

インターネット VPN 対応ルータ

*Futurenet* **XR** シリーズ

インターネット VPN 設定例集

L2TPv3 フィルタ編

Ver.1.0.0

---

## 目次

<b>1. L2TPv3 フィルタの利用例 1</b> .....	<b>4</b>
1-1. 構成例 .....	4
1-2. 要件 .....	5
1-3. 設定例 .....	9
センタールータ (XR_A) .....	9
拠点ルータ (XR_B) .....	13
<b>2. L2TPv3 フィルタの利用例 2</b> .....	<b>22</b>
2-1. 構成例 .....	22
2-2. 要件 .....	23
2-3. 設定例 .....	27
センタールータ (XR_A) .....	27
拠点 1 ルータ (XR_B) .....	37
拠点 2 ルータ (XR_C) .....	41
<b>3. L2TPv3 フィルタの利用例 3</b> .....	<b>45</b>
3-1. 構成例 .....	45
3-2. 要件 .....	46
3-3. 設定例 .....	52
センタールータ (XR_A) .....	52
拠点 1 ルータ (XR_B) .....	66
拠点 2 ルータ (XR_C) .....	70

## はじめに

本書は XR シリーズを利用した設定例集になります。

本書を利用する際は、各製品のユーザーズガイドおよび L2TPv3 設定例集も合わせてご利用下さい。

### 注意事項

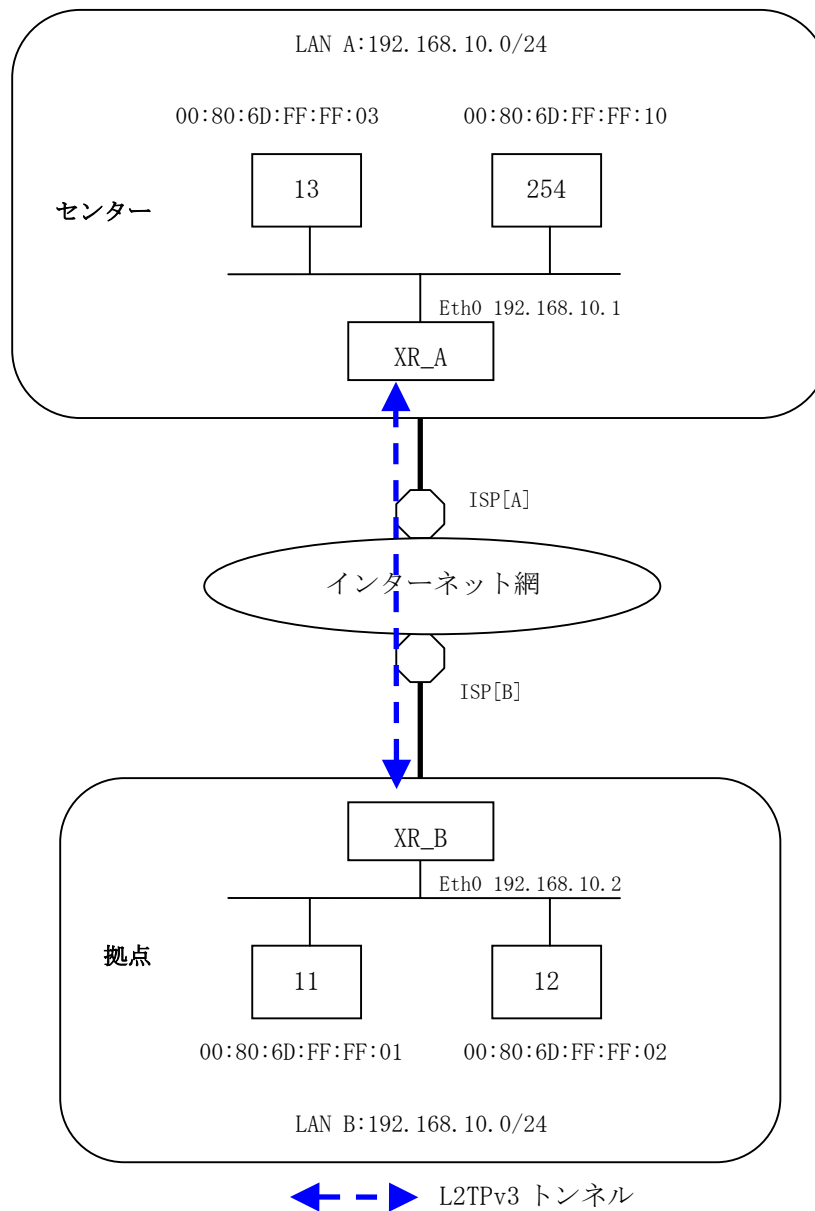
- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書を利用し運用した結果発生した問題に関しましては、責任を負いかねますのでご了承下さい。
- 本書で解説している L2TPv3 フィルタ機能は beta 版のため、正式版では一部機能・設定に違いがある場合があります。ご了承下さい。

## 1. L2TPv3 フィルタの利用例 1

この設定例は、L2TPv3 を利用して拠点間接続を実現している環境で、指定した端末以外のアクセスを一部制限する設定例です。

この例では、XR\_B で送信元 MAC アドレスが許可されている端末 11 からの ARP、IP トラフィックおよびそれ以外の端末からの宛先 端末 254 の ARP、および宛先 端末 254 TCP ポート 80 の IP トラフィックは許可し、それ以外のトラフィックは全て破棄しています。

### 1-1. 構成例



## 1-2. 要件

➤ インタフェースおよび PPP/PPPoE

- インターネットには PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- IP マスカレード、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。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点)
LAN 側インタフェース	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.10.2
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	10.10.20.1
PPPoE ユーザ名	test1@centurysys	test2@centurysys
PPPoE パスワード	test1pass	test2pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続

➤ L2TPv3

- XR\_A(センター)では、XR\_B(拠点)と L2TPv3 で接続するための設定しています。
- XR\_B(拠点)では、XR\_A(センター)と L2TPv3 で接続するための設定しています。
- PPPoE 接続で利用しているため、Bind Interface として「ppp0」を指定しています。

主な L2TPv3 機能設定のパラメータ

	XR_A(センター)	XR_B(拠点)
Local hostname	XR_A	XR_B
Local Router-ID	172.20.10.1	172.20.20.1
MAC Address 学習機能	有効	有効

主な L2TPv3 Tunnel 設定のパラメータ

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
Peer IP	10.10.20.1	10.10.10.1
Remote Hostname	XR_B	XR_A
Remote RouterID	172.20.20.1	172.20.10.1
Bind Interface	ppp0	ppp0

主な L2TPv3 Xconnect Interface 設定のパラメータ

	XR_A(センター)	XR_B(拠点)
対向拠点	XR_B(拠点)	XR_A(センター)
Peer ID	172.20.20.1	172.20.10.1
Interface	eth0	eth0
Remote End ID	1	1
Reschedule Interval	30	45
Auto	有効	有効

➤ L2TPv3 フィルタ

- XR\_B の Xconnect Interface IN Filter でフィルタリングを行います。
- 送信元 MAC アドレスで許可されている端末 11 からの ARP, IP トラフィックは許可。
- それ以外の端末からの宛先 254 の ARP, および宛先 254 TCP ポート 80 の IP トラフィックは許可。
- それ以外のトラフィックは全て破棄。

主な L2TPv3 フィルタ Root Filter 設定のパラメータ

	XR_B(拠点)
Root Filter Name	root-filter1
Default Policy	deny

主な L2TPv3 フィルタ Layer2 ACL 設定のパラメータ

	XR_B(拠点)		
Layer2 ACL Name	l2-filter1	l2-filter2	l2-filter3
Policy	deny	deny	deny
Source MAC		00:80:6D:FF:FF:01	
Destination MAC			
Protocol/Length	ARP	IPv4	IPv4

主な L2TPv3 フィルタ IPv4 Extend ACL 設定のパラメータ

	XR_B(拠点)	
Extend ACL Name	ip-filter1	ip-filter2
Policy	permit	permit
Source IP	192.168.10.11	
Destination IP		192.168.10.254
IP Protocol		TCP
Destination Port		80

主な L2TPv3 フィルタ ARP Extend ACL 設定のパラメータ

	XR_B(拠点)	
Extend ACL Name	arp-filter1	arp-filter2
Policy	permit	permit
Source MAC	00:80:6D:FF:FF:01	
Destination MAC		
Source IP		
Destination IP		192.168.10.254

ACL は以下のようなツリー構造になっています。

```
root-filter1
  + 12-filter2
    deny    00:80:6d:ff:ff:01 any          IPv4
    + ip-filter1
      permit
  + 12-filter3
    deny    any          any          IPv4
    + ip-filter2
      permit
  + 12-filter1
    deny    any          any          ARP
    + arp-filter1
      permit
    + arp-filter2
      permit
  + default deny
```

➤ その他

- フィルタ設定[入力フィルタ]で、WAN 側インタフェースで受信した「L2TP」パケットを許可する設定にしています。



### 1-3. 設定例

#### センタールータ (XR\_A)

##### ポイント

XR\_B(拠点)と L2TPv3 接続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]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IP アドレスの設定を変更した場合、即設定が反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test1@centurysys
パスワード	test1pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

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

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時 PADTを強制送 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時 PADTを強制送
-------------------------	---

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。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート	LOG
ppp0	パケット受信時	許可	l2tp					<input type="checkbox"/>

L2TP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<L2TPv3>

[L2TPv3 機能設定]

Local hostname	XR_A
Local Router-ID	172.20.10.1
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
FMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_A(センター)の Local hostname, Local Router-ID を設定します。MAC アドレス学習機能を使用する場合は「有効」に設定してください。(デフォルトは有効です)

[L2TPv3 Tunnel 設定 1]

Description	
Peerアドレス	10.10.20.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	XR_B
Remote RouterID設定	172.20.20.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	ppp0

XR\_B(拠点)に対する L2TPv3 Tunnel を設定します。

Vendor ID 設定で「20376:CENTURY」を選択しています。

ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 1]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.20.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	30 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_B(拠点)に対する Xconnect Interface を設定します。

**【L2TPv3】**

L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
--------	--

L2TPv3 を起動します。

## 拠点ルータ (XR\_B)

### ポイント

XR\_A(センター)に対して L2TPv3 接続を行います。

L2TPv3 フィルタで指定した端末以外のアクセスを一部制限しています。

### <<インタフェース設定>>

[Ethernet0 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.2
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 の設定をします。

※IP アドレスの設定を変更した場合、即設定が反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test2@centurysys
パスワード	test2pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

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

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時 PADTを強制送 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時 PADTを強制送
-------------------------	---

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。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛先アドレス	宛先ポート	LOG
ppp0	パケット受信時	許可	l2tp					<input type="checkbox"/>

L2TP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<L2TPv3>

[L2TPv3 機能設定]

Local hostname	XR_B
Local Router-ID	172.20.20.1
MAD Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAD Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMU Discover設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_B(拠点)の Local hostname, Local Router-ID を設定します。MAC アドレス学習機能を使用する場合は「有効」に設定してください。(デフォルトは有効です)

[L2TPv3 Tunnel 設定 1]

Description	
Peerアドレス	10.10.10.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	XR_A
Remote RouterID設定	172.20.10.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	ppp0

XR\_A(センター)に対する L2TPv3 Tunnel を設定します。

Vendor ID 設定で「20376:CENTURY」を選択しています。

ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 1]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.10.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	45 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_A(センター)に対する Xconnect Interface を設定します。

**【L2TPv3】**

L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
--------	--

L2TPv3 を起動します。

〈L2TPv3 フィルタ〉

[Root Filter 設定]

Index	1
Root Filter Name	root-filter1
Default Policy	deny <input type="button" value="v"/>

Root Filter として「root-filter1」を定義します。  
ルートポリシーは「deny」を選択します。



[Layer2 ACL 設定]

Layer2 ACL として「l2-filter1」, 「l2-filter2」, 「l2-filter3」を定義します。

Layer2 ACL Name	l2-filter1
Policy	deny
Source MAC	
Destination MAC	
Protocol/Length	ARP or [0x0600-0xffff]

Layer2 ACL として「l2-filter1」を定義します。

ポリシーは「deny」を選択します。

Protocol として「ARP」を指定します。

Layer2 ACL Name	l2-filter2
Policy	deny
Source MAC	00:80:6D:FF:FF:01
Destination MAC	
Protocol/Length	IPv4 or [0x0600-0xffff]

Layer2 ACL として「l2-filter2」を定義します。

ポリシーは「deny」を選択します。

Source MAC として「00:80:6D:FF:FF:01」を設定します。

Protocol として「IPv4」を選択します。

Layer2 ACL Name	l2-filter3
Policy	deny
Source MAC	
Destination MAC	
Protocol/Length	IPv4 or [0x0600-0xffff]

Layer2 ACL として「l2-filter3」を定義します。

ポリシーは「deny」を選択します。

Protocol として「IPv4」を指定します。

[IPv4 Extend ACL 設定]

IPv4 Extend ACL として「ip-filter1」, 「ip-filter2」を定義します。

Extend ACL Name	ip-filter1
Policy	permit
Source IP	192.168.10.11
Destination IP	
TOS	[0-0xff]
IP Protocol	---- or [0-255]
Source Port	[1-65535]
Destination Port	[1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

IPv4 Extend ACL として「ip-filter1」を定義します。

ポリシーは「permit」を選択します。

Source IP は「192.168.10.11」を指定し、該当する IP トラフィックを許可します。

Extend ACL Name	ip-filter2
Policy	permit
Source IP	
Destination IP	192.168.10.254
TOS	[0-0xff]
IP Protocol	TCP or [0-255]
Source Port	[1-65535]
Destination Port	80 [1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

IPv4 Extend ACL として「ip-filter2」を定義します。

ポリシーは「permit」を選択します。

Destination IP は「192.168.10.254」, Protocol, Destination Port は「TCP 80 番ポート」を指定し、該当する IP トラフィックを許可します。

[ARP Extend ACL 設定]

ARP Extend ACL として「arp-filter1」, 「arp-filter2」を定義します。

Extend ACL Name	arp-filter1
Policy	permit
OPCODE	---- or [0-65535]
Source MAC	00:80:6D:FF:FF:01
Destination MAC	
Source IP	
Destination IP	

ARP Extend ACL として「arp-filter1」を定義します。

ポリシーは「permit」を選択します。

Source MAC 「00:80:6D:FF:FF:01」を指定し、該当する ARP トラフィックを許可します。

Extend ACL Name	arp-filter2
Policy	permit
OPCODE	---- or [0-65535]
Source MAC	
Destination MAC	
Source IP	
Destination IP	192.168.10.254

ARP Extend ACL として「arp-filter2」を定義します。

ポリシーは「permit」を選択します。

Destination IP 「192.168.10.254」を指定し、該当する ARP トラフィックを許可します。

[配下の拡張 ACL 設定]

Layer2 ACL では、それぞれ拡張 ACL を指定することができます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Protocol/Length	edit	extend
1	l2-filter1	deny			ARP	<a href="#">edit</a>	<a href="#">extend</a>
2	l2-filter2	deny	00:80:6D:FF:FF:01		IPv4	<a href="#">edit</a>	<a href="#">extend</a>
3	l2-filter3	deny			IPv4	<a href="#">edit</a>	<a href="#">extend</a>

[[l2-filter1 の場合]]

Seq.No.	<input type="text" value="1"/>
Name	<input type="text" value="arp-filter1"/> ▼

Seq.No.	<input type="text" value="2"/>
Name	<input type="text" value="arp-filter2"/> ▼

l2-filter1 では、「arp-filter1」, 「arp-filter2」を選択します。

[[l2-filter2 の場合]]

Seq.No.	<input type="text" value="1"/>
Name	<input type="text" value="ip-filter1"/> ▼

l2-filter2 では、「ip-filter1」を選択します。

[[l2-filter3 の場合]]

Seq.No.	<input type="text" value="1"/>
Name	<input type="text" value="ip-filter2"/> ▼

l2-filter3 では、「ip-filter2」を選択します。

[配下の Layer2 ACL 設定]

Root Filter では、Layer2 ACL を指定することができます。

この例では、より多く参照されると考えられる順番で Layer2 ACL を設定しています。

Index	Root Filter Name	edit	layer2
1	root-filter1	<a href="#">edit</a>	<a href="#">layer2</a>

Seq.No.	<input type="text" value="1"/>
Layer2 ACL Name	<input type="text" value="l2-filter2"/> ▼

Seq.No.	<input type="text" value="2"/>
Layer2 ACL Name	<input type="text" value="l2-filter3"/> ▼

Seq.No.	<input type="text" value="3"/>
Layer2 ACL Name	<input type="text" value="l2-filter1"/> ▼

root-filter1 では、「l2-filter2」, 「l2-filter3」, 「l2-filter1」を選択します。

[L2TPv3 Filter 設定]

Interface	eth0
ACL(in)	<input type="text" value="root-filter1"/> ▼
ACL(out)	<input type="text" value="----"/> ▼

「root-filter1」を Interface Filter の IN Filter で設定します。

[機能設定]

本機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
-----	--

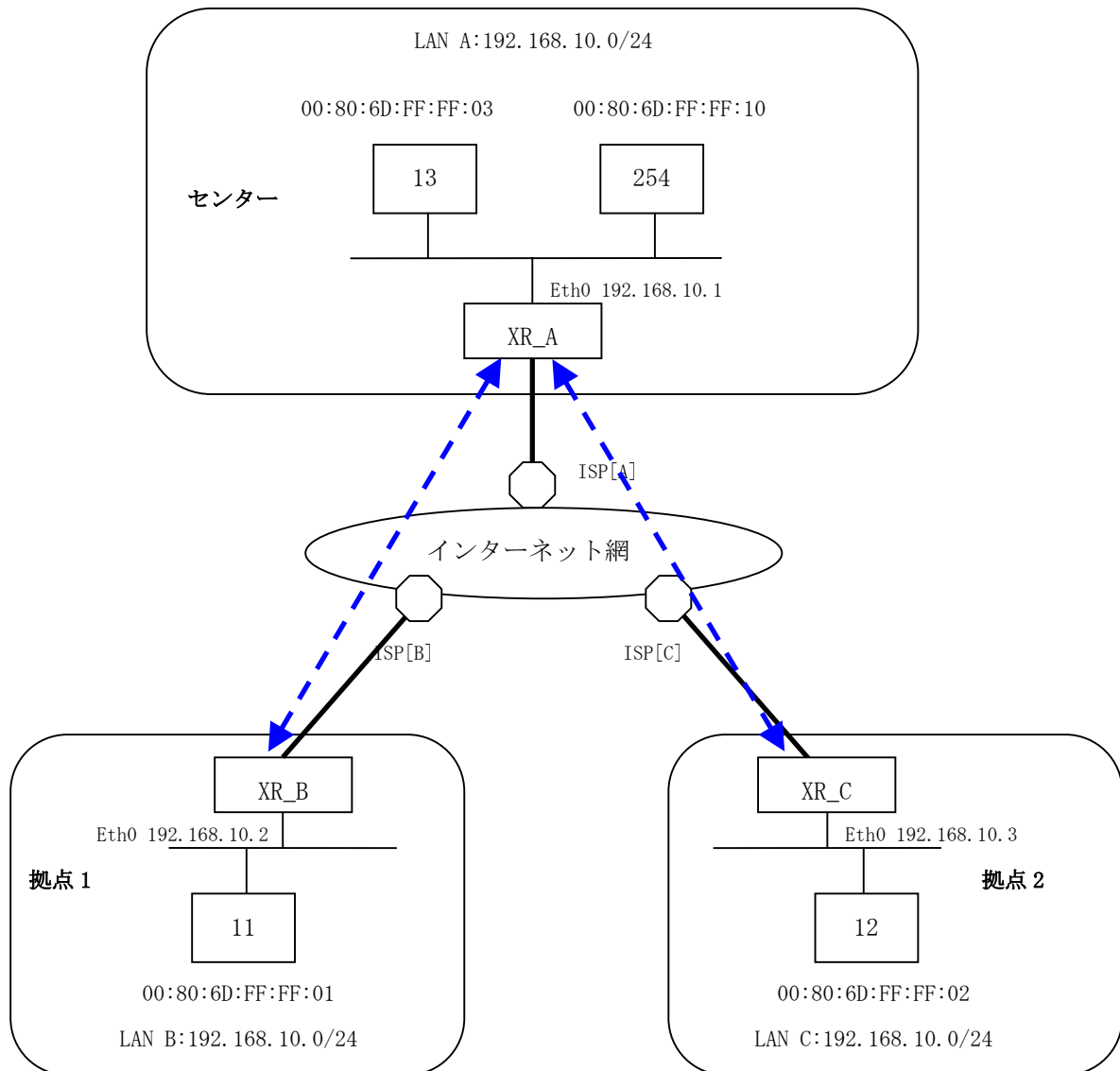
L2TPv3 フィルタを有効にします。

## 2. L2TPv3 フィルタの利用例 2

この設定例は、センターに対して一部アクセス制限を行いつつ、拠点間での通信は破棄します。

この例では、XR\_A で宛先 端末 13 の ARP、宛先 端末 13 で宛先ポート「TCP ポート 80」および ICMP の IP トラフィックは許可し、それ以外のトラフィックは全て破棄します。また XR\_A を経由した XR\_B、XR\_C 間での通信はできません。

### 2-1. 構成例



## 2-2. 要件

➤ インタフェースおよび PPP/PPPoE

- XR\_A(センター), XR\_B(拠点 1), XR\_C(拠点 2)はインターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの IP マスカレード, ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.10.2	192.168.10.3
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	10.10.20.1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys	test3@centurysys
PPPoE パスワード	test1pass	test2pass	test3pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続	PPPoE 接続

➤ L2TPv3

- XR\_A(センター)では、XR\_B(拠点 1), XR\_C(拠点 2)と L2TPv3 で接続するための設定しています。
- XR\_B(拠点 1)では、XR\_A(センター)と L2TPv3 で接続するための設定しています。
- XR\_C(拠点 2)では、XR\_A(センター)と L2TPv3 で接続するための設定しています。
- XR\_A(センター), XR\_B(拠点 1), XR\_C(拠点 2)では PPPoE 接続を利用しているため、Bind Interface として「ppp0」を指定しています。

主な L2TPv3 機能設定のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
Local hostname	XR_A	XR_B	XR_C
Local Router-ID	172.20.10.1	172.20.20.1	172.20.30.1
MAC Address 学習機能	有効	有効	有効

主な L2TPv3 Tunnel 設定のパラメータ

対向拠点	XR_A(センター)		XR_B(拠点 1)	XR_C(拠点 2)
	XR_B(拠点 1)	XR_C(拠点 2)	XR_A(センター)	XR_A(センター)
Peer IP	10.10.20.1	10.10.30.1	10.10.10.1	10.10.10.1
Remote Hostname	XR_B	XR_C	XR_A	XR_A
Remote RouterID	172.20.20.1	172.20.30.1	172.20.10.1	172.20.10.1
Bind Interface	ppp0	ppp0	ppp0	ppp0

主な L2TPv3 Xconnect Interface 設定のパラメータ

対向拠点	XR_A(センター)		XR_B(拠点 1)	XR_C(拠点 2)
	XR_B(拠点 1)	XR_C(拠点 2)	XR_A(センター)	XR_A(センター)
Peer ID	172.20.20.1	172.20.30.1	172.20.10.1	172.20.10.1
Interface	eth0	eth0	eth0	eth0
Remote End ID	1	1	1	1
Reschedule Interval	30	0	45	45
Auto	有効	有効	有効	有効
Split Horizon	有効	有効	無効	無効



➤ L2TPv3 フィルタ

- XR\_A の Xconnect Interface OUT Filter でフィルタリングを行います。
- 宛先 13 の ARP, および宛先 13 TCP ポート 80, ICMP の IP トラフィックは許可。
- それ以外のトラフィックは全て破棄。
- XR\_A を経由した XR\_B, XR\_C 間での通信は不可。

主な L2TPv3 フィルタ Root Filter 設定のパラメータ

	XR_A(センター)
Root Filter Name	root-filter1
Default Policy	deny

主な L2TPv3 フィルタ Layer2 ACL 設定のパラメータ

	XR_A(センター)	
Layer2 ACL Name	l2-filter1	l2-filter2
Policy	deny	deny
Source MAC		
Destination MAC		
Protocol/Length	ARP	IPv4

主な L2TPv3 フィルタ IPv4 Extend ACL 設定のパラメータ

	XR_A(センター)	
Extend ACL Name	ip-filter1	ip-filter2
Policy	permit	permit
Source IP		
Destination IP	192.168.10.13	192.168.10.13
IP Protocol	TCP	ICMP
Destination Port	80	

主な L2TPv3 フィルタ ARP Extend ACL 設定のパラメータ

	XR_A(センター)
Extend ACL Name	arp-filter1
Policy	permit
Source MAC	
Destination MAC	
Source IP	
Destination IP	192.168.10.13

ACL は以下のようなツリー構造になっています。

```
root-filter1
  + l2-filter2
    deny any any IPv4
    + ip-filter1
      permit
    + ip-filter2
      permit
  + l2-filter1
    deny any any ARP
  + default deny
```

➤ その他

- フィルタ設定[入力フィルタ]で、WAN 側インタフェースで受信した「L2TP」パケットを許可する設定にしています。

## 2-3. 設定例

### センタールータ (XR\_A)

#### ポイント

拠点 1, 2 と L2TPv3 で接続するための設定を行います。

L2TPv3 フィルタで一部アクセス制限を行い、かつ拠点間での通信は破棄します。

#### <<インタフェース設定>>

[Ethernet0 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IP アドレスの設定を変更した場合、即設定が反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test1@centurysys
パスワード	test1pass

PPPoE 接続で使用するユーザ ID、パスワードを登録します。

[接続設定]

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

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時 PADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出
-------------------------	--

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。

<<フィルタ設定>>

[入力フィルタ]

インタフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	l2tp					<input type="checkbox"/>

L2TP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<L2TPv3>

[L2TPv3 機能設定]

Local hostname	XR_A
Local Router-ID	172.20.10.1
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
FMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_A(センター)の Local hostname, Local Router-ID を設定します。MAC アドレス学習機能を使用する場合は「有効」に設定してください。(デフォルトは有効です)

[L2TPv3 Tunnel 設定 1]

Description	
Peerアドレス	10.10.20.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	XR_B
Remote RouterID設定	172.20.20.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	ppp0

XR\_B(拠点)に対する L2TPv3 Tunnel を設定します。  
Vender ID 設定で「20376:CENTURY」を選択しています。  
ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 1]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.20.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	30 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

XR\_B(拠点)に対する Xconnect Interface を設定します。

Session 間でのフレーム転送を行わないため、Split Horizon を有効にしています。

[L2TPv3 Tunnel 設定 2]

Description	<input type="text" value=""/>
Peerアドレス	<input type="text" value=""/> (例:192.168.0.1)
パスワード	<input type="text" value=""/> (英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効 <input type="button" value="v"/>
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	<input type="text" value=""/>
Local RouterID設定	<input type="text" value=""/>
Remote Hostname設定	XR_C
Remote RouterID設定	172.20.30.1
Vendor ID設定	20376:CENTURY <input type="button" value="v"/>
Bind Interface設定	ppp0

XR\_C(拠点 2)に対する L2TPv3 Tunnel を設定します。

XR\_C(拠点 2)の WAN 側 IP アドレスが動的 IP アドレスのため、Peer アドレスは「空欄」に設定していません。

ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 2]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.30.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

XR\_C(拠点 2)に対する Xconnect Interface を設定します。

XR\_C(拠点 2)の WAN 側 IP アドレスが動的 IP アドレスのため、Reschedule Interval 設定を「0」に設定しています。

Session 間でのフレーム転送を行わないため、Split Horizon を有効にしています。

【L2TPv3】

L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
--------	--

L2TPv3 を起動します。

<L2TPv3 フィルタ>

[Root Filter 設定]

Index	1
Root Filter Name	root-filter1
Default Policy	deny <input type="button" value="v"/>

Root Filter として「root-filter1」を定義します。

ルートポリシーは「deny」を選択します。

[Layer2 ACL 設定]

Layer2 ACL として「l2-filter1」, 「l2-filter2」を定義します。

Layer2 ACL Name	l2-filter1
Policy	deny
Source MAC	
Destination MAC	
Protocol/Length	ARP or [0x0600-0xffff]

Layer2 ACL として「l2-filter1」を定義します。

ポリシーは「deny」を選択します。

Protocol として「ARP」を指定します。

Layer2 ACL Name	l2-filter2
Policy	deny
Source MAC	
Destination MAC	
Protocol/Length	IPv4 or [0x0600-0xffff]

Layer2 ACL として「l2-filter2」を定義します。

ポリシーは「deny」を選択します。

Protocol として「IPv4」を選択します。



[IPv4 Extend ACL 設定]

IPv4 Extend ACL として「ip-filter1」, 「ip-filter2」を定義します。

Extend ACL Name	ip-filter1
Policy	permit
Source IP	
Destination IP	192.168.10.13
TOS	[0-0xff]
IP Protocol	TCP or [0-255]
Source Port	[1-65535]
Destination Port	80 [1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

IPv4 Extend ACL として「ip-filter1」を定義します。

ポリシーは「permit」を選択します。

Destination IP は「192.168.10.13」, Protocol, Destination Port は「TCP 80 番ポート」を指定し、該当する IP トラフィックを許可します。

Extend ACL Name	ip-filter2
Policy	permit
Source IP	
Destination IP	192.168.10.13
TOS	[0-0xff]
IP Protocol	ICMP or [0-255]
Source Port	[1-65535]
Destination Port	[1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

IPv4 Extend ACL として「ip-filter2」を定義します。

ポリシーは「permit」を選択します。

Destination IP は「192.168.10.13」, Protocol は「ICMP」を指定し、該当する IP トラフィックを許可します。

[ARP Extend ACL 設定]

ARP Extend ACL として「arp-filter1」を定義します。

Extend ACL Name	arp-filter1
Policy	permit
OPCODE	---- or [0-65535]
Source MAC	
Destination MAC	
Source IP	
Destination IP	192.168.10.13

ARP Extend ACL として「arp-filter1」を定義します。

ポリシーは「permit」を選択します。

Destination IP は「192.168.10.13」を指定し、該当する ARP トラフィックを許可します。

[配下の拡張 ACL 設定]

Layer2 ACL では、それぞれ拡張 ACL を指定することができます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Protocol/Length	edit	extend
1	l2-filter1	deny			ARP	<a href="#">edit</a>	<a href="#">extend</a>
2	l2-filter2	deny			IPv4	<a href="#">edit</a>	<a href="#">extend</a>

[[l2-filter1 の場合]]

Seq.No.	<input type="text" value="1"/>
Name	<input type="text" value="arp-filter1"/> ▼

l2-filter1 では、「arp-filter1」を選択します。

[[l2-filter2 の場合]]

Seq.No.	<input type="text" value="1"/>
Name	<input type="text" value="ip-filter1"/> ▼

Seq.No.	<input type="text" value="2"/>
Name	<input type="text" value="ip-filter2"/> ▼

l2-filter3 では、「ip-filter1」, 「ip-filter2」を選択します。

[配下の Layer2 ACL 設定]

Root Filter では、Layer2 ACL を指定することができます。

この例では、より多く参照されると考えられる順番で Layer2 ACL を設定しています。

Index	Root Filter Name	edit	layer2
1	root-filter1	<a href="#">edit</a>	<a href="#">layer2</a>

Seq.No.	<input type="text" value="1"/>
Layer2 ACL Name	<input type="text" value="l2-filter2"/> ▼

Seq.No.	<input type="text" value="2"/>
Layer2 ACL Name	<input type="text" value="l2-filter1"/> ▼

root-filter1 では、「l2-filter2」, 「l2-filter1」を選択します。

[L2TPv3 Filter 設定]

Interface	eth0
ACL(in)	---- ▼
ACL(out)	root-filter1 ▼

「root-filter1」を Interface Filter の OUT Filter で設定します。

[機能設定]

本機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
-----	--

L2TPv3 フィルタを有効にします。

## 拠点 1 ルータ (XR\_B)

### ポイント

XR\_A(センター)に対して L2TPv3 接続を行います。

### <<インタフェース設定>>

[Ethernet0 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.2
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 の設定をします。

※IP アドレスの設定を変更した場合、即設定が反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

### <<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test2@centurysys
パスワード	test2pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

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

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時 PADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出
-------------------------	--

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。

<<フィルタ設定>>

[入力フィルタ]

インタフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	l2tp					<input type="checkbox"/>

L2TP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<L2TPv3>

[L2TPv3 機能設定]

Local hostname	XR_B
Local Router-ID	172.20.20.1
MAD Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAD Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_B(拠点 1)の Local hostname, Local Router-ID を設定します。MAC アドレス学習機能を使用する場合は「有効」に設定してください。(デフォルトは有効です)

[L2TPv3 Tunnel 設定 1]

Description	
Peerアドレス	10.10.10.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	XR_A
Remote RouterID設定	172.20.10.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	ppp0

XR\_A(センター)に対する L2TPv3 Tunnel を設定します。  
Vender ID 設定で「20376:CENTURY」を選択しています。  
ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 1]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.10.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	45 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_A(センター)に対する Xconnect Interface を設定します。

**【L2TPv3】**

L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
--------	--

L2TPv3 を起動します。



## 拠点 2 ルータ (XR\_C)

### ポイント

XR\_A(センター)に対して L2TPv3 接続を行います。

### <<インタフェース設定>>

[Ethernet0 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.3
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 の設定をします。

※IP アドレスの設定を変更した場合、即設定が反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

### <<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test3@centurysys
パスワード	test3pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

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

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時 PADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出
-------------------------	--

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。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	l2tp					<input type="checkbox"/>

L2TP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<L2TPv3>

[L2TPv3 機能設定]

Local hostname	XR_C
Local Router-ID	172.20.30.1
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Ageing Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_C(拠点 2)の Local hostname, Local Router-ID を設定します。MAC アドレス学習機能を使用する場合は「有効」に設定してください。(デフォルトは有効です)

[L2TPv3 Tunnel 設定 1]

Description	
Peerアドレス	10.10.10.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	XR_A
Remote RouterID設定	172.20.10.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	ppp0

XR\_A(センター)に対する L2TPv3 Tunnel を設定します。

Vendor ID 設定で「20376:CENTURY」を選択しています。

ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 1]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.10.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	45 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_A(センター)に対する Xconnect Interface を設定します。

**【L2TPv3】**

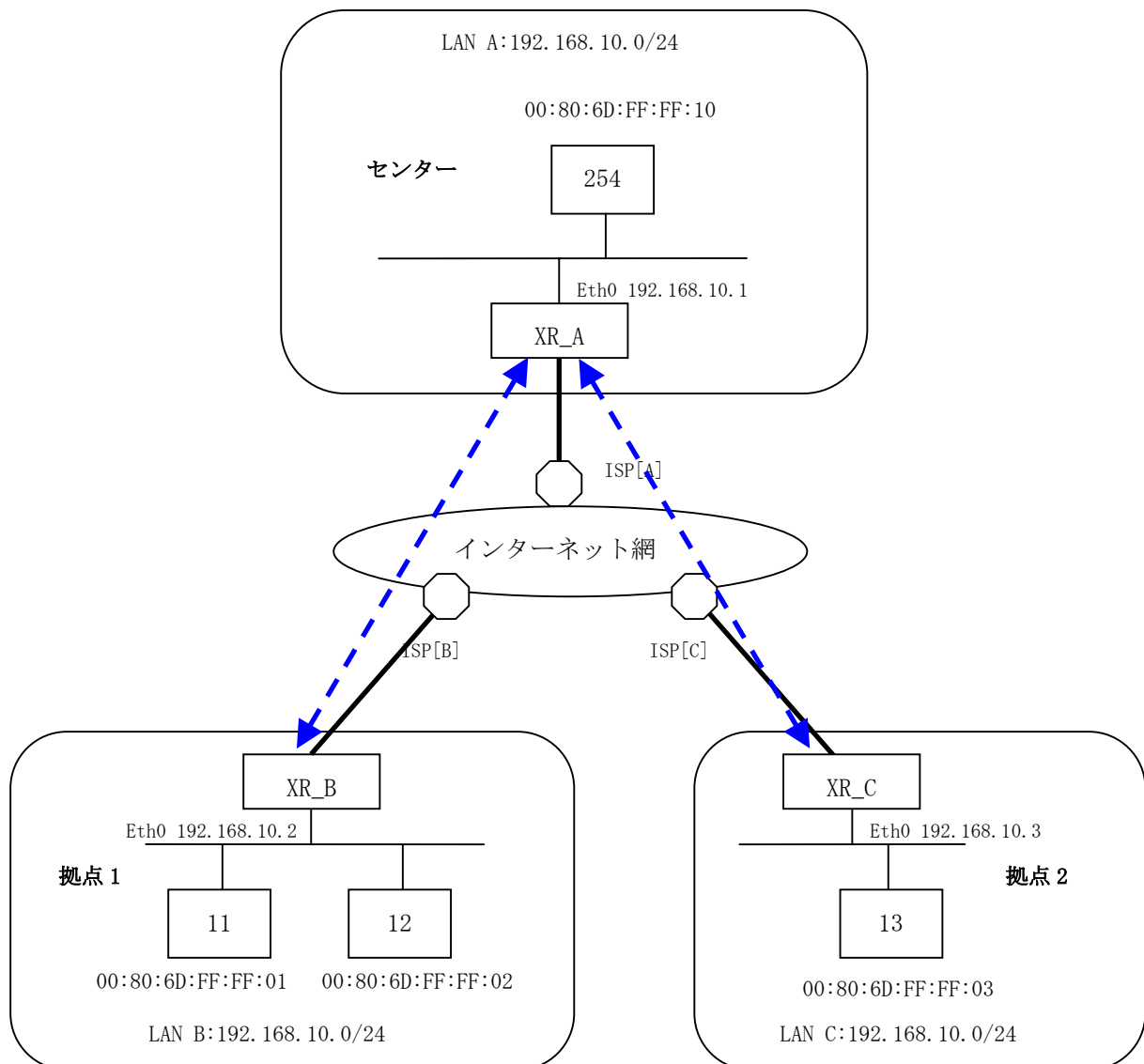
L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
--------	--

L2TPv3 を起動します。

### 3. L2TPv3 フィルタの利用例 3

この設定例は、拠点からセンターに対しての通信および拠点間での通信で一部アクセス制限を行います。この例では XR\_A で、送信元 MAC アドレスで許可されている端末 11, 13 の ARP, IP トラフィックを許可します。また、それ以外の端末からの宛先 端末 254 の ARP, および宛先 端末 254 TCP ポート 80, ICMP の IP トラフィックは許可します。それ以外のトラフィックは全て破棄します。

#### 3-1. 構成例



### 3-2. 要件

➤ インタフェースおよび PPP/PPPoE

- XR\_A(センター), XR\_B(拠点 1), XR\_C(拠点 2)はインターネットに PPPoE で接続します。
- PPPoE 接続は、自動再接続するように設定しています。
- WAN 側インタフェースの IP マスカレード, ステートフルパケットインスペクションは「有効」にしています。

主なインタフェースおよび PPP/PPPoE のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
LAN 側インタフェース	Ether0	Ether0	Ether0
LAN 側 IP アドレス	192.168.10.1	192.168.10.2	192.168.10.3
WAN 側インタフェース	Ether1[ppp0]	Ether1[ppp0]	Ether1[ppp0]
WAN 側 IP アドレス	10.10.10.1	10.10.20.1	動的 IP
PPPoE ユーザ名	test1@centurysys	test2@centurysys	test3@centurysys
PPPoE パスワード	test1pass	test2pass	test3pass
WAN 側接続回線	PPPoE 接続	PPPoE 接続	PPPoE 接続

➤ L2TPv3

- XR\_A(センター)では、XR\_B(拠点 1), XR\_C(拠点 2)と L2TPv3 で接続するための設定しています。
- XR\_B(拠点 1)では、XR\_A(センター)と L2TPv3 で接続するための設定しています。
- XR\_C(拠点 2)では、XR\_A(センター)と L2TPv3 で接続するための設定しています。
- XR\_A(センター), XR\_B(拠点 1), XR\_C(拠点 2)では PPPoE 接続を利用しているため、Bind Interface として「ppp0」を指定しています。

主な L2TPv3 機能設定のパラメータ

	XR_A(センター)	XR_B(拠点 1)	XR_C(拠点 2)
Local hostname	XR_A	XR_B	XR_C
Local Router-ID	172.20.10.1	172.20.20.1	172.20.30.1
MAC Address 学習機能	有効	有効	有効

主な L2TPv3 Tunnel 設定のパラメータ

対向拠点	XR_A(センター)		XR_B(拠点 1)	XR_C(拠点 2)
	XR_B(拠点 1)	XR_C(拠点 2)	XR_A(センター)	XR_A(センター)
Peer IP	10.10.20.1	10.10.30.1	10.10.10.1	10.10.10.1
Remote Hostname	XR_B	XR_C	XR_A	XR_A
Remote RouterID	172.20.20.1	172.20.30.1	172.20.10.1	172.20.10.1
Bind Interface	ppp0	ppp0	ppp0	ppp0

主な L2TPv3 Xconnect Interface 設定のパラメータ

対向拠点	XR_A(センター)		XR_B(拠点 1)	XR_C(拠点 2)
	XR_B(拠点 1)	XR_C(拠点 2)	XR_A(センター)	XR_A(センター)
Peer ID	172.20.20.1	172.20.30.1	172.20.10.1	172.20.10.1
Interface	eth0	eth0	eth0	eth0
Remote End ID	1	1	1	1
Reschedule Interval	30	0	45	45
Auto	有効	有効	有効	有効
Split Horizon	無効	無効	無効	無効

➤ L2TPv3 フィルタ

- XR\_A の Session Filter In Filter でフィルタリングを行います。
- 送信元 MAC アドレスが端末 11, 13 の ARP, IP トラフィックは許可。
- 端末 11, 13 以外の端末からの宛先 端末 254 の ARP, および宛先 端末 254 で TCP ポート 80 番, ICMP の IP トラフィックは許可。
- それ以外のトラフィックは全て破棄。

主な L2TPv3 フィルタ Root Filter 設定のパラメータ

	XR_A(センター)	
Root Filter Name	root-filter1	root-filter2
Default Policy	deny	deny

主な L2TPv3 フィルタ Layer2 ACL 設定のパラメータ

	XR_A(センター)			
Layer2 ACL Name	l2-filter1-arp	l2-filter1-ipv4	l2-filter2-arp	l2-filter2-ipv4
Policy	deny	deny	deny	deny
Source MAC				
Destination MAC				
Protocol/Length	ARP	IPv4	ARP	IPv4

主な L2TPv3 フィルタ IPv4 Extend ACL 設定のパラメータ

	XR_A(センター)			
Extend ACL Name	ip-filter1	ip-filter2	ip-filter-other1	ip-filter-other2
Policy	permit	permit	permit	permit
Source IP	192.168.10.11	192.168.10.13		
Destination IP			192.168.10.254	192.168.10.254
IP Protocol			TCP	ICMP
Destination Port			80	



主な L2TPv3 フィルタ ARP Extend ACL 設定のパラメータ

Extend ACL Name	arp-filter1	arp-filter2	arp-filter-other
Policy	permit	permit	permit
Source MAC	00:80:6D:FF:FF:01	00:80:6D:FF:FF:03	
Destination MAC			
Source IP			
Destination IP			192.168.10.254

ACL は以下のようなツリー構造になっています。

```
root-filter1
+ 12-filter1-ipv4
  deny    any          any          IPv4
  + ip-filter1
    permit
  + ip-filter-other1
    permit
  + ip-filter-other2
    permit
+ 12-filter1-arp
  deny    any          any          ARP
  + arp-filter1
    permit
  + arp-filter-other
    permit
+ default deny
```

```
root-filter2
+ 12-filter2-ipv4
  deny    any          any          IPv4
  + ip-filter2
    permit
  + ip-filter-other1
    permit
  + ip-filter-other2
    permit
+ 12-filter2-arp
  deny    any          any          ARP
  + arp-filter2
    permit
  + arp-filter-other
    permit
+ default deny
```

➤ その他

- フィルタ設定[入力フィルタ]で、WAN 側インタフェースで受信した「L2TP」パケットを許可する設定にしています。

### 3-3. 設定例

#### センタールータ (XR\_A)

##### ポイント

拠点 1, 2 と L2TPv3 で接続するための設定を行います。

L2TPv3 フィルタで拠点からセンターに対しての通信および拠点間での通信で一部アクセス制限を行います。

#### <<インタフェース設定>>

[Ethernet0 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IP アドレスの設定を変更した場合、即設定が反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

#### <<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test1@centurysys
パスワード	test1pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

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

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時 PADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出
-------------------------	--

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。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	l2tp					<input type="checkbox"/>

L2TP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<L2TPv3>

[L2TPv3 機能設定]

Local hostname	XR_A
Local Router-ID	172.20.10.1
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
FMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_A(センター)の Local hostname, Local Router-ID を設定します。MAC アドレス学習機能を使用する場合は「有効」に設定してください。(デフォルトは有効です)

[L2TPv3 Tunnel 設定 1]

Description	
Peerアドレス	10.10.20.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	XR_B
Remote RouterID設定	172.20.20.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	ppp0

XR\_B(拠点)に対する L2TPv3 Tunnel を設定します。

Vendor ID 設定で「20376:CENTURY」を選択しています。

ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 1]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.20.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	30 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_B(拠点)に対する Xconnect Interface を設定します。

[L2TPv3 Tunnel 設定 2]

Description	<input type="text" value=""/>
Peerアドレス	<input type="text" value=""/> (例:192.168.0.1)
パスワード	<input type="text" value=""/> (英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効 <input type="button" value="v"/>
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	<input type="text" value=""/>
Local RouterID設定	<input type="text" value=""/>
Remote Hostname設定	XR_C <input type="text" value=""/>
Remote RouterID設定	172.20.30.1 <input type="text" value=""/>
Vendor ID設定	20376:CENTURY <input type="button" value="v"/>
Bind Interface設定	ppp0 <input type="text" value=""/>

XR\_C(拠点 2)に対する L2TPv3 Tunnel を設定します。

XR\_C(拠点 2)の WAN 側 IP アドレスが動的 IP アドレスのため、Peer アドレスは「空欄」に設定しています。

Vendor ID 設定で「20376:CENTURY」を選択しています。

ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 2]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.30.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_C(拠点 2)に対する Xconnect Interface を設定します。

XR\_C(拠点 2)の WAN 側 IP アドレスが動的 IP アドレスのため、Reschedule Interval 設定を「0」に設定しています。

**【L2TPv3】**

L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
--------	--

L2TPv3 を起動します。



### <L2TPv3 フィルタ>

#### [Root Filter 設定]

Root Filter Name	root-filter1
Default Policy	deny

Root Filter として「root-filter1」を定義します。  
ルートポリシーは「deny」を選択します。

Root Filter Name	root-filter2
Default Policy	deny

Root Filter として「root-filter2」を定義します。  
ルートポリシーは「deny」を選択します。

#### [Layer2 ACL 設定]

Layer2 ACL として「l2-filter1-arp」, 「l2-filter2-arp」, 「l2-filter1-ipv4」, 「l2-filter2-ipv4」を定義します。

Layer2 ACL Name	l2-filter1-arp
Policy	deny
Source MAC	
Destination MAC	
Protocol/Length	ARP or [0x0600-0xffff]

Layer2 ACL として「l2-filter1-arp」を定義します。  
ポリシーは「deny」を選択します。  
Protocol として「ARP」を指定します。

Layer2 ACL Name	l2-filter2-arp
Policy	deny
Source MAC	
Destination MAC	
Protocol/Length	ARP or [0x0600-0xffff]

Layer2 ACL として「l2-filter2-arp」を定義します。  
ポリシーは「deny」を選択します。  
Protocol として「ARP」を指定します。

Layer2 ACL Name	l2-filter1-ipv4
Policy	deny
Source MAC	
Destination MAC	
Protocol/Length	IPv4 or [0x0600-0xffff]

Layer2 ACL として「l2-filter1-ipv4」を定義します。

ポリシーは「deny」を選択します。

Protocol として「IPv4」を指定します。

Layer2 ACL Name	l2-filter2-ipv4
Policy	deny
Source MAC	
Destination MAC	
Protocol/Length	IPv4 or [0x0600-0xffff]

Layer2 ACL として「l2-filter2-ipv4」を定義します。

ポリシーは「deny」を選択します。

Protocol として「IPv4」を指定します。

[IPv4 Extend ACL 設定]

IPv4 Extend ACL として「ip-filter1」, 「ip-filter2」, 「ip-filter-other1」, 「ip-filter-other2」を定義します。

Extend ACL Name	ip-filter1
Policy	permit
Source IP	192.168.10.11
Destination IP	
TOS	[0-0xff]
IP Protocol	---- or [0-255]
Source Port	[1-65535]
Destination Port	[1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

IPv4 Extend ACL として「ip-filter1」を定義します。

ポリシーは「permit」を選択します。

Source IP は「192.168.10.11」を指定し、該当する IP トラフィックを許可します。

Extend ACL Name	ip-filter2
Policy	permit
Source IP	192.168.10.13
Destination IP	
TOS	[0-0xff]
IP Protocol	---- or [0-255]
Source Port	[1-65535]
Destination Port	[1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

IPv4 Extend ACL として「ip-filter2」を定義します。

ポリシーは「permit」を選択します。

Source IP は「192.168.10.13」を指定し、該当する IP トラフィックを許可します。

Extend ACL Name	ip-filter-other1
Policy	permit
Source IP	
Destination IP	192.168.10.254
TOS	[0-0xff]
IP Protocol	TCP or [0-255]
Source Port	[1-65535]
Destination Port	80 [1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

IPv4 Extend ACL として「ip-filter-other1」を定義します。

ポリシーは「permit」を選択します。

Destination IP は「192.168.10.254」、Protocol, Destination Port は「TCP 80 番ポート」を指定し、該当する IP トラフィックを許可します。

Extend ACL Name	ip-filter-other2
Policy	permit
Source IP	
Destination IP	192.168.10.254
TOS	[0-0xff]
IP Protocol	ICMP or [0-255]
Source Port	[1-65535]
Destination Port	[1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

IPv4 Extend ACL として「ip-filter-other2」を定義します。

ポリシーは「permit」を選択します。

Destination IP は「192.168.10.254」、Protocol は「ICMP」を指定し、該当する IP トラフィックを許可します。

[ARP Extend ACL 設定]

ARP Extend ACL として「arp-filter1」, 「arp-filter2」, 「arp-filter-other」を定義します。

Extend ACL Name	arp-filter1
Policy	permit
OPCODE	---- or [0-65535]
Source MAC	00:80:6D:FF:FF:01
Destination MAC	
Source IP	
Destination IP	

ARP Extend ACL として「arp-filter1」を定義します。

ポリシーは「permit」を選択します。

Source MAC は「00:80:6D:FF:FF:01」を指定し、該当する ARP トラフィックを許可します。

Extend ACL Name	arp-filter2
Policy	permit
OPCODE	---- or [0-65535]
Source MAC	00:80:6D:FF:FF:03
Destination MAC	
Source IP	
Destination IP	

ARP Extend ACL として「arp-filter2」を定義します。

ポリシーは「permit」を選択します。

Source MAC は「00:80:6D:FF:FF:03」を指定し、該当する ARP トラフィックを許可します。

Extend ACL Name	arp-filter-other
Policy	permit
OPCODE	---- or [0-65535]
Source MAC	
Destination MAC	
Source IP	
Destination IP	192.168.10.254

ARP Extend ACL として「arp-filter-other」を定義します。

ポリシーは「permit」を選択します。

Destination IP は「192.168.10.254」を指定し、該当する ARP トラフィックを許可します。

[配下の拡張 ACL 設定]

Layer2 ACL では、それぞれ拡張 ACL を指定することができます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Protocol/Length	edit	extend
1	l2-filter1-arp	deny			ARP	<a href="#">edit</a>	<a href="#">extend</a>
2	l2-filter2-arp	deny			ARP	<a href="#">edit</a>	<a href="#">extend</a>
3	l2-filter1-ipv4	deny			IPv4	<a href="#">edit</a>	<a href="#">extend</a>
4	l2-filter2-ipv4	deny			IPv4	<a href="#">edit</a>	<a href="#">extend</a>

[[l2-filter1-arp の場合]]

Seq.No.	<input type="text" value="1"/>
Name	<input type="text" value="arp-filter1"/> ▼

一番目として「arp-filter1」を選択します。

Seq.No.	<input type="text" value="2"/>
Name	<input type="text" value="arp-filter-other"/> ▼

二番目として「arp-filter-other」を選択します。

[[l2-filter2-arp の場合]]

Seq.No.	<input type="text" value="1"/>
Name	<input type="text" value="arp-filter2"/> ▼

一番目として「arp-filter2」を選択します。

Seq.No.	<input type="text" value="2"/>
Name	<input type="text" value="arp-filter-other"/> ▼

二番目として「arp-filter-other」を選択します。

[[l2-filter1-ipv4 の場合]]

Seq.No.	<input type="text" value="1"/>
Name	<input type="text" value="ip-filter1"/> ▼

一番目として「ip-filter1」を選択します。

Seq.No.	2
Name	ip-filter-other1 ▼

二番目として「ip-filter-other1」を選択します。

Seq.No.	3
Name	ip-filter-other2 ▼

三番目として「ip-filter-other2」を選択します。

[[l2-filter2-ipv4 の場合]]

Seq.No.	1
Name	ip-filter2 ▼

一番目として「ip-filter2」を選択します。

Seq.No.	2
Name	ip-filter-other1 ▼

二番目として「ip-filter-other1」を選択します。

Seq.No.	3
Name	ip-filter-other2 ▼

三番目として「ip-filter-other2」を選択します。

[配下の Layer2 ACL 設定]

Root Filter では、Layer2 ACL を指定することができます。

この例では、より多く参照されると考えられる順番で Layer2 ACL を設定しています。

Index	Root Filter Name	edit	layer2
1	root-filter1	<a href="#">edit</a>	<a href="#">layer2</a>
2	root-filter2	<a href="#">edit</a>	<a href="#">layer2</a>

[[root-filter1 の場合]]

Seq.No.	<input type="text" value="1"/>
Layer2 ACL Name	<input type="text" value="l2-filter1-ipv4"/> ▼

Seq.No.	<input type="text" value="2"/>
Layer2 ACL Name	<input type="text" value="l2-filter1-arp"/> ▼

root-filter1 では、「l2-filter1-ipv4」, 「l2-filter1-arp」を選択します。

[[root-filter2 の場合]]

Seq.No.	<input type="text" value="1"/>
Layer2 ACL Name	<input type="text" value="l2-filter2-ipv4"/> ▼

Seq.No.	<input type="text" value="2"/>
Layer2 ACL Name	<input type="text" value="l2-filter2-arp"/> ▼

root-filter2 では、「l2-filter2-ipv4」, 「l2-filter2-arp」を選択します。

[L2TPv3 Filter 設定]

PeerID : RemoteEndID	172.20.20.1
ACL(in)	<input type="text" value="root-filter1"/> ▼
ACL(out)	<input type="text" value="----"/> ▼

PeerID 「172.20.20.1」に「root-filter1」を Session Filter の IN Filter で設定します。

PeerID : RemoteEndID	172.20.30.1
ACL(in)	<input type="text" value="root-filter2"/> ▼
ACL(out)	<input type="text" value="----"/> ▼

PeerID 「172.20.30.1」に「root-filter2」を Session Filter の IN Filter で設定します。



[機能設定]

本機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
-----	--

L2TPv3 フィルタを有効にします。

## 拠点 1 ルータ (XR\_B)

### ポイント

XR\_A(センター)に対して L2TPv3 接続を行います。

### <<インタフェース設定>>

[Ethernet0 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.2
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 の設定をします。

※IP アドレスの設定を変更した場合、即設定が反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

### <<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test2@centurysys
パスワード	test2pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

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

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時 PADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出
-------------------------	--

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。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	l2tp					<input type="checkbox"/>

L2TP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<L2TPv3>

[L2TPv3 機能設定]

Local hostname	XR_B
Local Router-ID	172.20.20.1
MAD Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAD Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMU Discoverv設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_B(拠点 1)の Local hostname, Local Router-ID を設定します。MAC アドレス学習機能を使用する場合は「有効」に設定してください。(デフォルトは有効です)

[L2TPv3 Tunnel 設定 1]

Description	
Peerアドレス	10.10.10.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	XR_A
Remote RouterID設定	172.20.10.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	ppp0

XR\_A(センター)に対する L2TPv3 Tunnel を設定します。

Vender ID 設定で「20376:CENTURY」を選択しています。

ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。

[L2TPv3 Xconnect 設定 1]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.10.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	45 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_A(センター)に対する Xconnect Interface を設定します。

**【L2TPv3】**

L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
--------	--

L2TPv3 を起動します。

## 拠点 2 ルータ (XR\_C)

### ポイント

XR\_A(センター)に対して L2TPv3 接続を行います。

### <<インタフェース設定>>

[Ethernet0 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.3
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 の設定をします。

※IP アドレスの設定を変更した場合、即設定が反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

### <<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test3@centurysys
パスワード	test3pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

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

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、ルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時 PADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出
-------------------------	--

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。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG
ppp0	パケット受信時	許可	l2tp					<input type="checkbox"/>

L2TP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

<<各種サービスの設定>>

<L2TPv3>

[L2TPv3 機能設定]

Local hostname	XR_C
Local Router-ID	172.20.30.1
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_C(拠点 2)の Local hostname, Local Router-ID を設定します。MAC アドレス学習機能を使用する場合は「有効」に設定してください。(デフォルトは有効です)

[L2TPv3 Tunnel 設定 1]

Description	
Peerアドレス	10.10.10.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hide設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	XR_A
Remote RouterID設定	172.20.10.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	ppp0

XR\_A(センター)に対する L2TPv3 Tunnel を設定します。  
Vender ID 設定で「20376:CENTURY」を選択しています。  
ppp0 インタフェースを使用するため、Bind Interface として「ppp0」を設定しています。



[L2TPv3 Xconnect 設定 1]

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel設定選択	172.20.10.1 <input type="button" value="v"/>
L2Frame受信-インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	45 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XR\_A(センター)に対する Xconnect Interface を設定します。

**【L2TPv3】**

L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
--------	--

L2TPv3 を起動します。

Futurenet XR シリーズ インターネット VPN 設定例集

L2TPv3 フィルタ編

2006 年 8 月

発行 センチュリー・システムズ株式会社

2006 CENTURYSYSTEMS INC. ALL rights reserved.

---