RX3141

ユーザーマニュアル

2004 年 10 月 21 日

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 RX3141 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 RX3141 の設定方法と、本製品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 Gigabit スイッチ、9KByte のジャンボフレームに対応
- WAN:10/100Base-T Ethernet 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
- DHCP サーバを通してネットワークアドレスを自動的に割り当て
- IP ルート、DNS 設定と DDNS 設定を含む各種サービス
- 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

RX3141 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 に割り当てたパブリックインターネットアドレスが最低1つ
- Ethernet 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が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、RX3141 は「ルータ」「ゲートウェイ」「本製品」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：**Router Setup ➔ Connection** は「**Router Setup メニュー** をクリックし **Connection** 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

- **太字**は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です。

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連する重要度の高いメッセージです。

2 RX3141 を準備する

2.1 パッキングリスト

RX3141 には以下のものが付属しています。

- システムユニット、RX3141
- AC アダプタ
- ユーザーマニュアル（本書）
- 多言語クイックガイドの入った CD

2.2 ハードウェア

- LAN
  - 4 ポート Gigabit スイッチ
  - オートスピードネゴシエーション
  - 9KB ジャンボフレーム対応
  - 4K MAC アドレステーブル（自動学習機能/エージング機能付き）
- WAN
  - 10/100M Ethernet
  - オート MDI/MDIX

2.3 ソフトウェア

2.3.1 NAT 機能

RX3141 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、RX3141 にはこれとはリバース NAT 機能があり、ユーザが 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。RX3141 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範囲内で行われます。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範囲から選択されます。
- リバース NAPT—インバウンド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・インペクション（SPI：Stateful Packet Inspection）
- 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
- Log

2.3.2.1 ステートフル・パケット・インペクション

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。

RX3141 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、プロトコルに基づき、フィルタリング。
- フィルタールール構成のため、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機能

RX3141 Firewall 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やる分割攻撃・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、デスオブピン、Land I 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。

RX3141 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

2.4.1.1 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。RX3141 の上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 RX3141 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。 RX3141 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。

2.4.1.2 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、RX3141 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。

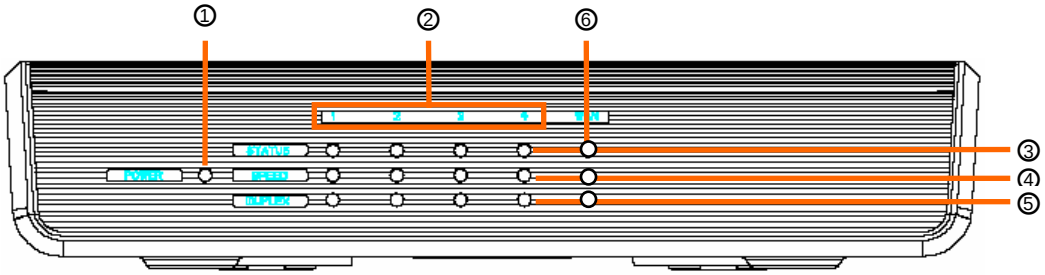


図 2.1. フロントパネル LED

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	**1 – 4**			LAN ポート LED を識別。各 LAN ポートの状態を 3 つの LED で表示。（STATUS、SPEED、DUPLEX）
③	STATUS	グリーン	ON	イーサネットリンクが確立、アクティブ
			点滅	データ転送/受信中
				イーサネットリンクなし
			OFF	
④	SPEED	グリーン	ON	転送スピード 1000Mbps
		オレンジ	ON	転送スピード 100Mbps
			OFF	転送スピード 10Mbps またはリンクなし
⑤	DUPLEX	オレンジ	ON	LAN ポートが全 2 重通信法式で動作中
			Blinking	LAN ポートが半 2 重通信法式で動作中で衝突が起こっている
			OFF	LAN ポートが半 2 重通信法式で動作中で、衝突なし
⑥	**WAN**			WAN ポート LED を識別
③	STATUS	グリーン	ON	イーサネットリンクが確立されアクティブ
			OFF	イーサネットリンクなし
④	SPEED	グリーン	ON	転送スピード 100Mbps
			点滅	グリーン：データ転送/受信中

	LED の表示	色	状態	内容
		オレンジ	ON	転送スピード 10Mbps
			点滅	データ転送/受信中
			OFF	リンクなし
⑤	DUPLEX	オレンジ	ON	LAN ポートが全 2 重通信法式で動作中
			OFF	LAN ポートが半 2 重通信法式で動作中で、衝突なし

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。

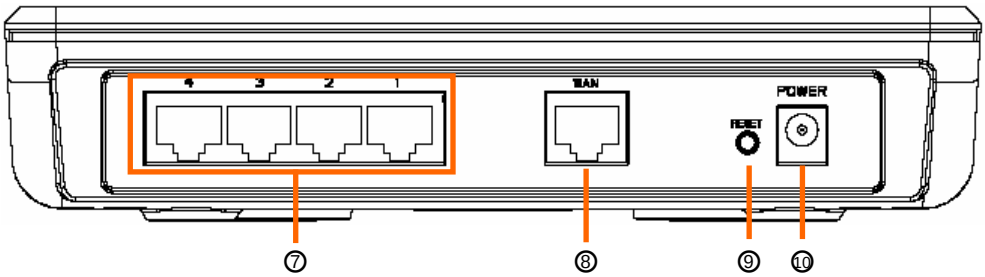
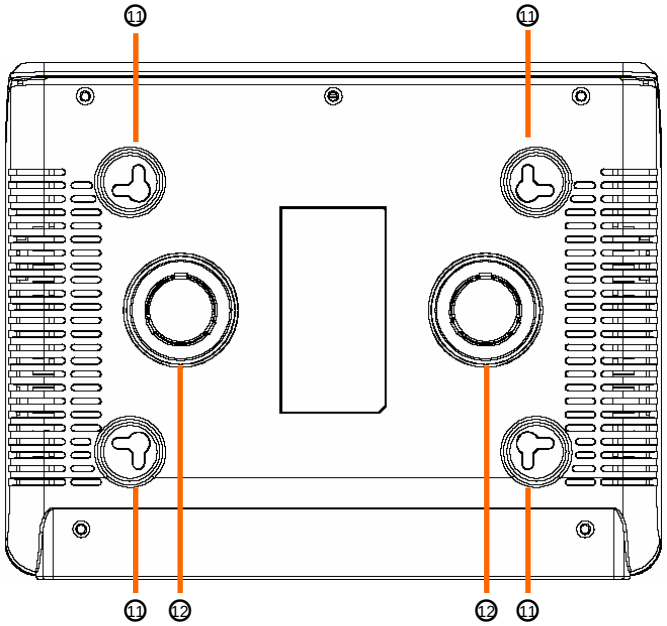


図 2.2. リアパネルコネクタ

表 2.3. リアパネルの表示と LED

	表示	内容
⑦	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。
⑧	WAN	**WAN ポート**:WAN デバイスに接続(ADSL やケーブルモデム)
⑨	RESET	**リセットボタン** 1. デバイスをリセット 2. 5秒以上押すと、システム設定をリセットし、工場出荷状態のデフォルトに戻す
⑩	POWER	**POWER 入力ジャック**:**同梱の** AC アダプタに接続

2.4.3 底面



⑪ 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。

⑫ **マグネット：**磁石で金属面に設置できます。

2.5 設置オプション

使用条件に応じ、デスクトップ、マグネットマウント、ウォールマウントの3通りの設置方法が可能です。

2.5.1 デスクトップ

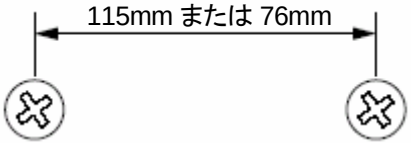
デスク等の水平な場所に設置する場合です。省スペース設計ですので、場所をとりません。

2.5.2 マグネットマウント

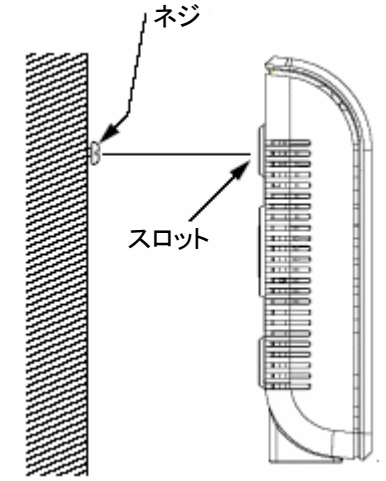
着磁性のある金属面に設置します。(PCラック、キャビネット等)

2.5.3 ウォールマウント

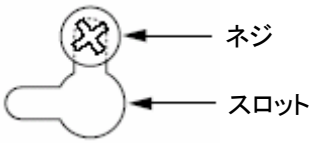
1. フロントパネルまたはリアパネルを上に向けて設置する場合は、壁面にネジを2本 115mm の間隔、側面を上に設置する場合は 76mm 間隔で、2本のネジが水平になるように設置します。スロットは 4 箇所あり、隣接するスロットを2つ選択することになります。



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スイッチの位置を調節します。



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、スイッチの位置を調節。

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終了したら、18 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設定は対応する章ををご覧ください。

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。*本製品、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

RX3141 :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3台以下の場合、イーサネットケーブルで本製品イーサー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4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 アダプタを取り付ける

AC アダプタ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 アダプタを RX3141 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。

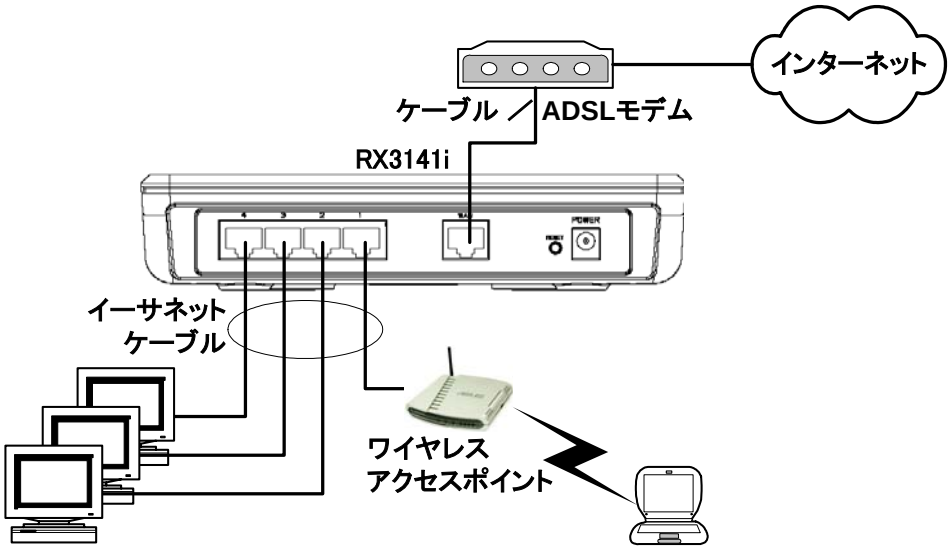


図 3.2. ハードウェア接続

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 アダプタがしっかり RX3141 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。
1 – 4 STATUS 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、RX3141 も正常に動作しています。

3.2 Part 2 – 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

デフォルトでは、RX3141 は自動的に必要なネットワーク設定をコンピュータに割り当てますので (IP アドレス、DNS サーバ IP アドレス、デフォルトゲートウェー 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 RX3141 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 タスクバーから、「スタート」 ボタンをクリックし、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 タスクバーで、**「スタート」**ボタンから→**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イ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、システム再起動してください。

   次に RX3141 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 タスクバーから **「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。10 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イ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、システム再起動してください。

   次に RX3141 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の名前を検索し、**「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、**「デフォルトゲートウェイ」**タブをクリック。**「新しいゲートウェイ」**のアドレス入力欄に 192.168.1.1 と入力し(RX3141 のデフォルト LAN ポート IP アドレス) 、**「追加」**ボタンをクリックし、デフォルト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ウインドウが表示されたら、**「OK」ボタン** をクリックし、システム再起動してください。

3.2.5 Windows® NT 4.0 workstations

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 タスクバーから **「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。10 に進んでください。
4. インターネットプロトコル (TCP/IP) が表示されていない場合は、**「追加」**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**「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イ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、Window には「DHCP と呼ばれる TCP/IP サービスが動的に設定し、IP 情報を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 RX3141 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。
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）。

- 常時特定のコンピュータに関連付けたいパブリック IP アドレスを1つ以上取得していている場合（例：パブリックウェブサーバとしてッ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、RX3141 の LAN IP がデフォルト値として 192.168.1.1 に設定されていいます。初回の設定では RX3141 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、デフォルトゲートウェイに 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、13～15 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、デフォルトゲートウェイ用の 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 RX3141 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、以降の記載(to change the LAN port IP address accordingly)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 – RX3141 の簡単設定

ここでは、RX3141 の「Configuration Manager」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、ここでの記載は本製品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をご覧ください。

3.3.1 RX3141 のセットアップ

手順

1. Configuration Manager 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. RX3141 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、アドレスの欄に下の URL を入力し、「**Enter**」キーを押します。

   http://192.168.1.1

   これは RX3141 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。

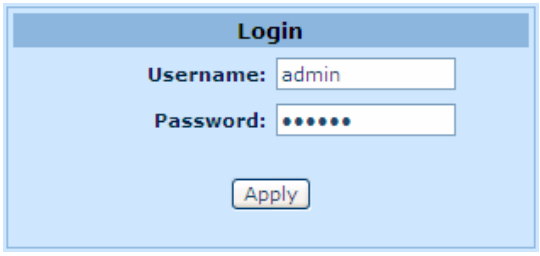


図 3.3. Login 画面

   RX3141 の接続の際に問題がある場合は、RX3141 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、もう1つの方法は 192.168.1.0 ネットワーク内のコンピュータの IP アドレスを任意のアドレスに設定します。例:192.168.1.2

3. ユーザーネームとパスワードを入力し、Apply をクリックし、 Configuration Manager にログインします。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「ログインパスワードとシステム全般の設定」参照)

System Status の画面はログインのたびに表示されます。(下図参照)

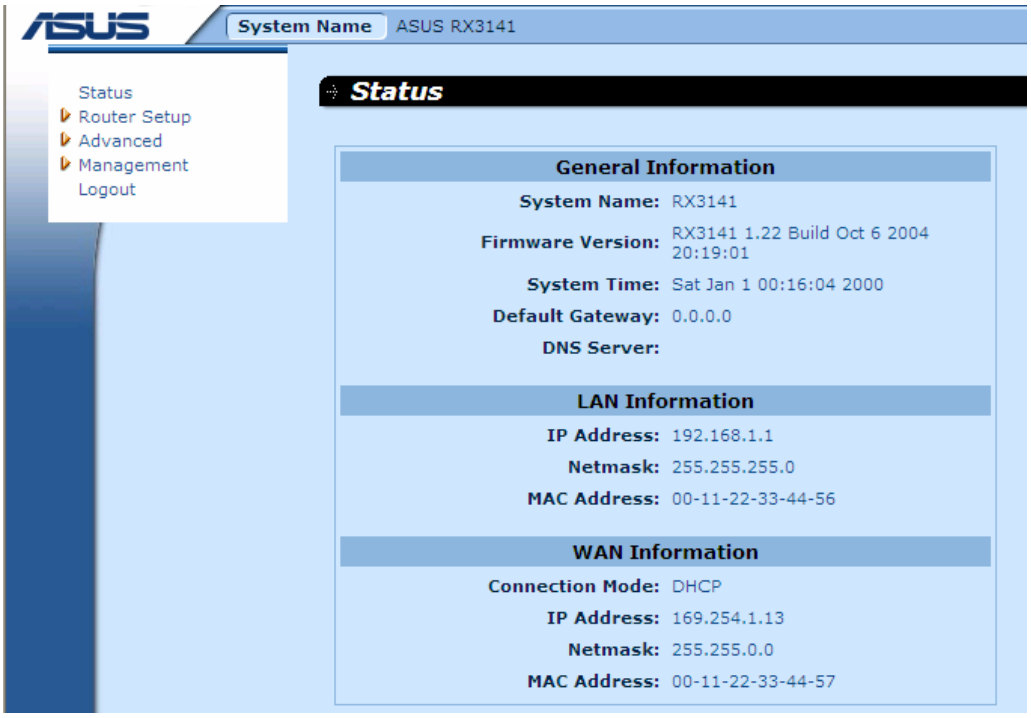


図 3.4. System Status 画面

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、RX3141 では LAN 上の全てのコンピュータが有効になっており、RX3141 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 が早く点滅し、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、Appendix 13 のトラブルシューティングをご覧ください。

3.3.3 デフォルトルーター設定

プロバイダへの DSL 接続を制御するほかに、RX3141 には様々なネットワーク機能が満載です。RX3141 には家庭や SOHO などの環境での使用を想定したデフォルト設定がされています。

表 3.2 は、主なデフォルト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。ネットワーク構成に詳しい場合は、各設定を確認し、ネットワーク構成要件を充たしているか確認してください。詳しくない場合は、デフォルト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 Manager 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. デフォルト設定一覧

オプション	デフォルト設定	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 ～192.168.1.149	RX3141 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 PART2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 Port IP Address	静的 IP アドレス:192.168.1.1 サブネットマスク:255.255.255.0	RX3141 上の LAN ポートの IP アドレスです。LAN ポートは RX3141 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 5.1.1 をご覧ください。

4 Configuration Manager

RX3141 には予めインストールされたプログラム *Configuration Manager* が組み込まれています。RX3141 にインストールされたソフトウエ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。RX3141 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 Manager の基本的な使用方法について記載しました。

4.1 Configuration Manager にログインする

Configuration Manager は既に RX3141 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。

- RX3141 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。

RX3141 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、RX3141 上の LAN ポート用に予め設定した IP アドレスです。入力すると下図のようなログイン画面が表示されます。

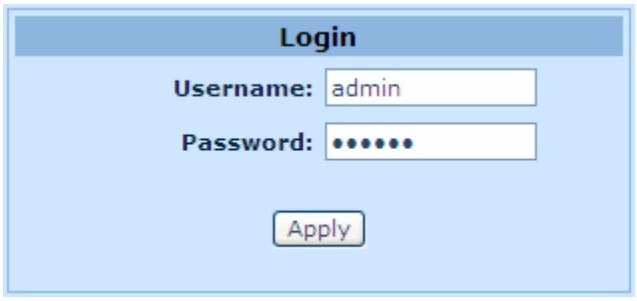


図 4.1. Configuration Manager ログイン 画面

2. ユーザーネームとパスワードを入力し、 Apply 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

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

System Status の画面はログインのたびに表示されます。(24 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 Manager とやり取りして RX3141 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。

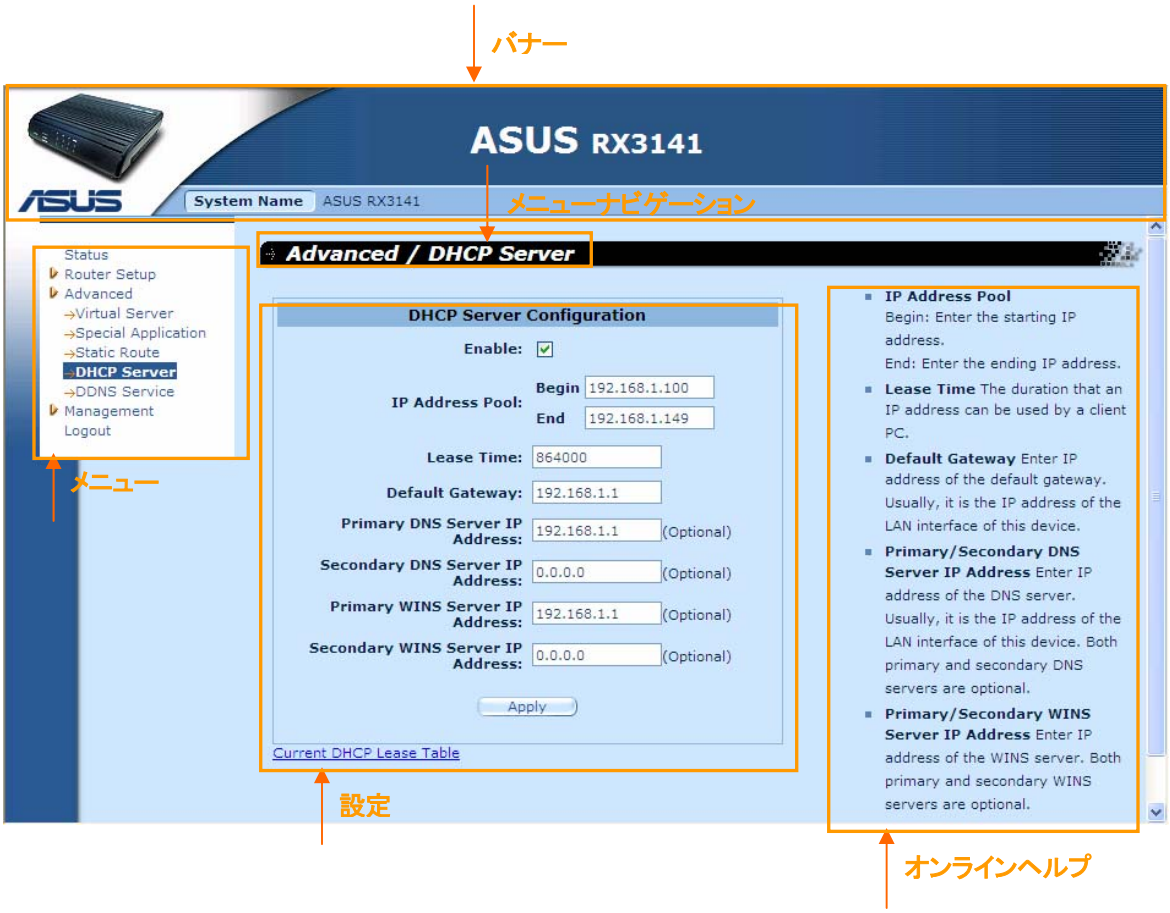


図 4.2. 一設定画面

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 をクリックします。
- 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** – 選択した項目を消去
Browse...	**閲覧**
Undo	**元に戻す**
Cancel	**キャンセル**
OK	**OK**
Open	**開く**
Save	**保存**
	**フォルダ オフ**
	**フォルダ オン**
	**項目**

4.3 システムの概要

システムの概要を知るには、Configuration Manager 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。

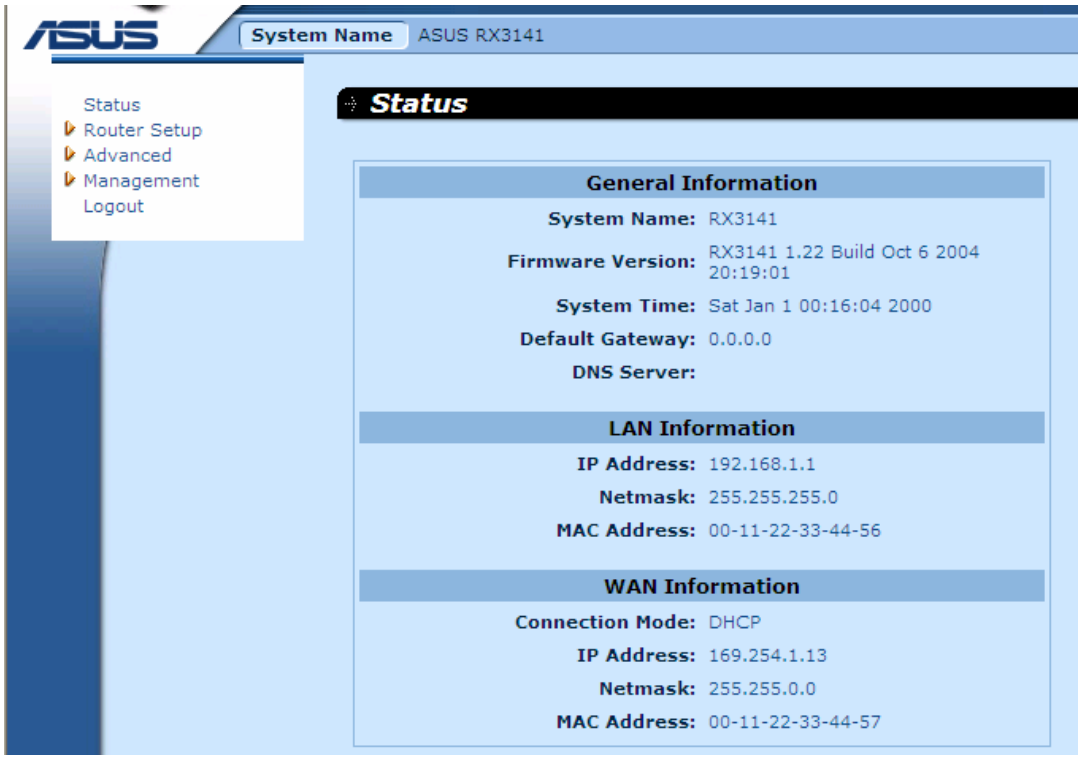


図 4.3. System Information 画面

5 ルータ接続の設定

本章では、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 RX3141 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。RX3141 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。RX3141 のデフォルト 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。RX3141 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 Appendix 12 参考)

デフォルト 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

下記は、LAN IP 設定に有効なパラメータを示したものです。

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	RX3141 の LAN IP アドレスです。ユーザーのコンピュータで使用し、RX3141 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 RX3141 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、デフォルトサブネットマスク 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、デフォルトの 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、Router Connection Setup Configuration の画面が表示されます。

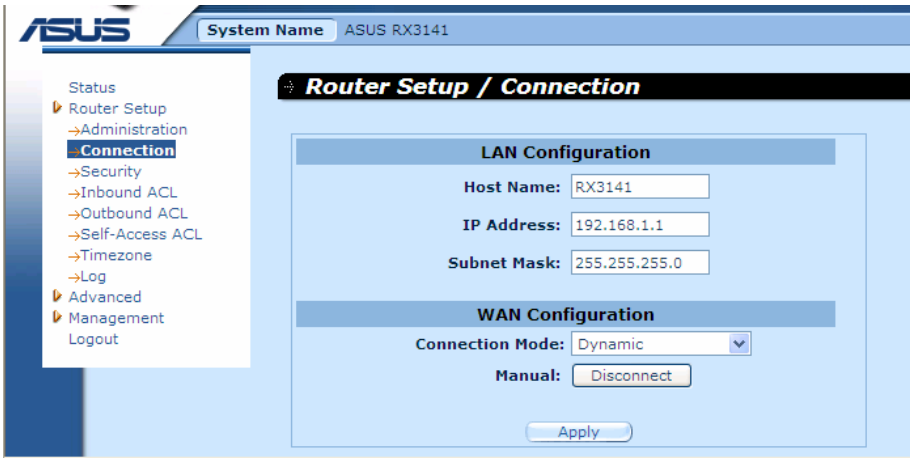
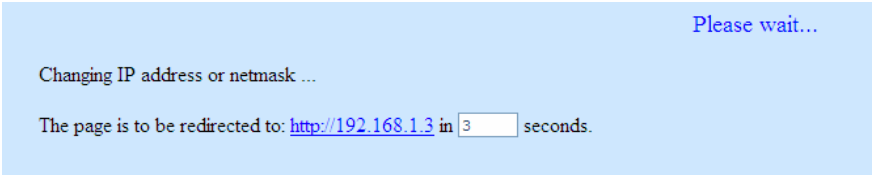


図 5.1. Router Connection Setup Configuration – LAN Configuration

2. (オプション I) RX3141 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. RX3141 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 Manager への再ログインを促します。

5.2 WAN 設定

本章では、プロバイダとの通信を目的とし、RX3141 上の WAN インターフェースの WAN 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。

5.2.1 WAN 接続モード

RX3141 には、4種類の WAN 接続方法があります。– PPPoE (マルチセッション)、PPPoE unnumbered(アンナンバード)、動的 IP 、静的 IP です。プロバイダの要求に合わせ、Network Setup Configuration 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。(下図参照)

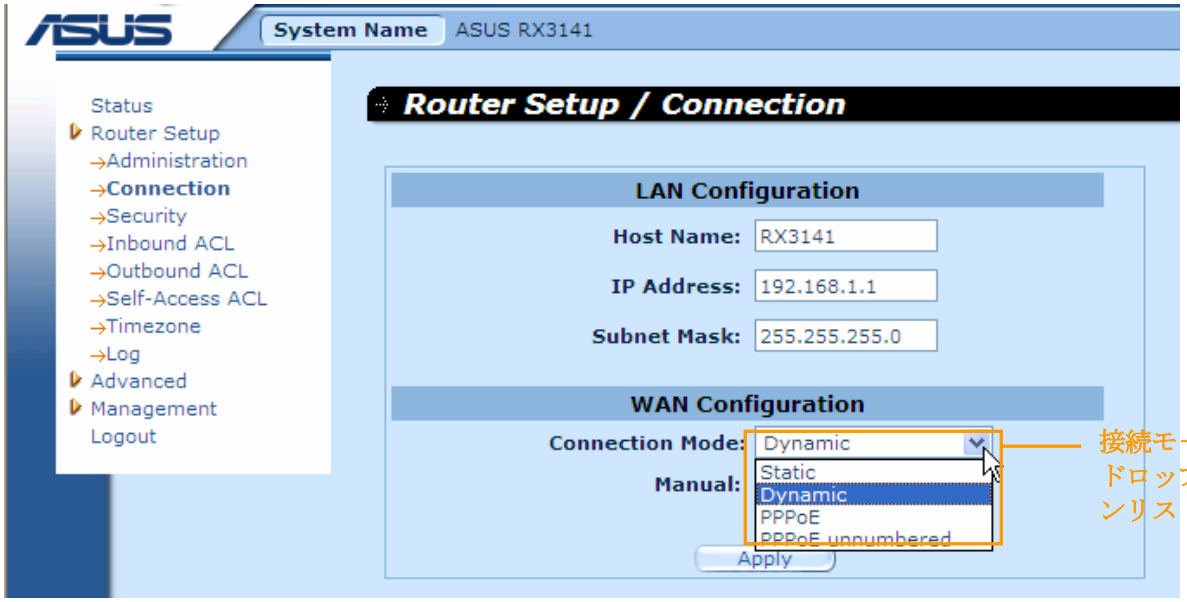


図 5.2. Network Setup Configuration 画面– WAN 設定

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。

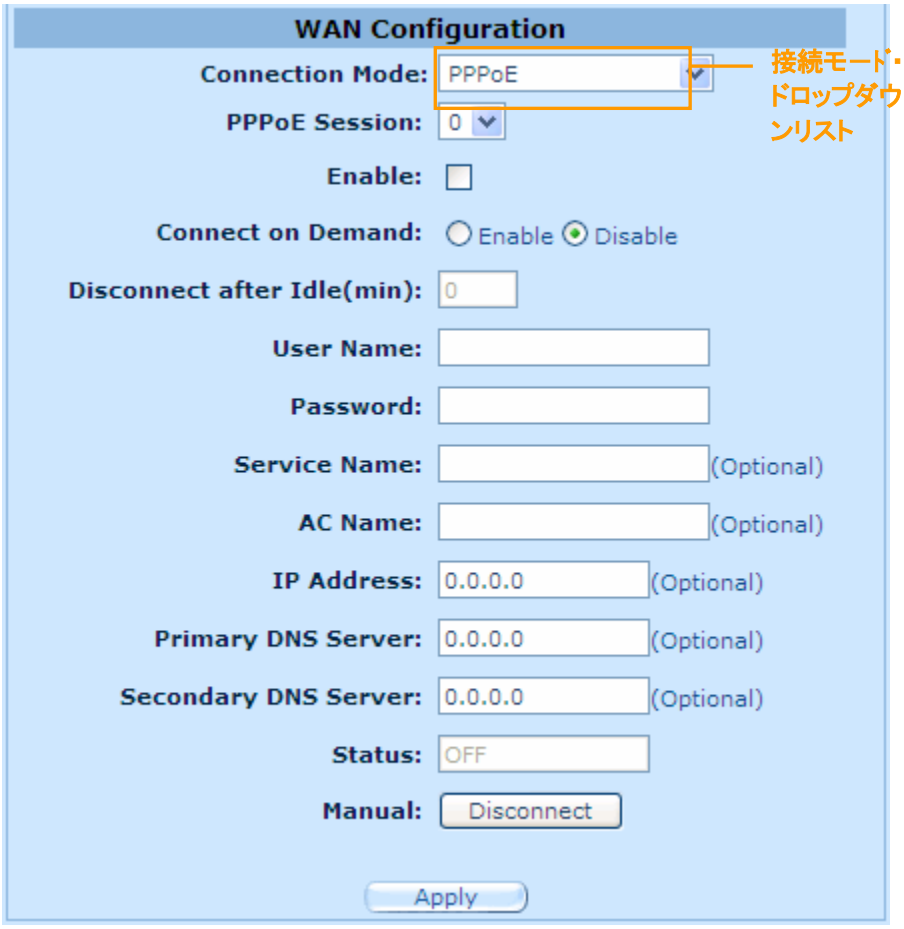


図 5.3. WAN – PPPoE 設定

5.2.2.1 WAN PPPoE 設定パラメータ

下の表は、PPPoE 接続モードで有効なパラメータの一覧です。

表 5.2. WAN PPPoE 設定パラメータ

設定	説明
Connection Mode	接続モードの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。
Connection on Demand	ラジオボタンで **Enable** と **Disable** を切り替えます。
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。
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 Manager 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。
IP Address	プロバイダが PPPoE 接続のための静的 IP を要求する場合のみ、静的 IP アドレスを入力します。これは、プロバイダが指定するものです。（殆どのプロバイダの場合設定する必要はありません）
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。
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 Router Connection configuration 画面を開きます。
2. WAN 接続モードドロップダウンリストから **PPPoE** を選択。(図 5.3 参照)
3. PPPoE Session ID ドロップダウンリストから PPPoE セッション ID を選択。現在、2つのセッションをサポートしています。
4. 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。
5. (オプション)プロバイダが指定している場合は、サービスネームを入力します。
6. **Disconnect after Idle (min)** と **Connect on Demand** を設定します。
7. Apply クリックし設定を保存します。

5.2.2.3 WAN 用に PPPoE マルチセッション

下の図を参照し、WAN 用の PPPoE マルチセッションを設定してください。下図は一例です。

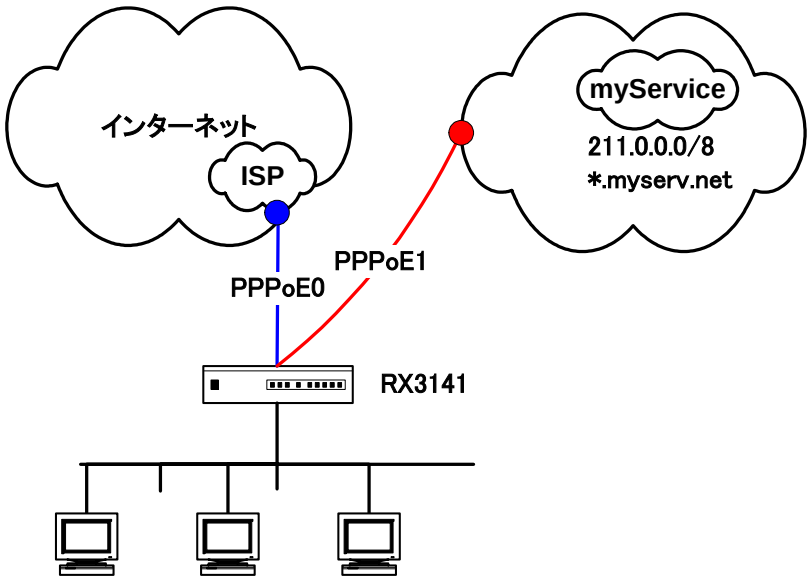


図 5.4. WAN – PPPoE マルチセッションの例

1. **Router Setup** ➔ **Connection** メニューから Router Connection configuration 画面を開きます。

通常のように、各 PPPoE セッション用の PPPoE を設定します(セクション 5.2.2.2 参照)。最高2つの PPPoE セッションをサポートしており、下の図は2つの PPPoE セッションを設定した例です。

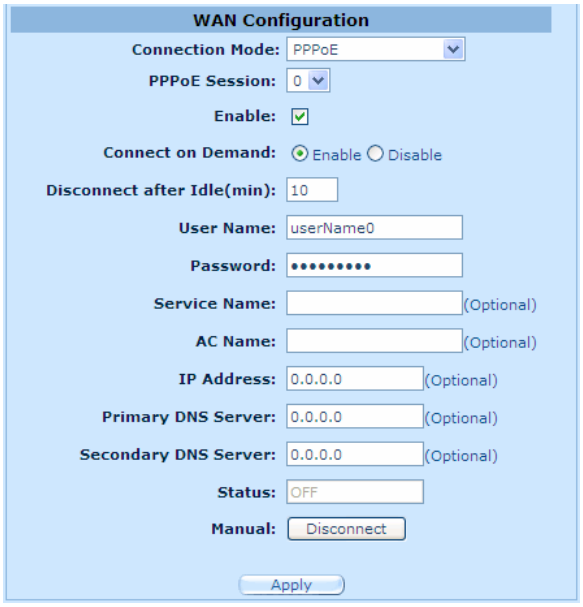


図 5.5. WAN – PPPoE0 Settings

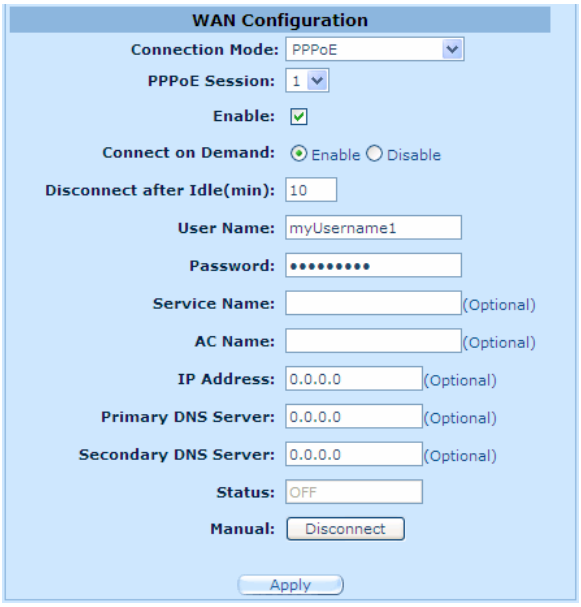


図 5.6. WAN – PPPoE1 Settings

2. ファイアウォールのアウトバウンド ACL ルールを設定し、指定されたトラフィックを各対象となる PPPoE セッションに転送します。セクション 9.5 のアウトバウンド ACL ルール を参照し、ACL ルールを設定してください。下の2つの図は2つのアウトバウンド ACL ルール用の設定で、左の図はネットワークアドレスとサブネットマスクで宛先ネットワークを特定し、右の図はドメインネームで特定します。2つの ACL ルールのうち1つだけ必要ですが、IP アドレスとドメインネームを使用して myService ネットワークにアクセスする場合は、両方のルール設定が必要です。

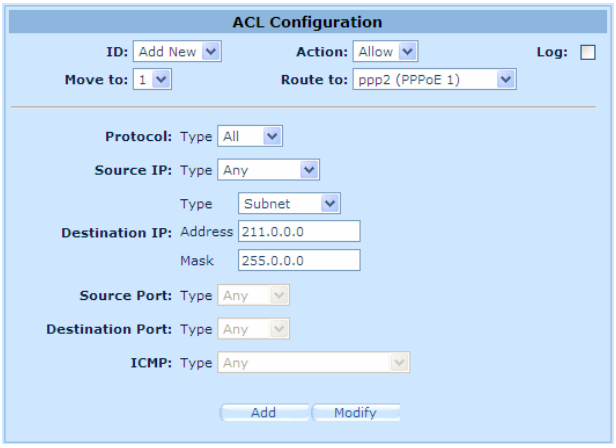


図 5.7. WAN – ACL ルール設定1

(ネットワークアドレスとサブネットマスク使用し PPPOE1 セッションにパケットを転送)

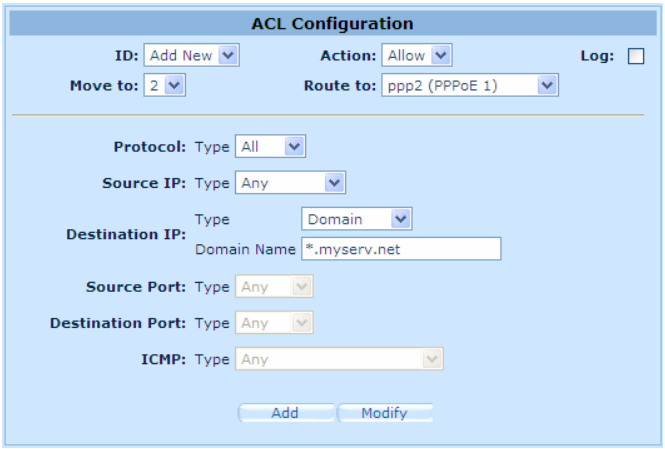


図 5.8. WAN – ACL ルール設定2

(ドメインネームで PPPOE1 セッションにパケットを転送)

3. 下図 5.9 の「Existing Outbound ACL」のように、ルール設定が終了したか確認してください。3つめのルールはデフォルトのアウトバウンド ACL ルールで、全てのアウトバウンドトラフィックをファイアウォールに通します。このルールを消去した場合は設定する必要があります(図 5.10 のデフォルトのアウトバウン

ド ACL 設定を参照）。このルールでは PPPoE1 セッション用に送るように設定したものを除き、全てのアウトバウンドトラフィックを PPPoE0 セッションに送ります。

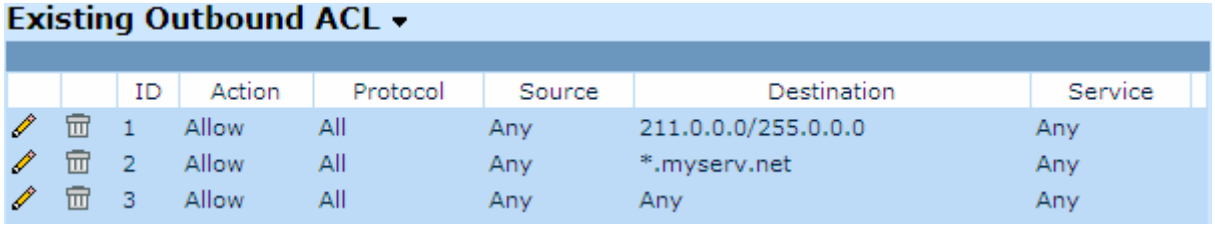


図 5.9. WAN –PPPoE マルチセッション用アウトバウンド ACL ルール設定の例

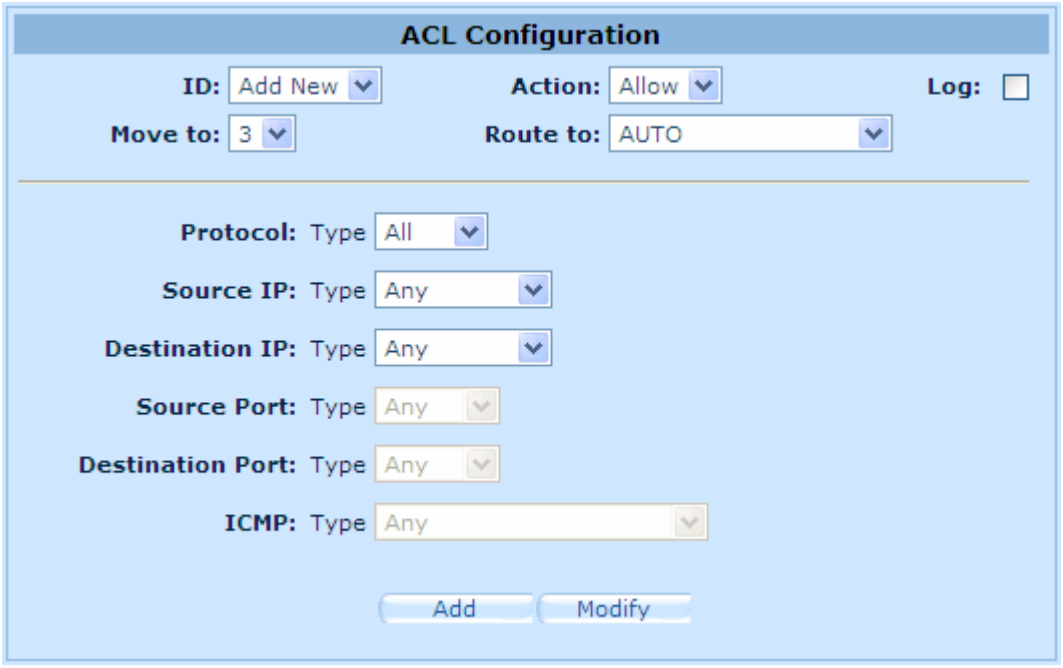


図 5.10. WAN –PPPoE マルチセッション用デフォルトアウトバウンド ACL ルールの例

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。

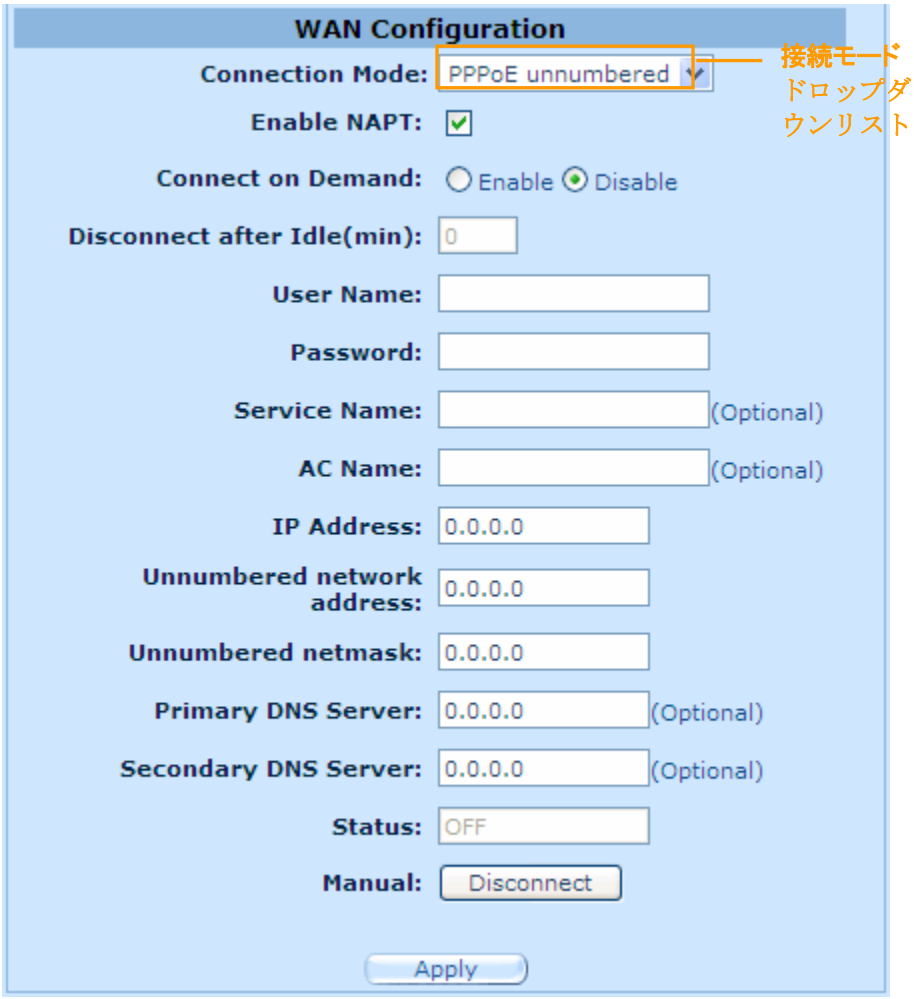


図 5.11. WAN – PPPoE アンナンバード設定

5.2.3.1 WAN PPPoE アンナンバード設定パラメータ

下の表5.3は、PPPoE アンナンバード接続モード用の有効な設定パラメータの一覧です。

表 5.3. WAN PPPoE アンナンバード設定パラメータ

設定	説明
Connection Mode	接続モード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。
Connect on Demand	ラジオボタンで **Enable** と **Disable** を切り替えます。
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。
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。
Unnumbered netmask	プロバイダ指定のサブネットマスクを入力します。
User Name and Password	プロバイダ用のユーザーネームとパスワードを入力します。 （注： Configuration Manager 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。
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 Router Connection configuration 画面を開きます。
2. WAN 接続モードドロップダウンリストから **PPPoE Unnumbered** を選択します。
3. 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。
4. (オプション)プロバイダが指定している場合は、サービスネームを入力します。
5. **Disconnect after Idle (min)** と **Connect on Demand** を設定します。
6. 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使用されています。

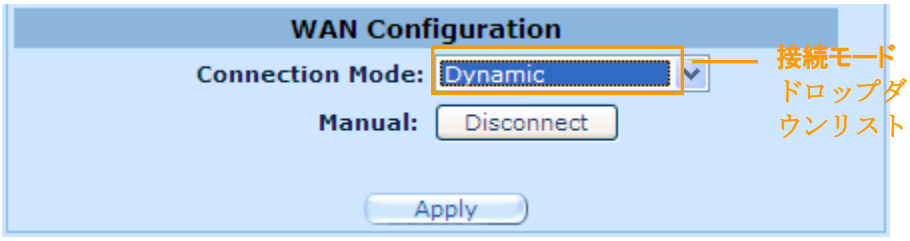


図 5.12. WAN – 動的 IP (DHCP クライアント) 設定

5.2.4.1 WAN 用の動的 IP 設定

手順

1. **Router Setup** ➔ **Connection** メニューから Router Connection configuration 画面を開きます。
2. 接続モードドロップダウンリストから Dynamic を選択します。(上図 5.12 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。
3. Apply をクリックし変更を保存します。

5.2.5 静的 IP

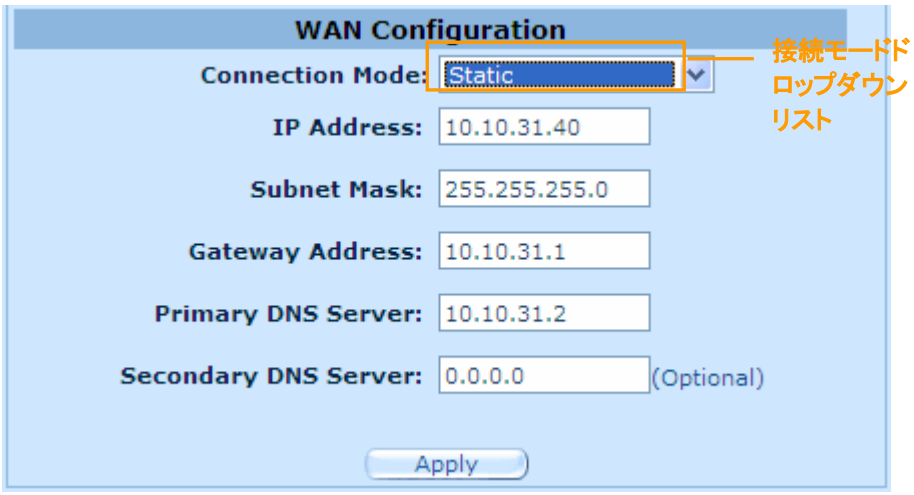


図 5.13. WAN – 静的 IP の設定

5.2.5.1 WAN 静的 IP 設定パラメータ

下図は静的IP接続モード用の有効な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
Connection Mode	接続モードドロップダウンリストから Static を選択します。
IP Address	プロバイダ指定の WAN IP アドレス
Subnet Mask	プロバイダ指定の WAN 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。RX3141 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。

5.2.5.2 WAN 用の静的 IP の設定

手順

1. **Router Setup** ➔ **Connection** メニューから Router Connection configuration 画面を開きます。
2. 接続モードドロップダウンリストから Static を選択します。(図 5.13 参照)
3. IP アドレスの欄に WAN IP アドレスをん入力してください。この情報はプロバイダ指定のものです。
4. 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。
5. 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。

6. 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 DNS サーバはオプションです。
7. Apply をクリックし変更を保存します。

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、本製品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 アドレスの範囲から 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、アドレス範囲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しなくてはいけません。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 アドレス範囲 で、LAN 側の DHCP サーバとして設定することができます。アドレス範囲を変更する場合は、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 サーバ設定画面を開きます。

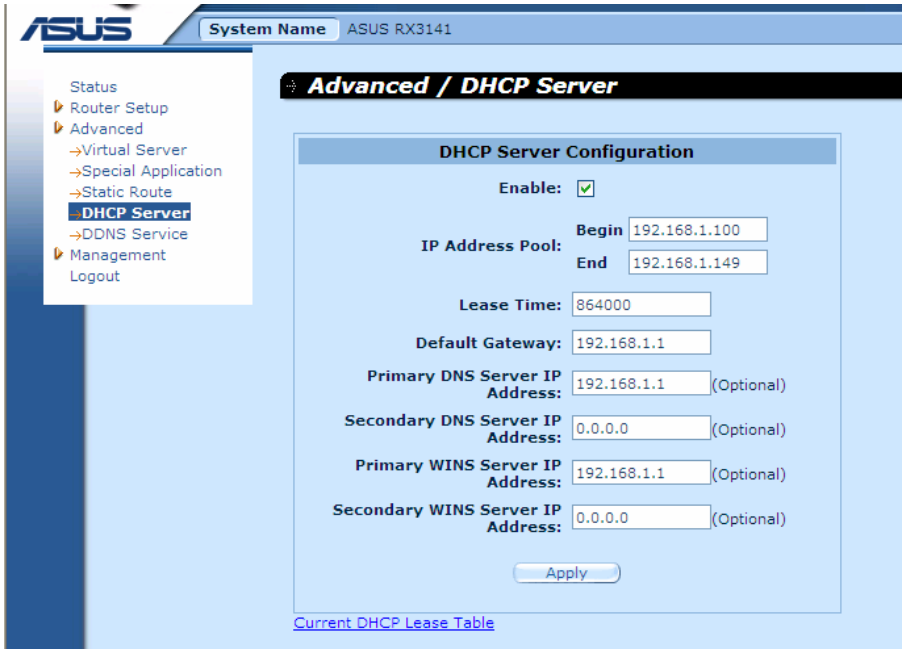


図 6.1. DHCP サーバ設定画面

2. *IP Address Pool (Begin/End Address)*、Sub*net Mask*、*Lease Time*、*Default Gateway IP Address* のフィールドに情報を入力します。他のフィールド(*Primary/Secondary DNS Server IP Address* and *Primary/Secondary WINS Server IP Address*)はオプションですが、Primary DNS server IP address には必要な情報を入力することをお勧めします。Primary DNS Server IPAddress フィールドには、LAN IP または ISP の DNS IP を入力します。下の表 6.1 は、DHCP 設定項目の詳細です。

表 6.1. DHCP 設定項目

フィールド	説明
Enable	LAN 用に DHCP サーバサービスを有効にします。
IP Address Pool Begin/End	DHCP アドレス範囲の最小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	設定範囲内の IP アドレスを受け取るコンピュータ用のデフォルトゲートウェイのアドレス。デフォルトゲートウェイは、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 RX3141 の LAN ポート IP アドレスです。
Primary/Secondary DNS Server IP Address	設定範囲内の 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 ISP に存在します。DNS プロキシとして使う RX3141 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 アドレス範囲から 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すれば、この項目に情報を入力する必要はありません。

3. 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

本製品を、LAN の DHCP サーバとして機能させると、コンピュータに割り当てられた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、現行の IP アドレス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。

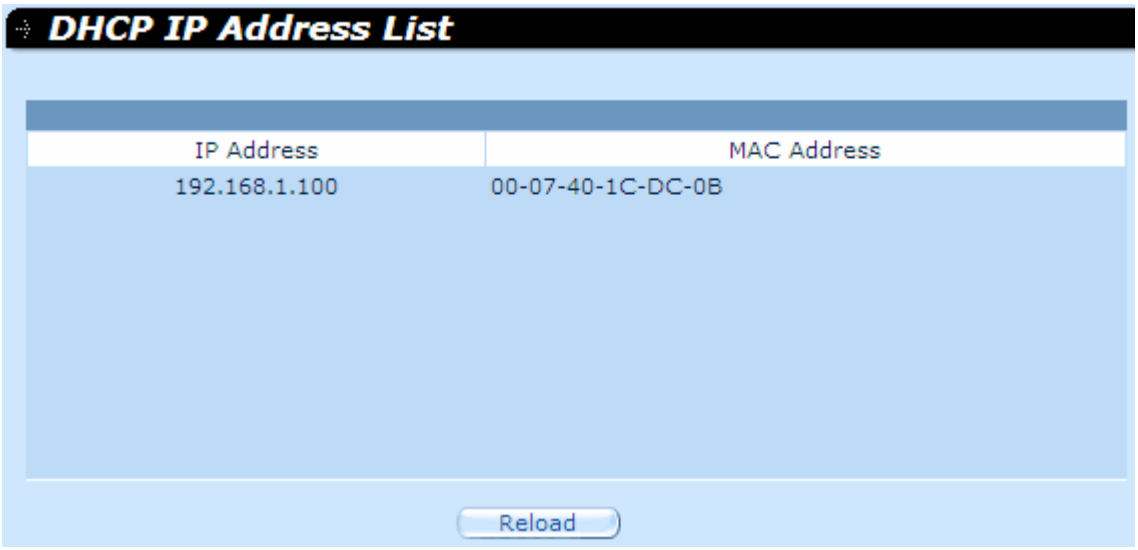


図 6.2. DHCP 割り当て表

7 静的経路設定

Configuration Manager 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、特定の送信先へ向けられている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 経路が特定すると、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デフォルト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、デフォルトゲートウェイが全てのインターネットトラフィックを RX3141 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 コンピュータはデフォルト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）
- RX3141 のデフォルトゲートウェイは全てのアウトバウンドインターネットトラフィックを ISP 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、ISP が自動的にデフォルトゲートウェイを割り当てます。（デフォルト経路の追加方法 7.2.2 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、2 つ以上の ISP 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 静的経路

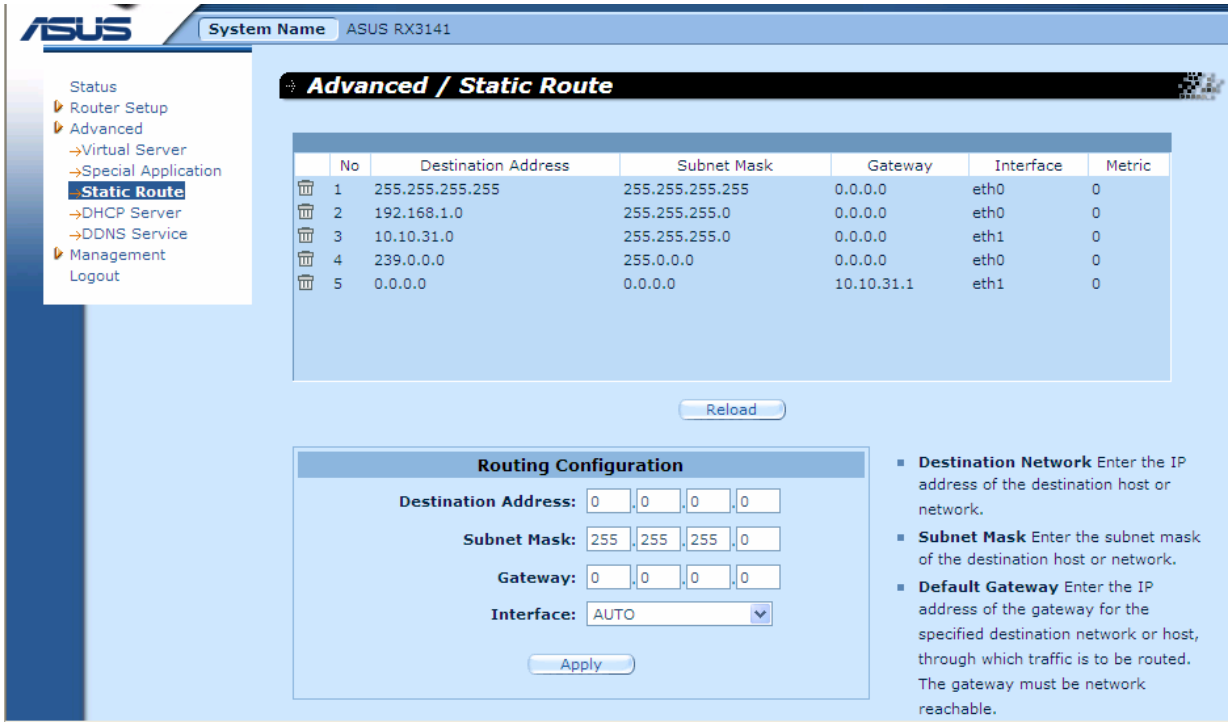


図 7.1. 経路設定画面

7.2.1 静的経路設定項目

下の表は静的経路の設定項目です。

表 7.1. 静的経路設定項目

フィールド	説明
Destination Address	送信先の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、数字のゼロを設定し、他に経路が定義されていない送信先に使う経路であることを示します（デフォルトゲートウェイを作成する経路）。デスティネーション IP はネットワーク ID と同じである必要があります。デフォルト経路は、0.0.0.0 というデスティネーション IP を使います。ネットワーク ID に関する詳細は Appendix 12 をご覧ください。
Subnet Mask	デスティネーション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のかを示します（詳細 Appendix 12 参照）。サブネットマスクのデフォルト経路は 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。 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。

7.2.2 静的経路を追加する

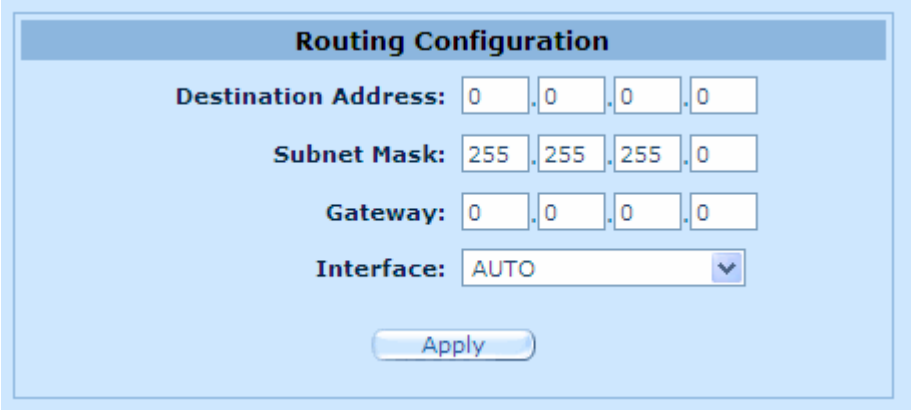


図 7.2. 静的経路設定画面

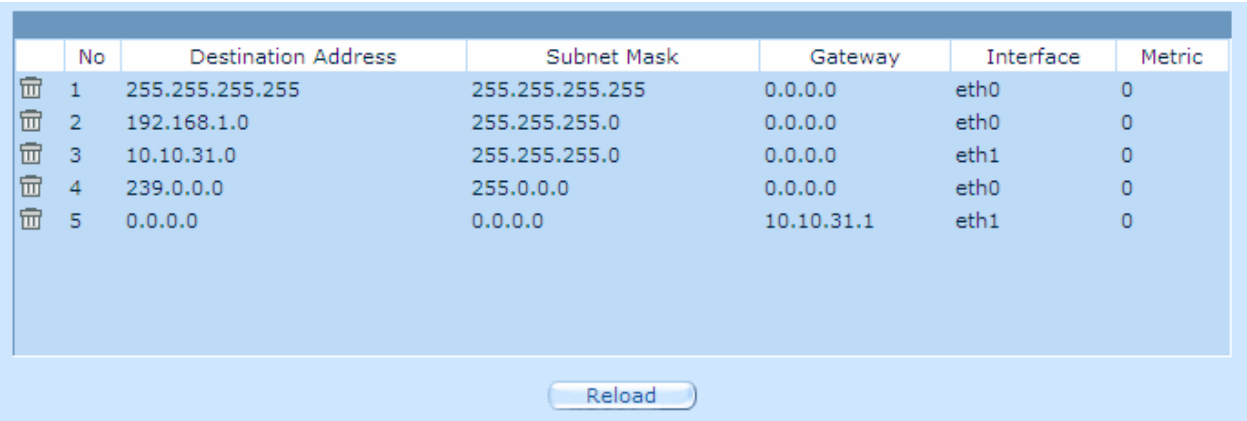
静的経路を経路制御表に追加する

1. **Advanced** ➔ **Static Route** の順にクリックして静的経路設定画面を開きます。
2. 静的経路情報（デスティネーション IP アドレス、デスティネーションサブネットマスク、ゲートウェイ IP アドレス、インターフェース）をそれぞれのフィールドに入力します。

   詳細は、表 7.1. をご覧ください。

   Destination IP Address と **Subnet Mask** のフィールドに「0.0.0.0」と入力し、LAN のデフォルトゲートウェイを定義する経路を作成します。
3. Apply をクリックして新しい経路を追加します。

7.2.3 静的経路を削除する



No	Destination Address	Subnet Mask	Gateway	Interface	Metric
1	255.255.255.255	255.255.255.255	0.0.0.0	eth0	0
2	192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
3	10.10.31.0	255.255.255.0	0.0.0.0	eth1	0
4	239.0.0.0	255.0.0.0	0.0.0.0	eth0	0
5	0.0.0.0	0.0.0.0	10.10.31.1	eth1	0

図 7.3. 経路制御表(例)

手順

1. **Advanced ➔ Static Route** の順にクリックして、静的経路設定画面を開きます。
2. 経路制御表の削除する経路の アイコンをクリックします。

警告

デフォルトゲートウェイの経路はむやみに削除しないでください。インターネット接続不能になることがあります。.

7.2.4 静的経路制御表を確認する

IP が有効なコンピュータやルータは、ユーザがよくアクセスする IP アドレスを記録します。それぞれの *デスティネーション 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*になりす。

Advanced ➔ Static Route の順にクリックして、本製品の経路制御表を確認します。経路制御表は、図 7.1 のように静的経路設定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(デスティネーションネットワークの IP アドレス、デスティネーションネットワークのサブネットマスク、トラフィックを転送するゲートウェイのIPアドレスを含む)の情報を表示します。

8 DDNS（ダイナミック DNS）設定

DDNS(Dynamic DNS)は、IP アドレスの変更があっても（コンピュータの再起動時や ISP の DHCP サーバが IP のリースをリセットした場合）同じドメイン名を持つことができるサービスです。本製品は 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う、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 は以下の機能を持つ DDNS クライアントをサポートします。

- 外部インターフェースを検出した際の DNS 履歴（追加）の更新
- DNS 強制更新

HTTP DDNS クライアントのみのサポートです。

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利用して DNS 履歴を動的に更新します。プロバイダが DNS 内の DNS 履歴を更新することになります。本製品は HTTP をトリガーとして更新を行います。また、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

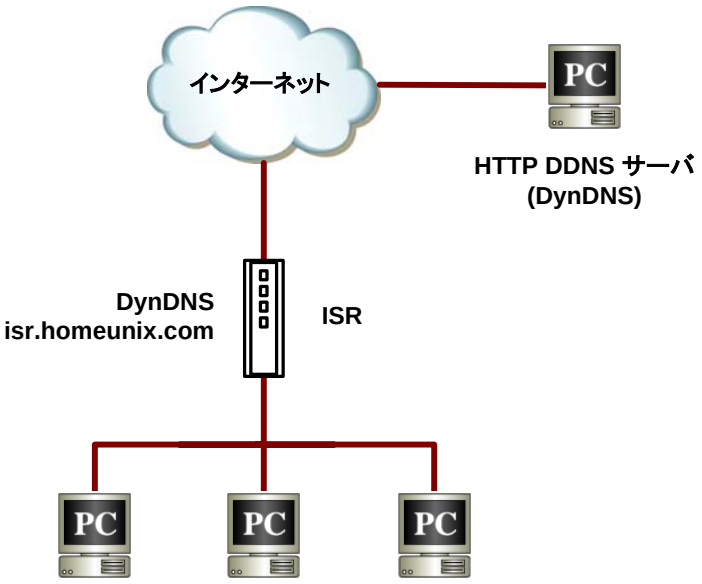


図 8.1. ネットワーク（HTTP DDNS）

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。本製品は、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設定されます。

8.1 DDNS 設定項目

表 8.1 は DDNS サービスの設定項目です。

表 8.1. DDNS 設定項目

フィールド	説明
Status DDNS の状態を表示します。	
Dynamic DNS	
Enable	DDNSサービスを有効にします。
Disable	DDNSサービスを無効にします。
Domain Name ISP に登録したドメイン名を入力します。ホスト名が「host1」でドメイン名が「yourdomain.com」の場合の FQDN「完全修飾ドメイン名」は「host1.yourdomain.com」になります。	
Username DDNSサービスプロバイダより提供されたユーザ名を入力します。	
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

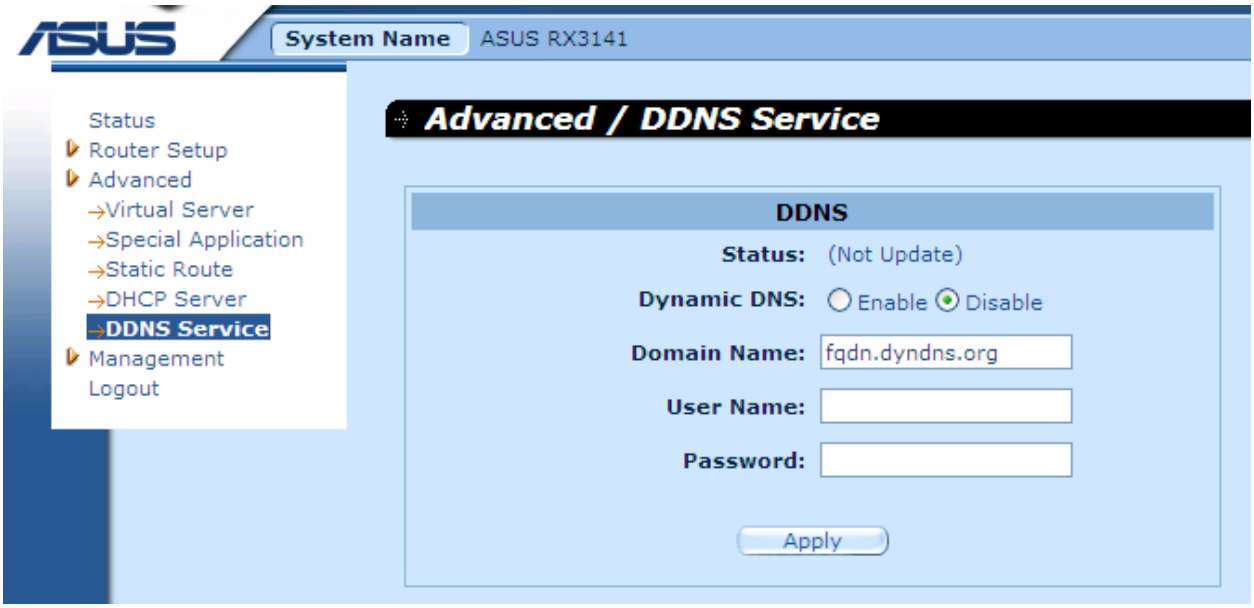


図 8.2. HTTP DDNS 設定画面

HTTP DDNS 設定手順

1. DDNS サービスプロバイダに登録済みのドメイン名が必要です。登録が済んでいない場合は、www.dyndns.org（英文）を参照して登録を終了させてください。
2. Configuration Manager から、**Advanced ➔ DDNS Service** に進み、DDNS 設定画面を開きます。
3. DDNS 設定画面で、「Enable」を選択し、DDNS を有効にします。
4. 「Domain Name」のフィールドにドメイン名を入力します。
5. DDNS サービスプロバイダから提供されたユーザ名とパスワードを入力します。
6. Apply ボタンをクリックして、DDNS サービスプロバイダに DNS 更新要求を送信します。WAN ポートの状態が変わると、DNS は更新リクエストを自動的に DDNS サービスプロバイダへ送信します。

9 ファイアウォールと NAT の設定

本製品は、ファイアウォール/NAT 機能を搭載しており、DoS（Denial of Service）攻撃や LAN への悪意のあるアクセスからシステムを守ります。また、攻撃やアクセスの監視方法を設定することができます。

ルータのセキュリティ設定、ネットワークを通過するデータを制御するために ACL (Access Control List) ルールの作成、修正、削除をします。ファイアウォール設定画面では以下のことを行います。

- ルータのセキュリティ設定、DoS 設定
- インバウンド/アウトバウンド/セルフアクセス ACL ルールの作成、修正、削除、確認
- ファイアウォールログの確認

***注意**: ACL ルールを定義すると、全ての受信パケットはルールに基づいて調査されます。ルールにはネットワーク、インターネットプロトコル、送信方向（例:LAN からインターネットまたはその逆）、送信元のコンピュータの IP アドレス、デスティネーション IP アドレス、他のパケットに付随する特徴が含まれます。*

ルールにマッチしたパケットは、設定したアクションに従って、受信される（デスティネーションに到達）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している状態か判断します。すでに確立された通信の場合は、パケットを通過させます。マッチしない場合は、パケットを破棄します。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ている場合はデフォルトで有効です。特別な設定は必要ありません。ファイアウォールの設定についての詳細は、セクション 9.2.1 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。本製品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についての詳細は、セクション 9.2.1 をご覧ください。

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

9.1.3.1 ACL ルールの優先順位

それぞれの ACL ルールにはルール ID が割り当てられます（番号が小さい ID が優先）。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し、ACL ルールテーブルと照合させてパケットをドロップするか転送するかの決定を行います。番号が小さい ID の ACL ルールから順にチェックを行いマッチするまでチェックを行います。マッチがなかった場合は、アクションの設定にしたがってパケットは破棄されるか転送されます。

9.1.3.2 ACL ルールと接続追跡

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確立されたことのある接続かどうかをすばやく確認することができます。確立された接続であれば、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、ACL ルールが 192.168.1.1 から 192.168.2.1 のアウトバウンド ICMP パケットを許可する設定にした場合、192.168.1.1 が ICMP エコー要求（ping パケット）を 192.168.2.1 へ送ると、192.168.2.1 は 192.168.1.1 へ ICMP エコー応答を送ります。ステートフルパケットインスペクションエンジンは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追加させるので、インバウンド ACL ルールを新しく作成する必要はありません。

9.1.4 デフォルト ACL ルール

本製品は 3 タイプのデフォルトアクセスルールをサポートします。

- Inbound Access Rules：LAN への受信アクセス制御
- Outbound Access Rules：LAN 上のホストから外部ネットワークへの送信アクセス制御
- Self-Access Rules： RX3141 自体へのアクセス制御

Default Inbound Access Rules

デフォルトではインバウンドアクセスルールは設定されていません。外部ホストからの内部ホストへのトラフィックは全て拒否されます。

Default Outbound Access Rules

デフォルトアウトバウンドアクセスルールは LAN から外部ネットワークへ NAT を使って外部ネットワークに全て転送します。

Default Self Access Rules

デフォルトセルフアクセスルールは、LAN からルータへの http、Ping、DNS、DHCP アクセスを許可します。

警告

ACL ルールテーブルからデフォルト ACL ルールを削除する必要はありません。デフォルトルールより優先順位の高いルールを作成することをお勧めします。

9.2 セキュリティ設定

9.2.1 ベーシックルータセキュリティ設定項目

表 9.1 はベーシックルータセキュリティ設定で可能な設定項目です。

表 9.1. ベーシックルータセキュリティ設定項目

フィールド	説明
Firewall	ファイアウォールの設定
NAT	NATの設定
Log Port Probing	有効にすると、閉じたポートへ接続が試みられるとログファイルへ記録します。
Stealth Mode	有効にすると、閉じたTCP/UDPポートに接続しようとする外部ホストに応答しません。

ファイアウォールの基本設定手順

1. **Router Setup** ➔ **Security** の順にクリックして図 9.1 のルータセキュリティ設定画面を開きます。
2. それぞれのオプションで必要なものにチェックを入れます。
3. Apply をクリックして設定を保存します。

9.2.2 DoS 設定

本製品は、なりすまし、LAND、Ping of Death、スマーフ、などの DoS (Denial of Service) 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 ルーズ/ストリクトソースルーティングパケットをドロップします。例えば、セキュリティデバイスと RX3141 のファイアウォールを組み合わせて、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」の防御も可能です。本製品の DoS 防御機能についての詳細は、表 2.1 と 9.2 をご覧ください。

9.2.2.1 DoS 防御設定項目

表 9.2はDoS攻撃についての説明です。チェックボックスにチェックを入れてそれぞれのDoS攻撃に対する 防御を有効にしてください。

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。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IPへ膨大な量の応答が向けられることになります。
SYN/ICMP/UDP Flooding	SYN/ICMP/UDPフラッド。大量のTCP SYN/ICMP/UDPを短時間で送りつけます。本製品では、通常のトラフィックへの影響を避けるためにフラッドパケットをドロップすることはできません。
TCP XMAS/NULL/FIN Scan	特殊なフォーマットのパケットを送り、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攻撃に利用します。 XMAS scan: シーケンス番号0番、FIN、URG、PUSHビットの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が可能かどうかを確かめます。エラーが生じますが、サービスが生きているかどうかで帰ってくるエラーが異なるため、サービスを見分けるために利用されます。
Teardrop	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。受信側の操作システム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はこの攻撃に対して脆弱です。LAN内のコンピュータが最近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。

9.2.2.2 DoS 設定

DoS 設定手順

1. **Router Setup ➔ Security** の順にクリックし、図 9.1 のルータセキュリティ設定画面を開きます。
2. それぞれの DoS 攻撃のタイプにチェックをいれます。
3. Apply をクリックして設定を保存します。

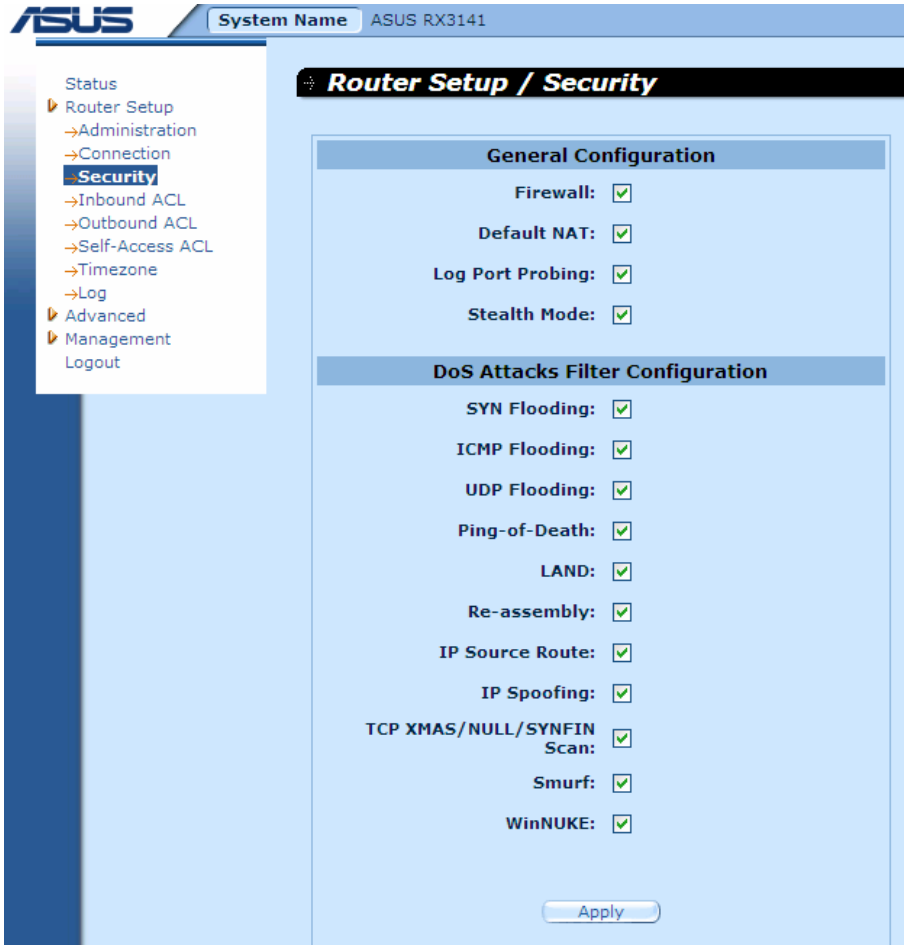


図 9.1. ルータセキュリティ設定画面

9.3 ACL ルール設定項目

9.3.1 ACL ルール設定項目

表 9.3 は、ファイアウォールのインバウンド、アウトバウンド、セルフアクセス ACLルールの設定項目です。

表 9.3. ACL ルール設定項目

フィールド	説明
ID	
Add New	クリックして新しく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て、設定を修正します。
Mave ルールの優先順位を設定します。本製品のファイアウォールはルールの優先順位に基づいて動作します。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
他の番号	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。
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通過させます。
Deny	**拒否** 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**拒否**します。
Route to (アウトバウンドACL用) このオプションは、PPPoE アンナンバードやPPPoEマルチセッション用のポリシールーティングに使用します。 設定オプションは、AUTO、ppp0 (unnumbered)、ppp1 (1st PPPoE session)、ppp2 (2nd PPPoE session) です。オプションはドロップダウンリストから選択します。AUTOに設定すると、経路制御表の情報に基づいてパケットの経路が決まります。	
Log ACLルールでロギングする場合はチェックボックスにチェックを入れます。	
Protocol ドロップダウンリストからプロトコルタイプを選択します。設定オプションは、All、TCP、UDP、ICMP、IGMP、AH、ESPです。	
Source IP ルールを適用させる**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を使って以下の設定オプションを1つ選択します。	
Any	インバウンドトラフィック用にインターネット上ののコンピュータのようなソースネットワークにあるコンピュータや、アウトバウンドトラフィック用にローカルネットワークにあるコンピュータにルールを適用します。
IP Address	ルールを適用するIPアドレスを特定します。

フィールド	説明
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ている全てのコンピュータをインクルードします。このオプションを選択すると、以下の項目が設定可能になります。
Address	適切なIPアドレスを入力します。
Mask	対応するサブネットマスクを入力します。
Self (セルフアクセスルール用)	ルータ自身を示します。
Destination IP 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を使って以下の設定オプションを1つ選択します。	
Any	インバウンドトラフィックようにローカルネットワークにある全てのコンピュータ、アウトバウンドトラフィックようにインターネット上のコンピュータにルールを適用します。
IP Address, Subnet	オプションを選択して詳細を入力します。(上記**Source IP** の項目参照)
Self (for self access rule only)	ルータ自身を示します。
Domain	パソコンのDNSサーバとして本製品を利用した場合のみ利用可能なオプションです。全てのシステムを再起動後にドメイン名とIPアドレスの関連付けは削除されます。マルチプルACLルールは、同じドメイン名とIPアドレスの関連付けに加わります。 ▶ 最大 30 のドメイン名をサポートします。 ▶ それぞれのドメイン名 / IP アドレスの関連付けは、LAN クライアントが DNS クエリーを RX3141 に発行したときのみ更新されます。例えば、ブラウザに、http://www yahoo.com というアドレスを入力すると、内部データベースがファイアウォールによって参照され、www.yahoo.com と IP アドレスが関連付けられます。 ▶ 1 つのドメイン名に、256 の IP アドレスの関連付けることができます。 ▶ ワイルドカードキャラクタ「*」をドメイン名に使うことができます。以下は利用方法例です。 1. www.google.* : www.google.com と ww.google.net にマッチし www.google.com.tw にはマッチしません。 2. www.google.*.*: www.google.com.tw と www.google.com.sg にマッチし www.google.com にはマッチしません。 3. .com.tw :www.google.com.tw と www.com.tw にマッチし、com.tw にはマッチしません。 4. *.com :google.com と abc.com にマッチし www.google.com, com にはマッチしません。 5. *: どのドメイン名にもマッチします。 6. . (ピリオド): どのドメイン名にもマッチします。

フィールド	説明
Source Port ルールを適用するソースポートを設定します。ドロップダウンリストを使って以下の設定オプションを1つ選択します。	
Any	任意のソースポート番号のアプリケーション全てにルールを適用します。
Single	特定のソースポート番号のアプリケーションにルールを適用します。
Port Number	ソースポート番号を入力します。
Range	特定のポートレンジのアプリケーションにルールを適用します。このオプションを選択すると、以下の項目が設定可能になります。
Start Port	ポートレンジの一番小さいポート番号を入力します。
End Port	ポートレンジの一番大きいポート番号を入力します。
Destination Port ルールを適用する送信先ポートを設定します。ドロップダウンリストを使って以下の設定オプションを1つ選択します。	
Any	任意の送信先ポート番号のアプリケーションにルールを適用します。
Single, Range	オプションを選択して詳細を入力します。（上記**Source IP** の項目参照）
ICMP（プロトコルタイプがICMPの場合のみ有効） ACLルール用にICMPメッセージタイプを選択します。対応するICMPメッセージタイプは以下の通りです。 • Any（全て） • 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（あて先到達不能） • 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）	

9.4 インバウンド ACL ルール設定

図 9.2 のように、インバウンドACL設定画面でACLルールを作成すると、LAN上のコンピュータへの受信を制御（許可、拒否）することができます。

この画面のオプションでは以下のことが設定可能です。

- ルールの追加と設定
- ルールの修正
- ルールの削除
- インバウンド ACL ルールの確認

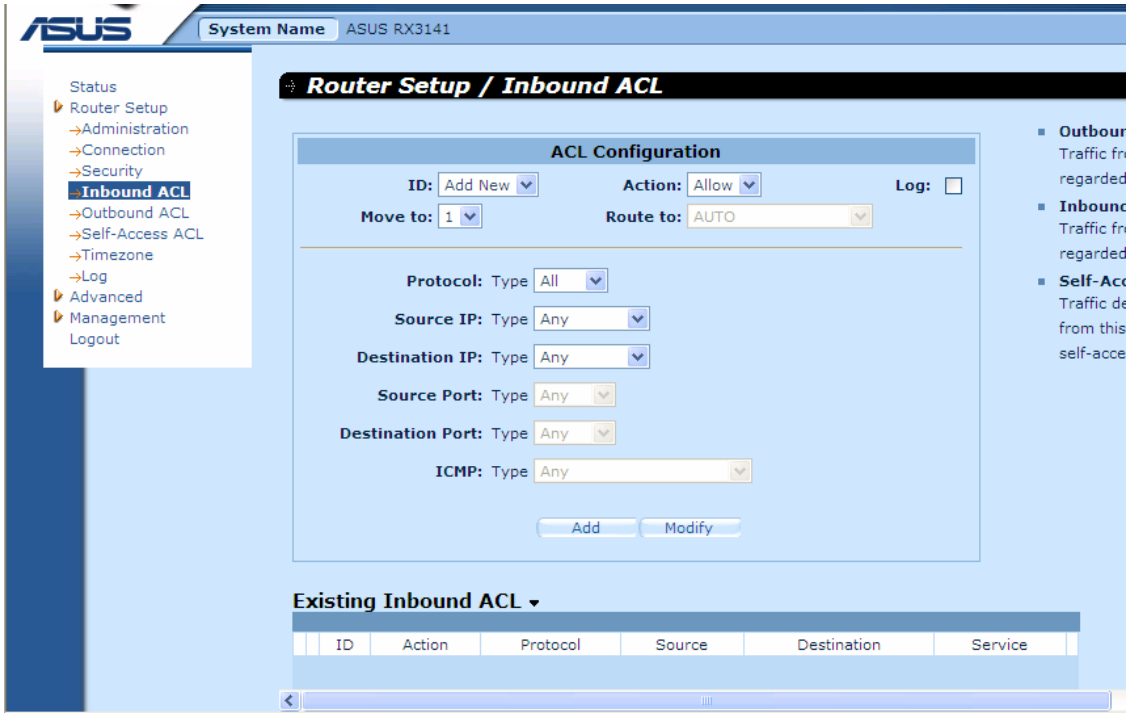


図 9.2. インバウンド ACL 設定画面

9.4.1 インバウンド ACL ルールの追加

インバウンド ACL ルール追加手順

1. **Router Setup** ➔ **Inbound ACL** の順にクリックして図 9.2 のインバウンド ACL 設定画面を開きます。
2. 「**ID**」ドロップダウンリストから「**Add New**」を選択します。
3. 「**Action**」ドロップダウンリストからアクション「Allow（許可）」または「Deny（拒否）」を選択します。
4. 他のフィールドを変更します：ソース/デスティネーション IP、ソース/デスティネーション ポート、プロトコル、ICMP メッセージタイプ、ログ（詳細表 9.3 参照）
5. 「**Move to**」のドロップダウンリストから番号を選択しルールに優先順位を割り当てます。最優先項目には1を割り当てます。優先順位の高い順に小さい番号から割り当てます。

6. Add ボタンをクリックして新しい ACL ルールを作成します。新しい ACL ルールはインバウンド ACL 設定画面の下半分にあるインバウンドアクセスコントロールリストに表示されます。

図 9.3 は、インバウンド HTTP (Web サーバ)サービスを許可するルールの作成方法を示しています。このルールでは、インバウンド HTTP トラフィックは IP アドレスが 192.168.1.28 のホストへ導かれます。新しく追加したインバウンド ACL ルールは、図 9.4 の Existing Inboud ACL に表示されます。

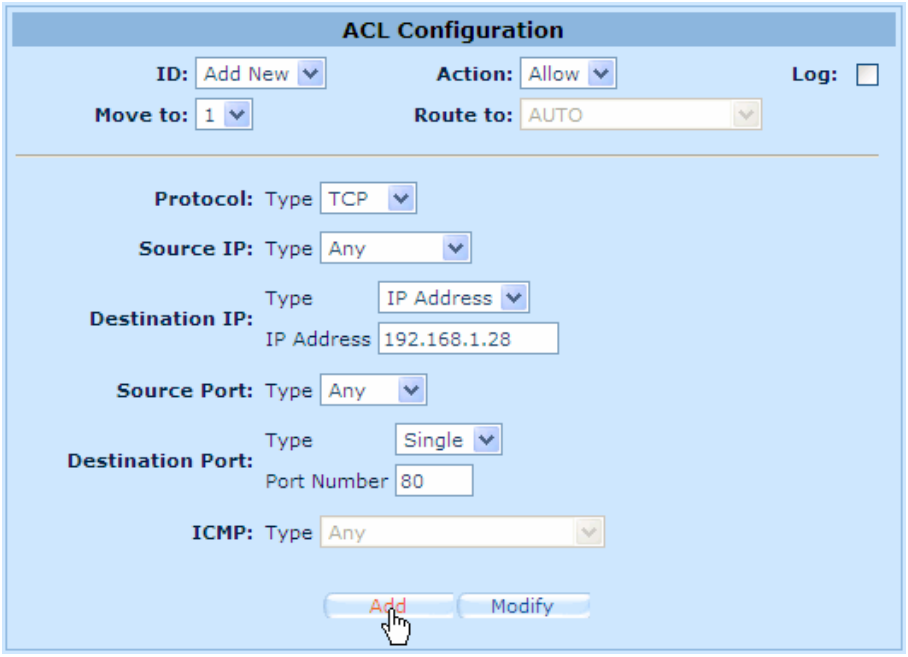


図 9.3. インバウンド ACL 設定(用例)

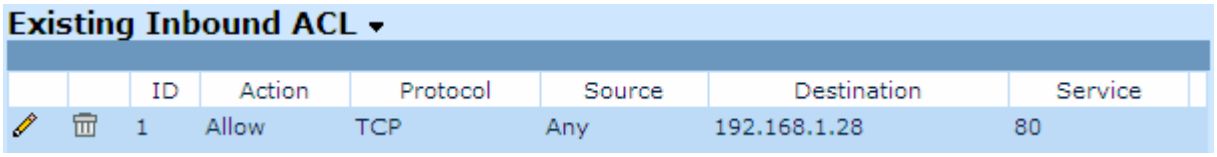


図 9.4 インバウンド ACL リストテーブル

9.4.2 インバウンド ACL ルール修正例

インバウンド ACL ルール修正手順

1. **Router Setup ➔ Inbound ACL** の順にクリックして図 9.2 のインバウンド ACL 設定画面を開きます。
2. インバウンド ACL テーブルにある修正するルールの アイコンをクリック、または「**ID**」ドロップダウンリストからルール番号を選択します。
3. 以下のフィールドを修正します:アクション、ソース/デスティネーション IP、ソース/デスティネーションポート、プロトコル、ICMP メッセージタイプ、ログ。(詳細表 9.3 参照)
4. Modify ボタンをクリックしてこの ACL ルールを修正します。インバウンド ACL 設定画面の下半分にあるインバウンドアクセスコントロールリストに修正した ACL ルールの新しい設定が表示されます。

9.4.3 インバウンド ACL ルールを削除する

Router Setup ➔ Inbound ACL の順にクリックしてインバウンド ACL 設定画面を開き、削除するルールの前にある をクリックします。

9.4.4 インバウンド ACL ルールを確認する

Router Setup ➔ Inbound ACL の順にクリックしてインバウンド ACL 設定画面を開くと、画面の下に現在のインバウンド ACL ルールが表示されます。

9.5 アウトバウンド ACL ルール

図 9.5 のアウトバウンドACLルール設定画面でACLルールを作成することによって、LAN上のコンピュータへのインターネット、外部ネットワークアクセスを制御（許可、拒否）することができます。

この画面のオプションでは以下のことが設定可能です。

- ルールの追加と設定
- ルールの修正
- ルールの削除
- アウトバウンド ACL ルールの確認

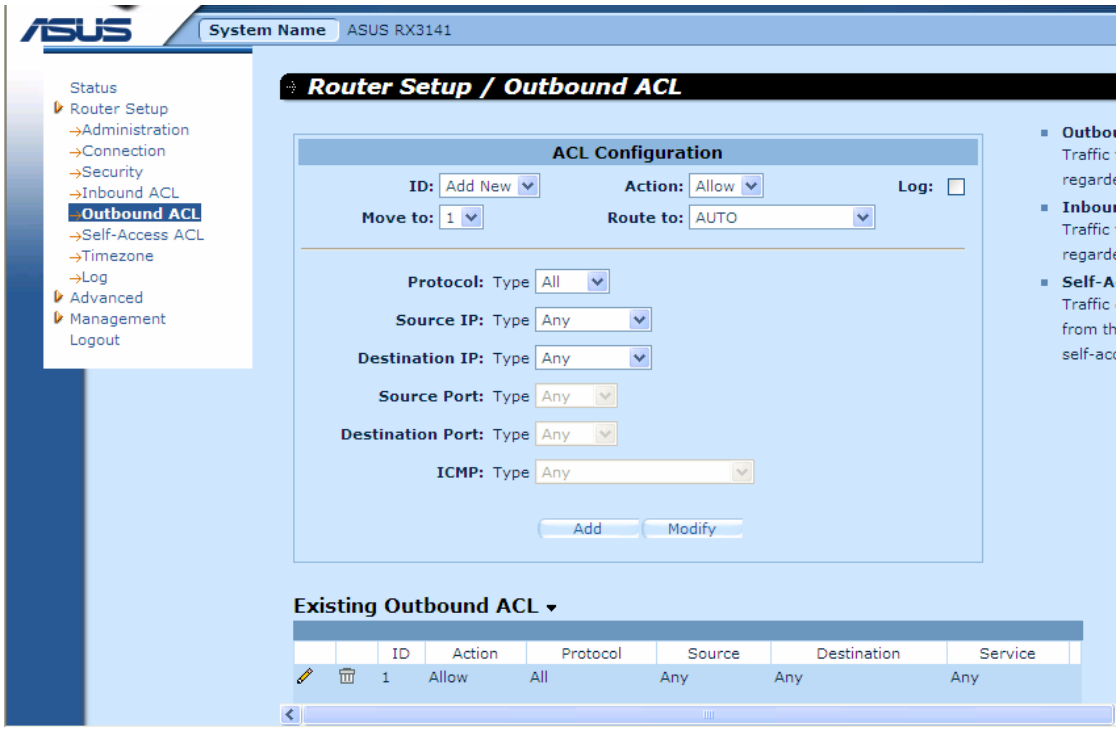


図 9.5. アウトバウンド ACL 設定画面

9.5.1 アウトバウンド ACL ルールの追加

アウトバウンド ACL ルール追加手順

1. **Router Setup ➔ Outbound ACL** の順にクリックして 図 9.5 のアウトバウンド ACL 設定画面を開きます。
2. 「**ID**」ドロップダウンリストから「**Add New**」を選択します。
3. 「**Action**」ドロップダウンリストからアクション「Allow（許可）」または「Deny（拒否）」を選択します。
4. 「**Move to**」のドロップダウンリストから番号を選択しルールに優先順位を割り当てます。最優先項目には 1を割り当てます。優先順位の高い順に小さい番号から割り当てます。
5. パケットを送信する際に使用するインターフェースを選択します。設定オプションは、AUTO、ppp0 (unnumbered)、ppp1 (PPPoE 0)、ppp2 (PPPoE 1)です。大抵の場合は、ACL ルールにマッチしたパケットのトラフィックの送信先をルータが自動に決定する AUTO を選択します。
6. 以下のフィールドを修正します：アクション、ソース/デスティネーション IP、ソース/デスティネーションポート、プロトコル、ICMP メッセージタイプ、ログ。（詳細表 9.3 参照）
7. Add ボタンをクリックして新しい ACL ルールを作成します。新しい ACL ルールはアウトバウンド ACL 設定画面の下半分にあるアウトバウンドアクセスコントロールリストに表示されます。

図 9.6 は、アウトバウンド HTTP トラフィックを許可するルールの作成方法を示しています。このルールでは、アウトバウンド HTTP トラフィック（デスティネーションポート 80)は、LAN 上の IP アドレスが 192.168.1.15 のホスト用に外部ネットワークのホストに転送されます新しく追加したアウトバウンド ACL ルールは図 9.7 の Existing Outbound ACL に表示されます。

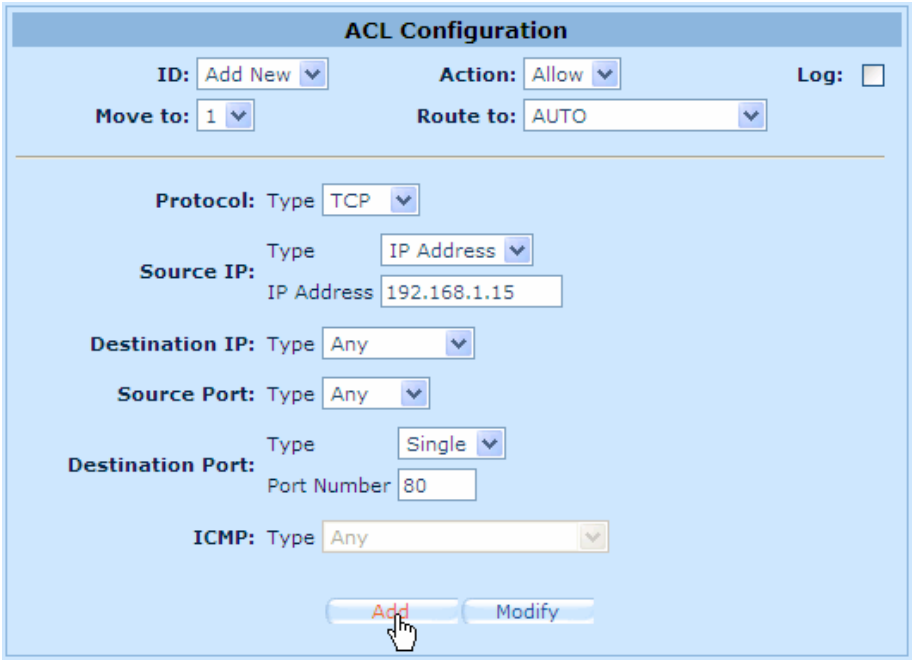


図 9.6. アウトバウンド ACL 設定（用例）

Existing Outbound ACL

		ID	Action	Protocol	Source	Destination	Service
✎	🗑	1	Allow	TCP	192.168.1.15	Any	80
✎	🗑	2	Allow	All	Any	Any	Any

図 9.7 アウトバウンド ACL リストテーブル例

9.5.2 アウトバウンド ACL ルールを修正する

アウトバウンド ACL ルール修正手順

1. **Router Setup** ➔ **Outbound ACL** の順にクリックして図 9.5 のアウトバウンド ACL ルール設定画面を開きます。
2. アウトバウンド ACL テーブルにある修正するルールの アイコンをクリック、または「**ID**」ドロップダウンリストからルール番号を選択します。
3. 以下のフィールドを修正します：アクション、ソース/デスティネーション IP、ソース/デスティネーションポート、プロトコル、ICMP メッセージタイプ、ログ。（詳細表 9.3 参照）
4. Modify ボタンをクリックしてこの ACL ルールを修正します。アウトバウンド ACL 設定画面の下半分にあるアウトバウンドアクセスコントロールリストに修正した ACL ルールの新しい設定が表示されます。

9.5.3 アウトバウンド ACL ルールを削除する

Router Setup ➔ **Outbound ACL** の順にクリックしてアウトバウンド ACL 設定画面を開き、削除するルールの前にある をクリックします。

9.5.4 アウトバウンド ACL ルールを確認する

Router Setup ➔ **Outbound ACL** の順にクリックしてアウトバウンド ACL 設定画面を開きます。

9.6 セルフアクセス ACL ルール設定 – (Router Setup ➔ Self-Access ACL)

図 9.8 のセルフアクセスルール設定画面で、本製品（RX3141）自体の双方向のアクセス制御をします。

- セルフアクセスルールの追加
- セルフアクセスルールの修正
- 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

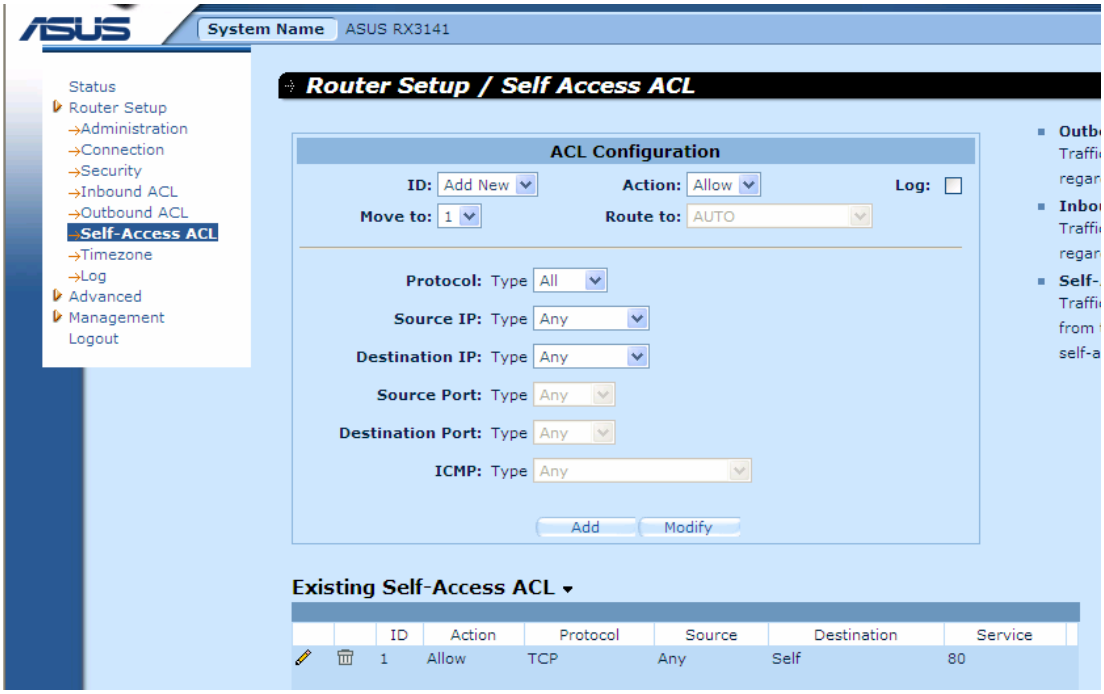


図 9.8. セルフアクセスルール設定画面

9.6.1 セルフアクセスルールの追加

セルフアクセスルール追加手順

1. **Router Setup** ➔ **Self Access ACL** の順にクリックして図 9.8 のセルフアクセスルール設定画面を開きます。
2. 「**ID**」ドロップダウンリストから「**Add New**」を選択します。
3. 「**Action**」ドロップダウンリストからアクション「Allow（許可）」または「Deny（拒否）」を選択します。
4. 「**Move to**」のドロップダウンリストから番号を選択しルールに優先順位を割り当てます。最優先項目には 1を割り当てます。優先順位の高い順に小さい番号から割り当てます。
5. 以下のフィールドを修正します：アクション、ソース/デスティネーション IP、ソース/デスティネーションポート、プロトコル、ICMP メッセージタイプ、ログ。（詳細表 9.3 参照）
6. Add ボタンをクリックして新しいセルフアクセスルールを作成します。新しい ACL ルールはセルフアクセスルール設定画面の下半分にある Existing Self-Access ACL に表示されます。

用例

図 9.9 は、TCP ポート 80 トラフィック（ HTTP トラフィック）が RX3141 へのアクセスを許可されるというセルフアクセスルール設定例です。

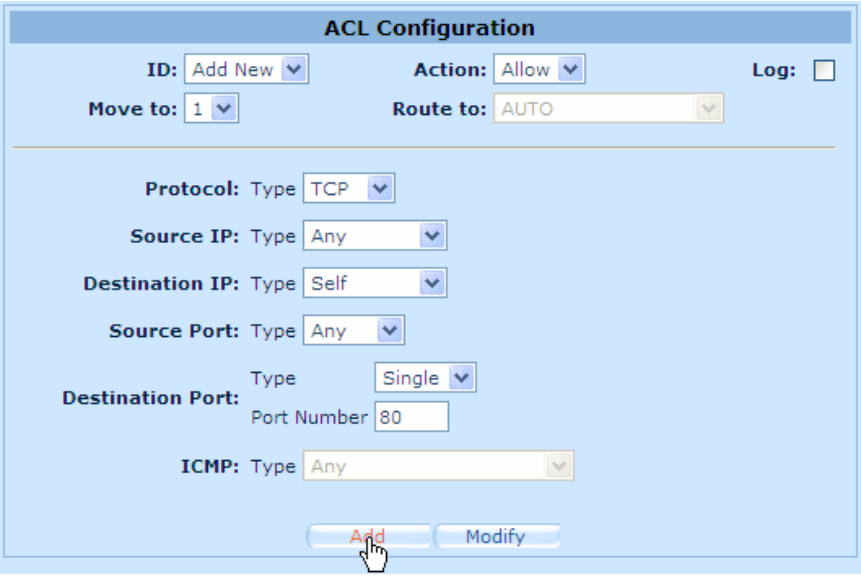


図 9.9. セルフアクセス ACL 設定(用例)

9.6.2 セルフアクセスルールを修正する

セルフアクセスルール修正手順

1. **Router Setup** ➔ **Self Access ACL** の順にクリックして図 9.8 のセルフアクセスルール設定画面を開きます。
2. **Existing Self-Access ACL** テーブルにある修正するルールの アイコンをクリック、または「**ID**」ドロップダウンリストからルール番号を選択します。
3. 設定を変更します。
4. Apply ボタンを押して変更を保存します。セルフアクセスルール設定画面の下半分にある **Existing Self-Access ACL** に ACL ルールの新しい設定が表示されます。

9.6.3 セルフアクセスルールを削除する

Router Setup ➔ **Self Access ACL** の順にクリックしてセルフアクセスルール設定画面を開き、削除するルールの前にある をクリックします。

9.6.4 セルフアクセスルールを確認する

Router Setup ➔ **Self-Access ACL** の順にクリックしてセルフアクセスルール設定画面を開きます。

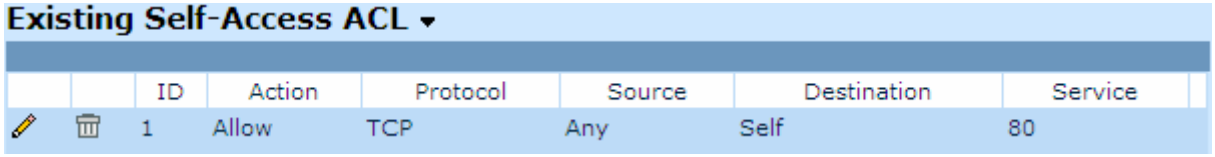


図 9.10 Existing Self-Access ACL

9.7 ファイアウォールログ – (Router Setup ➔ Log)

Router Setup ➔ Log の順にクリックして、ファイアウォールログ画面を開くと、セキュリティルールに反するログを確認することができます。図 9.11 はファイアウォールログの一例です。ログ画面の下にある Reload ボタンをクリックすると更新されたログを確認することができます。

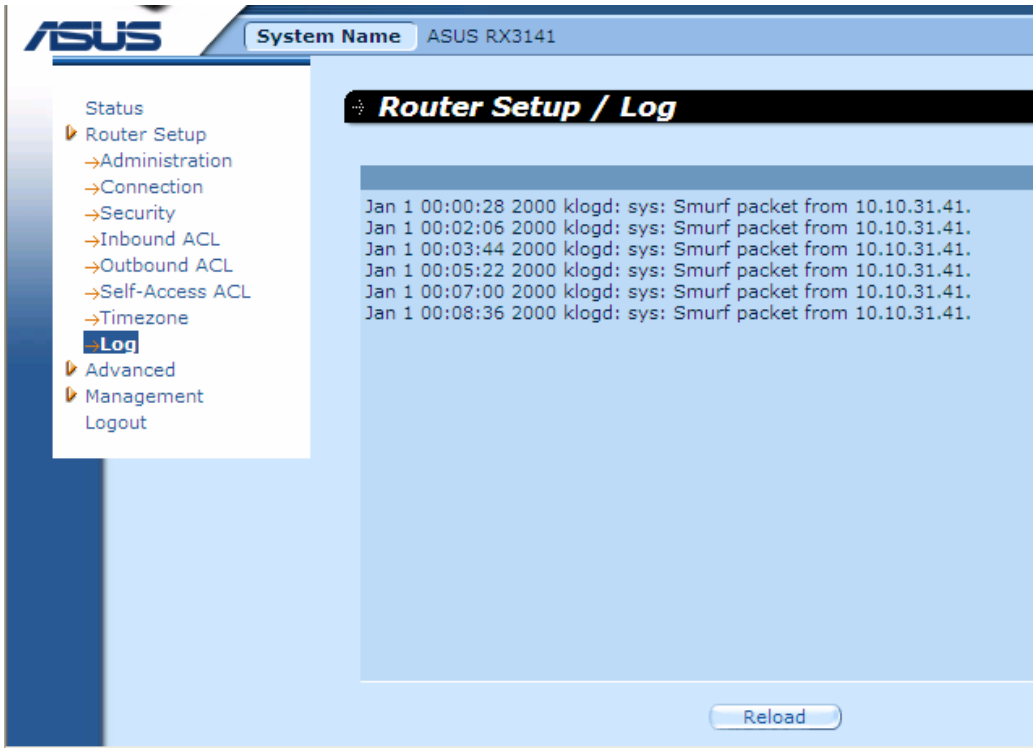


図 9.11 ファイアウォールログ(例)

9.7.1 ログフォーマット

本製品では2タイプのログをサポートしています。– システムセキュリティログとファイアウォールアクセスコントロールログです。それぞれ「sys」、「fw」と表記されます。以下はログフォーマットの説明です。

システムセキュリティログ 例:

Jan 1 00:01:22 2000 klogd: sys: TCP XMAS/NULL packet from 192.168.1.100.

説明:**Jan 1 00:01:22 2000**(攻撃のあった時間)、**klogd: sys** (この攻撃はシステムセキュリティモデルによって検出されました)、**TCP XMAS/NULL**(検出された攻撃のタイプ)、**192.168.1.100**(攻撃のソース)

ファイアウォールアクセスコントロールログ 例

Jan 1 00:03:11 2000 klogd: fw: OUTBOUND rule=1 allow icmp from 192.168.1.100 to 211.1.1.1 type=8 code=0 id=512

説明:**Jan 1 00:03:11 2000** (アクセスのあった時間)、**klogd: fw**,(ファイアウォールアクセスコントロールに関係するログ)、**OUTBOUND**(トラフィックの方向)、**rule=1**,(トラフィックの IP 情報とマッチしたルール)、**allow**,(ファイアウォールのアクション)、**icmp**(トラフィックのプロトコルタイプ)**192.168.1.100**(トラフィックのソース)**211.1.1.1**(トラフィックのデスティネーション)、type=8(ICMP メッセージタイプ)code=0(ICMP メッセージコード)id=512(ICMP メッセージ ID)

10 仮想サーバとスペシャルアプリケーション

本章は、以下の設定手順の説明をします。

- 仮想サーバ
- スペシャルアプリケーション

NAT は、上記のアプリケーションをサポートするための技術です。

10.1 NAT 概要

NAT(Network Address Translation)によって、本製品のようなデバイスが、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)ネットワーク間の代理人のように機能します。つまり、外部ネットワークに対して、NAT IP アドレスは、コンピュータのグループを代表することになります。NAT は、ネットワークのグローバル IP アドレスの節約、IP アドレッシング業務の簡易化メカニズムです。 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へのセキュリティを提供します。

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

IP マスカレードとも呼ばれるこの機能は、1 つのグローバルアドレスにいくつも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 10.1 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へ、マッピングすることによって、インターネットにアクセスすることを示しています。

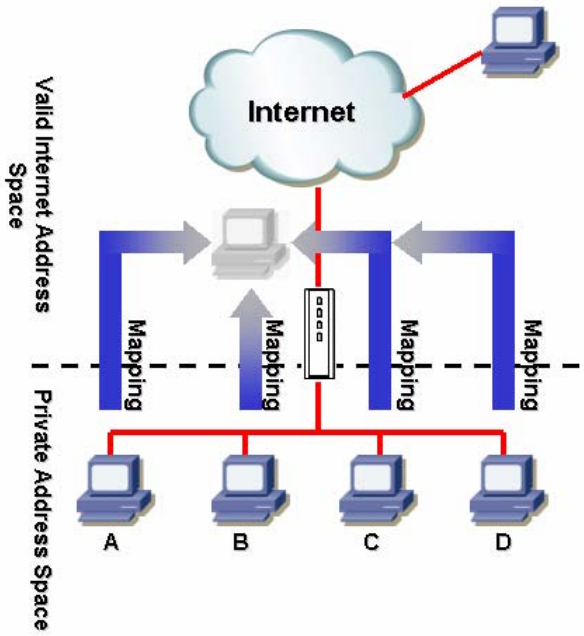


図 10.1 NAPT – 1 つのグローバル IP アドレスに内部 PC をマッピング

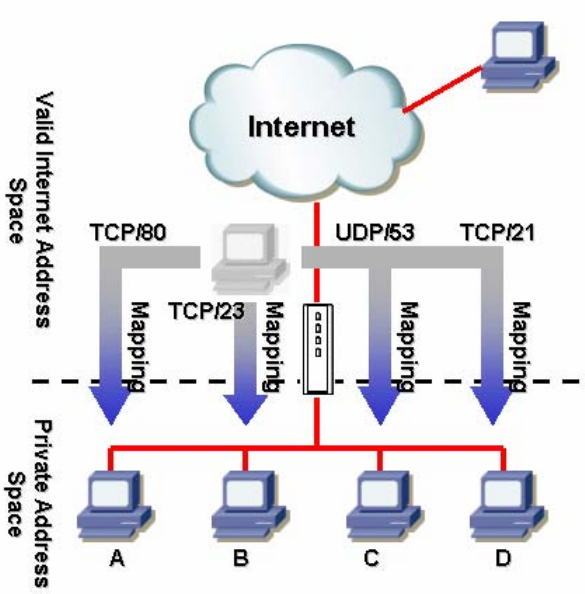


図 10.2 Reverse NAPT –プロトコル、ポート番号、IP アドレスに基づき、受信パケットを内部ホストに中継

10.1.2 リバース NAPT / 仮想サーバ

リバース NAPT は、インバウンドマッピング、ポートマッピング、仮想サーバとも呼ばれます。外部から RX3141 に入ってくるパケットを、ACL ルールで特定したプロトコル、ポート番号、IP アドレスに基づいて、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 10.2 は、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、それぞれのサービスのインバウンドトラフィックがそれぞれのサービスのホストに導かれることを示しています。

10.2 仮想サーバの設定

RX3141 の仮想サーバ機能は、インターネット上の外部ユーザーがアクセス可能なパブリックサーバ(Web、電子メール、FTP サーバなど) を最大 10 種類まで設定することができます。サービスは、固定 IP アドレスで構成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、ルータが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

RX3141 は 1 度に1台のサーバしかサポートしません。

10.2.1 仮想サーバ設定項目

表 10.1は、仮想サーバ設定で可能な設定項目と説明です。

表 10.1 仮想サーバ設定項目

設定項目	説明
Enable	あらかじめ設定してあるアプリケーションのリストからアプリケーションを選択します。対応するプロトコルとリダイレクトポート範囲は自動的に選択されます。手動で設定する場合は、「Manual Setting」を選択してください。チェックボックスにチェックを入れてポリシーを有効にします。あらかじめ設定してあるアプリケーションについては、表 10.2 をごらんください。
Protocol	ドロップダウンリストからプロトコルタイプを選択します。設定オプションは All、TCP、UDP、TCP/UDP、ESP です。
Redirect Port Range	ポート番号を入力します。
To IP Address	サーバ IP アドレスを入力します。

表 10.2. アプリケーション用ポート番号

アプリケーション	サービスポート番号
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
HTTP8080	TCP 8080-8080
HTTPS	TCP 443-443
I-phone 5.0	TCP/UDP 22555-22555
ISAKMP	UDP 500-500
mIrc	6601-700
MSN Messenger	1863 ALG
Need for Speed 5	9400-9400
Netmeeting Audio	TCP 1731-1731

アプリケーション	サービスポート番号
Netmeeting Call	TCP 1720-1720
Netmeeting Conference	UDP 49500-49700
Netmeeting File Transfer	TCP 1503-1503
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	13223-13223
Red Alert II	1234-1237
SMTP	TCP 25-25
Sudden Strike	2300-2400
TELNET	TCP 23-23
Win VNC	UDP 5800-5900

10.2.2 仮想サーバ 設定例

FTP サーバ設定手順

1. **Advanced** ➔ **Virtual Server** の順にクリックして、図 10.3 の仮想サーバ設定画面を開きます。
2. Enable のドロップダウンリストから **FTP** を選択し、チェックボックスにチェックを入れポリシーを有効にします。Protocol と Redirect Port Range は自動的に選択されます。
3. FTP サーバの IP アドレスを入力します。ここでの IP アドレスはプライベート IP アドレスです。
4. Apply をクリックして設定を保存します。

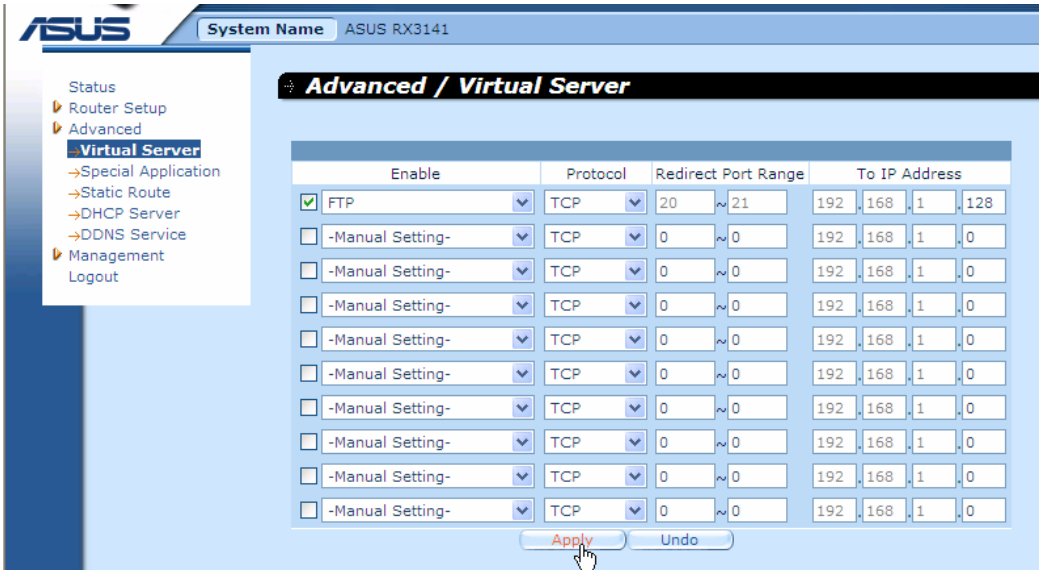


図 10.3 仮想サーバ設定画面　例

5. 本製品はセキュリティー面から、各仮想サーバに外部ユーザーの内部サーバへのアクセスを許可するように適切なインバウンド ACL ルールを仮想サーバ設定画面で設定しない限り、外部ユーザーからの全てのアクセス要求を拒否します。例えば、外部ネットワークから FTP サーバへのアクセスを許可する場合は、図 10.4 のようにインバウンド ACL ルールを定義する必要があります。「Destination IP」は、仮想サーバ設定画面の「**To IP Address**」の IP アドレスです。「Destination Port」は、仮想サーバ設定画面の「**Redirect Port Range**」のポート番号です。特定の IP アドレスからの FTP サーバへのアクセスを制限する場合は、インバウンド ACL ルールの「Source IP」の設定を変更します。例えば、インバウンド ACL ルールのソース IP が「198.175.2.10」の場合、FTP サーバへの外部アクセスはこの特定の IP アドレスからのアクセスを除いて全ての拒否されます。インバウンド ACL ルールについての詳細は **9.4 インバウンド ACL ルール設定**をご覧ください。

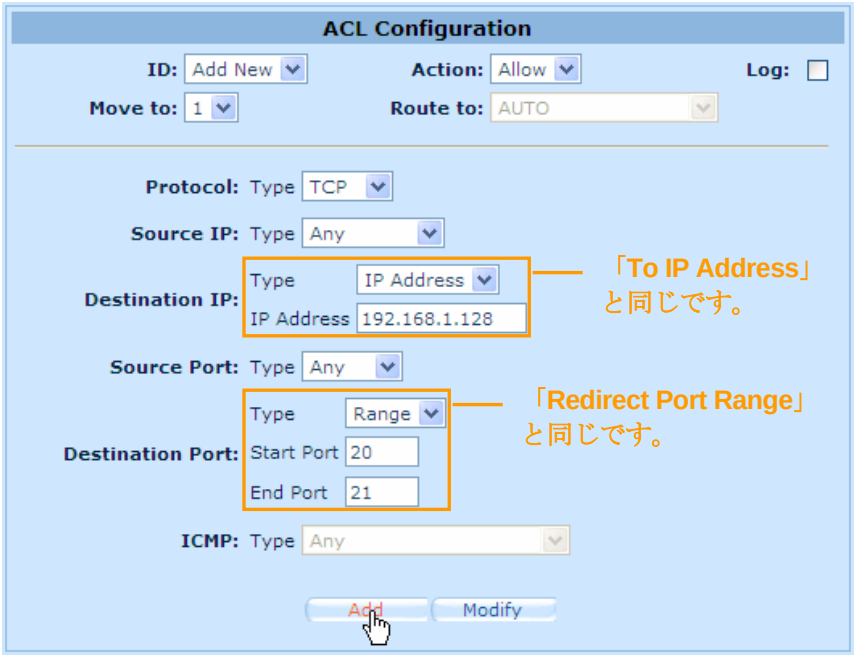


図 10.4 仮想サーバ 例 – インバウンド ACL ルールでスペシャルアプリケーションを設定

データ転送に TCP/UDP ポートを使うアプリケーションは、NAT 機能のため通常本製品のようなルータではご利用できませんが、スペシャルアプリケーションを設定することによって、いくつかのアプリケーションをご利用いただけるようになります。


注

1 度に 1 台の PC が使えるスペシャルアプリケーションは 1 つだけです。

10.2.3 スペシャルアプリケーション設定項目

表 10.1 はスペシャルアプリケーション設定で可能な設定項目と説明です。

表 10.3. スペシャルアプリケーション設定項目

設定項目	説明
Enable	あらかじめ設定してあるアプリケーションのリストからアプリケーションを選択します。対応するプロトコルとリダイレクトポート範囲は自動的に選択されます。手動で設定する場合は、「Manual Setting」を選択してください。 チェックボックスにチェックを入れてポリシーを有効にします。
Application Name	アプリケーションの名前です。
Outgoing (Trigger) Port Range	アウトバウンドパケットを送信する際にアプリケーションが使うポート範囲です。送信ポート番号はトリガーとして機能します。ルータがこのポート番号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受信ポート番号の対応するインバウンドパケットがルータを通過できるようになります。よく使われるアプリケーションが使うポート番号については、表 10.4 をご覧ください。
Incoming Port Range	使用されるインバウンドパケットに対応するポート範囲です。よく使われるアプリケーションが使うポート番号については、表 10.4 をご覧ください。

表 10.4 よく使われるアプリケーションのポート番号

アプリケーション	Outgoing Port Number	Incoming Port Range
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	12120,12122,24150–24220
Quick Time 4	554	6970–6999
wowcall	8000	4000–4020

10.2.4 スペシャルアプリケーション 設定例

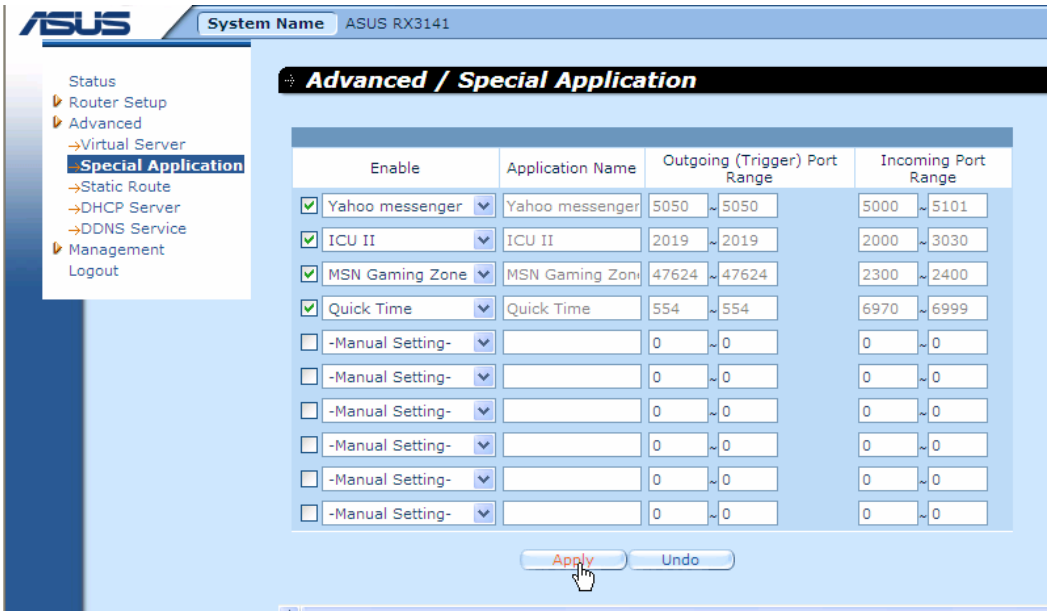


図 10.5. スペシャルアプリケーション設定画面

Quick Time 用のスペシャルアプリケーション設定手順

1. **Advanced** ➔ **Special Application** の順にクリックして、図 10.5 のスペシャルアプリケーション設定画面を開きます。
2. Enable のドロップダウンリストから **Quick Time** を選択し、チェックボックスにチェックを入れポリシーを有効にします。Application Name、Outgoing(Trigger)Port Range、Incoming Port Range は自動的に選択されます。
3. Apply をクリックして設定を保存します。
4. RX3141 のデフォルトアウトバウンド ACL ルールでは、全てのアウトバウンドトラフィックを外部ネットワークへ転送します。このデフォルトアウトバウンド ACL ルールでは、スペシャルアプリケーション設定画面で定義したアプリケーションは誰でも使うことができます。セキュリティなどの理由で、特定のユーザに対してアプリケーションの使用に制限を加えたい場合は、アウトバウンド ACL ルールの設定を行い、アウトバウンドアクセスを制御します（図 10.6）。図 10.6 の例は、192.168.1.110 ～ 192.168.1.115 の IP アドレス範囲のホストに対して制限を加えたものです。デフォルト ACL ルールではスペシャルアプリケーション設定画面のアプリケーション設定を誰でもが使えるので、アクセス制限を有効にするには、デフォルトファイアウォールアウトバウンド ACL ルールを削除する必要があります。アウトバウンド ACL ルール設定画面のアウトバウンド ACL ルール（図 10.7）の前にある アイコンをクリックすると、デフォルトアウトバウンド ACL ルールを削除することができます。オンボード ACL ルールについての詳細は、**9.5 アウトバウンド ACL ルール**をご覧ください。

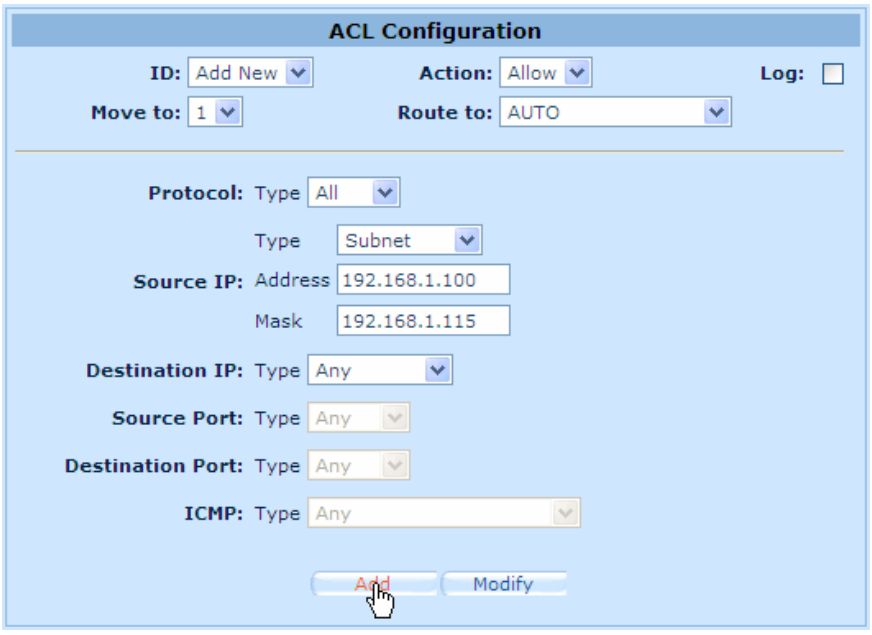


図 10.6. スペシャルアプリケーション 例 – アウトバウンド ACL ルール

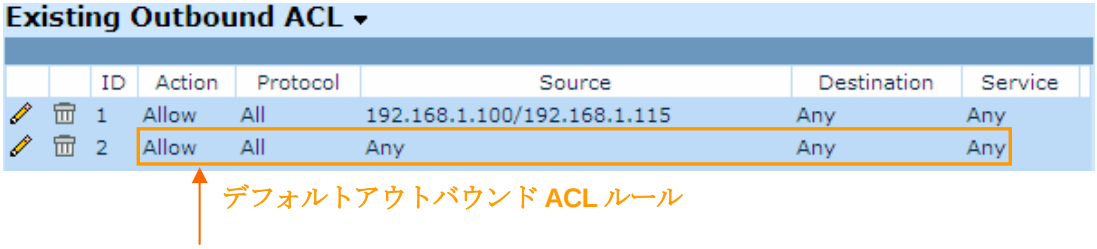


図 10.7. アウトバウンド ACL ルール

11 システム管理

本性では、管理設定で行える以下の管理業務の説明をします。

- パスワードとシステム全般設定の修正
- システム情報の確認
- システム日時の修正
- システム設定のリセット
- システムの再起動
- ファームウェアのアップデート
- システム設定のバックアップ/リストア

11.1 ログインパスワードとシステム全般の設定

初めて管理設定にログインする時に使うデフォルトユーザー名とパスワードはそれぞれ(admin 、admin)です。

注

このユーザー名とパスワードは管理設定にログインする時に使うもので、ISP に接続する際に使うパスワードとは異なります。

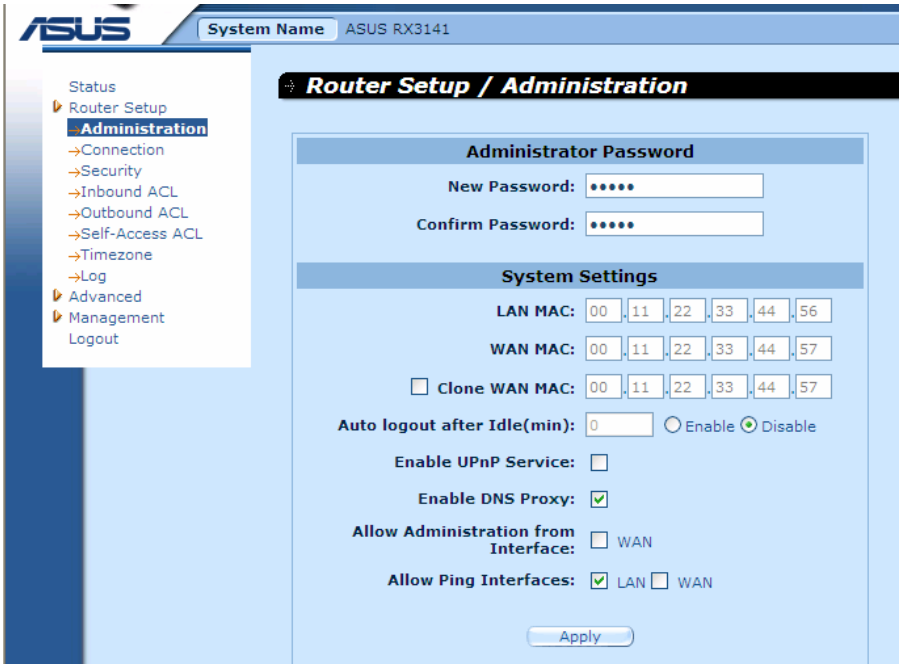


図 11.1. システム管理設定画面

システム管理設定画面(図 11.1)で、ログインパスワードや RX3141 システム全般の設定を変更することができます。以下の手順に従って、パスワード変更、システム全般の設定をしてください。

1. **Router Setup** ➔ **Administration** m の順にクリックし、システム管理設定画面(図 11.1)を開きます。

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 フィールドにもう一度同じパスワードを入力します。パスワードは大文字、小文字を区別した 16 字までの英数字です。

2. WAN 用に MAC アドレスをクローンする

a) インターネットアクセス用に ISP に登録済みの MAC アドレスが必要な場合は、登録済みの MAC アドレスを入力します。指定がない場合はデフォルト（工場出荷時の WAN ポート用 MAC アドレス）を使います。

3. Auto logout after idle (min) 無動作時の自動ログアウト

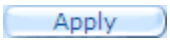
a) このオプションを有効にするには、「Enable」のラジオボタンをクリックし、タイムアウトまでの時間（分）を入力します。無効にする場合は、「Disable」のラジオボタンをクリックするか、テキストフィールドに「0」と入力します。このオプションを有効に設定して、ブラウザを通してシステムを設定中にアイドルタイマが切れると、ルータから自動的に切断されます。システム設定を続行する場合はもう一度 RX3141 にログインする必要があります。

4. Enable UPnP service：UpnP サービスの設定をします。

5. Enable DNS Proxy：DNS プロキシサービスの設定をします。

6. Allow Administration from Interface：WAN ポートを通したリモート管理の設定をします。

7. Allow Ping Interface：LAN/WAN のチェックボックスにチェックを入れると、LAN/WAN インターフェースから RX3141 に Ping が打てるようになります。このオプションは、LAN のみを有効にすることを強くお勧めします。

8. 

ボタンをクリックして設定を保存します。

11.2 システム情報を確認する

システム情報画面は RX3141 にログインすると表示されます。システム全般の情報を確認することができます。

図 11.2. システム状態

11.3 日時の設定

RX3141 は日時を記録し、計算やさまざまなデータの報告に使います。本製品にはリアルタイムクロックは内臓していないので、外部タイムサーバを利用して時間を正確に維持します。外部タイムサーバは 3 台まで設定することができます。「**Enable**」にチェックを入れて SNTP (Simple Network Time Protocol) を有効にし、時間を正確に維持してください。

注

RX3141 の日時設定は、パソコン上の日時には影響しません。

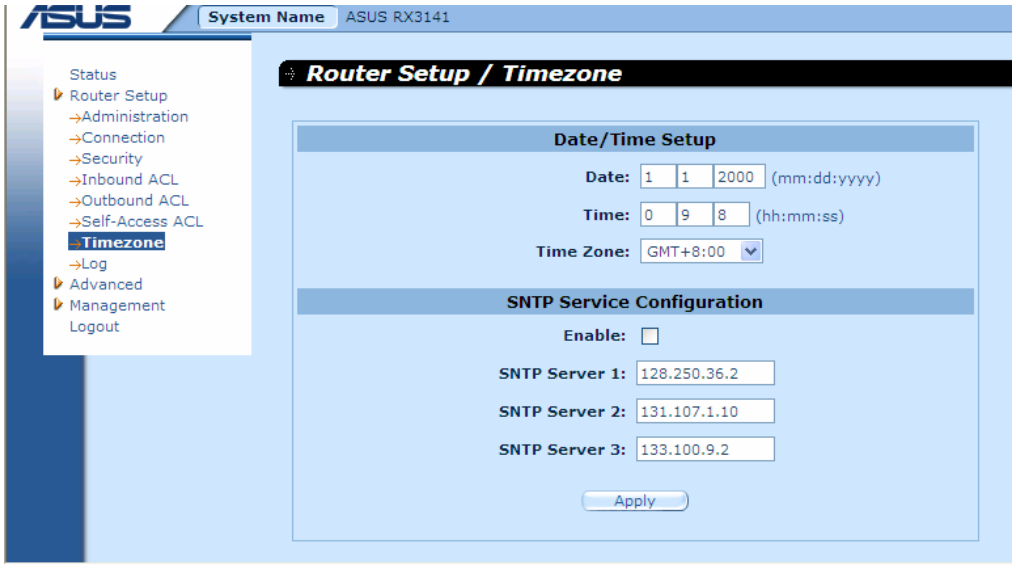


図 11.3 日時設定画面

ルータの時間を正確に維持する

1. **Router Setup** ➔ **Timezone** の順にクリックして、図 11.3 の日時設定画面を開きます。
2. ドロップダウンリストからタイムゾーンを選択します。
3. 「**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ます。
4. システム時間を更新する時に使う SNTP サーバ用に、IP アドレスを入力します。
5. Apply ボタンをクリックして設定を保存します。

時間を手動で入力することもできますが、システムを再起動したり電源をオフにしたりすると、デフォルトの時間(1/1/2000 00:00:00)に戻ります。

11.3.1 システム日時を確認する

Router Setup ➔ **Timezone** の順にクリックして Configuration Manager にログインしてシステム日時を確認することができます。SNTP サービスが有効に設定されていない場合や、SNTP サーバがシステム再起動後や電源をオフにした場合にアクセスできるように設定されていない場合は、システム時間はデフォルトの 1/1/2000 00:00:00 に戻ります。

11.4 工場出荷時のデフォルト設定にリセット

11.4.1 GUI で工場出荷時のデフォルト設定にリセットする

間違った設定をしてしまった場合など、工場出荷時のデフォルト設定に戻すことによって、トラブルを解消することができます。その場合は、以下の手順に従ってシステムをリセットします。

1. **Management** ➔ **Factory Reset** の順にクリックして、工場出荷時リセット画面へログインします。図 11.4 は、工場出荷時リセット画面です。

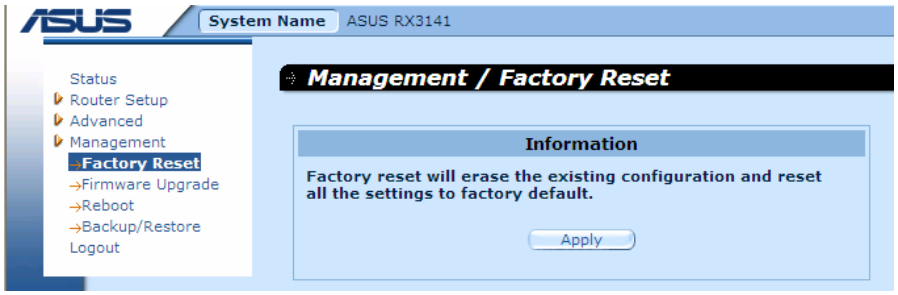


図 11.4. 工場出荷時リセット画面

2. Apply ボタンをクリックしてシステム設定を工場出荷時デフォルトに戻します。
3. 確認のため 図 11.5 のダイアログウィンドウがポップアップします。OK ボタンをクリックして続行するか、Cancel ボタンをクリックしてキャンセルします。

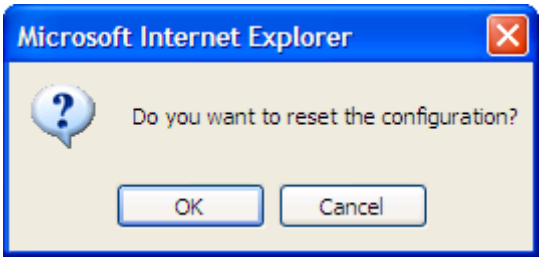


図 11.5. 工場出荷時リセット確認ダイアログウィンドウ

4. RX3141 再起動後に工場出荷時のデフォルト設定に戻ります。再起動中に図 11.6 のカウントダウンタイマーが表示されます。

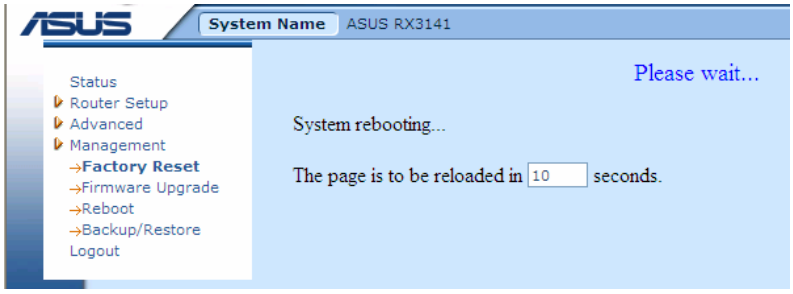


図 11.6. 工場出荷時リセットカウントダウンタイマー

11.4.2 リセットボタンで工場出荷時デフォルトにリセットする

注

パスワードを忘れたり、RX3141 の IP アドレスを忘れたりして、RX3141 へアクセスすることができなくなった場合は、リアパネルのリセットボタンを 5 秒以上押してシステム設定をデフォルトに戻します。

11.5 ファームウェアの更新

ASUSTeK は RX3141 用のファームウェアをアップグレードする場合があります。システムソフトウェアは*イメージ*と呼ばれるファイルに入っています。Configuration Manager で簡単にファームウェアのイメージをアップロードすることができます。以下の手順に従ってイメージをアップグレードが可能です。

1. **Management** ➔ **Firmware Upgrade** の順にクリックして図 11.7 のファームウェア更新画面を開きます。

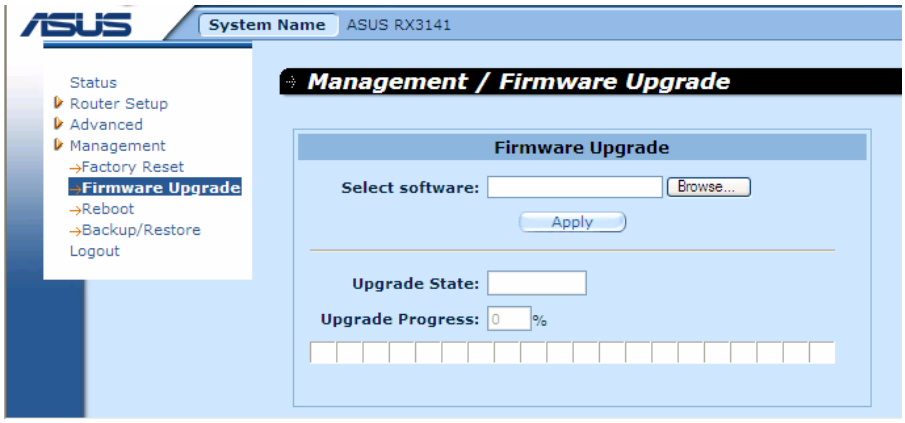


図 11.7. ファームウェア更新画面

2. 「Select software」のテキストボックスにファームウェアイメージのパスと名前を入力するか、Browse... ボタンをクリックしてファイルの選択画面を開きファームウェアファイルを選択します。

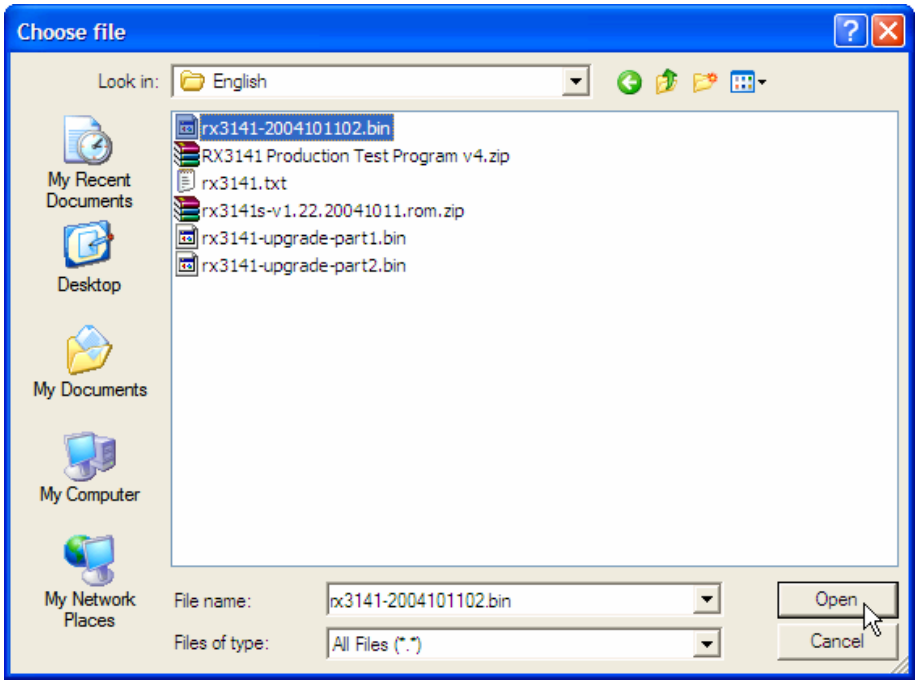


図 11.8. ファイルの選択画面

3. Open ボタンをクリックしてファームウェアを更新します。確認のため下のようなダイアログウィンドウがポップアップします。OK ボタンをクリックして続行するか、Cancel ボタンをクリックしてキャンセルします。

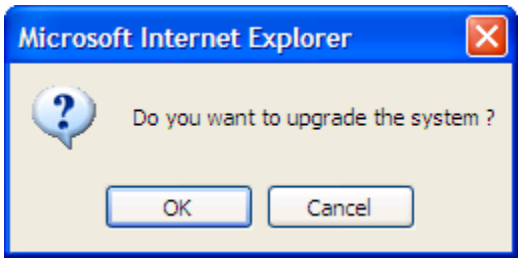


図 11.9. ファームウェア更新確認

4. 下図のようにファームウェアの更新状態が表示されます。

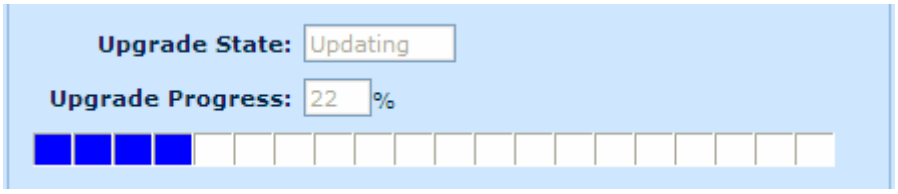


図 11.10. ファームウェア更新状態

5. ファームウェアの更新が終了すると、図 11.11 のカウントダウンタイマーが表示されます。タイマーが 0 になると RX3141 に再接続されます。自動的に接続されない場合は、手動で接続してください。

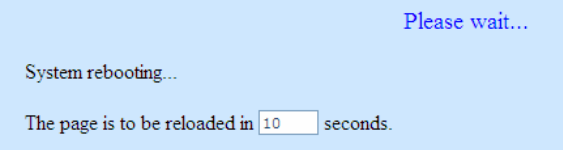


図 11.11. ファームウェア更新カウントダウンタイマー

6. RX3141 に再接続されたら、**Status** をクリックして、新しいファームウェアが正しく更新されていることを確認します。新しいシステム情報画面を確認するのに Web ブラウザのキャッシュをクリアする必要がある場合があります。以下は、Microsoft Internet Explorer 用のブラウザキャッシュのクリア手順です。

   a) 「ツール」をクリックします。

   b) 「インターネットオプション」をクリックします。

   c) 「ファイルの削除」ボタンをクリックするとブラウザキャッシュはクリアされます。

11.6 システムの再起動

1. **Management** ➔ **Reboot** の順にクリックして、図 11.12 のシステム再起動画面を開きます。
2. Apply ボタンをクリックします。

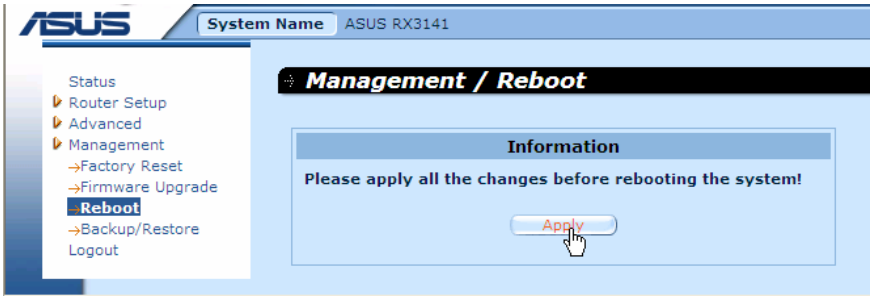


図 11.12. システム再起動画面

3. 図 11.13 のダイアログがポップアップします。OK ボタンをクリックして続行するか、Cancel ボタンでキャンセルします。

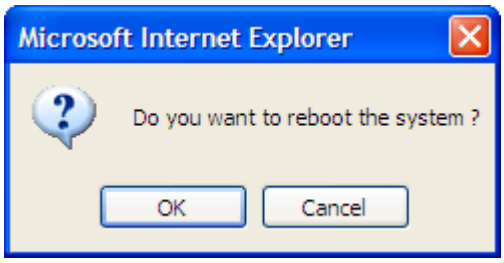


図 11.13. システム再起動確認

下図のタイマーが 0 に」なると RX3141 に再接続されます。

4. 図 11.14 は、再接続までの時間（秒）です。

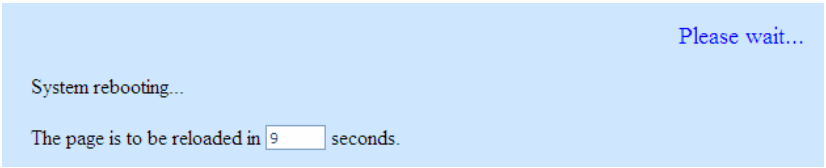


図 11.14. 再起動カウントダウンタイマー

11.7 . システム設定管理

11.7.1 システム設定のバックアップ

以下の手順に従ってシステム設定のバックアップを行います。

1. **Management ➔ Backup/Restore** の順にクリックして図 11.15 のバックアップ画面を開きます。

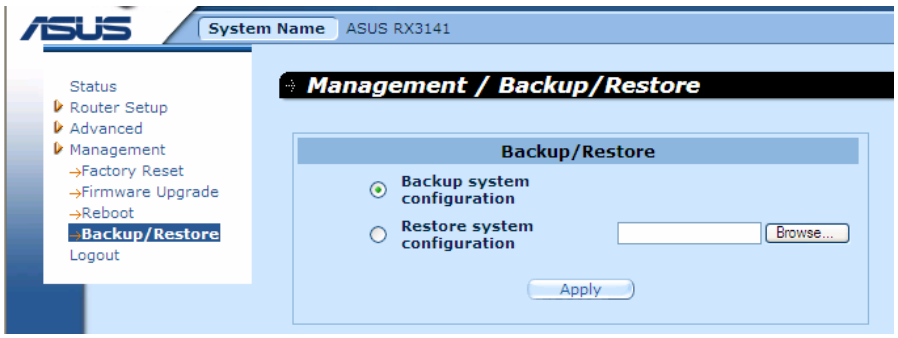


図 11.15. バックアップ画面

2. 「**Backup system configuration**」のラジオボタンをクリックします。
3. 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。
4. Microsoft Windows をお使いの場合は、「**ファイルダウンロード**」ダイアログウィンドウがポップアップします。図 11.16 のように、Save ボタンをクリックします。

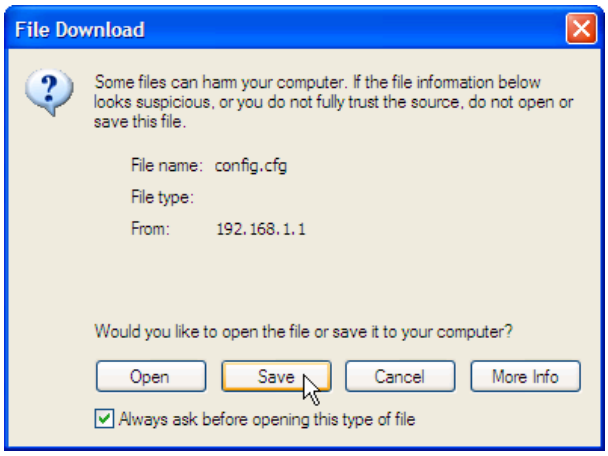


図 11.16. バックアップ画面– ファイルダウンロードダイアログ

5. 図 11.17 のように、バックアップファイルに任意のファイル名を入力し、Save ボタンをクリックして続行します。

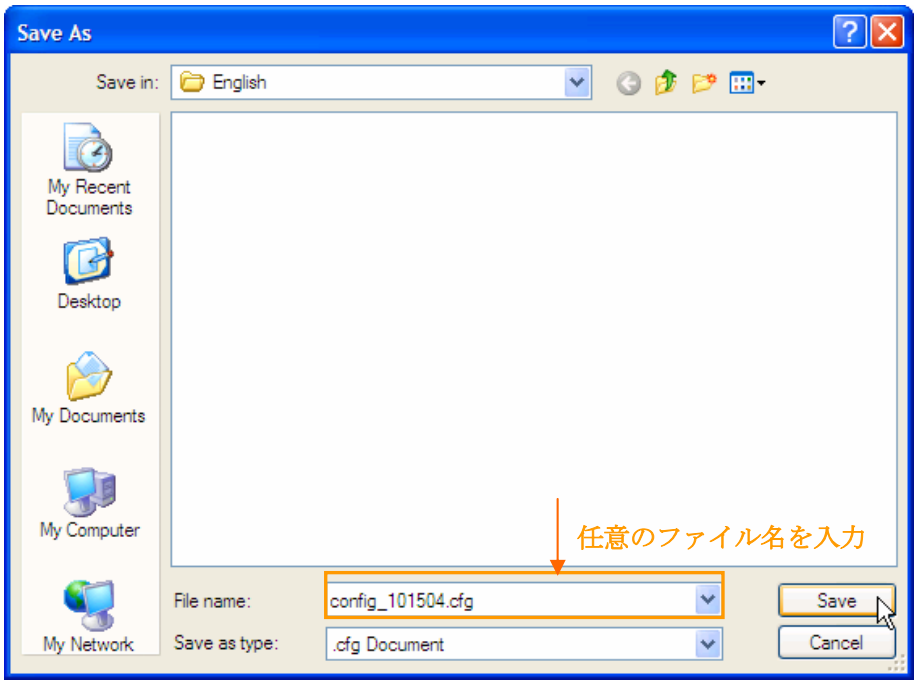


図 11.17 バックアップ画面 – 名前を付けて保存

6. 最後に 図 11.18 のような、システム設定が保存されたことを確認するメッセージが表示されます。

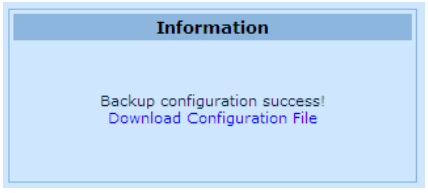


図 11.18. システム設定バックアップ完了メッセージ

11.7.2 システム設定のリストア

以下の手順に従ってシステム設定のリストアを行います。

1. **Management ➔ Backup/Restore** の順にクリックして、リストア画面を開きます。
2. リストアするシステム設定のファイルのパスと名前をテキストフィールドに入力します。

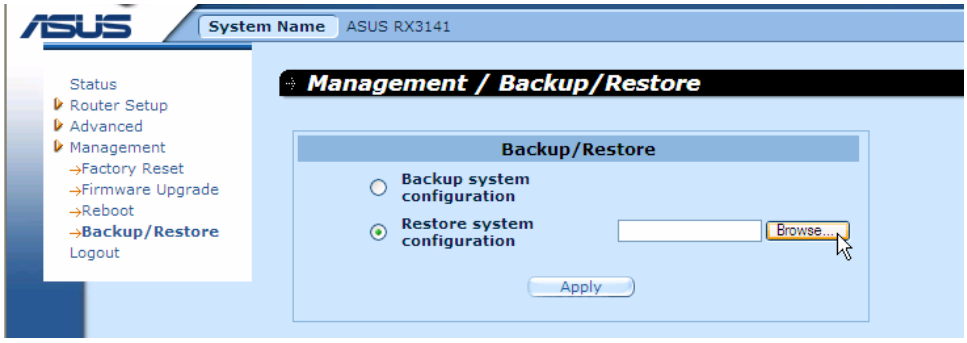


図 11.19 リストア画面

又は、Browse... ボタンをクリックして、システム設定ファイルを選択します。図 11.20 のような「ファイルの選択」ウィンドウがポップアップします。リストアするファイルを選択し Open ボタンをクリックして続行します。

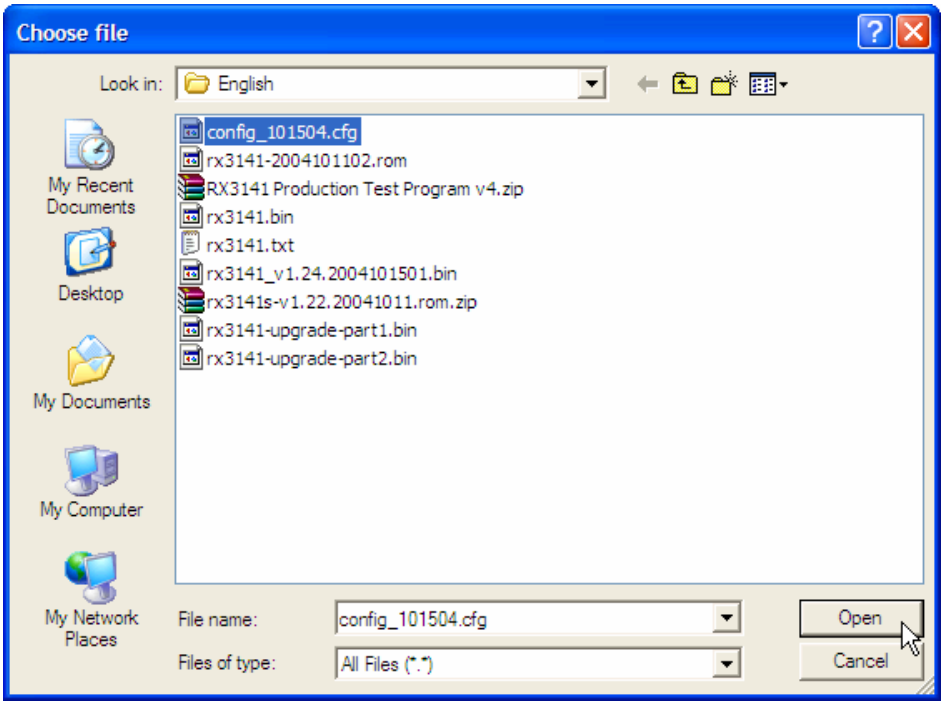


図 11.20. リストア画面 – ファイルの選択

3. OK ボタンをクリックしてシステム設定をリストアします。

4. 図 11.21 のシステム設定がリストアされたことを確認するメッセージがポップアップします。リストアしたシステム設定は RX3141 の再起動後に有効になります。

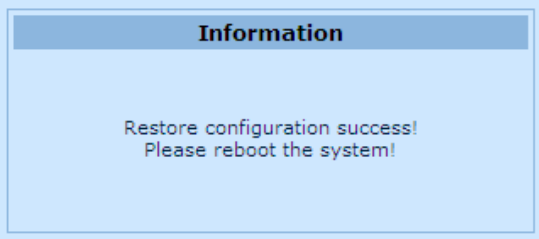


図 11.21. システム設定リストア完了メッセージ

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

このセクションは、IP アドレス for IPv4 (version 4 of the Internet Protocol)用の IP アドレスに関連する説明です。IPv6 アドレスに関しては記載していません。

また、このセクションでは 2 進数、bit、Byte に関する基本的な知識を理解している前提で進めます 2 進数、bit、Byte に関する詳細は、Appendix 12 をご覧ください。

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(コンピュータやデバイス)を特定するためのものです。IP アドレスは、0 から 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 と呼びます。

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、電話番号と同じように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 アドレスの始めの部分はネットワーク ID で、残りがホスト ID になります。ネットワーク ID の長さは、ネットワーククラスによって異なります。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

一般的によく使われるネットワーククラスは、A、B、C です（クラス D は特殊用途で用いるため省略）。それぞれのネットワークの用途や性質は異なります。

クラス A：インターネット上で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 の巨大なネットワークは、合計で 2,000,000,000 以上のホストを持つことができます。サイズが巨大なため、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利用します。

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 のホストを割り当てることができ、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はできませんが、ネットワークの数は最高で、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

- ネットワーククラスはフィールド 1 から簡単にわかります
  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 で抜けている数値は特殊な用途のための値です。）
- ホスト ID：全てのフィールドで、0 または 255 以外の値であれば、どの数値でも利用することができます。0 または 255 は特殊な用途のための値です。

12.3 サブネットマスク

定義
マスク

普通の IP アドレスのように見えますが、2 進数のパターンがあり、IP アドレスのどの部分が、ネットワーク ID とホスト ID であるのかを示します。ネットワーク ID は 2 進数で 1 になり、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のにサブネットマスクを用います。

255.255.255.128

これを 2 進数に書き換えると何が起こったのかがよくわかります。

11111111. 11111111. 11111111.10000000

クラス C アドレスなので、フィールド 1 からフィールド 3 はネットワーク ID ですが、フィールド 4 の先頭の数字が 1 になっています。これは、サブネットが 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 から 255 の代わりに)0 から 127 の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 の始めの 2 ビットが4つのサブネット(00、01、10、11)を示します。フィールド 4 の残りの 6 ビットにホスト ID として 0 から 63 の値が割り当てられます。

注

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以下の通りです。

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サブネットは存在しないため、デフォルト(初期値)と呼ばれます。

13 トラブルシューティング

本製品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、さまざまな IP ユーティリティの利用方法をご紹介します。

ここでの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
電源を入れても電源 LED が点灯しない	本製品に付属の AC アダプタが、本製品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接続後も LINK WAN LED が点灯しない	本製品に付属のタイプと同じイーサネットケーブルが、ADSL のイーサネットポートまたはケーブルモデムと本製品の WAN ポートにしっかり接続されていることと、ADSL またはケーブルモデムの電源が入っていることを確認してください。また、本製品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接続後も LINK LAN LED が点灯しない	イーサネットケーブルが LAN ハブまたはパソコンと本製品にしっかりと接続されていること、パソコンまたはハブの電源が入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満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)の場合は Cat 5 ケーブルをお使いください。10Mbit/秒ケーブルとは下位互換性があります。
インターネットアクセス	
パソコンがインターネットにアクセスできない	Ping ユーティリティを使ってお使いのパソコンが本製品の LAN IP アドレス(デフォルト:192.168.1.1)と通信可能かどうかを確認します。Ping が帰ってこない場合は、もう一同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は、(登録済みのパブリックアドレスとは異なります)以下のことを確認してください。 • コンピュータのゲートウェイ 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(詳細はクイックスタートガイド Part 2 の IP 情報をご覧ください)。異なる場合は、パソコンが自動的に IP 情報を受け取れるように設定してください。 • DNS サーバが有効であるかどうかを ISP に問い合わせて確認してください。また、自動的に情報を受信できるように、アドレス、パソコンを設定をしてください。 • RX3141 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 アドレスに変換す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範囲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

問題	トラブルシューティング
	（詳細 セクション1参照）。デフォルト設定は、前もって定義された動的に割り当てられたアドレス用の NAT ルールです。
インターネットの Web ページがパソコンに表示されない	上の項目を読んで、DNS サーバが ISP に対応しているかどうかを確認してください。ISP の DNS サーバとの接続性を Ping ユーティリティを使ってテストしてください。
Configuration Manager プログラム	
Configuration Manager のユーザ ID またはパスワードを忘れた.	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 ID もパスワードも「admin」です。変更して忘れてしまった場合は、デバイスをリセットしてデフォルト設定に戻してください（詳細 セクション 11.4 参照）。**警告:** デバイスをリセットするとカスタム設定は全て消去され、工場出荷状態になります。
ブラウザから Configuration Manager プログラムにアクセスできない	Ping ユーティリティを使って、パソコンが本製品の LAN IP アドレス（デフォルト：192.168.1.1）と通信していることを確認します。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 アドレスが本製品の 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 Manager 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って問題を検出する

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ほかのコンピュータを認識しているかどうかを確認するとき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、の順にクリックしてテキストボックスに下のように入力します。

ping 192.168.1.1

OK をクリックします。IP アドレスの部分には、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ようにはパブリック IP アドレスを入力します。

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。

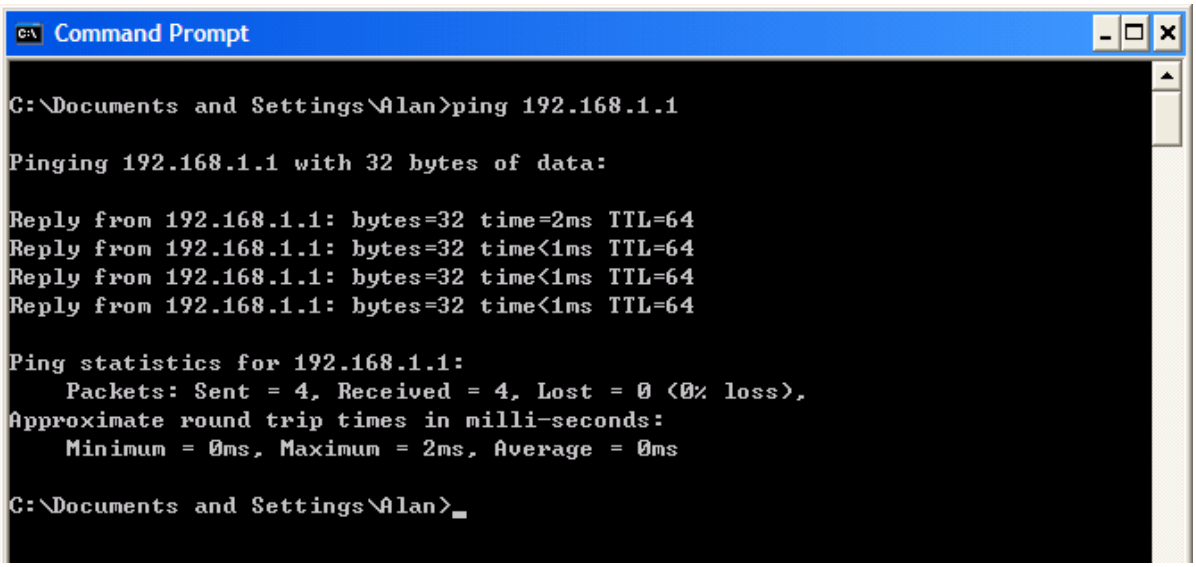


図 13.1. Ping ユーティリティを使う

ターゲットコンピュータが見つからない場合は、「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、本製品へのパスが使用可能かどうかを確認することができます。(デフォルト LAN IP アドレス「192.168.1.1」、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 アドレスがわからない場合は、nslookup コマンドを利用します。

ほとんどの IP が有効な OS で、コマンドプロンプト、またはシステム管理ユーティリティで同じコマンドが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と対応する IP アドレスを特定することがでいます。 名前を特定すると、nslookup コマンドが DNS サーバ(たいていの場合 ISP 内)を検索します。ISP の DNS に名前が検出されないと、上位サーバまで要求され、入力された名前が検出されるまで検索を続けます。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 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下のように入力します。

nslookup

OK をクリックします。コマンドプロンプトの「>」の後ろに、インターネットアドレスを入力します。
(例:www.absnews.com)

検出されれば、図 13.2 のように対応する IP アドレスが表示されます。

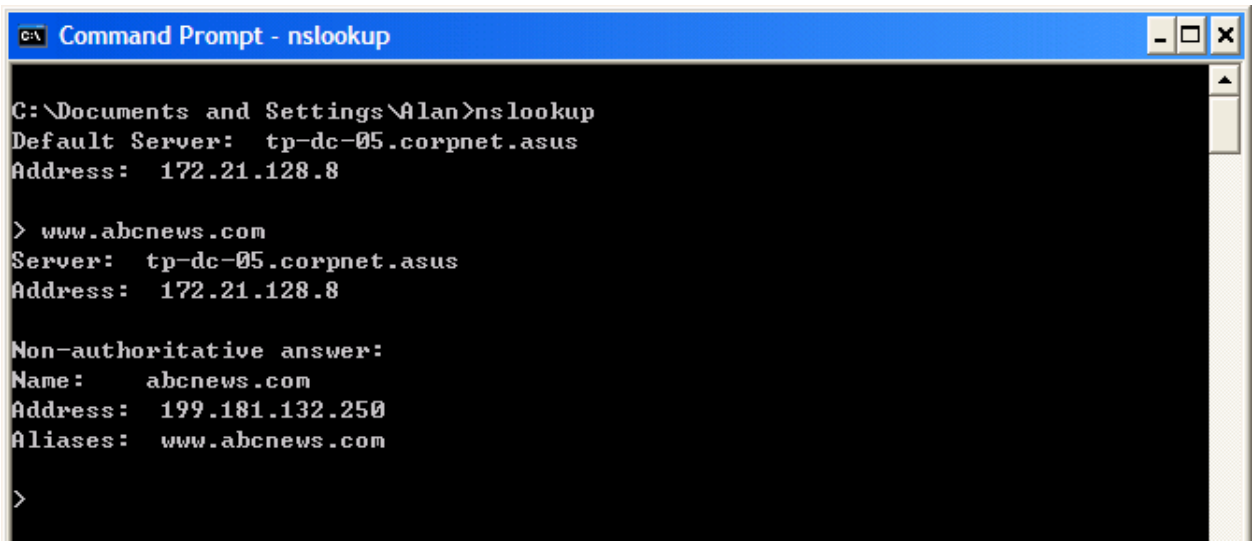


図 13.2. nslookup ユーティリティを使う

1 つのインターネット名にいくつかのアドレスが対応していることがありますが、これは、トラフィックの多い Web サイトにはよくあることで、重複サーバを利用し、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 Index

＜アルファベット表記＞