



BR500S Webリファレンス

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットや LAN をさらに活用するために、本装置をご利用ください。

2008年9月

本装置の外観・仕様は、予告なしに変更することがあります。

本装置は日本国内用に設計されています。海外では使用できません。

This equipment is designed for use in Japan only and cannot be used in any other country.

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。

従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

Microsoft Corporation のガイドラインに従って画面写真を使用しています。

本書の内容につきましては万全を期しておりますが、お気づきの点がございましたら、当社のサービス取扱所へお申しつけください。

© 2008 NTTEAST・NTTWEST

目次

はじめに	2
本書の使いかた	5
本書の読者と前提知識	5
本書における商標の表記について	5
1 「設定メニュー」を表示する	6
2 インターネットへISDN 接続かんたん設定	7
2.1 必須設定	7
2.2 オプション設定	8
3 インターネットへ専用線接続かんたん設定	10
3.1 必須設定	10
3.2 オプション設定	10
4 PPPoE かんたん設定	12
4.1 必須設定	12
4.2 オプション設定	12
5 オフィスへISDN 接続かんたん設定	14
5.1 必須設定	14
5.2 オプション設定	15
6 オフィスへ専用線接続かんたん設定	16
6.1 必須設定	16
6.2 オプション設定	16
7 プライベートLAN 構築かんたん設定	18
7.1 必須設定	18
7.2 オプション設定	19
8 セグメント接続／分割かんたん設定	20
8.1 LAN0	20
8.2 LAN1	20
9 パスワード情報	21
10 装置情報	22
10.1 ルータ名称情報	22
10.2 タイムサーバ情報	23
10.3 システムログ情報	24
10.4 SNMP 情報	25
10.5 ファームウェア更新情報	28
10.6 異常時動作情報	29
10.7 ループバック情報	30
10.8 サーバ機能情報	31
11 スケジュール情報	33
11.1 月間／週間予約情報	33
11.2 電話番号変更予約情報	35
11.3 構成定義切り替え予約情報	36
12 WAN 情報	37
13 LAN 情報	43
13.1 共通情報	44
13.2 IP 関連	54
13.3 IPv6 関連	80
13.4 ブリッジ関連	95
13.5 MPLS 関連	98
14 シリアル情報	102
14.1 共通情報	102

14.2	モデム情報	103
15	相手情報	104
15.1	ネットワーク情報	104
15.2	共通情報	105
15.3	接続先情報	107
15.4	PPP 関連	137
15.5	IP 関連	139
15.6	IPv6 関連	163
15.7	ブリッジ関連	182
15.8	MPLS 関連	185
15.9	着信相手識別情報	188
16	テンプレート情報	189
17	AAA 情報	210
17.1	グループ ID 情報	210
17.2	AAA ユーザ情報	211
18	ルーティングプロトコル情報	217
18.1	インタフェース情報	217
18.2	ルーティングマネージャ情報	217
18.3	RIP 関連	223
18.4	BGP 関連	228
18.5	OSPF 関連	240
18.6	IPv6 ルーティングマネージャ情報	251
18.7	IPv6 RIP 関連	253
19	マルチキャスト情報	256
19.1	IP マルチキャスト情報	256
19.2	IP マルチキャストスタティック経路情報	258
20	UPnP 情報	259
20.1	基本情報	259
21	MPLS 情報	260
21.1	基本情報	260
22	ブリッジ情報	261
22.1	ブリッジグループ情報	261
23	ProxyDNS 情報 / URL フィルタ情報	265
23.1	順引き情報	266
23.2	逆引き情報	268
24	ホストデータベース情報	270
索引	272

本書の使いかた

本書では、本装置の設定メニューで表示される画面について説明しています。

また、CD-ROMの中の README ファイルには大切な情報が記載されていますので、併せてお読みください。


本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。


本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。


マークについて


本書で使用しているマーク類は、以下のような内容を表しています。


 **ヒント** 本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。

こんな事に気をつけて 本装置をご使用になる際に、注意していただきたいことを説明しています。

 **補足** 操作手順で説明しているものの他に、補足情報を説明しています。

 **参照** 操作方法など関連事項を説明している箇所を示します。

 **警告** 製造物責任法 (PL) 関連の警告事項をあらわしています。本装置をお使いの際は必ず守ってください。

 **注意** 製造物責任法 (PL) 関連の注意事項をあらわしています。本装置をお使いの際は必ず守ってください。

本書における商標の表記について

Microsoft、Windows および Windows NT は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

Windows[®] XP の正式名称は、Microsoft[®] Windows[®] XP Professional operating system、または Microsoft[®] Windows[®] XP Home Edition operating system です。

Windows[®] Me の正式名称は、Microsoft[®] Windows[®] Millennium Edition operating system です。

Windows[®] 98 の正式名称は、Microsoft[®] Windows[®] 98 operating system です。

Windows[®] 95 の正式名称は、Microsoft[®] Windows[®] 95 operating system です。

Windows[®] 2000 の正式名称は、Microsoft[®] Windows[®] 2000 Server Network operating system、または Microsoft[®] Windows[®] 2000 Professional operating system です。

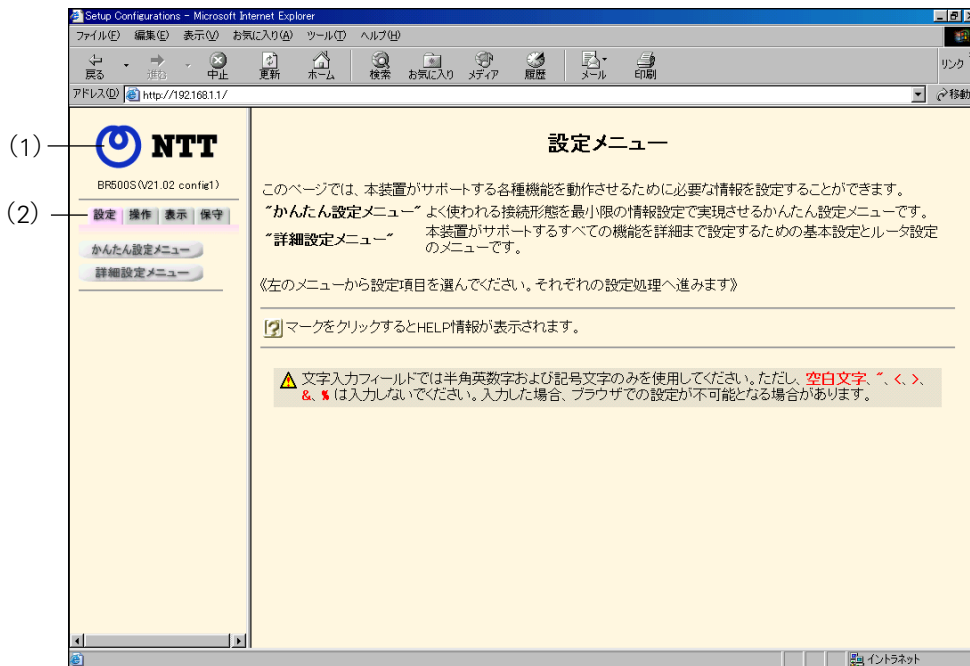
Windows NT[®] 4.0 の正式名称は、Microsoft[®] Windows NT[®] Server network operating system Version 4.0、または Microsoft[®] Windows NT[®] Workstation operating system Version 4.0 です。

MD5 は、RSA Security Inc. が開発した暗号およびハッシュアルゴリズムです。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

1 「設定メニュー」を表示する

「かんたん設定」をサポートしているかどうかで「設定」タブをクリックしたときに表示される画面が異なります。



画面左側に表示されるタブをクリックすると、ブラウザの表示が変わります。

- (1) 本装置ロゴ : クリックすると、トップページが表示されます。
- (2) 「設定」タブ : クリックすると、「かんたん設定メニュー」ボタンと「詳細設定メニュー」ボタンが表示されます。

☛ 参照 [操作] タブ、[表示] タブおよび [保守] タブについて
BR500S Web ユーザーズガイド「[2.1 操作メニューを使う](#)」(P.17)、[「2.2 表示メニューを使う](#)」(P.23)、[「2.3 保守メニューを使う](#)」(P.96)

こんな事に気をつけて

文字入力フィールドでは、半角文字 (0～9、A～Z、a～z および記号) だけを使用してください。ただし、空白文字、「**]**」、「**<**」、「**>**」、「**&**」、「**%**」は入力しないでください。

☛ 参照 BR500S Web ユーザーズガイド「[1.5 文字入力フィールドで入力できる文字一覧](#)」(P.12)

2 インターネットへISDN接続かんたん設定

[操作] 「設定メニュー」 → [かんたん設定メニュー] → インターネットへ「ISDN接続」

インターネットへISDN接続かんたん設定 ?

⚠ 基本設定およびルータ設定で設定した情報は無効になります。

■ 必須設定 ?

接続先の電話番号	<input type="text"/>
ユーザ認証ID	<input type="text"/>
ユーザ認証パスワード	<input type="password"/>

■ オプション設定 ?

IPアドレス	<input type="text" value="192.168.3.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
DNSサーバ	<input checked="" type="checkbox"/> 自動取得 <input type="text"/>
接続先の電話番号2	<input type="text"/>
接続先の電話番号3	<input type="text"/>
常時接続機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない 無通信監視タイム <input type="text" value="0"/> 秒 課金単位時間 <input type="text" value="0"/>
接続先ネットワーク名	<input type="text" value="rmt1"/>
接続先名	<input type="text" value="ep0-0"/>
アドレス変換	<input type="radio"/> 使用しない <input checked="" type="radio"/> マルチNAT UPnP機能 <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
MP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
かんたんフィルタ	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

2.1 必須設定

接続先の電話番号

半角数字32桁以内で指定します。－、(、) が区切り文字として使用できます。

《指定例》

01-2345-6789

01(2345)6789

ユーザ認証ID

接続先より通知されたIDを半角英数字64文字以内で指定します。

ユーザ認証パスワード

接続先より通知されたパスワードを半角英数字64文字以内で指定します。

2.2 オプション設定

IP アドレス／ネットマスク

本装置の IP アドレスとネットマスクを指定します。ただし、既存のネットワークに接続するのでなければ、修正は不要です。

IP アドレスに 0.0.0.0 を指定すると通信ができなくなります。

DNS サーバ

必要に応じて接続先、またはネットワーク管理者に指示された DNS サーバの IP アドレスを指定します。指定する値は DHCP サーバ機能により広報されます。省略、または 0.0.0.0 を指定する場合は、広報を行いません。また、“自動取得” をチェックする場合は、本装置の IP アドレスを DNS サーバアドレスとして広報します。実際の DNS サーバアドレスは回線接続時に相手システムより取得し、ProxyDNS 機能が名前解決を行います。自動取得は相手システムが DNS サーバアドレスの広報機能 (RFC1877) をサポートしている場合にだけ使用できます。

接続先の電話番号 2 / 3

マルチダイヤルを行う場合に指定します。記述方法は、接続先の電話番号と同じです。

常時接続機能

インターネットへ ISDN 接続機能を使用して常時接続する場合は“使用する”を選択します。

無通信監視タイマ

ISDN 回線の無通信監視タイマを 0～3600 秒の範囲で指定します。その時間を超えても、通信が行われなかった場合は、ISDN 回線を自動的に切断します。なお、0 を指定した場合は、自動切断を行いません。

課金単位時間

課金単位時間を 0.0～3600.0 秒の範囲で指定します。ここで指定する時間は無通信監視による回線切断のときに参照され、同じ料金で最大の接続時間を得よう回線切断タイミングを調整します。なお、0 を指定した場合は、課金単位の調整を行いません。

接続ネットワーク名

ネットワークを識別する名称を半角英数字 8 文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字 8 文字以内で指定します。

アドレス変換

1 つのグローバル側 IP アドレスを使用して、複数台のパソコンからネットワークにアクセスする場合は、“マルチ NAT” を選択します。

UPnP 機能

UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合は“使用する”を選択します。

MP

MP 接続をする場合は、“使用する”を選択します。“使用する”を選択した場合は、データ通信量に応じて適宜増減します。

かんたんフィルタ

かんたんフィルタは、通常の使用方法で起こりやすい以下の問題を回避するためのIPフィルタを簡単に設定できます。

Windows NT[®]、Windows[®] 95などによるMicrosoft Networkを使用している場合、お客様のネットワーク設定によっては、NetBIOS over TCPによって定期的に出送されるパケットにより自動発信してしまう場合があります。この問題を回避するために、NetBIOS over TCPが使用するTCPおよびUDPのサービスポートの137～139を遮断するフィルタを設定します。

ping (ICMP echo) などのコマンドにより自動発信してしまう場合があります。この問題を回避するために、ICMP プロトコルによる自動発信を抑止するフィルタを設定します。なお、回線が接続状態にあるときには、ICMP パケットを通過させます。

syslog、TIME、NTP (SNTP) により自動発信してしまう場合があります。この問題を回避するために、それぞれのプロトコルによる自動発信を抑止するフィルタを設定します。なお、回線が接続状態にあるときには、それぞれのパケットを通過させます。

Windows[®] 2000から本装置を経由してインターネットへ接続する場合、Windows[®] 2000が送信する予期しないDNSパケットにより自動発信してしまう場合があります。この問題を回避するために、ProxyDNS 情報に問い合わせタイプがSOA (6)、SRV (33) のDNSパケットを破棄するフィルタ、ホストデータベース情報にIPアドレスが「127.0.0.1」のホスト名は「localhost」を設定します。

3 インターネットへ専用線接続かんたん設定

[操作] 「設定メニュー」 → [かんたん設定メニュー] → インターネットへ「専用線接続」

インターネットへ専用線接続かんたん設定 ?

⚠ 基本設定およびルータ設定で設定した情報は無効になります。

■ 必須設定 ?

IPアドレス	<input type="text" value="192.168.1.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
使用する回線速度	<input checked="" type="radio"/> 64Kbps <input checked="" type="radio"/> 128Kbps
DNSサーバ	<input type="text"/>

■ オプション設定 ?

接続ネットワーク名	<input type="text" value="rmt0"/>
接続先名	<input type="text" value="ap0-0"/>
ドメイン名	<input type="text"/>
アドレス変換	<input checked="" type="radio"/> 使用しない <input type="radio"/> マルチNAT
	グローバルアドレス <input type="text"/>
	アドレス個数 <input type="text" value="1"/> 個
	UPnP機能 <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

設定終了
キャンセル

3.1 必須設定

IPアドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。マルチNATを使用する場合は、ローカルなIPアドレス、使用しない場合は、プロバイダから割り当てられたIPアドレスを指定します。

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

使用する回線速度

使用する回線速度を選択します。

DNSサーバ

接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。0.0.0.0を指定した場合は、広報を行いません。

3.2 オプション設定

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字8文字以内で指定します。

ドメイン名

必要に応じて接続先、またはネットワーク管理者に指示されたドメイン名を半角英数字80文字以内で指定します。省略時は、DHCPサーバによる広報を行いません。

アドレス変換

マルチ NAT を使用すると、プロバイダから取得している IP アドレス個数以上の端末を利用できます。使用する場合は、“マルチ NAT” を選択します。WAN 側に固定のアドレスを1つ、または複数持っている場合は、“グローバルアドレス” と “アドレス個数” を設定します。

グローバルアドレス

グローバルアドレスを先頭とする “アドレス個数” 分のアドレスが本装置の WAN IP アドレスとなります。

アドレス個数

1～16の範囲で指定します。


UPnP 機能


UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合は “使用する” を選択します。

4 PPPoE かんたん設定


[操作] 「設定メニュー」 → [かんたん設定メニュー] → インターネットへ「PPPoE 接続」

PPPoEかんたん設定

 基本設定およびルータ設定で設定した情報は無効になります。

■ 必須設定 

ユーザ認証ID	<input type="text"/>
ユーザ認証パスワード	<input type="password"/>

■ オプション設定 

IPアドレス	<input type="text" value="192.168.1.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
DNSサーバ	<input type="checkbox"/> 自動取得 <input type="text"/>
接続ネットワーク名	<input type="text" value="rmt0"/>
接続先名	<input type="text" value="ep0-0"/>
PPPoEで使用するインタフェース	<input checked="" type="radio"/> LAN0 <input type="radio"/> LAN1
常時接続機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 無通信監視タイム <input type="text" value="0"/> 秒
アドレス変換	<input type="radio"/> 使用しない <input checked="" type="radio"/> マルチNAT UPnP機能 <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
LAN0転送レート	<input type="text" value="自動認識"/>
LAN1転送レート	<input type="text" value="自動認識"/>

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

4.1 必須設定

ユーザ認証 ID / パスワード

PPPoE で接続する際に使用する、ユーザ認証 ID とパスワードを 64 桁以内で指定します。

4.2 オプション設定

IP アドレス / ネットマスク

プライベート側の IP アドレスとネットマスクを指定します。本装置では、PPPoE で使用するよう指定したインタフェースの反対側のインタフェースが自動的にプライベート側となります。

DNS サーバ

必要に応じて接続先またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略または0.0.0.0を指定する場合は広報を行いません。また、“自動取得”を選択する場合は、本装置のIPアドレスをDNSサーバアドレスとして広報します。実際のDNSサーバアドレスは回線接続時に相手システムより取得し、ProxyDNS機能が名前解決を行います。自動取得は相手システムがDNSサーバアドレスの広報機能（RFC1877）をサポートしている場合にだけ使用できます。

接続ネットワーク名

ネットワークを識別する名称を8文字以内で指定します。

接続先名

接続先を識別する名称を8文字以内で指定します。

PPPoE で使用するインタフェース

PPPoE で使用するインタフェースを選択します。

常時接続機能

PPPoE を使用して常時接続を行う場合は“使用する”を選択します。

無通信監視タイマ

常時接続機能を使用しない場合の無通信監視タイマを0～3600秒の範囲で指定します。ここで指定した時間に通信が行われなかった場合、自動的に切断します。0を指定した場合は、自動的に切断しません。

アドレス変換

1つのグローバル側IPアドレスを使用して、複数台のパソコンからネットワークにアクセスする場合は、“マルチNAT”を選択します。

UPnP 機能

UPnP 対応装置やUPnP 対応アプリケーションプログラムを使用する場合は“使用する”を選択します。

LAN0 / 1 転送レート

LANインタフェースに接続するネットワークの転送レートを選択します。“自動認識”を選択した場合、本装置はHUBとのネゴシエーションにより速度と全二重/半二重を自動決定します。固定で指定する場合は、接続されているHUBの仕様に合わせます。


こんな事に気をつけて


“自動認識”は接続ネットワークの環境によって正しく動作しない場合があります。その場合は“自動認識”ではなく固定の設定を行います。

5 オフィスへISDN 接続かんたん設定


[操作] 「設定メニュー」 → [かんたん設定メニュー] → オフィスへ「ISDN 接続」

オフィスへISDN接続かんたん設定

 基本設定およびルータ設定で設定した情報は無効になります。

■ 必須設定 

接続先の電話番号	<input type="text"/>
ユーザ認証ID(発信)	<input type="text"/>
ユーザ認証パスワード(発信)	<input type="text"/>
ユーザ認証ID(着信)	<input type="text"/>
ユーザ認証パスワード(着信)	<input type="text"/>
IPアドレス	<input type="text" value="192.168.1.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/> ▼
相手ルータのIPアドレス	<input type="text" value="192.168.2.1"/>
相手ルータのネットマスク	<input type="text" value="24 (255.255.255.0)"/> ▼

■ オプション設定 

DHCPサーバ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する <input type="text" value="DNSサーバ広報"/>
常時接続機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない 無通信監視タイム <input type="text" value="60"/> 秒 課金単位時間 <input type="text" value="0"/>
接続ネットワーク名	<input type="text" value="rmt1"/>
接続先名	<input type="text" value="jap0-0"/>
MP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
ヘッダ圧縮	<input type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
データ圧縮	<input type="checkbox"/> LZS

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

5.1 必須設定

接続先の電話番号

半角数字32桁以内で指定します。－、(、) が区切り文字として使えます。

《指定例》

01-2345-6789

01(2345)6789

ユーザ認証ID／パスワード（発信）

本装置から発信接続するとき使用する認証IDとパスワードを半角英数字64文字以内で指定します。

ユーザ認証パスワード／パスワード（着信）

本装置から着信接続するとき使用する認証IDとパスワードを半角英数字64文字以内で指定します。

IP アドレス／ネットマスク

本装置の IP アドレスとネットマスクを指定します。ただし、既存のネットワークに接続するのでなければ、修正は不要です。

IP アドレスに 0.0.0.0 を指定すると通信ができなくなります。

相手ルータの IP アドレス／ネットマスク

相手ルータの IP アドレスとネットマスクを指定します。本装置はこの指定で得られるネットワークに対してスタティックルートを指定します。

5.2 オプション設定

DHCP サーバ

DHCP サーバを使用する場合は、“使用する”を選択します。

DNS サーバ広報

必要に応じて接続先、またはネットワーク管理者に指示された DNS サーバの IP アドレスを指定します。指定する値は DHCP サーバ機能により広報されます。省略、または 0.0.0.0 を指定する場合は、広報を行いません。

常時接続機能

オフィスへ ISDN 接続機能を使用して常時接続を行う場合は“使用する”を選択します。

無通信監視タイマ

ISDN 回線の無通信監視タイマを 0～3600 秒の範囲で指定します。その時間を超えても、通信が行われない場合は、ISDN 回線を自動的に切断します。なお、0 を指定した場合は、自動切断を行いません。

課金単位時間

課金単位時間を 0.0～3600.0 秒の範囲で指定します。ここで指定する時間は無通信監視による回線切断のときに参照され、同じ料金で最大の接続時間を得よう回線切断タイミングを調整します。なお、0 を指定した場合は、課金単位の調整を行いません。

接続ネットワーク名

ネットワークを識別する名称を半角英数字 8 文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字 8 文字以内で指定します。

MP

MP 接続をする場合は、“使用する”を選択します。“使用する”を選択した場合は、データ通信量に応じて適宜増減します。

ヘッダ圧縮

送受信するヘッダを圧縮します。ヘッダ圧縮のアルゴリズムは、VJ ヘッダ圧縮 (RFC1144 に準拠) および IP ヘッダ圧縮 (RFC2507 / RFC2508 に準拠) をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

データ圧縮


送受信するデータを圧縮します。データ圧縮のアルゴリズムは、LZS をサポートします。使用する指定の場合も、実際にデータ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

6 オフィスへ専用線接続かんたん設定


[操作] 「設定メニュー」 → [かんたん設定メニュー] → オフィスへ「専用線接続」

オフィスへ専用線接続かんたん設定

▲ 基本設定およびルータ設定で設定した情報は無効になります。

■ 必須設定 

IPアドレス	<input type="text" value="192.168.1.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
相手ルータのIPアドレス	<input type="text" value="192.168.2.1"/>
相手ルータのネットマスク	<input type="text" value="24 (255.255.255.0)"/>
使用する回線速度	<input checked="" type="radio"/> 64Kbps <input checked="" type="radio"/> 128Kbps

■ オプション設定 

接続ネットワーク名	<input type="text" value="rmt1"/>
接続先名	<input type="text" value="ap0-0"/>
DHCPサーバ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する <input type="text" value="DNSサーバ広報"/>
ヘッダ圧縮	<input type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
データ圧縮	<input type="checkbox"/> LZS

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

6.1 必須設定

IPアドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。
IPアドレスに0.0.0.0を指定すると通信ができなくなります。

相手ルータのIPアドレス／ネットマスク

相手ルータのIPアドレスとネットマスクを指定します。
本装置は、この指定で得られるネットワークに対してスタティックルートを指定します。

使用する回線速度

使用する回線速度を選択します。

6.2 オプション設定

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字8文字以内で指定します。

DHCP サーバ

DHCP サーバを使用する場合は、“使用する”を選択します。

DNS サーバ広報

必要に応じて接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略、または0.0.0.0を指定する場合は、広報を行いません。

ヘッダ圧縮

送受信するヘッダを圧縮します。ヘッダ圧縮のアルゴリズムは、VJヘッダ圧縮 (RFC1144 に準拠) およびIPヘッダ圧縮 (RFC2507 / RFC2508 に準拠) をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

データ圧縮

送受信するデータを圧縮します。データ圧縮のアルゴリズムは、LZSをサポートします。使用する指定の場合も、実際にデータ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

7 プライベートLAN構築かんたん設定

[操作] 「設定メニュー」 → [かんたん設定メニュー] → LAN間接続「プライベートLAN接続」

プライベートLAN構築かんたん設定

基本設定およびルータ設定で設定した情報は無効になります。

■必須設定

グローバル側IPアドレス	<input checked="" type="radio"/> DHCPで自動的に取得する <input type="radio"/> 指定する <div style="margin-top: 5px;"> <input type="text" value="IPアドレス"/> <input type="text" value="ネットマスク 2 (192.0.0.0)"/> </div>
プライベート側IPアドレス	<input type="text" value="IPアドレス 192.168.1.1"/> <input type="text" value="ネットマスク 24 (255.255.255.0)"/>
グローバル側インタフェース	<input checked="" type="radio"/> LAN0 <input type="radio"/> LAN1

■オプション設定

デフォルトルータ	<input type="text"/>
DNSサーバアドレス	<input type="text"/>
DHCPサーバ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する <input type="text" value="デフォルトルータ広報 192.168.1.1"/> <input type="text" value="DNSサーバ広報 192.168.1.1"/> <input type="text" value="ドメイン名広報"/>
UPnP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
LAN0転送レート	<input type="text" value="自動認識"/>
LAN1転送レート	<input type="text" value="自動認識"/>

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

7.1 必須設定

グローバル側IPアドレス

このインタフェースのIPアドレスの取得方法を指定します。本装置をDHCPクライアントとして運用する場合は“DHCPで自動的に取得する”を選択します。IPアドレス、ネットマスクを指定する場合は“指定する”を選択し、以下の項目を設定します。

こんな事に気をつけて

- 本装置をDHCPクライアントとして運用するには上流側にDHCPサーバが稼働している必要があります。
- グローバル側IPアドレスで“指定する”で設定すると、RIP情報が流れていないネットワークではデフォルトルータとDNSサーバアドレスを設定する必要があります。

IPアドレス/ネットマスク

本装置のグローバル側のIPアドレスとネットマスクを指定します。

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

プライベート側IPアドレス/ネットマスク

本装置のプライベート側のIPアドレスとネットマスクを指定します。

グローバル側インタフェース

LAN0とLAN1のどちらをグローバル側のインタフェースにするか選択します。

7.2 オプション設定

デフォルトルータ

本装置のデフォルトルータアドレスを指定します。ただし、グローバル側のIPアドレスを“DHCPで自動的に取得する”を選択している場合で、DHCPサーバがデフォルトルータを広報していれば自動的に取得するので指定する必要はありません。“指定する”を選択している場合はこの指定が優先されます。

DNSサーバアドレス

本装置を接続したネットワークの先に存在するDNSサーバアドレスを指定します。ただし、グローバル側のIPアドレスを“DHCPで自動的に取得する”を選択している場合で、DHCPサーバがDNSサーバアドレスを広報していれば自動的に取得するので指定する必要はありません。“指定する”を選択している場合はこの指定が優先されます。

DHCPサーバ

本装置をプライベート側ネットワークのDHCPサーバとして使用する場合は、“使用する”を選択します。

デフォルトルータ広報

DHCPサーバで広報するデフォルトルータのIPアドレスを指定します。省略するか0.0.0.0を指定するとDHCPサーバによる広報を行いません。

DNSサーバ広報

DNSサーバのIPアドレスを指定します。省略するか0.0.0.0を指定するとDHCPサーバによる広報を行いません。ProxyDNSを使用する場合は、本装置のIPアドレスを指定します。

ドメイン名広報

ドメイン名を80文字以内で指定します。省略するとDHCPサーバによる広報を行いません。RFC1034では英数字、“.”、“-”で指定することを推奨しています。

UPnP機能

UPnP対応装置やUPnP対応アプリケーションプログラムを使用する場合は“使用する”を選択します。

LAN0 / 1 転送レート

LANインタフェースに接続するネットワークの転送レートを選択します。“自動認識”を選択した場合、本装置はHUBとのネゴシエーションにより速度と全二重/半二重を自動決定します。固定で指定する場合は、接続されているHUBの仕様に合わせます。

こんな事に気をつけて

“自動認識”は接続ネットワークの環境によって正しく動作しない場合があります。その場合は“自動認識”ではなく固定の設定を行ってください。

8 セグメント接続／分割かんたん設定

[操作] 「設定メニュー」 → [かんたん設定メニュー] → LAN間接続「セグメント接続／分割」

セグメント接続／分割かんたん設定 ?

▲ 基本設定およびルータ設定で設定した情報は無効になります。

LAN0 ?

IPアドレス	<input type="text" value="192.168.0.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
転送レート	<input type="text" value="自動認識"/>

LAN1 ?

IPアドレス	<input type="text" value="192.168.1.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
転送レート	<input type="text" value="自動認識"/>

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

8.1 LAN0

LAN0に接続するネットワークの設定を行います。

IPアドレス／ネットマスク

LAN0側のネットワークで使用する装置のIPアドレス／ネットマスクを指定します。

転送レート

LAN0側のネットワークの転送レートを選択します。“自動認識”を選択した場合、本装置はHUBとのネゴシエーションにより速度と全二重／半二重を自動決定します。固定で指定する場合は、接続されているHUBの仕様に合わせます。

こんな事に気をつけて

“自動認識”は接続ネットワークの環境によって正しく動作しない場合があります。その場合は“自動認識”ではなく固定の設定を行ってください。

8.2 LAN1

LAN1に接続するネットワークの設定を行います。

IPアドレス／ネットマスク

LAN1側のネットワークで使用する装置のIPアドレス／ネットマスクを指定します。

転送レート

LAN1側のネットワークの転送レートを選択します。“自動認識”を選択した場合、本装置はHUBとのネゴシエーションにより速度と全二重／半二重を自動決定します。固定で指定する場合は、接続されているHUBの仕様に合わせます。

こんな事に気をつけて

“自動認識”は接続ネットワークの環境によって正しく動作しない場合があります。その場合は“自動認識”ではなく固定の設定を行ってください。


9 パスワード情報

[操作] 「設定メニュー」→基本設定「パスワード情報」

パスワード情報

この装置に対するパスワードを設定できます。
 管理者パスワードを設定した場合、設定メニューでは必ず管理者パスワードを問合わせるようになります。ユーザパスワードは、設定メニュー以外で利用できるパスワードです。設定メニュー以外でパスワードを問合わせるかどうか、および、どのパスワードが利用できるかを設定できます。

なお、コンソール、TELNET および FTP によるログイン時にもこのパスワードが使用されます。

■パスワード情報 

管理者パスワード	<input type="text"/>
管理者パスワードの確認	<input type="text"/>
ユーザパスワード	<input type="text"/>
ユーザパスワードの確認	<input type="text"/>
パスワード入力	操作メニュー <input type="radio"/> 管理者のみ <input type="radio"/> 管理者とユーザ <input type="radio"/> 不要
	表示メニュー <input type="radio"/> 管理者のみ <input type="radio"/> 管理者とユーザ <input type="radio"/> 不要
	保守メニュー <input type="radio"/> 管理者のみ <input type="radio"/> 管理者とユーザ <input type="radio"/> 不要

設定終了後、更新をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置を操作するときのパスワードを設定します。

パスワードの入力によって操作できる時間は10分間です。それ以降の操作では、再びパスワードの入力を要求されます。なお、パスワードの設定は、更新直後から有効になります。

管理者パスワード

設定メニューを設定する際に入力するパスワードを16文字以内で指定します。

管理者パスワードの確認

上記で指定した管理者パスワードをもう一度指定します。

ユーザパスワード

設定メニュー以外で使用するパスワードを16文字以内で指定します。

ユーザパスワードの確認

上記で指定したユーザパスワードをもう一度指定します。

パスワード入力

操作メニュー、表示メニューおよび保守メニューを操作する際に、パスワードが必要な場合は、“管理者のみ”または“管理者とユーザ”を選択します。

管理者のみ

操作する際に、管理者パスワードの入力が必要です。

管理者とユーザ

操作する際に、管理者またはユーザパスワードの入力が必要です。

不要

操作する際に、パスワード入力は必要ありません。

10 装置情報

[操作] 「設定メニュー」→基本設定「装置情報」

装置情報		
ルータ名称情報	タイムサーバ情報	システムログ情報
SNMP情報	ファームウェア更新情報	異常時動作情報
ループバック情報	サーバ機能情報	

装置固有の機能についての設定ができます。

10.1 ルータ名称情報

[操作] 「設定メニュー」→基本設定「装置情報」→[ルータ名称情報]

ルータ名称情報 ?

ルータ名称

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ルータ名称

本装置の任意な名称を32文字以内で指定します。ルータ名称を設定すると、DHCPクライアント機能でDHCPサーバにルータ名称が広報されます。そのため、DHCPサーバからはこの名称で管理することができます。

こんな事に気をつけて

SNMP設定情報の機器名称で“ルータ名称を使用する”を選択した場合、この名称がSNMPの機器名称として使用されます。

10.2 タイムサーバ情報

[操作] 「設定メニュー」→基本設定「装置情報」→[タイムサーバ情報]

■タイムサーバ情報	
タイムサーバ機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
サーバ設定	<input checked="" type="radio"/> DHCPで取得する <small>※IPv4のDHCPクライアントの設定が必要です。</small>
	<input type="radio"/> 設定する
	プロトコル <input checked="" type="radio"/> TIMEプロトコル <input type="radio"/> SNTPプロトコル
	タイムサーバIPアドレス <input type="text"/>
自動時刻設定間隔	<input type="text"/> 日

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

タイムサーバ機能

ネットワーク上のタイムサーバから時刻情報を取得することによって、内部時計を自動的に設定する場合は、“使用する”を選択します。

サーバ設定

使用するタイムサーバを指定します。“DHCPで取得する”を選択した場合は、DHCPクライアントの設定が必要です。直接IPアドレスで設定する場合は、“設定する”を選択し、プロトコルを選択して、タイムサーバIPアドレスを指定します。

プロトコル

タイムサーバから時刻情報を取得するときのプロトコルを選択します。

TIMEプロトコル

TIMEプロトコル（TCP）を使用する場合に指定します。

SNTPプロトコル

簡易NTPプロトコル（UDP）を使用する場合に指定します。

タイムサーバIPアドレス

タイムサーバのIPv4 / IPv6 アドレスを指定します。
有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:fff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

自動時刻設定間隔

タイムサーバから定期的に時刻情報を取得するときの取得周期を0～10日の範囲で指定します。省略または0を設定すると、起動（再起動）時だけ時刻情報を取得します。

10.3 システムログ情報

[操作] 「設定メニュー」 → 基本設定「装置情報」 → [システムログ情報]

■システムログ情報	
システムログ送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 送信先ホスト <input type="text"/>
セキュリティログ	<input type="checkbox"/> PPP <input type="checkbox"/> IPフィルタ <input type="checkbox"/> URLフィルタ <input type="checkbox"/> NAT <input type="checkbox"/> DHCP
重複メッセージの出力	<input checked="" type="radio"/> する <input type="radio"/> しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

接続切断、トラブルなどのさまざまな情報のシステムログをネットワーク上のシステムログサーバに対して送信することができます。その場合のファシリティ、プライオリティは以下のとおりです。

ファシリティ : local7 (23)

プライオリティ : error、warn、info、notice (※1)

※1) noticeはセキュリティログを使用する場合だけ出力されます。

☛ 参照 プライオリティ、ファシリティの設定は、コマンドリファレンスの syslog pri および syslog facility を参照してください。

システムログ送信

syslog 形式でシステムログサーバにシステムログ情報を送信する場合は、“送信する”を選択します。

送信先ホスト

送信先のIPアドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

重複メッセージの出力


システムログにメッセージを出力するとき、直前に出力したメッセージと重複した場合に出力する場合は、“する”を選択します。

セキュリティログ

PPPの認証エラー情報、IPフィルタ、URLフィルタ、NATにより遮断されたパケットのログ情報、および、DHCPサーバが割り当てたIPアドレスログなどを採取します。

10.4 SNMP 情報

[操作] 「設定メニュー」 → 基本設定 「装置情報」 → [SNMP 情報]

■SNMP情報 	
SNMPエージェント機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
ルータ管理者	<input type="text"/>
機器名称	ルータ名称を使用する (ルータ名称情報が設定されていないため選択できません) <input checked="" type="radio"/> 指定する 機器名称 <input type="text"/>
機器設置場所	<input type="text"/>
エージェントアドレス	<input type="text"/>
SNMPホスト1	<input checked="" type="radio"/> publicとする(任意のホストを対象とする) <input type="radio"/> 指定する コミュニティ名 <input type="text"/> IPアドレス <input type="text"/> トラップ <input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 書き込み要求 <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト2	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名 <input type="text"/> IPアドレス <input type="text"/> トラップ <input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 書き込み要求 <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト3	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名 <input type="text"/> IPアドレス <input type="text"/> トラップ <input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 書き込み要求 <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト4	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名 <input type="text"/> IPアドレス <input type="text"/> トラップ <input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 書き込み要求 <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト5	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名 <input type="text"/> IPアドレス <input type="text"/> トラップ <input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 書き込み要求 <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト6	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名 <input type="text"/> IPアドレス <input type="text"/> トラップ <input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 書き込み要求 <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する

SNMPホスト7	<input checked="" type="radio"/> 指定しない	
	<input type="radio"/> 指定する	
	コミュニティ名	<input type="text"/>
	IPアドレス	<input type="text"/>
	トラップ	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する
書き込み要求	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する	
SNMPホスト8	<input checked="" type="radio"/> 指定しない	
	<input type="radio"/> 指定する	
	コミュニティ名	<input type="text"/>
	IPアドレス	<input type="text"/>
	トラップ	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する
書き込み要求	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

SNMP エージェント機能

SNMP エージェント機能を使用すると、SNMP マネージャの動作しているほかのシステムから本装置の状態を監視できます。SNMP エージェント機能を使用する場合は“使用する”を選択し、以下の項目を設定します。

ルータ管理者

本装置の管理者名を 40 文字以内で指定します。区切り文字は、“_” や “.” を使用します。

機器名称

機器名称としてルータ名称を使用する場合は、“ルータ名称を使用する”を選択します。“指定する”を選択した場合は、本装置の名称を 32 文字以内で指定します。

機器設置場所

本装置の設置場所を 72 文字以内で指定します。

エージェントアドレス

SNMP エージェントの IP アドレスを指定します。トラップ送信時の自装置のアドレスにも使用されます。SNMP エージェント機能を使用する場合は必ず設定してください。“0.0.0.0”を指定すると、エージェントアドレスを指定しないものとみなします。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

SNMP ホスト

SNMP によるアクセスを許可するホストを設定します。ホストは 8 つまで指定できます。“public とする”を選択すると、コミュニティ名 “public” で任意のホストからのアクセスを許可します。コミュニティ名を変える場合やホストを限定する場合は、“指定する”を選択し、コミュニティ名・IP アドレス・トラップ送信可否を指定します。

コミュニティ名

SNMP により情報交換するグループのコミュニティ名を 32 文字以内で指定します。

IPアドレス

SNMPによるアクセスを許可するホストのIPアドレスを指定します。“0.0.0.0”を指定すると、任意のホストからのアクセスを許可します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

トラップ

このSNMPホストに対してトラップを送信する場合は、“送信する”を選択します。ただし、任意のホスト(0.0.0.0)を指定している場合は、トラップの送信は行われません。

書き込み要求

このSNMPホストから書き込み要求を許可する場合は、“許可する”を選択します。ただし、任意のホスト(0.0.0.0)を指定している場合は、書き込み要求は許可されません。

10.5 ファームウェア更新情報

[操作] 「設定メニュー」→基本設定「装置情報」→[ファームウェア更新情報]

■ファームウェア更新情報	
転送元ホスト名	<input type="text"/>
ログインID	<input type="text"/>
ログインパスワード	<input type="text"/>
ファイルロケーション	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ファームウェアを入れ替えたり、レベルアップを行うときに、転送元となるホストに接続するための情報を設定します。ファームウェアの更新操作は保守メニューから行うことができます。

転送元ホスト名

更新ファームウェアが存在するホスト名を 128 文字以内で指定します。IPv4/IPv6 アドレスを指定することもできます。

こんな事に気をつけて

ProxyDNS 機能が設定されていない場合、ホスト名指定によるファームウェア更新は行えません。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:fff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

ログインID

ファームウェア更新用のログインIDを 16 文字以内で指定します。

ログインパスワード

ファームウェア更新用のパスワードを 32 文字以内で指定します。

ファイルロケーション

更新用ファームウェアのロケーションを 80 文字以内で指定します。

10.6 異常時動作情報

[操作] 「設定メニュー」 → 基本設定「装置情報」 → [異常時動作情報]

■異常時動作情報 ?	
CE保守ログイン	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
ウォッチドッグリセット機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
温度異常時の動作	<input checked="" type="radio"/> 運用継続 <input type="radio"/> システムダウン

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置になんらかの異常が発生した場合の動作を設定します。

CE 保守ログイン

CE 専用パスワードによるログインを許可する場合は、“許可する”を選択します。

ウォッチドッグリセット機能

ウォッチドッグリセット機能を起動する場合は、“使用する”を選択します。“使用する”を選択した場合、本装置がハングアップすると 16～48 秒以内にリセットがかかり再起動します。

温度異常時の動作

温度異常を検出した場合にシステムダウンを行うか、そのまま運用を継続するかを選択します。

10.7 ループバック情報

[操作] 「設定メニュー」→基本設定「装置情報」→[ループバック情報]

■ループバック情報	
IPアドレス	<input type="text"/>
OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する エリア定義番号 <input type="text" value="0"/>
PHP機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IPアドレス

ループバックインタフェースに割り当てる追加IPアドレスを指定します。ループバックインタフェースに割り当てたIPアドレスを通信に使用する場合は、以下の範囲の中で通信可能なアドレスを指定します。省略または0.0.0.0を設定した場合、IPアドレスを使用しないものとします。

有効範囲)

1.0.0.1-126.255.255.254

128.0.0.1-191.255.255.254

192.0.0.1-223.255.255.254

こんな事に気をつけて

- ほかのインタフェースと違うネットワークのIPアドレスを設定する必要があります。
- 127.0.0.1はループバックインタフェースにすでに設定されています。ループバック情報として127.0.0.1を設定する必要はありません。

OSPF機能

ループバックに割り当てたIPアドレスをOSPFで広報するかどうかを選択します。“使用する”を選択した場合、IPアドレスが設定されているときだけOSPFで広報します。広報するIPアドレスは、設定したIPアドレスだけです。すでに設定されているIPアドレス127.0.0.1は広報しません。

ループバックインタフェースも含めて、OSPFを使用できるインタフェースは、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。

エリア定義番号

広報を行うOSPFエリア情報の定義番号を指定します。指定する定義番号のOSPFエリア情報はあらかじめ設定しておく必要があります。OSPFエリア情報の設定は、「ルーティングプロトコル情報」の「OSPF関連」にあります。

PHP機能

ループバックインタフェースあてのLSPのPHP機能を設定します。PHP機能を無効にする場合は、“使用しない”を選択します。PHP機能を有効にする場合は、“使用する”を選択します。MPLSトンネル接続を使用する場合に、自側エンドポイントとIPアドレスが同じとき、設定に関係なく“使用しない”が設定されます。

10.8 サーバ機能情報

[操作] 「設定メニュー」 → 基本設定「装置情報」 → [サーバ機能情報]

■サーバ機能情報		
FTPサーバ機能		<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止
TELNETサーバ機能		<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止
SSHサーバ機能	SSH	<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止
	SFTP	<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止
HTTPサーバ機能		<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止
DNSサーバ機能		<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止
SNTPサーバ機能		<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止
TIMEサーバ機能	TCP	<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止
	UDP	<input checked="" type="radio"/> IPv4 / <input type="radio"/> IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置の各サーバ機能を有効にするか停止するかを設定します。

FTPサーバ機能

FTPサーバ機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

TELNETサーバ機能

TELNETサーバ機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

SSHサーバ機能

SSH

SSHサーバによるログイン機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

SFTP

SFTPサーバによるFTP機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

HTTP サーバ機能

HTTP サーバ機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

DNS サーバ機能

DNS サーバ機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

SNTP サーバ機能

SNTP サーバ機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

TIME サーバ機能

TCP

TCP による TIME サーバ機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

UDP

UDP による TIME サーバ機能を有効にするプロトコルを選択します。

- IPv4 / IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

11 スケジュール情報

[操作] 「設定メニュー」→基本設定「スケジュール情報」

スケジュール情報

[月間／週間予約情報](#)
 [電話番号変更予約情報](#)
 [構成定義切り替え予約情報](#)

このページでは、スケジュール予約情報を設定できます。設定するスケジュール予約をクリックしてください。スケジュールの一覧が表示されますので、各予約で必要な処理のボタンをクリックしてください。

▲スケジュール機能を使用する際には、正しい時刻が設定されているか確認してください。現在の時刻は **Tue Nov 12 12:05:16 2002** です。

11.1 月間／週間予約情報

[操作] 「設定メニュー」→基本設定「スケジュール情報」→ [月間／週間予約情報]

■月間／週間予約情報 ?

＼	動作	予約時刻	終了時刻	周期	操作	
1	-	-	-	-	修正	削除
2	-	-	-	-	修正	削除
3	-	-	-	-	修正	削除
4	-	-	-	-	修正	削除
5	-	-	-	-	修正	削除
6	-	-	-	-	修正	削除
7	-	-	-	-	修正	削除
8	-	-	-	-	修正	削除
9	-	-	-	-	修正	削除
10	-	-	-	-	修正	削除
11	-	-	-	-	修正	削除
12	-	-	-	-	修正	削除
13	-	-	-	-	修正	削除
14	-	-	-	-	修正	削除
15	-	-	-	-	修正	削除
16	-	-	-	-	修正	削除
<input type="button" value="全削除"/>						

保存した情報は、設定反映後に有効になります。

現在、設定されている月間または週間の予約が表示されています。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→基本設定「スケジュール情報」→[月間/週間予約情報]→[修正]

動作

発信抑止/着信抑止/課金情報クリア/強制切断/リモートパワーオンの中から予約する処理動作を選択します。

発信抑止

指定した時刻の間、自動発信を抑止します。

着信抑止

指定した時刻の間、自動着信を抑止します。

課金情報クリア

予約時刻に課金情報をクリアします。

モデム統計情報クリア

予約時刻にモデム統計情報をクリアします。

強制切断

予約時刻に強制切断を実施します。

リモートパワーオン

予約時刻にホストデータベース情報でMACアドレスが登録されている Wake up on LAN に対応したすべてのパソコンに対してリモートパワーオン処理を実施します。

予約時刻

選択した動作を実行（開始）する時刻と実行周期を指定します。

終了時刻

選択した動作を終了する時刻を指定します。動作として発信抑止または着信抑止を選択した場合だけ設定できます。ここで予約時刻よりも早い時刻を指定した場合、実行は翌日の時刻になります。

11.2 電話番号変更予約情報

[操作] 「設定メニュー」→基本設定「スケジュール情報」→[電話番号変更予約情報]

■電話番号変更予約情報				
実行日時	電話番号変更情報	操作		
1	-	修正	削除	
2	-	修正	削除	
3	-	修正	削除	
4	-	修正	削除	
全削除				
保存した情報は、設定反映後に有効になります。				

現在、設定されている電話番号変更予約が表示されています。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→基本設定「スケジュール情報」→[電話番号変更予約情報]→[修正]

■電話番号変更予約情報				
実行日時	電話番号変更情報	操作		
実行日時	20 <input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日 <input type="text"/> 時 <input type="text"/> 分			
1 電話番号変更情報	変更前1	<input type="text"/>	変更後1	<input type="text"/>
	変更前2	<input type="text"/>	変更後2	<input type="text"/>
	変更前3	<input type="text"/>	変更後3	<input type="text"/>
	変更前4	<input type="text"/>	変更後4	<input type="text"/>
保存 キャンセル 一覧へ戻る				

実行日時

電話番号を変更する日時を西暦で2000～2036年の範囲で指定します。

電話番号変更情報

変更前と変更後の電話番号をそれぞれ32桁以内で指定します。

11.3 構成定義切り替え予約情報

[操作] 「設定メニュー」 → 基本設定「スケジュール情報」 → [構成定義切り替え予約情報]

■構成定義切り替え予約情報		
実行日時	構成定義切り替え予約	操作
1	-	修正 削除

保存した情報は、設定反映後に有効になります。

[操作] 「設定メニュー」 → 基本設定「スケジュール情報」 → [構成定義切り替え予約情報] → [修正]

■構成定義切り替え予約情報		
実行日時	構成定義切り替え予約	操作
1	実行日時 20 <input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日 <input type="text"/> 時 <input type="text"/> 分 動作 <input type="text" value="構成定義情報1で再起動"/>	保存 キャンセル 一覧へ戻る

本装置は構成定義情報が2つ存在します。指定時刻に運用する構成定義情報を切り替えることができます。

なお、現在運用中の構成定義情報は保守メニューの「構成定義情報切り替え」で知ることができます。

こんな事に気をつけて

指定時刻になると、本装置は自動的に再起動され、構成定義情報が切り替わります。その際、データ通信中の場合は接続が切断されます。

実行日時

構成定義情報を切り替える日時を西暦で2000～2036年の範囲で指定します。

動作

切り替える構成定義情報を指定します。

12 WAN 情報

[操作] 「設定メニュー」 → ルータ設定 「WAN 情報」

現在、設定されている WAN インタフェースが表示されています。処理するボタンをクリックし、次のページへ進みます。本装置に接続する回線に関する物理的な情報（回線の種類や電話番号などの契約に関する情報）を設定します。装置全体で 1 個設定できます。

回線インタフェース

本装置に接続する回線の種類を選択します。

- ISDN
INS ネット 64 などの ISDN 回線交換接続を使用する場合には選択します。
- 専用線
ハイ・スーパーデジタル（HSD）や DA64 などの専用線を使用する場合には選択します。
- フレームリレー
フレームリレー回線を使用する場合には選択します。

◇ ISDN の場合

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「WAN情報」 → [追加] → [基本情報]

■基本情報							
ポート	基本 0						
自動接続	<input type="radio"/> すべて禁止 <input checked="" type="radio"/> 相手毎に設定						
着信動作	<input type="radio"/> すべて禁止 <input checked="" type="radio"/> 相手毎に設定						
自局番号チェック	<input checked="" type="radio"/> しない <input type="radio"/> する						
	<table border="1"> <tr> <td>チェックする番号1</td> <td>電話番号を指定</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>サブアドレス</td> <td><input type="text"/></td> </tr> </table>	チェックする番号1	電話番号を指定	<input type="text"/>		サブアドレス	<input type="text"/>
	チェックする番号1	電話番号を指定	<input type="text"/>				
		サブアドレス	<input type="text"/>				
<table border="1"> <tr> <td>チェックする番号2</td> <td>電話番号を指定</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>サブアドレス</td> <td><input type="text"/></td> </tr> </table>	チェックする番号2	電話番号を指定	<input type="text"/>		サブアドレス	<input type="text"/>	
チェックする番号2	電話番号を指定	<input type="text"/>					
	サブアドレス	<input type="text"/>					
グローバル着信	<input type="radio"/> 利用しない <input checked="" type="radio"/> 利用する						
発信者番号通知	<input checked="" type="radio"/> 網契約に従う <input type="radio"/> しない <input type="radio"/> する						
	<table border="1"> <tr> <td>通知する電話番号</td> <td>電話番号を指定</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>サブアドレス</td> <td><input type="text"/></td> </tr> </table>	通知する電話番号	電話番号を指定	<input type="text"/>		サブアドレス	<input type="text"/>
通知する電話番号	電話番号を指定	<input type="text"/>					
	サブアドレス	<input type="text"/>					
レイヤ1起動種別	<input checked="" type="radio"/> 常時起動 <input type="radio"/> 呼毎起動						
	回線停止猶予時間 <input type="text" value="60"/> 秒						

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ポート

回線を接続するポート（基本0）が表示されます。

自動接続

この回線に対する自動接続を装置全体で禁止するときに“すべて禁止”を選択します。“すべて禁止”を選択した場合は、いかなる通信データ発生時にも自動的に接続しません。“相手毎に設定”を選択した場合は、相手情報のネットワーク情報で設定します。

着信動作

この回線に対する着信動作を装置全体で禁止するときに“すべて禁止”を選択します。“すべて禁止”を選択した場合は、すべてのデータ通信の着信を拒否し、発信専用となります。“相手毎に設定”を選択した場合は、相手情報のネットワーク情報の接続先情報で設定します。

自局番号チェック

ダイヤルイン番号やi・ナンバー、サブアドレスを利用して着信機器識別するときに“する”を選択し、使用する番号を指定します。この番号は2つまで設定できます。

電話番号は、“電話番号を指定”、“i・ナンバー情報1（契約者回線番号）”、“i・ナンバー情報2/3（追加の番号）”のどれかを選択します。“電話番号を指定”を選択した場合は、その右の記入欄に電話番号を32桁まで指定します。また、どの場合にもサブアドレスは19桁まで指定できます。“電話番号を指定”を選択し、右の記入欄に電話番号を記述しないでサブアドレスだけを指定した場合は、電話番号は任意となります。

グローバル着信を行う場合は「グローバル着信」で“利用する”を選択します。

発信者番号通知

発信者番号通知の内容を変更する場合に設定します。通常は“網契約に従う”を選択します。“する”を選択した場合は、通知する電話番号とサブアドレスを指定します。電話番号は32桁まで、サブアドレスは19桁まで指定できます。

レイヤ1起動種別

回線同期確立手順の方式（レイヤ1起動種別）を選択します。

回線停止猶予時間

“呼毎起動”を指定した場合に、通信終了後の回線停止猶予時間を1～300秒の範囲で指定します。省略時は、60秒が設定されます。

【接続制御情報】

[操作] 「設定メニュー」 → ルータ設定「WAN情報」 → [追加] → [接続制御情報]

■接続制御情報 ?

通信時間による発信抑止	<input checked="" type="radio"/> しない <input type="radio"/> する				
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">上限時間</td> <td style="width: 50%; text-align: right;">[] 日</td> </tr> <tr> <td>制御動作</td> <td style="text-align: right;"> <input checked="" type="radio"/> 発信抑止のみ <input type="radio"/> システムログ出力のみ </td> </tr> </table>	上限時間	[] 日	制御動作	<input checked="" type="radio"/> 発信抑止のみ <input type="radio"/> システムログ出力のみ
上限時間	[] 日				
制御動作	<input checked="" type="radio"/> 発信抑止のみ <input type="radio"/> システムログ出力のみ				
課金額による発信抑止	<input checked="" type="radio"/> しない <input type="radio"/> する				
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">上限金額</td> <td style="width: 50%; text-align: right;">3000 円</td> </tr> <tr> <td>制御動作</td> <td style="text-align: right;"> <input checked="" type="radio"/> 発信抑止のみ <input type="radio"/> システムログ出力のみ </td> </tr> </table>	上限金額	3000 円	制御動作	<input checked="" type="radio"/> 発信抑止のみ <input type="radio"/> システムログ出力のみ
上限金額	3000 円				
制御動作	<input checked="" type="radio"/> 発信抑止のみ <input type="radio"/> システムログ出力のみ				

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

通信時間による発信抑止

この回線を使用した通信総時間の自動発信を抑止する場合は、“する”を選択します。

上限時間

制限を行う総通信時間を、1秒～999時間の範囲で指定します。省略することはできません。

制限動作

制限時間に達したときに行う動作を選択します。“発信抑止”を選択した場合は、それ以降の自動発信の抑止とシステムログの出力を行います。“システムログ出力のみ”を選択した場合は、自動発信の抑止は行わずにシステムログの出力を行います。

課金額による発信抑止

この回線を使用した課金合計金額の自動発信を抑止する場合は、“する”を選択します。

上限金額

制限を行う総通信時間を、1～999999円の範囲で指定します。省略することはできません。

制限動作

制限金額に達したときに行う動作を選択します。“発信抑止”を選択した場合は、それ以降の自動発信の抑止とシステムログの出力を行います。“システムログ出力のみ”を選択した場合は、自動発信の抑止は行わずにシステムログの出力を行います。

◇専用線の場合

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「WAN情報」 → [追加] → [基本情報]

■基本情報	
ポート	基本 0
回線速度	64Kbps

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 | キャンセル

ポート

回線を接続するポート（基本0）が表示されます。

回線速度

接続する専用線の回線速度を選択します。

◇ フレームリレーの場合

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「WAN情報」 → [追加] → [基本情報]

■基本情報	
ポート	基本 0
回線速度	64 Kbps
PVC状態確認手順	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
CLLMメッセージ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
輻輳通知ビット	<input checked="" type="checkbox"/> FECN <input checked="" type="checkbox"/> BECN

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ポート

回線を接続するポート（基本0）が表示されます。

回線速度

接続するフレームリレーの回線速度を選択します。

PVC 状態確認手順

PVC 状態確認手順を使用する場合は、“使用する”を選択します。PVC 状態確認手順は以下の機能を持っています。

- ユーザ網間のリンクの正常性を確認する機能
- ユーザーユーザー間の PVC 状態を通知する機能

こんな事につけて

- この機能を使用するには通信事業者と契約する必要があります。
- 本装置は PVC 状態確認手順の双方向手順はサポートしておりません。

CLLM メッセージ

CLLM メッセージ受信時に輻輳制御を行う場合は、“使用する”を選択します。CLLM メッセージは、網が網状態（輻輳、故障）を通知するためにユーザに送出するメッセージです。本装置は通知内容に合わせて動作します。

こんな事につけて

この機能を使用するには通信事業者と契約する必要があります。

輻輳通知ビット

輻輳制御に利用するビットを選択します。選択したビットがセットされたパケットを受信した場合、本装置は網を正常な状態に戻すためにパケットの送信を抑制します。

13 LAN情報

[操作] 「設定メニュー」→ルータ設定「LAN情報」

LAN情報
LAN情報

LAN情報 ?

インタフェース	ポート:VLAN ID	プロトコル	操作
LAN0	基本 0	IPv4 使用する [192.168.1.1]	修正 削除
		IPv6 使用しない	
		ブリッジ 使用しない	
		MPLS 使用しない	
		EoMPLS 使用しない	

<LAN情報追加フィールド>

インタフェース 疑似ルータ

追加 キャンセル

保存した情報は、設定反映後に有効になります。

現在、設定されている LAN インタフェースが表示されています。LAN インタフェースは、装置全体で物理インタフェースと VLAN インタフェースの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。ただし、物理インタフェースの有効な定義は存在する LAN ポートの数までです。処理するボタンをクリックし、次のページへ進みます。

インタフェース

設定する LAN インタフェースの種別を以下の中から選択します。

追加する LAN インタフェースを疑似ルータとして使用する場合は、設定するインタフェースを以下から選択し、“疑似ルータ”をチェックします。

- 物理 LAN
物理的に接続された LAN を使用する場合に選択します。
- VLAN
物理 LAN 上に仮想的な LAN を使用する場合に選択します。

[操作] 「設定メニュー」→ルータ設定「LAN0 情報 (物理 LAN)」→ [修正]

LAN0情報(物理LAN)

共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
------	------	--------	--------	--------

このページではLAN情報を設定することができます。上記の各関連項目をクリックすると詳細な設定項目が表示されます。

「LAN情報」で選択するインタフェースによって表示が異なります。

また、「疑似ルータ」をチェックした場合、「IPv6関連」と「MPLS関連」の項目はありません。

13.1 共通情報

◇ インタフェース：物理LAN

[操作] 「設定メニュー」 → ルータ設定「LAN0情報（物理LAN）」 → [修正] → [共通情報]

LAN0情報(物理LAN)	
共通情報	IP関連
	IPv6関連
	ブリッジ関連
	MPLS関連
基本情報	VRRPグループ情報

また、「疑似ルータ」をチェックした場合、「VRRPグループ情報」の項目はありません。

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「LAN0情報（物理LAN）」 → [修正] → [共通情報] → [基本情報]

■基本情報					
ポート番号	<table border="1"> <tr> <td>master</td> <td>基本0</td> </tr> <tr> <td>backup</td> <td>バックアップなし</td> </tr> </table>	master	基本0	backup	バックアップなし
master	基本0				
backup	バックアップなし				
優先使用ポート	<input checked="" type="radio"/> master <input type="radio"/> 先にリンクアップしたポート				
転送レート	自動認識				
シェーピング	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 最大送信レート <input type="text"/> Mbps				
VRRP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する パスワード <input type="text"/>				
MTUサイズ	1500 バイト				
自動復旧	<table border="1"> <tr> <td>モード</td> <td><input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない</td> </tr> <tr> <td>初期状態</td> <td><input checked="" type="radio"/> 非閉塞 <input type="radio"/> 閉塞</td> </tr> </table>	モード	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	初期状態	<input checked="" type="radio"/> 非閉塞 <input type="radio"/> 閉塞
モード	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない				
初期状態	<input checked="" type="radio"/> 非閉塞 <input type="radio"/> 閉塞				
MDI	<input checked="" type="radio"/> MDI <input type="radio"/> MDI-X				
輻射時透過フレーム選択	すべて破壊				

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 | キャンセル

「疑似ルータ」をチェックした場合、「VRRP機能」の項目はありません。

ポート番号

master

起動時に使用する物理ポート番号を選択します。

backup

masterで設定したポートで障害が発生した場合に、切り替えて使用する物理ポート番号を選択します。

優先使用ポート

masterポートとbackupポートの両方が使用可能なときに使用するポートを選択します。

- master
masterポートを優先的に使用します。
- 先にリンクアップしたポート
masterポートとbackupポートのどちらか先にリンクアップして使用可能になったポートを使用します。

転送レート

接続する回線の転送レートを以下から選択します。

- 自動認識 (通信速度を自動的に設定する場合)
- 100Mbps - 全二重
- 100Mbps - 半二重
- 10Mbps - 全二重
- 10Mbps - 半二重

シェーピング

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

シェーピング (リミッタ) 機能を設定します。シェーピング機能を使用する場合は“使用する”を選択し、最大送信レートを指定します。最大送信レートで設定したレートに送信を抑制します。

最大送信レート

最大送信レートを1～100000Kbpsの範囲で指定します。Kbpsは1000bpsを、Mbpsは1000Kbpsを意味します。

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを“使用する”に設定してください。

VRRP 機能

VRRPを使用する場合は、“使用する”を選択します。VRRPを使用するとルータの冗長構成を組むことができます。VRRPを使用しない場合は、以降の設定は無効になります。

パスワード

マスタが送信する Advertisement パケットに認証情報を含める場合は設定します。このインタフェースから送信されるすべての Advertisement パケットに適用されます。たとえば、同じネットワークでグループIDを重複させて別グループとして扱う、などの特別な環境である場合に設定します。8文字以内で指定します。

MTU サイズ

最大パケット送信サイズ (Maximum Transmission Unit) を200～1500バイトの範囲で指定します。

IPv6通信で利用する場合は、1280バイト以上の値を指定します。

ブリッジを利用する場合は、1500バイトを指定します。1500バイト未満を指定すると正しくブリッジ通信できない場合があります。

RIPを利用する場合は、576バイト以上を指定します。576バイト未満を指定するとRIPパケットが送信されない場合があります。

自動復旧

LANインタフェースに関するLAN自動復旧の設定をします。

モード

LAN障害時の自動復旧の動作モードを設定します。“しない”に設定した場合、LAN障害が復旧してもオペレータ指示があるまで接続を復旧しません。

初期状態

初期状態を“閉塞”にすると、閉塞状態で動作を開始し、オペレータからの閉塞状態解除指示を待ちます。

MDI

MDIのモードを以下から選択します。

- MDI
- MDI-X

LAN1～3ポートでのみ設定することができます。LAN0ポートは、to HUB to PCスイッチでだけ設定を変更することができます。

輻輳時透過フレーム選択

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

輻輳時に透過する入力フレーム種別を以下から選択します。

- すべて透過（輻輳時でも入力フレームを制限しません）
- VLANのみ透過（輻輳時には、VLAN 以外の入力フレームは破棄します）
- IPv4のみ透過（輻輳時には、IPv4 以外の入力フレーム（IPv6、PPPoE など）は破棄します）
- すべて破棄（輻輳時には、すべての入力フレームを破棄します）

[VRRP グループ情報]

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [共通情報] → [VRRP グループ情報]

⚠ VLAN インタフェースの場合、この機能は使用できません。

■ VRRP グループ情報 ?

グループ番号	グループ ID	プライオリティ	AD 送信間隔	プリエンプトモード	操作
0	-	-	-	-	修正 削除
1	-	-	-	-	修正 削除

保存した情報は、設定反映後に有効になります。

現在、このインタフェースに設定されている VRRP グループ情報の定義が表示されています。VRRP グループは、それぞれのインタフェースで 2 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [共通情報] → [VRRP グループ情報] → [修正]

LAN 情報 - **VRRP グループ 0 情報**

基本情報 VRRP トリガ情報

【基本情報】

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[共通情報]→[VRRP グループ情報]→[修正]→[基本情報]

■基本情報	
グループID	<input type="text"/>
プライオリティ	<input checked="" type="radio"/> マスタ(255) <input type="radio"/> バックアップ 優先度 <input type="text"/> 仮想IPアドレス <input type="text"/> <input type="text"/>
AD送信間隔	<input type="text"/> 秒
ブリエンプトモード	<input checked="" type="radio"/> ON <input type="radio"/> OFF 移行禁止時間 <input type="text"/> 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

グループID

VRRP グループのグループID を1～255の範囲で指定します。VRRP グループは、指定したグループID で識別（グループ化）されます。グループID は、装置内で重複しないように指定してください。

プライオリティ

マスタまたはバックアップを選択します。

- マスタ
プライオリティが255のVRRP グループメンバとして動作します。また、仮想IPアドレスは、このインタフェースのIPアドレスとなります。
- バックアップ
以下の優先度および仮想IPアドレスを設定します。VRRP グループ内で、プライオリティが一番高いVRRP グループメンバがマスタとなります。プライオリティは、数値が大きいほど高くなります。プライオリティは、なるべくVRRP グループ内で差をつけて設定してください。トリガを使用する場合は、プライオリティに1を指定しないでください。また、トリガを使用する場合は、“バックアップ”を選択します。“マスタ”を選択すると、該当グループがバックアップ状態となったときにVRRP を設定したLANが通信できなくなります。グループ内でもっとも優先度が高いグループがマスタになります。

優先度

プライオリティを1～254の範囲で指定します。

仮想IPアドレス

VRRP グループ内では、同じ仮想IPアドレスを指定します。VRRP グループ内にマスタを設定されたVRRP グループメンバが存在する場合は、その設定されたインタフェースのIPアドレスを指定します。自装置のインタフェースに設定されたIPアドレスを指定しないでください。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

AD送信間隔

マスタが送信するAdvertisement パケットの送信間隔を1～255秒の範囲で指定します。VRRP グループ内では同じ値を使用します。本装置とVRRP を構成する他装置にも同じ値を指定します。省略時は、1秒が設定されます。

プリエンプトモード

通常は“ON”を選択します。

“OFF”を選択した場合、自装置 VRRP グループメンバの優先度が高くても、マスタである他装置の VRRP グループメンバがすでに存在すると、マスタになることはできません。“OFF”を選択した場合は、ネットワークの状態が不安定で、マスタの交代が頻繁に発生する場合に有効です。移行禁止時間秒は、マスタより先にバックアップのシステムが立ち上がり、本来マスタになるべき VRRP グループに制御が移らないのを防ぎます。

移行禁止時間

システム立ち上がりからプリエンプトモード OFF 状態を抑制する時間です。0～900 秒の範囲で指定します。省略時は、0 秒が設定されます。

[VRRP トリガ情報]

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [共通情報] → [VRRP グループ情報] → [修正] → [VRRP トリガ情報]

■VRRPトリガ情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

トリガ定義番号	トリガ種別	減算プライオリティ	インタフェース	あて先IPアドレス	操作											
全削除																
<VRRPトリガ情報入力フィールド>																
減算プライオリティ	254															
トリガ種別	<input checked="" type="radio"/> インタフェースダウントリガ(ifdown) <input type="text" value="インタフェース"/> <input type="button" value="すべて"/>															
	<input type="radio"/> ルートダウントリガ(route) <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td rowspan="2" style="width: 15%;">ネットワーク</td> <td colspan="4"> <input checked="" type="radio"/> デフォルトルート <input type="radio"/> 経路を指定する </td> </tr> <tr> <td style="width: 15%;">あて先IPアドレス</td> <td style="width: 15%;"><input type="text"/></td> <td style="width: 15%;">あて先アドレスマスク</td> <td style="width: 15%;"><input type="text" value="0 (0.0.0.0)"/></td> </tr> </table>					ネットワーク	<input checked="" type="radio"/> デフォルトルート <input type="radio"/> 経路を指定する				あて先IPアドレス	<input type="text"/>	あて先アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>		
	ネットワーク	<input checked="" type="radio"/> デフォルトルート <input type="radio"/> 経路を指定する														
		あて先IPアドレス	<input type="text"/>	あて先アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>											
インタフェース	指定なし															
<input type="radio"/> ノードダウントリガ(node) <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">あて先IPアドレス</td> <td style="width: 15%;"><input type="text"/></td> </tr> <tr> <td>送出インタフェース</td> <td>指定なし</td> </tr> <tr> <td>再送間隔</td> <td>5 秒</td> </tr> <tr> <td>タイムアウト時間</td> <td>16 秒</td> </tr> <tr> <td>正常時送信間隔</td> <td>17 秒</td> </tr> <tr> <td>異常時送信間隔</td> <td>30 秒</td> </tr> </table>					あて先IPアドレス	<input type="text"/>	送出インタフェース	指定なし	再送間隔	5 秒	タイムアウト時間	16 秒	正常時送信間隔	17 秒	異常時送信間隔	30 秒
あて先IPアドレス	<input type="text"/>															
送出インタフェース	指定なし															
再送間隔	5 秒															
タイムアウト時間	16 秒															
正常時送信間隔	17 秒															
異常時送信間隔	30 秒															
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>																

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、このVRRPグループメンバに設定されているVRRPトリガ情報の定義が表示されています。VRRPトリガの定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定した条件が発生した場合に、該当するVRRPグループメンバの優先度を下げます。条件に当てはまるすべてのトリガに適用されます。このインタフェースに異常が発生しない限り、減算されるプライオリティの最小は1です。

減算プライオリティ

設定した条件が発生した場合、「VRRPグループ情報」の「基本情報」で設定したプライオリティを減算する値を1～254の範囲で指定します（プライオリティ1より低い値までは減算されません）。省略時は、254が設定されます。

トリガ種別

トリガとなる種別を以下の3つから選択します。

- インタフェースダウントリガ (ifdown)
指定されたインタフェースがダウンした場合にトリガを適用します。有効ではないインタフェースは動作上、無視されます。
- ルートダウントリガ (route)
指定された経路情報が存在しない、または中継インタフェースが変化した場合にトリガを適用します。
- ノードダウントリガ (node)
設定したノードに対して ICMP ECHO パケットを送信します。応答がタイムアウトした場合にトリガを適用します。ICMP ECHO パケットの送信元 IP アドレスは、VRRP が設定された LAN インタフェースの IP アドレスとなります。応答を受診するための経路情報が正しくない場合は、不当に異常を検出することがあります。

インタフェース

トリガの対象となるインタフェースを選択します。“すべて”を選択した場合は、すべての物理インタフェースが対象です。

ネットワーク

デフォルトルートまたは経路の指定を選択します。ネットワーク指定を選択した場合は以降のあて先 IP アドレス、あて先アドレスマスクを設定します。

あて先 IP アドレス / あて先アドレスマスク

あて先 IP アドレスとあて先アドレスマスクでホスト経路またはネットワーク経路を設定します。

インタフェース

“指定なし”を選択した場合は経路情報が存在すればトリガは適用されません。それ以外では経路情報によるパケット送出インタフェースが設定と異なる、または経路情報が存在しない場合にトリガが適用されます。

あて先 IP アドレス

ICMP ECHO パケットの送出先 IP アドレスを指定します。IP アドレスは、以下の範囲で指定します。

有効範囲)

1.0.0.1-126.255.255.254

128.0.0.1-191.255.255.254

192.0.0.1-223.255.255.254

送出インタフェース

ICMP ECHO パケットを送出するインタフェースを指定します。“指定なし”の場合は送出時の経路情報によって決定されます。

再送間隔

ICMP ECHO パケットの応答が受信されない場合に、再送する時間を 1～60 秒の範囲で指定します。送信から指定した再送間隔まで応答がない場合に、ICMP ECHO パケットを再送します。省略時は、5 秒が設定されます。

タイムアウト時間

ICMP ECHO パケットの再送を繰り返しても応答が受信されず、タイムアウトするまでの時間を、([再送間隔+1]～240) 秒の範囲で指定します。タイムアウトによって、トリガが適用されます。省略時は、(再送間隔×3+1) 秒が設定されます。

正常時送信間隔

ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する時間を、([タイムアウト時間+1]～255) 秒の範囲で指定します。正常に受信されている状態での周期送信間隔です。省略時は、タイムアウト時間+1 秒が設定されます。

異常時送信間隔

ICMP ECHO パケットのタイムアウトが発生してから応答が受信されるまでの、周期送信する間隔を 1～255 秒の範囲で指定します。応答が受信された場合は、トリガを適用しないで正常状態に戻ります。省略時は、30 秒が設定されます。

◇ インタフェース : VLAN

[操作] 「設定メニュー」 → ルータ設定「LAN0 情報 (VLAN)」 → [修正] → [共通情報]

LAN0情報(VLAN)				
共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
基本情報	VLANプライオリティマッピング情報		VRRPグループ情報	

「疑似ルータ」をチェックした場合、「VRRP グループ情報」の項目はありません。

「VRRP グループ情報」は、「インタフェース : 物理 LAN」を参照してください。

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「LAN 情報 (VLAN)」 → [修正] → [共通情報] → [基本情報]

■ 基本情報	
出力先	LAN0
VLAN ID	1
プライオリティ	0
VRRP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する パスワード <input type="text"/>
MTUサイズ	1500 バイト

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 | キャンセル

「疑似ルータ」をチェックした場合、「VRRP 機能」の項目はありません。

出力先

VLAN フレームの出力先インタフェースを選択します。すでに設定済みの物理インタフェースだけ選択できます。

VLAN ID

VLAN ID を 1 ~ 4094 の範囲で指定します。

プライオリティ

VLAN インタフェースのフレーム送出時に、VLAN タグのプライオリティフィールドに格納される値を 10 進数を使用して 0 ~ 7 の範囲で指定します。

VRRP 機能

VRRP を使用する場合は、「使用する」を選択します。VRRP を使用するとルータの冗長構成を組むことができます。VRRP を使用しない場合は、以降の設定が無効になります。

パスワード

マスタが送信する Advertisement パケットに認証情報を含める場合に、パスワードを 8 文字以内で指定します。このインタフェースから送信されるすべての Advertisement パケットに適用されます。たとえば、同じネットワークでグループ ID を重複させて別グループとして扱う、などの特別な環境である場合に設定します。

MTUサイズ

最大パケット送信サイズ (Maximum Transmission Unit) を 200～1500 バイトの範囲で指定します。

IPv6通信で利用する場合は、1280バイト以上の値を指定します。RIPを利用する場合は、576バイト以上を指定します。576バイト未満のMTUサイズを指定するとRIPパケットが送信されない場合があります。

こんな事に気をつけて

VLAN機能を使用すると、Ethernet フレームに4バイトのVLANタグが付加され、最大1522バイトのEthernetフレームが送出されることになります。通常のEthernetフレームの最大サイズは1518バイトです。そのため、その状態では1522バイトのフレームに対応していない機器とは接続することはできません。1522バイトのフレームに対応していない機器と接続する場合は、VLAN インタフェースのMTUサイズを1496に変更してください。

[VLANプライオリティマッピング情報]

[操作] 「設定メニュー」 → ルータ設定「LAN 情報 (VLAN)」 → [修正] → [共通情報]
→ [VLAN プライオリティマッピング情報]

■ VLANプライオリティマッピング情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

プロトコル	TOS/Traffic Class	プライオリティ	操作
全削除			
<VLANプライオリティマッピング情報入力フィールド>			
プロトコル	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6		
TOS/Traffic Class	<input type="text"/>		
プライオリティ	<input type="text" value="0"/>		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、このLANに定義されているプライオリティマッピング情報が表示されています。VLAN プライオリティマッピングの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

プロトコル

プロトコルを以下の2つから選択します。

- IPv4
- IPv6

TOS/Traffic Class

IPのTOSフィールド値またはIPv6のTraffic Class フィールド値を“any”、または16進数を使用して、0～ffの範囲で指定します。複数の値を指定する場合は、“,”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は“any”が設定されます。

プライオリティ

設定するVLANのプライオリティを10進数を使用して0～7の範囲で指定します。

13.2 IP 関連

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]

LAN0情報(物理LAN)				
共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
IPアドレス情報		セカンダリIPアドレス情報		RIP情報
OSPF情報		スタティック経路情報		IPフィルタリング情報
TOS値書き換え情報		RIPフィルタリング情報		NAT情報
静的NAT情報		帯域制御(WFQ)情報		DHCP情報
ICMP情報		マルチキャスト情報		BGP/MPLS VPN情報
BGP/MPLS VPNスタティック経路情報		ARP情報		

「疑似ルータ」をチェックした場合、「セカンダリIPアドレス情報」、「RIP 情報」、「OSPF 情報」、「RIP フィルタリング情報」、「DHCP 情報」、「ICMP 情報」、「マルチキャスト情報」、「BGP/MPLS VPN 情報」、「BGP/MPLS VPN スタティック経路情報」、「ARP 情報」の項目はありません。

◇ IP アドレス情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[IP アドレス情報]

■ IPアドレス情報 ?

IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IPアドレス	<input type="radio"/> DHCPで自動的に取得する
	<input checked="" type="radio"/> 指定する
	IPアドレス <input type="text" value="192.168.1.1"/>
	ネットマスク <input type="text" value="2 (192.0.0.0)"/>
	ブロードキャストアドレス <input type="text" value="ネットワークアドレス+オール1"/>

※DHCPのサーバ機能使用時、IPアドレスを変更する場合は DHCP 機能の“割当て先頭アドレス”も確認してください。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

「疑似ルータ」をチェックした場合、「IPv4」の項目はありません。また、疑似ルータは DHCP 機能を使用できないため、「IP アドレス」の項目で DHCP による IP アドレスの自動取得を選択する項目はありません。

IPv4

IPv4 通信を行う場合は、「使用する」を選択します。

IP アドレス

このインタフェースの IP アドレス情報の取得方法を設定します。本装置を DHCP クライアントとして運用する場合は「DHCP で自動的に取得する」を選択します。IP アドレス、ネットマスク、ブロードキャストアドレスを指定する場合は「指定する」を選択します。

IP アドレス

本装置の IP アドレスを指定します。

IP アドレスに 0.0.0.0 を指定すると通信ができなくなります。

(有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

ネットマスク

本装置のネットマスクを指定します。

ブロードキャストアドレス

ブロードキャストアドレスを以下から選択します。通常は“ネットワークアドレス+オール1”を選択します。

- 0.0.0.0
- 255.255.255.255
- ネットワークアドレス+オール0
(ネットワークアドレスのホスト部をオール0にしたもの)
- ネットワークアドレス+オール1
(ネットワークアドレスのホスト部をオール1にしたもの)

◇セカンダリIPアドレス情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP関連]→[セカンダリ IPアドレス情報]

■セカンダリIPアドレス情報	
IPアドレス	<input type="text"/>
ネットマスク	2 (192.0.0.0)
ブロードキャストアドレス	ネットワークアドレス+オール1

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

本装置は1つのインタフェースに複数のIPアドレスを持つことができます。複数のIPアドレスを使用する場合はここを指定します。

こんな事に気をつけて

セカンダリIPアドレスの属するネットワークには、以下のサービスは行いません。

- RIPの送受信機能
- OSPFの送受信機能
- DHCP機能

IPアドレス

セカンダリアドレスのIPアドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

ネットマスク

セカンダリアドレスのネットマスクを指定します。

ブロードキャストアドレス

セカンダリアドレスのブロードキャストアドレスを以下から選択します。通常は“ネットワークアドレス+オール1”を選択します。

- 0.0.0.0
- 255.255.255.255
- ネットワークアドレス+オール0
(ネットワークアドレスのホスト部をオール0にしたもの)
- ネットワークアドレス+オール1
(ネットワークアドレスのホスト部をオール1にしたもの)

◇ RIP 情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [IP 関連] → [RIP 情報]

RIP 情報	
RIP 送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> V1 で送信する <input type="radio"/> V2 で送信する <input type="radio"/> V2 (Multicast) で送信する
RIP 受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1 で受信する <input type="radio"/> V2、V2 (Multicast) で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》 メトリック値 <input type="text" value="0"/>	
《 RIP V2 使用時に認証/パケットを破棄しない時は RIP V2 パスワードを設定してください。》 認証/パケット <input type="radio"/> 破棄する <input checked="" type="radio"/> 破棄しない パスワード <input type="text"/>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

RIP を使用できるインタフェースの定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

NAT 機能と併用することはできません。

RIP 送信

RIP 情報を送信するかどうかを選択します。送信する設定にすると、RIP 情報を定期的に送信します。RIP 送信を行う場合は、RIP の種類を選択します。

- V1
ルーティングプロトコルに RIP V1 を使用し、ブロードキャストで送信します。
- V2
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストで送信します。
- V2 (Multicast)
ルーティングプロトコルに RIP V2 を使用し、マルチキャストで送信します。

RIP 受信

RIP 情報を受信するかどうかを選択します。RIP 受信を行う場合は、RIP の種類を選択します。

- V1
ルーティングプロトコルに RIP V1 を使用し、受信します。
- V2、V2 (Multicast)
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストおよびマルチキャストを受信します。

メトリック値

RIP 送信時に加算するメトリック値を選択します。

認証パケット

RIP V2 使用時にだけ有効な設定です。RIP V2 では、同じパスワードグループでだけ RIP 情報の交換を行うことができます。パスワード認証による RIP 情報の交換を行う場合は、“破棄しない”を選択し、パスワードを16文字以内で指定します。“破棄する”を選択した場合は、パスワード認証による RIP 情報の交換は行いません。

◇ OSPF 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[OSPF 情報]

■OSPF情報	
OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
エリア定義番号	0
出力コスト	10
指定ルータ優先度	1
Helloパケット送信間隔	10 秒
隣接ルータ停止確認間隔	40 秒
パケット再送間隔	5 秒
LSUパケット送信遅延時間	1 秒
認証方式	<input checked="" type="radio"/> 認証を行わない <input type="radio"/> テキスト認証 鍵種別 <input checked="" type="radio"/> 文字列 <input type="radio"/> 16進数 認証鍵 <input type="text"/> <input type="radio"/> MD5認証 MD5認証鍵ID <input type="text"/> MD5認証鍵 <input type="text"/>
パケット送信	<input type="radio"/> 抑止する <input checked="" type="radio"/> 抑止しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ループバックインタフェースも含めて、OSPF を使用できるインタフェースの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

NAT 機能と併用することはできません。

OSPF 機能

OSPF を使用する場合は、“使用する” を選択します。

エリア定義番号

エリアの定義番号を10進数を使用して指定します。OSPF エリア情報は、「ルーティングプロトコル情報」→[OSPF 関連] で設定することができます。省略時は、0 が設定されます。

出力コスト

OSPF 出力コストを 1～65535 の範囲で指定します。省略時は、10 が設定されます。

指定ルータ優先度

指定ルータおよび副指定ルータを決定するための優先度を 0～255 の範囲で指定します。値が大きいほど優先度は高くなります。省略時は、1 が設定されます。

こんな事に気をつけて

値が 0 の場合は、指定ルータおよび副指定ルータにはなりません。

Hello パケット送信間隔

OSPF 隣接関係の維持に使用する、Hello パケットの送信間隔を指定します。通常は、“10 秒” を指定します。

有効範囲)

1～18 時間

1～1092 分

1～65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ Hello パケットの送信間隔を指定してください。

隣接ルータ停止確認間隔

OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。隣接ルータ停止確認間隔は、Hello パケット送信間隔より大きな値を指定する必要があります。Hello パケット送信間隔の 4 倍を設定することをお勧めします。通常は“40 秒” を指定します。

有効範囲)

1～18 時間

1～1092 分

1～65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ隣接ルータ停止確認間隔を指定してください。隣接ルータ停止確認間隔は、装置起動時に指定ルータおよび副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を指定した場合は、経路交換の開始が遅れます。

パケット再送間隔

OSPF パケットを再送する間隔を指定します。省略時は、5 秒が設定されます。

有効範囲)

1～18 時間

1～1092 分

3～65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。省略時は、1 秒が設定されます。

有効範囲)

1～18 時間

1～1092 分

1～65535 秒

こんな事に気をつけて

一般的な装置では、LSU を作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

認証方式

パケット認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が“文字列”の場合は、8 文字以内で指定します。鍵種別が“16 進数”の場合は、16 進数を使用して 16 桁以内で指定します。16 桁未満の鍵を指定した場合、左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。

MD5 認証鍵 ID

MD5 認証鍵 ID を 1～255 の範囲で指定します。

MD5 認証鍵

MD5 認証鍵を指定します。16 文字以内で指定します。

パケット送信

OSPFパケットの送信を抑止する場合は、“抑止する”を選択します。

◇スタティック経路情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正] → [IP関連] → [スタティック経路情報]

■スタティック経路情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

あて先IPアドレス/マスク	中継ルータアドレス	メトリック値	優先度	操作
<input type="button" value="全削除"/>				
<スタティック経路情報入力フィールド>				
ネットワーク	<input type="radio"/> デフォルトルート 中継ルータアドレス <input style="width: 100%;" type="text"/>			
	<input checked="" type="radio"/> ネットワーク指定 あて先IPアドレス <input style="width: 100%;" type="text"/> あて先アドレスマスク <input style="width: 100%;" type="text" value="0 (0.0.0.0)"/> 中継ルータアドレス <input style="width: 100%;" type="text"/>			
	メトリック値	<input style="width: 100%;" type="text" value="1"/>		
	優先度	<input style="width: 100%;" type="text" value="0"/>		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されているスタティック経路情報の定義が表示されています。スタティック経路の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。「疑似ルータ」をチェックした場合、“メトリック値”と“優先度”の項目はありません。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。

- デフォルトルート
中継ルータアドレスを指定します。
- ネットワーク指定
あて先IPアドレス、あて先アドレスマスク、中継ルータアドレスを指定します。

メトリック値

スタティック経路情報をRIPに再配布するときのメトリック値を、1～15から選択します。RIPに再配布したときは、設定したRIPメトリック値+1のメトリック値でRIPテーブルに登録されます。

優先度

スタティック経路情報の優先度を、10進数を使用して0～254で指定します。省略時は、0が設定されます。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
EBGP	20
OSPF	110
RIP	120
IBGP	200
DNS	15

複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、「ルーティングプロトコル情報」の「ルーティングマネージャ情報」にある ECMP 情報で、ECMP を使用するよう設定します。ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。

- 優先度が0のスタティック経路情報と、優先度が0以上のスタティック経路情報は同時に設定できません。
 - 優先度が同じで、メトリック値が違うスタティック経路情報は同時に設定できません。
-

◇ IPフィルタリング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP関連]→[IPフィルタリング情報]

■IPフィルタリング情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号 ICMPタイプ ICMPコード	TCP接続要求	TOS	方向	操作
							修正 初期化
条件にあてはまらない場合の動作			透過				
全削除							
<IPフィルタリング情報入力フィールド>							
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断						
プロトコル	すべて (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)						
送信元情報	IPアドレス	<input type="text"/>					
	アドレスマスク	0 (0.0.0.0)					
	ポート番号	<input type="text"/>					
あて先情報	IPアドレス	<input type="text"/>					
	アドレスマスク	0 (0.0.0.0)					
	ポート番号	<input type="text"/>					
ICMP	タイプ	<input type="text"/>					
	コード	<input type="text"/>					
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外						
TOS	<input type="text"/>						
方向	入出力						
追加 キャンセル							

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている IP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。IP フィルタリングの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

「条件にあてはまらない場合の動作」の「初期化」ボタンをクリックすると、初期状態（透過）が設定されます。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IP フィルタリングの動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の6つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

フィルタリング条件としてのIPアドレスおよびアドレスマスクを指定します。チェック対象となったパケットのIPアドレスと定義したアドレスマスクの論理積と、定義したIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。

“any”を指定した場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は“,”で区切ります。範囲指定の場合は“-”で区切ります。送信元情報とあて先情報で合わせて10組まで指定できます。

ICMP

タイプ

フィルタリング条件としてICMPパケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMPタイプ値を複数指定する場合は“,”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPタイプ値をフィルタリングの対象とします。

コード

フィルタリング条件としてICMPパケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMPコード値を複数指定する場合は“,”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPコード値をフィルタリングの対象とします。

TCP 接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

TOS

フィルタリング条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は“,”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も設定しない場合はすべてのTOSフィールド値をフィルタリングの対象とします。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
- 出力のみ
出力パケットだけをフィルタリングする対象とします。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下の2つを逆転した条件でフィルタリングします。
 - 送信元 IP アドレス / アドレスマスク とあて先 IP アドレス / アドレスマスク
 - 送信元ポート番号 とあて先ポート番号入力パケットは、IP アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対しても TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とします。

◇ IPフィルタリング情報（条件にあてはまらない場合の動作）

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP関連]→[IPフィルタリング情報]
→「条件にあてはまらない場合の動作」[修正]

■IPフィルタリング情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	プロトコル	送信元IPアドレス/マスク	送信元ポート番号	TCP接続要求	TOS	方向	操作
			あて先IPアドレス/マスク					
			あて先ポート番号					
			ICMPタイプ					
			ICMPコード					

<IPフィルタリング情報入力フィールド(条件にあてはまらない場合)>

動作

透過
 遮断
 SPI

情報保持タイム 分

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されているIPフィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

こんな事に気をつけて

動作に遮断やSPIを指定し、IPフィルタリング情報でWWWやDHCPに対するアクセスを透過する設定を行わなかった場合、本装置に対しWWWブラウザからアクセスできない、または、DHCP機能が使用できなくなることがあります。

動作

IPフィルタリング定義のどれにも一致しない場合の動作を以下の3つから選択します。

- 透過
IPフィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IPフィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IPフィルタリング定義のどれにも一致しないで、プロトコルがTCPの場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルがUDPやそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイマ

SPIセッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

◇ TOS 値書き換え情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [IP 関連] → [TOS 値書き換え情報]

■TOS 値書き換え情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	プロトコル	送信元IPアドレス/マスク	TOS	操作
		送信元ポート番号	新TOS	
		あて先IPアドレス/マスク		
		あて先ポート番号		

<TOS 値書き換え情報入力フィールド>

プロトコル すべて 番号指定: “その他”を選択時のみ有効です

送信元情報	IPアドレス	<input type="text"/>
	アドレスマスク	<input type="text" value="0 @.0.0.0"/>
	ポート番号	<input type="text"/>
あて先情報	IPアドレス	<input type="text"/>
	アドレスマスク	<input type="text" value="0 @.0.0.0"/>
	ポート番号	<input type="text"/>
TOS		<input type="text"/>
新TOS		<input type="text"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

現在、このネットワークに設定されている TOS 値書き換え情報の定義が表示されています。処理は優先順位 1 から順に行われます。TOS 値書き換えの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された TOS 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

プロトコル

TOS 値書き換えの条件としてプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

TOS 値書き換え条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

TOS 値書き換え条件としてのIPアドレスおよびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

TOS 値書き換え条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。

“any”を指定する場合は、すべてのポート番号がTOS書き換えの対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報で合わせて10組まで指定できます。

TOS

TOS 値書き換えの条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTOSフィールド値を書き換えの対象とします。

新TOS

IPパケットに新しく指定するTOSフィールド値を16進数を使用して、0～ffの範囲で指定します。

◇ RIP フィルタリング情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [IP 関連] → [RIP フィルタリング情報]

RIP フィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
全削除					
<RIP フィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断				
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信				
フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定				
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致			
	IP アドレス	<input type="text"/>			
	アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>			
メトリック値	<input type="text"/>				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている RIP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

フィルタリング対象に該当する RIP 経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリング条件に該当するかチェックするタイミングを以下の 2 つから選択します。

- 受信
RIP パケット受信時に、フィルタリング条件に該当するかチェックします。
- 送信
RIP パケット送信時に、フィルタリング条件に該当するかチェックします。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報がフィルタリングの対象となります。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できません。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

- 完全に一致
指定した IP アドレスとアドレスマスクが完全に一致した RIP 経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定した IP アドレスと、RIP 経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、その RIP 経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になったRIP経路情報のメトリック値を変更ができます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

◇ NAT 情報

[操作] 「設定メニュー」→ルータ設定「LAN情報」→[修正]→[IP関連]→[NAT情報]

■NAT情報	
NATの使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ ※NATの使用とDHCPリレーサービスの併用はできません
グローバルアドレス	<input type="text"/>
アドレス個数	1 個
アドレス割当てタイム	5 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsecパスルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

NATの使用

“マルチNAT”を選択すると、複数の端末と併用できます。“静的NATのみ”を選択すると静的NAT情報の条件に一致しないパケットは変換されません。NATを使用しない場合は、以降の設定は無効です。

こんな事に気をつけて

本装置では相手情報とLAN情報の各インタフェースでアドレス変換機能を設定できます。ただし、使用する場合は、グローバルアドレスを使用するインタフェースだけで設定します。また、基本NATと静的NATで同一グローバルアドレスを使用しないでください。

グローバルアドレス

特定のグローバルアドレスを使用するときに指定します。指定しない場合は自動で割り当てられます。

アドレス個数

複数個のグローバルアドレスを使用する場合は、上述のグローバルアドレスを先頭とし連続した複数のアドレスを指定できます。その個数を1～16の範囲で指定します。なお、アドレス個数の設定はグローバルアドレスを指定した場合にだけ有効です。省略時は、1が設定されます。

アドレス割当てタイム

アドレス変換情報は一定の時間、該当する通信が行われないと、自動的に解放されます。解放するための猶予時間を0～24時間の範囲で指定します。0を指定すると、タイムによる情報の解放は行われません。省略時は、5分が設定されます。

NAT セキュリティ

- 通常
相手サーバがNATを使用している際など、要求先とは別のアドレスから応答します。
- 高い
ftp や dns の要求する相手からの応答かどうかをチェックします。

IPsec パススルー

- 有効
相手ごとに1つのIPsecパスを接続することができます。
- 無効
IPsecクライアントがNATトラバーサル機能を使用することができます。

こんな事に気をつけて

IPsecクライアントがNATトラバーサル機能を使用する場合は、IPsecパススルーを“無効”に設定します。IPsecパススルーを“有効”に設定すると、相手ごとに1つのIPsecパスしか接続することができません。

◇ 静的 NAT 情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [IP 関連] → [静的 NAT 情報]

■ 静的 NAT 情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

プライベートアドレス	プライベートポート番号	グローバルアドレス	グローバルポート番号	プロトコル	操作
条件にあてはまらない場合の動作				破棄	修正 初期化
全削除					

<静的NAT情報入力フィールド>

プライベート IP 情報	IP アドレス	ポート番号	すべて (番号指定: <input type="text"/> “その他”を選択時のみ有効です)	グローバル IP 情報	IP アドレス	ポート番号	すべて (番号指定: <input type="text"/> “その他”を選択時のみ有効です)	プロトコル	すべて (番号指定: <input type="text"/> “その他”を選択時のみ有効です)
--------------	---------	-------	--	-------------	---------	-------	--	-------	--

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

NAT 機能を使用すると、アドレス変換情報を固定で持つことができます。現在、設定されている固定のアドレス情報の定義が表示されています。静的 NAT の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックします。

「条件にあてはまらない場合の動作」の「初期化」ボタンをクリックすると、初期状態（透過）が設定されます。

プライベート IP 情報

IP アドレス

固定でアドレス変換を行う場合にローカルネットワーク側の IP アドレスを指定します。省略できません。

ポート番号

固定でアドレス変換を行う場合にローカルネットワーク側のポート番号を選択します。“その他”を選択し、ポート番号を指定する場合は、10進数を使用して1～65535の範囲で指定します。

なお、グローバルポート番号を範囲指定した場合、その範囲のグローバルポート番号は指定したプライベートポート番号を先頭とした範囲に変換されます。

たとえば、プライベートポート番号に1000を指定し、グローバルポート番号に10000-11000を指定すると、グローバルポート番号の10000から11000はプライベートポート番号の1000から2000に変換されます。

グローバル IP 情報

IP アドレス

固定でアドレス変換を行う場合にリモートネットワーク側の IP アドレスを指定します。省略時は、すべてのグローバルアドレスに対して有効な指定となります。

ポート番号

固定でアドレス変換を行う場合にリモートネットワーク側のポート番号を選択します。“その他”を選択し、ポート番号を指定する場合は、10進数を使用して1～65535の範囲から1つ、または“-”で区切った1組の範囲を指定します。

プロトコル

固定でアドレス変換を行う場合に対象となるプロトコルを以下の8つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- esp (50)
- ah (51)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

◇ 静的 NAT 情報 (条件にあてはまらない場合の動作)

[操作] 「設定メニュー」 → ルータ設定 「LAN 情報」 → [修正] → [IP 関連] → [静的 NAT 情報]
→ 「条件にあてはまらない場合の動作」 [修正]

静的 NAT 情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

プライベートアドレス	プライベートポート番号	プロトコル	操作
グローバルアドレス	グローバルポート番号		
<静的 NAT 情報入力フィールド(条件にあてはまらない場合)>			
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 破棄		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>			
<input type="button" value="全削除"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている静的 NAT 定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。

動作

静的 NAT 定義のどれにも一致しない場合の IP フィルタリングの動作を以下の 2 つから選択します。

- 透過
静的 NAT 定義のどれにも一致しない場合にパケットを透過します。
- 破棄
静的 NAT 定義のどれにも一致しない場合にパケットを破棄します。

◇帯域制御 (WFQ) 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP関連]→[帯域制御 (WFQ) 情報]

■帯域制御(WFQ)情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

定義番号	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号	対象TOSフィールド値 帯域	操作
<input type="button" value="全削除"/>				
<帯域制御(WFQ)情報入力フィールド>				
プロトコル		すべて <input type="button" value="▼"/> (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)		
送信元情報	IPアドレス	<input type="text"/>		
	アドレスマスク	0 (0.0.0.0) <input type="button" value="▼"/>		
	ポート番号	<input type="text"/>		
あて先情報	IPアドレス	<input type="text"/>		
	アドレスマスク	0 (0.0.0.0) <input type="button" value="▼"/>		
	ポート番号	<input type="text"/>		
対象TOSフィールド値		<input type="text"/>		
帯域		<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="button" value="▼"/> <input type="radio"/> 帯域を他と共有 <input type="button" value="▼"/> 共有できる定義が存在しません		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

現在、このインタフェースに設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

プロトコル

帯域制御の対象となるプロトコルを以下の6つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPアドレス／アドレスマスク

帯域制御の対象となるIPアドレスおよびアドレスマスクを指定します。対象となるパケットのIPアドレスと定義するアドレスマスクの論理積と、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

対象TOSフィールド値

帯域制御の対象となるTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTOSフィールド値を帯域制御の対象とします。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

IPv4/IPv6以外のパケットは、すべて非優先（ベストエフォート）として扱われます。

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

◇ DHCP 情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [IP 関連] → [DHCP 情報]

▲ DHCPクライアントで運用する場合、設定はIPアドレス情報で行ってください。

DHCP 情報

使用しない

リレー機能を使用する

DHCPサーバIPアドレス1

DHCPサーバIPアドレス2

サーバ機能を使用する

割当て先頭IPアドレス

割当てアドレス数

リース期間 日

デフォルトルータ広報

DNSサーバ広報

セカンダリDNSサーバ広報

ドメイン名広報

※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

DHCP 機能

それぞれのインタフェースのDHCP機能を設定することができます。本装置を該当インタフェースのネットワークのDHCPサーバとして使用する場合は、“サーバ機能を使用する”を選択します。また、ほかのネットワークのDHCPサーバを、このネットワークのDHCPサーバとして使用することもできます。その場合は、“リレー機能を使用する”を選択し、利用するDHCPサーバのIPアドレスを指定します。該当インタフェースをDHCPクライアントとして運用する場合は、“IPアドレス情報の設定で”DHCPで自動的に取得する”を選択します。

割当て先頭IPアドレス

DHCPサーバ機能によって、割り当てる連続したアドレス群の先頭のIPアドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

割当てアドレス数

DHCPサーバ機能で割り当てるアドレス数を1~253の範囲で指定します。省略時は、32が設定されます。ホストデータベース機能を使用すると、特定のDHCPクライアントに対して固有のIPアドレスを割り当てることができます。この場合のIPアドレスは、割当て先頭IPアドレスと割当てアドレス数によって規定される動的割り当て範囲である必要はありません。

リース期間

DHCPサーバ機能によって割り当てたIPアドレスを貸し出す期間を、1時間以上、365日未満の範囲で指定します。0を指定した場合は、無期限が設定されます。省略時は、1日が設定されます。

デフォルトルータ広報

DHCPサーバで広報するデフォルトルータのIPアドレスを指定します。省略するか0.0.0.0を指定するとDHCPサーバによる広報は行いません。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

DNS サーバ広報

DNS サーバの IP アドレスを指定します。省略するか 0.0.0.0 を指定すると DHCP サーバによる広報は行いません。ProxyDNS を使用する場合は、本装置の IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

セカンダリ DNS サーバ広報

セカンダリ DNS サーバの IP アドレスを指定します。省略するか 0.0.0.0 を指定すると DHCP サーバによる広報は行いません。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

ドメイン名広報

ドメイン名を 80 文字以内で指定します。省略時は、DHCP サーバによる広報は行いません。

◇ ICMP 情報

[操作] 「設定メニュー」 → ルータ設定 「LAN 情報」 → [修正] → [IP 関連] → [ICMP 情報]

■ICMP情報 ⓘ

ICMPリダイレクトパケット 送信する 送信しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ICMP リダイレクトパケット

ICMP リダイレクトパケットを送信する場合は、“送信する”を選択します。

◇マルチキャスト情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP関連]→[マルチキャスト情報]

■マルチキャスト情報	
マルチキャスト機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> static <input type="radio"/> PIM-DM <input type="radio"/> PIM-SM
TTLしきい値	<input type="text" value="1"/>
PIMプリファレンス値	<input type="text" value="1024"/>
上流ルータの種類	<input checked="" type="radio"/> PIMルータのみ <input type="radio"/> すべて

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

マルチキャストを使用できるインタフェースの定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。

マルチキャスト機能

LAN上でマルチキャスト機能を使用する場合は、マルチキャスト・プロトコルを選択します。

こんな事に気をつけて

- マルチキャスト機能を使用するすべてのインタフェース上で、同じプロトコルを選択してください。同時に複数のプロトコルを使用することはできません。
- NAT 機能と併用することはできません。

TTL しきい値

LAN上でマルチキャスト機能を使用するときの TTL しきい値を 10 進数を使用して 1～255 の範囲で指定します。初期値は 1 です。

PIM-SM の PIM Register パケットによりカプセル化されるマルチキャスト・パケットは、出力先インタフェースの TTL しきい値の設定にかかわらず出力されます。

PIM プリファレンス値

PIM の Assert メッセージに格納されるプリファレンス値を 10 進数を使用して 1～65535 の範囲で指定します。初期値は 1024 です。

並列な経路の存在のためにマルチキャスト・パケットが重複した場合は、PIM Assert メッセージによって、片側の転送経路が遮断されます。この際、プリファレンス値の小さい方の経路が有効になります。PIM Assert メッセージの発行時には、Assert 対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインタフェースのプリファレンス値を Assert メッセージに格納します。Assert メッセージが出力されるインタフェースのプリファレンス値が格納されるわけではありません。

上流ルータの種類

本装置より上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送される場合、どの種類のルータからのマルチキャストパケット転送を許可するかを指定します。

上流ルータが PIM ルータでない場合（マルチキャストパケットをスタティック経路によって転送するルータであった場合）に転送を許可する場合は、“すべて”を選択します。

こんな事に気をつけて

受信インタフェースと同一の IP セグメントから送信された（直接接続されたホストからの）マルチキャストパケットは、上流ルータの設定にかかわらず転送が行われます。

◇ BGP/MPLS VPN 情報

[操作] 「設定メニュー」 → ルータ設定 「LAN 情報」 → [修正] → [IP 関連] → [BGP/MPLS VPN 情報]

■ BGP/MPLS VPN 情報	
BGP/MPLS VPN 機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
VRF 定義番号	<input type="text" value="0"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

BGP/MPLS VPN 機能

BGP/MPLS VPN を利用する場合は、“使用する” を選択します。

こんな事に気をつけて

- BGP/MPLS VPN で使用できる IBGP は 1 セッションだけです。
- IP-VPN 接続と併用することはできません。

VRF 定義番号

BGP/MPLS VPN 機能を利用する場合は、VRF を定義する必要があります。VRF の定義番号を 10 進数を使用して指定します。VRF 情報は「ルーティングプロトコル情報」
－ [BGP 関連] － [VRF 情報] で設定します。

こんな事に気をつけて

BGP/MPLS VPN で構成された VPN ネットワーク内では EBGP/OSPF/RIP は使用できません。

◇ BGP/MPLS VPN スタティック経路情報

[操作] 「設定メニュー」 → ルータ設定 「LAN 情報」 → [修正] → [IP 関連]
→ [BGP/MPLS VPN スタティック経路情報]

■ BGP/MPLS VPN スタティック経路情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

定義番号	あて先IPアドレス	あて先アドレスマスク	中継ルータアドレス	操作
全削除				
<スタティック経路情報入力フィールド>				
ネットワーク	<input type="radio"/> デフォルトルート 中継ルータアドレス <input type="text"/>			
	<input checked="" type="radio"/> ネットワーク指定 あて先IPアドレス <input type="text"/> あて先アドレスマスク <input type="text" value="0 (0.0.0.0)"/> 中継ルータアドレス <input type="text"/>			
	追加 キャンセル			
	設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。			

現在、設定されている BGP/MPLS VPN スタティック経路情報の定義が表示されています。スタティック経路の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。ただし、デフォルトルートおよび同じ「あて先IPアドレス」はインタフェースごとに1つだけ設定できます。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

- BGP/MPLS VPN スタティック経路情報で優先度は設定できません。優先度は1となります。
- デフォルトルートおよび同じ「あて先IPアドレス」はインタフェースごとに1つだけ設定できます。

ネットワーク

“デフォルトルート” または “ネットワーク指定” を選択します。

- デフォルトルート
中継ルータアドレスを指定します。
- ネットワーク指定
あて先IPアドレス、あて先アドレスマスク、中継ルータアドレスを指定します。

◇ ARP 情報

[操作] 「設定メニュー」 → ルータ設定 「LAN 情報」 → [修正] → [IP 関連] → [ARP 情報]

■ ARP 情報	
ARP 定期送信機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 送信間隔 <input type="text"/> 分
Proxy ARP 機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
ローカル Proxy ARP 機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ARP 定期送信機能

ARP を定期的に送信する機能です。ARP 定期送信機能を使用する場合は、“使用する” を選択し、送信間隔を設定します。

送信間隔

10 進数を使用して、10～1200 秒の範囲で指定します。

Proxy ARP 機能

本装置を経由して到達できる IPv4 アドレスに対する ARP 要求に対し代理応答する機能です。代理応答させない場合は“使用しない”を選択します。

ローカル Proxy ARP 機能

ARP 要求を受信したインタフェースの IPv4 ネットワーク範囲すべての要求に対し、代理応答する機能です。この機能は、端末間の直接通信が意図的に禁止されているネットワークでだけ使用してください。

13.3 IPv6 関連

[操作] 「設定メニュー」 → ルータ設定「LAN0 情報 (物理 LAN)」 → [修正] → [IPv6 関連]

LAN0情報(物理LAN)				
共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
IPv6基本情報		IPv6 RIP情報		IPv6スタティック経路情報
IPv6フィルタリング情報		IPv6 Traffic Class値書き換え情報		IPv6 RIPフィルタリング情報
IPv6帯域制御(QWFQ)情報				

◇ IPv6 基本情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [IPv6 関連] → [IPv6 基本情報]

■ IPv6基本情報 ?

IPv6 使用しない 使用する

インタフェースID 自動 指定する

IPv6 アドレス	アドレスまたはプレフィックス	Valid Lifetime		Pref. Lifetime		フラグ
		期限有	無期限	期限有	無期限	
	<input type="text"/>	30	<input type="text"/> 日 <input type="checkbox"/>	7	<input type="text"/> 日 <input type="checkbox"/>	c:0
	<input type="text"/>	30	<input type="text"/> 日 <input type="checkbox"/>	7	<input type="text"/> 日 <input type="checkbox"/>	c:0
	<input type="text"/>	30	<input type="text"/> 日 <input type="checkbox"/>	7	<input type="text"/> 日 <input type="checkbox"/>	c:0
	<input type="text"/>	30	<input type="text"/> 日 <input type="checkbox"/>	7	<input type="text"/> 日 <input type="checkbox"/>	c:0

ルータ広報 送信しない 送信する

最大送信間隔	<input type="text"/> 600 秒
最小送信間隔	<input type="text"/> 200 秒
Router Lifetime	<input type="text"/> 1800 秒
MTU	<input type="text"/>
Reachable Time	<input type="text"/> 0 ミリ秒
Retrans Timer	<input type="text"/> 0 ミリ秒
Cur Hop Limit	<input type="text"/> 64
フラグ	<input type="text"/> 00

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IPv6

IPv6通信を行う場合は、“使用する”を選択します。

インタフェースID

“自動”を選択する場合は、装置のMACアドレスから自動生成されるインタフェースIDを使用します。通常は、“自動”を選択します。

“指定する”を選択する場合は、16ビットごとに区切り文字(:)を入れて、16進数を使用して16桁でインタフェースIDを指定します。このとき、他装置と同じインタフェースIDとならないような値を指定します。

記述例) 2001:db8:7654:3210

IPv6 アドレス

この装置で使用する IPv6 アドレスを 4 個まで設定できます。

アドレスまたはプレフィックス

本装置の LAN 側の IPv6 アドレスを標準的な IPv6 アドレス表記方式で指定します。本装置ではプレフィックス長は 64 に固定されます。インタフェース ID 部分がすべて 0 の場合、指定したアドレスはプレフィックスとして解釈され、実際に利用するアドレスはそのアドレスにインタフェース ID を付与したものとなります。リンクローカルアドレスは指定できません。

IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は、上位を “dhcp@インタフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インタフェース名には、IPv6 DHCP クライアント機能が動作している rmt インタフェースを指定します。

記述例)

2001:db8:1111:1000:1:2:3:4

完全な IPv6 アドレスとして解釈されます。

2001:db8:1111:1000::

プレフィックスとして解釈され、インタフェース ID 部分にはインタフェース ID が付与されます。

dhcp@rmt0:1000::1

rmt0 インタフェースで動作している IPv6 DHCP クライアントが取得したプレフィックスを使用して完全な IPv6 アドレスを指定します。

dhcp@rmt0:1000::

rmt0 インタフェースで動作している IPv6 DHCP クライアントが取得したプレフィックスを使用してプレフィックスを指定します。

Valid Lifetime

ルータ広報のプレフィックス情報ごとに設定する Valid Lifetime を指定します。通常は、“30 日” を指定します。

有効範囲)

0～365 日

0～8760 時間

0～525600 分

0～31536000 秒

期限を定めない場合（無期限の場合）は、チェックボックスをチェックします。

IPv6 アドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した Valid Lifetime と比較して短い方が有効になります。

Pref. Lifetime

ルータ広報のプレフィックス情報ごとに設定する Preferred Lifetime を指定します。通常は、“7 日” を指定します。

有効範囲)

0～365 日

0～8760 時間

0～525600 分

0～31536000 秒

期限を定めない場合（無期限の場合）は、チェックボックスをチェックします。

IPv6 アドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した Preferred Lifetime と比較して短い方が有効になります。

フラグ

ルータ広報のプレフィックス情報ごとに設定するフラグフィールドの内容を 16 進数を使用して 2 桁で指定します。この領域の値として、RFC2461 で以下の値が定義されています。必要に応じて以下の値の論理和を設定します。

- on-link flag 80
- autonomous address-configuration flag 40

通常は “c0” を指定します。

ルータ広報

ルータ広報メッセージ (router advertisement message) を送信する場合は“送信する”を選択し、以下の項目を設定します。

最大送信間隔

ルータ広報メッセージの最大送信間隔を指定します。初期値は600秒です。省略はできません。

有効範囲) 4～1800

最小送信間隔

ルータ広報メッセージの最小送信間隔を指定します。初期値は200秒です。省略はできません。

有効範囲) 3～最大送信間隔の3／4

Router Lifetime

ルータ広報で送信する Router Lifetime を指定します。初期値は1800秒です。省略はできません。

有効範囲) 0または最大送信間隔～9000

MTU

ルータ広報で送信する MTU option を指定します。省略時は、MTU option を含みません。

有効範囲) 1280～1500

Reachable Time

ルータ広報で送信する Reachable Time を指定します。省略値は0ミリ秒です。

有効範囲) 0～3600000

Retrans Timer

ルータ広報で送信する Retrans Timer を指定します。省略値は0ミリ秒です。

有効範囲) 0～4294967295

Cur Hop Limit

ルータ広報で送信する Cur Hop Limit を指定します。省略値は64です。

有効範囲) 0～255

フラグ

ルータ広報の本体部分に設定するフラグフィールドの内容を16進数を使用して2桁で指定します。この領域の値として、RFC2461で以下の値が定義されています。必要に応じて以下の値の論理和を設定します。省略値は00です。

- Managed address configuration flag 80
- Other stateful configuration flag 40

◇ IPv6 RIP 情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [IPv6 関連] → [IPv6 RIP 情報]

IPv6 RIP 情報											
RIP送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する メトリック値 <input type="text" value="0"/>										
RIP受信	<input checked="" type="radio"/> 受信しない <input type="radio"/> 受信する										
集約経路送信	<table border="1"> <thead> <tr> <th>集約経路</th> <th>破棄経路設定</th> </tr> </thead> <tbody> <tr> <td> <input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/> </td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> </tbody> </table>	集約経路	破棄経路設定	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する
	集約経路	破棄経路設定									
	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/>	<input checked="" type="checkbox"/> 設定する									
	<input type="text"/>	<input checked="" type="checkbox"/> 設定する									
<input type="text"/>	<input checked="" type="checkbox"/> 設定する										
<input type="text"/>	<input checked="" type="checkbox"/> 設定する										
サイトローカルプレフィックス	<input type="radio"/> 交換しない <input checked="" type="radio"/> 交換する										

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 | キャンセル

RIPを使用できるインターフェースの定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。

RIP 送信

RIPを送信する場合は、“送信する”を選択します。

メトリック値

“送信する”を選択した場合に、加算するメトリック値を選択します。

RIP 受信

RIPを受信する場合は、“受信する”を選択します。

集約経路送信

RIPで集約経路を送信する場合に、集約して広報する経路を設定します。

集約経路

デフォルトルートまたはネットワーク指定を選択し、集約して広報する経路を指定します。

集約経路情報は、集約される経路情報がないときでも広報されます。また、同じあて先の経路情報がルーティングテーブルにないときでも広報され、ルーティングテーブルには設定されません。

- デフォルトルート
集約経路情報としてデフォルトルートだけを広報します。
- ネットワーク指定
集約経路情報をプレフィックス/プレフィックス長で指定します。指定した集約経路情報は広報され、集約経路情報に含まれる経路情報は広報されません。

破棄経路設定

広報した集約経路情報により本装置に送られたIPパケットをルーティングするための経路情報がないときに、そのあて先へは到達不能であることをICMPv6で通知することができます。チェックしないときは、そのあて先への経路がないことがICMPv6で通知されます。

チェックしたときは、集約経路情報と同じあて先の経路情報が破棄経路としてルーティングテーブルが設定されます。

サイトローカルプレフィックス

サイトローカルプレフィックスを交換する場合は、“交換する”を選択します。

◇ IPv6 スタティック経路情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 スタティック経路情報]

IPv6 スタティック経路情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

あて先プレフィックス/プレフィックス長	中継ルータアドレス	メトリック値	優先度	操作
全削除				
<IPv6 スタティック経路情報入力フィールド>				
<input type="radio"/> デフォルトルート 中継ルータアドレス <input style="width: 150px;" type="text"/>				
<input checked="" type="radio"/> ネットワーク指定 ネットワーク あて先プレフィックス/プレフィックス長 <input style="width: 150px;" type="text"/> / <input style="width: 30px;" type="text"/>				
中継ルータアドレス <input style="width: 150px;" type="text"/>				
メトリック値	<input type="text" value="1"/>			
優先度	<input type="text" value="0"/>			
追加 キャンセル				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在 LAN 側に設定されている IPv6 スタティック経路情報の定義が表示されています。IPv6 スタティック経路の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

IPv6 経路情報を固定で設定できます。ただし、デフォルトルートは装置に 1 つしか設定できません。

ネットワーク

“デフォルトルート” または “ネットワーク指定” を選択します。

- デフォルトルート
中継ルータアドレスを指定します。
- ネットワーク指定
あて先プレフィックス/プレフィックス長、中継ルータアドレスを指定します。
あて先ネットワークにリンクローカルアドレスは指定できません。ICMPv6 Redirect を正常に動作させるためには、中継ルータアドレスはリンクローカルアドレスで指定する必要があります。

メトリック値

このスタティック経路情報を RIP に再配布するときのメトリック値を、1～15 から選択します。RIP に再配布したときは、設定した RIP メトリック値 + 1 のメトリック値で RIP テーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10進数を使用して0～254で指定します。省略時は、0が設定されます。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度 (省略時)
RIP	120
DNS	15
DHCP	10

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。

- 優先度が0のスタティック経路情報と、優先度が0以上のスタティック経路情報は同時に設定できません。
 - 優先度が同じスタティック経路情報は同時に設定できません。
-

◇ IPv6 フィルタリング情報

[操作] 「設定メニュー」 → ルータ設定 「LAN 情報」 → [修正] → [IPv6 関連] → [IPv6 フィルタリング情報]

■ IPv6 フィルタリング情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	プロトコル	送信元IPv6アドレス/プレフィックス長	TCP接続要求	Traffic Class	方向	操作
			送信元IPv6アドレス/プレフィックス長				
			送信元ポート番号				
			あて先IPv6アドレス/プレフィックス長				
			あて先ポート番号				
			ICMPv6タイプ				
			ICMPv6コード				
条件にあてはまらない場合の動作						透過	修正 初期化
全削除							

<IPv6フィルタリング情報入力フィールド>

動作 透過 遮断

プロトコル すべて (番号指定: “その他”を選択時のみ有効です)

送信元情報
 IPv6アドレス/プレフィックス長 /
 ポート番号

あて先情報
 IPv6アドレス/プレフィックス長 /
 ポート番号

ICMPv6
 タイプ
 コード

TCP接続要求 対象 対象外

Traffic Class

方向 入力のみ

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このインタフェースに設定されている IPv6 フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 フィルタリングの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく行えません。

「条件にあてはまらない場合の動作」の「初期化」ボタンをクリックすると、初期状態（透過）が設定されます。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリングの動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の5つから選択します。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～254の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

フィルタリング条件としてのIPv6 アドレスおよびプレフィックス長を指定します。以下が等しい場合に条件に一致します。

- チェック対象となるパケットのIPv6 アドレスと定義するプレフィックス長の論理積
- 定義するIPv6 アドレスとプレフィックス長の論理積

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。

“any”を指定した場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

ICMPv6

タイプ

フィルタリング条件としてICMPv6 パケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMPv6タイプ値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPv6タイプ値をフィルタリングの対象とします。

コード

フィルタリング条件としてICMPv6 パケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMPv6コード値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPv6コード値をフィルタリングの対象とします。

TCP 接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

Traffic Class

フィルタリング条件としてIPv6 パケットのTraffic Class 値を16進数を使用して0～ffの範囲または“any”で指定します。Traffic Class 値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのTraffic Class 値をフィルタリングの対象とします。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
 - 送信元 IPv6 アドレス/プレフィックス長とあて先 IPv6 アドレス/プレフィックス長
 - 送信元ポート番号とあて先ポート番号リバースを指定した場合、入力パケットは IPv6 アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対しても TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

◇ IPv6 フィルタリング情報 (条件にあてはまらない場合の動作)

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 フィルタリング情報]
→「条件にあてはまらない場合の動作」[修正]

■ IPv6 フィルタリング情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	プロトコル	送信元IPv6アドレス/プレフィックス長	送信元ポート番号	TCP 接続 要求	Traffic Class	方向	操作
			あて先IPv6アドレス/プレフィックス長	あて先ポート番号				
			ICMPv6タイプ					
			ICMPv6コード					

<IPv6 フィルタリング情報入力フィールド(条件にあてはまらない場合)>

動作

透過
 遮断
 SPI

情報保持タイム 分

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている IPv6 フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断やSPIを指定し、IPv6 フィルタリング情報でWWWやDHCPに対するアクセスを透過する設定を行わなかった場合、本装置に対しWWWブラウザからアクセスできない、または、DHCP機能が使用できなくなることがあります。

動作

IPv6 フィルタリング定義のどれにも一致しない場合の動作を以下の3つから選択します。

- 透過
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IPv6 フィルタリング定義のどれにも一致しないで、プロトコルがTCPの場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルがUDPやそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイム

SPIセッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

◇ IPv6 Traffic Class 値書き換え情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]
→ [IPv6 Traffic Class 値書き換え情報]

IPv6 Traffic Class 値書き換え情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	プロトコル	送信元IPv6アドレス/プレフィックス長 送信元ポート番号 あて先IPv6アドレス/プレフィックス長 あて先ポート番号	Traffic Class 新Traffic Class	操作
				全削除

<IPv6 Traffic Class値書き換え情報入力フィールド>

プロトコル	すべて (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)
送信元情報	IPv6アドレス/プレフィックス長: <input style="width: 80%;" type="text"/> / <input style="width: 20%;" type="text"/> ポート番号: <input style="width: 95%;" type="text"/>
あて先情報	IPv6アドレス/プレフィックス長: <input style="width: 80%;" type="text"/> / <input style="width: 20%;" type="text"/> ポート番号: <input style="width: 95%;" type="text"/>
Traffic Class	<input style="width: 95%;" type="text"/>
新Traffic Class	<input style="width: 95%;" type="text"/>

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている IPv6 Traffic Class 値書き換え情報の定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Traffic Class 値書き換えの定義数は、BR500S 仕様一覧 [「2.3 システム最大値一覧」](#) (P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

プロトコル

IPv6 Traffic Class 書き換え条件としてプロトコルを以下の 5 つから選択します。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、“その他”を選択し、10 進数を使用して、0～254 の範囲で指定します。

送信元/あて先情報

IPv6 Traffic Class 値書き換え条件としてのアドレス情報を設定します。

IPv6 アドレス/プレフィックス長

IPv6 Traffic Class 値書き換え条件としての IPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットの IPv6 アドレスと定義するプレフィックス長の論理積、定義する IPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

IPv6 Traffic Class 値書き換え条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が書き換えの対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

Traffic Class

IPv6 Traffic Class 値書き換え条件としてIPv6パケットのTraffic Class 値を16進数を使用して0～ffの範囲または“any”で指定します。Traffic Class フィールド値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのIPv6 Traffic Class 値を書き換えの対象とします。

新 Traffic Class

IPv6パケットに新しく指定するIPv6 Traffic Class 値を16進数を使用して、0～ffの範囲で指定します。

◇ IPv6 RIP フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 RIP フィルタリング情報]

■ IPv6 RIP フィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
全削除					
<IPv6 RIP フィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断				
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信				
フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定				
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致			
	プレフィックス / プレフィックス長	<input type="text"/> / <input type="text"/>			
メトリック値	<input type="text"/>				
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている RIP フィルタリング定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

RIP 受信（送信）時には、優先順位の高い定義から順に受信（送信）方向の条件を参照し、一致した条件があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、受信（送信）方向のすべての条件に一致しない RIP 経路情報は遮断されます。

動作

フィルタリング対象に該当する RIP 経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合に RIP 経路情報を透過します。
- 遮断
条件と一致した場合に RIP 経路情報を遮断します。

方向

フィルタリングを RIP 受信時に行うか、RIP 送信時に行うかを選択します。

- 受信
RIP 受信時に、フィルタリングを行います。
- 送信
RIP 送信時に、フィルタリングを行います。

フィルタリング条件

フィルタリング条件を指定します。

- すべて
すべての経路情報がフィルタリングの対象となります。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。
 - 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致した RIP 経路情報をフィルタリング対象とします。“マスクした結果が一致”を選択すると、指定したプレフィックスと、RIP 経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その RIP 経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になった RIP 経路情報のメトリック値を変更できます。送信時の RIP 経路にメトリック値を設定した場合、「RIP 情報」で設定した加算メトリック値は加算されません。省略または 0 を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

◇ IPv6 帯域制御 (WFQ) 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→ [修正] → [IPv6 関連] → [IPv6 帯域制御 (WFQ) 情報]

■ IPv6 帯域制御(WFQ)情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

定義番号	プロトコル	送信元IPv6アドレス/プレフィックス長 送信元ポート番号 あて先IPv6アドレス/プレフィックス長 あて先ポート番号	対象Traffic Class 値 帯域	操作
<input type="button" value="全削除"/>				
<IPv6帯域制御(WFQ)情報入力フィールド>				
プロトコル		すべて <input type="button" value="▼"/> (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)		
送信元情報	IPv6アドレス/プレフィックス長	<input type="text"/> / <input type="text"/>		
	ポート番号	<input type="text"/>		
あて先情報	IPv6アドレス/プレフィックス長	<input type="text"/> / <input type="text"/>		
	ポート番号	<input type="text"/>		
対象Traffic Class 値		<input type="text"/>		
帯域		<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="button" value="▼"/> <input type="radio"/> 帯域を他と共有 <input type="button" value="共有できる定義が存在しません"/>		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

プロトコル

帯域制御の対象となるプロトコルを以下の5つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

帯域制御の対象となるIPv6アドレスおよびプレフィックス長を指定します。対象となるパケットのIPv6アドレスと定義するプレフィックス長の論理積と、定義するIPv6アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“,”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 Traffic Class 値

帯域制御の対象となるIPv6パケットのTraffic Class値を16進数を使用して、0～ffの範囲または“any”で指定します。Traffic Class値を複数指定する場合は、“,”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTraffic Class値を帯域制御の対象とします。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

IPv4/IPv6以外のパケットは、すべて非優先（ベストエフォート）として扱われます。

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

13.4 ブリッジ関連

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[ブリッジ関連]

LAN0情報(物理LAN)				
共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
ブリッジ情報		MACフィルタリング情報	静的MAC学習テーブル情報	

◇ブリッジ情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[ブリッジ関連]→[ブリッジ情報]

■ブリッジ情報 ?

ブリッジ機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する		
グループ識別子	<input type="text" value="0"/>		
STP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する		
	パスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する <input type="text"/>	
	インタフェース優先度	<input type="text" value="128"/>	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ブリッジ機能

接続相手とブリッジで通信する場合は、“使用する”を選択します。

インタフェース優先度

STPで使用するインタフェースごとの優先度を0～255の範囲で指定します。値が小さい方が優先となります。

グループ識別子

ブリッジのグループ識別子を10進数で指定します。0～7の範囲で指定します。省略時は0が設定されます。

STP機能

STP機能を利用して経路制御を行う場合は、“使用する”を選択して、以下の項目を設定します。グループ識別子に0を設定した場合だけ、STPを利用することができます。この設定項目はブリッジ機能を使用する場合だけ有効です。

パスコスト

STPで利用するパスコストを選択します。“指定する”を選択する場合は、1～65535の範囲で指定します。パスコストの適性値が不明な場合は、“自動決定”を選択すると、自動的にパスコストが決定されます。

◇ MACフィルタリング情報

[操作] 「設定メニュー」→ルータ設定「LAN情報」→[修正]→[ブリッジ関連]→[MACフィルタリング情報]

■MACフィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	送信元MACアドレス	フォーマット種別	操作
		あて先MACアドレス	LSAP/type値	
<input type="button" value="全削除"/>				
<MACフィルタリング情報入力フィールド>				
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断			
送信元MACアドレス	すべて <input type="button" value="▼"/> アドレス指定(“指定する”を選択時のみ有効です) <input style="width: 100%;" type="text"/>			
あて先MACアドレス	すべて <input type="button" value="▼"/> アドレス指定(“指定する”を選択時のみ有効です) <input style="width: 100%;" type="text"/>			
フォーマット種別	すべて <input type="button" value="▼"/> (“LLC形式”の場合はLSAP、“Ethernet形式”の場合はtype値を入力してください) <input style="width: 100%;" type="text"/>			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在のインタフェースのMACフィルタリング情報の定義が表示されています。MACフィルタリングの定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

LANモジュールで送受信する際にフィルタリング処理を行います。優先順位の高い定義から順にフレームのチェックを行い、フィルタリング条件が一致した場合に定義された動作を行います。

動作

フィルタリング条件に一致したときのMACフィルタリングの動作を以下の2つから選択します。

- 透過
フィルタリング条件と一致する場合にフレームを透過します。
- 遮断
フィルタリング条件と一致する場合にフレームを遮断します。

送信元／あて先 MAC アドレス

MACアドレスを以下の項目から選択します。“指定する”を選択する場合は、アドレス指定にMACアドレスを16進数で指定します。

- すべて
すべてのMACアドレスを対象とします。
- ブロードキャスト
ブロードキャストMACアドレスを対象とします。
- マルチキャスト
ブロードキャストMACアドレスおよびマルチキャストMACアドレスを対象とします。
- 指定する
アドレス指定に指定するMACアドレスを対象とします。MACアドレスは、「xx:xx:xx:xx:xx:xx」(xxは2桁の16進数)の形式で指定します。

フォーマット種別

フィルタリング対象のフォーマットを以下の項目から選択します。“LLC形式”の場合は、LSAPを16進数を使用して、0～ffffの範囲で指定し、“Ethernet形式”の場合は、type値を16進数を使用して、5dd～ffffの範囲で指定します。

- LLC形式
LLC形式のフレームを対象とします。
- Ethernet形式
Ethernet形式のフレームを対象とします。
- すべて
すべてのフレームを対象とします。

◇ 静的MAC学習テーブル情報

[操作] 「設定メニュー」→ルータ設定「LAN情報」→[修正]→[ブリッジ関連]
→[静的MAC学習テーブル情報]

静的MAC学習テーブル情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

MACアドレス	操作
全削除	
<静的MAC学習テーブル情報入力フィールド>	
MACアドレス	追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在、設定されている静的MAC学習テーブルの一覧です。静的MAC学習テーブル情報の定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

MACアドレス

MACアドレスは、「xx:xx:xx:xx:xx:xx」(xxは2桁の16進数)の形式で指定します。

13.5 MPLS 関連

[操作] 「設定メニュー」→ルータ設定「LAN0 情報 (物理 LAN)」→ [修正] → [MPLS 関連]

LAN0 情報 (物理 LAN)				
共通情報	IP 関連	IPv6 関連	ブリッジ 関連	MPLS 関連
MPLS 基本情報		LDP 情報	EoMPLS 情報	

◇ MPLS 基本情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→ [修正] → [MPLS 関連] → [MPLS 基本情報]

MPLS 基本情報	
MPLS 機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
ラベル配布プロトコル	LDP

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

MPLS 機能

LAN 上で MPLS 機能を使用する場合は、“使用する”を選択します。

ラベル配布プロトコル

LAN 上で行うラベル配布プロトコルを選択します。

◇ LDP 情報

[操作] 「設定メニュー」 → ルータ設定 「LAN 情報」 → [修正] → [MPLS 関連] → [LDP 情報]

Hello タイマ	
interval	5 秒
Hold Time	<input type="radio"/> infinity <input checked="" type="radio"/> 指定する 15 秒
KeepAlive タイマ	
interval	1 分
timeout	3 分
LDP ラベル 広報方式	<input checked="" type="radio"/> DU <input type="radio"/> DoD
LDP ラベル 保持方式	<input type="radio"/> liberal <input checked="" type="radio"/> conservative
PHP 機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IPv4 Transport アドレス	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

Hello タイマ

interval

Hello の送信間隔のタイマを 1～65535 秒の範囲で指定します。初期値は 5 秒です。省略はできません。

有効範囲)
 1～18 時間
 1～1092 分
 1～65535 秒

HoldTime

近隣関係の維持を判定するため HoldTime のタイマを 1～65534 秒の範囲で指定します。
 近隣関係の維持を判定する場合は、HoldTime に infinity を選択します。初期値は 15 秒です。省略はできません。

有効範囲)
 1～18 時間
 1～1092 分
 1～65534 秒

こんな事に気をつけて

HoldTime の値は、interval の値より小さくすることはできません。HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

KeepAlive タイマ

interval

KeepAlive の送信間隔のタイマを 1～65535 秒の範囲で指定します。初期値は 1 分です。省略はできません。

有効範囲)
 1～18 時間
 1～1092 分
 1～65535 秒

timeout

LDP セッションの維持を判定するため KeepAlive の timeout のタイマを 1～65535 秒の範囲で指定します。初期値は 3 分です。省略はできません。

有効範囲)
 1～18 時間
 1～1092 分
 1～65535 秒

こんな事に気をつけて

timeout の値は、interval の値より小さくすることはできません。timeout の値は interval の値の 3 倍以上を設定することを推奨します。

LDP ラベル広報方式

Downstream Unsolicitedを使用する場合は、“DU”を選択します。Downstream On Demandを使用する場合は、“DoD”を選択します。

LDP ラベル保持方式

liberalを使用する場合は“liberal”を選択します。
conservativeを使用する場合は“conservative”を選択します。

PHP 機能

インタフェースあてのLSPのPHP機能を設定します。
PHP機能を無効にする場合は、“使用しない”を選択します。PHP機能を有効にする場合は、“使用する”を選択します。MPLS トンネル接続を使用する場合に、自側エンドポイントとIPアドレスが同じとき、設定に関係なく“使用しない”が設定されます。

IPv4 Transport アドレス

インタフェース単位でLDPが相手装置との通信に用いる送信元IPv4アドレスを分ける必要がある場合、本装置に設定されたIPv4アドレスを指定します。0.0.0.0を指定した場合は、MPLS情報の設定のIPv4 Transport Addressの設定に従います。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

こんな事に気をつけて

必ず本装置に存在するアドレスを指定してください。
本装置に存在しないアドレスをインタフェースに指定した場合は、そのインタフェースではLDPを使用できません。

◇ EoMPLS 情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [MPLS 関連] → [EoMPLS 情報]

■ EoMPLS 情報	
EoMPLS 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
VC ID	<input type="text"/>
相手装置の IPv4 アドレス	<input type="text"/>
VC タイプ	auto
EXP 値書き換え	<input checked="" type="radio"/> 固定値 <input type="text" value="0"/> <input type="radio"/> VLAN タグのプライオリティを使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

EoMPLS 機能

EoMPLS 機能を使用する場合は“使用する”を選択します。

VC ID

LAN 定義の VC ID を 10 進数を使用して 1 ～ 4294967295 で指定します。EoMPLS 通信の相手装置と同じ値を指定します。

相手装置の IPv4 アドレス

EoMPLS 通信の相手装置の IPv4 アドレスを指定します。相手装置で指定した IPv4 Transport Address と同じ値を指定します。0.0.0.0 および 255.255.255.255 は使用できません。

有効範囲)

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

VC タイプ

相手装置で同じ VC ID を持つインタフェースと同じ値を指定します。

- auto
LAN 定義から、Ethernet または VLAN かを自動的に識別します。
- ethernet
LAN 定義に関係なく VC Type を Ethernet に設定します。
- vlan
LAN 定義に関係なく VC Type を Ethernet VLAN に設定します。

EXP 値書き換え

固定の EXP 値を使用する場合、“固定値”を選択し、書き換える EXP 値を 10 進数を使用して 0 ～ 7 で指定します。“固定値”を選択して、EXP 値を省略時は、0 が設定されます。VLAN タグのプライオリティを使用する場合は、“VLAN タグのプライオリティを使用する”を選択します。初期値は、EXP 値 0 です。


14 シリアル情報

[操作] 「設定メニュー」 → [詳細設定メニュー] → ルータ設定「シリアル情報」

シリアル情報
共通情報
モデム情報

14.1 共通情報

[操作] 「設定メニュー」 → [詳細設定メニュー] → ルータ設定「シリアル情報」 → [共通情報]

■共通情報 	
COMポート	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
COMポート通信速度	115200 ▾
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

COMポート

本装置のCOMポートにモデムを接続して、モデム接続を利用する場合は、“使用する”を選択します。

COMポート通信速度

COMポートの通信速度を選択します。

14.2 モデム情報

[操作] 「設定メニュー」 → [詳細設定メニュー] → ルータ設定「シリアル情報」 → [モデム情報]

■モデム情報		?
ダイヤル方式	<input checked="" type="radio"/> トーン式 <input type="radio"/> パルス式	
ダイヤルトーンの検出	<input checked="" type="radio"/> する <input type="radio"/> しない	
スピーカ	モード	キャリア検出までONにする
	音量	<input type="radio"/> 小 <input checked="" type="radio"/> 中 <input type="radio"/> 大

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 | キャンセル

ダイヤル方式

使用するアナログ回線のダイヤル方式を選択します。

ダイヤルトーンの検出

ダイヤルする前にダイヤルトーンを検出する場合は、“する”を選択します。

スピーカ

モード

モデムのスピーカの鳴り方を選択します。

音量

モデムのスピーカの音量を選択します。

15 相手情報

[操作] 「設定メニュー」→ルータ設定「相手情報」

相手情報	
ネットワーク情報	着信相手識別情報

15.1 ネットワーク情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]

表示条件入力

接続先種別	表示回数	表示範囲
全表示	10	

※ネットワーク情報の表示条件を設定してください。

■ネットワーク情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。

ネットワーク名 (相手定義番号)	プロトコル	接続先	操作
全削除			
<ネットワーク情報追加フィールド>			
ネットワーク名	rmt0	<input type="checkbox"/> 疑似ルータ	
		追加	キャンセル

保存した情報は、設定反映後に有効になります。

現在、設定されている接続相手のネットワーク情報の定義が表示されています。ネットワークの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

表示条件入力

ネットワーク情報の表示条件を接続先種別、表示回数、および表示範囲によって指定することができます。設定することによって、ネットワーク情報の一覧に見たい情報だけを表示させることができます。

ネットワーク名

このネットワークを識別するための名称を8文字以内で指定します。追加するネットワークを疑似ルータとして使用する場合は、“疑似ルータ”をチェックします。

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]

相手情報 - ネットワーク情報(rmt0)	
共通情報	接続先情報 PPP関連 IP関連 IPv6関連 ブリッジ関連 MPLS関連
このページではネットワーク情報を設定することができます。 上記の各項目をクリックしてください。詳細な設定項目が表示されます。	

「疑似ルータ」をチェックした場合、「PPP関連」、「IPv6 関連」、「ブリッジ関連」および「MPLS 関連」の項目はありません。

15.2 共通情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[共通情報]

相手情報 - ネットワーク情報(rmt0)	
共通情報	接続先情報 PPP関連 IP関連 IPv6関連 ブリッジ関連 MPLS関連
基本情報	

◇基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[共通情報]→[基本情報]

■基本情報	
ネットワーク名	<input type="text" value="rmt0"/>
MTUサイズ	<input type="text" value="1500"/> バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input checked="" type="radio"/> 使用しない
	<input type="radio"/> 使用する
	最大送信レート <input type="text"/> Mbps
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

ルーティングの対象となるネットワークの情報を設定します。

ネットワーク名

このネットワークを識別するための名称を8文字以内で指定します。

MTU サイズ

最大パケット送信サイズ (Maximum Transmission Unit) を 200～1500 バイトの範囲で指定します。IPv6 通信で利用する場合は、1280 バイト以上の値を指定します。

また、IPv6 トンネル (IPv6 over IPv4) を利用する場合は、1280 バイトを指定します。

PPPoE (PPP over Ethernet) を利用する場合は、1454 バイトを指定します。

ブリッジを利用する場合は、1500 バイトを指定します。1500 未満を指定すると、正しくブリッジ通信ができない場合があります。

RIP を利用する場合は、576 バイト以上を指定します。576 バイト未満の MTU を指定すると、RIP パケットが送信されない場合があります。

自動接続

データ通信発生時に自動的に接続する場合は、“使用する”を選択します。

こんな事に気をつけて

使用するインタフェースの設定 (WAN 接続) で自動接続をすべて禁止している場合は、自動接続を行うことができません。

シェーピング

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

シェーピング (リミッタ) 機能を設定します。シェーピング機能を使用する場合は“使用する”を選択し、最大送信レートを指定します。最大送信レートで設定したレートに送信を抑制します。

最大送信レート

最大送信レートを 1～100000Kbps の範囲で指定します。Kbps は 1000bps を、Mbps は 1000Kbps を意味します。

こんな事に気をつけて

- シェーピング機能は、以下の接続先種別では動作しません。
 - ISDN
 - フレームリレー
 - モデム
 - IP トンネル
- 回線に LAN を使用して、帯域制御機能を有効に動作させる場合は、シェーピングを“使用する”に設定してください。

15.3 接続先情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]

相手情報 - ネットワーク情報(rmt0)						
共通情報	接続先情報	PPP関連	IP関連	IPv6関連	ブリッジ関連	MPLS関連
接続先情報						

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[接続先情報]

《接続先は、各ネットワークの合計で 100箇所まで設定でき、複数のプロバイダを利用条件により切り替えることができます。》

■接続先情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	接続先名 (接続先定義番号)	種別	操作
全削除			
<接続先情報追加フィールド>			
接続先名	ap0-0		
接続先種別	<input type="radio"/> 専用線接続		
	<input type="radio"/> ISDN接続		
	ダイヤル1	電話番号	
		サブアドレス	
	<input type="radio"/> フレームリレー接続		
	DLCI		
	<input type="radio"/> モデム接続		
	ダイヤル1	電話番号	
	<input type="radio"/> PPPoE接続		
	<input type="radio"/> IPトンネル接続		
<input type="radio"/> IPsec/IKE接続			
<input type="radio"/> 別インタフェースから送出			
<input type="radio"/> MPLSトンネル接続			
<input checked="" type="radio"/> パケット破棄			

追加 キャンセル

保存した情報は、設定反映後に有効になります。

「疑似ルータ」をチェックした場合、接続先種別は「別インタフェースから送出」の項目のみです。

現在、設定されている接続先情報の定義が表示されています。マルチルーティングを行う場合は、優先順位の1から順に評価され最初に条件が成立した接続先にデータが流れます。接続先の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

選択する接続種別によって、表示が異なります。

接続先名

この接続先を識別するための名称を8文字以内で指定します。

接続先種別

この接続先の種別を以下から選択します。

- 専用線接続
専用線回線を使用して接続する場合に選択します。使用するにはWAN 情報で専用線回線が設定されている必要があります。
- ISDN 接続
ISDN回線を使用して接続する場合に選択します。使用するにはWAN 情報でISDN回線が設定されている必要があります。

ダイヤル 1

接続に使用する電話番号を指定します。本装置では、複数の電話番号を指定できますが、それは「接続先情報」－「基本情報」で設定します。着信時には自動認識します。電話番号は32桁以内、サブアドレスは19桁以内で指定します。

- フレームリレー接続
フレームリレー回線を使用して接続する場合に選択します。使用するにはWAN 情報でフレームリレー回線が設定されている必要があります。

DLCI

DLCIを10進数を使用して16～991の範囲で指定します。DLCIを設定できるネットワークは、BR500S 仕様一覧「[2.1 ソフトウェア仕様](#)」(P.14)を参照してください。DLCIは、フレームリレーを使用するときに1本の物理回線上に設定される複数の論理的な通信路（データリンク）を識別するための識別子です。

- モデム接続
モデムを使用して接続する場合に選択します。

ダイヤル 1

接続に使用する電話番号を指定します。本装置では、複数の電話番号を指定できますが、それは「接続先情報」－「基本情報」で設定します。着信時には自動認識します。電話番号は32桁以内で指定します。

- PPPoE 接続
PPPoEを使用して接続する場合に選択します。使用するにはLAN 情報が設定されている必要があります。
- IP トンネル接続
IP トンネルを使用して接続する場合に選択します。IP トンネルに使用するIPv6またはIPv4の設定は別のLAN 情報または相手情報で設定します。本装置では、IP トンネル接続として、以下の2つがあります。
 - IPv6 over IPv4
 - Ethernet over IP

- IPsec/IKE 接続
IPsec/IKE トンネルを使用して接続する場合に選択します。IPsec/IKE トンネルに使用するIPv6またはIPv4の設定は別の相手情報で設定します。
- 別インタフェースから送出
パケット送出先として別インタフェースを使用して接続する場合に選択します。
- MPLS トンネル接続
MPLSトンネルを使用して接続する場合に選択します。
- パケット破棄
送信するパケットをすべて破棄する場合に選択します。


◇専用線接続

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: 専用線接続)]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
専用線接続		
基本情報	接続制御情報	PPP情報
マルチルーティング情報		

[基本情報]

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: 専用線接続)] → [基本情報]

基本情報		
接続先名	<input type="text" value="ap0-0"/>	
使用インタフェース	<input type="text" value="WAN1"/>	
DNSサーバ	<input type="text"/>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/>	<input type="button" value="キャンセル"/>	

接続先名

この接続先を識別するための名称を8文字以内で指定します。

使用インタフェース

専用線接続で使用する WAN インタフェースを選択します。あらかじめ WAN 情報で専用線インタフェースの設定をしておく必要があります。

DNS サーバ

接続の際に使用する DNS サーバの IP アドレスを指定します。ProxyDNS 機能を使用する場合に必要です。省略するか 0.0.0.0 を指定した場合は、自動取得となります。255.255.255.255 を指定した場合は、DNS サーバは使用しません。また、この IP アドレスは、PPP のネゴシエーションの中で相手から要求があった場合、相手に受け渡す DNS サーバアドレスとしても使用します。

【接続制御情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: 専用線接続)] → [接続制御情報]

■接続制御情報 ?

接続先監視	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
	送信元IPアドレス	<input type="text"/>
	あて先IPアドレス	<input type="text"/>
	正常時送信間隔	<input type="text"/> 秒
	再送間隔	1 <input type="text"/> 秒
	タイムアウト時間	<input type="text"/> 秒
	異常時送信間隔	<input type="text"/> 秒
	送信 TTL/HopLimit	255
	監視方式	<input checked="" type="radio"/> 常時監視 <input type="radio"/> 無通信時監視

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

接続先監視

接続先の生存確認を行うための動作情報を選択します。指定したあて先IPアドレスにICMP ECHOパケットを送信します。タイムアウト時間までに応答がない場合に、この接続先を使用できない状態にします。その後、異常時送信間隔ごとにICMP ECHOパケットを送信し、接続先の復旧を待ち、復旧後にこの接続先を使用できる状態にします。

送信元IPアドレス

ICMP ECHOパケットの送信元IPアドレスとして、本装置に設定している自側IPv4/IPv6アドレスのどれかを指定します。指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

あて先IPアドレス

監視対象となる接続先のIPv4/IPv6アドレスを指定します。指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

正常時送信間隔

ICMP ECHOパケットの応答が正常に受信されている状態で、ICMP ECHOパケットを次に送信する間隔を、10進数を使用して1～60秒の範囲で指定します。

再送間隔

ICMP ECHOパケットの正常時の送信に対して応答がない場合、ICMP ECHOパケットを再送する間隔を、10進数を使用して1～(タイムアウト時間-1)秒の範囲で指定します。省略時は、1秒が設定されます。

タイムアウト時間

ICMP ECHOパケットの送信から生存確認失敗とするまでの時間を、10進数を使用して5～180秒の範囲で指定します。タイムアウト時間までに応答がない場合、監視対象との接続に障害が発生したとみなし、この接続先を使用できない状態にします。

異常時送信間隔

ICMP ECHOパケットのタイムアウトが発生してから、接続先の障害が復旧し応答が受信されるまでの間、ICMP ECHOパケットを送信する間隔を、10進数を使用して60～600秒の範囲で指定します。

送信TTL/HopLimit

ICMP ECHOパケットを送信するときのIP TTL値を、1～255の範囲で指定します。省略時は、255が設定されます。

監視方式

監視方式を以下の2つから選択します。

- 常時監視
常時、監視を行います。
- 無通信時監視
無通信時に、監視を行います。

【PPP 情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: 専用線接続)] → [PPP 情報]

■ PPP情報 ⓘ

MP接続 しない する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

MP 接続

MP 接続を行う場合は、“する” を選択します。

【マルチルーティング情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: 専用線接続)] → [マルチルーティング情報]

■マルチルーティング情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号	TOS	操作
全削除					
<マルチルーティング情報入力フィールド>					
動作	この接続先を <input type="button" value="使用する"/> <input type="button" value="使用しない"/> <input type="button" value="予約する"/>				
プロトコル	すべて <input type="button" value="指定"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)				
送信元情報	IPアドレス	<input type="text"/>			
	アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>			
	ポート番号	<input type="text"/>			
あて先情報	IPアドレス	<input type="text"/>			
	アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>			
	ポート番号	<input type="text"/>			
TOS	<input type="text"/>				
追加 <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、この接続先に設定されているマルチルーティング情報の定義が表示されています。処理は優先順位1から順に行われます。マルチルーティングの定義は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。

動作

マルチルーティングの動作を以下の3つから選択します。

- 使用する
条件と一致した場合に、この接続先を使用します。
- 使用しない
条件と一致した場合に、この接続先を使用しません。
- 予約する
条件と一致し、以降の接続先を使用することができない場合に、この接続先を使用します。

プロトコル

マルチルーティング条件としてプロトコルを以下の6つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

マルチルーティング条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

マルチルーティング条件としてのIPアドレスおよびアドレスマスクを指定します。チェック対象となったパケットのIPアドレスと定義したアドレスマスクの論理積と、定義したIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

マルチルーティング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定した場合は、すべてのポート番号がマルチルーティングの対象となります。また、ポート番号を複数指定する場合は“,”で区切ります。範囲指定の場合は“-”で区切ります。送信元情報とあて先情報で合わせて10組まで指定できます。

TOS

マルチルーティング条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は“,”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も設定しない場合はすべてのTOSフィールド値をマルチルーティングの対象とします。

◇ ISDN 接続

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: ISDN 接続)]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
ISDN接続		
基本情報	接続制御情報	着信制御情報
PPP情報	マルチルーティング情報	

「マルチルーティング情報」は、「専用線接続」を参照してください。

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: ISDN 接続)] → [基本情報]

■ 基本情報		
接続先名	ap0-0	
使用インタフェース	WAN0	
ダイヤル1	電話番号	03-7777-7777
	サブアドレス	
	相手種別	ISDN
ダイヤル2	電話番号	
	サブアドレス	
	相手種別	ISDN
ダイヤル3	電話番号	
	サブアドレス	
	相手種別	ISDN
DNSサーバ		

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

接続先名

この接続先を識別するための名称を8文字以内で指定します。この名前は手動接続の際にも使用されます。

使用インタフェース

ISDN 接続で使用する WAN インタフェースを選択します。あらかじめ WAN 情報で ISDN 回線インタフェースの設定をしておく必要があります。

ダイヤル1 / 2 / 3

接続に使用する電話番号は3つまで指定できます。ダイヤル1の電話番号にかからないときにはダイヤル2に、ダイヤル2の電話番号にかからないときはダイヤル3にダイヤルします。相手種別は発信時にのみ参照されます。接続先の通信速度および通信手順を選択します。着信時には自動認識します。電話番号は32桁以内、サブアドレスは19桁以内で指定します。なお、64kPIAFS着信時には、設定したサブアドレスは無視されます。

DNS サーバ

接続の際に使用する DNS サーバの IP アドレスを指定します。ProxyDNS 機能を使用する際に必要です。省略するか 0.0.0.0 を指定した場合は、自動取得となります。
255.255.255.255 を指定した場合は、DNS サーバは使用しません。また、この IP アドレスは PPP のネゴシエーションの中で相手から要求があった場合、相手に受け渡す DNS サーバアドレスとしても使用します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

[接続制御情報]

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: ISDN 接続)] → [接続制御情報]

■ 接続制御情報	
常時接続機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
無通信監視タイマ	送受信パケット (について) <input type="text" value="0"/> 秒
接続制限	<input type="checkbox"/> 指定した時間を超えて接続しない <input type="text" value=""/> 時間
	<input type="checkbox"/> 指定した課金を超えて接続しない <input type="text" value=""/> 円
課金単位時間	昼間(月～金) (08:00～19:00) <input type="text" value="0"/> 秒
	夜間(土日の昼間) (19:00～23:00) <input type="text" value="0"/> 秒
	深夜・早朝 (23:00～08:00) <input type="text" value="0"/> 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

常時接続機能

“使用する”を選択すると、ほかの設定や通信の有無にかかわらず接続状態を保持します。相手から切断された場合や回線エラーによって切断された場合は、自動で再接続します。ただし、本装置で手動切断を行うと、次に手動接続を行うまで自動接続動作は行いません。

また、“使用する”を選択すると、表示される画面が変わります。設定項目については、[専用線接続] の「接続制御情報」を参考に設定します。使用しない場合は、以下の項目を設定します。

無通信監視タイマ

無通信監視タイマを 0～3600 秒の範囲で指定します。ここで指定した時間の間に、監視対象となるパケットが存在しなかった場合は、自動的に切断します。なお、省略、または 0 を指定した場合、自動切断を行いません。

接続制限

この接続先に対する発信抑制を接続時間と課金によって行うことができます。発信抑制を行う場合は、それぞれチェックボックスを指定して、時間は 1～999 時間、金額は 1～999999 円の範囲で指定します。チェックボックスを指定した場合、時間および金額の省略はできません。

課金単位時間

各時間帯の課金単位時間を 0.0 ～ 3600.0 秒の範囲で指定します。ここで設定した時間は無通信監視による回線切断のときに参照され、同じ料金でもっとも接続時間が長くなるように回線切断タイミングを調整します。なお、昼間時間帯に 0 を設定した場合、課金単位の調整は行いません。また、夜間時間帯や深夜・早朝時間帯に 0 を設定した場合、その前の時間帯の設定を利用します。

こんな事に気をつけて

この機能を使用する場合は、操作メニューの時刻設定を使用して本装置の時刻を正しく設定してください。時刻が正しく設定されていない場合、課金単位時間は昼間の値だけが使用されます。祝祭日には対応していません。

【着信制御情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: ISDN 接続)] → [着信制御情報]

■ 着信制御情報	
着信許可	<input type="radio"/> 許可しない <input checked="" type="radio"/> 許可する
発信者番号による識別	<input type="radio"/> 番号チェックしない <input checked="" type="radio"/> 接続先電話番号でチェックする <input type="radio"/> 指定する接続先電話番号でチェックする
	相手電話番号 <input type="text"/>
	相手サブアドレス <input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

着信許可

この接続先からの着信を許可する場合は、“許可する”を選択します。

発信者番号による識別

着信時の相手識別の方法には、発信者番号通知を用いる方法と、認証 ID を用いる方法があります。

- 番号チェックをしない
発信者番号による相手識別は行ません。
- 接続先電話番号でチェックする
発信者番号通知を用いて相手を識別します。この場合「基本情報」で設定した電話番号で相手を識別します。
- 指定する接続先電話番号でチェックをする
相手識別のために相手電話番号および相手サブアドレスを指定します。電話番号は 32 桁以内、サブアドレスは 19 桁以内で指定します。

【PPP 情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: ISDN 接続)] → [PPP 情報]

■ PPP 情報		?
認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP	
送信認証情報	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>
受諾認証情報	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>
MP 接続	<input checked="" type="radio"/> しない <input type="radio"/> する	
	BAP/BACP 利用 <input checked="" type="radio"/> しない <input type="radio"/> する <small>※ 発信者番号による識別で番号をチェックしない場合は着信相手識別情報の設定が有効</small>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

認証方式

着信時に利用する認証プロトコルを選択します。どちらも指定しない場合は、その相手からの着信は認証しません。

送信確認情報

発信時に使用する認証 ID を 64 桁以内、認証パスワードを 64 桁以内で指定します。

受諾認証情報

着信時に受け付ける認証 ID を 64 桁以内、認証パスワードを 64 桁以内で指定します。発信者番号による識別は「着信制御情報」で設定できます。

MP 接続

MP 接続を行う場合は、“する” を選択します。

BAP/BACP 利用

BAP/BACP を利用する場合は、“する” を選択します。ただし、発信者番号による識別が行われなかった相手からの着信については、「相手情報」 - 「着信相手識別情報」の設定が参照されます。発信者番号による識別は、「着信制御情報」で設定できます。

◇フレームリレー接続

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加(接続先種別: フレームリレー接続)]

相手情報-ネットワーク情報(rmt0)- 接続先情報(ap0-0)		
フレームリレー接続		
基本情報	接続制御情報	マルチルーティング情報

「接続制御情報」および「マルチルーティング情報」は、[専用線接続] を参照してください。

【基本情報】

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加(接続先種別: フレームリレー接続)]→[基本情報]

■基本情報 ?	
接続先名	ap0-0
使用インタフェース	WAN3
DLCI	16
CIR	0

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

接続先名

この接続先を識別するための名称を8文字以内で指定します。

使用インタフェース

フレームリレー接続で使用する WAN インタフェースを選択します。あらかじめ WAN 情報でフレームリレー回線インタフェースの設定をしておく必要があります。

DLCI

DLCI を 16～991 の範囲で指定します。DLCI を設定できるネットワークは、BR500S 仕様一覧「[2.1 ソフトウェア仕様](#)」(P.14) を参照してください。DLCI は、フレームリレーを使用する場合、一本の物理回線上に設定される複数の論理的な通信路(データリンク)を識別するための識別子です。

CIR

CIR を選択します。CIR は網が正常な状態で保証されるスループットです。本装置が輻輳制御動作を行う場合は CIR を基準としてスループットを制御します。

◇モデム接続

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加(接続先種別:モデム接続)]

相手情報-ネットワーク情報(rmt0)- 接続先情報(ap0-0)		
モデム接続		
基本情報	接続制御情報	着信制御情報
PPP情報	マルチルーティング情報	

「マルチルーティング情報」は、[専用線接続]を参照してください。

【基本情報】

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加(接続先種別:モデム接続)]→[基本情報]

■基本情報		
接続先名	ap0-0	
使用インタフェース	serial0	
ダイヤル1	電話番号	03-7777-7777
ダイヤル2	電話番号	
ダイヤル3	電話番号	
DNSサーバ		

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

接続先名

この接続先を識別するための名称を8文字以内で指定します。この名前は手動接続の際にも使用されます。

使用インタフェース

本装置では、モデム接続で使用するインタフェースは固定です。

ダイヤル1／2／3

接続に用いる電話番号は3つまで指定できます。ダイヤル1の電話番号にかからないときにはダイヤル2に、ダイヤル2がかからないときはダイヤル3の電話番号にダイヤルします。

DNSサーバ

接続の際に使用するDNSサーバのIPアドレスを指定します。ProxyDNS機能を使用する際に必要です。省略するか0.0.0.0を指定した場合は、自動取得となります。255.255.255.255を指定した場合、DNSサーバは使用しません。また、このアドレスはPPPのネゴシエーションの中で相手から要求があった場合、相手に受け渡すDNSサーバアドレスとしても使用します。

【接続制御情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: モデム接続)] → [接続制御情報]

■接続制御情報	
無通信監視タイ マ	送受信/パケット <input type="text" value="0"/> 秒
接続制限	<input type="checkbox"/> 指定した時間を超えて接続しない <input type="text" value=""/> 時間
課金単位時間	昼間(月～金) (08:00～19:00) <input type="text" value="0"/> 秒
	夜間(土日の昼間) (19:00～23:00) <input type="text" value="0"/> 秒
	深夜・早朝 (23:00～08:00) <input type="text" value="0"/> 秒
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

無通信監視タイマ

無通信監視タイマを0～3600秒の範囲で指定します。ここで指定した時間の間に、監視対象となるパケットが存在しなかった場合は、自動的に切断します。なお、省略、または0を指定した場合、自動切断を行いません。

接続制限

この接続先に対する発信抑制を接続時間によって行うことができます。発信抑制を行う場合は、それぞれチェックボックスを指定して、時間は1～999時間の範囲で指定します。チェックボックスを指定した場合、時間の省略はできません。

課金単位時間

各時間帯の課金単位時間を0.0～3600.0秒の範囲で指定します。ここで設定した時間は無通信監視による回線切断のときに参照され、同じ料金でもっとも接続時間が長くなるように回線切断タイミングを調整します。なお、昼間時間帯に0を設定した場合、課金単位の調整は行いません。また、夜間時間帯や深夜・早朝時間帯に0を設定した場合、その前の時間帯の設定を利用します。

こんな事に気をつけて

この機能を使用する場合は、操作メニューの時刻設定を使用して本装置の時刻を正しく設定してください。時刻が正しく設定されていない場合、課金単位時間は昼間の値だけが使用されます。祝祭日には対応していません。

【着信制御情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: モデム接続)] → [着信制御情報]

■ 着信制御情報	
着信許可	<input type="radio"/> 許可しない <input checked="" type="radio"/> 許可する
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

着信許可

この接続先からの着信を許可する場合は、“許可する”を選択します。モデム接続では、発信者番号による識別はできません。

【PPP 情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: モデム接続)] → [PPP 情報]

■ PPP 情報		
送信認証情報	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>
受諾認証情報	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

送信確認情報

発信時に使用する認証 ID を 64 桁以内、認証パスワードを 64 桁以内で指定します。

受諾認証情報

着信時に受け付ける認証 ID を 64 桁以内、認証パスワードを 64 桁以内で指定します。モデム接続では、発信者番号による識別はできません。

◇ PPPoE 接続


[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: PPPoE 接続)]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
PPPoE接続		
基本情報	接続制御情報	PPP情報
PPPoE情報	マルチルーティング情報	

「マルチルーティング情報」は、「専用線接続」を参照してください。

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: PPPoE 接続)] → [基本情報]

■基本情報		
接続先名	<input type="text" value="ap0-0"/>	
使用インタフェース	<input type="text" value="LAN1"/>	
DNSサーバ	<input type="text"/>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/>	<input type="button" value="キャンセル"/>	

接続先名

この接続先を識別するための名称を8文字以内で指定します。この名前も手動接続の場合にも使用されます。

使用インタフェース

通信を行うインタフェースを選択します。

DNS サーバ

接続の際に使用する DNS サーバの IP アドレスを指定します。ProxyDNS 機能を使用する際に必要です。省略するか 0.0.0.0 を指定した場合は、自動取得となります。255.255.255.255 を指定した場合、DNS サーバは使用しません。また、この IP アドレスは PPP のネゴシエーションの中で相手から要求があった場合、相手に受け渡す DNS サーバアドレスとしても使用します。

【接続制御情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: PPPoE 接続)] → [接続制御情報]

■接続制御情報	
常時接続機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
無通信監視タイマ	送受信パケット (について) <input type="text" value="0"/> 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

常時接続機能

“使用する”を選択すると、ほかの設定や通信の有無にかかわらず接続状態を保持します。相手から切断された場合や回線エラーによって切断された場合は、自動で再接続します。ただし、本装置で手動切断を行うと、次に手動接続を行うまで自動接続動作は行いません。

また、“使用する”を選択すると、表示される画面が変わります。設定項目については、[専用線接続] の「接続制御情報」を参考に設定します。使用しない場合は、以下の項目を設定します。

無通信監視タイマ

無通信監視タイマを0～3600秒の範囲で指定します。ここで指定した時間の間に、監視対象となるパケットが存在しなかった場合は、自動的に切断します。なお、省略、または0を指定した場合、自動切断を行いません。

【PPP 情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: PPPoE 接続)] → [PPP 情報]

■ PPP情報		?
送信認証情報	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

送信認証情報

認証 ID

送信時に使用する認証 ID を 64 文字以内の文字列で指定します。

認証パスワード

送信時に使用する認証パスワードを 64 文字以内の文字列で指定します。

【PPPoE 情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: PPPoE 接続)] → [PPPoE 情報]

■ PPPoE情報		?
アクセスコンセントレータ名(AC-Name)	<input type="text"/>	
サービス名(Service-Name)	<input type="text"/>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

アクセスコンセントレータ名(AC-Name)

アクセスコンセントレータ名を 64 文字以内の文字列で指定します。

サービス名 (Service-Name)

サービス名を 64 文字以内の文字列で指定します。

◇ IP トンネル接続


[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報]
→ [追加 (接続先種別: IP トンネル接続)]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)	
IPトンネル接続	
基本情報	接続制御情報

「接続制御情報」は、「専用線接続」を参照してください。

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報]
→ [追加 (接続先種別: IP トンネル接続)] → [基本情報]

■基本情報 	
接続先名	<input type="text" value="ap0-0"/>
自側エンドポイント	<input type="text"/>
相手側エンドポイント	<input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/>	<input type="button" value="キャンセル"/>

接続先名

この接続先を識別するための名称を8文字以内で指定します。

自側／相手側エンドポイント

- IPv6 over IPv4 の場合
IPv4 形式のIP アドレスを指定します。
- Ethernet over IP の場合
IPv4 トンネルの場合はIPv4形式、IPv6 トンネルの場合はIPv6形式のアドレスを指定してください。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.25.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

◇ IPsec/IKE 接続

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: IPsec/IKE 接続)]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
IPsec/IKE接続		
基本情報	接続制御情報	IPsec情報
IKE情報	マルチルーティング情報	

「接続制御情報」および「マルチルーティング情報」は、[専用線接続] を参照してください。

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: IPsec/IKE 接続)] → [基本情報]

■ 基本情報 ?

接続先名	ap0-0	
鍵交換モード	<input checked="" type="radio"/> Aggressive Mode(Initiator)使用	
	自側エンドポイント	
	相手側エンドポイント	202.168.1.1
	自装置識別情報	shisya
	IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN
	<input type="radio"/> Aggressive Mode(Responder)使用	
	自側エンドポイント	
	相手側エンドポイント	
	相手装置識別情報	
	IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN
	<input type="radio"/> Main Mode使用	
	相手側エンドポイント	
	自側エンドポイント	
	<input type="radio"/> 手動鍵使用	
	相手側エンドポイント	
自側エンドポイント		
<input type="radio"/> IKE(は他の接続先情報を使用)		
接続先名	使用できる接続先情報が存在しません	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

接続先名

この接続先を識別するための名称を8文字以内で指定します。

鍵交換モード

鍵交換モードを以下の5つから選択します。

- Aggressive Mode(Initiator)使用
自側エンドポイントが可変 IP アドレスで IPsec/IKE を利用して通信する場合に選択します。Aggressive Mode(Initiator) を利用する場合、相手エンドポイント装置に Aggressive Mode(Responder) が設定されている必要があります。
- Aggressive Mode(Responder)使用
相手側エンドポイントが可変 IP アドレスで IPsec/IKE を利用して通信をする場合に選択します。相手側エンドポイントが固定 IP アドレスで Aggressive Mode を使用する場合は、相手側エンドポイントを指定してください。Aggressive Mode(Responder) を利用する場合、相手エンドポイント装置に Aggressive Mode(Initiator) が設定されている必要があります。
- Main Mode 使用
相手側／自側エンドポイントが固定 IP アドレスで IPsec/IKE を利用して通信する場合に選択します。Main Mode を利用する場合、相手エンドポイント装置に Main Mode が設定されている必要があります。
- 手動鍵使用
手動鍵設定での IPsec を利用して通信をする場合に選択します。手動鍵を利用する場合、相手エンドポイント装置に手動鍵の設定がされている必要があります。
- IKE は他の接続先情報を使用
同じエンドポイントアドレス間で IPsec SA を複数使用する場合に選択します。

自側／相手側エンドポイント

IPv4/IPv6 アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:fff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

自側エンドポイントとして IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は、上位を “dhcp@インタフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で入力します。インタフェース名には、IPv6 DHCP クライアント機能が動作している rmt インタフェースを指定します。なお、IPv6 DHCP クライアントが取得したプレフィックスを使用できるのは、「鍵交換モード」で “Aggressive Mode (Initiator) 使用” を設定したときだけです。

自装置／相手装置識別情報

自装置／相手装置を識別する名前を 64 文字以内で指定します。

ID タイプ

ネゴシエーションの交換タイプを選択します。

接続先名

IKE 定義が設定されている接続先情報を選択します。

[IPsec 情報 (自動鍵)]

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: IPsec/IKE 接続)] → [IPsec 情報 (自動鍵)]

⚠ 設定ホストと本装置との通信パケットが対象パケットとなる設定を行うとその設定ホストからの設定変更ができなくなる場合があります。

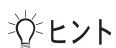
■ IPsec 情報(自動鍵) ?

対象 パケ ット	自側IPアド レス/マスク	IPv4すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アド レス/プレフィックス長形式で入力してください。
	相手側IPアド レス/マスク	IPv4すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アド レス/プレフィックス長形式で入力してください。
SA の 設 定	暗号アルゴ リズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴ リズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグ ループ	使用しない
	SA有効時間	0 時間
	SA有効デー タ量	0 GByte
SA 更 新	Initiator 時 間 デ ー タ 量	90 秒 0 MByte
	Responder時	<input type="radio"/> 更新しない <input checked="" type="radio"/> 更新する
		時間 30 秒 データ量 0 MByte

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

この画面は、「IPsec/IKE 接続」 - 「基本情報」の「鍵交換モード」で、「手動鍵使用」以外を選択した場合に表示されます。



◆ IPsec で使用するプロトコル

IPsec で使用するプロトコルは、IPsec の設定により決定します。プロトコルは AH と ESP があり、1 つの IPsec 情報定義に暗号情報と認証情報の両方を指定すると認証付き ESP となります。

アルゴリズムの組み合わせは、以下のとおりです。

暗号情報	認証情報	プロトコル
暗号化しない	<input type="radio"/>	AH (認証)
<input type="radio"/>	認証なし	ESP (暗号)
<input type="radio"/>	<input type="radio"/>	ESP (認証+暗号)

暗号情報○: des-cbc、3des-cbc、aes-cbc、または null

認証情報○: hmac-md5 または hmac-sha1

※ 「暗号化しない」とは、暗号アルゴリズムを1つも選択しないことを指します。

「認証なし」とは、認証アルゴリズムで“認証なし”を選択または認証アルゴリズムを1つも選択しないことを指します。

対象パケット

自側／相手側 IP アドレス／マスク

IPsec を適用するセッションの送信元 IP アドレスおよびアドレスマスクと、あて先 IP アドレスおよびアドレスマスクを以下の3つから選択します。アドレスを指定する場合は、“指定する”を指定します。

- IPv4 すべて
IPv4 アドレスをすべて選択します。
- IPv6 すべて
IPv6 アドレスをすべて選択します。
- 指定する
IP アドレス／マスクを IPv4/IPv6 形式で指定します。

SA の設定

暗号アルゴリズム

トンネリングするパケットの暗号アルゴリズムを使用する場合に選択します。複数選択した場合、des-cbc、3des-cbc、aes-cbc、nullの順に比較されます。暗号アルゴリズムを選択しない場合は、パケットの暗号化を行いません。

認証アルゴリズム

トンネリングするパケットの認証アルゴリズムを選択します。複数選択した場合、hmac-md5、hmac-sha1、認証なしの順に比較されます。認証アルゴリズムを選択しない場合および“認証なし”だけを選択した場合は、パケットの認証を行いません。

PFS 時の DH グループ

自動鍵交換の鍵を生成するための鍵素材です。値が大きい程セキュリティ強度は高くなります。ただし、装置の負荷が高くなる場合があります。使用しない場合は、“使用しない”を選択します。

SA 有効時間

SAの有効期限を以下の範囲で指定します。指定した時間が経過した時点で、SAの有効期限が切れ、IKEによってSA情報や鍵情報が自動的に更新されます。省略時は、8時間が設定されます。

有効範囲)
600～86400 秒
10～1440 分
1～24 時間

SA 有効データ量

SAの有効期限をデータ量で指定します。指定したデータ量を経過した時点で、SAの有効期限が切れ、IKEによってSA情報や鍵情報が自動的に更新されます。省略時は、0が設定されデータ量によるSA更新が行われません。

有効範囲)
2400～110592000 キロバイト
3～108000 メガバイト
1～105 ギガバイト

SA 更新

SAの更新時間を設定します。

Initiator 時

自側が Initiator の場合に、IPsec SA の有効時間または有効データ量が満了になる前に IPsec で SA の更新を行うための時間とデータ量を指定します。また、IPsec SA 更新のデータ量は、IPsec SA の有効データ量が定義されていない場合は無効となります。省略時は時間が 90 秒、データ量が 0KByte が設定されます。

相手側の Responder 時の SA 更新時間とデータ量と同じにならないように設定してください。

時間

30～180 秒の範囲で指定します。省略時は、90 秒が設定されます。

データ量

120～230400KByte の範囲で指定します。省略時は、0KByte が設定されます。

Responder 時

自側が Responder の場合に、IPsec SA の有効時間または有効データ量が満了になる前に IPsec SA の更新を行う場合は、“更新する”を選択します。“更新する”を選択した場合、更新を行う時間とデータ量を設定します。“更新しない”を選択した場合、Responder 側からの SA の更新は行いません。また、IPsec SA 更新のデータ量は、IPsec SA の有効データ量が定義されていない場合は無効となります。

相手側の Initiator 時の SA 更新時間とデータ量と同じにならないように指定してください。

時間

30～180 秒の範囲で指定します。省略時は、30 秒が設定されます。

データ量

120～230400KByte の範囲で指定します。省略時は、0KByte が設定されます。

【IPsec 情報（手動鍵）】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加（接続先種別：IPsec/IKE 接続）] → [IPsec 情報（手動鍵）]

⚠ 設定ホストと本装置との通信パケットが対象パケットとなる設定を行うとその設定ホストからの設定変更ができなくなる場合があります。

■ IPsec 情報(手動鍵) ?

対象パケット (送信用)	自側IPアドレス	<input type="text"/>	
	自側アドレスマスク	0 (0.0.0)	
	相手側IPアドレス	<input type="text"/>	
	相手側アドレスマスク	0 (0.0.0)	
SAの設定 (送信用)	SPI値	<input type="text"/> (16進数)	
	暗号アルゴリズム	des-cbc	
	暗号鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
		鍵	<input type="text"/>
	認証鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
		鍵	<input type="text"/>
対象パケット (受信用)	相手側IPアドレス	<input type="text"/>	
	相手側アドレスマスク	0 (0.0.0)	
	自側IPアドレス	<input type="text"/>	
	自側アドレスマスク	0 (0.0.0)	
SAの設定 (受信用)	SPI値	<input type="text"/> (16進数)	
	暗号アルゴリズム	des-cbc	
	暗号鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
		鍵	<input type="text"/>
	認証鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
		鍵	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

この画面は、「IPsec/IKE 接続」 - 「基本情報」の「鍵交換モード」で、「手動鍵使用」を選択した場合に表示されます。「対象パケット（送信用）／（受信用）」は、「IPsec 情報（自動鍵）」を参照してください。

SA の設定（送信用）／（受信用）

SPI 値

SPI 値は、暗号情報や認証情報を定義したセキュリティパラメタインデックスです。相手装置の設定と同じ値を指定する必要があります。SPI 値を 100 ~ ffffffff の 16 進数の範囲で指定します。

暗号アルゴリズム

トンネリングするパケットの暗号アルゴリズムを選択します。“暗号化しない”を選択した場合は、パケットの暗号化を行いません。

暗号鍵

- 鍵識別
鍵の識別を指定します。
- 鍵
暗号アルゴリズムで使用する暗号鍵を 16 進数および文字列を使用して、以下の範囲で指定します。

暗号アルゴリズム	入力範囲 (16 進数鍵)	入力範囲 (文字列鍵)
DES-CBC	1～16 桁	8 文字
3DES-CBC	1～48 桁	24 文字
AES-CBC	1～32 桁	16 文字

16 進数で 16 桁 (DES-CBC 指定時 (3DES-CBC 指定時は 48 桁、AES-CBC 指定時は 32 桁)) 未満の鍵を指定した場合は、16 (48) 桁になるまで、自動的に "0" でパディングされます。

文字列で指定する場合は、8 文字 (DES-CBC 指定時 (3DES-CBC 指定時は 24 文字、AES-CBC 指定時は 16 文字)) 固定の鍵長で指定します。暗号情報のアルゴリズムに "暗号化しない" を選択した場合は、省略できます。

認証アルゴリズム

トンネリングするパケットの認証アルゴリズムを選択します。"認証なし" を選択した場合、パケットの認証を行いません。

認証鍵

- 鍵識別
鍵の識別を指定します。
- 鍵
認証アルゴリズムで使用する認証鍵を 16 進数および文字列を使用して、以下の範囲で指定します。

暗号アルゴリズム	入力範囲 (16 進数鍵)	入力範囲 (文字列鍵)
HMAC-MD5	1～32 桁	16 文字
HMAC-SHA1	1～40 桁	20 文字

16 進数で 32 桁 (HMAC-MD5 指定時、HMAC-SHA1 指定時は 40 桁) 未満の鍵を指定した場合は、32 (40) 桁になるまで、自動的に "0" でパディングされます。

文字列で指定する場合は、16 文字 (HMAC-MD5 指定時、HMAC-SHA1 指定時は 20 文字) 固定の鍵長で指定します。認証情報のアルゴリズムに "認証なし" を選択した場合は、省略できます。

[IKE 情報]

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: IPsec/IKE 接続)] → [IKE 情報]

■ IKE 情報		?
IKE 認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	<input type="text"/>
IKE 認証方式		shared
ポート番号		500
SA の設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間
初回再送時間		10 秒
再送回数		3 回
IKEネゴシエーション開始動作		<input checked="" type="radio"/> 対象パケット送信契機 <input type="radio"/> 対象回線接続契機
IKEセッション監視	あて先IPアドレス	<input type="text"/>
	タイムアウト時間	5 秒
	正常時送信間隔	10 秒
	異常時送信間隔	3 分
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

IKE 認証鍵

IKE の認証に用いる鍵を設定します。本装置の IKE 認証には事前共有鍵方式を使用しているため、ここでは事前共有鍵 (Pre-shared key) の設定を行います。事前共有鍵は、IKE を利用した IPsec 通信を行う相手ごとに、また相手装置側でも同じ鍵を設定する必要があります。

鍵識別

鍵の識別を選択します。

鍵

鍵を 16 進数および文字列で以下の範囲で指定します。

入力範囲 (16 進数鍵)	入力範囲 (文字列鍵)
1 ~ 256 桁	1 ~ 128 文字

IKE 認証方法

IKE の鍵交換で、相手を認証するための認証方法を指定します。本装置では事前共有 (秘密) 鍵方式 (shared) を使用します。

ポート番号

IKE プロトコルで使用する UDP のポート番号を 10 進数を使用して 1 ~ 65535 の範囲で指定します。IKE プロトコルでは通常ポート 500 番を使用しますので、通常は、“500” を指定します。省略時は、“500” が設定されます。

SA の設定

暗号アルゴリズム

IKE セッションの送受信パケットを暗号化/複号化するためのアルゴリズムを選択します。

認証 (ハッシュ) アルゴリズム

IKE セッションのネゴシエーションパケットを認証するためのアルゴリズムを選択します。

DH グループ (Diffie-Hellman グループ)

自動鍵交換で鍵を生成するための鍵素材を選択します。値が大きい程セキュリティ強度は高くなります。ただし、鍵生成のための計算に時間がかかるため、装置の負荷が高くなる場合があります。

SA 有効時間

IKE SA の有効期限を以下の範囲で指定します。指定した時間が経過した時点で、SA の有効期限が切れ、IKE SA 情報や鍵情報が IKE によって自動的に更新されます。省略時は、24 時間が設定されます。

有効範囲)

600～86400 秒

10～1440 分

1～24 時間

初回再送時間

IKE の初回再送時間を 10 進数を使用して、1～60 秒の範囲で指定します。省略時は、10 秒が設定されます。

再送回数

IKE の再送回数を 10 進数を使用して、1～10 回の範囲で指定します。省略時は、3 回が設定されます。

IKE ネゴシエーション開始動作

IKE ネゴシエーション開始動作を選択します。対象回線接続契機を選択した場合は、対象パケット送信契機も含まれます。

IKE セッション監視

指定されたあて先 IP アドレスに対して ICMP ECHO パケットを送信します。タイムアウト時間までに応答がない場合に IPsec/IKE SA を解放します。

あて先 IP アドレス

ICMP ECHO パケットの送出先 IP アドレス指定します。あて先 IP アドレスに 0.0.0.0、または省略時 IKE セッション監視をしません。また、正常時送信間隔、異常時送信間隔は初期値になります。

有効範囲)

1.0.0.1-126.255.255.254

128.0.0.1-191.255.255.254

192.0.0.1-223.255.255.254

タイムアウト時間

タイムアウト時間を、10 進数を使用して 5～180 秒の範囲で指定します。タイムアウト時間までに応答がない場合、監視対象ホストがダウンしたものとみなし、IPsec/IKE SA を解放します。省略時は、5 秒が設定されます。

正常時送信間隔

正常に受信されている状態での周期間隔です。ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する間隔を 10 進数を使用して 1～60 秒の範囲で指定します。省略時は、10 秒が設定されます。

異常時送信間隔

ICMP ECHO パケットのタイムアウトが発生してから応答が受信されるまでの周期送信する間隔を、10 進数を使用して 60～600 秒の範囲で指定します。応答が受信された場合は正常時送信間隔状態に戻ります。省略時は、3 分が設定されます。

こんな事に気をつけて

同時に接続先監視が設定されている場合、IKE セッション監視は動作せず、接続先監視だけが動作します。接続先監視は「接続制御情報」で設定できます。

◇ MPLS トンネル接続

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: MPLS トンネル接続)]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
MPLSトンネル接続		
基本情報	接続制御情報	マルチルーティング情報

「接続制御情報」および「マルチルーティング情報」は、[専用線接続] を参照してください。

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: MPLS トンネル接続)] → [基本情報]

■基本情報		[?]
接続先名	<input type="text" value="ap0-0"/>	
送出先インタフェース	<input type="text" value="LAN0"/>	
IPv4転送先ルータ	<input type="text"/>	
自側エンドポイント	<input type="text"/>	
相手側エンドポイント	<input type="text"/>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

接続先名

この接続先を識別するための名称を8文字以内で指定します。

送出先インタフェース

パケットを送出するインタフェースを選択します。

IPv4 転送先ルータ

LANインタフェースにパケットを送出する際の転送先ルータのアドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

自側エンドポイント

IPv4形式のアドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

相手側エンドポイント

IPv4形式のアドレスを指定します。送出先インタフェースがLANインタフェースの場合は必ず設定してください。転送ルータのアドレスには利用するLANインタフェースと同じセグメントにする必要があります。異なるセグメントの場合、転送は行えません。

有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

◇別インタフェースから送出


[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: 別インタフェースから送出)]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
別インタフェースから送出		
基本情報	接続制御情報	マルチルーティング情報

「疑似ルータ」をチェックした場合、「接続制御情報」および「マルチルーティング情報」の項目はありません。「接続制御情報」および「マルチルーティング情報」は、[専用線接続] を参照してください。

【基本情報】

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: 別インタフェースから送出)] → [基本情報]

基本情報		
接続先名	ap0-0	
送出先インタフェース	LAN0	
転送先ルータ	IPv4ルータ	
	IPv6ルータ	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
保存	キャンセル	

接続先名

この接続先を識別するための名称を8文字以内で指定します。

送出先インタフェース

パケットを送出するインタフェースを選択します。

転送先ルータ (IPv4/IPv6 ルータ)

LANインタフェースにパケットを送出するときの転送先ルータのIPアドレスを指定します。

送出先インタフェースがLANインタフェースの場合は、必ず設定してください。転送ルータのIPアドレスは、利用するLANインタフェースと同じセグメントにする必要があります。異なるセグメントの場合は、転送することができません。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


◇ パケット破棄

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加 (接続先種別: パケット破棄)] → [パケット破棄]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)
パケット破棄
基本情報

[基本情報]

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報] → [追加] → [パケット破棄] → [基本情報]

■基本情報 	
接続先名	<input type="text" value="ap0-0"/>
パケット破棄	<input type="radio"/> しない <input checked="" type="radio"/> する <small>※“破棄しない”を選択した場合、この接続先情報は削除されます。</small>
<small>設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。</small>	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

接続先名

この接続先を識別するための名称を8文字以内で指定します。この接続先利用時には、すべてのパケットが破棄されます。

パケット破棄

送信するパケットをすべて破棄する場合は、“する”を選択します。


15.4 PPP 関連

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [PPP 関連]

相手情報 - ネットワーク情報(rmt0)	
共通情報	接続先情報
PPP関連	IP関連
IPv6関連	ブリッジ関連
MPLS関連	
圧縮情報	MP情報

◇ 圧縮情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [PPP 関連] → [圧縮情報]

■ 圧縮情報 	
ヘッダ圧縮 (IPCP)	<input checked="" type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	<input type="checkbox"/> IPヘッダ圧縮
データ圧縮 (CCP)	<input type="checkbox"/> LZS
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

送信するパケットのヘッダ部分の圧縮を行う機能です。使用する設定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

ヘッダ圧縮 (IPCP)

IPCP で使用する圧縮アルゴリズムを選択します。

- VJ
VJヘッダ圧縮 (RFC1144 準拠) を使用してヘッダ圧縮を行います。
- IPヘッダ圧縮
IPヘッダ圧縮 (RFC2507 / RFC2508 準拠) を使用してヘッダ圧縮を行います。

ヘッダ圧縮 (IPV6CP)

IPV6CP で使用する圧縮アルゴリズムを選択します。

- IPヘッダ圧縮
IPヘッダ圧縮 (RFC2507 / RFC2508 準拠) を使用してヘッダ圧縮を行います。

データ圧縮 (CCP)

CCP で使用するデータ圧縮アルゴリズムを選択します。

- LZS
LZS 圧縮 (RFC1974 準拠) を使用してデータ圧縮を行います。

こんな事に気をつけて

圧縮機能を MP で使用する場合、「ネットワーク情報」 - 「PPP 関連」 - 「MP 情報」の受信パケット順序制御で“する”を選択してください。受信パケット順序制御しないと圧縮機能が正しく動作しません。

◇ MP 情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [PPP 関連] → [MP 情報]

MP 回線初回リンク数

回線接続時に接続するチャンネル数を指定できます。

トラフィックによる増減

回線負荷に応じて帯域幅（1B、2B）を自動的にコントロールする機能を使用する場合は、“する”を選択し、回線増減の条件も指定します。指定した回線使用率を超えた（削減の場合は下回った）状態が“猶予時間”以上続いた時点で、回線の接続（削減の場合は切断）を行います。回線使用率は0～100%、猶予時間は0～3600秒の範囲で指定できます。

受信パケット順序制御

MPを使用すると、パケットの順序が入れ替って届く場合があります。正しい順序に並べ変えて受信する場合は“する”を選択します。

こんな事に気をつけて

MPを使用する場合、受信パケット順序制御で“しない”を選択すると、以下の機能が正しく動作しません。

- ブリッジ機能
- ヘッダ圧縮機能
- データ圧縮機能

15.5 IP 関連

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]

相手情報 - ネットワーク情報(rmt0)						
共通情報	接続先情報	PPP関連	IP関連	IPv6関連	ブリッジ関連	MPLS関連
IP基本情報	RIP情報	OSPF情報				
スタティックルーティング情報	IPフィルタリング情報	TOS値書き換え情報				
RIPフィルタリング情報	NAT情報	静的NAT情報				
帯域制御(WFQ)情報	マルチキャスト情報	EXP値書き換え情報				

「疑似ルータ」をチェックした場合、「RIP 情報」、「OSPF 情報」、「RIP フィルタリング情報」、「NAT 情報」、「静的 NAT 情報」、「マルチキャスト情報」および「EXP 値書き換え情報」の項目はありません。

◇ IP 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]
→ [IP 基本情報]

IP基本情報 ?

IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する <div style="margin-left: 20px;"> 相手IPアドレス <input style="width: 100px;" type="text"/> 自側IPアドレス <input style="width: 100px;" type="text"/> </div>
MSS書き換え	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する <div style="margin-left: 20px;"> 書き換えサイズ <input style="width: 30px;" type="text"/> バイト </div>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

「疑似ルータ」をチェックした場合、「IP アドレス」の項目はありません。

IP アドレス

このネットワーク情報の IP アドレスを固定で使用する場合は「設定する」を選択します。「相手側 IP アドレス」または「自側 IP アドレス」の一方だけを指定し、他方を省略することもできます。動的に割り当てられる環境で、誤って IP アドレスを設定した場合は、ルーティング動作は行いますが、ルータから通信できないことがあります。また、RIP を使用する場合はどちらか一方を省略することはできません。両方とも指定するか「設定しない」を選択します。BGP または OSPF を使用する場合は、両方とも指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

こんな事に気をつけて

OSPF を使用するインタフェースはそれぞれ異なったネットワークに属する IP アドレスを設定する必要があります。同じネットワークに属する IP アドレスを設定した場合、OSPF を使用しないインタフェースとして扱われます。

MSS 書き換え

MSS 書き換え機能の設定をします。MSS 書き換え機能を使用する場合、「使用する」を選択し、書き換えサイズを 0 または 160 ~ 1460 の範囲で指定します。PPPoE (PPP over Ethernet) を利用する場合は、1414 に設定します。0 を指定した場合は、MSS 書き換え機能が無効となります。

◇ RIP 情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連] → [RIP 情報]

RIP情報	
RIP送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input checked="" type="radio"/> 受信しない <input type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》 メトリック値 <input type="text" value="0"/>	
《 RIP V2使用時に認証パケットを破棄しない時はRIP V2パスワードを設定してください。》 認証パケット <input type="radio"/> 破棄する <input checked="" type="radio"/> 破棄しない パスワード <input type="text"/>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

RIP を使用できるインターフェースの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

NAT 機能と併用することはできません。

RIP 送信

RIP 情報を送信するかどうかを選択します。送信する設定にすると、RIP 情報を定期的送信します。RIP 送信を行う場合は、RIP の種類を選択します。

- V1
ルーティングプロトコルに RIP V1 を使用し、ブロードキャストで送信します。
- V2
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストで送信します。
- V2 (Multicast)
ルーティングプロトコルに RIP V2 を使用し、マルチキャストで送信します。

RIP 受信

RIP 情報を受信するかどうかを選択します。RIP 受信を行う場合は、RIP の種類を選択します。

- V1
ルーティングプロトコルに RIP V1 を使用し、受信します。
- V2、V2 (Multicast)
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストおよびマルチキャストを受信します。

メトリック値

RIP 送信時に加算するメトリック値を選択します。

認証パケット

RIP V2 使用時にだけ有効な設定です。RIP V2 では、同じパスワードグループでだけ RIP 情報の交換を行うことができます。パスワード認証による RIP 情報の交換を行う場合は、“破棄しない”を選択し、パスワードを16文字以内で設定します。“破棄する”を選択した場合は、パスワード認証による RIP 情報の交換は行いません。

◇ OSPF 情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]→[OSPF情報]

■OSPF情報	
OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
エリア定義番号	0
出力コスト	10
Hello/パケット送信間隔	10 秒
隣接ルータ停止確認間隔	40 秒
パケット再送間隔	5 秒
LSUパケット送信遅延時間	1 秒
認証方式	<input checked="" type="radio"/> 認証を行わない
	<input type="radio"/> テキスト認証
	鍵種別 <input checked="" type="radio"/> 文字列 <input type="radio"/> 16進数 認証鍵 <input type="text"/>
	<input type="radio"/> MD5認証
	MD5認証鍵ID <input type="text"/>
	MD5認証鍵 <input type="text"/>
パケット送信	<input type="radio"/> 抑止する <input checked="" type="radio"/> 抑止しない
送信方法	<input checked="" type="radio"/> マルチキャストで送信 <input type="radio"/> ユニキャストで送信
MTU値確認	<input checked="" type="radio"/> 確認する <input type="radio"/> 確認しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ループバックインタフェースも含めて、OSPFを使用できるインタフェースの定義数は、BR500S仕様一覧「2.3 システム最大値一覧」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

- NAT機能と併用することはできません。
- OSPFを使用できるインタフェースには上限があります。OSPFを使用するインタフェースの合計が本装置の上限を超えないように設定する必要があります。

OSPF 機能

OSPF を使用するかどうかを選択します。

エリア定義番号

OSPF エリア情報のエリア定義番号を 10 進数を使用して指定します。OSPF エリア情報は、「ルーティングプロトコル情報」 - 「OSPF 関連」 で設定することができます。省略時は、0 が設定されます。

出力コスト

OSPF 出力コストを 1～65535 の範囲で指定します。省略時は、10 が設定されます。

Hello パケット送信間隔

OSPF 隣接関係の維持に使用する、Hello パケットの送信間隔を指定します。通常は、“10 秒” を指定します。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ Hello パケットの送信間隔を指定してください。

隣接ルータ停止確認間隔

OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。隣接ルータ停止確認間隔は、Hello パケット送信間隔より大きな値を指定する必要があります。Hello パケット送信間隔の 4 倍を設定することをお勧めします。通常は“40 秒” を指定します。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ隣接ルータ停止確認間隔を指定してください。隣接ルータ停止確認間隔は、装置起動時に指定ルータおよび副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を設定した場合は、経路交換の開始が遅れます。

パケット再送間隔

OSPF パケットを再送する間隔を指定します。省略時は、5 秒が設定されます。

有効範囲)
1～18 時間
1～1092 分
3～65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。省略時は、1 秒が設定されます。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

こんな事に気をつけて

LSA は、生成されてから 1 時間が経過すると破棄されます。LSU 送信遅延時間に 1 時間以上を指定しないでください。正しくルーティングできない場合があります。

認証方式

パケット認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が“文字列”の場合は、8 文字以内で指定します。鍵種別が“16 進数”の場合は、16 進数を使用して 16 桁以内で指定します。16 桁未満の値を指定したときは左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。

MD5 認証鍵 ID

MD5 認証鍵 ID を 1～255 の範囲で指定します。

MD5 認証鍵

MD5 認証鍵を指定します。16 文字以内で指定します。

パケット送信

OSPF パケットの送信を抑制するかどうかを選択します。

送信方法

OSPF パケットの送信方法を選択します。OSPF パケットをマルチキャストで受信できない装置と接続する場合は、“ユニキャストで送信”を選択します。

MTU 値確認

隣接ルータと OSPF パケットの MTU 値の確認を行うかどうかを選択します。隣接ルータの仕様により、MTU 値の不整合が回避できないときは、“確認しない”を選択します。

◇スタティック経路情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]
→[スタティック経路情報]

■スタティック経路情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

あて先IPアドレス/マスク	メトリック値	優先度	操作
全削除			
<スタティック経路情報入力フィールド>			
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定		
	あて先IPアドレス	<input type="text"/>	
	あて先アドレスマスク	0 (0.0.0.0)	
メトリック値	1		
優先度	0		
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「疑似ルータ」をチェックした場合、「メトリック値」および「優先度」の項目はありません。

現在、相手側に設定されているスタティック経路の情報の定義が表示されています。BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次の処理に進みます。

「疑似ルータ」をチェックした場合、「メトリック値」と「優先度」の項目はありません。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。“ネットワーク指定”を指定した場合は、あて先IPアドレス/アドレスマスクを指定します。

メトリック値

このスタティック経路情報をRIPに再配布するときのメトリック値を、1～15から選択します。RIPに再配布したときは、設定したRIPメトリック値+1のメトリック値でRIPテーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10進数を使用して0～254の範囲で指定します。省略時は、0が設定されます。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
EBGP	20
OSPF	110
RIP	120
IBGP	200
DNS	15

複数のスタティック経路情報でECMP機能を使用するときは、あて先、RIPメトリック値、優先度がそれぞれ同じになるようにスタティック経路情報を設定します。また、ECMP機能を使用する場合は、「ルーティングプロトコル情報」の「ルーティングマネージャ情報」にある「ECMP情報」でECMPを使用するように設定します。ECMPとなるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で4個まで定義できます。

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。

- 優先度が0のスタティック経路情報と、優先度が0以上のスタティック経路情報は同時に設定できません。
 - 優先度が同じで、メトリック値が違うスタティック経路情報は同時に設定できません。
-

◇ IPフィルタリング情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]
→[IPフィルタリング情報]

■IPフィルタリング情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号 ICMPタイプ ICMPコード	TCP接続要求	TOS	方向	操作
条件にあてはまらない場合の動作			透過	修正 初期化			
全削除							
<IPフィルタリング情報入力フィールド>							
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断						
プロトコル	すべて <input type="checkbox"/> (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)						
送信元情報	IPアドレス	<input type="text"/>					
	アドレスマスク	0 (0.0.0.0) <input type="text"/>					
	ポート番号	<input type="text"/>					
あて先情報	IPアドレス	<input type="text"/>					
	アドレスマスク	0 (0.0.0.0) <input type="text"/>					
	ポート番号	<input type="text"/>					
ICMP	タイプ	<input type="text"/>					
	コード	<input type="text"/>					
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外						
TOS	<input type="text"/>						
方向	入出力 <input type="text"/>						
追加 キャンセル							

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されているIPフィルタリング情報の定義が表示されています。処理は優先順位1から順に行います。IPフィルタリングの定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致する場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

「条件にあてはまらない場合の動作」の「初期化」ボタンをクリックすると、初期状態（透過）が設定されます。

こんな事に気をつけて

WWWやDHCPに対するアクセスを制限する設定を行った場合、WWWブラウザからアクセスできない、または、DHCP機能が使用できなくなることがあります。

動作

IP フィルタリングの動作を以下の3つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 透過 (接続中のみ)
条件と一致する場合に、回線が接続しているときはパケット透過し、切断しているときは遮断します。
- 遮断
条件と一致する場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の6つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

フィルタリング条件としてのIPアドレスおよびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと定義するアドレスマスクの論理積、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。

“any”を指定する場合は、すべてのポート番号をフィルタリングの対象とします。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

ICMP

タイプ

フィルタリング条件としてICMPパケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMPタイプ値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPタイプ値をフィルタリングの対象とします。

コード

フィルタリング条件としてICMPパケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMPコード値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPコード値をフィルタリングの対象とします。

TCP 接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

TOS

フィルタリング条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTOSフィールド値をフィルタリングの対象とします。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
- 出力のみ
出力パケットだけをフィルタリングする対象とします。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
 - 送信元 IP アドレス/アドレスマスクとあて先 IP アドレス/アドレスマスク
 - 送信元ポート番号とあて先ポート番号


なお、入力パケットは IP アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対しても TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。

- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

◇ IP フィルタリング情報 (条件にあてはまらない場合の動作)

[操作] 「設定メニュー」→ルータ設定「相手情報」→[修正]→[IP関連]→[IP フィルタリング情報]
→「条件にあてはまらない場合の動作」[修正]

■ IP フィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 

優先順位	動作	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号 ICMPタイプ ICMPコード	TCP接続要求	TOS	方向	操作
<IPフィルタリング情報入力フィールド(条件にあてはまらない場合)>							
	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断 <input type="radio"/> SPI						
	情報保持タイム <input type="text" value="5"/> 分						
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>							
<input type="button" value="全削除"/>							

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

「疑似ルータ」をチェックした場合、「SPI」および「情報保持タイム」の項目はありません。

「条件にあてはまらない場合の動作」は、このネットワークに設定されているIPフィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断やSPIを指定し、IPフィルタリング情報でWWWやDHCPに対するアクセスを透過する設定を行わなかった場合、本装置に対しWWWブラウザからアクセスできない、または、DHCP機能が使用できなくなることがあります。

動作

IP フィルタリング定義のどれにも一致しない場合の動作を以下の4つから選択します。

- 透過
IP フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 透過（接続中のみ）
IP フィルタリング定義のどれにも一致しない場合に、回線が接続しているときはパケットを透過し、切断しているときは遮断します。
- 遮断
IP フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IP フィルタリング定義のどれにも一致しないで、プロトコルがTCPの場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルがUDPやそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイマ

SPIセッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

◇ TOS 値書き換え情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連]
→ [TOS 値書き換え情報]

■ TOS 値書き換え情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	プロトコル	送信元IPアドレス/マスク 送信元ポート番号	TOS	操作
		あて先IPアドレス/マスク あて先ポート番号	新TOS	

<TOS値書き換え情報入力フィールド>

プロトコル すべて 番号指定: "その他"を選択時のみ有効です

送信元情報	IPアドレス	<input type="text"/>
	アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>
	ポート番号	<input type="text"/>
あて先情報	IPアドレス	<input type="text"/>
	アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>
	ポート番号	<input type="text"/>
TOS		<input type="text"/>
新TOS		<input type="text"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

現在、このネットワークに設定されている TOS 値書き換え情報の定義が表示されています。処理は優先順位 1 から順に行います。TOS 値書き換えの定義数は、BR500S 仕様一覧 [2.3 システム最大値一覧] (P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致する場合に定義された TOS 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

プロトコル

TOS 値書き換えの条件としてプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

TOS 値書き換え条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

TOS 値書き換え条件としてのIPアドレスおよびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

TOS 値書き換え条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。

“any”を指定する場合は、すべてのポート番号がTOS書き換えの対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報で合わせて10組まで指定できます。

TOS

TOS 値書き換えの条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTOSフィールド値を書き換えの対象とします。

新TOS

IPパケットに新しく指定するTOSフィールド値を16進数を使用して、0～ffの範囲で指定します。

◇ RIP フィルタリング情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連] → [RIP フィルタリング情報]

■RIPフィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
全削除					
<RIPフィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断				
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信				
フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定				
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致			
	IPアドレス	<input type="text"/>			
	アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>			
メトリック値	<input type="text"/>				
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている RIP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、(送信方向/受信方向の)すべての条件に一致しないRIP経路情報は遮断されます。

動作

フィルタリング条件に該当する RIP 経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリング条件に該当するかどうかをチェックします。RIP パケット受信時にチェックするか、送信時にチェックするかを選択します。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定します。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致したRIP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、RIP経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、そのRIP経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になったRIP経路情報のメトリック値を変更できます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

◇ NAT 情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連] → [NAT 情報]

■ NAT 情報	
NATの使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ
グローバルアドレス	<input type="text"/>
アドレス個数	<input type="text" value="1"/> 個
アドレス割当てタイマ	<input type="text" value="5"/> 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsecパススルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

NAT の使用

“マルチ NAT” を選択すると、複数の端末と併用できます。“静的 NAT のみ” を選択すると静的 NAT 情報の条件に一致しないパケットは変換されません。NAT を使用しない場合は、以降の設定は無効です。

こんな事に気をつけて

本装置では相手情報と LAN 情報のインタフェースでアドレス変換機能を設定できます。ただし、使用する場合は、グローバルアドレスを使用するインタフェースだけで設定します。また、基本 NAT と静的 NAT で同一グローバルアドレスを使用しないでください。

グローバルアドレス

特定のグローバルアドレスを使用するときに指定します。指定しない場合は自動で割り当てられます。

アドレス個数

複数個のグローバルアドレスを使用する場合は、上述のグローバルアドレスを先頭とし、連続した複数のアドレスを指定します。その個数を 1～16 の範囲で指定します。なお、アドレス個数の設定は、グローバルアドレスを指定した場合にだけ有効です。省略時は、1 が設定されます。

アドレス割当てタイマ

アドレス変換情報は一定の時間、該当する通信が行われないと、自動的に解放されます。解放するための猶予時間を 0～24 時間の範囲で指定します。0 を指定すると、タイマによる情報の解放は行われません。省略時は、5 分が設定されます。

NAT セキュリティ

- 通常
相手サーバが NAT を使用している際など、要求先とは別のアドレスから応答します。
- 高い
ftp や dns の要求する相手からの応答かどうかをチェックします。

IPsec パススルー

- 有効
相手ごとに 1 つの IPsec パスを接続することができます。
- 無効
IPsec クライアントが NAT トラバーサル機能を使用することができます。

こんな事に気をつけて

IPsec クライアントが NAT トラバーサル機能を使用する場合は、IPsec パススルーを“無効”に設定します。IPsec パススルーを“有効”に設定すると、相手ごとに 1 つの IPsec パスしか接続することができません。

◇ 静的 NAT 情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連]
→ [静的 NAT 情報]

静的 NAT 情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

プライベートアドレス	プライベートポート番号	グローバルアドレス	グローバルポート番号	プロトコル	操作
条件にあてはまらない場合の動作		破棄		修正	初期化
全削除					
<静的 NAT 情報入力フィールド>					
プライベート IP 情報	IP アドレス	<input type="text"/>			
	ポート番号	すべて	番号指定: <input type="text"/> “その他”を選択時のみ有効です		
グローバル IP 情報	IP アドレス	<input type="text"/>			
	ポート番号	すべて	番号指定: <input type="text"/> “その他”を選択時のみ有効です		
プロトコル		すべて	番号指定: <input type="text"/> “その他”を選択時のみ有効です		
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

マルチ NAT を使用すると、アドレス変換情報を固定で持つことができます。現在、設定されている固定のアドレス変換情報の定義が表示されています。静的 NAT の定義の定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

プライベート IP 情報

IP アドレス

固定でアドレス変換を行う場合に、ローカルネットワーク側の IP アドレスを指定します。省略できません。

ポート番号

固定でアドレス変換を行う場合に、ローカルネットワーク側のポート番号を選択します。“その他”を選択して、ポート番号を指定する場合は、10 進数を使用して 1～65535 の範囲で指定します。

なお、グローバルポート番号を範囲指定する場合は、その範囲のグローバルポート番号は、指定したプライベートポート番号を先頭とした範囲へ変換されます。

たとえば、プライベートポート番号に 1000 を指定し、グローバルポート番号に 10000-11000 を指定すると、グローバルポート番号の 10000 から 11000 はプライベートポート番号の 1000 から 2000 に変換されます。

グローバル IP 情報

IP アドレス

固定でアドレス変換を行う場合にリモートネットワーク側の IP アドレスを指定します。省略時は、すべてのグローバルアドレスに対して有効な設定となります。

ポート番号

固定でアドレス変換を行う場合にリモートネットワーク側のポート番号を選択します。“その他”を選択して、ポート番号を指定する場合は、10 進数を使用して 1～65535 の範囲から 1 つ、または “-” で区切った 1 組の範囲を指定します。

プロトコル

固定でアドレス変換を行う場合に対象となるプロトコルを以下の8つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- esp (50)
- ah (51)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

◇静的NAT情報（条件にあてはまらない場合の動作）

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]→[静的NAT情報]→「条件にあてはまらない場合の動作」[修正]

静的NAT情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

プライベートアドレス	プライベートポート番号	グローバルアドレス	グローバルポート番号	プロトコル	操作
<静的NAT情報入力フィールド(条件にあてはまらない場合)>					
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 破棄				
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>					
<input type="button" value="全削除"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている静的NAT定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。

動作

静的NAT定義のどれにも一致しない場合のIPフィルタリングの動作を以下の2つから選択します。

- 透過
静的NAT定義のどれにも一致しない場合にパケットを透過します。
- 破棄
静的NAT定義のどれにも一致しない場合にパケットを破棄します。

◇帯域制御 (WFQ) 情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]
→[帯域制御 (WFQ) 情報]

■帯域制御(WFQ)情報				
※追加情報は一覧の最後尾の入力フィールドで設定してください。				
定義番号	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号	対象TOSフィールド値 帯域	操作
全削除				
<帯域制御(WFQ)情報入力フィールド>				
プロトコル	すべて (番号指定: [] “その他”を選択時のみ有効です)			
送信元情報	IPアドレス	<input type="text"/>		
	アドレスマスク	0 (0.0.0.0)		
	ポート番号	<input type="text"/>		
あて先情報	IPアドレス	<input type="text"/>		
	アドレスマスク	0 (0.0.0.0)		
	ポート番号	<input type="text"/>		
対象TOSフィールド値	<input type="text"/>			
帯域	<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません			
追加 キャンセル				
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。				

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

現在、このネットワークに設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

プロトコル

帯域制御の対象となるプロトコルを以下の6つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPアドレス／アドレスマスク

帯域制御の対象となるIPアドレスおよびアドレスマスクを指定します。対象となるパケットのIPアドレスと定義するアドレスマスクの論理積と、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

対象TOSフィールド値

帯域制御の対象となるTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTOSフィールド値を帯域制御の対象とします。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

IPv4/IPv6以外のパケットは、すべて非優先（ベストエフォート）として扱われます。
回線にLANを使用して、帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

◇マルチキャスト情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]
→[マルチキャスト情報]

■マルチキャスト情報	
マルチキャスト機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> static <input type="radio"/> PIM-DM <input type="radio"/> PIM-SM
TTLしきい値	1
PIMプリファレンス値	1024
上流ルータの種類	<input checked="" type="radio"/> PIMルータのみ <input type="radio"/> すべて

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

マルチキャスト機能

リモートインタフェース上でマルチキャスト機能を使用する場合は、どれかのマルチキャスト・プロトコルを選択します。マルチキャストを利用する場合は、インタフェースにIPアドレスを手動で割り当てます。IPアドレスが設定されていないインタフェースでの動作はサポートしていません。

こんな事に気をつけて

- マルチキャスト機能を使用するすべてのインタフェース上で、同じプロトコルを選択してください。同時に複数のプロトコルを利用することはできません。
- NAT機能と併用することはできません。

TTLしきい値

LAN上でマルチキャスト機能を使用するときのTTLしきい値を10進数を使用して1～255の範囲で指定します。初期値は1です。

PIM-SMのPIM Registerパケットによりカプセル化されるマルチキャスト・パケットは、出力先インタフェースのTTLしきい値の設定にかかわらず出力されます。

PIMプリファレンス値

PIMのAssertメッセージに格納されるプリファレンス値を10進数を使用して1～65535の範囲で指定します。初期値は1024です。

並列な経路の存在のためにマルチキャスト・パケットが重複した場合は、PIM Assertメッセージによって、片側の転送経路が遮断されます。この際、プリファレンス値の小さい方の経路が有効になります。PIM Assertメッセージの発行時には、Assert対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインタフェースのプリファレンス値をAssertメッセージに格納します。Assertメッセージが出力されるインタフェースのプリファレンス値が格納されるわけではありません。

上流ルータの種類

本装置から上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送される場合、どの種類のルータからのマルチキャストパケット転送を許可するかを設定します。

上流ルータがPIMルータでない場合（マルチキャストパケットをスタティック経路によって転送するルータであった場合）に転送を許可する場合は、“すべて”を選択します。

こんな事に気をつけて

受信インタフェースと同一のIPセグメントから送信された（直接接続されたホストからの）マルチキャストパケットは、上流ルータの設定にかかわらず転送が行われます。

◇ EXP 値書き換え情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連]
→ [EXP 値書き換え情報]

■EXP値書き換え情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号	TOS	EXP	操作
<input type="button" value="全削除"/>					
<EXP値書き換え情報入力フィールド>					
プロトコル		すべて <input type="button" value="▼"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)			
送信元情報	IPアドレス	<input type="text"/>			
	アドレスマスク	<input type="text" value="0 0.0.0.0"/>			
	ポート番号	<input type="text"/>			
あて先情報	IPアドレス	<input type="text"/>			
	アドレスマスク	<input type="text" value="0 0.0.0.0"/>			
	ポート番号	<input type="text"/>			
TOS		<input type="text"/>			
EXP		<input type="text"/>			
					<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている EXP 値書き換え情報の定義が表示されています。処理は優先順位 1 から順に行われます。EXP 値書き換えの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された EXP 値を書き換えます。ただし、分割されたパケットに対しては正しく行えません。

プロトコル

EXP 値書き換え条件としてプロトコルを以下の 6 つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他” を選択し、10 進数を使用して、1～255 の範囲で指定します。

送信元／あて先情報

EXP 値書き換え条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

EXP 値書き換え条件としての IP アドレスおよびアドレスマスクを指定します。チェック対象となったパケットの IP アドレスと定義したアドレスマスクの論理積と、定義した IP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

EXP 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号が書き換えの対象となります。また、ポート番号を複数指定する場合は、“;” で区切ります。範囲指定の場合は“-” で区切ります。ポート番号は、送信元情報とあて先情報で合わせて 10 組まで指定できます。

TOS

EXP 値書き換え条件として IP パケットの TOS フィールド値を 16 進数を使用して 0～ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は “;” で区切ります。範囲指定の場合は“-” で区切ります。10 組まで指定できます。何も指定しない場合はすべての TOS フィールド値を書き換えの対象とします。

EXP

書き換える EXP 値を、0～7 の範囲で指定します。

15.6 IPv6 関連

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連]

相手情報 - ネットワーク情報(rmt2)						
共通情報	接続先情報	PPP関連	IP関連	IPv6関連	ブリッジ関連	MPLS関連
	IPv6基本情報		IPv6 RIP情報		IPv6スタティック経路情報	
	IPv6フィルタリング情報		IPv6 Traffic Class値書き換え情報		IPv6 RIPフィルタリング情報	
	IPv6帯域制御(WFQ)情報		IPv6 DHCP情報			

◇ IPv6 基本情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連] → [IPv6 基本情報]

■ IPv6基本情報 ?

IPv6	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する				
インタフェースID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input style="width: 100px;" type="text"/>				
IPv6 アドレス	アドレスまたはプレフィックス	Valid Lifetime 期限有 無期限	Pref. Lifetime 期限有 無期限	フラグ	
	<input style="width: 150px;" type="text"/>	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0	
	<input style="width: 150px;" type="text"/>	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0	
	<input style="width: 150px;" type="text"/>	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0	
ルータ広報	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する				
	最大送信間隔	<input style="width: 50px;" type="text"/> 秒			
	最小送信間隔	<input style="width: 50px;" type="text"/> 秒			
	Router Lifetime	<input style="width: 50px;" type="text"/> 秒			
	MTU	<input style="width: 50px;" type="text"/>			
	Reachable Time	<input style="width: 50px;" type="text"/> ミリ秒			
	Retrans Timer	<input style="width: 50px;" type="text"/> ミリ秒			
	Cur Hop Limit	<input style="width: 50px;" type="text"/>			
フラグ	<input style="width: 50px;" type="text"/>				

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IPv6

IPv6の通信を使用する場合は、“使用する”を選択します。

インタフェース ID

“自動”を選択する場合は、装置のMACアドレスから自動生成されるインタフェースIDを使用します。通常は“自動”を選択します。

“指定する”を選択する場合は、16ビットごとに区切り文字(:)を入れて、16桁の16進数でインタフェースIDを指定します。このとき、他装置と違うインタフェースIDを指定します。

記述例) 2001:db8:7654:3210

IPv6 アドレス

この装置で使用するIPv6アドレスを4個まで設定できます。

アドレスまたはプレフィックス

本装置の相手側のIPv6アドレスを標準的なIPv6アドレスで指定します。本装置ではプレフィックス長は64に固定されます。インタフェースID部分がすべて0の場合は、指定するアドレスはプレフィックスとして解釈されます。実際に利用するアドレスは、そのアドレスにインタフェースIDを付与したものとなります。リンクローカルアドレスは指定できません。

IPv6 DHCPクライアントが取得したプレフィックスを使用する場合は、上位を“dhcp@インタフェース名”の形式で指定し、下位80ビット分を標準的なIPv6アドレス表記方式で指定します。インタフェース名には、IPv6 DHCPクライアント機能が動作しているrmtインタフェースを指定します。

記述例)

2001:db8:1111:1000:1:2:3:4

完全なIPv6アドレスとして解釈されます。

2001:db8:1111:1000::

プレフィックスとして解釈され、インタフェースID部分にはインタフェースIDが付与されます。

dhcp@rmt0:1000::1

rmt0インタフェースで動作しているIPv6 DHCPクライアントが取得したプレフィックスを使用して完全なIPv6アドレスを指定します。

dhcp@rmt0:1000::

rmt0インタフェースで動作しているIPv6 DHCPクライアントが取得したプレフィックスを使用してプレフィックスを指定します。

Valid Lifetime

ルータ広報のプレフィックス情報ごとに設定するValid Lifetimeを指定します。通常は、“30日”を指定します。
(有効範囲)

0～365日

0～8760時間

0～525600分

0～31536000秒

期限を定めない場合（無期限の場合）は、チェックボックスをチェックします。

Pv6アドレスにIPv6 DHCPクライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCPクライアントが取得したValid Lifetimeと比較して短い方が有効になります。

Pref. Lifetime

ルータ広報のプレフィックス情報ごとに設定するPreferred Lifetimeを指定します。通常は、“7日”を指定します。
(有効範囲)

0～365日

0～8760時間

0～525600分

0～31536000秒

期限を定めない場合（無期限の場合）は、チェックボックスをチェックします。

IPv6アドレスにIPv6 DHCPクライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCPクライアントが取得したPreferred Lifetimeと比較して短い方が有効になります。

フラグ

ルータ広報のプレフィックス情報ごとに設定するフラグフィールドの内容を2桁の16進数で指定します。この領域の値として、RFC2461で以下の値が定義されています。必要に応じて以下の値の論理和を設定します。

- on-link flag 80
- autonomous address-configuration flag 40

通常は“c0”を指定します。

ルータ広報

ルータ広報メッセージ (router advertisement message) を送信する場合は“送信する”を選択し、以下の項目を設定します。

最大送信間隔

ルータ広報メッセージの最大送信間隔を指定します。初期値は600秒です。省略はできません。

有効範囲) 4～1800

最小送信間隔

ルータ広報メッセージの最小送信間隔を指定します。初期値は200秒です。省略はできません。

有効範囲) 3～最大送信間隔の3／4

Router Lifetime

ルータ広報で送信する Router Lifetime を指定します。初期値は1800秒です。省略はできません。

有効範囲) 0または最大送信間隔～9000

MTU

ルータ広報で送信する MTU option を指定します。省略時は、MTU option を含みません。

有効範囲) 1280～1500

Reachable Time

ルータ広報で送信する Reachable Time を指定します。省略値は0ミリ秒です。

有効範囲) 0～3600000

Retrans Timer

ルータ広報で送信する Retrans Timer を指定します。省略値は0ミリ秒です。

有効範囲) 0～4294967295

Cur Hop Limit

ルータ広報で送信する Cur Hop Limit を指定します。省略値は64です。

有効範囲) 0～255

フラグ

ルータ広報の本体部分に設定するフラグフィールドの内容を16進数を使用して2桁で指定します。この領域の値として、RFC2461で以下の値が定義されています。必要に応じて以下の値の論理和を設定します。省略値は00です。

- Managed address configuration flag 80
- Other stateful configuration flag 40

◇ IPv6 RIP 情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連] → [IPv6 RIP 情報]

IPv6 RIP 情報											
RIP 送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する メトリック値 <input type="text" value="0"/>										
RIP 受信	<input checked="" type="radio"/> 受信しない <input type="radio"/> 受信する										
集約経路送信	<table border="1"> <thead> <tr> <th>集約経路</th> <th>破棄経路設定</th> </tr> </thead> <tbody> <tr> <td> <input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/> </td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> </tbody> </table>	集約経路	破棄経路設定	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する
	集約経路	破棄経路設定									
	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/>	<input checked="" type="checkbox"/> 設定する									
	<input type="text"/>	<input checked="" type="checkbox"/> 設定する									
<input type="text"/>	<input checked="" type="checkbox"/> 設定する										
<input type="text"/>	<input checked="" type="checkbox"/> 設定する										
サイトローカルプレフィックス	<input type="radio"/> 交換しない <input checked="" type="radio"/> 交換する										

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

RIP を使用できるインタフェースの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。

RIP 送信

RIP を送信する場合は、“送信する” を選択します。

メトリック値

“送信する” を選択した場合に、加算するメトリック値を選択します。

RIP 受信

RIP を受信する場合は、“受信する” を選択します。

集約経路送信

RIP で集約経路を送信する場合に、集約して広報する経路を設定します。

集約経路

デフォルトルートまたはネットワーク指定を選択し、集約して広報する経路を指定します。

集約経路情報は、集約される経路情報がないときでも広報されます。また、同じあて先の経路情報がルーティングテーブルにないときでも広報され、ルーティングテーブルには設定されません。

- デフォルトルート
集約経路情報としてデフォルトルートだけを広報します。
- ネットワーク指定
集約経路情報をプレフィックス/プレフィックス長で指定します。指定した集約経路情報は広報され、集約経路情報に含まれる経路情報は広報されません。

破棄経路設定

広報した集約経路情報により本装置に送られたIPv6パケットをルーティングするための経路情報がないときに、そのあて先へは到達不能であることをICMPv6で通知することができます。チェックしないときは、そのあて先への経路がないことがICMPv6で通知されます。

チェック時は、集約経路情報と同じあて先の経路情報が破棄経路としてルーティングテーブルに設定されます。

◇ IPv6 スタティック経路情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]→[IPv6 スタティック経路情報]

現在、相手側に設定されているIPv6スタティック経路情報の定義が表示されています。IPv6スタティック経路の定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

IPv6経路情報を固定で設定できます。ただし、デフォルトルートは装置に1つしか設定できません。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。“ネットワーク指定”を選択した場合は、あて先プレフィックス/プレフィックス長を指定します。あて先ネットワークにリンクローカルアドレスは指定できません。

メトリック値

このスタティック経路情報をRIPに再配布するときのメトリック値を、1～15から選択します。RIPに再配布したときは、設定したRIPメトリック値+1のメトリック値でRIPテーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10進数を使用して0～254の範囲で指定します。省略時は、0が設定されます。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
RIP	120
DNS	15
DHCP	10

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。

- 優先度が0のスタティック経路情報と、優先度が0以上のスタティック経路情報は同時に設定できません。
 - 優先度が同じスタティック経路情報は同時に設定できません。
-

◇ IPv6 フィルタリング情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連] → [IPv6 フィルタリング情報]

■ IPv6 フィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	送信元IPv6アドレス/プレフィックス長	送信元ポート番号	あて先IPv6アドレス/プレフィックス長	あて先ポート番号	ICMPv6タイプ	ICMPv6コード	TCP接続要求	Traffic Class	方向	操作
条件にあてはまらない場合の動作								透過		修正 初期化	
全削除											

<IPv6 フィルタリング情報入力フィールド>

動作 透過 透過(接続中のみ) 遮断

プロトコル すべて (番号指定: "その他"を選択時のみ有効です)

送信元情報
 IPv6アドレス/プレフィックス長
 ポート番号

あて先情報
 IPv6アドレス/プレフィックス長
 ポート番号

ICMPv6
 タイプ
 コード

TCP接続要求 対象 対象外

Traffic Class

方向 入力のみ

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このインタフェースに設定されている IPv6 フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行います。IPv6 フィルタリングの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく行えません。

「条件にあてはまらない場合の動作」の「初期化」ボタンをクリックすると、初期状態（透過）が設定されます。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリングの動作を以下の3つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 透過（接続中のみ）
条件と一致する場合に、回線が接続されていればパケットを透過し、切断されていれば遮断します。
- 遮断
条件と一致した場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の5つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～254の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

フィルタリング条件としてのIPv6アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6アドレスと定義するプレフィックス長の論理積、定義するIPv6アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件として、ポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。

“any”を指定した場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

ICMPv6

タイプ

フィルタリング条件としてICMPv6パケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMPv6タイプ値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPv6タイプ値をフィルタリングの対象とします。

コード

フィルタリング条件としてICMPv6パケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMPv6コード値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPv6コード値をフィルタリングの対象とします。

TCP 接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

Traffic Class

フィルタリング条件としてIPv6パケットのTraffic Class値を16進数を使用して0～ffの範囲または“any”で指定します。Traffic Class値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのTraffic Class値をフィルタリングの対象とします。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
 - 送信元 IPv6 アドレス/プレフィックス長とあて先 IPv6 アドレス/プレフィックス長
 - 送信元ポート番号とあて先ポート番号

なお、リバースを指定した場合は、入力パケットは IPv6 アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対しても TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。

- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

◇ IPv6 フィルタリング情報 (条件にあてはまらない場合の動作)

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]
→[IPv6 フィルタリング情報]→「条件にあてはまらない場合の動作」[修正]

IPv6 フィルタリング情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	プロトコル	送信元IPv6アドレス/プレフィックス長	送信元ポート番号	TCP 接続 要求	Traffic Class	方向	操作
			あて先IPv6アドレス/プレフィックス長	あて先ポート番号				
			ICMPv6タイプ					
			ICMPv6コード					

<IPv6 フィルタリング情報入力フィールド(条件にあてはまらない場合)>

動作

- 透過
- 透過(接続中のみ)
- 遮断
- SPI

情報保持タイム 分

保存 キャンセル 一覧へ戻る

全削除

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている IPv6 フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断やSPIを指定し、IPv6 フィルタリング情報でWWWやDHCPに対するアクセスを透過する設定を行わなかった場合、本装置に対しWWWブラウザからアクセスできない、または、DHCP機能が使用できなくなることがあります。

動作

IPv6 フィルタリング定義のどれにも一致しない場合の動作を以下の4つから選択します。

- 透過
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 透過 (接続中のみ)
条件と一致する場合に、回線が接続されていればパケットを透過し、切断されていれば遮断します。
- 遮断
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IPv6 フィルタリング定義のどれにも一致しないで、プロトコルがTCPの場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルがUDPやそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイム

SPIセッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

◇ IPv6 Traffic Class 値書き換え情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連] → [IPv6 Traffic Class 値書き換え情報]

■ IPv6 Traffic Class 値書き換え情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	プロトコル	送信元IPv6アドレス/プレフィックス長 送信元ポート番号	Traffic Class	操作
		あて先IPv6アドレス/プレフィックス長 あて先ポート番号	新Traffic Class	

<IPv6 Traffic Class 値書き換え情報入力フィールド>

プロトコル (番号指定: "その他"を選択時のみ有効です)

送信元情報	IPv6アドレス/プレフィックス長	<input type="text"/>
	ポート番号	<input type="text"/>
あて先情報	IPv6アドレス/プレフィックス長	<input type="text"/>
	ポート番号	<input type="text"/>
Traffic Class		<input type="text"/>
新Traffic Class		<input type="text"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている IPv6 Traffic Class 値書き換え情報の定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Traffic Class 値書き換えの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

プロトコル

IPv6 Traffic Class 書き換え条件としてプロトコルを以下の 5 つから選択します。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、“その他” を選択し、10 進数を使用して、0～254 の範囲で指定します。

送信元／あて先情報

IPv6 Traffic Class 値書き換え条件としてのアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

IPv6 Traffic Class 値書き換え条件としての IPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットの IPv6 アドレスと定義するプレフィックス長の論理積、定義する IPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

IPv6 Traffic Class 値書き換え条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定した場合は、すべてのポート番号が書き換えの対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

Traffic Class

IPv6 Traffic Class 値書き換え条件としてIPv6パケットのIPv6 Traffic Class 値を16進数を使用して0～ffの範囲または“any”で指定します。Traffic Class フィールド値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのIPv6 Traffic Class 値を書き換えの対象とします。


新 Traffic Class

IPv6パケットに新しく指定するIPv6 Traffic Class 値を16進数を使用して、0～ffの範囲で指定します。

◇ IPv6 RIP フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]
→ [IPv6 RIP フィルタリング情報]

IPv6 RIP フィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
全削除					
<IPv6 RIP フィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断				
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信				
フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定				
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致			
	プレフィックス / プレフィックス長	<input type="text"/> / <input type="text"/>			
メトリック値	<input type="text"/>				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている RIP フィルタリング定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

RIP 受信（送信）時には、優先順位の高い定義から順に受信（送信）方向の条件を参照し、一致した条件があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、受信（送信）方向のすべての条件に一致しない RIP 経路情報は遮断されます。

動作

フィルタリング対象に該当する RIP 経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合に RIP 経路情報を透過します。
- 遮断
条件と一致した場合に RIP 経路情報を遮断します。

方向

フィルタリングを RIP 受信時に行うか、RIP 送信時に行うかを選択します。

- 受信
RIP 受信時に、フィルタリングを行います。
- 送信
RIP 送信時に、フィルタリングを行います。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報がフィルタリングの対象となります。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致したRIP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したプレフィックスと、RIP経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、そのRIP経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になったRIP経路情報のメトリック値を変更できます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

◇ IPv6 帯域制御 (WFQ) 情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連] → [IPv6 帯域制御 (WFQ) 情報]

■ IPv6帯域制御(WFQ)情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

定義番号	プロトコル	送信元IPv6アドレス/プレフィックス長 送信元ポート番号 あて先IPv6アドレス/プレフィックス長 あて先ポート番号	対象Traffic Class 値 帯域	操作
				全削除

<IPv6帯域制御(WFQ)情報入力フィールド>

プロトコル (番号指定: “その他”を選択時のみ有効です)

送信元情報	IPv6アドレス/プレフィックス長	<input type="text"/>
	ポート番号	<input type="text"/>
あて先情報	IPv6アドレス/プレフィックス長	<input type="text"/>
	ポート番号	<input type="text"/>
対象Traffic Class値		<input type="text"/>
帯域		

最優先
 ベストエフォート
 使用率 %
 使用帯域 Kbps
 帯域を他と共有

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IPv6 アドレス、ポート番号、IPv6 Traffic Class 値の条件を元に帯域を割り当てます。

プロトコル

帯域制御の対象となるプロトコルを以下の5つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、“その他” を選択し、10進数を使用して、0～254の範囲で指定します。

送信元/あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPv6 アドレス/プレフィックス長

帯域制御の対象となるIPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6 アドレスと定義するプレフィックス長の論理積と、定義するIPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 Traffic Class 値

帯域制御の対象となるIPv6パケットのTraffic Class 値を16進数を使用して、0～ffの範囲または“any”で指定します。Traffic Class 値を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTraffic Class 値を帯域制御の対象とします。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

IPv4/IPv6以外のパケットは、すべて非優先（ベストエフォート）として扱われます。
回線にLANを使用して、帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

◇ IPv6 DHCP 情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連] → [IPv6 DHCP 情報]

IPv6 DHCP 情報			
DHCP 機能		<input checked="" type="radio"/> 使用しない <input type="radio"/> クライアント機能を使用する <input type="radio"/> サーバ機能を使用する	
クライアント / サーバ 機能共通	DUID	<input checked="" type="radio"/> 自動 <input type="radio"/> 文字列で指定する <input type="text"/> <input type="text"/> <input type="radio"/> 16進数で指定する <input type="text"/> <input type="text"/>	
	IAID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>	
クライアント 機能	プレフィックス 要求	<input type="radio"/> しない <input checked="" type="radio"/> する <input type="checkbox"/> 旧方式を使用する <small>※draft-troan-dhcpv6-opt-prefix-delegation-01.txt に準拠したサーバを使用する場合は、“旧方式を使用する”をチェックしてください。</small>	
	DNSサーバアドレス要求	<input checked="" type="radio"/> する <input type="radio"/> しない	
	リジェクト経路	<input checked="" type="radio"/> Blackhole <input type="radio"/> Reject	
サーバ機能	プリファレンス 値	<input type="text" value="0"/>	
	プレフィックス 広報	<input type="radio"/> しない <input checked="" type="radio"/> する プレフィックス <input type="text"/> / <input type="text"/>	
		Valid Lifetime	<input type="radio"/> 期限有 <input type="text"/> 日 <input checked="" type="radio"/> 無期限
		Pref. Lifetime	<input type="radio"/> 期限有 <input type="text"/> 日 <input checked="" type="radio"/> 無期限
		自動経路設定	<input checked="" type="radio"/> する <input type="radio"/> しない
	DNSサーバ広報	<input type="text"/>	
セカンダリ DNSサーバ広報	<input type="text"/>		

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

DHCP 機能

それぞれのインタフェースのIPv6 DHCP 機能を以下の3つから選択します。

- 使用しない
DHCP 機能を使用しません。
- クライアント機能を使用する
該当インタフェースをIPv6 DHCP クライアントとして運用します。

- サーバ機能を使用する
本装置を該当インタフェースのネットワークのIPv6 DHCP サーバとして使用します。

クライアント／サーバ機能共通

DUID

DUID を以下の3つから選択します。

- 自動
DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 文字列で指定する
ASCII コードを使用して 130 文字以内で DUID を指定します。
- 16 進数で指定する
16 進数を使用して 260 桁以内で DUID を指定します。

クライアント機能

IAID

IAID を以下の2つから選択します。

- 自動
自動生成される IAID を使用します。通常は、この設定を使用します。
- 指定する
10 進数を使用して 1～4294967295 の範囲で指定します。

プレフィックス要求

DHCP サーバにプレフィックスを要求する場合は、“する”を選択します。“する”を選択した場合に、draft-troan-dhcpv6-opt-prefix-delegation-01.txt に準拠したサーバを利用するときは、“旧方式を使用する”をチェックします。

DNS サーバアドレス要求

DHCP サーバに DNS サーバアドレスを要求する場合は、“する”を選択します。

リジェクト経路

DHCP サーバから取得したプレフィックスのリジェクト経路を以下の2つから選択します。

- Blackhole
リジェクト経路あてのパケットを受信しても送信元にエラー報告をしません。
- Reject
リジェクト経路あてのパケットを受信した場合、送信元にエラー報告をします。

サーバ機能

プリファレンス値

DHCP サーバのプリファレンス値を 10 進数を使用して 0～255 の範囲で指定します。DHCP クライアントはこの値が大きい DHCP サーバを選択します。省略時は 0 が設定されます。

プレフィックス広報

DHCP クライアントに割り当てるプレフィックスを設定します。クライアントにプレフィックスを割り当てる場合は、“する”を選択し、以降の項目を設定します。

プレフィックス

クライアントに割り当てるプレフィックスとプレフィックス長を設定します。プレフィックス長は 48～64 の範囲で指定します。

有効範囲)

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:fff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Valid Lifetime

割り当てるプレフィックスの Valid Lifetime を指定します。

有効範囲)

0～365日

0～8760時間

0～525600分

0～31536000秒

Pref. Lifetime

割り当てるプレフィックスの Preferred Lifetime を指定します。Pref. Lifetime は、Valid Lifetime より短い時間になるように設定します。

有効範囲)

0～365日

0～8760時間

0～525600分

0～31536000秒

自動経路設定

クライアントに割り当てたプレフィックスへの経路を自動で設定する場合は“する”を選択します。

DNS サーバ広報

DNS サーバの IPv6 アドレスを指定します。省略時は、DHCP サーバによる広報を行いません。

有効範囲)

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:fff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

セカンダリ DNS サーバ広報

セカンダリ DNS サーバの IPv6 アドレスを指定します。省略時は、DHCP サーバによる広報を行いません。

有効範囲)

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:fff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

15.7 ブリッジ関連

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[ブリッジ関連]

相手情報 - ネットワーク情報(rmt0)		
共通情報	接続先情報	PPP関連
	IP関連	IPv6関連
	ブリッジ関連	MPLS関連
ブリッジ情報	MACフィルタリング情報	静的MAC学習テーブル情報

◇ブリッジ情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[ブリッジ関連]→[ブリッジ情報]

■ブリッジ情報		[?]
ブリッジ機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
グループ識別子	0	
STP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
	パスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する
	インタフェース優先度	128
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
保存 キャンセル		

ブリッジ機能

接続相手とブリッジで通信する場合は、“使用する”を選択します。

グループ識別子

ブリッジのグループ識別子を10進数で指定します。0～7の範囲で指定します。省略時は0が設定されます。

STP機能

STP機能を利用して経路制御を行う場合は、“使用する”を選択し、以下の項目を設定します。グループ識別子に0を設定した場合だけ、STPを利用することができます。この設定項目はブリッジ機能を使用する場合だけ有効です。

パスコスト

STPで利用するパスコストを選択します。“指定する”を選択する場合は、1～65535の範囲で指定します。パスコストの適性値が不明な場合は、“自動決定”を選択すると、自動的にパスコストが決定されます。

インタフェース優先度

STPで使用するインタフェースごとの優先度を0～255の範囲で指定します。値が小さい方が優先となります。

こんな事に気をつけて

ブリッジ機能をMPで使用する場合、「ネットワーク情報」→「PPP関連」→「MP情報」の受信パケット順序制御で“する”を選択してください。受信パケット順序制御しないと順序に依存するプロトコルの通信が停止する場合があります。

◇ MACフィルタリング情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [ブリッジ関連] → [MACフィルタリング情報]

■MACフィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	送信元MACアドレス	フォーマット種別	操作
		あて先MACアドレス	LSAP/type値	
<input type="button" value="全削除"/>				
<MACフィルタリング情報入力フィールド>				
動作	<input type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input checked="" type="radio"/> 遮断			
送信元MACアドレス	すべて <input type="button" value="▼"/> アドレス指定("指定する"を選択時のみ有効です) <input style="width: 100%;" type="text"/>			
あて先MACアドレス	すべて <input type="button" value="▼"/> アドレス指定("指定する"を選択時のみ有効です) <input style="width: 100%;" type="text"/>			
フォーマット種別	すべて <input type="button" value="▼"/> ("LLC形式"の場合はLSAP、"Ethernet形式"の場合はtype値を入力してください) <input style="width: 100%;" type="text"/>			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在のインタフェースのMACフィルタリング情報の定義が表示されています。MACフィルタリングの定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

WANモジュールで送受信する際にフィルタリング処理を行います。優先順位の高い定義から、順にフレームのチェックを行い、フィルタリング条件が一致した場合に定義された動作を行います。

動作

フィルタリング条件に一致したときの動作を以下の3つから選択します。

- 透過
フィルタリング条件と一致する場合に透過します。
- 透過 (接続中のみ)
フィルタリング条件と一致した場合に、回線が接続しているときはフレームを透過し、切断しているときは遮断します。
- 遮断
フィルタリング条件と一致する場合に遮断します。

送信元／あて先 MACアドレス

MACアドレスを以下の項目から選択します。“指定する”を選択する場合は、アドレス指定にMACアドレスを16進数で指定します。

- すべて
すべてのMACアドレスを対象とします。
- ブロードキャスト
ブロードキャストMACアドレスを対象とします。
- マルチキャスト
ブロードキャストMACアドレスおよびマルチキャストMACアドレスを対象とします。
- 指定する
アドレス指定に指定するMACアドレスを対象とします。MACアドレスは、「xx:xx:xx:xx:xx:xx」(xxは2桁の16進数)の形式で指定します。

フォーマット種別

フィルタリング対象のフォーマットを以下の項目から選択します。“LLC形式”の場合は、LSAPを16進数を使用して、0～ffffの範囲で指定し、“Ethernet形式”の場合は、type値を16進数を使用して、5dd～ffffの範囲で指定します。

- LLC形式
LLC形式のフレームを対象とします。
- Ethernet形式
Ethernet形式のフレームを対象とします。
- すべて
すべてのフレームを対象とします。

◇静的MAC学習テーブル情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[ブリッジ関連]→[静的MAC学習テーブル情報]

静的MAC学習テーブル情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

MACアドレス	操作
全削除	
<静的MAC学習テーブル情報入力フィールド>	
MACアドレス	<input type="text"/> <input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在、設定されている静的MAC学習テーブルの一覧です。静的MAC学習テーブルの定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

MACアドレス

MACアドレスは、「xx:xx:xx:xx:xx:xx」(xxは2桁の16進数)の形式で指定します。

15.8 MPLS 関連

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [MPLS 関連]

相手情報 - ネットワーク情報(rmt0)	
共通情報	接続先情報
PPP関連	IP関連
IPv6関連	ブリッジ関連
MPLS関連	
MPLS基本情報	LDP情報

◇ MPLS 基本情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [MPLS 関連] → [MPLS 基本情報]

■ MPLS 基本情報 ?	
MPLS機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
ラベル配布プロトコル	LDP
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
保存	キャンセル

MPLS 機能

リモート上で MPLS 機能を使用する場合は、“使用する”を選択します。

ラベル配布プロトコル

WAN 上で行うラベル配布プロトコルを選択します。

◇ LDP 情報

[操作] 「設定メニュー」 → ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [MPLS 関連] → [LDP 情報]

LDP 情報		
Hello タイマ	interval	5 秒
	HoldTime	<input type="radio"/> infinity <input checked="" type="radio"/> 指定する 15 秒
KeepAlive タイマ	interval	1 分
	timeout	3 分
LDP ラベル 広報方式	<input checked="" type="radio"/> DU <input type="radio"/> DoD	
LDP ラベル 保持方式	<input checked="" type="radio"/> liberal <input type="radio"/> conservative	
PHP 機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPv4 Transport アドレス	<input type="text"/>	
Multicast Hello	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 | キャンセル

Hello タイマ

interval

Hello の送信間隔のタイマを 1～65535 秒の範囲で指定します。初期値は 5 秒です。省略はできません。

有効範囲)
 1～18 時間
 1～1092 分
 1～65535 秒

HoldTime

近隣関係の維持を判定するため HoldTime のタイマを 1～65534 秒の範囲で指定します。初期値は 15 秒です。省略はできません。

有効範囲)
 1～18 時間
 1～1092 分
 1～65534 秒

こんな事に気をつけて

HoldTime の値は、interval の値より小さくすることはできません。HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

KeepAlive タイマ

interval

KeepAlive の送信間隔のタイマを 1～65535 秒の範囲で指定します。初期値は 1 分です。省略はできません。

有効範囲)
 1～18 時間
 1～1092 分
 1～65535 秒

timeout

LDP セッションの維持を判定するための KeepAlive の timeout のタイマを 1～65535 秒の範囲で指定します。初期値は 3 分です。省略はできません。

有効範囲)
 1～18 時間
 1～1092 分
 1～65535 秒

こんな事に気をつけて

timeout の値は、interval の値より小さくすることはできません。timeout の値は interval の値の 3 倍以上を設定することを推奨します。

LDP ラベル広報方式

Downstream Unsolicitedを使用する場合は、“DU”を選択します。Downstream On Demandを使用する場合は、“DoD”を選択します。

LDP ラベル保持方式

liberalを使用する場合は“liberal”を選択します。
conservativeを使用する場合は“conservative”を選択します。

PHP 機能

インタフェースあてのLSPのPHP機能を設定します。
PHP機能を無効にする場合は、“使用しない”を選択します。PHP機能を有効にする場合は、“使用する”を選択します。MPLS トンネル接続を使用する場合に、自側エンドポイントとIPアドレスが同じとき、設定に関係なく“使用しない”が設定されます。

IPv4 Transport アドレス

インタフェース単位でLDPが相手装置との通信に用いる送信元IPv4アドレスを分ける必要がある場合、本装置に設定されたIPv4アドレスを指定します。

0.0.0.0を指定した場合は、MPLS情報の設定のIPv4 Transport Addressの設定に従います。省略時は、0.0.0.0が設定されます。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

こんな事に気をつけて

IPv4 Transport アドレスは、必ず本装置に存在するアドレスを指定してください。

本装置に存在しないアドレスをインタフェースに指定した場合は、そのインタフェースではLDPを使用できません。

Multicast Hello

LDP Multicast Helloを送出するかどうかを設定します。

こんな事に気をつけて

MPLS トンネル接続を使用するインタフェースのトンネルエンドポイントに指定した装置がEoMPLS通信の相手装置となる場合は、本設定を必ず“送信しない”に設定してください。“送信する”を指定した場合は、VCラベルを交換できない通常のLDPセッションが確立してしまうため、EoMPLS通信で用いるVC LSPができず、EoMPLS通信を行う事ができません。それ以外の場合では必ず“送信する”を設定してください。“送信しない”を設定した場合はLDPの隣接関係が構築できず、LDPのセッションが確立できなくなります。

15.9 着信相手識別情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[着信相手識別情報]

■着信相手識別情報	
着信許可	<input type="radio"/> しない <input type="radio"/> する
認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
MP接続	<input type="radio"/> しない <input type="radio"/> する
	BAP/BACP利用 <input type="radio"/> しない <input type="radio"/> する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

発信者番号で識別できなかった相手からの着信について利用する情報です。

着信許可

発信者番号で識別できなかった相手からの着信を許可する場合は、“する”を選択します。

認証方式

着信時に利用する認証プロトコルを選択します。どちらのプロトコルも選択しなかった場合は、認証を行いません。

MP接続

着信時にMP接続を行う場合は、“する”を選択します。

BAP/BACP利用

BAP/BACPを利用する場合は、“する”を選択します。

16 テンプレート情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報」

テンプレート情報
テンプレート情報

■テンプレート情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

テンプレート名	使用するrmtインタフェース	操作
tmp0	rmt30~rmt34	修正 削除
全削除		

<テンプレート情報追加フィールド>

テンプレート名	<input type="text" value="tmp1"/>	追加 キャンセル
---------	-----------------------------------	------------

保存した情報は、設定反映後に有効になります。

現在、設定されているテンプレート情報が表示されます。テンプレート情報の最大定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。必要な処理のボタンをクリックし、次のページへ進みます。

テンプレート名

テンプレートの名称を8文字以内で指定します。

[操作] 「設定メニュー」→ルータ設定「テンプレート情報」→ [追加]

テンプレート情報 - **テンプレート情報(tmp1)**

共通情報	PPP関連	IP関連	IPv6関連
-------------	--------------	-------------	---------------

◇ 共通情報

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [共通情報]

■ 基本情報	
テンプレート名	tmp1
使用インタフェース	WAN0
使用するrmtインタフェース	rmt30 から 5 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信パケット (について) 0 秒
参照するAAA情報	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する AAAグループID

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

テンプレート名

テンプレートの名称を8文字以内で指定します。

使用インタフェース

テンプレート着信で使用するWANインタフェースを選択します。あらかじめ、WAN情報でISDN回線インタフェースを設定しておく必要があります。

使用する rmt インタフェース

テンプレート着信で使用する開始rmtインタフェース番号とインタフェース数を10進数を使用して指定します。

こんな事に気をつけて

テンプレート着信用に予約したrmtインタフェース番号に該当する相手定義番号には一切設定しないでください。定義が存在する場合は、該当する相手定義を削除してから予約してください。予約した範囲に該当する相手定義が存在した場合は、テンプレート着信は無効になります。

MTUサイズ

テンプレート着信で使用するrmtインタフェースに対して送信するパケットのMTU値を10進数を使用して200～1500で指定します。MTU値を変更すると、rmtインタフェースに対して送信するパケットの最大長が変更されます。また、PPPネゴシエーションにより、相手MRU値と相手MRRU値をMTU値まで小さくすることができます。省略時は、1500が指定されます。

無通信監視タイマ

テンプレート着信で接続したときの無通信監視時間を設定します。通信監視の対象パケットの無通信監視時間を0～3600秒の範囲で指定します。0秒を指定した場合は、監視を行いません。設定された間、監視対象となるパケットがない場合に無通信として回線を切断します。省略時は、無通信監視を行わないものとみなされます。

参照する AAA 情報

テンプレート着信で認証および着信時に参照するAAA情報を指定する場合は、“指定する”を選択します。

AAA グループ ID

AAAグループIDを10進数を使用して、2以内で指定します。省略時は、AAA情報は参照されません。


◇ PPP 関連

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [PPP 関連]

テンプレート情報 - テンプレート情報(tmp1)	
共通情報	PPP関連
IP関連	IPv6関連
認証情報	圧縮情報

【認証情報】

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [PPP 関連] → [認証情報]

■ 認証情報 	
認証方式	<input type="radio"/> PAP <input type="radio"/> CHAP <input checked="" type="radio"/> PAP/CHAP
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
保存	キャンセル

認証方式

着信時に利用する認証プロトコルを以下の3つから選択します。

- PAP
- CHAP
- PAP/CHAP

【圧縮情報】

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [PPP 関連] → [圧縮情報]

■圧縮情報	
ヘッダ圧縮 (IPCP)	<input checked="" type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	<input type="checkbox"/> IPヘッダ圧縮
データ圧縮 (CCP)	<input type="checkbox"/> LZS

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

送信するパケットのヘッダ部分の圧縮を行う機能です。使用する設定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

ヘッダ圧縮 (IPCP)

IPCP で使用する圧縮アルゴリズムを選択します。

- VJ
VJヘッダ圧縮 (RFC1144 準拠) を使用してヘッダ圧縮を行います。
- IPヘッダ圧縮
IPヘッダ圧縮 (RFC2507 / RFC2508 準拠) を使用してヘッダ圧縮を行います。

ヘッダ圧縮 (IPV6CP)

IPV6CP で使用する圧縮アルゴリズムを選択します。

- IPヘッダ圧縮
IPヘッダ圧縮 (RFC2507 / RFC2508 準拠) を使用してヘッダ圧縮を行います。

データ圧縮 (CCP)

CCP で使用するデータ圧縮アルゴリズムを選択します。

- LZS
LZS 圧縮 (RFC1974 準拠) を使用してデータ圧縮を行います。

◇ IP 関連

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [IP 関連]

テンプレート情報 - テンプレート情報(tmp1)			
共通情報	PPP関連	IP関連	IPv6関連
IP基本情報	IPフィルタリング情報		TOS値書き換え情報
帯域制御(WFQ)情報			

[IP 基本情報]

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [IP 関連] → [IP 基本情報]

■ IP基本情報 ?

DNSサーバ	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する <input style="width: 150px;" type="text"/>
MSS書き換え	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 書き換えサイズ <input style="width: 50px;" type="text"/> バイト
割当てIPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する 先頭IPアドレス <input style="width: 150px;" type="text"/> アドレス数 <input style="width: 50px;" type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

DNS サーバ

相手先と接続するときに通知する DNS サーバのアドレスを設定します。“設定しない”を選択した場合は、DNS サーバが存在しない、または 0.0.0.0 となります。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

MSS 書き換え

MSS 書き換え機能の設定をします。MSS 書き換え機能を使用する場合、“使用する”を選択し、書き換えサイズを 0 または 160 ~ 1460 の範囲で指定します。0 を指定した場合は、MSS 書き換え機能が無効となります。

割当て IP アドレス

AAA ユーザ情報で相手側 ID アドレスが指定されていない (IP アドレスが固定の必要がない) の着信相手に対して、割り当てる IP アドレスの範囲を設定します。割り当てアドレス数の定義最大値は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

[IPフィルタリング情報]

[操作] 「設定メニュー」→ルータ設定「テンプレート情報」→[追加]→[IP関連]→[IPフィルタリング情報]

■IPフィルタリング情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号 ICMPタイプ ICMPコード	TCP接続要求	TOS	方向	操作
条件にあてはまらない場合の動作			透過	修正 初期化			
全削除							
<IPフィルタリング情報入力フィールド>							
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断						
プロトコル	すべて (番号指定: <input type="text"/> "その他"を選択時のみ有効です)						
送信元情報	IPアドレス	<input type="text"/>					
	アドレスマスク	0 (0.0.0.0)					
	ポート番号	<input type="text"/>					
あて先情報	IPアドレス	<input type="text"/>					
	アドレスマスク	0 (0.0.0.0)					
	ポート番号	<input type="text"/>					
ICMP	タイプ	<input type="text"/>					
	コード	<input type="text"/>					
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外						
TOS	<input type="text"/>						
方向	入出力						
追加 キャンセル							

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このテンプレートに設定されているIPフィルタリング情報の定義が表示されています。処理は優先順位1から順に行います。IPフィルタリングの定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致する場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

「条件にあてはまらない場合の動作」の「初期化」ボタンをクリックすると、初期状態（透過）が設定されます。

こんな事に気をつけて

WWWやDHCPに対するアクセスを制限する設定を行った場合、WWWブラウザからアクセスできない、または、DHCP機能が使用できなくなることがあります。

動作

IP フィルタリングの動作を以下の2つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 遮断
条件と一致する場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の6つから選択します。()内はプロトコル番号です。

- すべて
- TCP (6)
- UDP (17)
- ICMP (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

フィルタリング条件としてのIPアドレスおよびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと定義するアドレスマスクの論理積、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。

“any”を指定する場合は、すべてのポート番号をフィルタリングの対象とします。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

ICMP

タイプ

フィルタリング条件としてICMPパケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMPタイプ値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPタイプ値をフィルタリングの対象とします。

コード

フィルタリング条件としてICMPパケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMPコード値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPコード値をフィルタリングの対象とします。

TCP 接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

TOS

フィルタリング条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTOSフィールド値をフィルタリングの対象とします。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
- 出力のみ
出力パケットだけをフィルタリングする対象とします。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
 - 送信元 IP アドレス/アドレスマスクとあて先 IP アドレス/アドレスマスク
 - 送信元ポート番号とあて先ポート番号

なお、入力パケットは IP アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対しても TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。

- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に選択します。

[IPフィルタリング情報 (条件にあてはまらない場合の動作)]

[操作] 「設定メニュー」→ルータ設定「テンプレート情報」→[追加]→[IP関連]→[IPフィルタリング情報]
→「条件にあてはまらない場合の動作」[修正]

■IPフィルタリング情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	プロトコル	送信元IPアドレス/マスク	送信元ポート番号	TCP接続要求	TOS	方向	操作
			あて先IPアドレス/マスク					
			あて先ポート番号					
			ICMPタイプ					
			ICMPコード					

<IPフィルタリング情報入力フィールド(条件にあてはまらない場合)>

動作

透過
 遮断
 SPI

情報保持タイム 分

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このテンプレートに設定されているIPフィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断やSPIを指定し、IPフィルタリング情報でWWWやDHCPに対するアクセスを透過する設定を行わなかった場合、本装置に対しWWWブラウザからアクセスできない、または、DHCP機能が使用できなくなることがあります。

動作

IPフィルタリング定義のどれにも一致しない場合の動作を以下の3つから選択します。

- 透過
IPフィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IPフィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IPフィルタリング定義のどれにも一致しないで、プロトコルがTCPの場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルがUDPやそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイマ

SPIセッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

[TOS 値書き換え情報]

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [IP 関連] → [TOS 値書き換え情報]

■TOS 値書き換え情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号	TOS 新TOS	操作
全削除				
<TOS 値書き換え情報入力フィールド>				
プロトコル		すべて (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)		
送信元 情報	IPアドレス	<input type="text"/>		
	アドレスマスク	0 (0.0.0.0)		
	ポート番号	<input type="text"/>		
あて先 情報	IPアドレス	<input type="text"/>		
	アドレスマスク	0 (0.0.0.0)		
	ポート番号	<input type="text"/>		
TOS		<input type="text"/>		
新TOS		<input type="text"/>		
追加 キャンセル				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

現在、このテンプレートに設定されている TOS 値書き換え情報の定義が表示されています。処理は優先順位 1 から順に行われます。TOS 値書き換えの定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された TOS 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

プロトコル

TOS 値書き換えの条件としてプロトコルを以下の 6 つから選択します。() 内はプロトコル番号です。

- すべて
- TCP (6)
- UDP (17)
- ICMP (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他” を選択し、10 進数を使用して、1～255 の範囲で指定します。

送信元／あて先情報

TOS 値書き換え条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

TOS 値書き換え条件としての IP アドレスおよびアドレスマスクを指定します。

チェック対象となるパケットの IP アドレスと、定義する IP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

TOS 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定する場合は、すべてのポート番号が TOS 書き換えの対象となります。また、ポート番号を複数指定する場合は、“;” で区切ります。範囲指定の場合は、“-” で区切ります。送信元情報とあて先情報で合わせて 10 組まで指定できます。

TOS

TOS 値書き換えの条件として IP パケットの TOS フィールド値を 16 進数を使用して、0～ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は、“;” で区切ります。範囲指定の場合は、“-” で区切ります。10 組まで指定できます。何も指定しない場合は、すべての TOS フィールド値を書き換えの対象とします。

新 TOS

IP パケットに新しく指定する TOS フィールド値を 16 進数を使用して、0～ff の範囲で指定します。

【帯域制御 (WFQ) 情報】

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [IP 関連]
→ [帯域制御 (WFQ) 情報]

■帯域制御(WFQ)情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

定義番号	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号	対象TOSフィールド 値 帯域	操作
<input type="button" value="全削除"/>				
<帯域制御(WFQ)情報入力フィールド>				
プロトコル		すべて <input type="button" value="▼"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)		
送信元 情報	IPアドレス	<input type="text"/>		
	アドレス マスク	0 (0.0.0.0) <input type="button" value="▼"/>		
	ポート 番号	<input type="text"/>		
あて先 情報	IPアドレス	<input type="text"/>		
	アドレス マスク	0 (0.0.0.0) <input type="button" value="▼"/>		
	ポート 番号	<input type="text"/>		
対象TOSフィールド 値		<input type="text"/>		
帯域		<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="button" value="▼"/> <input type="radio"/> 帯域を他と共有 <input type="button" value="共有できる定義が存在しません"/> <input type="button" value="▼"/>		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

こんな事に気をつけて

本機能は、ご自身で設定しないでください。本機能を使用する場合は、弊社の工事保守者に連絡してください。

現在、このインタフェースに設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

プロトコル

帯域制御の対象となるプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- TCP (6)
- UDP (17)
- ICMP (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPアドレス／アドレスマスク

帯域制御の対象となるIPアドレスおよびアドレスマスクを指定します。対象となるパケットのIPアドレスと定義するアドレスマスクの論理積と、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

対象TOSフィールド値

帯域制御の対象となるTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTOSフィールド値を帯域制御の対象とします。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

◇ IPv6 関連

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [IPv6 関連]

テンプレート情報 - テンプレート情報(tmp1)		
共通情報	PPP関連	IP関連
IPv6基本情報	IPv6フィルタリング情報	IPv6 Traffic Class値書き換え情報
IPv6帯域制御(WFQ)情報		

[IPv6 基本情報]

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [IPv6 関連] → [IPv6 基本情報]

■ IPv6基本情報 ?

IPv6	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
インタフェースID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input style="width: 100px;" type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IPv6

テンプレート着信で使用する rmt インタフェースで、IPv6 の通信を使用する場合は、“使用する” を選択します。

インタフェースID

テンプレート着信で使用する rmt インタフェースで利用する ID を設定します。“自動” を選択する場合は、装置の MAC アドレスから自動生成される EUI-64 形式のインタフェース ID を使用します。通常は、“自動” を選択します。

“指定する” を選択する場合は、16ビットごとに区切り文字 (:) を入れて、16進数を使用して16桁でインタフェースIDを指定します。このとき、他装置と同じインタフェースIDとならないような値を指定します。

記述例)

2001:db8:7654:3210

動作

IPv6 フィルタリングの動作を以下の2つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の5つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～254の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

フィルタリング条件としてのIPv6アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6アドレスと定義するプレフィックス長の論理積、定義するIPv6アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

ポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定した場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は、“;”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

ICMPv6

タイプ

フィルタリング条件としてICMPv6パケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMPv6タイプ値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPv6タイプ値をフィルタリングの対象とします。

コード

フィルタリング条件としてICMPv6パケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMPv6コード値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのICMPv6コード値をフィルタリングの対象とします。

TCP 接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

Traffic Class

フィルタリング条件としてIPv6パケットのTraffic Class値を16進数を使用して0～ffの範囲または“any”で指定します。Traffic Class値を複数指定する場合は“;”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのTraffic Class値をフィルタリングの対象とします。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
 - 送信元 IPv6 アドレス/プレフィックス長とあて先 IPv6 アドレス/プレフィックス長
 - 送信元ポート番号とあて先ポート番号リバースを指定した場合は、入力パケットは IPv6 アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対しても TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に選択します。

【IPv6 フィルタリング情報（条件にあてはまらない場合の動作）】

[操作] 「設定メニュー」→ルータ設定「テンプレート情報」→[追加]→[IPv6 関連]
→[IPv6 フィルタリング情報]→「条件にあてはまらない場合の動作」[修正]

IPv6 フィルタリング情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	プロトコル	送信元IPv6アドレス/プレフィックス長	送信元ポート番号	あて先IPv6アドレス/プレフィックス長	あて先ポート番号	ICMPv6タイプ	ICMPv6コード	TCP 接続 要求	Traffic Class	方向	操作

<IPv6 フィルタリング情報入力フィールド(条件にあてはまらない場合)>

動作

透過
 遮断
 SPI

情報保持タイム 分

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このテンプレートに設定されている IPv6 フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断やSPIを指定し、IPv6 フィルタリング情報でWWWやDHCPに対するアクセスを透過する設定を行わなかった場合、本装置に対しWWWブラウザからアクセスできない、または、DHCP機能が使用できなくなることがあります。

動作

IPv6 フィルタリング定義のどれにも一致しない場合の動作を以下の3つから選択します。

- 透過
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IPv6 フィルタリング定義のどれにも一致しないで、プロトコルがTCPの場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルがUDPやそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイマ

SPIセッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

[IPv6 Traffic Class 値書き換え情報]

[操作] 「設定メニュー」 → ルータ設定「テンプレート情報」 → [追加] → [IPv6 関連]
→ [IPv6 Traffic Class 値書き換え情報]

IPv6 Traffic Class 値書き換え情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	プロトコル	送信元IPv6アドレス/プレフィックス長 送信元ポート番号 あて先IPv6アドレス/プレフィックス長 あて先ポート番号	Traffic Class 新Traffic Class	操作
				全削除

<IPv6 Traffic Class 値書き換え情報入力フィールド>

プロトコル (番号指定: “その他”を選択時のみ有効です)

送信元情報	IPv6アドレス/プレフィックス長	<input style="width: 95%;" type="text"/>
	ポート番号	<input style="width: 95%;" type="text"/>
あて先情報	IPv6アドレス/プレフィックス長	<input style="width: 95%;" type="text"/>
	ポート番号	<input style="width: 95%;" type="text"/>
Traffic Class		<input style="width: 95%;" type="text"/>
新Traffic Class		<input style="width: 95%;" type="text"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このテンプレートに設定されている IPv6 Traffic Class 値書き換え情報の定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Traffic Class 値書き換えの定義数は、BR500S 仕様一覧 [「2.3 システム最大値一覧」\(P.19\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

プロトコル

IPv6 Traffic Class 書き換え条件としてプロトコルを以下の 5 つから選択します。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～254の範囲で指定します。

送信元/あて先情報

IPv6 Traffic Class 値書き換え条件としてのアドレス情報を設定します。

IPv6 アドレス/プレフィックス長

IPv6 Traffic Class 値書き換え条件としての IPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットの IPv6 アドレスと定義するプレフィックス長の論理積、定義する IPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

IPv6 Traffic Class 値書き換え条件としてポート番号を 10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定した場合は、すべてのポート番号が書き換えの対象となります。また、ポート番号を複数指定する場合は、“,”で区切ります。範囲指定の場合は“-”で区切ります。送信元情報とあて先情報を合わせて 10組まで指定できます。

Traffic Class

Traffic Class 値書き換え条件としてIPv6パケットのTraffic Class 値を16進数を使用して0～ffの範囲または“any”で指定します。Traffic Class フィールド値を複数指定する場合は“,”で区切ります。範囲指定の場合は“-”で区切ります。10組まで指定できます。何も指定しない場合はすべてのTraffic Class 値を書き換えの対象とします。

新 Traffic Class

IPv6パケットに新しく指定する Traffic Class 値を16進数を使用して、0～ffの範囲で指定します。

[IPv6 帯域制御 (WFQ) 情報]

[操作] 「設定メニュー」→ルータ設定「テンプレート情報」→[追加]→[IPv6 関連]
→ [IPv6 帯域制御 (WFQ) 情報]

■ IPv6帯域制御(WFQ)情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。

定義番号	プロトコル	送信元IPv6アドレス/プレフィックス長 送信元ポート番号 あて先IPv6アドレス/プレフィックス長 あて先ポート番号	対象Traffic Class 値 帯域	操作
全削除				
<IPv6帯域制御(WFQ)情報入力フィールド>				
プロトコル		すべて (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)		
送信元情報	IPv6アドレス/プレフィックス長	<input type="text"/>		
	ポート番号	<input type="text"/>		
あて先情報	IPv6アドレス/プレフィックス長	<input type="text"/>		
	ポート番号	<input type="text"/>		
対象Traffic Class 値		<input type="text"/>		
帯域		<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません		
追加 キャンセル				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このテンプレートに設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、BR500S仕様一覧「2.3 システム最大値一覧」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IPv6アドレス、ポート番号、IPv6 Traffic Class 値の条件を元に帯域を割り当てます。

プロトコル

帯域制御の対象となるプロトコルを以下の5つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

帯域制御の対象となるIPv6アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6アドレスと定義するプレフィックス長の論理積と、定義するIPv6アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“,”で区切ります。範囲指定の場合は、“-”で区切ります。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 Traffic Class 値

帯域制御の対象となるIPv6パケットのTraffic Class値を16進数を使用して、0～ffの範囲または“any”で指定します。Traffic Class値を複数指定する場合は、“,”で区切ります。範囲指定の場合は、“-”で区切ります。10組まで指定できます。何も指定しない場合は、すべてのTraffic Class値を帯域制御の対象とします。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域(%)を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

17 AAA 情報

[操作] 「設定メニュー」 → ルータ設定 「AAA 情報」

AAA 情報
グループID情報

17.1 グループID 情報

[操作] 「設定メニュー」 → ルータ設定 「AAA 情報」 → [グループID 情報]

グループID	グループ名	操作
全削除		
<グループID情報追加フィールド>		
グループ名	<input type="text"/>	
追加 キャンセル		

保存した情報は、設定反映後に有効になります。

現在、設定されているグループID 情報が表示されています。グループID 情報の定義数は、BR500S 仕様一覧 [「2.3 システム最大値一覧」](#) (P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

グループ名

グループ名を 0x21、0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

17.2 AAA ユーザ情報

[操作] 「設定メニュー」 → ルータ設定「AAA情報」 → [グループID情報] → [追加]

■AAAユーザ情報

定義番号	ユーザID	操作
全削除		

<AAAユーザ情報追加フィールド>

ユーザID

追加 キャンセル

保存した情報は、設定反映後に有効になります。

現在、設定されているAAAユーザ情報が表示されています。AAAユーザ情報の定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

ユーザID

ユーザIDを0x21、0x23～0x7eを使用して64文字以内で設定します。

[操作] 「設定メニュー」 → ルータ設定「AAA情報」 → [グループID情報] → [追加] → [AAAユーザ情報] → [追加]

AAA情報 - グループID情報(0) - **AAAユーザ情報(0)**

認証情報 IP関連 IPv6関連

◇ 認証情報

[操作] 「設定メニュー」 → ルータ設定「AAA 情報」 → [グループ ID 情報] → [追加] → [AAA ユーザ情報] → [追加] → [認証情報]

■ 認証情報	
ユーザID	<input type="text"/>
認証パスワード	<input type="password"/>
発信者番号による識別	<input checked="" type="radio"/> 番号チェックしない <input type="radio"/> 番号チェックする
	相手電話番号 <input type="text"/>
	相手サブアドレス <input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

ユーザID

ユーザIDを0x21、0x23～0x7eを使用して64文字以内で指定します。省略時は、認証情報を使用できません。

認証パスワード

認証パスワードを0x21、0x23～0x7eを使用して64文字以内で指定します。省略時は、認証情報のパスワードは使用できません。表示画面では暗号化された認証パスワードが表示されます。

発信者番号による識別

CLID相手判定で、発信者番号による識別を行う場合は、“番号チェックする”を設定します。

相手電話番号

相手の電話番号を0～9の数字と“*”、“#”、“-”、“(”、“)”、“\”を使用して、32桁以内のASCII文字列で指定します。

相手サブアドレス

相手のサブアドレスを、0x21、0x23～0x7eを使用して、19桁以内のASCII文字列で指定します。

こんな事に気をつけて

PIAFS (64Kbps) 着信時には、相手サブアドレスは無視されますので、設定しないでください。


◇ IP 関連

[操作] 「設定メニュー」 → ルータ設定「AAA 情報」 → [グループ ID 情報] → [追加] → [AAA ユーザ情報] → [追加] → [IP 関連]

AAA 情報 - グループ ID 情報(0) - AAA ユーザ 情報(0)		
認証情報	IP 関連	IPv6 関連
IP 基本情報	スタティック 経路情報	

[IP 基本情報]

[操作] 「設定メニュー」 → ルータ設定「AAA 情報」 → [グループ ID 情報] → [追加] → [AAA ユーザ情報] → [追加] → [IP 関連] → [IP 基本情報]

■ IP 基本情報		
自側 IP アドレス	<input type="text"/>	
相手側 IP アドレス	<input checked="" type="radio"/> テンプレート定義の設定に従う <input type="radio"/> 指定する	
	IP アドレス	<input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
保存	キャンセル	

自側 IP アドレス

自側 IP アドレスを指定します。省略または 0.0.0.0 を指定した場合は、IP アドレスなし (unnumbered) として動作します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

相手側 IP アドレス

相手側 IP アドレスとしてテンプレート定義で指定した割当て IP アドレスの設定内容に従うか、個別に指定するかを選択します。“指定する”を選択し、0.0.0.0 を指定した場合は、設定を IP アドレスなし (unnumbered) として動作します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

【スタティック経路情報】

[操作] 「設定メニュー」 → ルータ設定「AAA情報」 → [グループID情報] → [追加] → [AAAユーザ情報] → [追加] → [IP関連] → [スタティック経路情報]

■スタティック経路情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

あて先IPアドレス/マスク	メトリック値	優先度	操作
全削除			
<スタティック経路情報入力フィールド>			
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定		
	あて先IPアドレス <input type="text"/> あて先アドレスマスク <input type="text" value="0 (0.0.0.0)"/>		
メトリック値	<input type="text" value="1"/>		
優先度	<input type="text" value="1"/>		
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

ネットワーク

“デフォルトルート” または “ネットワーク指定” を選択します。“ネットワーク指定” を選択した場合は、あて先IPアドレス/アドレスマスクを指定します。

メトリック値

このスタティック経路情報をRIPに再配布するときのメトリック値を、1～15から選択します。RIPに再配布したときは、設定したRIPメトリック値+1のメトリック値でRIPテーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10進数を使用して1～254の範囲で指定します。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
EBGP	20
OSPF	110
RIP	120
IBGP	200
DNS	15

複数のスタティック経路情報でECMP機能を使用するときは、あて先、RIPメトリック値、優先度がそれぞれ同じになるようにスタティック経路情報を設定します。また、ECMP機能を使用する場合は、「ルーティングプロトコル情報」の「ルーティングマネージャ情報」にある「ECMP情報」でECMPを使用するように設定します。ECMPとなるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で4個まで定義できます。

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定する場合、優先度が同じで、メトリック値が違うスタティック経路情報は同時に設定できません。

◇ IPv6 関連

[操作] 「設定メニュー」 → ルータ設定「AAA情報」 → [グループID情報] → [追加] → [AAAユーザ情報] → [追加] → [IPv6関連]

AAA情報 - グループID情報(0) - AAAユーザ情報(0)		
認証情報	IP関連	IPv6関連
IPv6基本情報	IPv6スタティック経路情報	

【IPv6 基本情報】

[操作] 「設定メニュー」 → ルータ設定「AAA情報」 → [グループID情報] → [追加] → [AAAユーザ情報] → [追加] → [IPv6関連] → [IPv6基本情報]

■ IPv6基本情報 ?

インタフェースID	<input checked="" type="radio"/> テンプレート定義の設定に従う <input type="radio"/> 自動 <input type="radio"/> 指定する <input style="width: 100px;" type="text"/>
-----------	---

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

インタフェースID

“自動”を選択する場合は、装置のMACアドレスから自動生成されるインタフェースIDを使用します。通常は、“自動”を選択します。

“指定する”を選択する場合は、16ビットごとに区切り文字(:)を入れて、16進数を使用して16桁でインタフェースIDを指定します。このとき、他装置と同じインタフェースIDとならないような値を指定します。省略時は、テンプレート定義の設定に従います。

記述例)

2001:db8:7654:3210

[IPv6 スタティック経路情報]

[操作] 「設定メニュー」 → ルータ設定「AAA 情報」 → [グループ ID 情報] → [追加] → [AAA ユーザ情報] → [追加] → [IPv6 関連] → [IPv6 スタティック経路情報]

■ IPv6 スタティック経路情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

	あて先プレフィックス/プレフィックス長	メトリック値	優先度	操作
				全削除
<IPv6スタティック経路情報入力フィールド>				
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定			
	あて先プレフィックス/プレフィックス長	<input style="width: 100%;" type="text"/>		
メトリック値	<input type="text" value="1"/>			
優先度	<input type="text" value="1"/>			
				<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

IPv6 経路情報を固定で設定できます。ただし、デフォルトルートは装置に 1 つしか設定できません。

ネットワーク

“デフォルトルート” または “ネットワーク指定” を選択します。“ネットワーク指定” を選択した場合は、あて先プレフィックス/プレフィックス長を指定します。あて先ネットワークにリンクローカルアドレスは指定できません。

メトリック値

このスタティック経路情報を RIP に再配布するときのメトリック値を、1～15 から選択します。RIP に再配布したときは、設定した RIP メトリック値 +1 のメトリック値で RIP テーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10 進数を使用して 1～254 の範囲で指定します。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
RIP	120
DNS	15
DHCP	10

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定する場合、優先度が同じスタティック経路情報は同時に設定できません。

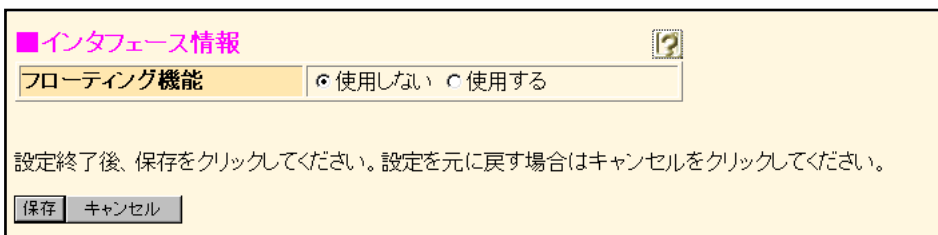
18 ルーティングプロトコル情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」



18.1 インタフェース情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [インタフェース情報]



フローティング機能

インタフェースのフローティング機能を使用する場合は、“使用する”を選択します。“使用しない”を選択した場合、インタフェースの状態変動に関係なく、インタフェース経路をルーティングテーブルに追加します。“使用する”を選択した場合、インタフェースが通信可能（リンクアップなど）状態であればインタフェース経路をルーティングテーブルに追加します。通信不可能（リンクダウンなど）状態であれば、ルーティングテーブルから削除します。また、ルーティングプロトコル優先度が0のスタティック経路情報についても、インタフェースの状態変動によってルーティングテーブルへの追加／削除を制御します。

本設定は、IPv4 機能、IPv6 機能で共通です。

18.2 ルーティングマネージャ情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [ルーティングマネージャ情報]



◇再配布情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [ルーティングマネージャ情報]
→ [再配布情報]

■再配布情報		
RIP	インタフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
BGP	インタフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
OSPF	インタフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: <input type="text"/> メトリックタイプ: type2
LDP	インタフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	RIP経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	BGP経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	OSPF経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

RIP

RIPに再配布する経路情報を設定します。

インタフェース経路情報

インタフェース経路情報を RIP に再配布する場合は、“再配布する”を選択します。

スタティック経路情報

スタティック経路情報を RIP に再配布する場合は、“再配布する”を選択します。

BGP 経路情報

BGP 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

OSPF 経路情報

OSPF 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

DNS 経路情報

DNS 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

BGP

BGP に再配布する経路情報を設定します。

インタフェース経路情報

インタフェース経路情報を BGP に再配布する場合は、“再配布する”を選択します。

スタティック経路情報

スタティック経路情報を BGP に再配布する場合は、“再配布する”を選択します。

こんな事に気をつけて

デフォルトルートを BGP で広報する場合は、BGP 相手情報でデフォルトルートを“広報する”に設定してください。

RIP 経路情報

RIP 経路情報を BGP に再配布する場合は、“再配布する”を選択します。

OSPF 経路情報

OSPF 経路情報を BGP に再配布する場合は、“再配布する”を選択します。

DNS 経路情報

DNS 経路情報を BGP に再配布する場合は、“再配布する”を選択します。

OSPF 広報

OSPF に再配布する経路情報を設定します。

インタフェース経路情報

インタフェース経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

スタティック経路情報

スタティック経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

RIP 経路情報

RIP 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

BGP 経路情報

BGP 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

DNS 経路情報

DNS 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を選択します。

LDP

LDP に再配布する経路情報を設定します。

インタフェース経路情報

インタフェース経路情報を LDP に再配布する場合は、“再配布する”を選択します。

スタティック経路情報

スタティック経路情報を LDP に再配布する場合は、“再配布する”を選択します。

RIP 経路情報

RIP 経路情報を LDP に再配布する場合は、“再配布する”を選択します。

BGP 経路情報

BGP 経路情報を LDP に再配布する場合は、“再配布する”を選択します。

OSPF 経路情報

OSPF 経路情報を LDP に再配布する場合は、“再配布する”を選択します。

◇優先度情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [ルーティングマネージャ情報] → [優先度情報]

優先度	
RIP	120
EBGP	20
IBGP	200
OSPF	110
DNS	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

優先度

複数のルーティングプロトコルで同じ経路情報を受信した場合や受信した経路情報がスタティック経路情報と同じだった場合、どの経路情報を優先的に使用するかを優先度で判断します。優先度を10進数を使用して、1～254の範囲で指定し、より小さい値が、より高い優先度を示します。

RIP

RIP 経路情報の優先度を指定します。省略時は、120が設定されます。

EBGP

EBGP 経路情報の優先度を指定します。省略時は、20が設定されます。

IBGP

IBGP 経路情報の優先度を指定します。省略時は、200が設定されます。

OSPF

OSPF 経路情報の優先度を指定します。省略時は、110が設定されます。

DNS

DNS 経路情報の優先度を指定します。省略時は、15が設定されます。

こんな事に気をつけて

- 優先度は、ほかのプロトコルやスタティック経路情報に設定されている値と同じ値は指定しないでください。
- スタティック経路情報の優先度の初期値は0です。

◇ ECMP 情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [ルーティングマネージャ情報]
→ [ECMP 情報]

ECMP情報	
ECMP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> ラウンドロビン方式 <input type="radio"/> ハッシュ方式
OSPF使用ECMP数	<input type="text" value="1"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ECMP 機能

IPv4ルーティング機能で、ECMP（Equal-Cost Multipath）を使用しない場合は、“使用しない”を選択します。また、ECMPを使用する場合は、ECMPの送出パス選択方式を、以下の2つから選択します。

- ラウンドロビン方式
ラウンドロビン方式とは、パケットごとに送出パスを順次切り替える方式です。すべてのトラフィックがほぼ均等に分散される利点がある一方、通信の連続性（それぞれの通信セッションが同じパスを利用する）とパケットの到達順は送信時から保証されないという欠点があります。
- ハッシュ方式
ハッシュ方式とは、送信元IPアドレス、あて先IPアドレスを元にハッシュ値を計算し、その値に従って送出パスを決定する方式です。通信の連続性および到達順はほぼ保証されますが、トラフィックが一部の通信パスにかたよる可能性があります。

OSPF 使用 ECMP 数

OSPFが生成した経路情報で、ECMPで扱う経路の最大値を1～4の範囲で指定します。ECMP機能を使用しない場合は、設定は無効となります。

18.3 RIP 関連

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [RIP 関連]

ルーティングプロトコル情報						
インタフェース 情報	ルーティングマ ネージャ情報	RIP 関連	BGP 関連	OSPF 関連	IPv6 ルーティ ングマネージャ 情報	IPv6 RIP 関連
RIP タイマ情報		RIP マルチパス情報		RIP 再配布フィルタリング情報		
RIP ユニキャスト送信情報		RIP 相手フィルタリング情報				

◇ RIP タイマ情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [RIP 関連] → [RIP タイマ情報]

RIP タイマ情報		
定期広報タイマ	間隔	30 秒
	ゆらぎ幅	50 %
有効期限タイマ		3 分
ガーベージタイマ		2 分

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

定期広報タイマ

間隔

RESPONSE パケットで定期的に経路を広報する間隔を指定します。初期値は 30 秒です。指定できる範囲は以下のとおりです。

有効範囲)
10 ~ 3600 秒
1 ~ 60 分
1 時間

ゆらぎ幅

定期広報タイマのゆらぎ幅を指定します。初期値は 50% です。指定できる範囲は以下のとおりです。

有効範囲) 0 ~ 50%

有効期限タイマ

RESPONSE パケットで更新されない経路情報の有効期限を指定します。初期値は 180 秒です。指定できる範囲は以下のとおりです。

有効範囲)
10 ~ 3600 秒
1 ~ 60 分
1 時間

ガーベージタイマ

有効期限が切れた場合に、その経路情報をメトリック 16 で広報する時間を指定します。初期値は 120 秒です。指定できる範囲は以下のとおりです。

有効範囲)
10 ~ 3600 秒
1 ~ 60 分
1 時間

◇ RIP マルチパス情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[RIP関連]→[RIPマルチパス情報]

■RIPマルチパス情報 ?

マルチパス数

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 | キャンセル

マルチパス数

RIPで受信可能な同じあて先への経路情報数を指定します。指定できる範囲は1～2です。

◇ RIP再配布フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[RIP関連]→[RIP再配布フィルタリング情報]

■RIP再配布フィルタリング情報 ?

※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	フィルタリング条件	操作
全削除			
<RIP再配布フィルタリング情報入力フィールド>			
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定	
フィルタリング条件	検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IPアドレス <input style="width: 100px;" type="text"/> アドレスマスク <input style="width: 100px;" type="text" value="0.0.0.0"/>	追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されているRIP再配布フィルタリング情報の定義が表示されています。処理は優先順位1から順に行われます。RIP再配布フィルタリング情報の定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

RIPに再配布する経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

対象とするフィルタリング条件を設定します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、再配布経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。


こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

◇ RIP ユニキャスト送信情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [RIP関連]
→ [RIP ユニキャスト送信情報]

■RIPユニキャスト送信情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 

送信先IPアドレス	送信RIPバージョン	操作
<input type="button" value="全削除"/>		
<RIPユニキャスト送信情報入力フィールド>		
送信先IPアドレス	<input type="text"/>	
送信RIPバージョン	<input type="radio"/> V1 <input checked="" type="radio"/> V2	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在、設定されている RIP ユニキャスト送信情報の定義が表示されています。RIP ユニキャスト送信情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

送信先IPアドレス

RIP をユニキャストで送信する送信先の IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

送信RIPバージョン

ユニキャストで送信する RIP のバージョンを選択します。

◇ RIP 相手フィルタリング情報

[操作] 「設定メニュー」 → ルータ設定 「ルーティングプロトコル情報」 → [RIP 関連]
→ [RIP 相手フィルタリング情報]

RIP 相手フィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	フィルタリング条件	操作
全削除			
<RIP 相手フィルタリング情報入力フィールド>			
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断		
フィルタリング条件	<input checked="" type="radio"/> すべて		
	<input type="radio"/> 相手側 IP アドレス指定 IP アドレス <input style="width: 100px;" type="text"/>		
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されている RIP 相手フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP 相手フィルタリング情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した相手情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

受信した RIP 情報の動作を以下の 2 つから選択します。

- 透過
フィルタリング条件と一致した場合に、相手ルータからの RIP パケットを透過します。
- 遮断
フィルタリング条件と一致した場合に、相手ルータからの RIP パケットを遮断します。

フィルタリング条件

対象とする相手情報を設定します。

- すべて
すべての相手ルータからの RIP パケットをフィルタリング対象とします。
- 相手側 IP アドレス指定
指定した RIP 送信元 IP アドレスをフィルタリング対象とします。
有効範囲)
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

こんな事に気をつけて

すべてのフィルタリング条件に一致しない相手ルータからの RIP パケットは遮断されます。

18.4 BGP 関連

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [BGP 関連]

ルーティングプロトコル情報						
インタフェース 情報	ルーティングマ ネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティ ングマネージャ 情報	IPv6 RIP関連
BGP情報		BGPネットワーク情報		BGP集約経路情報		
BGP相手情報		BGP再配布フィルタリング情報		VRF情報		
MPLS連携情報						

◇ BGP 情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [BGP 関連] → [BGP 情報]

■ BGP 情報	
BGP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
自AS番号	<input type="text"/>
自ID番号	<input type="text" value="0.0.0.0"/>
BGPネットワーク	<input type="checkbox"/> 常に広報する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

BGP 機能

BGP を使用する場合は、“使用する” を選択します。

こんな事に気をつけて

- バージョン4だけをサポートしています。
- BGP の認証機能はサポートしていません。
- 経路情報を、ルーティングテーブルの最大数または BGP エントリの最大数まで保持している場合、BGP で受信した経路情報は破棄されます。破棄された経路情報は、その後、ルーティングテーブルまたは BGP エントリに空きができた場合でも、ルーティングテーブルに反映されません。
- NAT 機能と併用できません。
- BGP 使用中に [設定反映] ボタンをクリックした場合、接続中のセッションが切断され、BGP が再起動されます。

自 AS 番号

本装置の属する AS 番号を 10 進数を使用して、1～65535 の範囲で指定します。自 AS 番号は省略できません。

自 ID 番号

BGP 接続で、自装置を唯一に示す ID を設定します。ID は、ほかルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。

設定を省略または 0.0.0.0 を指定した場合、以下のとおり ID を自動的に選択し、使用します。

- ループバックインタフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択し、使用します。
- ループバックインタフェースに追加 IP アドレスが設定されていない場合は、LAN インタフェース / リモートインタフェースに設定されている IPv4 アドレスの中からインタフェースの Up / Down の状態に関係なく最大の IPv4 アドレスを選択し、使用します。なお、リモートインタフェースの相手側 IP アドレスと LAN インタフェースのセカンダリ IP アドレスは選択対象となりません。

BGP ネットワーク

BGP ネットワークを、常に広報する場合に指定します。指定しない場合は、BGP ネットワーク情報で設定したネットワークが経路情報として有効な場合だけ BGP で広報します。指定した場合は、経路情報に関係なく BGP ネットワーク情報で設定した経路情報を BGP で広報します。

◇ BGP ネットワーク情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[BGP 関連]→[BGP ネットワーク情報]

■BGPネットワーク情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

あて先IPアドレス/マスク 操作

<BGPネットワーク情報入力フィールド>

あて先IPアドレス	<input type="text"/>
あて先アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在、設定されている BGP ネットワーク情報の定義が表示されています。BGP ネットワーク情報を設定することによって、必要な経路情報だけを選択して広報することができます。無効となった経路情報は広報されません。なお、BGP ネットワーク情報は、広報する経路情報を BGP に再配布する必要はありません。

BGP ネットワーク情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

「BGP 情報」で、「BGP ネットワーク」を常に広報すると設定することによって、「BGP ネットワーク情報」で設定した経路を経路情報に関係なく広報することができます。

あて先 IP アドレス / アドレスマスク

広報する経路情報のあて先 IP アドレスとアドレスマスクを指定します。

こんな事に気をつけて

BGP/MPLS VPN では、BGP ネットワーク情報は広報されません。

◇ BGP 集約経路情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[BGP 関連] → [BGP 集約経路情報]

■BGP集約経路情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

集約IPアドレス/マスク	集約対象経路	操作
全削除		
<BGP集約経路情報入力フィールド>		
集約IPアドレス	<input type="text"/>	
集約アドレスマスク	0 (0.0.0.0)	
集約対象経路	<input checked="" type="radio"/> 広報する <input type="radio"/> 広報しない	
		追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在、設定されている BGP 集約経路情報の定義が表示されています。BGP 集約情報を設定することによって、集約経路に含まれる経路情報があった場合に、集約経路情報を生成して広報することができます。集約経路に含まれる経路情報がすべて無効となった場合、集約経路情報は広報されません。なお、集約対象となるのは、BGP に再配布された経路情報、または、BGP ネットワーク情報で有効となっている経路情報です。

BGP 集約経路情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

集約 IP アドレス / アドレスマスク

集約経路情報の集約 IP アドレスとアドレスマスクを指定します。

集約対象経路

- 広報する
集約経路情報のほかに集約経路情報で集約される個々の経路の両方を広報します。
- 広報しない
集約経路情報を広報し、集約される個々の経路情報は広報しません。

こんな事に気をつけて

BGP/MPLS VPN では、BGP 集約経路情報の設定は無効となります。

◇ BGP 相手情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [BGP関連] → [BGP相手情報]

■BGP相手情報				
定義番号	IPアドレス	AS番号	Holdタイム	操作
<input type="button" value="追加"/> <input type="button" value="全削除"/>				

保存した情報は、設定反映後に有効になります。

現在、設定されている BGP の相手情報の定義が表示されています。BGP の相手情報の定義数 (BGP 最大接続数) は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

BGP/MPLS VPNを使用する場合、相手情報は1つだけ設定できます。

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [BGP関連] → [BGP相手情報] → [追加]

ルーティングプロトコル情報 - BGP相手情報(0)		
BGP相手基本情報	BGPフィルタリング情報	BGP拡張機能情報

[BGP相手基本情報]

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [BGP関連] → [BGP相手情報] → [追加] → [BGP相手基本情報]

■BGP相手基本情報	
相手側IPアドレス	<input type="text"/>
相手AS番号	<input type="text"/>
自側IPアドレス	<input type="text" value="0.0.0.0"/>
KeepAliveタイム	<input type="text" value="30"/> 秒
Holdタイム	<input type="text" value="90"/> 秒
MEDメトリック値	<input type="text" value="0"/>
ASパスプリベンド	<input type="text" value="0"/>
EBGP MULTI HOP	<input type="text" value="1"/>
LOCALPREF	<input type="text" value="100"/>
NEXTHOP SELF	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
デフォルトルート	<input checked="" type="radio"/> 広報しない <input type="radio"/> 広報する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

相手側 IP アドレス

BGP 接続を行う相手装置の IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

相手 AS 番号

BGP 接続する相手装置の AS 番号を 10 進数を使用して、1 ~ 65535 の範囲で指定します。指定する AS 番号は、自 AS 番号と異なる番号を指定します。IP-VPN 接続を行う場合は、自装置の属する AS 番号とは異なる値を設定する必要があります。BGP/MPLS VPN を使用する場合は、本装置と同じ AS 番号を設定します。

こんな事に気をつけて

- BGP/MPLS VPN を使用する場合、相手情報は 1 つだけ設定することができます。
- IP-VPN 接続と BGP/MPLS VPN は併用することはできません。

自側 IP アドレス

BGP セッションに特定のインタフェースアドレスを設定する場合に指定します。設定しない場合、BGP セッションで使用するインタフェースの IP アドレスが自動的に使用されます。BGP/MPLS VPN を使用する場合は、「装置情報」 - 「ループバック情報」に設定した IP アドレスを設定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

KeepAlive タイマ

相手装置との通信状態を確認するために送信する KeepAlive メッセージの送信間隔を指定します。Hold タイマ設定値の 1/3 以上を設定した場合、Hold タイマ設定値の 1/3 が設定されます。また、ネゴシエーションにより相手装置の Hold タイマ値が採用され、その 1/3 よりも大きな値を KeepAlive タイマで設定していた場合は、相手装置の Hold タイマ値の 1/3 を KeepAlive タイマ値として使用します。KeepAlive タイマ値は以下の範囲で指定します。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

Keep Alive タイマの値は、Hold タイマより小さい値を指定してください。

Hold タイマ

相手装置との間で、通信異常と判断する無通信状態の時間 (タイマ) を指定します。このタイマ値は、相手装置とのネゴシエーションで決まり、装置間でより小さな値が使用されます。Hold タイマ値は以下の範囲で指定します。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

3 ~ 65535 秒

こんな事に気をつけて

相手装置とのネゴシエーションによって、相手装置の Hold タイマ値が使用された場合は、その値の 3分の1の値が KeepAlive タイマとして使用されます。

MED メトリック値

EBGP で広報する経路情報に付加する MED メトリック値を 10 進数を使用して、0 ~ 4294967295 の範囲で指定します。

AS パスプリペンド

EBGP で広報する経路情報に付加する AS 番号の個数を 10 進数を使用して、0 ~ 4 の範囲で指定します。

EBGP MULTI HOP

相手装置と EBGP マルチホップ接続する場合の IP パケットの TTL 値を 10 進数を使用して、1～255 の範囲で指定します。BGP 相手装置とルータを経由して接続する場合は、経由するルータの数を EBGP MULTI HOP に加算して指定します。また、リモート側の IP アドレスに LAN 側の IP アドレスを設定している場合は EBGP MULTI HOP を 1 加算して指定します。

LOCALPREF

EBGP で受信する経路情報のローカル優先度を指定します。ローカル優先度は、IBGP で広報され、同じ自律システム内での優先経路選択に使用され、大きい値がより高い優先度を示します。初期値は 100 です。

NEXTHOP SELF

IBGP で広報する経路情報のネクストホップ情報を、自装置の IP アドレスに変更する場合は、“有効” を選択します。

デフォルトルート

BGP でデフォルトルートの広報を許可する場合は、“広報する” を選択します。

【BGPフィルタリング情報】

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [BGP関連] → [BGP相手情報] → [追加] → [BGPフィルタリング情報]

■BGPフィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	動作	方向	フィルタリング条件	MEDメトリック値	AS/パスプリベント	操作
全削除						
<BGPフィルタリング情報入力フィールド>						
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断					
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信					
フィルタリング条件	<input checked="" type="radio"/> AS番号指定 <div style="border: 1px solid gray; padding: 2px; width: 100px; margin-bottom: 5px;">AS番号</div> <input type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定 <div style="border: 1px solid gray; padding: 2px; margin-top: 5px;"> 検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致 </div> <div style="border: 1px solid gray; padding: 2px; margin-top: 5px;">IPアドレス</div> <div style="border: 1px solid gray; padding: 2px; margin-top: 5px;">アドレスマスク 0 (0.0.0.0)</div>					
MEDメトリック値	<input type="text" value="0"/>					
AS/パスプリベント	<input type="text" value="0"/>					
LOCALPREF	<input type="text" value="100"/>					
追加 キャンセル						

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されているBGPフィルタリング情報の定義が表示されています。処理は優先順位1から順に行われます。BGPフィルタリングの定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

BGP受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないBGP経路情報は遮断されます。

BGP送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないBGP経路情報は遮断されます。

こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- BGP/MPLS VPNで、BGPフィルタリング情報は無効となります。

動作

フィルタリング条件に該当する経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリング条件に該当するかどうかをチェックするタイミングを選択します。

- 受信
BGPパケット受信時にチェックします。
- 送信
BGPパケット送信時にチェックします。

フィルタリング条件

フィルタリング条件を選択します。

- AS番号指定
経由したAS番号をフィルタリングの対象とします。
AS番号は1～65535の範囲で指定します。
- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、BGP経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致したBGP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、BGP経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、そのBGP経路情報をフィルタリング対象とします。

MED メトリック値

フィルタリング条件で透過になったBGP経路情報のメトリック値を変更できます。MEDメトリック値は、0～4294967295の範囲で指定します。初期値は0です。

こんな事に気をつけて

- 送信時のフィルタを設定した場合、「BGP相手基本情報」のMEDメトリック値の設定は無効となります。
- MEDメトリック値の設定は、EBGP送信時のフィルタリングでだけ有効となります。受信時のフィルタリングでのMEDメトリック値の設定は無効となります。

AS パスプリペンド

フィルタリング結果で透過になったBGP経路情報に付加するAS番号の個数を変更できます。ASパスプリペンドは、0～4の範囲で指定します。初期値は0です。

こんな事に気をつけて

- 送信時のフィルタリングを設定した場合、「BGP相手基本情報」のASパスプリペンドの設定は無効となります。
- ASパスプリペンドの設定は、EBGP送信時のフィルタリングでだけ有効となります。受信時のフィルタリングに本設定を行っても、AS番号の追加は行われません。

LOCALPREF

フィルタリング条件で透過になった経路情報に対して、付加するLOCALPREFを10進数を使用して、0～4294967295の範囲で指定します。初期値は100です。

こんな事に気をつけて

- 受信時のフィルタリングを設定した場合、「BGP相手基本情報」のLOCALPREFは無効となります。
- LOCALPREFは、EBGP受信時のフィルタリングでだけ有効となります。送信時のフィルタリングに本設定を行っても、LOCALPREFの設定は無効となります。

【BGP 拡張機能情報】

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [BGP 関連] → [BGP 相手情報] → [追加] → [BGP 拡張機能情報]

■BGP拡張機能情報 ?

アドレスファミリー情報	IPv4ユニキャスト
エンフォースマルチホップ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

アドレスファミリー情報

BGP で使用するアドレスファミリーを選択します。

こんな事に気をつけて

BGP/MPLS VPNを使用する場合は、VPN IPv4ユニキャストを設定する必要があります。

エンフォースマルチホップ

エンフォースマルチホップを使用する場合は、“使用する”を選択します。“使用する”を選択した場合は、EBGPのマルチホップ環境で、TTL値が1のUPDATEパケットを受信しても破棄しません。

◇ BGP 再配布フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[BGP関連]
→[BGP再配布フィルタリング情報]

■BGP再配布フィルタリング情報
※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	フィルタリング条件	操作
全削除			
<BGP再配布フィルタリング情報入力フィールド>			
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断		
フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定		
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	
	IPアドレス	<input type="text"/>	
	アドレスマスク	0 (0.0.0.0)	
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されている BGP 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。BGP 再配布フィルタリング情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は遮断されます。
- BGP/MPLS VPN で、BGP 再配布フィルタリング情報は無効となります。

動作

BGP に再配布するフィルタリング条件の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

対象とするフィルタリング条件を設定します。

- すべて
すべての経路情報をフィルタリング対象とする場合に指定します。
- デフォルトルート
デフォルトルートをフィルタリング対象とする場合に指定します。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、再配布経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

◇ VRF 情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [BGP関連] → [VRF情報]

■ VRF情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

定義番号	ルート識別子		BGP/MPLS VPN広報		操作
	AS番号	識別番号	スタティック経路情報	インタフェース経路情報	
全削除					
<VRF情報入力フィールド>					
ルート識別子	AS番号	<input type="text"/>			
	識別番号	<input type="text"/>			
BGP/MPLS VPN広報	スタティック経路情報	<input type="radio"/> 再配布しない <input type="radio"/> 再配布する			
	インタフェース経路情報	<input type="radio"/> 再配布しない <input type="radio"/> 再配布する			
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

BGP/MPLS VPNは、VPN単位にVRF情報を持ち、経路情報を別々に管理します。

VRF情報の定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

ルート識別子

BGP/MPLS VPNで使用するルート識別子をAS番号とIDで指定します。AS番号は自装置の属するAS番号を10進数を使用して1～65535の範囲で設定します。識別番号は、VPNを一意に示すIDを10進数を使用して0～4294967295の範囲で設定します。

こんな事に気をつけて

ほかのVRF情報で設定されている識別番号と同じ値を設定することはできません。

BGP/MPLS VPN 広報

BGP/MPLS VPNでBGPに再配布する経路情報を選択します。BGP/MPLS VPNスタティック経路の経路情報をBGPに再配布する場合は、“再配布する”を選択します。

スタティック経路情報

本装置に設定されているBGP/MPLS VPNスタティック経路情報をBGPに再配布するかどうかを選択します。

インタフェース経路情報

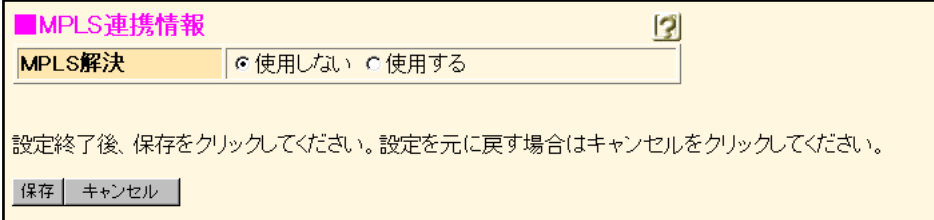
VPNで使用するインタフェースの経路情報をBGPに再配布する場合は、“再配布する”を選択します。


こんな事に気をつけて

「BGP/MPLS VPN 広報」－「スタティック経路」の設定で“再配布する”を選択し、また、スタティック経路情報と同じあて先の経路情報をBGP/MPLS VPNで受信した場合、BGP/MPLS VPNスタティック経路情報を優先します。

◇ MPLS 連携情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [MPLS 連携情報]



■MPLS連携情報 

MPLS解決 使用しない 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

MPLS 解決

MPLS 解決を使用する場合は、“使用する”を選択します。“使用する”を選択した場合、BGPで受信した経路の解決にMPLSを使用し、MPLSのラベルパスにマッピングします。MPLSトンネル接続上でBGPを用いる場合は、“使用しない”を選択してください。

18.5 OSPF 関連

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連]

ルーティングプロトコル情報		
ルーティングマネージャ情報	RIP関連	OSPF関連
ルータID情報	OSPFエリア情報	AS境界ルータ情報
AS外部経路集約情報	OSPF再配布フィルタリング情報	

◇ルータID 情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [ルータ ID 情報]

ルータID情報 ?

ルータID

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存

ルータID

OSPF 接続で、自装置を唯一に示す ID を設定します。ID は、ほかルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。

設定を省略または 0.0.0.0 を指定した場合、以下のとおり ID を自動的に選択し、使用します。

- ループバックインタフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択し、使用します。
- ループバックインタフェースに追加 IP アドレスが設定されていない場合は、LAN インタフェース／リモートインタフェースに設定されている IPv4 アドレスの中からインタフェースの Up / Down の状態に関係なく最大の IPv4 アドレスを選択し、使用します。なお、リモートインタフェースの相手側 IP アドレスと LAN インタフェースのセカンダリ IP アドレスは選択対象となりません。

こんな事に気をつけて

OSPF ルータ ID は、他装置と重複しないように指定してください。正しくルーティングできない場合があります。

◇ OSPF エリア情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [OSPF エリア情報]

■OSPFエリア情報				
エリア定義番号	エリアID	エリア種別	コスト値	操作
<input type="button" value="追加"/> <input type="button" value="全削除"/>				
保存した情報は、設定反映後に有効になります。				

現在、この装置に設定されている OSPF エリア情報の定義が表示されています。エリア定義数は、BR500S 仕様一覧 [2.3 システム最大値一覧] (P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

[OSPF エリア情報]

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [OSPF エリア情報] → [追加]

ルーティングプロトコル情報 - OSPF エリア情報 (0)		
OSPF エリア基本情報	経路集約情報	サマリLSA入出力可否情報
バーチャルリンク情報		

[OSPF エリア基本情報]

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [OSPF エリア情報] → [追加] → [OSPF エリア基本情報]

■OSPFエリア基本情報	
エリアID	<input type="text"/>
エリア種別	<input checked="" type="radio"/> 通常エリア <input type="radio"/> スタブエリア <input type="radio"/> 準スタブエリア
デフォルトルートコスト値	<input type="text" value="1"/> <small>※ エリア種別がスタブエリアもしくは準スタブエリアの場合のみ有効です。</small>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

エリアID

エリアIDをアドレス（ドット形式）または10進数を使用して指定します。

こんな事に気をつけて

OSPFを利用する場合は、エリアIDを必ず設定してください。

エリア種別

バックボーンエリア以外のエリアに対し、エリア種別を選択します。

こんな事に気をつけて

バックボーンエリアにスタブエリアまたは準スタブエリアを設定した場合も、通常エリアとして動作します。

デフォルトルートコスト値

エリア境界ルータがスタブエリアまたは準スタブエリアに広報するデフォルトルートのコストを0～16777215の範囲で指定します。

【経路集約情報】

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[OSPF 関連]→[OSPF エリア情報]→[追加]→[経路集約情報]

■経路集約情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

集約経路	操作
全削除	
<経路集約情報入力フィールド>	
ネットワークアドレス	<input type="text"/>
ネットマスク	<input type="text" value="0 (0.0.0.0)"/>
コスト	<input type="text"/>
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、この装置に設定されている経路集約情報の定義が表示されています。1 エリアでの経路集約情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワークアドレス

エリア内部経路で集約するネットワークアドレスを指定します。

ネットマスク

ネットマスクを選択します。

コスト

集約経路情報のコストを10進数を使用して0～16777215の範囲で指定します。省略時は、集約される経路情報の中でもっとも大きい値のコストが使用されます。

[サマリ LSA 入力可否情報]

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [OSPF エリア情報]
→ [追加] → [サマリ LSA 入力可否情報]

■サマリLSA入出力可否情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	方向	対象経路情報	操作
全削除				
<サマリLSA入出力可否情報入力フィールド>				
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断			
方向	<input checked="" type="radio"/> 入力 <input type="radio"/> 出力			
対象経路情報	<input checked="" type="radio"/> すべて			
	<input type="radio"/> 経路情報指定			
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致		
	IPアドレス	<input type="text"/>		
	アドレスマスク	<input type="text" value="0.0.0.0"/>		
追加 キャンセル				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているサマリ LSA 入出力可否定義の一覧です。処理は優先順位 1 から順に行われます。サマリ LSA 入出力可否の定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

サマリ LSA の入力時は、優先順位の高い定義から順に入力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。

また、入力方向のすべての対象経路情報に一致しないサマリ LSA 経路情報は遮断されます。サマリ LSA の出力時は、優先順位の高い定義から順に出力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。また、出力方向のすべての対象経路情報に一致しないサマリ LSA 経路情報は遮断されます。

動作

対象経路情報に該当するサマリ LSA の動作を以下の 2 つから選択します。

- 透過
対象経路情報と一致した場合にサマリ LSA をエリア間で透過します。
- 遮断
対象経路情報と一致した場合にサマリ LSA をエリア間で遮断します。

方向

サマリ LSA 入出力可否の判断を行うタイミングを選択します。

- 入力
サマリ入出力可否の判断を、ほかのエリアからの入力時に行う場合にチェックします。
- 出力
サマリ入出力可否の判断を、ほかのエリアからの出力時に行う場合にチェックします。

対象経路情報

入力可否の対象となる経路情報を選択します。

- **すべて**
すべてのサマリLSAを入出力可否情報の対象とします。
- **経路情報指定**
入出力可否の対象とする経路情報を指定します。
経路情報を指定するときは、サマリLSA経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。“完全に一致”を選択すると、指定したIPアドレスとアドレスマスクが完全に一致したサマリLSA経路情報を入出力可否の対象とします。
“マスクした結果が一致”を選択すると、指定したIPアドレスと、サマリLSA経路情報を、指定したアドレスマスクでマスクした結果が一致した場合、そのサマリLSA経路情報を入出力可否の対象とします。

こんな事に気をつけて

「OSPF関連集約経路情報」で設定している集約経路情報は、そのエリアからの出力時には遮断できません。
以下の経路情報は、サマリLSA入出力可否の対象となりません。

- 各エリアのAS境界ルータから注入されたAS外部経路
 - スタブエリアおよび準スタブエリアのエリア境界ルータが注入するデフォルト経路
 - type4のサマリLSA
-

[バーチャルリンク情報]

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [OSPF エリア情報] → [追加] → [バーチャルリンク情報]

■バーチャルリンク情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

接続先ルータ ID	Hello/パケット送信間隔	隣接ルータ停止確認間隔	認証方式	操作

全削除

<バーチャルリンク情報入力フィールド>

接続先ルータID

Hello/パケット送信間隔 秒

隣接ルータ停止確認間隔 秒

パケット再送間隔 秒

LSU/パケット送信遅延時間 秒

認証方式

認証を行わない

テキスト認証

鍵種別 文字列 16進数

認証鍵

MD5認証

認証鍵ID

認証鍵

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、この装置に設定されているバーチャルリンク情報の定義が表示されています。バーチャルリンク情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

接続先ルータ ID

接続先ルータの OSPF ルータ ID を指定します。

Hello パケット送信間隔

バーチャルリンク接続先との OSPF 隣接関係の維持に使用する Hello パケットの送信間隔を指定します。奨励値は“10 秒”です。

有効範囲)

1～18 時間

1～1092 分

1～65535 秒

こんな事に気をつけて

バーチャルリンク接続先と同じ Hello パケット送信間隔を指定してください。異なる値を指定するとルーティングを行うことができません。

隣接ルータ停止確認間隔

バーチャルリンクでの OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。Hello パケット送信間隔より大きな値を設定する必要があります。Hello パケット送信間隔の 4 倍をお勧めします。通常は“40 秒”を指定します。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

こんな事に気をつけて

バーチャルリンク接続先と同じ隣接ルータ停止確認間隔を指定してください。異なる値を指定するとルーティングを行うことができません。

パケット再送間隔

バーチャルリンクで OSPF パケットを再送する間隔を指定します。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。

有効範囲)
1～18 時間
1～1092 分
1～65535 秒

こんな事に気をつけて

一般的な装置では、LSU を作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

認証方式

パケットに対する認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が“文字列”の場合は、8 文字以内で指定します。鍵種別が“16 進数”の場合は、16 進数を使用して 16 桁以内で指定します。16 桁未満の鍵を指定した場合は、16 桁になるまで 0x0 でパディングされます。

MD5 認証鍵 ID

バーチャルリンクの MD5 認証で使用する鍵 ID を 1～255 の範囲で指定します。

MD5 認証鍵

バーチャルリンクの MD5 認証で使用する鍵を指定します。16 文字以内で指定します。

◇ AS境界ルータ情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[OSPF 関連] →[AS境界ルータ情報]

■AS境界ルータ情報	
デフォルトルート	<input checked="" type="radio"/> 広報しない <input type="radio"/> 広報する <input type="radio"/> AS外部経路に存在する場合に広報する
メトリック値	<input type="text" value="10"/>
外部メトリック種別	<input type="text" value="type2"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

デフォルトルート

デフォルトルートを広報する際の条件を選択します。

メトリック値

デフォルトルートのメトリック値を0～16777214の範囲で指定します。


外部メトリック種別


外部メトリックの種別を選択します。

◇ AS 外部経路集約情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[OSPF 関連]→[AS 外部経路集約情報]

■AS 外部経路集約情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 

ネットワークアドレス	ネットマスク	操作
全削除		
<AS 外部経路集約情報入力フィールド>		
ネットワークアドレス	<input type="text"/>	
ネットマスク	0 (0.0.0.0) 	
		追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている AS 外部経路集約情報の定義が表示されています。処理は、優先順位 1 から順に行われます。AS 外部経路集約情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワークアドレス

AS 外部経路で集約するネットワークアドレスを指定します。

ネットマスク

ネットマスクを選択します。

◇ OSPF 再配布フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連]
→ [OSPF 再配布フィルタリング情報]

■OSPF再配布フィルタリング情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。

優先順位	動作	フィルタリング条件	操作
全削除			
<OSPF再配布フィルタリング情報入力フィールド>			
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断		
フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定		
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	
	IPアドレス	<input type="text"/> アドレスマスク <input type="text" value="0.0.0.0"/>	
メトリック	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する		
	メトリック値	<input type="text"/> メトリックタイプ <input type="text" value="type2"/>	
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、このネットワークに設定されている OSPF 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。OSPF 再配布フィルタリング情報の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない再配布経路情報は遮断されます。

動作

OSPF に再配布する再配布経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

対象とするフィルタリング条件を設定します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できません。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致” または、“マスクした結果が一致” を選択します。

検索条件

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、再配布経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

デフォルトルートをOSPFに再配布する場合は、「AS境界ルータ情報」の設定も必要となります。

メトリック

経路情報をOSPFに再配布する際のメトリック値、メトリックタイプを指定する場合は、“指定する”を選択します。“指定しない”を選択した場合は、「ルーティングマネージャ情報」で設定したメトリック値、および、メトリックタイプとなります。なお、本設定は動作に“透過”を設定した場合に有効です。

メトリック値

OSPFに再配布する際のメトリック値を0～16777214の範囲で指定します。

こんな事に気をつけて

動作に遮断を指定した場合、メトリック値は指定できません。

メトリックタイプ

OSPFに再配布する際のメトリックタイプを選択します。

18.6 IPv6 ルーティングマネージャ情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [IPv6ルーティングマネージャ情報]

ルーティングプロトコル情報						
インタフェース 情報	ルーティングマ ネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティ ングマネージャ 情報	IPv6 RIP関連
IPv6再配布情報		IPv6優先度情報				

◇ IPv6 再配布情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [IPv6ルーティングマネージャ情報]
→ [IPv6再配布情報]

IPv6再配布情報		?
RIP	インタフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
	DHCP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

RIP

インタフェース経路情報

インタフェース経路情報を RIP に再配布するかどうかを選択します。

スタティック経路情報

スタティック経路情報を RIP に再配布するかどうかを選択します。

DNS経路情報

DNS経路情報を RIP に再配布するかどうかを選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

DHCP経路情報

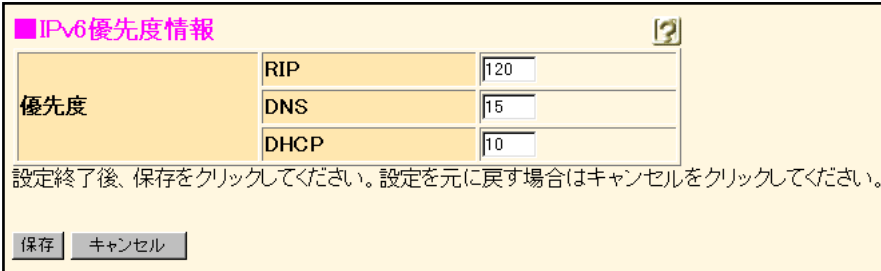
DHCP経路情報を RIP に再配布するかどうかを選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

◇ IPv6 優先度情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [IPv6ルーティングマネージャ情報] → [IPv6 優先度情報]



優先度	プロトコル	値
	RIP	120
	DNS	15
	DHCP	10

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

優先度

複数のルーティングプロトコルで同じ経路情報を受信した場合や受信した経路情報がスタティック経路情報と同じだった場合、どの経路情報を優先的に使用するかを優先度で判断します。

優先度は、10進数を使用して1～254で指定します。より小さい値が、より高い優先度を示します。

RIP

RIP 経路情報の優先度を指定します。省略時は、120が設定されます。

DNS

DNS 経路情報の優先度を指定します。省略時は、15が設定されます。

DHCP

DHCP 経路情報の優先度を指定します。省略時は、10が設定されます。

こんな事に気をつけて

- 優先度は、ほかのプロトコルやスタティック経路情報に設定されている値と同じ値は指定しないでください。
- スタティック経路情報の優先度の初期値は0です。

18.7 IPv6 RIP 関連

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [IPv6 RIP 関連]

ルーティングプロトコル情報						
インタフェース 情報	ルーティングマ ネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティ ングマネージャ 情報	IPv6 RIP関連
IPv6 RIPタイマ情報		IPv6 RIPマルチパス情報		IPv6 RIP再配布フィルタリング情報		

◇ IPv6 RIP タイマ情報

[操作] 「設定メニュー」 → ルータ設定「ルーティングプロトコル情報」 → [IPv6 RIP 関連]
→ [IPv6 RIP タイマ情報]

■ IPv6 RIPタイマ情報 ?

定期広報タイマ	30	秒
有効期限タイマ	3	分
ガーベージタイマ	2	分

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

定期広報タイマ

RESPONSE パケットで定期的に経路を広報する間隔を指定します。初期値は30秒です。

有効範囲)
10～3600秒
1～60分
1時間

ガーベージタイマ

有効期限が切れた場合に、その経路情報をメトリック16で広報する時間を指定します。初期値は120秒です。

有効範囲)
10～3600秒
1～60分
1時間

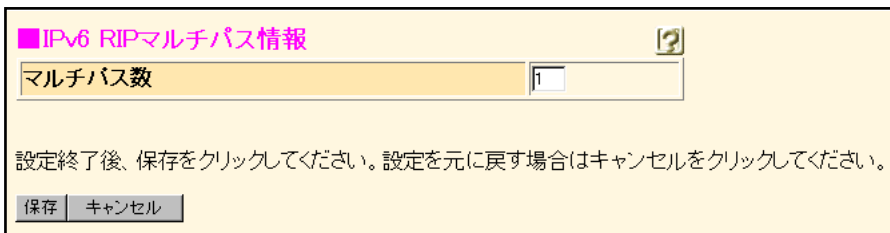
有効期限タイマ

RESPONSE パケットで更新されない経路情報の有効期限を指定します。初期値は180秒です。

有効範囲)
10～3600秒
1～60分
1時間

◇ IPv6 RIP マルチパス情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連]
→ [IPv6 RIP マルチパス情報]

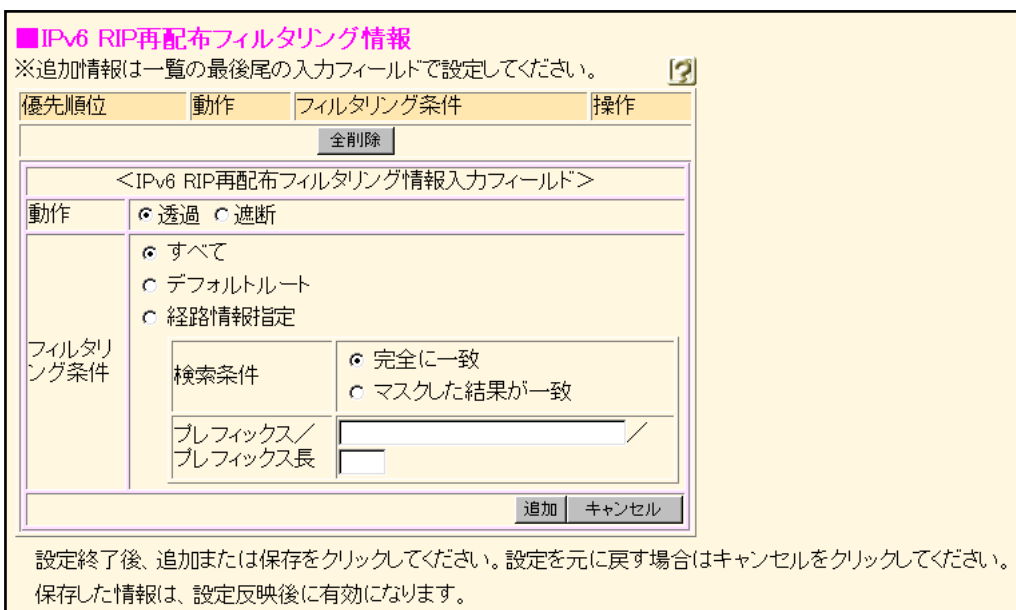


マルチパス数

RIPで受信可能な同じあて先への経路情報数を指定します。指定できる範囲は1～2です。初期値は1です。

◇ IPv6 RIP 再配布フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連]
→ [IPv6 RIP 再配布フィルタリング情報]



現在、設定されているRIP再配布フィルタリング情報の定義が表示されています。処理は優先順位1から順に行われます。RIP再配布フィルタリング情報の定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

RIPに再配布する経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

対象とするフィルタリング条件を設定します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したプレフィックスと、再配布経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

19 マルチキャスト情報

[操作] 「設定メニュー」→ルータ設定「マルチキャスト情報」

マルチキャスト情報	
IPマルチキャスト情報	IPマルチキャストスタティック経路情報

19.1 IPマルチキャスト情報

[操作] 「設定メニュー」→ルータ設定「マルチキャスト情報」→[IPマルチキャスト情報]

IPマルチキャスト情報 ?

PIM-SM	RP候補	<input checked="" type="radio"/> しない <input type="radio"/> する IPアドレス <input type="text" value="0.0.0.0"/> プライオリティ <input type="text" value="0"/>
	BSR候補	<input checked="" type="radio"/> しない <input type="radio"/> する IPアドレス <input type="text" value="0.0.0.0"/> プライオリティ <input type="text" value="0"/>
	SPTへの経路変更	<input type="radio"/> しない <input checked="" type="radio"/> 即時 <input type="radio"/> 転送速度 <input type="text"/> Kbps
<input checked="" type="radio"/> register <input type="radio"/> チェックサム		<input checked="" type="radio"/> ヘッダ部 <input type="radio"/> パケット全体

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

PIM-SM

RP候補

ランデブー・ポイント (RP) の設定です。マルチキャスト・ルーティングプロトコルに PIM-SM を利用する場合は、RPとして動作するルータがネットワーク上に1台以上必要です。RPの設定は、1台のルータだけで行っても、複数のルータで行っても構いません。トラフィックを分散する場合は、複数台のルータでRPの設定を行っておきます。

IPアドレス

RPとして動作するインタフェースのIPアドレスを指定します。0.0.0.0を指定または指定しない場合は、RPとして動作できるインタフェースを自動で検索します。

有効範囲)

1.0.0.1～126.255.255.254
 128.0.0.1～191.255.255.254
 192.0.0.1～223.255.255.254

プライオリティ

RPのプライオリティ情報を10進数を使用して、0～255の範囲で指定します。数が小さいほど優先度は高くなります。初期値は0です。

BSR 候補

ブート・ストラップ・ルータ (BSR) の設定です。マルチキャスト・ルーティングプロトコルに PIM-SM を利用する場合は、BSR として動作するルータがネットワーク上に必要です。BSR の設定は、1 台のルータだけで行っても、複数のルータで行っても構いません。障害に強いネットワークを構成する場合は、複数台のルータで BSR の設定を行っておきます。

IP アドレス

BSR として動作するインタフェースの IP アドレスを指定します。0.0.0.0 を指定または指定しない場合は、BSR として動作できるインタフェースを自動で検索します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

プライオリティ

BSR のプライオリティ情報を 10 進数を使用して、0 ~ 255 の範囲で指定します。数が大きいほど優先度は高くなります。初期値は 0 です。

SPT への経路変更

SPT (Shortest Path Tree) への経路変更を選択します。SPT の設定は、マルチキャスト・パケットを受信者となる last hop router 上で行います。

即時

SPT への経路変更を転送速度に関係なく即時行う場合に選択します。通常は、この設定を選択します。

転送速度

転送速度によって SPT への経路変更を行う場合に選択します。マルチキャスト・トラフィックがしきい値となる転送速度を上回ったときに SPT が切り替わります。1 ~ 100000Kbps または 1 ~ 100Mbps の範囲で指定します。

register

PIM Register パケットを設定します。マルチキャスト・パケットを送信するルータ上で行います。

チェックサム

PIM Register パケットの送信時のチェックサムの計算方法を設定することができます。

PIM Register パケットのチェックサムの計算範囲は、RFC2362 ではヘッダ部だけで計算するように定義されていますが、一部のルータはパケット全体で計算します。このようなルータが RP を行う場合は、PIM Register パケットが受信されない可能性があるため、チェックサムの計算範囲を“パケット全体”に変更する必要があります。

本装置は PIM Register パケットの受信時に、ヘッダ部 (RFC2362 準拠) とパケット全体の 2 つの方法で計算するため、本装置が RP を行う場合は、どちらの計算方法のパケットを受信しても問題はありません。

19.2 IP マルチキャストスタティック経路情報

[操作] 「設定メニュー」→ルータ設定「マルチキャスト情報」→[IP マルチキャストスタティック経路情報]

■IPマルチキャストスタティック経路情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

定義番号	配信元ホストアドレス	操作
	マルチキャストグループアドレス	
	入力インタフェース	
	出力インタフェース	

<IPマルチキャストスタティック経路情報入力フィールド>

配信元ホストアドレス	<input type="text"/>
マルチキャストグループアドレス	<input type="text"/>
入力インタフェース	<input type="text" value="LAN0"/>
出力インタフェース	<input type="text"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。

現在、設定されている IP マルチキャストスタティック経路情報の定義が表示されています。IP マルチキャストスタティック経路の定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

配信元ホストアドレス

配信元ホストを IPv4 アドレスで指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

出力インタフェース

出力インタフェースを指定します。LAN0 ~ max または、rmt0 ~ max で指定してください。複数指定する場合は、“;” で区切ります。範囲指定の場合は“-” で区切ります。出力インタフェースは 20 個まで設定できます。

マルチキャストグループアドレス

マルチキャストグループアドレスを 224.0.1.0 ~ 239.255.255.255 の範囲の IPv4 アドレスで指定してください。

入力インタフェース

入力インタフェースを選択してください。

20 UPnP 情報

[操作] 「設定メニュー」 → ルータ設定 「UPnP 情報」

UPnP 情報
基本情報

20.1 基本情報

[操作] 「設定メニュー」 → ルータ設定 「UPnP 情報」 → [基本情報]

■ 基本情報 ?

UPnP機能 使用しない 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

UPnP 機能

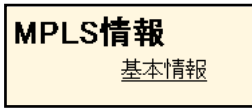
UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合は“使用する”を選択します。

こんな事に気をつけて

- UPnP 対応装置のマニュアルを参照して、UPnP 機能を使用するように設定されていることを確認してください。
- UPnP 対応装置は DHCP 機能を利用することで簡単に使用できるようになっていますので、本装置の DHCP サーバ機能を使用することをおすすめします。
- マルチ NAT 機能を使用しないインタフェースに UPnP 対応装置を接続してください。マルチ NAT 機能を使用するインタフェースへの通信に対して VoIP NAT トラバースル機能が動作します。

21 MPLS 情報

[操作] 「設定メニュー」 → ルータ設定 「MPLS 情報」



21.1 基本情報

[操作] 「設定メニュー」 → ルータ設定 「MPLS 情報」 → 「基本情報」

■基本情報 ?

MPLS TTL伝達	<input type="radio"/> しない <input checked="" type="radio"/> する
router ID	<input type="text"/>
LDP 制御方式	<input checked="" type="radio"/> independent <input type="radio"/> ordered
IPv4 Transport アドレス	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

MPLS TTL 伝達

MPLS から IP、または IP から MPLS にパケットを交換するときに、TTL の情報を伝達する場合は、“する” を選択します。

LDP

router ID

使用するルータを特定する ID を有効な IPv4 アドレスで指定します。0.0.0.0 の場合、LDP 機能は動作しません。

制御方式

LDP の制御方式を選択します。

IPv4 Transport アドレス

LDP がピアとの通信に使用する送信元 IPv4 アドレスを指定します。装置のループバックインタフェースに設定した IPv4 アドレスを指定します。0.0.0.0 を指定した場合は、LDP が動作するインタフェースの IPv4 アドレスが IPv4 Transport Address として使用されます。省略時は、0.0.0.0 が設定されます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

22 ブリッジ情報

[操作] 「設定メニュー」→ルータ設定「ブリッジ情報」

ブリッジ情報

ブリッジグループ情報

22.1 ブリッジグループ情報

[操作] 「設定メニュー」→ルータ設定「ブリッジ情報」→ [ブリッジグループ情報]

■ブリッジグループ情報				
グループ識別子	学習テーブル生存時間	IPv4ルーティング機能	IPv6ルーティング機能	操作
0	5分	使用する	使用する	修正 削除
1	5分	使用する	使用する	修正 削除
2	5分	使用する	使用する	修正 削除
3	5分	使用する	使用する	修正 削除
4	5分	使用する	使用する	修正 削除
5	5分	使用する	使用する	修正 削除
6	5分	使用する	使用する	修正 削除
7	5分	使用する	使用する	修正 削除
8	5分	使用する	使用する	修正 削除
9	5分	使用する	使用する	修正 削除
10	5分	使用する	使用する	修正 削除
11	5分	使用する	使用する	修正 削除
12	5分	使用する	使用する	修正 削除
13	5分	使用する	使用する	修正 削除
14	5分	使用する	使用する	修正 削除
15	5分	使用する	使用する	修正 削除
16	5分	使用する	使用する	修正 削除
17	5分	使用する	使用する	修正 削除
18	5分	使用する	使用する	修正 削除

19	5分	使用する	使用する	修正 削除
全削除				
保存した情報は、設定反映後に有効になります。				

ブリッジグループ情報設定項目はブリッジ機能を使用する場合だけ有効です。ブリッジグループ情報の定義は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

◇ブリッジグループ情報（グループ識別子0の場合）

[操作] 「設定メニュー」→ルータ設定「ブリッジ情報」→[ブリッジグループ情報]→「グループ識別子0」[修正]

<ブリッジグループ情報入力フィールド>		
学習テーブル生存時間	5 分	
IPv4ルーティング機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
	転送ポリシー <input checked="" type="radio"/> strict <input type="radio"/> loose	
IPv6ルーティング機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
	転送ポリシー <input checked="" type="radio"/> strict <input type="radio"/> loose	
リモートインタフェース間ブリッジ	<input type="radio"/> する <input checked="" type="radio"/> しない	
STP	ブリッジの優先度	32768
	ブリッジのHello待ち時間	20 秒
	ブリッジのHello送出間隔	2 秒
	フォワーディング遅延時間	15 秒
保存 キャンセル 一覧へ戻る		

学習テーブル生存時間

グループ識別子0で設定した学習テーブル生存時間が全グループで使用されます。初期値は5分です。

有効範囲)

1～11日

1～277時間

1～16666分

10～1000000秒

IPv4 ルーティング機能

IPv4をルーティングによって制御する場合は、“使用する”を選択します。

転送ポリシー

IPv4ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送するかどうかを選択します。

受信フレームのあて先MACアドレスが受信インタフェースあてであるが、あて先IPアドレスが受信インタフェースあてではない場合、IPv4ブリッジ動作時に、グループ内からグループ外へルーティングによって転送します。

IPv4をルーティングするインタフェースで受信したパケットが、ルーティングによってIPv4をブリッジするインタフェースへ出力される場合、IPv4ブリッジ動作時に、グループ外からグループ内へルーティングによって転送します。

strictを選択した場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

- strict
IPv4ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送しません。
- loose
IPv4ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送します。

IPv6 ルーティング機能

IPv6をルーティングによって制御する場合は、“使用する”を選択します。

転送ポリシー

IPv6ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送するかどうかを選択します。

受信フレームのあて先MACアドレスが受信インタフェースあてであるが、あて先IPアドレスが受信インタフェースあてではない場合、IPv6ブリッジ動作時に、グループ内からグループ外へルーティングによって転送します。

IPv6をルーティングするインタフェースで受信したパケットが、ルーティングによってIPv6をブリッジするインタフェースへ出力される場合、IPv6ブリッジ動作時に、グループ外からグループ内へルーティングによって転送します。

strictを選択した場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

- strict
IPv6ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送しません。
- loose
IPv6ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送します。

リモートインタフェース間ブリッジ

リモートインタフェースから受信したフレームを別のリモートインタフェースへブリッジする場合は、“する”を選択します。

STP

ブリッジの優先度

ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を0～65535の範囲で指定します。ブリッジの優先度は、値の小さい方がより優先となります。この設定項目はSTPを使用する場合だけ有効です。

ブリッジのHello待ち時間

ルートブリッジまたは代表ブリッジから送出される構成情報BPDUの待ち時間を6～40秒の範囲で指定します。この設定項目はSTPを使用する場合だけ有効です。

ブリッジのHello送出間隔

ルートブリッジになったときに送出する構成情報BPDUの送出間隔を1～10秒の範囲で指定します。この設定項目はSTPを使用する場合および本装置がルートブリッジとして動作する場合だけ有効です。

フォワーディング遅延時間

構成情報BPDUが、一番時間がかかる経路に届く時間を設定します。フォワーディング遅延時間を4～30秒の範囲で指定します。この設定項目はSTPを使用する場合および本装置がルートブリッジとして動作する場合だけ有効です。

◇ブリッジグループ情報（グループ識別子1～7の場合）

[操作] 「設定メニュー」→ルータ設定「ブリッジ情報」→[ブリッジグループ情報]→[グループ識別子1] [修正]

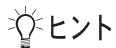
<ブリッジグループ情報入力フィールド>	
学習テーブル生存時間	5分
1 IPv4ルーティング機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 転送ポリシー <input checked="" type="radio"/> strict <input type="radio"/> loose
	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 転送ポリシー <input checked="" type="radio"/> strict <input type="radio"/> loose
リモートインタフェース間ブリッジ	<input checked="" type="radio"/> する <input type="radio"/> しない
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>	

「学習テーブル生存時間」、「IPv4ルーティング機能」、「IPv6ルーティング機能」および「リモートインタフェース間ブリッジ」は「ブリッジグループ情報（グループ識別子0の場合）」を参照してください。

23 ProxyDNS 情報／URL フィルタ情報

[操作] 「設定メニュー」→ルータ設定「ProxyDNS 情報 URL フィルタ情報」

ProxyDNS情報／URLフィルタ情報	
順引き情報	逆引き情報
このページではProxyDNSとURLフィルタの設定ができます。URLフィルタは順引き情報で設定します。	



ヒント

◆ ProxyDNS には以下の機能があります。

- DNS サーバの自動切り替え機能

パソコンに本装置のIPアドレスをDNSサーバとして登録しておく、接続先によって問い合わせるDNSサーバを自動的に切り替えます。

- DNS サーバ機能

ホストデータベース情報にホスト名とIPアドレスのペアを登録しておく、ProxyDNSは該当ホスト名へのアクセスを登録されたIPアドレスへのアクセスとして切り替えます。

- URL フィルタ機能

特定のドメイン名（範囲指定も可）へのアクセスを禁止することができます。この機能は順引き情報設定で設定します。

- DNS 問い合わせタイプフィルタ機能

送信元IPアドレス範囲から送信される特定の問い合わせタイプのDNSパケットを破棄することができます。この機能は順引き情報設定で設定します。

23.1 順引き情報

[操作] 「設定メニュー」→ルータ設定「ProxyDNS 情報 URL フィルタ情報」→ [順引き情報]

■ 順引き情報

※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	ドメイン名	動作	DNSサーバアドレス/ ネットワーク名	操作
	タイプ		ネットワーク名	
	送信元IPアドレス		経路自動作成	

< 順引き情報入力フィールド >

ドメイン名	<input type="text"/>
タイプ	すべて (番号指定 <input type="text"/> “その他”を選択時のみ有効です。)
送信元IPアドレス	<input type="text"/> <input type="checkbox"/> ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	<input type="radio"/> 廃棄する <input type="radio"/> 接続先のDNSサーバへ問い合わせる ネットワーク名 <input type="text" value="rmt0"/>
	<input type="radio"/> 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる ネットワーク名 <input type="text" value="rmt0"/>
	<input type="radio"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する
	<input type="radio"/> 設定したDNSサーバへ問い合わせる DNSサーバアドレス <input type="text"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

順引き情報はドメイン名によりDNSサーバを切り替える範囲を指定する場合、特定のドメイン名へのアクセスを禁止する場合、送信元IPアドレス範囲からの特定の問い合わせタイプのDNSパケットを破棄する場合など、ドメイン名・問い合わせタイプ・送信元IPアドレスの組み合わせによりいろいろな使い方ができます。定義数は、BR500S仕様一覧「[2.3 システム最大値一覧](#)」(P.19)を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

ドメイン名

対象とするドメイン名の範囲を80文字以内で指定します。ただし、以下のように、“*” および “?” はワイルドカードとして使用されるため、ドメイン名には使用できません。なお、ドメイン名のチェックには大文字／小文字の区別はありません。

“*” : 0文字以上の任意の文字に一致する

“?” : 1文字の任意文字に一致する

記述例)

条件	一致
www.*.com	www.testa.com、 www.test1.test.com
test	www.test.com、test.com、 test.co.jp
www.test?.com	www.test1.com、www.test2.com、 www.testA.com

タイプ

対象とする問い合わせタイプを以下から選択します。()内はタイプの番号です。

- すべて (PTR (12) を除く)
- A (1)
- NS (2)
- CNAME (5)
- SOA (6)
- HINFO (13)
- MX (15)
- AAAA (28)
- SRV (33)
- その他

任意のタイプを指定する場合は、“その他”を選択し、10進数を使用して、1～11、13～65535の範囲で指定します。

送信元IPアドレス

フィルタリング条件としての送信元IPアドレスをIPv4アドレス／ネットマスク、またはIPv6アドレス／プレフィックスの形式で設定します。

動作

対象ドメイン、問い合わせタイプ、送信元IPアドレスに対する動作を以下の4つから選択します。

- 廃棄する
該当ドメインの転送を無効にするフィルタ (URL フィルタ) または、該当問い合わせタイプのDNSパケットの転送を無効にするフィルタ (問い合わせタイプフィルタ) として利用します。
- 接続先のDNSサーバへ問い合わせる
接続先情報で設定されたDNSサーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
- 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる
接続先情報で設定したDNSサーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
“接続先のDNSサーバへ問い合わせる”との違いは、必ず指定したネットワークを経由してDNSサーバへ問い合わせることです。また、解決したホストへのホスト経路自動作成に“する”を選択することにより、DNS解決したホストへのホスト経路を自動で作成することができます。
- 設定したDNSサーバへ問い合わせる
特定のDNSサーバへ問い合わせます。問い合わせるDNSサーバのIPv4/IPv6アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:fff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

23.2 逆引き情報

[操作] 「設定メニュー」 → ルータ設定「ProxyDNS 情報 URL フィルタ情報」 → [逆引き情報]

■逆引き情報
 ※追加情報は一覧の最後尾の入力フィールドで設定してください。 ?

優先順位	ネットワークアドレス	動作	DNSサーバアドレス/ ネットワーク名 経路自動作成	操作
全削除				
<逆引き情報入力フィールド>				
ネットワーク アドレス	<div style="border: 1px solid gray; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 100%;"> <p>すべて (“指定する”を選択時のみ有効です。)</p> <input style="width: 90%;" type="text"/> </div> <div style="width: 10%; text-align: right;"> <input type="checkbox"/> </div> </div> <p>※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。</p> </div>			
動作	<div style="border: 1px solid gray; padding: 5px;"> <p><input checked="" type="radio"/> 廃棄する</p> <p><input type="radio"/> 接続先のDNSサーバへ問い合わせる</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> ネットワーク名 rmt0 </div> <p><input type="radio"/> 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> ネットワーク名 rmt0 </div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する </div> <p><input type="radio"/> 設定したDNSサーバへ問い合わせる</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> DNSサーバアドレス <input style="width: 80%;" type="text"/> </div> </div>			
<div style="display: flex; justify-content: flex-end; gap: 10px;"> 追加 キャンセル </div>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存した情報は、設定反映後に有効になります。

逆引き情報は IP アドレスにより DNS サーバを切り替える範囲を指定する場合に使用します。定義数は、BR500S 仕様一覧「[2.3 システム最大値一覧](#)」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

ネットワークアドレス

対象とするネットワークアドレスを以下の4つから選択します。

- すべて
IPv4 と IPv6 両方を選択します。
- IPv4 すべて
IPv4 アドレスをすべて選択します。
- IPv6 すべて
IPv6 アドレスをすべて選択します。
- 指定する
IPv4 アドレス/ネットマスクまたは IPv6 アドレス/プレフィックスの形式で指定します。

動作

対象ドメインに対する動作を以下の3つから選択します。

- 廃棄する
該当ネットワークの転送を無効にするフィルタを指定します。
- 接続先の DNS サーバへ問い合わせる
接続先情報で設定された DNS サーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
- 接続先の DNS サーバへ指定ネットワークを経由して問い合わせる
接続先情報で設定した DNS サーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
“接続先の DNS サーバへ問い合わせる”との違いは、必ず指定したネットワークを経由して DNS サーバへ問い合わせることです。また、解決したホストへのホスト経路自動作成に”する”を選択することにより、DNS 解決したホストへのホスト経路を自動で作成することができます。
- 設定した DNS サーバへ問い合わせる
特定の DNS サーバへ問い合わせます。問い合わせる DNS サーバの IPv4/IPv6 アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:fff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

24 ホストデータベース情報

[操作] 「設定メニュー」→ルータ設定「ホストデータベース情報」

ホストデータベース情報		
1~16	17~32	33~48
49~64	全表示	

[操作] 「設定メニュー」→ルータ設定「ホストデータベース情報」→[全表示]

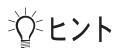
■ホストデータベース情報					
※全削除ボタンが一番最後にあります。					
\	ホスト名	IPv4アドレス	MACアドレス	電源制御	操作
		IPv6アドレス			
1	-	-	-	-	修正 削除
2	-	-	-	-	修正 削除
3	-	-	-	-	修正 削除
4	-	-	-	-	修正 削除
5	-	-	-	-	修正 削除

58	-	-	-	-	修正 削除
59	-	-	-	-	修正 削除
60	-	-	-	-	修正 削除
61	-	-	-	-	修正 削除
62	-	-	-	-	修正 削除
63	-	-	-	-	修正 削除
64	-	-	-	-	修正 削除
全削除					
保存した情報は、設定反映後に有効になります。					

登録しているホストデータベース情報の定義が表示されています。ホストデータベースの定義数は、BR500S 仕様一覧「2.3 システム最大値一覧」(P.19) を参照してください。処理するボタンをクリックし、次のページへ進みます。

[操作] 「設定メニュー」→ルータ設定「ホストデータベース情報」→ [修正]

■ホストデータベース情報					
※全削除ボタンが一番最後にあります。					
\	ホスト名	IPv4アドレス	MACアドレス	電源制御	操作
		IPv6アドレス			
1	ホスト名	<input type="text"/>	<input type="text"/>	<input type="text"/>	
	IPv4アドレス	<input type="text"/>	<input type="text"/>	<input type="text"/>	
	IPv6アドレス	<input type="text"/>	<input type="text"/>	<input type="text"/>	
	MACアドレス	<input type="text"/>	<input type="text"/>	<input type="text"/>	
	リモート電源制御	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外			
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>					



ヒント

◆ホストデータベースには以下の機能があります。

- DNSサーバ機能
「ホスト名」「IPアドレス」のペアを登録することにより、ProxyDNSのDNSサーバ機能を使用することができます。
- リモートパワーオン機能
「MACアドレス」を登録することにより、Wake up on LAN機能を使用することができます。
- DHCPスタティック機能
「IPアドレス」「MACアドレス」のペアを登録することにより、DHCPで割り当てられるIPアドレスを端末固有のものとすることができます。

ホスト名

DNSサーバ機能で使用されます。80文字以内で指定します。使用できる文字は半角英数字、“.”、“-”です。その他の記号は使用できません。

IPv4 アドレス

DNSサーバ機能およびDHCPスタティック機能で使用されます。

IPv6 アドレス

DNSサーバ機能で使用されます。

MACアドレス

DHCPスタティック機能、リモートパワーオン機能で使用されます。MACアドレスは以下の形式で指定します。

xx:xx:xx:xx:xx:xx (xxは2桁の16進数)

電源制御 (リモート電源制御)

本装置と同じセグメントに存在するWake up on LAN対応機器を、リモートパワーオン指示の対象とする場合は、“対象”を選択します。

この設定はスケジュール機能や手動操作でリモートパワーオンを指示する場合に使用されます。

索引

A

AAA 情報	210
AAA ユーザ情報	211
AH	128
ARP 情報 (LAN)	79
AS 外部経路集約情報 (ルーティング)	248
AS 境界ルータ情報 (ルーティング)	247

B

BGP/MPLS VPN 情報 (LAN)	77
BGP/MPLS VPN スタティック経路情報 (LAN)	78
BGP 相手基本情報 (ルーティング)	231
BGP 相手情報 (ルーティング)	231
BGP 拡張機能情報 (ルーティング)	236
BGP 関連 (ルーティング)	228
BGP 再配布フィルタリング情報 (ルーティング)	237
BGP 集約経路情報 (ルーティング)	230
BGP 情報 (ルーティング)	228
BGP ネットワーク情報 (ルーティング)	229
BGP フィルタリング情報 (ルーティング)	234

D

DHCP 情報 (LAN)	74
DHCP スタティック機能	271
DNS サーバ機能	265, 271
DNS サーバの自動切り替え機能	265
DNS 問い合わせタイプフィルタ機能	265

E

ECMP 情報 (ルーティング)	222
EoMPLS 情報 (LAN)	101
ESP	128
EXP 値書き換え情報 (相手)	161

I

ICMP 情報 (LAN)	75
IKE 情報 (相手)	132
IPsec/IKE 接続 (IPsec/IKE) (相手)	126
IPsec 情報 (自動鍵) (相手)	128
IPsec 情報 (手動鍵) (相手)	130
IPv6 DHCP 情報 (相手)	179
IPv6 RIP 関連 (ルーティング)	253
IPv6 RIP 再配布フィルタリング情報 (ルーティング)	254

IPv6 RIP 情報 (LAN)	83
IPv6 RIP 情報 (相手)	166
IPv6 RIP タイマ情報 (ルーティング)	253
IPv6 RIP フィルタリング情報 (LAN)	92
IPv6 RIP フィルタリング情報 (相手)	175
IPv6 RIP マルチパス情報 (ルーティング)	254
IPv6 Traffic Class 値書き換え情報 (LAN)	90
IPv6 Traffic Class 値書き換え情報 (相手)	173
IPv6 Traffic Class 値書き換え情報 (テンプレート)	207
IPv6 関連 (AAA)	215
IPv6 関連 (LAN)	80
IPv6 関連 (相手)	163
IPv6 関連 (テンプレート)	202
IPv6 基本情報 (AAA)	215
IPv6 基本情報 (LAN)	80
IPv6 基本情報 (相手)	163
IPv6 基本情報 (テンプレート)	202
IPv6 再配布情報 (ルーティング)	251
IPv6 スタティック経路情報 (AAA)	216
IPv6 スタティック経路情報 (LAN)	84
IPv6 スタティック経路情報 (相手)	167
IPv6 帯域制御 (WFQ) 情報 (LAN)	93
IPv6 帯域制御 (WFQ) 情報 (相手)	177
IPv6 帯域制御 (WFQ) 情報 (テンプレート)	208
IPv6 フィルタリング情報 (LAN)	86
IPv6 フィルタリング情報 (相手)	169
IPv6 フィルタリング情報 (テンプレート)	203
IPv6 優先度情報 (ルーティング)	252
IPv6 ルーティングマネージャ情報	251
IP アドレス情報 (LAN)	54
IP 関連 (AAA)	213
IP 関連 (LAN)	54
IP 関連 (相手)	139
IP 関連 (テンプレート)	193
IP 基本情報 (AAA)	213
IP 基本情報 (相手)	139
IP 基本情報 (テンプレート)	193
IP トンネル接続 (相手)	125
IP フィルタリング情報 (LAN)	61
IP フィルタリング情報 (相手)	146
IP フィルタリング情報 (テンプレート)	194
IP マルチキャスト情報	256
IP マルチキャストスタティック経路情報	258
ISDN 接続 (相手)	114
ISDN (WAN)	38

L

LAN0 (セグメント)	20
LAN1 (セグメント)	20
LAN 情報	43

LDP 情報 (LAN)	99
LDP 情報 (相手)	186

M

MAC フィルタリング情報 (LAN)	96
MAC フィルタリング情報 (相手)	183
MPLS 関連 (LAN)	98
MPLS 関連 (相手)	185
MPLS 基本情報 (LAN)	98
MPLS 基本情報 (相手)	185
MPLS 情報	260
MPLS トンネル接続 (相手)	134
MPLS 連携情報 (ルーティング)	239
MP 情報 (相手)	138

N

NAT 情報 (LAN)	68
NAT 情報 (相手)	155

O

OSPF エリア基本情報 (ルーティング)	241
OSPF エリア情報 (ルーティング)	241
OSPF 関連 (ルーティング)	240
OSPF 再配布フィルタリング情報 (ルーティング)	249
OSPF 情報 (LAN)	57
OSPF 情報 (相手)	141

P

PPPoE 情報 (相手)	124
PPPoE 接続 (相手)	122
PPP 関連 (相手)	137
PPP 関連 (テンプレート)	191
PPP 情報 (相手)	111, 117, 121, 124
ProxyDNS 情報	265

R

RIP 相手フィルタリング情報 (ルーティング)	227
RIP 関連 (ルーティング)	223
RIP 再配布フィルタリング情報 (ルーティング)	224
RIP 情報 (LAN)	56
RIP 情報 (相手)	140
RIP タイマ情報 (ルーティング)	223
RIP フィルタリング情報 (LAN)	67
RIP フィルタリング情報 (相手)	153
RIP マルチパス情報 (ルーティング)	224
RIP ユニキャスト送信情報 (ルーティング)	226

S

SNMP 情報	25
---------------	----

T

TOS 値書き換え情報 (LAN)	65
TOS 値書き換え情報 (相手)	151
TOS 値書き換え情報 (テンプレート)	198

U

UPnP 情報	259
URL フィルタ機能	265
URL フィルタ情報	265

V

VLAN プライオリティマッピング情報 (VLAN) (LAN)	53
VRF 情報 (ルーティング)	238
VRRP グループ情報 (LAN)	46
VRRP トリガ情報 (VRRP グループ) (LAN)	49

W

WAN 情報	37
--------------	----

あ

相手情報	104
圧縮情報 (相手)	137
圧縮情報 (テンプレート)	192

い

異常時動作情報	29
インタフェース情報	217

お

オプション設定 (PPPoE)	12
オプション設定 (インターネットへ ISDN)	8
オプション設定 (インターネットへ専用線接続)	10
オプション設定 (オフィスへ ISDN 接続)	15
オプション設定 (オフィスへ専用接続)	16
オプション設定 (プライベート LAN)	19

か

かんたん設定メニュー	6
かんたん設定 (PPPoE)	12
かんたん設定 (インターネットへ ISDN 接続)	7
かんたん設定 (インターネットへ専用線接続)	10

かんたん設定 (オフィスへ ISDN 接続)	14
かんたん設定 (オフィスへ専用線接続)	16
かんたん設定 (プライベート LAN 構築)	18

き

基本情報 (IPsec/IKE 接続) (相手)	126
基本情報 (IP トンネル接続) (相手)	125
基本情報 (ISDN) (相手)	114
基本情報 (MPLS トンネル) (相手)	134
基本情報 (MPLS)	260
基本情報 (PPPoE) (相手)	122
基本情報 (UPnP)	259
基本情報 (VLAN) (LAN)	51
基本情報 (VRRP グループ) (LAN)	47
基本情報 (相手)	105
基本情報 (専用線) (相手)	109
基本情報 (パケット破棄) (相手)	136
基本情報 (物理 LAN) (LAN)	44
基本情報 (フレームリレー) (相手)	118
基本情報 (別インタフェースから送出) (相手)	135
基本情報 (モデム接続) (相手)	119
逆引き情報	268
共通情報 (LAN)	44
共通情報 (相手)	105
共通情報 (シリアル)	102
共通情報 (テンプレート)	190

く

グループ ID 情報	210
グループ識別子 0	262
グループ識別子 1 ~ 7	264

け

経路集約情報 (ルーティング)	242
月間/週間予約情報	33

こ

構成定義切り替え予約情報	36
--------------------	----

さ

サーバ機能情報	31
再配布情報 (ルーティング)	218

し

システムログ情報	24
順引き情報	266
詳細設定メニュー	6
シリアル情報	102

す

スケジュール情報	33
スタティック経路情報 (AAA)	214
スタティック経路情報 (LAN)	59
スタティック経路情報 (相手)	144

せ

静的 MAC 学習テーブル情報 (LAN)	97
静的 NAT 情報 (LAN)	69
静的 NAT 情報 (相手)	156
セカンダリ IP アドレス情報 (LAN)	55
セグメント接続/分割 (かんたん設定)	20
接続先情報 (相手)	107
接続制御情報 (相手)	110, 115, 120, 123
設定メニュー	6
専用線接続 (相手)	109
専用線 (WAN)	41

そ

装置情報	22
------------	----

た

帯域制御 (WFQ) 情報 (LAN)	72
帯域制御 (WFQ) 情報 (相手)	158
帯域制御 (WFQ) 情報 (テンプレート)	200
タイムサーバ情報	23

ち

着信相手識別情報 (相手)	188
着信制御情報 (相手)	116, 121

て

テンプレート情報	189
電話番号変更予約情報	35

に

認証情報 (AAA)	212
認証情報 (テンプレート)	191

ね

ネットワーク情報	104
----------------	-----

は

バーチャルリンク情報 (ルーティング)	245
パケット破棄 (相手)	136
パスワード情報	21

ひ

必須設定 (PPPoE)	12
必須設定 (インターネットへ ISDN)	7
必須設定 (インターネットへ専用線接続)	10
必須設定 (オフィスへ ISDN 接続)	14
必須設定 (オフィスへ専用線接続)	16
必須設定 (プライベート LAN)	18

ふ

ファームウェア更新情報	28
ブリッジ関連 (LAN)	95
ブリッジ関連 (相手)	182
ブリッジグループ情報	261
ブリッジ情報	261
ブリッジ情報 (LAN)	95
ブリッジ情報 (相手)	182
フレームリレー接続 (相手)	118
フレームリレー (WAN)	42

へ

別インタフェースから送出 (相手)	135
-------------------------	-----

ほ

ホストデータベース情報	270
-------------------	-----

ま

マルチキャスト情報	256
マルチキャスト情報 (LAN)	76
マルチキャスト情報 (相手)	160
マルチルーティング情報 (相手)	112

も

モデム情報 (シリアル)	103
--------------------	-----

ゆ

優先度情報 (ルーティング)	221
----------------------	-----

り

リモートパワーオン機能	271
-------------------	-----

る

ルータ ID 情報 (ルーティング)	240
ルータ名称情報	22
ルーティングプロトコル情報	217
ルーティングマネージャ情報	217
ループバック情報	30