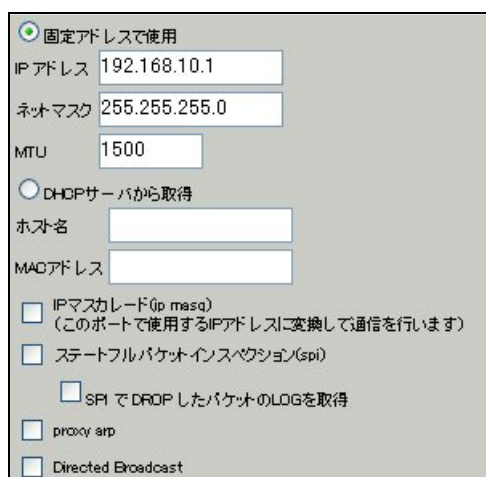
3-3-2. 設定例

プライベート IP アドレスのネットワーク内にあるサーバをインターネットからアクセス可能にするための設定をします。

<<インタフェース設定>>

[Ethernet0 の設定]

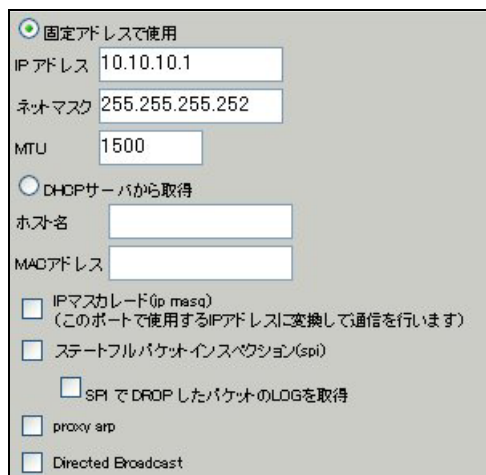
IP アドレスに「192.168.10.1」を設定します。



☒ 固定アドレスで使用する
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション spi
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

IP アドレスに「10.10.10.1」、ネットマスクに「255.255.255.252」を設定します。



☒ 固定アドレスで使用する
IP アドレス 10.10.10.1
ネットマスク 255.255.255.252
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション spi
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[その他の設定]

デフォルトゲートウェイの設定	
	10.10.10.2

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ, TELNET サーバをインターネットからアクセス可能にするための設定をします。
インターネットから「10. 10. 10. 1」で TCP ポート 80 番宛てのパケットを受信した場合は、192. 168. 10. 100
に転送します。

インターネットから「10. 10. 10. 1」で TCP ポート 23 番宛てのパケットを受信した場合は、192. 168. 10. 101
に転送します。

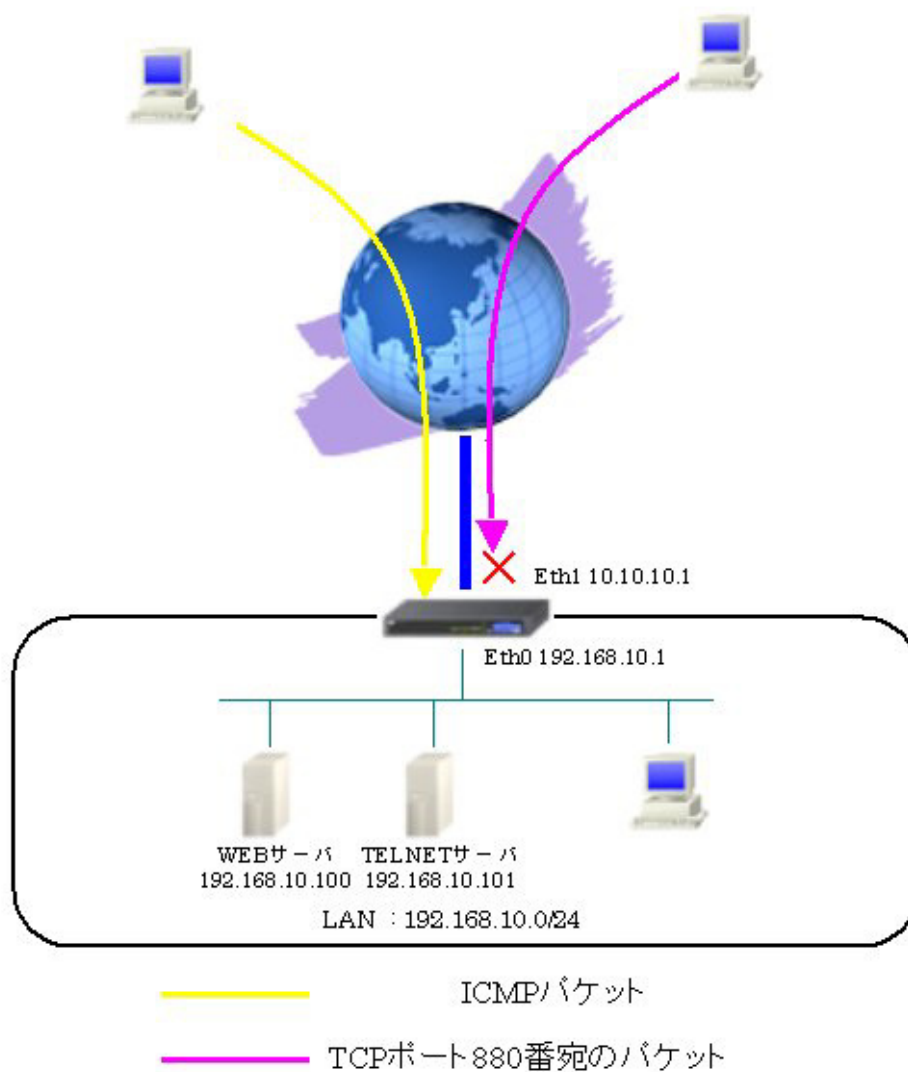
サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.10.100	10.10.10.1	tcp	80	eth1
192.168.10.101	10.10.10.1	tcp	23	eth1

4. フィルタ設定

4-1. 入力フィルタ設定

入力フィルタでは外部からルータ宛に送信されたパケットのうち、ルータ自身で受信し処理するものを対象とします。本設定例ではインターネットからの ICMP パケットは許可するが、Web 設定画面へのアクセス（TCP ポート 880 番）は破棄する設定です。

4-1-1. 構成図



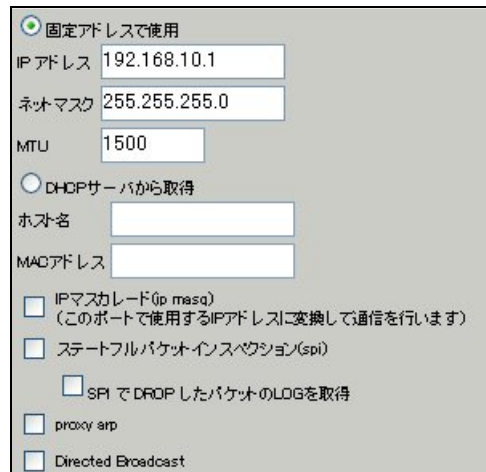
4-1-2. 設定例

外部からの XR へのアクセスを制限します。

<<インタフェース設定>>

[Ethernet0 の設定]

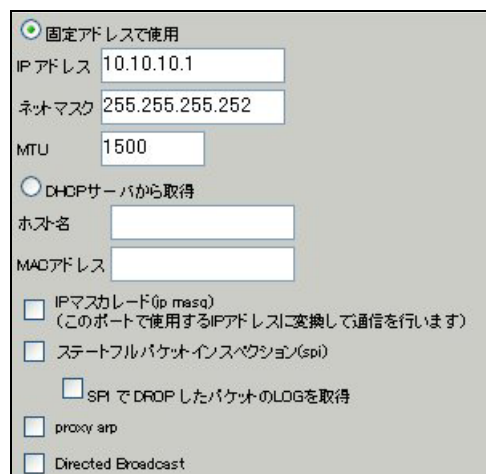
IP アドレスに「192.168.10.1」を設定します。



The screenshot shows the configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Below these fields, there are several checkboxes: 'IP Masquerade (ip masq)' (unchecked), 'Stateful Packet Inspection (spi)' (unchecked), 'SPI Log' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

[Ethernet1 の設定]

IP アドレスに「10.10.10.1」, ネットマスクに「255.255.255.252」を設定します。



The screenshot shows the configuration window for Ethernet1. The 'Fixed IP Address' radio button is selected. The IP address is set to 10.10.10.1, the netmask to 255.255.255.252, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Below these fields, there are several checkboxes: 'IP Masquerade (ip masq)' (unchecked), 'Stateful Packet Inspection (spi)' (unchecked), 'SPI Log' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

[その他の設定]

デフォルトゲートウェイの設定	
	10.10.10.2

<<フィルタ設定>>

[入力フィルタ]

インターネット側から本装置宛の ICMP パケットを許可しています。

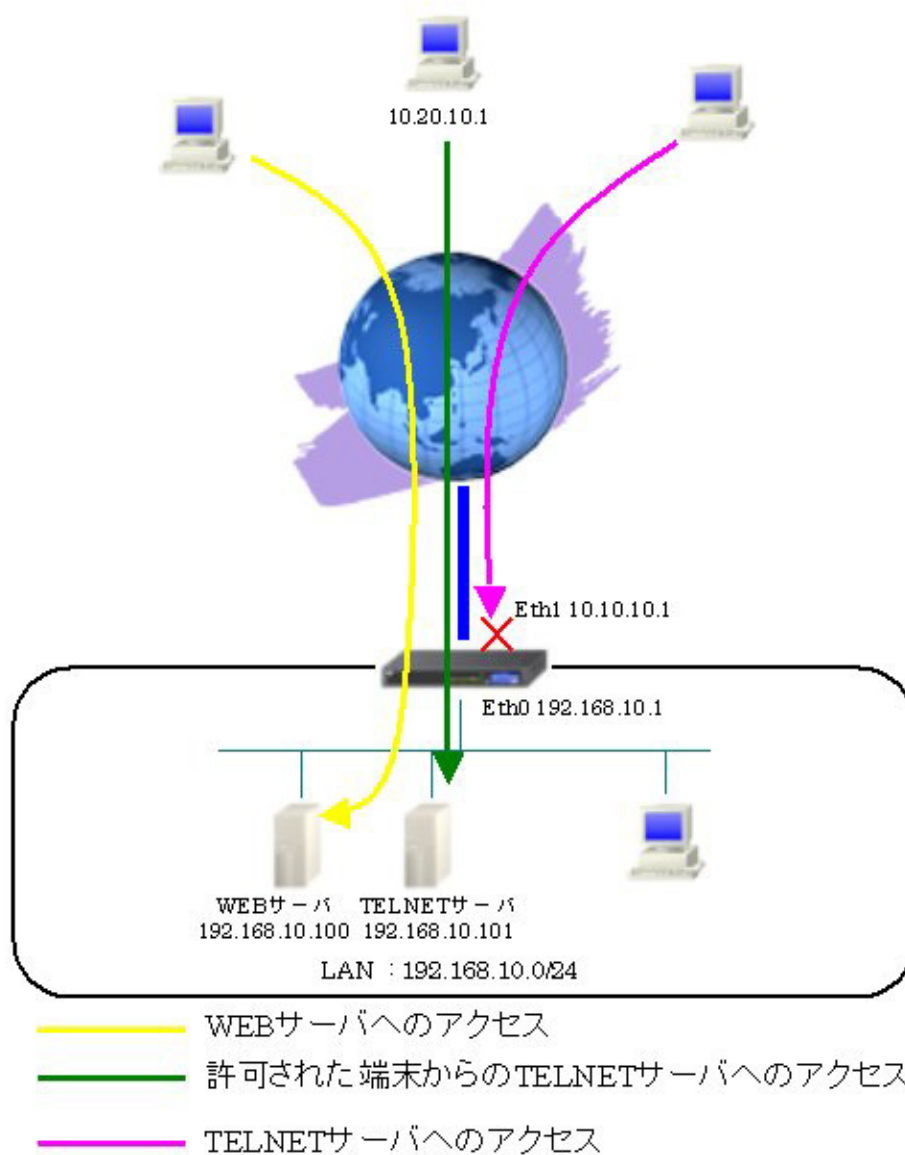
インターネット側から本装置宛の TCP ポート 880 番宛のパケットを破棄しています。

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	宛先アドレス	宛先ポート	ICMP type/code	送信元MACアドレス	LOG
eth1	パケット受信時	許可	icmp							☐
eth1	パケット受信時	破棄	tcp				880			☐

4-2. 転送フィルタ設定

転送フィルタでは本装置で内部転送（本装置がルーティング）するパケットを制御するときに利用します。本設定例ではバーチャルサーバでインターネットに公開している WEB サーバ、TELNET サーバに対して WEB サーバへのアクセスは許可、TELNET サーバへは指定した IP アドレスからのアクセスのみ許可し、その他からの TELNET アクセスは破棄する設定です。

4-2-1. 構成図



4-2-2. 設定例

ルータを経由するパケットに対してアクセス制限を行います。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

The screenshot shows the configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'Obtain from DHCP server' radio button is unselected. The host name and MAC address fields are empty. Below these fields are several checkboxes: 'IP masquerade (ip masq)' (unchecked), 'Stateful packet inspection (spi)' (unchecked), 'SPI log for dropped packets' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

[Ethernet1 の設定]

IP アドレスに「10.10.10.1」、ネットマスクに「255.255.255.252」を設定します。

The screenshot shows the configuration window for Ethernet1. The 'Fixed IP Address' radio button is selected. The IP address is set to 10.10.10.1, the netmask to 255.255.255.252, and the MTU to 1500. The 'Obtain from DHCP server' radio button is unselected. The host name and MAC address fields are empty. Below these fields are several checkboxes: 'IP masquerade (ip masq)' (unchecked), 'Stateful packet inspection (spi)' (unchecked), 'SPI log for dropped packets' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

[その他の設定]

デフォルトゲートウェイの設定	
	10.10.10.2

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ, TELNET サーバをインターネットからアクセス可能にするための設定をします。
インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、
「192.168.10.100」に転送します。
インターネットから「10.10.10.1」で TCP ポート 23 番宛てのパケットを受信した場合は、
「192.168.10.101」に転送します。

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
192.168.10.100	10.10.10.1	tcp	80	eth1
192.168.10.101	10.10.10.1	tcp	23	eth1

<<フィルタ設定>>

[転送フィルタ]

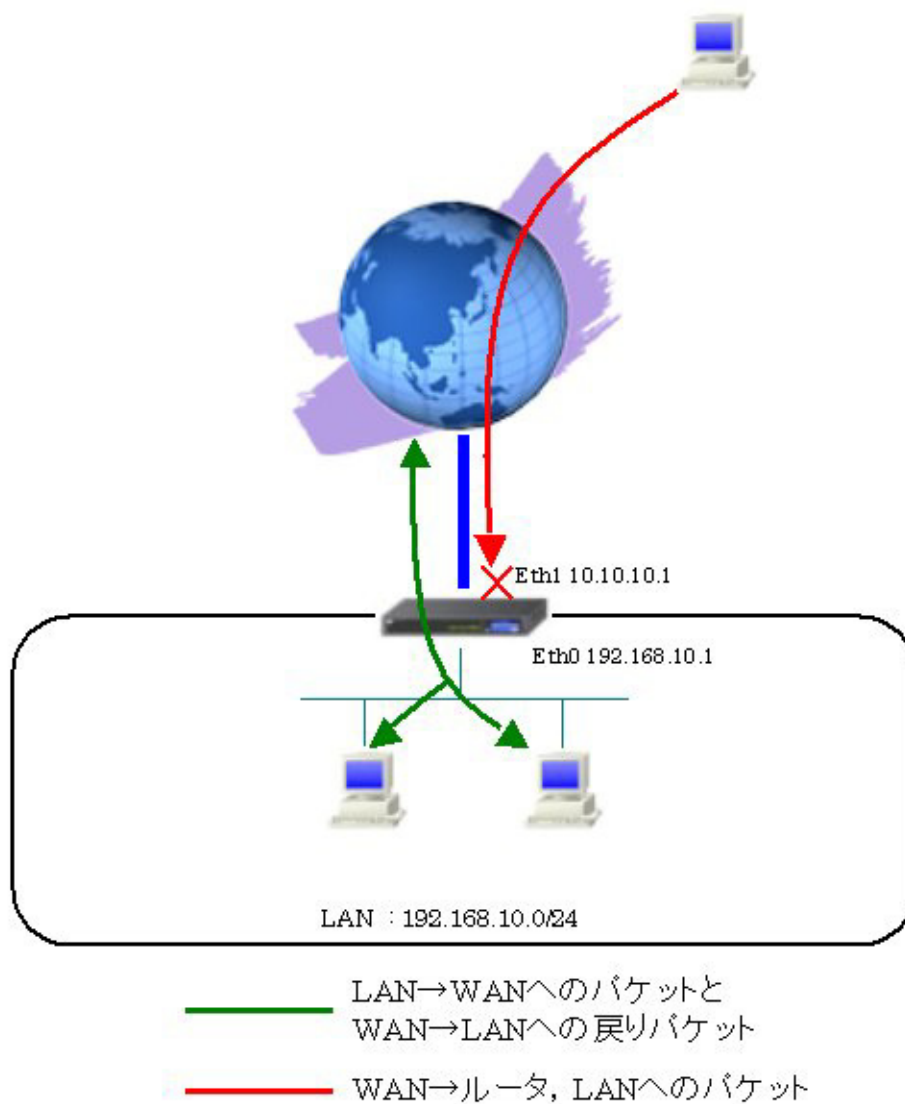
LAN 上にある WEB サーバ, TELNET サーバをインターネットからアクセス可能にするための設定をします。
インターネットからの WEB サーバ (TCP ポート 80 番) 宛のパケットを許可しています。
インターネットから送信元 IP アドレス「10.20.10.1」で TELNET サーバ (TCP ポート 23 番) 宛のパケットを許可しています。
インターネットから送信元 IP アドレス「10.20.10.1」以外の TELNET サーバ (TCP ポート 23 番) 宛のパケットを破棄しています。

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	宛先アドレス	宛先ポート	ICMP type/code	送信元MACアドレス
eth1	パケット受信時	許可	tcp				80		
eth1	パケット受信時	許可	tcp	10.20.10.1			23		
eth1	パケット受信時	破棄	tcp				23		

4-3. 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ともいわれる機能です。

4-3-1. 構成図

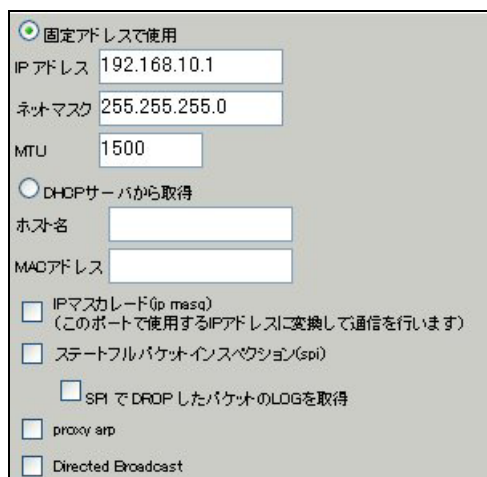


4-3-2. 設定例

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



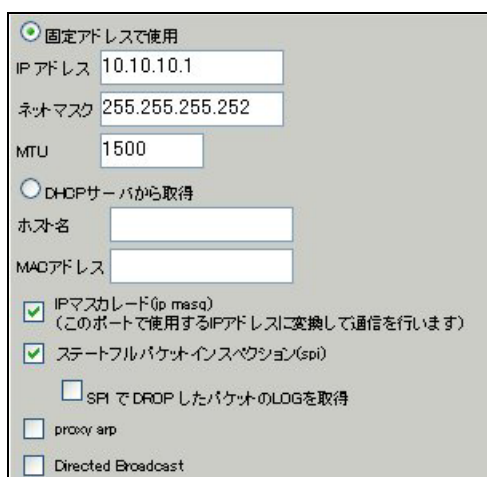
☒ 固定アドレスで使用
 IP アドレス 192.168.10.1
 ネットマスク 255.255.255.0
 MTU 1500
☐ DHCPサーバから取得
 ホスト名
 MACアドレス
☐ IPマスカレード(ip masq)
 (このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション spi
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

IP アドレスに「10.10.10.1」, ネットマスクに「255.255.255.252」を設定します。

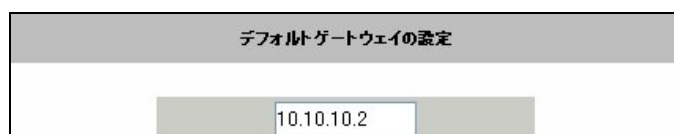
WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

※ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にしています。



☒ 固定アドレスで使用
 IP アドレス 10.10.10.1
 ネットマスク 255.255.255.252
 MTU 1500
☐ DHCPサーバから取得
 ホスト名
 MACアドレス
☒ IPマスカレード(ip masq)
 (このポートで使用するIPアドレスに変換して通信を行います)
☒ ステートフルパケットインスペクション spi
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[その他の設定]



デフォルトゲートウェイの設定

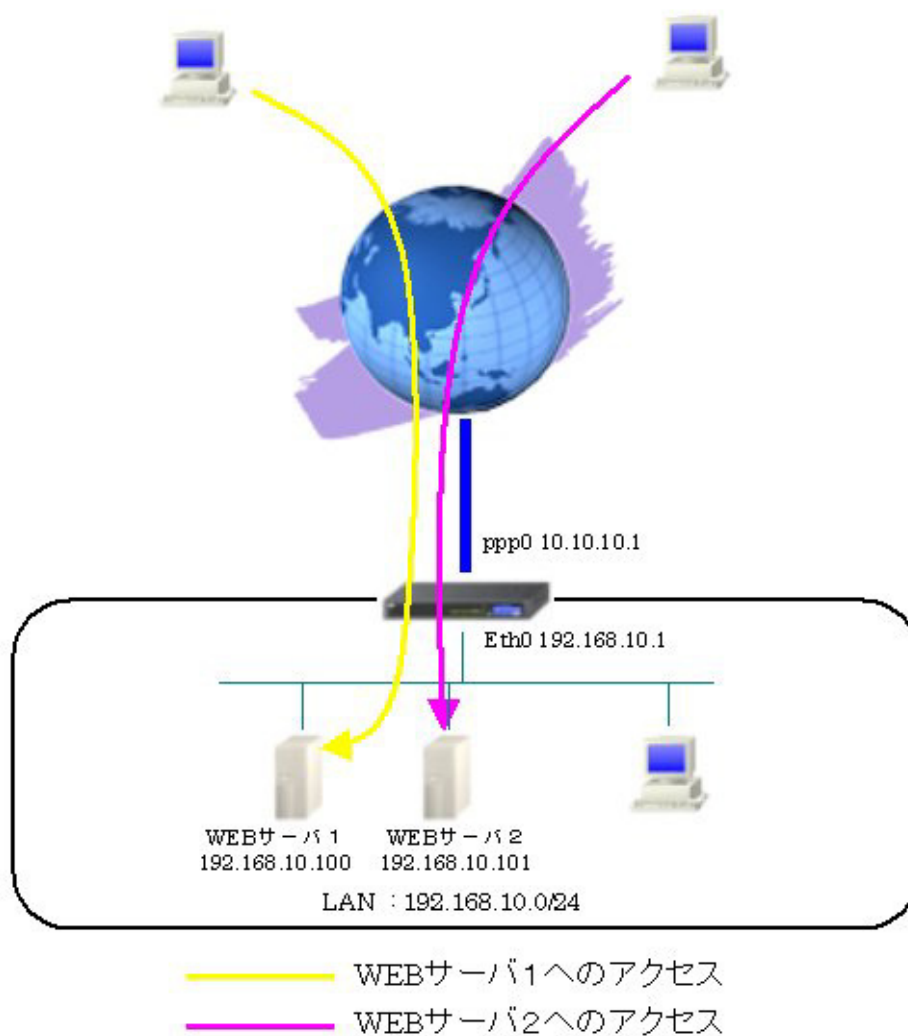
10.10.10.2

5. NAT/フィルタ応用設定

5-1. NAT でのサーバ公開 1 (ポートマッピング)

バーチャルサーバ設定例では変換前後のポート番号は同じでしたが、変換前後のポート番号を指定することにより、下記例のように複数の WEB サーバに対してのアクセスが可能になります。

5-1-1. 構成図



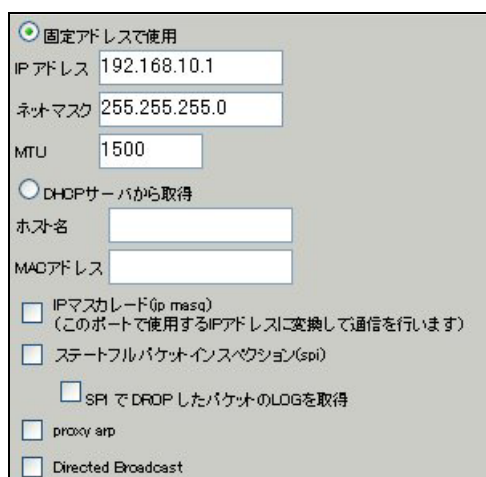
5-1-2. 設定例

グローバル IP アドレス「10.10.10.1」の TCP ポート 80 番宛てのパケットを受信した場合は、「192.168.10.100」 TCP ポート 80 番に、「10.10.10.1」で TCP ポート 8080 番宛てのパケットを受信した場合は、「192.168.10.101」 TCP ポート 80 番に NAT 変換します。

<<インタフェース設定>>

[Ethernet0 の設定]

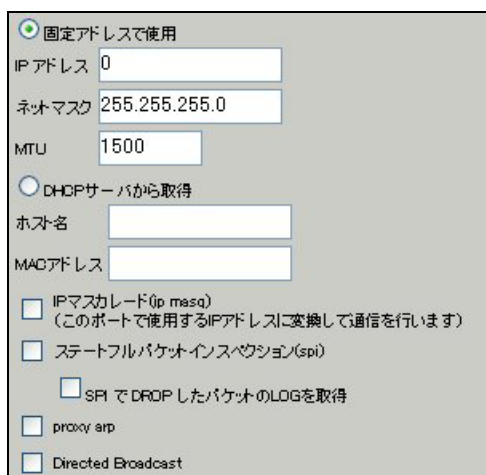
IP アドレスに「192.168.10.1」を設定します。



[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。



<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバ 1, 2 をインターネットからアクセス可能にするための設定をします。

インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ 1 (TCP ポート 80 番) 宛のパケットを許可します。

インターネットから宛先 IP アドレス「192.168.10.101」で WEB サーバ 2 (TCP ポート 80 番) 宛のパケットを許可します。

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	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット受信時	許可	tcp			192.168.10.100	80			☐
ppp0	パケット受信時	許可	tcp			192.168.10.101	80			☐

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ 1, 2 をインターネットからアクセス可能にするための設定をします。

インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、「192.168.10.100」TCP ポート 80 番に転送します。

インターネットから「10.10.10.1」で TCP ポート 8080 番宛てのパケットを受信した場合は、「192.168.10.101」TCP ポート 80 番に転送します。

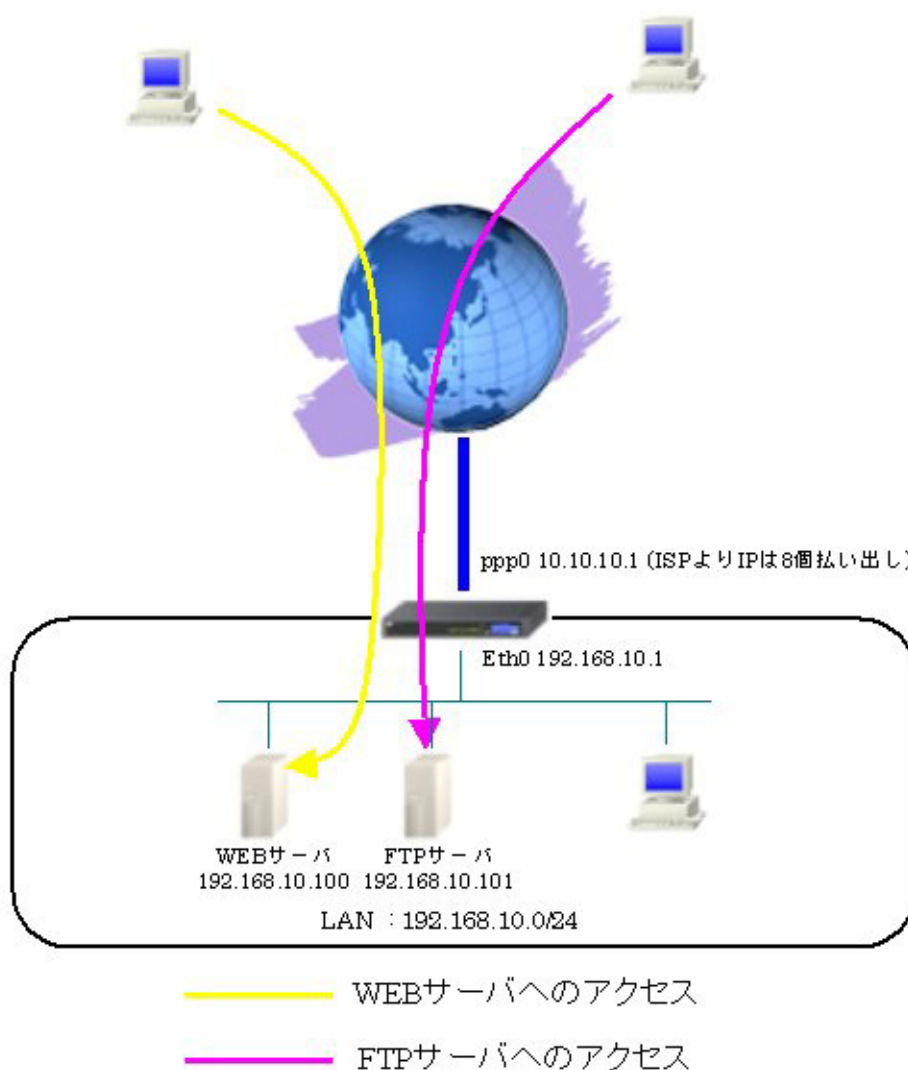
サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.10.100	10.10.10.1	tcp	80	ppp0
192.168.10.101:80	10.10.10.1	tcp	8080	ppp0

5-2. NAT でのサーバ公開 2 (複数 IP+PPPoE)

複数のグローバル IP アドレスが割り当てられる場合、それぞれのグローバル IP アドレス毎にプライベート IP アドレスを持ったサーバに対してのバーチャルサーバ設定をすることにより、異なるグローバル IP アドレスでそれぞれのサーバに対してアクセスすることができます。

本設定例は WAN 側の回線に PPPoE を利用した例になります。

5-2-1. 構成図



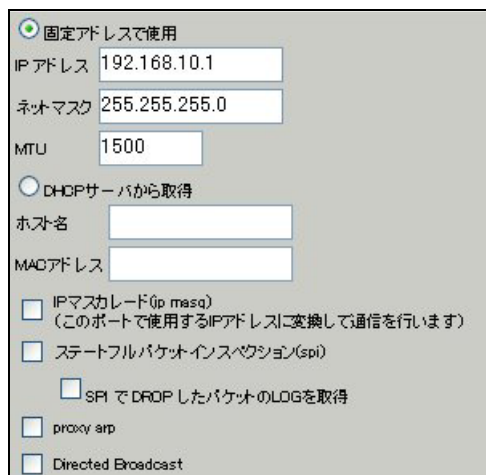
5-2-2. 設定例

グローバル IP アドレス「10.10.10.1」は「192.168.10.100」に、「10.10.10.2」は「192.168.10.101」に NAT 変換します。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

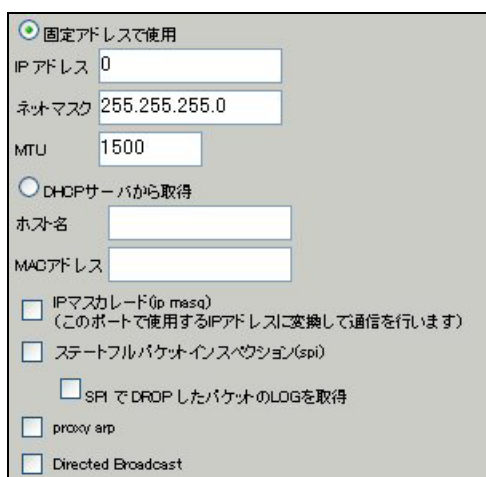


☒ 固定アドレスで使用
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルバケットインスペクション(spi)
☐ SPI で DROP したバケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。



☒ 固定アドレスで使用
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルバケットインスペクション(spi)
☐ SPI で DROP したバケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバ, FTP サーバへインターネットからアクセス可能にするための設定をします。
インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ (TCP ポート 80 番) 宛のパケットを許可します。

インターネットから宛先 IP アドレス「192.168.10.101」で FTP サーバ (TCP ポート 20, 21 番) 宛のパケットを許可します。

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	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット受信時	許可	tcp			192.168.10.100	80			☐
ppp0	パケット受信時	許可	tcp			192.168.10.101	20:21			☐

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ, FTP サーバへインターネットからアクセス可能にするための設定をします。
インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、
「192.168.10.100」TCP ポート 80 番に転送します。

インターネットから「10.10.10.2」で TCP ポート 20, 21 番宛てのパケットを受信した場合は、
「192.168.10.101」TCP ポート 20, 21 番に転送します。

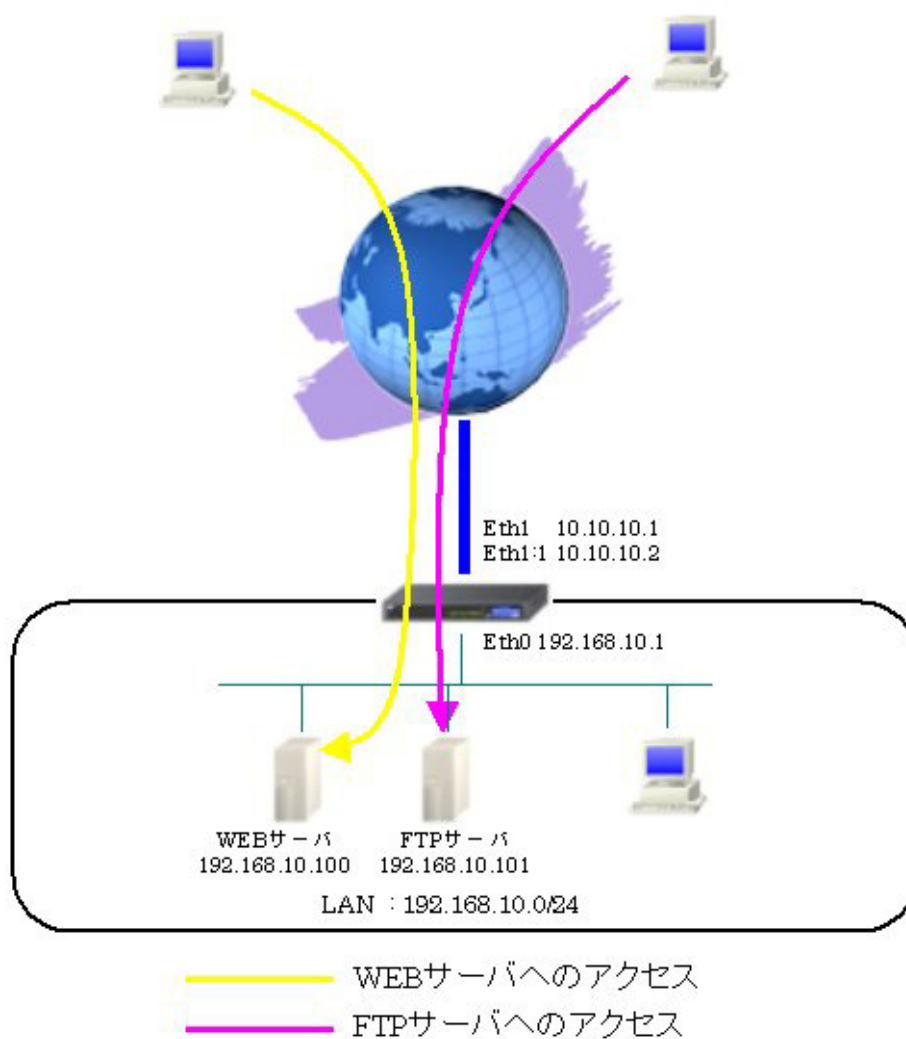
サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.10.100	10.10.10.1	tcp	80	ppp0
192.168.10.101	10.10.10.2	tcp	20:21	ppp0

5-3. NAT でのサーバ公開 3 (複数 IP+Ether)

複数のグローバル IP アドレスが割り当てられる場合、それぞれのグローバル IP アドレス毎にプライベート IP アドレスを持ったサーバに対してのバーチャルサーバ設定をすることにより、異なるグローバル IP アドレスでそれぞれのサーバに対してアクセスすることができます。

本設定例は WAN 側の回線に Ethernet を利用した例になります。

5-3-1. 構成図



5-3-2. 設定例

グローバル IP アドレス「10.10.10.1」は「192.168.10.100」に、「10.10.10.2」は「192.168.10.101」に NAT 変換します。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

The screenshot shows the configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. The checkboxes for 'IP Masquerade (ip masq)', 'Stateful Packet Inspection (spi)', 'SPI Log', 'proxy arp', and 'Directed Broadcast' are all unselected.

[Ethernet1 の設定]

IP アドレスに「10.10.10.1」, ネットマスクに「255.255.255.248」を設定します。

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にしています。WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

The screenshot shows the configuration window for Ethernet1. The 'Fixed IP Address' radio button is selected. The IP address is set to 10.10.10.1, the netmask to 255.255.255.248, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. The checkboxes for 'IP Masquerade (ip masq)' and 'Stateful Packet Inspection (spi)' are checked. The checkboxes for 'SPI Log', 'proxy arp', and 'Directed Broadcast' are unselected.

[その他の設定]

デフォルトゲートウェイの設定	
	10.10.10.6

<<仮想インタフェース設定>>

WAN 側で利用するグローバル IP アドレス「10.10.10.2」を設定します。

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
eth1	1	10.10.10.2	255.255.255.248

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバ、FTP サーバへインターネットからアクセス可能にするための設定をします。
インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ（TCP ポート 80 番）宛のパケットを許可します。

インターネットから宛先 IP アドレス「192.168.10.101」で FTP サーバ（TCP ポート 20, 21 番）宛のパケットを許可します。

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	宛先アドレス	宛先ポート	ICMP type/code	送信元MACアドレス	LOG
eth1	パケット受信時	許可	tcp			192.168.10.100	80			☐
eth1	パケット受信時	許可	tcp			192.168.10.101	20:21			☐

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバ、FTP サーバへインターネットからアクセス可能にするための設定をします。
インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、
「192.168.10.100」 TCP ポート 80 番に転送します。

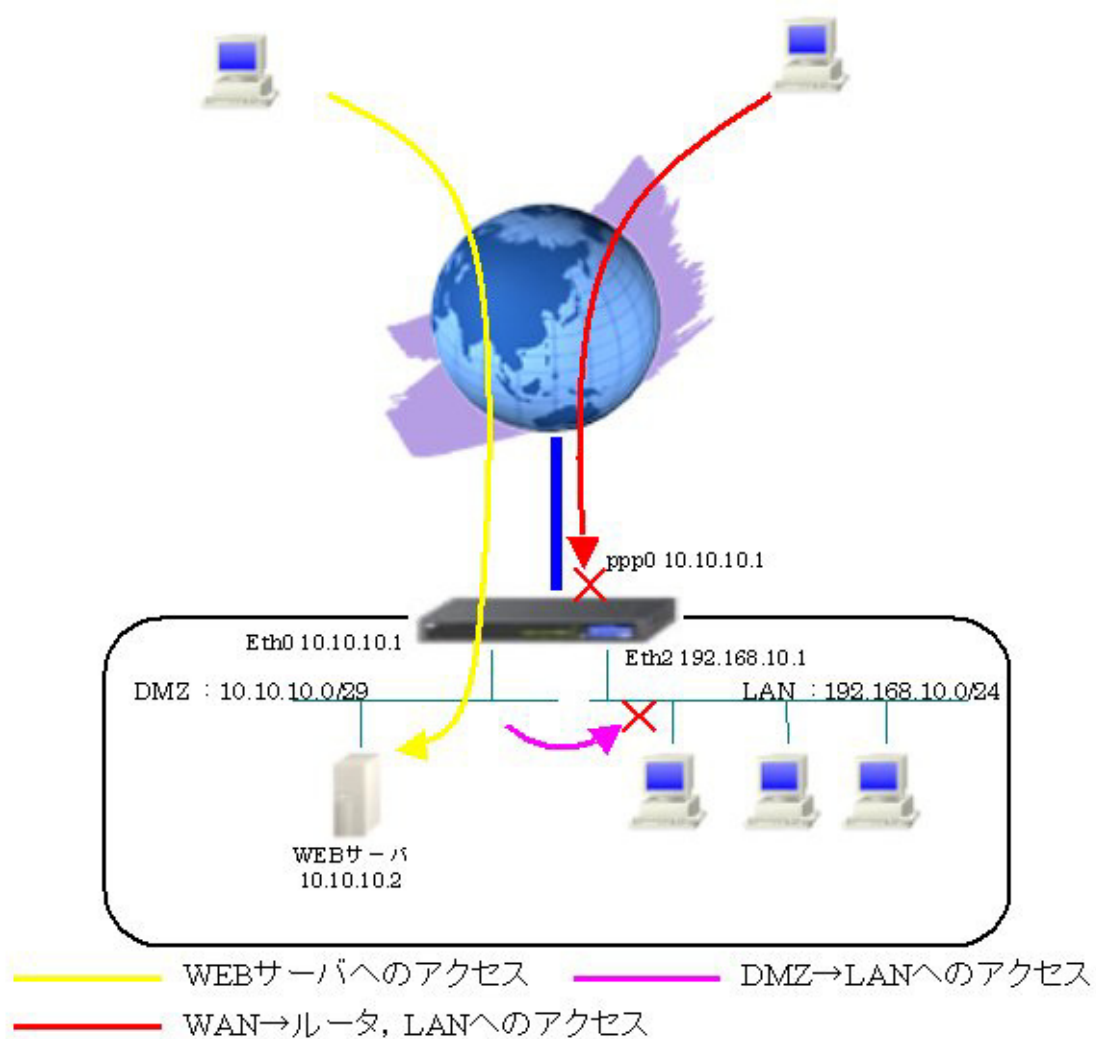
インターネットから「10.10.10.2」で TCP ポート 20, 21 番宛てのパケットを受信した場合は、
「192.168.10.101」 TCP ポート 20, 21 番に転送します。

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
192.168.10.100	10.10.10.1	tcp	80	eth1
192.168.10.101	10.10.10.2	tcp	20:21	eth1

5-4. DMZ 構築例 (PPPoE)

XR シリーズで XR-540/C のように 3 ポート (3 セグメント) 以上を有する製品では、インターネットに公開するサーバと社内 LAN を物理的に分けて構成することが可能です。

5-4-1. 構成図



5-4-2. 設定例

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「10.10.10.1」、ネットマスクに「255.255.255.248」を設定します。

DMZ から LAN, WAN へのアクセスを制限するために、ステートフルパケットインスペクションを「有効」に設定します。

☒ 固定アドレスで使用
IP アドレス 10.10.10.1
ネットマスク 255.255.255.248
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☒ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

☒ 固定アドレスで使用
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet2 の設定]

IP アドレスに「192.168.10.1」を設定します。

IP アドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500
☐ IP マスカレード (ip masq) (このポートで使用するIPアドレスに変換して通信を行います)	
☐ ステートフルパケットインスペクション (spi)	
☐ SPI で DROP したパケットの LOG を取得	
☐ proxy arp	
☐ Directed Broadcast	

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

ppp0 インタフェースに割り当てる IP アドレス「10.10.10.1」を設定します。

UnNumbered-PPP回線使用時に設定できます	
IPアドレス	10.10.10.1 回線接続時に割り付けるグローバルIPアドレスです

[接続設定]

IP マスカレードを「無効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MF(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROP したパケットの LOG を取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出
	☒ 非接続SessionのIPv4Packet受信時 PADTを強制送出
	☒ 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<フィルタ設定>>

[転送フィルタ]

DMZ 上にある WEB サーバに対してインターネットからアクセス可能にするための設定をします。

インターネット側からの宛先 IP アドレス「10.10.10.2」の WEB サーバ (TCP ポート 80 番) 宛のパケットを許可します。

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	宛先アドレス	宛先ポート	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット受信時	許可	tcp			10.10.10.2	80			☐

<<NAT 設定>>

[送信元 NAT]

LAN 上にある「192.168.10.0/24」のネットワーク内の端末の送信元 IP アドレスを ppp0 からパケット送信時に「10.10.10.1」に変換します。

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
192.168.10.0/24	10.10.10.1	ppp0

5-4-3. 設定例補足

本設定例では DMZ 内の端末からの WAN アクセスを制限しています。設定としては、「インタフェース設定」→「Ethernet0 の設定」の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ためです。

WAN アクセスを許可する場合は、以下の設定を追加する必要があります。

<<フィルタ設定>>

[転送フィルタ]

DMZ 上にある端末からインターネットへアクセス可能にするための設定をします。

ppp0 から送信される送信元 IP アドレス「10.10.10.0/29」の packets を許可します。

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	宛先アドレス	宛先ポート	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット送信時	許可	全て	10.10.10.0/29						☐

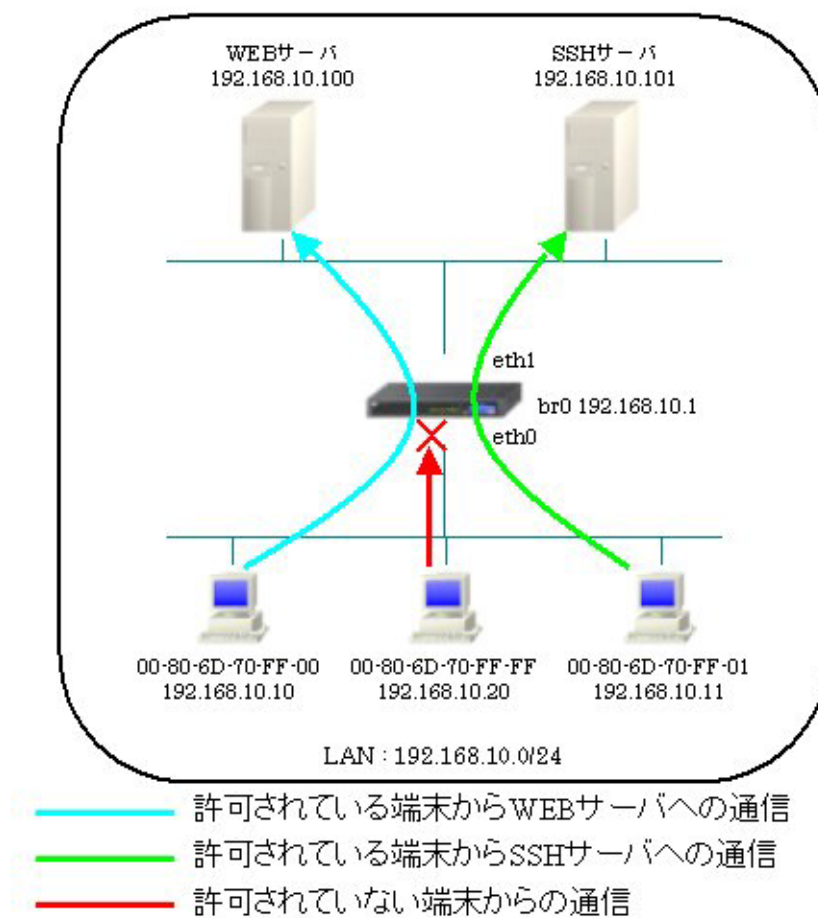
6. ブリッジフィルタ設定

6-1. 同一 LAN 内でのアクセス制御

XR をブリッジモードで使用することによりブリッジフィルタを使用することができます。

本設定例では同一 LAN 内の特定のエリアを XR で分離し、ブリッジフィルタで各サーバへのアクセスを制限しています。

6-1-1. 構成図



6-1-2. 設定例

同一 LAN 内にある WEB サーバおよび SSH サーバへのアクセスを制限します。

<<インタフェース設定>>

[Bridge の設定]

ブリッジインタフェースのインタフェース番号を設定します。

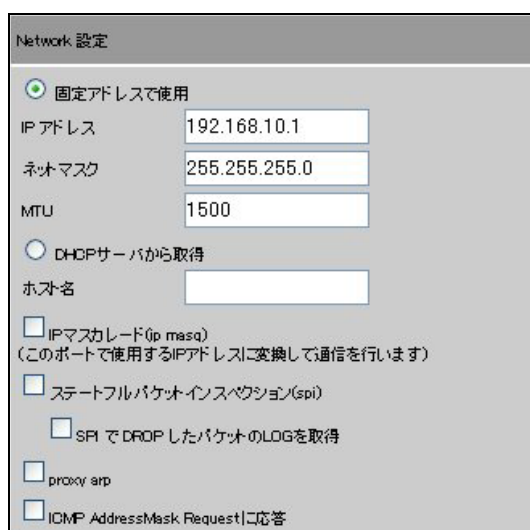
本設定例では、Ethernet0 と Ethernet1 でブリッジを設定します。



The screenshot shows the 'Basic Settings' (基本設定) tab for a bridge. The 'Interface Name' (インターフェース名) is set to 'br0' with a range of '[0-4095]' and a 'Valid' (有効) checkbox checked. Under the 'Interface Settings' (Interface 設定) section, 'Ethernet0' and 'Ethernet1' are selected with checkboxes, while 'Ethernet2' is not. The 'Use' (使用する) radio button is selected, and the 'VLAN ID' field is empty.

IP アドレスに「192.168.10.1」、ネットマスクに「255.255.255.0」を設定します。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。



The screenshot shows the 'Network Settings' (Network 設定) tab. The 'Fixed Address Usage' (固定アドレスで使用する) radio button is selected. The 'IP Address' (IP アドレス) is '192.168.10.1' and the 'Netmask' (ネットマスク) is '255.255.255.0'. The 'MTU' is set to '1500'. The 'DHCP Server Acquisition' (DHCPサーバから取得) radio button is not selected. The 'Host Name' (ホスト名) field is empty. Several checkboxes are present: 'IP Masquerade (p masq)' (IPマスカレード(p masq)), 'Stateful Packet Inspection (spi)' (ステートフルパケットインスペクション spi), 'SPI Log' (SPI で DROP したパケットのLOGを取得), 'Proxy ARP' (proxy arp), and 'ICMP AddressMask Request Response' (ICMP AddressMask Request 応答). The first three checkboxes are unchecked.

<<ブリッジフィルタ設定>>

ブリッジフィルタは全て詳細設定で設定を行っています。

<転送フィルタ>

[No. 1]

eth0→eth1 への送信元 MAC アドレス「00:80:6D:70:FF:00」の端末からの ARP フレームを許可する設定をします。

No.	1
入力インタフェース	☐ Not eth0
出力インタフェース	☐ Not eth1
送信元MACアドレス	☐ Not
宛先MACアドレス	☐ Not
Policy	許可 v
待機	☐ 有効

● ARP	OPCODE	☐ Not ---- v	[0-65535]
	送信元MACアドレス	☐ Not 00:80:6D:70:FF:00	
	宛先MACアドレス	☐ Not	
	送信元IPアドレス	☐ Not	
	宛先IPアドレス	☐ Not	

[No. 2]

eth0→eth1 への送信元 MAC アドレス「00:80:6D:70:FF:00」の端末からのプロトコルタイプが IPv4 で送信元 IP アドレス「192.168.10.10」、宛先 IP アドレス「192.168.10.100」TCP ポート 80 番宛のフレームを許可する設定をします。

No.	2
入力インタフェース	☐ Not eth0
出力インタフェース	☐ Not eth1
送信元MACアドレス	☐ Not 00:80:6D:70:FF:00
宛先MACアドレス	☐ Not
Policy	許可 v
待機	☐ 有効

● IPv4	送信元IPアドレス	☐ Not 192.168.10.10	
	宛先IPアドレス	☐ Not 192.168.10.100	
	TOS	☐ Not	
	IP Protocol	☐ Not TCP v	
	送信元ポート	☐ Not	[1-65535]*
	宛先ポート	☐ Not 80	[1-65535]*

[No. 3]

eth0→eth1 への送信元 MAC アドレス「00:80:6D:70:FF:01」の端末からの ARP フレームを許可する設定をします。

No.	3
入カインタフェース	☐ Not eth0
出カインタフェース	☐ Not eth1
送信元MACアドレス	☐ Not
宛先MACアドレス	☐ Not
Policy	許可 ▼
待機	☐ 有効

● ARP	OPCODE	☐ Not	----	[0-65535]
	送信元MACアドレス	☐ Not	00:80:6D:70:FF:01	
	宛先MACアドレス	☐ Not		
	送信元IPアドレス	☐ Not		
	宛先IPアドレス	☐ Not		

[No. 4]

eth0→eth1 への送信元 MAC アドレス「00:80:6D:70:FF:01」の端末からのプロトコルタイプが IPv4 で送信元 IP アドレス「192.168.10.11」、宛先 IP アドレス「192.168.10.101」TCP ポート 22 番宛のフレームを許可する設定をします。

No.	4
入カインタフェース	☐ Not eth0
出カインタフェース	☐ Not eth1
送信元MACアドレス	☐ Not 00:80:6D:70:FF:01
宛先MACアドレス	☐ Not
Policy	許可 ▼
待機	☐ 有効

● IPv4	送信元IPアドレス	☐ Not	192.168.10.11	
	宛先IPアドレス	☐ Not	192.168.10.101	
	TOS	☐ Not		
	IP Protocol	☐ Not	TCP ▼	
	送信元ポート	☐ Not		[1-65535]*
	宛先ポート	☐ Not	22	[1-65535]*

[No. 5]

eth0→eth1 へのその他の通信は破棄する設定をします。

No.	5
入力インタフェース	☐ Not eth0
出力インタフェース	☐ Not eth1
送信元MACアドレス	☐ Not
宛先MACアドレス	☐ Not
Policy	破棄 ▼
待機	☐ 有効

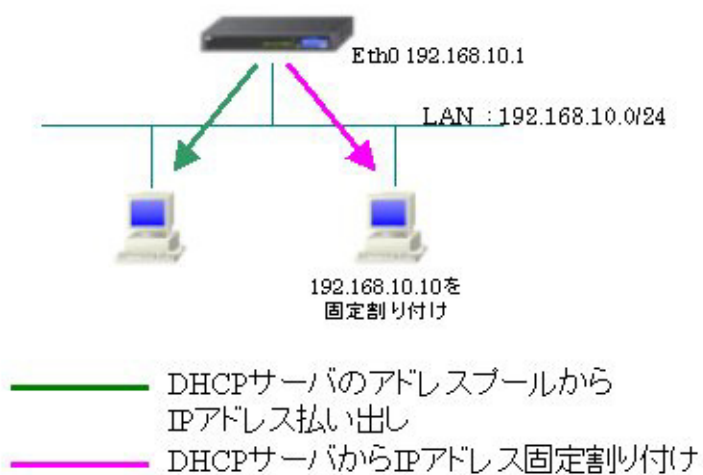
7. DHCP 設定

7-1. DHCP サーバ設定

DHCP サーバとして利用することにより、LAN 側の端末に自動的に IP アドレス等の設定を行うことが可能です。

また IP アドレスの固定割り付けの設定を行うことにより、DHCP クライアントの MAC アドレス毎に常に同じ IP アドレスを割り当てることができます。

7-1-1. 構成図



7-1-2. 設定例

MAC アドレス「00:80:6d:70:ff:ff」の端末には IP アドレス「192.168.10.10」を割り当て、その他の端末にはリース範囲の IP アドレスを割り当てます。

なお固定割り付けで割り当てる IP アドレスはリース範囲外である必要があります。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

<<各種サービスの設定>>

<DHCP (Relay) サーバ>

[DHCP 設定]

「DHCP サーバを使用する」を選択します。

[DHCP サーバ設定]

DHCP サーバで割り当てる IP アドレスの範囲等を設定します。

使用する	☒
インタフェース	eth0
ネットワーク	192.168.10.0
サブネットマスク	255.255.255.0
ブロードキャスト	192.168.10.255
リース開始アドレス	192.168.10.100
リース終了アドレス	192.168.10.200
ルータアドレス	192.168.10.1
ドメイン名	example.co.jp
プライマリDNS	192.168.10.1
セカンダリDNS	
標準リース時間	600
最大リース時間	7200
プライマリMINSサーバ	
セカンダリMINSサーバ	
スコープID	

[DHCP IP アドレス固定割り付け設定]

MAC アドレス「00:80:6d:70:ff:ff」の端末に IP アドレス「192.168.10.10」を割り付けます。

MACアドレス	IPアドレス
00:80:6d:70:ff:ff	192.168.10.10

【DHCP (Relay) サーバ】

DHCP (Relay) サーバを起動します。

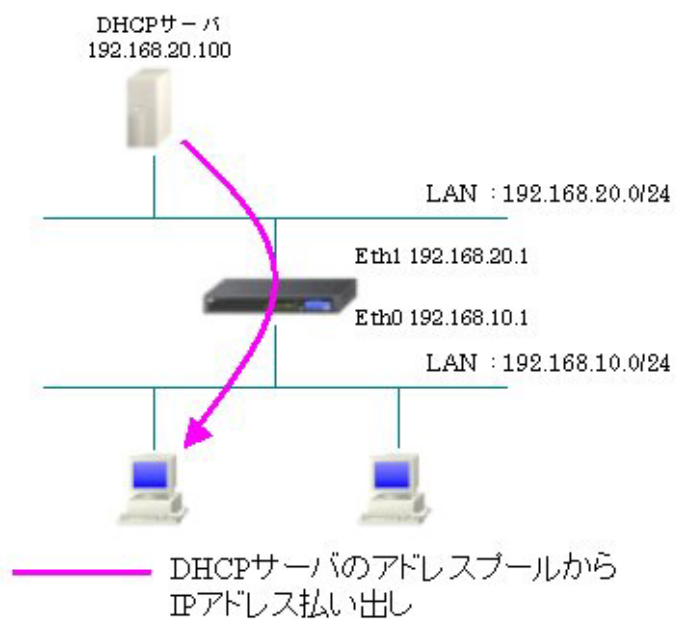
※動作中の場合は、一度「停止」→「起動」を行ってください。

DHCP(Relay)サーバ	☐ 停止 ☒ 起動
----------------	--

7-2. DHCP リレー設定

DHCP リレー機能を利用することにより、異なるネットワークにある DHCP サーバで IP アドレスを一括管理している場合、XR 経由で端末に IP アドレスを払い出すことができます。

7-2-1. 構成図



7-2-2. 設定例

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

The screenshot shows the configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Below these fields are several checkboxes: 'IP Masquerade (ip masq)' (unchecked), 'Stateful Packet Inspection (spi)' (unchecked), 'SPI Log' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

[Ethernet1 の設定]

IP アドレスに「192.168.20.1」を設定します。

The screenshot shows the configuration window for Ethernet1. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.20.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Below these fields are several checkboxes: 'IP Masquerade (ip masq)' (unchecked), 'Stateful Packet Inspection (spi)' (unchecked), 'SPI Log' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

<<各種サービスの設定>>

<DHCP (Relay) サーバ>

[DHCP 設定]

「DHCP リレーを使用する」を選択します。

DHCP サーバの IP アドレスとして「192.168.20.100」を設定します。

サーバの選択	☐ DHCPサーバを使用する ☒ DHCPリレーを使用する
DHCPリレーサーバ使用時に設定して下さい	
上位DHCPサーバの IPアドレス	192.168.20.100
DHCP relay over XXX	☒ 使用しない ☐ 使用する

【DHCP (Relay) サーバ】

DHCP (Relay) サーバを起動します。

※動作中の場合は、一度「停止」→「起動」を行ってください。

DHCP(Relay)サーバ	☐ 停止 ☒ 起動
----------------	--

8. 攻撃検出設定

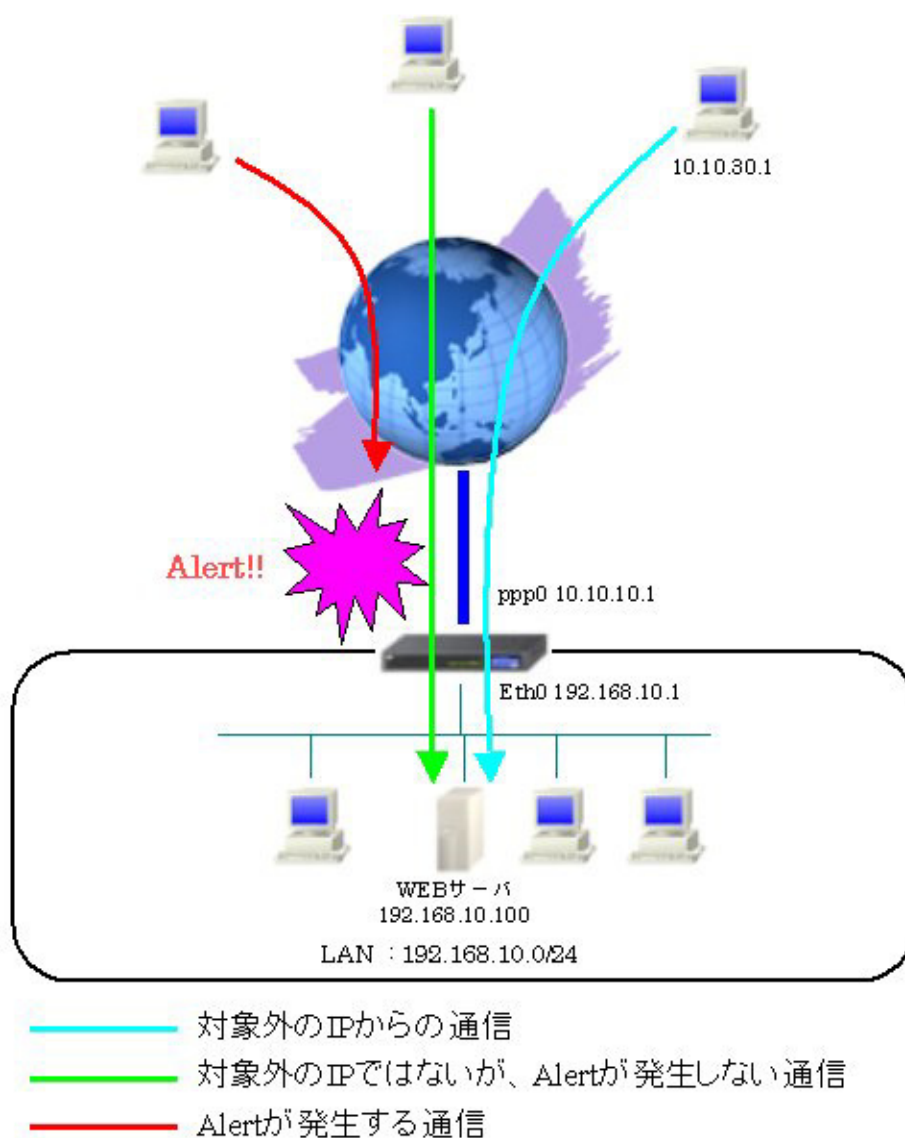
8-1. アクティブファイアウォールの利用

攻撃検出機能により Alert が発生した場合、その後同一の IP アドレスからの通信を自動でブロックすることができます。

通信のブロックは一定時間経過後に解除されます。

本設定例では、バーチャルサーバ機能を利用して Web サーバを公開し、フィルタ設定でポート番号 80 のみ許可しています。

8-1-1. 構成図



8-1-2. 設定例

「IP アドレス 10.10.10.1 ポート 80」を「IP アドレス 192.168.10.100 ポート 80」に NAT 変換します。
攻撃検出機能を有効に、アクティブファイアウォールを使用します。ただし対象外 IP アドレスとして
「10.10.30.1」を設定しています。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

固定アドレスで使用
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

固定アドレスで使用
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLDP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバへインターネットからアクセス可能にするための設定をします。

インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ（TCP ポート 80 番）宛のパケットを許可します。

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	宛先アドレス	宛先ポート	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット受信時	許可	tcp			192.168.10.100	80			☐

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバへインターネットからアクセス可能にするための設定をします。

インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、「192.168.10.100」TCP ポート 80 番に転送します。

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
192.168.10.100	10.10.10.1	tcp	80	ppp0

<<各種サービスの設定>>

<攻撃検出サービス>

[インタフェース設定]

攻撃検出を行うインタフェースとして「ppp0」、IP アドレスとして「10.10.10.1」を設定します。

攻撃検出後のブロック時間を「5」分とし、False Positive Unblock を「無効」に設定しています。

※False Positive Unblock とは本来攻撃ではないが、攻撃と間違えて遮断する可能性のあるものをブロック “しない”（「有効」）か “する”（「無効」）かを設定します。

本設定例では、本来攻撃ではない通信もブロックの対象としています。

インタフェース	ppp0
IPアドレス	10.10.10.1
ブロック時間	5 分
False Positive Unblock	☐ 有効 ☒ 無効

[対象外 IP アドレス設定]

通信をブロックしない送信元 IP アドレスとして「10.10.30.1」を設定しています。

※仮に対象外 IP アドレスからの攻撃を検出しても通信のブロック対象とはなりません。

対象外IPアドレス
10.10.30.1

【攻撃検出サービス】

攻撃検出サービスを起動します。

※動作中の場合は、一度「停止」→「起動」を行ってください。

攻撃検出サービス	☐ 停止 ☒ 起動
----------	--

8-1-3. 設定例補足（メール送信設定）

本設定例では攻撃検出サービスにより不正アクセスを検知し、ブロックします。

この設定に加えてメール送信設定をおこなうことにより、ブロックした送信元 IP アドレスをメールで通知するといったことも可能です。

<<システム設定>>

<メール送信機能の設定>

[基本設定]

メール送信のための基本設定を行います。

本設定例では、メール認証の方式として SMTP-Auth(plain) を使用しています。

基本設定	
メール認証	☐ 認証しない ☐ POP before SMTP ☐ SMTP-Auth(login) ☒ SMTP-Auth(plain)
SMTPサーバアドレス	smtp.example.co.jp
SMTPサーバポート	25
POPサーバアドレス	
ユーザID	xr
パスワード	systemmail

シスログメールを送信するための設定を行います。

検出文字列の指定では、「Blocking host」を指定しています。これによりシスログで「Blocking host」の文字列と一致したログが出力された場合にメールを送信することができます。

以下は送信時のメール内容例です。

Jun 30 14:35:29 localhost snortsam[6122]: Blocking host 10.10.50.1 completely for 300 seconds (Sig_ID: 100000121).

シスログのメール送信	
ログのメール送信	☐ 送信しない ☒ 送信する
送信先メールアドレス	admin@example.co.jp
送信元メールアドレス	xr@example.co.jp
件名	Log keyword detection
検出文字列の指定	文字列は1行に255文字まで、最大32個(行)までです。 Blocking host

【DNS キャッシュ】

メール送信時の名前解決を可能にするため、DNS キャッシュ機能を起動します。

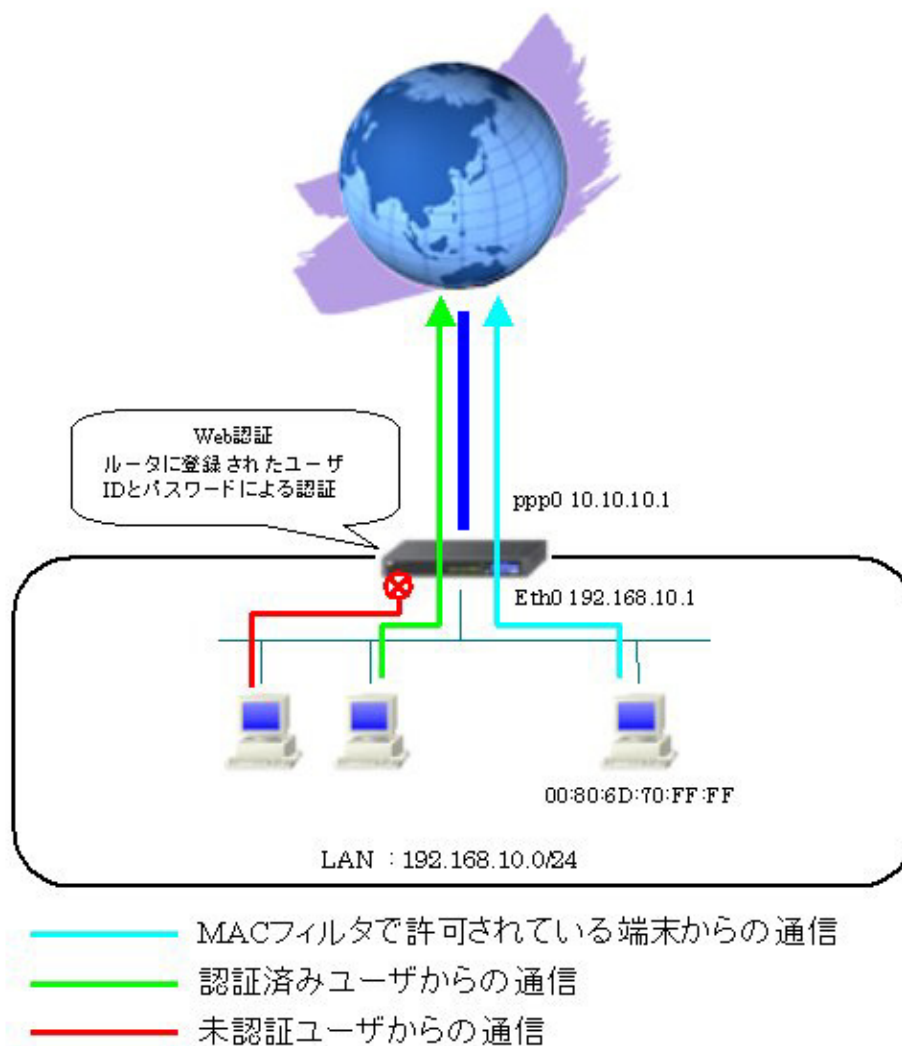


9. Web 認証設定（ゲートウェイ認証設定）

9-1. ユーザ認証

XR を経由する通信を行う場合に、XR でユーザ ID、パスワードによる認証を必要とするように設定することが可能です。これにより外部へアクセスできるユーザを制限するといった利用方法も可能になります。

9-1-1. 構成図



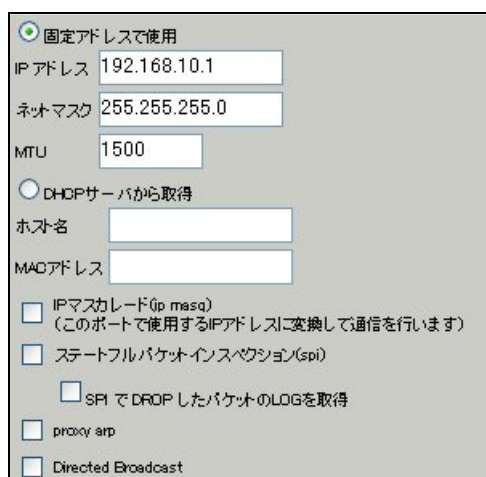
9-1-2. 設定例

Web 認証機能の MAC フィルタで許可されている端末「00:80:6D:70:FF:FF」のみ認証を必要とせず、その他の端末は認証を必要とするように設定します。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



☒ 固定アドレスで使用する

IP アドレス 192.168.10.1

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

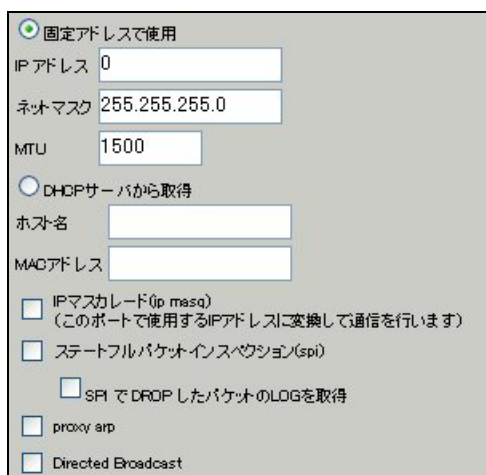
☐ proxy arp

☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。



☒ 固定アドレスで使用する

IP アドレス 0

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<Web 認証設定>>

[基本設定]

インターネット側へ通信する際に XR でのユーザ認証を必要とするように設定します。

また MAC アドレスフィルタを利用するため、「使用する」を選択しています。

基本設定		
本機能	☐ 使用しない	☒ 使用する
認証	☐ しない (URL転送のみ)	☒ する
80/tcp 監視	☒ 行わない	☐ 行う
MACアドレスフィルタ	☐ 使用しない	☒ 使用する

URL 転送は行わないため、設定していません。

URL転送		
URL		
通常認証後	☒ 行わない (デフォルト)	☐ 行う
強制認証後	☒ 行わない (エンドユーザ要求URL)	☐ 行う

XR でアカウントの管理を行うため、「ローカル」を選択します。

認証方法		
☒ ローカル	☐ RADIUSサーバ→ローカル	☐ RADIUSサーバ

認証で許可された通信が無通信状態となってから 30 分経過した場合は、切断するよう設定しています。

接続許可時間	
☒ アイドルタイムアウト	30 分 (1~43200)
☐ 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	

[ユーザ設定]

認証で使用するユーザ ID、パスワードを設定します。

ユーザID	パスワード
user	pass

[MAC アドレスフィルタ]

認証を必要とせず通信が可能な端末を登録します。インタフェースはフィルタリングを行うインタフェースを設定します。

MACアドレスフィルタの追加	
MACアドレス	00:80:6d:70:ff:ff
インタフェース	eth0
動作	許可 ▼

MAC アドレスフィルタ登録後は、以下のように表示されます。

MACアドレス	インタフェース	動作	設定変更
00:80:6d:70:ff:ff	eth0	許可	編集 削除

[ログ設定]

Web 認証時のアクセスログおよびエラーログを取得するように設定しています。

※ログを取得する場合は、SYSLOG サービスは必ず「起動」してください。

エラーログ	☐ 使用しない	☒ syslogに取る
アクセスログ	☐ 使用しない	☒ syslogに取る

9-1-3. 設定例補足（ユーザ認証方法）

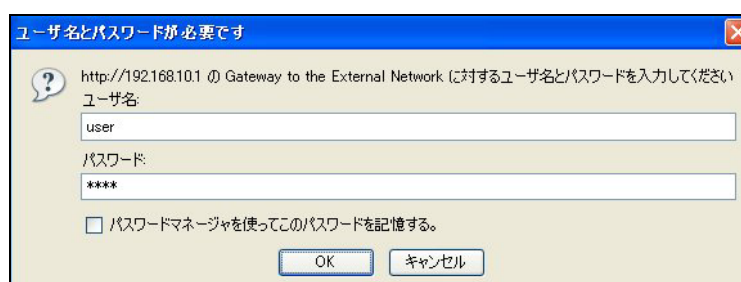
本設定例では端末から一度 XR にアクセスし、そこで認証を行う必要があります。

端末から XR の認証画面にアクセスします。

アクセスする際は本設定例の場合、以下の形式でアドレスを指定してアクセスします。

http://192.168.10.1/login.cgi

アクセス後、認証画面がポップアップしますので、ユーザ ID、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、インターネット側へのアクセスが可能になります。

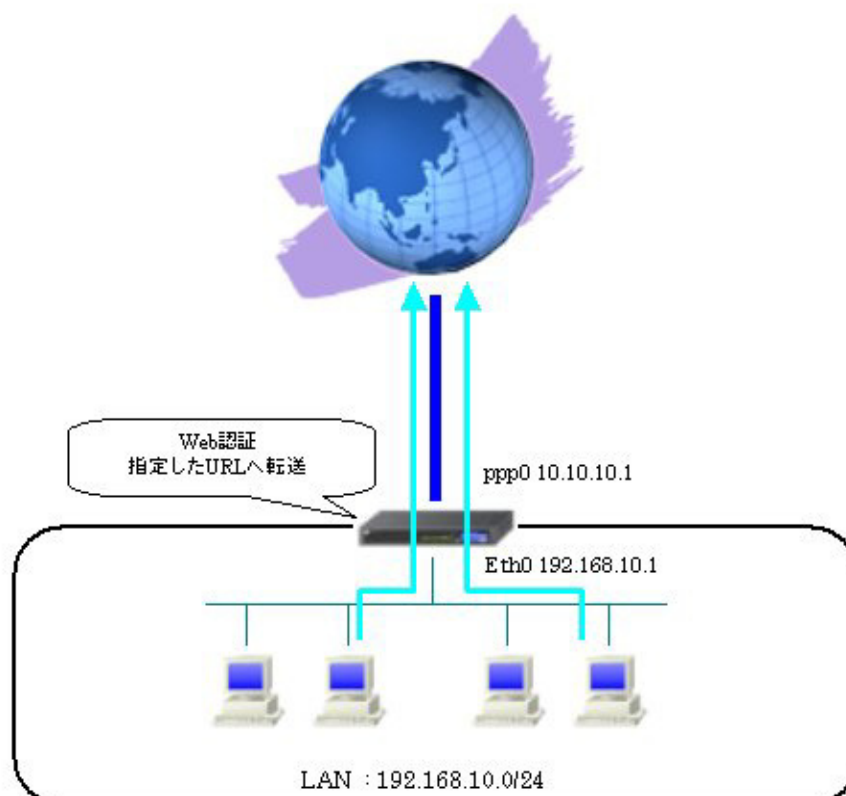
You can connect to the External Network (user@192.168.10.100).

Date: Tue Jul 1 14:07:00 2008

9-2. URL 転送

Web 認証機能では単にユーザ認証という用途だけではなく、XR 配下の端末が Web アクセスを行った際に、XR で指定した URL へ転送させるといったことも可能です。

9-2-1. 構成図



9-2-2. 設定例

ユーザ認証を行わず URL 転送を行う場合、あらかじめ許可しておく通信を設定しておく必要があります。本設定例では Web 認証フィルタで UDP ポート 53 番をあらかじめ許可しています。それ以外の通信に関しては、あらかじめ許可されていないため、Web 認証による URL 転送後に通信可能になります。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

☒ 固定アドレスで使用する
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルバケットインスペクション(spi)
☐ SPI で DROP したバケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。

☒ 固定アドレスで使用する
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルバケットインスペクション(spi)
☐ SPI で DROP したバケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<Web 認証設定>>

[基本設定]

インターネット側へ通信する際にユーザ認証を必要とせず、URL 転送のみ行うように設定しています。
80/tcp 監視を「行う」を選択し、TCP ポート 80 番の接続があったときに、強制的に Web 認証を行うように設定します。

基本設定		
本機能	☐ 使用しない	☒ 使用する
認証	☒ しない (URL 転送のみ)	☐ する
80/tcp 監視	☐ 行わない	☒ 行う
MACアドレスフィルタ	☒ 使用しない	☐ 使用する

転送する URL を設定します。

強制認証後に URL 転送が行われるように設定します。

URL 転送		
URL	http://www.centurysys.co.jp	
通常認証後	☒ 行わない (デフォルト)	☐ 行う
強制認証後	☐ 行わない (エンドユーザ要求URL)	☒ 行う

Web 認証で許可された通信が無通信状態となってから 30 分経過した場合は、切断するよう設定しています。

接続許可時間	
☒ アイドルタイムアウト	30 分 (1~43200)
☐ 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	

[フィルタ設定]

あらかじめ許可しておく通信として UDP ポート 53 番を許可しています。

これにより Web アクセス時に行う名前解決は、Web 認証の対象とはならないようにしています。

※このフィルタ設定は「フィルタ設定」→「Web 認証フィルタ」と同じものです。

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	宛先アドレス	宛先ポート	ICMP type/code	送信元MACアドレス	LOG
eth0	パケット受信時	許可	udp				53			☐

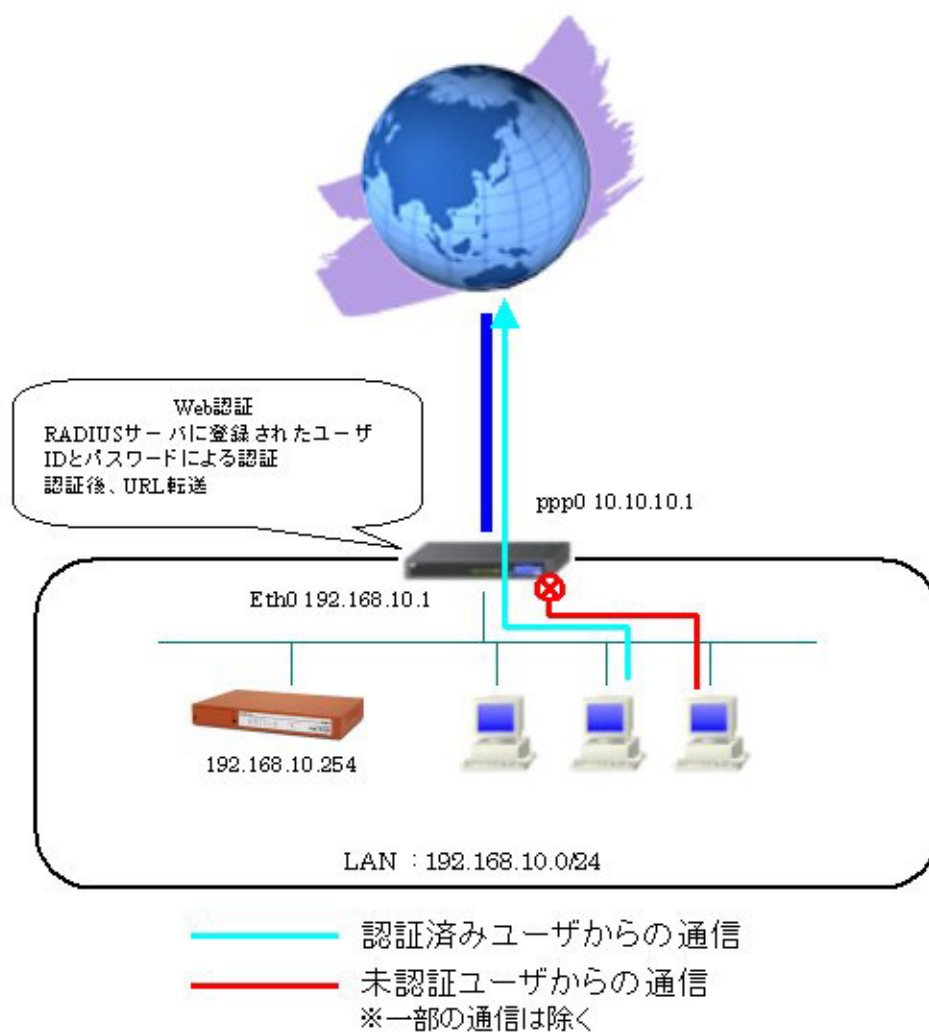
9-3. ユーザ強制認証+URL 転送+RADIUS 連携

Web 認証機能で TCP ポート 80 番の接続を監視し、この接続があった際に認証画面がポップアップするように設定することが可能です。

そしてユーザ認証成功後、指定した URL へ転送することも可能です。

またアカウントの管理を XR ではなく、RADIUS サーバで管理することも可能です。本設定例では RA-630 でアカウントの管理を行っています。

9-3-1. 構成図



9-3-2. 設定例

《XR の設定》

Web 認証機能で 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際に認証画面がポップアップするように設定します。

その際あらかじめ許可しておく通信を設定しておく必要があります。

本設定例では Web 認証フィルタで UDP ポート 53 番をあらかじめ許可しています。それ以外の通信に関しては、あらかじめ許可されていないため、Web 認証によるユーザ認証後、通信可能になります。

《＜インターフェース設定＞》

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

☒ 固定アドレスで使用する
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※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、この論理インターフェースを使って PPPoE 接続を行います。

☒ 固定アドレスで使用する
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<Web 認証設定>>

[RADIUS 設定]

RADIUS サーバに関する設定を行います。

本設定例ではアトリビュートとして「Idle-Timeout」を設定しています。これにより RADIUS サーバより送信される Idle-Timeout を利用することが可能です。

プライマリサーバ設定	
IPアドレス	192.168.10.254
ポート番号	☐ 1645 ☒ 1812 ☐ 手動設定
secret	secret

サーバ共通設定	
NAS-IP-Address	192.168.10.1
NAS-Identifier	XR

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	Idle-Timeout_28 ▼
セッションタイムアウト	指定しない ▼

[基本設定]

TCP ポート 80 番の接続を監視し、この接続があった際に認証画面がポップアップするように、80/tcp 監視を「行う」を選択します。

基本設定		
本機能	☐ 使用しない	☒ 使用する
認証	☐ しない (URL転送のみ)	☒ する
80/tcp 監視	☐ 行わない	☒ 行う
MACアドレスフィルタ	☒ 使用しない	☐ 使用する

転送する URL を設定します。

強制認証後に URL 転送が行われるように設定します。

URL 転送		
URL	http://www.centurysys.co.jp	
通常認証後	☒ 行わない (デフォルト)	☐ 行う
強制認証後	☐ 行わない (エンドユーザ要求URL)	☒ 行う

RADIUS サーバでのみアカウントの管理を行うため、「RADIUS サーバ」を選択します。

認証方法		
☐ ローカル	☐ RADIUSサーバ→ローカル	☒ RADIUSサーバ

接続許可時間は「アイドルタイムアウト」を選択します。

※RADIUS サーバからの該当アトリビュートがなければ、ここで設定した値を使用します。

接続許可時間	
☒ アイドルタイムアウト	30 分 (1~43200)
☐ 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	

[フィルタ設定]

あらかじめ許可しておく通信として UDP ポート 53 番を許可しています。

これにより Web アクセス時に行う名前解決は、Web 認証の対象とはならないようにしています。

※このフィルタ設定は「フィルタ設定」→「Web 認証フィルタ」と同じものです。

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	ICMP type/code	送信元MACアドレス	LOG
eth0	パケット受信時	許可	udp				53			☐

《RA-630 の設定》

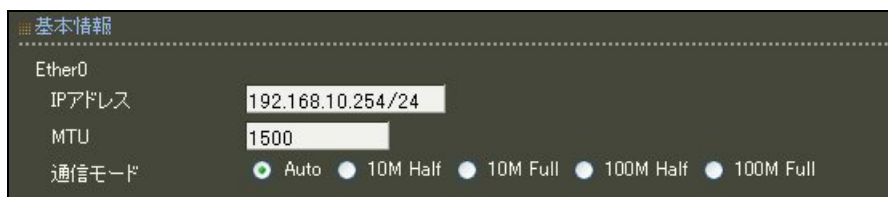
<<管理機能>>

<ネットワーク>

[基本情報]

Ether0 で IP アドレスに「192.168.10.254/24」を設定します。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。



設定後は以下のように表示されます。

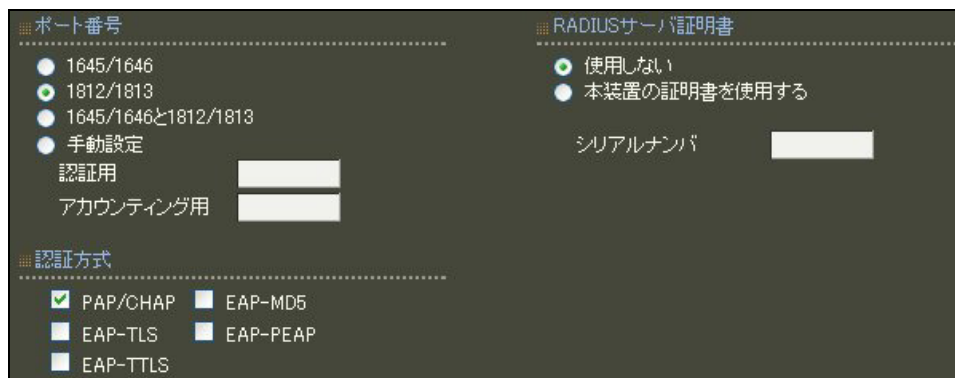
Ether0	IPアドレス	192.168.10.254/24	編集
	MTU	1500	
	通信モード	Auto	

<<RADIUS>>

<サーバ>

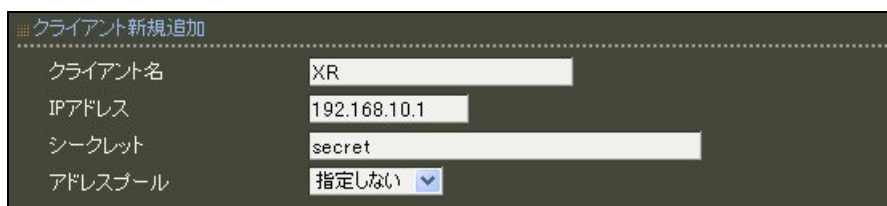
[基本情報]

XR で設定しているポート番号と同じポート番号「1812/1813」、認証方式として「PAP/CHAP」を選択します。



[クライアント]

RADIUS クライアントである XR の情報を登録します。



＜プロフィール＞

[ユーザ基本情報]

ユーザを作成するためにはユーザ基本情報プロフィールの作成が必要です。

認証方式として「PAP/CHAP」を選択します。

ユーザ基本情報プロフィール 新規追加	
プロフィール名	xrbasic
認証方式	PAP/CHAP
同時接続数	
IPアドレス割り当て	☒ 未使用 ☐ RADIUSクライアント ☐ アドレスプール ☐ 固定
アドレスプール	指定しない

[応答アトリビュート]

応答アトリビュートプロフィールを作成します。

応答アトリビュートプロフィール 新規追加	
プロフィール名	xrreply

応答アトリビュート一覧の「xrreply」の新規追加からアトリビュートとして「Idle-Timeout」を選択し、値として「1800」を設定しています。

応答アトリビュート 新規追加	
プロフィール名	xrreply
アトリビュート	Idle-Timeout
値	1800

[ユーザプロフィール]

作成したユーザ基本情報を選択してユーザプロフィールを作成します。

ユーザプロフィール 新規追加	
プロフィール名	xruser
基本	xrbasic
認証	指定しない
証明書	指定しない
応答	xrreply
グループ	指定しない

<ユーザ>

[ユーザ]

ユーザ ID/パスワードを設定します。本設定例ではユーザ ID「user」、パスワード「pass」と設定しています。

プロフィールはユーザプロフィールで作成した「xruser」を選択します。

ユーザ 新規追加

ユーザID: user

パスワード: pass

プロフィール: xruser

固定IPアドレス払い出し

IPアドレス:

ネットマスク:

アカウントのロック

ロック: ☒ ロックしない ☐ ロックする

<<RADIUS>>

<サーバ>

[起動・停止]

RADIUS サーバを起動し設定を反映させます。

起動・停止

現在の状態: 停止中

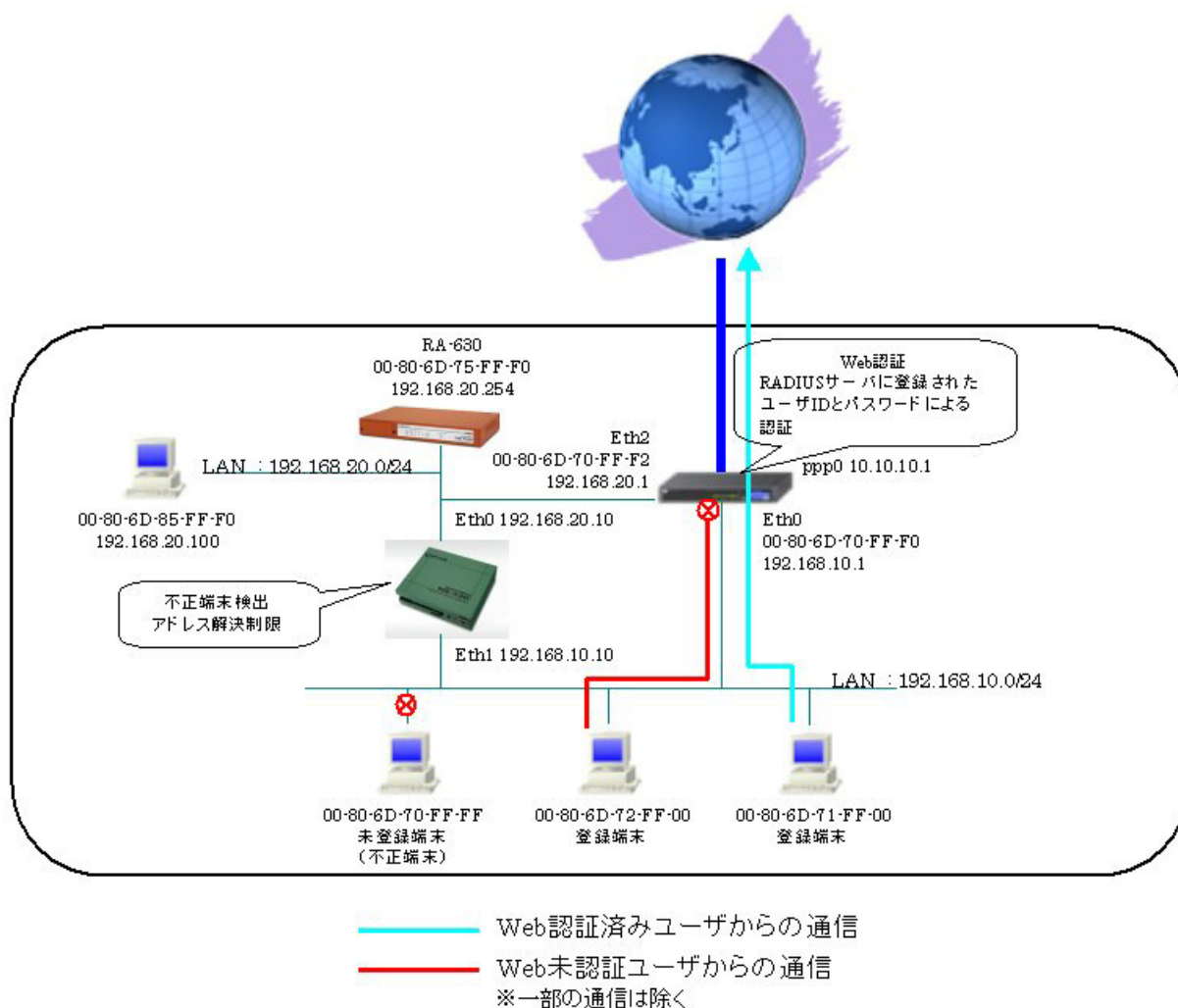
起動

9-4. Web 認証機能ソリューション例（NS-430 との併用）

Web 認証機能ではルータ経由での通信の可否を制御することが可能ですが、ルータ配下の社内セグメントへの接続の可否を制御することはできません。そこで社内セグメントへの不正接続を防止する機能に特化した「NS-430」をルータ配下のスイッチに接続し、不正接続を防止します。

なお Web 認証および NS-430 で使用するユーザ ID、パスワードは RADIUS サーバで一括管理することが可能です。本設定例では RA-630 でアカウントの管理を行っています。

9-4-1. 構成図



9-4-2. 設定例

《XR の設定》

Web 認証機能で 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際に認証画面がポップアップするように設定します。

その際あらかじめ許可しておく通信を設定しておく必要があります。

本設定例では Web 認証フィルタで UDP ポート 53 番をあらかじめ許可しています。それ以外の通信に関しては、あらかじめ許可されていないため、Web 認証によるユーザ認証後、通信可能になります。

《＜インターフェース設定＞》

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

☒ 固定アドレスで使用する
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※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、この論理インターフェースを使って PPPoE 接続を行います。

☒ 固定アドレスで使用する
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet2 の設定]

IP アドレスに「192.168.20.1」を設定します。

IP アドレス	192.168.20.1
ネットマスク	255.255.255.0
MTU	1500
☐ IP マスカレード (ip masq)	(このポートで使用する IP アドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション (spi)	
☐ SPI で DROP したパケットの LOG を取得	
☐ proxy arp	
☐ Directed Broadcast	

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<Web 認証設定>>

[RADIUS 設定]

RADIUS サーバに関する設定を行います。

本設定例ではアトリビュートとして「Idle-Timeout」を設定しています。これにより RADIUS サーバより送信される Idle-Timeout を利用することが可能です。

プライマリサーバ設定	
IPアドレス	192.168.20.254
ポート番号	☐ 1645 ☒ 1812 ☐ 手動設定
secret	secret

サーバ共通設定	
NAS-IP-Address	192.168.20.1
NAS-Identifier	XR

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	Idle-Timeout_28
セッションタイムアウト	指定しない

[基本設定]

TCP ポート 80 番の接続を監視し、この接続があった際に認証画面がポップアップするように、80/tcp 監視を「行う」を選択します。

基本設定		
本機能	☐ 使用しない	☒ 使用する
認証	☐ しない (URL転送のみ)	☒ する
80/tcp 監視	☐ 行わない	☒ 行う
MACアドレスフィルタ	☒ 使用しない	☐ 使用する

転送する URL を設定します。

強制認証後に URL 転送が行われるように設定します。

URL 転送		
URL	http://www.centurysys.co.jp	
通常認証後	☒ 行わない (デフォルト)	☐ 行う
強制認証後	☐ 行わない (エンドユーザ要求URL)	☒ 行う

RADIUS サーバでのみアカウントの管理を行うため、「RADIUS サーバ」を選択します。

認証方法		
☐ ローカル	☐ RADIUSサーバ→ローカル	☒ RADIUSサーバ

接続許可時間は「アイドルタイムアウト」を選択します。

※RADIUS サーバからの該当アトリビュートがなければ、ここで設定した値を使用します。

接続許可時間	
☒ アイドルタイムアウト	30 分 (1~43200)
☐ 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	

[フィルタ設定]

あらかじめ許可しておく通信として UDP ポート 53 番を許可しています。

これにより Web アクセス時に行う名前解決は、Web 認証の対象とはならないようにしています。

※このフィルタ設定は「フィルタ設定」→「Web 認証フィルタ」と同じものです。

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	ICMP type/code	送信元MACアドレス	LOG
eth0	パケット受信時	許可	udp				53			☐

《NS-430 の設定》

機器情報をホワイトリストに登録し、その情報を元にアドレス解決制限を行っています。

ホワイトリストに登録されていない機器に関しては、MAC アドレスをユーザ ID/パスワードとして、Radius サーバへ認証/アカウンティングを行います。

<<管理機能>>

<インタフェース>

[イーサネット]

Ether0 で IP アドレスに「192.168.20.10/24」を設定します。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

IPアドレス	192.168.20.10/24
デフォルトルート	
メトリック	[0-255]
フィルタ名	
MTU	1500 byte [68-1500] (デフォルト:1500)
通信モード	☒ 自動 100M 全二重

Ether1 で IP アドレスに「192.168.10.10/24」を設定します。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

IPアドレス	192.168.10.10/24
デフォルトルート	
メトリック	[0-255]
フィルタ名	
MTU	1500 byte [68-1500] (デフォルト:1500)
通信モード	☒ 自動 100M 全二重

設定後は以下のように表示されます。

インタフェース	IPアドレス	フィルタ名	MTU	通信モード	編集	削除
Ether0	192.168.20.10/24		1500	auto	編集	
Ether1	192.168.10.10/24		1500	auto	編集	削除

<<ネットワーク監視機能>>

<RADIUS 連携>

[RADIUS]

RADIUS サーバの設定を行います。

プライマリ		
IPアドレス	192.168.20.254	
ポート番号	1812/1813 ▼	
認証ポート	1812	[1024-60000]
アカウンティングポート	1813	[1024-60000]
クライアントIPアドレス	192.168.20.10	
シークレット	ns430secret	

認証およびアカウンティングを使用するように設定しています。

動作設定		
認証	使用する ▼	
アカウンティング	使用する ▼	
タイムアウト	5	秒 [3-30] (デフォルト:5)
最大試行回数	3	[1-10] (デフォルト:3)
アクセプトキャッシュ保持時間	300	秒 [30-86400] (デフォルト:300)
リジェクトキャッシュ保持時間	300	秒 [30-86400] (デフォルト:300)

[アトリビュート]

キャッシュ保持時間でアトリビュートとして「Session-Timeout」を選択します。

登録先キャッシュ/リスト名		
アトリビュート	取得しない ▼	
ベンダID		[1-65535]
タイプ		[1-255]
キャッシュ保持時間		
アトリビュート	Session-Timeout(27) ▼	
ベンダID		[1-65535]
タイプ		[1-255]

<ネットワーク監視>

[端末リスト]

端末情報をホワイトリストへの登録します。

本設定例では以下のルールでホワイトリストに登録します。

機器名	MAC アドレス	リスト
監視端末	00-80-6D-85-FF-F0	ホワイトリスト
RA-630（RADIUS）	00-80-6D-75-FF-F0	ホワイトリスト
XR(eth0 側)	00-80-6D-70-FF-F0	ホワイトリスト
XR(eth2 側)	00-80-6D-70-FF-F2	ホワイトリスト

MAC アドレス「00-80-6D-85-FF-F0」をホワイトリストに登録します。

リスト名	ホワイトリスト ▼
MACアドレス	00-80-6D-85-FF-F0
IPアドレス	192.168.20.100
備考	

MAC アドレス「00-80-6D-75-FF-F0」をホワイトリストに登録します。

リスト名	ホワイトリスト ▼
MACアドレス	00-80-6D-75-FF-F0
IPアドレス	192.168.20.254
備考	

MAC アドレス「00-80-6D-70-FF-F0」をホワイトリストに登録します。

リスト名	ホワイトリスト ▼
MACアドレス	00-80-6D-70-FF-F0
IPアドレス	192.168.10.1
備考	

MAC アドレス「00-80-6D-70-FF-F2」をホワイトリストに登録します。

リスト名	ホワイトリスト ▼
MACアドレス	00-80-6D-70-FF-F2
IPアドレス	192.168.20.1
備考	

ホワイトリスト登録後は、以下のように表示されます。

端末リスト					
ホワイトリスト					
	MACアドレス	IPアドレス	備考	編集	削除
	00-80-6D-85-FF-F0	192.168.20.100		編集	削除
	00-80-6D-75-FF-F0	192.168.20.254		編集	削除
	00-80-6D-70-FF-F0	192.168.10.1		編集	削除
	00-80-6D-70-FF-F2	192.168.20.1		編集	削除

[基本設定]

ネットワーク監視で「使用する」、制限設定でアラート、接続制限で「使用する」を選択します。
優先リスト名で「ホワイトリスト」、デフォルト動作で「拒否」を選択しています。

ネットワーク監視	使用する
ローカルキャッシュ	
定期解放	使用しない
保持時間	5 分 [1-144000]
制限設定	
アラート	使用する
接続制限	使用する
優先リスト名	ホワイトリスト
デフォルト動作	拒否

[アドレス解決制限]

アドレス解決制限で「使用する」を選択します。

アラートを「使用する」にし、端末検出ログとしてホワイトキャッシュ、ローカルキャッシュ、アクセプトキャッシュおよびリジェクトキャッシュを取得するように設定しています。

アドレス解決制限	使用する
アラート	
アラート	使用する
端末検出ログ	
端末検出ログ	取得する
ホワイトキャッシュ	取得する
ブラックキャッシュ	取得しない
ローカルキャッシュ	取得する
アクセプトキャッシュ	取得する
リジェクトキャッシュ	取得する

《RA-630 の設定》

<<管理機能>>

<ネットワーク>

[基本情報]

Ether0 で IP アドレスに「192.168.20.254/24」を設定します。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

設定後は以下のように表示されます。

<<RADIUS>>

<サーバ>

[基本情報]

XR, NS で設定しているポート番号と同じポート番号「1812/1813」、認証方式として「PAP/CHAP」を選択します。

[クライアント]

RADIUS クライアントである XR の情報を登録します。

RADIUS クライアントである NS-430 の情報を登録します。

クライアント新規追加	
クライアント名	NS430
IPアドレス	192.168.20.10
シークレット	ns430secret
アドレスプール	指定しない

<プロフィール>

[ユーザ基本情報]

Web 認証用のユーザを作成するためにはユーザ基本情報プロフィールの作成が必要です。
認証方式として「PAP/CHAP」を選択します。

ユーザ基本情報プロフィール 新規追加	
プロフィール名	xrbasic
認証方式	PAP/CHAP
同時接続数	
IPアドレス割り当て	☒ 未使用 ☐ RADIUSクライアント ☐ アドレスプール ☐ 固定
アドレスプール	指定しない

[応答アトリビュート]

Web 認証用の応答アトリビュートプロフィールを作成します。

応答アトリビュートプロフィール 新規追加	
プロフィール名	xrreply

応答アトリビュート一覧の「xrreply」の新規追加からアトリビュートとして「Idle-Timeout」を選択し、
値として「1800」を設定しています。

応答アトリビュート 新規追加	
プロフィール名	xrreply
アトリビュート	Idle-Timeout
値	1800

[ユーザプロフィール]

作成したユーザ基本情報, 応答アトリビュートを選択して Web 認証用のユーザプロフィールを作成します。

<ユーザ>

[ユーザ]

Web 認証用のユーザ ID/パスワードを設定します。本設定例ではユーザ ID「user」、パスワード「pass」と設定しています。

プロフィールはユーザプロフィールで作成した「xruser」を選択します。

<プロフィール>

[ユーザ基本情報]

NS-430 用のユーザを作成するためにはユーザ基本情報プロフィールの作成が必要です。

認証方式として「PAP/CHAP」を選択します。

[応答アトリビュート]

NS-430 用の応答アトリビュートプロファイルを作成します。

■ 応答アトリビュートプロファイル 新規追加	
プロファイル名	ns430reply

応答アトリビュート一覧の「ns430reply」の新規追加からアトリビュートとして「Session-Timeout」を選択し、値として「180」を設定しています。

■ 応答アトリビュート 新規追加	
プロファイル名	ns430reply
アトリビュート	Session-Timeout ▼
値	180

[ユーザプロフィール]

作成したユーザ基本情報、応答アトリビュートを選択して NS-430 用のユーザプロフィールを作成します。

ユーザプロフィール 新規追加

プロフィール名	ns430user
基本	ns430basic
認証	指定しない
証明書	指定しない
応答	ns430reply
グループ	指定しない

<ユーザ>

[ユーザ]

NS-430 用のユーザ ID/パスワードを設定します。ユーザ ID/パスワードは、認証する端末の MAC アドレスを設定します。

NS-430 から RADIUS サーバにユーザ ID/パスワードを送信する際には MAC アドレスの英文字は全て大文字になります。

プロフィールはユーザプロフィールで作成した「ns430user」を選択します。

ユーザ 新規追加

ユーザID	00-80-6D-71-FF-00
パスワード	00-80-6D-71-FF-00
プロフィール	ns430user

固定IPアドレス払い出し

IPアドレス	
ネットマスク	

アカウントのロック

ロック ☒ ロックしない ☐ ロックする

その他設定が必要なユーザを登録後、以下のように表示されます。

ユーザ						
No.	lock	ユーザID	プロフィール	IPアドレス	詳細	証明書
1		user	xruser	-	表示	
2		00-80-6D-71-FF-00	ns430user	-	表示	
3		00-80-6D-72-FF-00	ns430user	-	表示	

<<RADIUS>>

<サーバ>

[起動・停止]

RADIUS サーバを起動し設定を反映させます。



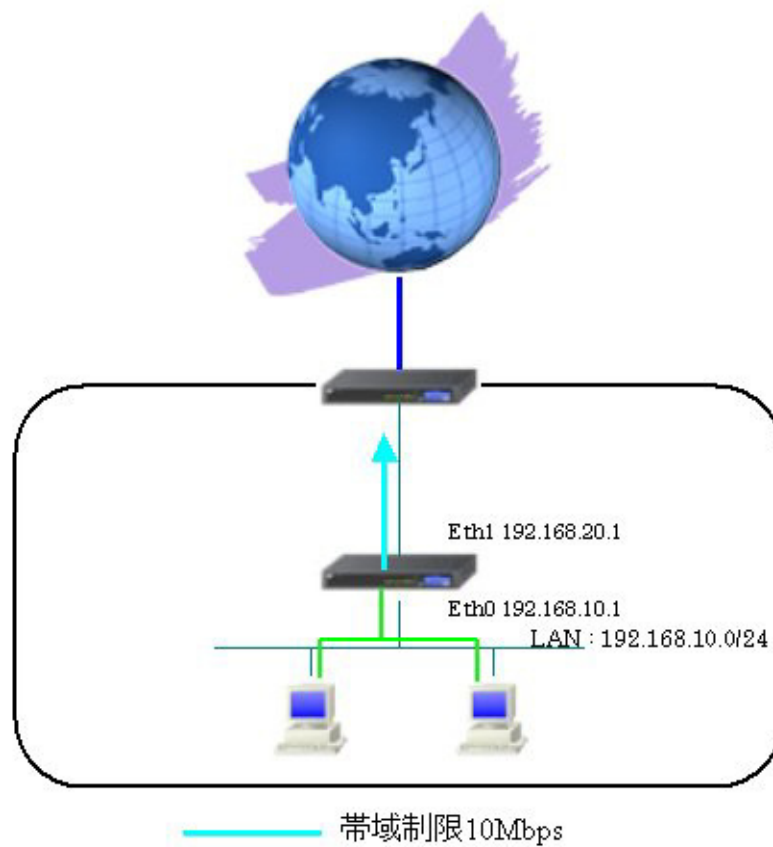
10. QoS 設定

10-1. 帯域制限

XR では TBF を利用することにより帯域制限を行うことができます。

本設定例では帯域を 10000Kbps (10Mbps) に制限しています。

10-1-1. 構成図



10-1-2. 設定例

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

The screenshot shows the configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Below these fields are several checkboxes: 'IP Masquerade (ip masq)' (unchecked), 'Stateful Packet Inspection (spi)' (unchecked), 'SPI Log' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

[Ethernet1 の設定]

IP アドレスに「192.168.20.1」を設定します。

The screenshot shows the configuration window for Ethernet1. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.20.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server Acquisition' radio button is unselected. The host name and MAC address fields are empty. Below these fields are several checkboxes: 'IP Masquerade (ip masq)' (unchecked), 'Stateful Packet Inspection (spi)' (unchecked), 'SPI Log' (unchecked), 'proxy arp' (unchecked), and 'Directed Broadcast' (unchecked).

<<QoS 設定>>

<QoS 詳細設定>

[Interface Queueing 設定]

eth1 で利用するキューイング方式として「tbf」を選択し、制限 Rate「10000 Kbit/s」(10Mbps)、Buffer Size「20k byte」を設定しています。

※TBF とは帯域制御方法の一つでトークンパケットにトークンがある一定の速度（トークン速度）で収納していきます。このトークン 1 個ずつがパケットを 1 個ずつ積み、トークン速度を超えない範囲でパケットを送信していきます。（帯域制限を行う場合に利用されます）

Interface名	eth1
Queueing Discipline	tbf
prio queue limit (prio選択時有効)	
TBF Parameter設定	
制限Rate	10000 Kbit/s
Buffer Size	20k byte
Limit Byte (tokenが利用できるようになるまで Queueing可能なbyte数)	byte

【QoS 機能】

QoS 簡易設定・詳細設定を有効にします。

※動作中の場合は、一度「無効」→「有効」を行ってください。

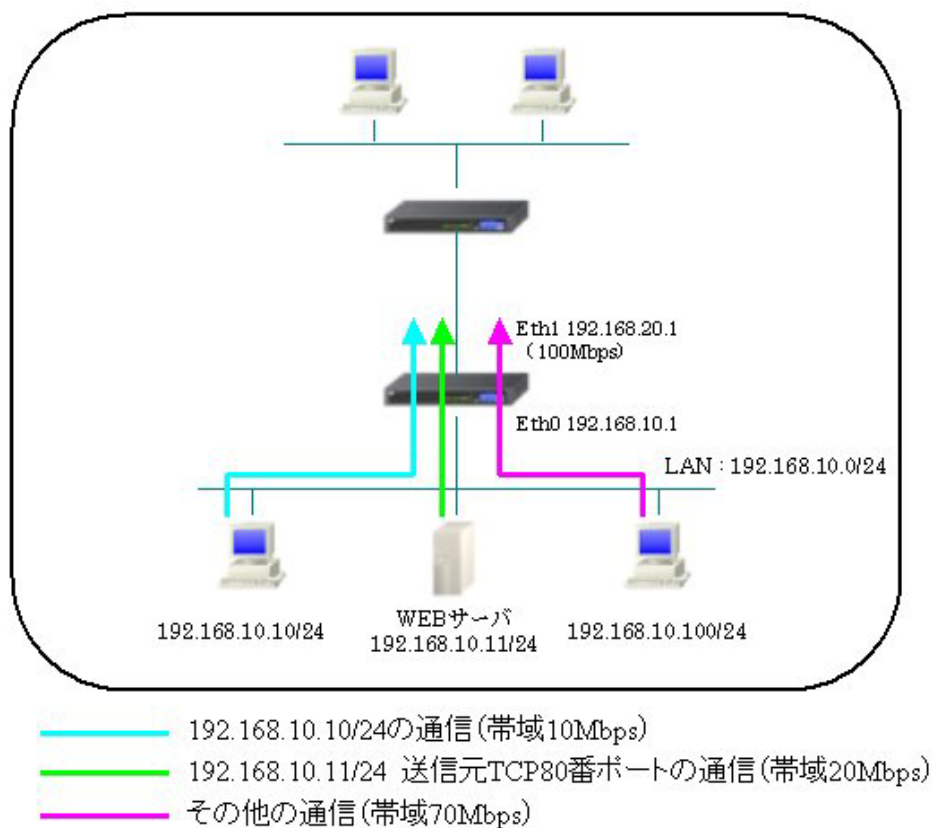
QoS簡易設定 QoS詳細設定	☒ 有効 ☐ 無効
--------------------	--

10-2. 帯域制御（簡易 QoS 設定と詳細 QoS 設定の利用）

XR では簡易 QoS 機能以外により詳細な設定を可能にする詳細 QoS 設定を実装しています。これによりより細かい設定ができるようになっています。

本設定例ではキューイング方式は CBQ, TBF, SFQ を利用しています。

10-2-1. 構成図



10-2-2. 設定例

本設定例の制御条件は以下のようになります。

- a. 10000kbps, 20000kbps, 70000kbps の3つのクラスを作成します。
- b. 10000kbps, 20000kbps のクラスでは「TBF」を行います。
- c. 70000kbps のクラスでは「SFQ」を行います。
- d. 送信元 IP アドレスが 192.168.10.10 のパケットを 10000Kbps のクラスに送ります。
- e. 送信元 IP アドレスが 192.168.10.11 で送信元ポートが TCP 80 番のパケットを 20000Kbps のクラスに送ります。
- f. その他の通信(d と e で選別したパケット以外)は 70000Kbps のクラスに送ります。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

☒ 固定アドレスで使用する
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

IP アドレスに「192.168.20.1」を設定します。

☒ 固定アドレスで使用する
IP アドレス 192.168.20.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

<<QoS 設定>>

<QoS 簡易設定>

[回線帯域設定]

eth1 インタフェースの回線帯域を設定します。本設定例では「100000Kbit/s」(100Mbps)を設定しています。

インターフェース名	eth1	回線帯域	0 Kbit/s
インターフェース名	eth1	回線帯域	100000 Kbit/s

[QoS 簡易設定(登録・編集)]

送信元 IP アドレスが 192.168.10.10 の通信に「10000Kbit/s」(10Mbps)を割り当てる設定を行います。帯域は借用しません。

設定番号	2
クラス帯域	10000 Kbit/s [必須]
インターフェース名	eth1
プロトコル番号(*)	(1-255)
送信元IPアドレス(*)	192.168.10.10/32
送信元ポート番号(*)	(1-65535)
宛先IPアドレス(*)	
宛先ポート(*)	(1-65535)
優先度	1 (1-8) [必須]
帯域借用	☐ する ☒ しない
(*)印項目は1項目以上指定して下さい	

[QoS 簡易設定(登録・編集)]

送信元 IP アドレスが 192.168.10.11 で送信元ポートが TCP 80 番の通信に「20000Kbit/s」(20Mbps)を割り当てる設定を行います。帯域は借用しません。

設定番号	3
クラス帯域	20000 Kbit/s [必須]
インターフェース名	eth1
プロトコル番号(*)	6 (1-255)
送信元IPアドレス(*)	192.168.10.11/32
送信元ポート番号(*)	80 (1-65535)
宛先IPアドレス(*)	
宛先ポート(*)	(1-65535)
優先度	1 (1-8) [必須]
帯域借用	☐ する ☒ しない

(*)印項目は1項目以上指定して下さい

設定後は以下のように表示されます。

インターフェース名 eth1 回線帯域 100000 Kbit/s 切替/回線帯域設定 情報表示											
	クラス	親クラス	帯域	プロトコル	送信元 IP アドレス	送信元ポート番号	宛先 IP アドレス	宛先ポート番号	優先度	帯域借用	操作
1	1	0	100000						1	しない	削除
2	10	1	10000		192.168.10.10/32				1	しない	編集, 削除
3	11	1	20000	6	192.168.10.11/32	80			1	しない	編集, 削除

<QoS 詳細設定>

[パケット分類設定]

[パケット入力時の設定]

[No. 1]

QoS 簡易設定ではクラス分けを行う際にプロトコル、IP アドレス、ポート番号を設定する必要がありましたが、条件を特に指定せず eth0 で受信したその他のパケットに対しても別途クラスを設定します。ここでは eth0 インタフェースで受信したパケットに対しては「mark」「1」とする設定を行います。

設定番号	1	
パケット分類条件		
プロトコル	(Protocol番号)	☐ Not条件
送信元アドレス		☐ Not条件
送信元ポート	(ポート番号/範囲指定は:番号連結)	☐ Not条件
宛先アドレス		☐ Not条件
宛先ポート	(ポート番号/範囲指定は:番号連結)	☐ Not条件
インターフェース	eth0	☐ Not条件
TOS/MARK/DSCP値	☐ TOS ☒ MARK ☐ DSCP ☒ マッチ条件無効 上記で選択したマッチ条件に対応する設定値 TOS Bit値 hex: 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay MARK値 (1~999) DSCP Bit値 hex(0~3f)	

TOS/MARK/DSCP値の設定	
設定対象	☐ TOS/Precedence ☒ MARK ☐ DSCP
設定値	• MARK設定 (1~999) 1 • TOS/Precedence設定 選択して下さい TOS Bit 選択して下さい Precedence Bit • DSCP設定 選択して下さい DSCP Bit

設定後は以下のように表示されます。

パケット入力時の設定 [切替:ローカル/パケット出力時]									
パケット分類条件							設定値		
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	インターフェース	TOS/MARK/DSCP値	TOS/MARK/DSCP値		Configure
1					eth0		MARK	1	Edit/Remove

[CLASS 分けフィルタ設定]

Priority はすでに QoS 簡易設定で設定済みの設定を優先させるため、それよりも大きい値を設定します。

(本設定例では「3」を設定しています)

またパケット分類設定で作成した情報を利用するため、Marking 情報によるフィルタを選択し、先ほど設定した Mark 値「1」を設定します。

設定番号	3
Description	
Priority	3 (1-999)
☐ パケットヘッダ情報によるフィルタ	
プロトコル	(Protocol番号)
送信元アドレス	
送信元ポート	(ポート番号)
宛先アドレス	
宛先ポート	(ポート番号)
TOS値	(hex 0-fe)
DSCP値	(hex 0-3f)
☒ Marking情報によるフィルタ	
Mark値	1 (1-999)

設定後は以下のように表示されます。(QoS 簡易設定で設定した項目も含まれます)

	FilterType	Description	Priority	プロトコル	送信元アドレス	送信元ポート	宛先アドレス	宛先ポート	TOS値	DSCP値	MARK値	Configure
1	Packet Head		1		192.168.10.10/32							Edit Remove
2	Packet Head		2	6	192.168.10.11/32	80						Edit Remove
3	Mark		3								1	Edit Remove

[CLASS 設定]

親クラスの下に置くクラスの中で、QoS 簡易設定で指定した通信以外のその他の通信に関するクラスを設定します。

CLASS 分けフィルタ設定で設定したフィルタ No.3（パケット分類設定で設定したその他の通信）の通信に「70000Kbit/s」（70Mbps）を割り当てる設定を行います。帯域は借用しません。

Description	
Interface名	eth1
Class ID	12
親class ID	1
Priority	1
Rate設定	70000 Kbit/s
Class内Average Packet Size設定	1000 byte
Maximum Burst設定	100
Bounded設定	☒ 有効 ☐ 無効
Filter設定 (Filter番号を入力してください)	1. 3 2. 3. 4. 5. 6. 7. 8. 9. 10.

設定後は以下のように表示されます。（QoS 簡易設定で設定した項目も含まれます）

	Description	Interface名	ID	親 CLASS ID	Priority	Rate	平均 Packet Size	Maximum Burst	Configure
1		eth1	1	0	1	10000Kbit/s	1000	100	Edit Remove
2		eth1	10	1	1	10000Kbit/s	1000	100	Edit Remove
3		eth1	11	1	1	20000Kbit/s	1000	100	Edit Remove
4		eth1	12	1	1	70000Kbit/s	1000	100	Edit Remove

[CLASS Queueing 設定]

CLASS 設定で設定したクラス内で更にキューイングを行うため、CLASS Queueing 設定を行います。

[No. 1]

ID「10」のクラスで QDISC 番号を「20」とし、キューイング方式として「tbf」を選択し、制限 Rate「10000 Kbit/s」(10Mbps)、Buffer Size「20k byte」を設定しています。

※TBF とは帯域制御方法の一つでトークンパケツにトークンがある一定の速度（トークン速度）で収納していきます。このトークン 1 個ずつがパケットを 1 個ずつかみ、トークン速度を超えない範囲でパケットを送信していきます。（帯域制限を行う場合に利用されます）

Description	
Interface名	eth1
QDISC番号	20
MAJOR ID	1
class ID	10
Queueing Discipline	tbf ▼
prio limit (FFIFO選択時有効)	
TEF Parameter設定	
制限Rate	10000 Kbit/s
Buffer Size	20k byte
Limit Byte (tokenが利用できるようになるまで queueing可能なbyte数)	byte

[No. 2]

ID「11」のクラスで QDISC 番号を「21」とし、キューイング方式として「tbf」を選択し、制限 Rate「20000 Kbit/s」(20Mbps)、Buffer Size「40k byte」を設定しています。

Description	
Interface名	eth1
QDISC番号	21
MAJOR ID	1
class ID	11
Queueing Discipline	tbf ▼
prio limit (FFIFO選択時有効)	
TEF Parameter設定	
制限Rate	20000 Kbit/s
Buffer Size	40k byte
Limit Byte (tokenが利用できるようになるまで queueing可能なbyte数)	byte

[No. 3]

ID「12」のクラスでQDISC番号を「22」とし、キューイング方式として「sfq」を選択しています。

※SFQ とはラウンドロビンで順番にトラフィックが送信され、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。

Description	
Interface名	eth1
QDISC番号	22
MAJOR ID	1
class ID	12
Queueing Discipline	sfq 

設定後は以下のように表示されます。

	Description	Interface名	QDISC 番号	種別	CLASS ID	MAJOR 番号	Configure
1		eth1	20	tbf	10	1	Edit Remove
2		eth1	21	tbf	11	1	Edit Remove
3		eth1	22	sfq	12	1	Edit Remove

【QoS 機能】

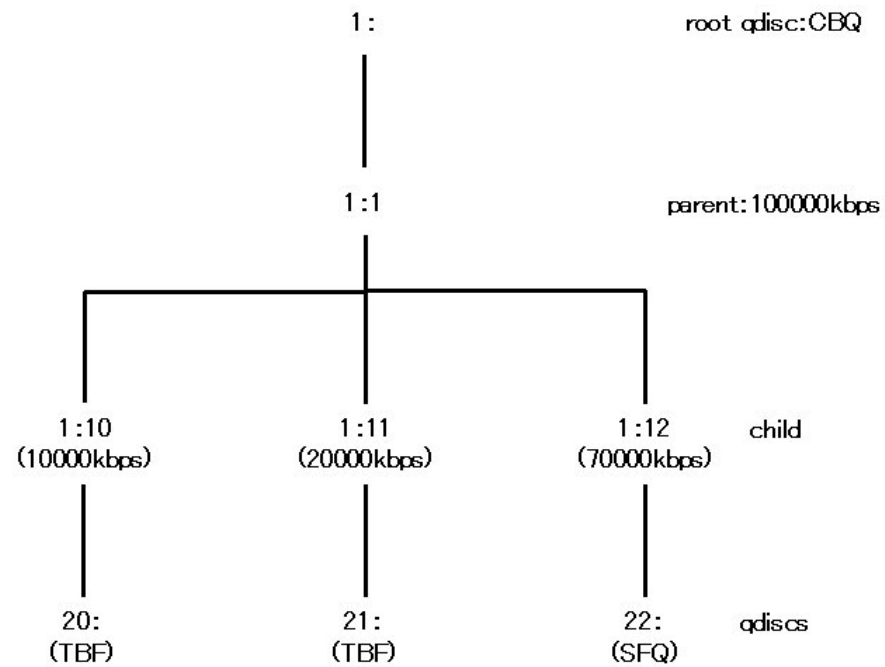
QoS 簡易設定・詳細設定を有効にします。

※動作中の場合は、一度「無効」→「有効」を行ってください。

QoS簡易設定 QoS詳細設定	☒ 有効 ☐ 無効
--	--

10-2-3. 設定例補足（クラス階層図）

本設定例は以下のようなクラス階層になっています。

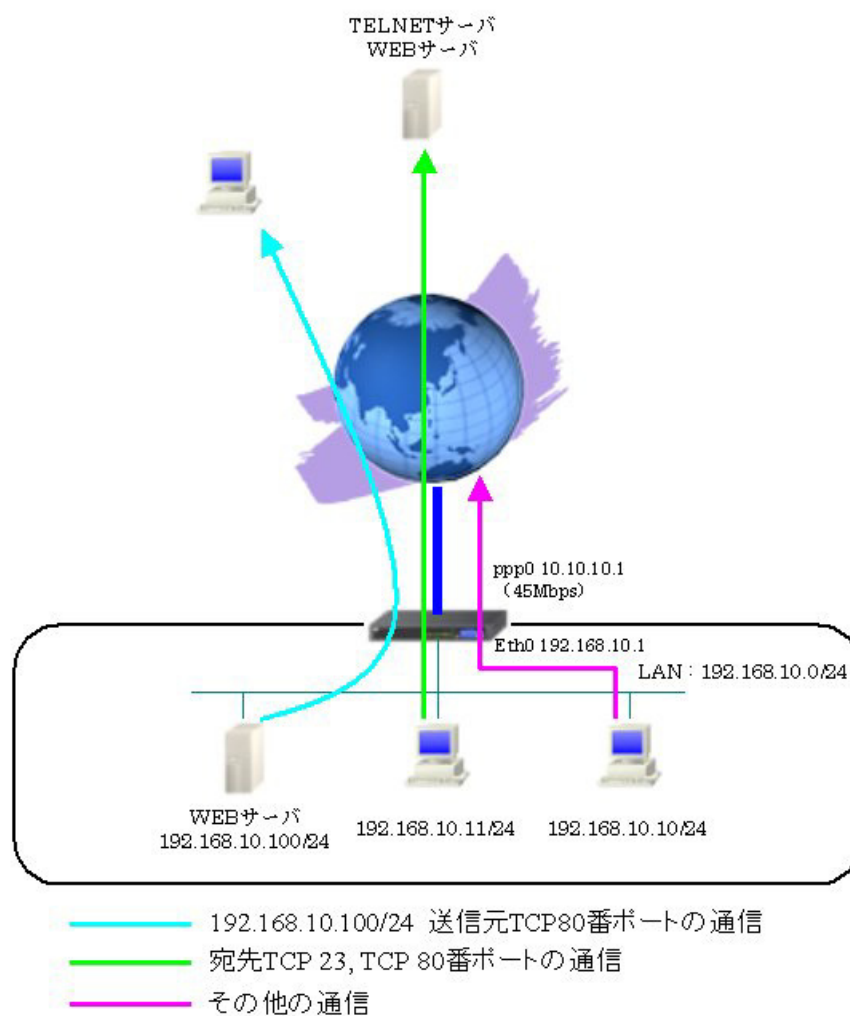


10-3. PPPoE での帯域制御+優先制御

本設定例では PPPoE 接続で WEB サーバを公開し、帯域制御、優先制御を行います。

本設定例ではキューイング方式は CBQ, TBF, PQ, SFQ を利用しています。

10-3-1. 構成図



10-3-2. 設定例

本設定例の制御条件は以下のようになります。

- a. 20000kbps, 10000kbps, 15000kbps の3つのクラスを作成します。
- b. 20000kbps のクラスでは「TBF」を行います。
- c. 10000kbps のクラスでは「PQ」を行います。
- d. 15000kbps のクラスでは「SFQ」を行います。
- e. 送信元 IP アドレスが 192.168.10.100 で送信元ポートが TCP 80 番のパケットを 20000Kbps のクラスに送ります。
- f. 宛先ポートが telnet(TCP 23 番), www(TCP 80 番)のパケットを 10000Kbps のクラスに送ります。
- g. 10000Kbps のクラスでは PQ による優先制御を行い、優先度は telnet(TCP 23 番) > www(TCP 80 番)とします。
- h. その他の通信(e と f で選別したパケット以外)は 15000Kbps のクラスに送ります。

<<インタフェース設定>>

[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。

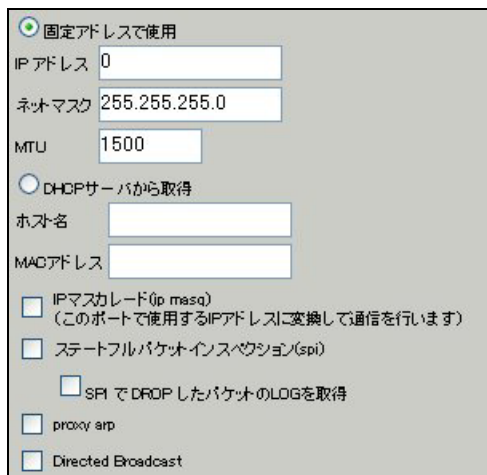
The screenshot shows a configuration window for Ethernet0. The 'Fixed IP Address' radio button is selected. The IP address is set to 192.168.10.1, the netmask to 255.255.255.0, and the MTU to 1500. The 'DHCP Server' radio button is unselected. Below these are empty text boxes for 'Host Name' and 'MAC Address'. At the bottom, there are several unchecked checkboxes: 'IP Masquerade (ip masq)', 'Stateful Packet Inspection (spi)', 'SPI for DROP packet LOG', 'proxy arp', and 'Directed Broadcast'.

☒ 固定アドレスで使用する
IP アドレス 192.168.10.1
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(ip masq) (このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast

[Ethernet1 の設定]

PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。



☒ 固定アドレスで使用する

IP アドレス

ネットマスク

MTU

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

<<PPP/PPPoE 設定>>

[接続先設定]

PPPoE 接続で使用するユーザ ID とパスワードを設定します。

ユーザID	test1@centurysys
パスワード	test1pass

[接続設定]

ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定します。

接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケットインスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定します。

PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時にPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています
------	-------------

<<フィルタ設定>>

[転送フィルタ]

LAN 上にある WEB サーバをインターネットからアクセス可能にするための設定をします。

インターネットから宛先 IP アドレス「192.168.10.100」で WEB サーバ（TCP ポート 80 番）宛のパケットを許可します。

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	宛先アドレス	宛先ポート	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット受信時	許可	tcp			192.168.10.100	80			☐

<<NAT 設定>>

[バーチャルサーバ]

LAN 上にある WEB サーバをインターネットからアクセス可能にするための設定をします。

インターネットから「10.10.10.1」で TCP ポート 80 番宛てのパケットを受信した場合は、「192.168.10.100」に転送します。

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
192.168.10.100	10.10.10.1	tcp	80	ppp0

<QoS 詳細設定>

[パケット分類設定]

[パケット入力時の設定]

[No. 1]

eth0 インタフェースで受信した送信元 IP アドレス「192.168.10.100」プロトコル番号 6(TCP)送信元ポート 80 番のパケットに対しては「mark」「1」とする設定を行います。

設定番号	1	
パケット分類条件		
プロトコル	6 (Protocol番号)	☐ Not条件
送信元アドレス	192.168.10.100	☐ Not条件
送信元ポート	80 (ポート番号/範囲指定:で番号連結)	☐ Not条件
宛先アドレス		☐ Not条件
宛先ポート		☐ Not条件
インターフェース	eth0	☐ Not条件
TOS/MARK/DSCP値	☐ TOS ☒ MARK ☐ DSCP ☒ マッチ条件無効 ☐ 上記で選択したマッチ条件に対応する設定値 TOS Bit値 hex 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay MARK値 (1-999) DSCP Bit値 hex(0-3f)	

TOS/MARK/DSCP 値の設定	
設定対象	☐ TOS/Precedence ☒ MARK ☐ DSCP
設定値	MARK設定 (1-999) 1 TOS/Precedence設定 選択して下さい TOS Bit 選択して下さい Precedence Bit DSCP設定 選択して下さい DSCP Bit

[No. 2]

eth0 インタフェースで受信したプロトコル番号 6(TCP)宛先ポート 23 番のパケットに対しては「mark」
「2」とする設定を行います。

設定番号	2	
パケット分類条件		
プロトコル	6 (Protocol番号)	☐ Not条件
送信元アドレス		☐ Not条件
送信元ポート	(ポート番号/範囲指定:で番号連結)	☐ Not条件
宛先アドレス		☐ Not条件
宛先ポート	23 (ポート番号/範囲指定:で番号連結)	☐ Not条件
インターフェース	eth0	☐ Not条件
TOS/MARK/ DSCP値	☐ TOS ☐ MARK ☐ DSCP ☒ マッチ条件無効 上記で選択したマッチ条件に対応する設定値 TOS Bit値 hex 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay MARK値 (1-999) DSCP Bit値 hex(0-3f)	

TOS/MARK/DSCP値の設定	
設定対象	☐ TOS/Precedence ☒ MARK ☐ DSCP
設定値	• MARK設定 (1-999) 2 • TOS/Precedence設定 選択して下さい ▼ TOS Bit 選択して下さい ▼ Precedence Bit • DSCP設定 選択して下さい ▼ DSCP Bit

[No. 3]

eth0 インタフェースで受信したプロトコル番号 6(TCP)宛先ポート 80 番のパケットに対しては「mark」
「3」とする設定を行います。

設定番号	3	
パケット分類条件		
プロトコル	6 (Protocol番号)	☐ Not条件
送信元アドレス		☐ Not条件
送信元ポート	(ポート番号/範囲指定:で番号連結)	☐ Not条件
宛先アドレス		☐ Not条件
宛先ポート	80 (ポート番号/範囲指定:で番号連結)	☐ Not条件
インターフェース	eth0	☐ Not条件
TOS/MARK/ DSCP値	☐ TOS ☐ MARK ☐ DSCP ☒ マッチ条件無効 上記で選択したマッチ条件に対応する設定値 TOS Bit値 hex 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay MARK値 (1~999) DSCP Bit値 hex(0~3f)	

TOS/MARK/DSCP 値の設定	
設定対象	☐ TOS/Precedence ☒ MARK ☐ DSCP
設定値	• MARK設定 (1~999) 3 • TOS/Precedence設定 選択して下さい ▼ TOS Bit 選択して下さい ▼ Precedence Bit • DSCP設定 選択して下さい ▼ DSCP Bit

[No. 4]

上記 No. 1, 2, 3 以外の eth0 インタフェースで受信したパケットに対しては「mark」「4」とする設定を行います。

設定番号	4	
パケット分類条件		
プロトコル	6 (Protocol番号)	☐ Not条件
送信元アドレス		☐ Not条件
送信元ポート	(ポート番号/範囲指定:で番号連結)	☐ Not条件
宛先アドレス		☐ Not条件
宛先ポート	(ポート番号/範囲指定は:で番号連結)	☐ Not条件
インターフェース	eth0	☐ Not条件
TOS/MARK/DSCP値	☐ TOS ☐ MARK ☐ DSCP ☒ マッチ条件無効 上記で選択したマッチ条件に対応する設定値	
TOS Bit値 hex: 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay MARK値 (1~999) DSCP Bit値 hex(0~3f)		

TOS/MARK/DSCP値の設定	
設定対象	☐ TOS/Precedence ☒ MARK ☐ DSCP
設定値	・MARK設定 (1~999) 4 ・TOS/Precedence設定 選択して下さい ▼ TOS Bit 選択して下さい ▼ Precedence Bit ・DSCP設定 選択して下さい ▼ DSCP Bit

設定後は以下のように表示されます。

パケット入力時の設定 [切替:ローカルパケット出力時]									
パケット分類条件							設定値		
	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	インターフェース	TOS/MARK/DSCP値	TOS/MARK/DSCP値	Configure
1	6	192.168.10.100	80			eth0		MARK 1	Edit Remove
2	6				23	eth0		MARK 2	Edit Remove
3	6				80	eth0		MARK 3	Edit Remove
4						eth0		MARK 4	Edit Remove

[CLASS 分けフィルタ設定]

[No. 1]

パケット分類設定で作成した Mark 値「1」を No.1 に設定します。Priority は「1」を設定しています。

設定番号	1
Description	src19216810100srcport80
Priority	1 (1-999)
☐ パケットヘッダ情報によるフィルタ	
プロトコル	(Protocol番号)
送信元アドレス	
送信元ポート	(ポート番号)
宛先アドレス	
宛先ポート	(ポート番号)
TOS値	(hex0-fe)
DSCP値	(hex0-3f)
☒ Marking情報によるフィルタ	
Mark値	1 (1-999)

[No. 2]

パケット分類設定で作成した Mark 値「2」を No.2 に設定します。Priority は「2」を設定しています。

設定番号	2
Description	dstport23
Priority	2 (1-999)
☐ パケットヘッダ情報によるフィルタ	
プロトコル	(Protocol番号)
送信元アドレス	
送信元ポート	(ポート番号)
宛先アドレス	
宛先ポート	(ポート番号)
TOS値	(hex0-fe)
DSCP値	(hex0-3f)
☒ Marking情報によるフィルタ	
Mark値	2 (1-999)

[No. 3]

パケット分類設定で作成した Mark 値「3」を No. 3 に設定します。Priority は「3」を設定しています。

設定番号	3
Description	dstport80
Priority	3 (1-999)
☐ パケットヘッダ情報によるフィルタ	
プロトコル	(Protocol番号)
送信元アドレス	
送信元ポート	(ポート番号)
宛先アドレス	
宛先ポート	(ポート番号)
TOS値	(hex 0-fe)
DSCP値	(hex 0-3f)
☒ Marking情報によるフィルタ	
Mark値	3 (1-999)

[No. 4]

パケット分類設定で作成した Mark 値「4」を No. 4 に設定します。Priority は「4」を設定しています。

設定番号	4
Description	other
Priority	4 (1-999)
☐ パケットヘッダ情報によるフィルタ	
プロトコル	(Protocol番号)
送信元アドレス	
送信元ポート	(ポート番号)
宛先アドレス	
宛先ポート	(ポート番号)
TOS値	(hex 0-fe)
DSCP値	(hex 0-3f)
☒ Marking情報によるフィルタ	
Mark値	4 (1-999)

設定後は以下のように表示されます。

	FilterType	Description	Priority	プロ トコ ル	送信 元ア ドレス	送信元 ポート	宛先 アドレ ス	宛先 ポート	TOS 値	DSCP 値	MARK 値
1	Mark	src19216810100srcport80	1								1
2	Mark	dstport23	2								2
3	Mark	dstport80	3								3
4	Mark	other	4								4

[Interface Queueing 設定]

ppp0 で利用するキューイング方式として「cbq」を選択します。

Interface名	ppp0
Queueing Discipline	cbq ▼

回線帯域は接続回線の物理的な帯域幅を設定します。(本設定例では 100000Kbps としています)

CBQ Parameter設定	
回線帯域	100000 Kbit/s
平均パケットサイズ	1000 byte

設定後は以下のように表示されます。

	Interface名	種別	制限Rate	Buffer	回線帯域	平均Packet Size
1	ppp0	cbq			100000Kbit/s	1000

[CLASS 設定]

[No. 1]

親クラスの設定をします。Rate は「45000Kbit/s」(45Mbps)を割り当てています。

Description	parent									
Interface名	ppp0									
Class ID	1									
親class ID	0									
Priority	1									
Rate設定	45000 Kbit/s									
Class内Average Packet Size設定	1000 byte									
Maximum Burst設定	100									
Bounded設定	☒ 有効 ☐ 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.

[No. 2]

CLASS 分けフィルタ設定で設定したフィルタ No. 1（パケット分類設定で設定した送信元 IP アドレス「192.168.10.100」送信元ポート TCP 80 番の通信）の通信に「20000Kbit/s」（20Mbps）を割り当てる設定を行います。帯域は借用しません。

Description	child10									
Interface名	ppp0									
Class ID	10									
親class ID	1									
Priority	1									
Rate設定	20000 Kbit/s									
Class内Average Packet Size設定	1000 byte									
Maximum Burst設定	100									
Bounded設定	☒ 有効 ☐ 無効									
Filter設定 (Filter番号を入力してください)	1. 1	2.	3.	4.	5.	6.	7.	8.	9.	10.

[No. 3]

CLASS 分けフィルタ設定で設定したフィルタ No. 2, 3（パケット分類設定で設定した宛先ポート TCP 23, 80 番の通信）の通信に「10000Kbit/s」（10Mbps）を割り当てる設定を行います。帯域は借用しません。

Description	child11									
Interface名	ppp0									
Class ID	11									
親class ID	1									
Priority	1									
Rate設定	10000 Kbit/s									
Class内Average Packet Size設定	1000 byte									
Maximum Burst設定	100									
Bounded設定	☒ 有効 ☐ 無効									
Filter設定 (Filter番号を入力してください)	1. 2	2. 3	3.	4.	5.	6.	7.	8.	9.	10.

[No. 4]

CLASS 分けフィルタ設定で設定したフィルタ No. 4（パケット分類設定で設定したその他の通信）の通信に「15000Kbit/s」（15Mbps）を割り当てる設定を行います。帯域は借用しません。

Description	child12
Interface名	ppp0
Class ID	12
親class ID	1
Priority	1
Rate設定	15000 Kbit/s
Class内Average Packet Size設定	1000 byte
Maximum Burst設定	100
Bounded設定	☒ 有効 ☐ 無効
Filter設定 (Filter番号を入力してください)	1. 4 2. 3. 4. 5. 6. 7. 8. 9. 10.

設定後は以下のように表示されます。

	Description	Interface名	ID	親 CLASS ID	Priority	Rate	平均 Packet Size	Maximum Burst
1	parent	ppp0	1	0	1	45000Kbit/s	1000	100
2	child10	ppp0	10	1	1	20000Kbit/s	1000	100
3	child11	ppp0	11	1	1	10000Kbit/s	1000	100
4	child12	ppp0	12	1	1	15000Kbit/s	1000	100

[CLASS Queueing 設定]

CLASS 設定で設定したクラス内で更にキューイングを行うため、CLASS Queueing 設定を行います。

[No. 1]

ID「10」のクラスで QDISC 番号を「20」とし、キューイング方式として「tbf」を選択し、制限 Rate「20000 Kbit/s」(20Mbps)、Buffer Size「40k byte」を設定しています。

※TBF とは帯域制御方法の一つでトークンパケツにトークンがある一定の速度（トークン速度）で収納していきまふ。このトークン 1 個ずつがパケツを 1 個ずつかみ、トークン速度を超えない範囲でパケツを送信していきまふ。(帯域制限を行う場合に利用されまふ)

Description	qdisc20
Interface名	ppp0
QDISC番号	20
MAJOR ID	1
class ID	10
Queueing Discipline	tbf
prifo limit (FFIFO選択時有効)	
TEF Parameter設定	
制限Rate	20000 Kbit/s
Buffer Size	40k byte
Limit Byte (tokenが利用できるようになるまで queuing可能なbyte数)	byte

[No. 2]

ID「11」のクラスでQDISC番号を「21」とし、キューイング方式として「pq」を選択し、Band数は初期値の3バンド(3クラス)を利用しています。

CLASS分けフィルタの設定番号とパケットを送るクラス番号(優先度)を関連づけます。

クラス1：送信元ポート TCP 23 番

クラス3：送信元ポート TCP 80 番

Description	qdisc21
Interface名	ppp0
QDISC番号	21
MAJOR ID	1
class ID	11
Queueing Discipline	pq

PQ Parameter設定	
最大Band数設定	3 default 3 (2-5)
priority-map設定	1 2 2 2 1 2 0
Marking Filterの選択 (PacketヘッダによるFilter設定は選択できません)	FilterNo. Class No.
	1. 2 1
	2. 3 3
	3.
	4.
	5.
	6.
	7.
	8.
	9.
10.	

[No. 3]

ID「12」のクラスでQDISC番号を「22」とし、キューイング方式として「sfq」を選択しています。

※SFQ とはラウンドロビンで順番にトラフィックが送信され、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。

Description	qdisc22
Interface名	ppp0
QDISC番号	22
MAJOR ID	1
class ID	12
Queueing Discipline	sfq ▼

設定後は以下のように表示されます。

	Description	Interface名	QDISC 番号	種別	CLASS ID	MAJOR 番号
1	qdisc20	ppp0	20	tbf	10	1
2	qdisc21	ppp0	21	pa	11	1
3	qdisc22	ppp0	22	sfq	12	1

【QoS 機能】

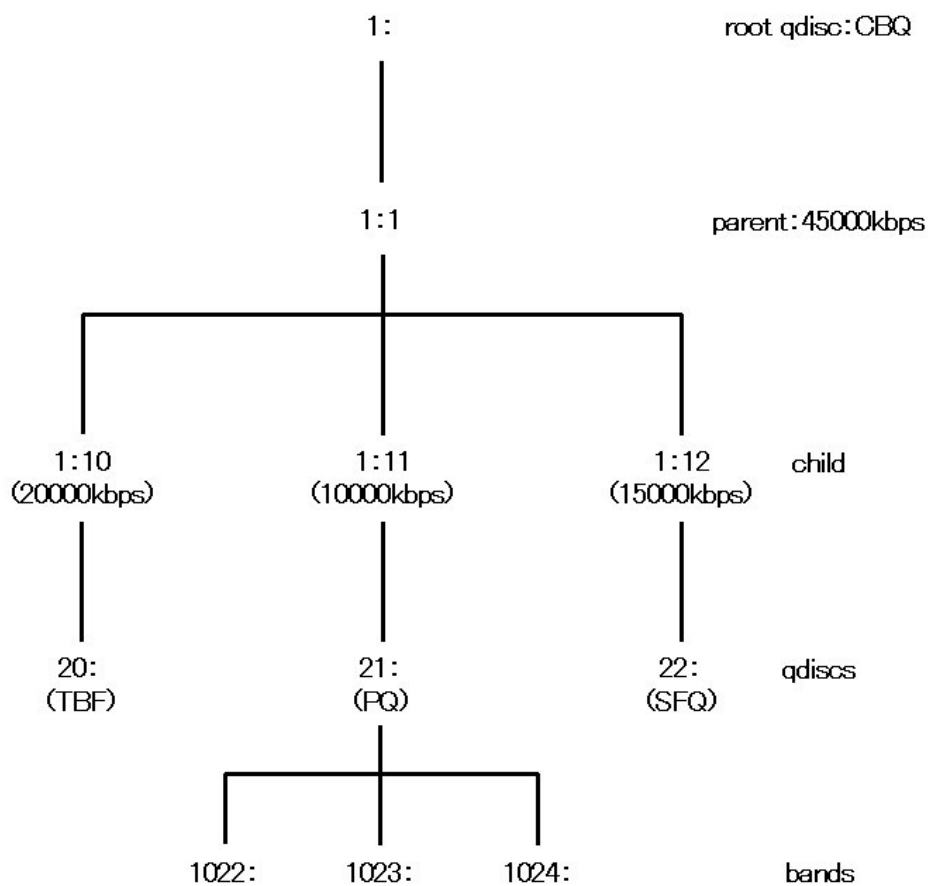
QoS 簡易設定・詳細設定を有効にします。

※動作中の場合は、一度「無効」→「有効」を行ってください。

QoS簡易設定 QoS詳細設定	☒ 有効 ☐ 無効
--	--

10-3-3. 設定例補足（クラス階層図）

本設定例は以下のようなクラス階層になっています。



11. サポートデスクへのお問い合わせ

11-1. サポートデスクへのお問い合わせに関して

サポートデスクにお問い合わせ頂く際は、以下の情報をお知らせ頂けると効率よく対応させて頂くことが可能ですので、ご協力をお願い致します。

- ご利用頂いている XR 製品の機種名, バージョン番号
- ご利用頂いている XR 製品を含んだネットワーク構成
- 不具合の内容および不具合の再現手順（何を行った場合にどのような問題が発生したのかをできるだけ具体的にお知らせ下さい）
- ご利用頂いている XR 製品での不具合発生時のログ
- ご利用頂いている XR 製品の設定ファイル, 各種ステータス情報（取得方法に関しましては、ご利用頂いている製品のユーザーズガイドをご参照下さい）

11-2. サポートデスクのご利用に関して

電話サポート

電話番号：0422-37-8926

電話での対応は以下の時間帯で行います。

月曜日 ～ 金曜日 10:00 AM - 5:00 PM

ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail： support@centurysys.co.jp

FAXサポート

FAX 番号：0422-55-3373

電子メール、FAX は 毎日 24 時間受け付けております。

ただし、システムのメンテナンスやビルの電源点検のため停止する場合があります。その際は弊社ホームページ等にて事前にご連絡いたします。

FutureNet XR シリーズ

設定例集

Ver1.1.0

2008 年 8 月

発行 センチュリー・システムズ株式会社

Copyright(c) 2008 Century Systems Co., Ltd. All Rights Reserved.
