FutureNet XR シリーズ

設定例集

Ver 1.2.0

※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

CENTURY SYSTEMS

目次

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(URL フィルタおよび BGP4 のみ Ver3.6.0)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

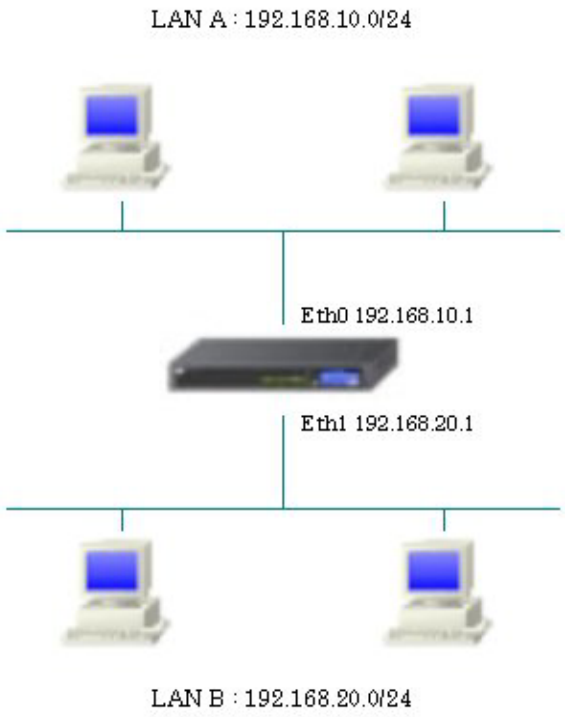
Version	更新内容
1.0.0	初版
1.1.0	ブリッジフィルタ，DHCP，攻撃検出，Web 認証，QoS 設定例追加
1.2.0	ソースルート，URL フィルタ，BGP4（切断監視）設定例追加

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



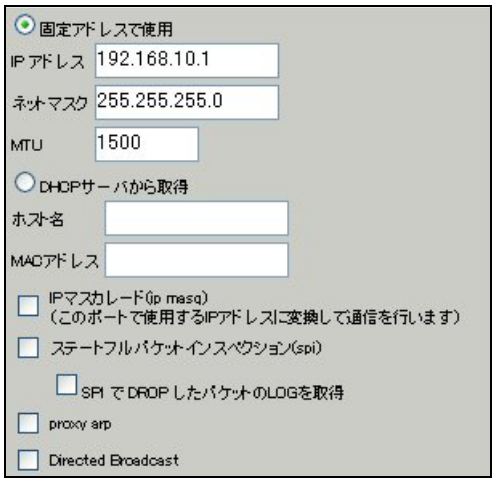
1-1-2. 設定例

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>>

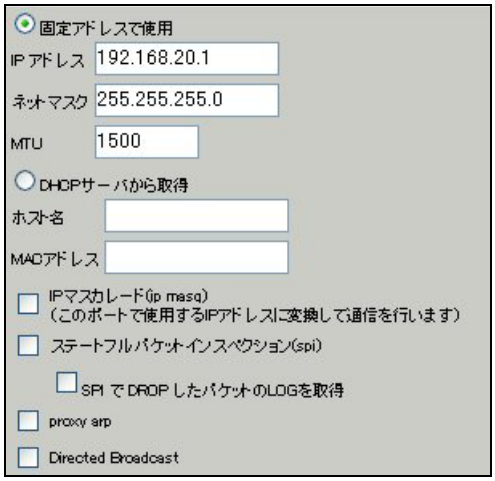
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



[Ethernet1 の設定]

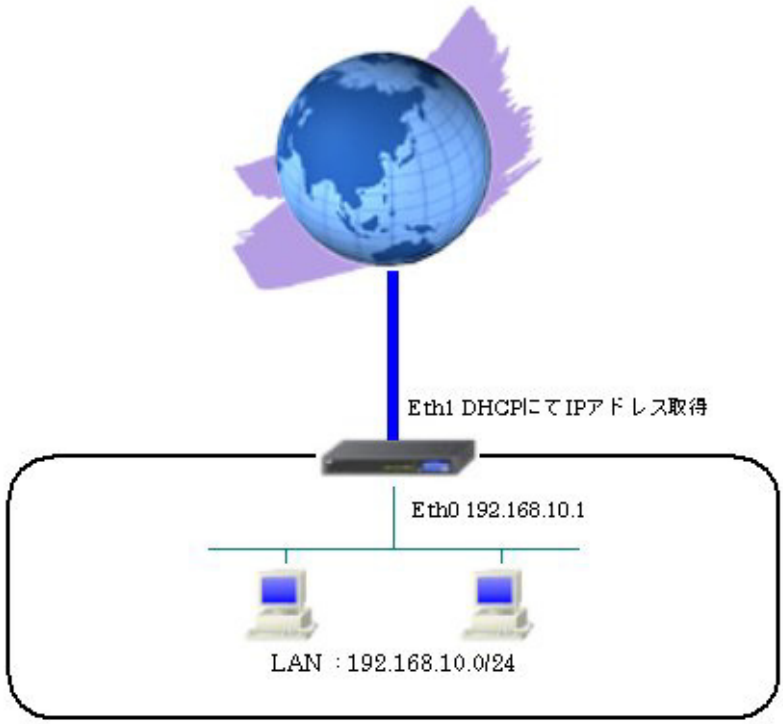
IP アドレスに「192.168.20.1」を設定します。



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



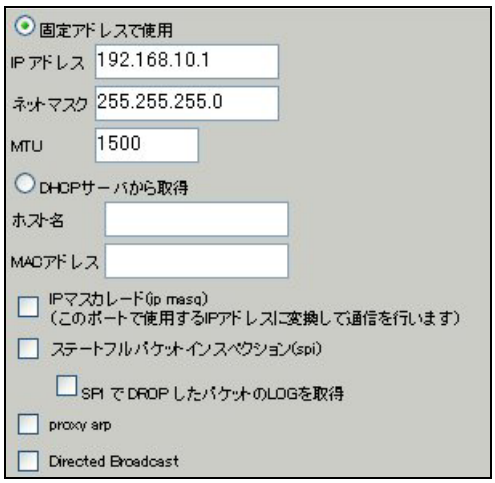
1-2-2. 設定例

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]

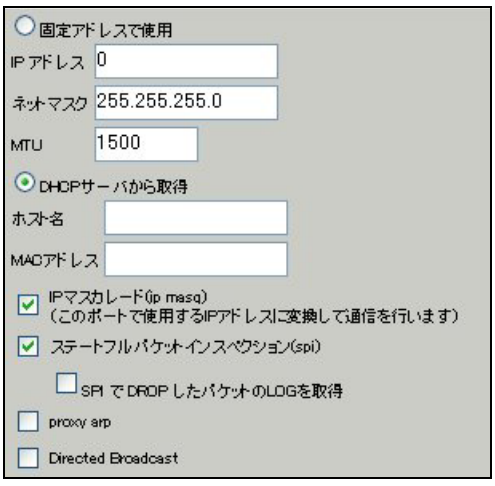
IP アドレスに「192.168.10.1」を設定します。



[Ethernet1 の設定]

「DHCP サーバから取得」を選択します。

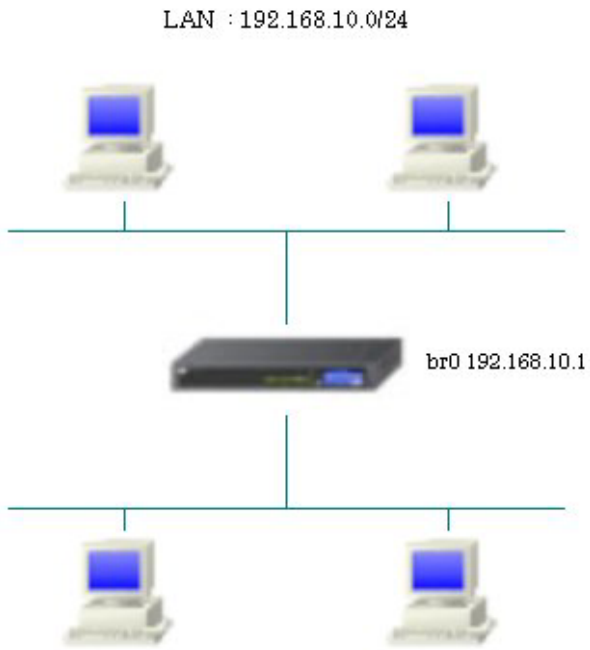
※ルータ配下の端末がインターネットアクセス可能になるように IP マスカレードを「有効」にし、WAN からのパケットをフィルタリングするためにステートフルパケットインスペクションを「有効」に設定しています。



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

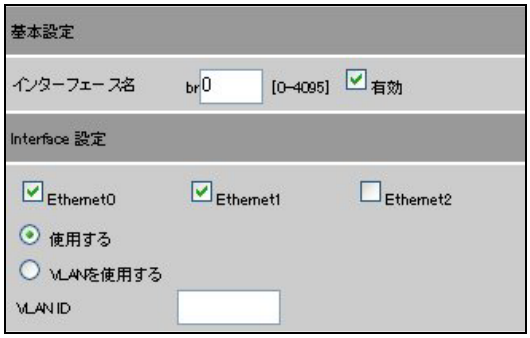
本設定例では二つの同一ネットワークを接続するための設定を行っています。

<<インタフェース設定>>

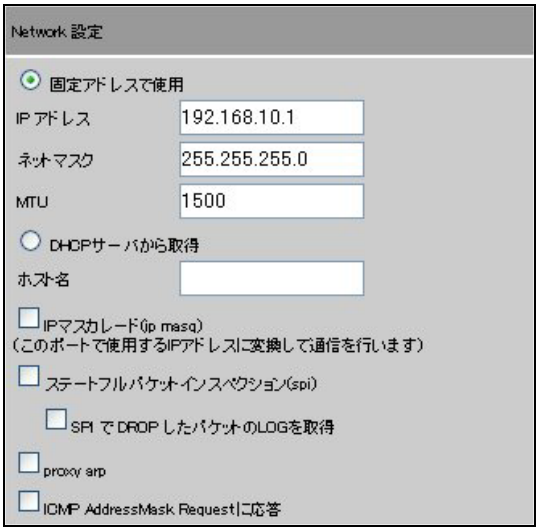
[Bridge の設定]

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、Ehernet0 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。

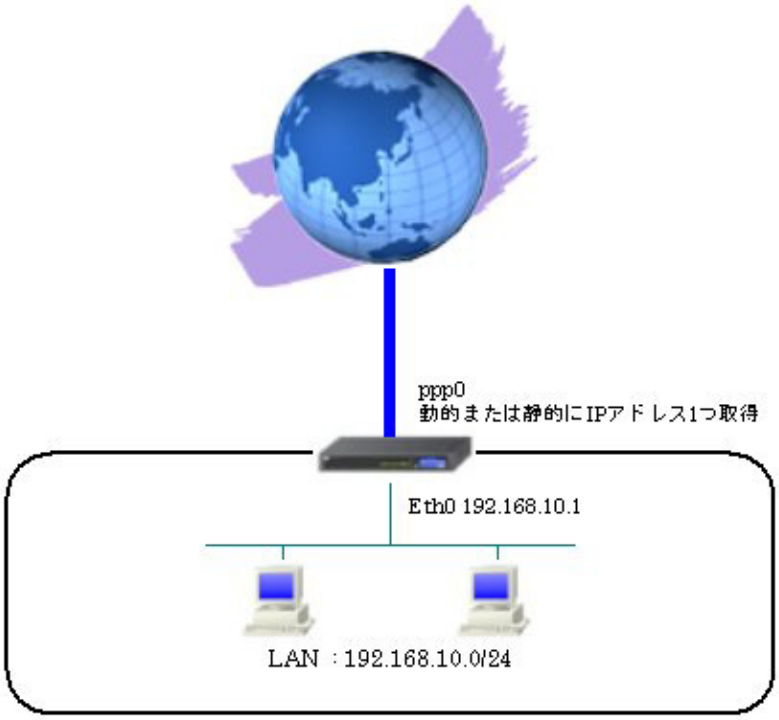


2. PPPoE 設定

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



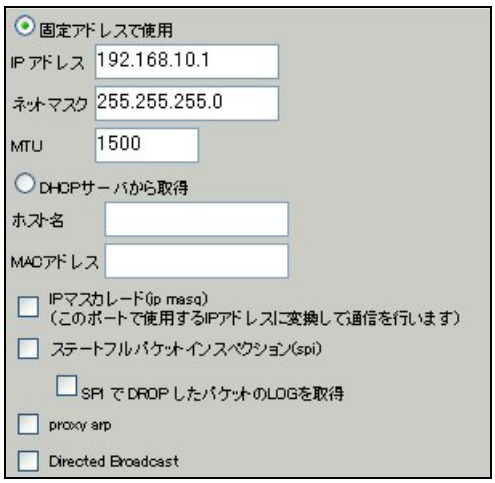
2-1-2. 設定例

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]

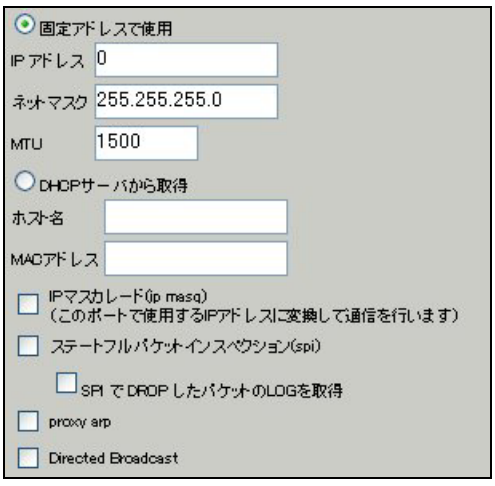
IP アドレスに「192.168.10.1」を設定します。



[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]

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

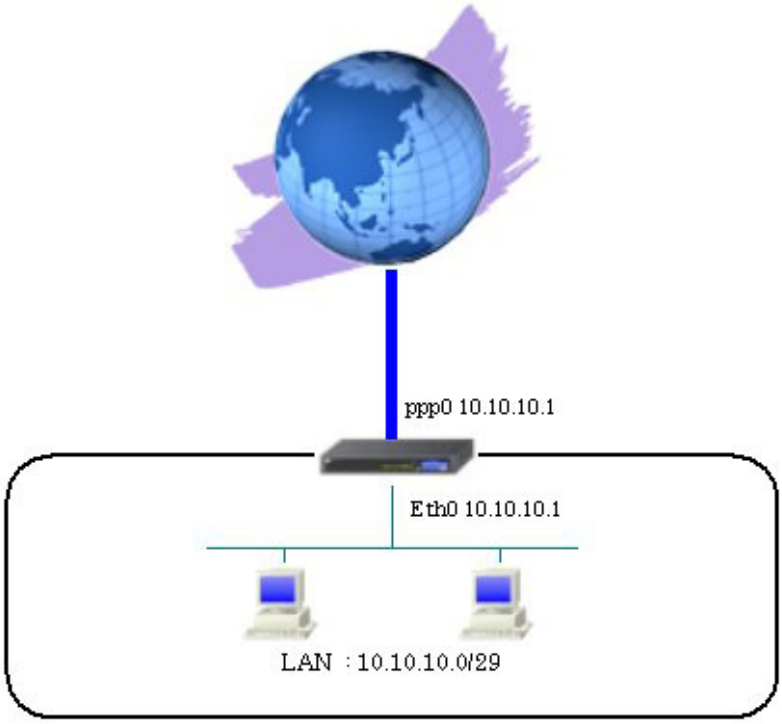
接続が完了した場合、回線状態が以下のように表示されます。

回線状態	主回線で接続しています

2-2. 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



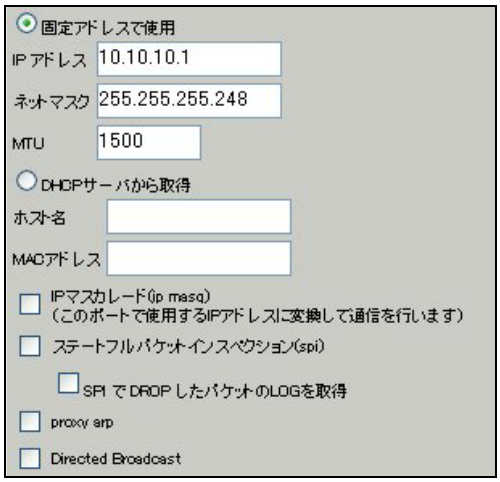
2-2-2. 設定例

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]

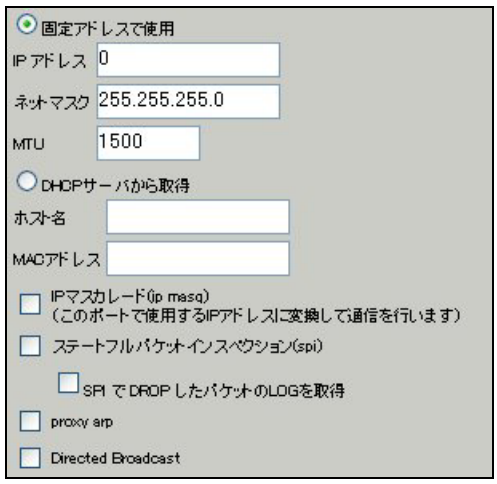
IP アドレスに「10.10.10.1」,ネットマスクに「255.255.255.248」を設定します。



[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

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

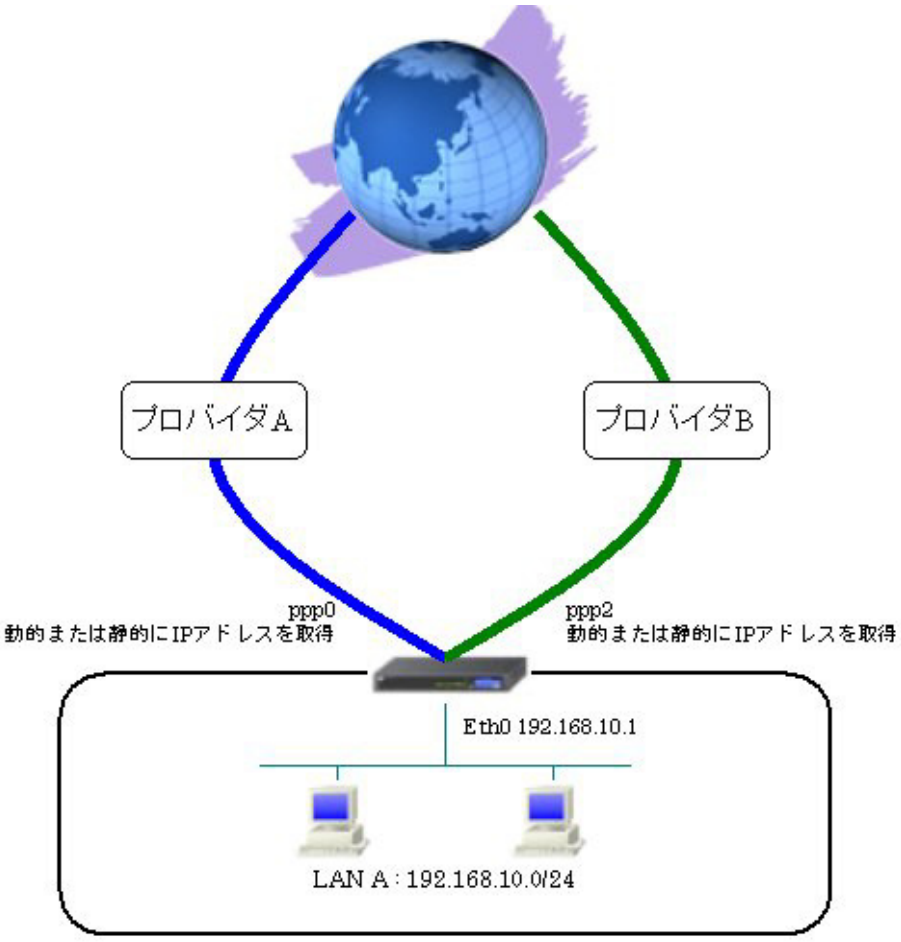
接続が完了した場合、回線状態が以下のように表示されます。

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

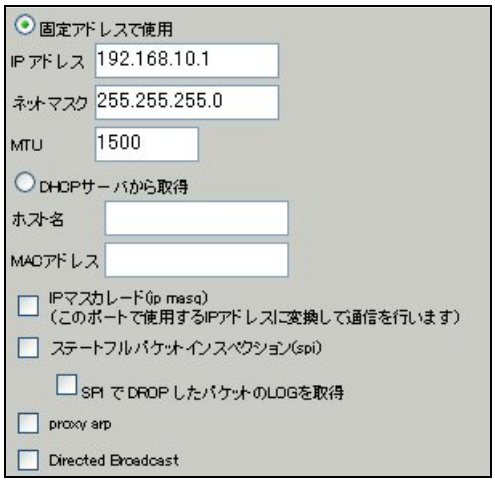


2-3-2. 設定例

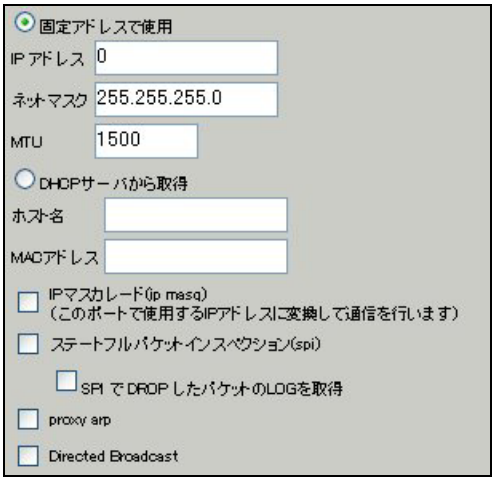
PPPoE 接続（主回線，マルチ回線）に必要な設定を行います。
また宛先 IP アドレスが「10.100.0.0/24」の時には、マルチ回線を利用し、それ以外の宛先 IP アドレスに対しては主回線を利用するように設定しています。

<<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。



[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 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 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 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。

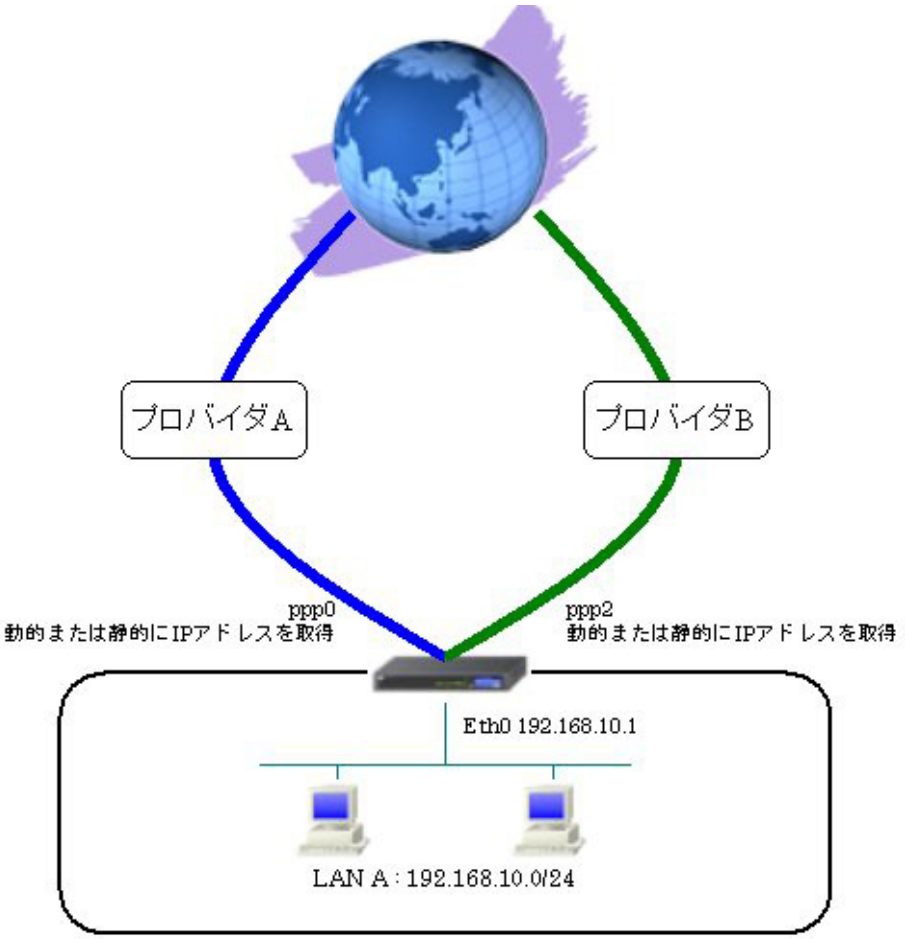
アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
10.100.0.0	255.255.255.0	ppp2		1

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



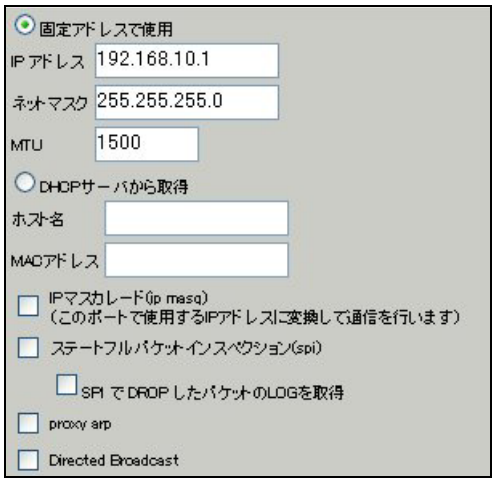
2-4-2. 設定例

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を主回線（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]

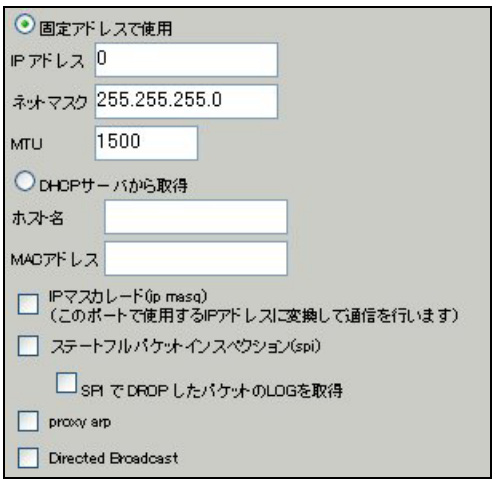
IP アドレスに「192.168.10.1」を設定します。



[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。



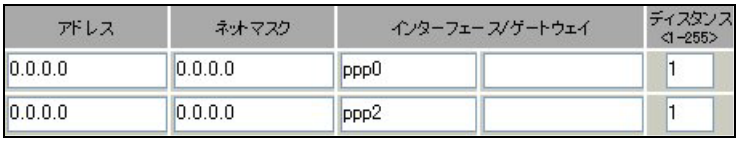
<<システム設定>>

[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。

<<スタティックルート設定>>

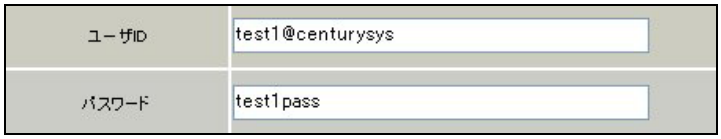
主回線（ppp0）とマルチ回線（ppp2）をデフォルトルートとして設定します。



<<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。



[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。

［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

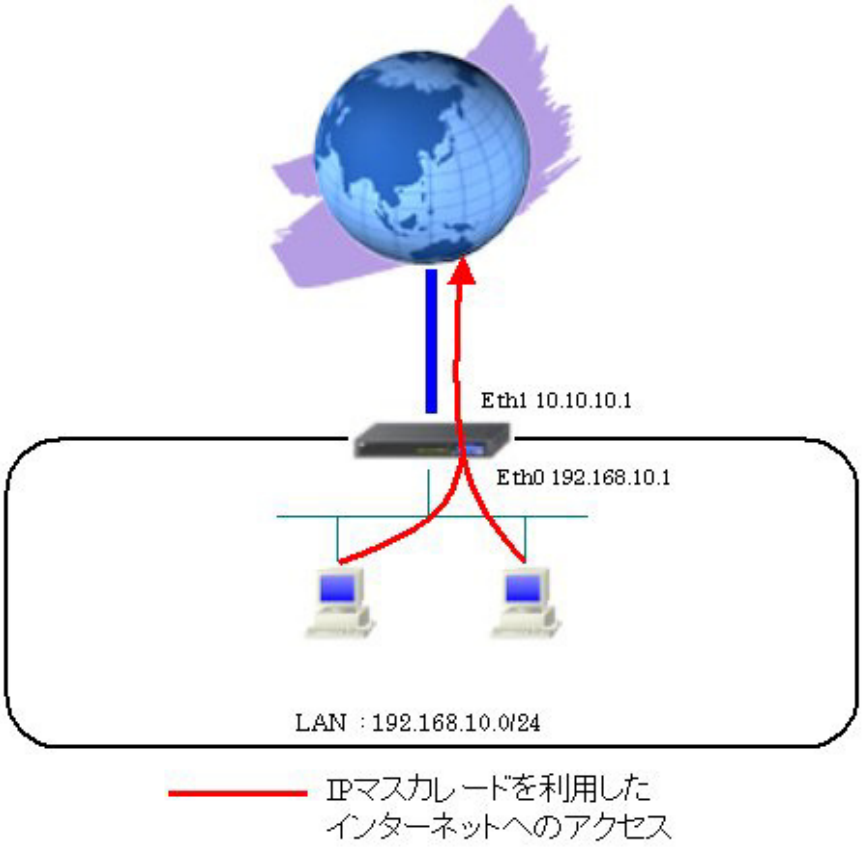
接続が完了した場合、回線状態が以下のように表示されます。

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



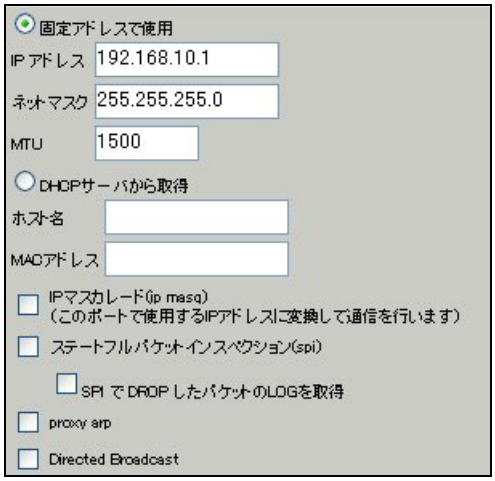
3-1-2. 設定例

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。

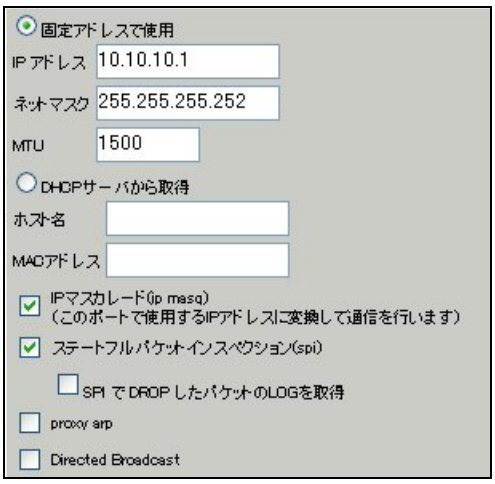


[Ethernet1 の設定]

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。

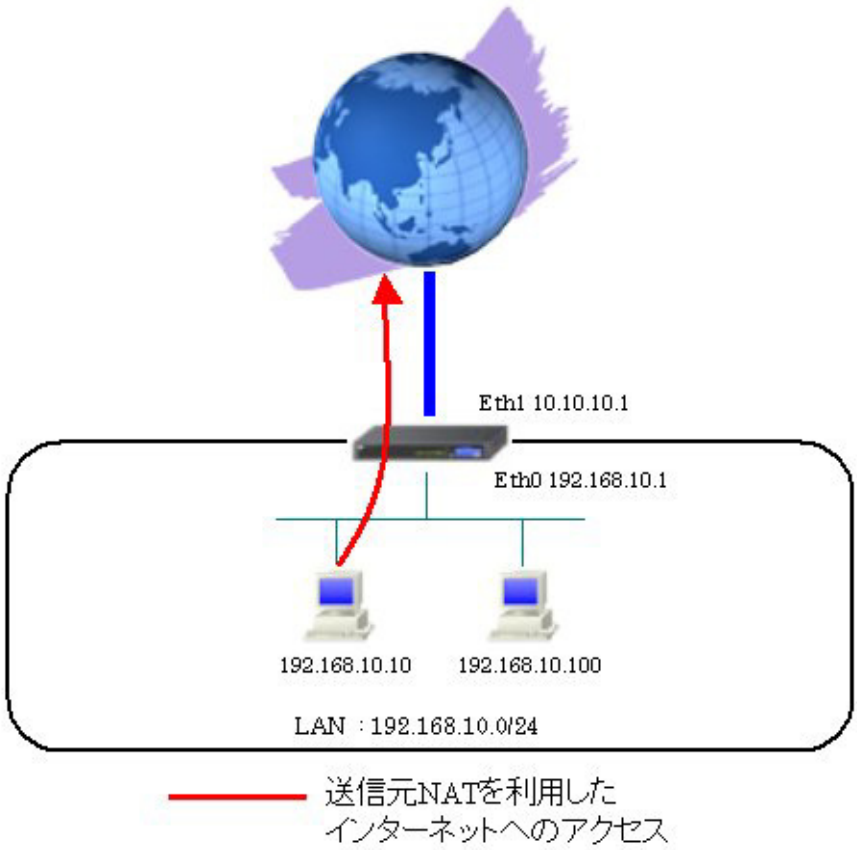


[その他の設定]

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



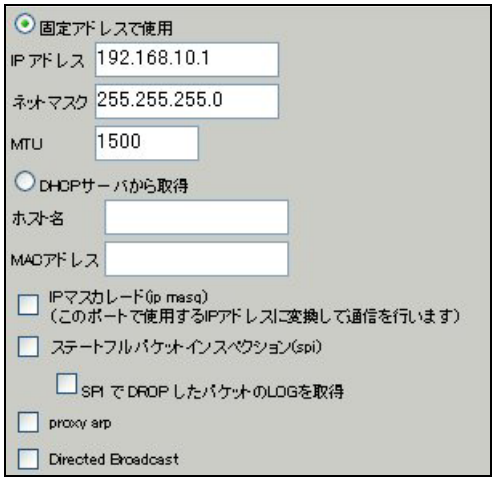
3-2-2. 設定例

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]

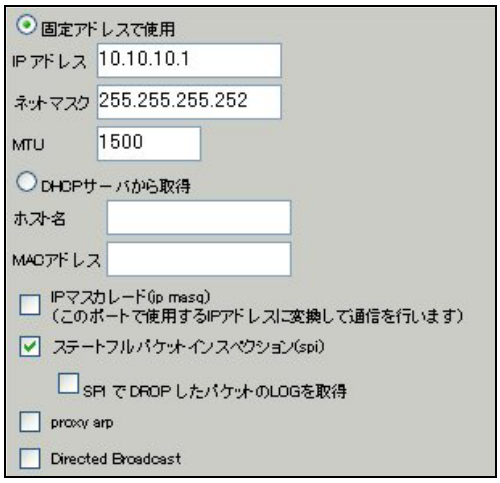
IP アドレスに「192.168.10.1」を設定します。



[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。



［その他の設定］

<<NAT 設定>>

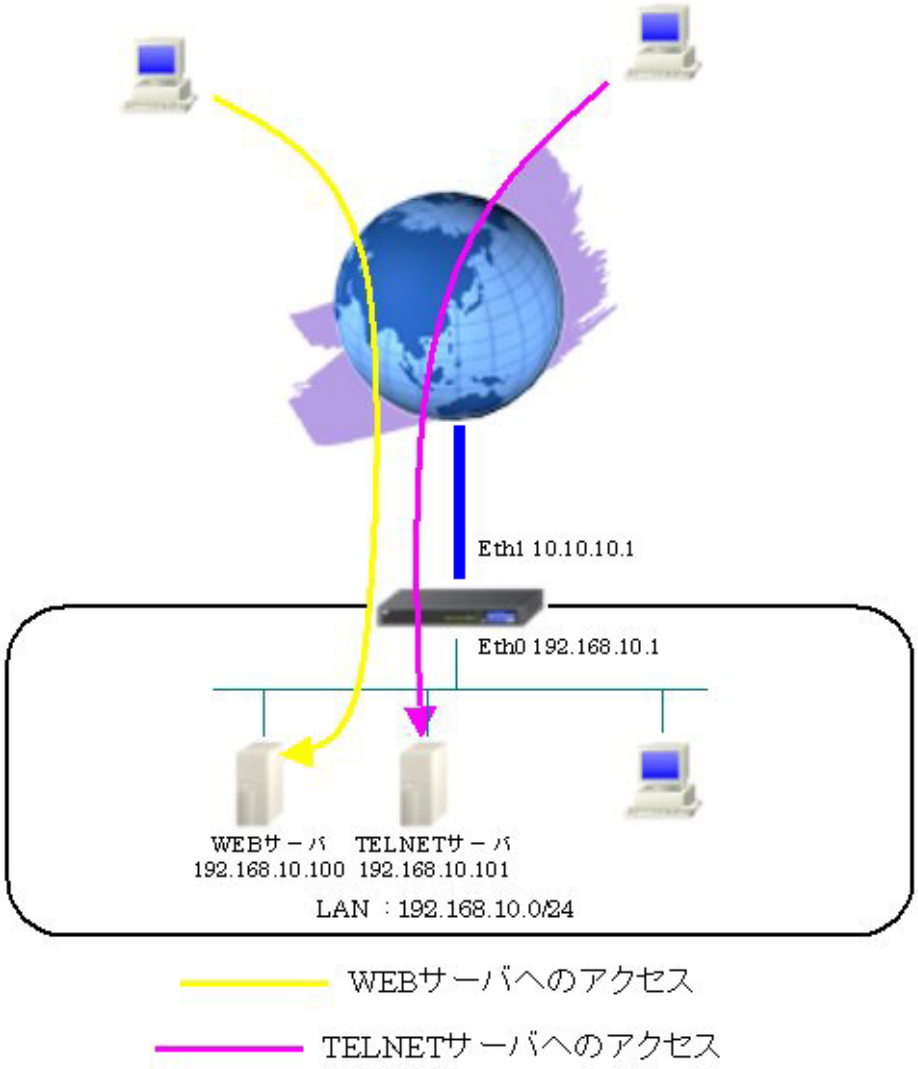
［送信元 NAT］

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。

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



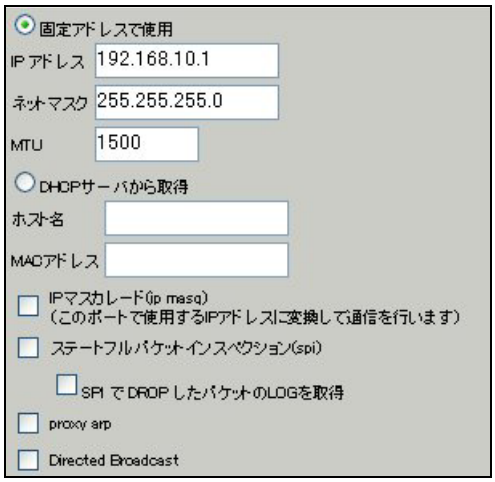
3-3-2. 設定例

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>>

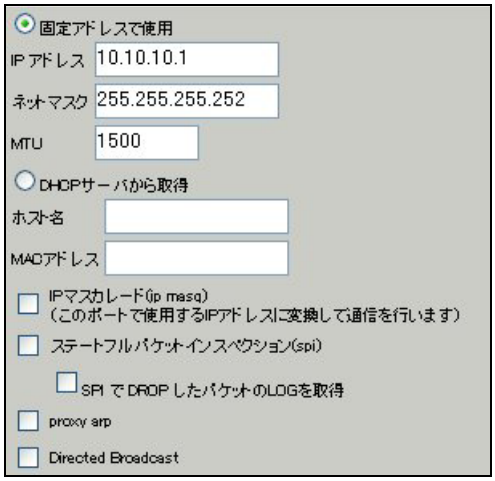
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



[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。



[その他の設定]

<<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。

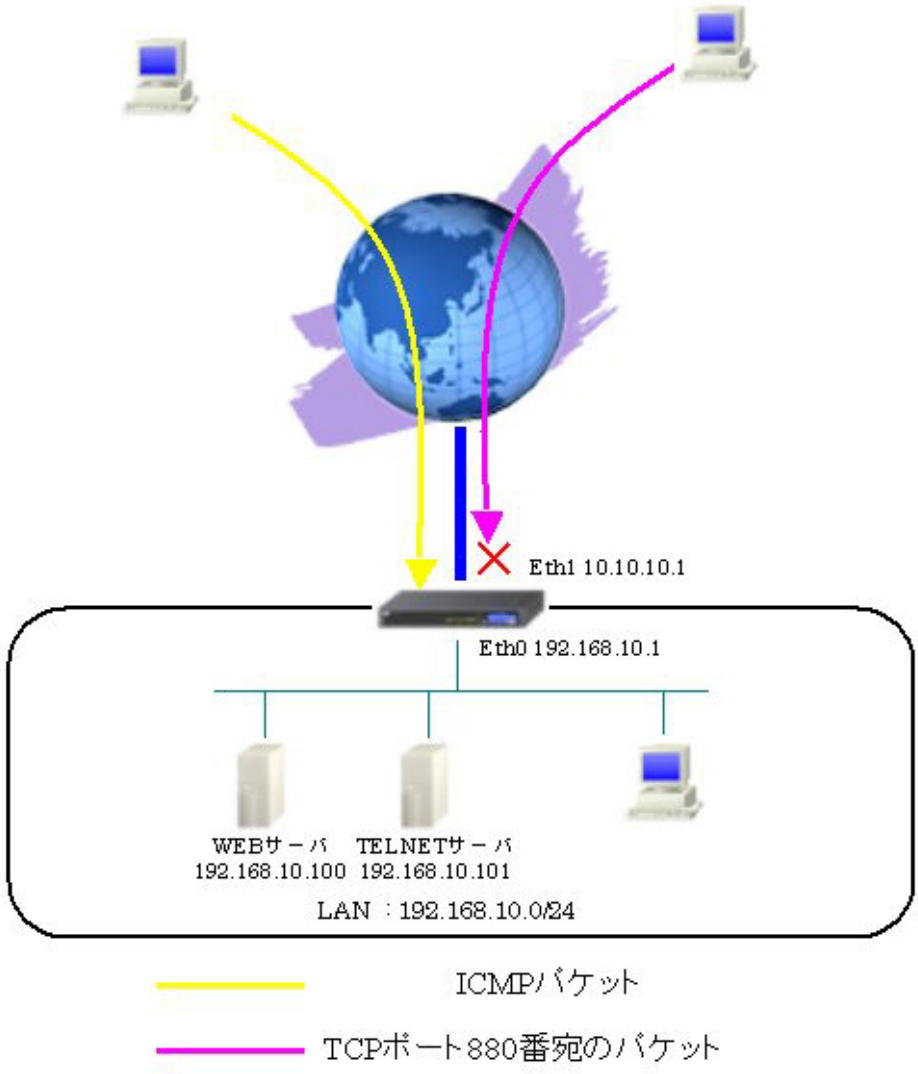
サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.10.100	10.10.10.1	tcp	80	eth1
192.168.10.101	10.10.10.1	tcp	23	eth1

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



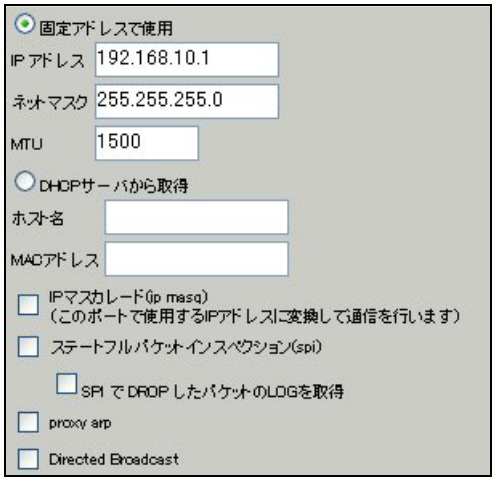
4-1-2. 設定例

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>>

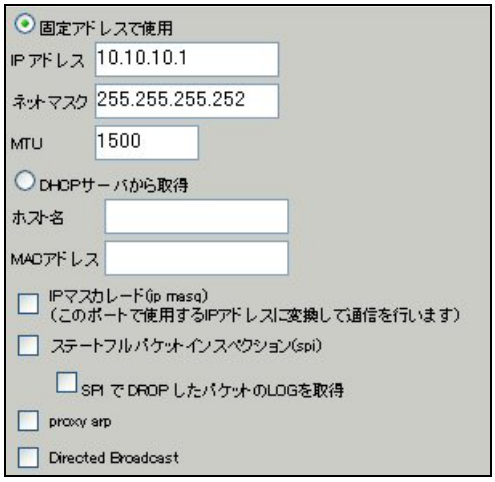
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



[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。



[その他の設定]

<<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。

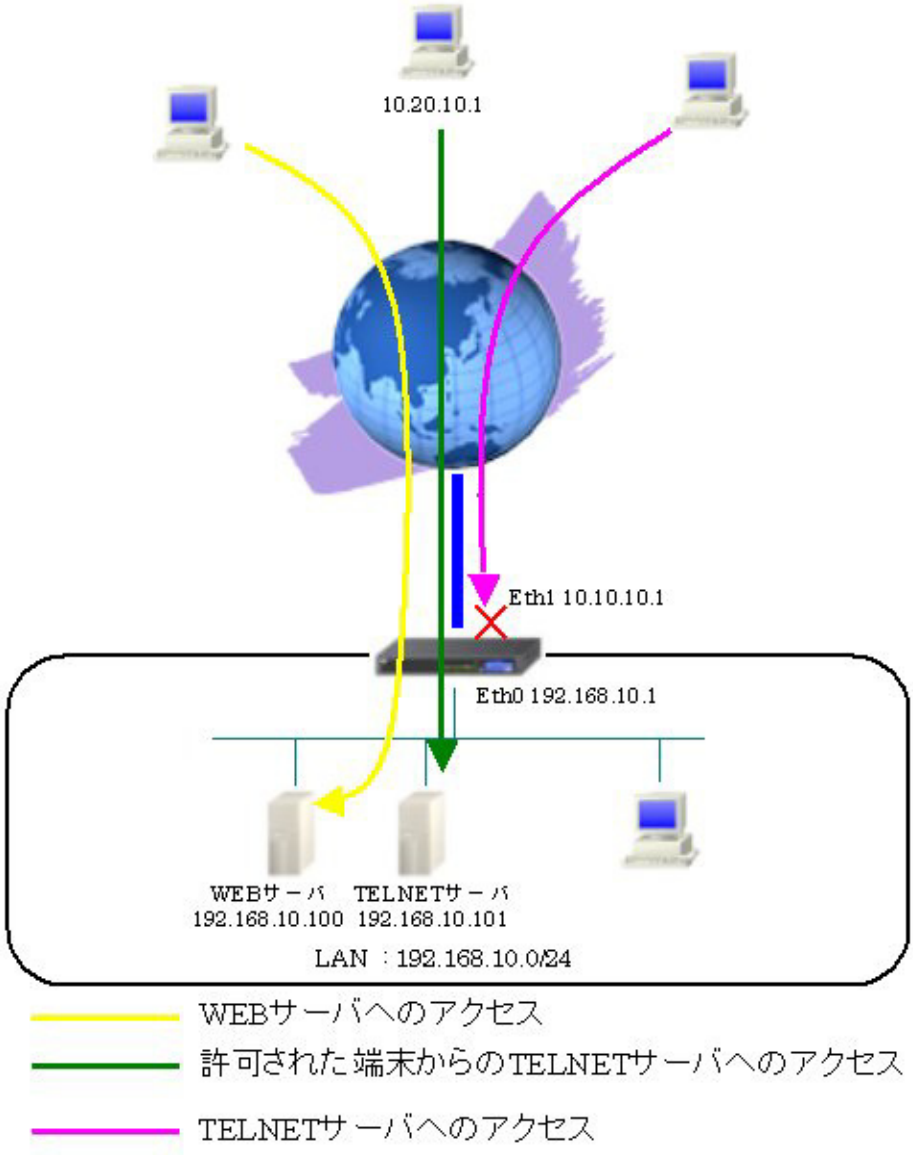
インターネット側から本装置宛の TCP ポート 880 番宛のパケットを破棄しています。

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	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
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



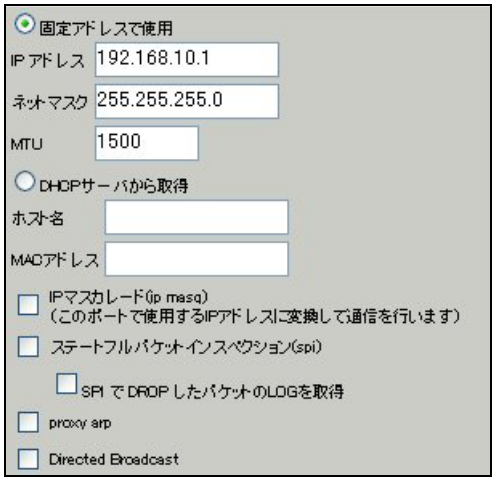
4-2-2. 設定例

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>>

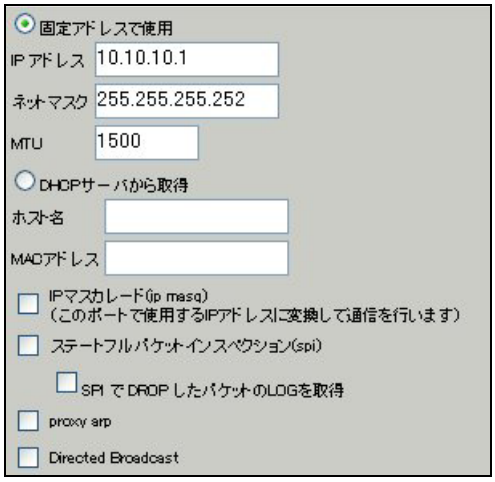
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



[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。



[その他の設定]

<<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。

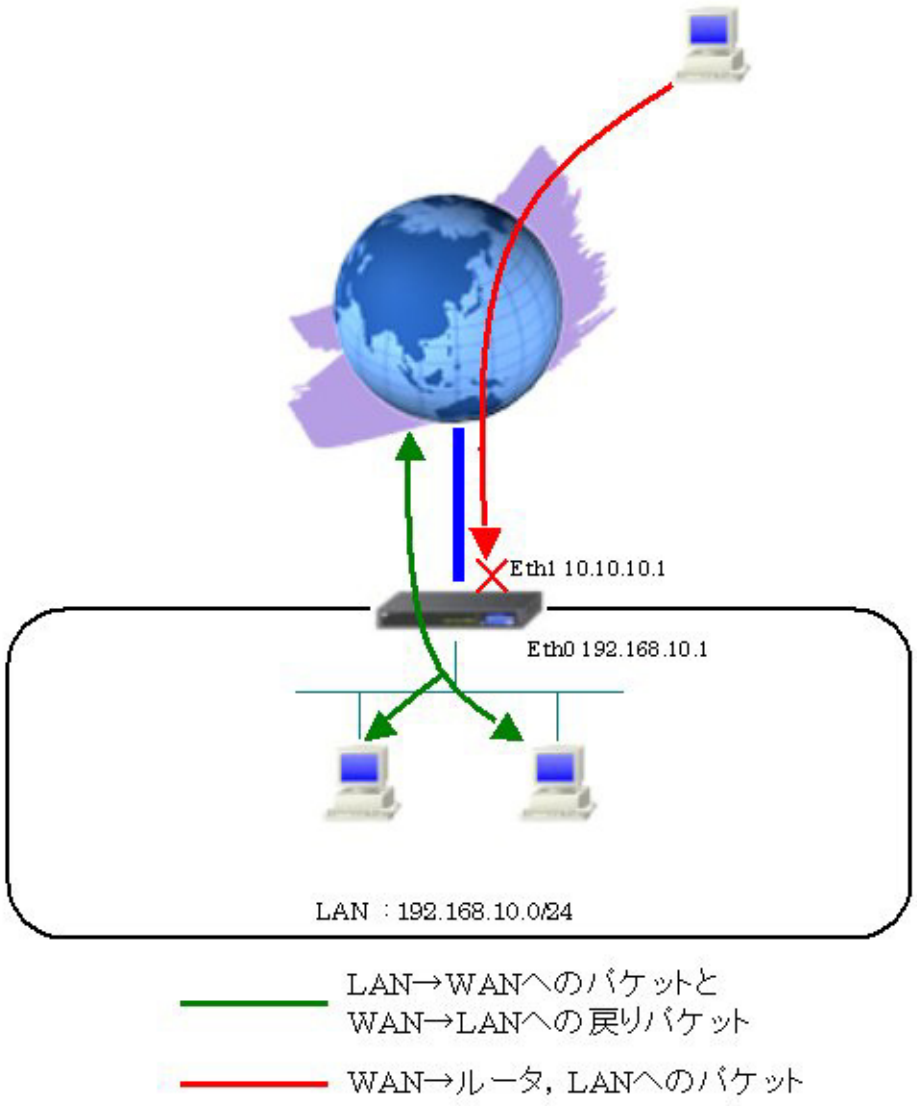
インターネットから送信元 IP アドレス「10.20.10.1」以外の TELNET サーバ（TCP ポート 23 番）宛のパケットを破棄しています。

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	あて先アドレス	あて先ポート	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

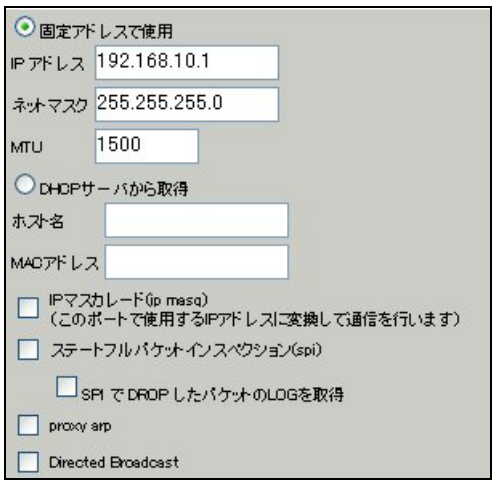


4-3-2. 設定例

<<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。

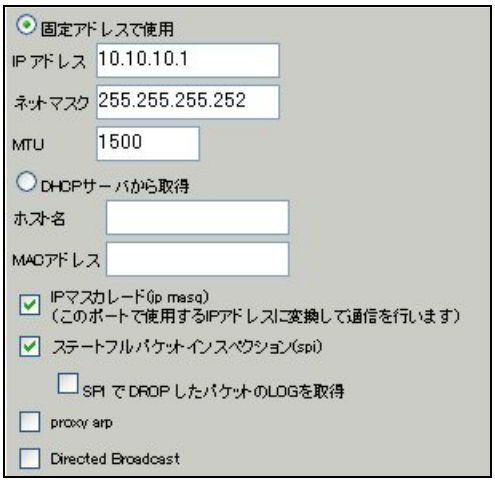


[Ethernet1 の設定]

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。



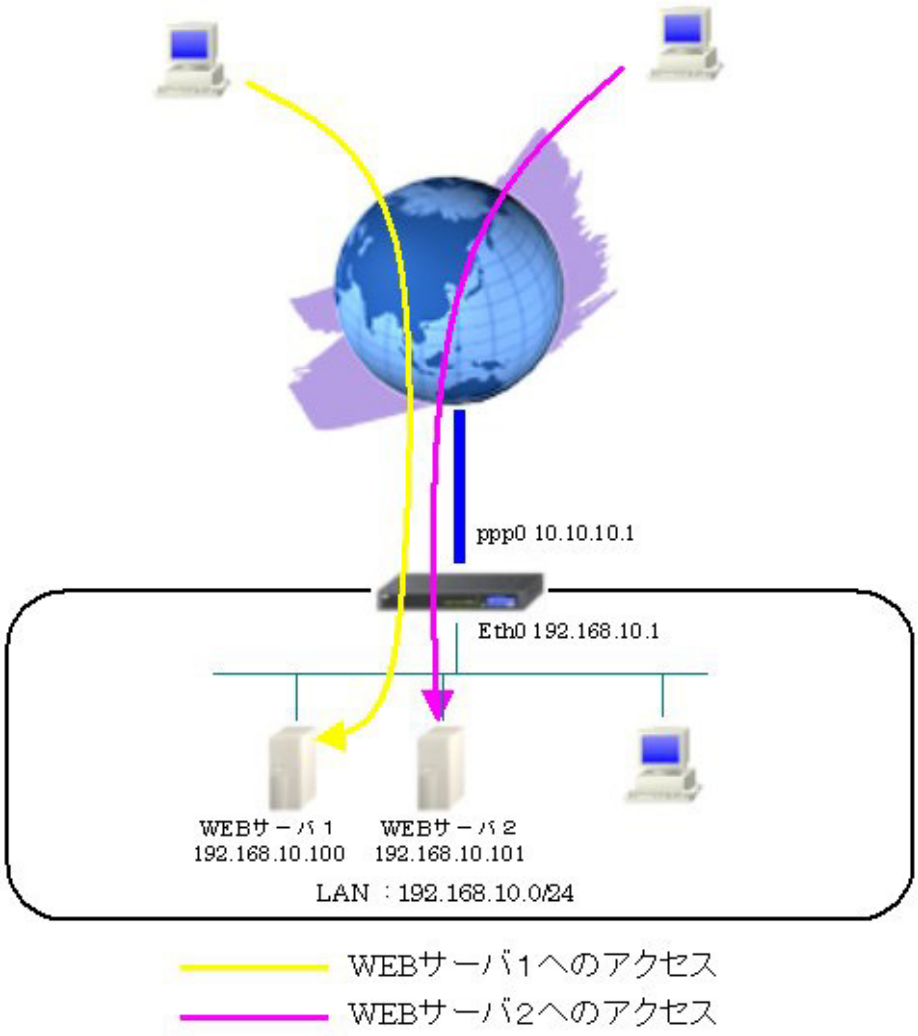
[その他の設定]

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



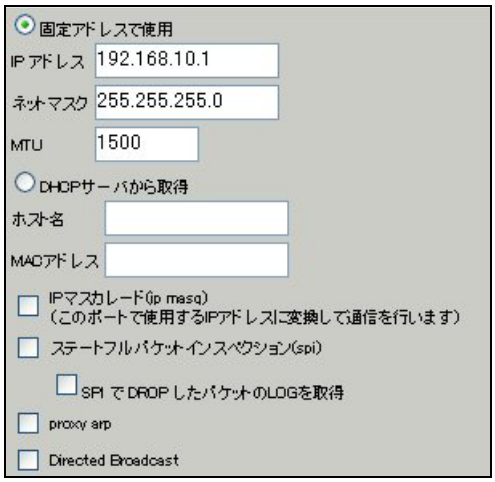
5-1-2. 設定例

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]

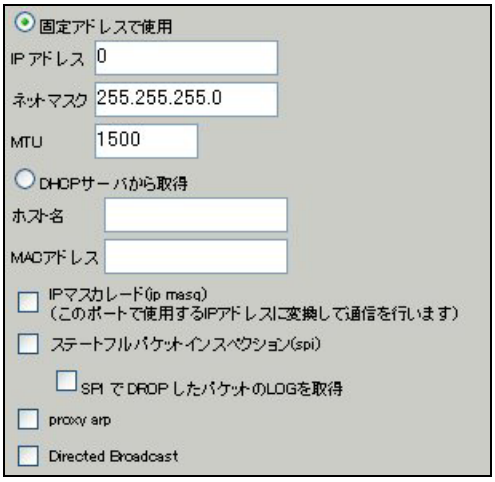
IP アドレスに「192.168.10.1」を設定します。



[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。

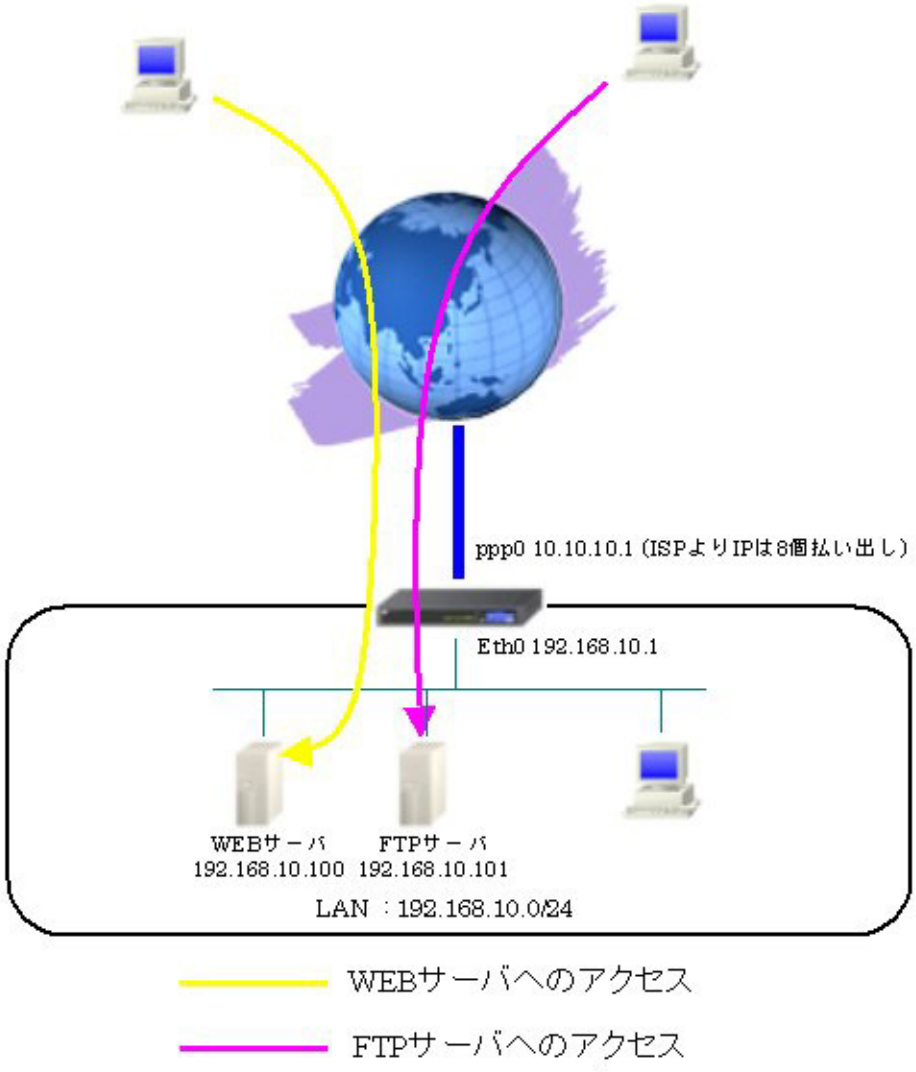
インターネットから「10.10.10.1」で TCP ポート 8080 番宛てのパケットを受信した場合は、「192.168.10.101」TCP ポート 80 番に転送します。

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



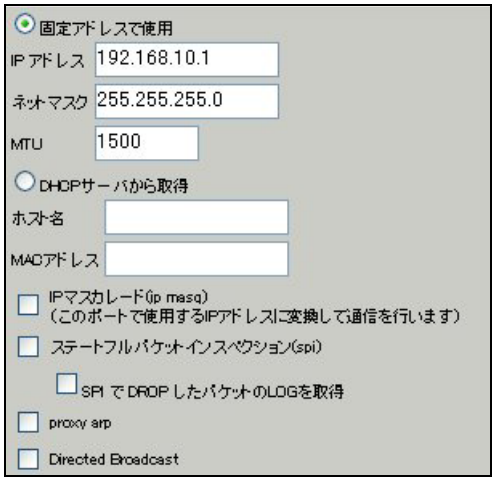
5-2-2. 設定例

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]

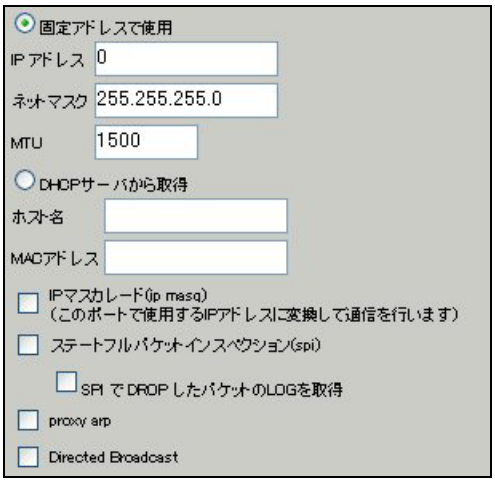
IP アドレスに「192.168.10.1」を設定します。



[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，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。

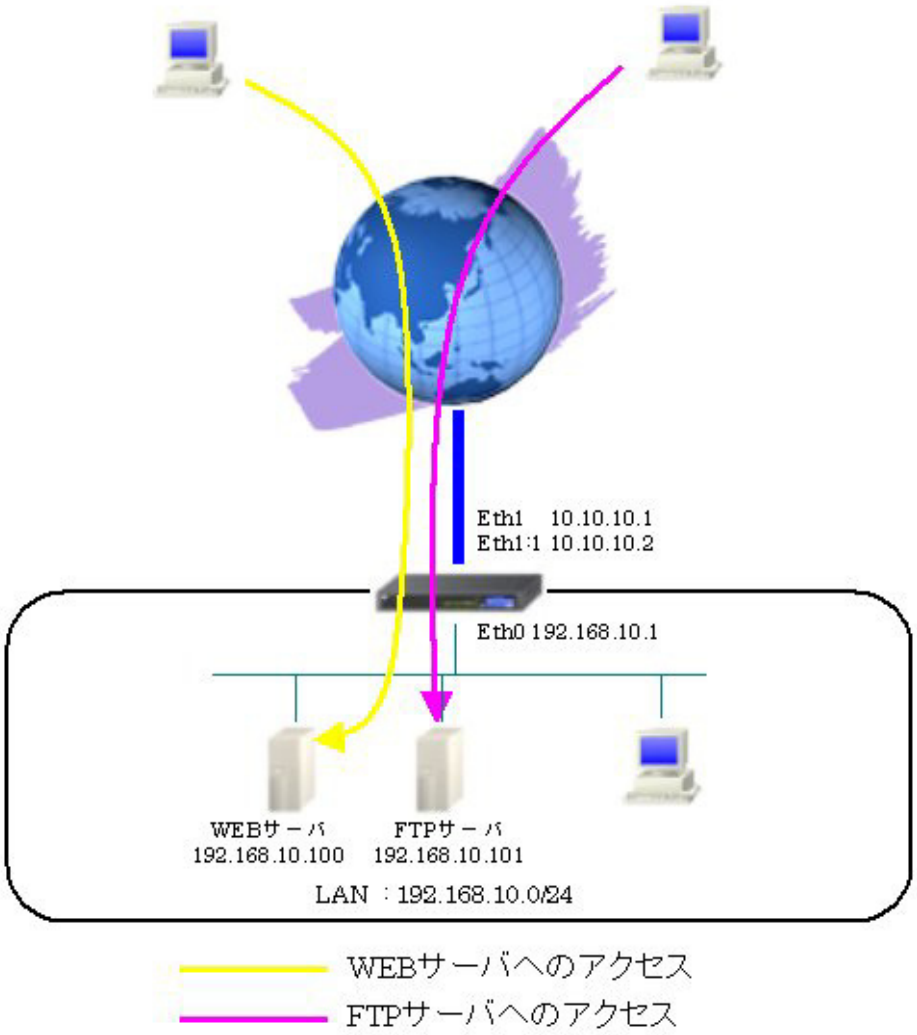
インターネットから「10.10.10.2」で TCP ポート 20,21 番宛てのパケットを受信した場合は、「192.168.10.101」TCP ポート 20,21 番に転送します。

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



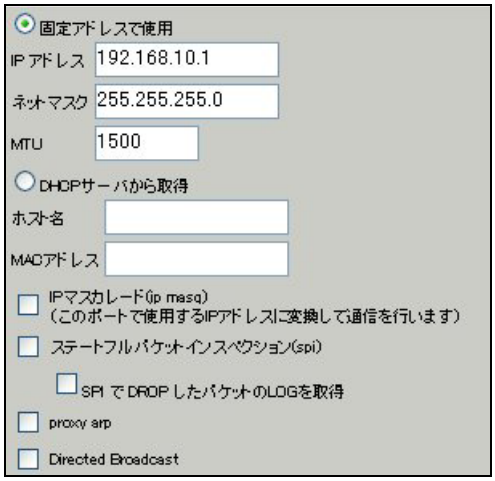
5-3-2. 設定例

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。

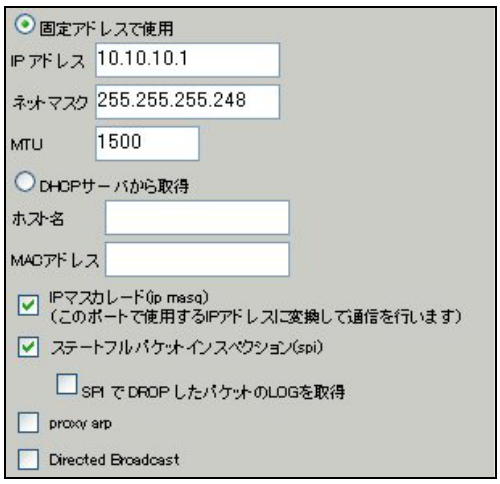


[Ethernet1 の設定]

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。



[その他の設定]

<<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	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
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。

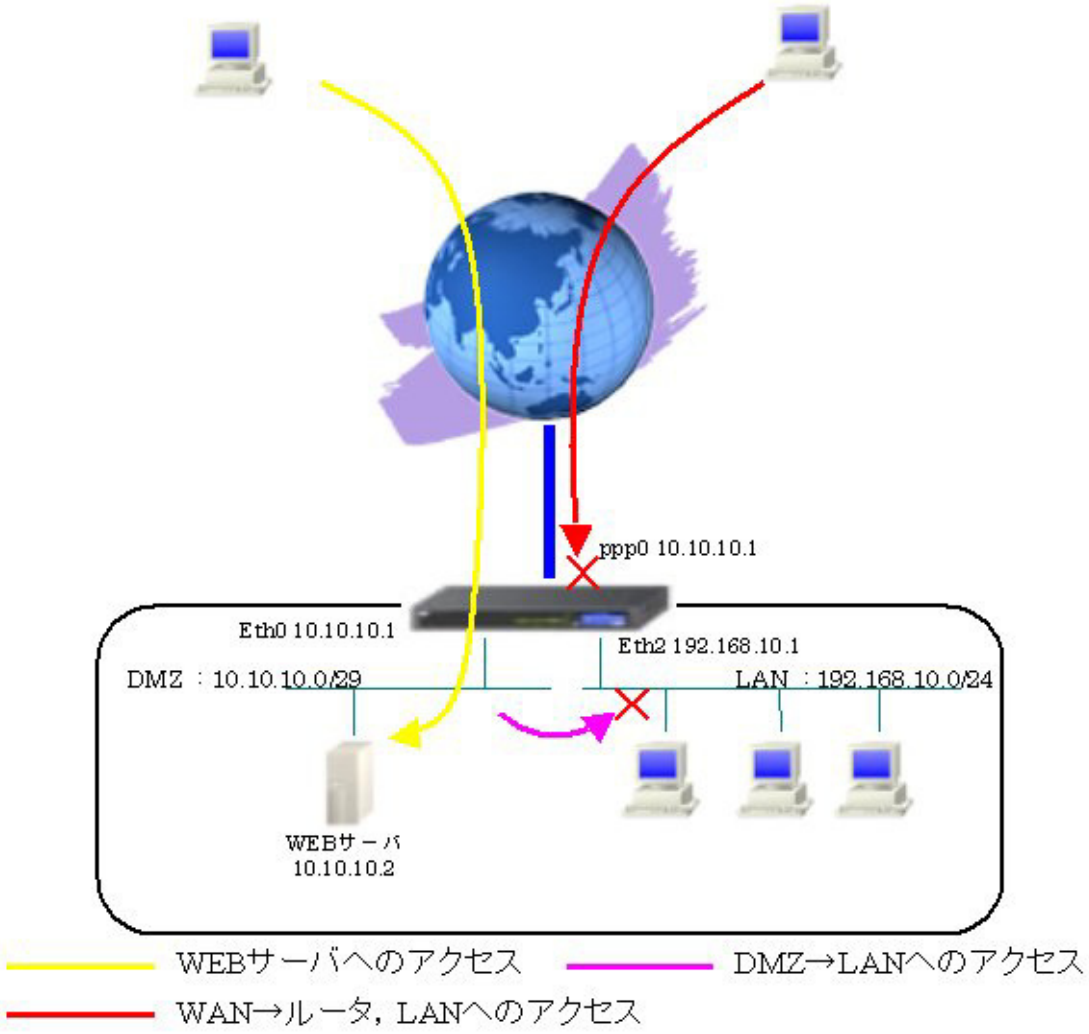
インターネットから「10.10.10.2」で TCP ポート 20,21 番宛てのパケットを受信した場合は、「192.168.10.101」TCP ポート 20,21 番に転送します。

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



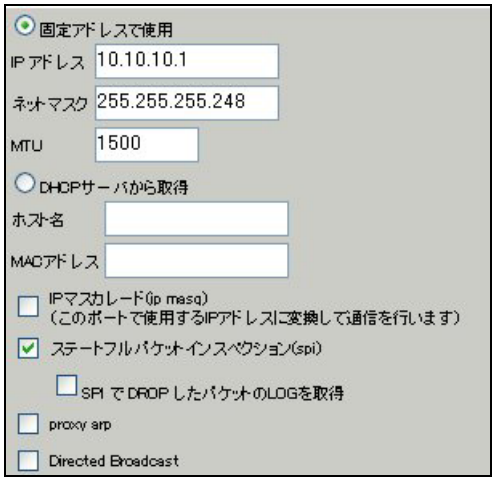
5-4-2. 設定例

<<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。

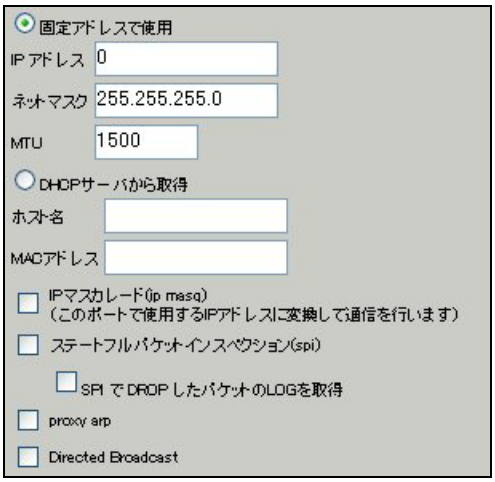
DMZ から LAN, WAN へのアクセスを制限するために、ステートフルパケットインスペクションを「有効」に設定します。



[Ethernet1 の設定]

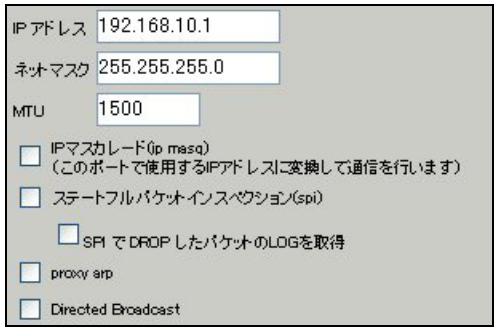
PPPoE 接続で使用するため、IP アドレスに「0」を設定します。

※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。



[Ethernet2 の設定]

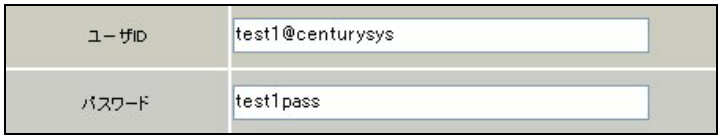
IP アドレスに「192.168.10.1」を設定します。



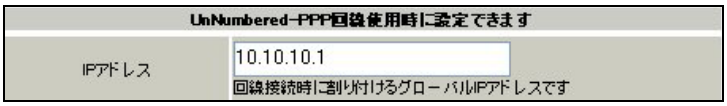
<<PPP/PPPoE 設定>>

[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。



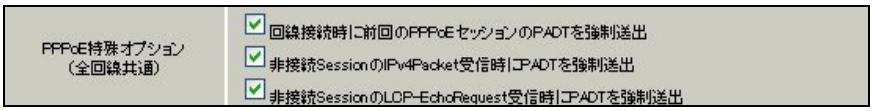
ppp0 インタフェースに割り当てる IP アドレス「10.10.10.1」を設定します。



[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。

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。



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。

<<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。

<<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。

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]

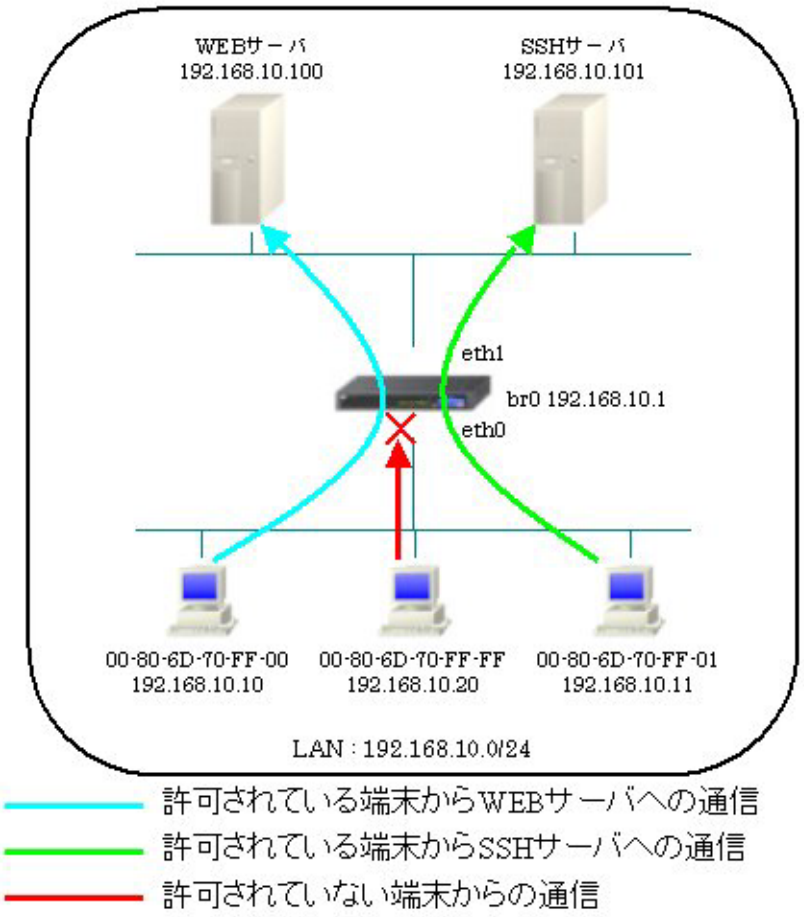
DMZ 上にある端末からインターネットへアクセス可能にするための設定をします。
ppp0 から送信される送信元 IP アドレス「10.10.10.0/29」のパケットを許可します。

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

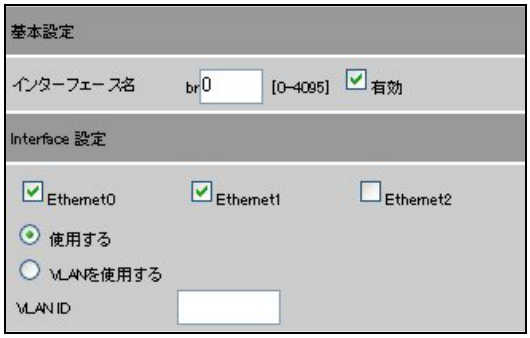
同一 LAN 内にある WEB サーバおよび SSH サーバへのアクセスを制限します。

<<インタフェース設定>>

[Bridge の設定]

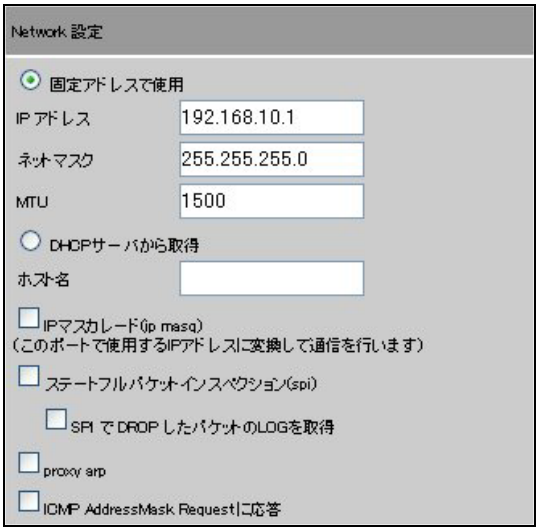
ブリッジインタフェースのインタフェース番号を設定します。

本設定例では、Ehernet0 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。

※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。



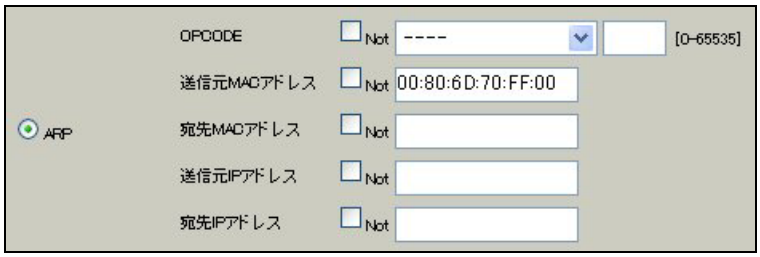
<<ブリッジフィルタ設定>>

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>

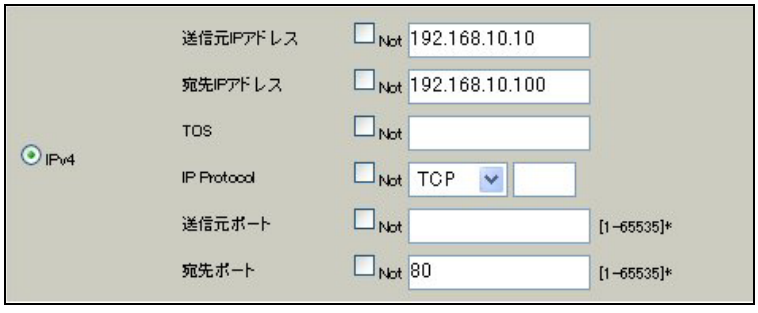
[No.1]

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。



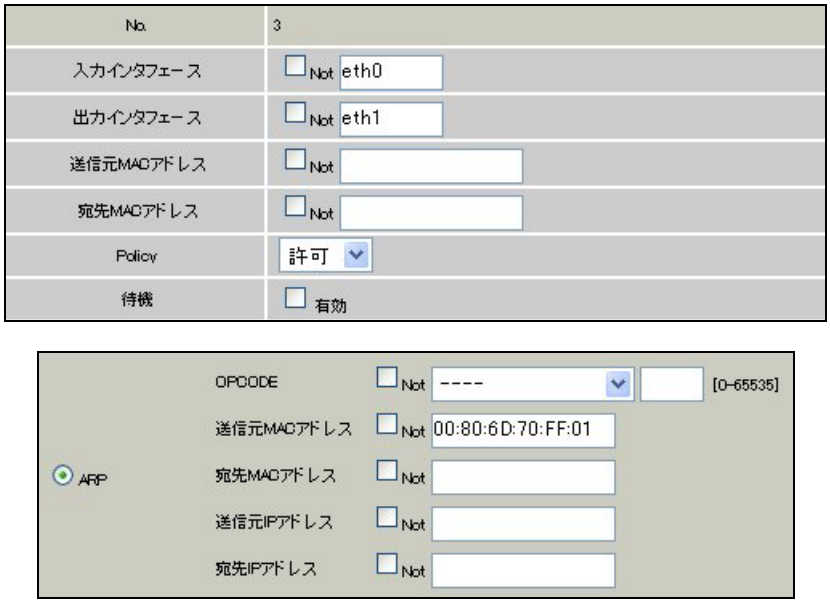
[No.2]

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。



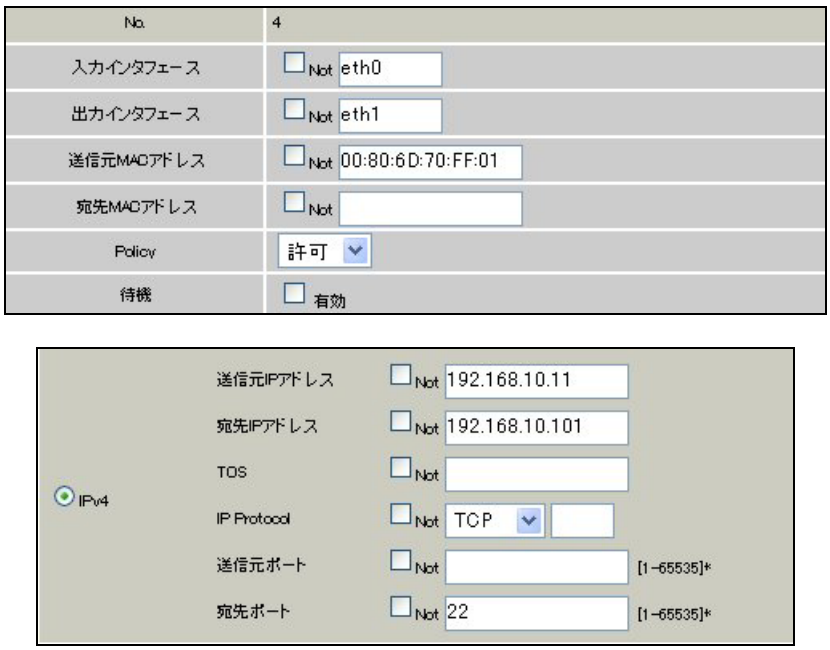
[No.3]

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。



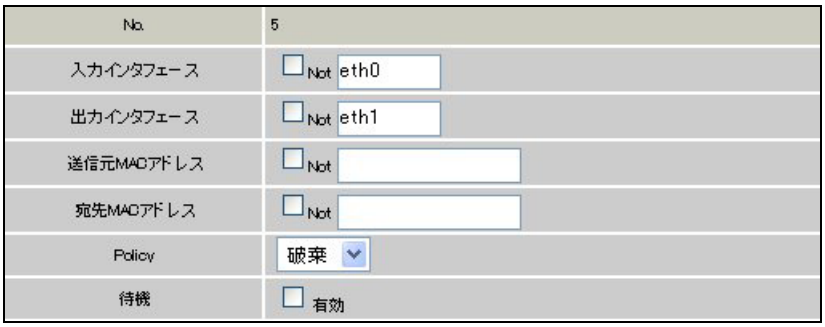
[No.4]

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.5]

eth0→eth1 へのその他の通信は破棄する設定をします。

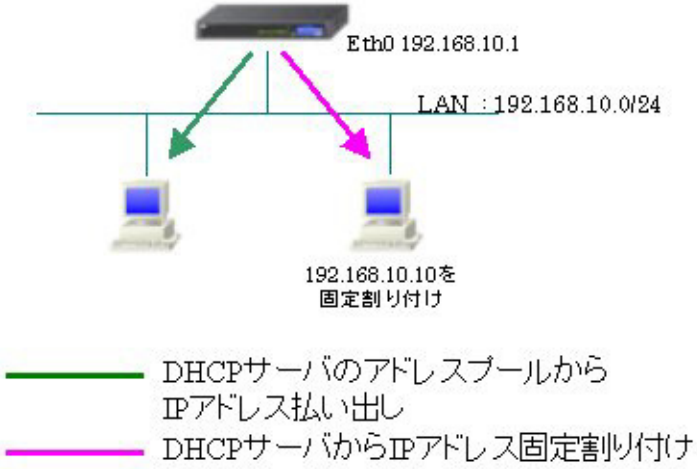


7. DHCP 設定

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することが可能です。
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

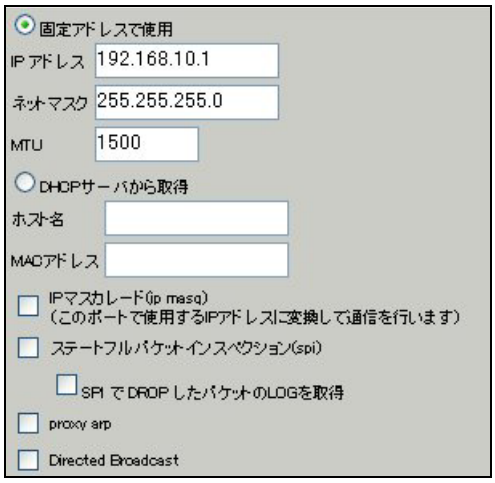


7-1-2. 設定例

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。



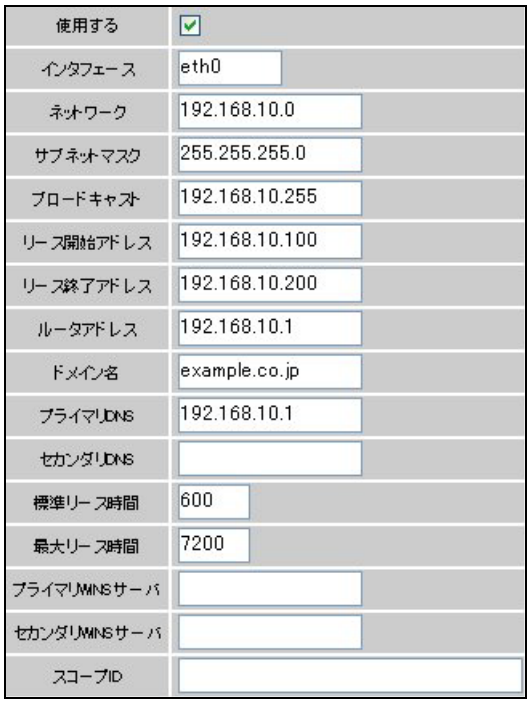
<<各種サービスの設定>>

<DHCP(Relay)サーバ>

[DHCP 設定]
「DHCP サーバを使用する」を選択します。

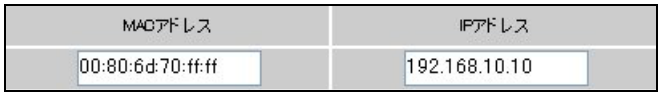
[DHCP サーバ設定]

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。



[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。



【DHCP(Relay)サーバ】

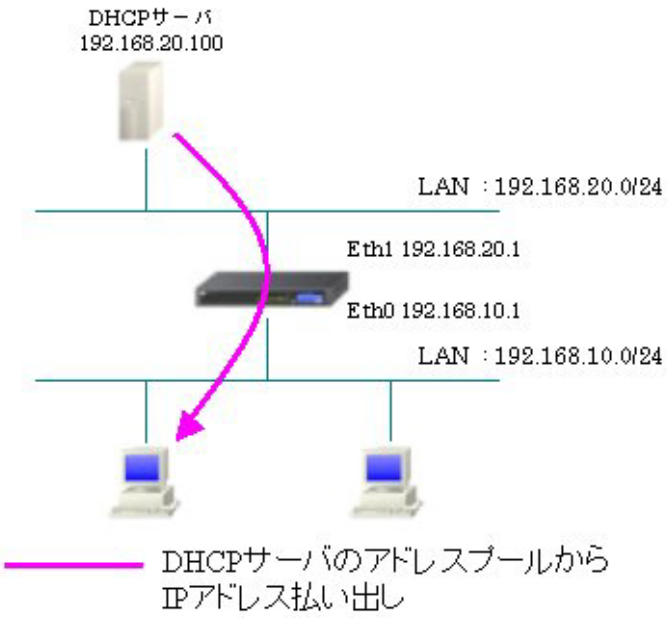
DHCP(Relay)サーバを起動します。

※動作中の場合は、一度「停止」→「起動」を行ってください。

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

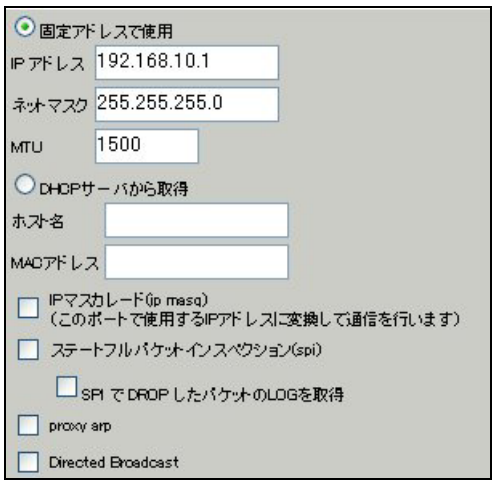


7-2-2. 設定例

<<インタフェース設定>>

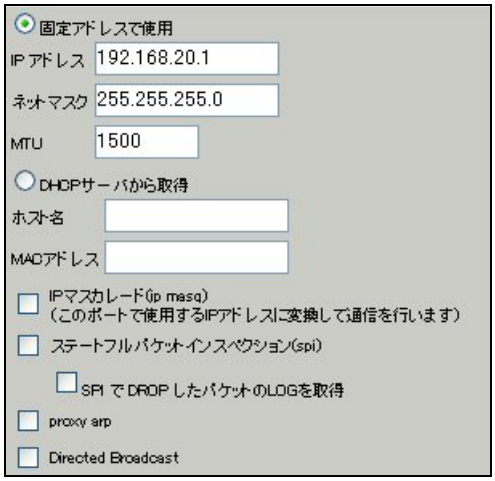
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



[Ethernet1 の設定]

IP アドレスに「192.168.20.1」を設定します。



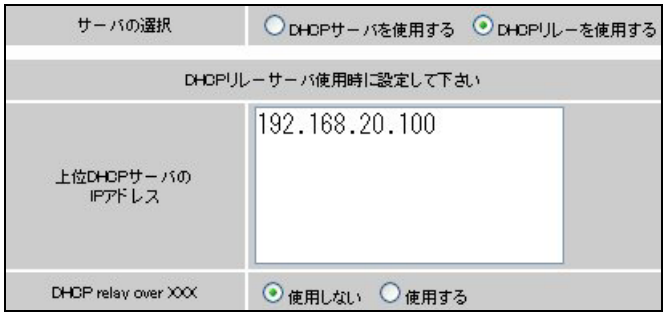
<<各種サービスの設定>>

<DHCP(Relay)サーバ>

[DHCP 設定]

「DHCP 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。



【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。

8. 攻撃検出設定

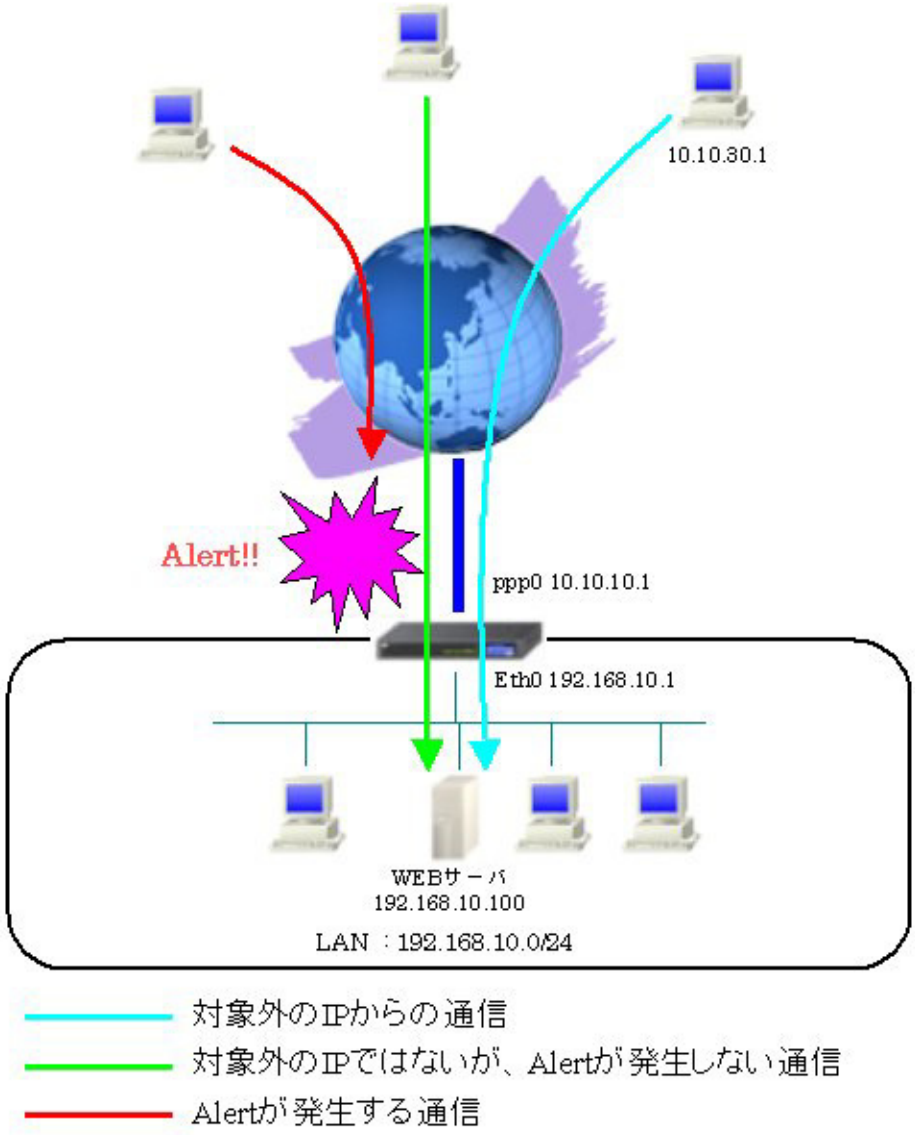
8-1. アクティブファイアウォールの利用

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



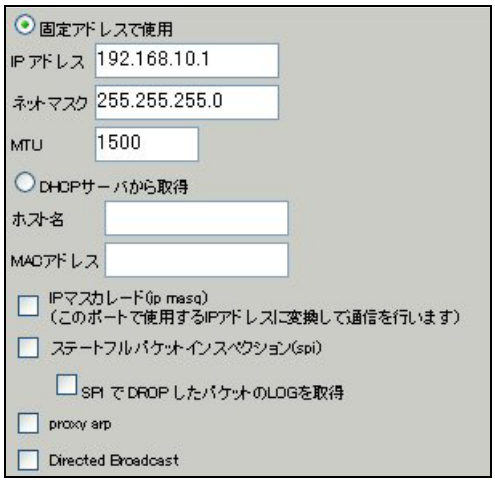
8-1-2. 設定例

「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]

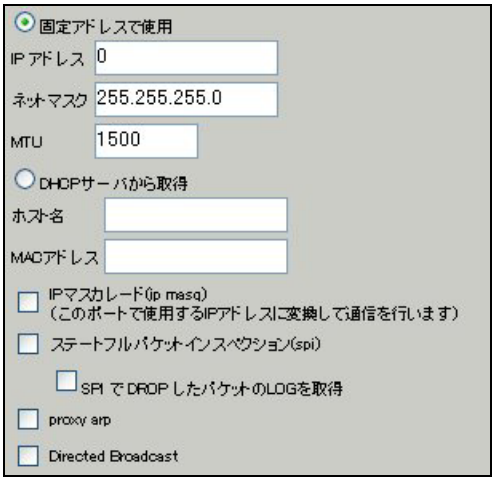
IP アドレスに「192.168.10.1」を設定します。



[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。

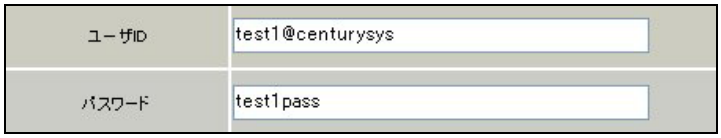
※PPPoE で接続する場合には“ppp”という論理インタフェースを自動的に生成し、この論理インタフェースを使って PPPoE 接続を行います。



<<PPP/PPPoE 設定>>

[接続先設定]

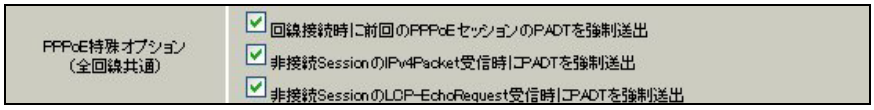
PPPoE 接続で使用するユーザ ID とパスワードを設定します。



[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。

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。



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。

<<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	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			□

<<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。

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。

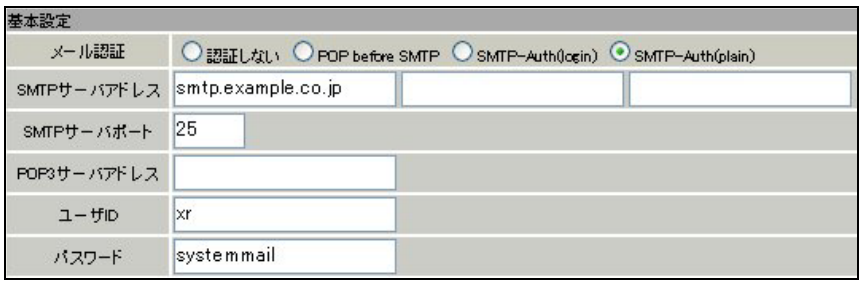
<<システム設定>>

<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。



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).

【DNS キャッシュ】

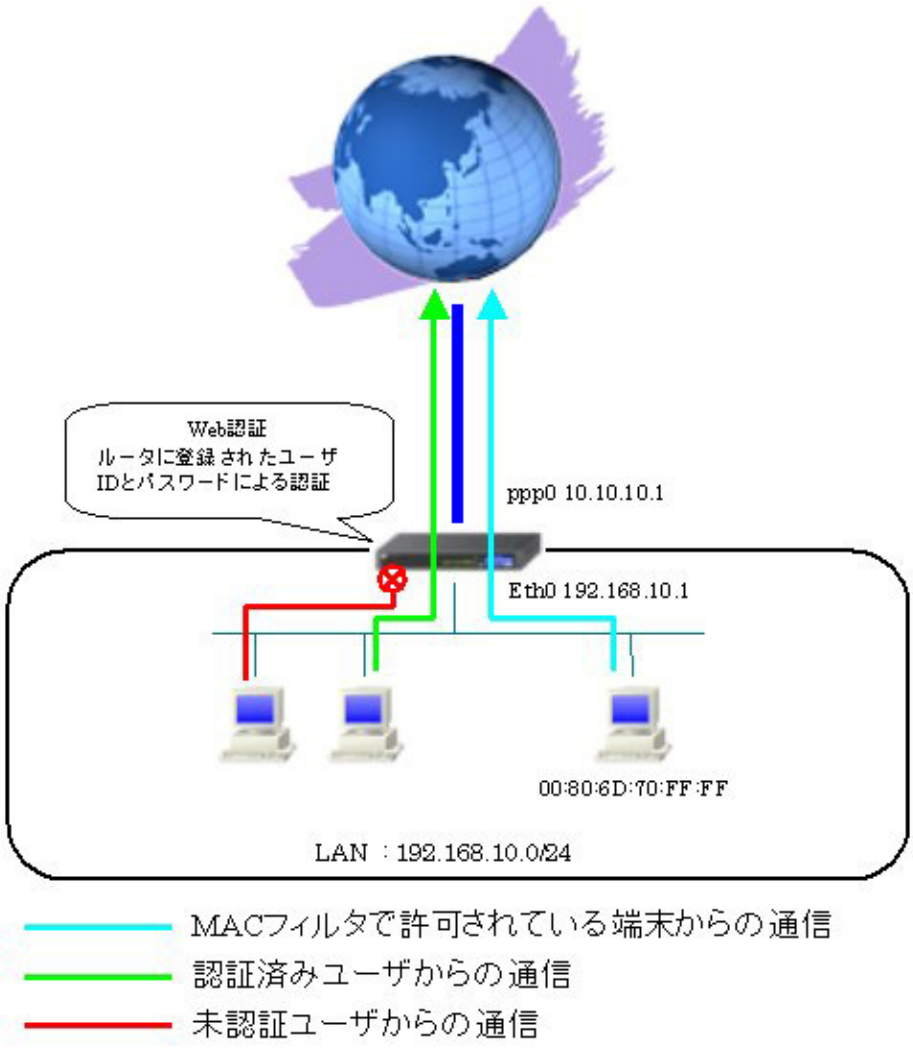
メール送信時の名前解決を可能にするため、DNS キャッシュ機能を起動します。

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



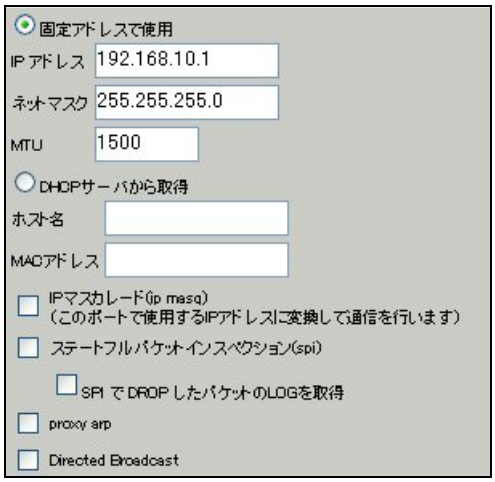
9-1-2. 設定例

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]

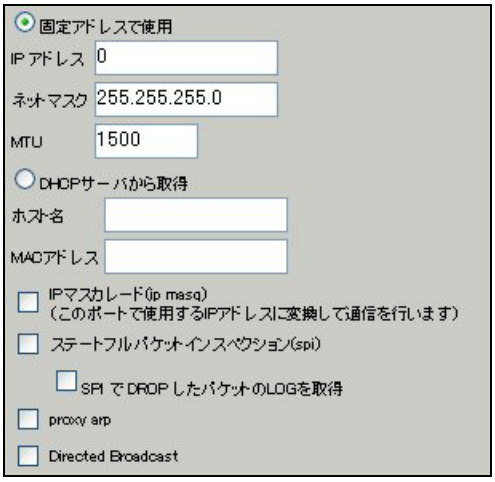
IP アドレスに「192.168.10.1」を設定します。



[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。

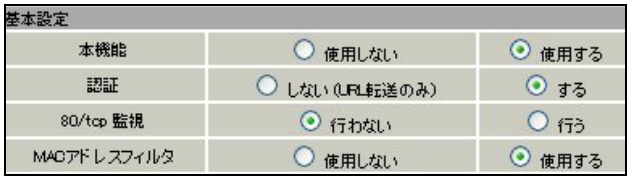
回線状態	主回線で接続しています

<<Web 認証設定>>

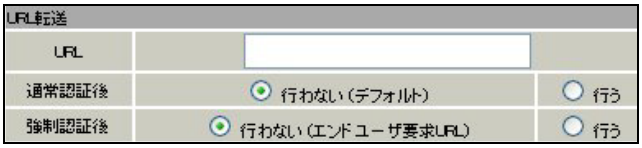
[基本設定]

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。

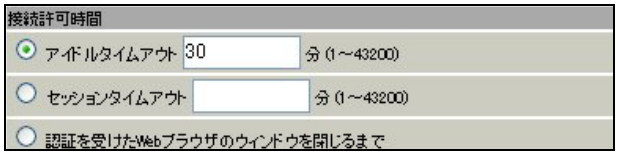


URL 転送は行わないため、設定していません。



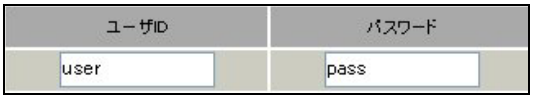
XR でアカウントの管理を行うため、「ローカル」を選択します。

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。



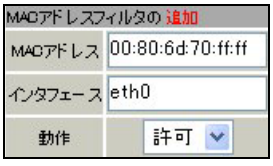
[ユーザ設定]

認証で使用するユーザ ID，パスワードを設定します。

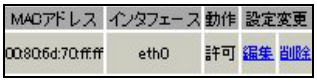


[MAC アドレスフィルタ]

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。



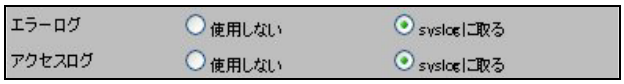
MAC アドレスフィルタ登録後は、以下のように表示されます。



［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。



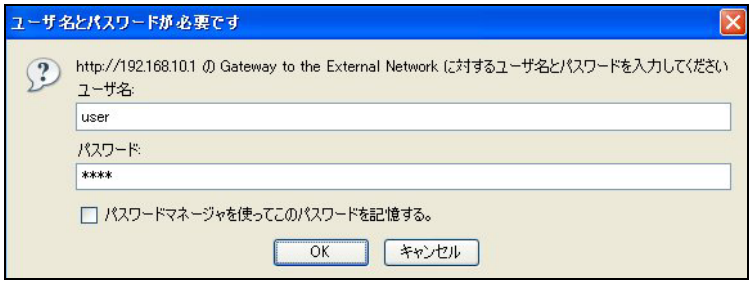
9-1-3. 設定例補足（ユーザ認証方法）

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。

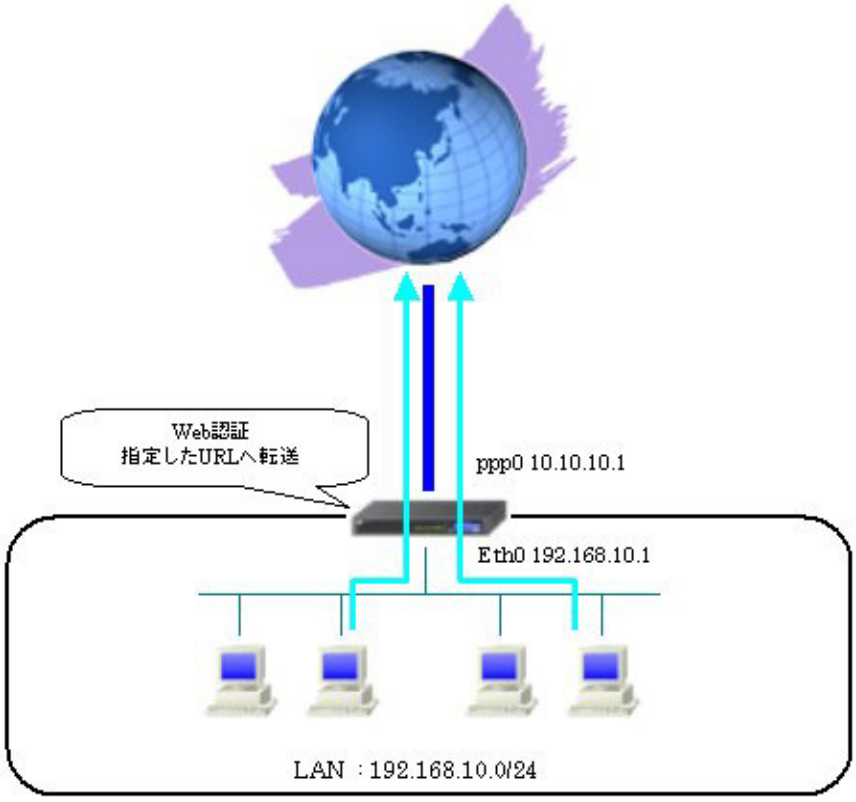
You can connect to the External Network (user@192.168.10.100).

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



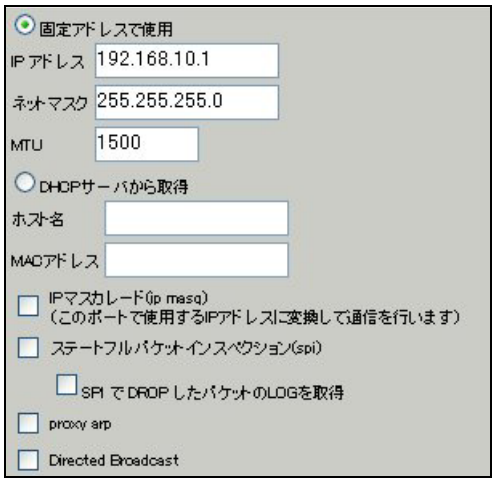
9-2-2. 設定例

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]

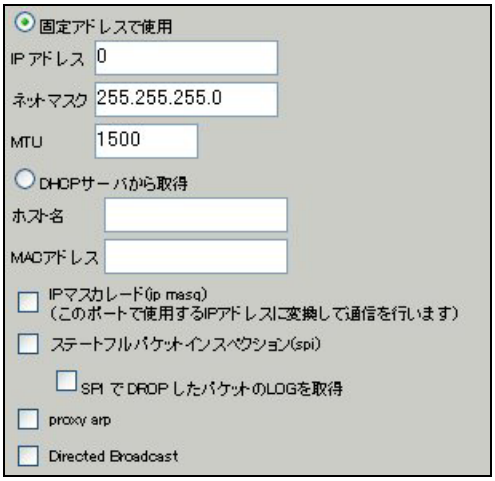
IP アドレスに「192.168.10.1」を設定します。



[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

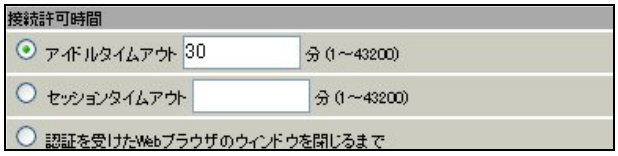
<<Web 認証設定>>

［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 番のコネクションがあったときに、強制的に Web 認証を行うように設定します。

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。

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。



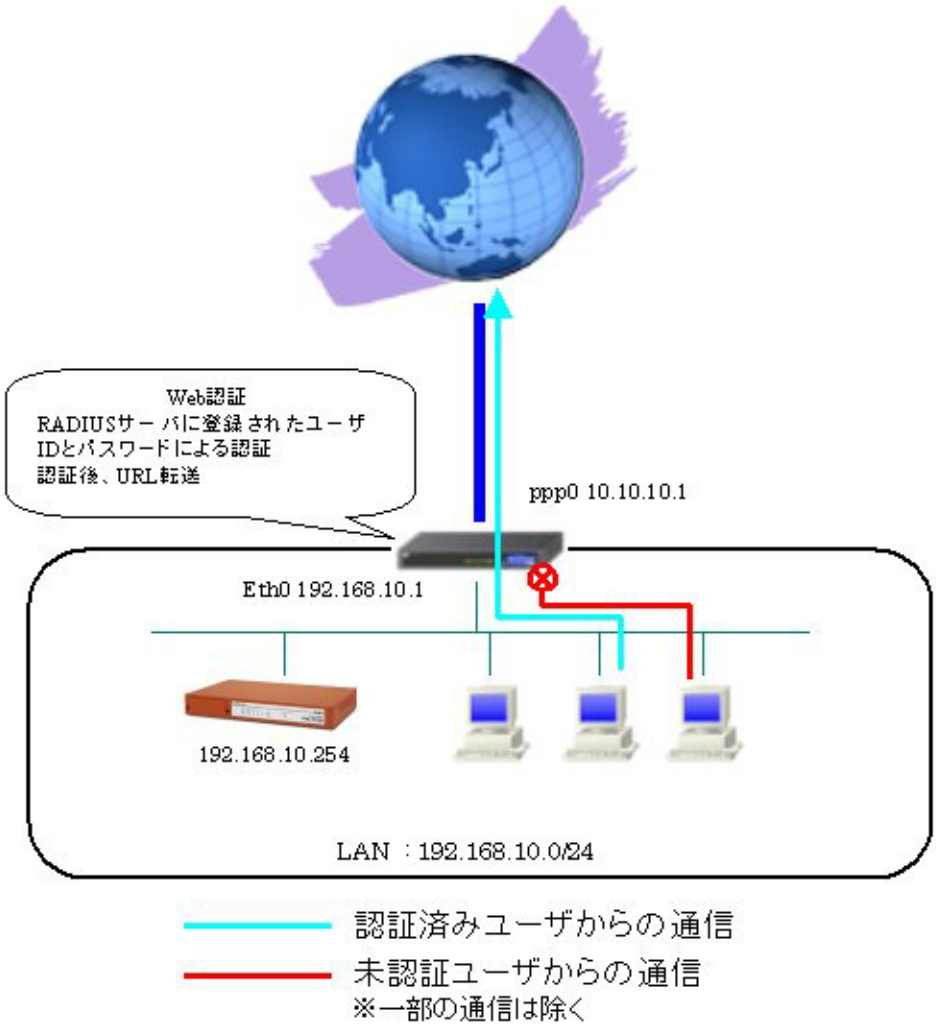
［フィルタ設定］

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。

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

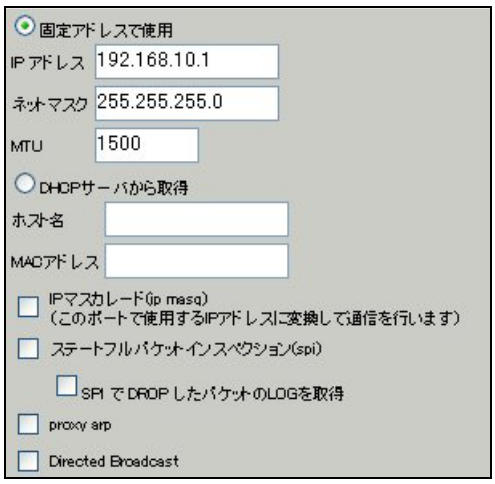
《XR の設定》

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>>

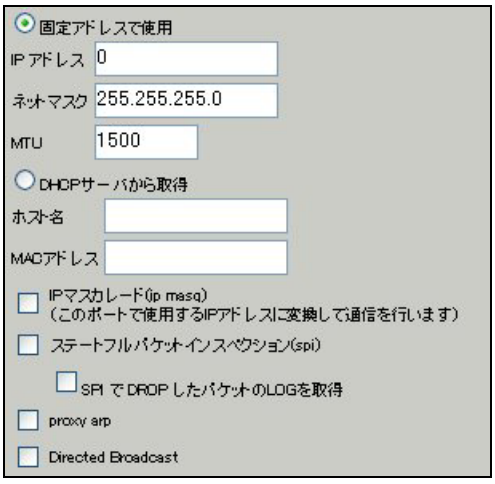
[Ethernet0 の設定]

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。

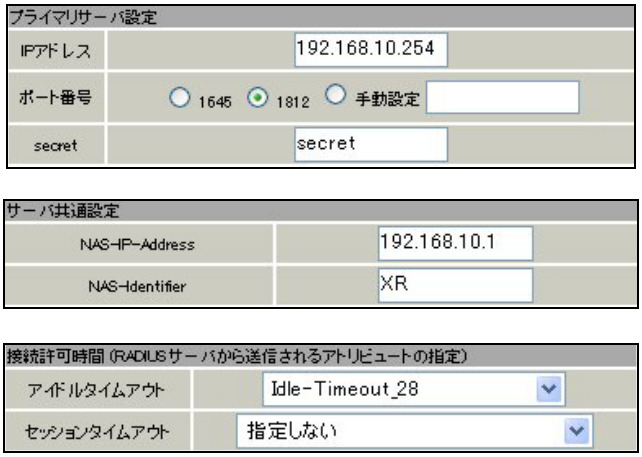
回線状態	主回線で接続しています

<<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。



[基本設定]

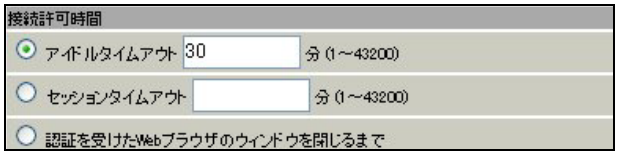
TCP ポート 80 番のコネクションを監視し、このコネクションがあった際に認証画面がポップアップするように、80/tcp 監視を「行う」を選択します。

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。

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。

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。



［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》

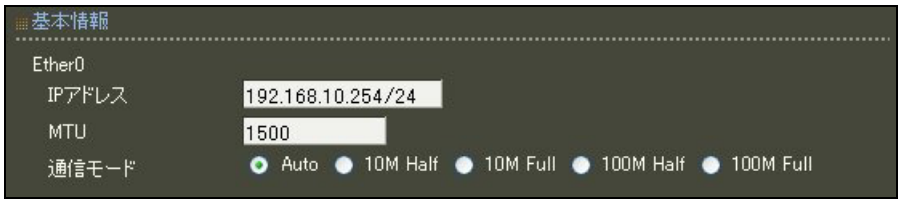
<<管理機能>>

<ネットワーク>

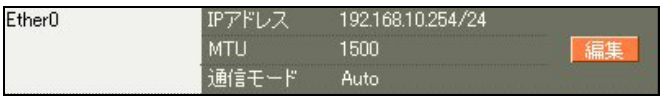
[基本情報]

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。



<<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。

<プロファイル>

[ユーザ基本情報]

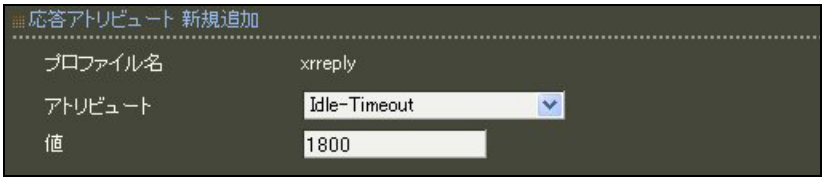
ユーザを作成するためにはユーザ基本情報プロファイルの作成が必要です。

認証方式として「PAP/CHAP」を選択します。

[応答アトリビュート]

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。



[ユーザプロファイル]

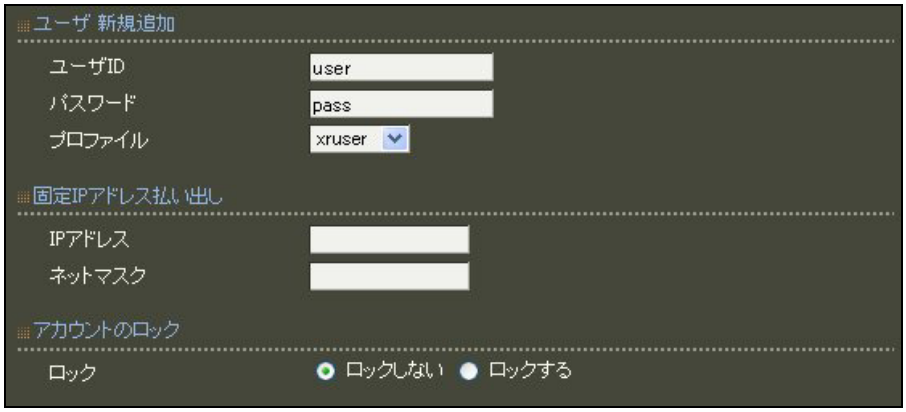
作成したユーザ基本情報を選択してユーザプロファイルを作成します。

<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。

プロファイルはユーザプロファイルで作成した「xruser」を選択します。



<<RADIUS>>

<サーバ>

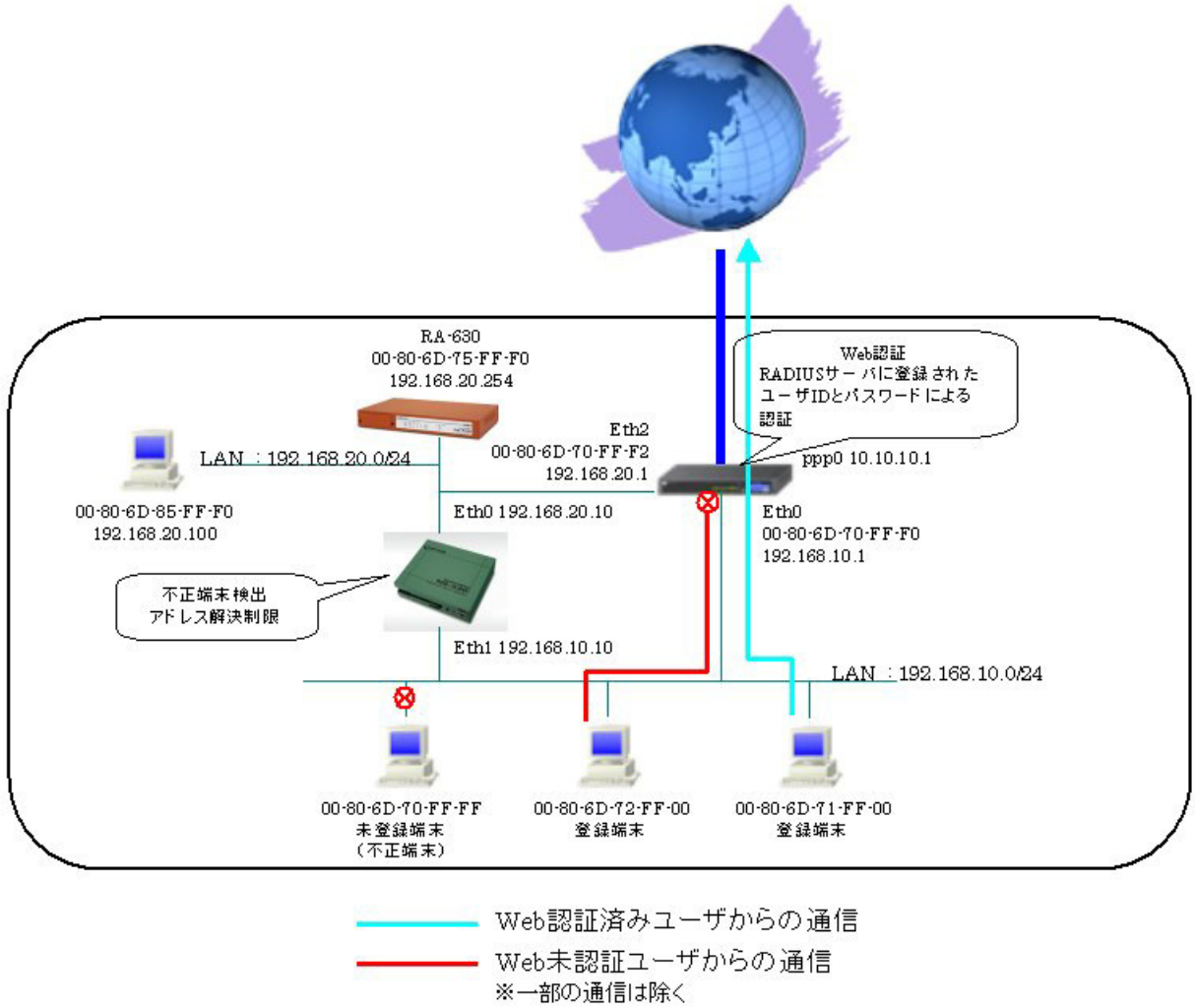
[起動・停止]

RADIUS サーバを起動し設定を反映させます。

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

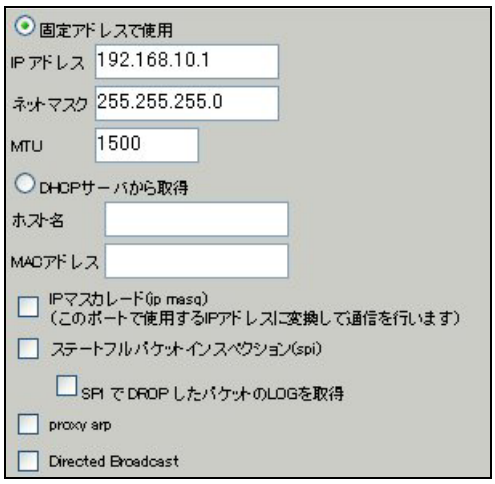
《XR の設定》

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>>

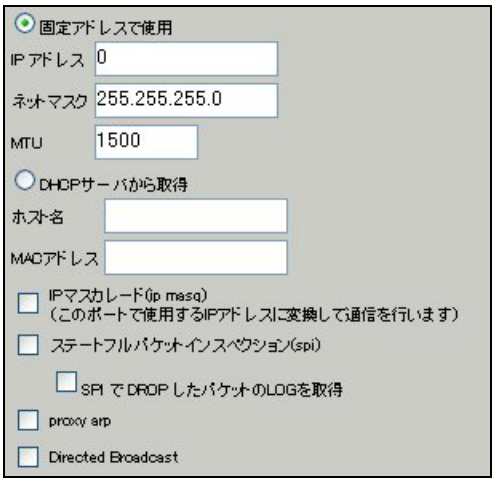
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



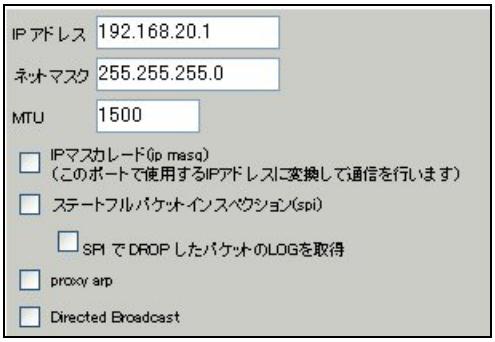
[Ethernet1 の設定]

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。



[Ethernet2 の設定]

IP アドレスに「192.168.20.1」を設定します。



<<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

<<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。

[基本設定]

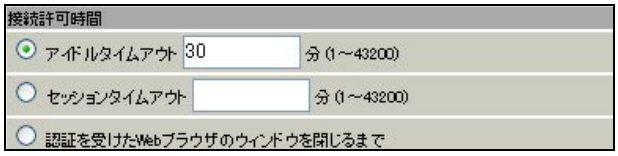
TCP ポート 80 番のコネクションを監視し、このコネクションがあった際に認証画面がポップアップするように、80/tcp 監視を「行う」を選択します。

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。

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。

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。



［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。

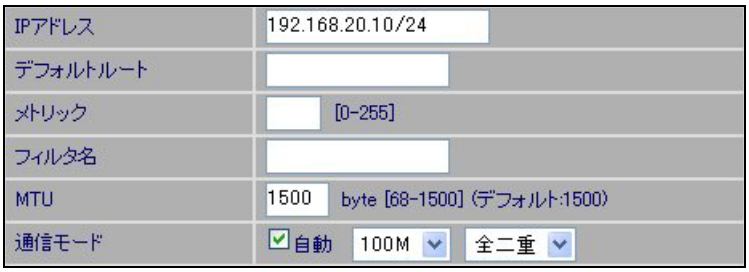
<<管理機能>>

<インタフェース>

[イーサネット]

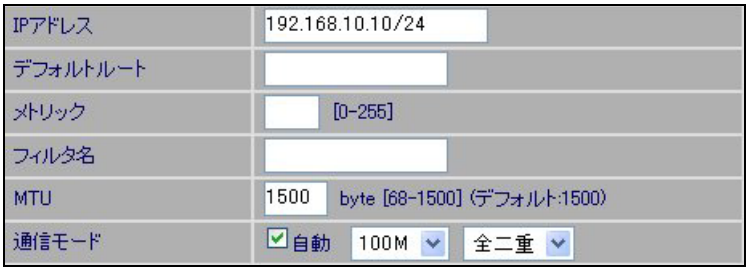
Ether0 で IP アドレスに「192.168.20.10/24」を設定します。

※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。



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。



設定後は以下のように表示されます。

<<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>

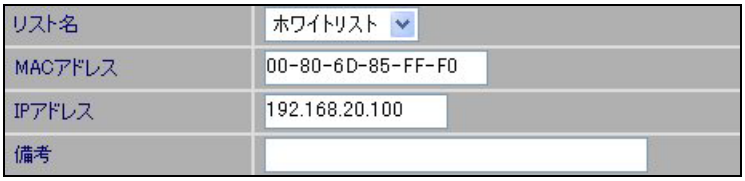
［端末リスト］

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。



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。

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。

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。

ホワイトリスト登録後は、以下のように表示されます。

[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。

[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。

《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>>

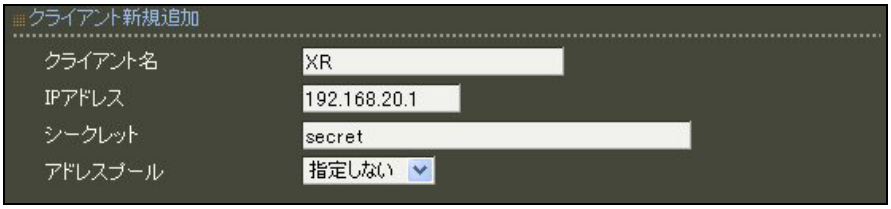
<サーバ>

［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。

<プロファイル>

[ユーザ基本情報]

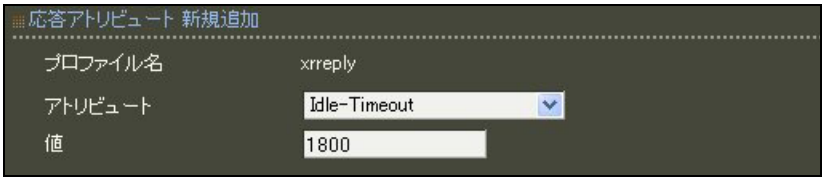
Web 認証用のユーザを作成するためにはユーザ基本情報プロファイルの作成が必要です。

認証方式として「PAP/CHAP」を選択します。

[応答アトリビュート]

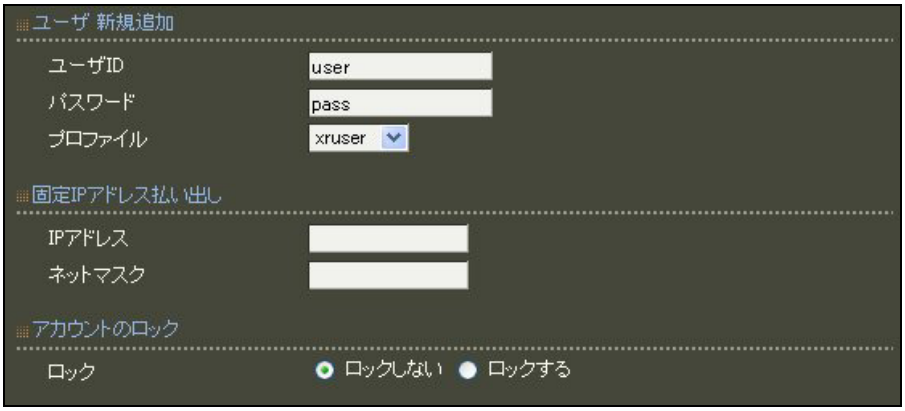
Web 認証用の応答アトリビュートプロファイルを作成します。

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。



[ユーザプロファイル]
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ァイルを作成します。

<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。
プロファイルはユーザプロファイルで作成した「xruser」を選択します。

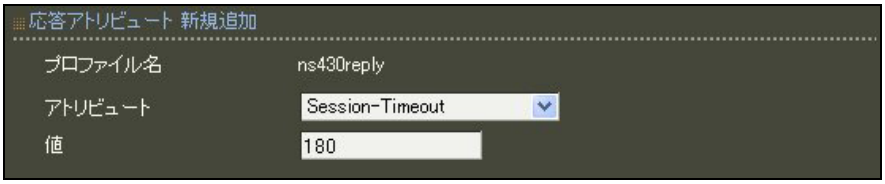


<プロファイル>
[ユーザ基本情報]
NS-430 用のユーザを作成するためにはユーザ基本情報プロファイルの作成が必要です。
認証方式として「PAP/CHAP」を選択します。

[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。



[ユーザプロファイル]

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 用のユーザプロファイルを作成します。

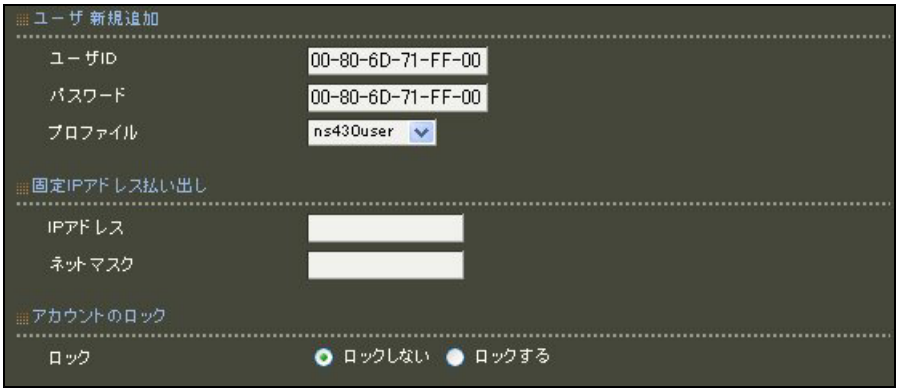
<ユーザ>

[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。

プロファイルはユーザプロファイルで作成した「ns430user」を選択します。



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。

<<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。

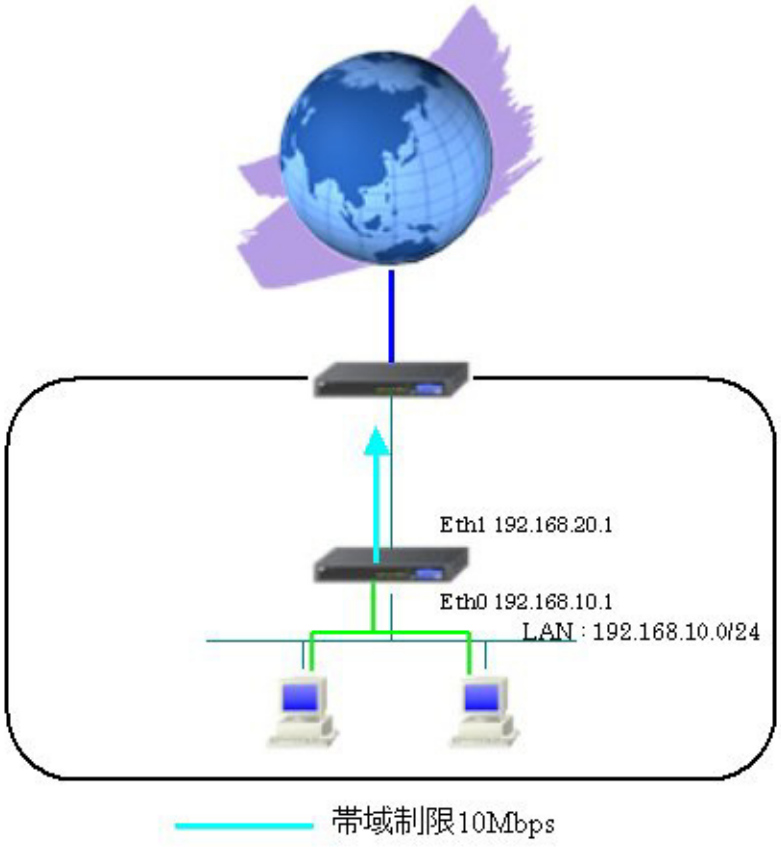
10. QoS 設定

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

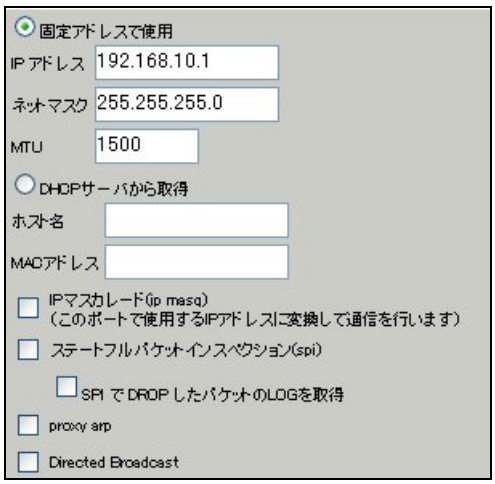


10-1-2. 設定例

<<インタフェース設定>>

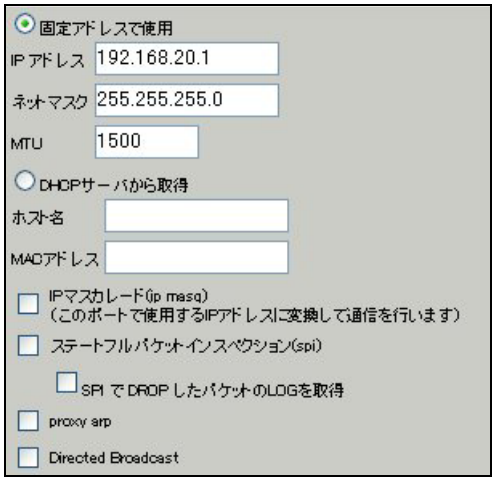
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



[Ethernet1 の設定]

IP アドレスに「192.168.20.1」を設定します。



<<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バケツにトークンをある一定の速度（トークン速度）で収納していきます。このトークン１個ずつがパケットを１個ずつつつかみ、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)

Interface名	eth1
Queueing Discipline	tbf
pfifo queue limit (pfifo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。

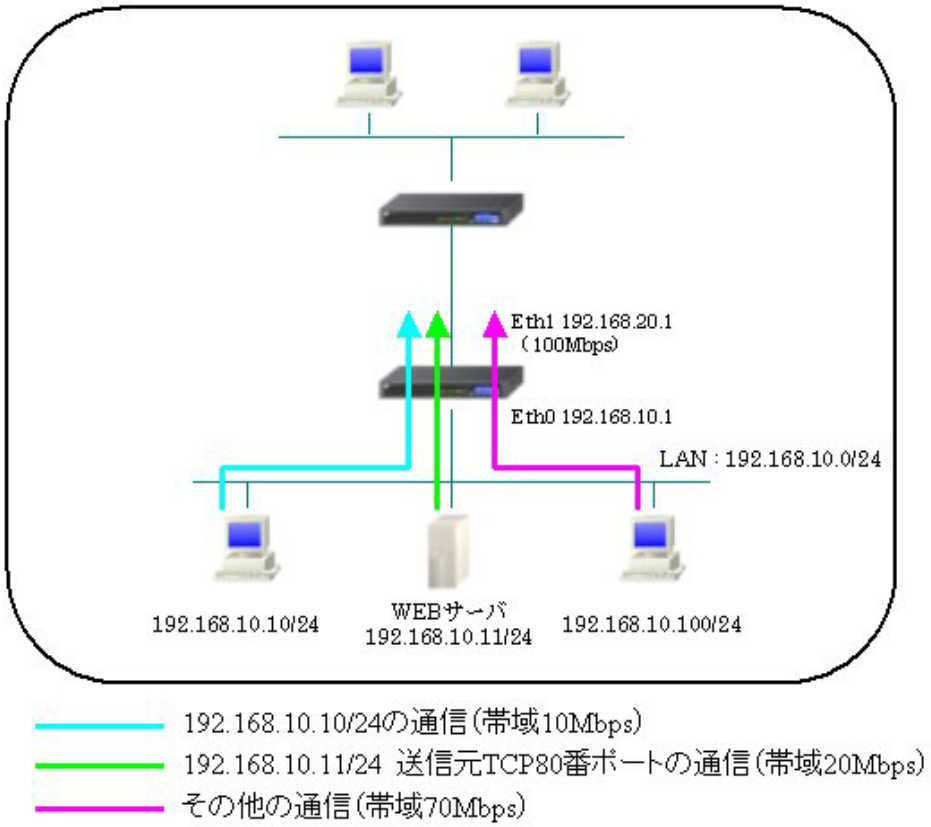
QoS簡易設定 QoS詳細設定	◉有効 ○無効

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

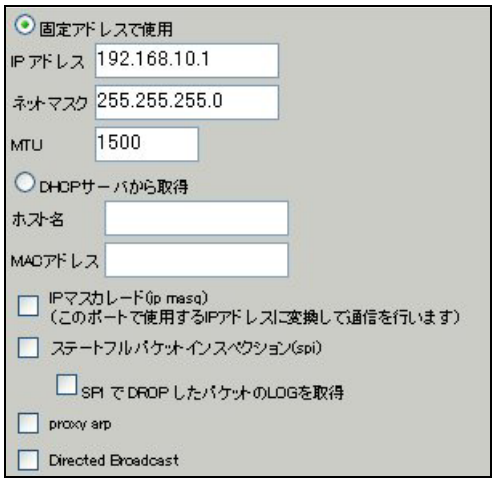
本設定例の制御条件は以下のようになります。

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>>

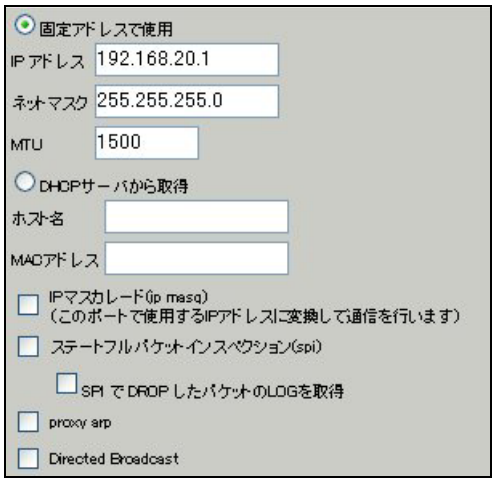
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



[Ethernet1 の設定]

IP アドレスに「192.168.20.1」を設定します。



<<QoS 設定>>

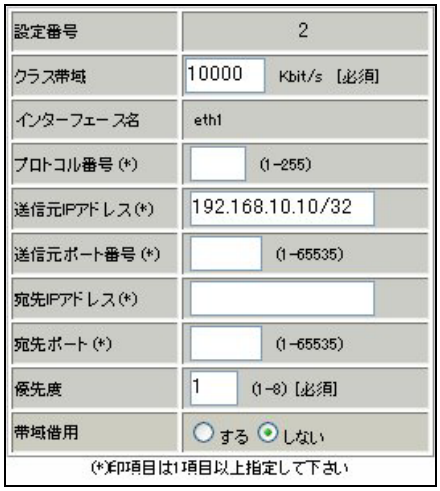
<QoS 簡易設定>

[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。

[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。



[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

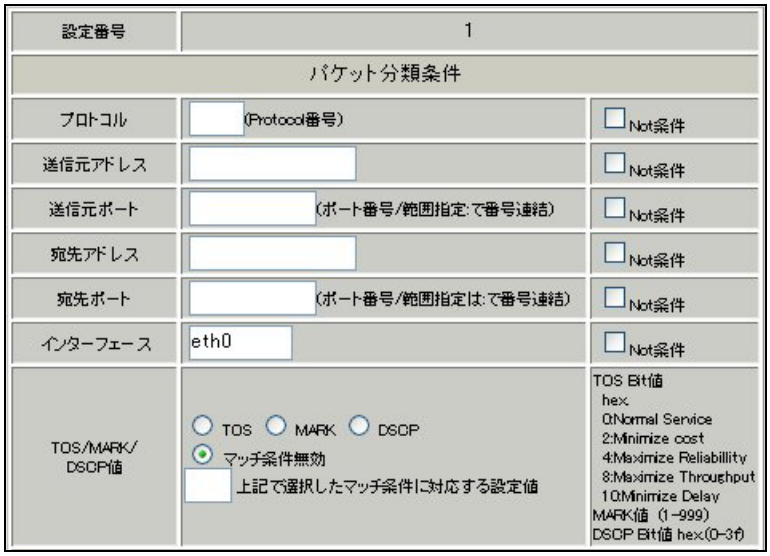
<QoS 詳細設定>

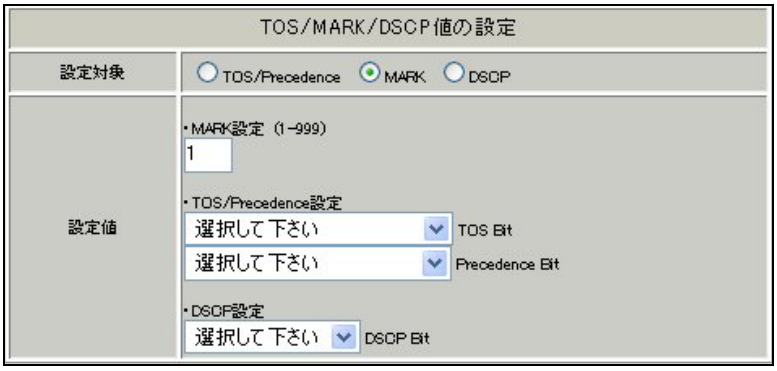
[パケット分類設定]

[パケット入力時の設定]

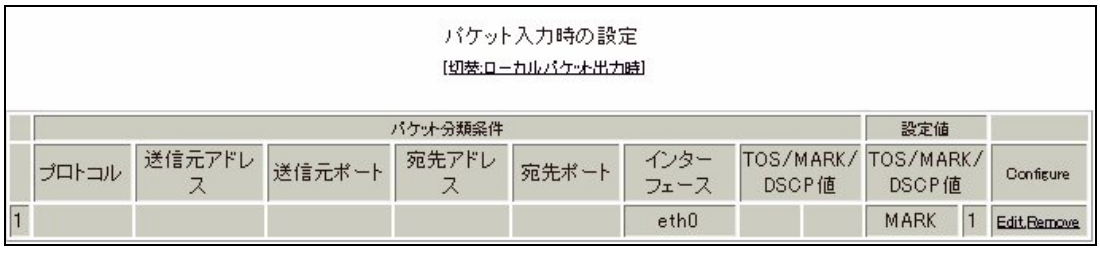
[No. 1]

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。





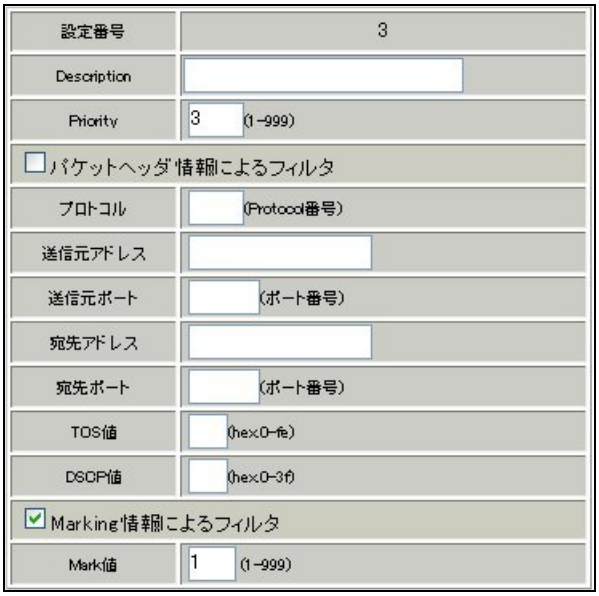
設定後は以下のように表示されます。



[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	100000Kbit/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バケツにトークンをある一定の速度（トークン速度）で収納していきます。このトークン１個ずつがパケットを１個ずつつかみ、トークン速度を超えない範囲でパケットを送信していきます。(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
pfifo limit (PFIFO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 queuing可能なbyte数)	byte

[No.2]

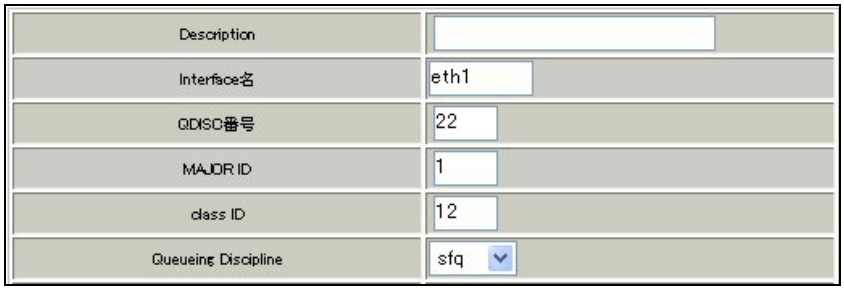
ID「11」のクラスで QDISC 番号を「21」とし、キューイング方式として「tbf」を選択し、制限 Rate「20000 Kbit/s」(20Mbps), Buffer Size「40k byte」を設定しています。

Description	
Interface名	eth1
QDISC番号	21
MAJOR ID	1
class ID	11
Queueing Discipline	tbf
pfifo limit (PFIFO選択時有効)	
TBF 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.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。



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

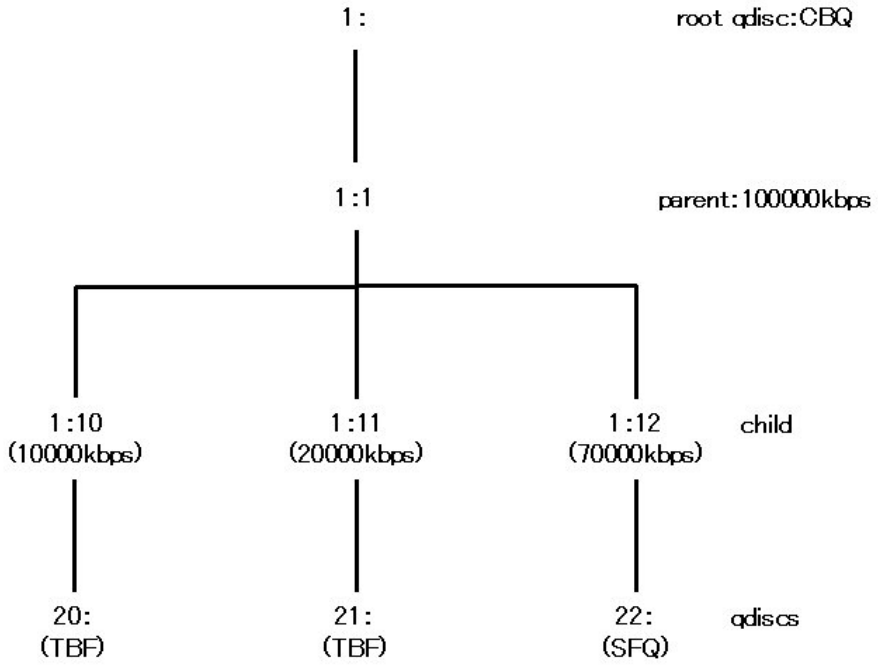
【QoS 機能】

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。

10-2-3. 設定例補足（クラス階層図）

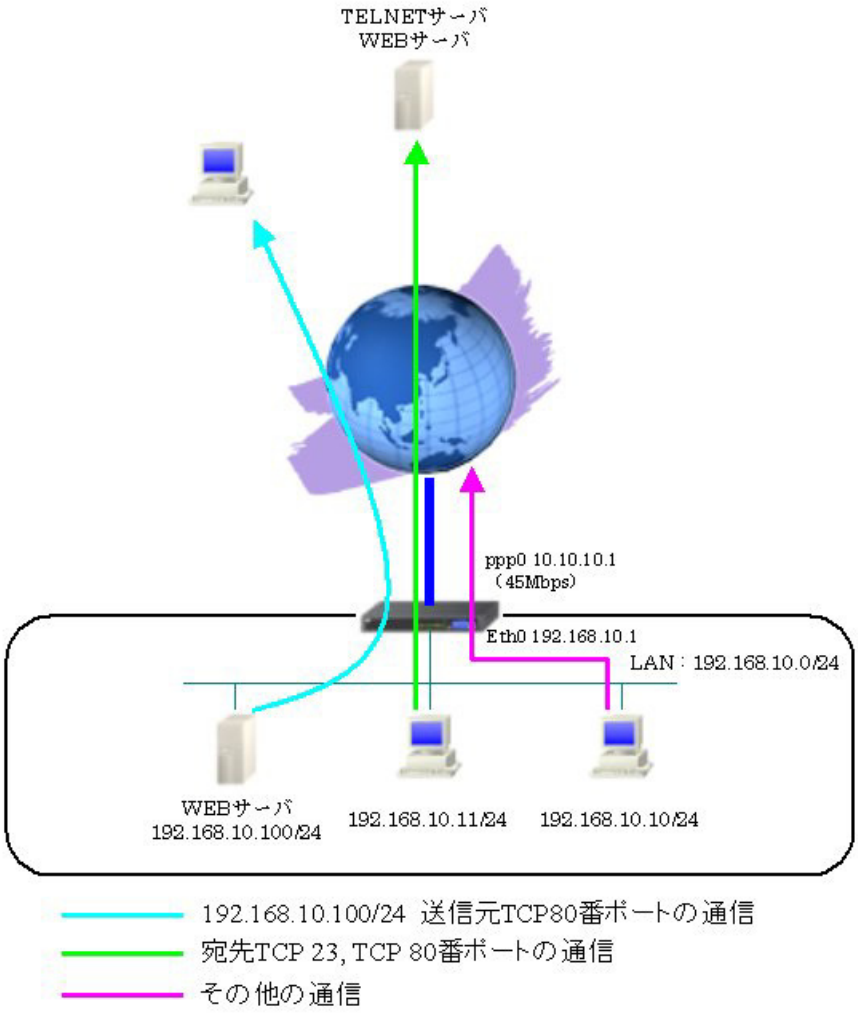
本設定例は以下のようなクラス階層になっています。



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

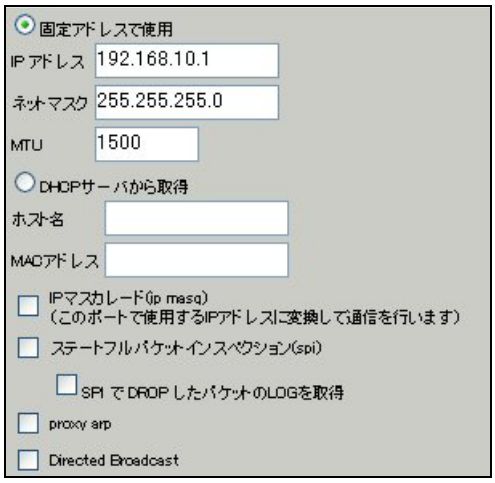
本設定例の制御条件は以下のようになります。

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]

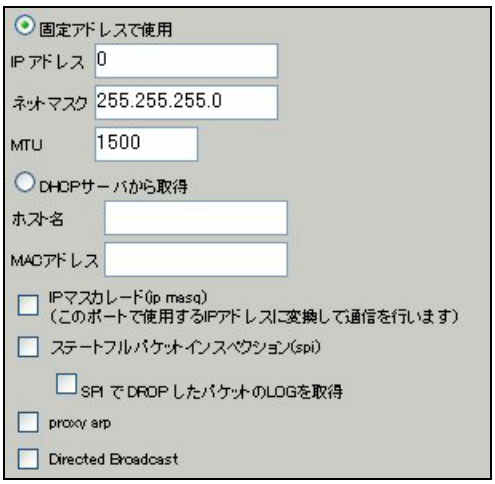
IP アドレスに「192.168.10.1」を設定します。



[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	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			

<<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	(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) 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]

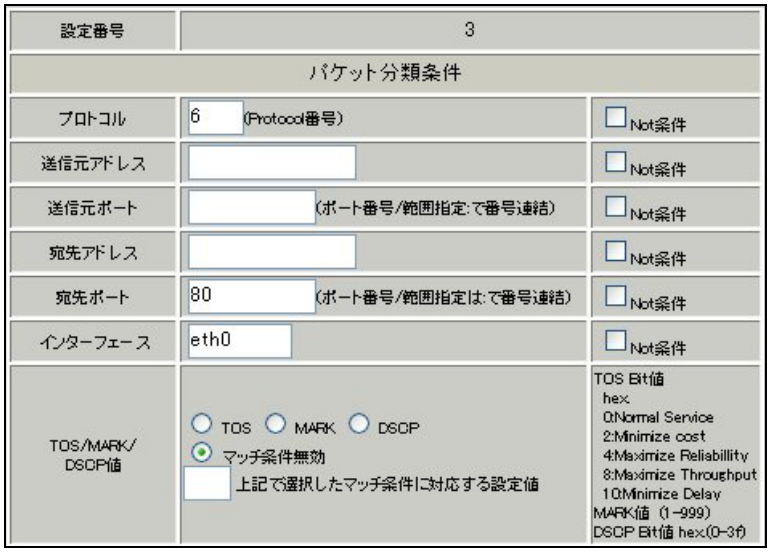
eth0 インタフェースで受信したプロトコル番号 6(TCP)宛先ポート 23 番のパケットに対しては「mark」「2」とする設定を行います。

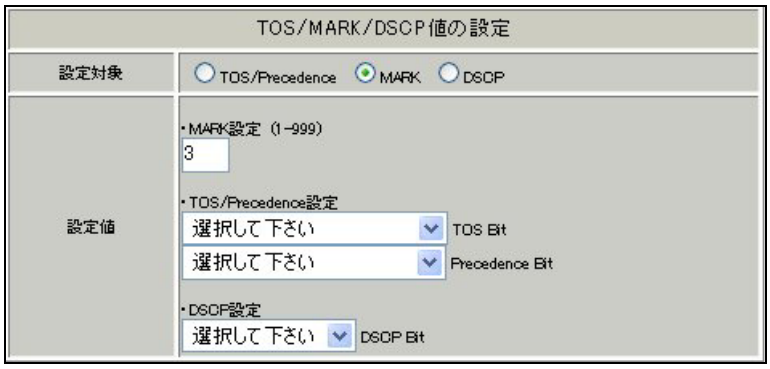
設定番号	2	
パケット分類条件		
プロトコル	6 (Protocol番号)	Not条件
送信元アドレス		Not条件
送信元ポート	(ポート番号/範囲指定:で番号連結)	Not条件
宛先アドレス		Not条件
宛先ポート	23 (ポート番号/範囲指定は:で番号連結)	Not条件
インターフェース	eth0	Not条件
TOS/MARK/DSCP値	TOS MARK DSCP マッチ条件無効 上記で選択したマッチ条件に対応する設定値	TOS Bit値 hex 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput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





[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	(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: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 Reliabillity 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	(hex0-fe)
DSCP値	(hex0-3f)
☑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	(hex0-fe)
DSCP値	(hex0-3f)
☑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バケツにトークンをある一定の速度（トークン速度）で収納していきます。このトークン１個ずつがパケットを１個ずつつかみ、トークン速度を超えない範囲でパケットを送信していきます。(帯域制限を行う場合に利用されます)

Description	qdisc20
Interface名	ppp0
QDISC番号	20
MAJOR ID	1
class ID	10
Queueing Discipline	tbf
pfifo limit (PFIFO選択時有効)	
TBF 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

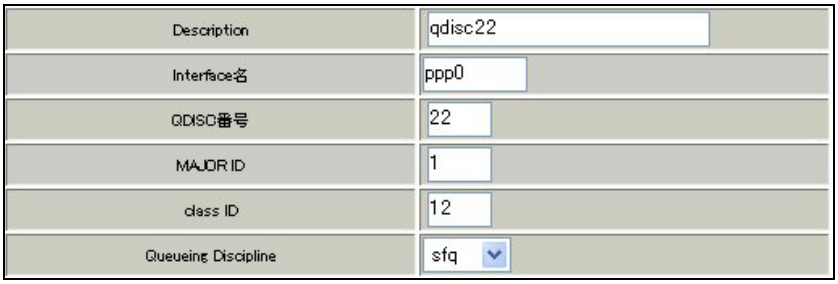
Description	qdisc21
Interface名	ppp0
QDISC番号	21
MAJOR ID	1
class ID	11
Queueing Discipline	pq

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。



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	pq	11	1
3	qdisc22	ppp0	22	sfq	12	1

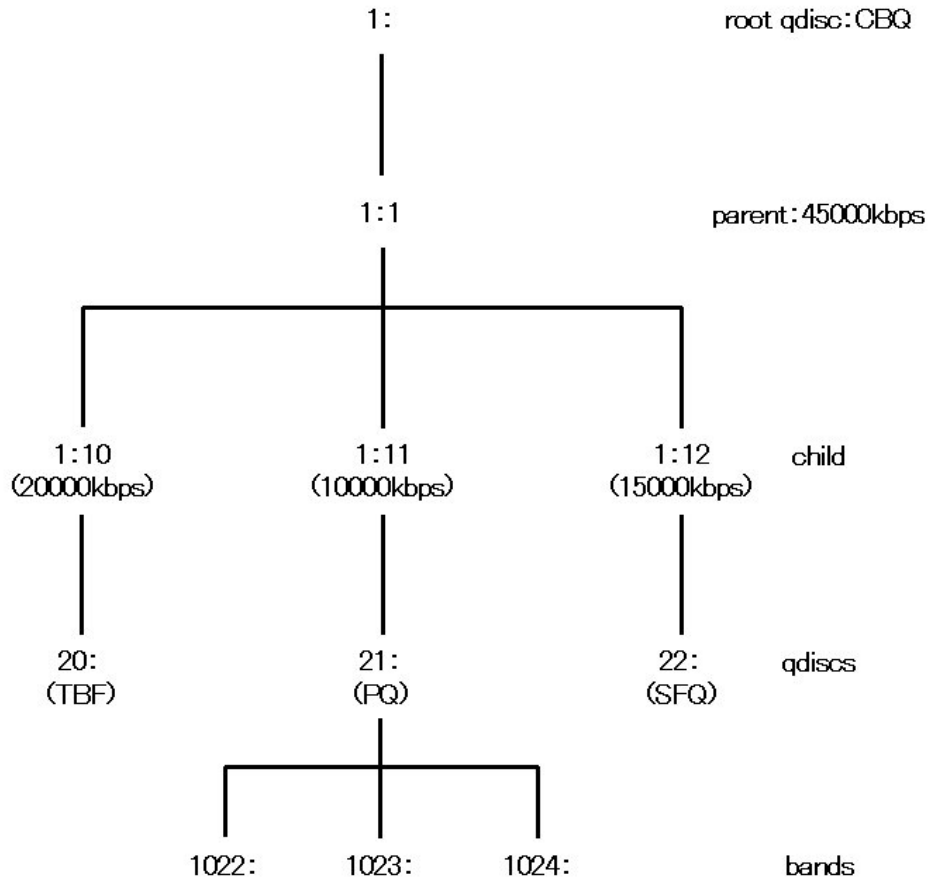
【QoS 機能】

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。

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。

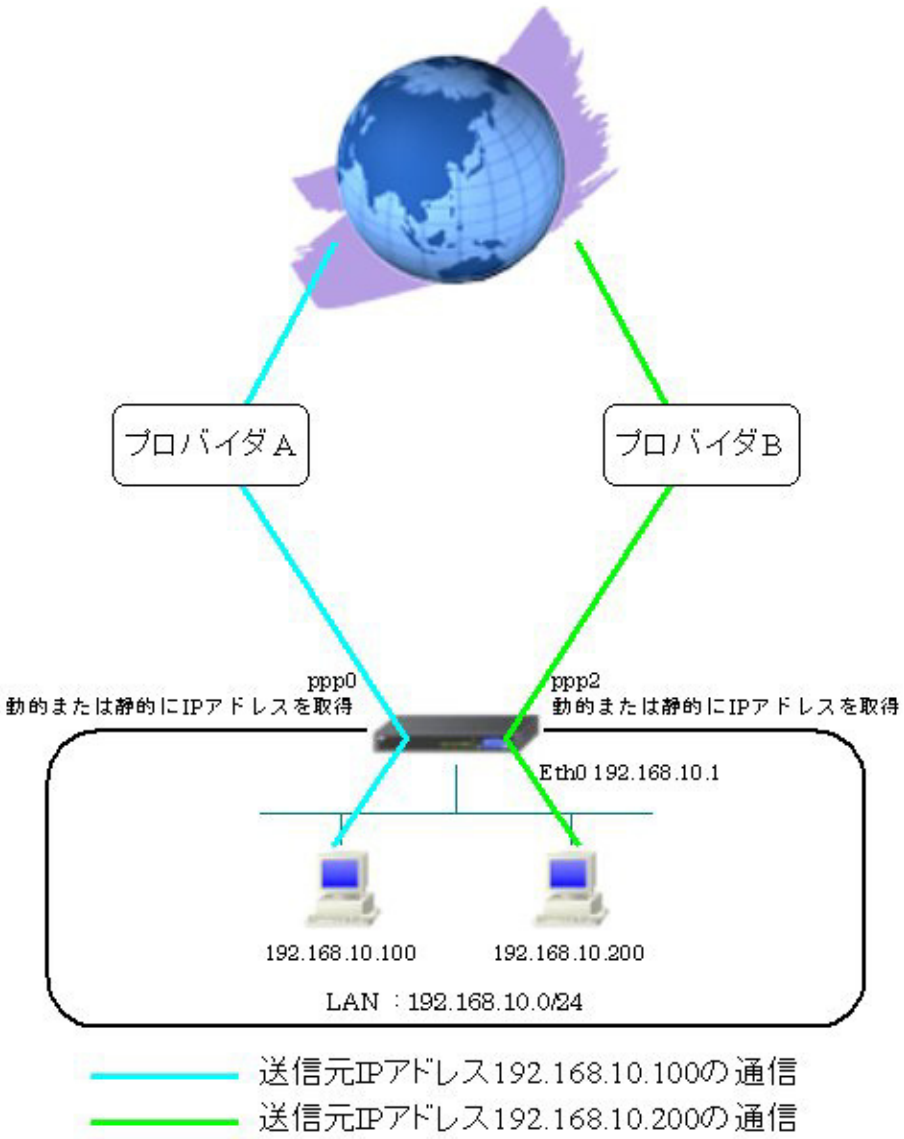


11. ソースルート設定

11-1. PPPoE でのソースルートの利用

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。これにより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。

11-1-1. 構成図



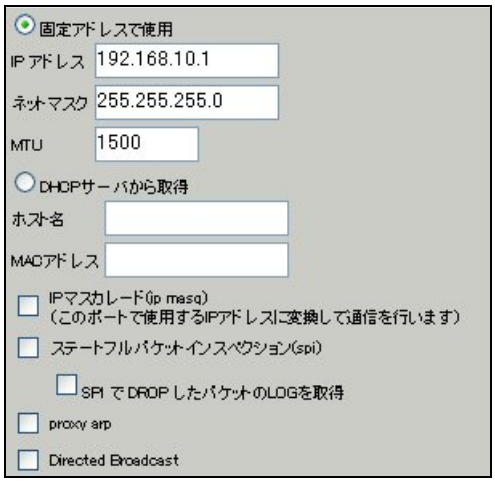
11-1-2. 設定例

送信元 IP アドレス「192.168.10.100/24」はプロバイダ A を、「192.168.10.200/24」はプロバイダ B を利用するように設定します。(ソースルートは「192.168.10.200/24」に対してのみ設定しています)

<<インタフェース設定>>

[Ethernet0 の設定]

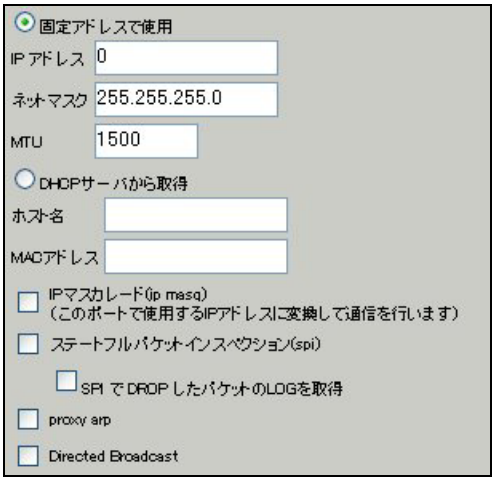
IP アドレスに「192.168.10.1」を設定します。



[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 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 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 マルチ接続 #2で接続しています

<<ソースルート設定>>

[ソースルートのテーブル設定]
ソースルートで利用する際の上位ルータの IP アドレスおよび DEVICE を設定します。
本設定では ppp2 インタフェースのみ設定しています。

テーブルNO	IP	DEVICE
1		ppp2

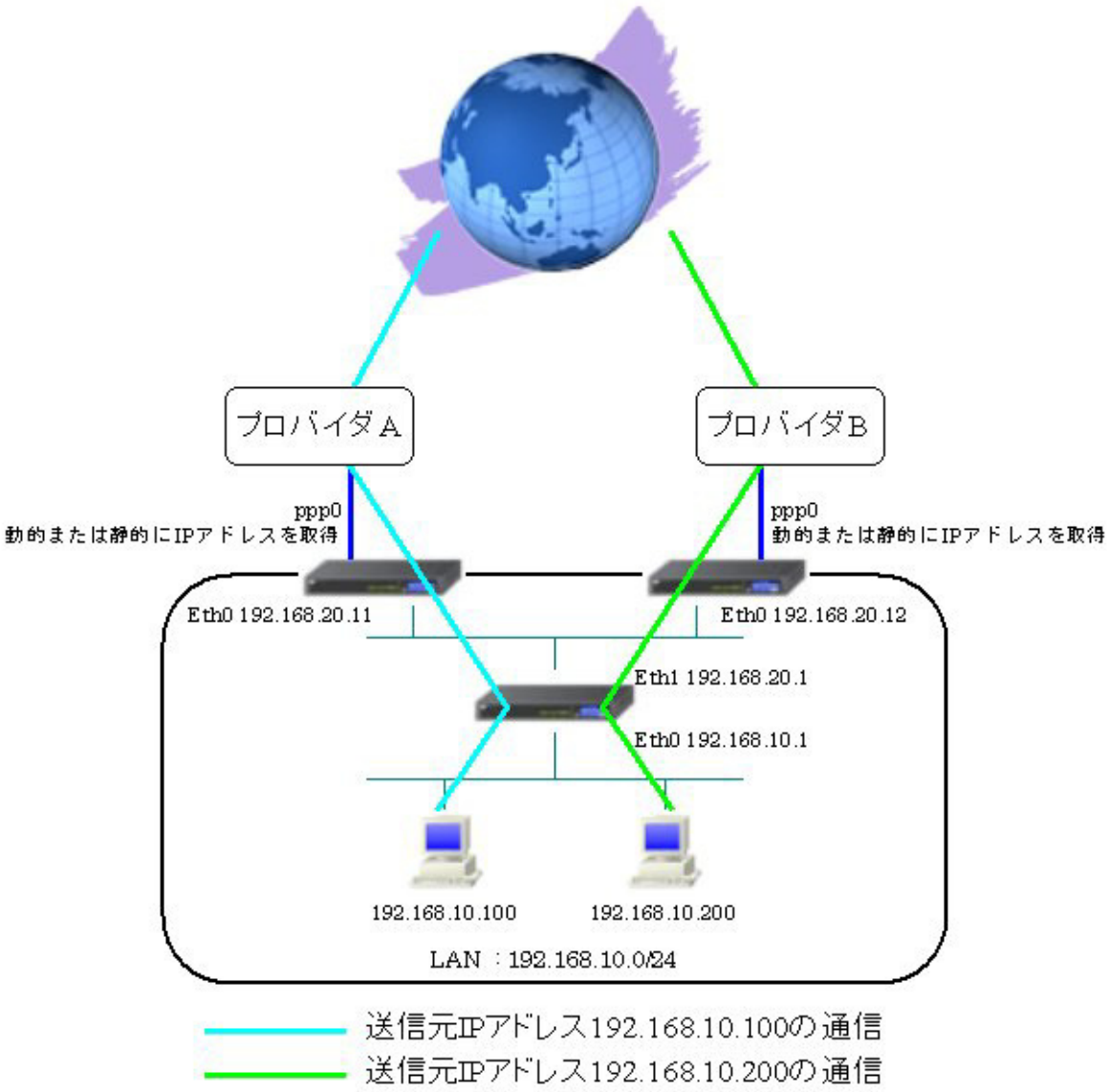
[ソースルートのルール設定]
送信元 IP アドレス，送信先 IP アドレス(限定しない場合は空欄)およびソースルートのテーブル設定で設定したテーブル No（本設定例では１）を設定します。

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	192.168.10.200		1

11-2. Ether でのソースルートの利用

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。
本設定例ではインターネット接続しているルータ配下の XR でソールルート機能を利用して負荷分散を行っています。

11-2-1. 構成図



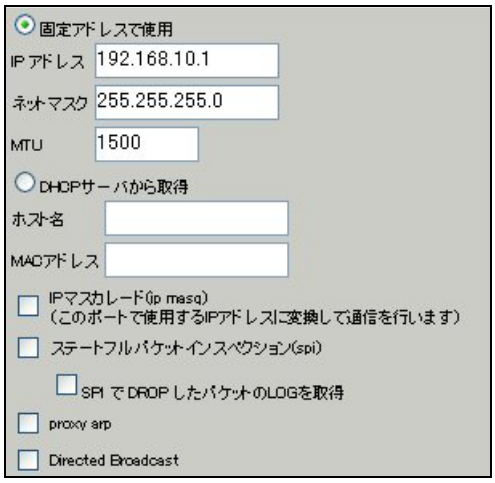
11-2-2. 設定例

送信元 IP アドレス「192.168.10.100/24」はプロバイダ A を、「192.168.10.200/24」はプロバイダ B を利用するように設定します。(ソースルートは「192.168.10.200/24」に対してのみ設定しています)
※本設定例ではソースルートを設定するルータのみ設定を記載しています。

<<インタフェース設定>>

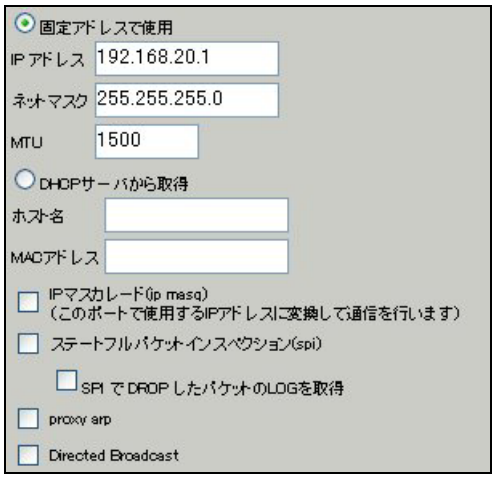
[Ethernet0 の設定]

IP アドレスに「192.168.10.1」を設定します。



[Ethernet1 の設定]

IP アドレスに「192.168.20.1」を設定します。



[その他の設定]

デフォルトゲートウェイを設定します。

<<ソースルート設定>>

[ソースルートのテーブル設定]

ソースルートで利用する際の上位ルータの IP アドレスおよび DEVICE を設定します。

本設定では IP アドレス「192.168.20.12」, DEVICE「eth1」を設定します。

テーブルNO	IP	DEVICE
1	192.168.20.12	eth1

[ソースルートのルール設定]

送信元 IP アドレス, 送信先 IP アドレス(限定しない場合は空欄)およびソースルートのテーブル設定で設定したテーブル No（本設定例では１）を設定します。

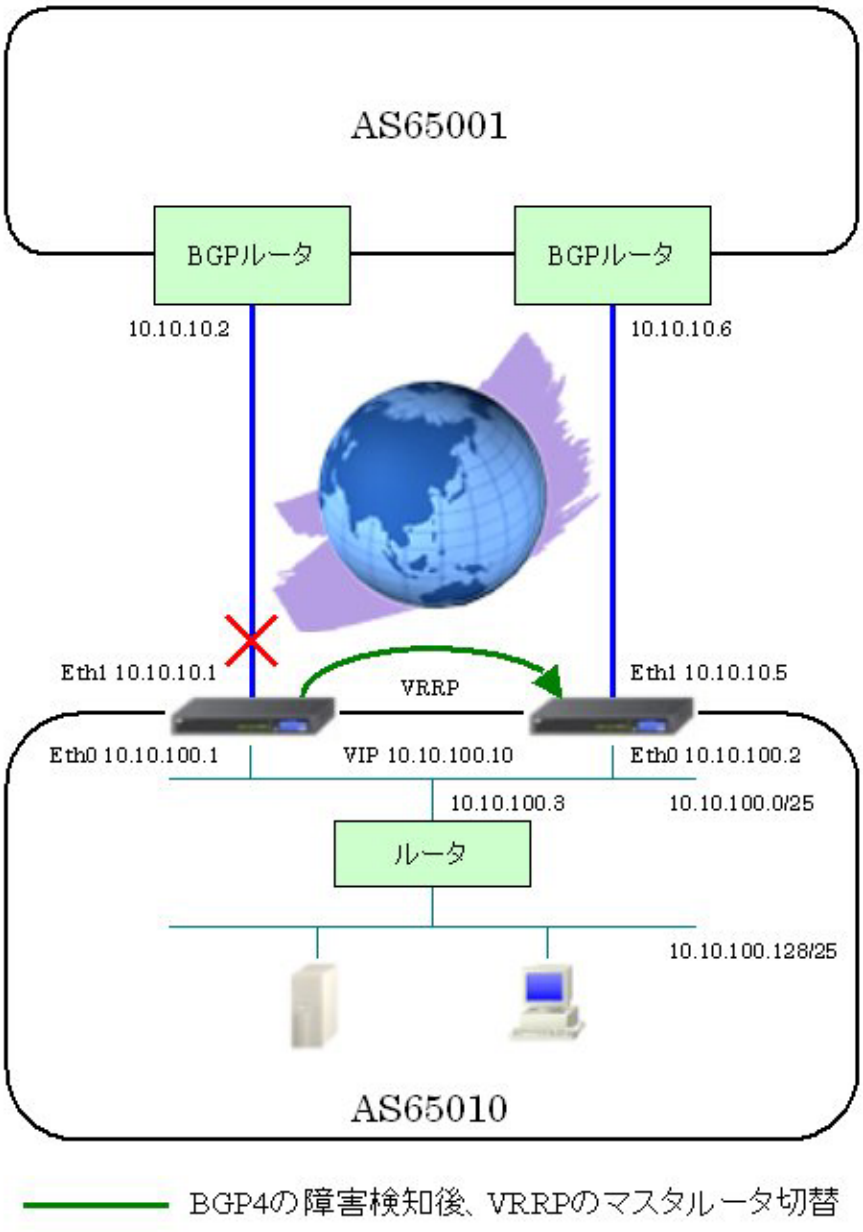
ルールNO	送信元ネットワークアドレス	送信先ネットワークアドレス	ソースルートのテーブルNO
1	192.168.10.200		1

12. BGP4 設定

12-1. ネットワークイベント機能 BGP4 切断監視の利用

BGP4 とネットワークイベント機能 BGP4 切断監視を組み合わせて利用することにより、BGP4 の neighbor state 状態を監視し、Neighbor state に変化があった場合にイベントを発生させることができます。本設定例では BGP4 で Neighbor state が Established へ変化した時に、VRRP の優先度を変更させています。

12-1-1. 構成図



12-1-2. 設定例

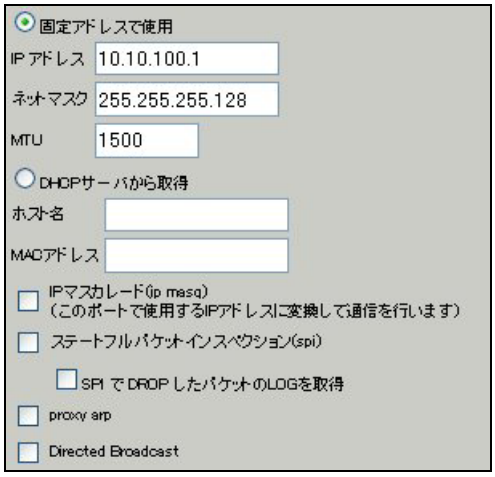
XR で AS65001 の BGP スピーカに対して BGP4 による接続ができるよう設定を行います。
またネットイベント機能の BGP4 切断監視を使用し、Neighbor state を監視します。状態変化が発生した際に VRRP の優先度を変更します。

《XR_A の設定》

<<インタフェース設定>>

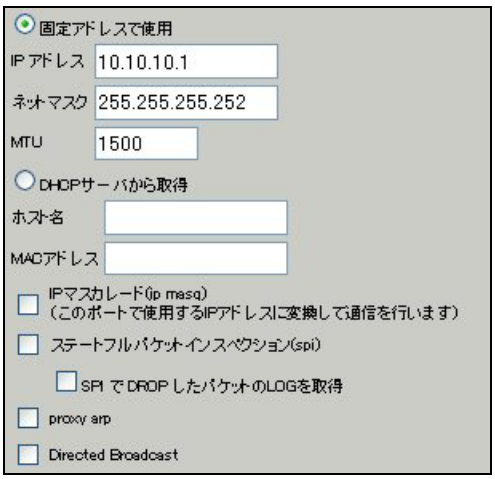
[Ethernet0 の設定]

IP アドレスに「10.10.100.1」,ネットマスクに「255.255.255.128」を設定します。



[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」を設定しています。



<<各種サービスの設定>>

【ダイナミックルーティング】-> <BGP4>

BGP4 設定前に BGP4 サービスを起動しておきます。

BGP4	○ 停止 ◉ 起動

<ダイナミックルーティング> -> <BGP4>

[BGP 機能設定]

AS 番号およびルータ ID を設定します。

AS Number	65010 (1-65535)
Router-ID	10.100.100.1 (ex192.168.0.1)
Scan Time	5 (5-60)
connected再配信	○ 有効 ◉ 無効 route-map設定
staticルート再配信	○ 有効 ◉ 無効 route-map設定
RIPルート再配信	○ 有効 ◉ 無効 route-map設定
OSPFルート再配信	○ 有効 ◉ 無効 route-map設定
Distance for routes external to the AS	20 (1-255)
Distance for routes internal to the AS	200 (1-255)
Distance for local routes	200 (1-255)
network import-check	○ 有効 ◉ 無効
always-compare-med	○ 有効 ◉ 無効
enforce-first-as	○ 有効 ◉ 無効
Bestpath AS-Path ignore	○ 有効 ◉ 無効
Bestpath med missing-as-worst	○ 有効 ◉ 無効
default local-pref	(0-4294967295)

[BGP4 Neighbor 設定]

対向の BGP スピーカの IP アドレス，AS 番号を設定します。

Neighbor Address	10.10.10.2 (ex192.168.1.1)
Remote AS Number	65001 (1-65535)
Keepalive interval	60 (0-65535)
Holdtime	180 (0,3-65535)
Next Connect Timer	120 (0-65535)
default-originate	○有効 ◉無効
nexthop-self	○有効 ◉無効
update-source	(interfaceを指定)
ebgp-multihop	(1-255)
soft-reconfiguration inbound	○有効 ◉無効
Apply map to incoming routes	(routemap名指定)
Apply map to outbound routes	(routemap名指定)
Filter incoming updates	(ACL名指定)
Filter outgoing updates	(ACL名指定)

[BGP4 Network 設定]

BGP で配信したいネットワークを設定します。

Speficy a network to announce via BGP	10.10.100.0/24 (ex192.168.0.0/24)
backdoor	○有効 ◉無効

【ダイナミックルーティング】-> <BGP4>

BGP4 を再起動します。

BGP4	○停止 ◉起動	動作中	再起動

<<各種サービスの設定>>

<VRRP サービス>

[VRRP の設定]

BGP の Neighbor state が Established 以外の時の VRRP 優先度を設定します。

No.	使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
1	Ether 0	使用しない	51	100	10.10.100.10	1	指定しない	

【VRRP サービス】

VRRP 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。

VRRPサービス	○停止 ◉起動

<<ネットワークイベント設定>>

[BGP4 切断監視設定]

監視する BGP スピーカの IP アドレスを指定します。

これがトリガとなります。

NO	enable	トリガー番号	BGP4 Neighbor Address
1	☑	1	10.10.10.2

[VRRP 優先度変更設定]

指定した BGP スピーカとの Neighbor state が Established になったときの VRRP の優先度を設定します。

NO	ルータID	優先度
1	51	200

[イベント実行テーブル設定]

実行イベントとして「VRRP 優先度」を選択します。

NO	実行イベント設定	オプション設定
1	VRRP優先度	1

[ネットワークイベント設定]

「トリガ番号」は、この例では「BGP4 切断監視設定」で指定した番号を、「実行イベントテーブル番号」は「イベント実行テーブル設定」を設定します。

NO	トリガー番号	実行イベントテーブル番号
1	1	1

[ネットワークイベントサービス設定]
この設定例では、「ネットワークイベント」と「BGP4 切断監視」を使用しますので、この二つを起動します。

<<スタティックルート設定>>

宛先 IP アドレスが「10.10.100.128/25」の時は、配下のルータへパケットを転送するように設定します。

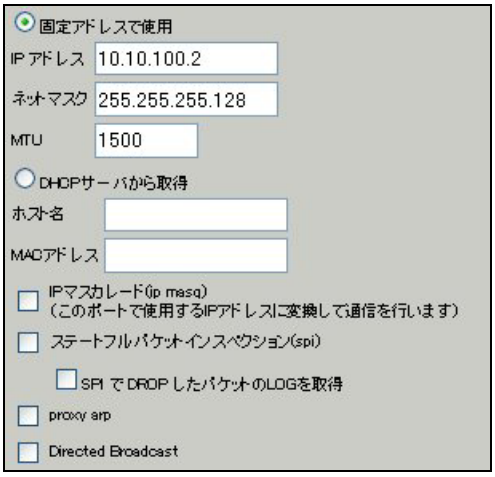
アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
10.10.100.128	255.255.255.128		10.10.100.3	1

《XR_B の設定》

<<インタフェース設定>>

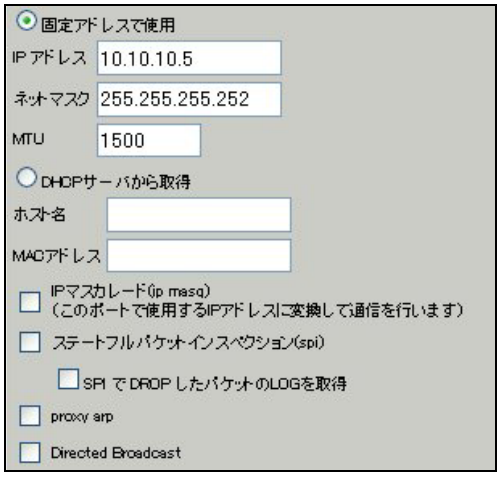
[Ethernet0 の設定]

IP アドレスに「10.10.100.2」,ネットマスクに「255.255.255.128」を設定します。



[Ethernet1 の設定]

IP アドレスに「10.10.10.5」,ネットマスクに「255.255.255.252」を設定しています。



<<各種サービスの設定>>

【ダイナミックルーティング】-> <BGP4>

BGP4 設定前に BGP4 サービスを起動しておきます。

BGP4	○ 停止 ◉ 起動

<ダイナミックルーティング> -> <BGP4>

[BGP 機能設定]

AS 番号およびルータ ID を設定します。

AS Number	65010 (1-65535)
Router-ID	10.100.100.2 (ex192.168.0.1)
Scan Time	5 (5-60)
connected再配信	○ 有効 ◉ 無効 route-map設定
staticルート再配信	○ 有効 ◉ 無効 route-map設定
RIPルート再配信	○ 有効 ◉ 無効 route-map設定
OSPFルート再配信	○ 有効 ◉ 無効 route-map設定
Distance far routes external to the AS	20 (1-255)
Distance far routes internal to the AS	200 (1-255)
Distance far local routes	200 (1-255)
network import-check	○ 有効 ◉ 無効
always-compare-med	○ 有効 ◉ 無効
enforce-first-as	○ 有効 ◉ 無効
Bestpath AS-Path ignore	○ 有効 ◉ 無効
Bestpath med missing-as-worst	○ 有効 ◉ 無効
default local-pref	(0-4294967295)

[BGP4 Neighbor 設定]

対向の BGP スピーカの IP アドレス，AS 番号を設定します。

Neighbor Address	10.10.10.6 (ex192.168.1.1)
Remote AS Number	65001 (1-65535)
Keepalive interval	60 (0-65535)
Holdtime	180 (0,3-65535)
Next Connect Timer	120 (0-65535)
default-originate	○有効 ◉無効
nexthop-self	○有効 ◉無効
update-source	(interfaceを指定)
ebgp-multihop	(1-255)
soft-reconfiguration inbound	○有効 ◉無効
Apply map to incoming routes	(routemap名指定)
Apply map to outbound routes	(routemap名指定)
Filter incoming updates	(ACL名指定)
Filter outgoing updates	(ACL名指定)

[BGP4 Network 設定]

BGP で配信したいネットワークを設定します。

Speficy a network to announce via BGP	10.10.100.0/24 (ex192.168.0.0/24)
backdoor	○有効 ◉無効

【ダイナミックルーティング】-> <BGP4>

BGP4 を再起動します。

BGP4	○停止 ◉起動	動作中	再起動

<<各種サービスの設定>>

<VRRP サービス>

[VRRP の設定]

XR_A の BGP Neighbor state が Established 以外の時に Master になるように VRRP 優先度を設定します。

使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
Ether 0	使用しない	51	150	10.10.100.10	1	指定しない	

【VRRP サービス】

VRRP 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。

VRRPサービス	○停止 ◉起動

<<スタティックルート設定>>

宛先 IP アドレスが「10.10.100.128/25」の時は、配下のルータへパケットを転送するように設定します。

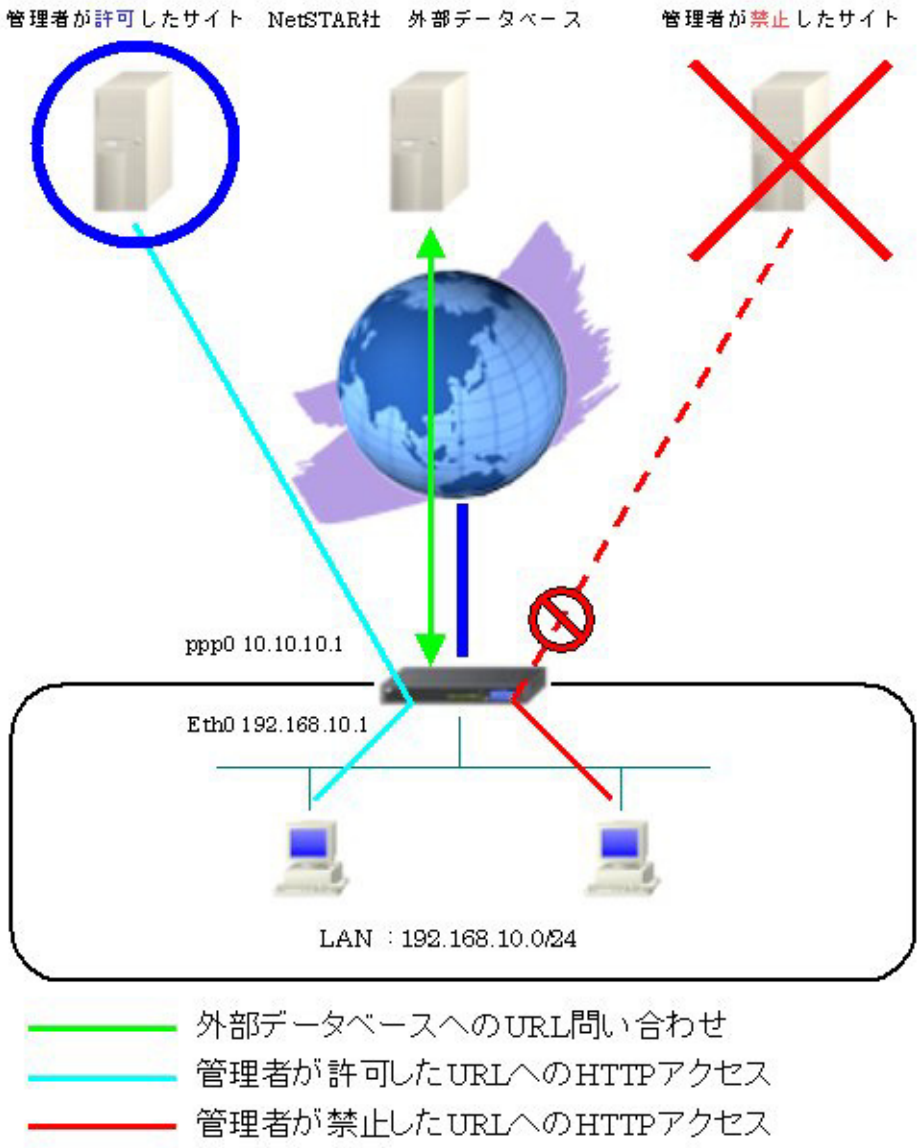
アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
10.10.100.128	255.255.255.128		10.10.100.3	1

13. URL フィルタ設定

13-1. URL フィルタの利用

URL フィルタ機能では、ユーザから外部への HTTP アクセスを制御することで、管理者がユーザにアクセスさせたくないサイトの HTTP を遮断し、ユーザにアクセスできなくさせることが可能です。
XR シリーズの URL フィルタ機能は、XR と NetSTAR 社の外部データベースが連携してユーザの HTTP アクセスを制御します。

13-1-1. 構成図



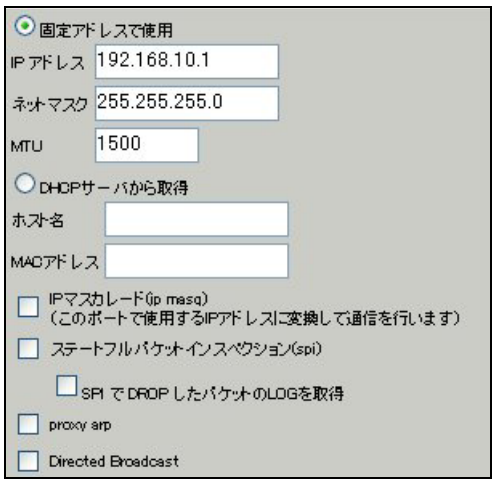
13-1-2. 設定例

XR で URL フィルタを行い、ユーザにアクセスさせたくないサイトの HTTP アクセスを遮断します。

<<インタフェース設定>>

[Ethernet0 の設定]

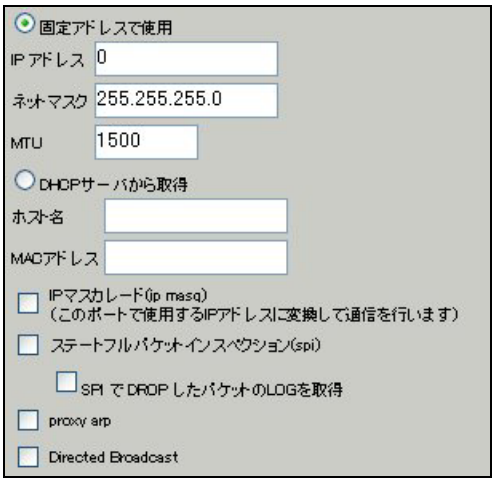
IP アドレスに「192.168.10.1」を設定します。



[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 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 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

【DNS キャッシュ】

URL フィルタのライセンスサーバに対して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。

DNSキャッシュ	○停止 ◉起動

<<URL フィルタ設定>>

[基本設定]

URL フィルタ設定機能の使用と、フィルタリングをおこなうインタフェースを設定します。

本設定では URL フィルタを行うインタフェースとして Ethernet0 を設定しています。

[プレフィルタ設定]

NetSTAR 社の外部データベースとの連携を必要とせず、XR 単体で行うフィルタリングルールを設定します。

[ホワイトリスト/ブラックリスト設定]

外部データベースへの問い合わせとは別に、ユーザが URL を透過/遮断させるリストを、本装置内部に登録することができます。

本設定例では文字列として「centurysys」を登録し、この文字列を含む URL へのアクセスは禁止しています。

[URL フィルタポリシー設定]

直接 IP アドレスを指定した URL へのアクセスを行う場合に、アクセスを「許可」(透過) するか、「遮断」(遮断) するかを選択します。

本設定例では直接 IP アドレスを指定した URL へのアクセスを許可しています。

［ルールセット設定］

ユーザグループに設定されたユーザからの HTTP アクセスに対して、HTTP リクエストのフィルタリングをおこないます。

本設定例ではフィルタリングを適用する IP アドレスとして「any」を設定しています。

URL カテゴリとして「企業」を選択しています。

URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

［ログ設定］

URL フィルタの遮断ログおよびシステムログを取得するように設定しています。

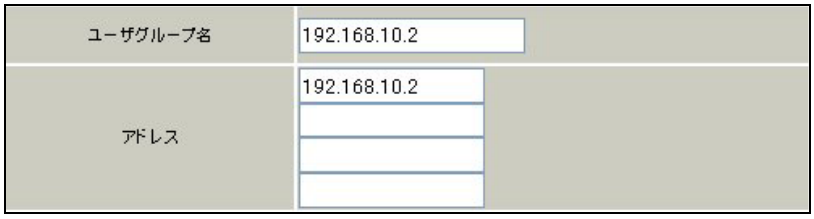
※ログを取得する場合は、SYSLOG サービスは必ず「起動」してください。

13-1-3. 設定例補足 1 （ルールセット設定における IP アドレス範囲指定）

URL フィルタ機能では IP アドレス毎に適用する URL カテゴリを変えることも可能です。下記例では以下の条件でルールセット設定を行います。

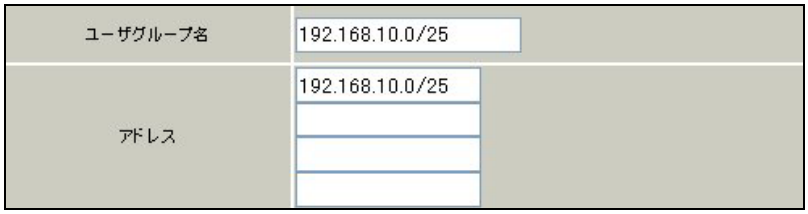
・「192.168.10.2」の端末では URL カテゴリを「ルールを選択しない」とする。
・「192.168.10.0/25」の範囲の端末では URL カテゴリを「大学」とする。
・「192.168.10.128/26」の範囲の端末では URL カテゴリを「企業」とする。
・「any」で URL カテゴリを「全選択」とする。
※マッチングは、画面に表示されている順におこなわれますので、設定順序にはご注意下さい。

[ルールセット設定]
ユーザグループに設定されたユーザからの HTTP アクセスに対して、HTTP リクエストのフィルタリングをおこないます。
一番目のルールとして IP アドレス「192.168.10.2」を設定しています。



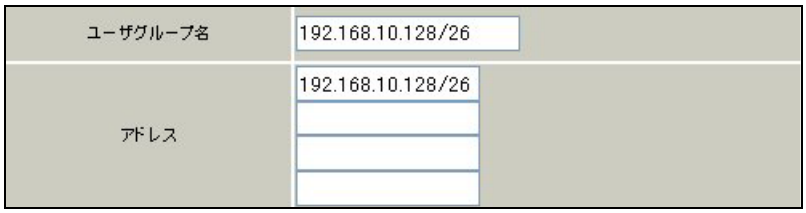
URL カテゴリとして「ルールを選択しない」を選択しています。
URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

二番目のルールとして IP アドレス「192.168.10.0/25」を設定しています。

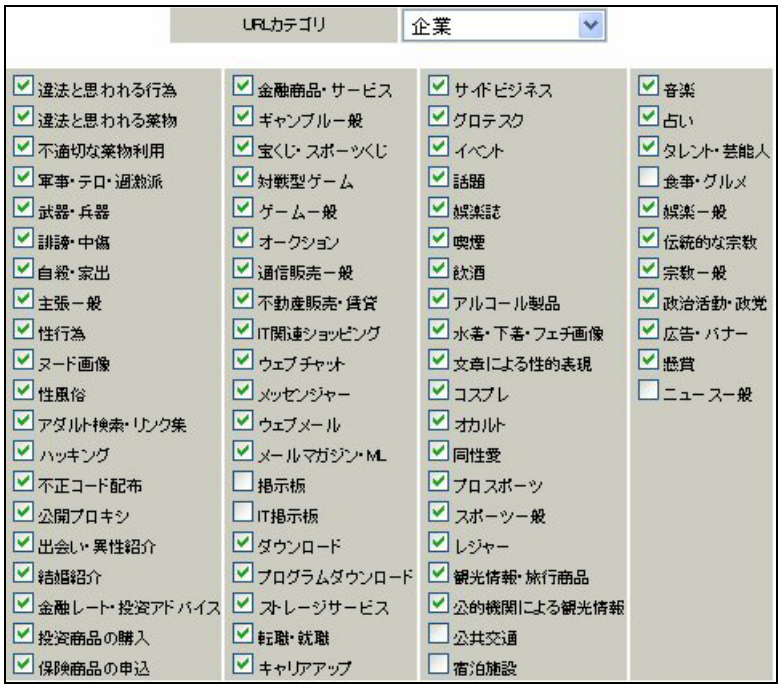


URL カテゴリとして「大学」を選択しています。
URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

三番目のルールとして IP アドレス「192.168.10.128/26」を設定しています。



URL カテゴリとして「企業」を選択しています。
URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。



最後のルールとして IP アドレスとして「any」を設定しています。

URL カテゴリとして「全選択」を選択しています。
URL カテゴリの設定では、チェックを入れたカテゴリの URL が「遮断」されます。

ルールセット設定設定後は、以下のようになります。

No.	ユーザグループ	URLカテゴリ
1	192.168.10.2 設定	設定
2	192.168.10.0/25 設定	設定
3	192.168.10.128/26 設定	設定
4	other 設定	設定

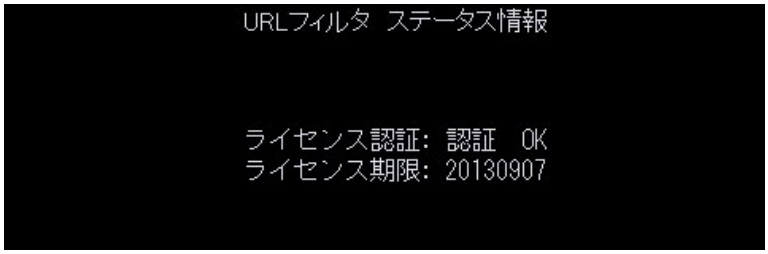
13-1-4. 設定例補足２（ライセンス認証とフィルタによる遮断）

URL フィルタ機能では NetSTAR 社の外部データベースを利用する場合、NetSTAR 社のライセンスサーバに対し、ライセンス認証有効の可否について問い合わせを行います。

なおライセンス認証は、以下のタイミングで行われます。

・ユーザが URL フィルタの使用を開始した場合
・URL フィルタの使用を開始してから一定時間(48 時間)経過した場合
・本装置を再起動した場合

ライセンス認証に成功した場合は、以下のような画面が表示されます。



URL フィルタで遮断対象の URL へアクセスした場合は、以下の画面をユーザの Web ブラウザに表示すると共に http アクセスを遮断します。

13-1-5. 設定例補足３（URL フィルタのログ）

URL フィルタ機能では http アクセスを透過・遮断した際のログを取得することも可能です。
以下はログ表示例です。

・プレフィルタ設定
www.centurysys.co.jp への http アクセスを透過した場合
urlfilterd: [prefilter][accept]src ip[192.168.10.100],url[www.centurysys.co.jp/].

www.centurysys.co.jp への http アクセスを遮断した場合
urlfilterd: [prefilter][drop]src ip[192.168.10.100],url[www.centurysys.co.jp/].

・URL カテゴリ設定（外部データベース）
www.centurysys.co.jp への http アクセスを透過した場合
urlfilterd: [url category][accept]src ip[192.168.10.100],url[www.centurysys.co.jp/].

www.centurysys.co.jp への http アクセスを遮断した場合
urlfilterd: [url category][drop]src ip[192.168.10.100],url[www.centurysys.co.jp/].

14. サポートデスクへのお問い合わせ

14-1. 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）

14-2. 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

Ver1.2.0

2008 年 10 月

発行　センチュリー・システムズ株式会社