RX3042H

ユーザーマニュアル

レビジョン 1.0

2006 年 12 月

もくじ

図の一覧リスト

表の一覧リスト

1 概要

この度は ASUS RX3042H（以下、本ルータと記載）をお買い求め頂き、ありがとうございます。お使いのLAN（ローカルエリアネットワーク）は ADSL やケーブルモデム等の高速ブロードバンド接続を使用することでインターネットにアクセス可能です。

このユーザーマニュアルは本ルータの設定方法と、本ルータを最大限利用していただくためのカスタマイズ方法について記載しています。

1.1 特長

- LAN：4 ポートファストイーサネットスイッチ
- WAN： Dual 10/100Base-T イーサネットで LAN 内部のコンピュータ全てからインターネットアクセスが可能
- Firewall & NAT (Network Address Translation） 機能で LAN 環境のインターネットアクセスを保護
- IP ルート、DNS 設定と DDNS 設定を含む DHCP サーバサービスを通してネットワークアドレスを自動的に割り当て
- デュアル WAN または WAN / DMZ サポートのユーザー設定が可能
- USBストレージサポート（ファームウェアの更新が必要）
- ブラウザから設定プログラムにアクセス可能 (Microsoft Internet Explorer 6.0 以降）

1.2 システム条件

本ルータのシステム条件は以下のとおりです。

- ADSL またはケーブルモデムと対応するサービスと動作環境と、ユーザーの WAN に割り当てられた パブリックインターネットアドレスが最低 1 つ
- イーサネット 10Base-T / 100Base-T / 1000Base-T ネットワークインターフェースカード (NIC） 搭載のコンピュータ1台以上
- （オプション） イーサネットハブ / スイッチ（イーサネットネットワークで 5 台以上を本ルータに接続する場合）

- ウェブベースの GUI でのシステム設定時 : ウェブブラウザ (Microsoft IE 6.0 以降)

1.3 本書の使用に当たって

1.3.1 表記について

- 略語の定義は最初の表記時に記載しました。
- 簡略化を図るため、本ルータは「ルータ」「ゲートウェイ」と表記していることがあります。
- LAN とネットワークは共にイーサネットで接続したコンピュータ群を指します。
- マウスを使用した操作は “→” で表記しました。
  例： System → Network Setup は「System メニューをクリックし Network Setup サブメニューをクリックする」という意味です。

1.3.2 文字表記について

- メニューまたはドロップダウンリストから選択する項目、またはプログラム上で入力する文字列は「」で表記しました。

1.3.3 特別なメッセージ

本書では以下のアイコンでユーザーの注意を促しています。

注 : 現在のトピックに関する説明と役に立つ情報です。

定義：専門用語または略語等の説明です。また、これらは「用語集」にも記載しました。

警告：人体の安全またはシステムの保全に関する重要度の高いメッセージです。

2 RX3042H を準備する

2.1 パッケージの内容

本ルータには以下のものが含まれています。

- システムユニット、RX3042H
- AC アダプター
- イーサネットケーブル （「ストレートスルー」タイプ）

2.2 ハードウェア

LAN
- 4 ポート ファストイーサネットスイッチ
- オートスピードネゴシエーション

WAN
- デュアル 10/100M イーサネットポート
- オート MDI/MDIX

2.3 ソフトウェア

2.3.1 NAT 機能

本ルータを使用すると、NAT 機能で高速インターネット回線を 1 回線共有することができ、また接続された LAN セグメントをホストするのに必要な複数の接続にかかるコストを節約できます。この機能では、ネットワーク・アドレスは公表されません。 インターネットにアクセスする際は、有効なアドレスで LAN に接続したホストの登録されていない IP アドレスをマッピングします。また、本ルータにはこれとは別にリバース NAT 機能 があり、ユーザーが E メールサーバ、ウェブサーバなどの様々なサービスをホストすることを可能にします。NAT の規則は変換メカニズムを管理します。本ルータは以下の NAT をサポートします。

- NAPT (Network Address and Port Translation）は IP マスカレードまたは ENAT (Enhanced NAT）と呼ばれ、複数の内部ホストを 1 つの有効な IP アドレスにマッピングします。 通常、マッピングはネットワークレンジ内で行われます。パケットは全て

全世界で有効な IP アドレスで変換されます：ポート番号はネットワークポートレンジから選択されます。

- リバース NAPT — 着信マッピングやポートマッピング、仮想サーバとも呼ばれます。 このルールで特定されたプロトコル、ポート番号及び IP アドレスに基づき、ルータに向かうパケットは全て内部ホストにリレーされます。これは複数のサービスが異なった内部ホスト上でホストされる際に役に立ちます。

2.3.2　ファイアウォール機能

本ルータ実装のファイアウォールは以下の機能で、ユーザーのネットワークが攻撃・悪用されないよう保護します。

- ステートフル・パケット・インスペクション
- パケットフィルタリング (ACL:Access Control List)
- サービス妨害攻撃防御機能
- ログ

2.3.2.1 ステートフル・パケット・インスペクション

本ルータのファイアウォールは「 ステートフル・パケット・インスペクション」を採用。 パケットからセキュリティに関する決定に必要な状況に即した情報を抽出し、その情報を後続の接続を検証するために保存します。また、アプリケーションを認識し、ダイナミックセッションを構築して動的接続を可能にすることで、不要なポートを開きません。以上から、拡張性と高い安全性を実現するソリューションと言えるでしょう。

2.3.2.2 パケットフィルタリング (ACL : Access Control List)

ACL ルールはネットワークセキュリティの基本的な構造の 1 つです。 ファイアウォールは各パケットをモニターし、ヘッダーの受信着信情報を解読し、ソースアドレスや宛先アドレス、ソースポート、宛先ポート、ACL ルールで定義されたプロトコルの内容に基づき、パケットを通過させるかを決定します。

ACL はサブネットを分離する非常に適切な手段です。ネットワーク内のセキュリティの第一線として使用され、特定の着信パケットをブロックし、ネットワーク内に侵入させません。

本ルータのファイアウォールの ACL 方式のサポート内容：

- 宛先 IP アドレスとソース IP アドレス、ポート番号とプロトコルに基づき、フィルタリング
- フィルタールール設定のため、ワイルドカードを使用
- フィルタールールの優先度

2.3.2.3 サービス妨害攻撃防御機能

本ルータのファイアウォールには、知られているタイプのインターネット攻撃から内部のネットワークを保護する攻撃防御エンジンがあります。 SYN フルードや、 IP スマーフ、LAND 攻撃、 ピンオブデス等のあらゆる分割攻撃・サービス妨害攻撃 (DoS）から自動的にシステムを保護します。(例：Windows システムをインターネット経由でクラッシュさせることでよく知られている「WinNuke」に対応）また、IP スプーフや、ピンオブデス、 Land 攻撃、分割攻撃などの一般的かつ多様なインターネット攻撃からシステムを保護します。

本ルータが対応する防御 / 検出機能のタイプは表 2.1 に記載しました。

表 2.1. DoS 攻撃

攻撃のタイプ	攻撃名
分割攻撃	Bonk、Boink、Teardrop（New Tear）、Overdrop、Opentear、Syndrop、 Jolt、 IP フラグメンテーションオーバーラップ
ICMP 攻撃	Ping of Death、Smurf、Twinge
フラッダー	ICMP フラッダー、UDP フラッダー、SYN フラッダーのみにロギング
ポートスキャン	TCP SYN Scan のみにロギング攻撃 パケットドロップ： TCP XMAS Scan、TCP Null Scan、TCP Stealth Scan
PF ルールでの防御	Echo-Chargen、Ascend Kill
その他	IP スプーフ、LAND 攻撃 Targa、Winnuke

2.3.2.4 ALG(Application Level Gateway）

FTP のようなアプリケーションは、個別のアプリケーションパラメータに基づき動的に接続を開きます。本ルータ上のファイアウォールを通過するために、アプリケーションに付随するパケットは対応する通過ルールが必要です。このような規則がない場合、パケットは本ルータファイアウォールに遮断されます。動的に（セキュリティを脅かすことなく）規則を作成するのは不可能ですので、Application Level Gateways (ALG）の形式を採る情報が構築され、アプリケーションのためにパケットを解析し、動的に関連付けます。本ルータの NAT は FTP や、Netmeeting などのアプリケーションに対応する複数の ALG を提供します。

2.3.2.5 ログ

セキュリティを脅かす可能性のあるネットワーク内のイベントは、本ルータのシステムログファイルに記録されます。 記録されるのは、パケットの着信時間や、ファイアウォールの行動記録 / 行動理由など、最低限の情報です。

2.4　使用する前に

2.4.1　フロントパネル

フロントパネルには LED インジケータがあり、ユニットの状態を表示します。

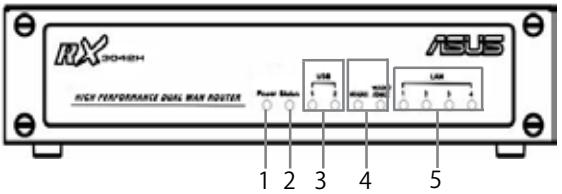


図 2.1 フロントパネル LED

表 2.2 フロントパネルの表示と LED

	LED の表示	色	状態	内容
1	Power	グリーン	ON	電源オン
			OFF	電源オフ
2	Status	グリーン		
3	USB			USB ポートインジケータ
	1-2	グリーン	OFF	USB デバイスを非検出
			ON	USB デバイスを検出
4	WAN1、WAN2/DMZ		OFF	リンクなし
		グリーン	ON	100Mbps リンクを検出
			点滅	100Mbps アクティビティを検出
		オレンジ	ON	10Mbps リンクを検出
			点滅	10Mbps アクティビティを検出
5	LAN			LAN ポートインジケータ
	1-4		OFF	リンクなし
		グリーン	ON	100Mbps リンクを検出
			点滅	100Mbps アクティビティを検出
		オレンジ	ON	10Mbps リンクを検出
			点滅	10Mbps アクティビティを検出

2.4.2　リアパネル

リアパネルにはユニットのデータ用のポートと電源接続用のポートがあります。

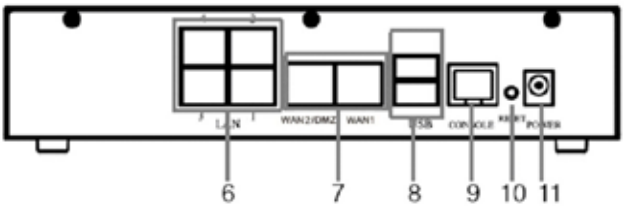
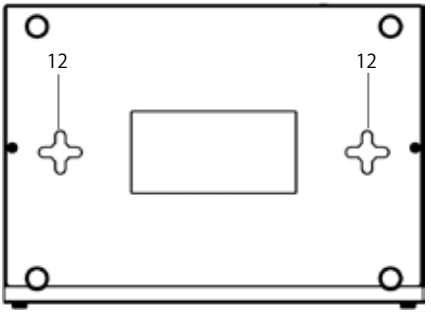


図 2.2 リアパネルコネクタ

表 2.3 リアパネルの表示と LED

	表示	内容
6	1--4	LAN ポート：PC のイーサネットポートに接続、または LAN のハブ / スイッチ上のアップリンクポートに接続。イーサネットケーブルを使用。
7	WAN1、WAN2/DMZ	WAN ポート：WAN デバイスに接続（ADSL、ケーブルモデム、DMZ ネットワーク）
8	USB	USB 1.1 または 2.0 デバイスに接続
9	Console	本ルータではサポートしていません
10	RESET	リセットボタン 1. デバイスを再起動 2. 5 秒以上押すと、システム設定をリセットし、工場出荷状態の初期設定に戻す
11	POWER	POWER 入力ジャック：同梱の AC アダプターに接続

2.4.3 底面



12. ウォールマウントスロット： 壁面に設置する際の溝です。 各ケーブルの長さに応じて、設置方向を 4 つの方法から選択できます。

2.5 設置オプション

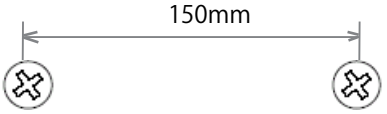
使用条件に応じ、デスクトップ、ウォールマウントの２通りの設置方法が可能です。

2.5.1 デスクトップ

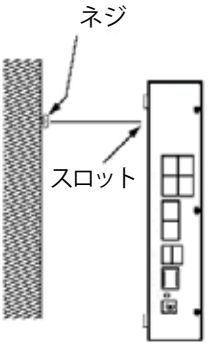
デスク等の水平な場所に設置する場合です。省スペース設計ですので、場所を取りません。

2.5.2 ウォールマウント

1. 壁面に 150mm 間隔で、 ２本のネジが水平になるように設置します。



2. 下図のように、ネジとスロットの位置を合わせ、スロットにネジが入るようにルータの位置を調節します。ウォールマウントデザインは４方向に取り付けが可能です。(リアサイドが上、下、左、右)



ネジとスロットの位置を合わせます。

スロットにネジが入るように、ルータの位置を調節。 上図のようにルータをゆっくりと下に押して固定します。

3 クイックスタートガイド

本章では、ネットワークの構築、インターネット接続について記載します。

- Part 1：ハードウェアの設定
- Part 2：インターネット接続のための設定
- Part 3： LAN を使用したネットワークの基本設定

デバイスのセットアップと設定が完了したら、20 ページの説明を参照し、設定が正しいかどうか確認してください。

ここでは、プロバイダとの ADSL またはケーブルモデムサービスの設定が終了した状態を仮定しています。またここでの説明は家庭や SOHO 等の環境での使用を仮定しています。追加設定などの詳細情報は対応する Chapter をご覧ください。

3.1 Part 1 — ハードウェアの接続

Part 1 では、本製品を ADSL やケーブルモデム (電源ジャック、ケーブル出力に接続)、コンセント、コンピュータ、ネットワークに接続します。

警告：始める前に、全てのデバイスの電源をオフにしてください。 本ルータ、コンピュータ、 LAN ハブ / スイッチも含みます。

図 3.1 ハードウェア接続図を参考に接続してください。

3.1.1 Step 1. ADSL ／ ケーブルモデムに接続

本ルータ：イーサネットケーブルの一方をリアパネルにある WAN ポートに接続します。もう一方を ADSL またはケーブルモデムのイーサネットポートへ接続します。

3.1.2　Step 2. コンピュータ／ネットワーク接続

LAN 上のコンピュータが 4 台以下の場合、イーサネットケーブルで本製品イーサネットポートへ直接コンピュータを接続することができます。 イーサネットケーブルの一方は、本製品のイーサネットスイッチポート (1–4) のいずれかに接続し、もう一方はコンピュータのイーサネットポートへ接続します。

LAN 上に 5 台以上のコンピュータがある場合は、イーサネットケーブルの一方をハブまたはスイッチ (アップリンクポート：ハブまたはスイッチの説明書をご覧ください）に接続し、もう一方は本製品のイーサネットスイッチポート (1–4) に接続します。

注：内蔵スイッチやコンピュータへの接続は、クロスオーバーまたはストレートスルーのイーサネットケーブルを使用できます。内蔵スイッチのハブ / スイッチはどちらのタイプのケーブルでも接続可能です。

3.1.3　Step 3. AC アダプターを取り付ける

AC アダプターの一方をデバイスの後ろの POWER 入力ジャックに接続し、もう一方を電源に接続します。

3.1.4　Step 4. 各デバイスの電源を入れる

AC アダプターを 本ルータの POWER 入力ジャックに接続します。次に ADSL またはケーブルモデムの電源をオンにします。最後にコンピュータと LAN デバイス（無線アクセスポイント、ハブ、スイッチ等）の電源をオンにして起動します。

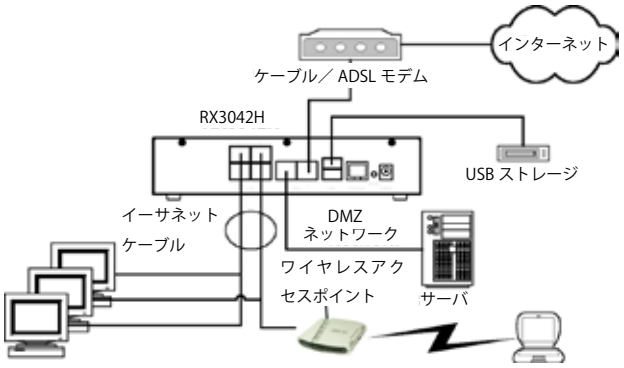


図 3.1 ハードウェア接続

LED が下の表のように点灯するか確認します。

表 3.1 LED インジケータ

LED:	状態
POWER	デバイスの電源がオンのときはグリーンです。点灯しない場合は、AC アダプターがしっかり本ルータに接続されていることと、コンセントが電源に接続されていることを確認してください。
LAN LED	デバイスが LAN と通信可能なときはグリーンが点灯し、LAN コンピュータのデータ送受信中は点滅します。
WAN	プロバイダとの接続が確立したときはグリーンが点灯。インターネットとのデータ送受信中は点滅します。

各 LED が正常に点灯すれば、本ルータも正常に動作しています。

3.2　Part 2 ー コンピュータの設定

ここでは、コンピュータのネットワーク設定について記載します。

3.2.1　始める前に

初期設定では、本ルータは自動的に必要なネットワーク設定を割り当てますので (IP アドレス、 DNS サーバ IP アドレス、 初期設定ゲートウェイ IP アドレス)、コンピュータ側がこの設定を承認するように設定するだけです。

注:手動で設定する場合、ユーザーマニュアル 17 ページの「静的IPアドレスを割り当てる」をご覧ください。

- イーサネット経由で本ルータとコンピュータを接続する場合、インストールした OS に対応する指示に従ってください。

3.2.2　Windows® XP

1. Windows タスクバーの「スタート」ボタン→「コントロールパネル」を選択。
2. 「ネットワーク」接続のアイコンをダブルクリック。
3. LAN または高速インターネットのウィンドウで、 ネットワークインターフェースカード (NIC) に対応するアイコンを右クリックし、「プロパティ」をクリック。(大抵このアイコンはローカルエリア接続と表示)

   ローカルエリア接続のダイアログボックスには現在インストールしているネットワークデバイスが表示されます。
4. インターネットプロトコル (TCP/IP) の左のボックスにチェックが入っていることを確認し、「プロパティ」ボタンをクリック。
5. インターネットプロトコル (TCP/IP) のプロパティダイアログボックスで、「 IP アドレスを自動的に取得する」と「DNS サーバのアドレスを自動的に取得する」と表示されたラジオボタンをクリックします。
6. 「OK」ボタンを 2 回クリックして変更を保存し、コントロールパネルを閉じます。

3.2.3 Windows® 2000

IP プロトコルを確認し、必要ならインストールします。

1. Windows タスクバーの「スタート」ボタン→「設定」→「コントロールパネル」へ。
2. 「ネットワークとダイヤルアップ接続」アイコンをダブルクリック。
3. ネットワークとダイヤルアップ接続の画面で、「ローカルエリア接続」のアイコンを右クリックし、「プロパティ」を選択。

   ローカルエリア接続プロパティ ダイアログボックスには、現在取り付けてあるネットワークコンポーネントがリストアップされます。リストにインターネットプロトコル (TCP/IP) がある場合は、そのプロトコルはすでに有効です。10 に進んでください。
4. インターネットプロトコル (TCP/IP) が表示されない場合は、「インストール」ボタンをクリック。
5. 「ネットワークコンポーネントのタイプを選択」のダイアログボックスで、プロトコルを選択し、「追加」ボタンをクリック。
6. ネットワークプロトコルのリストから「インターネットプロトコ

ル (TCP/IP)」 を選択し、「OK」ボタンをクリック。

Windows 2000 インストール CD または他のメディアからファイルのインストールを促すウィザードが表示された場合は、指示に従いインストールしてください。

7. 再起動を促すダイアログが表示されたら、「OK」ボタンをクリックし、システムを再起動してください。

次に、本ルータが割り当てたネットワーク設定を承認するため、コンピュータの設定を行います。

8. コントロールパネルで「ネットワークとダイヤルアップ接続」アイコンをダブルクリック。
9. ネットワークとダイヤルアップ接続の画面で、「ローカルエリア接続」アイコンを右クリックし、「プロパティ」を選択。
10. ローカルエリア接続プロパティ ダイアログボックスで「インターネットプロトコル (TCP/IP)」を選択し「プロパティ」ボタンをクリック。
11. インターネットプロトコル (TCP/IP) プロパティ ダイアログボックスで 「 IP アドレスを自動的に取得する」と「DNS サーバのアドレスを自動的に取得する」と表示されたラジオボタンをクリックします。
12. 「OK」ボタンを２回クリックして変更を保存し、コントロールパネルを閉じます。

3.2.4 Windows® 95、98、Me

1. Windows タスクバーの「スタート」 ボタン→「設定」 →「コントロールパネル」へ。
2. ネットワークアイコンをダブルクリック。

ネットワークダイアログボックスで、「TCP/IP →」で始まるエントリとネットワークアダプターの名前を検索し、「プロパティ」ボタンをクリック。エントリを探すにはスクロールする必要があるときがあります。リスト内にエントリがある場合は、TCP/IP プロトコルは既に有効になっています。 8 に進んでください。

3. インターネットプロトコル (TCP/IP) が表示されていない場合は、 「追加」ボタンをクリック。
4. 「ネットワークコンポーネントのタイプを選択」のダイアログ

ボックスでプロトコルを選択し「追加」ボタンをクリック。

5. 製造元リストから「Microsoft 」を選択し、ネットワークプロトコルリストから「 TCP/IP」を選択し「OK」ボタンをクリック。

   Windows 95、98、Me のインストール CD または他のメディアからファイルのインストールを促すウィザードが表示された場合は、指示に従いインストールしてください。

6. 再起動を促すダイアログが表示されたら、「OK」ボタンをクリックし、システムを再起動してください。

   次に本ルータが割り当てたネットワーク設定を承認するため、コンピュータの設定を行います。

7. コントロールパネルで、ネットワークアイコンをダブルクリック。

8. ネットワークダイアログボックスで、「TCP/IP →」で始まるエントリとネットワークアダプターの名前を選択し、「プロパティ」ボタンをクリック。

9. TCP/IP プロパティ ダイアログボックスで、「 IP アドレスを自動的に取得する」と表示されたラジオボタンをクリックします。

10. TCP/IP プロパティ ダイアログボックスで、「初期設定ゲートウェイ」タブをクリック。「新しいゲートウェイ」のアドレス入力のフィールドに 192.168.1.1 と入力し (本ルータの初期設定 LAN ポート IP アドレス ） 、「追加」ボタンをクリックし、初期設定ゲートウェイのエントリを追加します。

11. 「OK」ボタンを２回クリックして変更を保存し、コントロールパネルを閉じます。

12. 再起動を促すダイアログが表示されたら、「OK」ボタンをクリックし、システムを再起動してください。

3.2.5 Windows® NT 4.0 Workstation

IP プロトコルを確認し、必要ならインストールします。

1.Windows NT のタスクバーの「スタート」ボタン→「設定」→「コントロールパネル」へ。

2. コントロールパネルで、「ネットワーク」アイコンをダブルクリック。

3. ネットワークダイアログボックスで、「プロトコル」のタブをクリック。

   プロトコルのタブには現在取り付けられているネットワークプロ

トコルが表示されます。リスト内にエントリがある場合は、TCP/IP プロトコルは既に有効になっています。 9に進んでください。

4. インターネットプロトコル (TCP/IP) が表示されていない場合は、「追加」ボタンをクリック。
5. 「ネットワークプロトコルを選択」のダイアログボックスで TCP/IP を選択し、「OK」ボタンをクリック。

   Windows NT のインストールCDまたは他のメディアからファイルのインストールを促すウィザードが表示された場合は、指示に従いインストールしてください。
   ファイルのインストールが終わると、ウィンドウには「DHCP と呼ばれる TCP/IP サービスをセットアップし、IP 情報を動的に割り当てることが可能」という意味のメッセージが表示されます。
6. 「はい」ボタンをクリックし、再起動を要求されたら「OK」ボタンをクリックします。

   次に 本ルータが割り当てたネットワーク設定を承認するため、コンピュータの設定を行います。
7. 「コントロールパネル」で、「ネットワーク」アイコンをダブルクリック。
8. ネットワークダイアログボックスで、「プロトコル」のタブをクリック。
9. プロトコルタブで「TCP/IP」を選択し、「プロパティ」ボタンをクリック。
10. Microsoft TCP/IP プロパティ ダイアログボックスで、「DHCP サーバから IP アドレスを取得する」と表示されたラジオボタンをクリック。
11. 「OK」ボタンを 2 回クリックして変更を保存し、コントロールパネルを閉じます。

3.2.6 静的 IP アドレスを割り当てる

IP アドレスを自動ではなく、手動で直接コンピュータに割り当てる必要があることがあります (静的割り当て)。以下の場合、静的割り当てが必要です (必ずしも必要とは限りません)。

- 特定のコンピュータに常時関連付けたいパブリック IP アドレスを 1 つ以上取得している場合 (例：パブリックウェブサーバとしてコンピュータを使用する場合など)

- LAN に複数の異なるサブネットを維持する場合

ただし、本ルータの LAN IP は初期設定値として 192.168.1.1 に設定されています。初回の設定では本ルータとの接続を確立するため、お使いのコンピュータのアドレスを 192.168.1.0 ネットワークで割り当てる必要があります（例：192.168.1.2）。サブネットマスクに 255.255.255.0、初期設定ゲートウェイに 192.168.1.1 を入力します。これらの設定は、実際のネットワーク環境に応じて、変更することが可能です。

各コンピュータに静的情報を割り当てる場合は、14、17 ページの IP プロトコルの設定・確認に関する記載をお読みください。設定したら、インターネットプロトコル (TCP/IP) プロパティを表示するため、以降の説明に従ってください。コンピュータと DNS サーバ、初期設定ゲートウェイ用の IP アドレスの動的割り当てを有効にする代わりに、ラジオボタンをクリックし、手動で情報を入力することも可能です。

注：お使いのコンピュータが全て本ルータの LAN ポートと同じサブネット内にあるように、IP アドレスを設定する必要があります。手動で IP 情報を全てのコンピュータに割り当てる場合は、Chapter 5 の記載に従い LAN ポート IP アドレスを変更してください。

3.3 Part 3 ー RX3042H の簡単設定

ここでは、本ルータの「Configuration Management」にログインし、ルータの基本設定を行います。設定に必要な情報は、契約されているプロバイダにお問い合わせください。また、ここでの記載は本ルータを立ち上げるための最低限の手順です。詳細は対応する項目をご覧ください。

3.3.1　RX3042H のセットアップ

手順

1. Configuration Management に入る前に、HTTP プロキシ設定がブラウザで無効になっていることを確認してください。IE では、「ツール」→「インターネットオプション」→「接続タブ」→「LAN 設定」へ進み、「LAN にプロキシサーバを使用する」のチェックを外してください。
2. 本ルータにある 4 つの LAN ポートの 1 つに接続した任意のコン

ピュータで Web ブラウザを開き、アドレスのフィールドに下の URL を入力し、「Enter」キーを押します。

http://192.168.1.1

これは 本ルータの LAN ポート用に予め設定された IP アドレスです。下の図のようにログイン・ウィンドウが表示されます。

図 3.2 ログイン 画面

本ルータの接続の際に問題がある場合は、本ルータからの IP アドレスの割り当てを承認するためのコンピュータ側の設定がされているかどうか確認します。また、ユーザーの PC の IP アドレスを 192.168.1.0 ネットワーク内の任意の IP アドレスに設定しても解決できます。例：192.168.1.2

3. ユーザーネームとパスワードを入力し、「OK」をクリックし、Configuration Management にログインします。初回のログインでは、下の初期設定を使用します。

ユーザーネーム : admin
パスワード : admin

パスワードは随時変更可能です。(セクション 11.2「ログインパスワードとシステム設定」参照)

システム Status 画面はログインのたびに表示されます。
(図 3.3 参照)

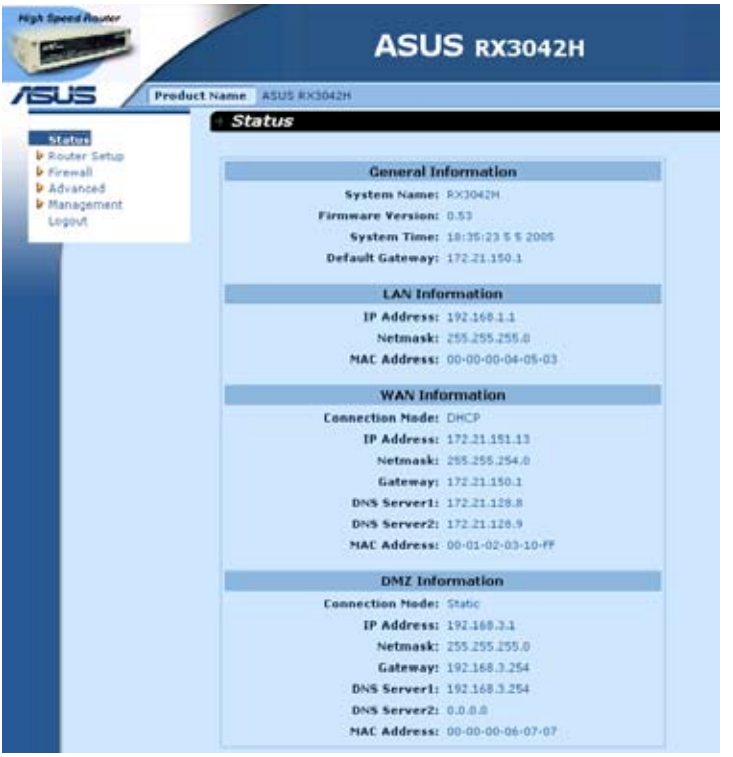


図 3.3 システム Status 画面

4. Chapter 5「ルータ接続の設定」の記載に従い、LAN と WAN の設定を行います。

基本設定が終了したら、以降の記載を参照し、インターネット接続ができるか確認します。

3.3.2　セットアップをテストする

以上の設定で、本ルータでは LAN 上の全てのコンピュータが有効になっており、本ルータの ADSL またはケーブルモデム接続でインターネットにアクセスできるはずです。

インターネット接続をテストするには、ブラウザを開き任意の URL(例：*http://www.asus.com*）を入力します。WAN と表示された LED が速く点滅し、サイトに接続すると点灯します。これでブラウザからサイトの閲覧が可能になりました。

LED が点灯しない、またはサイトが表示されない場合は、Chapter 13 のトラブルシューティングをご覧ください。

3.3.3　ルータの初期設定

プロバイダへの DSL 接続を制御するほかに、本ルータには様々なネットワーク機能が満載です。本ルータには家庭や SOHO などの環境での使用を想定した初期設定がされています。

表 3.2 は、主な初期設定を表にまとめたものです。 これらを含む全ての機能は本書の以降のページに記載しました。 ネットワーク設定に詳しい場合は各設定を確認し、ネットワーク設定要件を充たしているか確認してください。必要な場合は指示に従って変更してください。詳しくない場合は、初期設定は変更せずに使用するか、プロバイダにお問い合わせください。

設定の変更の際は、必ず Chapter 4 に記載の Configuration Management プログラムへのアクセスと使用に関する一般情報を参照してください。また設定変更の際は、プロバイダに連絡することを強くお勧めします。

表 3.2 初期設定一覧

オプション	初期設定	説明 / 手順
DHCP (Dynamic Host Configuration Protocol)	DHCP サーバは以下のアドレスで有効： 192.168.1.100 〜 192.168.1.200	本ルータは お使いの LAN コンピュータへの動的割り当て用のプライベート IP アドレスのプールを維持。 このサービスを利用するためには、IP 情報を動的に受け取るためのコンピュータ設定が必要です。 詳細はクイックスタートガイドの Part 2 に記載があります。DHCP サービスの詳細はセクション 6.1 をご覧ください。
LAN ポート IP アドレス	静的 IP アドレス： 192.168.1.1 サブネットマスク： 255.255.255.0	本ルータ上の LAN ポートの IP アドレスです。LAN ポートは本ルータをイーサネットネットワークに接続します。一般的にはこのアドレスの変更は不要です。詳細はセクション 5.1 LAN 設定 ,5.1.1 LAN IP アドレス の項をご覧ください。

4 Configuration Management

本ルータには予めインストールされたプログラム Configuration Management が組み込まれています。本ルータにインストールされたソフトウェアのインターフェースを利用して、ネットワークに必要なデバイス設定を可能にしています。本ルータに接続したコンピュータのブラウザから、LAN ポートまたは WAN ポートを介してアクセスできます。

ここでは、Configuration Management の基本的な使用方法について記載しました。

4.1 Configuration Management にログインする

Configuration Management は既に本ルータにインストールされています。アクセスするには、以下の条件が必要です。

- 本ルータ上の LAN・WAN ポートに接続したコンピュータ 1 台（クイックガイド参照）
- 上のコンピュータにインストールしたブラウザ。本プログラムは Microsoft Internet Explorer® 6.0 以降で動作するように設定してあります。

  本ルータに接続したコンピュータから、LAN ポートまたは WAN ポートを介して、アクセス可能です。ただし、ここでの記載例は LAN ポートで接続した例です。

1. LAN コンピュータからブラウザを開き、次のアドレスを入力します。

   http://192.168.1.1

これは、本ルータ上の LAN ポート用に予め設定した IP アドレスです。入力すると図 4.1 のようなログイン画面が表示されます。

図 4.1 Configuration Management ログイン画面

2. ユーザーネームとパスワードを入力し「OK」をクリック。

初回のログインでは、下のデフォルトを使用します。

ユーザーネーム　：admin

パスワード　　：admin

注：パスワードは随時変更可能です。（セクション 11.2「ログインパスワードとシステム設定」参照）

システム Status の画面はログインのたびに表示されます。(25 ページの 図 4.3 参照)

4.2　設定画面のレイアウト

一般設定画面には、バナーとメニュー、メニューナビゲーション、設定、オンラインヘルプが表示されます。クリックすると、各メニューグループが展開し、各設定の画面にアクセスします 。設定画面のフレームは、Configuration Management とやり取りして本ルータの各設定を行う場所です。メニューナビゲーションは、メニューを通してどのように現在の設定がアクセス可能かを示します。

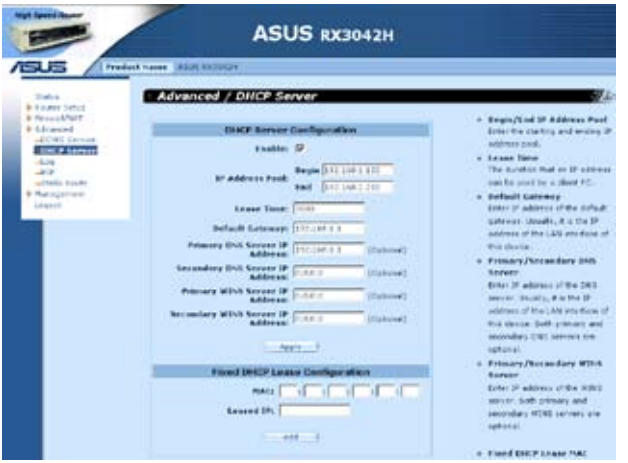


図 4.2 一般的な Configuration Management 設定画面

4.2.1 メニューナビゲーション

- 各メニューを展開表示するにはメニューかアイコン をダブルリックします。
- 展開表示を元に戻すには、再度メニューかアイコン をダブルクリックします。
- 各設定の画面を開くには、メニューかアイコン → をダブルクリックします。

4.2.2 ボタン及びアイコン

下のボタンとアイコンは、このアプリケーションを通じて一般的に表示するものです。下は機能を表にしたものです。

表 4.1 良く利用するボタンとアイコン

ボタン / アイコン	機能
Apply	変更を保存
Add	新しい設定をシステムに追加。例：静的経路やファイアウォール ACL ルールなど
Modify	システム内の既存の設定を変更。例: 静的経路やファイアウォール ACL ルールなど
Reload	データ・設定変更後の現在の画面を再表示
	編集する項目を選択
	ゴミ箱ー選択した項目を消去

4.3　システムの概要

システムの概要を知るには、Configuration Management にログインして Status メニューをクリックします。下の図 4.3 はサンプルです。

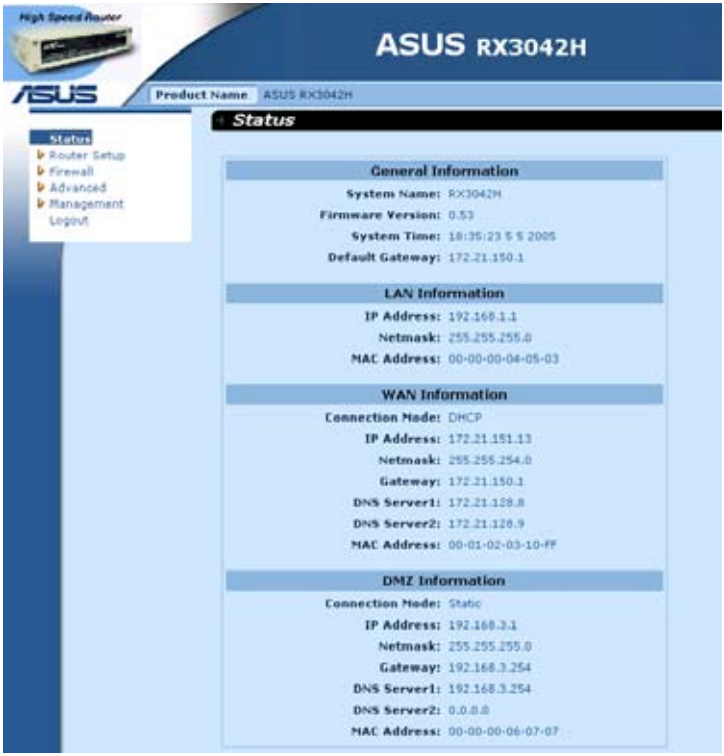


図 4.3 システム Status 画面

5 ルータ接続の設定

ここでは LAN 内のコンピュータが互いに通信し、インターネットにアクセスするための基本設定を記載しています。ネットワークセットアップには LAN 設定と WAN 設定があります。

5.1 LAN 設定

5.1.1 LAN IP アドレス

LAN 上に複数のコンピュータを接続して本ルータを使用する場合は、コンピュータを内蔵型イーサネットスイッチのイーサネットポートに接続する必要があります。また独自の IP アドレスを LAN 内の各デバイスに割り当てる必要があります。本ルータをネットワーク内でノードとして割り当てている LAN IP アドレスは LAN 内の各コンピュータと同一のサブネット内になければなりません。本ルータの初期設定 LAN IP アドレスは 192.168.1.1 です。

定義：ネットワークノードとはあるデバイスとネットワークをつなぐ中継点。本ルータの LAN ポートやコンピュータ上のネットワークインターフェースカード等がノードにあたります。（詳細 Chapter 12 参照）

初期設定 IP アドレスを変更して、ユーザーのネットワークに使用したい IP アドレスを使用することもできます。

5.1.2 LAN 設定パラメータ

表 5.1 は、LAN IP の設定パラメータです。

表 5.1 LAN 設定パラメータ

設定	説明
ホストネーム	識別用のみ
IP アドレス	本ルータの LAN IP アドレスです。ユーザーのコンピュータで使用し、本ルータの LAN ポートを識別。 注：プロバイダがユーザーに割り当てるパブリック IP アドレスとユーザーの LAN IP アドレスは異なります。パブリック IP アドレスはインターネットに対し 本ルータ上の WAN ポートを識別します。
サブネットマスク	LAN サブネットマスクは LAN IP アドレスのどの部分が 1 つのネットワークを表すのか、またどの部分がネットワークノードとして特定しているのかを識別。ユーザーのデバイスは、初期設定サブネットマスク 255.255.255.0 として予め設定されています。

5.1.3 LAN IP アドレスを設定する

以下の手順で、初期設定 LAN IP アドレスを変更します。

1. 「Router Setup」→「Connection」メニューに進みます。下図のようにネットワークセットアップ設定画面が表示されます。

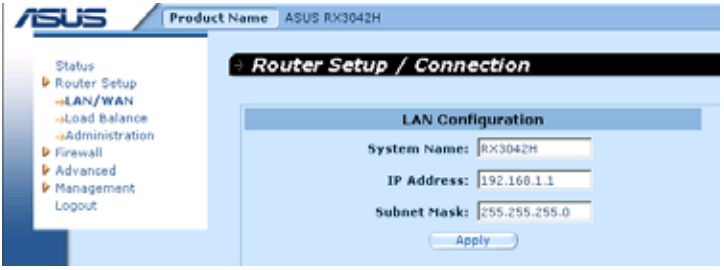
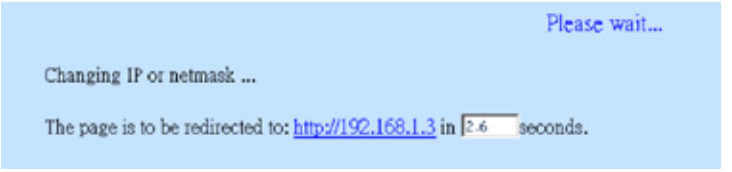


図 5.1 ネットワークセットアップ設定 - LAN Configuration

2. (オプション） 本ルータ用のホストネームを入力。ホストネームは識別用で、他の用途はありません。
3. 本ルータの LAN IP アドレスとサブネットマスクを入力します。
4. WAN ポートのセットアップをしていない場合は、 WAN Configuration のセクションの記載を参照し、設定してください。

5. 「Apply」をクリックし、設定を保存します。イーサネット接続を使用している場合と、IP アドレスまたはサブネットマスクを変更した場合は、接続は一時切断されます。
6. 下のようなメッセージが表示されます。



7. タイマーで設定した一定の時間が経過すると、Configuration Management への再ログインを促します。

5.2　WAN/DMZ 設定

本章では、プロバイダとの通信を目的とし、 本ルータ上の WAN インターフェースの WAN/DMZ 設定の方法を記載します。 以下に、WAN 用の IP アドレス、 DHCP と DNS サーバの設定を説明していきます。

DMZ（非武装地帯）は 企業のプライベート LAN のような信頼できる内部ネットワークと、インターネットのような信頼できない外部ネットワークの間に位置する、ホストまたは小さなネットワークです。一般的に、DMZ は Web サーバ、FTP サーバ、SMTP (e-mail) サーバ、 DNS サーバ のような、インターネットのトラフィックにアクセス可能なデバイスを含みます。DMZ には企業の機密情報は含まれません。DMZ が危険にさらされるイベントでは、その他の企業情報が公表されることはありません。

注：DMZ に対応しているのは静的 IP 接続モードのみです。

5.2.1　WAN 接続モード

本ルータには、 5 種類の WAN 接続方法があります。 – 静的 IP、 動的 IP、PPPoE (マルチセッション)、 PPPoE アンナンバード、PPTP です。プロバイダの要求に合わせ、ネットワークセットアップ設定画面のドロップダウンリストから、これらのいずれかを選択します。(図 5.2 参照)

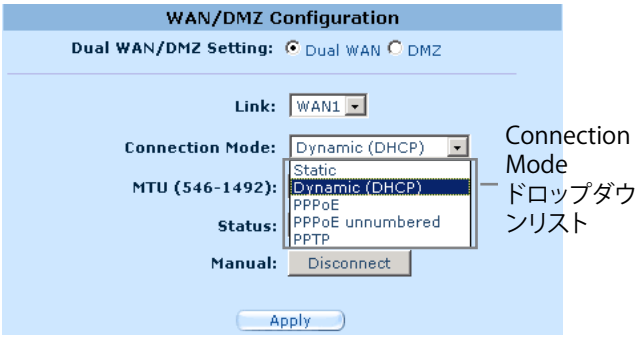


図 5.2 ネットワークセットアップ設定画面 -WAN Configuration

5.2.2 PPPoE

PPPoE 接続は ADSL サービスプロバイダで 最も多く使用されています。

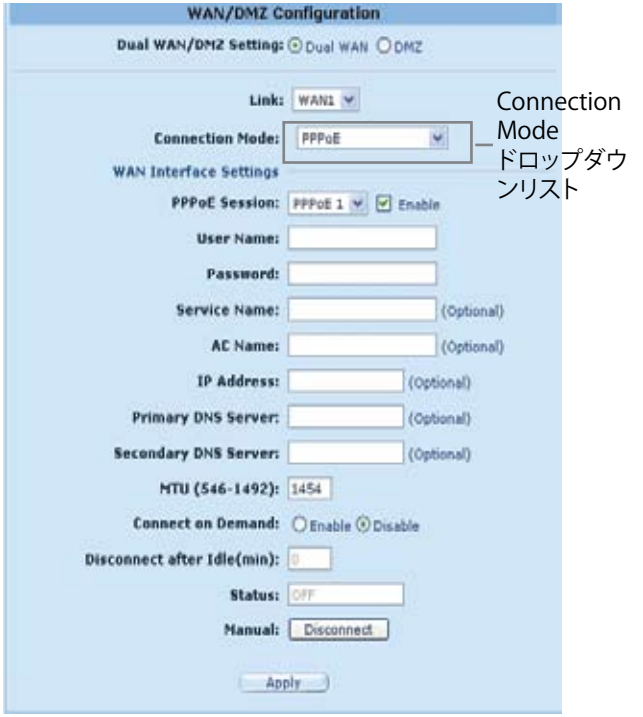


図 5.3. WAN – PPPoE 設定

5.2.2.1 WAN PPPoE 設定パラメータ

表 5.2 は PPPoE 接続モードの設定パラメータです。

表 5.2. WAN PPPoE 設定パラメータ

設定	説明
Link	設定するポートを選択します。オプションには WAN1、WAN2、DMZ があります。
Connection Mode	ドロップダウンリストから PPPoE を選択。
PPPoE Session	この PPPoE セッション用の PPPoE セッション ID を選択。 注：同時 PPPoE セッションは 2 セッションまで可能。
Enable	チェックボックスで PPPoE セッションの有効・無効を切り替えます。
User Name and Password	プロバイダ指定のユーザーネームとパスワードを入力します。（注：Configuration Management にログインする際の情報とは異なります。）
Service Name	プロバイダ指定のサービスネームを入力。これはオプションですが、要求するプロバイダもあります。
AC Name	プロバイダ指定のアクセスコンセントレーターネームを入力。 これはオプションですが、要求するプロバイダもあります。
IP Address	プロバイダが WAN 用に いつも同じ IP アドレスを取得することを許可した場合 IP アドレスを入力します。
Primary / Secondary DNS Server	プライマリ / セカンダリ DNS の IP アドレスは、PPPoE がプロバイダが設定する DNS IP アドレスを自動的に検出するため、オプションです。ただし、他の DNS サーバを使用したい場合は、IP アドレスを入力してください。
MTU	送信パケットの最大サイズを指定することができます。PPPoE 用の MTU の値は 546 ～ 1492 です。初期設定値は 1454 です。
Disconnect after idle (min.)	アイドル状態が続いた場合のインターネット接続を切断するまでのタイムアウトの時間を設定します。「0 」を 入力した場合は、切断されません。注：SNTP サービスを利用している場合、このサービスはタイムアウト機能を阻害します。

設定	説明
Connect on Demand	ラジオボタンで「Enable」と「Disable」を切り替えます。
Status	オン：PPPoE 接続が確立。 オフ：PPPoE 接続が非確立。 Connecting： PPPoE 接続モードでプロバイダとの接続を試行中。
Manual Disconnect/ Connect	「Disconnect」又は「Connect」のボタンをクリックすることにより、プロバイダとの接続と切断を手動で操作することが可能。

5.2.2.2 WAN 用の PPPoE 設定

手順

1. 「Router Setup」→「Connection」メニューからネットワークセットアップ設定画面を開きます。
2. PPPoE 接続モード用に設定する WAN ポート (WAN1/WAN2） を選択します。
3. 「WANConnection Mode」ドロップダウンリストから 「PPPoE」を選択。（ 図 5.3 参照）
4. 「PPPoE session ID」ドロップダウンリストから「PPPoE Session ID」を選択。現在、 2 つのセッションをサポートしています。
5. プロバイダが要求している場合は、サービスネームを入力します。
6. (オプション） プロバイダが要求している場合は、サービスネームおよび AC ネームを入力します。
7. (オプション） プロバイダが WAN 用に いつも同じ IP アドレスを取得することを許可している場合、 IP アドレス フィールドにその IP アドレスを入力します。（それ以外は省略）
8. (オプション） DNS サーバを指定する場合は、プライマリおよびセカンダリ DNS サーバの IP アドレスを入力します。（それ以外は省略）
9. (オプション） 必要な場合 MTU の値を変更してください。入力する値が分からない場合はそのままにしてください。動的 IP 接続モード用の MTU の値は 546 から 1492 です。初期設定値は 1454 です。

10.「Disconnect after Idle (min)」と「Connect on Demand」を設定します。

11.「Apply」をクリックし設定を保存します。

5.2.3　PPPoE アンナンバード

ADSL サービスプロバイダの中には、PPPoE アンナンバードサービスを提供しているものがあり、ご契約のプロバイダがこのサービスを提供している場合は、この接続モードを選択してください。

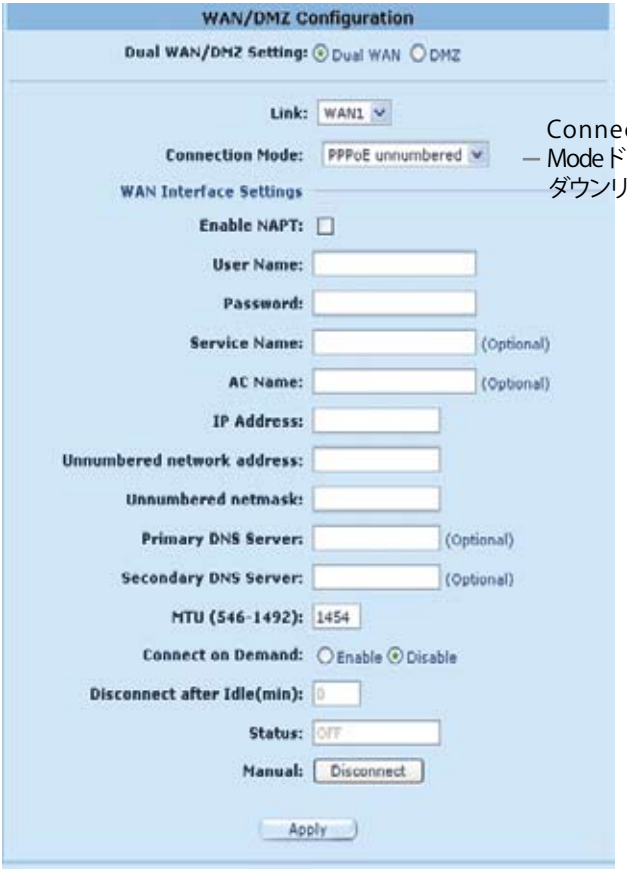


図 5.4. WAN – PPPoE アンナンバード設定

5.2.3.1 WAN PPPoE アンナンバード設定パラメータ

表 5.3 は、PPPoE アンナンバード接続モードの設定パラメータです。

表 5.3. WAN PPPoE アンナンバード設定パラメータ

設定	説明
Link	設定するポートを選択します。有効なオプションには WAN1、WAN2、DMZ があります。
Connection Mode	ドロップダウンリストから「PPPoE Unnumbered」を選択します。一般的には、各ネットワークインターフェースは固有の IP アドレスを持っていますが、アンナンバードインターフェースはこの固有の IP アドレスを持ちません。このため、このオプションを選択すると 、WAN と LAN は同一の IP アドレスを使用することになります。この場合、使用されるネットワーク IP アドレスが少なくなり、ルーティングテーブルも小さくてすむため、ネットワークリソースの節約になります。
Enable NAPT	この接続用に NAPT を有効にするかどうかの切り替えを行います。
User Name and Password	プロバイダにログインする際のユーザーネームとパスワードを入力します。（注：Configuration Management にログインする際の情報とは異なります。）
Service Name	プロバイダ指定のサービスネームを入力。これはオプションですが、要求するプロバイダもあります。
AC Name	プロバイダ指定のアクセスコンセントレーターネームを入力。これはオプションですが、要求するプロバイダもあります。
IP Address	PPPoE アンナンバード接続用の静的 IP アドレスを入力します。この IP アドレスはプロバイダ指定のものです。
Unnumbered Network Address	プロバイダ指定のネットワークアドレスを入力します。
Primary / Secondary DNS Server	プライマリ / セカンダリ DNS の IP アドレスは、PPPoE がプロバイダが設定する DNS IP アドレスを自動的に検出するため、オプションです。ただし、他の DNS サーバを使用したい場合は、IP アドレスを入力してください。

設定	説明
MTU	送信パケットの最大サイズを指定することができます。PPPoE 用の MTU の値は 546 ～ 1492 です。初期設定値は 1454 です。
Disconnect after Idle (min.)	アイドル状態が続いた場合のインターネット接続を切断するまでのタイムアウトの時間を設定します。「0 」を 入力した場合は切断されません。注 : SNTP サービスを利用している場合、このサービスはタイムアウト機能を阻害します。
Connect on Demand	ラジオボタンで「Enable」と「Disable」を切り替えます。
Status	オン：PPPoE アンナンバード接続が確立 オフ：PPPoE アンナンバード接続が非確立 Connecting：PPPoE アンナンバード接続モードでプロバイダとの接続を試行中
Manual Disconnect/ Connect	「Disconnect」 又は「Connect」のボタンをクリックすることにより、プロバイダとの接続と切断を手動で操作することが可能。

5.2.3.2 WAN 用の PPPoE アンナンバードを設定

手順

1. 「Router Setup」→「Connection」メニューから ネットワークセットアップ設定画面を開きます。
2. PPPoE アンナンバード接続モード用に設定する WAN ポート (WAN1/WAN2) を選択します。
3. 「WANConnection Mode」ドロップダウンリストから「PPPoE Unnumbered」 を選択します。(図 5.4 参照)
4. この接続に NAT を使用する場合、「NAPT」ボックスをチェックします。
5. プロバイダ指定のユーザーネームとパスワードを入力します。
6. (オプション) プロバイダが指定している場合、サービスネームおよび AC ネームを入力します。
7. プロバイダ指定の IP アドレス、アンナンバードネットワークアドレス、アンナンバードネットマスクを入力します。
8. (オプション) DNS サーバを指定する場合はプライマリおよびセカンダリ DNS サーバの IP アドレスを入力します。(それ以外は省略)
9. (オプション) 必要な場合 MTU の値を変更してください。入力す

る値が分からない場合はそのままにしてください。動的 IP 接続モード用の MTU の値は 546 ～ 1492 です。初期設定値は 1454 です。

10.「Disconnect after Idle (min)」と 「Connect on Demand」を設定します。

11.「Apply」をクリックし、設定を保存します。

5.2.4 動的 IP

動的 IPはケーブルモデムプロバイダで最も良く利用されています。

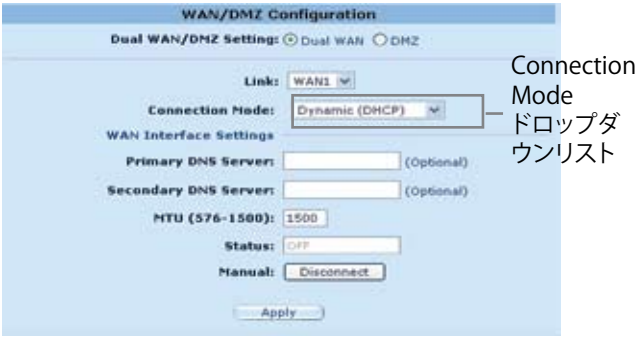


図 5.5. WAN – 動的 IP (DHCP クライアント） 設定

5.2.4.1 WAN 用の動的 IP 設定

手順

1.「Router Setup」→「 Connection」メニューから「ネットワークセットアップ」設定画面を開きます。

2. 動的接続モードを設定する WAN ポート (WAN1/WAN2） を選択します。

3. 「Connection Mode」ドロップダウンリストから「Dynamic」を選択します。（上図 5.5 参照）注：プライマリ / セカンダリ DNS の IP アドレスは、プロバイダの DHCP サーバが自動的に割り当てます。

4. (オプション） 必要な場合 MTU の値を変更してください。入力する値が分からない場合はそのままにしてください。動的 IP 接続モード用の MTU の値は 546 ～ 1500 です。初期設定値は 1500 です。
5. 「Apply」をクリックし設定を保存します。

5.2.5 静的 IP

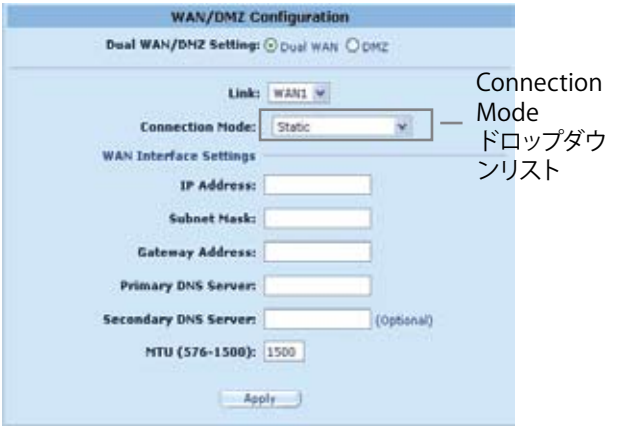


図 5.6. WAN – 静的 IP 設定

5.2.5.1 WAN / DMZ 静的 IP 設定パラメータ

表 5.4 は静的 IP 接続モードの設定パラメータです。

表 5.4. WAN 静的 IP 設定パラメータ

設定	説明
Link	有効なオプションには WAN1/WAN2 、WAN/DMZ があります。
Connection Mode	ドロップダウンリストから「Static」を選択します。
IP Address	WAN/DMZ IP アドレスです。WAN IP アドレスはプロバイダ指定のパブリックアドレスです。 一方、DMZ IP アドレスはプライベート IP アドレスです。

設定	説明
Subnet Mask	WAN/DMZ サブネットマスクです。一般的には 255.255.255.0 に設定されています。
Gateway Address	プロバイダ指定のゲートウェイ IP アドレスです。本ルータ上の WAN と同じサブネット内になければなりません。
Primary/ Secondary DNS Server	プライマリ DNS サーバの IP アドレスは必ず入力してください。セカンダリ DNS サーバはオプションです。
MTU	送信パケットの最大サイズを指定することができます。静的 IP 接続用の MTU の値は 546 ～ 1500 です。初期設定値は 1500 です。

5.2.5.2 WAN / DMZ 用の静的 IP の設定

手順

1.「Router Setup」→「Connection」メニューから「ネットワークセットアップ」設定画面を開きます。
2. 静的接続モード用に設定する WAN ポート (WAN1/WAN2）または DMZ ポート を選択します。
3.「Connection Mode」ドロップダウンリストから「Static」を選択します。（図 5.6 参照）
4. IP アドレスのフィールドに WAN IP アドレスを入力してください。この情報はプロバイダ指定のものです。
5. WAN 用のサブネットマスクを入力します。この情報はプロバイダ指定のものです。一般的に、255.255.255.0 に設定されています。
6. プロバイダ指定のゲートウェイアドレスを入力してください。
7. プライマリ DNS サーバの IP アドレスを入力してください。この情報はプロバイダ指定のものです。セカンダリ、サード DNS サーバはオプションです。
8. (オプション） 必要な場合 MTU の値を変更してください。入力する値が分からない場合はそのままにしてください。静的 IP 接続モード用の MTU の値は 546 ～ 1500 です。初期設定値は 1500 です。
9.「Apply」をクリックし設定を保存します。

5.2.6 PPTP

ユーザーに PPTP 接続を使用したログインを要求するプロバイダもあります。

5.2.6.1 WAN PPTP 設定パラメータ

表 5.5 は PPTP 接続モードの設定パラメータです。

表 5.5. WAN PPTP 設定パラメータ

設定	説明
Link	設定するポートを選択します。有効なオプションには WAN1、WAN2、DMZ があります。
Connection Mode	ドロップダウンリストから PPTP を選択します。
WAN Interface IP	WAN IP アドレスをどのように設定するか選択します。Static (手動で IP アドレスを設定)、Dynamic(DHCP サーバから自動的に入手）が選択できます。
Static	WAN IP がプロバイダ指定の固定 IP の場合、この接続モードを選択します。
IP Address	プロバイダ指定の WAN IP アドレスを入力します。
Subnet Mask	プロバイダ指定の WAN IP 用のサブネットマスクを入力します。
Gateway Address	プロバイダ指定の WAN 用のゲートウェイ IP アドレスを入力します。
Dynamic (DHCP)	WAN IP アドレスをプロバイダの DHCP サーバから自動的に取得した場合、この接続モードを選択します。
User Name and Password	プロバイダにログインする際に使用するユーザーネームとパスワード を入力します。(注： Configuration Management にログインする際の情報とは異なります。)
Server IP Address	プロバイダ指定の PPTP サーバ IP アドレスを入力します。
MTU	通信パケットの最大数を指定できます。PPTP 用の MTU の値は 546 ～ 1460 です。初期設定値は 1460 です。
MPPE	Microsoft Point-to-Point Encryption プロトコルを表します。パケットをこのプロトコルで暗号化する場合、このボックスをチェックします。
Connect on Demand	ラジオボタンで 「Enable」と「Disable」を切り替えます。

設定	説明
Disconnect after Idle (min)	アイドル状態が続いた場合のインターネット接続を切断するまでのタイムアウトの時間を設定します。「0」を 入力した場合は、切断されません。注：SNTP サービスを利用している場合、このサービスはタイムアウト機能を阻害します。
Status	オン：PPTP 接続が確立 オフ： PPTP 接続が非確立 Connecting：本ルータが PPTP 接続モードでプロバイダとの接続を試行中。
Manual Disconnect/ Connect	「Disconnect」または「Connect」のボタンをクリックすることにより、プロバイダとの接続と切断を手動で操作することが可能。

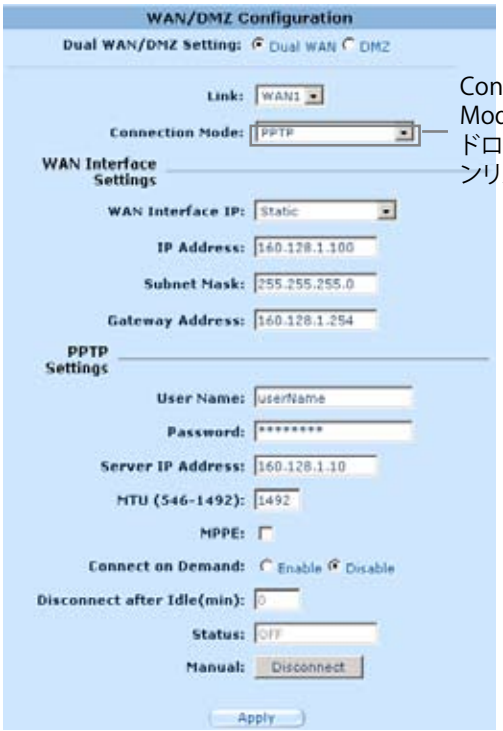


図 5.7. WAN – PPTP 設定

5.2.6.2 WAN 用の PPTP の設定

手順

1.「Router Setup」→「Connection」メニューから「ネットワークセットアップ設定」画面を開きます。
2. PPTP 接続モード用に設定する WAN ポート (WAN1/WAN2）を選択します。
3. 「WAN Connection Mode」ドロップダウンリストから「PPTP」を選択します。（図 5.7 参照）
4. WAN IP をどのように取得するか選択します（Static または Dynamic）プロバイダが固定 IP アドレスを指定した場合、WAN インターフェース IP ドロップダウンリストで「Static」を選択します。不明な点はプロバイダにご相談ください。
5. WAN IP を手動で設定する場合、WAN 用に IP アドレス、サブネットマスク、ゲートウェイ IP アドレスを入力します。
6. プロバイダ指定のユーザーネームとパスワードを入力します。
7. プロバイダ指定の PPTP サーバ IP アドレスを入力します。
8. (オプション）必要な場合 MTU の値を変更してください。入力する値が分からない場合はそのままにしてください。PPTP 接続モード用の MTU の値は 546 ～ 1460 です。初期設定値は 1460 です。
9. パケットを MPPE プロトコルで暗号化する場合、 MPPE ボックスをチェックします。
10.「Disconnect after Idle (min)」と「Connect on Demand」を設定します。
11.「Apply」をクリックし設定を保存します。

5.3 WANロードバランシングとラインバックアップ

本ルータは WAN 接続上のロードバランシングとラインバックアップをサポートしています。本機能は「デュアル WAN」が Router Connection Configuration 画面で選択されているときのみ利用できます（「Router Setup」→「Connection」メニューからアクセス可能）。

WAN ロードバランシング機能は、 WAN 上に事前に設定された帯域幅要求に応じて、本ルータ上の 2 つの WAN の通信アクティビティ

を割り当てます。他にサポートしている機能はWANポート用のフェイルオーバー機能です。WANリンクの1つがダウンしたとき、本ルータはダウンしたWANポートに向かうトラフィックをまだ動作中のWANポートに割り当てます。

ラインバックアップ機能は連続したインターネットアクセスを確保するためのもう1つの機能です。プライマリWANリンクがダウンしたとき、インターネットアクセスは自動的にバックアップWANリンクに切り替えられます。

5.3.1 WANロードバランシングとラインバックアップ設定パラメータ

表5.6はWANロードバランシングとラインバックアップの 設定パラメータです。

表 5.6. WAN ロードバランシングとラインバックアップ設定パラメータ

設定	説明
Load Balance	有効な3つのオプションから1つを選択してください。 Disable：WANロードバランシングとラインバックアップ機能を両方とも無効にします。 Auto Mode：ロードバランシングを利用する場合選択します。ロードバランシングに使用されるアルゴリズムはラウンドロビンに重点を置いています。 Line Backup：バックアップが必要な場合選択します。現在の実装では、プライマリリンクは常にWAN1に、バックアップリンクは常にWAN2に設定されます。
WAN1/WAN2 Bandwidth	WAN間で割り当てたいトラフィック量の動作倍率を入力します。0 ～ 100%間で入力できます。 例： WAN1を80%、WAN2を20%で設定した場合、トラフィックの80%がWAN1に、トラフィックの20%がWAN2に割り当てられます。
Connectivity Check	ラジオボタンで「Enable」と「Disable」を切り替えます。WANポート用のリンクステータスをモニタするために使用します。無効にした場合、本ルータはフェイルオーバーを実行しません。つまり、WANリンクの1つがダウンした場合、ダウンしたリンクに割り当てられていたトラフィックは、動作中のリンクに再割り当てされません。このオプションを有効にしておくことをお勧めします。ただし、 接続用に確認されるゲートウェイまたは （次項へ）

設定	説明
Connectivity Check (続き)	（続き）特定のネットワークデバイスがパケットに応答しない場合、この機能を無効にする必要があります。無効にしない場合、本ルータは WAN リンクステータスを正しく把握できず、ロードバランシング、ラインバックアップに影響を及ぼします。
Connectivity Check Interval	WAN リンクステータス用に本ルータが確認する時間の間隔です。許容値は 1 ～ 60 秒です。
Connectivity Check IP Address (WAN1)	トラフィックが通過する特定のネットワークデバイスの IP アドレスを入力します。このフィールドはオプションです。トラフィックが特定のネットワークデバイスを通過することを知らない限り、IP アドレスをここで指定する必要はありません。
Connectivity Check IP Address (WAN2)	トラフィックが通過する特定のネットワークデバイスの IPアドレスを入力します。このフィールドはオプションです。トラフィックが特定のネットワークデバイスを通過することを知らない限り、IPアドレスをここで指定する必要はありません。

5.3.2　WAN ロードバランシングの設定

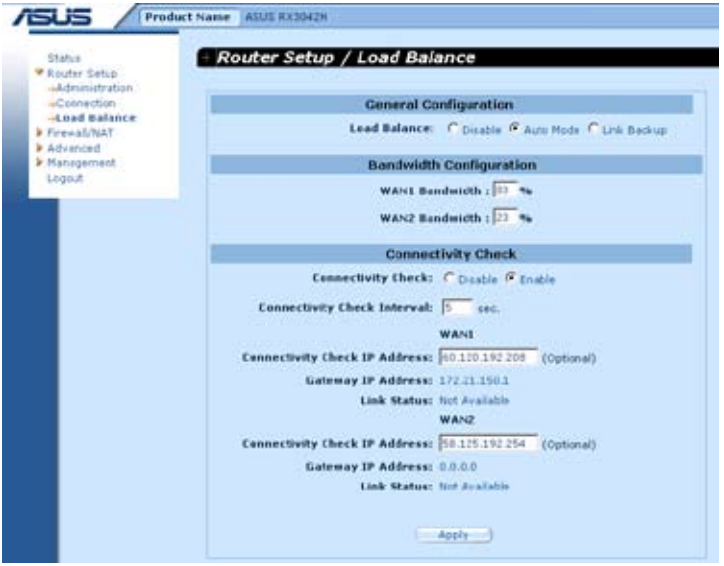


図 5.8. ロードバランシング設定

手順

1. 「Router Setup」 →「Load Balance」 メニューから 「Load Balancing Configuration」 画面を開きます。
2. 「Load Balance」のフィールドから「Auto Mode」を選択します。
3. 2 つの WAN 間で割り当てたいトラフィック量の動作倍率を入力します。許容値は 0 ～ 100% です。2 つの数の合計で 100% になります。
4. 「Connectivity Check」で「enable」または「disable」を選択します。このオプションを有効にした場合、以下の項目も入力してください。

a） 「Connectivity Check Interval」を入力します。

b）（オプション） WAN1 および WAN2 用に「Connectivity Check IP Address」を入力します。

5. 「Apply」をクリックし、設定を保存します。

5.3.3 WAN ラインバックアップの設定

手順

1. 「Router Setup」→「Load Balance」メニューから 「Load Balancing Configuration 」画面を開きます。
2. 「Load Balance」のフィールドから「Line Backup」を選択します。
3. 「Connectivity Check」で「enable」または「disable」を選択します。このオプションを有効にした場合、以下の項目も入力してください。

   a） 「Connectivity Check Interval」を入力します。

   b）（オプション） WAN1 および WAN2 用に「Connectivity Check IP Address」を入力します。

4. 「Apply」をクリックし、設定を保存します。

5.4 ポートミラーリング

ポートミラーリングは LAN 上のセキュリティを強化するメカニズムです。このメカニズムを適応させると LAN 上のいかなるネットワークアクティビティも追跡され、記録されます。

5.4.1 ポートミラーリング設定パラメータ

表 5.7 はポートミラーリング設定パラメータです。

表 5.7. ポートミラーリング設定パラメータ

設定	説明
Mirror Mode	ポートミラーリングを利用する場合ドロップダウンリストから「Enable」を選択します。
Monitor Port	モニタポート用のポート番号を選択します。そのモニタポートは、他のポートで送受信されるパケットをモニタするのに使用します。
Ingress Port	選択したポートが受信するパケットをモニタします（クリックして選択。）選択したポートに送信されるパケットは全てコピーされ、そのコピーはモニタポートに配信されます。注： Ingress Port を選択する場合、対応する Egress Port を選択する必要があります。例：Ingress Port 2 を選択する場合、 Egress Port 2 を同様に選択する必要があります。
Egress Port	選択したポートから送信されるパケットをモニタします（クリックして選択）。選択したポートから送信されるパケットは全てコピーされ、そのコピーはモニタポートに配信されます。
Reload	保存した設定を訂正する場合このボタンをクリックします。注：この機能は 「Apply」ボタンをクリックした後は機能しません。

• Ingress Port をモニタするためには、対応する Egress Port を同様に選択する必要があります。

•モニタポートが指定された場合、Ingress 、Egress ロケーションマップには表示されません。

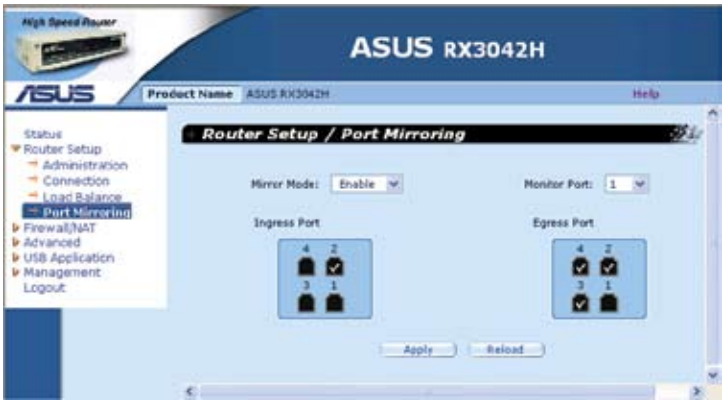


図 5.9. Port Mirroring 設定画面

5.4.2 ポートミラーリングの設定

手順

1. 「Router Setup」 →「Port Mirroring」 メニューから「Port Mirroring Configuration」画面を開きます。
2. 「Mirror Mode」ドロップダウンリストから「Enable」を選択します。
3. ドロップダウンリストから「Monitor Port」番号を選択します。選択した Ingress/Egress Port のトラフィックはコピーされミラーポートに送信されます。
4. トラフィックをモニタしたい Ingress/Egress Port を選択します。
   注： Ingress Port を選択する場合、対応する Egress Port を選択する必要があります。例： Ingress Port 2 を選択した場合、 Egress Port 2 を同様に選択する必要があります。
5. 「Apply」ボタンをクリックし、設定を保存します。

6 DHCP サーバ設定

6.1 DHCP (Dynamic Host Control Protocol)

6.1.1 DHCP とは ?

DHCP とは、ネットワーク上のコンピュータへの IP 情報の割り当て、配信を管理するプロトコルです。

DHCP を有効にすると、本ルータのようなデバイスが、ネットワークに接続したコンピュータに一時的に IP アドレスを割り当てます。IP アドレスを割り当てるデバイスのことを DHCP サーバ、受信するデバイスのことを DHCP クライアントと呼びます。

注： クイックガイドで前述したように、LAN PC に IP アドレスをそれぞれ設定するか、動的に（自動的に）IP 情報を受け取るように設定することができます。動的に情報を割り当てる設定をする場合は、DCHP サーバからの IP アドレスの割り当てを受け取るように PC を DHCP クライアントとして設定します。

DHCP サーバは、あらかじめ定義された IP アドレスプールから IP アドレスを選び、インターネットとセッションがあると、コンピュータに特定の時間だけ IP アドレスを割り当てます。 また、必要に応じて、モニタ、回収、再配信します。

DHCP が有効なネットワークでは、IP 情報は静的ではなく動的に割り当てられます。DHCP クライアントは、ネットワークに接続すると、アドレスプール内から毎回異なるアドレスを割り当てられます。

6.1.2 DHCP を使う理由

DHCP は、ネットワークを介して IP アドレスの管理・配信を行います。DHCP がないと、全てのコンピュータそれぞれに、 IP アドレスやその他関連情報を設定する必要があります。DHCP は一般的に、頻繁に拡大したり更新されたりする大規模なネットワークで使われます。

6.1.3 DHCP サーバを設定する

注：本製品はあらかじめ定義された 192.168.1.100 から 192.168.1.149 （サブネットマスク：255.255.255.0）の IP アドレスレンジ内で、LAN 側の DHCP サーバとして設定することができます。 アドレスレンジを変更する場合は、以下の手順に従ってください。

まず、 DHCP サーバに割り当てられた DHCP 情報を受け入れるようにパソコンを設定します。

1. 「Advanced」→「DHCP Server」の順にクリックして 図 6.1 の「DHCP Server Configuration」 画面を開きます。

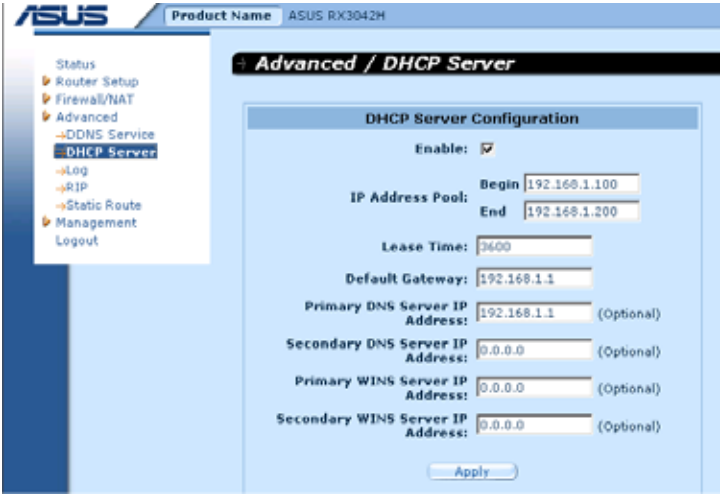


図 6.1. DHCP Server Configuration 画面

2. 「IP Address Pool (Begin/End Address)」、「Lease Time」、「Default Gateway IP Address」 のフィールドに情報を入力します。
3. 「Primary DNS Server IP Address」 のフィールドに、LAN IP または プロバイダの DNS IP を入力します。
4. (オプション）「Secondary DNS Server IP Address」 と「Primary/Secondary WINS Server IP Address」を各フィールドに入力します。

表 6.1 は、DHCP 設定項目の詳細です。

表 6.1. DHCP 設定パラメータ

フィールド	説明
Enable	LAN 用 DHCP サーバサービスを有効／無効にします。
IP Address Pool Begin/ End	DHCP アドレスレンジの最小値と最大値を特定します。
Lease Time	LAN に接続したデバイスが割り当てられたアドレスを使用する時間。
Default Gateway IP Address	設定レンジ内の IP アドレスを受け取るコンピュータ用の初期設定ゲートウェイのアドレス。初期設定ゲートウェイは、インターネット通信をするために DHCP クライアントが一番初めに接続されるデバイスです。 一般的に本ルータの LAN ポート IP アドレスです。
Use WAN DNS Server Address	ラジオボタンで 、WAN インターフェースにより設定または入手される DNS サーバの「Enable」または「Disable」を切り替えます。「Enable」 を選択し、WAN DNS サーバを利用できない場合、本ルータは LAN コンピュータ用の DNS プロキシとして機能します。WAN DNS サーバが利用できる場合は、LAN コンピュータは本ルータ DNS プロキシの代わりに DNS の 要求を直接 WAN DNS サーバに送信します。
Primary/ Secondary DNS Server IP Address	設定レンジの IP アドレスを受信するコンピュータが使う DNS（Domain Name System）の IP アドレスです。DNS サーバは、Web ブラウザに入力したインターネット名を同等の IP アドレスに変換します。一般的にはサーバはプロバイダに存在します。DNS プロキシとして使う本ルータの LAN IP アドレスを入力して、 LAN から DNS サーバに DNS 要求を転送し、 LAN コンピュータに結果を中継します。この項目はオプションです。
Primary/ Secondary WINS Server IP Address (optional)	DHCP IP アドレスレンジから IP アドレスを受信するコンピュータが使う WINS サーバの IP アドレスです。WINS サーバがネットワーク上に存在しなければ、この情報を入力する必要はありません。

5.「Apply」をクリックして、DHCP サーバ設定を保存します。

6.1.4 DHCP アドレスを確認する

本ルータが LAN の DHCP サーバとして機能すると、コンピュータに割り当てられた全てのアドレスを記録します。 DHCP サーバ設定画面の下側にある「Current DHCP Lease Table」のリンクをクリックすると、下の図 6.2 のような画面で、既存の IP アドレス割り当て表全てを確認することができます。

DHCP 割り当て表には、割り当てられた IP アドレスと対応する MAC アドレスが表示されます。

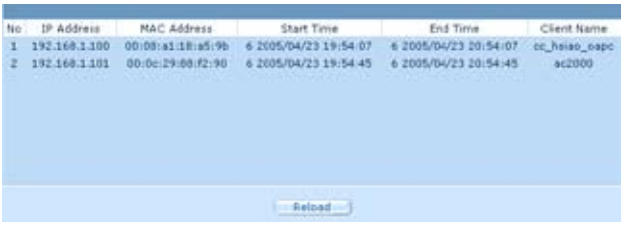


図 6.2. DHCP 割り当て表

6.1.5 固定 DHCP 割り当て

DHCP サーバから IP を取得するホスト用に固定 DHCP アドレスが要求された場合、固定 DHCP 割り当てが使用されます。 まず、DHCP サーバが割り当てる DHCP 情報を受け入れるよう、パソコンを設定する必要があります。

6.1.5.1 Fixed DHCP Lease Configuration 画面へのアクセス ー（Advanced → DHCP Server）

「Advanced」→「DHCP Server」メニューから「Fixed DHCP Lease Configuration」画面を開きます。（図 6.3 参照）

注：「Fixed DHCP Lease Configuration」画面を開くと、存在する割り当てリストが、図 6.3 のように 画面下半分に表示されます。

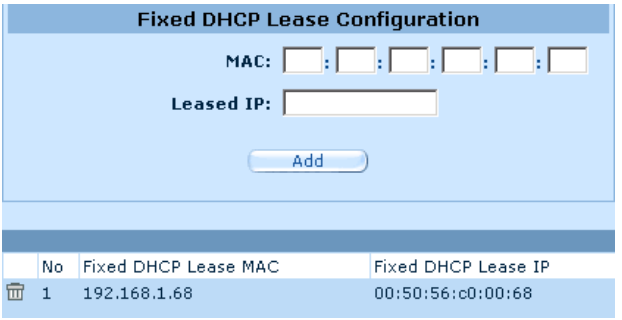


図 6.3. Fixed DHCP Lease Configuration 画面

6.1.5.2 固定 DHCP 割り当ての追加

手順

1. 「Advanced」→「DHCP Server」メニューから「Fixed DHCP Lease Configuration」画面を開きます。(図 6.3)
2. MAC アドレスと固定 IP アドレスを 要求しているホストの希望する IP アドレスを入力します。 下の表 6.2 は固定 DHCP 割り当て設定パラメータの詳細です。

表 6.2. 固定 DHCP 割り当て設定パラメータ

フィールド	説明
Fixed DHCP Lease MAC	DHCP サーバからの固定 IP アドレスを必要とするデバイスの ハードウェア ID
Fixed DHCP Lease IP	DHCP から割り当てられる IP アドレス。注：この IP アドレスは DHCP IP プール外に設定することを推奨します。

3. 「Add」ボタンをクリックして新しい固定 DHCP 割り当てエントリを追加します。

6.1.5.3 固定 DHCP 割り当ての削除

固定 DHCP 割り当てを削除するためには、削除する固定 DHCP 割り当ての左にある をクリックします。

6.1.5.4 固定 DHCP 割り当て表の確認

現在の着信固定 DHCP 割り当てを確認するには 「Advanced」→

「DHCP Server」メニューから「Fixed DHCP Lease Configuration」画面を開きます。

6.2 DNS

6.2.1 DNS とは

DNS（Domain Name System）サーバは ユーザーが Web ブラウザに入力したドメイン名（例:「yahoo.com」）を、対応する数で示され、インターネットルーティングに使用される IP アドレスに置き換えます。

パソコンユーザーがブラウザにドメイン名を入力すると、パソコンは最初に、DNS サーバに対応する IP アドレスを取得するように要求します。DNS サーバは自身のデータベースでドメイン名を調べます。そこで見つからないとき、 上位の DNS サーバと交信します。アドレスが見つかると要求しているパソコンに返送され、通信記録として IP パケットで参照できます。

6.2.2 DNS アドレスの割り当て

複数の DNS アドレスがあれば、サーバの 1 つがダウンしたとき、または回線が混雑したときに代わりを提供でき便利です。プロバイダは一般的にプライマリ／セカンダリ DNS アドレスを提供しますが、追加のアドレスを提供する場合もあります。LAN パソコンはこれらの DNS アドレスを以下のいずれかの方法で確認します。

- 静的に:プロバイダが DNS サーバアドレスを指定している場合、パソコンの IP プロパティを変更することで各パソコンに割り当てることができます。
- DHCP サーバより動的に： 本ルータの DHCP サーバで DNS アドレスを設定できます。また、DHCP サーバは、DNS アドレスをパソコンに割り当てることができます。 DHCP サーバの設定の手順はセクション 6.1.3 「DHCP サーバを設定する」を参照してください。

以上のいずれかの方法で、プロバイダの DNS サーバでの実際のアドレスを指定できます（パソコン上または DHCP Server Configuration 画面内）。または本ルータで LAN ポートのアドレスを指定することもできます（例：192.168.1.1）。 LAN ポート IP アドレスを指定するとき、デバイスは次のセクションで述べる DNS リレーを行います。

注：パソコン上または DHCP プールで、実際の DNS アドレスを指定した場合、 DNS リレー機能は使用されません。

6.2.3　DNS リレーの設定

DNS アドレスとしてデバイスの LAN ポート IP アドレスを指定すると、インターネットセキュリティルータは自動で「DNS リレー」を行います。つまり、デバイス自体は DNS サーバではないため、LAN パソコンからのドメインネーム探索要求をプロバイダの DNS サーバに転送します。そして DNS サーバの 応答をパソコンにリレーします。

DNS リレーを実行するには、本ルータは接続する DNS サーバの IP アドレスを保持する必要があります。本ルータはこれらのアドレスを、次の方法のどちらか一方または両方で確認します。

- PPPoE 接続 または 動的 IP 接続を通して確認： 本ルータがプロバイダと PPPoE (「5.2.2 PPPoE」、「5.2.3 PPPoE アンナンバード」参照） 接続または 動的 IP （「5.2.4 動的 IP」参照）接続をしているとき、プライマリ／セカンダリ DNS アドレス は PPPoE プロトコル経由で確認されます。このオプションを使用すると、プロバイダが DNS アドレスを変更しても、パソコンまたは本ルータの再設定は不要です。
- 本ルータでの設定：WAN 設定画面でもプロバイダの DNS アドレスを指定できます。（ 図 5.3、図 5.4、 図 5.5、 図 5.6 参照）

手順

1. 「DHCP Server Configuration」画面の「DNS Server IP Address」のフィールドに LAN IP を入力します。（図 6.1 参照）
2. 本ルータの DHCP サーバが割り当てた IP アドレスを使用するように、LAN PC を設定します。または、本ルータの LAN IP アドレスを、DNS サーバアドレスとして LAN の各パソコン用に手動で入力します。

注：DNS リレーを有効にする前に LAN パソコンに割り当てられた DNS アドレスは、パソコンを再起動するまで有効です。DNS リレーは、パソコンの DNS アドレスが LAN IP アドレスであるときにだけ実行されます。

同様に、DNSリレーを有効にした後にDNSアドレス（LAN IP アドレス以外）をDHCPプール内またはパソコン上で静的に指定した場合、そのアドレスは DNSリレーアドレスの代わりに使用されます。

7 経路設定

Configuration Management で、インターネットのネットワークデータ通信用に特定の経路を設定することができます。以下の説明は、基本的な経路の概念と静的経路の作成方法です。大抵の場合は静的経路の設定は必要ありません。

7.1 IP 経路

ルータの主要な役割は、特定の送信先へ向かうデータを受信した場合に、次にどのデバイスにデータを送信するかを判断することです。IP 経路を特定すると、ルータがこの判断を行う際のルールを設定したことになります。

7.1.1 静的経路を特定する必要がある？

大抵の場合は必要ありません。家庭や小さなオフィスのネットワークでは、LAN コンピュータやルータ用の初期設定ゲートウェイを設定する経路が、インターネットトラフィックに最適な経路です。

- LAN コンピュータでは、初期設定ゲートウェイが全てのインターネットトラフィックを本ルータの LAN ポートに導きます。TCP/IP を修正した時に割り当てるか、インターネットへのアクセスの際にサーバから情報を動的に受信するように設定しているため、LAN コンピュータは初期設定ゲートウェイを把握しています。（詳細：クイックスタートガイド Part 2 参照）
- 本ルータのデフォルトゲートウェイは全ての送信インターネットトラフィックをプロバイダのルータへ導くように設定されています。デバイスとインターネット接続のネゴシエーションの際に、プロバイダが自動的に初期設定ゲートウェイを割り当てます。（初期設定経路の追加方法 7.3.2 「静的経路を追加する」参照）

２つ以上のネットワークかサブネットを設定している場合や、２つ以上の プロバイダサーバと接続している場合、リモート LAN に接続している場合は、静的経路の設定が必要な場合があります。

7.2 RIP（Routing Information Protocol）を使用する動的経路設定

RIP を使用すると複数のルータ間での経路情報の通信が可能になり、経路は自動的に更新されます。RIP を「System Services Configuration」画面で有効にすることをお勧めします。（図 11.1）

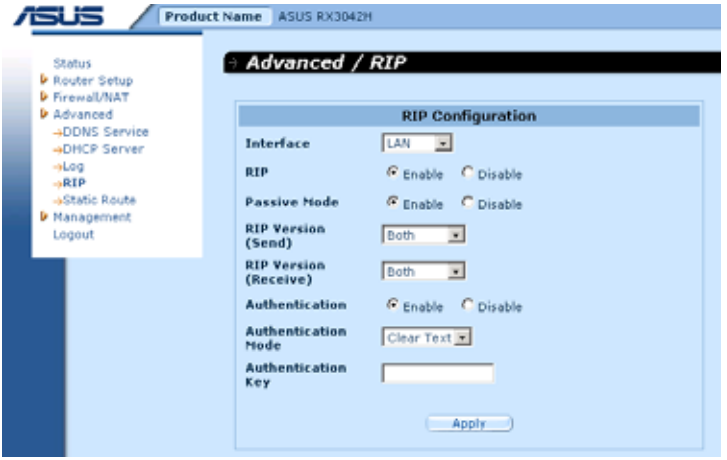


図 7.1. RIP Configuration 画面

7.2.1 RIP 設定パラメータ

下の表は静的経路設定用の設定パラメータです。

表 7.1. 静的経路設定のパラメータ

フィールド	説明
Interface	経路情報の交換に使用するインターフェースを選択します。選択オプションは LAN、WAN1、WAN2、PPPoE1、PPPoE2、PPPoE3、PPPoE4 です。
RIP	「Enable」または「Disable」ラジオボタンで選択したインターフェース用の「RIP」の有効 / 無効を切り替えます。まず、「Management / System Services Configuration」画面で RIP サービスを有効にする必要があります。

フィールド	説明
Passive Mode	このインターフェース用に設定した RIP を、他のルータから経路情報を受信するためだけに使用する場合、この項目を有効にします。送受信する場合は無効にします。
RIP Version (Send)	経路情報を送信する RIP バージョンを選択します。オプションは「Version 1」、「Version 2」、「Both」です。
RIP Version (Receive)	経路情報を送信する RIP バージョンを選択します。オプションは「Version 1」、「Version 2」、「Both」です。
Authentication	「Enable」または「Disable」ラジオボタンで、経路情報を交換する際に使用する認証の有効 / 無効を切り替えます。経路情報を交換するルータは全て、同じ認証キーを使用します。
Authentication Mode	RIP 認証モードをドロップダウンリストから選択します。サポートしているモードは「Clear Text」と「MD5」です。
Authentication Key	経路情報を交換するルータ全てが共有する認証キーを入力します。

7.2.2 RIP を設定する

RIP の有効 / 無効を切り替える手順

1. 「System Services Configuration」画面で、「Enable」または「Disable」ラジオボタンをクリックします。(図 11.1)
2. 経路情報の交換に使用するインターフェースをドロップダウンリストから選択します。
3. 「Enable」ラジオボタンをクリックし、選択したインターフェース用の RIP を有効にします。
4. RIP を「Passive」モードで動作させるかを「Enable」または「Disable」ラジオボタンで選択します。
5. 経路情報の送受信用の RIP バージョンを選択します。利用可能オプションは「Version 1」、「Version 2」、「Both」です。
6. 認証を必要とするかどうかを「Enable」または「Disable」ラジオボタンで選択します。

7. （オプション）認証を有効にすると、認証モードと認証キーを設定する必要があります。

8. 「Apply」ボタンをクリックし設定を適用します。

7.3 静的経路

図 7.2. Static Route Configuration 画面

7.3.1 静的経路設定パラメータ

下の表は静的経路用の設定パラメータです。

表 7.2. 静的経路 設定パラメータ

フィールド	説明
Destination Address	送信先コンピュータまたは送信先ネットワーク全体の IP アドレスを特定します。または数字ゼロを設定し、他に経路が定義されていない送信先に使用する経路であることを示します（これはデフォルトゲートウェイを作成する経路）。送信先 IP はネットワーク ID です。初期設定の経路は送信先 IP「0.0.0.0」です。ネットワーク ID の詳細は Chapter 12 をご覧ください。

フィールド	説明
Subnet Mask	送信先アドレスのどの部分が、ネットワーク、ネットワーク上のコンピュータであるかを示します。（ネットワークマスクの詳細は Chapter 12 を参照）サブネットマスク用の初期設定の経路は「0.0.0.0」です。
Gateway	ゲートウェイ IP アドレス
Interface	設定オプションは AUTO、Eth0（LAN）、Eth1（WAN）、PPPoE：0（unnumbered）、PPPoE：1（1st PPPoE session）、PPPoE：2（2nd PPPoE session）です。これらのオプションはドロップダウンリストで選択します。AUTO を選択すると、ゲートウェイ IP アドレスに基づいて自動的にインターフェースを割り当て、パケットを送信します。

7.3.2 静的経路を追加する

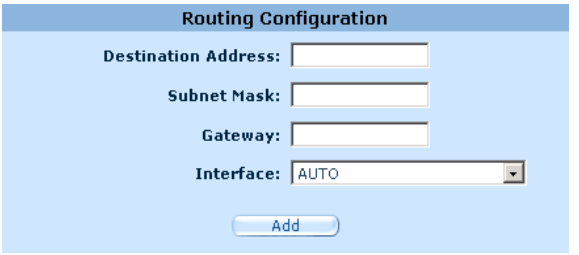


図 7.3. 静的経路設定 画面

静的経路を経路制御表に追加する手順

1. 「Advanced」→「Static Route」メニューの順にクリックし、「Static Route Configuration」画面を開きます。
2. 静的経路情報（Destination IP Address、Subnet Mask、Gateway、Interface）を各フィールドに入力します。

   詳細は 表 7.2 をご覧ください。

   AN のデフォルトゲートウェイを定義する経路を作成するには、「Destination IP Address」と「Subnet Mask」のフィールドに「0,0,0,0」と入力します。
3. 「Add」ボタンをクリックし、新しい経路を適用します。

7.3.3 静的経路を削除する

図 7.4. 経路表（例）

手順

1. 「Advanced」→「Static Route」メニューの順にクリックし、「Static Route Configuration」画面を開きます。
2. 経路表が表示されますので、削除する経路のアイコン をクリックします。

警告：初期設定のゲートウェイは理由なく削除しないでください。インターネット接続ができなくなることがあります。

7.3.4 静的経路制御表を参照する

IP が有効なコンピュータやルータは全て、ユーザーが頻繁にアクセスする IP アドレスを記録します。各送信先 IP アドレス用に、データが取る 1 番目のホップ IP アドレスを表にします。これがデバイスの経路制御表になります。

本ルータの経路制御表を参照するには、「Advanced」→「Static Route」メニューの順にクリックします。経路制御表は図 7.2 のように「Static Route Configuration」画面の上半分に表示されます。

経路制御表には、1 行に 1 経路（送信先ネットワークの IP アドレス、送信先ネットワークのサブネットマスク、トラフィック転送用のゲートウェイの IP 等）の情報を表示します。

8 DDNS 設定

DDNS（Dynamic DNS）は、IP アドレスに変更があった場合でも（PC の再起動や ISP の DHCP サーバが IP のリースをリセットした場合など）、同じドメイン名を持つことができるサービスです。本ルータは WAN IP アドレスが変更されると、DDNS サービスプロバイダに接続し、IP アドレスの代わりにドメイン名を使い、WEB サーバや FTP サーバのような Web サービスの設定をサポートします。DDNS は以下の機能で DDNS クライアントをサポートしています。

- 外部インターフェースを検出した際に DNS 履歴を更新（追加）する機能
- DNS 強制更新機能

HTTP DDNS クライアント

HTTP DDNS クライアントは DDNS サービスプロバイダが提供するメカニズムを使用して DNS 履歴を動的に更新します。この場合、サービスプロバイダが DNS 内の DNS 履歴を更新します。本ルータは HTTP をトリガーとして更新を行います。また、本ルータは下のサービスプロバイダで HTTP DDNS 更新をサポートします。

- www.dyndns.org

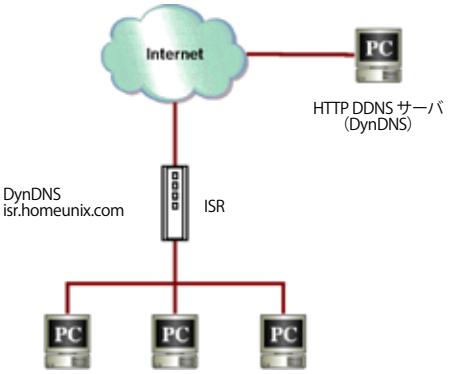


図 8.1. ネットワーク（HTTP DDNS）

設定した DDNS インターフェースの IP アドレスが変更されると、DDNS 更新は特定の DDNS サービスプロバイダへ送られます。本ルータは DDNS サービスプロバイダから入手した DDNS ユーザ名とパスワードで構成されます。

8.1 DDNS 設定パラメータ

表 8.1 は DDNS サービス用の設定パラメータです。

表 8.1. DDNS 設定パラメータ

フィールド	説明
Interface	DDNS サービスを使用するインターフェースを選択します。
Status	DDNS の状態を表示します。
Enable DDNS	DDNS サービスを有効にする場合は、ボックスにチェックを入れます。
Domain Name	登録したドメインネームを入力します。例：本ルータのホストネームは「host1」、ドメインネームが「yourdomain.com」の場合、FQDN 完全修飾ドメインネーム「host1.yourdomain.com」となります。
Username	DDNS サービスプロバイダより提供されたユーザーネームを入力します。
Password	DDNS サービスプロバイダより提供されたパスワードを入力します。

8.2 HTTP DDNS クライアントの設定

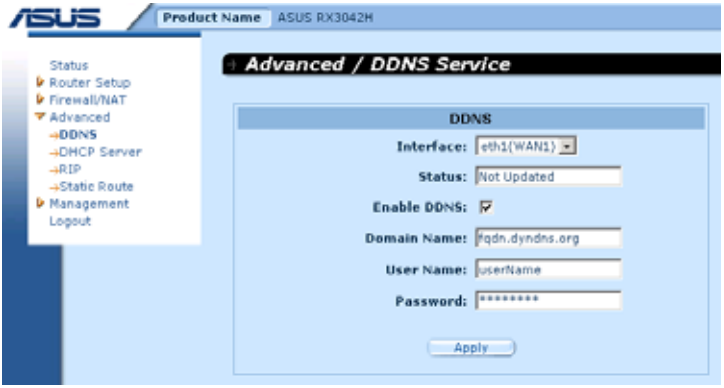


図 8.2. HTTP DDNS Configuration 画面

HTTP DDNS を設定する手順：

1. DDNS サービスプロバイダに登録済みのドメインネームが必要です。未登録の場合は、www.dyndns.org（英文）を参照し登録してください。
2. 「Advanced」→「DDNS Service」メニューの順にクリックし、「DDNS Configuration」画面を開きます。
3. DDNS サービスを使用するインターフェースを選択します。
4. 「Enable DDNS」のボックスにチェックを入れ、DDNS サービスを有効にします。
5. 登録済のドメインネームを「Domain Name」フィールドに入力します。
6. DDNS サービスプロバイダ提供のユーザーネームとパスワードを入力します。
7. 「Apply」ボタンをクリックし、DNS 更新リクエストを DDNS サービスプロバイダに送信します。WAN ポートの状態が変更された場合、DNS 更新リクエストは DDNS サービスプロバイダに自動的に送信されます。

9 ファイアウォールと NAT の設定

本ルータは、内蔵型ファイアウォール /NAT 機能を搭載しており、インターネットアクセス共有を提供する一方で、サービス拒否攻撃（DoS）等のユーザーの LAN へのアクセス攻撃からシステムを保護します。また、各攻撃やアクセスの監視方法を設定することができます。

ここでは、ルータのセキュリティ設定およびネットワークを通過するデータを制御するための ACL（Access Control List）ルールを作成・修正・削除する方法を記載しました。ファイアウォール設定画面では、以下の設定が可能です。

- 世界標準のファイアウォール の設定と DoS 設定
- ACL ルールの作成・修正・削除・参照

注：ACL ルールを定義すると、全ての受信パケットはある基準に基づいて調査されます。基準にはネットワークまたはインターネットのプロトコル、送信方向（例：LAN からインターネットまたはその逆）、送信元コンピュータの IP アドレス、受信先の IP アドレス、他のパケットに付随する特長が含まれます。

基準を充たすパケットは、設定したアクションに従って、受信される（送信先に転送）か拒否（破棄）されることになります。

9.1 ファイアウォール

9.1.1 ステートフルパケットインスペクション

ステートフルパケットインスペクションエンジンは、ファイアウォールを通過するパケットの通信状態を記録しているステートテーブルを保存します。ファイアウォールは「トンネル」を作り、通過するパケットがステートフルパケットインスペクションエンジンに保存されているかを判断します。既に確立された通信はパケットを通過させ、条件を充たさない場合パケットは破棄されます。通信が切断されると、この「トンネル」は閉じられます。ステートフルパケットインスペクションは、ファイアウォールが有効に設定されいる場合は初期設定で有効になっていますので、特別な設定は不要です。ファイアウォールの設定については、セクション 9.3.1 をご覧ください。

9.1.2 DoS（Denial of Service）プロテクション

DoS プロテクションとステートフルパケットインスペクション は、重要なネットワーク保護機能です。本ルータのファイアウォールが有効に設定されている限り、特別な設定をする必要はありません。また、ファイアウォールは工場出荷時の状態で有効に設定されています。ファイアウォールの設定の詳細は、セクション 9.3.1 をご覧ください。

9.1.3 ファイアウォールと Access Control List（ACL）

9.1.3.1 ACL ルールの優先順位

ACL ルールには全てルール ID が割り当てられます（番号が小さい ID を優先）。ファイアウォールはパケットのヘッダ情報からトラフィックをモニターし、ACL ルールテーブルと照合して、パケットの破棄 / 転送を判断します。全てのルールに照らし、番号が小さい ID の ACL ルールから順に照合を行います。マッチしなかった場合は設定したアクションに従って、パケットは破棄または転送されます。

9.1.3.2 接続追跡

ファイアウォールのステートフルパケットインスペクションエンジンは、ネットワーク接続状態を追跡します。ステートテーブル内の接続に関する情報を保存することによって、ファイアウォールを通過したパケットが、以前に接続したことがあるかを即座に確認します。以前に接続されたことがあれば、ACL ルール に照合せずにファイアウォールを通過させます。

例えば、ある ACL ルールで 192.168.1.1 から 192.168.2.1. の送信 ICMP パケットを許可するように設定した場合、192.168.1.1 が ICMP エコー要求（例：ping パケット）を 192.168.2.1 へ送ると、192.168.2.1 は 192.168.1.1 に ICMP エコー応答を送ります。本ルータでは、ステートフルパケットインスペクションエンジンが接続状態を追跡・記録し、ICMP エコー応答にファイアウォールを通過させるので、着信 ACL ルールを新しく作成する必要はありません。

9.1.4 ACL ルールの初期設定

本ルータがサポートするアクセスルールには次項に記載のとおり、２タイプあります。

- ACL ルール：LAN と DMZ（非武装地帯）上のコンピュータへのアクセス制御と、LAN と DMZ 上のホストから外部ネットワークへのアクセス制御
- セルフアクセスルール：本ルータ自体へのアクセス制御

初期設定のアクセスルール

- 外部ホストからの LAN と DMZ 上のホストへのトラフィックを全て拒否します。
- LAN からのトラフィックを全て NAT で外部ネットワークに転送します。

警告：ACL ルールテーブルから初期設定の ACL ルールを削除する必要はありません。初期設定より優先順位の高いルールを作成し、初期設定に上書きすることをお勧めします。

9.2 NAT

NAT（Network Address Translation）では、本ルータなどのデバイスを、インターネット（パブリックネットワーク）とローカル（プライベート）ネットワーク間を通信する媒体として動作させます。言い換えれば、ネットワークの外部に存在する対象物に対し、NAT IP アドレスは 1 つのコンピュータ群を代表するアドレスとなります。NAT はネットワークのグローバル IP の節約、IP アドレシング業務を簡易化するメカニズムといえます。また、NAT は IP アドレスを変換することで、実際のネットワークアドレスを隠し、ローカルネットワークを保護します。

サポートしている NAT モードは静的 NAT、動的 NAT、NAPT、リバース静的 NAT、リバース NAPT です。

9.2.1 NAPT（Network Address and Port Translation）、PAT（Port Address Translation）

IP マスカレードとも呼ばれ、1 つのグローバルアドレスに複数の内部ホストをマップします。ローカルネットワークのパケットは全てグローバルアドレスに変換され、ポート番号はパブリックネットワークポートの未使用ポートに変換されます。図 9.1 はローカルネットワーク上の全てのホストが、1 つのグローバル IP アドレスと異なる複数のポート番号にマッピングすることにより、インターネットにアクセスすることを示しています。

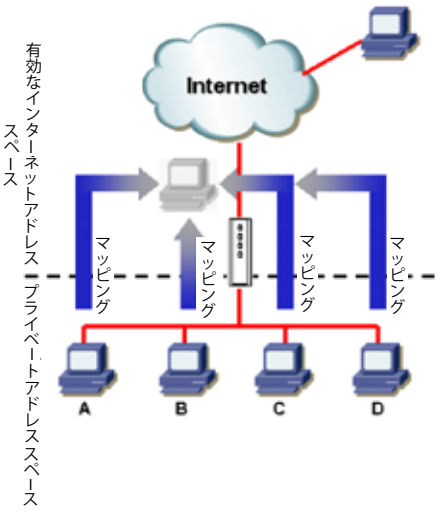


図 9.1 NAPT – 1 つのグローバル IP アドレスに内部 PC をマッピング

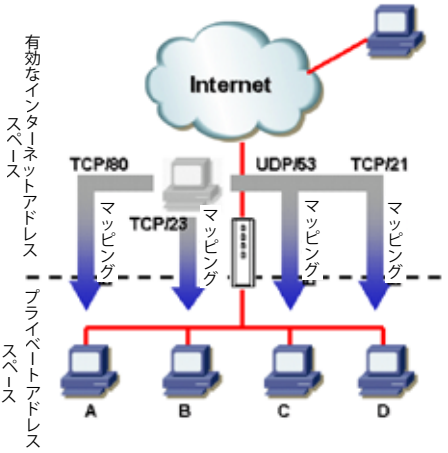


図 9.2 リバース NAPT – プロトコル、ポート番号、IP アドレスに基づき、受信パケットを内部ホストに中継

9.2.2 リバース NAPT / 仮想サーバ

リバース NAPT は、着信マッピング、ポートマッピング、仮想サーバとも呼ばれます。外部から 本ルータに送られるパケットを、ACL ルールで特定したプロトコルとポート番号、IP アドレスに基づき内部ホストに中継します。異なる内部ホストで複数のサービスを提供する場合に便利です。図 9.2 の PC <A> は Web サーバ（TCP/80）、PC <B> は Telnet サーバ（TCP/23）、PC <C> は DNS サーバ（UDP/53）、PC <D> は FTP サーバ（TCP/21）のホストで、各サービスの着信トラフィックが各サービスのホストに導かれることを示しています。

9.3 ファイアウォール設定（Firewall/NAT → Settings）

9.3.1 ファイアウォールオプション

表 9.1 はファイアウォールオプションのパラメータです。

表 9.1. ファイアウォールオプションのパラメータ

フィールド	説明
DoS Check	このチェックボックスで、DoS チェックの有効 / 無効を切り替えます。DoS チェックを無効にすると、以下の機能が無効になります。 • ステートフルパケットインスペクション • DoS 攻撃チェックを全てスキップする機能
Default NAT	WAN インターフェース経由のトラフィックが全て NAT デバイスで変換されている場合、このボックスにチェックを入れます。
Log Port Probing	このオプションを有効にすると、閉じられたポートへの接続の試行はログされます。
Stealth Mode	有効にすると、本ルータはリモートピアが閉じられた TCP/UDP ポートへ接続を試行しても、応答しません。

ファイアウォールを設定するには、以下の手順に沿ってください。

1. 「Firewall/NAT」→「Settings」メニューの順にクリックして「Firewall Settings Configuration」画面を開きます。（図 9.3）
2. 各チェックボックスで、ファイアウォールのオプションを設定します。
3. 「Apply」ボタンをクリックし、設定を適用します。

9.3.2 DoS 設定

本ルータは SYN フラッド、IP スマーフ、LAND、Ping of Death 等の Denial of Service（DoS）攻撃から内部ネットワークを保護する攻撃防御機能を搭載しており、ICMP リダイレクトや IP ルース / ストリクトソースルーティング（Loose/Strict Source Routing）パケットを破棄します。例えば、セキュリティデバイスと RX3042 のファイアウォールを組み合わせることで、インターネット上の無防備な Windows システムをクラッシュさせるプログラム「WinNuke」からの防御が可能です。また、本ルータのファイアウォールは様々なインターネット攻撃（IP スプーフ、Ping of Death、Land 攻撃など）からネットワークを保護します。本ルータの DoS 防御機能についての詳細は 表 2.1 をご覧ください。

9.3.2.1 DoS 防御設定パラメータ

表 9.2 は DoS 攻撃についての説明です。ボックスにチェックを入れると、各 DoS 攻撃に対する防御機能が有効になります。

表 9.2. DoS 攻撃定義

フィールド	説明
IP Source Route	「ソースルーティング」を利用してターゲットシステムに侵入します。
IP Spoofing	「なりすまし」とも呼ばれ、偽装した IP アドレスで TCP/IP パケットを作成します。偽装したパケットには応答を必要としません。
Land	発信元 IP アドレスと同じ送信先 IP アドレスをターゲットシステムに送信すると、ターゲットシステムは無限の自分自身への接続を解決しようとするため、システムが大幅に遅くなります。
Ping of Death	64KB 以上のパケットを送信し、システムをクラッシュさせます。
Smurf	ICMP エコー要求をブロードキャストします。送信元はターゲットの「なりすまし」です。受信先は ICMP エコー応答を送信しますが、なりすまし IP として利用されたターゲットへ膨大な量の応答が送くられることになります。

フィールド	説明
SYN/ ICMP/ UDP Flooding	SYN/ICMP/UDP フラッド。大量の TCP SYN/ICMP/UDP を短時間で送信します。本ルータでは、通常トラフィックへの影響を避けるため、フラッドパケットを破棄しません。 Threshold（閾値）：受信レート（パケット / 秒、pps）がこの値を超過すると、パケットは破棄されます。有効なレンジは 50 ～ 65535 です。
TCP XMAS/ NULL/ FIN Scan	特殊なフォーマットのパケットを送信し、システムをスキャンすることによって、どのサービスが利用可能かを確認し、攻撃に弱いサービスを調べて攻撃に利用します。 XMAS scan：シーケンス番号 0 番、FIN、URG、PUSH bit の TCP パケット。 NULL scan：シーケンス番号 0 番と制御ビットが 0 にセットされた TCP パケット。 FIN scan：「ステルス」でターゲットシステムをスキャンし、FIN スキャンを利用することで、実際に接続することなくシステムへの接続は可能かどうかを確かめます。エラーが生じますが、サービスが利用可能かで返ってくるエラーが異なるため、サービスを見分ける際に利用されます。
Re-assembly	ティアドロップ攻撃では、攻撃側の IP の 2 番目以降のフラグメントのオフセットが複雑になっています。受信側の OS がこの状況に対応していない場合は、システムがクラッシュする可能性があります。
WinNUKE	旧バージョンの Microsoft Windows OS はこの攻撃に対し脆弱です。LAN 内のコンピュータが最新のバージョンまたはパッチでアップデートされていない場合は、この項目を有効にすることをお勧めします。

9.3.2.2 DoS 設定

手順

1. 「Firewall」→「Settings」メニュー の順にクリックし、「ファイアウォール全般設定」画面を開きます。（図 9.3）
2. 個々の DoS 攻撃のタイプにチェックを入れます。
3. 「Apply」ボタンをクリックし、設定を適用します。

図 9.3. ファイアウォール 全般設定 画面

9.4　ACL ルール設定パラメータ

9.4.1　ACL ルール設定パラメータ

表 9.3 は、ファイアウォールの着信 ACL ルール、送信 ACL ルール、セルフアクセス ACL ルールの設定項目です。

表 9.3. ACL ルール設定パラメータ

フィールド	説明
Traffic Direction – 選択オプションをドロップダウンリストから選択し、ACL を設定します。 デュアル WAN 設定には 2 つのオプション – LAN → WAN、WAN → LAN WAN + DMZ 設定には 6 つのオプション – LAN → WAN、WAN → LAN、LAN → DMZ、DMZ → LAN、WAN → DMZ、DMZ → WAN	
ID	
Add New	クリックして ACL ルールを追加します。
Rule Number	ドロップダウンリストからルールを選択し、設定を変更します。
Move to ルールの優先順位を設定します。本ルータのファイアウォールはこの優先順位に基づき動作します。ルールに番号を割り当て優先順位を設定します。	
1	最優先
他の数値	優先順位の高いルールから順に小さい番号を割り当てます。
Log ACL ルールでロギングする場合はボックスにチェックを入れます。	
Action	
Allow	許可ルールとして設定します。 ルールにマッチするパケットを通過させます。
Deny	拒否ルールとして設定ます。 ルールにマッチするパケットを拒否させます。
Route to – パケットが特定のインターフェースに経路設定されている場合以外は「AUTO」にします。 設定オプションは AUTO、eth1（WAN1）、eth2（WAN2）、PPP1（WAN1-unnumbered）、PPP1（WAN2-unnumbered）、PPP3（WAN1-PPPoE1）、PPP4（WAN1-PPPoE2）、PPP5（WAN2-PPPoE1）、PPP6（WAN2-PPPoE2）です。WAN インターフェース が DMZ にセットされている場合、利用できるのは AUTO、eth1、PPP1/3/4 のみです。これらのオプションはドロップダウンリストから選択します。「AUTO」を選択した場合、経路制御表の情報に基づいてパケットの経路が決定されます。	

フィールド	説明
NAT	
None	この ACL ルールで NAT を使用しない場合、このオプションを選択します。
IP Address	ここで指定する IP アドレスは送信トラフィックのソース IP アドレスとして使用されます。
Auto	本ルータはトラフィックが転送されるインターフェースの IP アドレスを自動的にソース IP アドレスとして使用します。NAT が 送信トラフィックに使用される場合、このオプションを選択することをお勧めします。
Priority マッチしたトラフィックに転送優先順位を割り当て、優先度順位の高いパケットが優先されて送信されます。初期設定では、パケット転送の優先順位は IP ヘッダの TOS フィールド内の順位で決定されます。例:パケットの TOS 順位の値が 5 である場合、このパケットの転送順位は 5 となります。	
Source このオプションでは、このルールが適用されるソースネットワークを設定します。ドロップダウンリストで以下のオプションが選択可能です。	
Any	このルールをソースネットワーク内のコンピュータ全てに適用します。(例：着信トラフィック用のインターネット上のコンピュータや、送信トラフィック用のローカルネットワーク内のコンピュータ全て)
IP Address	このオプションで、このルールを適用する IP アドレスを特定します。
IP Address	適切なネットワークアドレスを特定します。
Subnet	IP サブネットに接続されたコンピュータ全てインクルードします。このオプションを有効にすると、以下のフィールドが利用可能になります。
フィールド	説明
Address	適切な IP アドレスを入力。
Mask	対応するサブネットマスクを入力。
MAC Address	このルールを適用する MAC アドレスを特定することができます。
MAC	希望する MAC アドレスを入力。

Destination ルールを適用する送信先のネットワークを設定します。ドロップダウンリストで以下のオプションから 1 つ選択します。	
Any	着信トラフィック用ローカルネットワークのコンピュータ全てと、送信トラフィック用のインターネット内のコンピュータ全てにこのルールを適用します。
IP Address、Subnet	オプションを選択し詳細を入力します。（上記 Source IP セクション参照）
Service ルールが適用されるサービスをドロップダウンリストから選択します。希望する サービス が見つからない場合、「Edit」ボタンをクリックし新しいサービスを追加してください。	
Time このルールを適用するタイムスロットを選択します。	
Enable	ACL ルールを指定した時間で有効にする場合、ボックスにチェックを入れます。チェックを外すとルールを常に適用します。
Date and Time	ACL ルール用に、希望する日時にチェックを入れます。

表 9.4. サービス設定パラメータ

フィールド	説明
Service Name 新しいサービスを識別するための名前を入力します。	
Protocol プロトコルタイプをドロップダウンリストから選択します。設定オプションは All、TCP、UDP、ICMP、IGMP、AH ESP、TCP/UDP です。	
Port このデバイスで使用するポートナンバーを特定します。ドロップダウンリストで以下のオプションから 1 つ選択します。	
Any	サービスは任意のアプリケーションを指定するために使用されます。
Single	サービスは特定のポートナンバーを使用します。
Port Number	ポートナンバーを入力します。

フィールド	説明
Range	サービスでポートレンジを使用する場合、この項目を選択します。このオプションを選択すると、以下のフィールドが入力可能になります。
Start Port	レンジの起点となるポートナンバーを入力します。
End Port	レンジの終点となるポートナンバーを入力します。

このオプションでは、このサービス用の ICMP メッセージタイプを選択します。サポートしている ICMP メッセージタイプは以下の通りです。

- Any（全て：初期設定値）
- 0：Echo reply（エコー応答）
- 1：Type 1（タイプ 1）
- 2：Type 2（タイプ 2）
- 3：Dst unreach：destination unreachable（宛先到達不能）
- 4：Src quench：source quench（発信制御）
- 5：Redirect（ルート変更）
- 6：Type 6（タイプ 6）
- 7：Type 7（タイプ 7）
- 8：Echo req：（エコー要求）
- 9：Router advertisement（ルータ通知）
- 10：Router solicitation（ルータ要求）
- 11：Time exceed：time exceeded（時間超過）
- 12：Parameter problem（パラメータ異常）
- 13：Timestamp request（タイムスタンプ要求）
- 14：Timestamp reply（タイムスタンプ応答）
- 15：Info request：information request（情報要求）
- 16：Info reply：information reply（情報応答）
- 17：Addr mask req：address mask request（アドレスマスク要求）
- 18：Addr mask reply：address mask reply（アドレスマスク応答）

9.5　ACL ルールを設定する –（Firewall → ACL）

「ACL Configuration」画面で ACL ルールを作成することで、ネットワークが信用できるか否かにかかわらず、アクセスを制御（許可 / 拒否）することができます。（図 9.4）
この画面で設定できるオプション

- ルールの追加とパラメータの設定
- ルールの変更
- ルールの削除
- ACL ルールの参照

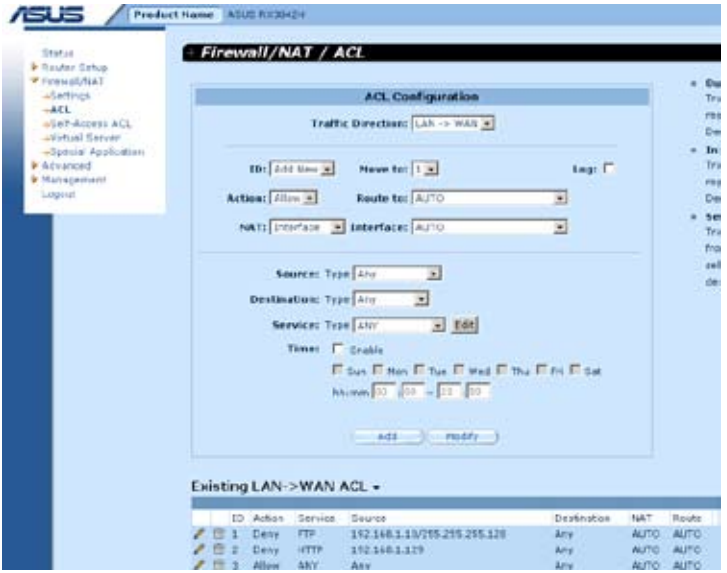


図 9.4. ACL Configuration 画面

9.5.1 ACL ルールを追加する

手順

1. 「Firewall」→「ACL」メニューの順にクリックし、「ACL Rule Configuration」画面を開きます。（図 9.4）
2. 「Traffic Direction」ドロップダウンリストからオプションを選択します。例：ACL を作成し、LAN から WAN へのトラフィックをフィルターする場合、「LAN → WAN」オプションを選択します。
3. 「ID」ドロップダウンリストから「Add New」を選択します。
4. 希望するアクション（許可 / 拒否）を「Action」ドロップダウンリストから選択します。
5. トラフィックを特定のインターフェースに設定する場合、「Route To」ドロップダウンリストからオプションを選択します。トラフィックを自動的に経路設定する場合は、「AUTO」を選択します。
6. NAT タイプを選択し、必要な関連情報を入力します。
7. 各フィールドの設定変更：ソース / 宛先 IP、サービス、タイム、ログ。（詳細：表 9.3 参照）

8. このルールの優先順位は、「Move to」ドロップダウンリストで割り当てます（「１」が最優先）。ファイアウォールは優先度が高いものからチェックを行います。
9. 「Add」ボタンをクリックし、新しい ACL ルールを作成します。作成すると、「Inbound ACL Configuration」画面の下にある新しい ACL ルールが着信アクセスコントロールのリストに表示されます。

図 9.5 は IP アドレス 192.168.1.129 のホストからの送信 HTTP トラフィックを拒否するルールを作成した例です。

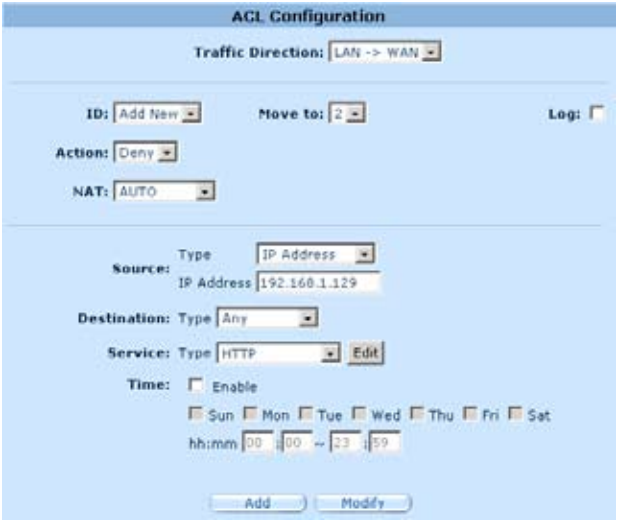


図 9.5. ACL 設定の 1 例

Existing LAN->WAN ACL

	ID	Action	Service	Source	Destination	NAT	Route
	1	Deny	FTP	192.168.1.10/255.255.255.128	Any	AUTO	AUTO
	2	Deny	HTTP	192.168.1.129	Any	AUTO	AUTO
	3	Allow	ANY	Any	Any	AUTO	AUTO

図 9.6. サンプル LAN → WAN ACL リスト表

9.5.2 ACL ルールを変更する

手順

1. 「Firewall/NAT」→「ACL」メニューの順にクリックし、「ACL Rule Configuration」画面を開きます。
2. 着信 ACL リスト表に表示されているアイコン から変更するルールのアイコンをクリックするか、ID ドロップダウンリストから変更するルールの番号を選択します。
3. IP、サービス、Time、Log の各項目で設定を変更します。（表 9.3 参照）
4. 「Modify」ボタンをクリックし、ACL ルールを変更します。新しい設定は「ACL Configuration」画面の下にあるアクセスコントロールのリストに表示されます。

9.5.3 ACL ルールを削除する

ACL ルールを削除する際は、ルールの左に表示されているアイコン をクリックします。

9.5.4 ACL ルールを表示する

既存の ACL ルールを表示するには、「Firewall/NAT」→「ACL」メニューの順にクリックして「ACL Rule Configuration」画面を開きます。開いたら、「Traffic Direction」のドロップダウンリストでトラフィックの方向を選択します。

9.6 セルフアクセス ACL ルールを設定する –（Firewall/NAT → Self-Access ACL）

セルフアクセスルールは本ルータの双方向のアクセスをコントロールし、各設定は「Self-Access Rule Configuration」画面で行います。（図 9.7 参照）

- セルフアクセスルールの追加
- セルフアクセスルールの変更
- セルフアクセスルールの削除
- セルフアクセスルールの確認

図 9.7. Self-Access ACL Configuration 画面

9.6.1　セルフアクセスルールの追加

手順

1. 「Firewall/NAT」→「Self-Access ACL」メニューの順にクリックし、「Self-Access Rule Configuration」画面を開きます。
2. 「ID」ドロップダウンリストから「Add New」を選択します。
3. 希望するアクション（許可 / 拒否）を「Action」ドロップダウンリストから選択します。
4. 「Move to」ドロップダウンリストから数値を選択し、このルールの優先順位を決定します（最優先は「１」）。ファイアウォールは優先順位が高いルールからチェックしていきます。
5. Source/Destination IP、Service、Time、Log の各項目で変更したい設定を変更します。（詳細：表 9.3 参照）
6. 「Add」ボタンをクリックし、新しいセルフアクセスルールを作成します。ここで作成した新しいルールは「Self-Access ACL Configuration」画面下の「Existing Self-Access ACL」リスト表に表示されます。

例

図 9.8 は、任意のソースから本ルータへの HTTP トラフィックを全て許可するセルフアクセス ACL 設定のサンプルです。

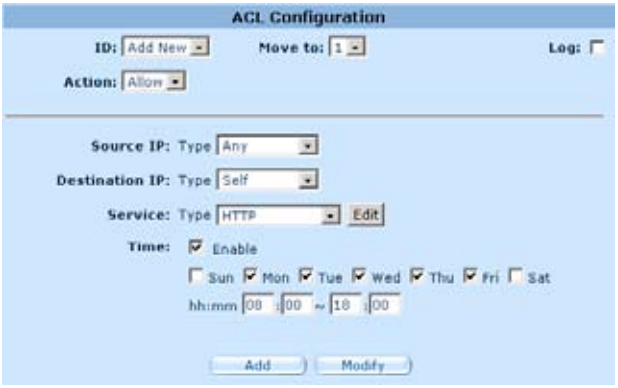


図 9.8. セルフアクセス ACL Configuration の 1 例

9.6.2 セルフアクセスルールの変更

手順

1. 「Firewall/NAT」→「Self-Access ACL」メニューの順にクリックし、「Self-Access ACL Configuration」画面を開きます。
2. 「Existing Self-Access ACL」の表から変更するセルフアクセスルールのアイコンをクリックするか、「ID」ドロップダウンリストから「Self-Access ACL」を選択します。
3. Action、Source/Destination IP、Service、Time、Log の各項目で変更したい設定を変更します。（詳細：表 9.3 参照）
4. 「Modifiy」ボタンをクリックし、変更を適用します。ここで変更した設定は、「Self-Access ACL Configuration」画面下にある「Existing Self-Access ACL」リストに表示されます。

9.6.3 セルフアクセスルールの削除

セルフアクセスルールを削除するには、ルールの左に表示されているアイコン をクリックします。

9.6.4　設定済みのセルフアクセスルールを参照する

既存のセルフアクセスルールを参照するには「Firewall/NAT」→「Self-Access ACL」メニューの順にクリックし、「Self-Access ACL Configuration」画面を開きます。

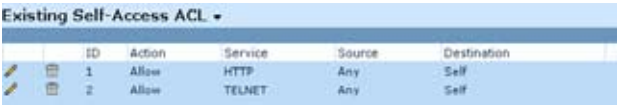


図 9.9 Self-Access ACL リストのサンプル

9.7　仮想サーバ（Vertual Server）を設定する

仮想サーバは、インターネット外部ユーザーがアクセス可能なパブリックサーバ（Web、E-mail、FTP サーバ等）を最高 10 まで設定することができます。各サービスは、固定 IP アドレスで設定した専用のサーバに提供されます。内部サービスアドレスは直接外部ユーザーがアクセスすることはできませんが、ルータはサービスポート番号によって要求されたサービスを特定し、適合する内部サーバにリダイレクトします。

注：本ルータは 1 度に 1 台のサーバしかサポートしません。

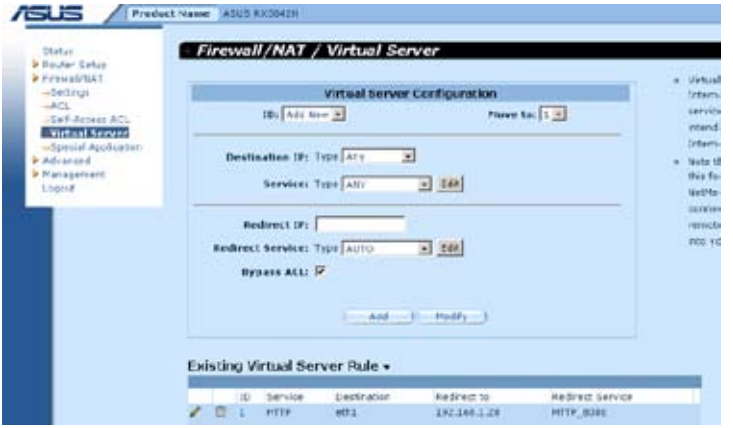


図 9.10. Virtual Server Configuration 画面

9.7.1　仮想サーバ設定パラメータ

表 9.5 は、仮想サーバの設定パラメータです。

表 9.5. 仮想サーバ設定パラメータ

設定	説明
ID	
Add New	クリックして、新しい仮想サーバを追加します。
Number	仮想サーバの ID をドロップダウンリストから選択し、設定を変更します。
Move to このオプションで、仮想サーバルールチェックの優先順位を設定します。NAT はこの順位に基づいて IP / ポートマッピング を行います。数を指定して優先順位を設定してください。	
1	最優先。
他の数値	他の数を指定し、ルールの優先順位を指定します。
Destination IP このオプションは、このルールを適用する送信先ネットワークを設定します。ドロップダウンリストで以下のオプションから選択します。	
Any	
IP Address	仮想サーバのパブリック IP アドレスが分かる場合、仮想サーバの IP アドレスを入力します。
Interface	選択したインターフェースの IP アドレスを送信先 IP アドレスとして使用します。以下のオプションが利用可能です。 eth1 (WAN1) eth2 (WAN2) ppp1 (WAN1 – unnumbered) ppp2 (WAN2 – unnumbered) ppp3 (WAN1 – PPPoE 1) ppp4 (WAN1 – PPPoE 2) ppp5 (WAN2 – PPPoE 1) ppp6 (WAN2 – PPPoE 2)
Service	ルールを適用するサービスをドロップダウンリストから選択します。希望するサービスがリスト内にない場合は、「Edit」ボタンをクリックし、新しいサービスを作成します。
Redirect IP	着信トラフィックを受信させるコンピュータ（通常は LAN 上のサーバ）の IP アドレスを入力します。例：LAN 上にある Web サーバの IP アドレスが 192.168.1.28 である場合、192.168.1.28 と入力。

設定	説明
Redirect Service	ルールを適用するサービスをドロップダウンリストから選択します。希望するサービスがリスト内にない場合は、「Edit」ボタンをクリックして新しいサービスを作成します。
Bypass ACL	仮想サーバ上で、ファイアウォールによるアクセスコントロールを実行しない場合、このオプションにチェックを入れます。チェックを入れると仮想サーバ提供のサービスへのアクセスを全てのユーザーに許可します。ユーザーを制限する場合は、このオプションのチェックを外し適切な ACL ルールを作成してください。

表 9.6. 一般的なアプリケーション用のポートナンバー

アプリケーション	サービスポートナンバー
AOE II (Server)	2300-2400
AUTH	113
Baldurs Gate II	2300-2400
Battle Isle	3004-3004
Counter Strike	27005-27015
Cu See Me	7648-7648、56800、24032
Diablo II	4000-4000
DNS	UDP 53-53
FTP	TCP 21-21
FTP	TCP 20(ALG)-21
GOPHER	TCP 70-70
HTTP	TCP 80-80
THHP8080	TCP 8080-80880
HTTPS	TCP 443-443
I-phone 5.0	TCP/UDP 22555-22555
ISAKMP	UDP 500-500
mirc	66011-700
MSN Messenger	1863 ALG
Need for Speed 5	9400-9400
Netmeeting Audio	TCPP 1731-1731
Netmeeting Call	TCP 1720-1720
Netmeeting Conference	UDP 495000-49700
Netmeeting File Transfer	TCP 1503--1503

アプリケーション	サービスポートナンバー
Netmeeting or VoIP	1503-1503、1720(ALG)
NEWS	TCP 119-119
PC Anywhere	TCP 5631
PC Anywhere	TCP 5631、UDP 5632
POP3	TCP 110-110
Powwow Chat	13233-13233
Red Alert II	1234-1237
SMTP	TCP 25-25
Sudden Strike	2300-2400
TELNET	TCP 23-23
Win VNC	UDP 5800-5800

9.7.2 仮想サーバ例 1 – Web サーバ

図 9.11 は Web サーバ 配置のネットワークを図にしたものです。この Web サーバは TCP ポート 8080 を使用する HTTP サービスを提供します。

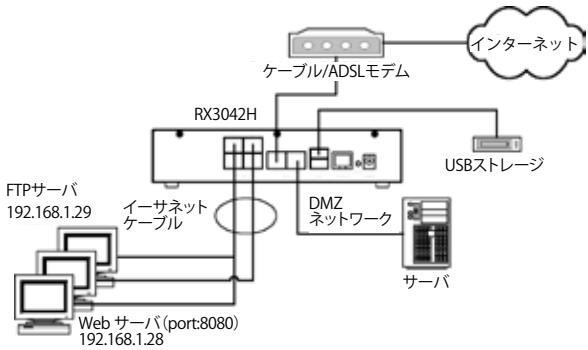


図 9.11. 仮想サーバの配置

以下は 図 9.11. に示した Web サーバをセットアップする手順です。

1. 「Firewall/NAT」→「Virtual Server」メニューの順にクリックし、「Virtual Server Configuration」画面を開きます。(図 9.10 参照)
2. 宛先 IP のタイプとサービスタイプを選択します。(図 9.12 参照)

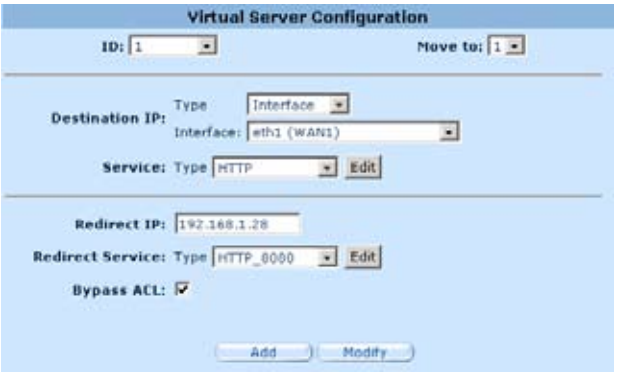


図 9.12. 仮想サーバ例 1 – Web サーバ

3. Web サーバの IP アドレス「192.168.1.28」を「Redirect IP」フィールドに入力します。

4. この Web サーバは標準的な TCP ポート 80 を使用していません。このため、http サービスを提供するには TCP ポート 80 を使用する http サービス用のサービスタイプを新規作成する必要があります。「Redirect Service」のフィールドの「Edit」ボタンをクリックし、新しいサービスを作成します。表示される「Service Configuration」画面で、サービスネームとプロトコル及びポートナンバーを入力し（図 9.13）、「Add to list」をクリックして新しいサービスタイプ「HTTP_8080」を作成します。最後に「Save & Exit」ボタンをクリックしこのサービスを保存します。

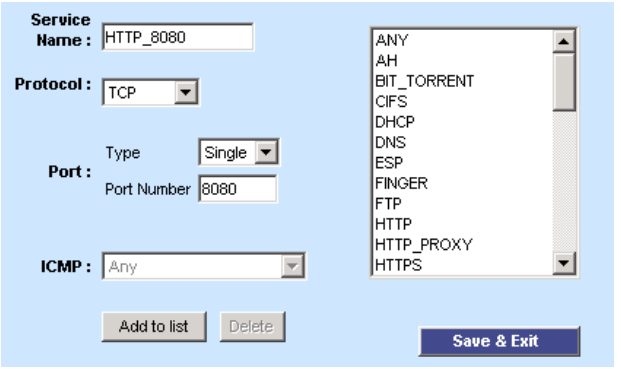


図 9.13. 新しいサービスの追加

5. サービス、HTTP_8080 を「Redirect Service」ドロップダウンリストから選択します。
6. 「Add」ボタンをクリックし、仮想サーバ設定を追加します。

9.7.3 仮想サーバ例 2 – FTP サーバ

図 9.11 は FTP サーバ配置のネットワークを示したものです。この FTP サーバは標準 FTP ポートを使用して FTP サービスを提供します。

以下は 図 9.11. に示した FTP サーバをセットアップする手順です。

1. 「Firewall/NAT」→「Virtual Server」メニューの順にクリックし、「Virtual Server Configuration」画面を開きます。（図 9.10）
2. 必要な情報を入力します。（図 9.12）
3. 「Add」ボタンをクリックし、仮想サーバ設定を追加します。

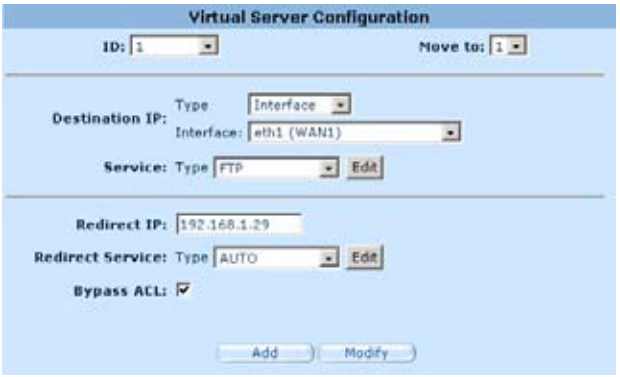


図 9.14. 仮想サーバ例 2 – FTP サーバ

9.7.4 仮想サーバ例 3 – FTP サーバ（アクセスコントロール付き）

この例は、前述の「仮想サーバ 例 2」に類似していますが、ファイアウォール ACL ルールによるアクセスコントロールを利用し、FTP サーバのネットワーク（168.192.128.0）へのアクセスを制限します。

手順

1. FTP 仮想サーバを作成する

a）「Firewall/NAT」→「Virtual Server」メニューの順にクリックし、「Virtual Server Configuration」画面を開きます。（図 9.10）

b）必要な情報を入力します。（図 9.12）

c）「Bypass ACL」ボックスにはチェックを入れないでください。

d）「Add」をクリックし仮想サーバ 設定を追加します。

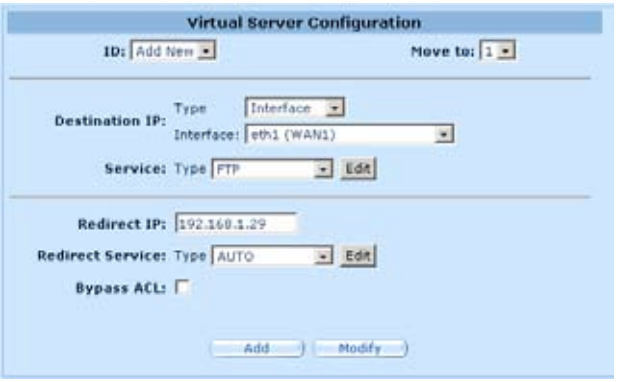


図 9.15. 仮想サーバ例 3 – FTP サーバ

2. ACL ルールを作成し FTP サーバへのアクセスをコントロールする

a）「Firewall」→「ACL」メニュー の順にクリックし、「ACL Rule Configuration」画面を開きます。（図 9.4）

b）「WAN → LAN」オプションを「Traffic Direction」ドロップダウンリストから選択します。

c）「Add New」を「ID」ドロップダウンリストから選択します。

d）「Allow」を「Action」ドロップダウンリストから選択します。

e）「Subnet」を「Source Type」ドロップダウンリストから選択します。

f）「Source：」 の「Address」 と「Mask」 の 各 フ ィ ー ル ド に「168.192.128.0」、「255.255.255.0」と入力します。

g）「FTP」を「Service Type」ドロップダウンリストから選択します。

h）「Move to」ドロップダウンリストから数値を選択し、このルールの優先順位を指定します（「１」が最優先）。ファイアウォールは優先度が高いものからチェックを行います。

i）「Add」ボタンをクリックし、新しい ACL ルールを追加します。

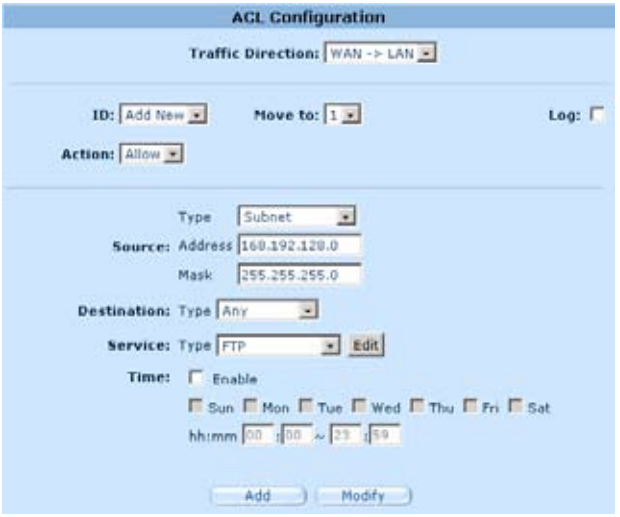


図 9.16. 仮想サーバ例 3 のファイアウォール ACL – FTP サーバ

9.8 スペシャルアプリケーションを設定する

特定のアプリケーションはデータ転送の際、複数の TCP/UDP ポートを使用しますが NAT 機能のため、これらのアプリケーションは本ルータで使用することができません。ただし、スペシャルアプリケーションを設定することで、これらのアプリケーションで利用できるものもあります。

注： 1 台の PC が 1 度に使用できるスペシャルアプリケーションは 1 つだけです。

9.8.1 スペシャルアプリケーションの設定パラメータ

表 9.7 は仮想サーバ の設定パラメータです。

表 9.7. スペシャルアプリケーションの設定パラメータ

設定	説明
Enabled	ボックスにチェックを入れポリシーを有効にします。
Trigger Protocol	プロトコルタイプをドロップダウンリストから選択します。選択オプションは TCP、UDP、TCP/UDP です。
Outgoing (Trigger) Port	アプリケーションが送信パケットを送信する際に使用するポートレンジです。送信ポートナンバーはトリガーとして機能します。ルータがこのポートナンバーの送信パケットを検出すると、「Incoming Port Range」フィールドで特定された着信ポートナンバーを含む着信パケットがルータを通過できるよう許可します。一般的なアプリケーションが使用するポートナンバーについては、表 9.8 をご覧ください。
Incoming Protocol	対応する着信パケットが使用するプロトコル。設定オプションは TCP、UDP、TCP/UDP。
Incoming Port	対応する着信パケットが使用するポートレンジ。一般的なアプリケーションが使用するポートナンバーについては 表 9.8 をご覧ください。このポートレンジは例のように表記します。例：100-200。複数のポートレンジは「,」で区切ります。例：100-200 , 700-800
Comment	アプリケーションの 説明 / コメントを入力します。例：アプリケーションの名前など

表 9.8. 一般的なアプリケーションのポートナンバー

アプリケーション	送信ポートナンバー	着信ポートナンバー
Battle.net	6112	6112
DialPad	7175	51200、51201、51210
ICU II	2019	2000-2038、2050-2051、2069、2085、3010-3030
MSN Gaming Zone	47624	2300-2400、28800-29000
PC to Phone	12053	12120、12122、150-24220
Quick Time 4	554	6970-6999
wowcall	8000	4000-4020
Yahoo Messenger	5050	5000-5101

9.8.2 スペシャルアプリケーションの例

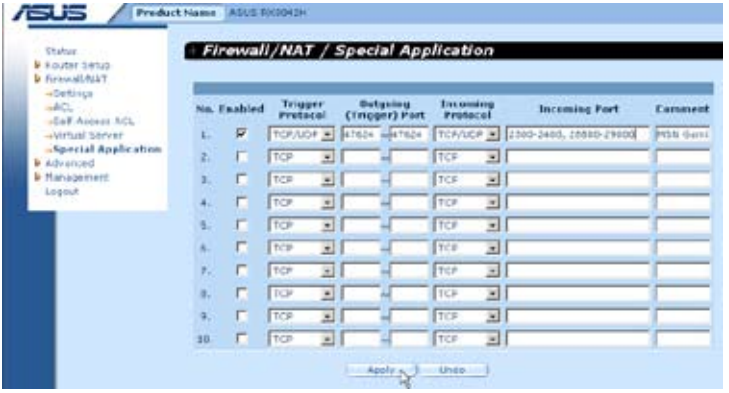


図 9.17. Special Application Configuration 画面

以下の手順は、MSN Gaming Zone 用のスペシャルアプリケーションのセットアップ手順です。

1. 「Firewall/NAT」→「Special Application」メニューの順にクリックし「Special Application Configuration」画面を開きます。（図 9.17）
2. 「Enabled」のボックスにチェックを入れます。
3. 「TCP/UDP」を「Trigger Protocol」ドロップダウンリストから選択します。アプリケーションが使用するプロトコルが TCP か UDP か不明な場合、「TCP/UDP」を選択します。
4. 「Outgoing Port」の各フィールドにレンジを入力します。（この例では「47624 ～ 47624」）
5. 「TCP/UDP」を「Incoming Protocol」ドロップダウンリストから選択します。アプリケーションが使用するプロトコルが TCP か UDP か不明な場合、「TCP/UDP」を選択します。
6. 「Incoming Port」のフィールドにレンジを入力します。（この例では「2300-2400」と「28800-29000」）
7. 「Comment」のフィールドにアプリケーションの名前を入力します。（例：MSN Gaming Zone）
8. 「Apply」ボタンをクリックし、設定を適用します。

10　USB アプリケーション

この Chapter では、FTP サービス経由でデータを共有するための USB ネットワークストレージの設定方法について記載しました。本ルータには USB ネットワークストレージ用の FTP サーバが組み込まれています。FTP サーバを使用する前に、ユーザーの USB ストレージが以下の条件を充たしていることを確認してください。

- HDD とフラッシュドライブのみをサポートしていること。CD ROM と DVD ドライブはサポートしていないこと。互換性のあるデバイスについては、www.asus.com をご覧ください。
- FAT/FAT32 と Linux EXT2 ファイルシステム用の読み込み / 書き込み機能をサポートすること。NTFS ファイルシステムをサポートしていないこと。
- 複数のパーティションが検出可能なデバイス：ただしパーティションは 5 つ目までしかアクセスできない。

注：本ルータは「Mass Storage Device」と検出される USB ストレージのみをサポートします（HDD やフラッシュドライブ）。ほとんどの互換性のある USB 記憶デバイスは plug and play ですので、接続する際は本ルータの電源をオフにする必要はありません。

10.1　USB デバイスを設定する

ネットワークストレージを設定する際は、以下の手順に沿ってください。

1. USB ストレージの電源がオンで、ルータ後部にある USB ポートに接続されていることを確認してください。
2. 「USB Application」→「Network Storage」メニューの順にクリックし、「Network Storage」画面を開きます。
3. USB ストレージにアクセスするため、「Character Set」ドロップダウンリストから適当な言語を選択します。USB ストレージが全て英語表記の場合は「English」を選択します。
4. 必要に応じて、FTP サービスをセットアップします。USB ストレージは FTP サービスを有効にするまで利用できません。FTP サーバ の設定を始めるには「Configuration」ボタンをクリックし、セクション 10.3「Configure FTP Service」の指示に沿って設定してください。

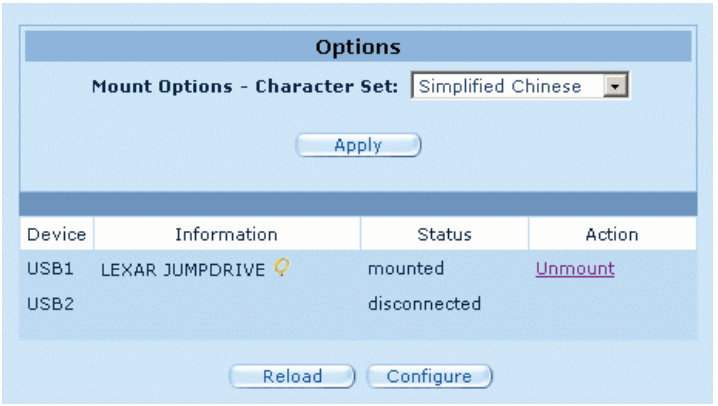


図 10.1. ネットワークストレージ – FTP サーバ設定

表 10.1. ネットワークストレージ設定

設定	説明
マウントオプション – 文字セット	USB ストレージにアクセスするため適当な言語を選択します。USB 記憶デバイスに簡体字中国語が含まれる場合、「Simplified Chinese」を選択します。選択オプションは簡体字中国語、繁体字中国語、英語です。
デバイス	USB 記憶デバイス 2 台までサポート
情報	USB デバイスのベンダー情報が表示されます。詳細を表示するにはアイコンをクリックします。
状態	Disconnected：デバイス未接続 Connected：デバイスは接続済みで使用されていない状態。FTP サービスが未設定、または USB ストレージのファイルシステムがサポートされていない場合に表示。 Mounted：デバイスは接続済みで使用中 FTP サーバが有効でデバイス上のファイルシステムがサポートされていれば、システムは自動的に接続した USB 記憶デバイスをマウント（実装）します。
アクション	Mount：本ルータが USB 記憶デバイスにアクセスできるようにし、FTP サーバからの本ルータへのアクセスを可能にします。 Unmount：USB ストレージをアンロードし、安全に取り外します。

10.2　接続した USB 記憶デバイスの状態を参照する

手順

1. 「USB Application」→「Network Storage」メニューの順にクリックし「Network Storage」画面を開きます。
2. 「Reload」ボタンをクリックし、接続した USB 記憶デバイスの最新の状態を表示します。

10.3　FTP サービスを設定する

手順

1. 「USB Application」→「Network Storage」メニューの順にクリックし、「Network Storage」画面を開きます。
2. 「Configuration」ボタンをクリックし、FTP サービスを設定します。
3. 希望のオプションをチェックします。詳細は表 10.2 をご覧ください。
4. （オプション）ユーザーネームとパスワードを入力し、ドロップダウンリストからアクセス権を選択します。このオプションは特定のユーザーが接続した USB ストレージにアクセスできる場合のみ必要なオプションです。
5. 「Apply」ボタンをクリックし、設定を適用します。

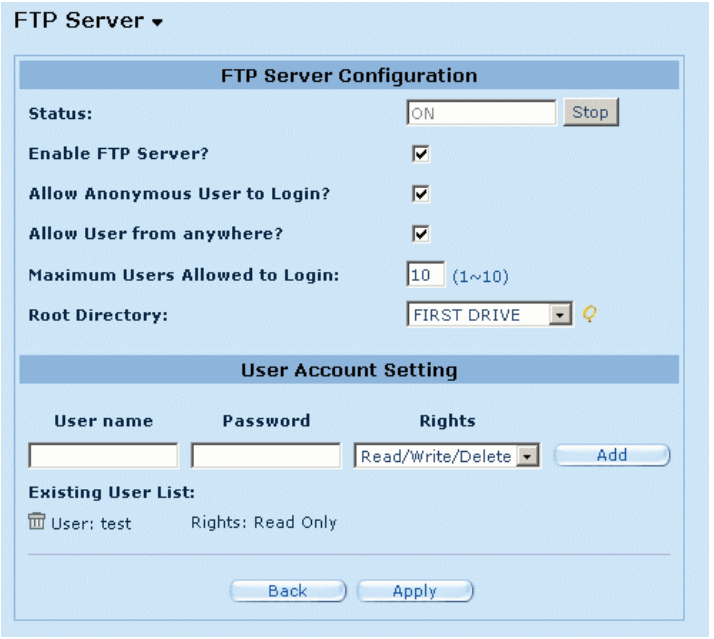


図 10.2. ネットワークストレージ – FTP Server 設定

表 10.2. FTP サーバ設定

設定	説明
Status	On：FTP サーバが有効 Off：FTP サーバが無効
Enable FTP Server	このボックスにチェックを入れると FTP サービスが有効になります。 FTP サーバが有効である場合、システムは接続した USB ストレージ デバイスを自動的に実装します。
Allow Anonymous User to Login	匿名ユーザーに FTP サービスへの読み取りアクセスを許可する場合、この項目を選択します。ユーザーネームは匿名または ftp で、パスワードは不要です。

設定	説明
Allow User from Anywhere	クライアントの所在地を制限しない場合はこの項目を選択します。この項目を選択しない場合は、Firewall/NAT → Sef-Access ACL で、FTP サービスにアクセスできるクライアントを制限する必要があります。 例：ユーザーの LAN ネットワーク 192.168.1.0/24 に FTP サービスへのアクセス権を与える。
Maximum Users Allowed to Login	FTP サービスに同時にログインできるユーザー数を入力します。最高 10 まで入力できます。
Root Directory	ユーザーの USB 記憶デバイスに複数のパーティションが存在する場合、適切なパーティション / ドライブを FTP サーバのルートディレクトリとして選択してください。 1 番目にマウントしたパーティションを FTP ルートディレクトリにする場合は、「First Drive」を選択してください。 FTP サーバがアクセスできるパーティションは 1 つだけです。

表 10.3. ユーザーアカウントの設定

設定	説明
User name	FTP アカウント用のユーザーネームを入力します。
Password	FTP アカウントのパスワードを入力します。
Rights	このフィールドはこの FTP アカウントに割り当てられたアクセス権を表示します。 Read/Write/Delete：このアカウントアクセス権を持つユーザーは、ドライブ上のファイルの読み取り / 書き込み / 削除が許可されます。 Read/Write：このアカウントアクセス権を持つユーザーは、ドライブ上のファイルの読み取り / 書き込みが許可されます。 Read Only：このアカウントアクセス権を持つユーザーはドライブ上のファイルの読み取りのみ許可されます。

11 システム管理

本章では、管理設定で実行できる管理業務を以下のように記載しました。

- 利用できるシステムサービスの設定
- パスワードの変更とシステム設定
- システム情報の閲覧
- システム日時の修正
- SNMP の設定
- システム設定を初期設定値に戻す
- システム設定のバックアップと復元
- システムの再起動
- ファームウェアの更新

11.1 システムサービスを設定する

図 11.1 のように、「System Services Configuration」の画面で 本ルータでサポートしているサービスの有効 / 無効を切り替えることができます。DDNS、SNTP、UPnP と RIP を除く全てのサービスは、初期設定で全て有効に設定されています。個々のサービスの設定を変更するには、以下の手順に沿ってください。

1. 「Management」→「System Services」メニューを開き、「System Services Configuration」設定画面を開きます。
2. 各項目のラジオボタン「Enable」/「Disable」で設定を変更します。
3. 「Apply」ボタンをクリックし変更を適用します。

図 11.1. System Services Configuration 画面

11.2　ログインパスワードとシステム設定

11.2.1 パスワードを変更する

「Configuration Management」に初めてログインするときは、初期設定値のユーザーネームとパスワード（admin と admin）を使用します。セキュリティの面から、このパスワードを変更することをお勧めします。

注：このユーザーネームとパスワードは「Configuration Management」用で、ISP に接続する際に使用するものではありません。

図 11.2. System Administration Configuration 画面

以下の手順に沿ってパスワードを変更します。

1. 「Router Setup」→「Administration」メニューと進み、「System Administration Configuration」画面を開きます。（図 11.2 参照）
2. ログインパスワードを変更する
   a）「New Password」のフィールドに新しいパスワードを入力し、確認のため「Confirm Password」のフィールドに再入力します。パスワードは最高 16 文字で大文字と小文字は区別されます。
3. 「Apply」ボタンをクリックします。

11.2.2 システム設定を設定する

以下の手順に沿って、システム設定を変更します。

1. 「Router Setup」→「Administration」メニューに進み、「System Administration Configuration」画面を開きます。（図 11.2 参照）

2. WAN 用 MAC アドレスをクローンする

a）プロバイダが提供するインターネットアクセス用の MAC アドレスを登録してある場合は、「Clone WAN MAC」のチェックボックスにチェックを入れ、登録されている MAC アドレスを入力します。

3. Allow Administration from WAN：このチェックボックスで WAN ポート経由の遠隔操作の有効 / 無効を切り替えます。

4. Allow Ping Interface：このオプションは、Ping を使用する LAN /WAN ポート経由のルータへのアクセスを制御することができます。有効にするインターフェースにチェックを入れてください。

5. 「Apply」ボタンをクリックし、設定を適用します。

11.3 シ ステム情報を閲覧する

「System Information」画面は本ルータにログインすると毎回表示されます。「Status」メニューをクリックしても、システム情報を閲覧することができます。この画面ではシステム全般の情報を閲覧することができます。

図 11.3. Status（システム情報）画面

11.4 日時を設定する

本ルータは日時を記録し、計算や様々なデータの報告に使用します。本ルータにはリアルタイムクロックが内蔵されていますが、外部タイムサーバを利用して時間データを維持することもできます。外部サーバは 3 台まで設定可能です。時間のデータを維持するには、「Enable」のチェックボックスにチェックを入れ、SNTP（Simple Network Time Protocol）サービスを有効にしてください。

注：本ルータの日時設定は、コンピュータ上の日時には影響しません。

図 11.4. Time Zone Congiguration 画面

ルータの時間を手動で変更する：

1. 「Management」→「Time Zone」メニューの順にクリックし、「Time Zone Configuration」画面を開きます。
2. 日時を入力します。
3. ドロップダウンリストでタイムゾーンを選択します。
4. 「Apply」ボタンをクリックし、設定を適用します。

リアルタイムクロックと外部タイムサーバの時間を同期化する手順：

1. 「Management」→「Time Zone」メニューの順にクリックし、「Time Zone Configuration」画面を開きます。
2. ドロップダウンリストでタイムゾーンを選択します。
3. 「Enable」にチェックを入れ、SNTP サービスを有効にします。
4. システムタイム更新に使用される SNTP サーバ用の IP アドレスを入力します。
5. 「Apply」ボタンをクリックし、設定を適用します。

11.4.1 システム日時を確認する

更新されたシステムの日時データを確認するには、「Configuration Management」にログインし、「Management」→「Time Zone」メニューをクリックします。

11.5 SNMP のセットアップ

SNMP（Simple Network Management Protocol）は名前の通り、ネットワーク管理に使用するプロトコルです。「SNMP Configuration」画面で SNMP サポートの有効 / 無効を切り替えることができます。

11.5.1 SNMP 設定パラメータ

表 11.1 は SNMP のセットアップの設定パラメータです。

表 11.1. SNMP 設定パラメータ

フィールド	説明
SNMP Enable	SNMP サポートを有効にするときのみ、ボックスにチェックを入れてください。
RO Community Name	コミュニティストリングはクリアテキストで設定され、SNMP 管理ステーションと本ルータのパスワードとして使用されます。この「Read Only」コミュニティネームは SNMP 管理ステーションが、本ルータの設定を読み取る際に使用します。
RW Community Name	コミュニティストリングはクリアテキストで設定され、SNMP 管理ステーションと本ルータ間のパスワードとして使用されます。この「Read and Write」コミュニティネームは SNMP 管理ステーションが、本ルータの設定の読み取りと設定を実行する際に使用します。
Trap Address	トラップメッセージは本ルータから発信され、本ルータの異変を SNMP 管理ステーションに伝えます。このフィールドには本ルータからのトラップメッセージを受信する SNMP 管理ステーションの IP アドレスを入力します。

11.5.2 SNMP を設定する

1. 「Management」→「SNMP」メニューの順にクリックし、「SNMP Configuration」画面を開きます。（図 11.5 参照）

図 11.5. SNMP Configuration 画面

2. 「SNMP Enable」ボックスにチェックを入れ、SNMP サポートを有効にします。
3. RO（read only）Community Name と R/W（read and write）Community Name を入力します。
4. 本ルータからトラップメッセージを受信する SNMP 管理ステーションの IP アドレスを入力します。
5. 「Apply」ボタンをクリックし、設定を適用します。

11.6 Log のセットアップ

ログメッセージはダイナミックメモリに保存され、システムを再起動すると失われます。ログメッセージのコピーを保存するには、Syslog サーバをセットアップし、本ルータにログメッセージをサーバに送信させます。

11.6.1 Syslog サーバでリモートログ機能をセットアップする

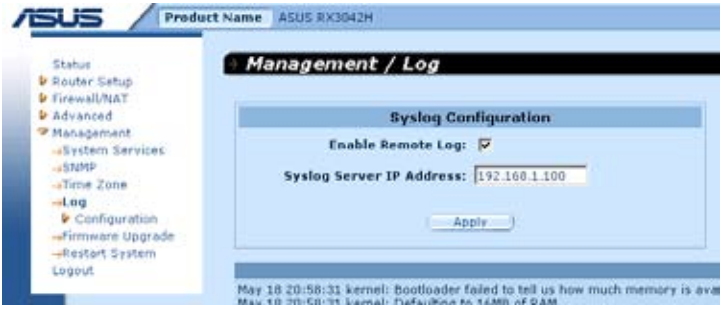


図 11.6. Syslog Configuration 画面

1. 「Management」→「Log」メニューの順にクリックし、「Log configuration」画面を開きます。（図 11.6 参照）
2. 「Enable Remote Log」ボックスにチェックを入れ、リモートログ機能を有効にします。
3. Syslog サーバ IP アドレスを「Syslog Server IP Address」のフィールドに入力します。
4. 「Apply」ボタンをクリックし、設定を適用します。

11.6.2 System Log を参照する

「Firewall/NAT」→「Log」メニューをクリックすると、ファイアウォールログ画面が開きログが表示されます。（図 11.7 はサンプルログ）画面下にある「Reload」ボタンをクリックすると、更新されたログメッセージが表示されます。ログをクリアするには「Clear Log」ボタンを、ログのコピーを保存するには「Download」ボタンをクリックします。

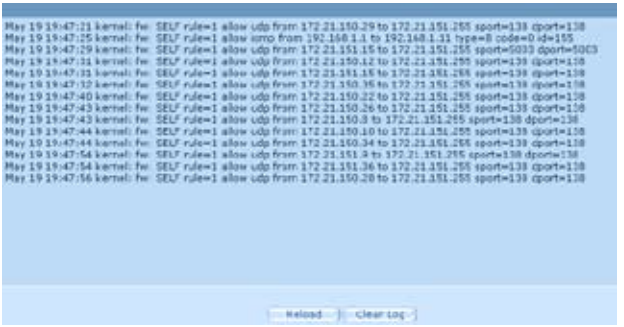


図 11.7 サンプルログ

11.7 システム設定を管理する

11.7.1 システム設定を工場出荷状態にリセットする

設定に誤りがあった場合など、システム設定を工場出荷時の状態にリセットする必要がある場合があります。リセットの際は以下の手順に沿ってください。

1. 「Management」→「Configuration」→「Factory Default」メニューの順にクリックし、「Factory Default Configuration」画面を開きます。（図 11.8 参照）

図 11.8 Factory Default 画面

2. 「Apply」ボタンをクリックし、システム設定を工場出荷状態の設定にリセットします。
3. 確認用のダイアログウィンドウが表示されますので（図 11.9）、リセットする場合は「OK」ボタンをクリックしてください。リセットしない場合は「Cancel」ボタンをクリックしてください。

図 11.9 リセット確認用画面

4. その後本ルータは再起動し設定がリセットされます。リセット中はリセットが終了するまでの時間がカウントダウンタイマーで表示されます。（図 11.10 参照）

図 11.10 工場出荷状態リセット カウントダウンタイマー

パスワードや IP アドレスを忘れたなど、本ルータにアクセスできなくなった場合は、リセットボタンを 5 秒間押してシステム設定を工場出荷状態にリセットしてください。本ルータの再起動後、システム設定は工場出荷状態に戻ります。

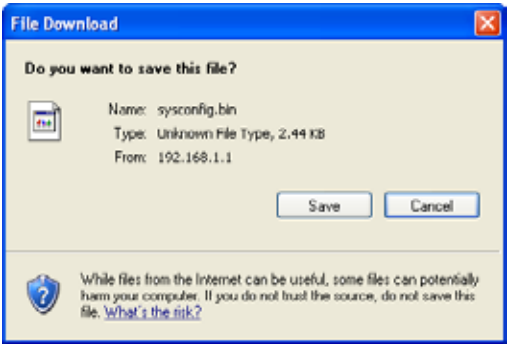
11.7.2 システム設定をバックアップする

手順

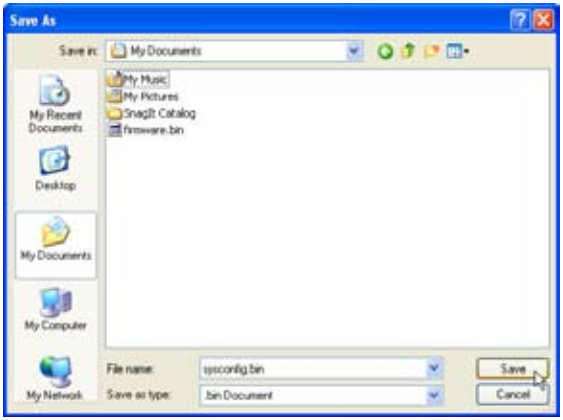
1. 「Management」→「Configuration」→「Backup」メニューの順にクリックし、「Configuration Backup」画面を開きます。
2. 「Apply」ボタンをクリックし、システム設定をバックアップします。

図 11.11 Backup Configuration 画面

3. 「Save」ボタンをクリックしシステム設定をバックアップします。



4. 「Save」ボタンをクリックしシステム設定をバックアップします。



11.7.3 システム設定を復元する

手順

1. 「Management」→「Configuration」→「Restore」メニューの順にクリックし、「System Configuration Restore」画面を開きます。

図 11.12 Restore Configuration 画面

2. 復元するシステム設定ファイルのパスと名前を「Configuration File」テキストボックスに入力します。また、「Browse...」ボタンをクリックしシステム設定ファイルをハードドライブから検索することもできます。ウィンドウが表示されますのでファイルを指定してください。（次項図 11.13）

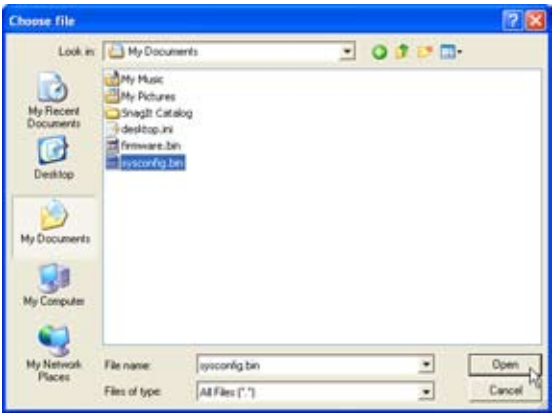


図 11.13 システム設定を選択

3. 「Apply」ボタンをクリックし、システム設定を復元します。下のような確認用のダイアログが表示されますので、継続するには「OK」ボタンを、キャンセルするには「Cancel」ボタンをクリックします。新しいシステム設定は本ルータ再起動すると、適用されます。

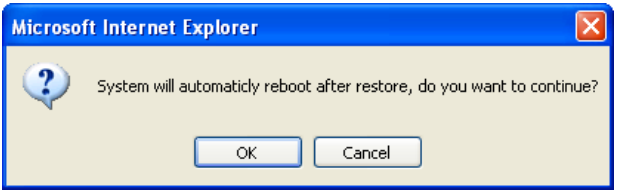


図 11.14 システム設定復元を確認するダイアログ

4. システム再起動までのカウントダウンタイマーが表示されます（図 11.15）。カウンターがゼロになると、本ルータに再接続します。自動的に再接続されない場合は、手動で再接続してください。

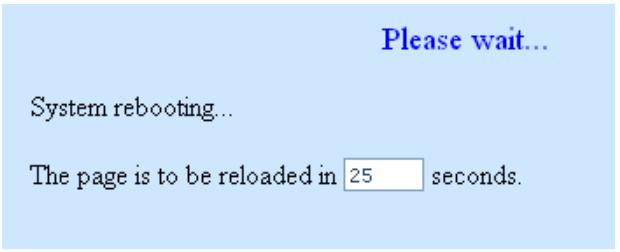


図 11.15 システム再起動 カウンタータイマー

11.8 ファームウェアを更新する

ASUSTeK では本ルータ用のファームウェアの更新版を随時提供しております。システムソフトウェアは全て 1 つのイメージを呼ばれるファイルに含まれています。「Configuration Management」では、ファームウェアイメージを簡単に更新することができます。手順は以下の通りです。

1. 「System」→「Firmware Upgrade」メニューをクリックし、「Firmware Upgrade」画面を開きます。（図 11.16）

図 11.16 Firmware Upgrade 画面

2. 「Select Firmware」テキストボックスにファームウェアイメージファイルのパスと名前を入力します。また、「Browse...」ボタンをクリックして、ファイルマネージャを開きコンピュータ内のファイルを検索することもできます（図 11.17）。

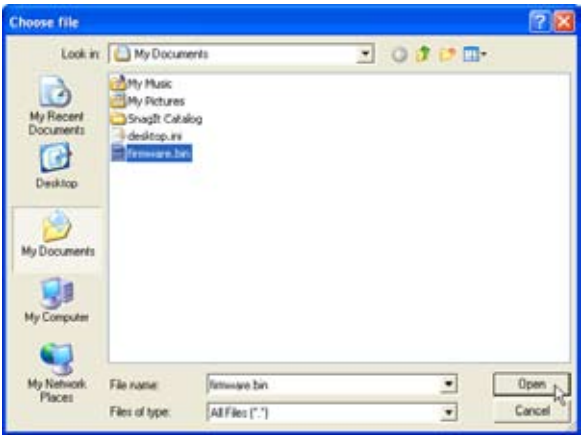


図 11.17 ファームウェアを検索

3. 「Apply」ボタンをクリックし、ファームウェアを更新します。下のような確認用のダイアログが表示されますので、実行するには「OK」ボタンを、キャンセルするには「Cancel」ボタンをクリックします。

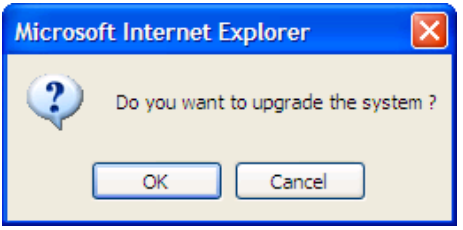


図 11.18 ファームウェアの更新を確認する画面

4. ファームウェアの更新状態が以下のように表示されます。（図 11.19）

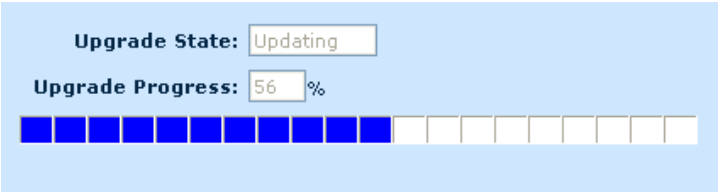


図 11.19 ファームウェア更新状態

5. ファームウェアの更新が完了すると下のようなカウントダウンタイマーが表示されます（図 11.20）。カウンターがゼロになると、本ルータに再接続します。自動的に再接続されない場合は、手動で再接続してください。

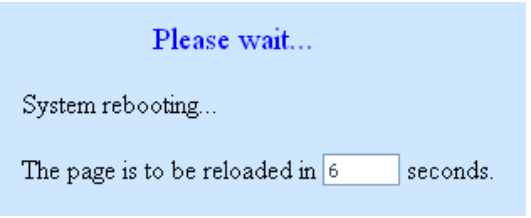


図 11.20 ファームウェア更新用システム再起動カウントダウンタイマー

6. 本ルータに再接続したら、「Status」メニューをクリックし、新しいファームウェアが正常に更新されたかを確認します。新しいシステム情報画面を参照するには、Web ブラウザのキャッシュをクリアする必要があります。クリアする手順は以下の通りです。（Microsoft Internet Explorer）

a）「ツール」メニューをクリック。

b）「インターネットオプション」をクリック。

c）「ファイルの削除」ボタンをクリックし、キャッシュをクリアします。

11.9 システムを再起動する

1. 「Management」→「Restart System」メニューをクリックし、「Restart System」画面を開きます。（図 11.21）
2. 「Apply」ボタンをクリックし、システムを再起動します。

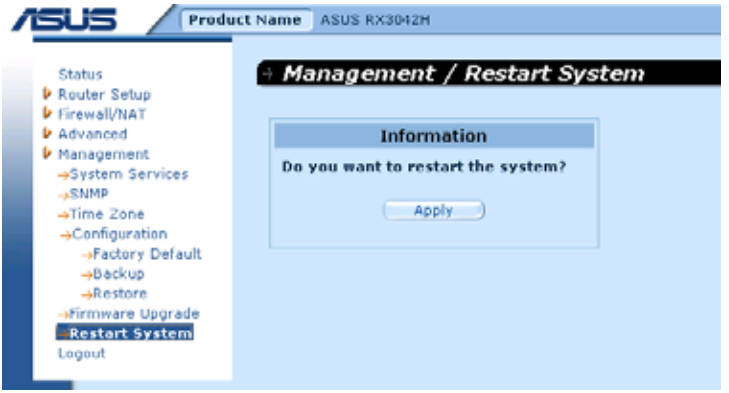


図 11.21 Restart System 画面

11.10 Configuration Management からログアウトする

「Configuration Management」からログアウトするには、「Logout」メニューをクリックして「Logout」画面を開き、「Apply」ボタンをクリックします。ブラウザに IE を使用している場合、ブラウザを閉じる前に次のような確認用画面が表示されます。（図 11.23）

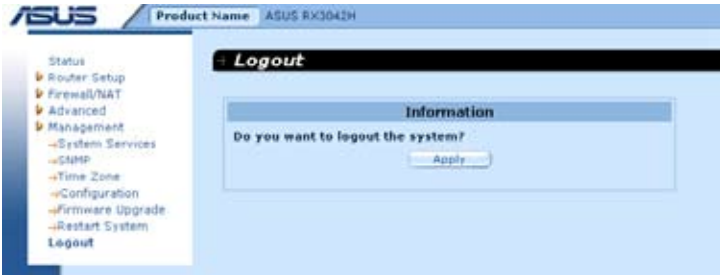


図 11.22 Logout

図 11.23 ブラウザを閉じる際の確認用ウィンドウ（IE）

12 IP アドレス、ネットワークマスク、サブネット

12.1 IP アドレス

注：このセクションでは、IPv4（version 4 of the Internet Protocol）用の IP アドレスについて記載しました。IPv6 アドレスに関しては記載していません。

インターネットの電話番号とも言える IP アドレスは、インターネット上の個々のノード（コントロールやデバイス）を特定するためのものです。0 ～ 255 の 4 つの数字で構成されており、それぞれがピリオドで区切られています（例：20.56.0.211）。また、左から順にフィールド 1、フィールド 2、フィールド 3、フィールド 4 と呼ばれています。

このような 10 進数をピリオドで区切った IP アドレスをドット付き 10 進法と言います。

12.1.1 IP アドレスの構造

IP アドレスは、電話番号と同じで階層アーキテクチャです。例えば 7 桁の電話番号は何千もの電話回線を特定する 3 桁の数字で始まり、1 本を特定する 4 桁の数字で終わります。

同様に IP アドレスにも 2 種類の情報が含まれています。

- ネットワーク ID

  インターネットやイントラネット内のネットワークを特定

- ホスト ID

  ネットワーク上のコンピュータやデバイスを特定

全ての IP アドレスのはじめの部分はネットワーク ID で、残りがホスト ID です。ネットワーク ID の長さは、ネットワークワーククラスによって異なります（詳細は次のセクション参照）。表 12.1 は IP アドレスの構造です。

表 12.1. IP アドレスの構造

	フィールド1	フィールド2	フィールド3	フィールド4
クラス A	ネットワーク ID	ホスト ID		
クラス B	ネットワーク ID		ホスト ID	
クラス C	ネットワーク ID			ホスト ID

IP アドレスの例

クラス A：10.30.6.125（ネットワーク = 10、ホスト = 30.6.125）

クラス B：129.88.16.49（ネットワーク = 129.88、ホスト = 16.49）

クラス C：192.60.201.11（ネットワーク = 192.60.201、ホスト = 11）

12.2 ネットワーククラス

通常使用されているネットワーククラスは A、B、C（クラス D も存在するが特殊用途）です。各ネットワークの用途と性質は以下のとおりです。

クラス A：インターネット上最大のネットワーク。 1つのネットワークに 16、000、000 以上のホストを割り当てることができます。最大 126 の巨大ネットワークは、合計で 2,000,000,000 以上のホストを持つことができます。サイズが巨大であるため、クラス A ネットワークは WAN や ISP のようなインターネットの基盤となる組織が使用しています。

クラス B：クラス A ネットワークよりは小さくなりますが、大きなネットワークです。 1つのネットワークに 65,000 のホストを持つことができ、ネットワークの数は最高 16,384 です。クラス B ネットワークはビジネスや政府機関などの大きな組織に適しています。

クラス C：最小のネットワークです。 1つのネットワークに最高 254 のホストしか割り当てることができませんが、ネットワークの数は最多で、2,097,152 です。インターネットに LAN 接続する場合は、ほとんどがこのクラス C ネットワークです。

IP アドレスに関する留意点：
クラスはフィールド1から簡単に識別することができます。

フィールド 1 = 1-126： クラス A
フィールド 1 = 128-191： クラス B
フィールド 1 = 192-223： クラス C

（フィールド 1 に含まれない数値は特殊用途）

- ホスト ID：特殊用途に使用される、全てのフィールドを0または 255 で設定した数値以外は、任意の数で設定可能です。

12.3 サブネットマスク

定義：マスクは通常の IP アドレスのように見えますが、2進法のパターンで、IP アドレスのどの部分がネットワーク ID でどの部分がホスト ID であるかを示します。ネットワーク ID は2進数の1で、ホスト ID は0になります。

サブネットマスク：サブネット（ネットワークを分割したもの）を定義するものです。サブネットのネットワーク ID はホスト ID の一部分を「借用」して作成されます。サブネットマスクでこれらのホスト ID を特定することができます。

例：クラス C ネットワーク「192.168.1」。 2つのサブネットに分割する際下のサブネットマスクを使用します。

255.255.255.128

これを2進数に書き換えると、以下のようになります。

11111111. 11111111. 11111111.10000000

クラス C のアドレスですので、フィールド 1 からフィールド 3 はネットワーク ID で、フィールド4の先頭の数字は1になっています。これは、サブネットマスクが2つ存在することを示します。サブネットのフィールド4の残りの7ビットにはホスト ID として（クラス C アドレス用の0～255 の代わりに）0～127 の数値が割り当てられます。

同様にクラス C ネットワークを4つのサブネットに分割するとマスクは以下のようになります。

255.255.255.192　または　11111111. 11111111. 11111111.11000000

フィールド 4 の1つ目の2ビットが4つのサブネット（00、01、10、11）を示します。各サブネットは残りの6ビットを使用して0～ 63 の数値でホスト ID を割り当てます。

ネットワーク ID ビットが特定されない場合は、サブネットマスクは存在しません。このような状態のマスクをデフォルトサブネットマスクと言います。デフォルトサブネットマスクは次項の通りです。

クラス A： 255.0.0.0

クラス B： 255.255.0.0

クラス C： 255.255.255.0

初めてネットワークが設定された状態ではサブネットは存在しないため、これらの値は初期設定と呼ばれます。

13 トラブルシューティング

本ルータをご利用中に生じる可能性のあるトラブルと解決策です。本章では、トラブルの解決策として、様々な IP ユーティリティの利用方法をご紹介します。

ここで記載した解決策でトラブルが解決されない場合は、カスタマーサポートまでお問い合わせください。

問題	トラブルシューティング
LED	
電源を入れても電源 LED が点灯しない	本ルータに付属の AC アダプタが、本ルータと電源にしっかりと接続されていることを確認してください。
イーサネットケーブルを接続しても LINK WAN LED が点灯しない	本ルータに付属のタイプと同じイーサネットケーブルが、ADSL またはモデムのイーサネットポートと、本ルータの WAN ポートに接続されていることを確認してください。また、ADSL またはケーブルモデムの電源がオンになっていることを確認してください。また、本ルータとブロードバンドモデムのネゴシエーションには約 30 秒かかります。
イーサネットケーブルを接続しても LINK LAN LED が点灯しない	イーサネットケーブルがしっかりと LAN ハブまたは PC と本ルータに接続されていることを確認してください。PC / ハブの電源がオンになっていることを確認してください。 ケーブルがネットワークの必要条件を充たしていることを確認してください。100 Mbit/ 秒のネットワーク（100BaseTx）には Cat 5 ケーブルをお使いください。10Mbit/ 秒のネットワークの場合、質の高くないケーブルでも対応できることがあります。
インターネットアクセス	
PC がインターネットにアクセスできない	Ping ユーティリティでお使いのパソコンが本ルータの LAN IP アドレス（初期設定 192.168.1.1）と通信可能かを確認します。Ping が帰ってこない場合、もう 1 度イーサネットケーブルの接続を確認してください。 静的プライベート IP アドレスがパソコンに割り当てられている場合（登録済のパブリックアドレスとは異なる）、以下の点を確認してください。 • コンピュータ上のゲートウェイ IP アドレスがパブリック IP アドレスであることを確認してください（クイックスターガイドのパート 2 の IP 情報を参照）。異なる場合は、アドレスを変更するか、パソコンが自動的に IP 情報を取得できるように設定してください。

問題	トラブルシューティング
PC がインターネットにアクセスできない（続き）	• ISP に DNS サーバが有効であるかを確認してください。また、自動的に情報を受信できるよう、アドレスとパソコンを設定してください。 • 本ルータの NAT ルールは、プライベート IP アドレスからパブリック IP アドレスに変換されるように定義してください。また、割り当てられた IP アドレスは NAT ルールで特定されているレンジ内である必要があります。または、他のデバイスが割り当てるアドレスをパソコンが承諾するように設定してください。（詳細：セクション 3.2「パート 2 - コンピュータの設定」参照）初期設定には、予め定義されたプールに動的に割り当てられた全てのアドレス用の NAT ルールが含まれます。
インターネットの Web 画面がパソコンに表示されない	上記の項目を読み、DNS サーバが ISP に対応しているかを確認してください。ISP の DNS サーバとの接続性を Ping ユーティリティでテストしてください。
Configuration Management プログラム	
Configuration Management のユーザー ID またはパスワードを忘れてしまった	デフォルト設定からパスワードを変更していない場合は、ユーザー ID もパスワードも「admin」です。変更した場合は、本デバイスをリセットし初期設定に戻してください（詳細：セクション 11.7.3 参照）。警告：リセットするとカスタム設定は全て消去され、工場出荷状態に戻ります。
ブラウザから Configuration Management プログラムにアクセスできない	Ping ユーティリティを使用して、パソコンが本デバイスの LAN IP アドレス（初期設定値 192.168.1.1）と通信していることを確認してください。Ping が帰ってこない場合は、イーサネットケーブルの配線を確認してください。 Internet Explorer 6.0 以降のものを使用してください。ブラウザで、Javascript® と Java® のサポートを有効にしてください。 パソコンの IP アドレスが本デバイスの LAN ポートに割り当てた IP アドレスと同じサブネット上にあることを確認してください。
Configuration Management の変更を保存できない	変更を行った際は、「Apply」ボタンをクリックして、変更を保存してください。

13.1　IP ユーティリティを使用して問題を検出する

13.1.1 Ping

Ping は、パソコンがネットワークやインターネット上の他のコンピュータを認識しているかどうかを確認する際に利用できるコマンドです。Ping コマンドは特定したコンピュータにメッセージを送ります。メッセージを受け取ったコンピュータは、メッセージを返信します。Ping を打つには、通信先のコンピュータの IP アドレスが必要です。

Windows ベースのコンピュータでは、「スタート」メニューから簡単に Ping を打つことができます。「スタート」→「ファイル名を指定して実行」の順にクリックしテキストボックスに以下のように入力します。

ping 192.168.1.1

「OK」をクリックします。LAN 上のプライベート IP アドレスやインターネットサイト用のパブリック IP を入力しても構いません。

ターゲットコンピュータがメッセージを受信すると、コマンドプロンプト画面には、図 13.1 のように表示されます。

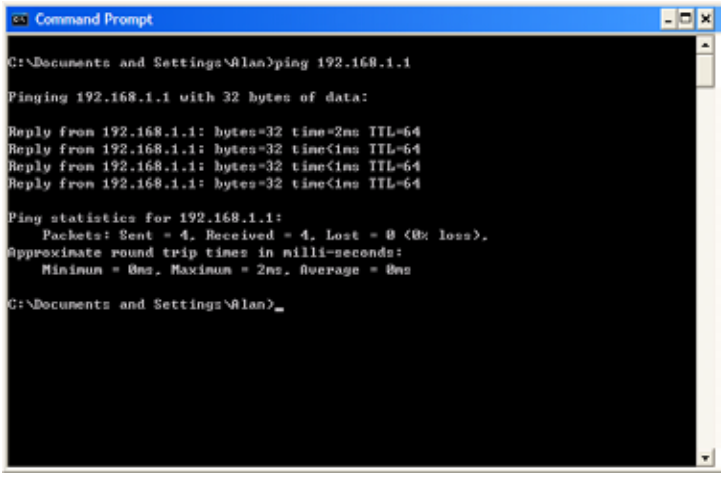


図 13.1. Ping ユーティリティを使う

ターゲットコンピュータが見つからない場合、「Request timed out」というメッセージが表示されます。

Ping コマンドを利用して、本ルータへのパスが使用可能かどうか確認することができます。初期設定 LAN IP アドレス 192.168.1.1 または他の割り当てられたアドレスを利用します。

また、www.yahoo.com（216.115.108.243）のような外部アドレスを入力して、インターネットへのアクセスが可能かどうかを確認することができます。インターネットロケーションの IP アドレスが分からない場合は、nslookup コマンドを使用します。

IP が有効な OS ではほとんど、コマンドプロンプトやシステム管理ユーティリティを使用して同じコマンドを実行することができます。

13.1.2 nslookup

nslookup コマンドで、インターネットのサイト名に対応する IP アドレスを特定することができます。名前を特定すると、nslookup コマンドが DNS サーバ（大抵は ISP 内）を検索します。ISP の DNS に名前が検出されないと、上位サーバを検出し、入力された名前が検出されるまで検出を続けます。検出すると IP アドレスが表示されます。

Windows ベースのコンピュータでは、「スタート」メニューから簡単に nslookup コマンドを実行することができます。「スタート」→「ファイル名を指定して実行」の順にクリックし、テキストボックスに以下のように入力します。

nslookup

「OK」をクリックし、コマンドプロンプトの「>」の後にインターネットアドレスを入力します。（例：www.absnews.com）検出されると、図 13.2 のように、対応する IP アドレスが表示されます。

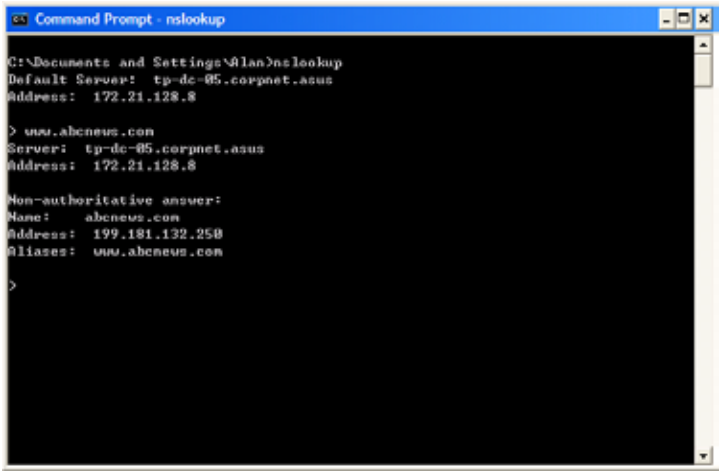


図 13.2. nslookup ユーティリティを使う

インターネット名 1 つに複数のアドレスが対応していることがありますが、これはトラフィック数の多い Web サイトによくあることで、複数の冗長サーバを利用し同じ情報を提供しています。

nslookup ユーティリティから退出するには、「exit」と入力し <Enter> を押します。

14 索引（50 音）

（50 音続き）

索引（アルファベット）