
FutureNet NXR,XR シリーズ

VPN 相互接続設定例集

Ver 1.0.0

センチュリー・システムズ株式会社



目次

目次	2
はじめに	3
改版履歴	4
1. IPsec 設定	5
1-1. PPPoE を利用した IPsec 接続設定 (センタ NXR, 拠点 XR)	6
1-2. PPPoE を利用した IPsec 接続設定 (センタ XR, 拠点 NXR)	21
2. GRE 設定	33
2-1. PPPoE を利用した GRE 接続設定	34
3. L2TPv3 設定	41
3-1. PPPoE を利用した L2TPv3 接続設定 (センタ NXR, 拠点 XR)	42
3-2. PPPoE を利用した L2TPv3 接続設定 (センタ XR, 拠点 NXR)	54
付録	63
IPsec 状態確認方法	64
GRE 状態確認方法	75
L2TPv3 状態確認方法	77
FutureNet サポートデスクへのお問い合わせ	81
FutureNet サポートデスクへのお問い合わせに関して	82
FutureNet サポートデスクのご利用に関して	86

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、FutureNet NXR 製品と XR 製品に対応しております。
- 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 NXR-120/C, XR-510/C の以下のバージョンをベースに作成しております。
FutureNet NXR シリーズ NXR-120/C Ver5.18.0
FutureNet XR シリーズ XR-510/C Ver3.7.8
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、コマンド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。
- 設定した内容の復帰(流し込み)を行う場合は、NXR シリーズでは CLI では「copy」コマンド、GUI では設定の復帰を、XR シリーズでは GUI で設定の復帰を行う必要があります。
- モバイル通信端末をご利用頂く場合で契約内容が従量制またはそれに準ずる場合、大量のデータ通信を行うと利用料が高額になりますので、ご注意ください。
- 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。

改版履歷

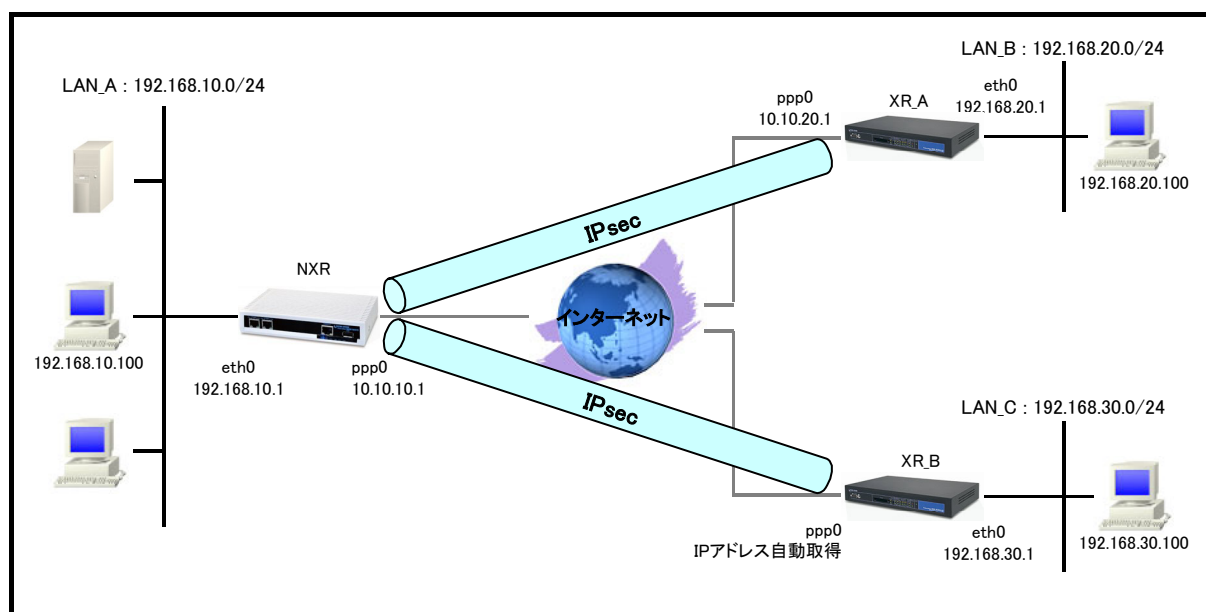
Version	更新內容
1.0.0	初版

1. IPsec 設定

1-1. PPPoE を利用した IPsec 接続設定(センタ NXR, 拠点 XR)

PPPoE 接続環境で NXR シリーズーXR シリーズ間で IPsec 接続を行う設定例です。この設定例では NXR、XR_A に WAN 側固定 IP アドレス、XR_B に WAN 側動的 IP アドレスが割り当てられる環境を想定しています。

【 構成図 】



- ・ この設定例では IPsec の監視方法として NXR では DPD、XR では IPsec Keepalive および DPD を設定します。
(☞) XR,NXR で DPD 監視を利用する場合は対向機器も DPD に対応している必要があります。
- ・ この設定例では NXR の IPsec 設定として Route Based IPsec を設定しています。(Policy Based IPsec を利用することも可能です)
- ・ 各拠点にある端末はそれぞれの拠点の NXR,XR からインターネットアクセスを行います。
- ・ この設定例では NXR のシステム LED 設定として ppp0 インタフェースアップ時に LED が点灯するように設定します。

【 設定例 】**[NXR の設定]**

```
nxr120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#ip access-linkdown
NXR(config-if)#exit
NXR(config)#ip route 192.168.20.0/24 tunnel 1
NXR(config)#ip route 192.168.30.0/24 tunnel 2
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR(config)#ipsec access-list LAN_B ip 192.168.10.0/24 192.168.20.0/24
NXR(config)#ipsec access-list LAN_C ip 192.168.10.0/24 192.168.30.0/24
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description XR_A
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 2
NXR(config-ipsec-isakmp)#lifetime 10800
NXR(config-ipsec-isakmp)#isakmp-mode main
NXR(config-ipsec-isakmp)#remote address ip 10.10.20.1
NXR(config-ipsec-isakmp)#keepalive 15 3 periodic restart
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description XR_A
NXR(config-ipsec-tunnel)#negotiation-mode auto
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#set pfs group2
NXR(config-ipsec-tunnel)#set sa lifetime 3600
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address LAN_B
NXR(config-ipsec-tunnel)#exit
NXR(config)#interface tunnel 1
NXR(config-tunnel)#tunnel mode ipsec ipv4
NXR(config-tunnel)#tunnel protection ipsec policy 1
NXR(config-tunnel)#ip tcp adjust-mss auto
NXR(config-tunnel)#exit
NXR(config)#ipsec isakmp policy 2
NXR(config-ipsec-isakmp)#description XR_B
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 2
NXR(config-ipsec-isakmp)#lifetime 10800
NXR(config-ipsec-isakmp)#isakmp-mode aggressive
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity fqdn xr
NXR(config-ipsec-isakmp)#keepalive 15 3 periodic clear
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 2
NXR(config-ipsec-tunnel)#description XR_B
```

——— 次のページに続きます ———

——— 前のページからの続きです ———

```

NXR(config-ipsec-tunnel)#negotiation-mode responder
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#set pfs group2
NXR(config-ipsec-tunnel)#set sa lifetime 3600
NXR(config-ipsec-tunnel)#set key-exchange isakmp 2
NXR(config-ipsec-tunnel)#match address LAN_C
NXR(config-ipsec-tunnel)#exit
NXR(config)#interface tunnel 2
NXR(config-tunnel)#tunnel mode ipsec ipv4
NXR(config-tunnel)#tunnel protection ipsec policy 2
NXR(config-tunnel)#ip tcp adjust-mss auto
NXR(config-tunnel)#exit
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys password test1pass
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR_A(config)#system led aux 1 interface ppp 0
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#exit
NXR#save config

```

NXR の設定に関しましてはご利用頂いている NXR 製品のユーザーズガイド(CLI 版)および FutureNetNXR 設定例集 IPsec 編をご参照ください。

なお以下は XR と IPsec 接続する際の注意事項となります。

NXR の工場出荷状態ではリンクダウンしているインタフェースの IP アドレス宛への通信はできません。

そのため XR 側で IPsec Keepalive を設定し、かつそのあて先 IP アドレスが NXR の LAN 側 IP アドレスの場合 NXR の LAN 側インタフェースがリンクダウンしていると XR 側では IPsec SA 確立→IPsec Keepalive で障害検知→IPsec SA 確立・・・を繰り返してしまいます。そのため NXR で当該インタフェースがリンクダウン状態でも通信可能にするため、以下のコマンドを LAN 側インタフェースに設定します。

1. <LAN 側(ethernet0)インタフェース設定>

```
NXR(config-if)#ip access-linkdown
```

リンクダウン状態でも、LAN 側(ethernet0)インタフェースの IP アドレスに対して通信ができるよう設定します。

2. <システム LED 設定>

```
NXR(config)#system led aux 1 interface ppp 0
```

ここでは ppp0 インタフェースの回線接続時に、AUX LED1 が点灯するように設定します。

〔XR_A の設定〕

1. <インタフェース設定>

設定メニューで「インタフェース設定」をクリックすると Ethernet0 インタフェース設定が表示されます。

Ethernet0ポート
[eth0]

☒ 固定アドレスで使用する

IP アドレス 192.168.20.1

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステータフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet0 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで使用するを選択
- ・ [IP アドレス] 192.168.20.1
- ・ [ネットマスク] 255.255.255.0

設定後[Ethernet 設定の保存]をクリックします。

画面上部の「Ethernet1 の設定」をクリックすると Ethernet1 インタフェース設定が表示されます。

Ethernet1ポート
[eth1]

☒ 固定アドレスで使用する

IP アドレス 0

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステータフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet1 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで使用するを選択
- ・ [IP アドレス] 0

設定後[Ethernet 設定の保存]をクリックします。

2. <PPPoE 設定>

設定メニューで「PPP/PPPoE 設定」をクリックすると接続設定が表示されます。

画面上部の「接続先設定 1」をクリックすると接続先設定 1が表示されます。

プロバイダ名	
ユーザID	test2@centurysys
パスワード	test2pass
DNSサーバ	☐ 割り当てられたDNSを使わない ☒ プロバイダから自動割り当て ☐ 手動で設定 プライマリ セカンダリ
LCPキープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	☒ 使用しない ☐ 使用する 使用するホスト 発行間隔は30秒固定、空欄の時はPING-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	☐ 無効 ☒ 有効(強制) MSS値 0 Byte (有効時にMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1462。ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

PPPoE の接続先で以下の項目を設定します。

- ・ [ユーザ ID] test2@centurysys
- ・ [パスワード] test2pass
(🔑) ISP から提供されたユーザ ID、パスワードを設定します。
- ・ [DNS サーバ] プロバイダから自動割り当て
- ・ [LCP キープアライブ] 30 秒
- ・ [MSS 設定] 有効
MSS 値 0

設定後[設定の保存]をクリックします。

設定メニューで「PPP/PPPoE 設定」をクリックします。

回線状態	回線は接続されていません				
接続先の選択	☒ 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	☐ RS232C	☐ Ether0	☒ Ether1		
接続形態	☐ 手動接続	☒ 常時接続			
RS232C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			
ICMP AddressMask Request	☐ 応答しない	☒ 応答する			

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

PPPoE の接続設定で以下の項目を設定します。

- ・ [接続先の選択] 接続先 1
- ・ [接続ポート] Ether1
- ・ [接続形態] 常時接続
- ・ [IP マスカレード] 有効
- ・ [ステートフルパケットインスペクション] 有効
- ・ [デフォルトルートの設定] 有効
- ・ [回線接続時に前回の PPPoE セッションの PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の IPv4Packet 受信時に PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出] 有効(チェック有)

設定後[接続]をクリックします。

(☞) [接続]をクリックすることにより設定の保存を行い、PPP/PPPoE 接続を開始します。

3. <フィルタ設定>

設定メニューで「フィルタ設定」をクリックすると入力フィルタ設定が表示されます。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	udp	10.10.10.1	500	10.10.20.1	500
2	ppp0	パケット受信時	許可	esp	10.10.10.1		10.10.20.1	

入力フィルタで以下の項目を設定します。

No.1

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] udp
- ・ [送信元アドレス] 10.10.10.1
- ・ [送信元ポート] 500
- ・ [あて先アドレス] 10.10.20.1
- ・ [あて先ポート] 500

No.2

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] esp
- ・ [送信元アドレス] 10.10.10.1
- ・ [あて先アドレス] 10.10.20.1

設定後[設定/削除の実行]をクリックします。

4. <IPsec 設定>

設定メニューで「各種サービスの設定」をクリックするとサービス一覧が表示されます。

サービス一覧の左側の「IPsec サーバ」をクリックすると IPsec 設定が表示されます。

画面上部の「本装置の設定」をクリックします。

本装置の設定の中にある「本装置側の設定1」をクリックします。

インターフェースのIPアドレス	10.10.20.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例: @xr.centurysys)

本装置側の設定1で以下の項目を設定します。

- ・ [インタフェースの IP アドレス] 10.10.20.1
- ・ [上位ルータの IP アドレス] %ppp0

設定後[設定の保存]をクリックします。

画面上部の IKE/ISAKMP ポリシーの設定の中の「IKE1」をクリックします。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	NXR
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	
インターフェースのID	(例: @xr.centurysys)
モードの設定	main モード
transform の設定	1番目 group2-aes128-sha1 2番目 使用しない 3番目 使用しない 4番目 使用しない
IKE のライフタイム	10800 秒 (1081~28800秒まで)
DPD の設定	
DPD	☒ 使用する ☐ 使用しない
監視間隔	15 秒 (10~3600秒まで)
リトライ回数	3 (0~80まで)
鍵の設定	
☒ PSKを使用する ☐ RSAを使用する (X509を使用する場合はRSAに設定してください)	ipseckey1

IKE1 で以下の項目を設定します。

- ・ [IKE/ISAKMP ポリシー名] NXR
- ・ [接続する本装置側の設定] 本装置側の設定 1
- ・ [インターフェースの IP アドレス] 10.10.10.1
- ・ [モードの設定] main モード
- ・ [transform の設定] group2-aes128-sha1
- ・ [IKE のライフタイム] 10800 秒
- ・ DPD の設定
 - [DPD] 使用する
 - [監視間隔] 15(秒)
 - [リトライ回数] 3
- ・ [鍵の設定] PSK を使用する
ipseckey1(事前共有鍵)

設定後[設定の保存]をクリックします。

画面上部の IPsec ポリシーの設定の中の「IPsec1」をクリックします。

☒ 使用する ☐ 使用しない ☐ Responderとして使用する ☐ On-Demandで使用する	
使用するIKEポリシー名の選択	NXR (IKE1)
本装置側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	3600 秒 (1081～86400秒まで)
DISTANCE	1 (1～255まで)
送受信パケット切断タイマー	(0～3600まで)

IPsec1 で以下の項目を設定します。

- ・ 使用するを選択
- ・ [使用する IKE ポリシー名の選択] NXR(IKE1)
- ・ [本装置側の LAN 側のネットワークアドレス] 192.168.20.0/24
- ・ [相手側の LAN 側のネットワークアドレス] 192.168.10.0/24
- ・ [PH2 の TransForm の選択] aes128-sha1
- ・ [PFS] 使用する
- ・ [DH Group の選択(PFS 使用時に有効)] group2
- ・ [SA のライフタイム] 3600 秒
- ・ [DISTANCE] 1

設定後[設定の保存]をクリックします。

画面上部の IPsec Keep-Alive 設定をクリックします。

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作Option	interface	backup SA
1	☒	192.168.20.1	192.168.10.1	30	3	60	連動	ipsec0	initiate

IPsec Keepalive で以下の項目を設定します。

Policy No.1

- ・ [enable]有効(チェック有)
- ・ [source address] 192.168.20.1
- ・ [destination address] 192.168.10.1
- ・ [interval(sec)] 30
- ・ [watch count] 3
- ・ [timeout/delay(sec)] 60
- ・ [動作 option] 連動
(👉) 「連動」を選択した場合は IPsec SA 確立後に監視を開始します。
- ・ [interface] ipsec0

設定後[設定/削除の実行]をクリックします。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。

IPsecサーバ	☐ 停止	☒ 起動	停止中	動作変更
----------	--------------------------	-------------------------------------	-----	------

サービス一覧で以下の項目を設定します。

[IPsec サーバ] 起動

設定後[動作変更]をクリックします。

5. <補足>

一部機種では工場出荷状態で DNS リレー/キャッシュ機能を停止しているものがあります。

DNS リレー/キャッシュ機能を起動する場合は以下の設定を行います。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。

DNSキャッシュ	☐ 停止	☒ 起動	停止中	動作変更
----------	--------------------------	-------------------------------------	-----	------

サービス一覧で以下の項目を設定します。

[DNS キャッシュ] 起動

設定後[動作変更]をクリックします。

[XR_B の設定]

1. <インタフェース設定>

設定メニューで「インタフェース設定」をクリックすると Ethernet0 インタフェース設定が表示されます。

Ethernet0ポート [eth0]	☒ 固定アドレスで使用する
	IPアドレス 192.168.30.1
	ネットマスク 255.255.255.0
	MTU 1500
	☐ DHCPサーバから取得
	ホスト名
	MACアドレス
	☐ IPマスカレード(p masq) (このポートで使用するIPアドレスに変換して通信を行います)
	☐ ステータフルパケットインスペクション(spi)
	☐ SPI で DROP したパケットのLOGを取得
	☐ proxy arp
	☐ Directed Broadcast
	☒ Send Redirects
	☒ ICMP AddressMask Requestに回答
	リンク監視 0 秒 (0-30) (リンクダウン時にルーティング情報の配信を停止します)
通信モード ☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M	

Ethernet0 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで選択
- ・ [IP アドレス] 192.168.30.1
- ・ [ネットマスク] 255.255.255.0

設定後[Ethernet 設定の保存]をクリックします。

画面上部の「Ethernet1 の設定」をクリックすると Ethernet1 インタフェース設定が表示されます。

Ethernet1 ポート
[eth1]

☒ 固定アドレスで使用する

IP アドレス 0

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステータスフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet1 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで使用するを選択
- ・ [IP アドレス] 0

設定後[Ethernet 設定の保存]をクリックします。

2 <PPPoE 設定>

設定メニューで「PPP/PPPoE 設定」をクリックすると接続設定が表示されます。

画面上部の「接続先設定 1」をクリックすると接続先設定 1が表示されます。

プロバイダ名

ユーザID test3@centurysys

パスワード test3pass

DNSサーバ

☐ 割り当てられたDNSを使わない

☒ プロバイダから自動割り当て

☐ 手動で設定

プライマリ

セカンダリ

LCPキープアライブ

チェック間隔 30 秒

☐ 回復確認出来なくなると回線を切断します

☐ 0秒を入力するとこの機能は無効になります

Pingによる接続確認

☒ 使用しない ☐ 使用する

使用するホスト

発行間隔は30秒固定、空欄の時はPPP-Gatewayに発行します

UnNumbered-PPP回線使用時に設定できます

IPアドレス

回線接続時に割り付けるグローバルIPアドレスです

PPPoE回線使用時に設定して下さい

MSS設定

☐ 無効 ☒ 有効(256)

MSS値 0 Byte

(有効時のMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1462。ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

PPPoE の接続先で以下の項目を設定します。

- ・ [ユーザ ID] test3@centurysys
- ・ [パスワード] test3pass
- (🔑) ISP から提供されたユーザ ID, パスワードを設定します。
- ・ [DNS サーバ] プロバイダから自動割り当て

- ・ [LCP キープアライブ] 30 秒
- ・ [MSS 設定] 有効
MSS 値 0

設定後[設定の保存]をクリックします。

設定メニューで「PPP/PPPoE 設定」をクリックします。

接続状態	回線は接続されていません
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	☐ RS232C ☐ Ether0 ☒ Ether1
接続形態	☐ 手動接続 ☒ 常時接続
RS232C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
ICMP AddressMask Request	☐ 応答しない ☒ 応答する

PPPoE特設オプション (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	

PPPoE の接続設定で以下の項目を設定します。

- ・ [接続先の選択] 接続先 1
- ・ [接続ポート] Ether1
- ・ [接続形態] 常時接続
- ・ [IP マスカレード] 有効
- ・ [ステートフルパケットインスペクション] 有効
- ・ [デフォルトルートの設定] 有効
- ・ [回線接続時に前回の PPPoE セッションの PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の IPv4Packet 受信時に PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出] 有効(チェック有)

設定後[接続]をクリックします。

(☞) [接続]をクリックすることにより設定の保存を行い、PPP/PPPoE 接続を開始します。

3. <フィルタ設定>

設定メニューで「フィルタ設定」をクリックすると入力フィルタ設定が表示されます。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	udp	10.10.10.1	500		500
2	ppp0	パケット受信時	許可	esp	10.10.10.1			

入力フィルタで以下の項目を設定します。

No.1

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] udp
- ・ [送信元アドレス] 10.10.10.1
- ・ [送信元ポート] 500
- ・ [宛先ポート] 500

No.2

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] esp
- ・ [送信元アドレス] 10.10.10.1

設定後[設定/削除の実行]をクリックします。

4. <IPsec 設定>

設定メニューで「各種サービスの設定」をクリックするとサービス一覧が表示されます。

サービス一覧の左側の「IPsec サーバ」をクリックすると IPsec 設定が表示されます。

画面上部の「本装置の設定」をクリックします。

本装置の設定の中にある「本装置側の設定1」をクリックします。

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

本装置側の設定1で以下の項目を設定します。

- ・ [インターフェースの IP アドレス] %ppp0
- ・ [インターフェースの ID] @xr

設定後[設定の保存]をクリックします。

画面上部の IKE/ISAKMP ポリシーの設定の中の「IKE1」をクリックします。

IKE/ISAKMPの設定	
IKE/ISAKMPポリシー名	NXR
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	
インターフェースのID	(例: @v.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-aes128-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	10800 秒 (1081~28800秒まで)
DPDの設定	
DPD	☒ 使用する ☐ 使用しない
監視間隔	15 秒 (10~3600秒まで)
リトライ回数	3 (0~60まで)
鍵の設定	
☒ PSKを使用する ☐ RSAを使用する (X509を使用する場合はRSAに設定してください)	ipseckey2

IKE1 で以下の項目を設定します。

- ・ [IKE/ISAKMP ポリシー名] NXR
- ・ [接続する本装置側の設定] 本装置側の設定 1
- ・ [インターフェースの IP アドレス] 10.10.10.1
- ・ [モードの設定] aggressive モード
- ・ [transform の設定] group2-aes128-sha1
- ・ [IKE のライフタイム] 10800 秒
- ・ DPD の設定
 - [DPD] 使用する
 - [監視間隔] 15(秒)
 - [リトライ回数] 3
- ・ [鍵の設定] PSK を使用する
ipseckey2(事前共有鍵)

設定後[設定の保存]をクリックします。

画面上部の IPSec ポリシーの設定の中の「IPsec1」をクリックします。

☒ 使用する
 ☐ 使用しない
 ☐ Responderとして使用する
 ☐ On-Demandで使用する

使用するIKEポリシー名の選択: NXR (IKE1)

本装置側のLAN側のネットワークアドレス: 192.168.30.0/24 (例:192.168.0.0/24)

相手側のLAN側のネットワークアドレス: 192.168.10.0/24 (例:192.168.0.0/24)

PH2のTransFormの選択: aes128-sha1

PFS: ☒ 使用する ☐ 使用しない

DH Groupの選択(PFS使用時に有効): group2

SAのライフタイム: 3600 秒 (1081~86400秒まで)

DISTANCE: 1 (1~255まで)

送受信パケット切断タイマー: (0~3600まで)

IPsec1 で以下の項目を設定します。

- ・ 使用するを選択
- ・ [使用する IKE ポリシー名の選択] NXR(IKE1)
- ・ [本装置側の LAN 側のネットワークアドレス] 192.168.30.0/24
- ・ [相手側の LAN 側のネットワークアドレス] 192.168.10.0/24
- ・ [PH2 の TransForm の選択] aes128-sha1
- ・ [PFS] 使用する
- ・ [DH Group の選択(PFS 使用時に有効)] group2
- ・ [SA のライフタイム] 3600 秒
- ・ [DISTANCE] 1

設定後[設定の保存]をクリックします。

画面上部の IPsec Keep-Alive 設定をクリックします。

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作Option*	interface	backup SA
1	☒	192.168.30.1	192.168.10.1	30	3	60	連動	ipsec0	initiate

IPsec Keepalive で以下の項目を設定します。

Policy No.1

- ・ [enable] 有効(チェック有)
- ・ [source address] 192.168.30.1
- ・ [destination address] 192.168.10.1
- ・ [interval(sec)] 30
- ・ [watch count] 3
- ・ [timeout/delay(sec)] 60
- ・ [動作 option] 連動
- ・ [interface] ipsec0

設定後[設定/削除の実行]をクリックします。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。

IPsecサービス
 ☐ 停止
 ☒ 起動
 ☐ 停止中

サービス一覧で以下のように設定します。

[IPsec サーバ] 起動

設定後[動作変更]をクリックします。

5. <補足>

一部機種では工場出荷状態で DNS リレー/キャッシュ機能を停止しているものがあります。

DNS リレー/キャッシュ機能を起動する場合は以下の設定を行います。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。

DNS キャッシュ	☐ 停止	☒ 起動	停止中	動作変更
-----------	--------------------------	-------------------------------------	-----	------

サービス一覧で以下のように設定します。

[DNS キャッシュ] 起動

設定後[動作変更]をクリックします。

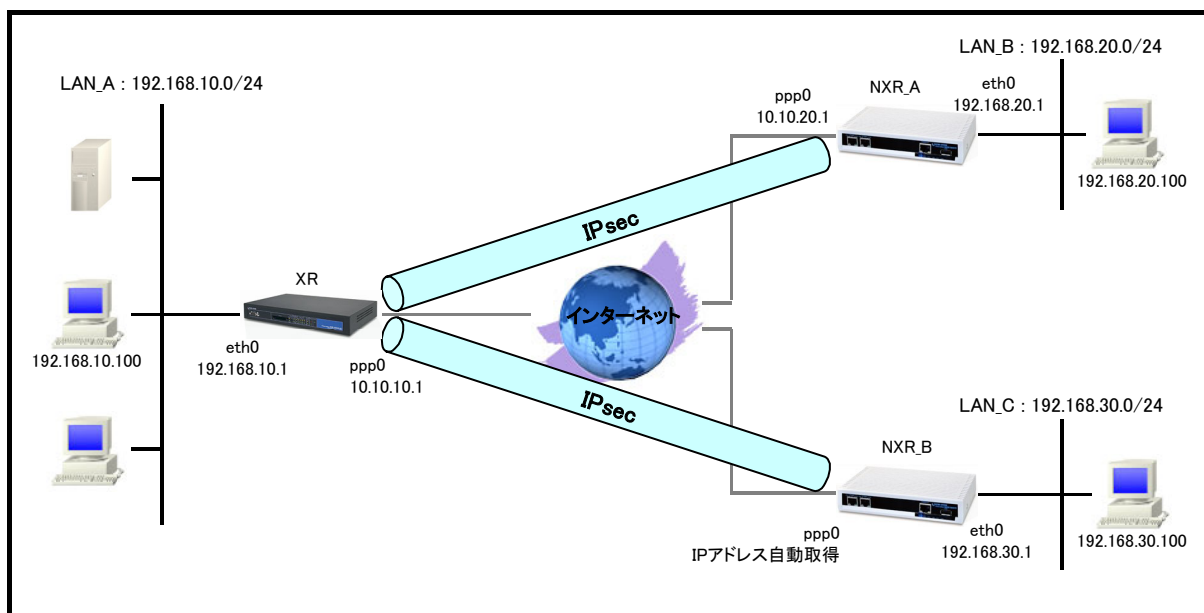
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.100	192.168.20.100	192.168.30.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	192.168.30.1
DNS サーバの IP アドレス	192.168.10.1	192.168.20.1	192.168.30.1

1-2. PPPoE を利用した IPsec 接続設定(センタ XR,拠点 NXR)

PPPoE 接続環境で NXR シリーズーXR シリーズ間で IPsec 接続を行う設定例です。この設定例では XR、NXR_A に WAN 側固定 IP アドレス、NXR_B に WAN 側動的 IP アドレスが割り当てられる環境を想定しています。

【 構成図 】



- ・ この設定例では IPsec の監視方法として NXR では DPD および Ping 監視(ネットワークイベント)、XR では IPsec Keepalive および DPD を設定します。
(👉) XR, NXR で DPD 監視を利用する場合は対向機器も DPD に対応している必要があります。
- ・ この設定例では NXR の IPsec 設定として Route Based IPsec を設定しています。(Policy Based IPsec を利用することも可能です)
- ・ 各拠点にある端末はそれぞれの拠点の NXR, XR からインターネットアクセスを行います。
- ・ この設定例では NXR のシステム LED 設定として ppp0 インタフェースアップ時, track1 のステータスアップ時に LED が点灯するように設定します。

【 設定例 】

〔XR の設定〕

1. <インタフェース設定>

設定メニューで「インタフェース設定」をクリックすると Ethernet0 インタフェース設定が表示されます。

Ethernet0 ポート
[eth0]

☒ 固定アドレスで使用する

IP アドレス 192.168.10.1

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet0 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで使用する
- ・ [IP アドレス] 192.168.10.1
- ・ [ネットマスク] 255.255.255.0

設定後[Ethernet 設定の保存]をクリックします。

画面上部の「Ethernet1 の設定」をクリックすると Ethernet1 インタフェース設定が表示されます。

Ethernet1 ポート
[eth1]

☒ 固定アドレスで使用する

IP アドレス 0

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet1 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで使用する
- ・ [IP アドレス] 0

設定後[Ethernet 設定の保存]をクリックします。

2 <PPPoE 設定>

設定メニューで「PPP/PPPoE 設定」をクリックすると接続設定が表示されます。

画面上部の「接続先設定 1」をクリックすると接続先設定 1が表示されます。

プロバイダ名	
ユーザID	test1@centurysys
パスワード	test1pass
DNSサーバ	☐ 割り当てられたDNSを使わない ☒ プロバイダから自動割り当て ☐ 手動で設定 プライマリ セカンダリ
LCPキープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	☒ 使用しない ☐ 使用する 使用するホスト 発行間隔は30秒固定、空欄の時はPAP-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	☐ 無効 ☒ 有効(強制) MSS値 0 Byte (有効時にMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は4092、ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

PPPoE の接続先で以下の項目を設定します。

- ・ [ユーザ ID] test1@centurysys
- ・ [パスワード] test1pass
(🔑) ISP から提供されたユーザ ID, パスワードを設定します。
- ・ [DNS サーバ] プロバイダから自動割り当て
- ・ [LCP キープアライブ] 30 秒
- ・ [MSS 設定] 有効
MSS 値 0

設定後[設定の保存]をクリックします。

設定メニューで「PPP/PPPoE 設定」をクリックします。

回線状態	回線は接続されていません				
接続先の選択	☒ 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	☐ RS232C	☐ Ether0	☒ Ether1		
接続形態	☐ 手動接続	☒ 常時接続			
RS232C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			
ICMP AddressMask Request	☐ 応答しない	☒ 応答する			
PPPoE特殊オプション (全回線共通)	☒ 回線接続時に前回のPPPoEセッションのPADTを強制送出 ☒ 非接続SessionのIPv4Packet受信時 PADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時 PADTを強制送出				

PPPoE の接続設定で以下の項目を設定します。

- ・ [接続先の選択] 接続先 1
- ・ [接続ポート] Ether1
- ・ [接続形態] 常時接続
- ・ [IP マスカレード] 有効
- ・ [ステートフルパケットインスペクション] 有効
- ・ [デフォルトルートの設定] 有効
- ・ [回線接続時に前回の PPPoE セッションの PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の IPv4Packet 受信時に PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出] 有効(チェック有)

設定後[接続]をクリックします。

(☞) [接続]をクリックすることにより設定の保存を行い、PPP/PPPoE 接続を開始します。

3. <フィルタ設定>

設定メニューで「フィルタ設定」をクリックすると入力フィルタ設定が表示されます。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	udp		500	10.10.10.1	500
2	ppp0	パケット受信時	許可	esp			10.10.10.1	

入力フィルタで以下の項目を設定します。

No.1

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] udp
- ・ [送信元ポート] 500
- ・ [あて先アドレス] 10.10.10.1
- ・ [あて先ポート] 500

No.2

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] esp
- ・ [あて先アドレス] 10.10.10.1

設定後[設定/削除の実行]をクリックします。

4. <IPsec 設定>

設定メニューで「各種サービスの設定」をクリックするとサービス一覧が表示されます。

サービス一覧の左側の「IPsec サーバ」をクリックすると IPsec 設定が表示されます。

画面上部の「本装置の設定」をクリックします。

本装置の設定の中にある「本装置側の設定1」をクリックします。

インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例: @vrcenturyvs)

本装置側の設定1で以下の項目を設定します。

- ・ [インタフェースの IP アドレス] 10.10.10.1
- ・ [上位ルータの IP アドレス] %ppp0

設定後[設定の保存]をクリックします。

画面上部の IKE/ISAKMP ポリシーの設定の中の「IKE1」をクリックします。

IKE/ISAKMPの設定	
IKE/ISAKMPポリシー名	NXR_A
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	10.10.20.1
上位ルータのIPアドレス	
インターフェースのID	(例: @centurysys)
モードの設定	main モード
transformの設定	1番目 group2-aes128-sha1 2番目 使用しない 3番目 使用しない 4番目 使用しない
IKEのライフタイム	10800 秒 (1081~28800秒まで)
DPDの設定	
DPD	☒ 使用する ☐ 使用しない
監視間隔	15 秒 (10~3600秒まで)
リトライ回数	3 (0~60まで)
鍵の設定	
☒ PSKを使用する ☐ RSAを使用する (RSAを使用する場合はRSAを設定してください)	ipseckey1

IKE1 で以下の項目を設定します。

- ・ [IKE/ISAKMP ポリシー名] NXR_A
- ・ [接続する本装置側の設定] 本装置側の設定 1
- ・ [インターフェースの IP アドレス] 10.10.20.1
- ・ [モードの設定] main モード
- ・ [transform の設定] group2-aes128-sha1
- ・ [IKE のライフタイム] 10800 秒
- ・ DPD の設定
 - [DPD] 使用する
 - [監視間隔] 15(秒)
 - [リトライ回数] 3
- ・ [鍵の設定] PSK を使用する
ipseckey1(事前共有鍵)

設定後[設定の保存]をクリックします。

画面上部の IPSec ポリシーの設定の中の「IPsec1」をクリックします。

☒ 使用する ☐ 使用しない ☐ Responderとして使用する ☐ On-Demandで使用する	
使用するIKEポリシー名の選択	NXR_A (IKE1)
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	3600 秒 (1001～86400秒まで)
DISTANCE	1 (1～255まで)
送受信 パケット切断タイマー	(0～3600まで)

IPsec1 で以下の項目を設定します。

- ・ 使用するを選択
- ・ [使用する IKE ポリシー名の選択] NXR_A(IKE1)
- ・ [本装置側の LAN 側のネットワークアドレス] 192.168.10.0/24
- ・ [相手側の LAN 側のネットワークアドレス] 192.168.20.0/24
- ・ [PH2 の TransForm の選択] aes128-sha1
- ・ [PFS] 使用する
- ・ [DH Group の選択(PFS 使用時に有効)] group2
- ・ [SA のライフタイム] 3600 秒
- ・ [DISTANCE] 1

設定後[設定の保存]をクリックします。

画面上部の IKE/ISAKMP ポリシーの設定の中の「IKE2」をクリックします。

IKE/ISAKMPの設定	
IKE/ISAKMPポリシー名	NXR_B
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェースのID	@nxr (例:@xrcenturysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-aes128-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	10800 秒 (1081~28800秒まで)
DPDの設定	
DPD	☒ 使用する ☐ 使用しない
監視間隔	15 秒 (10~3600秒まで)
リトライ回数	3 (0~60まで)
鍵の設定	
☒ PSKを使用する (X509を使用する場合はRSAに設定してください)	ipseckey2
☐ RSAを使用する	

IKE2 で以下の項目を設定します。

- ・ [IKE/ISAKMP ポリシー名] NXR_B
- ・ [接続する本装置側の設定] 本装置側の設定 1
- ・ [インターフェースの IP アドレス] 0.0.0.0
- ・ [インターフェースの ID] @nxr
- ・ [モードの設定] aggressive モード
- ・ [transform の設定] group2-aes128-sha1
- ・ [IKE のライフタイム] 10800 秒
- ・ DPD の設定
 - [DPD] 使用する
 - [監視間隔] 15(秒)
 - [リトライ回数] 3
- ・ [鍵の設定] PSK を使用する
ipseckey2(事前共有鍵)

設定後[設定の保存]をクリックします。

画面上部の IPSec ポリシーの設定の中の「IPsec2」をクリックします。

☐ 使用する ☐ 使用しない ☒ Responderとして使用する ☐ On-Demandで使用する	
使用するIKEポリシー名の選択	NXR_B (IKE2)
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.30.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	group2
SAのライフタイム	3600 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)
送受信 パケット切断タイマー	(0~3600まで)

IPsec2 で以下の項目を設定します。

- Responder として使用するを選択
- [使用する IKE ポリシー名の選択] NXR_B(IKE2)
- [本装置側の LAN 側のネットワークアドレス] 192.168.10.0/24
- [相手側の LAN 側のネットワークアドレス] 192.168.30.0/24
- [PH2 の TransForm の選択] aes128-sha1
- [PFS] 使用する
- [DH Group の選択(PFS 使用時に有効)] group2
- [SA のライフタイム] 3600 秒
- [DISTANCE] 1

設定後[設定の保存]をクリックします。

画面上部の IPsec Keep-Alive 設定をクリックします。

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作Option*	interface
1	☒	192.168.10.1	192.168.20.1	30	3	60	連動	ipsec0
2	☒	192.168.10.1	192.168.20.1	30	3	60	連動	ipsec0

IPsec Keepalive で以下の項目を設定します。

Policy No.1

- [enable] 有効(チェック有)
- [source address] 192.168.10.1
- [destination address] 192.168.20.1
- [interval(sec)] 30
- [watch count] 3
- [timeout/delay(sec)] 60
- [動作 option] 連動
- [interface] ipsec0

Policy No.2

- [enable] 有効(チェック有)
- [source address] 192.168.10.1
- [destination address] 192.168.30.1
- [interval(sec)] 30
- [watch count] 3
- [timeout/delay(sec)] 60
- [動作 option] 連動
- [interface] ipsec0

設定後[設定/削除の実行]をクリックします。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。

IPsecサー	☐ 停止 ☒ 起動 ☐ 停止中 動作変更
---------	--

サービス一覧で以下のように設定します。

[IPsec サーバ] 起動

設定後[動作変更]をクリックします。

5. <補足>

一部機種では工場出荷状態で DNS リレー/キャッシュ機能を停止しているものがあります。

DNS リレー/キャッシュ機能を起動する場合は以下の設定を行います。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。



サービス一覧で以下のように設定します。

[DNS キャッシュ] 起動

設定後[動作変更]をクリックします。

[NXR_A の設定]

```

nxr120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.20.1/24
NXR_A(config-if)#ip access-linkdown
NXR_A(config-if)#exit
NXR_A(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 udp 500 500
NXR_A(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 50
NXR_A(config)#ipsec access-list LAN_A ip 192.168.20.0/24 192.168.10.0/24
NXR_A(config)#ip route 192.168.10.0/24 tunnel 1
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#track 1 ip reachability 192.168.10.1 interface tunnel 1 10 2 delay 61
NXR_A(config)#ipsec local policy 1
NXR_A(config-ipsec-local)#address ip
NXR_A(config-ipsec-local)#exit
NXR_A(config)#ipsec isakmp policy 1
NXR_A(config-ipsec-isakmp)#description XR
NXR_A(config-ipsec-isakmp)#authentication pre-share ipseckey1
NXR_A(config-ipsec-isakmp)#hash sha1
NXR_A(config-ipsec-isakmp)#encryption aes128
NXR_A(config-ipsec-isakmp)#group 2
NXR_A(config-ipsec-isakmp)#lifetime 10800
NXR_A(config-ipsec-isakmp)#isakmp-mode main
NXR_A(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_A(config-ipsec-isakmp)#keepalive 15 3 periodic restart
NXR_A(config-ipsec-isakmp)#local policy 1
NXR_A(config-ipsec-isakmp)#netevent 1 reconnect
NXR_A(config-ipsec-isakmp)#exit
NXR_A(config)#ipsec tunnel policy 1
NXR_A(config-ipsec-tunnel)#description XR
NXR_A(config-ipsec-tunnel)#negotiation-mode auto
NXR_A(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_A(config-ipsec-tunnel)#set pfs group2
NXR_A(config-ipsec-tunnel)#set sa lifetime 3600
NXR_A(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_A(config-ipsec-tunnel)#match address LAN_A

```

----- 次のページに続きます -----

----- 前のページからの続きです -----

```

NXR_A(config-ipsec-tunnel)#exit
NXR_A(config)#interface tunnel 1
NXR_A(config-tunnel)#tunnel mode ipsec ipv4
NXR_A(config-tunnel)#tunnel protection ipsec policy 1
NXR_A(config-tunnel)#ip tcp adjust-mss auto
NXR_A(config-tunnel)#exit
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.20.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp authentication auto
NXR_A(config-ppp)#ppp username test2@centurysys password test2pass
NXR_A(config-ppp)#ipsec policy 1
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#system led aux 1 interface ppp 0
NXR_A(config)#system led aux 2 track 1
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#exit
NXR_A#save config

```

NXR の設定に関しましてはご利用頂いている NXR のユーザーズガイド(CLI 版)および FutureNetNXR 設定例集 IPsec 編をご参照ください。

なお以下は XR と IPsec 接続する上での注意事項となります。

NXR の工場出荷状態ではリンクダウンしているインタフェースへの通信はできません。

そのため XR 側で IPsec Keepalive を設定し、かつその宛先 IP アドレスが NXR の LAN 側 IP アドレスの場合、NXR の LAN 側インタフェースがリンクダウンしていると XR で IPsec SA 確立→IPsec Keepalive で障害検知→IPsec SA 確立・・・を繰り返してしまいます。そのため NXR で当該リンクダウン状態でも通信可能にするため以下のコマンドを LAN 側インタフェースに設定します。

1. <LAN 側(ethernet0)インタフェース設定>

```
NXR_A(config-if)#ip access-linkdown
```

リンクダウン状態でも、LAN 側(ethernet0)インタフェースの IP アドレスに対して通信ができるよう設定します。

またこの設定では Ping 監視およびネットワークイベントを設定します。

2. <トラック設定(Ping 監視)>

```
NXR_A(config-if)#track 1 ip reachability 192.168.10.1 interface tunnel 1 10 2 delay 61
```

送信間隔 10 秒で 2 回リトライを行い、応答が得られない場合はダウンに状態遷移します。

ダウン→アップへの状態遷移は Ping による応答確認ができた場合となります。

よって Ping による応答確認ができない(ICMP Echo Reply が無い)場合はダウン状態のままとなります。

ここでは delay も合わせて設定します。delay は復旧時(track のステータス状態がアップ)から実際にアップ時の動作を実行するまでの遅延時間を設定します。

delay タイマが動作している場合はダウン状態が維持され、この間も Ping 監視は行われます。なお delay タイマ中にダウンイベントを検知した場合は、delay タイマはキャンセルされます。

そして delay タイマがタイムアウトするとイベントアップとなります。このとき delay タイマ中にカウントした Ping 監視の失敗回数は 0 にクリアされ、再度 Ping 監視が開始されます。

(🔧) delay タイマがタイムアウトした場合は、netevent コマンドで指定した動作が実行されます。

3. <IPsec ISAKMP ポリシー設定 1>

```
NXR_A(config-if)#netevent 1 reconnect
```

track 1 コマンドで指定した Ping 監視で障害を検知した場合、IPsec トンネルの再接続を行う動作を指定します。

その他 NXR の詳細設定に関しましては、ご利用頂いている NXR のユーザズガイド(CLI 版)および FutureNetNXR 設定例集 IPsec 編をご参照ください。

4. <システム LED 設定>

```
NXR_A(config)#system led aux 1 interface ppp 0
```

ここでは ppp0 インタフェースの回線接続時に、AUX LED1 が点灯するように設定します。

```
NXR_A(config)#system led aux 2 track 1
```

ここでは track1 で設定した Ping 監視が OK(status is up)の時に、AUX LED2 が点灯するように設定します。

[NXR_B の設定]

```
nxr120#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.30.1/24
NXR_B(config-if)#ip access-linkdown
NXR_B(config-if)#exit
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any udp 500 500
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any 50
NXR_B(config)#ipsec access-list LAN_A ip 192.168.30.0/24 192.168.10.0/24
NXR_B(config)#ip route 192.168.10.0/24 tunnel 1
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#track 1 ip reachability 192.168.10.1 interface tunnel 1 10 2 delay 61
NXR_B(config)#ipsec local policy 1
NXR_B(config-ipsec-local)#address ip
NXR_B(config-ipsec-local)#self-identity fqdn nxr
NXR_B(config-ipsec-local)#exit
NXR_B(config)#ipsec isakmp policy 1
NXR_B(config-ipsec-isakmp)#description XR
NXR_B(config-ipsec-isakmp)#authentication pre-share ipseckey2
NXR_B(config-ipsec-isakmp)#hash sha1
NXR_B(config-ipsec-isakmp)#encryption aes128
NXR_B(config-ipsec-isakmp)#group 2
NXR_B(config-ipsec-isakmp)#lifetime 10800
NXR_B(config-ipsec-isakmp)#isakmp-mode aggressive
NXR_B(config-ipsec-isakmp)#remote address ip 10.10.10.1
NXR_B(config-ipsec-isakmp)#keepalive 15 3 periodic restart
NXR_B(config-ipsec-isakmp)#local policy 1
NXR_B(config-ipsec-isakmp)#netevent 1 reconnect
NXR_B(config-ipsec-isakmp)#exit
NXR_B(config)#ipsec tunnel policy 1
NXR_B(config-ipsec-tunnel)#description XR
```

——— 次のページに続きがあります ———

——— 前のページからの続きです ———

```

NXR_B(config-ipsec-tunnel)#negotiation-mode auto
NXR_B(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR_B(config-ipsec-tunnel)#set pfs group2
NXR_B(config-ipsec-tunnel)#set sa lifetime 3600
NXR_B(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR_B(config-ipsec-tunnel)#match address LAN_A
NXR_B(config-ipsec-tunnel)#exit
NXR_B(config)#interface tunnel 1
NXR_B(config-tunnel)#tunnel mode ipsec ipv4
NXR_B(config-tunnel)#tunnel protection ipsec policy 1
NXR_B(config-tunnel)#exit
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp authentication auto
NXR_B(config-ppp)#ppp username test3@centurysys password test3pass
NXR_B(config-ppp)#ipsec policy 1
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#system led aux 1 interface ppp 0
NXR_B(config)#system led aux 2 track 1
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#exit
NXR_B#save config

```

NXR_B の設定に関しましては NXR_A の設定、またはご利用頂いている NXR のユーザズガイド(CLI 版)および FutureNetNXR 設定例集 IPsec 編をご参照ください。

【 パソコンの設定例 】

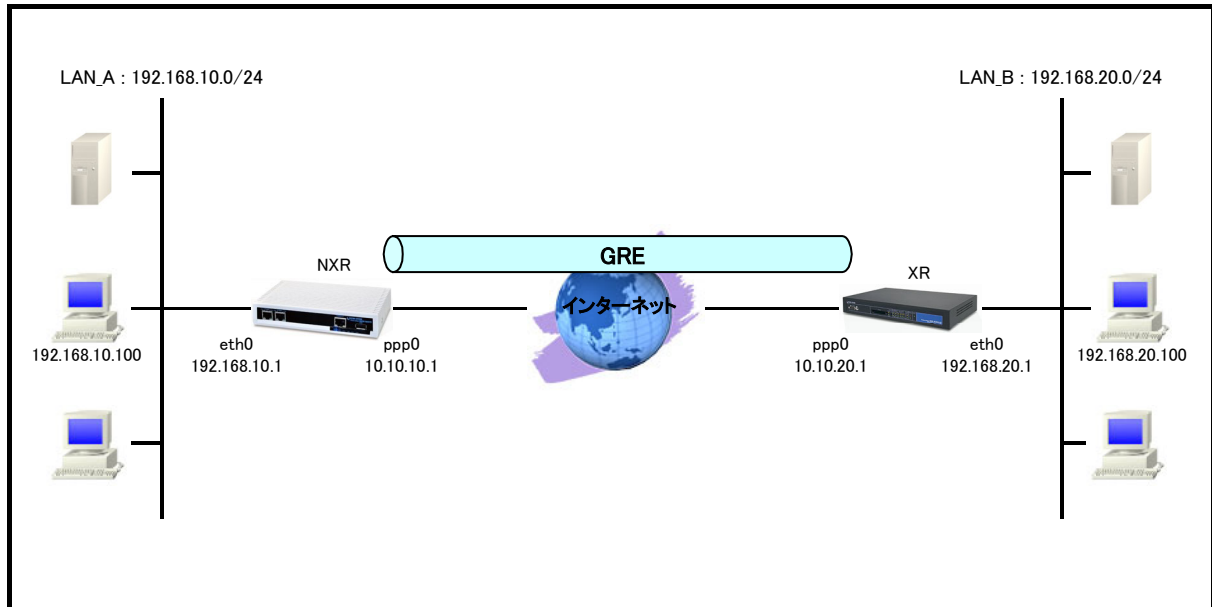
	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.100	192.168.20.100	192.168.30.100
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1	192.168.30.1
DNS サーバの IP アドレス	192.168.10.1	192.168.20.1	192.168.30.1

2. GRE 設定

2-1. PPPoE を利用した GRE 接続設定

PPPoE 接続環境で NXR シリーズーXR シリーズ間で GRE 接続を行う設定例です。

【 構成図 】



- ・ GRE で拠点間通信する場合は、拠点に設置したルータの WAN 側 IP アドレスは固定 IP アドレスが必要になります。
- ・ 各拠点にある端末はそれぞれの拠点の NXR, XR からインターネットアクセスを行います。
- ・ この設定例では NXR のシステム LED 設定として ppp0 インタフェース, トンネルインタフェースアップ時に LED が点灯するように設定します。

【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip access-list ppp0_in permit 10.10.20.1 10.10.10.1 47
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys password test1pass
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#interface tunnel 1
NXR(config-tunnel)#tunnel mode gre
NXR(config-tunnel)#description XR
NXR(config-tunnel)#ip address 172.16.10.1/30
NXR(config-tunnel)#mtu 1430
NXR(config-tunnel)#ip tcp adjust-mss auto
NXR(config-tunnel)#no ip redirects
NXR(config-tunnel)#tunnel source 10.10.10.1
NXR(config-tunnel)#tunnel destination 10.10.20.1
NXR(config-tunnel)#tunnel ttl 255
NXR(config-tunnel)#exit
NXR(config)#ip route 10.10.20.1/32 ppp 0
NXR(config)#ip route 192.168.20.0/24 tunnel 1
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#system led aux 1 interface ppp 0
NXR(config)#system led aux 2 interface tunnel 1
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#exit
NXR#save config
```

NXR の設定に関しましてはご利用頂いている NXR のユーザーズガイド(CLI 版)および FutureNetNXR 設定例集 GRE,IPinIP 編をご参照ください。

なおこの設定では以下のシステム LED を設定します。

1. <システム LED 設定>

```
NXR(config)#system led aux 1 interface ppp 0
```

ppp0 インタフェースの回線接続時に、AUX LED1 が点灯するように設定します。

```
NXR(config)#system led aux 2 interface tunnel 1
```

tunnel1 インタフェースアップ時に、AUX LED1 が点灯するように設定します。

〔XR の設定〕

1. <インタフェース設定>

設定メニューで「インタフェース設定」をクリックすると Ethernet0 インタフェース設定が表示されます。

Ethernet0 ポート
[eth0]

☒ 固定アドレスで使用する

IP アドレス 192.168.20.1

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステータスフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet0 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで選択
- ・ [IP アドレス] 192.168.20.1
- ・ [ネットマスク] 255.255.255.0

設定後[Ethernet 設定の保存]をクリックします。

画面上部の「Ethernet1 の設定」をクリックすると Ethernet1 インタフェース設定が表示されます。

Ethernet1 ポート
[eth1]

☒ 固定アドレスで使用する

IP アドレス 0

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステータスフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet1 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで選択
- ・ [IP アドレス] 0

設定後[Ethernet 設定の保存]をクリックします。

2 <PPPoE 設定>

設定メニューで「PPP/PPPoE 設定」をクリックすると接続設定が表示されます。

画面上部の「接続先設定 1」をクリックすると接続先設定1が表示されます。

プロバイダ名	
ユーザID	test2@centurysys
パスワード	test2pass
DNSサーバ	☐ 割り当てられたDNSを使わない ☒ プロバイダから自動割り当て ☐ 手動で設定 プライマリ セカンダリ
LCPキープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	☒ 使用しない ☐ 使用する 使用するホスト 発行間隔は30秒固定、空欄の時はPDP-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	☐ 無効 ☒ 有効(強制) MSS値 0 Byte (有効時にMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1452、ACLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

PPPoE の接続先で以下の項目を設定します。

- ・ [ユーザ ID] test2@centurysys
- ・ [パスワード] test2pass
(🔑) ISP から提供されたユーザ ID、パスワードを設定します。
- ・ [DNS サーバ] プロバイダから自動割り当て
- ・ [LCP キープアライブ] 30 秒
- ・ [MSS 設定] 有効
MSS 値 0

設定後[設定の保存]をクリックします。

設定メニューで「PPP/PPPoE 設定」をクリックします。

回線状態	回線は接続されていません				
接続先の選択	☒ 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	☐ RS232C	☐ Ether0	☒ Ether1		
接続形態	☐ 手動接続	☒ 常時接続			
RS232C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			
ICMP AddressMask Request	☐ 応答しない	☒ 応答する			
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				

PPPoE の接続設定で以下の項目を設定します。

- ・ [接続先の選択] 接続先 1
- ・ [接続ポート] Ether1

- ・ [接続形態] 常時接続
- ・ [IP マスカレード] 有効
- ・ [ステートフルパケットインスペクション] 有効
- ・ [デフォルトルートの設定] 有効
- ・ [回線接続時に前回の PPPoE セッションの PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の IPv4Packet 受信時に PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出] 有効(チェック有)

設定後[接続]をクリックします。

(☞) [接続]をクリックすることにより設定の保存を行い、PPP/PPPoE 接続を開始します。

3. <フィルタ設定>

設定メニューで「フィルタ設定」をクリックすると入力フィルタ設定が表示されます。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	gre	10.10.10.1		10.10.20.1	

入力フィルタで以下の項目を設定します。

No.1

- ・ [インターフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] gre
- ・ [送信元アドレス] 10.10.10.1
- ・ [あて先アドレス] 10.10.20.1

設定後[設定/削除の実行]をクリックします。

4. <GRE 設定>

設定メニューで「GRE 設定」をクリックすると GRE の一覧が表示されます。

画面上部の GRE インターフェース設定の「GRE1」をクリックします。

インタフェースアドレス	172.16.10.2/30 (例:192.168.0.1/30)
リモート(宛先)アドレス	10.10.10.1 (例:192.168.1.1)
ローカル(送信元)アドレス	10.10.20.1 (例:192.168.2.1)
PEERアドレス	172.16.10.1/30 (例:192.168.0.2/30)
TTL	255 (1-255)
MTU	1430 (最大値 1500)
Path MTU Discovery	☒ 有効 ☐ 無効
ICMP AddressMask Request	☒ 応答する ☐ 応答しない
TOS設定 (ECN Field設定不可)	☒ TOS値の指定 ☐ inherit(TOS値のコピー) TOS値: 0 (0x0-0xff)
GREoverIPSec	☐ 使用する ipsec 0 ☒ Routing Tableに依存
IDキーの設定	0 (0-4294967295)
GRE KeepAlive	☐ 有効 ☒ 無効 Interval 10 秒 Retry 3 回
End-to-End Checksumming	☐ 有効 ☒ 無効
MSS設定	☒ 有効 ☐ 無効 MSS値 0 Byte (有効時にMSS値が0の場合は、MSS値を自動設定(Clamp MSS to MTU)します。)

GRE1で以下の項目を設定します。

- ・ [インタフェースアドレス] 172.16.10.2/30
- ・ [リモート(宛先)IP アドレス] 10.10.10.1
- ・ [ローカル(送信元)IP アドレス] 10.10.20.1
- ・ [PEER アドレス] 172.16.10.1/30
- ・ [TTL] 255
- ・ [MTU] 1430
- ・ [Path MTU Discovery] 有効
- ・ [MSS 設定] 有効
- ・ MSS 値 0

設定後[追加/変更]をクリックします。

5. <スタティックルート設定>

設定メニューで「スタティックルート設定」をクリックするとスタティックルート設定が表示されます。

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>
1	10.10.10.1	255.255.255.255	ppp0	1
2	192.168.10.0	255.255.255.0	gre1	1

スタティックルート設定で以下の項目を設定します。

No.1

- ・ [アドレス] 10.10.10.1
- ・ [ネットマスク] 255.255.255.255
- ・ [インタフェース/ゲートウェイ] ppp0
- ・ [ディスタンス] 1

No.2

- ・ [アドレス] 192.168.10.0
- ・ [ネットマスク] 255.255.255.0
- ・ [インタフェース/ゲートウェイ] gre1
- ・ [ディスタンス] 1

設定後[設定/削除の実行]をクリックします。

6. <補足>

一部機種では工場出荷状態で DNS リレー/キャッシュ機能を停止しているものがあります。

DNS リレー/キャッシュ機能を起動する場合は以下の設定を行います。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。



サービス一覧で以下のように設定します。

[DNS キャッシュ] 起動

設定後[動作変更]をクリックします。

【 パソコンの設定例 】

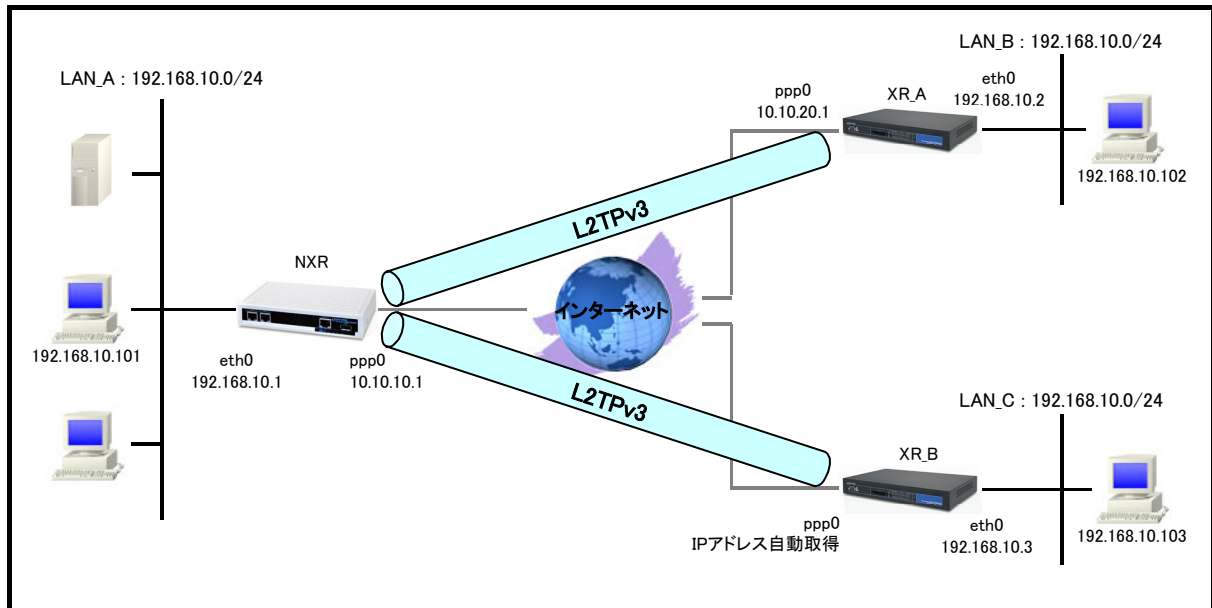
	LAN A のパソコン	LAN B のパソコン
IP アドレス	192.168.10.100	192.168.20.100
サブネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.20.1
DNS サーバの IP アドレス	192.168.10.1	192.168.20.1

3. L2TPv3 設定

3-1. PPPoE を利用した L2TPv3 接続設定(センタ NXR,拠点 XR)

PPPoE 接続環境で NXR シリーズーXR シリーズ間で L2TPv3 接続を行う設定例です。この設定例では NXR、XR_A に WAN 側固定 IP アドレス、XR_B に WAN 側動的 IP アドレスが割り当てられる環境を想定しています。

【 構成図 】



- ・ この設定例では L2TPv3 接続時の Vendor ID 設定として IETF を指定します。
- ・ この設定例では Ethernet0 インタフェースを L2TPv3 の Xconnect インタフェースに設定します。
- ・ XR 配下のネットワークは NXR を経由して通信することが可能です。
- ・ 各拠点にある端末はそれぞれの拠点の NXR, XR からインターネットアクセスを行います。

【 設定例 】

```
nrx120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nrx120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 115
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys password test1pass
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#l2tpv3 hostname nrx
NXR(config)#l2tpv3 router-id 172.20.10.1
NXR(config)#l2tpv3 mac-learning
NXR(config)#l2tpv3 mac-aging 300
NXR(config)#l2tpv3 path-mtu-discovery
NXR(config)#l2tpv3 tunnel 1
NXR(config-l2tpv3-tunnel)#description XR_A
NXR(config-l2tpv3-tunnel)#tunnel address 10.10.20.1
NXR(config-l2tpv3-tunnel)#tunnel hostname xra
NXR(config-l2tpv3-tunnel)#tunnel router-id 172.20.20.1
NXR(config-l2tpv3-tunnel)#tunnel vendor ietf
NXR(config-l2tpv3-tunnel)#exit
NXR(config)#l2tpv3 xconnect 1
NXR(config-l2tpv3-xconnect)#description XR_A
NXR(config-l2tpv3-xconnect)#tunnel 1
NXR(config-l2tpv3-xconnect)#xconnect ethernet 0
NXR(config-l2tpv3-xconnect)#xconnect end-id 1
NXR(config-l2tpv3-xconnect)#retry-interval 30
NXR(config-l2tpv3-xconnect)#ip tcp adjust-mss auto
NXR(config-l2tpv3-xconnect)#exit
NXR(config)#l2tpv3 tunnel 2
NXR(config-l2tpv3-tunnel)#description XR_B
NXR(config-l2tpv3-tunnel)#tunnel hostname xrb
NXR(config-l2tpv3-tunnel)#tunnel router-id 172.20.30.1
NXR(config-l2tpv3-tunnel)#tunnel vendor ietf
NXR(config-l2tpv3-tunnel)#exit
NXR(config)#l2tpv3 xconnect 2
NXR(config-l2tpv3-xconnect)#description XR_B
NXR(config-l2tpv3-xconnect)#tunnel 2
NXR(config-l2tpv3-xconnect)#xconnect ethernet 0
NXR(config-l2tpv3-xconnect)#xconnect end-id 1
NXR(config-l2tpv3-xconnect)#ip tcp adjust-mss auto
NXR(config-l2tpv3-xconnect)#exit
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#exit
NXR#save config
```

NXR の設定に関しましてはご利用頂いている NXR 製品のユーザーズガイド(CLI 版)および FutureNetNXR 設定例集 L2TPv3 編をご参照ください。

〔XR_A の設定〕

1. <インタフェース設定>

設定メニューで「インタフェース設定」をクリックすると Ethernet0 インタフェース設定が表示されます。

Ethernet 0 ポート
[eth0]

☒ 固定アドレスで使用する
☐ DHCPサーバから取得

IP アドレス 192.168.10.2
ネットマスク 255.255.255.0
MTU 1500

ホスト名
MACアドレス

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

☐ ステータスフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

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

Ethernet0 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで選択
- ・ [IP アドレス] 192.168.10.2
- ・ [ネットマスク] 255.255.255.0

設定後[Ethernet 設定の保存]をクリックします。

画面上部の「Ethernet1 の設定」をクリックすると Ethernet1 インタフェース設定が表示されます。

Ethernet 1 ポート
[eth1]

☒ 固定アドレスで使用する
☐ DHCPサーバから取得

IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500

ホスト名
MACアドレス

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

☐ ステータスフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

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

Ethernet1 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで選択
- ・ [IP アドレス] 0

設定後[Ethernet 設定の保存]をクリックします。

2 <PPPoE 設定>

設定メニューで「PPP/PPPoE 設定」をクリックすると接続設定が表示されます。

画面上部の「接続先設定 1」をクリックすると接続先設定 1 が表示されます。

プロバイダ名	
ユーザID	test2@centurysys
パスワード	test2pass
DNSサーバ	☐ 割り当てられたDNSを使わない ☒ プロバイダから自動割り当て ☐ 手動で設定 プライマリ セカンダリ
LCPキープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	☒ 使用しない ☐ 使用する 使用するホスト 発行間隔は30秒固定、空欄の時はPPP-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	☐ 無効 ☒ 有効(255) MSS値 0 Byte (有効時にMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1452、ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

PPPoE の接続先で以下の項目を設定します。

- ・ [ユーザ ID] test2@centurysys
- ・ [パスワード] test2pass
(🔑) ISP から提供されたユーザ ID, パスワードを設定します。
- ・ [DNS サーバ] プロバイダから自動割り当て
- ・ [LCP キープアライブ] 30 秒
- ・ [MSS 設定] 有効
MSS 値 0

設定後[設定の保存]をクリックします。

設定メニューで「PPP/PPPoE 設定」をクリックします。

回線状態	回線は接続されていません				
接続先の選択	☒ 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	☐ RS232C	☐ Ether0	☒ Ether1		
接続形態	☐ 手動接続	☒ 常時接続			
RS232C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			
ICMP AddressMask Request	☐ 応答しない	☒ 応答する			

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

PPPoE の接続設定で以下の項目を設定します。

- ・ [接続先の選択] 接続先 1
- ・ [接続ポート] Ether1
- ・ [接続形態] 常時接続
- ・ [IP マスカレード] 有効
- ・ [ステートフルパケットインスペクション] 有効
- ・ [デフォルトルートの設定] 有効
- ・ [回線接続時に前回の PPPoE セッションの PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の IPv4Packet 受信時に PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出] 有効(チェック有)

設定後[接続]をクリックします。

(☞) [接続]をクリックすることにより設定の保存を行い、PPP/PPPoE 接続を開始します。

3. <フィルタ設定>

設定メニューで「フィルタ設定」をクリックすると入力フィルタ設定が表示されます。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	l2tp	10.10.10.1		10.10.20.1	

入力フィルタで以下の項目を設定します。

No.1

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] l2tp
- ・ [送信元アドレス] 10.10.10.1
- ・ [あて先アドレス] 10.10.20.1

設定後[設定/削除の実行]をクリックします。

4. <L2TPv3 設定>

設定メニューで「各種サービスの設定」をクリックするとサービス一覧が表示されます。

サービス一覧の左側の「L2TPv3」をクリックすると L2TPv3 機能設定が表示されます。

Local hostname	xra
Local Router-ID	172.20.20.1
MAD Address学習機能	☒ 有効 ☐ 無効
MAD Address Aging Time	300 (30-1000sec)
Loop Detection設定	☐ 有効 ☒ 無効
Known Unicast設定	☐ 送信する ☒ 送信しない
PMTU Discovery設定	☒ 有効 ☐ 無効
受信ポート番号(over LDP)	1701 (default 1701)
PMTU Discovery設定(over LDP)	☒ 有効 ☐ 無効
SNMP機能設定	☐ 有効 ☒ 無効
SNMP Trap機能設定	☐ 有効 ☒ 無効
Debug設定 (Systemメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☒ L2TPエラーメッセージ出力

L2TPv3 機能設定で以下の項目を設定します。

- [Local hostname] xra
- [Local Router-ID] 172.20.20.1

設定後[設定]をクリックします。

画面上部の L2TPv3 Tunnel 設定をクリックし、「New Entry」をクリックします。

Description	NXR
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 Hiding設定	☐ 有効 ☒ 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	nrx
Remote RouterID設定	172.20.10.1
Vendor ID設定	0:IETF
Bind Interface設定	ppp0
送信プロトコル	☒ over IP ☐ over LDP
送信ポート番号	1701 (default 1701)

L2TPv3 Tunnel 設定で以下の項目を設定します。

- [Description] NXR
- [Peer アドレス] 10.10.10.1
- [Remote Hostname 設定] nrx
- [Remote RouterID 設定] 172.20.10.1
- [Vendor ID 設定] 0:IETF
- [Bind Interface 設定] ppp0
- [送信プロトコル] overIP

設定後[設定]をクリックします。

画面上部の L2TPv3 Xconnect Interface 設定をクリックし、「New Entry」をクリックします。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	172.20.10.1
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)	☒ 有効 ☐ 無効
MSS設定	☒ 有効 ☐ 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	☐ 有効 ☒ 無効
Known Unicast設定	☐ 送信する ☒ 送信しない
Circuit Down時Frame転送設定	☒ 送信する ☐ 送信しない
Split Horizon設定	☐ 有効 ☒ 無効

L2TPv3 Xconnect Interface 設定で以下の項目を設定します。

- ・ [Tunnel 設定選択] 172.20.10.1
- ・ [L2Frame 受信インタフェース設定] eth0
- ・ [Remote END ID 設定] 1
- ・ [Reschedule Interval 設定] 45
- ・ [Auto Negotiation 設定] 有効
- ・ [MSS 設定] 有効
- ・ [MSS 値] 0(自動設定)

設定後[設定]をクリックします。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。

L2TPv3	☐ 停止 ☒ 起動	停止中	動作変更
--------	--	-----	------

サービス一覧で以下の項目を設定します。

[L2TPv3] 起動

設定後[動作変更]をクリックします。

5. <補足>

一部機種では工場出荷状態で DNS リレー/キャッシュ機能を停止しているものがあります。

DNS リレー/キャッシュ機能を起動する場合は以下の設定を行います。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。

DNS キャッシュ	☐ 停止 ☒ 起動	停止中	動作変更
-----------	--	-----	------

サービス一覧で以下の項目を設定します。

[DNS キャッシュ] 起動

設定後[動作変更]をクリックします。

〔XR_B の設定〕

1. <インタフェース設定>

設定メニューで「インタフェース設定」をクリックすると Ethernet0 インタフェース設定が表示されます。

Ethernet0 ポート
[eth0]

☒ 固定アドレスで使用する
IP アドレス 192.168.10.3
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(p.masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast
☒ Send Redirects
☒ ICMP AddressMask Requestに回答
リンク監視 0 秒 (0-30)
(リンクダウン時にルーティング情報の配信を停止します)
通信モード
☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet0 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで選択
- ・ [IP アドレス] 192.168.10.3
- ・ [ネットマスク] 255.255.255.0

設定後[Ethernet 設定の保存]をクリックします。

画面上部の「Ethernet1 の設定」をクリックすると Ethernet1 インタフェース設定が表示されます。

Ethernet1 ポート
[eth1]

☒ 固定アドレスで使用する
IP アドレス 0
ネットマスク 255.255.255.0
MTU 1500
☐ DHCPサーバから取得
ホスト名
MACアドレス
☐ IPマスカレード(p.masq)
(このポートで使用するIPアドレスに変換して通信を行います)
☐ ステートフルパケットインスペクション(spi)
☐ SPI で DROP したパケットのLOGを取得
☐ proxy arp
☐ Directed Broadcast
☒ Send Redirects
☒ ICMP AddressMask Requestに回答
リンク監視 0 秒 (0-30)
(リンクダウン時にルーティング情報の配信を停止します)
通信モード
☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet1 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで選択
- ・ [IP アドレス] 0

設定後[Ethernet 設定の保存]をクリックします。

2 <PPPoE 設定>

設定メニューで「PPP/PPPoE 設定」をクリックすると接続設定が表示されます。

画面上部の「接続先設定 1」をクリックすると接続先設定 1が表示されます。

プロバイダ名	
ユーザID	test3@centurysys
パスワード	test3pass
DNSサーバ	☐ 割り当てられたDNSを使わない ☒ プロバイダから自動割り当て ☐ 手動で設定 プライマリ セカンダリ
LCPキープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	☒ 使用しない ☐ 使用する 使用するホスト 発行間隔は20秒固定、空欄の時はPPP-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	☐ 無効 ☒ 有効(強制) MSS値 0 Byte (有効時のMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1462。ACSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

PPPoE の接続先で以下の項目を設定します。

- ・ [ユーザ ID] test3@centurysys
- ・ [パスワード] test3pass
(🔑) ISP から提供されたユーザ ID, パスワードを設定します。
- ・ [DNS サーバ] プロバイダから自動割り当て
- ・ [LCP キープアライブ] 30 秒
- ・ [MSS 設定] 有効
MSS 値 0

設定後[設定の保存]をクリックします。

設定メニューで「PPP/PPPoE 設定」をクリックします。

回線状態	回線は接続されていません				
接続先の選択	☒ 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	☐ RS232C	☐ Ether0	☒ Ether1		
接続形態	☐ 手動接続	☒ 常時接続			
RS232C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			
ICMP AddressMask Request	☐ 応答しない	☒ 応答する			

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ICPADTを強制送出 ☒ 非接続SessionのLCP-EchoRequest受信時ICPADTを強制送出
-------------------------	--

PPPoE の接続設定で以下の項目を設定します。

- ・ [接続先の選択] 接続先 1

- ・ [接続ポート] Ether1
- ・ [接続形態] 常時接続
- ・ [IP マスカレード] 有効
- ・ [ステートフルパケットインスペクション] 有効
- ・ [デフォルトルートの設定] 有効
- ・ [回線接続時に前回の PPPoE セッションの PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の IPv4Packet 受信時に PADT を強制送出] 有効(チェック有)
- ・ [非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出] 有効(チェック有)

設定後[接続]をクリックします。

(🔗) [接続]をクリックすることにより設定の保存を行い、PPP/PPPoE 接続を開始します。

3. <フィルタ設定>

設定メニューで「フィルタ設定」をクリックすると入力フィルタ設定が表示されます。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット受信時	許可	l2tp	10.10.10.1			

入力フィルタで以下の項目を設定します。

No.1

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] l2tp
- ・ [送信元アドレス] 10.10.10.1

設定後[設定/削除の実行]をクリックします。

4. <L2TPv3 設定>

設定メニューで「各種サービスの設定」をクリックするとサービス一覧が表示されます。

サービス一覧の左側の「L2TPv3」をクリックすると L2TPv3 機能設定が表示されます。

Local hostname	xrb
Local Router-ID	172.20.30.1
MAC Address学習機能	☒ 有効 ☐ 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	☐ 有効 ☒ 無効
Known Unicast設定	☐ 送信する ☒ 送信しない
PMTU Discovery設定	☒ 有効 ☐ 無効
受信ポート番号(over LDP)	1701 (default 1701)
PMTU Discovery設定(over LDP)	☒ 有効 ☐ 無効
SNMP機能設定	☐ 有効 ☒ 無効
SNMP Trap機能設定	☐ 有効 ☒ 無効
Debug設定 (Syslogメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☒ L2TPエラーメッセージ出力

L2TPv3 機能設定で以下の項目を設定します。

- ・ [Local hostname] xrb
- ・ [Local Router-ID] 172.20.30.1

設定後[設定]をクリックします。

画面上部の L2TPv3 Tunnel 設定をクリックし、「New Entry」をクリックします。

Description	NXR
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 Hiding設定	☐ 有効 ☒ 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	nxr
Remote RouterID設定	172.20.10.1
Vendor ID設定	0:IETF
Bind Interface設定	ppp0
送信プロトコル	☒ over IP ☐ over UDP
送信ポート番号	1701 (default 1701)

L2TPv3 Tunnel 設定で以下の項目を設定します。

- ・ [Description] NXR
- ・ [Peer アドレス] 10.10.10.1
- ・ [Remote Hostname 設定] nxr
- ・ [Remote RouterID 設定] 172.20.10.1
- ・ [Vendor ID 設定] 0:IETF
- ・ [Bind Interface 設定] ppp0
- ・ [送信プロトコル] overIP

設定後[設定]をクリックします。

画面上部の L2TPv3 Xconnect Interface 設定をクリックし、「New Entry」をクリックします。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	172.20.10.1
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の場合は付与しない)
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)	☒ 有効 ☐ 無効
MSS設定	☒ 有効 ☐ 無効
MSS値(Byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	☐ 有効 ☒ 無効
Known Unicast設定	☐ 送信する ☒ 送信しない
Circuit Down時Frame転送設定	☒ 送信する ☐ 送信しない
Split Horizon設定	☐ 有効 ☒ 無効

L2TPv3 Xconnect Interface 設定で以下の項目を設定します。

- ・ [Tunnel 設定選択] 172.20.10.1
- ・ [L2Frame 受信インタフェース設定] eth0
- ・ [Remote END ID 設定] 1
- ・ [Reschedule Interval 設定] 45
- ・ [Auto Negotiation 設定] 有効

- ・ [MSS 設定] 有効
- ・ [MSS 値] 0(自動設定)

設定後[設定]をクリックします。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。



サービス一覧で以下の項目を設定します。

[L2TPv3] 起動

設定後[動作変更]をクリックします。

5. <補足>

一部機種では工場出荷状態で DNS リレー/キャッシュ機能を停止しているものがあります。

DNS リレー/キャッシュ機能を起動する場合は以下の設定を行います。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。



サービス一覧で以下の項目を設定します。

[DNS キャッシュ] 起動

設定後[動作変更]をクリックします。

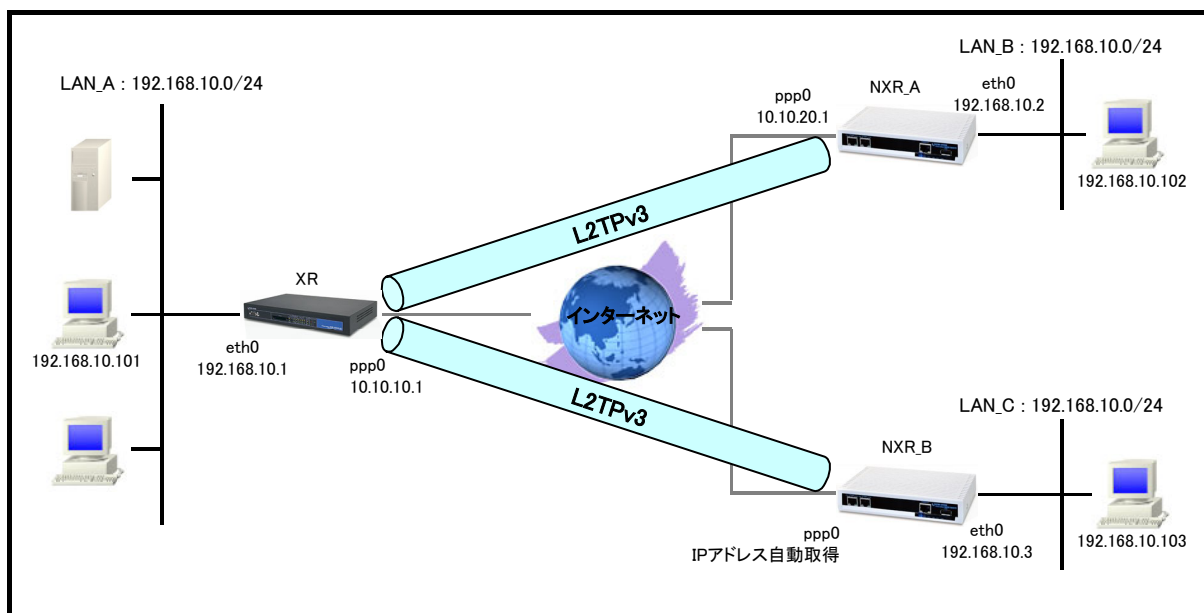
【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.101	192.168.10.102	192.168.10.103
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.2	192.168.10.3
DNS サーバの IP アドレス	192.168.10.1	192.168.10.2	192.168.10.3

3-2. PPPoE を利用した L2TPv3 接続設定(センタ XR,拠点 NXR)

PPPoE 接続環境で NXR シリーズーXR シリーズ間で L2TPv3 接続を行う設定例です。この設定例では XR、NXR_A に WAN 側固定 IP アドレス、NXR_B に WAN 側動的 IP アドレスが割り当てられる環境を想定しています。

【 構成図 】



- ・ この設定例では L2TPv3 接続時の Vendor ID 設定として IETF を指定します。
- ・ この設定例では Ethernet0 インタフェースを L2TPv3 の Xconnect インタフェースに設定します。
- ・ XR 配下のネットワークは NXR を経由して通信することが可能です。
- ・ 各拠点にある端末はそれぞれの拠点の NXR, XR からインターネットアクセスを行います。

【 設定例 】

〔XR の設定〕

1. <インタフェース設定>

設定メニューで「インタフェース設定」をクリックすると Ethernet0 インタフェース設定が表示されます。

Ethernet0 ポート
[eth0]

☒ 固定アドレスで使用する

IP アドレス 192.168.10.1

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet0 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで使用する
- ・ [IP アドレス] 192.168.10.1
- ・ [ネットマスク] 255.255.255.0

設定後[Ethernet 設定の保存]をクリックします。

画面上部の「Ethernet1 の設定」をクリックすると Ethernet1 インタフェース設定が表示されます。

Ethernet1 ポート
[eth1]

☒ 固定アドレスで使用する

IP アドレス 0

ネットマスク 255.255.255.0

MTU 1500

☐ DHCPサーバから取得

ホスト名

MACアドレス

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

☐ ステートフルパケットインスペクション(spi)

☐ SPI で DROP したパケットのLOGを取得

☐ proxy arp

☐ Directed Broadcast

☒ Send Redirects

☒ ICMP AddressMask Requestに回答

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

通信モード

☒ 自動 ☐ full-100M ☐ half-100M ☐ full-10M ☐ half-10M

Ethernet1 インタフェースで以下の項目を設定します。

- ・ 固定アドレスで使用する
- ・ [IP アドレス] 0

設定後[Ethernet 設定の保存]をクリックします。

2 <PPPoE 設定>

設定メニューで「PPP/PPPoE 設定」をクリックすると接続設定が表示されます。

画面上部の「接続先設定 1」をクリックすると接続先設定 1 が表示されます。

プロバイダ名	
ユーザID	test1@centurysys
パスワード	test1pass
DNSサーバ	☐ 割り当てられたDNSを使わない ☒ プロバイダから自動割り当て ☐ 手動で設定 プライマリ セカンダリ
LCPキープアライブ	チェック間隔 30 秒 ※回線確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	☒ 使用しない ☐ 使用する 使用するホスト 発行間隔は30秒固定、空欄の時はPDP-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	☐ 無効 ☒ 有効(強制) MSS値 0 Byte (有効時にはMSS値が0又は空の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1462、ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

PPPoE の接続先で以下の項目を設定します。

- ・ [ユーザ ID] test1@centurysys
- ・ [パスワード] test1pass
(🔑) ISP から提供されたユーザ ID、パスワードを設定します。
- ・ [DNS サーバ] プロバイダから自動割り当て
- ・ [LCP キープアライブ] 30 秒
- ・ [MSS 設定] 有効
MSS 値 0

設定後[設定の保存]をクリックします。

設定メニューで「PPP/PPPoE 設定」をクリックします。

回線状態	回線は接続されていません	
接続先の選択	☒ 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	☐ RS232C ☐ Ether0 ☒ Ether1	
接続形態	☐ 手動接続 ☒ 常時接続	
RS232C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	
ICMP AddressMask Request	☐ 応答しない ☒ 応答する	
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	

PPPoE の接続設定で以下の項目を設定します。

- ・ [接続先の選択] 接続先 1

- ・ [接続ポート] Ether1
- ・ [接続形態] 常時接続
- ・ [IP マスカレード] 有効
- ・ [ステートフルパケットインスペクション] 有効
- ・ [デフォルトルートの設定] 有効
- ・ [回線接続時に前回の PPPoE セッションの PADT を強制送付] 有効(チェック有)
- ・ [非接続 Session の IPv4Packet 受信時に PADT を強制送付] 有効(チェック有)
- ・ [非接続 Session の LCP-EchoRequest 受信時に PADT を強制送付] 有効(チェック有)

設定後[接続]をクリックします。

(👉) [接続]をクリックすることにより設定の保存を行い、PPP/PPPoE 接続を開始します。

3. <フィルタ設定>

設定メニューで「フィルタ設定」をクリックすると入力フィルタ設定が表示されます。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット受信時	許可	l2tp			10.10.10.1	

入力フィルタで以下の項目を設定します。

No.1

- ・ [インタフェース] ppp0
- ・ [動作] 許可
- ・ [プロトコル] l2tp
- ・ [宛て先アドレス] 10.10.10.1

設定後[設定/削除の実行]をクリックします。

4. <L2TPv3 設定>

設定メニューで「各種サービスの設定」をクリックするとサービス一覧が表示されます。

サービス一覧の左側の「L2TPv3」をクリックすると L2TPv3 機能設定が表示されます。

Local hostname	xr
Local Router-ID	172.20.10.1
MAD Address学習機能	☒ 有効 ☐ 無効
MAD Address Aging Time	300 (30~1000sec)
Loop Detection設定	☐ 有効 ☒ 無効
Known Unicast設定	☐ 送信する ☒ 送信しない
PMTU Discovery設定	☒ 有効 ☐ 無効
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	☒ 有効 ☐ 無効
SNMP機能設定	☐ 有効 ☒ 無効
SNMP Trap機能設定	☐ 有効 ☒ 無効
Debug設定 (Syslogメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☒ L2TPエラーメッセージ出力

L2TPv3 機能設定で以下の項目を設定します。

- ・ [Local hostname] xr
- ・ [Local Router-ID] 172.20.10.1

設定後[設定]をクリックします。

画面上部の L2TPv3 Tunnel 設定をクリックし、「New Entry」をクリックします。

Description	NXR_A
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 Hline設定	☐ 有効 ☒ 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	nxra
Remote RouterID設定	172.20.20.1
Vendor ID設定	0:ietf
Bind Interface設定	ppp0
送信プロトコル	☒ over IP ☐ over UDP
送信ポート番号	1701 (default 1701)

L2TPv3 Tunnel 設定で以下の項目を設定します。

- ・ [Description] NXR_A
- ・ [Peer アドレス] 10.10.20.1
- ・ [Remote Hostname 設定] nxra
- ・ [Remote RouterID 設定] 172.20.20.1
- ・ [Vendor ID 設定] 0:ietf
- ・ [Bind Interface 設定] ppp0
- ・ [送信プロトコル] overIP

設定後[設定]をクリックします。

画面上部の L2TPv3 Xconnect Interface 設定をクリックし、「New Entry」をクリックします。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	172.20.20.1
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の場合は付与しない)
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)	☒ 有効 ☐ 無効
MSS設定	☒ 有効 ☐ 無効
MSS値(Byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	☐ 有効 ☒ 無効
Known Unicast設定	☐ 送信する ☒ 送信しない
Circuit Down時Frame転送設定	☒ 送信する ☐ 送信しない
Split Horizon設定	☐ 有効 ☒ 無効

L2TPv3 Xconnect Interface 設定で以下の項目を設定します。

- ・ [Tunnel 設定選択] 172.20.10.1
- ・ [L2Frame 受信インタフェース設定] eth0
- ・ [Remote END ID 設定] 1
- ・ [Reschedule Interval 設定] 30
- ・ [Auto Negotiation 設定] 有効

- ・ [MSS 設定] 有効
- ・ [MSS 値] 0 (自動設定)

設定後[設定]をクリックします。

画面上部の L2TPv3 Tunnel 設定をクリックし、「New Entry」をクリックします。

Description	NXR_B
Peerアドレス	(例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hdlne設定	☐ 有効 ☒ 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	nxb
Remote RouterID設定	172.20.30.1
Vendor ID設定	0:IETF
Bind Interface設定	ppp0
送信プロトコル	☒ over IP ☐ over UDP
送信ポート番号	1701 (default 1701)

L2TPv3 Tunnel 設定で以下の項目を設定します。

- ・ [Description] NXR_B
- ・ [Peer アドレス] 空欄
- ・ [Remote Hostname 設定] nxrb
- ・ [Remote RouterID 設定] 172.20.30.1
- ・ [Vendor ID 設定] 0:IETF
- ・ [Bind Interface 設定] ppp0
- ・ [送信プロトコル] overIP

設定後[設定]をクリックします。

画面上部の L2TPv3 Xconnect Interface 設定をクリックし、「New Entry」をクリックします。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	172.20.30.1
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)	☒ 有効 ☐ 無効
MSS設定	☒ 有効 ☐ 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	☐ 有効 ☒ 無効
Known Unicast設定	☐ 送信する ☒ 送信しない
Circuit Down時Frame転送設定	☒ 送信する ☐ 送信しない
Split Horizon設定	☐ 有効 ☒ 無効

L2TPv3 Xconnect Interface 設定で以下の項目を設定します。

- ・ [Tunnel 設定選択] 172.20.30.1
- ・ [L2Frame 受信インタフェース設定] eth0
- ・ [Remote END ID 設定] 1

- ・ [Reschedule Interval 設定] 30
- ・ [Auto Negotiation 設定] 有効
- ・ [MSS 設定] 有効
- ・ [MSS 値] 0 (自動設定)

設定後[設定]をクリックします。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。



サービス一覧で以下の項目を設定します。

[L2TPv3] 起動

設定後[動作変更]をクリックします。

5. <補足>

一部機種では工場出荷状態で DNS リレー/キャッシュ機能を停止しているものがあります。

DNS リレー/キャッシュ機能を起動する場合は以下の設定を行います。

設定メニューで「各種サービスの設定」をクリックしサービス一覧を表示します。



サービス一覧で以下の項目を設定します。

[DNS キャッシュ] 起動

設定後[動作変更]をクリックします。

〔NXR_A の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr120(config)#hostname NXR_A
NXR_A(config)#interface ethernet 0
NXR_A(config-if)#ip address 192.168.10.2/24
NXR_A(config-if)#exit
NXR_A(config)#ip route 0.0.0.0/0 ppp 0
NXR_A(config)#ip access-list ppp0_in permit 10.10.10.1 10.10.20.1 115
NXR_A(config)#interface ppp 0
NXR_A(config-ppp)#ip address 10.10.20.1/32
NXR_A(config-ppp)#ip masquerade
NXR_A(config-ppp)#ip access-group in ppp0_in
NXR_A(config-ppp)#ip spi-filter
NXR_A(config-ppp)#ip tcp adjust-mss auto
NXR_A(config-ppp)#no ip redirects
NXR_A(config-ppp)#ppp username test2@centurysys password test2pass
NXR_A(config-ppp)#exit
NXR_A(config)#interface ethernet 1
NXR_A(config-if)#no ip address
NXR_A(config-if)#pppoe-client ppp 0
NXR_A(config-if)#exit
NXR_A(config)#l2tpv3 hostname nxra
NXR_A(config)#l2tpv3 router-id 172.20.20.1
NXR_A(config)#l2tpv3 mac-learning
NXR_A(config)#l2tpv3 mac-aging 300
NXR_A(config)#l2tpv3 path-mtu-discovery
NXR_A(config)#l2tpv3 tunnel 1
NXR_A(config-l2tpv3-tunnel)#description XR
NXR_A(config-l2tpv3-tunnel)#tunnel address 10.10.10.1
NXR_A(config-l2tpv3-tunnel)#tunnel hostname xr
NXR_A(config-l2tpv3-tunnel)#tunnel router-id 172.20.10.1
NXR_A(config-l2tpv3-tunnel)#tunnel vendor ietf
NXR_A(config-l2tpv3-tunnel)#exit
NXR_A(config)#l2tpv3 xconnect 1
NXR_A(config-l2tpv3-xconnect)#description XR
NXR_A(config-l2tpv3-xconnect)#tunnel 1
NXR_A(config-l2tpv3-xconnect)#xconnect ethernet 0
NXR_A(config-l2tpv3-xconnect)#xconnect end-id 1
NXR_A(config-l2tpv3-xconnect)#retry-interval 45
NXR_A(config-l2tpv3-xconnect)#ip tcp adjust-mss auto
NXR_A(config-l2tpv3-xconnect)#exit
NXR_A(config)#dns
NXR_A(config-dns)#service enable
NXR_A(config-dns)#exit
NXR_A(config)#exit
NXR_A#save config
```

〔NXR_B の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
nxr120(config)#hostname NXR_B
NXR_B(config)#interface ethernet 0
NXR_B(config-if)#ip address 192.168.10.3/24
NXR_B(config-if)#exit
NXR_B(config)#ip route 0.0.0.0/0 ppp 0
NXR_B(config)#ip access-list ppp0_in permit 10.10.10.1 any 115
NXR_B(config)#interface ppp 0
NXR_B(config-ppp)#ip address negotiated
```

----- 次のページに続きがあります -----

——— 前のページからの続きです ———

```

NXR_B(config-ppp)#ip masquerade
NXR_B(config-ppp)#ip access-group in ppp0_in
NXR_B(config-ppp)#ip spi-filter
NXR_B(config-ppp)#ip tcp adjust-mss auto
NXR_B(config-ppp)#no ip redirects
NXR_B(config-ppp)#ppp username test3@centurysys password test3pass
NXR_B(config-ppp)#exit
NXR_B(config)#interface ethernet 1
NXR_B(config-if)#no ip address
NXR_B(config-if)#pppoe-client ppp 0
NXR_B(config-if)#exit
NXR_B(config)#l2tpv3 hostname nxrb
NXR_B(config)#l2tpv3 router-id 172.20.30.1
NXR_B(config)#l2tpv3 mac-learning
NXR_B(config)#l2tpv3 mac-aging 300
NXR_B(config)#l2tpv3 path-mtu-discovery
NXR_B(config)#l2tpv3 tunnel 1
NXR_B(config-l2tpv3-tunnel)#description XR
NXR_B(config-l2tpv3-tunnel)#tunnel address 10.10.10.1
NXR_B(config-l2tpv3-tunnel)#tunnel hostname nxra
NXR_B(config-l2tpv3-tunnel)#tunnel router-id 172.20.10.1
NXR_B(config-l2tpv3-tunnel)#tunnel vendor ietf
NXR_B(config-l2tpv3-tunnel)#exit
NXR_B(config)#l2tpv3 xconnect 1
NXR_B(config-l2tpv3-xconnect)#description XR
NXR_B(config-l2tpv3-xconnect)#tunnel 1
NXR_B(config-l2tpv3-xconnect)#xconnect ethernet 0
NXR_B(config-l2tpv3-xconnect)#xconnect end-id 1
NXR_B(config-l2tpv3-xconnect)#retry-interval 30
NXR_B(config-l2tpv3-xconnect)#ip tcp adjust-mss auto
NXR_B(config-l2tpv3-xconnect)#exit
NXR_B(config)#dns
NXR_B(config-dns)#service enable
NXR_B(config-dns)#exit
NXR_B(config)#exit
NXR_B#save config

```

NXR の設定に関しましてはご利用頂いている NXR 製品のユーザーズガイド (CLI 版) および FutureNetNXR 設定例集 L2TPv3 編をご参照ください。

【 パソコンの設定例 】

	LAN A のパソコン	LAN B のパソコン	LAN C のパソコン
IP アドレス	192.168.10.101	192.168.10.102	192.168.10.103
サブネットマスク	255.255.255.0	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.10.1	192.168.10.2	192.168.10.3
DNS サーバの IP アドレス	192.168.10.1	192.168.10.2	192.168.10.3

付録

IPsec 状態確認方法

〔NXR〕

● ステータスの確認

IPsec の各トンネル状況を一覧で確認する場合は、show ipsec status brief コマンドを使用します。

＜実行例＞

```
nrx120#show ipsec status brief
TunnelName      Status
tunnel1          up
tunnel2          down
```

IPsec SA が確立している(IPsec established)ものを up,それ以外を down として表示します。

IPsec の SA 確立状況等を確認する場合は、show ipsec status コマンドを使用します。

また show ipsec status コマンドの後に tunnel <ポリシー番号>を指定することにより tunnel ポリシー毎にステータスを表示させることができます。これは多拠点収容構成で個々のポリシーを確認するのに有効です。

＜実行例＞

```
nrx120#show ipsec status
000 "tunnel1":192.168.30.0/24===10.10.30.1[nxrc]...10.10.10.1[10.10.10.1]===192.168.10.0/24; erouted; eroute
owner: #2
000 "tunnel1":   ike_life: 10800s; ipsec_life: 3600s; margin: 270s; inc_ratio: 100%
000 "tunnel1":   newest ISAKMP SA: #1; newest IPsec SA: #2;
000 "tunnel1":   IKE proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000 "tunnel1":   ESP proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000
000 #2: "tunnel1" STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 3212s; newest
IPSEC; eroute owner
000 #2: "tunnel1" esp.7a5cb4c1@10.10.10.1 (0 bytes) esp.9867e772@10.10.30.1 (0 bytes); tunnel
000 #1: "tunnel1" STATE_AGGR_I2 (sent AI2, ISAKMP SA established); EVENT_SA_REPLACE in 10291s;
newest ISAKMP
000
Connections:
Security Associations:
none
```

● ログの確認

ログは show syslog message コマンドで確認することができます。

(🔍) ここで設定しているシスログのプライオリティは info(初期値)となります。このプライオリティを debug に変更することによりより多くのログが出力されます。

IPsec 接続完了時には以下のようなログが出力されます。

➤ イニシエータでメインモード利用時

＜出力例＞


```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [strongSwan]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [XAUTH]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #1: ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP {using isakmp#1}
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established [ESP=>0x14bd33f0 <0xf49c1f56 DPD]
```

➤ レスポンダでメインモード利用時

＜出力例＞

```
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [strongSwan]
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #3: responding to Main Mode
pluto[XXXX]: "tunnel1" #3: sent MR3, ISAKMP SA established
pluto[XXXX]: "tunnel1" #3: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #4: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #4: IPsec SA established [ESP=>0x9c4fb981 <0xc30f38e1 DPD]
```

➤ イニシエータでアグレッシブモード利用時

＜出力例＞

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [strongSwan]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [XAUTH]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+0x4000000
{using isakmp#1}
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established [ESP=>0xc5e28ab0 <0x899ed286 DPD]
```

➤ レスポンダでアグレッシブモード利用時

＜出力例＞

```
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [strongSwan]
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #2: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #2: IPsec SA established [ESP=>0x899ed286 <0xc5e28ab0 DPD]
```

「ISAKMP SA established」が ISAKMP SA が確立したことを、「IPsec SA established」が IPsec SA が確立したことを示しています。

IPsec 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

➤ 対向機器からの応答がない(メインモード)

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
```

```
...
pluto[XXXX]: "tunnel1" #1: max number of retransmissions (20) reached STATE_MAIN_I1. No response(or no
acceptable response) to our first IKE message
pluto[XXXX]: "tunnel1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "tunnel1" #2: initiating Main Mode to replace #1
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ(UDP500)は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

➤ 対向機器からの応答がない(アグレッシブモード)

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
...
pluto[XXXX]: "tunnel1" #1: max number of retransmissions (20) reached STATE_AGGR_I1
pluto[XXXX]: "tunnel1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "tunnel1" #2: initiating Aggressive Mode #2 to replace #1, connection "tunnel1"
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ(UDP500)は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

➤ 該当するポリシーがない(イニシエータがメインモード)

<レスポнда側のログ出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Main Mode message received on 10.10.10.1:500 but no
connection has been authorized with policy=PSK
```

(☞) フェーズ1のモードは正しいか、対向のルータの IP アドレスの設定は正しいか、IPsec の設定の関連づけは正しいかなどを確認してください。

➤ 該当するポリシーがない(イニシエータがアグレッシブモード)

<レスポнда側のログ出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Aggressive Mode message received on 10.10.10.1:500 but no
connection has been authorized with policy=PSK
```

(☞) フェーズ1のモードは正しいか、IPsec の設定の関連づけは正しいかなどを確認してください。

➤ 事前共有鍵の不一致(メインモード)

<レスポнда側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: responding to Main Mode
pluto[XXXX]: "tunnel1" #1: "tunnel1" #1: next payload type of ISAKMP Identification Payload has an unknown
value
pluto[XXXX]: "tunnel1" #1: probable authentication failure (mismatch of preshared secrets?):
malformed payload in packet
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
pluto[XXXX]: "tunnel1" #1: next payload type of ISAKMP Hash Payload has an unknown value:
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

➤ 事前共有鍵の不一致(アグレッシブモード)

＜レスポнда側のログ出力例＞

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: received Hash Payload does not match computed value
pluto[XXXX]: "tunnel1" #1: sending notification INVALID_HASH_INFORMATION to 10.10.10.1:500
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

➤ フェーズ1の ID 不一致(イニシエータの self-identity 不一致)

＜レスポнда側のログ出力例＞

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: no suitable connection for peer 'nxr'
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: initial Aggressive Mode packet claiming to be from 10.10.30.1 but no
connection has been authorized
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: sending notification INVALID_ID_INFORMATION to 10.10.30.1:500
```

(☞) ipsec isakmp policy 設定モードの remote identity コマンドで設定した値(ID タイプを含む)が対向機器の self-identity と一致しているか確認してください。

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: packet from 10.10.10.1:500: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec local policy 設定モードの self-identity コマンドで設定した値(ID タイプを含む)が対向機器の remote identity と一致しているか確認してください。

➤ フェーズ1の ID 不一致(レスポндаの self-identity 不一致)

＜レスポнда側のログ出力例＞

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: packet from 10.10.30.1:500: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec isakmp policy 設定モードの remote identity コマンドで設定した値(ID タイプを含む)が対向機器の self-identity と一致しているか確認してください。

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: no suitable connection for peer '10.10.10.1'
pluto[XXXX]: "tunnel1" #1: initial Aggressive Mode packet claiming to be from 10.10.10.1but no connection has
been authorized
pluto[XXXX]: "tunnel1" #1: sending notification INVALID_ID_INFORMATION to 10.10.10.1:500
```

(☞) ipsec local policy 設定モードの self-identity コマンドで設定した値(ID タイプを含む)が対向機器の remoteidentity と一致しているか確認してください。

➤ フェーズ2の ID 不一致

＜レスポнда側のログ出力例＞

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: cannot respond to IPsec SA request because no connection is known
for 192.168.10.0/24==10.10.10.1[10.10.10.1]...10.10.30.1[nxrc]==192.168.30.0/24
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: sending encrypted notification INVALID_ID_INFORMATION
```

to10.10.30.1:500

(☞) ipsec access-list コマンドで設定した値が対向機器と対になっているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+0x4000000 {using isakmp#1}
pluto[XXXX]: "tunnel1" #1: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec access-list コマンドで設定した値が対向機器と対になっているか確認してください。

➤ PFS 設定の不一致(レスポнда側でのみ PFS を設定)

<レスポнда側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #2: we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #2: sending encrypted notification NO_PROPOSAL_CHOSEN to 10.10.30.1:500
```

(☞) ipsec tunnel policy 設定モードの set pfs コマンドで設定した値が対向機器と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+UP+0x4000000 {using isakmp#1}
pluto[XXXX]: "tunnel1" #1: ignoring informational payload, type NO_PROPOSAL_CHOSEN
```

(☞) ipsec tunnel policy 設定モードの set pfs コマンドを設定しているか確認してください。

[XR]

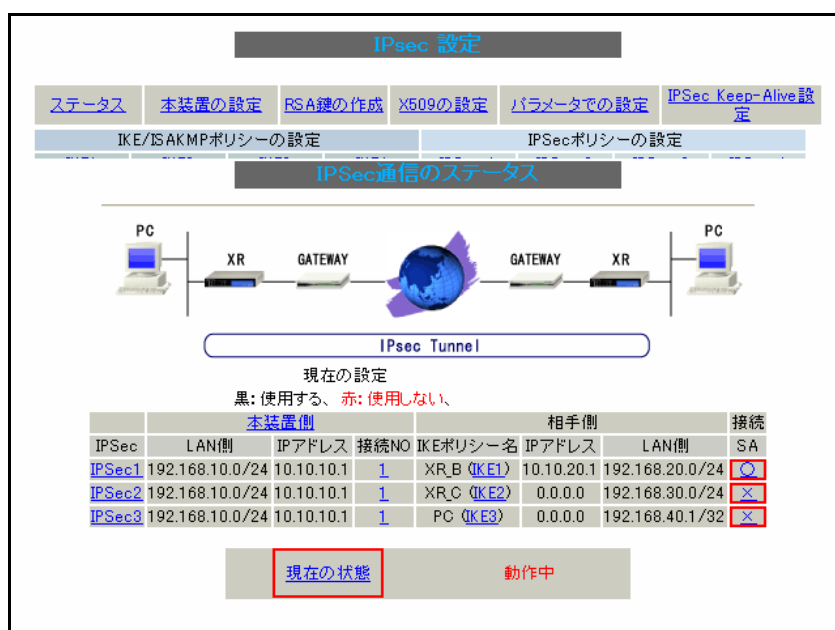
IPsec の各トンネル状況を一覧で確認する場合は、設定メニューで「各種サービスの設定」をクリックし、サービス一覧の左側の「IPsec サーバ」をクリックすると IPsec 設定および IPsec の各トンネル状況が表示されます。

IPsec の各トンネル状況は接続欄の下にある○、×で確認することができます。



IPsec の SA 確立状況等を確認する場合は、IPsec 通信のステータス画面の一番下にある「現在の状態」をクリックします。

また IPsec ポリシー毎に IPsec の SA 確立状況等を確認する場合は接続の下にある○、×をクリックすることで確認できます。これは多拠点収容構成で個々のポリシーを確認するのに有効です。



<表示例>

```
000 interface ipsec5/eth0 192.168.20.1
000 interface ipsec0/ppp0 10.10.20.1
000
000 "xripsec1": 192.168.20.0/24===10.10.20.1---10.255.2.1...10.10.10.1===192.168.10.0/24
000 "xripsec1": ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 270s; rekey_fuzz: 100%; keyingtries: 0
000 "xripsec1": policy: PSK+ENCRYPT+TUNNEL+PFS+DISABLEARRIVALCHECK; interface: ppp0; erouted
000 "xripsec1": newest ISAKMP SA: #1; newest IPsec SA: #2; eroute owner: #2
```

```
000 "xripsec1": IKE algorithm newest: AES_CBC_128-SHA-MODP1024
000 "xripsec1": ESP algorithm newest: AES_128-HMAC_SHA1; pfsgroup=MODP1024
000
000 #2: "xripsec1" STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 28259s; newest IPSEC;
eroute owner
000 #2: "xripsec1" esp.e764384a@10.10.10.1 esp.8bd9f8ac@10.10.20.1 tun.1002@10.10.10.1 tun.1001@10.10.20.1
000 #1: "xripsec1" STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 2974s; newest ISAKMP; DPD active
000

localhost Fri Mar 16 13:42:31 JST 2012
192.168.20.0/24 -> 192.168.10.0/24 => tun0xe764384a@10.10.10.1 (10)
ipsec0->ppp0 mtu=1500(1381)->1454
ipsec1->NULL mtu=1500(0)->0
ipsec2->NULL mtu=1500(0)->0
ipsec3->NULL mtu=1500(0)->0
ipsec4->NULL mtu=1500(0)->0
ipsec5->eth0 mtu=1500(1500)->1500
ipsec6->NULL mtu=1500(0)->0
esp0xe764384a@10.10.20.1 ESP_AES_128_CBC_HMAC_SHA1_96: dir=in src=10.10.10.1 iv_bits=128bits
iv=0x34793513980c22151d50770d52cab34c ooowin=64 seq=10 bit=0x3ff alen=160 aklen=160 eklen=128
life(c,s,h)=bytes(880,0,0)addtime(194,0,0)usetime(142,0,0)packets(10,0,0) idle=7
esp0xe764384a@10.10.10.1 ESP_AES_128_CBC_HMAC_SHA1_96: dir=out src=10.10.20.1 iv_bits=128bits
iv=0x10c7aced59bf26a90f7f255f74348d25 ooowin=64 seq=10 alen=160 aklen=160 eklen=128
life(c,s,h)=bytes(1360,0,0)addtime(194,0,0)usetime(142,0,0)packets(10,0,0) idle=7
tun0xe764384a@10.10.20.1 IPIP: dir=in src=10.10.10.1 life(c,s,h)=bytes(880,0,0)addtime(194,0,0)usetime(142,0,0)packets(10,0,0)
idle=7
tun0xe764384a@10.10.10.1 IPIP: dir=out src=10.10.20.1 life(c,s,h)=bytes(880,0,0)addtime(194,0,0)usetime(142,0,0)packets(10,0,0)
idle=7
Destination Gateway Genmask Flags MSS Window irtt Iface
10.255.2.1 0.0.0.0 255.255.255.255 UH 0 0 0 ipsec0
10.255.2.1 0.0.0.0 255.255.255.255 UH 0 0 0 ppp0
192.168.10.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.20.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.20.0 0.0.0.0 255.255.255.0 U 0 0 0 ipsec5
```

● ログの確認

ログは設定メニューで「システム設定」をクリックし、「ログの表示」をクリックすることにより表示されます。

(☞) ここで設定しているシスログのプライオリティは info(初期値)となります。このプライオリティを debug に変更することによりより多くのログが出力されます。

IPsec 接続完了時には以下のようなログが出力されます。

➤ イニシエータでメインモード利用時

<出力例>

```
pluto[XXXX]: "xripsec1" #1: initiating Main Mode
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_I1: initiate
pluto[XXXX]: "xripsec1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_I2: sent MI2, expecting MR2
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_I3: sent MI3, expecting MR3
pluto[XXXX]: "xripsec1" #1: ISAKMP SA established
pluto[XXXX]: "xripsec1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "xripsec1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+DISABLEARRIVALCHECK
pluto[XXXX]: "xripsec1" #2: STATE_QUICK_I1: initiate
pluto[XXXX]: "xripsec1" #2: sent QI2, IPsec SA established
```

➤ レスポンダでメインモード利用時

<出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "xripsec1" #1: responding to Main Mode
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_R1: sent MR1, expecting MI2
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_R2: sent MR2, expecting MI3
pluto[XXXX]: "xripsec1" #1: sent MR3, ISAKMP SA established
pluto[XXXX]: "xripsec1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "xripsec1" #2: responding to Quick Mode
pluto[XXXX]: "xripsec1" #2: STATE_QUICK_R1: sent QR1, inbound IPsec SA installed, expecting QI2
pluto[XXXX]: "xripsec1" #2: IPsec SA established
```

➤ イニシエータでアグレッシブモード利用時

＜出力例＞

```
pluto[XXXX]: "xripsec1" #1: initiating Aggressive Mode
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: initiate
pluto[XXXX]: "xripsec1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "xripsec1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "xripsec1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "xripsec1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+DISABLEARRIVALCHECK
pluto[XXXX]: "xripsec1" #2: STATE_QUICK_I1: initiate
pluto[XXXX]: "xripsec1" #2: sent QI2, IPsec SA established
```

➤ レスポンダでアグレッシブモード利用時

＜出力例＞

```
pluto[XXXX]: packet from 10.10.20.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: packet from 10.10.20.1:500: reset connection(xripsec1)
pluto[XXXX]: "xripsec1": terminating SAs using these connections(include using same isakmp sa)
pluto[XXXX]: "xripsec1"[1] 10.10.20.1 #1: responding to Aggressive Mode, state #2, connection "xripsec1"
pluto[XXXX]: "xripsec1"[1] 10.10.20.1 #1: STATE_AGGR_R1: sent AR1, expecting AI2
pluto[XXXX]: "xripsec1"[1] 10.10.20.1 #1: ISAKMP SA established
pluto[XXXX]: "xripsec1"[1] 10.10.20.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "xripsec1"[1] 10.10.20.1 #2: responding to Quick Mode
pluto[XXXX]: "xripsec1"[1] 10.10.20.1 #2: STATE_QUICK_R1: sent QR1, inbound IPsec SA installed, expecting QI2
pluto[XXXX]: "xripsec1"[1] 10.10.20.1 #2: IPsec SA established
```

「ISAKMP SA established」が ISAKMP SA が確立したことを、「IPsec SA established」が IPsec SA が確立したことを示しています。

IPsec 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

➤ 対向機器からの応答がない(メインモード)

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "xripsec1" #1: initiating Main Mode
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_I1: initiate
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_I1: retransmission; will wait 10s for response
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_I1: retransmission; will wait 20s for response
...
pluto[XXXX]: "xripsec1" #1: max number of retransmissions (20) reached STATE_MAIN_I1. No acceptable response to our first IKE message
pluto[XXXX]: "xripsec1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "xripsec1" #2: initiating Main Mode
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ(UDP500)は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

➤ 対向機器からの応答がない(アグレッシブモード)

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "xripsec1" #1: initiating Aggressive Mode
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: initiate
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: retransmission; will wait 10s for response
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: retransmission; will wait 20s for response
...
pluto[XXXX]: "xripsec1" #1: max number of retransmissions (20) reached STATE_AGGR_I1
pluto[XXXX]: "xripsec1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "xripsec1" #2: initiating Aggressive Mode
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ(UDP500)は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

➤ 該当するポリシーがない(イニシエータがメインモード)

＜レスポнда側のログ出力例＞

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Main Mode message received on 10.10.10.1:500 but no connection has been authorized
```

(☞) フェーズ1のモードは正しいか、対向のルータの IP アドレスの設定は正しいか、IPsec の設定の関連づけは正しいかなどを確認してください。

➤ 該当するポリシーがない(イニシエータがアグレッシブモード)

＜レスポнда側のログ出力例＞

```
pluto[XXXX]: packet from 10.10.30.1:500: initial Aggr Mode message received on 10.10.10.1:500 but no connection has been authorized
```

(☞) フェーズ1のモードは正しいか、IPsec の設定の関連づけは正しいか、インタフェースの ID は正しいかなどを確認してください。

➤ 事前共有鍵の不一致

＜レスポнда側のログ出力例＞

```
pluto[XXXX]: packet from 10.10.20.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "xripsec1" #1: responding to Main Mode
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_R1: sent MR1, expecting MI2
pluto[XXXX]: "xripsec1" #1: STATE_MAIN_R2: sent MR2, expecting MI3
pluto[XXXX]: "xripsec1" #1: probable authentication failure (mismatch of preshared secrets?): malformed payload in packet
```

(☞) お互いのルータで設定した事前共有鍵(PSK)の値が正しいか確認してください。

➤ フェーズ1の ID 不一致(イニシエータのインタフェース ID 不一致)

＜レスポнда側のログ出力例＞

```
pluto[XXXX]: packet from 10.10.30.1:500: initial Aggr Mode message received on 10.10.10.1:500 but no connection has been authorized
```

(☞) IKE/ISAKMP ポリシーの設定のインタフェースの ID で設定した値が対向機器で設定した ID と一致しているか確認してください。

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "xripsec1" #1: initiating Aggressive Mode
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: initiate
```



```
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: retransmission; will wait 10s for response
```

☞ 本装置側の設定のインタフェース ID で設定した値が対向機器で設定した ID と一致しているか確認してください。

(※)上記ログは対向機器からの応答が得られない場合にも同様のログが出力されます。

➤ フェーズ1の ID 不一致(レスポンス側のインタフェース ID 不一致)

＜レスポンス側のログ出力例＞

```
pluto[XXXX]: "xripsec1" [1] 10.10.30.1 #1: responding to Aggressive Mode, state #1, connection "xripsec1"
pluto[XXXX]: "xripsec1" [1] 10.10.30.1 #1: STATE_AGGR_R1: sent AR1, expecting AI2
pluto[XXXX]: "xripsec1" [1] 10.10.30.1 #1: ignoring informational payload, type INVALID_ID_INFORMATION
```

☞ IKE/ISAKMP ポリシーの設定のインタフェースの ID で設定した値が対向機器で設定した ID と一致しているか確認してください。

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "xripsec1" #1: initiating Aggressive Mode
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: initiate
pluto[XXXX]: "xripsec1" #1: no suitable connection for peer '@test'
pluto[XXXX]: "xripsec1" #1: sending notification INVALID_ID_INFORMATION to 10.10.10.1:500
```

☞ 本装置側の設定のインタフェース ID で設定した値が対向機器で設定した ID と一致しているか確認してください。

➤ フェーズ2の ID 不一致

＜レスポンス側のログ出力例＞

```
pluto[XXXX]: "xripsec1" [1] 10.10.30.1 #1: responding to Aggressive Mode, state #1, connection "xripsec1"
pluto[XXXX]: "xripsec1" [1] 10.10.30.1 #1: STATE_AGGR_R1: sent AR1, expecting AI2
pluto[XXXX]: "xripsec1" [1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "xripsec1" [1] 10.10.30.1 #1: cannot respond to IPsec SA request because no connection is known for 192.168.100.0/24===10.10.10.1...10.10.30.1[@ipsec2]===192.168.30.0/24
pluto[XXXX]: "xripsec1" [1] 10.10.30.1 #1: sending encrypted notification INVALID_ID_INFORMATION to 10.10.30.1:500
```

☞ IPsec ポリシーの設定で設定した値が対向機器と対になっているか確認してください。

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "xripsec1" #1: initiating Aggressive Mode
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: initiate
pluto[XXXX]: "xripsec1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "xripsec1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+DISABLEARRIVALCHECK
pluto[XXXX]: "xripsec1" #2: STATE_QUICK_I1: initiate
pluto[XXXX]: "xripsec1" #1: ignoring informational payload, type INVALID_ID_INFORMATION
```

☞ IPsec ポリシーの設定で設定した値が対向機器と対になっているか確認してください。

➤ PFS 設定の不一致(レスポンス側でのみ PFS を設定)

＜レスポンス側のログ出力例＞

```
pluto[XXXX]: "xripsec1" [5] 10.10.30.1 #6: responding to Aggressive Mode, state #6, connection "xripsec1"
pluto[XXXX]: "xripsec1" [5] 10.10.30.1 #6: STATE_AGGR_R1: sent AR1, expecting AI2
pluto[XXXX]: "xripsec1" [5] 10.10.30.1 #6: ISAKMP SA established
pluto[XXXX]: "xripsec1" [5] 10.10.30.1 #7: we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION
pluto[XXXX]: "xripsec1" [5] 10.10.30.1 #7: sending encrypted notification NO_PROPOSAL_CHOSEN to 10.10.30.1:500
```

☞ IPsec ポリシーの設定の PFS 設定が対向機器と一致しているか確認してください。

＜イニシエータ側のログ出力例＞

```
pluto[XXXX]: "xripsec1" #1: initiating Aggressive Mode
pluto[XXXX]: "xripsec1" #1: STATE_AGGR_I1: initiate
pluto[XXXX]: "xripsec1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "xripsec1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+DISABLEARRIVALCHECK
pluto[XXXX]: "xripsec1" #2: STATE_QUICK_I1: initiate
pluto[XXXX]: "xripsec1" #1: ignoring informational payload, type NO_PROPOSAL_CHOSEN
```

(☞) IPsec ポリシーの設定の PFS 設定が対向機器と一致しているか確認してください。

GRE 状態確認方法

[NXR]

● ステータスの確認

show interface コマンドでトンネルインタフェースがアップしているか確認することができます。

また show interface コマンドの後に tunnel <インタフェースナンバ>を指定することによりトンネルインタフェース毎にどのトンネルインタフェースが GRE または IPinIP で動作しているかなどの情報を確認することができます。

<実行例>

```
nrx120#show interface tunnel 1
tunnel1
    Link encap:GREIP Tunnel
    inet6 addr: fe80::xxx:xxxx:xxx:xxx/64 Scope:Link
    UP POINTOPOINT RUNNING NOARP  MTU:1476  Metric:1
    RX packets:50894 errors:0 dropped:0 overruns:0 frame:0
    TX packets:72219 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:32969347 (31.4 Mb)  TX bytes:64757919 (61.7 Mb)

tunnel1: gre/ip  remote 10.10.20.1  local 10.10.10.1  ttl 255  tos inherit pmtudisc
RX: Packets      Bytes      Errors CsumErrs OutOfSeq Mcasts
   50894        32969347      0      0      0      0
TX: Packets      Bytes      Errors DeadLoop NoRoute  NoBufs
   72219        64757919      0      0      0      0
```

[XR]

● ステータスの確認

GRE の各トンネル状況を一覧で確認する場合は、設定メニューで「GRE 設定」をクリックすると GRE 一覧表示が表示されます。

GRE インタフェースのリンクアップ状況は LinkState の下にある up, down で確認することができます。

GREの設定

GRE設定Index

一覧表示

[1-32]

[33-64]

GRE-インタフェース設定

GRE1

GRE2

GRE3

GRE4

GRE5

GRE6

GRE7

GRE8

GRE9

GRE10

GRE11

GRE12

GRE13

GRE14

GRE15

GRE16

GRE17

GRE18

GRE19

GRE20

GRE21

GRE22

GRE23

GRE24

GRE25

GRE26

GRE27

GRE28

GRE29

GRE30

GRE31

GRE32

GRE一覧表示

Interface 名	Interface Address	Remote Address	Local Address	Peer Address	MTU	ID Key	Check sum	PMTUD	ICMP	KeepAlive	Link State
gre1	172.16.102/30	1010101	1010201	172.16.101/30	1430		無効	有効	有効	無効	up
gre2	172.16.106/30	1010301	1010401	172.16.105/30	1430		無効	有効	有効	無効	down

各 GRE インタフェースの情報を確認する場合は、当該 GRE インタフェース設定の一番下にある「現在の状態」をクリックします。

現在の状態

Tunnel is up, Link is up

追加/変更

削除

<表示例>

GRE1 トンネルパラメータ情報

```
gre1: gre/ip  remote 10.10.10.1  local 10.10.20.1  ttl 255
keepalive not set.
RX: Packets      Bytes      Errors CsumErrs OutOfSeq Mcasts
    0            0            0      0      0      0
TX: Packets      Bytes      Errors DeadLoop NoRoute  NoBufs
    0            0            0      0      0      0
```

GRE1 トンネルインタフェース情報

```
gre1      Link encap:UNSPEC  HWaddr 0A-0A-14-01-BF-28-BF-FF-00-00-00-00-00-00-00
inet addr:172.16.10.2  P-t-P:172.16.10.1  Mask:255.255.255.252
UP POINTOPOINT RUNNING NOARP  MTU:1430  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

L2TPv3 状態確認方法

[NXR]

● ステータスの確認

L2TPv3 の情報を表示する場合は show l2tpv3 コマンドを使用します。

<実行例>

```
NXR_B#show l2tpv3

***** Global Information *****
MAC Learning enable(always), LoopDetect disable, known-unicast drop
RouterID is 172.20.30.1, Hostname is nxrb
snmp disable(disconnect) Trap disable
IP ToS configuration disable, Tunnel ToS is 0x00
fast-forwarding disable

***** Interface Information *****
NumXconnectInterfaces 1
Interface name is ethernet0, Interface is up, link status is up
LoopDetect is disable, known-unicast drop
      164 Frame Sent,          0 dropped,          0 errors
      165  received,          0 dropped,          0 known-unicast Frame

***** MAC Table Information *****
Interface ethernet0, NumMACs 1
HW Addr          time(sec)
XX:XX:XX:XX:XX:ca      299

***** FDB Information *****
attached Interface ethernet0, NumMACs 1
HW Addr          time(sec)      Session ID
XX:XX:XX:XX:XX:39      299      3702885691

***** Group Information *****
NumL2TPGroups 1
Group ID 1
preempt is disable
hold is disable
mac advertise is enable
Primary Xconnect      : PeerID(172.20.10.1), RemoteEND ID(1)
Secondary Xconnect    : PeerID(172.20.20.1), RemoteEND ID(1)
Primary Session ID    : 3702885691
Secondary Session ID  : 614246102
Active Session ID     : 3702885691

***** Tunnel/Session Information *****
NumL2TPTunnels 2
Tunnel MyID 296340432 AssignedID 3833487957 NumSessions 1 PeerIP 10.10.20.1 State established
Session LAC(S) MyID 614246102 AssignedID 3826302678 State established
Interface name is ethernet0, type is Ethernet
Circuit state is DOWN (local is down, Remote is up)
Group ID 1, Group State is Stand-by
      0 Packets sent,          0 dropped,          0 errors
      0  received,          0 dropped,          0 errors

Tunnel MyID 2323886230 AssignedID 2847244914 NumSessions 1 PeerIP 10.10.10.1 State established
Session LAC(S) MyID 3702885691 AssignedID 305076802 State established
Interface name is ethernet0, type is Ethernet
Circuit state is UP (local is up, Remote is up)
```

Group ID 1, Group State is Active		
165 Packets sent,	0 dropped,	0 errors
164 received,	0 dropped,	0 errors

「Tunnel ...State established」が確立したトンネルを、「Session ...te established」が確立したセッションを示しています。

また show l2tpv3 コマンドで表示される項目のうち、一部の項目のみ表示させることも可能です。
以下は L2TPv3 セッションの確立状況を確認する show l2tpv3 session コマンドを使用した例になります。
なお show l2tpv3 session コマンドの後に detail を指定することにより、より詳細なステータスを表示させることもできます。

＜実行例＞

```
NXR_B#show l2tpv3 session

Session Information Total tunnels 2 sessions 2

Tunnel MyID 296340432 AssignedID 3833487957
Session LAC(S) MyID 614246102 AssignedID 3826302678 State established
Interface name is ethernet0, type is Ethernet
Circuit state is DOWN (local is down, Remote is up)
Group ID 1, Group State is Stand-by
          0 Packets sent,          0 dropped,          0 errors
          0 received,            0 dropped,          0 errors

Tunnel MyID 2323886230 AssignedID 2847244914
Session LAC(S) MyID 3702885691 AssignedID 305076802 State established
Interface name is ethernet0, type is Ethernet
Circuit state is UP (local is up, Remote is up)
Group ID 1, Group State is Active
          280 Packets sent,          0 dropped,          0 errors
          279 received,            0 dropped,          0 errors
```

● ログの確認

ログは show syslog message コマンドで確認することができます。
(🔍) ここで設定しているシスログのプライオリティは info(初期値)となります。このプライオリティを debug に変更することによりより多くのログが出力されます。

L2TPv3 接続完了時には以下のようなログが出力されます。

＜出力例＞

```
l2tpv3[XXXX]: L2TP Session Established
l2tpv3[XXXX]: Peer IP = 10.10.10.1
l2tpv3[XXXX]: Peer ID = 172.20.10.1
l2tpv3[XXXX]: Remote END ID = 1
l2tpv3[XXXX]: Local Tunnel/Session ID = 2760457796/2128401404
l2tpv3[XXXX]: Remote Tunnel/Session ID = 544941557/1701490145
```

L2TPv3 セッションが確立したことを示す「L2TP Session Established」が出力されます。

L2TPv3 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

- L2TPv3 のホスト名やルータ ID が不一致

＜出力例＞

```
I2tpv3[XXXX]: Error: Peer 10.10.10.1 Authentication fail for create a tunnel
```

(☞) I2tpv3 hostname, I2tpv3 router-id コマンドで設定した値が対向機器と対になっているか確認してください。

➤ 対向からの応答がない(リスケジュール設定で再ネゴシエーションを行う)

<出力例>

```
I2tpv3[XXXX]: Error: Too many retransmissions on tunnel (2038817815/0); closing down  
I2tpv3[XXXX]: rescheduled I2tpv3 negotiation after 30sec
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、L2TP のフィルタは許可されているか L2TPv3 のサービスが起動しているかなどのポイントを確認してください。

[XR]

● ステータスの確認

L2TPv3 の情報を表示する場合は、設定メニューで「各種サービスの設定」をクリックしサービス一覧の左側の「L2TPv3」をクリックします。そして L2TPv3 ステータス表示→すべてのステータス情報表示の「表示する」をクリックします。

<実行例>

L2TPv3 Status 情報

***** Global Information *****

MAC Learning enable, LoopDetect disable, known-unicast drop
RouterID is 172.20.20.1, Hostname is xra
snmp disable(disconnect) Trap disable

***** Interface Information *****

NumXconnectInterfaces 1

Interface name is eth0, Interface is up, link status is up

LoopDetect is disable, known-unicast drop

L2RP disable

33587 Frame Sent,	0 dropped,	0 errors
14444 received,	5 dropped,	0 known-unicast Frame

***** MAC Table Information *****

Interface eth0, NumMACs 1

HW Addr	time(sec)
---------	-----------

XX:XX:XX:XX:XX:39	299
-------------------	-----

***** FDB Information *****

attached Interface eth0, NumMACs 1

HW Addr	time(sec)	Session ID
XX:XX:XX:XX:XX:ca	279	2061667679

***** Group Information *****

NumL2TPGroups 1

Group ID 32630

preempt is disable

hold is disable

Primary Xconnect : PeerID(172.20.10.1), RemoteEND ID(1)

Secondary Xconnect : n/a

Primary Session ID : 2061667679

Secondary Session ID : n/a

Active Session ID : 2061667679

***** Tunnel/Session Information *****

NumL2TPTunnels 1

```
Tunnel MyID 233151615 AssignedID 1171543176 NumSessions 1 PeerIP 10.10.10.1 State established
Session LAC(S) MyID 2061667679 AssignedID 2518366705 State established
Interface name is eth0, type is Ethernet
Circuit state is UP (local is up, Remote is up)
Group ID 32630, Group State is Active
      14444 Packets sent,          0 dropped,          0 errors
      33655   received,          0 dropped,          0 errors
```

「Tunnel ...State established」が確立したトンネルを、「Session ...te established」が確立したセッションを示しています。

● ログの確認

ログは show syslog message コマンドで確認することができます。

(☞) ここで設定しているシスログのプライオリティは info(初期値)となります。このプライオリティを debug に変更することによりより多くのログが出力されます。

L2TPv3 接続完了時には以下のようなログが出力されます。

<出力例>

```
I2tpv3[XXXX]: L2TP Session Established
I2tpv3[XXXX]: Peer IP = 10.10.20.1
I2tpv3[XXXX]: Peer ID = 172.20.20.1
I2tpv3[XXXX]: Remote END ID = 1
I2tpv3[XXXX]: Local Tunnel/Session ID = 2798426619/3632033519
I2tpv3[XXXX]: Remote Tunnel/Session ID = 3172425204/2071486458
```

L2TPv3 セッションが確立したことを示す「L2TP Session Established」が出力されます。

L2TPv3 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

- L2TPv3 のホスト名やルータ ID が不一致

<出力例>

```
I2tpv3[XXXX]: Error: Peer 10.10.10.1 Authentication fail for create a tunnel
```

(☞) L2TPv3 機能設定, L2TPv3 Tunnel 設定で設定した値が対向機器と対になっているか確認してください。

- 対向からの応答がない(リスケジュール設定で再ネゴシエーションを行う)

<出力例>

```
I2tpv3[XXXX]: Error: Too many retransmissions on tunnel (2038817815/0); closing down
I2tpv3[XXXX]: rescheduled I2tpv3 negotiation after 30sec
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、L2TP のフィルタは許可されているか L2TPv3 のサービスが起動しているかなどのポイントを確認してください。

FutureNet サポートデスクへのお問い合わせ

FutureNet 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。

※FutureNet サポートデスク宛にご提供頂きました情報は、製品のお問合せなどサポート業務以外の目的には利用致しません。

なおご提供頂く情報の取り扱いについて制限等がある場合には、お問い合わせ時または事前にその旨ご連絡下さい。(設定ファイルのプロバイダ情報や IPsec の事前共有鍵情報を削除してお送り頂く場合など)

弊社のプライバシーポリシーについては下記 URL の内容をご確認下さい。

<http://www.centurysys.co.jp/company/privacy.html>

<NXR,XR 共通>

■ ご利用頂いている NXR 製品を含むネットワーク構成図

(ご利用頂いている回線やルータを含むネットワーク機器の IP アドレスを記載したもの)

■ 障害・不具合の内容およびその再現手順

(いつどこで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)

□ 問い合わせ内容例1

○月○日○○時○○分頃より拠点 A と拠点 B の間で IPsec による通信ができなくなった。障害発生前までは問題なく利用可能だった。現在当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通は確認できたが、対向ルータの LAN 側 IP アドレス、配下の端末に対しては Ping による疎通は確認できない。障害発生前後で拠点 B のバックアップ回線としてモバイルカードを接続し、ppp1 インタフェースの設定を行った。設定を元に戻すと通信障害は解消する。

機器の内蔵時計は NTP で同期を行っている。

□ 問い合わせ内容例2

- 発生日時

○月○日○○時○○分頃

- 発生拠点

拠点 AB 間

- 障害内容

IPsec による通信ができなくなった。

- 切り分け内容

ルータ配下の端末から当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通確認可能。

対向ルータの LAN 側 IP アドレス、配下の端末に対しては Ping による疎通確認不可。

- 障害発生前後での作業

ルータの設定変更やネットワークに影響する作業は行っていない。

- 備考

障害発生前までは問題なく利用可能だった。

機器の内蔵時計は拠点 A の機器で 10 分、拠点 B の機器で 5 分遅れている。

□ 問い合わせ内容例3

現在 IPsec の設定中だが、一度も IPsec SA の確立および IPsec の通信ができていない。IPsec を設定している拠点からのインターネットアクセスおよび該当拠点への Ping による疎通確認も可能。設定例集および設定例集内のログ一覧は未確認。

□ 良くない問い合わせ内容例1

VPN ができない。

→VPN として利用しているプロトコルは何か。VPN のトンネルが確立できないのか、通信ができないのかなど不明。

□ 良くない問い合わせ内容例2

通信ができない。

→どのような通信がいつどこでできない(またはできなくなった)のかが不明。

<NXR>

※情報を取得される前に

シリアル接続で情報を取得される場合は取得前に下記コマンドを実行してください。

#terminal width 180(初期値に戻す場合は terminal no width)

■ ご利用頂いている NXR 製品での不具合発生時のログ

ログは以下のコマンドで出力されます。

#show syslog message

■ ご利用頂いている NXR 製品のテクニカルサポート情報の結果および設定ファイル

テクニカルサポート情報は以下のコマンドで出力されます。

show tech-support

■ 障害発生時のモバイル関連コマンドの実行結果(モバイルカード利用時のみ)

#show mobile <N> ap

#show mobile <N> phone-number

#show mobile <N> signal-level

※<N>はモバイルデバイスナンバ

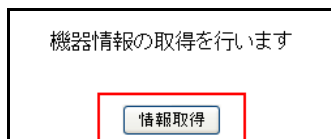
<XR>

■ テクニカルサポート情報(一部対応機種のみ)

※テクニカルサポート情報では設定ファイル、ログ、インフォメーション(情報表示や IPsec 情報など一部情報をマージしたもの)

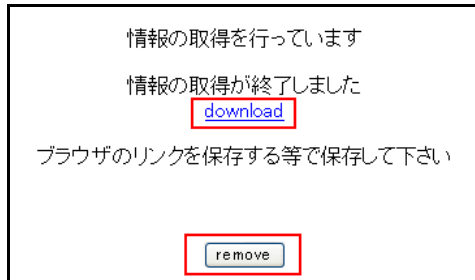
テクニカルサポート情報は以下方法で取得します。

設定メニューで「テクニカルサポート」をクリックします。



「download」を右クリックしリンク先の保存を使用して取得します。(ダウンロード後は「remove」をクリックして

作成したルータ内のファイルを削除してください)

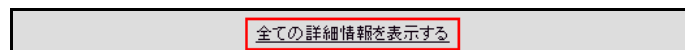


■ 詳細情報表示(一部対応機種のみ)

詳細情報表示は以下方法で取得します。

設定メニューで「詳細情報表示」をクリックします。

画面一番下の「全ての詳細情報を表示する」をクリックし、表示された情報を右クリックして全て選択した状態で再度右クリックして内容をコピーし、テキストエディタ等に内容をペースト(貼り付け)します。



※詳細情報表示に対応していない場合は、各サービスの設定からステータス情報を取得してください。

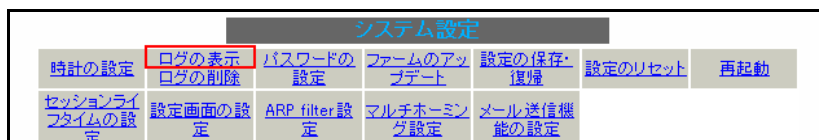
取得方法はご利用中の製品のユーザーズガイドをご参照下さい。

■ ご利用頂いている XR 製品での不具合発生時のログ

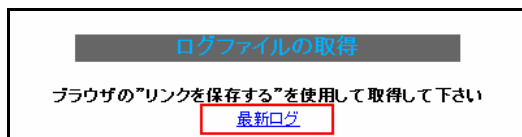
※テクニカルサポート情報機能がある場合は不要です。

ログは以下方法で取得します。

設定メニューで「システム設定」をクリックし、システム設定で「ログの表示」をクリックします。



画面一番下の「最新ログ」を右クリックしリンク先の保存を使用して取得します。(バックアップログがある場合は同様に右クリックしリンク先の保存を使用して取得します)

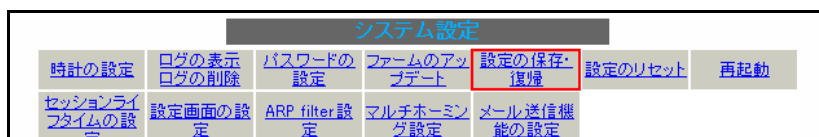


■ ご利用頂いている XR 製品の設定ファイル

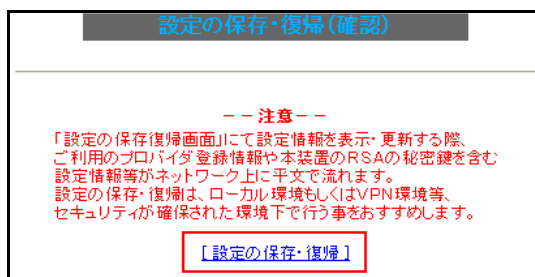
※テクニカルサポート情報機能がある場合は不要です。

設定ファイルは以下方法で取得します。

設定メニューで「システム設定」をクリックし、システム設定で「設定の保存・復帰」をクリックします。



設定の保存・復帰(確認)画面で「設定の保存・復帰」をクリックします。



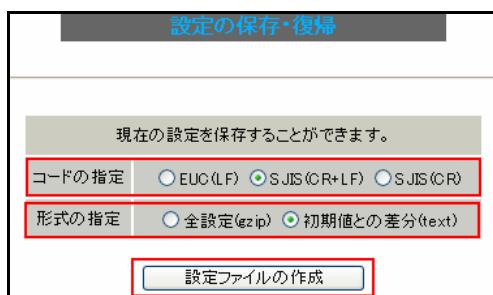
設定の保存・復元(確認)

--- 注意 ---

「設定の保存・復元画面」にて設定情報を表示・更新する際、ご利用のプロバイダ登録情報や本装置のRSAの秘密鍵を含む設定情報等がネットワーク上に平文で流れます。設定の保存・復元は、ローカル環境もしくはVPN環境等、セキュリティが確保された環境下で行う事をおすすめします。

[設定の保存・復元]

設定の保存・復元画面で「設定ファイルの作成」をクリックします。(コードの指定、形式の指定は任意)



設定の保存・復元

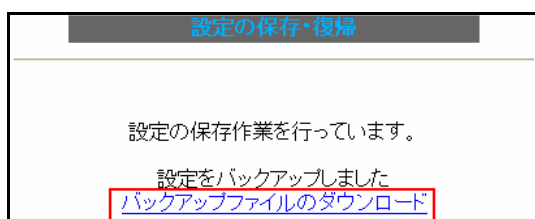
現在の設定を保存することができます。

コードの指定 ☐ EUC(LF) ☒ S-JIS(CR+LF) ☐ S-JIS(CR)

形式の指定 ☐ 全設定(gzip) ☒ 初期値との差分(text)

設定ファイルの作成

「バックアップファイルのダウンロード」を右クリックしリンク先の保存を使用して取得します。



設定の保存・復元

設定の保存作業を行っています。

設定をバックアップしました

[バックアップファイルのダウンロード](#)

上記情報取得の方法はご利用中の製品のユーザーズガイドにも記載されておりますので、そちらも合わせてご参照下さい。

FutureNet 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 NXR,XR シリーズ

VPN 相互接続設定例集

Ver 1.0.0

2012 年 4 月

発行 センチュリー・システムズ株式会社

Copyright(c) 2009-2012 Century Systems Co., Ltd. All Rights Reserved.
