D-Link DSR-500/1000/1000N

Unified Services VPN Router

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠警告	この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠警告

分解・改造をしない
分解禁止
機器が故障したり、異物が混入すると、やけどや火災の原因となります。

落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
禁止
故障の原因につながります。

発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
禁止
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼してください。

ぬれた手でさわらない
ぬれ手禁止
感電のおそれがあります。

水をかけたり、ぬらしたりしない
水ぬれ禁止
内部に水が入ると、火災、感電、または故障のおそれがあります。

油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない
禁止
火災、感電、または故障のおそれがあります。

内部に金属物や燃えやすいものを入れない
禁止
火災、感電、または故障のおそれがあります。

表示以外の電圧で使用しない
禁止
火災、感電、または故障のおそれがあります。

たこ足配線禁止
禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

設置、移動のときは電源プラグを抜く
禁止
火災、感電、または故障のおそれがあります。

雷鳴が聞こえたら、ケーブル / コード類にはさわらない
禁止
感電のおそれがあります。

ケーブル / コード類や端子を破損させない
禁止
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障につながります。

正しい電源ケーブル、コンセントを使用する
禁止
火災、感電、または故障の原因となります。

乳幼児の手の届く場所では使わない
禁止
やけど、ケガ、または感電の原因になります。

次のような場所では保管、使用をしない
禁止
・直射日光のあたる場所
・高温になる場所
・動作環境範囲外

光源をのぞかない
禁止
光ファイバケーブルの断面、コネクタ、および製品のコネクタをのぞきますと強力な光源により目を損傷するおそれがあります。

⚠注意

静電気注意
❗
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

コードを持って抜かない
❗
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

振動が発生する場所では使用しない
❗
接触不良や動作不良の原因となります。

付属品の使用は取扱説明書にしたがう
禁止
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。
本書の記載に従って正しい取り扱いをしてください。

無線に関するご注意

電波に関するご注意

DSR-1000N は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。
本製品は、日本国内でのみ使用できます。
以下の注意をよくお読みになりご使用ください。

◎ この機器を以下の場所では使用しないでください。
- 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
- 工場の製造ライン等で使用されている移動体識別用の構内無線局(免許を必要とする無線局)および特定小電力無線局(免許を必要としない無線局)
- 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。

◎ 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

5GHz 帯使用の無線機器に関するご注意

◎ 電波法により、5GHz 帯 (IEEE 802.11a) は屋外での使用が禁止されています。
◎ 従来の中心周波数（J52）を使用した機器とは通信チャンネルが異なるために通信できません。
◎ 802.11a（W53）使用時は気象レーダー等との電波干渉を避けるためにチャンネルを 自動的に変更する場合があります（DFS 機能）

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

DSR-1000N の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局) 並びにアマチュア無線局 (免許を必要とする無線局) が運用されています。

◎ この機器を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。
◎ 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。
◎ その他、この機器から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 /OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

◎ 通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。
- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

◎ 不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。
- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあけたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。
- 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
  - 電源ケーブル、延長ケーブル、またはプラグが破損した。
  - 製品の中に異物が入った。
  - 製品に水がかかった。
  - 製品が落下した、または損傷を受けた。
  - 操作方法に従って運用しているのに正しく動作しない。
- 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔を塞がないようにしてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。
- 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。
- 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプがわからない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。
- システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
  - 東日本では 100V/50Hz、西日本では 100V/60Hz
- また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。
- 付属の電源ケーブルのみを使用してください。
- 感電を防止するために、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3 ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグが付いている 3 線式コードを使用してください。
- 延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動からシステムコンポーネントを保護するには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたりつまずいたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いてください。
- 製品の移動は気をつけて行ってください。キャスタやスタビライザがしっかり装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

静電気障害を防止するために

静電気は、システム内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネントを静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃してください。

2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。

3. 静電気に敏感なコンポーネントの取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および同梱されている製品保証書をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

- 本書および同梱されている製品保証書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
また、テクニカルサポートご提供のためにはユーザ登録が必要となります。
http://www.dlink-jp.com/

目次

はじめに

本ユーザマニュアルは、インストールおよび操作方法を例題と共に記述しています。
また、本製品を使用して新しい D-Link のサービスルータの接続設定を行い、VPN トンネルをセットアップし、さらにファイアウォールルールの確立と一般的な管理業務を実行する方法について説明します。一般的な配置と使用するシナリオを各セクションで説明しています。
各構成パラメータに関する、より詳細な設定の手順や説明については、ルータの GUI 内にある各ページにアクセスできるオンラインヘルプを参照してください。

第 1 章 本製品のご利用にあたって

- 本製品の概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。

第 2 章 本製品の設置

- 本製品の基本的な設置方法と接続方法について説明します。

第 3 章 Web ベース設定ユーティリティ

- Web ベースの管理機能への接続方法および設定方法について説明します。

第 4 章 ネットワークの設定

- 本製品の LAN、WAN、DMZ、UPnP、キャプティブポータルの設定方法について説明します。

第 5 章 インターネット接続（WAN 設定）

- 本製品のインターネットへの接続について説明します。

第 6 章 無線アクセスポイント設定（DSR-1000N のみ）

- 本製品の無線アクセスポイント設定のためのウィザード、無線プロファイル、無線帯域設定、WPS などについて説明します。

第 7 章 安全なプライベートネットワーク設定

- 本製品が使用するルールを作成および適用することによってネットワークを安全にする方法について説明します。

第 8 章 IPSec / PPTP / L2TP VPN 設定

- ゲートウェイルータ間またはリモート PC クライアント間の安全な通信のための VPN 機能について説明します。

第 9 章 SSL VPN 設定

- このルータを通じてリモートユーザに提供する SSL サービスのオプションの設定方法について説明します。

第 10 章 高度な設定ツール

- 本製品のサポートする USB デバイス、各種認証、証明書の設定について説明します。

第 11 章 システム管理

- アクセスコントロール、SNMP、NTP、ログ、コンフィグレーションのバックアップと復元、ファームウェアのアップグレード、診断ツールなど管理用の機能について説明します。

第 12 章 ルータステータスおよび統計情報

- 本製品のシステム構成の詳細、トラフィック統計情報、アクティブなセッション情報について説明します。

第 13 章 トラブルシューティング

- 本製品のインストールと操作で発生する問題への解決策を提供します。

付録 A 用語解説

- 本説明書の中で使用する用語について説明します。

付録 B 工場出荷時設定

- 本製品の工場出荷時設定を記載しています。

付録 C ポートフォワーディングとファイアウォール設定に利用可能な標準サービス

- ポートフォワーディングとファイアウォール設定に利用可能な標準サービスについて記載します。

付録 D ログメッセージ

- 本製品のログメッセージを記載します。

本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "（13 ページ）をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
courier 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
courier 斜体	コマンド項目（可変または固定）。	*value*
< >	可変項目。< > にあたる箇所に値または文字を入力します。	<*value*>
[ ]	任意の固定項目。	[*value*]
[< >]	任意の可変項目。	[<*value*>]
{ }	{ } 内の選択肢から 1 つ選択して入力する項目。	{*choice1* | *choice2*}
|（垂直線）	相互排他的な項目。	*choice1* | *choice2*
Menu Name > Menu Option	メニュー構造を示します。	Device > Port > Port Properties は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。

第 1 章　本製品のご利用にあたって

ここでは、DSR シリーズの概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。

製品概要

D-Link サービスルータは、小中規模のビジネスに増加しているニーズを扱うために安全で高性能のネットワークソリューションを提供します。DSR-1000N の統合された高速の IEEE 802.11n 無線技術は、従来の有線ネットワークに匹敵する性能をより少ない制限で提供します。VPN（Virtual Private Network）トンネルや、IPSec（IP Security）、PPTP（Point-to-Point Tunneling Protocol）、L2TP（Layer 2 Tunneling Protocol）、および SSL（Secure Sockets Layer）などの機能を通じて最適なネットワークセキュリティを提供します。SSL VPN トンネルを使用していつでもどこでもクライアントレスリモートアクセスにより Road Warrior（モバイル接続）を行うことができます。

D-Link サービスルータは、以下に示す様々な利点を提供します。:

包括的な管理機能
DSR シリーズには 2 つの WAN ギガビットイーサネットがあり、ビジネス作業に対して最大の生産性を保証するポリシーベースサービス管理を提供します。フェイルオーバ機能は、有線接続が失われた場合に切断せずにデータトラフィックを保持します。外向きロードバランシング機能は、2 つの WAN インタフェースを経由して外向きトラフィックを調整して、高い稼働率をもたらすようにシステムの性能を最適化します。2 番目の WAN ソリューションでは、ご使用の LAN からサーバを隔離するために、ポートを Dedicated（専用）DMZ ポートとして設定できます。

優れた無線性能
DSR-1000N は、優れた無線性能を提供するように設計されており、2.4GHz または 5GHz* 周波数帯域のいずれかで操作可能な 802.11 a/b/g/n を搭載しています。MIMO（Multiple In Multiple Out）技術を使用すると、無線のカバーエリア内の「デッドスポット」を最小限度にするだけでなく高いデータ速度も提供できます。

*W52 のみ

堅牢な VPN 機能
十分な機能を備えた VPN（Virtual Private Network）は、ご使用のネットワークとの安全なリンクをモバイルで作業する人や支店に提供します。本製品は同時に 20 個（DSR-1000/1000N）、10 個（DSR-500）の SSL（Secure Socket Layer）VPN トンネルを管理できます。また、中央にある会社のデータベースにリモートアクセスを提供することでモバイルユーザが接続できます。サイト間 VPN トンネルは、IPSec（IP Security）プロトコル、PPTP（Point-to-Point Tunneling Protocol）、L2TP（Layer 2 Tunneling Protocol）を使用して暗号化された仮想リンクを通じた支店への接続を容易にします。DSR-500、DSR-1000/1000N は、それぞれ同時に 35 個および 70 個の IPSec VPN トンネルをサポートします。

効率的な D-Link グリーンテクノロジー
グローバルコミュニティの関連メンバとして、D-Link は環境に優しい製品の供給に徹しています。D-Link グリーン Wi-Fi と D-Link グリーンイーサネットは電力を節約して、無駄を防止します。D-Link グリーン WLAN スケジューラはオフピークの時間、無線電力を自動的に減少させます。同様に D-Link グリーンイーサネットプログラムは検出されたケーブル長とリンクステータスに基づいて電力利用を調整します。さらに、RoHS（Restriction of Hazardous Substances）と WEEE（Waste Electrical and Electronic Equipment）指令の遵守は D-Link のグリーン認定デバイスに環境面において責任ある選択を行います。

ポートについて

DSR シリーズは以下のポートおよびボタンを搭載しています。

ポート	DSR-500	DSR-1000	DSR-1000N
10BASE-T/100BASE-TX/1000BASE-T ポート	WAN x 2、LAN x 4（10/100/1000 Mbps）		
コンソールポート	1		
USB ポート	1	2	2
WPS ボタン	-	-	1

前面パネル

本製品の前面パネルには、ステータスを表示する Power/Status LED、USB ポート / LED、および LAN/WAN ポート / LED が配置されています。DSR-1000N では、さらに、WLAN 用の 5GHz/2.4GHz LED、および WPS ボタンも配置されています。

DSR-500

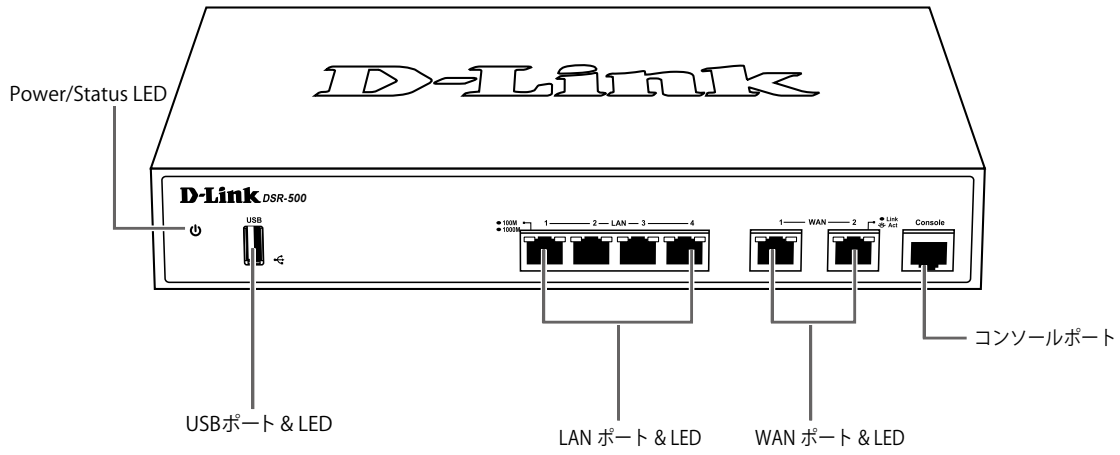


図 1-1　前面パネル図（DSR-500）

DSR-1000

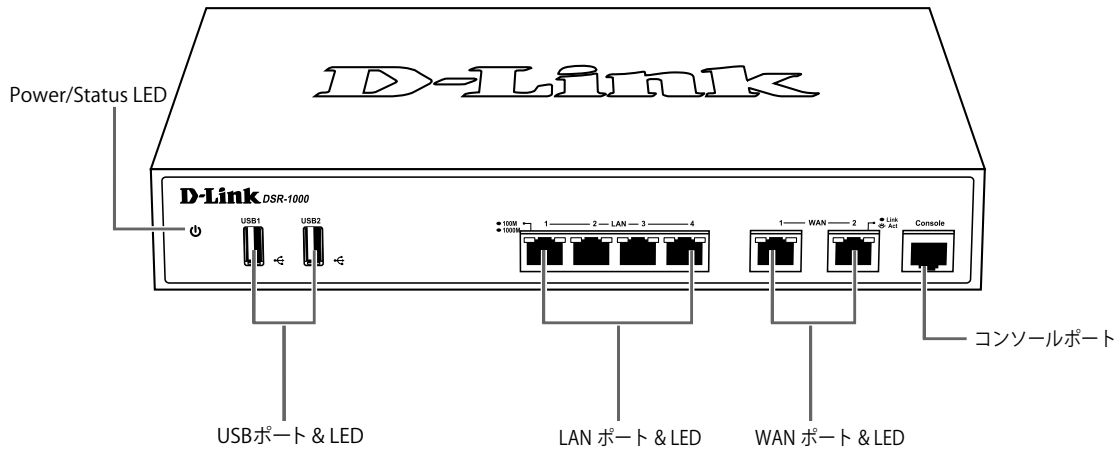


図 1-2　前面パネル図（DSR-1000）

DSR-1000N

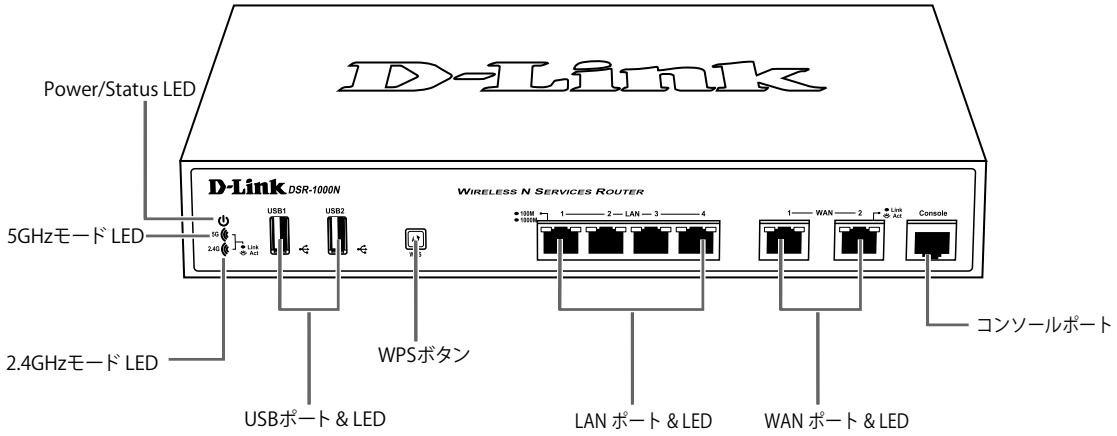


図 1-3　前面パネル図

前面パネルの各機能は以下の通りです。

機能	説明
Power / Status LED 5GHz / 2.4GHz WLAN LED*	本ルータの状態を示します。製品の電源をオンにした場合、電源が起動中、Power / Status LED は橙色に点灯します。起動には 1 分ほどかかり、起動が完了すると機能 LED は緑色の点灯に変わります。電源をオフにして再度オンにする場合には、オフの後に数秒待ってからオンにすることをお勧めします。
USB ポート / LED	以下の様々な USB 1.1 または 2.0 のデバイスをサポートすることができます。USB デバイスを接続し、認識されると緑色に点灯します。: • ネットワーク共有のためのフラッシュディスク、またはハードディスク。 • WCN 設定（未サポート） • プリンタ（未サポート）
WPS ボタン *	WPS システムを使用して他の無線機器と接続します。
LAN ポート	スイッチおよびハブなどのイーサネットデバイスと UTP ケーブルで接続します。
WAN ポート	ケーブルモデムまたは DSL モデムに UTP ケーブルを使用して接続します。WAN2 ポートは、 2 つの WAN 接続または内部サーバファーム用に WAN2 または DMZ をサポートする設定可能ポートです。
コンソールポート	RJ45-to-DB9 コンソールケーブルを通じて CLI（コマンドラインインタフェース）にアクセスするのに使用します。

* DSR-1000N のみ

LED 表示

DSR シリーズは、Power/Status、USB ポート、無線モード（DSR-1000N）、WAN / LAN ポート、および WPS（DSR-1000N）について LED をサポートしています。WAN / LAN ポートの LED は以下の通り、リンクスピードと TX/RX ステータスがあります。

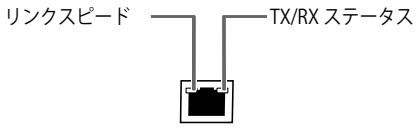


図 1-4　WAN/LAN LED 図

ステータス LED は以下の状態を表示します。

LED	状態	色	状態説明
Power / Status	点灯	橙	製品の電源を立ち上げ中です。
	点滅	橙	製品がクラッシュしているか、またはリカバリモード中です。
	点灯	緑	製品に電源が供給され正常に動作しています。
	点滅	緑	システムにファームウェアアップグレードの失敗などの欠陥があります。
	消灯	ー	製品に電源が供給されていません。
5GHz*	点灯	緑	5GHz 無線 LAN による通信が可能な状態です。
	点滅	緑	5GHz 無線 LAN によりデータを送受信しています。
2.4GHz*	点灯	緑	2.4GHz 無線 LAN による通信が可能な状態です。
	点滅	緑	2.4GHz 無線 LAN によりデータを送受信しています。
WAN / LAN リンクスピード	点灯	橙	1000Mbps でリンクが確立しています。
	点灯	緑	100Mbps でリンクが確立しています。
	消灯	ー	ポートは 10Mbps で動作中です。
WAN / LAN TX/RX ステータス	点灯	緑	リンクが確立しています。
	点滅		データを送受信しています。
	消灯	ー	リンクが確立していません。
USB	点灯	緑	USB デバイスが接続しています。
	消灯		USB デバイスが接続していません。
WPS*	点灯	青	処理を開始しています。
	点滅		接続に成功しました。
	消灯	ー	リンクが確立していません。

* DSR-1000N のみ

背面パネル

DSR シリーズの背面パネルには、リセットボタン、電源スイッチ、および電源コネクタが配置されています。また、DSR-1000N には、さらにアンテナ端子があります。

DSR-500/1000

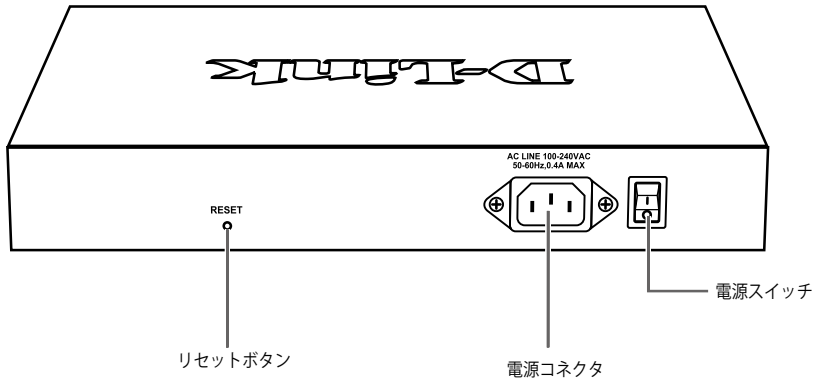


図 1-5　背面パネル図

DSR-1000N

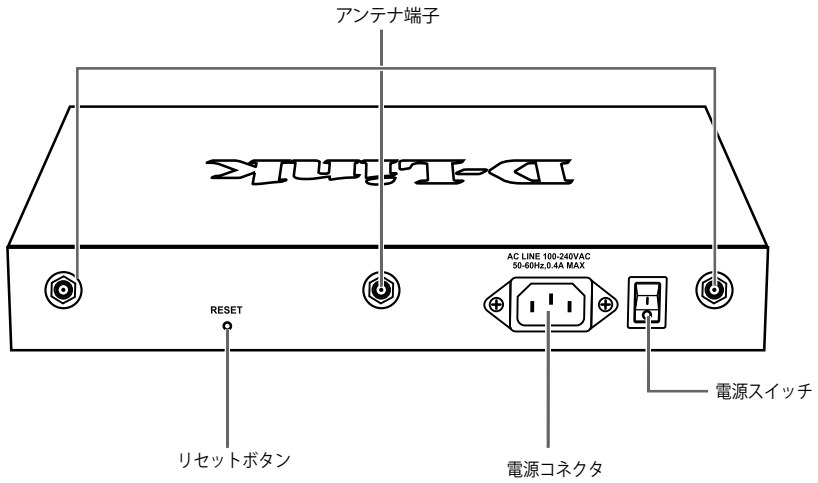


図 1-6　背面パネル図

背面パネル機能

部位	機能
リセットボタン	本製品を工場出荷時設定にリセットします。
電源コネクタ	付属の AC ケーブルを接続します。
電源スイッチ	本製品の電源スイッチです。
アンテナ端子 *	本製品に付属のアンテナを接続します。

* DSR-1000N のみ

第 2 章　製品の設置

パッケージの内容

ご購入いただいた製品の梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。
- 本体　x　1
- アンテナ　x　3（DSR-1000N のみ）
- AC 電源ケーブル　x　1
- ラックマウントキット 1 式（ ブラケット 2 枚、ネジ）
- UTP ケーブル　x　1
- コンソールケーブル（RJ45-to-DB9 ケーブル）　x　1
- ゴム足（貼り付けタイプ）　x　4
- クイックインストールガイド
- CD-ROM　x　1
- シリアルラベル

万一、不足しているものや損傷を受けているものがありましたら、弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

システム要件

本製品が動作するためには、以下のシステム条件が必要です。
- Internet Explorer 7.0 以上
- イーサネットへの接続

ネットワーク接続前の準備

製品の設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

- 製品は、しっかりとした水平面で耐荷重性のある場所に設置してください。
- 製品の上に重いものを置かないでください。
- 本製品から 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本製品の周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後 16cm 以上の空間を保つようにしてください。
- 製品は動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- 製品は強い電磁場が発生するような場所（モータの周囲など）や、振動、ほこり、および直射日光を避けて設置してください。
- 製品を水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

設置にあたってのご注意（DSR-1000N のみ）

本製品の使用により、動作範囲内にて無線でネットワークアクセスが可能になりますが、壁や天井など無線信号が通過する物体の数や厚さ、場所などにより、動作範囲が制約を受ける場合があります。一般的には、構造物の材質や設置場所での無線周波数のノイズが動作範囲に影響を与えます。

1. 本製品と他のネットワークデバイスとの間に入る壁や天井の数をできるだけ少なくしてください。一枚の壁や天井の影響により、本製品の動作範囲は 1 ～ 30 メートルの範囲となります。間に入る障害物の数を減らすようデバイスの位置を工夫してください。

2. ネットワークデバイス間の直線距離にご注意ください。厚さ 50 センチの壁を 45 度の角度で無線信号が通過する時、通り抜ける壁の厚みは約 1 メートルになります。2 度の角度で通過すると、通り抜ける厚みは 14 メートルになります。信号が障害物をなるべく直角に通過するような位置にデバイスを設置し、電波を受信しやすくしてください。

3. 無線信号の通過性能は建築材料により異なります。金属製のドアやアルミの金具などは動作範囲を小さくする可能性があります。無線 LAN デバイスや無線 LAN アダプタ使用のコンピュータの設置は、信号がなるべく乾式壁か開放された戸口などを通るような位置に設置してください。

4. 周波数ノイズを発生する電気機器や家電製品からは、最低でも 1、2 メートル離してデバイスを設置してください。

5. 2.4GHz のコードレス電話または X-10（シーリングファン、ライト、およびホームセキュリティシステムなどの無線製品）を使っている場合、ご使用の無線接続は著しく性能が低下するか、または完全に切断される可能性があります。2.4GHz 電話の親機は可能な限りご使用の無線機器から離れていることを確認してください。電話を使用していない場合でも、親機は信号を送信します。

6. 必ず付属の AC 電源ケーブルをご使用ください。

製品の設置

アンテナの取り付け（DSR-1000N のみ）

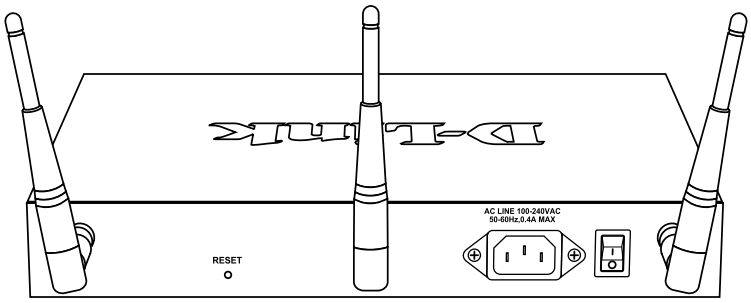


図 2-1　アンテナの取り付け

1. 付属の 3 本のアンテナを本体のアンテナ端子に取り付けます。取り付けの際には、アンテナは折り曲げずに本体のアンテナ接合部に接続し、右方向に締めます。
2. 取り付け後に折り曲げます。
3. 電波状況に合わせてアンテナの向きを変更します。

19 インチラックへの取り付け

以下の手順に従って本製品を標準の 19 インチラックに設置します。

ブラケットの取り付け

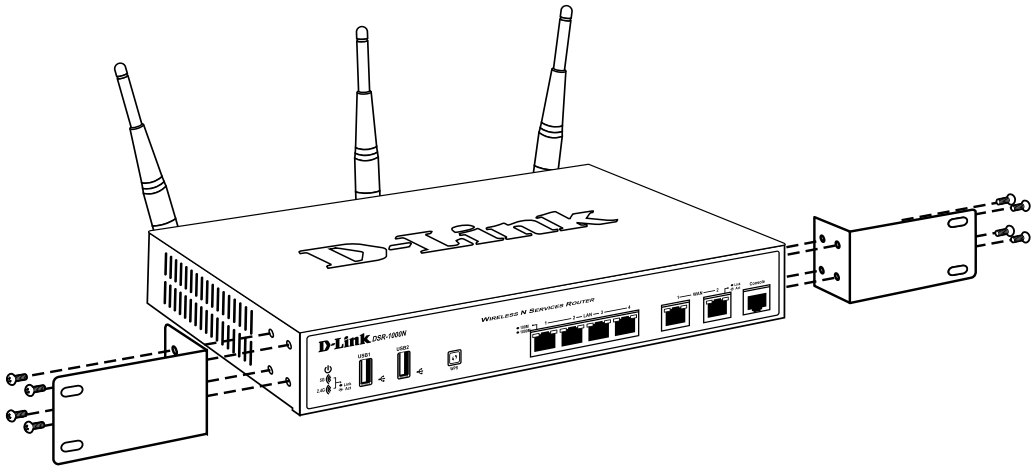


図 2-2　ブラケットの取り付け

ラックマウントキットに付属のネジを使用して、本製品にブラケットを取り付けます。完全にブラケットが固定されていることを確認し、本製品を以下の通り標準の 19 インチラックに固定します。

19 インチラックに本製品を取り付ける

警告 前面、側面にスタビライザを取り付けないで製品を設置すると、ラックが転倒し、場合によっては人身事故を引き起こすことがあります。そのため、ラック内に製品を取り付ける前に必ずスタビライザを取り付けてください。ラックにシステム / コンポーネントを取り付けた後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つだけとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。

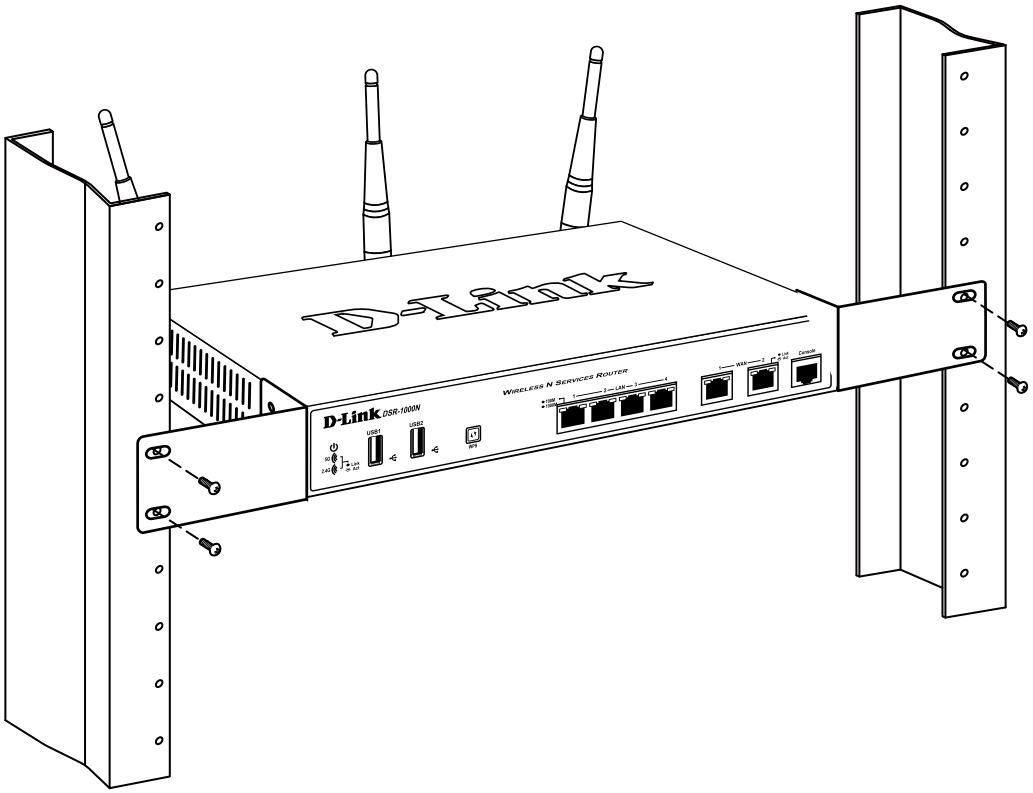


図 2-3　製品のラックへの設置

電源の投入

1. 電源ケーブルを本製品の電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。
2. 本製品に電源が供給されると、Power LED が緑色に点灯します。

第 3 章　Web ベース設定ユーティリティ

設定メニューの操作

本製品の設定は UTP ケーブルで接続した PC から行います。ここでは、Windows 7 で動作する画面で説明します。手順と画面は、他の Windows OS についても同じです。

LAN に接続した管理用の PC をルータに対して持っているとします。LAN 接続はルータで利用可能な有線イーサネットポートを経由するか、または、初期セットアップが一度終了した場合には、本製品は LAN でブリッジされるため、無線インタフェースを経由して管理可能です。マイクロソフト社の Internet Explorer または Mozilla Firefox などの Web ブラウザを使用してルータの Web マネージャにアクセスしてください。

ルータの LAN IP アドレスを変更した場合、ブラウザのアドレスバーにその IP アドレスを入力して、ルータの管理ユーザインタフェースにアクセスします。

1. プロキシサーバ機能を無効にします。Windows の「スタート」-「コントロールパネル」-「インターネットオプション」-「接続」タブ -「LAN の設定」の順にクリックし、「LAN にプロキシサーバを使用する」のチェックを外します。

2. Web ブラウザ（Internet Explorer）を起動します。

3. 本製品の IP アドレスと HTTP ポートの番号をアドレスに入力し（http://192.168.10.1）、「Enter」キーを押下します。設定用 PC と本製品の IP アドレスが同じサブネット内であることに注意してください。

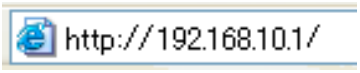


図 3-1　　アドレス入力画面

注意　本製品の IP アドレスが初期値から変更されている場合は、変更後のアドレスを入力します。

4. 接続に成功すると、以下のログイン画面が表示されます。

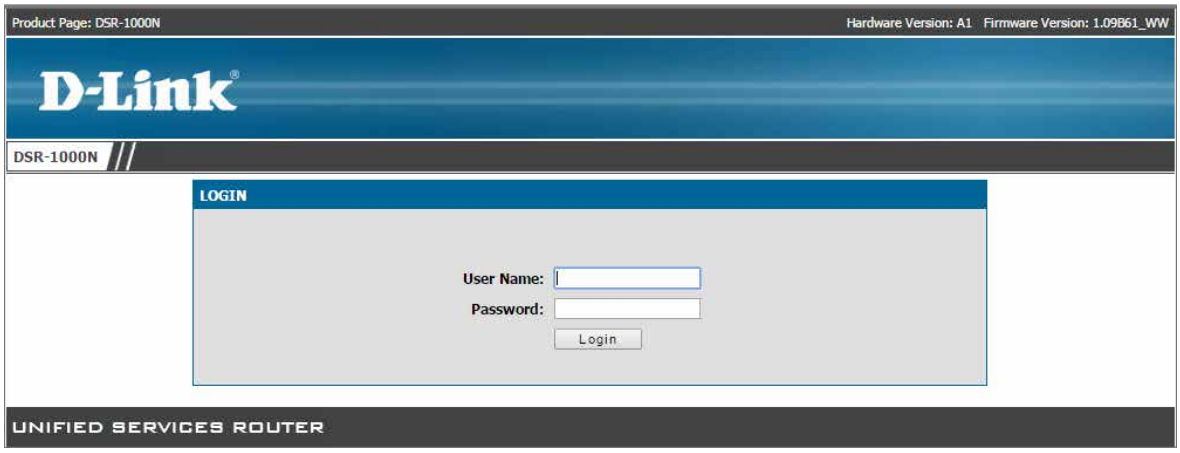


図 3-2　　LOGIN 画面

5. 「User Name」および「Password」に「admin」と入力して、「Login」ボタンをクリックします。

6. ログインに成功すると以下の画面が表示されます。

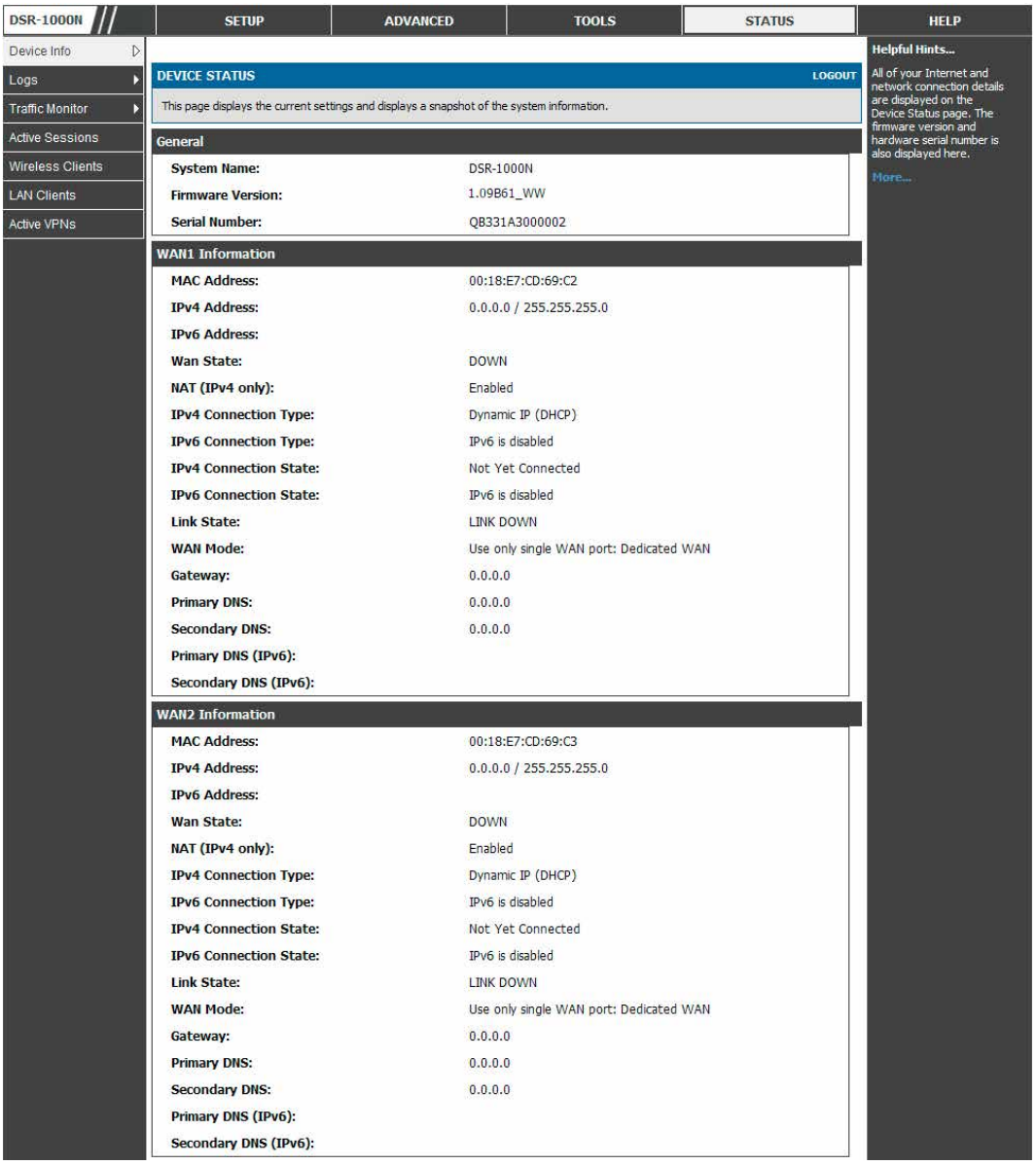


図 3-3　DEVICE STATUS 画面

7. 設定画面で変更を行った場合は、「Save Settings」ボタンを押して変更した設定を保存します。

第 4 章　ネットワークの設定

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

設定項目	説明	参照ページ
LAN 設定	IPv4/IPv6 ネットワーク用の LAN 設定、IPv6 通知、DHCP 予約 IP アドレスの設定などを行います。	22 ページ
VLAN 設定	ポート VLAN、マルチ VLAN サブネット設定などを行います。	32 ページ
DMZ 設定	DMZ ポートの設定、DMZ DHCP 予約 IP アドレスの設定などを行います。	36 ページ
UPnP 設定	UPnP を使用したデバイスの設定を行います。	40 ページ
キャプティブポータル	Web のポータル認証を経由したインターネット接続のための設定を行います。	41 ページ

LAN 設定

IPv4 ネットワーク用の LAN 設定

SETUP > Network Settings > LAN Setup Configuration メニュー

ここでは、その上で動作する DHCP サーバを含むルータの IPv4 LAN インタフェースを設定できます。

初期値では、ルータは WLAN または LAN ネットワーク上のホストに対して DHCP（Dynamic Host Configuration Protocol）サーバとして機能します。また、DHCP を使用して、DNS サーバ、WINS（Windows Internet Naming Service）サーバ、およびデフォルトゲートウェイに対するアドレスと共に PC とその他の LAN デバイスにも IP アドレスを割り当てることができます。DHCP サーバが有効な場合、ルータの IP アドレスは LAN と WLAN クライアントのためのゲートウェイアドレスとして機能します。LAN 内の PC には、この手順で指定されるアドレスプールから IP アドレスが割り当てられます。各プールアドレスは LAN 上でアドレスの重複を避けるために割り当て前にテストされます。

多くのアプリケーションでは、本製品の DHCP および TCP/IP 設定の初期値で動作します。ご使用のネットワーク上の PC を DHCP サーバにしたい場合、または手動で全 PC のネットワーク設定を行う場合には、DHCP モードを「None」に設定します。DHCP リレーは、DHCP のリース情報をネットワークの DHCP サーバである別の LAN デバイスから転送するのに使用されます。これは特に無線クライアントに役立ちます。

DNS サーバを使用する代わりに、WINS（Windows Internet Naming Service）サーバを使用できます。WINS サーバは、DNS サーバと同等ですが、ホスト名の解決のために NetBIOS プロトコルを使用します。DHCP クライアントからの DHCP 要求を承諾する場合、ルータの DHCP 設定には WINS サーバの IP アドレスがあります。

また、LAN のために DNS プロキシを有効にすることができます。これが有効な場合、ルータは、すべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信します。無効にすると、すべての DHCP クライアントが ISP の DNS IP アドレスを受信します。

以下の手順に従って、LAN 接続を行います。:

1. **SETUP > Network Settings > LAN Setup Configuration** の順にメニューをクリックし、以下の画面を表示します。

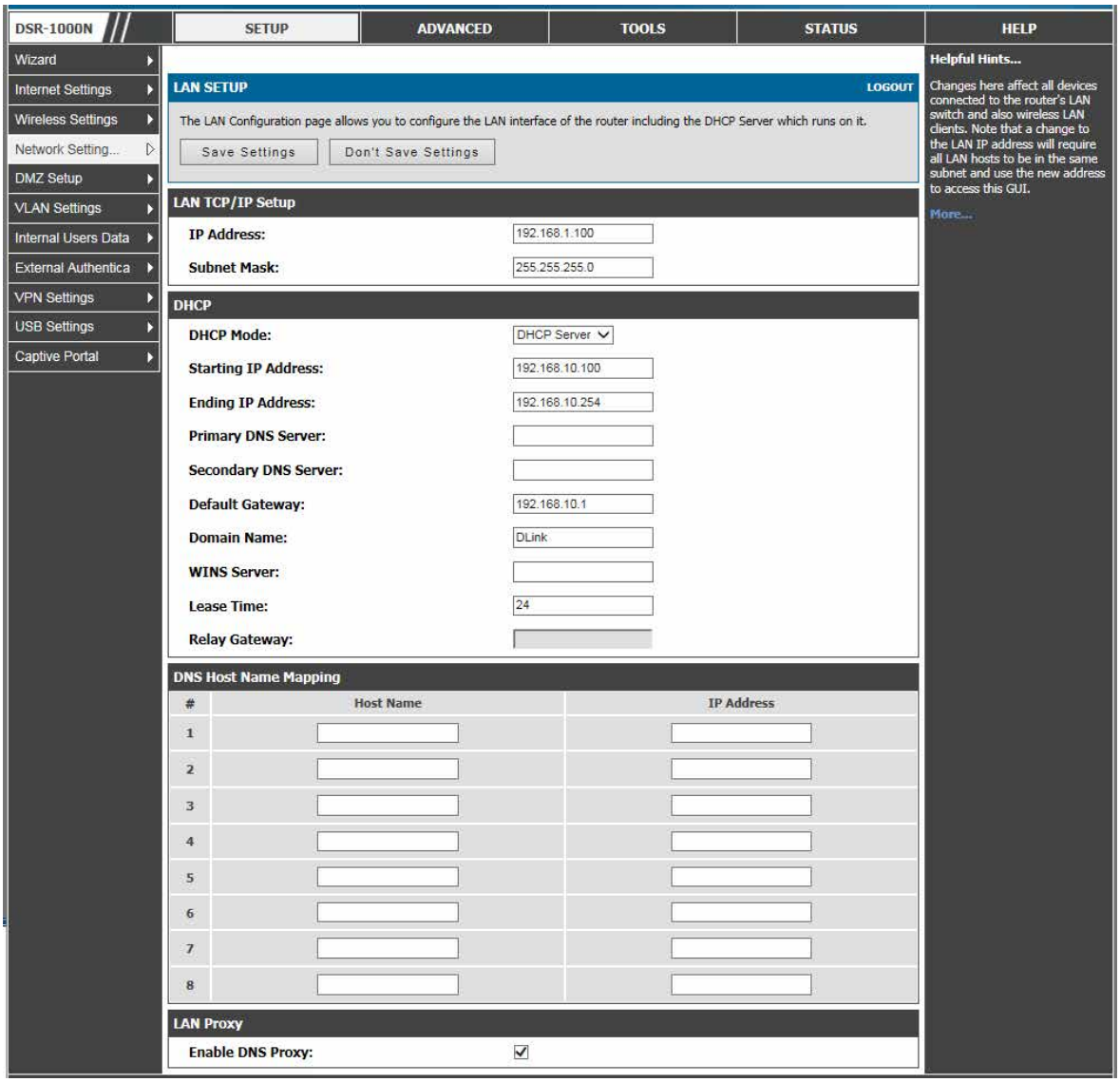


図 4-1　LAN SETUP 画面

2. 「LAN SETUP」ページで、ルータに以下の情報を入力します。:

項目	説明
IP Address	IP アドレス（工場出荷時設定 : 192.168.10.1）
Subnet Mask	サブネットマスク（工場出荷時設定 : 255.255.255.0）

注意 LAN IP アドレスの変更後に「Save Settings」ボタンをクリックするとブラウザが応答しなくなります。新しい IP アドレスを使用して再度接続をオープンしてログインしてください。変更した IP アドレスでルータにアクセスする前に LAN ホスト（ルータを管理するために使用されるマシン）が新たに割り当てられたプールから IP アドレスを取得していること、または、ルータの LAN サブネットのスタティック IP アドレスを持っていることに注意してください。

3. 「DHCP」セクションでは、「DHCP Mode」（DHCP モード）を選択します。:

項目	説明
None	ルータの DHCP サーバ機能を LAN に対して無効にします。
DHCP Server	本オプションを使用して、ルータは、DHCP でアドレスをリクエストしている LAN デバイスに対し、指定した範囲内の IP アドレスおよび追加で指定した情報を割り当てます。
DHCP Relay	このオプションを有効にすると、LAN 上の DHCP クライアントは異なるサブネットにある DHCP サーバから IP アドレスリースと対応する情報を受け取ることができます。リレーゲートウェイを指定します。これにより LAN クライアントが DHCP 要求を行うとリレーゲートウェイ IP アドレスを通してアクセス可能なサーバに送られます。

DHCP が有効な場合、以下の DHCP サーバパラメータを入力します。:

項目	説明
Starting / Ending IP Address	IP アドレスプールにおける連続したアドレスの最初と最後を入力します。LAN に参加するどの新しい DHCP クライアントにもこの範囲内の IP アドレスが割り当てらます。開始アドレスの初期値は「192.168.10.100」です。終了アドレスの初期値は「192.168.10.254」です。これらのアドレスは、ルータの LAN IP アドレスと同じ IP アドレスサブネット（ネットワーク）にあるべきです。LAN においてデバイスにスタティックな IP アドレスを割り当てるためにサブネット範囲の一部の保存しておく必要があります。
Primary / Secondary DNS Server	定義済み DNS（ドメインネームシステム）サーバを LAN で利用できる場合、ここに IP アドレスを入力します。
Default Gateway	初期値では、本設定はルータの LAN IP アドレスとなります。ネットワークのゲートウェイがこのルータでなければ、これを LAN サブネット内のどんな有効な IP にもカスタマイズすることができます。この場合、DHCP サーバは、デフォルトゲートウェイとして設定した IP アドレスを DHCP クライアントに付与します。
Domain Name	識別に使用するネットワークのドメイン名を入力します。
WINS Server（オプション）	WINS サーバの IP アドレスを入力します。またはご使用のネットワークに存在する場合には Windows NetBIOS サーバの IP アドレスを入力します。
Lease Time	IP アドレスがクライアントにリースされる期間（時）を入力します。
Relay Gateway	ゲートウェイアドレスを入力します。これは、「DHCP Mode」を「DHCP Relay」にした場合に本セクションの入力のみ必要です。

4. 「DNS Host Name Mapping 」セクションでは、以下の項目を設定します。:

項目	説明
Host Name	有効なホスト名を入力します。
IP Address	ホスト名に対する IP アドレスを入力します。

5. 「LAN Proxy 」セクションでは、以下の項目を設定します。:

項目	説明
Enable DNS Proxy	ルータがすべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信するためには、ボックスをチェックします。

6. 「Save Settings」ボタンをクリックし、すべての変更を適用します。

DHCP 予約 IP アドレスの設定

SETUP > Network Settings > LAN DHCP Reserved IPs メニュー

DHCP サーバ設定のために予約される IP アドレスを設定します。

本ルータの DHCP サーバは、DHCP サーバのデータベースに割り当てられるクライアントのネットワークインタフェースにおけるハードウェアアドレスと IP アドレスを追加することで明示的に LAN 上のコンピュータに TCP/IP 設定を割り当てることができます。DHCP サーバがクライアントからリクエストを受信するたびに、クライアントのハードウェアアドレスと、データベース内に存在するハードウェアアドレスリストを比較します。IP アドレスがデータベース内のコンピュータまたはデバイスに割り当てられていると、カスタマイズされた IP アドレスが設定され、そうでない場合は、IP アドレスは DHCP プールから自動的にクライアントに割り当てられます。

1. **SETUP > Network Settings > LAN DHCP Reserved IPs** の順にメニューをクリックし、以下の画面を表示します。

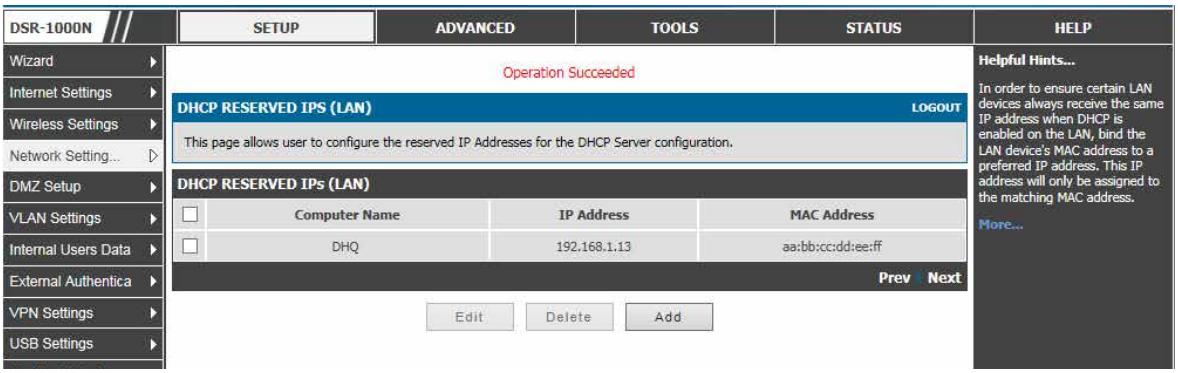


図 4-2　DHCP RESERVED IPs（LAN）画面

予約済み IP アドレスに行われるアクションは、以下の通りです。

項目	説明
先頭のチェックボックス	リスト内のすべての IP アドレスを選択します。
Edit	選択されたバインディングルールを編集するためには、クリックして「DHCP Reserved IPs for LAN」ページをオープンします。
Delete	選択した IP アドレス予約を削除します。
Add	新しいバインディングルールを追加するためには、クリックして「DHCP Reserved IPs for LAN」ページをオープンします。

スタティック IP の登録

1. 「Add」ボタンをクリックして以下の画面を表示します。

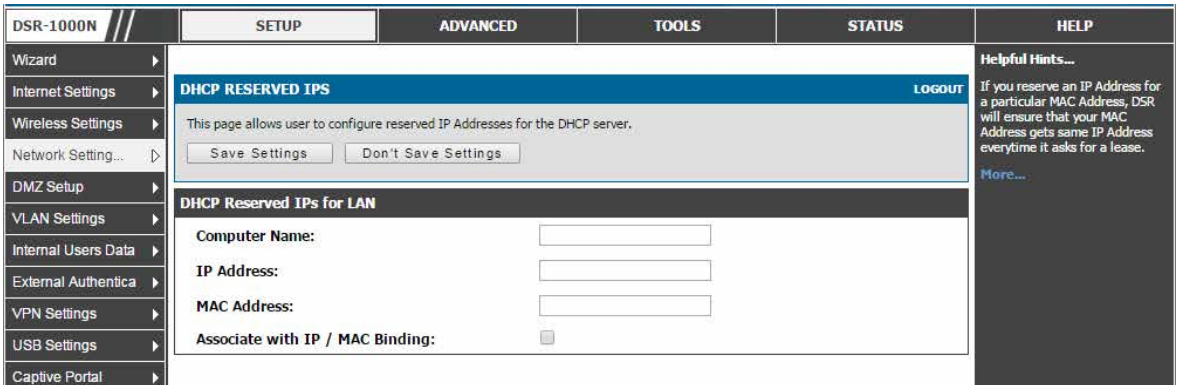


図 4-3　スタティック IP の追加

2. 以下の項目を入力します。

項目	説明
Computer Name	LAN ホストのユーザ定義名。
IP Address	DHCP サーバが予約するホストの LAN IP アドレス。
MAC Address	LAN 上にある場合には、予約 IP アドレスが割り当てられる MAC アドレス。
Associate with IP/MAC Binding	有効にすると、コンピュータ名、IP および MAC は IP/MAC バインディングを使用して関連付けられます。

3. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

注意 以下に示す製品ごとの DHCP 予約 IP アドレス数の制限にご注意ください。

- DSR-500 : 96
- DSR-1000/1000N :128

エントリの削除

1. 「DHCP RESERVED IPs（LAN）」画面で削除するエントリを選択後、「Delete」ボタンをクリックします。

LAN DHCP リースクライアント

SETUP > Network Settings > LAN DHCP Leased Clients メニュー

LAN DHCP サーバに接続するクライアントのリストを表示します。

1. **SETUP > Network Settings > LAN DHCP Leased Clients** の順にメニューをクリックし、以下の画面を表示します。

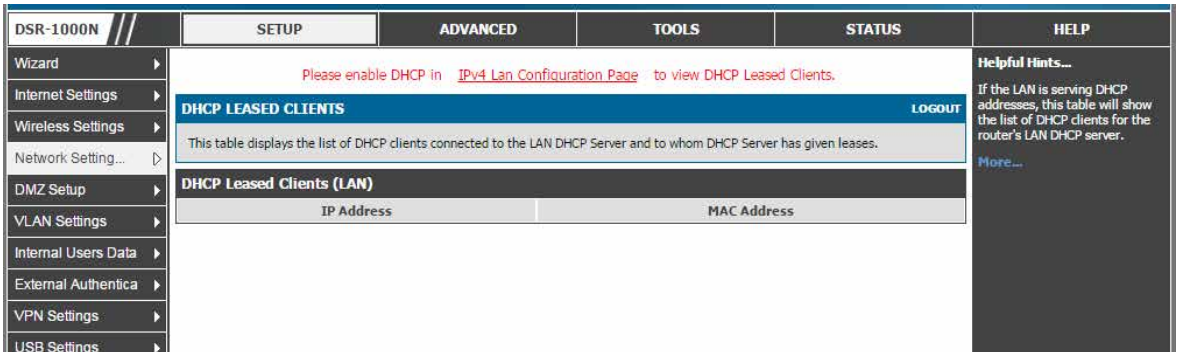


図 4-4　DHCP リースクライアント画面

2. 以下の項目を表示します。

項目	説明
IP Addresses	予約 IP リストに一致するホストの LAN IP アドレス。
MAC Addresses	設定済みの IP アドレス予約を持つ LAN ホストの MAC アドレス。

注意 本機能を使用するためには **SETUP > Network Settings > LAN Setup Configuration** で「DHCP Mode」を「DHCP Server」にする必要があります。

IPv6 ネットワーク用の LAN 設定

ADVANCED > IPv6 > IPv6 LAN > IPv6 LAN Config メニュー

ここでは IPv6 の関連する LAN 設定を行います。

IPv6 モードでは、（IPv4 モードと同様に）LAN DHCP サーバは初期値で無効です。有効にすると、DHCPv6 サーバは LAN に割り当てられている IPv6 Prefix Length（IPv6 プレフィックス長）と共に定義済みアドレスプールから IPv6 アドレスを供給します。

注意 IPv6 設定オプションを有効にするためには、**ADVANCED > IPv6 > IP Mode** で「IPv4 / IPv6 mode」を有効にする必要があります。

1. **ADVANCED > IPv6 > IP Mode** の順にメニューをクリックし、以下の画面を表示します。

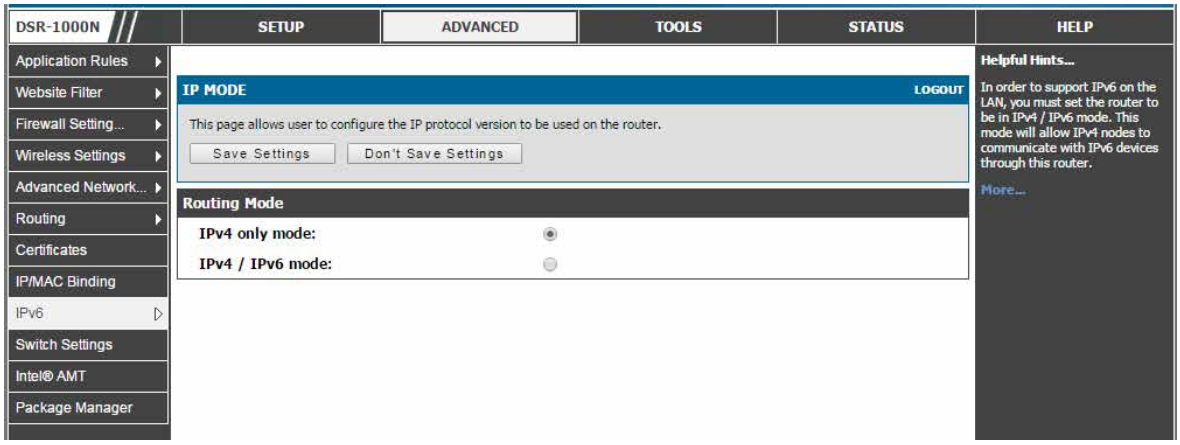


図 4-5　IPv6 LAN と DHCPv6 設定

「IPv4 / IPv6 mode」をチェックし、「Save Settings」ボタンをクリックします。本システムは再起動しますので、起動後再度ログインします。

2. **ADVANCED > IPv6 > IPv6 LAN > IPv6 LAN Config** の順にメニューをクリックし、以下の画面を表示します。

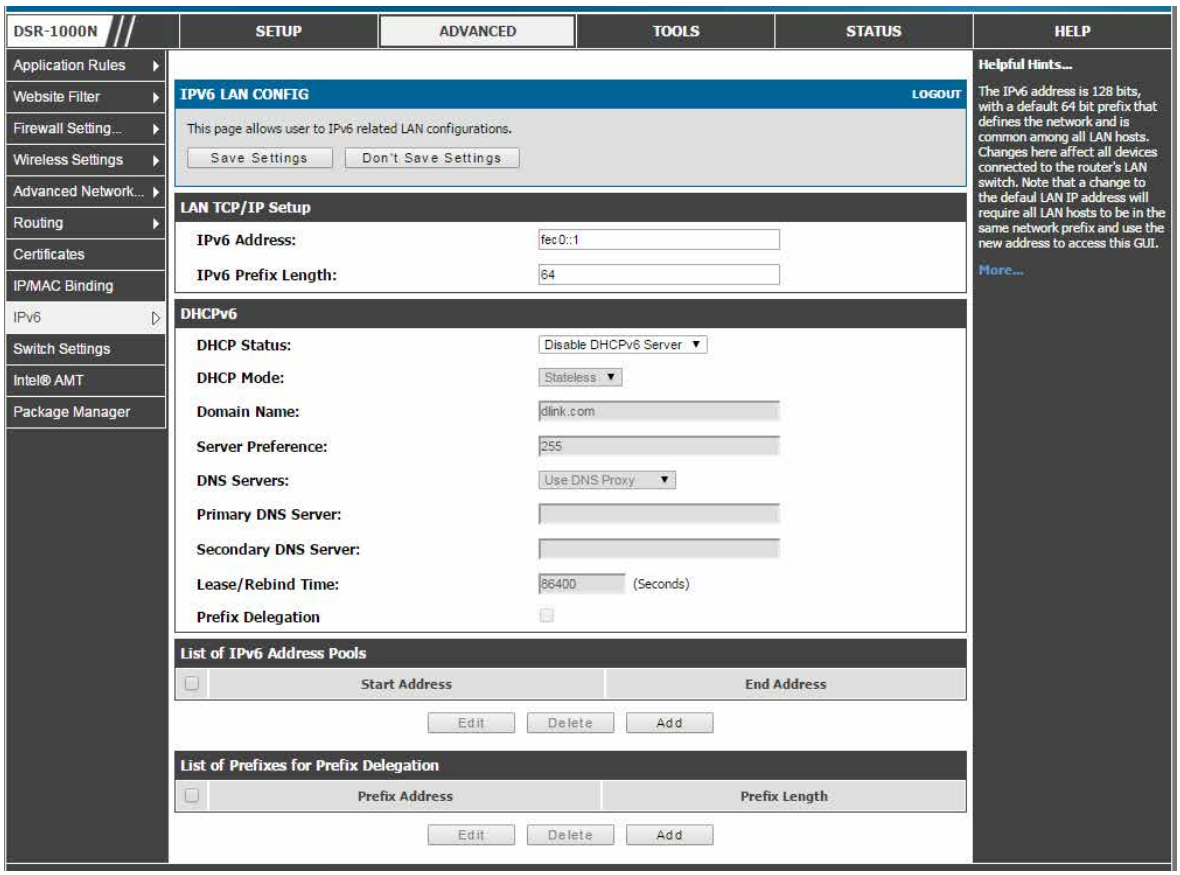


図 4-6　IPv6 LAN と DHCPv6 設定

LAN 設定

ルータの IPv6 LAN アドレスの初期値は「fec0::1」です。ご使用のネットワークの要件に基づいてこの 128 ビットの IPv6 アドレスを変更できます。ルータの LAN 設定を定義するために必要なフィールドにはプレフィックス長があります。IPv6 ネットワーク（サブネット）はプレフィックスと呼ばれるアドレスの開始ビットにより特定されます。初期値では、これは 64 ビットの長さです。ネットワーク内のすべてのホストには、それらの IPv6 アドレスに共通の開始ビットがあります。ネットワークアドレスに共通な開始ビット番号はプレフィックス長フィールドによって設定されます。

注意 LAN IP アドレスを変更した場合に「Save Settings」をクリックするとブラウザが応答しなくなります。新しい IP アドレスを使用して再度接続をオープンしてログインしてください。変更した IP アドレスでルータにアクセスする前に LAN ホスト（ルータを管理するために使用されるマシン）が新たに割り当てられたプールから IP アドレスを取得していること、または、ルータの LAN サブネットのスタティック IP アドレスを持っていることに注意してください。

IPv4 LAN ネットワークと同様に、ルータには DHCPv6 サーバ機能があります。有効な場合、ルータは、DHCP が供給するアドレスを希望する LAN デバイスに指定範囲内の IP アドレスと追加情報を割り当てます。

以下の設定は DHCPv6 サーバを設定するために使用されます。:

項目	説明
DHCP Status	DHCP 機能を「Enable DHCPv6 Server」（有効）/「Disable DHCPv6 Server」（無効）にします。有効にすると以下の項目が指定できます。
DHCP Mode	IPv6 DHCP サーバに「Stateless」または「Stateful」を指定します。 • Stateless - IPv6 LAN ホストが本ルータによって自動設定される場合に外部の IPv6 DHCP サーバを必要としません。この場合、ルータ通知デーモン（RADVD）をこのデバイスに設定する必要があります。また、ホストは自動設定のために ICMPv6 ルータディスカバリメッセージを使用します。LAN ノードに供給する管理アドレスはありません。 • Stateful - IPv6 LAN ホストは、必要な構成設定を提供するために外部の DHCPv6 サーバに依存します。
Domain Name	DHCPv6 サーバのドメイン名を設定します。（オプション）
Server Preference	サーバ優先度は、この DHCP サーバの優先度レベルを示すために使用されます。LAN ホストに対して最も高いサーバ優先度値を持つ DHCP サーバ通知メッセージは他の DHCP サーバの通知メッセージより優先されます。初期値は 255 です。
DNS Servers	• Use Below - DNS サーバの詳細を手動により以下に入力します。（Primary/Secondary DNS Server オプション） • Use DNS from ISP - LAN DHCP クライアントが ISP から DNS サーバの詳細を直接受信することを可能とします。 • Use DNS Proxy - ルータは、すべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信します。（WAN 設定パラメータ）
Primary / Secondary DNS Server	あらかじめ「DNS Servers」で「Use Below」を選択します。LAN 上に利用可能な定義済みドメインネームシステム（DNS）サーバがある場合、ここに IP アドレスを入力します。
Lease/Rebind Time	LAN クライアントに対する本ルータからの DHCPv6 リースの期間（秒）を設定します。
Prefix Delegation	DHCPv6 サーバでプレフィックスデリゲイションを有効にします。本オプションは DHCPv6 サーバのステートレスアドレス自動設定モードでのみ選択されます。

List of IPv6 Address Pools（IPv6 アドレスプール）

この機能により、ゲートウェイの DHCPv6 サーバが供給する IP アドレスの範囲に IPv6 デリゲイション（権限委譲）プレフィックスを定義できます。デリゲイションプレフィックスを使用して、割り当てられたプレフィックスに、特定の DHCP 情報の詳細にある LAN における他のネットワーク装置を通知する処理を自動化できます。

IPv6 プールの選択

1. 「List of IPv6 Address Pools」で使用するプールをチェックします。
2. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

IPv6 プールの登録

1. 「Add」ボタンをクリックして、以下の画面を表示します。

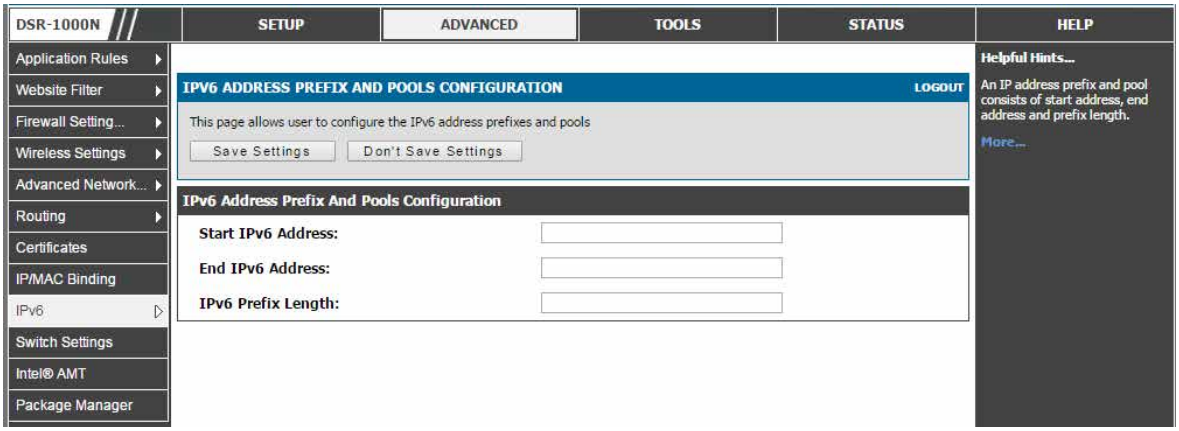


図 4-7　IPv6 Pool 設定

2. 「Start IPv6 Address」/「End IPv6 Address」にプールの開始 / 終了アドレス、「Profile Length」にプレフィックス長を入力します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

List of Prefixes for Prefix Delegation（プレフィックスデリゲイション）

以下の設定はプレフィックスデリゲイションを設定するために使用されます。

1. 「DHCPv6」セクションで、本オプションを選択して、DHCPv6 サーバでプレフィックスデリゲイションを有効にします。

2. 以下の項目を表示 / 追加します。

項目	説明
Prefix Address	DHCPv6 サーバプレフィックスプール内の IPv6 プレフィックスアドレス。
Prefix Length	プレフィックスアドレス長。

エントリの登録

1. 「Add」ボタンをクリックして、以下の画面を表示します。

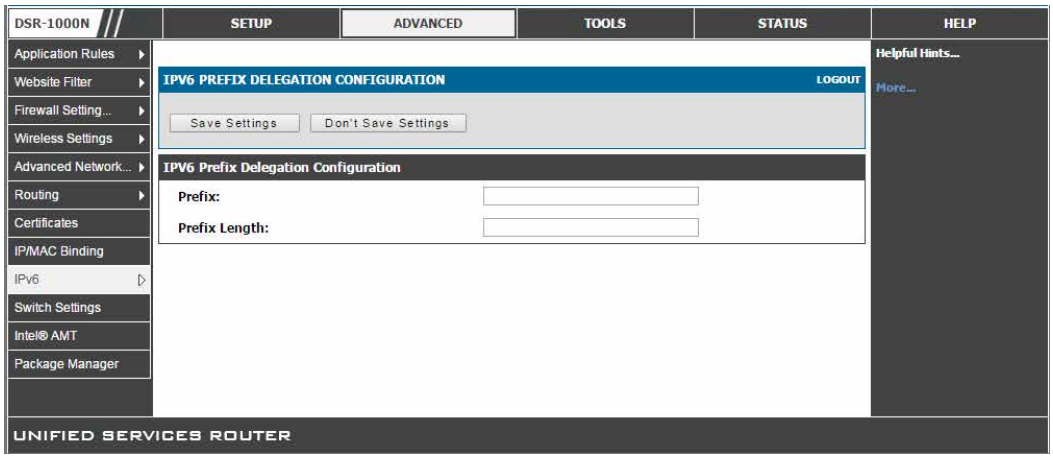


図 4-8　IPv6 Prefix Delegation Configuration 設定

2. 「Prefix」および「Prefix Length」を入力します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

IPv6 ルータ通知の設定

RA（ルータ通知）は LAN クライアントのための IPv4 DHCP 割り当てに似ているもので、ルータは詳細設定するためにデバイスに IP アドレスとサポートするネットワーク情報を割り当てます。ルータ通知は、IPv6 LAN のステートレスな自動設定のために IPv6 ネットワークで必要とされます。このルータにルータ通知デーモンを設定することによって、本製品は、LAN 上の RS を受信すると LAN 上のホストに対するレスポンスとしてルータ通知を送信します。

RADVD

ADVANCED > IPv6 > IPv6 LAN > Router Advertisement メニュー

ここではルータ通知デーモン (RADVD : Router Advertisement Daemon) に関連した設定を行うことができます。

1. **ADVANCED > IPv6 > IPv6 LAN > Router Advertisement** の順にメニューをクリックし、以下の画面を表示します。

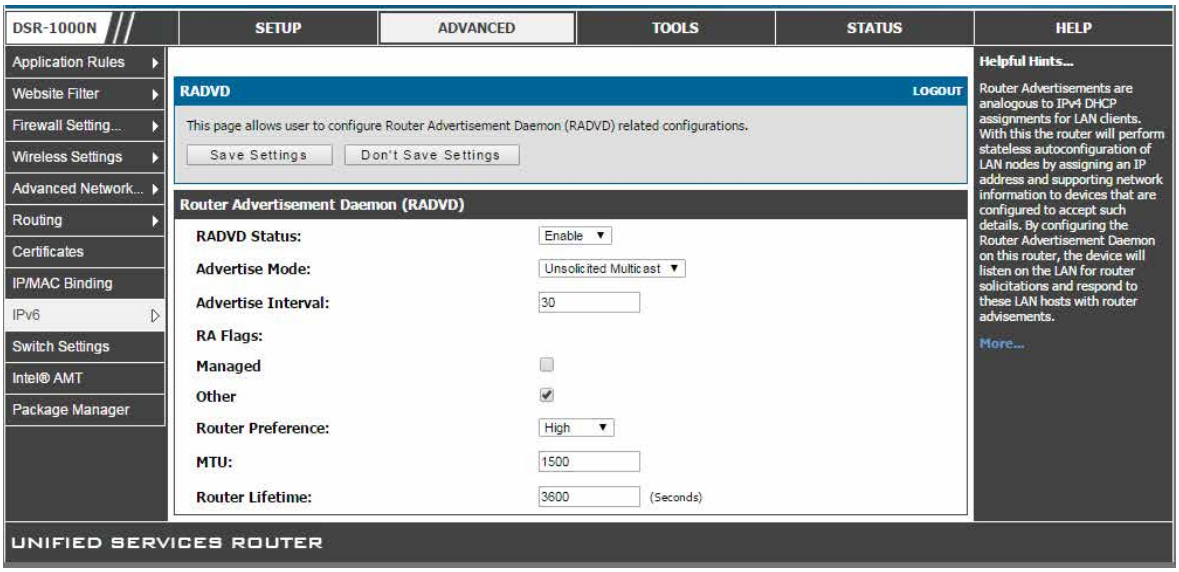


図 4-9　　ルータ通知デーモンの設定

LAN にステートレスな IPv6 自動設定をサポートするためには、「RADVD Status」を「Enable」に設定します。

以下の設定は RADVD を設定するために使用されます。:

項目	説明
Advertise Mode	• Unsolicited Multicast - ルータ通知（RA）をマルチキャストグループに所属する全インタフェースに送信します。 • Unicast only - RA を LAN 上の既知の IPv6 アドレスに制限し、全体的なネットワークトラフィックを減少させます。
Advertise Interval	「Advertise Mode」で「Unsolicited Multicast」を選択した場合、この間隔にはインタフェースからの通知間隔の最大時間を設定します。通知間の実際の時間はこの欄の 1/3 とこの欄の間のランダムな値となります。初期値は 30（秒）です。
RA Flags	これらのフラグの 1 つ、または両方と共にルータ通知（RA）を送信することができます。 • Managed - アドレス自動設定に管理 / ステートフルプロトコルを使用します。 • Other - ホストは（アドレス以外の）他の情報自動設定の管理 / ステートフルプロトコルを使用します。
Router Preference	ルータの RADVD 処理に関連付けられている優先度に「Low/Medium/High」から選択します。IPv6 クライアントの重複を回避するため、LAN 上に他の RADVD が有効なデバイスがある場合に本機能を使用します。
MTU	ルータ通知はこの MTU（Maximum Transmission Unit）値をルータによって自動構成される LAN 内のすべてのノードに設定します。初期値は 1500 です。
Router Lifetime	この値は、RA に存在しており、インタフェースのデフォルトルータとしてこのルータの有用性を示します。初期値は 3600（秒）です。この値が終了すると、新しい RADVD 交換がホストとこのルータ間で行われる必要があります。

「Save Settings」ボタンをクリックして設定内容を保存および適用します。

通知のプレフィックス

ADVANCED > IPv6 > IPv6 LAN > Advertisement Prefixes メニュー

ここではユーザは通知の時に使用される IPv6 プレフィックスを設定します。

ルータ通知と共に通知プレフィックスを設定することで、本ルータはステートレスアドレス自動設定の実行方法をホストに知らせることができます。ルータ通知は、Neighbor を決定し、ルータと同じリンク上にホストがあるかどうかを決定するサブネットプレフィックスのリストがあります。

注意 本機能を使用するためには **ADVANCED > IPv6 > IPv6 LAN > Router Advertisement** の「RADVD」画面で「RADVD Status」を「Enable」（有効）にする必要があります。

通知プレフィックスの登録

1. **ADVANCED > IPv6 > IPv6 LAN > Advertisement Prefixes** の順にメニューをクリックし、以下の画面を表示します。

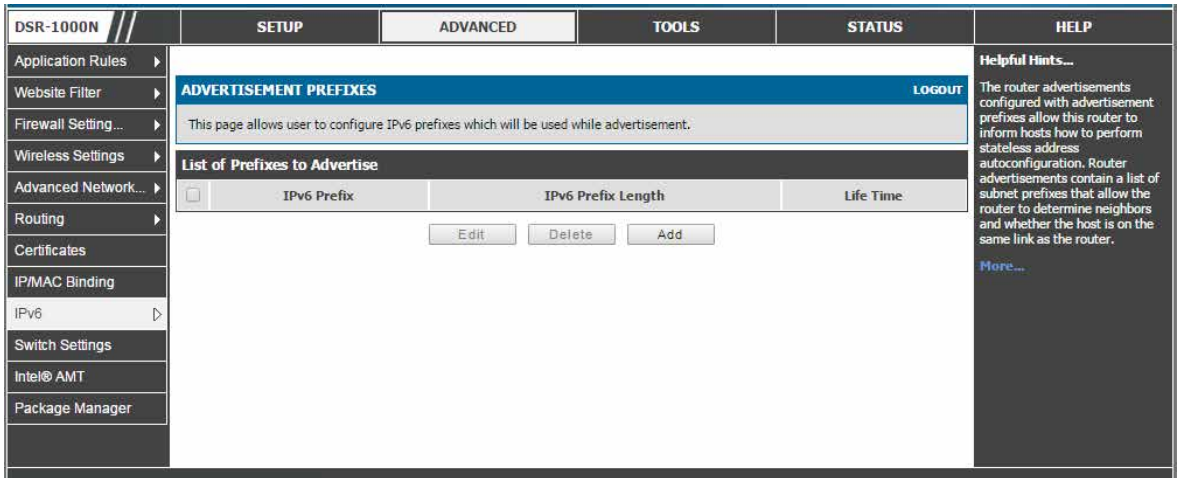


図 4-10　ADVERTISEMENT PREFIXES 画面

2. 「Add」ボタンをクリックして以下の画面を表示します。

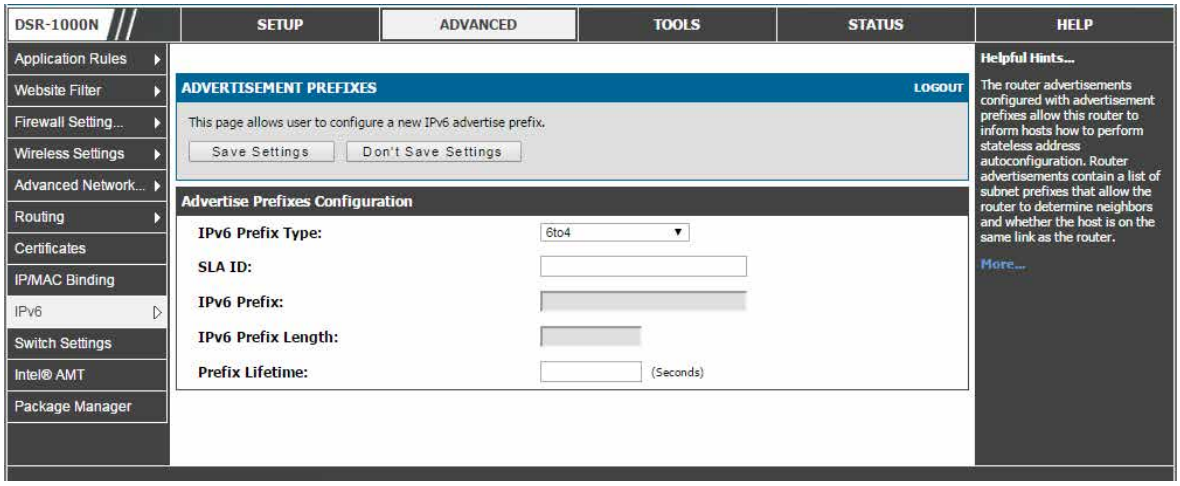


図 4-11　ADVERTISEMENT PREFIXES 画面 - 追加

ルータ通知に以下のプレフィックスオプションを設定することができます。:

項目	説明
IPv6 Prefix Type	ホストが IPv6 to IPv4 トンネルを確実にサポートするためには、「6to4」プレフィックスタイプを選択します。「Global/Local/ISATAP」を選択すると、ノードは他のすべての IPv6 ルーティングオプションをサポートすることができます。
SLA ID	SLA ID（Site-Level Aggregation Identifier）は、「6to4」プレフィックスタイプが選択された場合に利用することができます。これはルータ通知に使用されるルータの LAN インタフェースのインタフェース ID とするべきです。
IPv6 Prefix	「Global/Local/ISATAP」プレフィックスを使用する場合、この欄は本ルータが通知する IPv6 ネットワークを定義するために使用されます。
IPv6 Prefix Length	この値は、「Global/Local/ISATAP」プレフィックスを使用する場合、アドレスのネットワーク部分を定義する連続した IPv6 アドレスの高位のビット数を示す数値です。これは通常 64 です。
Prefix Lifetime	これは要求するノードが通知されたプレフィックスを使用できる期間（秒）を定義します。IPv4 ネットワークにおける DHCP リースタイムに似ています。

IPv6 通知プレフィックスを設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

DHCPv6 リースクライアント

ADVANCED > IPv6 > IPv6 LAN > IPv6 Leased Clients メニュー

LAN DHCPv6 サーバに接続する DHCPv6 クライアントおよびリースしている DHCPv6 サーバを表示します。

1. **ADVANCED > IPv6 > IPv6 LAN > IPv6 Leased Clients** の順にメニューをクリックし、以下の画面を表示します。

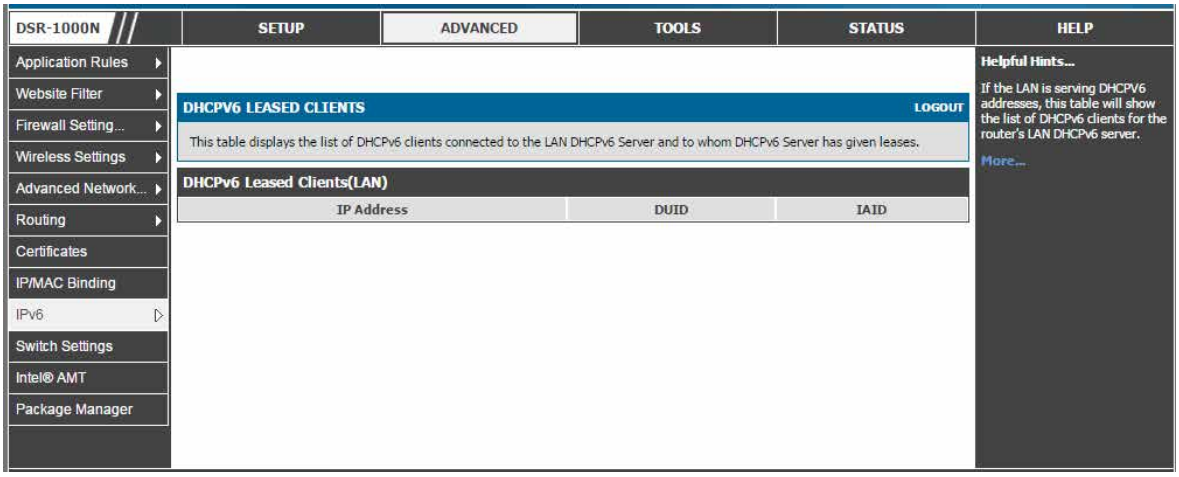


図 4-12　DHCP リースクライアント画面

2. 以下の項目を表示します。

項目	説明
IP Address	DHCP サーバの IP アドレスです。
DUID	DUID を表示します。各 DHCP クライアントとサーバには DUID があります。DHCP サーバは、設定パラメータの選択用にクライアントを識別するため、クライアントと共に IA と連携するために DUID を使用します。DHCP クライアントは、サーバが特定される必要があるメッセージのサーバを特定するのに DUID を使用します。
IAID	クライアントが選択した IA の識別子。各 IA には IAID があります。これは、そのクライアントに所属する IA の全 IAID で固有となるように選択されます。

VLAN 設定

ルータは、VLAN を使用することで LAN 上に分離した仮想ネットワークを構築できます。VLAN 識別子で定義したサブネットワークに通信するように LAN デバイスを設定できます。物理ポートから（へ）のトラフィックを一般の LAN から隔離できるように、固有の VLAN ID を LAN ポートに割り当てることができます。VLAN フィルタリングは、大規模なネットワークにあるデバイスのブロードキャストパケットを制限するために特に役に立ちます。

ルータの VLAN サポートは初期値では「Enabled」（有効）になっています。無効の場合、「VLAN Configuration」メニューで、ルータの VLAN サポートを有効にします。また、仮想 VLAN を定義するために次のセクションに進みます。また、仮想 VLAN により、ファイアウォールルールと VPN ポリシーにセグメンテーションを提供します。

注意 VLAN 機能を設定するためには、まず「Enable VLAN」を有効にする必要があります。

1. **SETUP > VLAN Settings > VLAN Configuration** の順にメニューをクリックし、以下の画面を表示します。

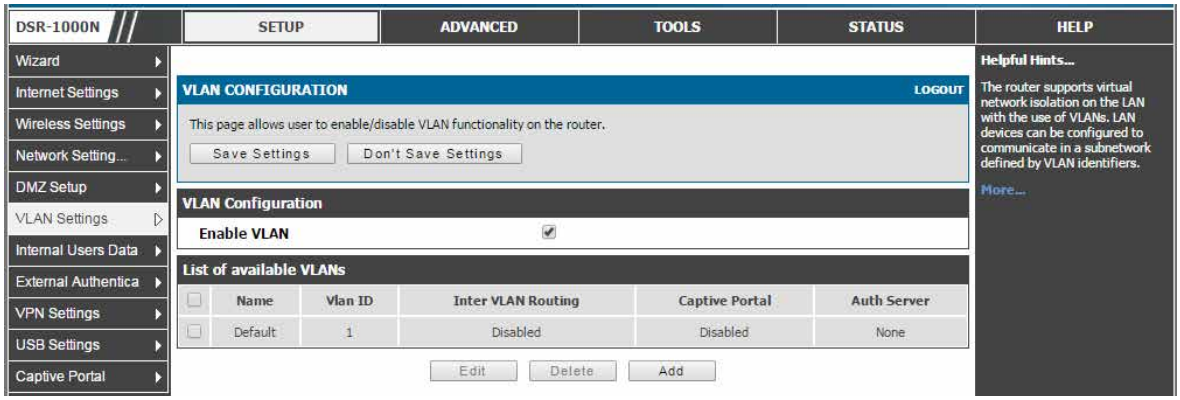


図 4-13　Enable VLAN 画面

2. 「Enable VLAN」をチェックして、VLAN を有効にします。初期値では、LAN ネットワークは Default VLAN に所属します。

ここでは有効な VLAN のリストの表示、VLAN の追加、編集または削除を行います。

行われるアクションは、以下の通りです。

項目	説明
Edit	選択した VLAN エントリを編集します。
Delete	選択した VLAN エントリを削除します。
Add	新しい VLAN エントリ追加します。

VLAN メンバシップの登録

1. 「Add」ボタンをクリックして以下の画面を表示します。

図 4-14　LAN への VLAN メンバシップの追加

2. VLAN メンバシップエントリを指定します。

項目	説明
VLAN Configuration	
Name	VLAN 名を指定します。
ID	VLAN ID 値（2-4093）を指定します。VLAN ID 1 はデフォルト VLAN に予約されており、これはインタフェースに受信するタグなしフレームに使用されます。
Inter VLAN Routing Enable	有効にすることによって、この VLAN ID に所属する LAN ホストからのトラフィックは「Inter VLAN Routing」が有効である別の定義済み VLAN ID に渡されます。
Captive Portal	VLAN ごとにキャプティブポータルを「Enable」（有効）/「Disable」（無効）にします。有効にすると、表示される「Captive Portal Config」セクション内の各項目を設定できます。
Captive Portal Config	
Authentication Server	この VLAN で利用できる認証サーバを表示します。この VLAN のキャプティブポータルにログインするすべてのユーザは、選択したサーバを通して認証されます。「Captive Portal」が有効である場合にだけ、本オプションは表示されます。利用可能な認証サーバ : Local User Database、Radius Server、LDAP Server、Active Directory、NT Domain および POP3
Authentication Type	認証サーバに「Radius Server」を選択した場合にのみ、本オプションを設定できます。有効な認証タイプは PAP/CHAP/MS-CHAP/MS-CHAPV2 です。
Captive Portal Profile	有効なキャプティブポータルログインプロファイルのリストを表示します。利用可能なプロファイルのいずれもこの VLAN で使用できます。
Create a Profile	新しいキャプティブポータルログインプロファイルと作成するためのリンクです。このリンクをクリックすると、新しいログインプロファイルを作成するページへ遷移します。
Redirect Type	キャプティブポータルログインページのリダイレクションタイプを指定します。HTTP または HTTPS のいずれかを選択します。

3. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ポートに VLAN を関連付ける

VLAN ID を持つ特定の LAN ポートを通してすべてのトラフィックにタグ付けをするためには、物理ポートに VLAN を関連付けすることができます。

SETUP > VLAN Settings > Port VLAN メニュー

ポート VLAN を設定することができます。ユーザはポートを選択し、VLAN にそれらを追加することができます。

1. **SETUP > VLAN Settings > Port VLAN** の順にメニューをクリックし、以下の画面を表示します。

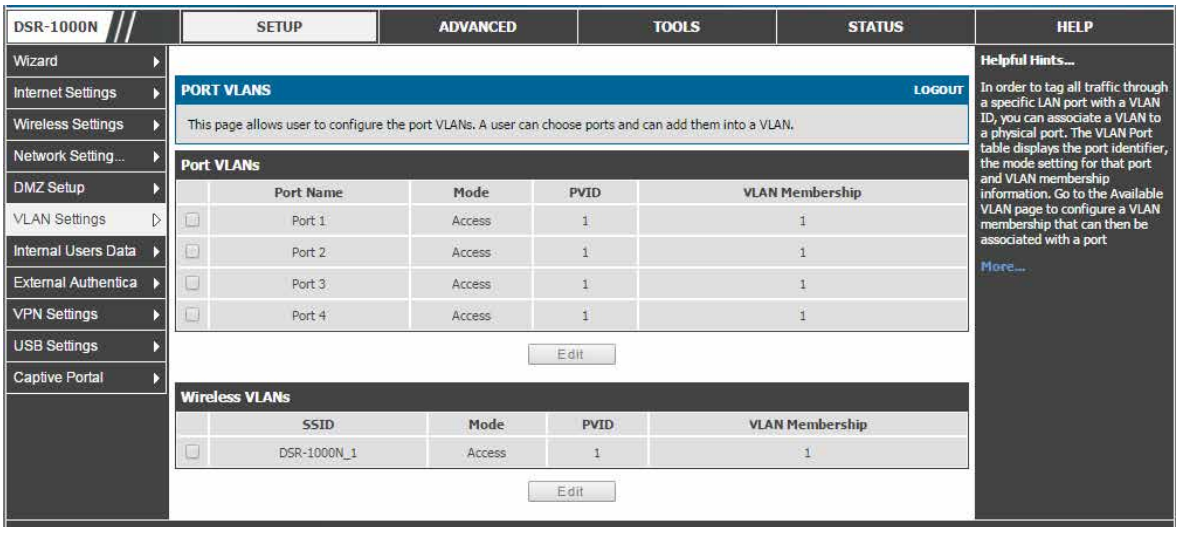


図 4-15　ポート VLAN のリスト

「PORT VLANs」ページには LAN と無線 LAN の VLAN メンバシップのプロパティが示されます。VLAN ポートテーブルは、ポートの識別子、ポートのモード設定、および VLAN メンバシップ情報を表示します。

注意　「Wireless VLANs」セクションは、DSR-1000N にのみ対応しています。

VLAN ポートテーブルの編集

1. 4 つの物理ポート、または設定したアクセスポイントから 1 つを選択して、「Edit」ボタンをクリックし、以下の画面を表示します。

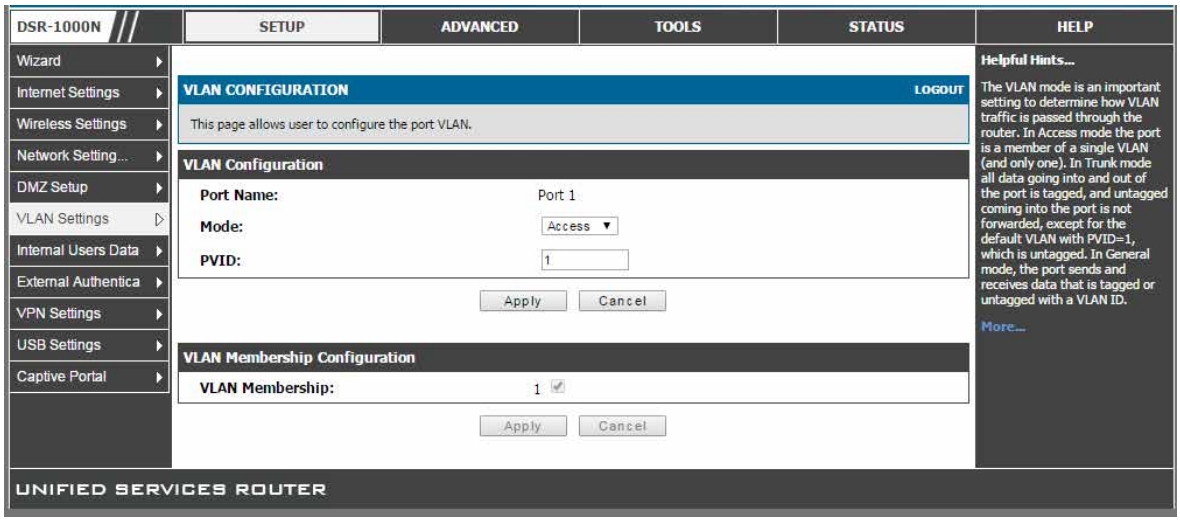


図 4-16　ポートへの VLAN メンバシップの編集

2. 編集ページは以下の設定オプションを提供します。:

項目	説明
VLAN Configuration	
Mode	VLAN のモードは、General、Access、または Trunk です。初期値は「Access」です。 • General ポートはユーザが選択可能な VLAN セットのメンバになることができます。ポートは VLAN ID を持つタグ付きまたはタグなしデータを送受信します。ポートへのデータがタグなしであると、定義済みの PVID をそれに割り当てます。例えば、ポート 3 が PVID 3 を持つ「General」ポートである場合、ポート 3 のタグなしデータには PVID 3 が割り当てられます。同じ PVID を持つポートから送信されたすべてのタグ付きデータからタグが取り外されます。これは、通常、２つのイーサネットポートを持つ IP 電話に使用されるモードです。電話からルータのスイッチポートに来るデータはタグ付けされます。接続するデバイスから電話を通過するデータはタグが取り外されます。 • Access ポートは単一の VLAN のメンバです。ポートに入力する、またポートから出力するすべてのデータがタグなしとなります。アクセスモードのポートを経由するトラフィックは他のすべてのイーサネットフレームに類似しています。 • Trunk ポートはユーザが選択可能な VLAN のメンバになることができます。ポートに入力される、またポートから出力されるすべてのデータがタグ付けされます。ポートに入力するタグなしデータは、ポート PVID=1 を持つデフォルト VLAN を除き転送されず、タグなしとなります。トランクポートは、同じ物理リンク上の複数 VLAN に対するトラフィックを多重化します。
PVID	「General」モードが選択される場合にポートの PVID を選択します。
VLAN Membership Configuration	
VLAN Membership	設定した VLAN メンバシップはポートの「VLAN Membership」設定に表示されます。もうひとつの VLAN メンバシップオプションを「General」または「Trunk」ポートに選択することによって、選択された VLAN メンバシップ ID 間にトラフィックを送信することができます。

3. 設定後、「Apply」ボタンをクリックして設定内容を保存および適用します。

マルチ VLAN サブネット

SETUP > VLAN Settings > Multiple VLAN Subnets メニュー

ここは有効なマルチ VLAN のサブネットのリストを表示します。また、マルチ VLAN を編集することもできます。

各設定済み VLAN ID が LAN 内のサブネットに直接マップできます。各 LAN ポートは固有の IP アドレスを割り当てることができ、この VLAN のデバイスに IP アドレスリースを割り当てるために VLAN 指定の DHCP サーバを設定できます。

1. **SETUP > VLAN Settings > Multiple VLAN Subnets** の順にメニューをクリックし、以下の画面を表示します。

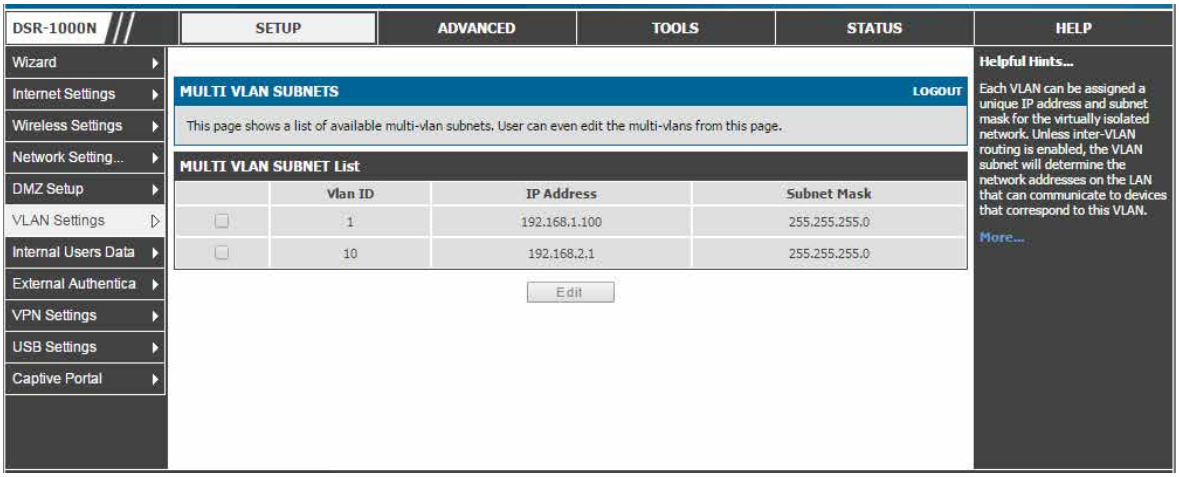


図 4-17　マルチ VLAN サブネットのリスト

ポート VLAN 属性の変更

1. 編集する VLAN をチェックして「Edit」ボタンをクリックし、以下の画面を表示します。

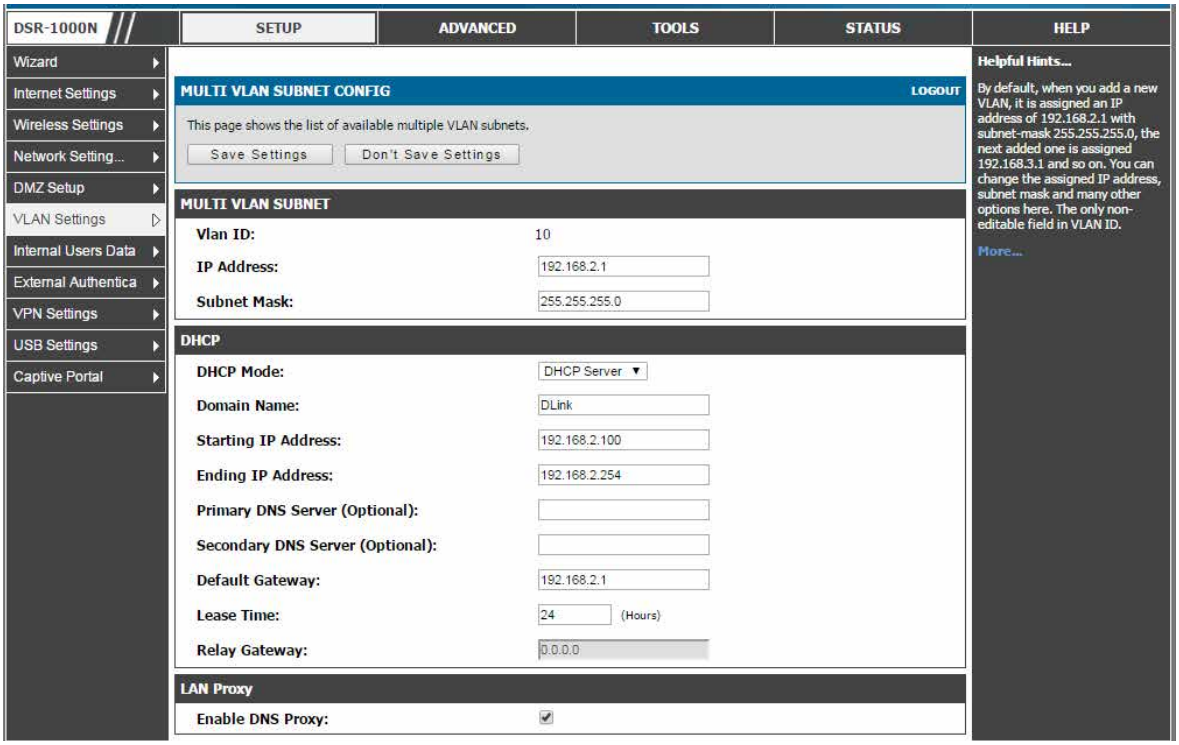


図 4-18　マルチ VLAN サブネット

2. 以下の項目を入力します。

項目	説明
MULTI VLAN SUBNET	
Vlan ID	同じサブネット範囲にあるすべてのメンバデバイスを持つ VLAN の PVID。
IP Address	この VLAN ID の LAN IP アドレスを入力します。
Subnet Mask	上記の IP アドレスのサブネットマスク
DHCP	
この VLAN が TCP/IP 設定をメンバデバイスに割り当てるようにします。	
DHCP Mode	• None - VLAN 上のコンピュータがスタティック IP アドレスで設定されている場合、または別の DHCP サーバを使用するように設定されている場合に選択します。 • DHCP Relay - リレーゲートウェイ情報を入力します。 • DHCP Server - DHCP サーバとしてルータを使用します。この場合、以下の情報を設定します。
Starting IP Address	IP アドレス範囲における最初の IP アドレスを入力します。このアドレスと終了 IP アドレスの間の IP アドレスは VLAN に参加するどの新しい DHCP クライアントにも割り当てられます。 注意 開始および終了 DHCP アドレスは、上で設定した VLAN の IP アドレスと同じ「ネットワーク」にあるべきです。
Ending IP Address	LAN ホストにリースするアドレス範囲における最後の IP アドレスを入力します。開始 IP アドレスとこの IP アドレス間の IP アドレスは VLAN に参加するどの新しい DHCP クライアントにも割り当てられます。 注意 開始および終了 DHCP アドレスは、上で設定した VLAN の IP アドレスと同じ「ネットワーク」にあるべきです。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。（オプション）
Secondary DNS Server	セカンダリ DNS サーバ IP アドレスを入力します。（オプション）
Default Gateway	デフォルトゲートウェイのアドレスを指定します。この VLAN に参加する新しい DHCP クライアントには、デフォルトゲートウェイとしてこのアドレスが付与されます。
Lease Time	IP アドレスがクライアントにリースされる期間（時）を指定します。
Relay Gateway	ゲートウェイアドレスを入力します。これは、DHCP リレーが DHCP モードに選択されている場合にこのセクションで必要とされる唯一の設定パラメータです。
LAN Proxy	
Enable DNS Proxy	このボックスをチェックして、この VLAN の DNS プロキシを有効にします。

3. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

DMZ 設定

本ルータは、セカンダリの WAN イーサネットポートまたは専用の DMZ ポートとして物理ポートの 1 つを設定することができます。DMZ はパブリックにオープンされてますが、ファイアウォールの背後にあるサブネットワークです。DMZ 上でインターネットに露出する特定のサービス / ポートを LAN に露出させないように、DMZ が LAN にセキュリティのレイヤを追加します。インターネット（Web または E メールサーバなど）に露出する必要のあるホストだけを DMZ ネットワークにおくことをお勧めします。ファイアウォールルールでは LAN または WAN の両方から DMZ に対して特定のサービス / ポートへのアクセスを許可することができます。DMZ ノードのどれかに対する攻撃がある場合、LAN も同様に被害を受けやすいというわけではありません。

DMZ ポートの設定

SETUP > DMZ Setup > DMZ Setup Configuration メニュー

DMZ を有効にします。

DMZ は LAN と比較するとよりファイアウォール制限が少ないネットワークです。このゾーンは、ホストサーバに使用されて、ホストサーバにパブリックアクセスを与えることができます。

DMZ 設定は LAN 設定と同様です。このゲートウェイの LAN インタフェースに付与された IP アドレスと同じにすることはできません。しかし、それを除き、DMZ ポートに割り当てられる IP アドレスまたはサブネットに制限はありません。

注意 DMZ ポートを設定するためには、**SETUP > Internet Settings > Configurable Port** 画面で「Configurable Port Status」（ルータの設定可能なポート）を「DMZ」にします。

1. **SETUP > Internet Settings > Configurable Port** の順にメニューをクリックし、以下の画面を表示します。

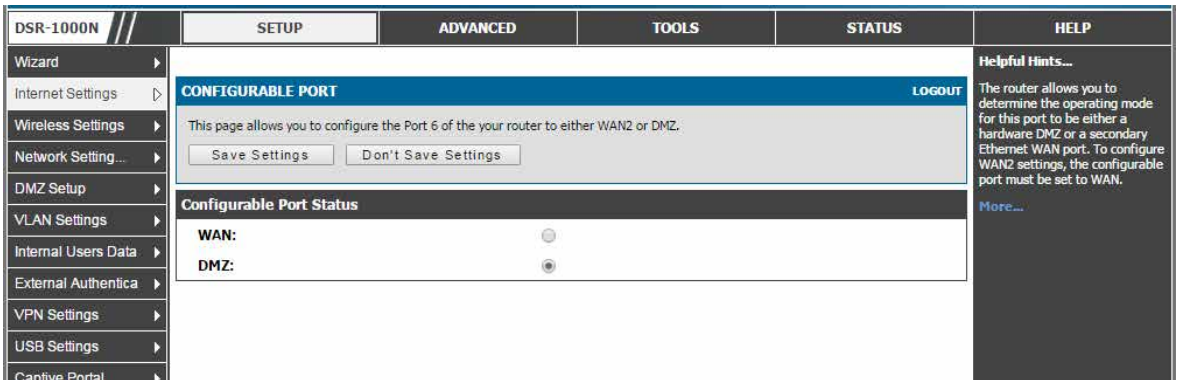


図 4-19　CONFIGURABLE PORT 画面

「Configurable Port Status」（ルータの設定可能なポート）を「DMZ」にして「Save Settings」ボタンをクリックして設定内容を保存および適用します。

2. **SETUP > DMZ Setup > DMZ Setup Configuration** の順にメニューをクリックし、以下の画面を表示します。

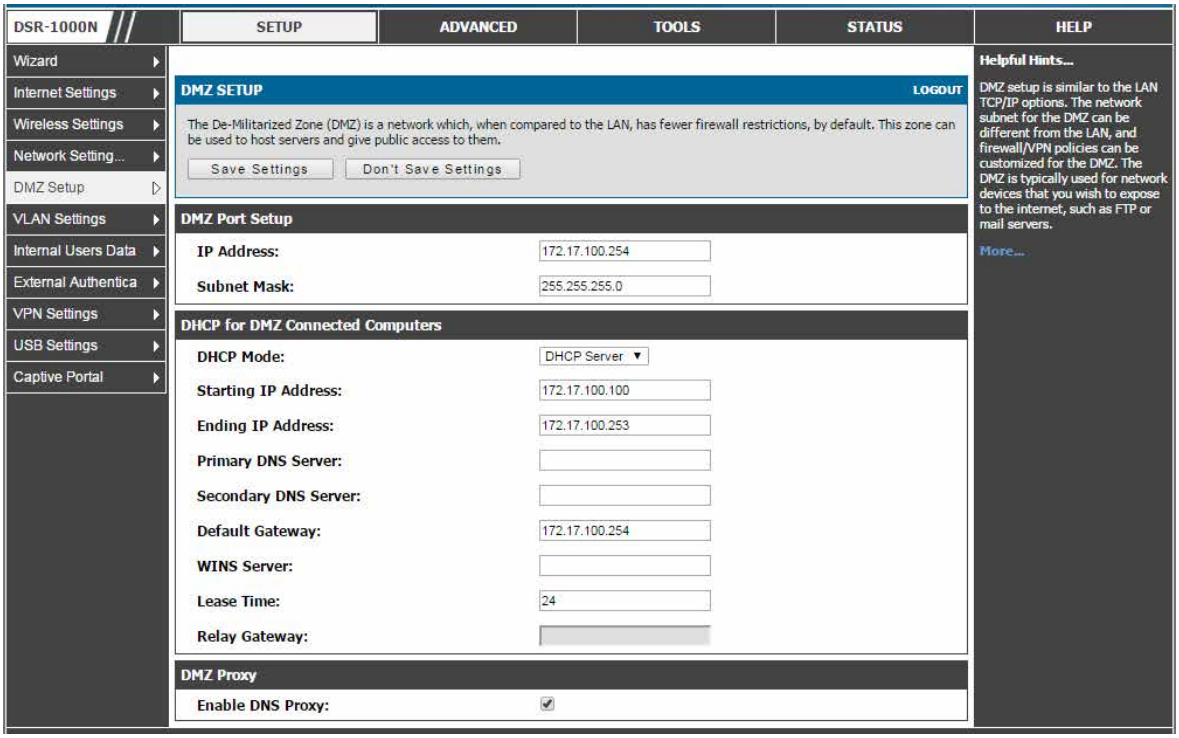


図 4-20　DMZ 設定

3. 以下の項目を入力します。

項目	説明
DMZ Port Setup	
IP Address	ルータの DMZ LAN IP アドレスを入力します。
Subnet Mask	上記の IP アドレスのサブネットマスク。
DHCP for DMZ Connected Computers	
DHCP Mode	• None - DMZ 上のコンピュータがスタティック IP アドレスで設定されている場合、または別の DHCP サーバを使用するように設定されている場合に選択します。 • DHCP Relay - リレーゲートウェイ情報を入力します。 • DHCP Server - DHCP サーバとしてルータを使用するために選択して以下の情報を設定します。
Starting IP Address	DMZLAN ホストにリースするアドレス範囲における最初の IP アドレスを入力します。
Ending IP Address	DMZLAN ホストにリースするアドレス範囲における最後の IP アドレスを入力します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	セカンダリ DNS サーバ IP アドレスを入力します。
WINS Server	WINS サーバの IP アドレス（オプション）。WINS（Windows Internet Naming Service）は、DNS サーバの同等ですが、ホスト名の解決のために NetBIOS プロトコルを使用します。ネットワークが Windows ベースのコンピュータだけから構成されて、名前解決に WINS サーバの使用を希望する場合、WINS サーバの IP アドレスを入力します。DHCP クライアントからの DHCP 要求を承諾する場合、ルータは DHCP 設定で WINS サーバの IP アドレスを含めます。
Default Gateway	デフォルトゲートウェイのアドレスを指定します。DMZ に参加する新しい DHCP クライアントには、デフォルトゲートウェイとしてこのアドレスが付与されます。
Lease Time	IP アドレスがクライアントにリースされる期間（時）を指定します。
Relay Gateway	ゲートウェイアドレスを入力します。これは、DHCP リレーが DHCP モードに選択されている場合にこのセクションで必要とされる唯一の設定パラメータです。
DMZ Proxy	
Enable DNS Proxy	このボックスをチェックして、この DMZ の DNS プロキシを有効にします。この機能が有効な場合、ルータは、すべての DNS 要求に対するプロキシとして動作し、（WAN 設定ページで設定されるように）ISP の DNS サーバと通信します。すべての DHCP クライアントが DNS プロキシが動作している IP（つまり、ボックスの DMZ IP）にそったプライマリ / セカンダリ DNS IP を受信します。無効にされると、すべての DHCP クライアントが DNS プロキシ IP アドレスを除いた ISP の DNS IP アドレスを受信します。この機能は「自動ロールオーバ」モードの場合に特に便利です。例えば、各接続用の DNS サーバが異なる場合、リンク障害により DNS サーバへのアクセスが不可能になるかもしれません。しかし、DNS プロキシが有効であると、クライアントは要求をルータにすることができます。さらに、ルータは順番にアクティブな接続の DNS サーバにそれらの要求を送信します。

4. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

DMZ DHCP の予約 IP

SETUP > DMZ Setup > DMZ DHCP Reserved IPs メニュー

DHCP サーバ設定のためにスタティックに予約される IP アドレスを設定します。

DHCP が DMZ で有効である場合、DMZ デバイスが同じ IP アドレスをいつも受信できるようにするためには、DMZ デバイスの MAC アドレスを希望する IP アドレスに割り当てます。

1. **SETUP > DMZ Setup > DMZ DHCP Reserved IPs** の順にメニューをクリックし、以下の画面を表示します。

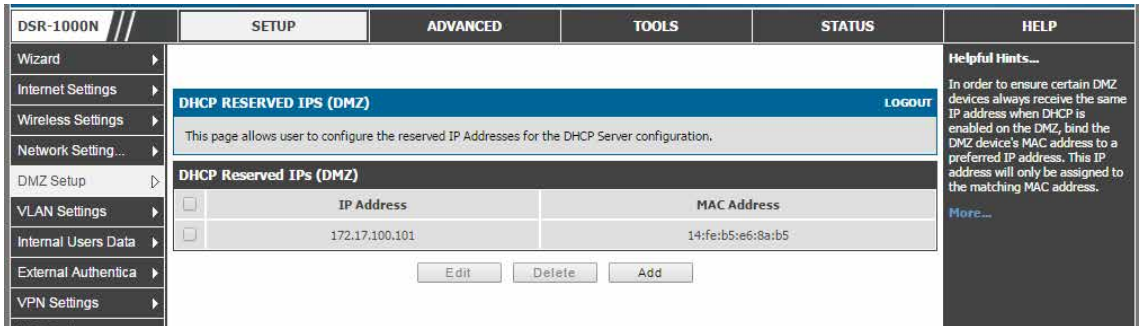


図 4-21　DHCP 予約 IP リスト画面（DMZ）

注意 DMZ ポートを設定するためには、**SETUP > Internet Settings > Configurable Port** 画面で「Configurable Port Status」（ルータの設定可能なポート）を「DMZ」にします。

注意 本機能を使用するためには **SETUP > DMZ Setup > DMZ Setup Configuration** で「DHCP Mode」を「DHCP Server」にする必要があります。

スタティック IP の登録

1. 「Add」ボタンをクリックして以下の画面を表示します。

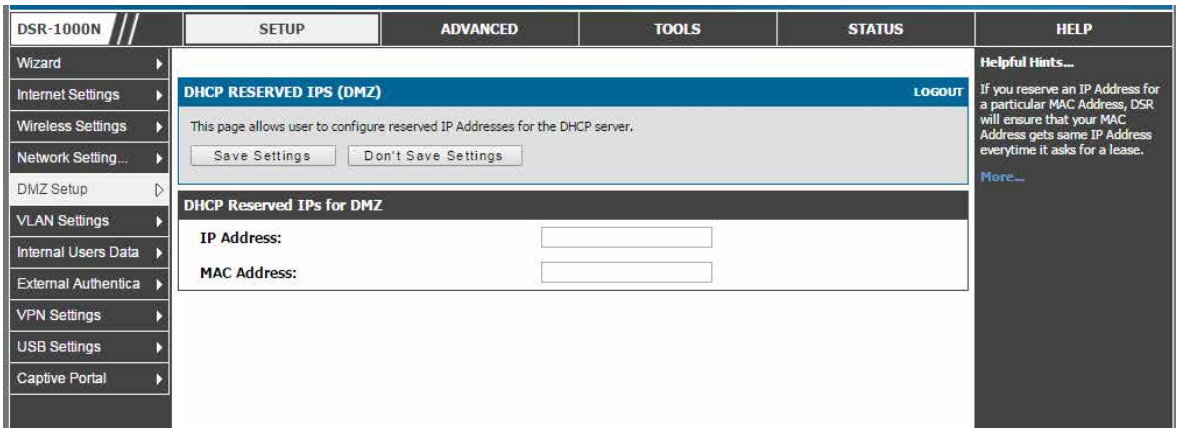


図 4-22　スタティック IP の追加（DMZ）

2. 以下の項目を入力します。

項目	説明
IP Address	DHCP サーバが予約するホストの DMZ IP アドレス。
MAC Address	それが DMZ 上にある場合には、予約された IP アドレスが割り当てられる MAC アドレス。

3. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

DMZ DHCP リースクライアント

SETUP > DMZ Setup > DMZ DHCP Leased Clients メニュー

DMZ DHCP サーバに接続する DHCP クライアントおよびどの DHCP サーバがリースしているかを表示します。

1. **SETUP > DMZ Setup > DMZ DHCP Leased Clients** 順にメニューをクリックし、以下の画面を表示します。

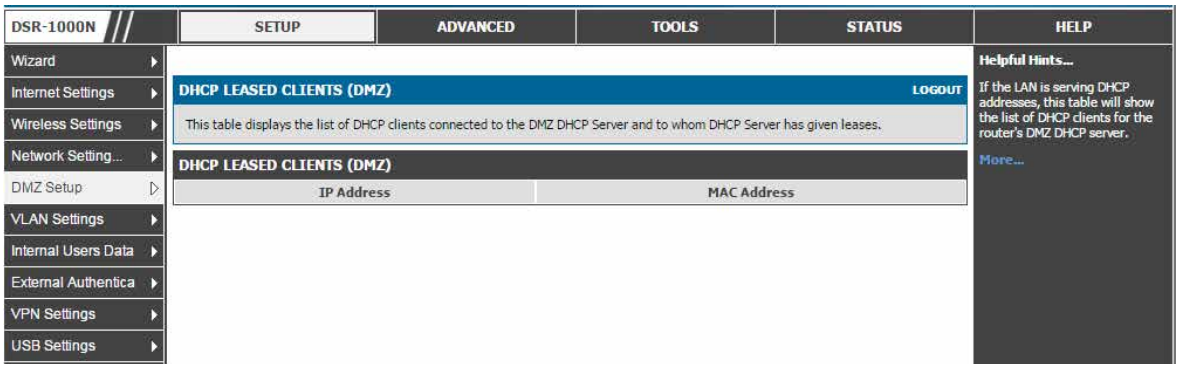


図 4-23　DHCP 予約 IP リスト画面（DMZ）

注意　本機能を使用するためには **SETUP > DMZ > DMZ Setup Configuration** で「DHCP Mode」を「DHCP Server」にする必要があります。

UPnP 設定

ADVANCED > Advanced Network > UPnP メニュー
本製品の UPnP 機能を設定します。

UPnP（Universal Plug and Play）は、ルータと通信できるネットワーク上のデバイスを検出し、自動設定を行う機能です。ネットワークデバイスが UPnP に検出されると、ネットワークデバイスが要求するトラフィックのプロトコル用に内部または外部ポートをオープンすることができます。

UPnP を有効にすると、LAN（または、追加済みのいずれかの VLAN）にある UPnP をサポートするデバイスを検出するようにルータを設定することができます。無効にすると、ルータはデバイスの自動設定を許可しません。

1. **ADVANCED > Advanced Network > UPnP** 順にメニューをクリックし、以下の画面を表示します。

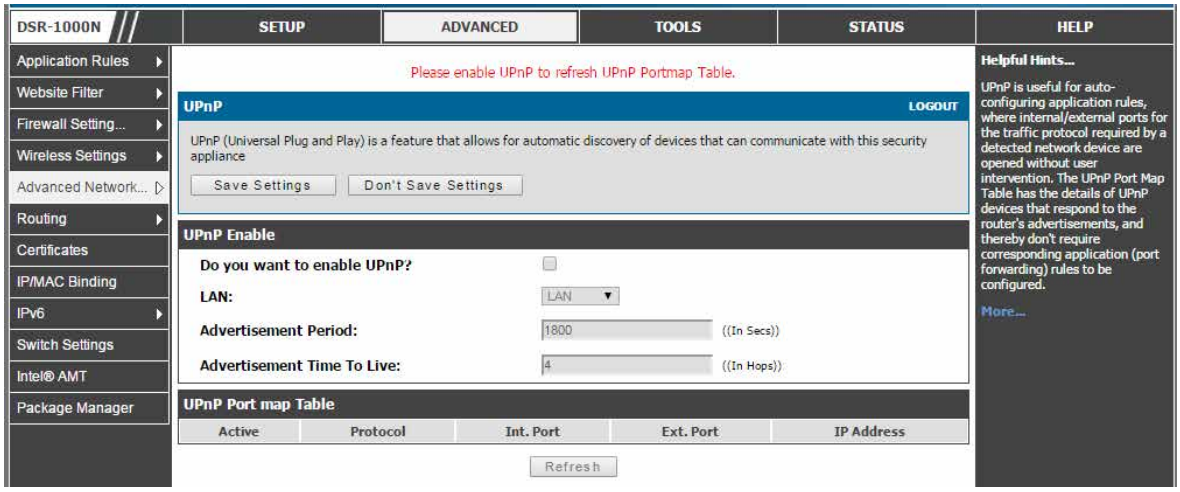


図 4-24　UPnP 設定

2. UPnP を使用するためには以下の設定を行います。:

項目	説明
UPnP Enable	
Do you want to enable UPnP?	UPnP を有効にする場合にチェックします。
LAN	必要に応じて、LAN 全体または指定した VLAN グループで UPnP を有効にします。有効な VLAN は LAN インタフェースにそってメニューに表示されます。
Advertisement Period	ルータがネットワーク上に UPnP 情報をブロードキャストする頻度です。大きい値はネットワークトラフィックを最小限にしますが、新しい UPnP デバイスをネットワークで特定する際に遅延をもたらします。
Advertisement Time to Live	これは各 UPnP パケットのホップで表現されます。また、パケットが破棄される前に伝播できるステップ数です。小さい値は UPnP ブロードキャスト範囲を制限します。初期値の 4 はスイッチ数が少ないネットワークでは一般的な数値です。
UPnP Port map Table	
UPnP ポートマップテーブルには、ルータ通知に応答する UPnP デバイスの詳細があります。各検出 DSR ルータに対して以下の情報が表示されます。	
Active	Yes / No は接続を確立した UPnP デバイスのポートが現在アクティブであるかどうかを示します。
Protocol	デバイスが使用しているネットワークプロトコル（HTTP、FTP など）。
Int. Port（Internal Port）	（もしあれば）UPnP によってオープンされた内部ポート。
Ext. Port（External Port）	（もしあれば）UPnP によってオープンされた外部ポート。
IP Address	本ルータが検出した UPnP デバイスの IP アドレス。

「Refresh」をクリックして、ポートマップテーブルを更新し、新しい UPnP デバイスを検索します。

3. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

キャプティブポータル

キャプティブポータルセッション

SETUP > Captive Portal > Captive Portal Sessions メニュー

LAN ユーザは DSR による Web のポータル認証を経由してインターネットにアクセスすることができます。また、キャプティブポータルは、ランタイム認証と呼ばれ、ユーザが Web アクセスのために HTTP 接続要求を開始しても、LAN サービスへのアクセスが必要がない Web カフェのシナリオに理想的です。ファイアウォールポリシーの下では、HTTP アクセスのために認証を必要とするユーザを定義して、一致するユーザの要求が行われると、DSR は要求に対して、ユーザ名 / パスワードの入力を求めます。HTTP アクセスを許可する前に、ログイン証明書をユーザデータベース内の RunTimeAuth ユーザと比較します。

注意 キャプティブポータルは LAN ユーザだけに利用可能であり、DMZ ホストでは利用できません。

1. **SETUP > Captive Portal > Captive Portal Sessions** 順にメニューをクリックし、以下の画面を表示します。

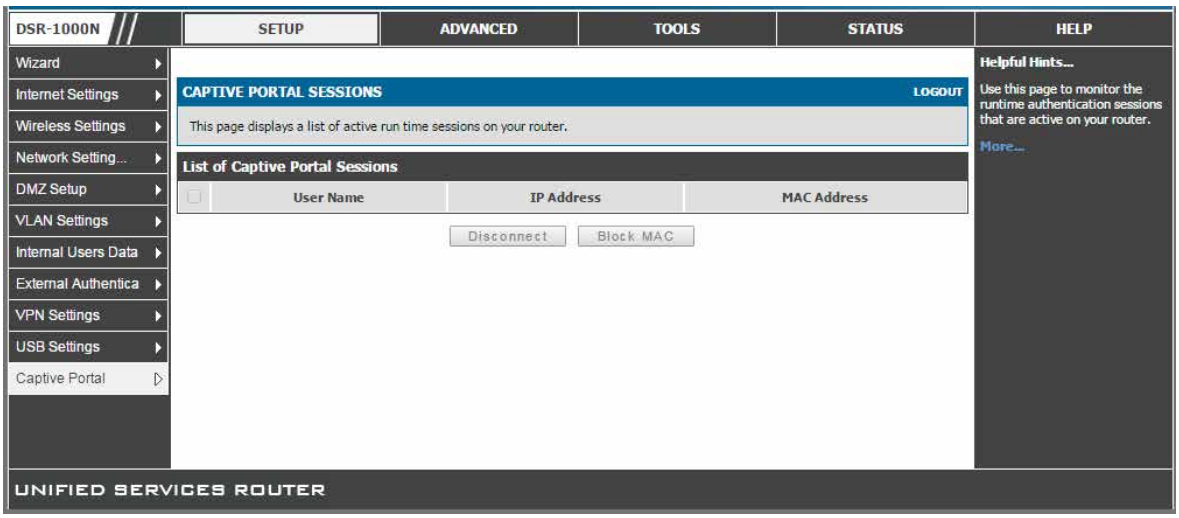


図 4-25　ランタイムセッション

ルータのファイアウォールを経由したアクティブなランタイムインターネットセッションはテーブルに示されます。

これらのユーザは、ローカルまたは外部ユーザデータベースに存在していて、インターネットアクセスを許可されたログイン証明書を持っています。「Disconnect」ボタンにより、DSR の管理者は選択した認証ユーザを破棄することができます。「Block MAC」ボタンは、結果的に選択したクライアントをブロックリストに追加することになり、このクライアントの現在および今後のセッションを防止します。

キャプティブポータル設定

SETUP > Captive Portal > Captive Portal Setup メニュー

キャプティブポータルは特定のインタフェースに選択的に認証を付与するためのセキュリティメカニズムです。本ページでは、設定済みのカスタムキャプティブポータルプロファイルを表示して、どれが使用中であるかを示します。

1. **SETUP > Captive Portal > Captive Portal Setup** 順にメニューをクリックし、以下の画面を表示します。

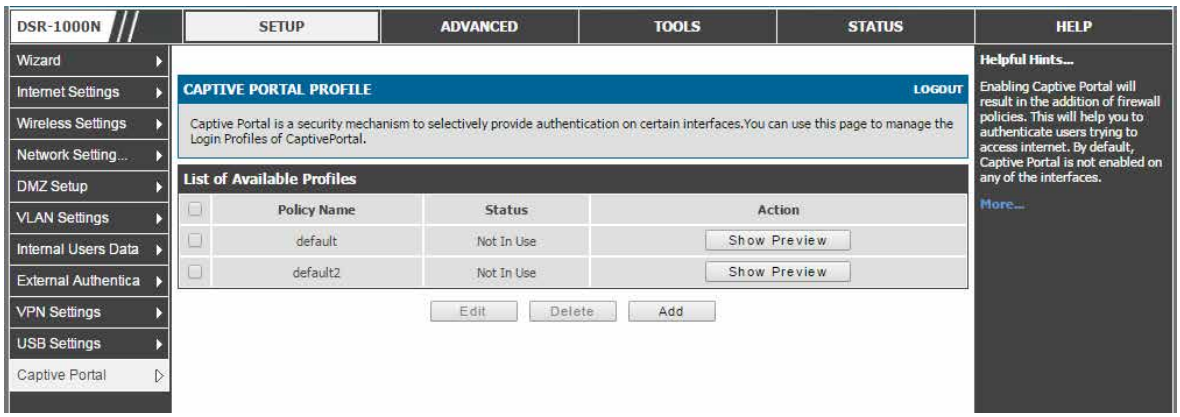


図 4-26　キャプティブポータル設定

2. 以下の項目を表示または設定します。

項目	説明
List of Available Profiles	
キャプティブポータルが有効な場合、これらのプロファイルのどれも「Captive Portal Login」ページで使用可能です。	
Edit	追加したプロファイルを編集します。「default」プロファイルは編集できません。
Delete	選択したプロファイルを削除します。「default」プロファイルと使用中のプロファイルは削除できません。
Add	新しいプロファイルを追加します。許可されるプロファイルの最大数は「default」を除いて 5 個です。
Show Preview	プロファイルが選択されると、ページのプレビューを表示します。

キャプティブポータル設定のカスタマイズ

SETUP > Captive Portal > Customized Captive Portal Setup メニュー

カスタマイズするキャプティブポータルログインページ情報を定義することができます。

新しくキャプティブポータルを作成するためには、固有のポリシー名を持つプロファイルを作成します。プロファイルは新しいセッションに表示されるエントリ画面を管理します。また、インターネットアクセスのためにサービスプロバイダを特定できるようにブラウザメッセージと背景色 / ヘッダをカスタマイズすることができます。

プロファイルの追加

1. 「List of Available Profiles」セクションの「Add」ボタンをクリックして以下の画面を表示します。

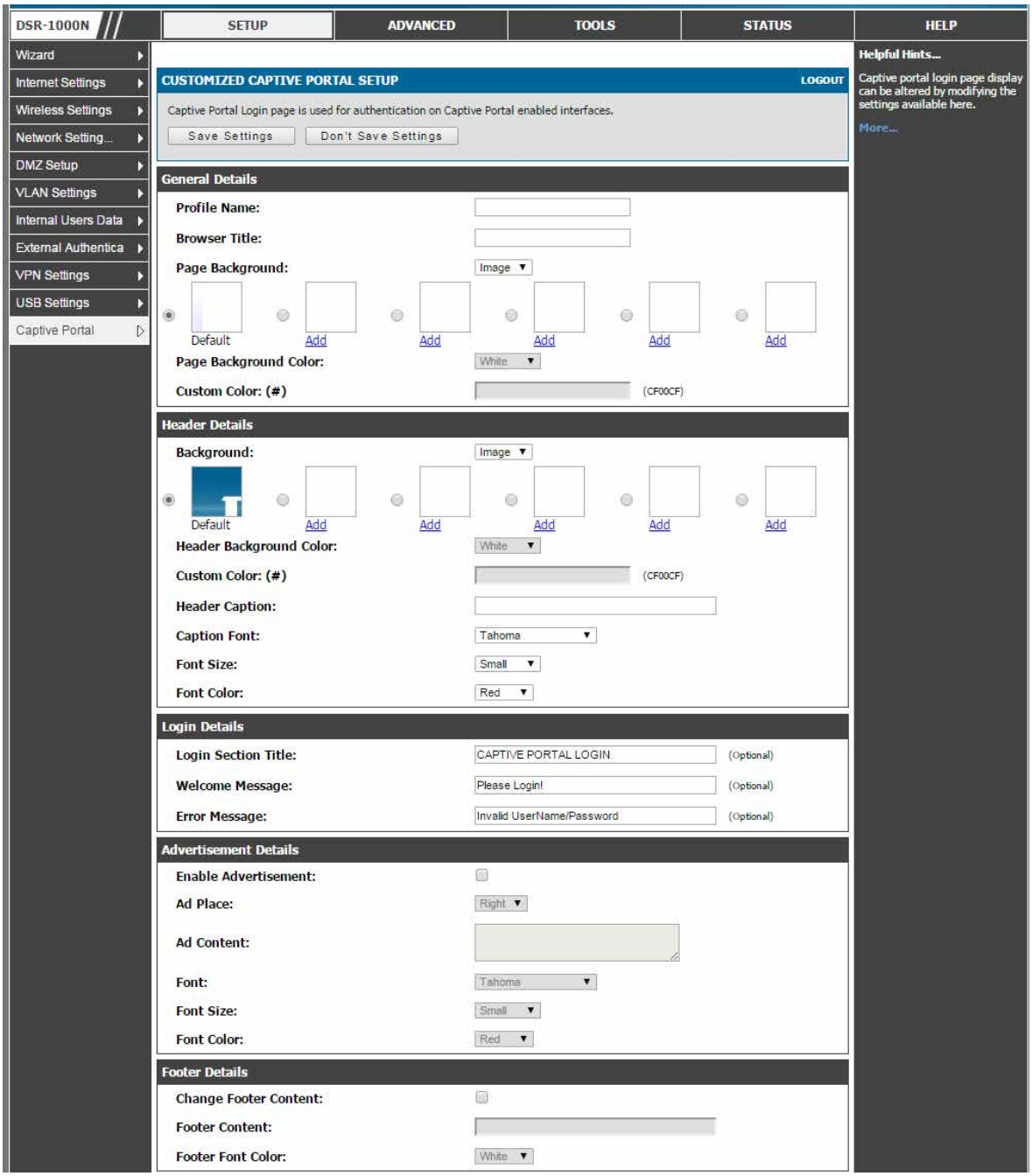


図 4-27　Captive Portal Setup 画面 - Add

2. キャプティブポータルログインページでは設定可能なパラメータを編集することで変更できます。

項目	説明
General Details	
Profile Name	追加するプロファイル名を設定します。
Browser Title	ブラウザタイトルを設定します。
Page Background Color	ページの背景色を設定します。
Custom Color	カスタム背景色を選択します。「Page Background Color」で「Custom」を選択すると入力できるようになります。

項目	説明
Header Details	
ページのヘッダ部分を表示する方法を設定します。	
Background	ヘッダ部分の背景を設定します。
Add	新しい画像を追加します。このプロファイルのヘッダイメージとして本画像を設定します。
Header Background Color	ヘッダ部分の背景色を設定します。
Custom Color	カスタムヘッダの背景色を選択します。「Header Background Color」で「Custom」を選択すると入力できるようになります。
Header Caption	ヘッダ部分に表示する文字列。
Caption Font	表示するヘッダ文字列のフォント。
Font Size	表示するヘッダ文字列のフォントサイズ。
Font Color	表示する文字列の色。
Login Details	
ページのログインエリア部分を表示する方法を設定します。	
Login Section Title	ログインボックスのタイトル。
Welcome Message	ユーザがページを参照した場合に表示するメッセージ。
Error Message	ユーザが無効の資格証明を入力した場合に表示するエラーメッセージ。
Advertisement Details	
Enable Advertisement	ログインページの通知を有効にします。ここでは、ユーザは「Captive Portal」ログインページに表示するのに必要とするカスタムメッセージ / 情報を設定できます。
Ad Place	表示する通知の場所（Right または Left）を選択します。
Ad Content	ログインページの通知内容を設定します。
Font	表示する情報のフォント。
Font Size	表示する情報のフォントサイズ。
Font Color	表示する情報の色。
Footer Details	
ページのフッタ部分を表示する方法を設定します。	
Change Footer Content	フッタ部分に表示する文字列を変更する場合にチェックします。
Footer Content	フッタ部分に表示する文字列。
Footer Font Color	表示するフッタの色。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

キャプティブポータルログインページの参照

1. 「List of Available Profiles」セクションで「Show Preview」ボタンをクリックします。

2. 以下のようにイメージが表示されます。

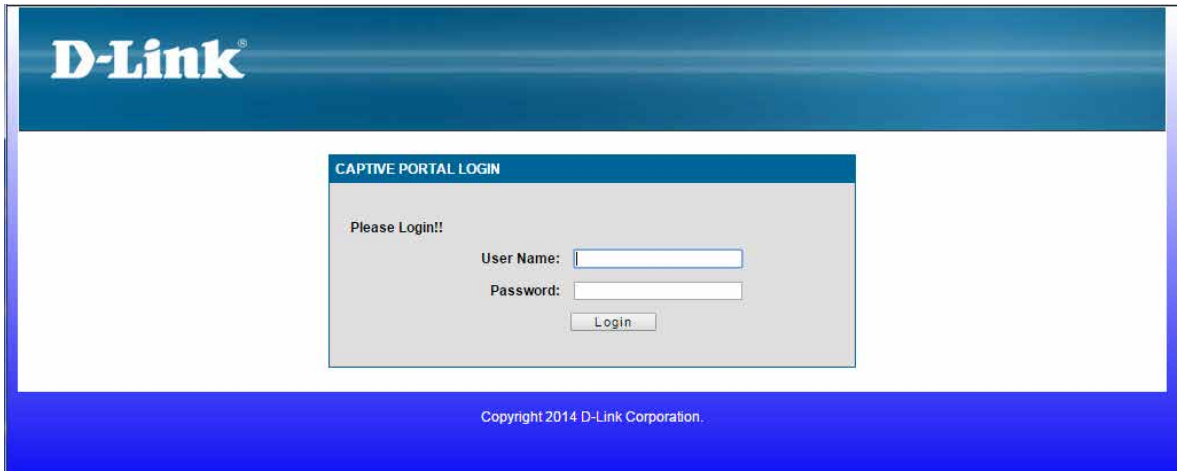


図 4-28　キャプティブポータルログインページのプレビュー画面

VLAN におけるキャプティブポータル

SETUP > VLAN Settings > VLAN Configuration メニュー

キャプティブポータルは、ポートベースで有効にします。キャプティブポータルを経由して特定の VLAN にあるホストを認証するように指定できます。これにより、他の VLAN と比較できるように固有の指示とブランド名を持つポータルとしてカスタマイズすることができます。この設定ページの最も重要なアスペクトは認証サーバを選択することです。選択したキャプティブポータル経由でインターネットアクセスを希望するすべてのユーザ（VLAN ホスト）が、選択したサーバ経由で認証されます。

1. **SETUP > VLAN Settings > VLAN Configuration** 順にメニューをクリックします。

2. 「VLAN CONFIGURATION」画面で「Add」ボタンをクリックして以下の画面を表示します。

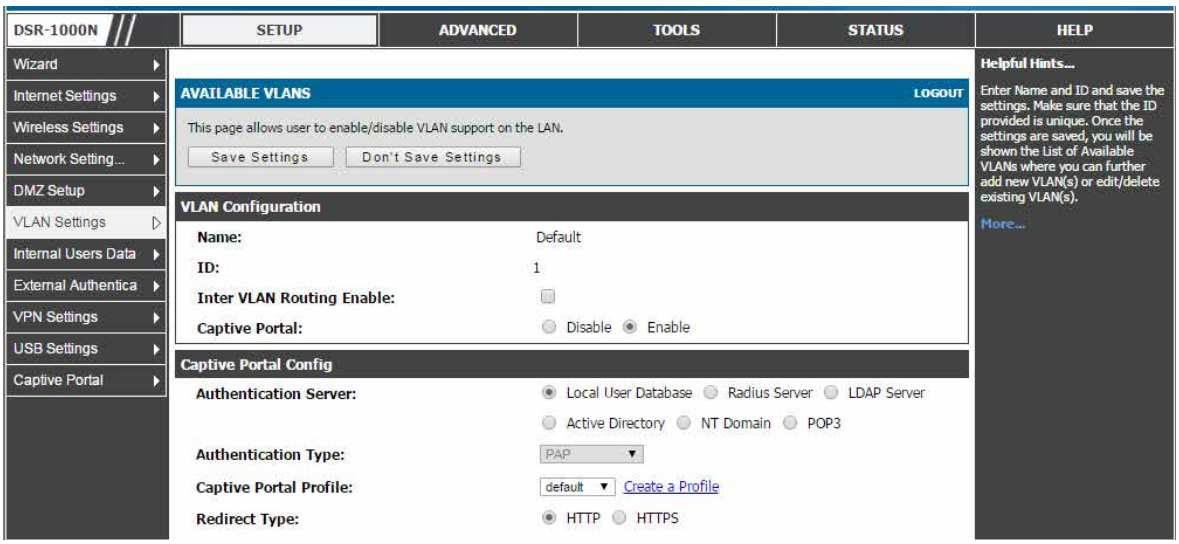


図 4-29　キャプティブポータルの VLAN ベースの設定

3. 「VLAN Configuration」セクションで「Captive Portal」に「Enable」を指定して、続く「Captive Portal Config」セクションを設定します。

4. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

注意　詳しくは「VLAN 設定」セクションをご参照ください。

第 5 章　インターネット接続（WAN 設定）

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

項目	説明	参照ページ
インターネットセットアップウィザード	インターネット接続のためのウィザードを使用します。	46 ページ
WAN 設定	手動の WAN 接続を行います。	49 ページ
帯域幅制御	帯域幅プロファイルにより WAN のトラフィックフローを制御します。	62 ページ
複数 WAN リンク機能	複数の WAN リンクにより接続の信頼性を向上します。	67 ページ
ルーティング設定	LAN、WAN 間のダイナミック / スタティックルーティングの設定を行います。	73 ページ
設定可能ポート - WAN オプション	セカンダリ WAN または DMZ ポートとして物理ポートを設定します。	83 ページ
WAN ポート設定	MTU、ポートスピードなどを WAN ポートに設定します。	83 ページ

このルータには、インターネットへの接続を確立するのに使用する 2 つの WAN ポートがあり、次の ISP 接続タイプをサポートしています : DHCP、Static、PPPoE、PPTP、または L2TP。

ご使用のインターネットサービスプロバイダ（ISP）を使用したインターネットサービスが手配されているものとします。ルータをセットアップするのに必要である設定情報については ISP またはネットワーク管理者にご確認ください。

インターネットセットアップウィザード

SETUP > Wizard > Internet > Internet Connection Setup Wizard メニュー
ご契約のインターネット接続のパスワード、タイムゾーン、および設定を変更するなどの一般的な設定タスクをウィザードを通して誘導します。

「Internet Connection Setup Wizard」はネットワークに慣れていないユーザに有効です。いくつかのわかりやすい設定ページを通じて ISP が提供する情報を設定することで、WAN 接続とご使用のネットワークにインターネットアクセスを有効にすることができます。

SETUP > Wizard > Internet の順にメニューをクリックし、以下の画面を表示します。

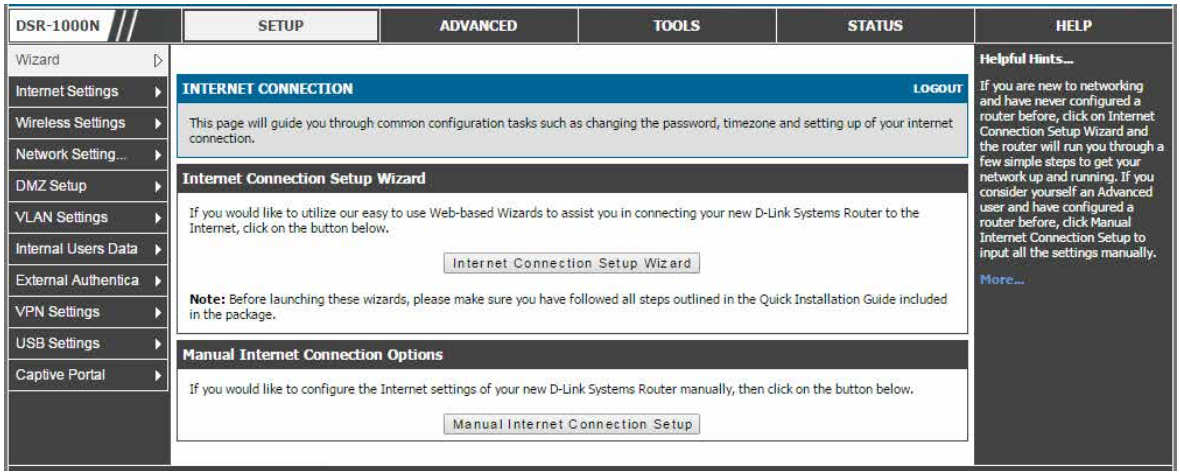


図 5-1　Internet Connection Setup Wizard

以下の手順で設定を行います。

1. ルータの管理者パスワードでログインすることによってウィザードを使用した設定を開始します。「Internet Connection Setup Wizard」ボタンをクリックして以下の画面を表示します。

図 5-2　Setup Wizard 画面 - 確認

最初に手順を確認して「Next」ボタンをクリックします。

2. パスワードの変更をします。

図 5-3　Setup Wizard 画面 - ルータパスワードの変更

「Next」ボタンをクリックします。

3. 位置しているタイムゾーンを設定します。

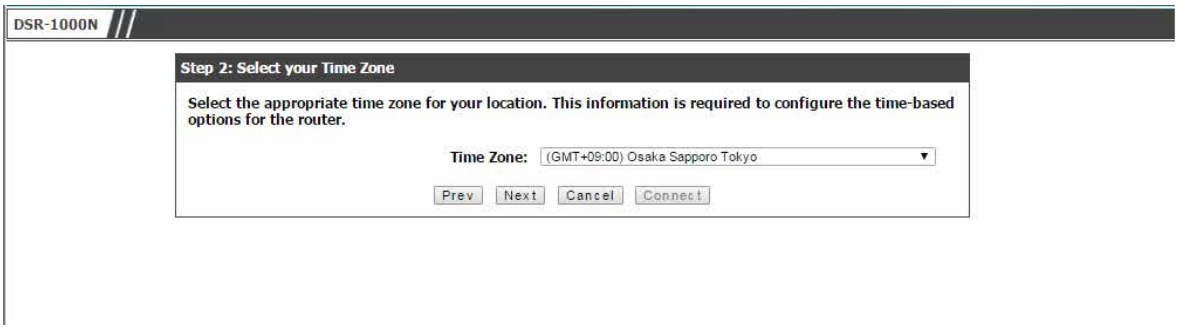


図 5-4　Setup Wizard 画面 - タイムゾーンの変更

「Next」ボタンをクリックします。

4. ISP の接続タイプを選択します。: DHCP、Static、PPPoE、PPTP または L2TP

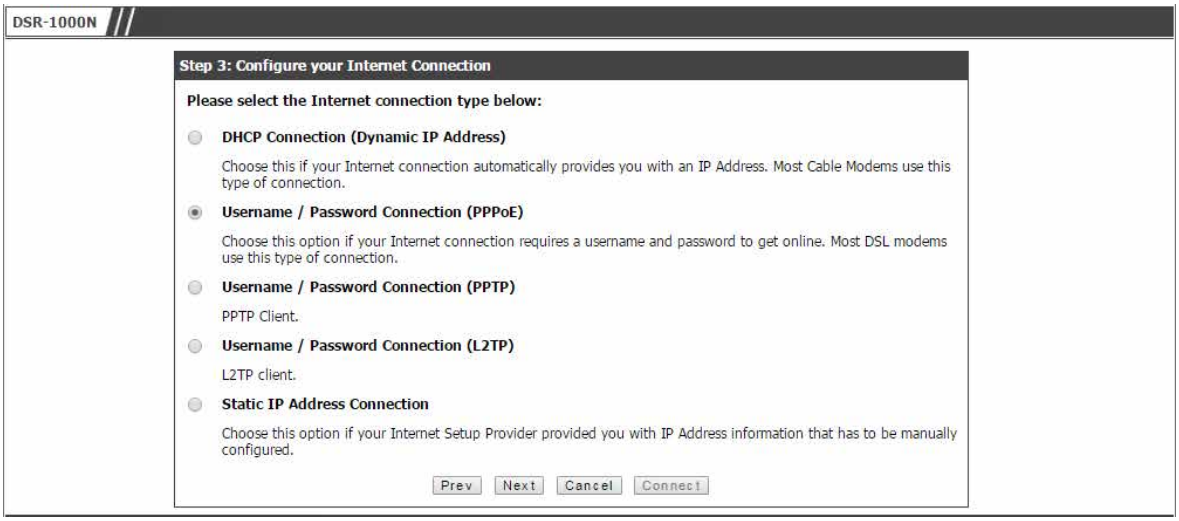


図 5-5　Setup Wizard 画面 - ISP 接続タイプの設定

接続タイプによっては、ユーザ名 / パスワードがこのルータへの ISP の登録に必要であるかもしれません。多くの場合、ISP がそのパラメータを指定しなければ、初期設定を使用できます。

「Next」ボタンをクリックします。

5. ISP の接続タイプごとの設定を行います。以下は PPPoE を選択した例です。

図 5-6　Setup Wizard 画面 - ISP 接続タイプに応じた設定（PPPoE）

「Next」ボタンをクリックします。

6. 最後に「Connect」ボタンをクリックし、ISP とのリンクの確立を確認します。

図 5-7　Setup Wizard 画面 - 完了

接続できることを確認後、このルータの他の機能を設定することができます。

WAN 設定

SETUP > Internet Settings > WAN1/2/3 Settings > WAN1/2/3 Setup メニュー
ここではインターネット接続を設定します。

注意 3G USB ドングルがサポートされていないため、日本では WAN3 は利用できません。

IP アドレス、アカウント情報などインターネット接続情報があることをあらかじめ確認してください。通常、この情報は ISP またはご使用のネットワーク管理者によって提供されます。

インターネット接続を有効にするためには、ルータが自動的に WAN 接続タイプを検出することを許可するか、以下の基本設定を手動で設定する必要があります。

項目	説明
ISP Connection Type	このルータのプライマリ WAN リンクに設定した ISP に基づいて、スタティック IP アドレス、DHCP クライアント、PPTP（Point-to-Point Tunneling Protocol）、PPPoE（Point-to-Point Protocol over Ethernet）、L2TP（Layer 2 Tunneling Protocol）を選択します。選択された ISP タイプに必要なフィールドが強調表示されます。ISP が必要であり、提供する以下の情報を入力します。:
PPPoE Profile Name	このメニューは、設定済みの PPPoE プロファイルを表示します。これは、複数の PPPoE 接続を設定する場合に特に便利です。（例 : 複数の PPPoE をサポートする日本の ISP）
ISP ログイン情報	これは PPTP と L2TP ISP に必要です。 • User Name • Password • Secret（L2TP にだけ必要）
MPPE Encryption	PPTP リンクのために、ご契約の ISP が MPPE（Microsoft Point-to-Point Encryption）を有効にするように要求する可能性があります。
Split Tunnel（PPTP および L2TP 接続でサポート）	スプリットトンネルが有効であると、DSR は ISP サーバからのデフォルトルートを予測できません。そのような場合、「Static Routing」ページでルーティングを設定することによって、手動でルーティングを処理する必要があります
Connectivity Type	いつも接続をオンに保つためには、「Keep Connected」をクリックします。接続がしばらくアイドル状態になった後にログアウトするためには、（ご契約の ISP コストがログオン時間に基づいている場合に役立ちます。）、「Idle Timeout」をクリックして、「Idle Time」フィールドに切断前に待機する時間（分）を入力します。
My IP Address	ISP が割り当てた IP アドレスを入力します。
Server IP Address	PPTP または L2TP の IP アドレスを入力します。

SETUP > Internet Settings > WAN1 Settings > WAN1 Setup の順にメニューをクリックし、以下の画面を表示します。

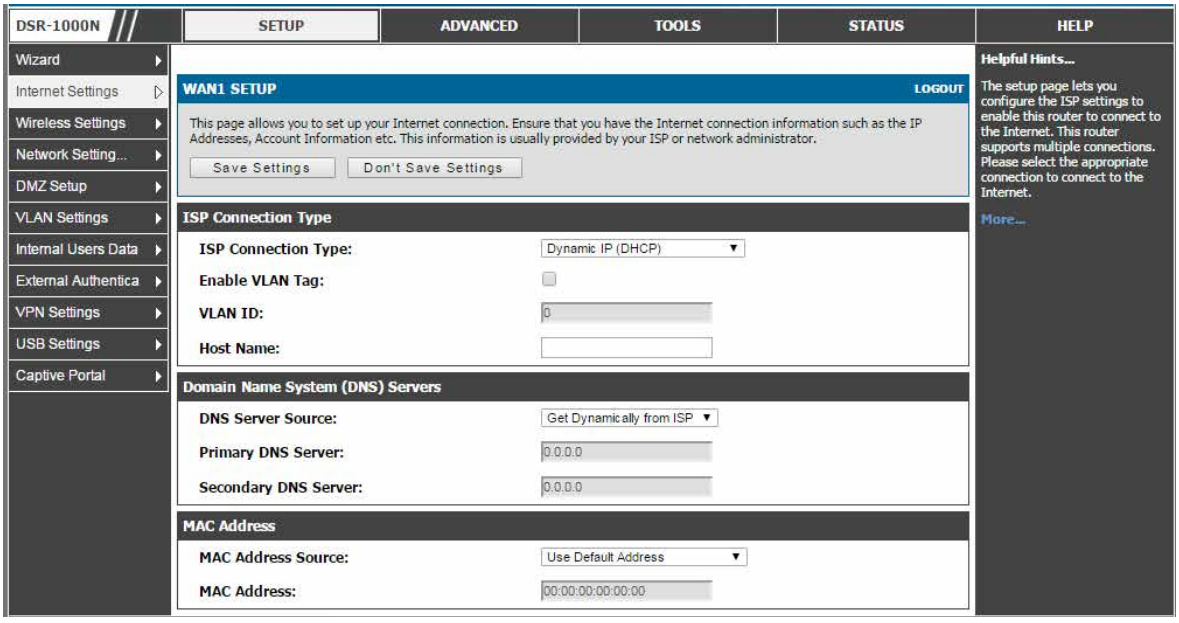


図 5-8　WAN SETUP 画面

「ISP Connection Type」（ISP への接続のタイプ）によって以下の項目を設定します。

Static IP（スタティック IP）

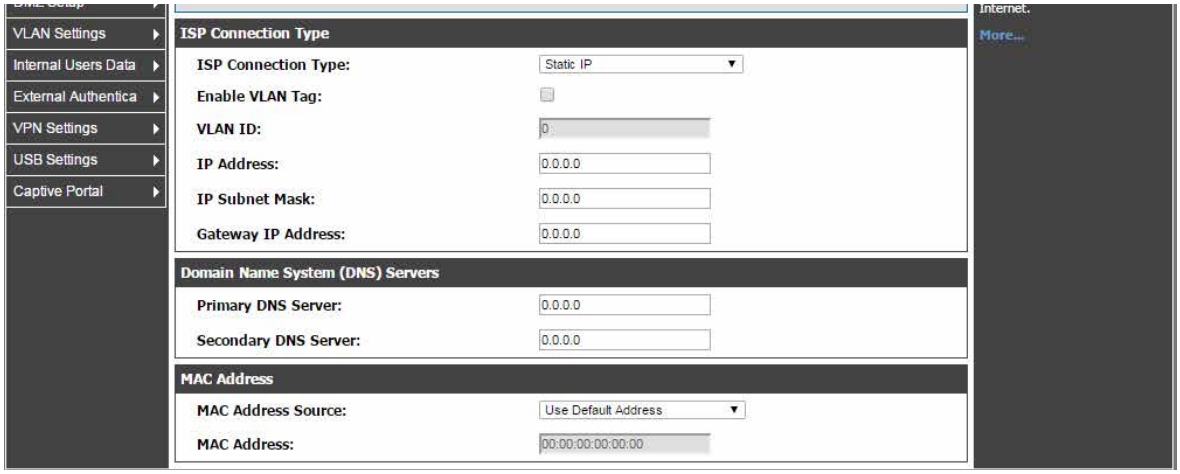


図 5-9　WAN 接続画面 - Static IP

以下の設定項目があります。

項目	説明
ISP Connection Type	
ISP Connection Type	「Static IP 」を選択します。
Enable VLAN Tag	チェックすると、VLAN タグが有効になります。
VLAN ID	「Enable VLAN Tag」を有効にした場合、VLAN ID を指定します。
IP Address	ご契約の ISP が割り当てたスタティック IP アドレスを入力します。
IP Subnet Mask	IPv4 サブネットマスクを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
Gateway IP Address	ISP のゲートウェイの IP アドレスを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
Domain Name System (DNS) Servers	
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。
MAC Address	
MAC Address Source	ご契約の ISP が MAC 認証を必要とし、別の MAC アドレスが以前に ISP に登録されていない場合には「Use Default Address」を選択します。 • Use Default Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Clone your PC's MAC Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Use this MAC Address - ISP が使用する MAC アドレスを割り当てた場合にこのオプションを選択します。また、以下の欄も入力します。
MAC Address	MAC アドレスを入力します。

Dynamic IP (DHCP)

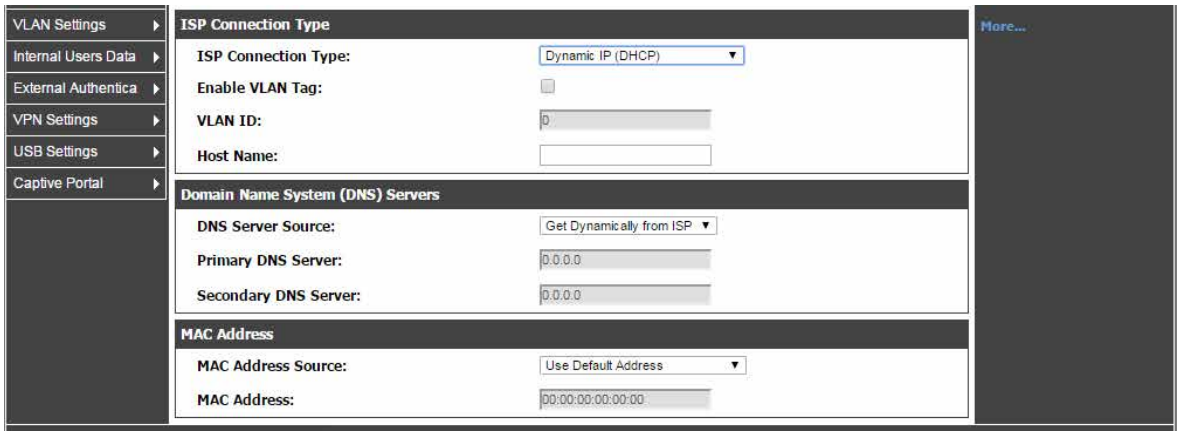


図 5-10　WAN 接続画面 - Dynamic IP

以下の設定項目があります。

項目	説明
ISP Connection Type	
ISP Connection Type	「Dynamic IP 」を選択します。
Enable VLAN Tag	チェックすると、VLAN タグが有効になります。
VLAN ID	「Enable VLAN Tag」を有効にした場合、VLAN ID を指定します。
Host Name	DHCP サーバに送信するためにホスト名オプションを指定します。
Domain Name System (DNS) Servers	
DNS Server Source	以下のオプションの 1 つを選択します。 • Get Dynamically from ISP - ISP がスタティックな DNS IP アドレスを割り当てなかった場合にこのオプションを選択します。 • Use These DNS Servers - ISP がスタティックな DNS IP アドレスを割り当てた場合にこのオプションを選択します。以下の欄を入力します。
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。
MAC Address	
MAC Address Source	ご契約の ISP が MAC 認証を必要とし、別の MAC アドレスが以前に ISP に登録されていない場合には「Use Default Address」を選択します。 • Use Default Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合に選択します。 • Clone your PC's MAC Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合に選択します。 • Use this MAC Address - ISP が使用する MAC アドレスを割り当てた場合に選択します。また、以下の欄も入力します。
MAC Address	MAC アドレスを入力します。

PPPoE

２つのタイプの PPPoE ISP（標準的なユーザ名 / パスワードの PPPoE および日本のマルチプル PPPoE）をサポートしています。

PPPoE (Username/Password)

標準的な ISP 用の PPPoE 設定です。多くの PPPoE ISP が単一の制御とデータ接続を使用しており、ISP ではログイン時に、DSR の認証に対してユーザ名 / パスワードを必要とします。この場合の ISP 接続のタイプは「PPPoE (Username/Password)」です。GUI は、PPPoE リンクを確立するために認証、サービス、および接続設定を求めます。

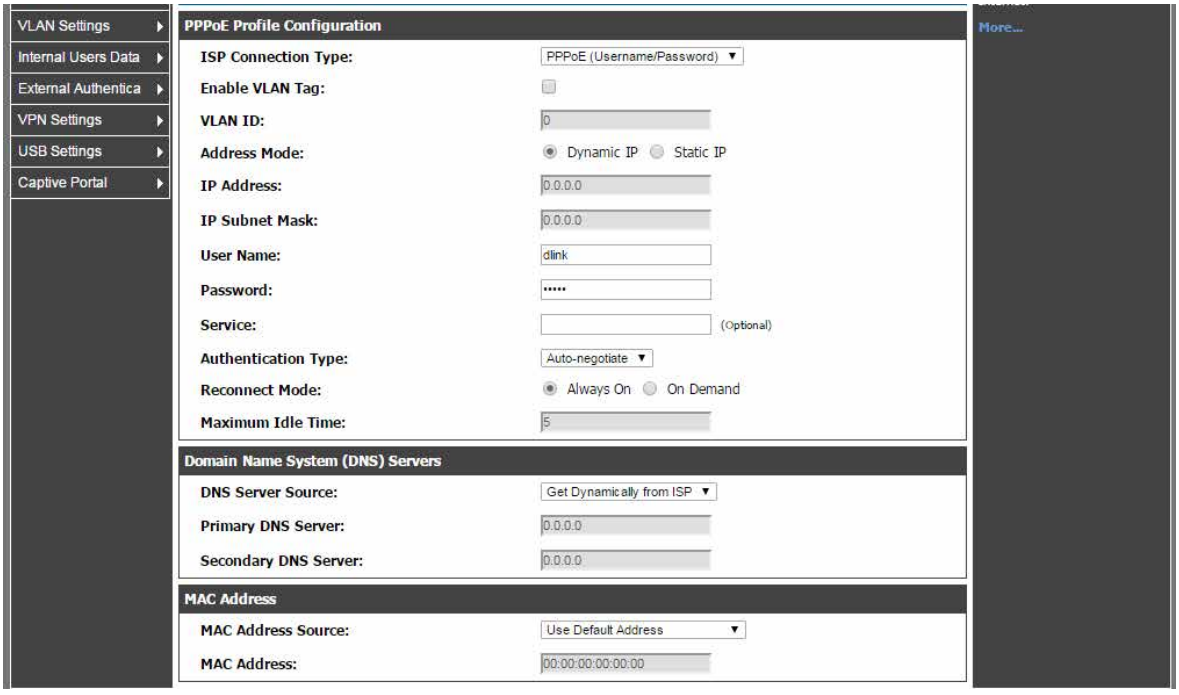


図 5-11　WAN 接続画面 - PPPoE

以下の設定項目があります。

項目	説明
PPPoE Profile Configuration	
ISP Connection Type	「PPPoE (Username/Password) 」を選択します。
Enable VLAN Tag	チェックすると、VLAN タグが有効になります。
VLAN ID	「Enable VLAN Tag」を有効にした場合、VLAN ID を指定します。
Address Mode	以下のオプションの 1 つを選択します。 • Dynamic IP - スタティック IP アドレスが割り当てられていない場合にこのオプションを選択します。ISP は DHCP ネットワークプロトコルを使用して IP アドレスを自動的に割り当てます。 • Static IP - ISP が固定の（スタティックまたはパーマネント）IP アドレスを割り当てた場合にこのオプションを選択します。以下の項目も設定します。
IP Address	ご契約の ISP が割り当てたスタティック IP アドレスを入力します。
IP Subnet Mask	IPv4 サブネットマスクを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
User Name	ISP へのログインに必要なユーザ名を入力します。
Password	ISP へのログインに必要なパスワードを入力します。
Service	同じユーザ名とパスワードの組合せを使用して 2 つのサーバを識別する必要がある場合にこの欄を使用します。PPP の場合、IP アドレスを使用してサーバを指定できない場合に、この欄を使用して接続する特定のサーバを指定できます。
Authentication Type	プロファイルが使用する認証タイプを指定します。（Auto-negotiate、PAP、CHAP、MS-CHAP、MS-CHAPv2）
Reconnect Mode	以下のオプションの 1 つを選択します。 • Always On - 接続は通常オンとなります。 • On Demand - 指定時間アイドル状態であると、接続は自動的に終了します。「Maximum Idle Time」欄に時間 (分) を入力します。この機能は、ご契約の ISP が接続時間に基づいて課金する場合に便利です。
Maximum Idle Time	アイドル時間の最大値を入力します。
Domain Name System (DNS) Servers	
DNS Server Source	以下のオプションの 1 つを選択します。 • Get Dynamically from ISP - ISP がスタティックな DNS IP アドレスを割り当てなかった場合にこのオプションを選択します。 • Use These DNS Servers - ISP がスタティックな DNS IP アドレスを割り当てた場合にこのオプションを選択します。以下の欄を入力します。
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。
MAC Address	
MAC Address Source	ご契約の ISP が MAC 認証を必要とし、別の MAC アドレスが以前に ISP に登録されていない場合には「Use Default Address」を選択します。 • Use Default Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Clone your PC's MAC Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Use this MAC Address - ISP が使用する MAC アドレスを割り当てた場合にこのオプションを選択します。また、以下の欄も入力します。
MAC Address	MAC アドレスを入力します。

Japanese multiple PPPoE

いくつかの ISP では、日本では非常に一般的である「Japanese Multiple PPPoE」の使用が、DSR と ISP 間でプライマリおよびセカンダリの PPPoE 接続を同時に確立するのに必要とされます。プライマリ接続は大量のデータおよびインターネットトラフィックに使用され、セカンダリ接続は DSR と ISP 間で特定の（制御）トラフィックを送信します。

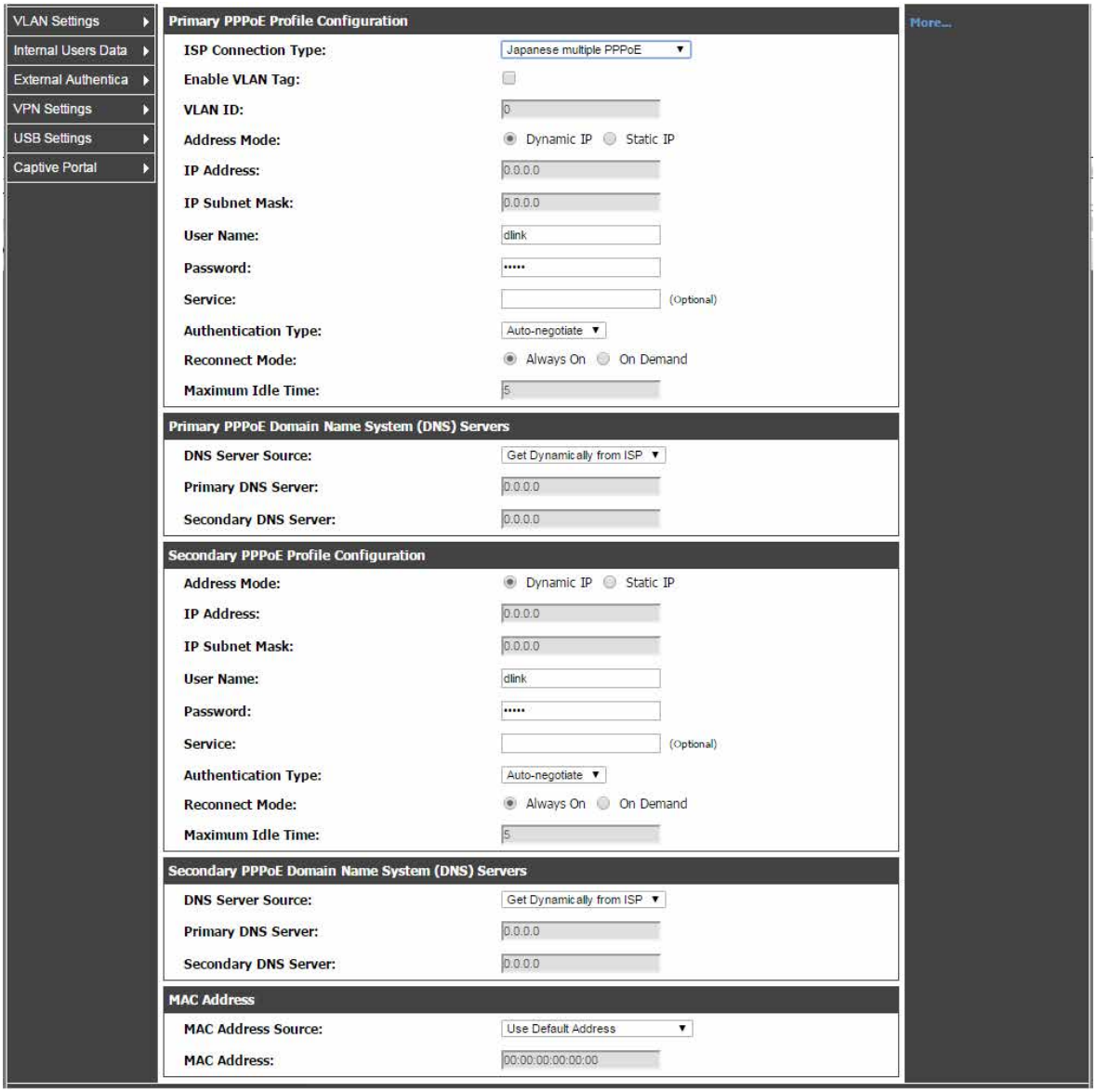


図 5-12　WAN 接続画面 - Japanese multiple PPPoE

以下の設定項目があります。

項目	説明
Primary PPPoE Profile Configuration	
ISP Connection Type	「Japanese multiple PPPoE」を選択します。
Enable VLAN Tag	チェックすると、VLAN タグが有効になります。
VLAN ID	「Enable VLAN Tag」を有効にした場合、VLAN ID を指定します。
Address Mode	以下のオプションの 1 つを選択します。 • Dynamic IP - スタティック IP アドレスが割り当てられていない場合にこのオプションを選択します。ISP は DHCP ネットワークプロトコルを使用して IP アドレスを自動的に割り当てます。 • Static IP - ISP が固定の（スタティックまたはパーマネント）IP アドレスを割り当てた場合にこのオプションを選択します。以下の項目も設定します。
IP Address	ご契約の ISP が割り当てたスタティック IP アドレスを入力します。
IP Subnet Mask	IPv4 サブネットマスクを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
User Name	ISP へのログインに必要なユーザ名を入力します。
Password	ISP へのログインに必要なパスワードを入力します。
Service	同じユーザ名とパスワードの組合せを使用して 2 つのサーバを識別する必要がある場合にこの欄を使用します。PPP の場合、IP アドレスを使用してサーバを指定できない場合に、この欄を使用して接続する特定のサーバを指定できます。
Authentication Type	プロファイルが使用する認証タイプを指定します。（Auto-negotiate、PAP、CHAP、MS-CHAP、MS-CHAPv2）
Reconnect Mode	以下のオプションの 1 つを選択します。 • Always On - 接続は通常オンとなります。 • On Demand - 指定時間アイドル状態であると、接続は自動的に終了します。「Maximum Idle Time」欄に時間 (分) を入力します。この機能は、ご契約の ISP が接続時間に基づいて課金する場合に便利です。
Maximum Idle Time	アイドル時間の最大値を入力します。
Primary PPPoE Domain Name System (DNS) Servers	
DNS Server Source	以下のオプションの 1 つを選択します。 • Get Dynamically from ISP - ISP がスタティックな DNS IP アドレスを割り当てなかった場合にこのオプションを選択します。 • Use These DNS Servers - ISP がスタティックな DNS IP アドレスを割り当てた場合にこのオプションを選択します。以下の欄を入力します。
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。
Secondary PPPoE Profile Configuration	
Address Mode	以下のオプションの 1 つを選択します。 • Dynamic IP - スタティック IP アドレスが割り当てられていない場合にこのオプションを選択します。ISP は DHCP ネットワークプロトコルを使用して IP アドレスを自動的に割り当てます。 • Static IP - ISP が固定の（スタティックまたはパーマネント）IP アドレスを割り当てた場合にこのオプションを選択します。以下の項目も設定します。
IP Address	ご契約の ISP が割り当てたスタティック IP アドレスを入力します。
IP Subnet Mask	IPv4 サブネットマスクを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
User Name	ISP へのログインに必要なユーザ名を入力します。
Password	ISP へのログインに必要なパスワードを入力します。
Service	同じユーザ名とパスワードの組合せを使用して 2 つのサーバを識別する必要がある場合にこの欄を使用します。PPP の場合、IP アドレスを使用してサーバを指定できない場合に、この欄を使用して接続する特定のサーバを指定できます。
Authentication Type	プロファイルが使用する認証タイプを指定します。（Auto-negotiate、PAP、CHAP、MS-CHAP、MS-CHAPv2）
Reconnect Mode	以下のオプションの 1 つを選択します。 • Always On - 接続は通常オンとなります。 • On Demand - 指定時間アイドル状態であると、接続は自動的に終了します。「Maximum Idle Time」欄に時間 (分) を入力します。この機能は、ご契約の ISP が接続時間に基づいて課金する場合に便利です。
Maximum Idle Time	アイドル時間の最大値を入力します。
Secondary PPPoE Domain Name System (DNS) Servers	
DNS Server Source	以下のオプションの 1 つを選択します。 • Get Dynamically from ISP - ISP がスタティックな DNS IP アドレスを割り当てなかった場合にこのオプションを選択します。 • Use These DNS Servers - ISP がスタティックな DNS IP アドレスを割り当てた場合にこのオプションを選択します。以下の欄を入力します。
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。

項目	説明
MAC Address	
MAC Address Source	ご契約の ISP が MAC 認証を必要とし、別の MAC アドレスが以前に ISP に登録されていない場合には「Use Default Address」を選択します。 • Use Default Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Clone your PC's MAC Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Use this MAC Address - ISP が使用する MAC アドレスを割り当てた場合にこのオプションを選択します。また、以下の欄も入力します。
MAC Address	MAC アドレスを入力します。

マルチプル PPPoE 接続には以下に示す主要な要素があります。:
- プライマリとセカンダリ接続は同時に行われます。
- 各セッションにはドメイン名索引のための DNS サーバソースがあるか、ISP でこれを割り当てることができるか、または GUI を通して設定済みです。
- DSR は LAN ユーザ用 DNS プロキシとして動作します。
- 明確に、セカンダリ接続のドメイン名（例 : *.flets）を特定する HTTP 要求だけが、このセカンダリ PPPoE 端末を通して利用可能なコンテンツにアクセスするのにセカンダリプロファイルを使用します。他の HTTP/HTTPS 要求のすべてがプライマリ PPPoE 接続を通過します。

日本のマルチプル PPPoE が設定されて、セカンダリ接続が起動する場合、いくつかの定義済みルートがそのインタフェースに追加されます。これらのルートが様々なサービスを主催する ISP の内部ドメインにアクセスするために必要とされます。また、**ADVANCED > Routing > Static Routing** の「STATIC ROUTING」ページを通してこれらのルートを設定することもできます。

PPTP (Username/Password)

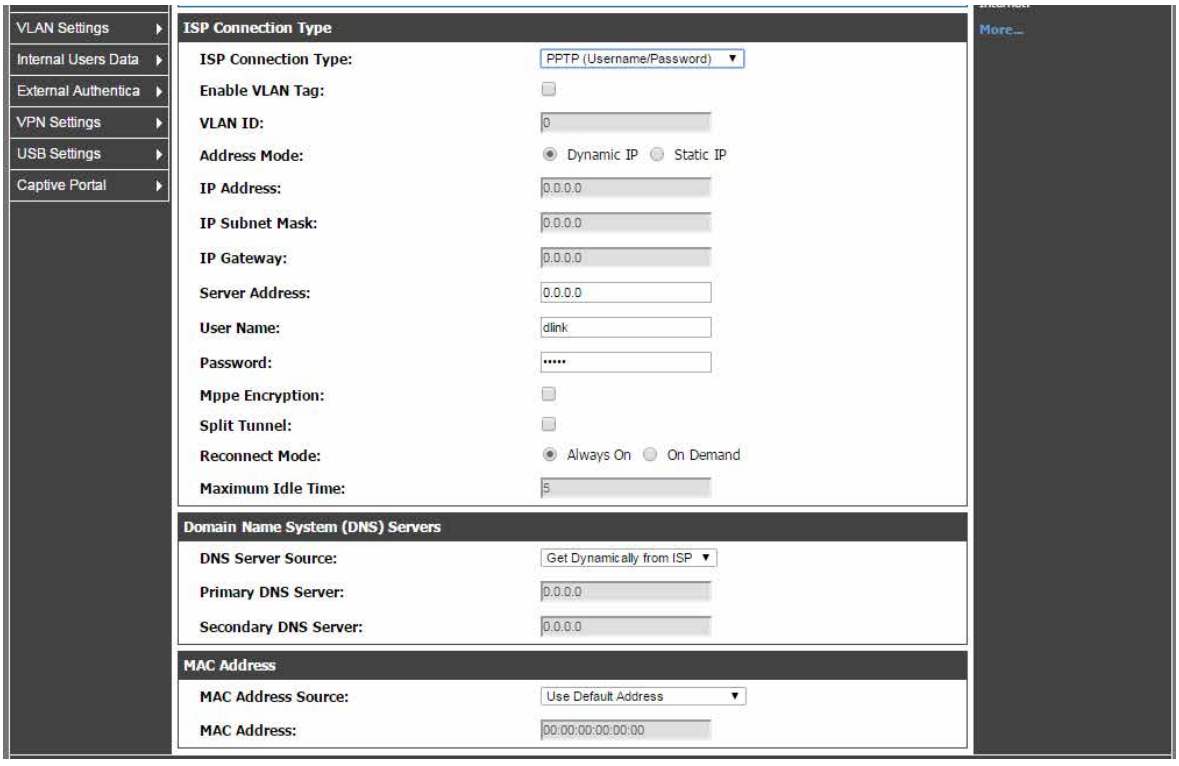


図 5-13　WAN 接続画面 - PPTP

以下の設定項目があります。

項目	説明
ISP Connection Type	
ISP Connection Type	「PPTP」を選択します。
Enable VLAN Tag	チェックすると、VLAN タグが有効になります。
VLAN ID	「Enable VLAN Tag」を有効にした場合、VLAN ID を指定します。
Address Mode	以下のオプションの 1 つを選択します。 • Dynamic IP - スタティック IP アドレスが割り当てられていない場合にこのオプションを選択します。ISP は DHCP ネットワークプロトコルを使用して IP アドレスを自動的に割り当てます。 • Static IP - ISP が固定の（スタティックまたはパーマネント）IP アドレスを割り当てた場合にこのオプションを選択します。以下の項目も設定します。
IP Address	ご契約の ISP が割り当てたスタティック IP アドレスを入力します。
IP Subnet Mask	IPv4 サブネットマスクを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
IP Gateway	ご契約の ISP が割り当てたゲートウェイアドレスを入力します。
Server Address	PPTP サーバの IP アドレスまたはドメイン名を入力します。
User Name	ISP へのログインに必要なユーザ名を入力します。
Password	ISP へのログインに必要なパスワードを入力します。
Mppe Encryption	PPTP サーバが MPPE 暗号化をサポートする場合にチェックします。
Split Tunnel	このオプションは PPTP および L2TP にだけ有効です。有効にすると、ゲートウェイ IP アドレスの追加をできないようにしますが、代わりに LAN トラフィックを送信するために特定のルートを追加する必要があります。
Reconnect Mode	以下のオプションの 1 つを選択します。 • Always On - 接続は通常オンとなります。 • On Demand - 指定時間アイドル状態であると、接続は自動的に終了します。「Maximum Idle Time」欄に時間 (分) を入力します。この機能は、ご契約の ISP が接続時間に基づいて課金する場合に便利です。
Maximum Idle Time	アイドル時間の最大値を入力します。
Domain Name System (DNS) Servers	
DNS Server Source	以下のオプションの 1 つを選択します。 • Get Dynamically from ISP - ISP がスタティックな DNS IP アドレスを割り当てなかった場合にこのオプションを選択します。 • Use These DNS Servers - ISP がスタティックな DNS IP アドレスを割り当てた場合にこのオプションを選択します。以下の欄を入力します。
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。
MAC Address	
MAC Address Source	ご契約の ISP が MAC 認証を必要とし、別の MAC アドレスが以前に ISP に登録されていない場合には「Use Default Address」を選択します。 • Use Default Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Clone your PC's MAC Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Use this MAC Address - ISP が使用する MAC アドレスを割り当てた場合にこのオプションを選択します。また、以下の欄も入力します。
MAC Address	MAC アドレスを入力します。

L2TP (Username/Password)

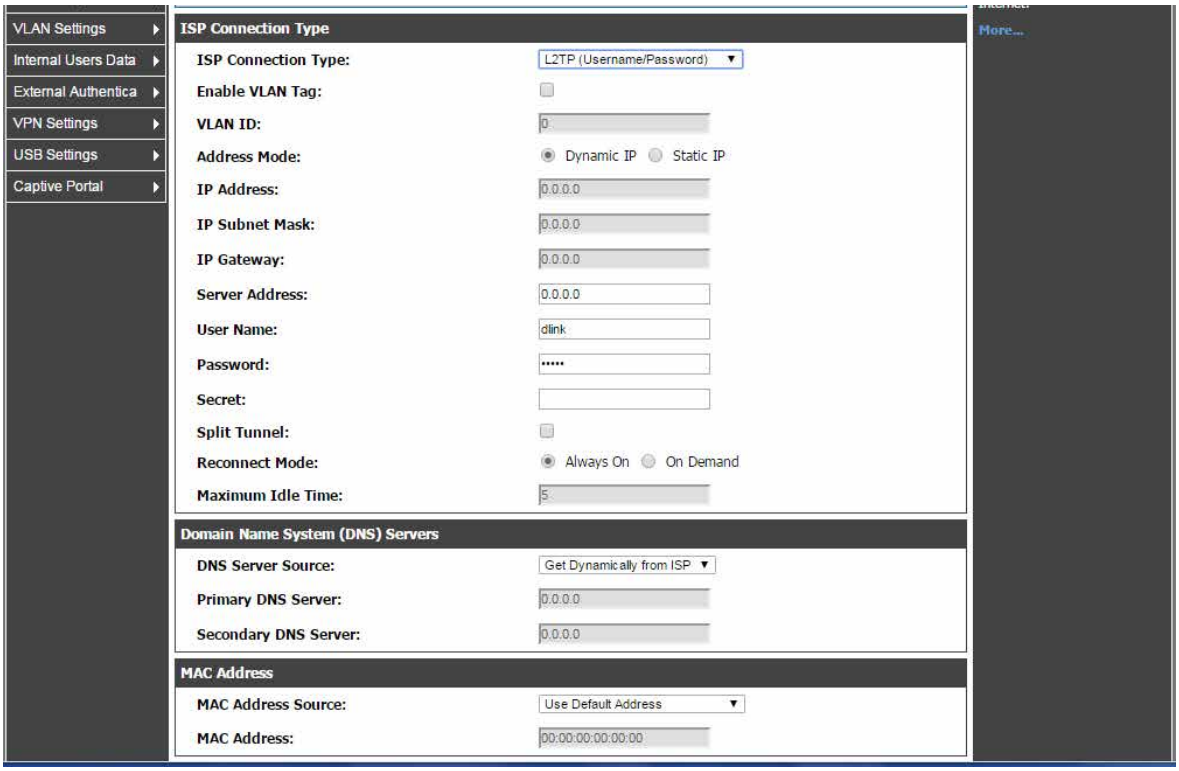


図 5-14　WAN 接続画面 - L2TP

以下の設定項目があります。

項目	説明
ISP Connection Type	
ISP Connection Type	「L2TP (Username/Password)」を選択します。
Enable VLAN Tag	チェックすると、VLAN タグが有効になります。
VLAN ID	「Enable VLAN Tag」を有効にした場合、VLAN ID を指定します。
Address Mode	以下のオプションの 1 つを選択します。 • Dynamic IP - スタティック IP アドレスが割り当てられていない場合にこのオプションを選択します。ISP は DHCP ネットワークプロトコルを使用して IP アドレスを自動的に割り当てます。 • Static IP - ISP が固定の（スタティックまたはパーマネント）IP アドレスを割り当てた場合にこのオプションを選択します。以下の項目も設定します。
IP Address	ご契約の ISP が割り当てたスタティック IP アドレスを入力します。
IP Subnet Mask	IPv4 サブネットマスクを入力します。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
IP Gateway	ご契約の ISP が割り当てたゲートウェイアドレスを入力します。
Server Address	L2TP サーバの IP アドレスまたはドメイン名を入力します。
User Name	ISP へのログインに必要なユーザ名を入力します。
Password	ISP へのログインに必要なパスワードを入力します。
Secret	シークレットフレーズを入力して、サーバ（L2TP 接続のみ）にログインします。
Split Tunnel	このオプションは PPTP および L2TP にだけ有効です。有効にすると、ゲートウェイ IP アドレスの追加をできないようにしますが、代わりに LAN トラフィックを送信するために特定のルートを追加する必要があります。
Reconnect Mode	以下のオプションの 1 つを選択します。 • Always On - 接続は通常オンとなります。 • On Demand - 指定時間アイドル状態であると、接続は自動的に終了します。「Maximum Idle Time」欄に時間（分）を入力します。この機能は、ご契約の ISP が接続時間に基づいて課金する場合に便利です。
Maximum Idle Time	アイドル時間の最大値を入力します。
Domain Name System (DNS) Servers	
DNS Server Source	以下のオプションの 1 つを選択します。 • Get Dynamically from ISP - ISP がスタティックな DNS IP アドレスを割り当てなかった場合にこのオプションを選択します。 • Use These DNS Servers - ISP がスタティックな DNS IP アドレスを割り当てた場合にこのオプションを選択します。以下の欄を入力します。
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。

項目	説明
MAC Address	
MAC Address Source	ご契約の ISP が MAC 認証を必要とし、別の MAC アドレスが以前に ISP に登録されていない場合には「Use Default Address」を選択します。 • Use Default Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Clone your PC's MAC Address - ルータを設定するために使用しているコンピュータの MAC アドレスを割り当てる場合にこのオプションを選択します。 • Use this MAC Address - ISP が使用する MAC アドレスを割り当てた場合にこのオプションを選択します。また、以下の欄も入力します。
MAC Address	MAC アドレスを入力します。

WAN ポート IP アドレス

ご契約の ISP はダイナミック（ログインするたびに新しく生成する）、またはスタティック（永久）な IP アドレスを割り当てます。「IP Address Source」オプションでは、アドレスが ISP によってスタティックに提供されるべきであるか、または各ログインの時にダイナミックに受信するべきかを定義することができます。スタティックである場合は、IP アドレス、IPv4 サブネットマスク、および ISP ゲートウェイの IP アドレスを入力します。PPTP および L2TP は設定するスタティック IP アドレスとサブネットを提供することもできますが、初期値では、ISP からその情報をダイナミックに受信するものとしています。

WAN DNS サーバ

WAN Domain Name Servers（DNS）の IP アドレスは通常 ISP からダイナミックに提供されますが、いくつかの場合、DNS サーバのスタティック IP アドレスを定義できます。DNS サーバは IP アドレスにインターネットドメイン名（例 : www.google.com）をマップします。「Domain Name System（DNS）Server」セクションの「DNS Server Source」で「Get Dynamically from ISP」（ご契約の ISP から自動的に DNS サーバアドレスを取得する）、または「Use These DNS Servers」（ISP の指定したアドレスを使用する）をクリックします。後者の場合、プライマリおよびセカンダリ DNS サーバのアドレスを入力します。接続性の問題を回避するためには、確実に正しいアドレスを入力してください。

DHCP WAN

DHCP クライアント接続のために、ISP に登録するルータの MAC アドレスを選択することができます。いくつかの場合、ISP がその LAN ホストを使用して登録する際に LAN ホストの MAC アドレスのクローンを作る必要があるかもしれません。「MAC Address」セクションで設定します。

IPv6 ネットワークにおける WAN 設定

ADVANCED > IPv6 > IPv6 WAN1 / 2 Config メニュー

ここでは IPv6 の関連する WAN1/WAN2 設定を行うことができます。

IPv6 WAN 接続のために、DHCPv6 クライアントとして設定する場合、このルータはスタティックな IPv6 アドレスを持つか、または接続情報を受信することができます。ISP がインターネットにアクセスするために固定アドレスを割り当てる場合には、スタティックな構成設定を完了する必要があります。ご使用のルータに割り当てられた IPv6 アドレスに加えて、ISP で定義された IPv6 プレフィックス長が必要とされます。デフォルト IPv6 ゲートウェイアドレスは、このルータがインターネットにアクセスするために接続する ISP のサーバです。インターネットアドレスの解決のために ISP の IPv6 ネットワークにおけるプライマリおよびセカンダリ DNS サーバが使用され、これらはスタティック IP アドレスとプレフィックス長と共に ISP から提供されます。

DHCP を通して ISP が WAN IP 設定の取得を許可する場合、ご使用の DHCPv6 クライアント構成の詳細を提供する必要があります。ゲートウェイ上の DHCPv6 クライアントをステートレスまたはステートフルとすることができます。ステートフルクライアントが選択されると、ゲートウェイはアドレスのリースのために ISP の DHCPv6 サーバに接続します。ステートレスの DHCP では、ISP で利用可能な DHCPv6 サーバは必要なくて、ICMPv6 検出メッセージがこのゲートウェイから生成されて、自動設定に使用されます。また、優先される DHCPv6 サーバの IP アドレスとプレフィックス長を指定する 3 番目のオプションがさらに利用可能となります。

1. **ADVANCED > IPv6 > IPv6 WAN1 Config** の順にメニューをクリックし、以下の画面を表示します。

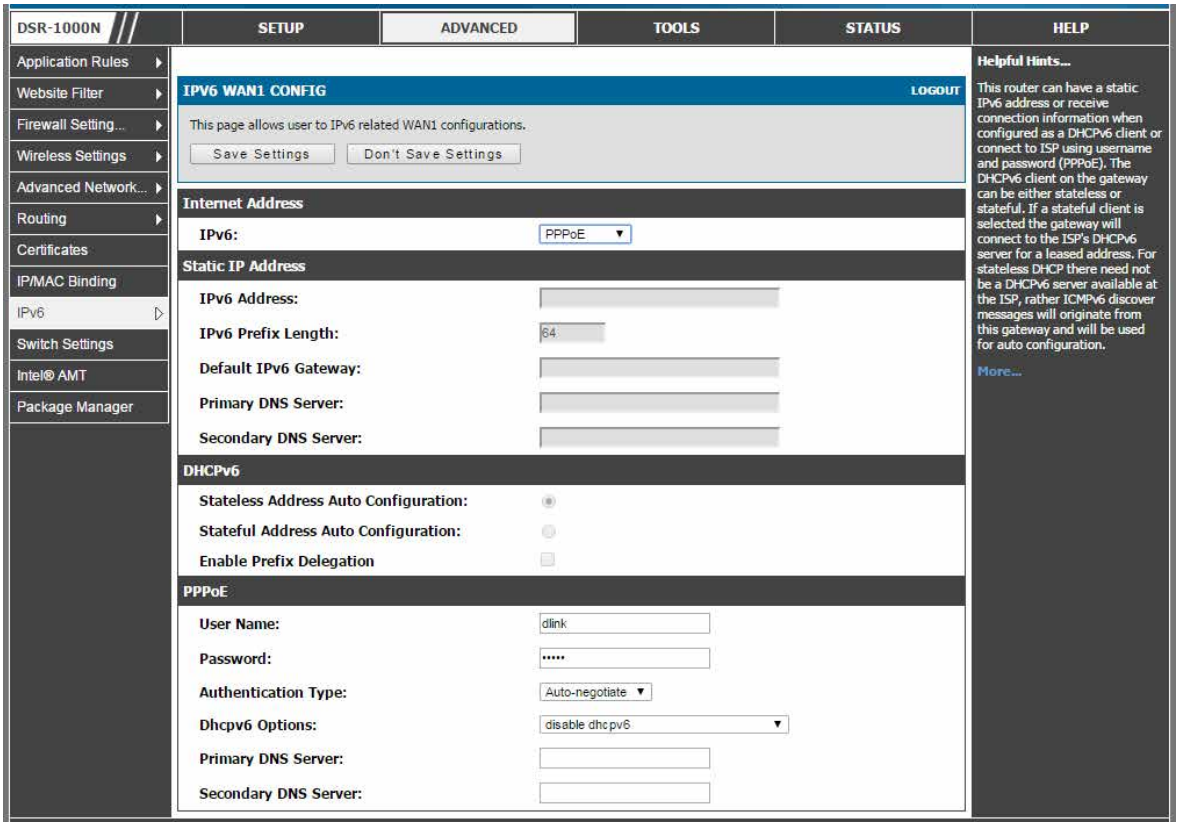


図 5-15　IPv6 WAN セットアップページ

2. 以下の項目を設定します。

項目	説明
Internet Address	
IPv6	DHCPv6 / Static IPv6 / PPPoE から選択します。 スタティック IP アドレスが ISP から割り当てられていない場合、「DHCPv6」を選択します。DHCP サーバは、DHCP ネットワークプロトコルを使用して IPv6 アドレスを自動的に割り当てます。ISP が固定の（スタティックまたはパーマネント）IP アドレスを割り当てた場合、「Static IPv6」を選択して、続く項目を設定します。
Static IP Address	
IPv6 が「Static IPv6」タイプの場合、以下の PPPoE フィールドが有効です。	
IPv6 Address	割り当てられたスタティック IPv6 アドレス。これはご契約の ISP に対してルータを特定します。
IPv6 Prefix Length	IPv6 ネットワーク（サブネット）はプレフィックスと呼ばれるアドレスの開始ビットにより特定されます。ネットワーク内のすべてのホストには、それらの IPv6 アドレスに同じ開始ビットがあります。ネットワークアドレスの一般的な開始ビット番号はプレフィックス長フィールドによって設定されます。
Default IPv6 Gateway	ISP ゲートウェイの IPv6 アドレス。通常、これは ISP またはご使用のネットワーク管理者によって提供されます。
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレス。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレス。
DHCPv6	
ISP が DHCPv6 である場合、ゲートウェイへの適切なアドレスを取得するために 2 つの方法があります。	
Stateless Address Auto Configuration	アドレスの割り当てにルータの通知を使用します。IPv6 RADVD プロトコルが DHCPv6 クライアントとしてこのルータを通知するために有効にされます。
Stateful Address Auto Configuration	ISP で利用可能などの DHCPv6 サーバからも IPv6 アドレスを要求します。
Prefix Delegation	このオプションを選択して、ISP で利用可能な DHCPv6 サーバからルータに通知プレフィックスを要求し、取得したプレフィックスは LAN 側に通知されたプレフィックスに更新されます。本オプションは DHCPv6 クライアントのステートレスアドレス自動設定モードでのみ選択されます。
PPPoE	
IPv6 が「PPPoE」タイプの場合、以下の PPPoE フィールドが有効です。	
Username	ISP へのログインに必要なユーザ名を入力します。
Password	ISP へのログインに必要なパスワードを入力します。
Authentication Type	プロファイルが使用する認証タイプ : Auto-negotiate/PAP/CHAP/MS-CHAP/MS-CHAPv2
Dhcpv6 Options	DHCPv6 クライアントのモードはこのモードで始まります。: disable DHCPv6 / stateless DHCPv6 / stateful DHCPv6/ Stateless dhcpv6 with Prefix delegation
Primary DNS Server	有効なプライマリ DNS サーバの IP アドレスを入力します。
Secondary DNS Server	有効なセカンダリ DNS サーバの IP アドレスを入力します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

WAN ステータスのチェック

SETUP > Internet Settings > WAN1 /2 /3 Settings > WAN1 /2 /3 Status メニュー

ここでは WAN1 / WAN2 インタフェースに関する現在の情報を表示します。また、情報に従って、インターネット接続を有効または無効にすることができます。

各 WAN ポートについて以下のような主な接続ステータス情報を参照することができます。

- 接続時間
- 接続タイプ : Dynamic IP または Static IP
- 接続状態 : WAN が ISP に接続しているかどうかを示します。「Link State」は WAN が適所で物理的な WAN 接続をしているかどうかを示します。WAN 接続状態がダウンしていても Link State は UP（例 : ケーブルが挿入されている）となります。
- IP アドレス / サブネットマスク
- ゲートウェイ IP アドレス

1. **SETUP > Internet Settings > WAN1 Settings > WAN1 Status** の順にメニューをクリックし、以下の画面を表示します。

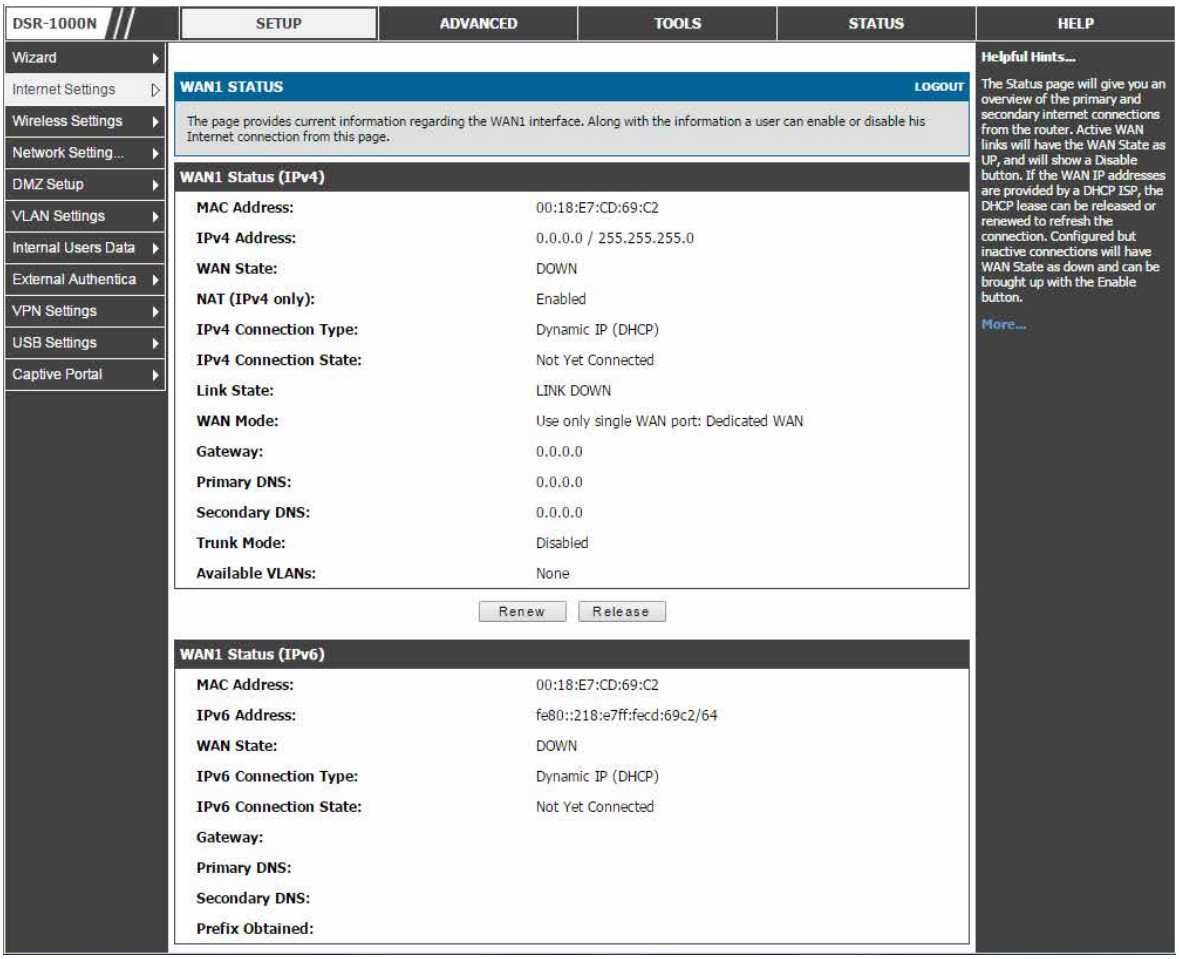


図 5-16　WAN ポートに関する接続ステータスの情報

2. WAN リンクを「Enable」/「Disable」ボタンをクリックして有効または無効にすることができます。ISP からダイナミックに受信する WAN 設定では、必要に応じてリンクパラメータを「Renew」（更新）または「Release」（解放）することができます。

帯域幅制御

帯域幅プロファイルの作成

ADVANCED > Advanced Network > Traffic Management > Bandwidth Profiles メニュー

ここでは設定済みの帯域幅プロファイルのリストを表示します。これらのプロファイルをトラフィックセレクタと共に使用することができます。

帯域幅プロファイルにより、LAN から WAN1 または WAN2 へのトラフィックフローを規制できます。これは、低優先度の LAN ユーザ（ゲストまたは HTTP サービス）がコスト節減または帯域幅優先度割り当ての目的で利用可能な WAN の帯域幅を占有しないことを保証するために役に立ちます。

帯域幅プロファイル設定では GUI からの帯域幅制御機能の有効化と制御パラメータを定義するプロファイルの追加を行います。次に、プロファイルはトラフィックセレクタに関連付けできます。そのため、帯域幅プロファイルは、セレクタと照合するトラフィックに適用されます。セレクタは、定義済みの帯域規制を起動する IP アドレスまたはサービスのような要素です。

1. **ADVANCED > Advanced Network > Traffic Management > Bandwidth Profiles** の順にメニューをクリックし、以下の画面を表示します。

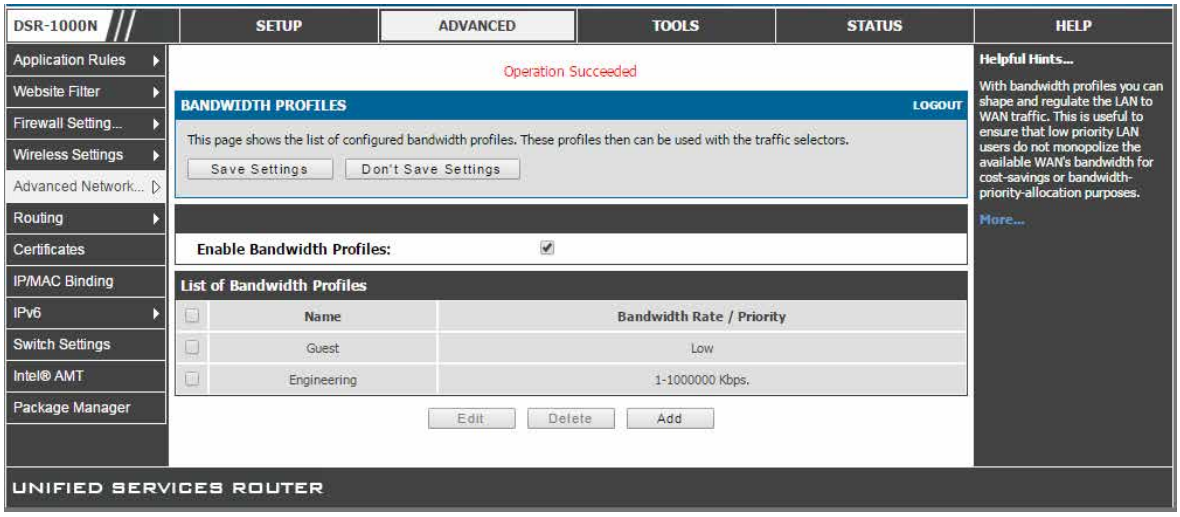


図 5-17　設定済み帯域幅プロファイルのリスト

2. 帯域幅プロファイルを有効にするためには、「Enable Bandwidth Profiles」をチェックして、「Save Settings」ボタンをクリックします。

新しい帯域幅プロファイルの作成

1. 「List of Bandwidth Profiles」で「Add」ボタンをクリックして以下の画面を表示します。

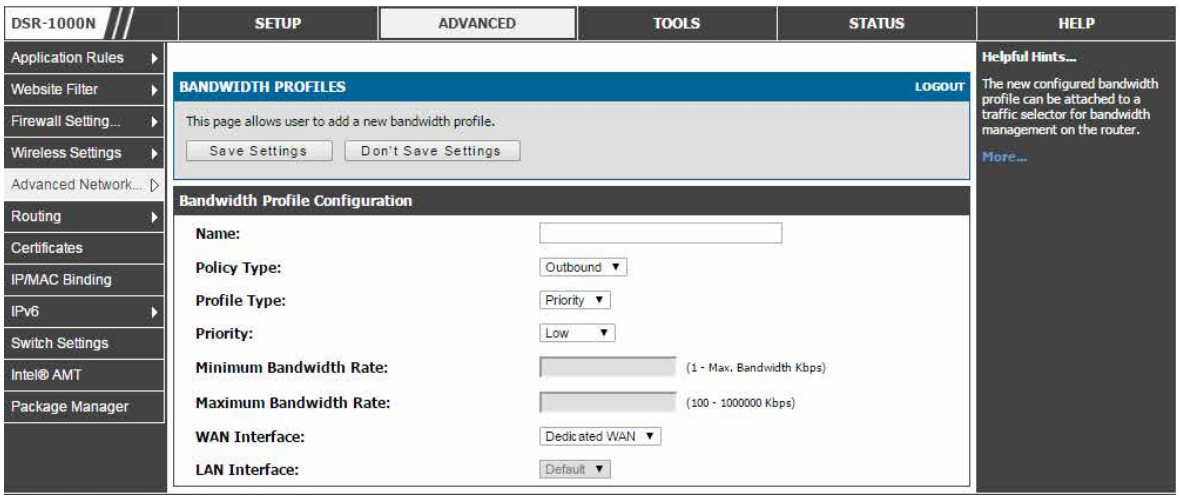


図 5-18　帯域幅プロファイル設定ページ

2. 以下の設定パラメータは、帯域幅プロファイルを定義するのに使用されます。:

項目	説明
Name	この識別子は、設定したプロファイルをトラフィックセレクタに関連付けるために使用されます。
Policy Type	「Outbound」（外向き）または「Inbound」（内向き）を選択します。
Profile Type	「Priority」（優先度）または「Rate」（レート）を使用した帯域幅の制限を選択することができます。
Priority	優先度使用する場合、「Low」（低）、「High」（高）、「Medium」（中）から選択できます。トラフィックセレクタ A に関連付けられた低優先度プロファイルとトラフィックセレクタ B に関連付けられた高優先度プロファイルがある場合、WAN 帯域幅割り当ての優先度はトラフィックセレクタ B のパケットに対するものとなります。
Minimum / Maximum Bandwidth Rate	より細やかな制御のために、「Profile Type」に「Rate」プロファイルタイプを選択した場合に使用できます。本オプションを使用して、このプロファイルが許可する最小および最大の帯域幅を制限できます。
WAN Interface	「Policy Type」が「Outbound」の場合にプロファイルを関連付ける WAN インタフェースを選択します。
LAN Interface	「Policy Type」が「Inbound」の場合にプロファイルを関連付ける LAN インタフェースを選択します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

トラフィックセレクタの設定

ADVANCED > Advanced Network > Traffic Management > Traffic Selectors メニュー

ここではトラフィックセレクタのリストを表示します。トラフィックセレクタはユーザが帯域幅プロファイルの割り当てを行えるサービスベースのルールです。

プロファイルを作成すると、次に、LAN から WAN までのトラフィックフローに関連付けられます。

1. **ADVANCED > Advanced Network > Traffic Management > Traffic Selectors** の順にメニューをクリックし、以下の画面を表示します。

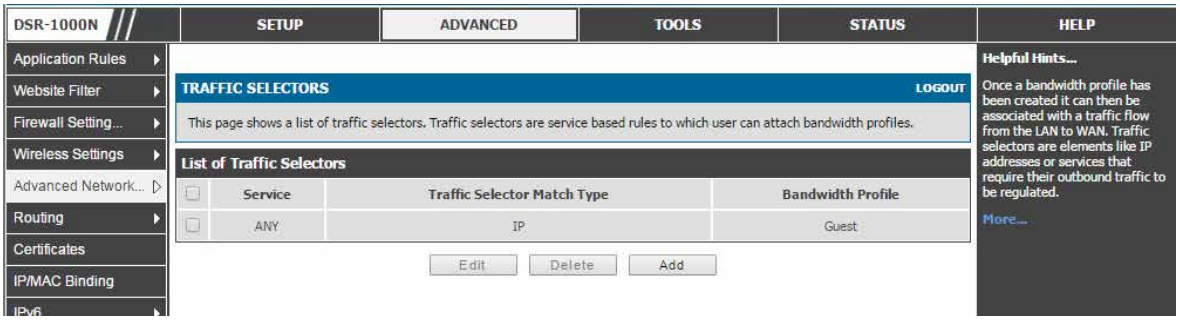


図 5-19　トラフィックセレクタのリスト

トラフィックセレクタの作成

1. 「Add」ボタンをクリックし、以下の画面を表示します。

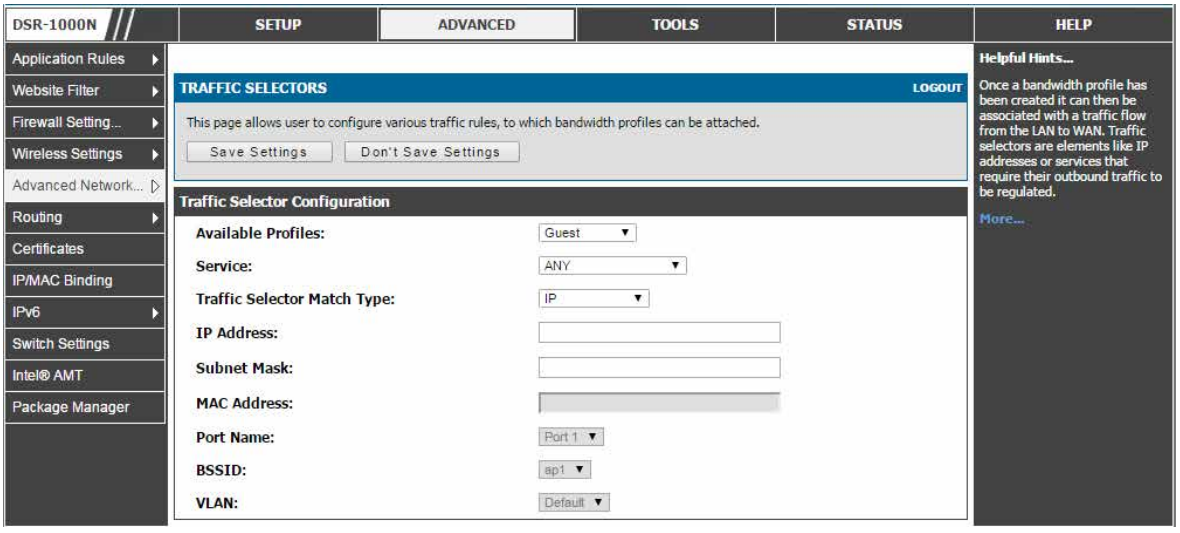


図 5-20　トラフィックセレクタの設定画面

2. トラフィックセレクタ設定は、以下の設定を使用して LAN トラフィックのタイプまたは送信元に帯域幅プロファイルを割り当てます。:

項目	説明
Available profiles	定義済み帯域幅プロファイルの 1 つを割り当てます。
Service	選択した帯域幅の規則を LAN から特定サービス（例 FTP）に適用させることができます。希望するサービスが見つからない場合、**ADVANCED > Firewall Settings > Custom Services** ページを通じてカスタムサービスを設定することができます。
Traffic Selector Match Type	帯域幅プロファイルを適用する場合にフィルタするパラメータ（IP、MAC Address、Port Name、VLAN または BSSID）を定義します。LAN 上の指定マシンは、IP アドレスまたは MAC アドレス経由で識別されます。または、プロファイルを LAN ポートまたは VLAN グループに適用します。さらに、帯域幅シェーピングのために BSSID によって無線ネットワークを選択することができます。選択したタイプにより、続く項目を設定します。すべての IP アドレスまたは特定のサブネットからサービスを制限するためには、内向きのトラフィックを規制するように IP アドレスと共にサブネットマスクフィールドを設定することができます。
IP Address	「Traffic Selector Match Type」に「IP」を選択した場合、LAN ホストの IP アドレスを入力します。
MAC Address	「Traffic Selector Match Type」に「MAC Address」を選択した場合、有効な MAC アドレスを入力します。
Port Name	「Traffic Selector Match Type」に「Port Name」を選択した場合、LAN ポート番号を選択します。
BSSID	「Traffic Selector Match Type」に「BSSID」を選択した場合、BSSID を選択します。
VLAN	「Traffic Selector Match Type」に「VLAN」を選択した場合、VLAN を選択します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ブリッジモードの帯域幅制御

トラフィック管理はクラシカルまたは NAT ルーティングモードに適用します。システムがブリッジモード（LAN1 と WAN2/DMZ ポートが同じネットワークにある）である場合、トラフィック管理の主な要素はブリッジのポート部分で有効なトラフィックタイプと帯域幅です。

帯域幅プロファイルでは、標準的なクラシカル / NAT ルーティングモードと比較されるブリッジモード内で有効なオプションの主な違いは、インタフェースオプションが適用されないことです。このプロファイルだけがブリッジネットワークに適用できるため、特定の外向きまたは内向きインタフェースと帯域幅プロファイルのアソシエーションはありません。同様に、ブリッジモードのトラフィックセレクタは、ブリッジネットワークに適用しないという概念であるため、ポート / SSID / VLAN 内の主な要素とはなりません。

ブリッジ帯域幅プロファイルの作成

ADVANCED > Advanced Network > Traffic Management > Bridge Bandwidth Profiles メニュー

ここでは設定済みのブリッジ帯域幅プロファイルのリストを表示します。これらのプロファイルをブリッジトラフィックセレクタと共に使用することができます。

1. **ADVANCED > Advanced Network > Traffic Management > Bridge Bandwidth Profiles** の順にメニューをクリックし、以下の画面を表示します。

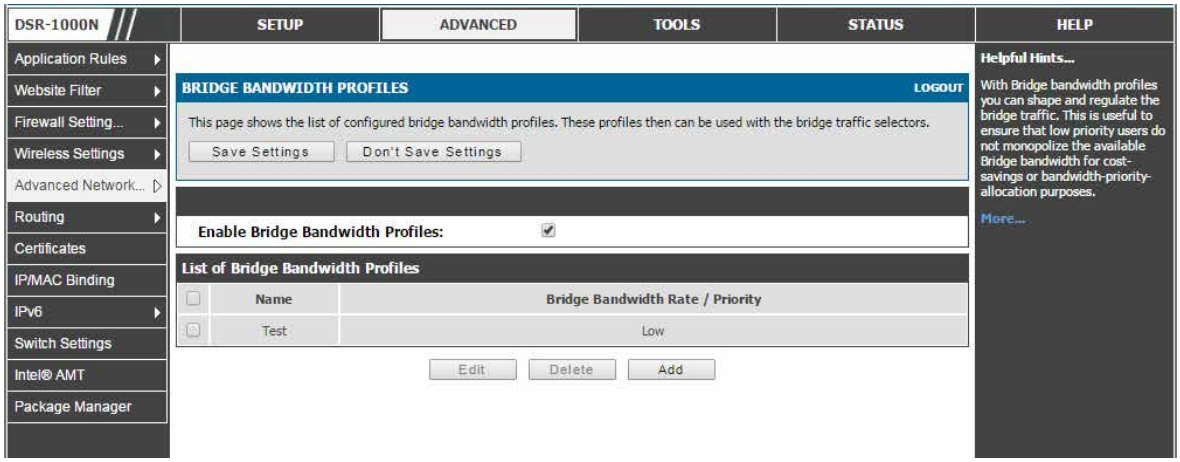


図 5-21　設定済みブリッジ帯域幅プロファイルのリスト

2. 帯域幅プロファイルを有効にするためには、「Enable Bridge Bandwidth Profiles」をチェックして、「Save Settings」ボタンをクリックします。

新しいブリッジ帯域幅プロファイルの作成

1. 「List of Bridge Bandwidth Profiles」で「Add」ボタンをクリックして以下の画面を表示します。

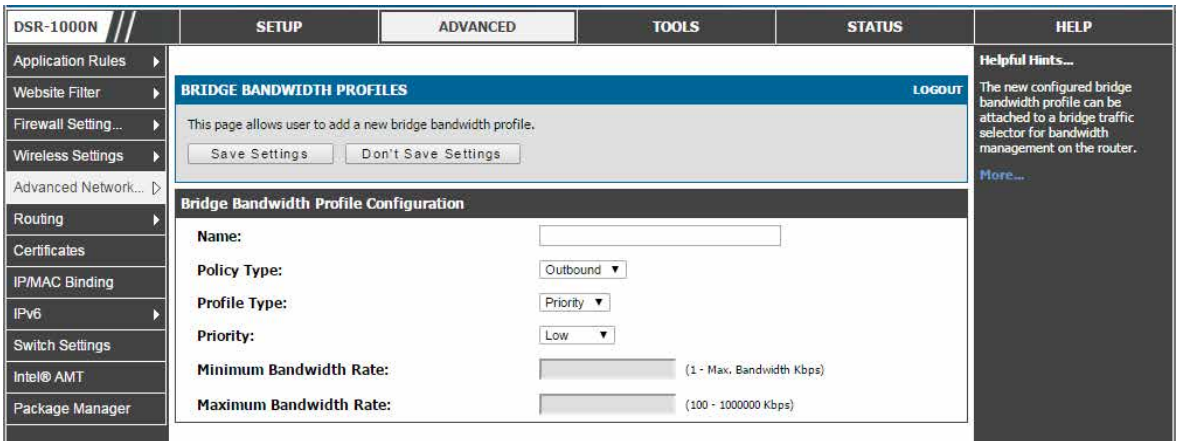


図 5-22　BRIDGE BANDWIDTH PROFILES 画面

2. 以下の設定項目を使用して、ブリッジ帯域幅プロファイルを定義します。

項目	説明
Name	設定したプロファイルをブリッジトラフィックセレクタに関連付けるために使用する識別子です。
Policy Type	「Outbound」（外向き）または「Inbound」（内向き）を選択します。
Profile Type	「Priority」（優先度）または「Rate」（レート）を使用したブリッジ帯域幅の制限を選択することができます。
Priority	プロファイルタイプが「Priority」の場合、「Low」、「Medium」、または「High」から選択します。
Minimum Bandwidth Rate	プロファイルタイプが「Rate」の場合、最小帯域幅レート (Kbps) を指定します。
Maximum Bandwidth Rate	プロファイルタイプが「Rate」の場合、最大帯域幅レート (Kbps) を指定します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ブリッジトラフィックセレクタの設定

ADVANCED > Advanced Network > Traffic Management > Bridge Traffic Selectors メニュー

ブリッジトラフィックセレクタのリストを表示します。ブリッジトラフィックセレクタはユーザがブリッジ帯域幅プロファイルの割り当てを行えるサービスベースのルールです。

プロファイルを作成すると、次に、LAN から WAN までのトラフィックフローに関連付けられます。

1. **ADVANCED > Advanced Network > Traffic Management > Bridge Traffic Selectors** の順にメニューをクリックし、以下の画面を表示します。

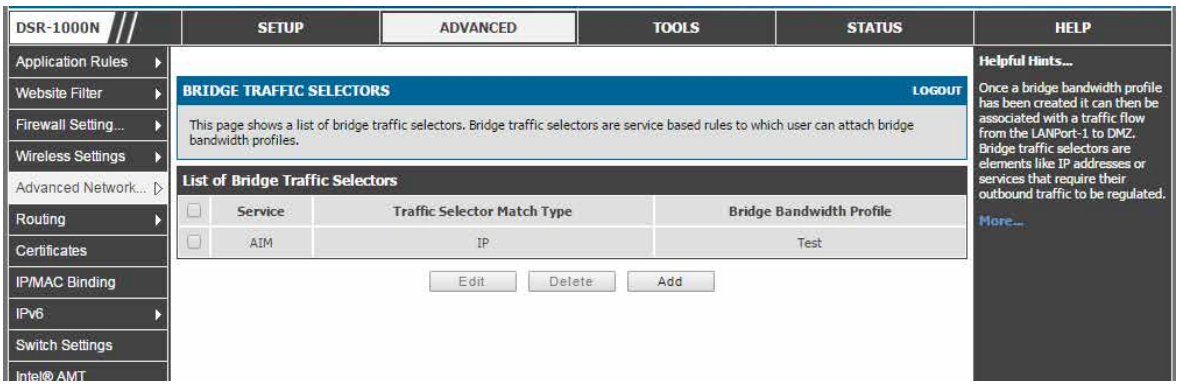


図 5-23　トラフィックセレクタのリスト

ブリッジトラフィックセレクタの作成

1. 「Add」ボタンをクリックし、以下の画面を表示します。

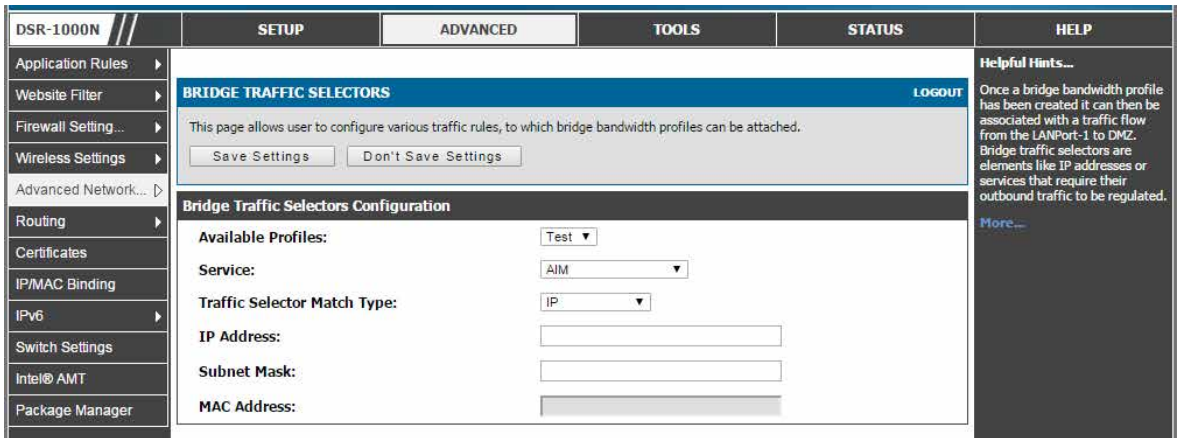


図 5-24　ブリッジトラフィックセレクタの設定画面

2. ブリッジトラフィックセレクタ設定は、以下の設定を使用して LAN トラフィックのタイプまたは送信元にブリッジ帯域幅プロファイルを割り当てます。

項目	説明
Available profiles	定義済みブリッジ帯域幅プロファイルの 1 つを割り当てます。
Service	選択したブリッジ帯域幅の規則を LAN から特定サービス（例 FTP）に適用させることができます。
Traffic Selector Match Type	照合タイプを選択します。
IP Address	「Traffic Selector Match Type」に「IP」を選択した場合、LAN ホストの IP アドレスを入力します。
MAC Address	「Traffic Selector Match Type」に「MAC Address」を選択した場合、有効な MAC アドレスを入力します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

複数 WAN リンク機能

このルータは複数 WAN リンクをサポートしています。これは、ポートの 1 つに不安定な WAN 接続がある場合に特定のインターネットに依存するサービスを優先することを保証するフェイルオーバとロードバランシング機能の長所を利用することができます。

SETUP > Internet Settings > WAN Mode メニュー
インターネット接続用の 2 つの WAN ポートにポリシーを設定することができます。

フェイルオーバまたはロードバランシングを使用するためには、WAN リンク障害検知を設定する必要があります。これは、インターネット上の DNS サーバへのアクセスまたはインターネットアドレスへの ping（ユーザ定義）に関係します。必要であれば、リンクが切断している思われる場合にリトライ回数を設定することができます。または、WAN ポートがダウンしているかどうかを判断する障害のしきい値を設定することができます。

1. **SETUP > Internet Settings > WAN Mode** の順にメニューをクリックし、以下の画面を表示します。

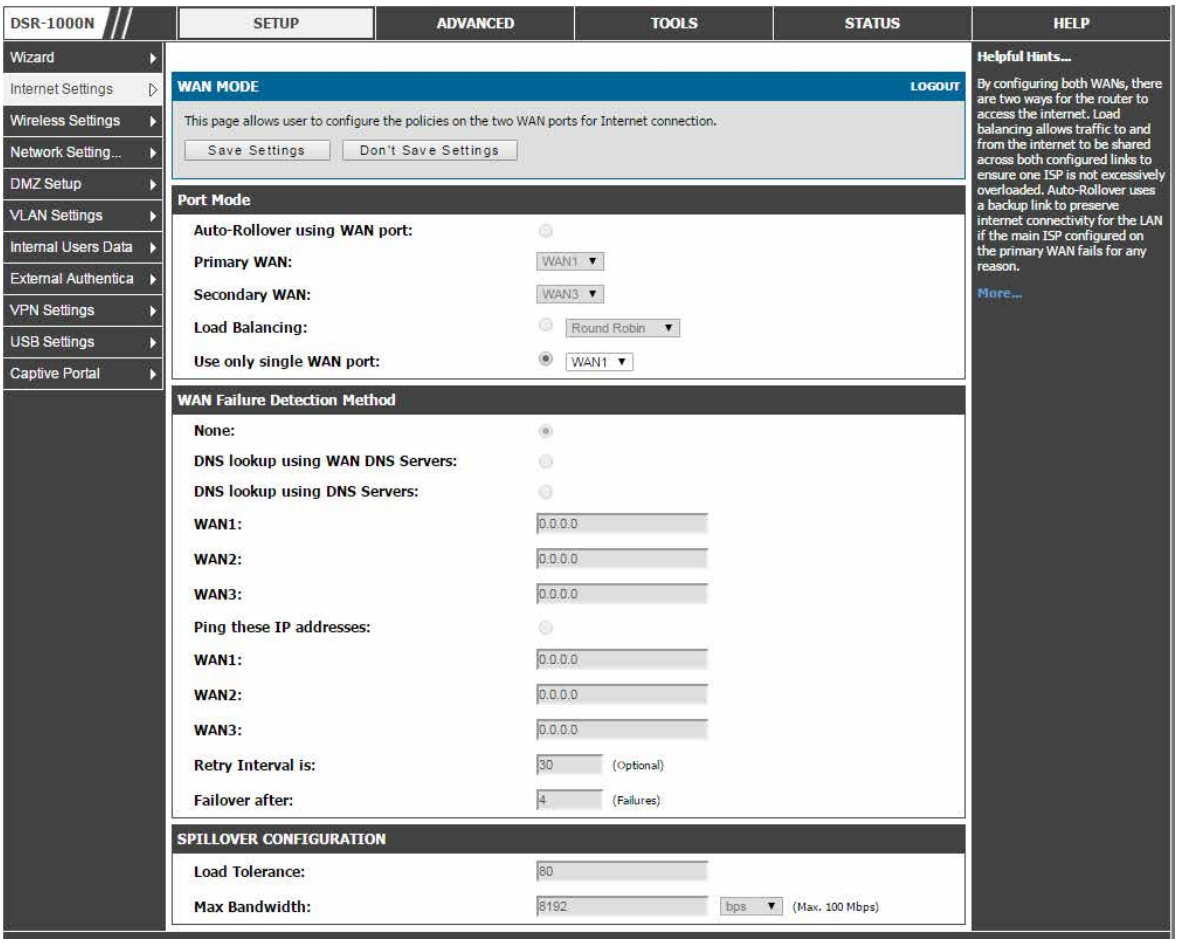


図 5-25　WAN MODE 画面

複数の WAN ポートが設定され、プロトコルバインディングが定義されると、ロードバランシングが利用可能になります。

2. 以下の項目があります。

項目	説明
Port Mode	
ポートモード設定により、1 つ以上有効である場合にルータが 1 つの WAN 接続だけを使用するか、両方使用するかを設定できます。インターネット接続のための 2 つの ISP リンクがある場合には、「自動ロールオーバモード」または「ロードバランシングモード」で設定することができます。	
Auto-Rollover using WAN port	バックアップの目的で冗長な ISP リンクの使用を希望する場合に選択し、このモードのためのプライマリリンクとして機能する WAN ポートを選択します。これを有効にする前にバックアップ WAN ポートが設定されていることを確認してください。設定すると、ステータスを検出するために一定間隔でプライマリリンクの接続をチェックします。
Primary WAN	選択した WAN はプライマリリンク (WAN1/WAN2) です。
Secondary WAN	選択した WAN はセカンダリリンクです。
Load Balancing	同時に複数の ISP リンクを使用する場合に選択します。ロードバランシングモードでは、2 つのリンクはそれらに割り当てられるプロトコルのデータを送信します。 • Round Robin - ラウンドロビンは、インターネットへの新しい接続が利用可能なリンク間でシフトされる場合に使用します。 • Spillover Mode - スピルオーバモードは、もう片方の WAN リンクが新しい接続に使用された後に帯域幅しきい値に到達するまで、すべての接続に単一の WAN リンクを使用します。
Use only single WAN port	LAN に 1 つの ISP 接続を設定する場合に選択し、ご契約の ISP に接続する WAN ポートを選択します。
WAN Failure Detection Method	
プライマリインターネットリンクの接続性をチェックするために、以下の故障検出方法の 1 つを選択できます。	
None	WAN 障害のチェックをしない場合に選択します。WAN モードが「ロードバランシング」に設定される場合にだけ、このオプションは有効です。
DNS lookup using WAN DNS Servers	プライマリ WAN の接続性を検出するのに使用されます。
DNS lookup using DNS Servers	プライマリリンクの接続性をチェックするためにカスタム DNS サーバの DNS 検索を指定できます。
Ping these IP addresses	IP アドレスに ping することで WAN の故障を検出します。この宛先ホストが信頼できることを確認してください。
Retry Interval is	上で設定した故障検出方法をルータが実行するべき頻度を指定します。
Failover after	これはフェイルオーバが開始される再試行の数を設定します。
SPILLOVER CONFIGURATION	
スピルオーバ設定によりスピルオーバモードオプションを設定することができます。	
Load Tolerance	ルータがセカンダリ WAN に切り替わる最大帯域幅（%）。
Max Bandwidth	この数値にはプライマリ WAN で許可される最大の帯域幅を設定します。帯域幅が設定した最大帯域数のロードトレランスを下回ると、ルータはセカンダリ WAN に切り替わります。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

自動フェイルオーバ

この場合、ご使用の WAN ポートの 1 つはすべてのインターネットトラフィックに対するプライマリインターネットリンクとして割り当てられます。セカンダリ WAN ポートは、プライマリリンクが何らかの理由でダウンした場合に冗長性のために使用されます。この機能を有効にする前に両方の WAN ポート（Primary、Secondary）には各 ISP に接続する設定を設定する必要があります。セカンダリ WAN ポートは、（いずれかのポートがプライマリとして割り当てられている）プライマリリンク上に障害が検出されるまで、未接続状態のままとなります。プライマリポート上に障害が発生すると、すべてのインターネットトラフィックがバックアップポートに転送されます。「Auto Failover」モードに設定されると、プライマリ WAN ポートのリンクステータスは、障害検出設定によって定義された間隔でチェックされます。

上記の「WAN Failure Detection Method」セクションを参照してください。

注意 WAN1 および WAN2 をプライマリインターネットリンクとして設定できます。

ロードバランシング

本機能により、同時に複数の WAN リンク（および、おそらく複数の ISP）を使用することができます。1 つ以上の WAN ポートを設定後、ロードバランシングオプションは、1 つ以上のリンクにトラフィックを送信することができるようになります。プロトコルバインディングは、インターネットフローを管理するために 1 つ以上の WAN ポートにサービスを分けて、割り当てるのに使用されます。ロードバランシングモードの場合、定義済み故障検出方式は、すべての設定済み WAN ポート上で定期的に使用されます。

DSR は、現在、ロードバランシングのために 3 つのアルゴリズムをサポートしています。

- Round Robin : このアルゴリズムは、1 つの WAN ポートの接続速度が他の速度と大きく異なる場合に特に役に立ちます。この場合、低い待ち時間であるサービス（VoIP など）をより高速なリンクに送信し、低容量のバックグラウンドトラフィック（SMTP など）は低速のリンクに転送するようにプロトコルバインディングを定義できます。プロトコルバインディングは次のセクションで説明します。

- Spill Over : スピルオーバ方式が選択されると、定義したしきい値に達するまで、プライマリ WAN は専用リンクとして機能します。この後、セカンダリ WAN は新しい接続に使用されます。スピルオーバロジックがプライマリからセカンダリ WAN に移動する外向き接続を管理するため、セカンダリ WAN の内向き接続は、本モードで許可されます。次のオプションを使用することによって、スピルオーバモードを設定できます。:
  - Load Tolerance : ルータがセカンダリ WAN に切り替わる最大帯域幅 (%) です。
  - Max Bandwidth : この数値には外向きトラフィックに対してプライマリ WAN で許可される最大の帯域幅を設定します 。

  外向きトラフィックに対してリンクの帯域が最大帯域数のロードトレランスを上回ると、ルータは次の接続をセカンダリ WAN に切り替えます。

  例えば、プライマリ WAN の最大帯域幅が 1Kbps であり、ロードトレランスが 70 に設定される場合です。新しい接続が確立されるたびに、帯域幅は増加します。ある接続数で帯域幅が 1Kbps の 70% に到達すると、新しい外向きの接続はセカンダリ WAN に切り替えられます。ロードトレランスの最大値は 80%、最小値は 20% です。

ロードバランシングは、1 つの WAN ポートの接続速度が他の速度と大きく異なる場合に特に役に立ちます。この場合、待ち時間が短いサービス（VoIP など）をより高速なリンクに送信し、低容量のバックグラウンドトラフィック（SMTP など）は低速のリンクに転送するようにプロトコルバインディングを定義できます。

以下の通り、複数の WAN ポートが設定され、プロトコルバインディングが定義されると、ロードバランシングが利用できます。

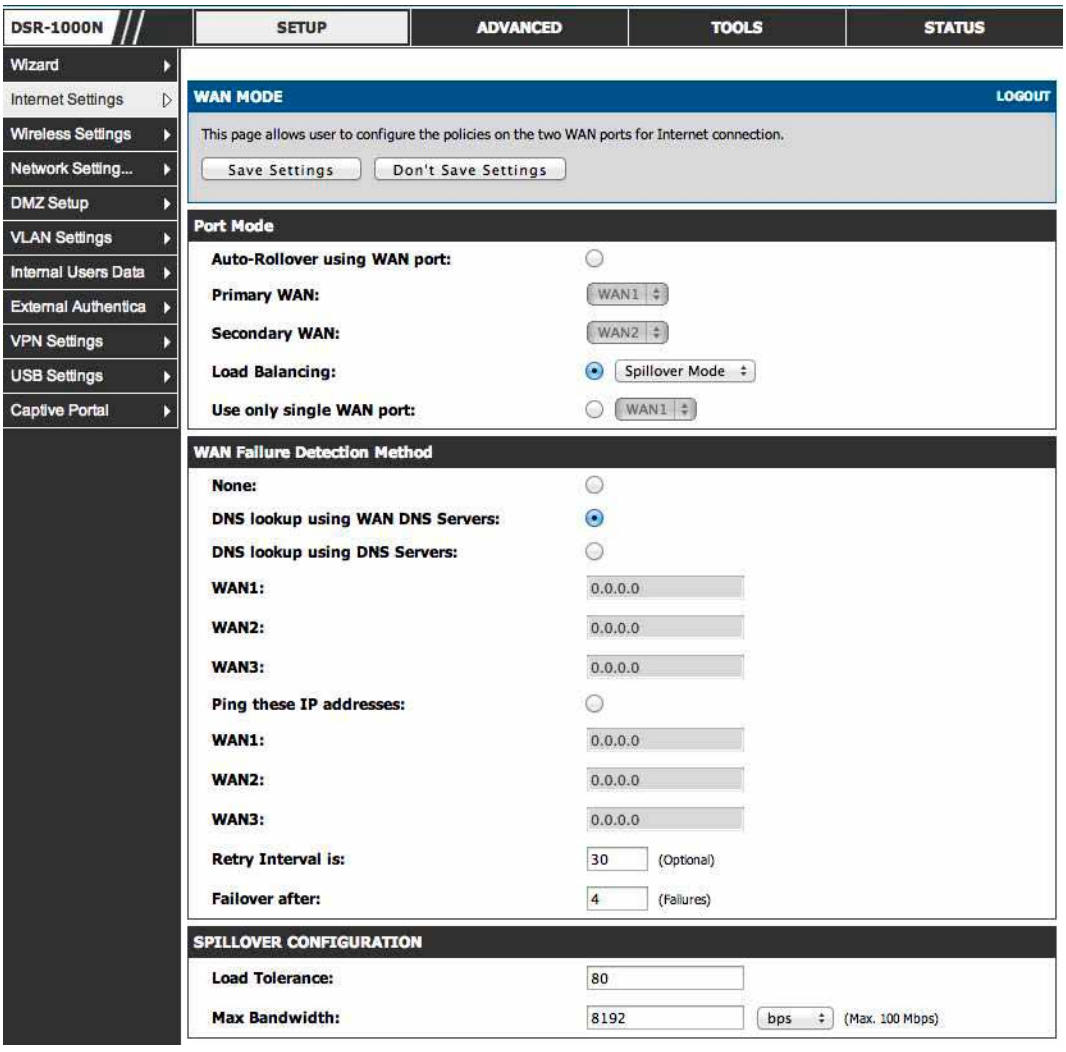


図 5-26　ロードバランシングの設定例

プロトコルバインディング

ADVANCED > Routing > Protocol Bindings メニュー

テーブルに現在定義済みの IP/MAC バインドルールのすべてを表示して、ルールにいくつかの操作を許可します。

プロトコルバインディングは、ロードバランス機能を使用する場合に有益です。設定したサービスまたはユーザ定義サービスのリストからいずれか選択すると、利用可能な WAN ポートの 1 つだけに送信するようにトラフィックのタイプを割り当てることができます。柔軟性を高めるために、送信先ネットワークまたはマシンと同様に送信元ネットワークまたはマシンを指定できます。例えば、1 セットの LAN IP アドレスに対する VoIP トラフィックを 1 つの WAN に割り当てることができます。また、残りの IP アドレスから来るどんな VoIP トラフィックももう一方の WAN リンクに割り当てることができます。ロードバランシングモードが有効で、1 つ以上の WAN が設定される場合にだけ、プロトコルバインディングは適用されます。

1. **ADVANCED > Routing > Protocol Bindings** の順にメニューをクリックし、以下の画面を表示します。

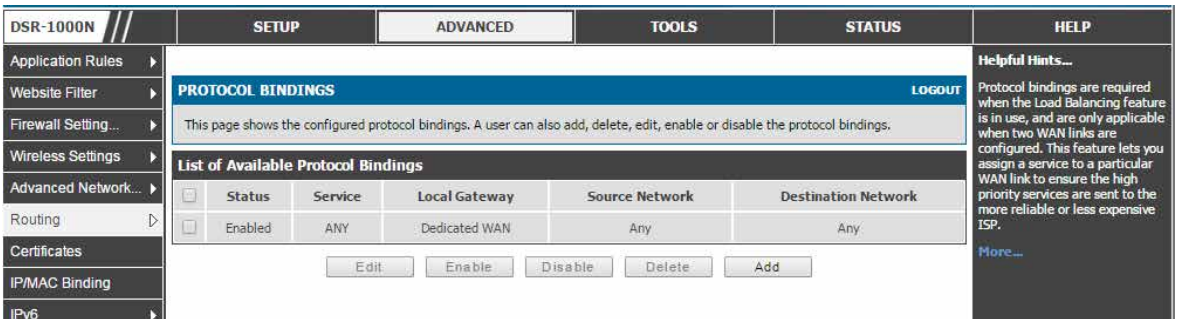


図 5-27　PROTOCOL BINDINGS 画面

有効なプロトコルバインディングのリストが表示されます。

プロトコルバインディングの追加

1. 「Add」ボタンをクリックして以下の画面を表示します。以下の画面はサービス および / または LAN 送信元を WAN および / または送信先ネットワークに割り当てるプロトコルバインディング設定例です。

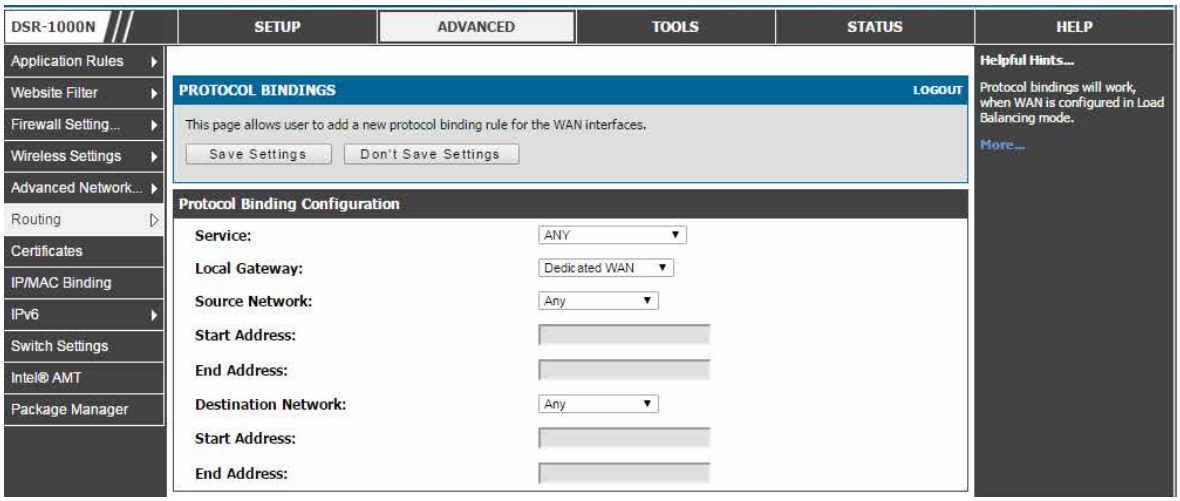


図 5-28　PROTOCOL BINDINGS 画面 - 追加

2. 以下の設定を設定します。

項目	説明
Service	プロトコルバインディングに利用可能な様々なサービスの 1 つを選択します
Local Gateway	このプロトコルバインディング（「Dedicated WAN」または「Configurable WAN」）にローカルなゲートウェイを設定するポートを選択します。
Source Network	以下の 1 つを選択します。 • Any - どの指定ネットワークも指定する必要がありません。 • Single Address - 1 台のコンピュータに制限します。このプロトコルバインディングの送信元ネットワークの一部であるコンピュータの IP アドレスを必要とします。 • Address Range - IP アドレス範囲内のコンピュータが送信元ネットワークの一部であることを許可する場合に選択します。開始アドレスと終了アドレスを必要とします。
Start Address	IP アドレス範囲の開始アドレスを入力します。
End Address	IP アドレス範囲の終了アドレスを入力します。

項目	説明
Destination Network	以下の 1 つを選択します。 • Any - どの指定ネットワークも指定する必要がありません。 • Single Address - 1 台のコンピュータに制限します。このプロトコルバインディングの送信先ネットワークの一部であるコンピュータの IP アドレスを必要とします。 • Address Range - IP アドレス範囲内のコンピュータが送信先ネットワークの一部であることを許可する場合に選択します。開始アドレスと終了アドレスを必要とします。
Start Address	IP アドレス範囲の開始アドレスを入力します。
End Address	IP アドレス範囲の終了アドレスを入力します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

IP エイリアス設定

SETUP > Internet Settings > IP Aliasing メニュー

IP エイリアスアドレスをポートに追加します。これにより、複数の IP アドレスを経由して単一の WAN イーサネットポートにアクセスできます。

1. **SETUP > Internet Settings > IP Aliasing** の順にメニューをクリックし、以下の画面を表示します。

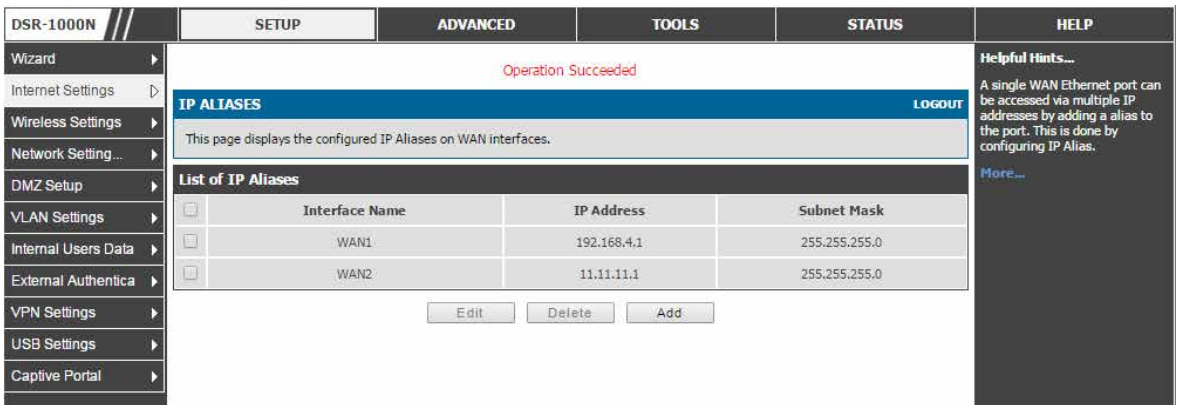


図 5-29　IP ALIASES 画面

設定済みの IP エイリアスを表示します。

2. 以下の項目が表示されます。

項目	説明
Interface Name	エイリアスが設定されているインタフェース。
IP Address	設定済み IP エイリアスの IP アドレス。
Subnet Mask	設定済み IP エイリアスのサブネットマスク。
Edit	IP エイリアス設定ページをオープンして、選択した IP エイリアス編集します。
Add	IP エイリアス設定ページをオープンして、新しく IP エイリアスを追加します。
Delete	選択した IP エイリアスを削除します。

IP エイリアスの追加、削除および編集ができます。

IP エイリアスの登録

1. 「Add」ボタンをクリックして以下の画面を表示します。

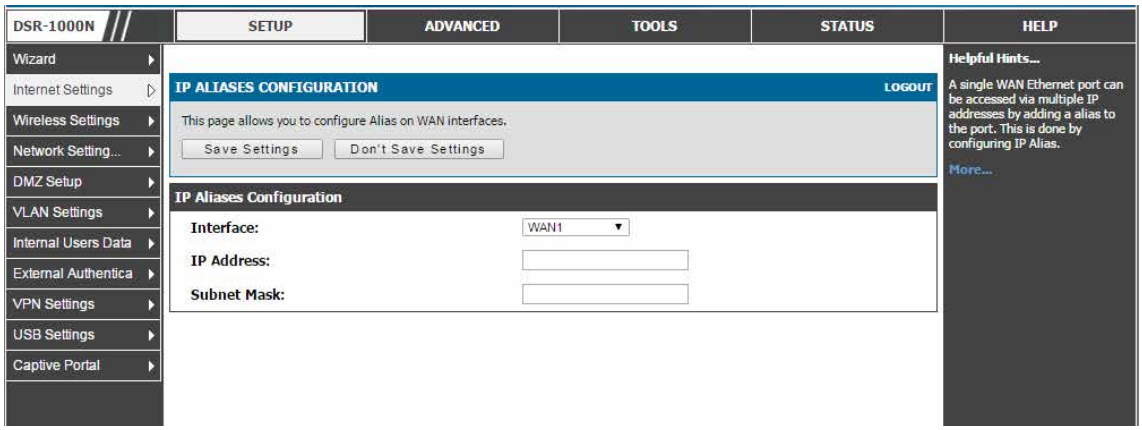


図 5-30　IP エイリアスの登録 画面

2. 以下の項目を設定します。

項目	説明
Interface	IP エイリアスを設定するインタフェースを設定します。
IP Address	IP エイリアスの IP アドレスを設定します。
Subnet Mask	IP エイリアスのサブネットマスクを設定します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。以前の設定に戻るためには「Don't Save Settings」をクリックします。

ルーティング設定

LAN と WAN 間のルーティングは、本ルータが物理インタフェースのいずれに受信されるトラフィックを処理する方法に影響を与えます。ゲートウェイのルーティングモードは安全な LAN とインターネット間のトラフィックフローの動作におけるコアとなります。

ルーティングモードの設定

SETUP > Internet Settings > Routing Mode メニュー

ここでは NAT、クラシカルルーティング、および透過などの異なるルーティングモードを設定します。また、RIP（Routing Information Protocol）を設定することもできます。

このデバイスは従来のルーティング、ネットワークアドレス変換（NAT）、および転送モードのルーティングをサポートしています。

以下はルーティングモードは、ダイナミックルーティング（RIP）と共に WAN と LAN 間のトラフィックルーティングを設定する例です。

1. **SETUP > Internet Settings > Routing Mode** の順にメニューをクリックし、以下の画面を表示します。

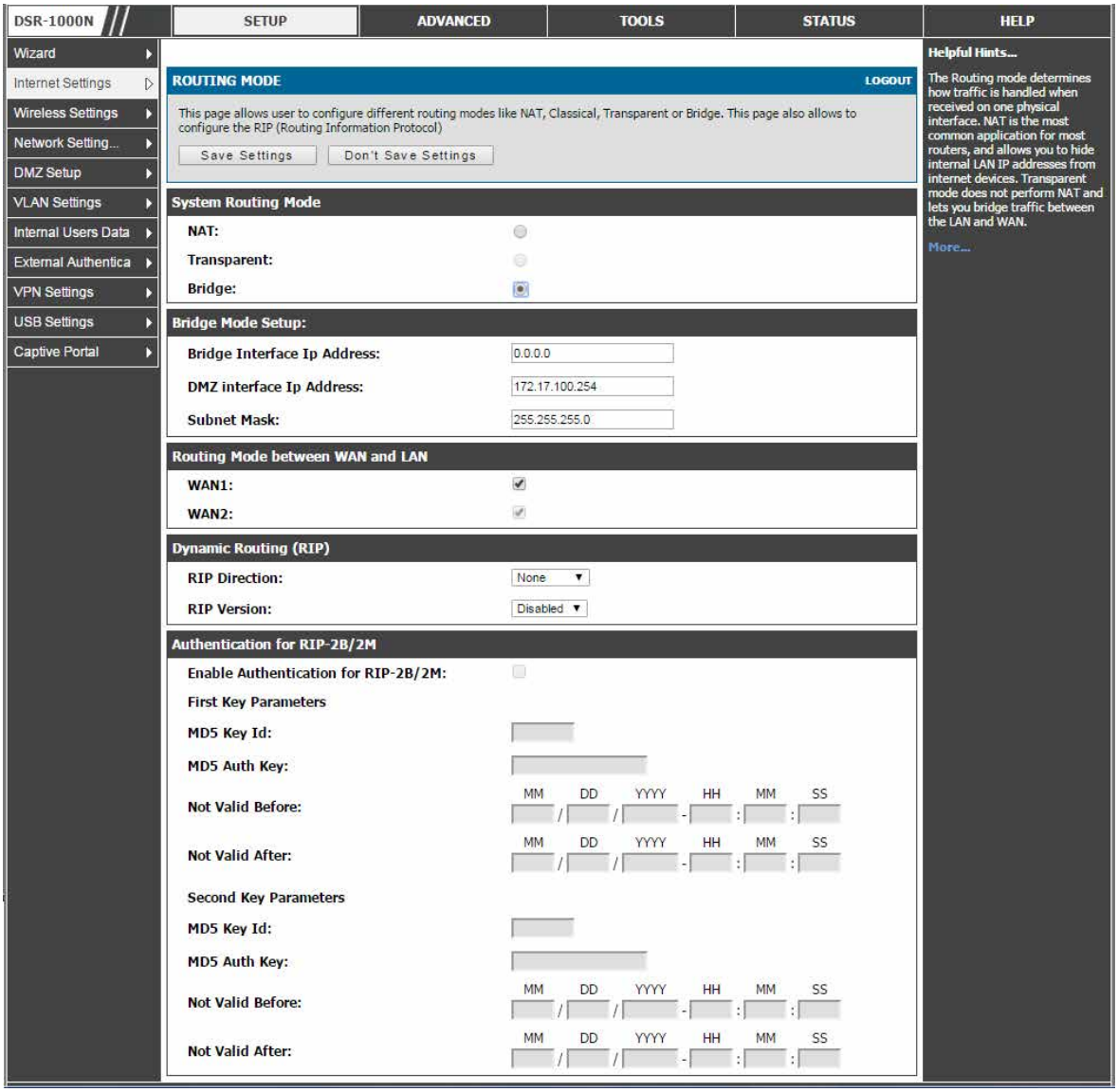


図 5-31　ルーティングモード設定

以下の項目があります。

項目	説明
NAT	NATはLANの複数のコンピュータがインターネット接続を共有できる技術です。LAN上のコンピュータは「プライベート」のIPアドレス範囲を使用し、一方、ルータのWANポートは1つの「パブリック」IPアドレスに設定されます。接続共有と共に、NATは内部のIPアドレスをインターネット上のコンピュータから隠します。NATは、ISPが1つのIPアドレスだけを割り当てた場合にだけ必要とされます。ルータ経由で接続するコンピュータは、プライベートサブネットからIPアドレスを割り当てられることが必要です。
Transparent	透過ルーティングモードが有効である場合、LANとWANの間のトラフィックにNATは実行されません。LANインタフェースに到着するブロードキャストとマルチキャストパケットは、ファイアウォールまたはVPNポリシーによってフィルタされない場合、WANに切り替えられます。逆もまた同様です。LANとWANが同じブロードキャストドメインにある場合に、透過モードを選択します。同じブロードキャストドメインでLANとWANを維持するためには、「Transparent」モードを選択します。これにより、ルータを終了するトラフィックおよび他の管理トラフィックを除き、LANからWANのトラフィック、およびWANからLANのトラフィックをブリッジすることができます。すべてのDSR機能がLANとWANが同じブロードキャストドメインにあるように設定されるものとする透過モードでサポートされます。
Bridge	ブリッジモードルーティングが有効である場合、最初の物理LANポートとセカンダリWAN/DMZ（ポート2）インタフェースはレイヤ2で共にブリッジされ、集約ネットワークを作成します。他のLANポートとプライマリWAN（WAN1）はこのブリッジの一部ではなく、ルータはこれらの他のポートのためにNATデバイスとして問い合わせます。LANポート1とWAN2/DMZインタフェースではブリッジモードで、ARP/RARPパケットをはじめL2とL3ブロードキャストトラフィックはパススルーされます。WAN2がタグ付きトラフィックを受信すると、LANポート1インタフェースにパケットを送信する前に、タグ情報は削除されます。
WAN1/WAN2	NATモードを有効にするWANインタフェースを選択します。未選択のWANインタフェースは「Classical Routing」モードになります。従来のルーティングを使用する場合、LAN上のデバイスにはそれらのパブリックIPアドレスでインターネットからに直接アクセスできます（適切なファイアウォールが設定であると仮定します）。ISPがご使用の各コンピュータにIPアドレスを割り当てた場合には、「Classic Routing」を使用します。

注意 NATルーティングには、既知の外部のドメイン名を使用して、LANおよびDMZ上の内部ネットワークユーザが内部のサーバ（例：内部のFTPサーバ）にアクセスできる「ヘアピンNAT」と呼ばれる機能があります。これは、LANが生成したトラフィックをそれらの外部名でLANサーバに到達するようにファイアウォールを経由してリダイレクトした後に「NATループバック」として参照されます。

注意 ブリッジモードオプションはDSR-500/1000/1000N製品だけで利用可能です。

ダイナミックルーティング（RIP）

SETUP > Internet Settings > Routing Mode メニュー

RIP（Routing Information Protocol）を使用したダイナミックルーティングは、LAN に一般的に使用される IGP（Interior Gateway Protocol）です。本ルータは、RIP を使用してトラフックフローを中断しないで LAN 内の変更を適用するために、LAN 内で他のサポートしているルータとルーティング情報を交換して、ルーティングテーブルのダイナミックな調整を行うことができます。

1. **SETUP > Internet Settings > Routing Mode** の順にメニューをクリックし、以下の画面を表示します。

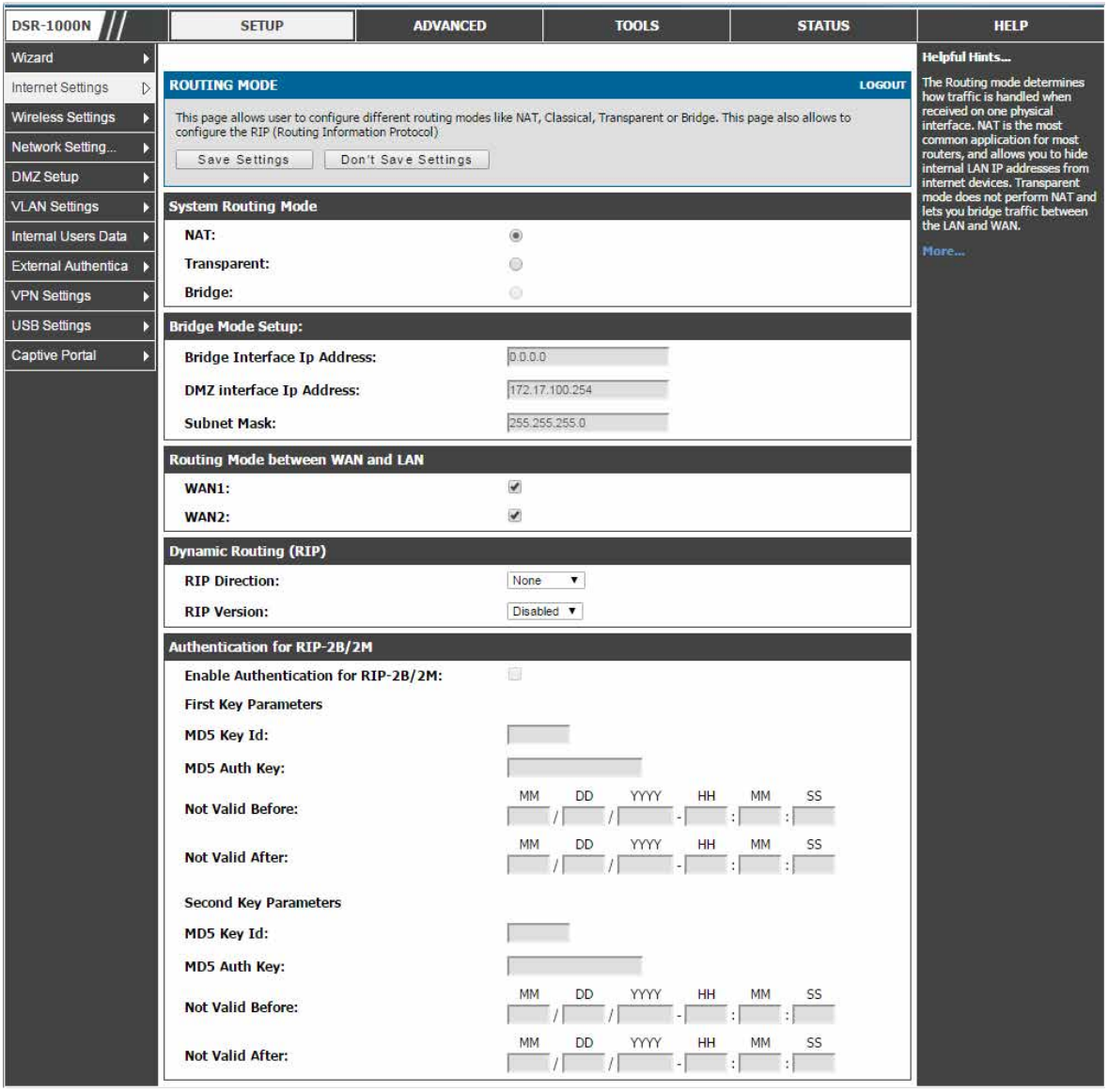


図 5-32　ダイナミックルーティングモード設定

2. 以下の項目から選択します。

項目	説明
System Routing Mode	
システムルーティングモードを選択します。 • NAT - LAN の複数のコンピュータがインターネット接続を共有できます。 • Transparent - LAN と WAN からのトラフィックをブリッジすることができます。 • Bridge - 物理的な LAN ポート 1 と WAN2/DMZ インタフェースのトラフィックをブリッジします。 注意　システムルーティングモードを切り換える場合、ルータはすべての内向きファイアウォールルールを削除します。	
DMZ interface Ip Address	DMZ インタフェースに割り当てる IP。
Subnet Mask	DMZ インタフェースの IP アドレスのサブネットマスク。
Bridge Mode Setup	
Bridge Interface Ip Address	ブリッジインタフェースに割り当てる IP。
DMZ interface Ip Address	DMZ インタフェースに割り当てる IP。
Subnet Mask	DMZ インタフェースの IP アドレスのサブネットマスク。

項目	説明
Routing Mode between WAN and LAN	
WAN1/WAN2	NAT モードを有効にする WAN インタフェースを選択します。
Dynamic Routing (RIP)	
RIP Direction	ルータが RIP パケットを送受信する方法を定義します。 • Both - ルータは双方向でルーティングテーブルをブロードキャストし、他のルータから受信した RIP 情報を処理します。RIP 機能をフルに活用するためには、この設定をお勧めします。 • Out Only - ルータは定期的にルーティングテーブルをブロードキャストしますが、他のルータから RIP 情報を受信しません。 • In Only - ルータは他のルータから RIP 情報を受信しますが、ルーティングテーブルをブロードキャストしません。 • None - ルータはルーティングテーブルのブロードキャスト、および他のルータからの RIP 情報の受信のいずれもしません。事実上、これは RIP を無効にします。
RIP Version	RIP バージョンは LAN 内の他のルーティングデバイスの RIP サポートに依存します。 • Disabled - RIP を無効にする場合に、これを設定します。 • RIP-1 - サブネット情報を含んでいないクラスベースのルーティングバージョンです。これは最も一般的にサポートされるバージョンです。 • RIP-2 - RIPv1 のすべての機能に加え、サブネット情報をサポートします。データは RIP-2B と RIP-2M の両方に RIP-2 形式で送信されますが、パケットが送信されるモードは異なります。 - RIP-2B - サブネット全体にデータをブロードキャストします。 - RIP-2M - マルチキャストアドレスにデータを送信します。 RIP-2B または RIP-2M が選択されたバージョンであれば、このルータと他のルータ（同じ RIP バージョンで設定済み）間には認証が必要となります。MD5 認証は第 1 / 第 2 キーの交換処理で使用されます。ルーティング情報の交換が LAN 上で検出された現在の、およびサポートされているルータと共に行われることを保証するために、認証キーの有効なライフタイムを設定することができます。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

スタティックルーティング

ADVANCED > Routing > Static Routing メニュー

ADVANCED > IPv6 > IPv6 Static Routing メニュー

ここではルータに設定済みのスタティックルートのリストを表示します。さらに、設定済みのルートの追加、削除および編集ができます。

このデバイスに手動でスタティックルートを追加すると、1 つのインタフェースから別のインタフェースまでのトラフィック経路の選択を定義できます。経路に変更を説明するために、このルータと他のデバイス間の通信はありません。一度設定されると、ネットワークの変更があるまで、スタティックルートは、アクティブであり、有効です。

IPv4 の場合

1. **ADVANCED > Routing > Static Routing** の順にメニューをクリックし、以下の画面を表示します。

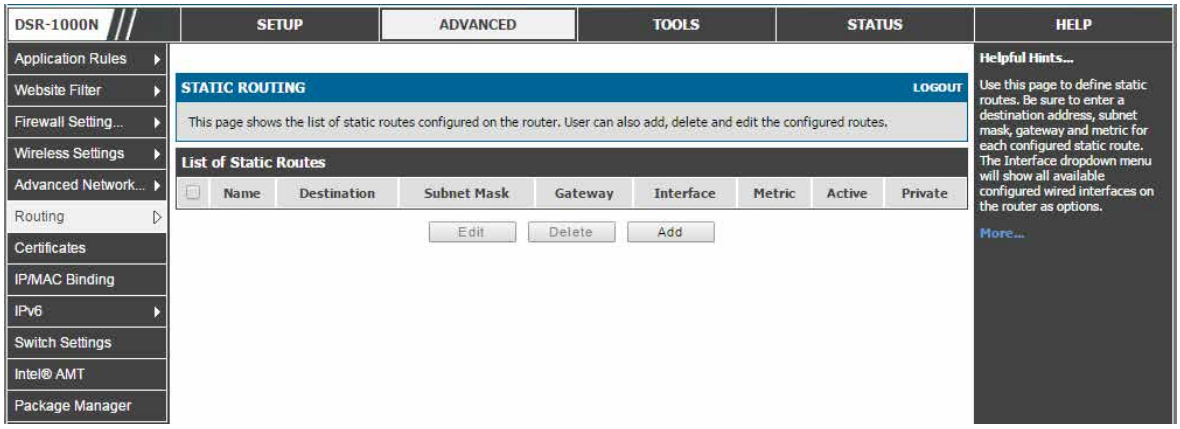


図 5-33　STATIC ROUTING 画面 - IPv4

IPv6 の場合

1. **ADVANCED > IPv6 > IPv6 Static Routing** の順にメニューをクリックし、以下の画面を表示します。

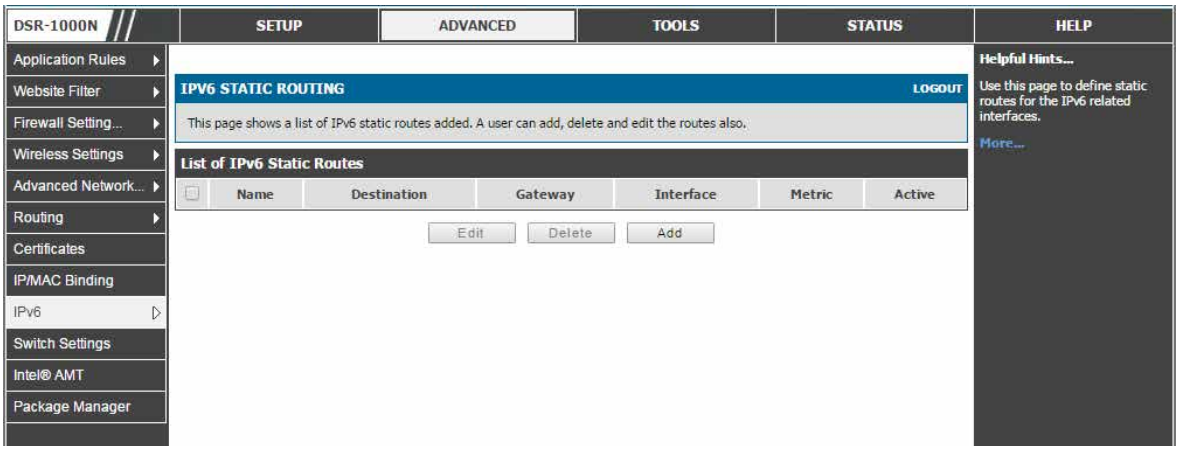


図 5-34　STATIC ROUTING 画面 - IPv6

「List of Static Routes」では、管理者によって手動で登録された全ルートが表示され、そのスタティックルートにいくつかの操作を許可します。「List of IPv4 Static Routes」と「List of IPv6 Static Routes」は同じフィールドを共有します（1 つの例外があります。）

スタティックルートの追加

1. 「STATIC ROUTING」画面で「Add」ボタンをクリックして以下の画面を表示します。

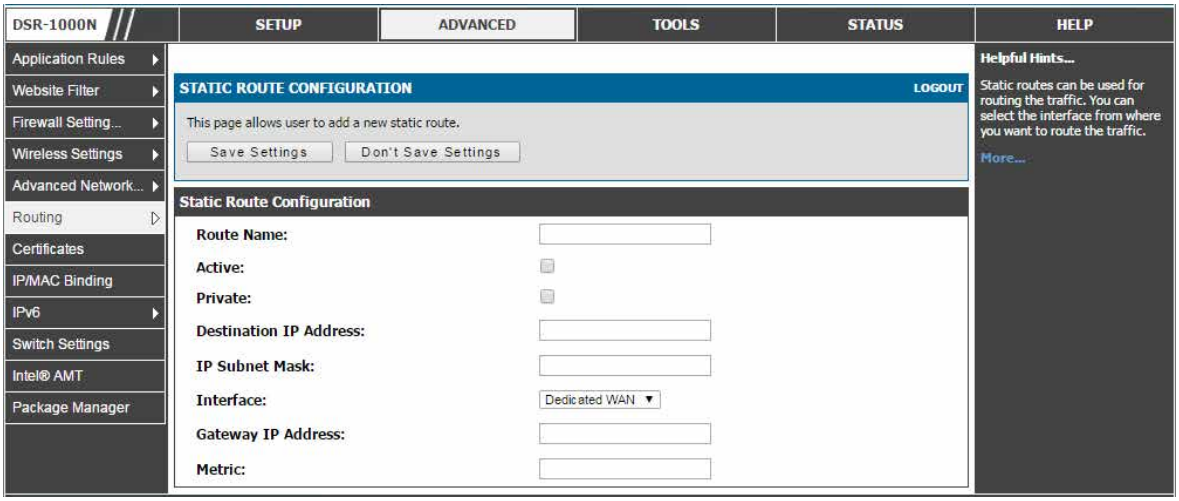


図 5-35　スタティックルート設定画面 - IPv4

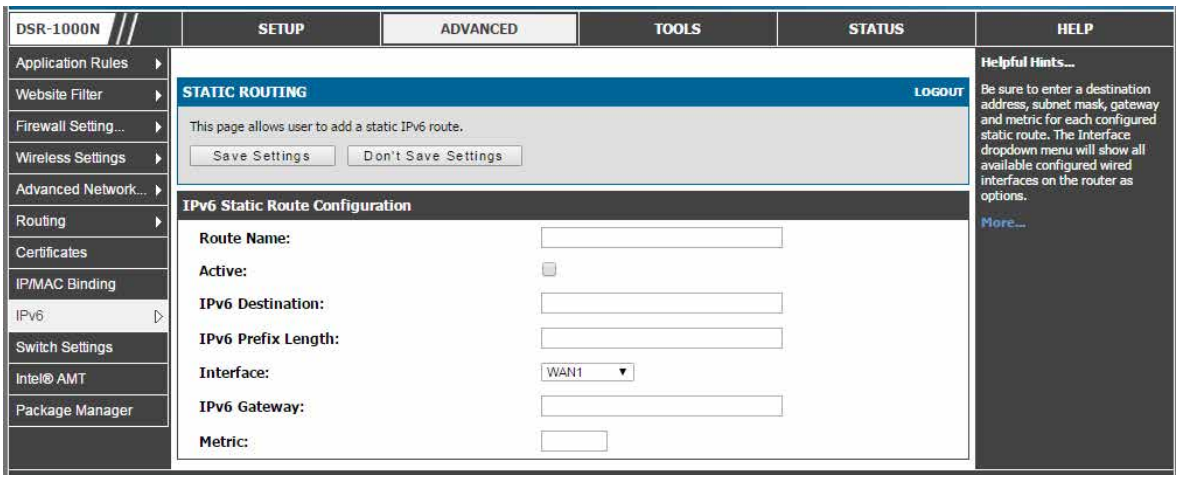


図 5-36　スタティックルート設定画面 - IPv6

2. 以下の項目を指定します。

項目	説明
Router Name	識別と管理のためのルート名。
Active	ルートをアクティブ、または無効にします。ルートをテーブルに追加し、必要でない場合に無効にすることができます。これによりエントリを削除および再追加せずに必要に応じてルートを使用することができます。RIP が有効な場合、無効のルートはブロードキャストされません。
Private	RIP が有効な場合、他のルータとルートを共有するかどうかを決定します。ルートを「プライベート」にすると、ルートは RIP ブロードキャストまたはマルチキャストで共有されません。これは、IPv4 スタティックルートだけに適用されます。
Destination IP Address	ルートはこの宛先または IPv4 アドレスに通じます。
IP Subnet Mask	IPv4 ネットワークだけに有効であり、このスタティックルートによって影響を受けるサブネットを識別します。
IPv6 Destination	ルートはこの宛先または IPv6 アドレスに通じます。
IPv6 Prefix Length	IPv6 のプレフィックス長を指定します。
Interface	本ルートがアクセス可能である物理的なネットワークインタフェース（Dedicated WAN、Configurable WAN、LAN > VLAN、DMZ）。
Gateway	宛先ホストまたはネットワークに到達できるゲートウェイの IPv4 アドレス。
IPv6 Gateway	宛先ホストまたはネットワークに到達できるゲートウェイの IPv6 アドレス。
Metric	ルートの優先度を決定します。同じ宛先に対して複数のルートが存在している場合、最も低いメトリックを持つルートが選択されます。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

OSPFv2 設定

ADVANCED > Routing > OSPF メニュー

OSPF は、単一のルーティングドメインにインターネットプロトコル (IP) パケットを送る内部のゲートウェイプロトコルです。これは、利用可能なルータからリンク状態情報を収集して、ネットワークのトポロジマップを構成します。OSPF バージョン 2 は、RFC2328-OSPF バージョン 2 に記述されるルーティングプロトコルです。OSPF は IGP (Interior Gateway Protocols) であり、ISP バックボーンやエンタープライズネットワークなどの大規模ネットワークに広く使用されます。

1. **ADVANCED > Routing > OSPF** の順にメニューをクリックし、以下の画面を表示します。

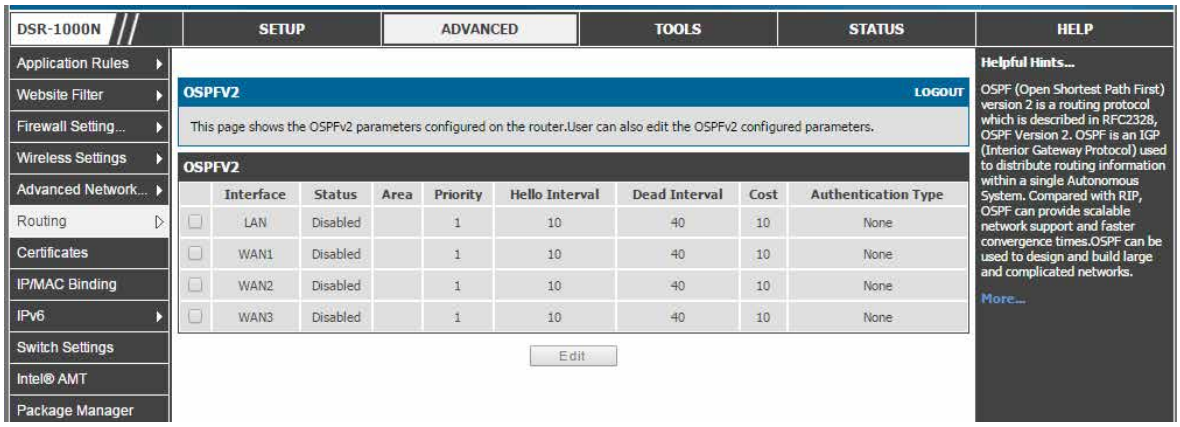


図 5-37　OSPFv2 の設定パラメータ

2. 以下の項目があります。

項目	説明
Interface	OSPFv2 を有効 / 無効にする物理ネットワークインタフェース。
Status	この欄は特定のインタフェース OSPFv2 の有効 / 無効状態を表示します。
Area	インタフェースが所属するエリア。共通セグメントを持つ 2 つのルータ : それらのインタフェースはセグメントで同じエリアに所属する必要があります。インタフェースは同じサブネットに属し、同一のサブネットマスクを持ちます。
Priority	ネットワークの OSPFv2 代表ルータの決定を補助します。高い優先度を持つルータほど代表ルータになる可能性が高くなります。値を 0 に設定すると、ルータはより代表ルータになる可能性が高くなります。初期値は 1 です。低い番号ほど高い優先度を意味します。
Hello Interval	Hello インターバルタイマの値（秒）。この値を設定すると、特定のインタフェースに設定時間ごとに Hello パケットが送信されます。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 10（秒）です。
Dead Interval	デバイスの Hello パケットが受信されなくなってから、Neighbor ルータがその OSPF ルータがダウンしていると判断するまでの時間（秒）。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 40（秒）です。OSPF では、2 つの Neighbor 間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません。

項目	説明
Cost	OSPFv2 インタフェースにパケットを送信するコスト。
Authentication Type	この欄では OSPFv2 に使用する認証タイプを表示します。 • None - インタフェースは OSPF パケットを認証しません。 • Simple - インタフェースはシンプルテキストキーを使用して OSPF パケットを認証します。 • MD5 - インタフェースは MD5 認証を使用して OSPF パケットを認証します。

設定項目の編集

1. 編集するエントリをチェック後、「Edit」ボタンをクリックします。

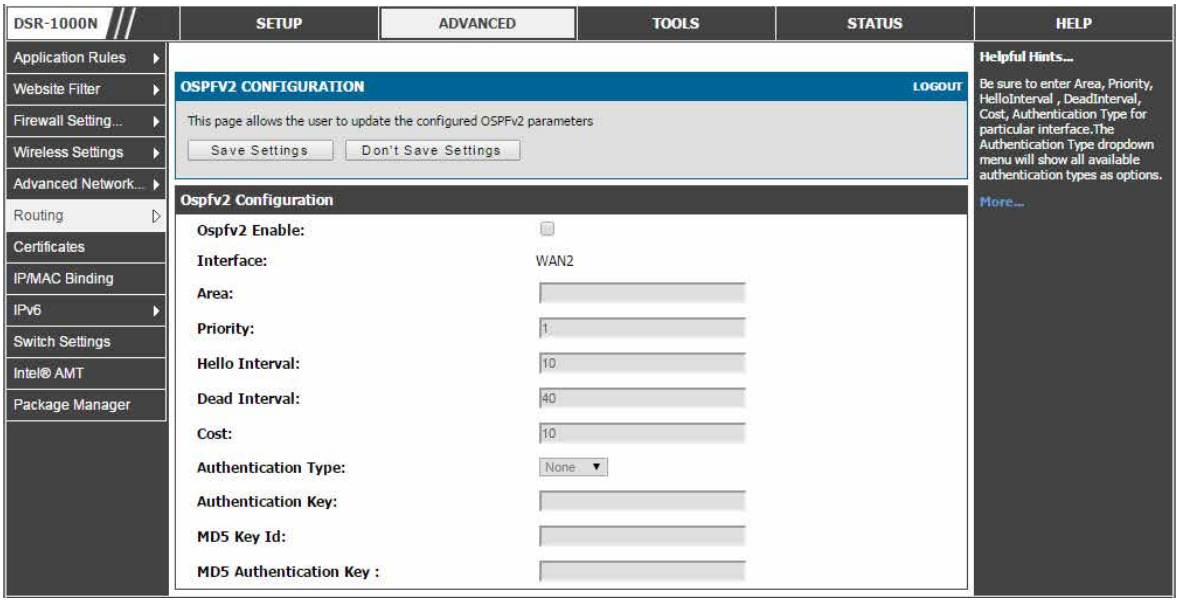


図 5-38　OSPFv2 コンフィグレーション 画面

2. 以下の項目を表示または設定します。

項目	説明
Ospfv2 Enable	チェックボックスを使用して OSPFv2 を有効 / 無効にします。
Interface	OSPFv2 を有効 / 無効にする物理ネットワークインタフェース。
Area	インタフェースが所属するエリア。1-255 の値を入力します。2 つのルータが共通セグメントを持つ場合、それらのインタフェースはセグメントで同じエリアに所属する必要があります。インタフェースは同じサブネットに属し、同一のサブネットマスクを持ちます。
Priority	ネットワークの OSPFv2 代表ルータの決定を補助します。高い優先度を持つルータほど代表ルータになる可能性が高くなります。値を 0 に設定すると、ルータはより代表ルータになる可能性が高くなります。初期値は 1 です。低い番号ほど高い優先度を意味します。
Hello Interval	Hello インターバル値（秒）。この値を設定すると、特定のインタフェースに設定時間ごとに Hello パケットが送信されます。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 10（秒）です。
Dead Interval	Hello パケットが受信されなくなってから、Neighbor ルータがその OSPF ルータがダウンしていると判断するまでの時間（秒）。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 40（秒）です。OSPF では、2 つの Neighbor 間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません
Cost	OSPFv2 インタフェースにパケットを送信するコスト
Authentication Type	この欄では OSPFv2 に使用する認証タイプを表示します。 • None - インタフェースは OSPF パケットを認証しません。 • Simple - インタフェースはシンプルテキストキーを使用して OSPF パケットを認証します。 • MD5 - インタフェースは MD5 認証を使用して OSPF パケットを認証します。
Authentication Key	認証タイプに Simple を使用しているネットワークセグメントにおける隣接 OSPF ルータに使用される特定のパスワードを割り当てます。ルーティングドメインに参加する、同一エリア内のルータには同じキーを設定する必要があります。
Md5 Key Id	認証タイプに MD5 を使用しているネットワークセグメントにおける隣接 OSPF ルータに使用される固有の MD5 キー ID を入力します。
Md5 Authentication Key	認証タイプに MD5 を使用しているネットワークセグメントにおける隣接 OSPF ルータに使用されるこの MD5 キーに認証キーを入力します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

OSPFv3 設定

ADVANCED > IPv6 > OSPF メニュー

OSPFv3 (Open Shortest Path First version 3) は IPv6 をサポートしています。ルータの OSPFv3 プロセスを有効にするためには、OSPFv3 プロセスをグローバルに有効とし、ルータ ID を OSPFv3 プロセスに割り当て、このプロセスを関連するインタフェースで有効にする必要があります。

1. **ADVANCED > IPv6 > OSPF** の順にメニューをクリックし、以下の画面を表示します。

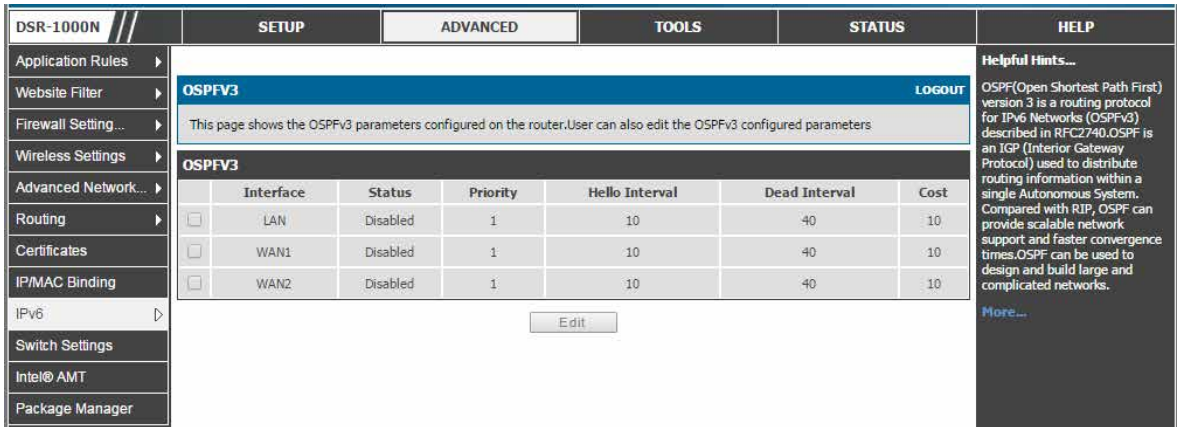


図 5-39　OSPFv3 の設定パラメータ

2. 以下の項目があります。

項目	説明
Interface	OSPFv3 を有効 / 無効にする物理ネットワークインタフェース。
Status	特定のインタフェース OSPFv3 の有効 / 無効状態を表示します。
Priority	ネットワークの OSPFv3 代表ルータの決定を補助します。高い優先度を持つルータほど代表ルータになる可能性が高くなります。値を 0 に設定すると、ルータはより代表ルータになる可能性が高くなります。初期値は 1 です。低い番号ほど高い優先度を意味します。
Hello Interval	Hello インターバルタイマの値（秒）。この値を設定すると、特定のインタフェースに設定時間ごとに Hello パケットが送信されます。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 10（秒）です。
Dead Interval	デバイスの Hello パケットが受信されなくなってから、Neighbor ルータがその OSPF ルータがダウンしていると判断するまでの時間（秒）。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 40（秒）です。OSPF では、2 つの Neighbor 間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません。
Cost	OSPFv3 インタフェースにパケットを送信するコスト。

設定項目の編集

1. 編集するエントリをチェック後、「Edit」ボタンをクリックします。

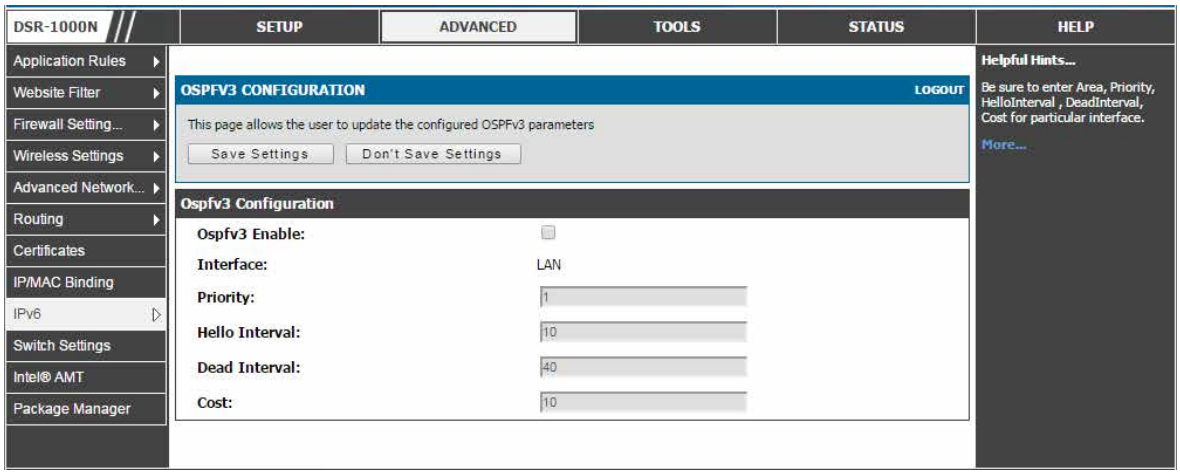


図 5-40　OSPFv3 コンフィグレーション 画面

2. 以下の項目を表示または設定します。

項目	説明
Ospfv3 Enable	チェックボックスを使用して OSPFv3 を有効 / 無効にします。
Interface	OSPFv3 を有効 / 無効にする物理ネットワークインタフェース。
Priority	ネットワークの OSPFv3 代表ルータの決定を補助します。高い優先度を持つルータほど代表ルータになる可能性が高くなります。値を 0 に設定すると、ルータはより代表ルータになる可能性が高くなります。初期値は 1 です。低い番号ほど高い優先度を意味します。
Hello Interval	Hello インターバル値（秒）。この値を設定すると、特定のインタフェースに設定時間ごとに Hello パケットが送信されます。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 10（秒）です。
Dead Interval	Hello パケットが受信されなくなってから、Neighbor ルータがその OSPF ルータがダウンしていると判断するまでの時間（秒）。本値は共通ネットワークに接続する全ルータで同じである必要があります。初期値は 40（秒）です。OSPF では、2 つの Neighbor 間でこれらのインターバルの値が全く同じである必要があります。異なるインターバル値を持つルータ同士はそのセグメントにおいて Neighbor ルータになることができません。
Cost	OSPFv3 インタフェースにパケットを送信するコスト。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

6to4 トンネル設定

ADVANCED > IPv6 > 6to4 Tunneling メニュー

6 to 4 トンネリング機能を有効または無効にします。

6 to 4 は、IPv4 から IPv6 まで移行するためのインターネット移行メカニズムであり、IPv6 パケットの IPv4 ネットワークへの転送を可能にするシステムです。チェックボックスを選択して「Enable Automatic Tunneling」を有効にし、IPv6 LAN からのトラフィックをリモート IPv6 ネットワークに到達するように IPv4 オプションに送信することができます。

本オプションが有効な場合、IPv4 アドレス情報は LAN 上の IPv6 アドレスに埋め込まれます。このオプションは IPv4 と IPv6 ノードの両方を使用するネットワークで非常に一般的です。

1. **ADVANCED > IPv6 > 6 to 4 Tunneling** の順にメニューをクリックし、以下の画面を表示します。

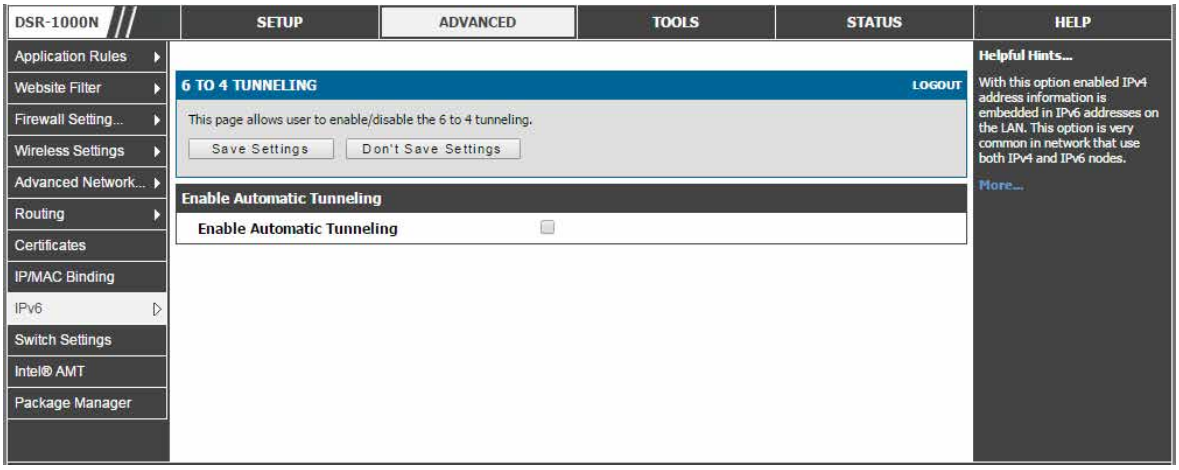


図 5-41　6 to 4 トンネルの有効化

2. 6 to 4 トンネルを有効にするためには、「Enable Automatic Tunneling」をチェックして「Save Settings」ボタンをクリックします。

ISATAP トンネル設定

ADVANCED > IPv6 > ISATAP Tunnels メニュー

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) は、IPv4 ネットワーク上のデュアルスタックノード間に IPv6 パケットを送信する IPv6 移行メカニズムです。ISATAP はサイトの境界ルータ検出方法と同様に IPv6-IPv4 互換性アドレス形式を指定します。また、ISATAP は、特定のリンクレイヤ（IPv6 のリンクレイヤとして使用される IPv4）における IPv6 の操作を指定します。

利用可能な ISATAP トンネルのリストを表示します。また、ISATAP トンネルの追加、削除および編集ができます。

ADVANCED > IPv6 > ISATAP Tunnels の順にメニューをクリックし、以下の画面を表示します。

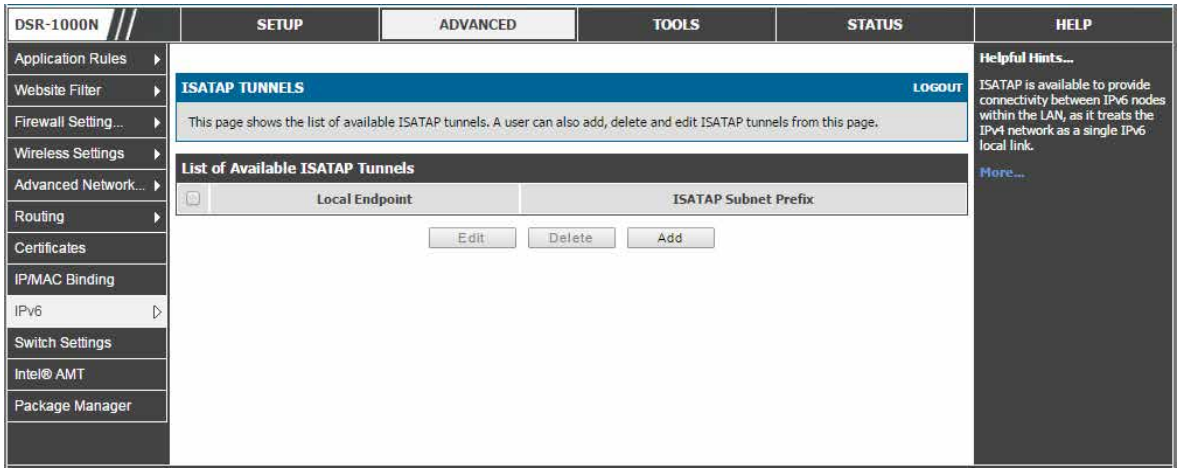


図 5-42　ISATAP トンネルのリスト

ISATAP トンネルの登録

1. 「Add」ボタンをクリックして以下の画面を表示します。

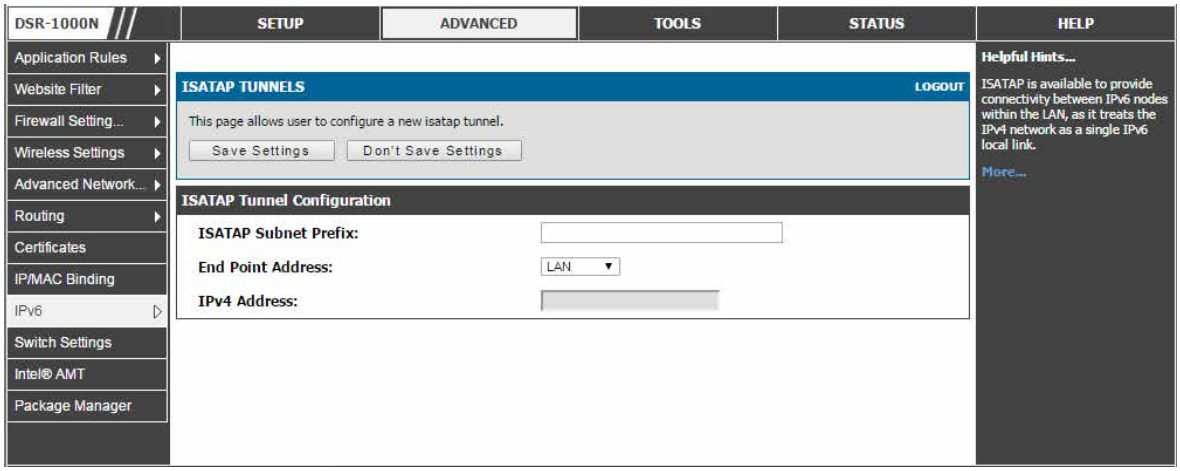


図 5-43　ISATAP トンネルの登録

2. 以下の項目を設定します。

項目	説明
ISATAP Subnet Prefix	このイントラネット用に論理的な ISATAP サブネットに割り当てられる 64 ビットのサブネットプレフィックスを指定します。ご契約の ISP またはインターネット登録から取得するか、または RFC 4193 から取得します。
Local End Point Address	このルータから開始するトンネルのエンドポイントアドレスを選択します。 • LAN - エンドポイントは、LAN インタフェース（LAN が IPv4 ネットワークであると仮定する）です。 • Other IP - 特定の LAN IPv4 アドレスとします。これを選択した場合、続く「IPv4 Address」欄でエンドポイントの IPv4 アドレスを指定します。
IPv4 Address	ローカルのエンドポイントアドレスを指定します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

設定可能ポート - WAN オプション

本ルータは、セカンダリの WAN イーサネットポートまたは専用 DMZ ポートとして設定できる物理ポートをサポートしています。ポートがセカンダリ WAN インタフェースになるように選択されると、WAN2 に関連するすべての設定ページが有効になります。

SETUP > Internet Settings > WAN2 Settings > WAN2 Setup メニュー
ここでは WAN2 のインターネット接続を設定できます。IP アドレス、アカウント情報などインターネット接続情報があることを確認してください。通常、この情報は ISP またはご使用のネットワーク管理者によって提供されます。

WAN2 の設定は WAN1 設定と同じです。「3G Internet」の設定はできません。

注意 本製品は 3G USB モデムを使用した通信に対応していないため、「3G Internet」の設定はできません。

WAN ポート設定

ADVANCED > Advanced Network > WAN Port Setup メニュー
ここではルータの WAN リンクに詳細な WAN オプション（物理的なポート設定）を設定することができます。

ISP アカウントが WAN ポート速度を定義するか、または MAC アドレスに関連付ける場合、ネットワークとのスムーズな接続を確実にするためにこの情報が必要とされます。

1. **ADVANCED > Advanced Network > WAN Port Setup** の順にメニューをクリックし、以下の画面を表示します。

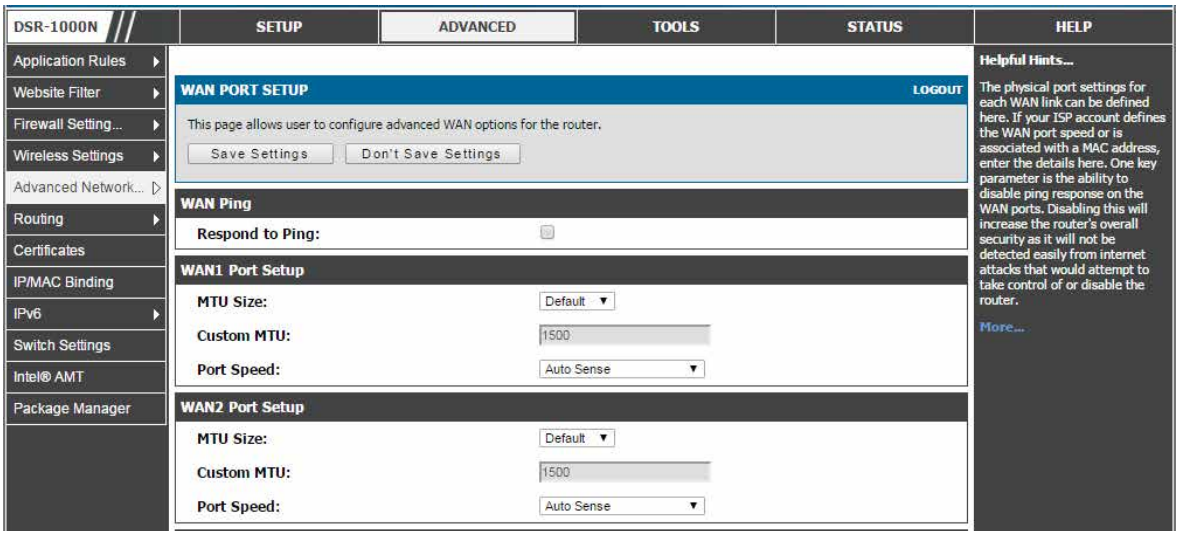


図 5-44　物理 WAN ポートの設定

2. 以下の項目を設定します。

項目	説明
MTU	すべてのポートでサポートされる MTU 値の初期値は 1500 です。これは、フラグメント化なしでインタフェースを通過できる最大パケットサイズです。 このサイズを増やすことはできますが、大きいパケットは、ネットワーク遅延を起こし、インタフェース速度を低下させます。1500 バイトのパケットサイズはネットワーク層におけるイーサネットプロトコルで許可される最大のサイズです。
Port Speed	「Auto Sense」が選択されると、ルータはポート速度を感知します。このオプションでは、最適なポート設定はルータとネットワークによって決定されます。 以下の 3 つのポート速度と共に、ポートのサポートに基づいてデュプレックス（half または full）を定義できます。: 10Mbps、100Mbps、および 1000Mbps（すなわち、1Gbps）。初期値は「Auto Sense」です。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

第 6 章　無線アクセスポイント設定（DSR-1000N のみ）

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

項目	説明	参照ページ
無線設定ウィザード	ウィザードに従って無線設定を行います。	84 ページ
無線プロファイル	AP を無線クライアントに関連付ける場合に使用する、セキュリティタイプ、暗号化、および認証を含めたプロファイルを設定します。	87 ページ
アクセスポイントの作成と使用	新しいアクセスポイント、仮想アクセスポイントの作成とプロファイルの割り当てを行います。	89 ページ
無線帯域の詳細設定の調整	有効なチャンネルと電力レベルを設定します。	93 ページ
WMM 設定	Wi-Fi マルチメディア設定を行います。	94 ページ
WDS 設定	WDS 設定を行います。	95 ページ
高度な無線設定	詳細な無線の通信パラメータを設定します。	97 ページ
WPS 設定	WPS の設定を行います。	98 ページ

DSR-1000N は無線 LAN クライアント用のアクセスポイント機能を設定可能な統合された 802.11n 無線帯域を搭載しています。セキュリティ / 暗号化 / 認証オプションは無線のプロファイルにまとめられ、各設定プロファイルは AP 設定メニューで選択することができます。プロファイルは、無線クライアントと AP 間のセキュリティを含む AP 用の様々なパラメータを定義しており、必要に応じて、同じデバイスの複数の AP インスタンス間で共有できます。

複数の「仮想」の AP を設定することによって、最大 4 つのユニークな無線ネットワークを作成することができます。そのような仮想 AP のそれぞれはその環境でサポートされるクライアントに対しては独立している AP（ユニークな SSID）として表示されますが、実際にはこのルータに統合される同じ物理周波数帯域で動作しています。

無線ネットワークを設定するためには以下の情報が必要です。:

- 無線ネットワークにアクセスすることが予想されるデバイスのタイプとそれらがサポートする Wi-Fi ™ モード。
- ルータの地理的な領域
- 無線ネットワークを保証するのに使用するセキュリティ設定。

注意　プロファイルは 1 つではなく複数の AP インスタンス（SSID）に適用される AP パラメータをグループ化したものとして考えることができます。そのため、同じパラメータが複数の AP インスタンスまたは SSID に使用される場合に重複を避けることができます。

無線設定ウィザード

SETUP > Wizard > Wireless Settings メニュー

ここでは一般的で簡単なステップ通してルータの無線インタフェースを設定するように誘導します。

「Wireless Network Setup Wizard」はネットワークに慣れていないユーザに有効です。いくつかの簡単な設定ページを通じて、ご使用の LAN 上の Wi-Fi ™ ネットワークを有効にして、サポートする 802.11 クライアントは設定したアクセスポイントに接続することができます。

1. **SETUP > Wizard > Wireless Settings** の順にメニューをクリックし、以下の画面を表示します。

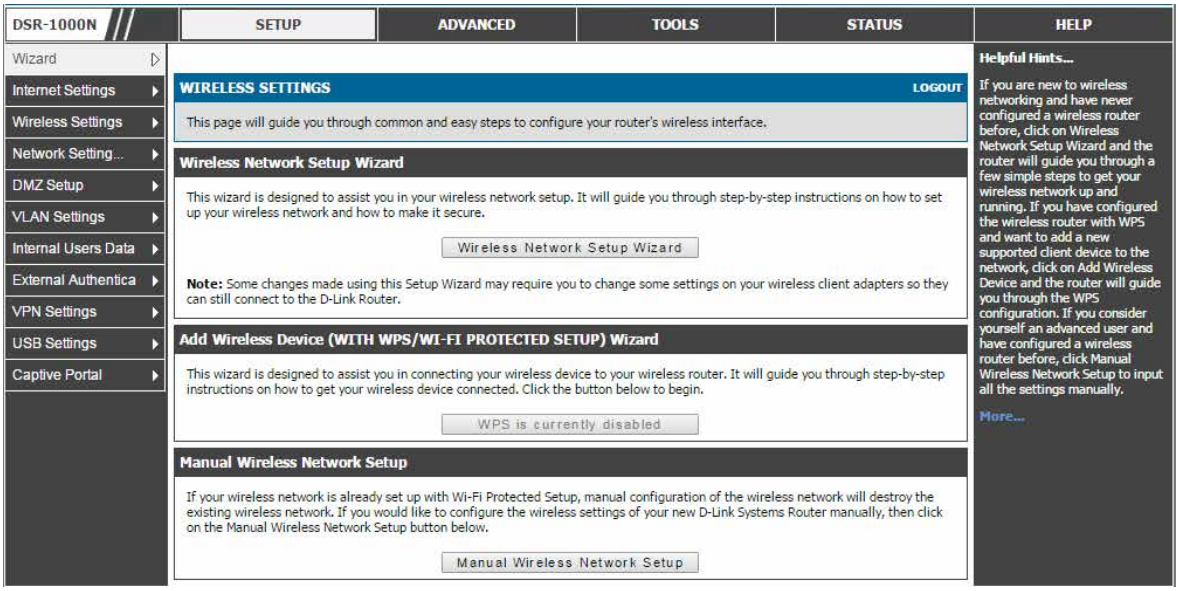


図 6-1　　無線ネットワークセットアップウィザード

Wireless Network Setup Wizard セクション（無線ネットワークセットアップウィザード）

このウィザードは、ルータに新しいアクセスポイントを作成して、安全にするための段階的な手順を提供します。

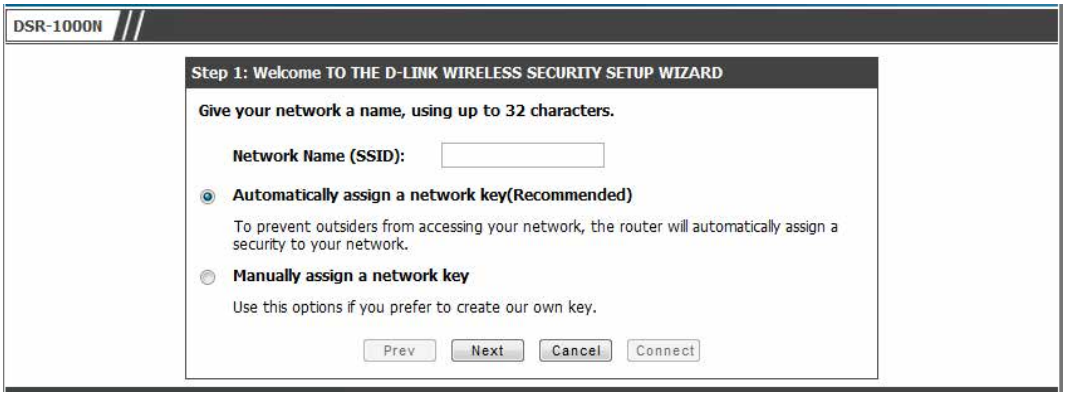


図 6-2　Setup Wizard 画面 -Step1

1. Network Name（SSID）の指定を行います。
「Network Name（SSID）」は、サポートしているクライアントによって検出される AP 識別子です。ウィザードはクライアント側のサポートによって、WPA / WPA2 セキュリティに「TKIP+AES」暗号を使用し、デバイスは同じ事前共有鍵を持つ WPA か WPA2 セキュリティのいずれかを使用してこの AP に関連付けします。

2. 事前共有鍵の設定を行います。

- Automatically assign a network key オプション
ウィザードには、自動的に AP に対してネットワークキーを生成するオプションがあります。このキーは WPA または WPA2 タイプのセキュリティのための事前共有鍵です。この PSK が付与されているサポートクライアントはこの AP に接続できます。（自動に割り当てられた）PSK の初期値は「passphrase」です。

- Manually assign a network key オプション
手動でネットワークキーを設定します。

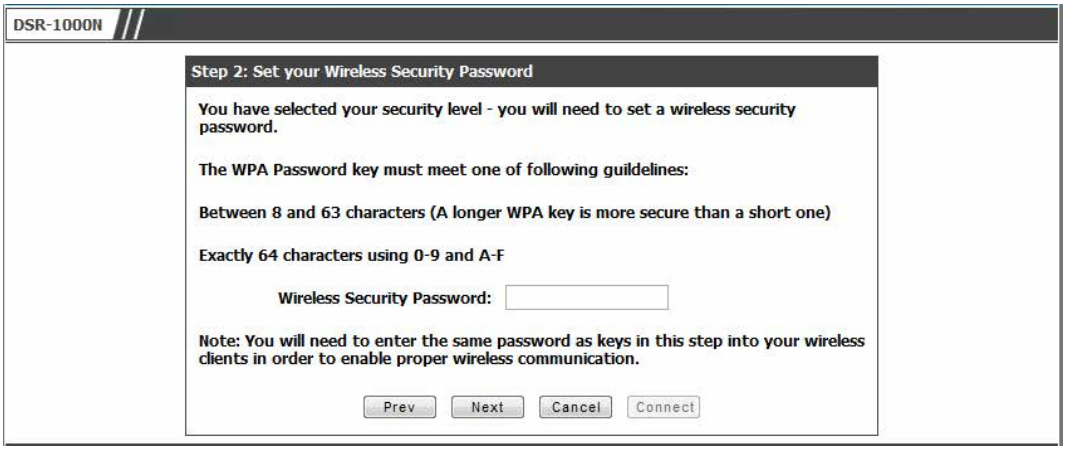


図 6-3　Setup Wizard 画面 -Step1

3. 「Next」ボタンをクリックして、ウィザードの終了画面を表示します。

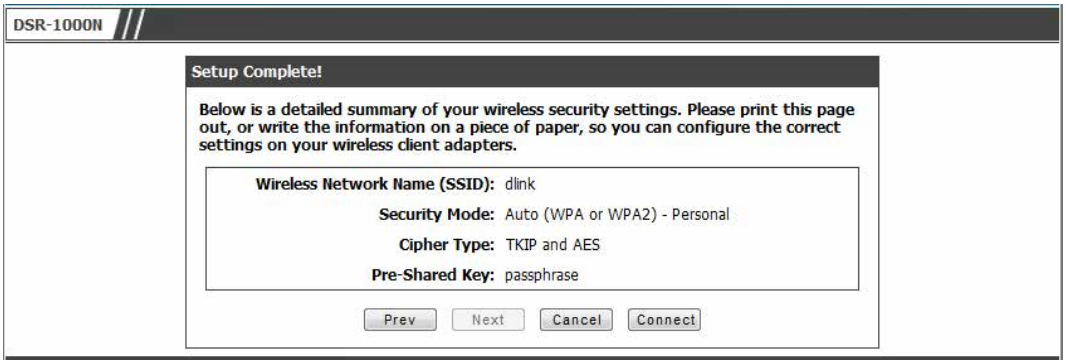


図 6-4　Setup Wizard 画面 -Setup Complete

ウィザードの最後の手順は、「Connect」ボタンをクリックすることです。これは、設定を確認し、この AP を有効にして LAN における有効性をブロードキャストします。

Add Wireless Device Wizard セクション（無線デバイスへの WPS の追加）

ADVANCED > Wireless Settings > WPS で「WPS Status」を「Enabled」（有効）にすると、サポートする WPS クライアントを非常に簡単にネットワークに参加させることができます。

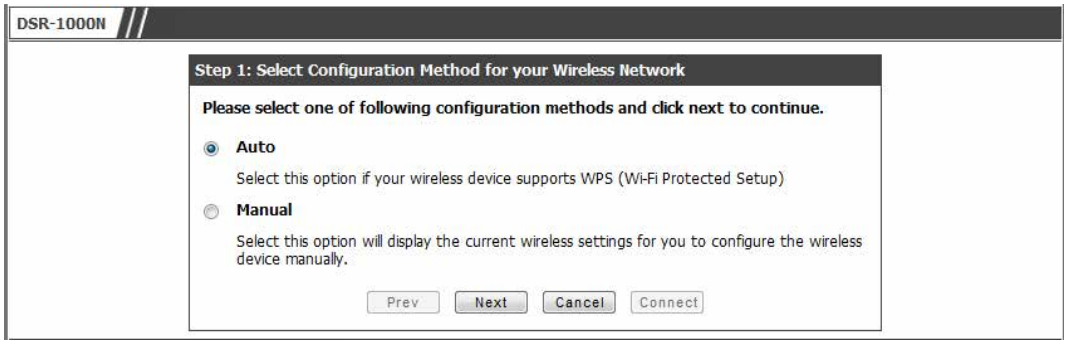


図 6-5　WPS 設定画面 - Step1

無線デバイスを接続するために「Auto」オプションを選択すると、2 つの一般的な WPS 設定オプションが表示されます。:

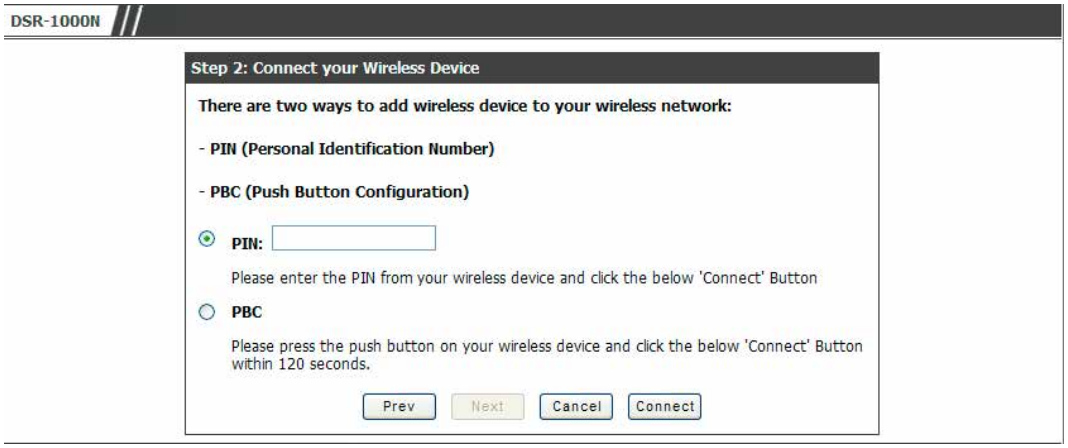


図 6-6　WPS 設定画面 - Step2

- PIN（Personal Identification Number）:
  WPS をサポートする無線デバイスは、英数字の PIN を持っている可能性があり、このフィールドに入力されると、AP はクライアントとのリンクを確立します。セットアップを完了するためには「Connect」ボタンをクリックして、クライアントに接続します。

- PBC（プッシュボタン設定）:
  PBC をサポートする無線デバイスでは、このボタンを押したままとし、2 分間以内に「PBC Connect」ボタンをクリックします。AP は、無線デバイスを検出して、クライアントとのリンクを確立します。

注意 WPS ウィザードを使用するためには、WPA/WPA2 セキュリティを搭載する少なくとも 1 つの AP を有効にして、WPS ウィザードを使用するためには **ADVANCED > Wireless Settings > WPS** ページで「WPS Status」を「Enabled」（有効）にする必要があります。

Manual Wireless Network Setup

Wizard ページのこのボタンは **SETUP > Wireless Settings > Access Points** ページにリンクします。この手動オプションでは、ウィザードによって新しい AP の追加、または既存の AP の設定変更を行うことができます。

無線プロファイル

SETUP > Wireless Settings > Profiles メニュー
無線アクセスポイントのためのプロファイルを設定します。

プロファイルは、複数の AP をまたいで共有できる無線設定のグループで、AP 設定で使用されます。AP を無線クライアントに関連付ける場合に使用する、セキュリティタイプ、暗号化、および認証をプロファイルに割り当てることができます。初期モードは「Open」（セキュリティなし）です。このモードは、無線クライアントがセキュリティプロファイルを使用して設定された AP に接続できるため安全ではありません。

1. **SETUP > Wireless Settings > Profiles** の順にメニューをクリックし、以下の画面を表示します。

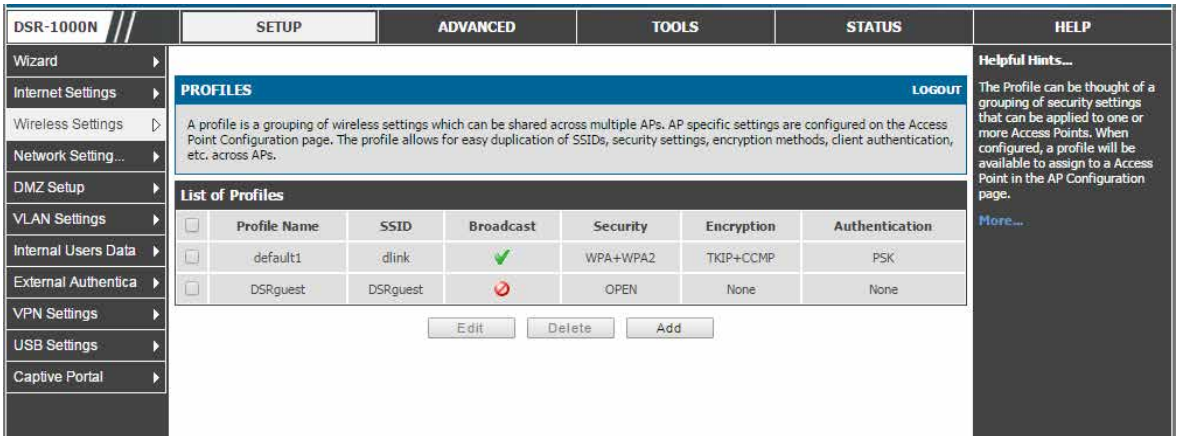


図 6-7　PROFILES 画面

「Available Profiles」のリストでは無線リンクを保証するのに利用可能なオプションの種類を示しています。

新しいプロファイルの作成
設定の組合せを識別する固有のプロファイル名を使用します。このプロファイルを使用して AP と通信を行うために、クライアントが使用する識別子となる固有の SSID を設定します。SSID のブロードキャスト選択することで、AP の範囲内にある互換性を持つ無線クライアントはこのプロファイルを検出できます。

1. 「Add」ボタンをクリックし、以下の画面を表示します。

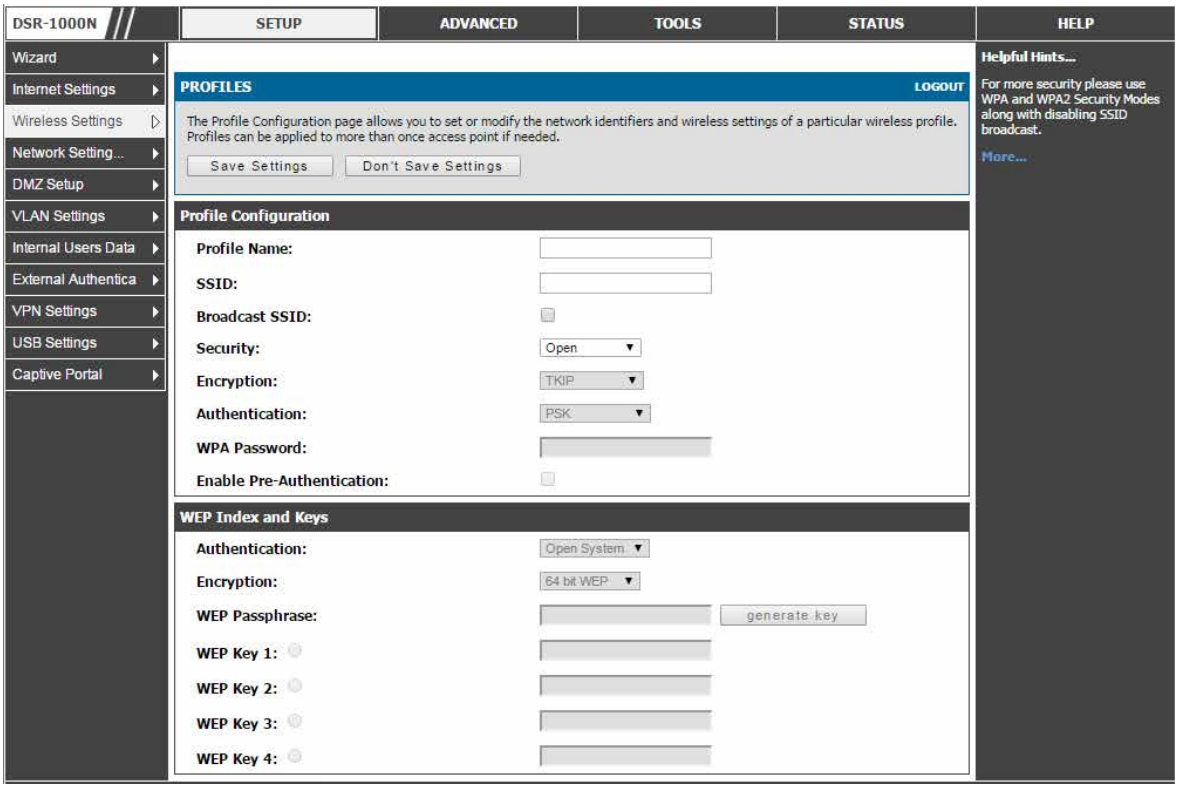


図 6-8　PROFILES 画面 - Add

APはWEP、WPA、WPA2、およびWPA+WPA2オプションを含むすべての802.11の高度なセキュリティモードを提供します。アクセスポイントのセキュリティは以下の「Profile Configuration」セクションの「Security」の選択によって設定されます。:

項目	説明
OPEN	この無線ゲートウェイに未認証デバイスがアクセスすることを許可するためにパブリックに「オープン」なネットワークを作成します。
WEP （Wired Equivalent Privacy）	スタティックな（事前共有）鍵を AP と無線クライアント間で共有することを必要とします。WEP は 802.11n データ速度をサポートしないことに注意してください。これは、旧式の 802.11 接続に適しています。
WPA （Wi-Fi Protected Access）	WEP より強い無線セキュリティのために選択します。必要に応じて、WPA の暗号化では TKIP と CCMP も使用します。認証は、「PSK」（事前共有鍵）、「RADIUS」（RADIUS サーバを持つエンタープライズモード）、または「PSK+RADIUS」（両方）とすることができます。WPS は 802.11n データ速度をサポートしないことに注意してください。これは、旧式の 802.11 接続に適しています。
WPA2	このセキュリティタイプは PSK（事前共有鍵）またはエンタープライズ（RADIUS サーバ）認証のいずれかの場合に CCMP 暗号化（および、TKIP 暗号化を追加するオプション）を使用します。
WPA + WPA2	これは暗号化アルゴリズムの TKIP および CCMP の両方を使用します。WPA クライアントは TKIP を使用し、WPA2 クライアントは CCMP 暗号化アルゴリズムを使用します。

「Save Settings」ボタンをクリックして設定内容を保存および適用します。

注意 「WPA+WPA2」はデバイスがサポートする中で最も強力なセキュリティを使用して AP に接続できるセキュリティオプションです。このモードでは、（古い無線プリンタなど）WPA2 キーだけをサポートする旧式のデバイスは、他の全無線クライアントが WPA2 を使用している安全な AP に接続することができます。

WEP セキュリティ

「Profile Configuration」の「Security」で「WEP」がセキュリティオプションとして選択されると、このセキュアな無線ネットワークへのアクセスを希望するクライアントと共有する固有のスタティックキーを設定する必要があります。このスタティックキーは覚えやすいパスフレーズと選択された暗号化長から生成されます。

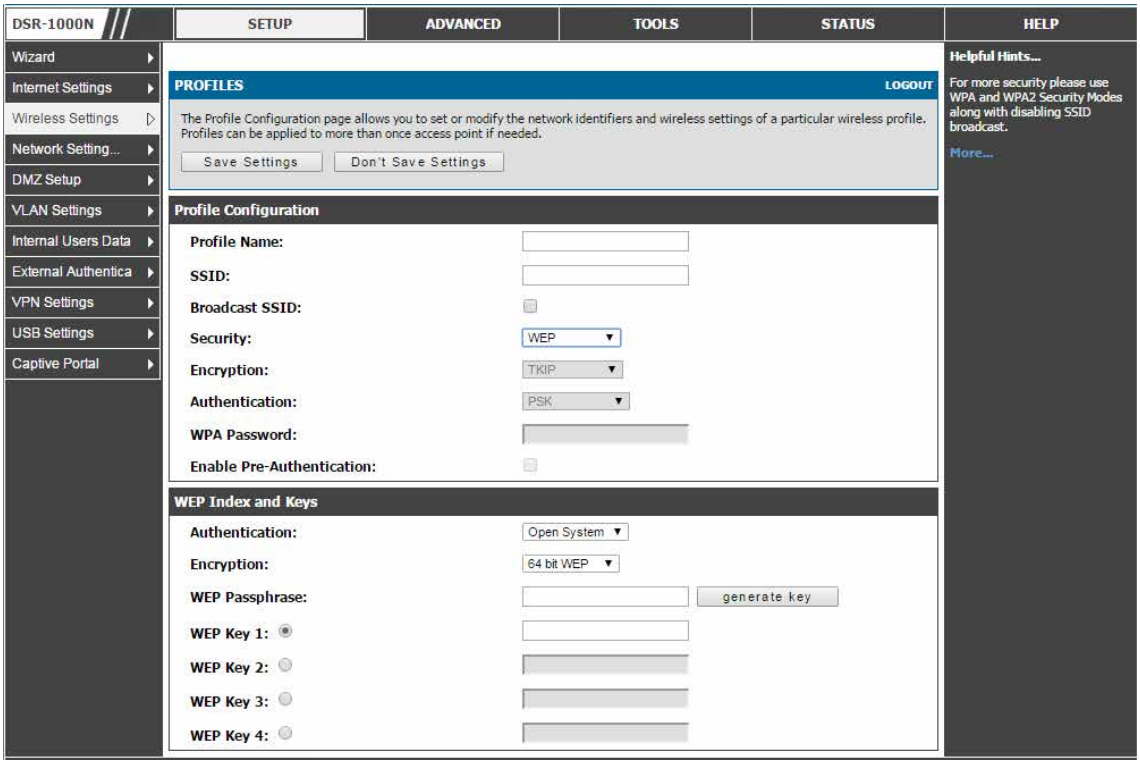


図 6-9　ネットワークセキュリティを設定するプロファイル構成

「WEP Index and Keys」セクションで以下の項目を指定します。

項目	説明
Authentication	「Open System」または「Shared Key」を選択します。
Encryption	暗号キーのサイズ（64 bit WEP または 128 bit WEP）を選択します。大きいサイズのキーほど強い暗号化を提供するため、キーの解読が難しくなります。
WEP Passphrase	4 つのユニークな WEP キーを生成するためには、暗号化キーサイズで決定されている長さの英数字のフレーズを入力して「generate Key」ボタンをクリックします。
WEP Key1-4	認証に使用するキーの 1 つを選択します。このデバイスに接続するためには、選択キーを無線クライアントと共有する必要があります。

「Save Settings」ボタンをクリックして設定内容を保存および適用します。

PSK を持つ WPA または WPA2

事前共有鍵（PSK）は、AP とクライアントの両方に設定された既知のパスフレーズであり、無線クライアントを認証するのに使用されます。アクセス可能なパスフレーズは 8 ～ 63 文字です。「Profile Configuration」セクションの「WPA Password」に入力します。

アクセスポイントの作成と使用

SETUP > Wireless Settings > Access Points メニュー

このデバイスに設定済みアクセスポイント (AP) を表示します。このサマリリストから、各 AP（すべての帯域）のステータスについて調査し、AP パラメータ設定にアクセスできます。

プロファイル（セキュリティ設定のグループ）を一度作成すると、ルータ上の AP にそれを割り当てることができます。AP の SSID は 802.11 環境にその有効性をブロードキャストするために設定され、WLAN ネットワークを確立するために使用されます。

AP 設定ページでは、新しい AP を作成して、利用可能なプロファイルの 1 つをそれにリンクすることができます。このルータは仮想アクセスポイント（VAP）として参照される複数の AP をサポートしています。固有の SSID を持つ各仮想 AP は、独立しているアクセスポイントとしてクライアントには現れます。この有益な機能は、ルータの周波数帯域がユーザが必要する場合にクライアントグループのセキュリティと処理能力を最適化するように設定できます。

1. **SETUP > Wireless Settings > Access Points** の順にメニューをクリックし、以下の画面を表示します。

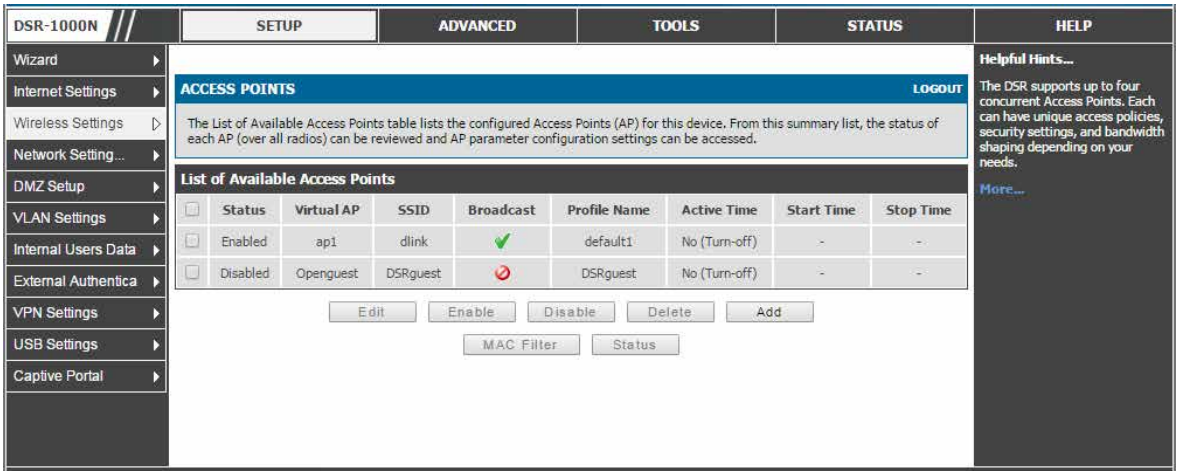


図 6-10　ACCESS POINTS 画面

以下の項目があります。

項目	説明
List of Available Access Points	
Status	AP の有効 / 無効状態を表示します。使用しない場合には無効とし、必要時に有効にすることができます。AP を無効にしても設定は削除されませんが、無線ビーコンの送信は停止します。AP を有効にした場合、無線ネットワークを作成し、コンピュータやその他デバイスが参加して AP に接続するデバイスと、または LAN 上のデバイスと通信することができます。
Virtual AP	この欄はアクセスポイント設定用の名称を表示します。
SSID	SSID（Service Set Identifier）は、この AP がサービスを行う無線ネットワークの名前であり、ブロードキャストがこの AP で有効である場合、802.11 環境にいるクライアントに参照されます。
Broadcast	SSID が AP が送信したビーコンフレームでブロードキャストされるかどうかを示します。SSID がブロードキャストされないと、無線デバイスはネットワーク名（SSID）を参照することはできません。緑色のチェックは、SSID がパブリックにブロードキャストされることを示しています。赤色のアイコンは、SSID がブロードキャストされず、デバイスはこの AP に接続するために正確に SSID を指定する必要があります。

項目	説明
Profile Name	AP に割り当てるセキュリティ、暗号化、および認証組合せに関する簡単な説明です。プロファイルは AP に固有である必要はありません。むしろ無線設定のグループ化が 1 つ以上のアクセスポイントに同時に適用できます。
Active Time	AP が 1 日の一定時間だけ機能するように設定するかどうかを示します。:「Yes」または「No」。
Start Time	AP が有効になる 1 日の時間。
Stop Time	AP が無効になる 1 日の時間。
ボタン	
Edit	選択した AP の設定を編集します。
Enable	選択した AP を有効にします。
Disable	選択した AP を無効にします。
Delete	選択した AP の設定を削除します。
Add	新しい AP を追加します。
MAC Filter	「MAC アドレスフィルタリング」と「ACL ポリシー設定」を設定します。
Status	AP のトラフィック統計情報と接続するクライアントのリストを表示します。

2. 設定済み AP（仮想 AP）のリストは周波数帯域に 1 つの有効な AP とその SSID をブロードキャストしていることを表示します。

VAP の作成

1. 「Add」ボタンをクリックします。AP 名を設定した後に、「Profile」プルダウンメニューは定義済みプロファイルの 1 つを選択するのに使用されます。

注意 AP 名は、GUI から AP を管理するのに使用される一意的識別子であり、AP がブロードキャストを有効にした場合にクライアントによって検出される SSID ではありません。

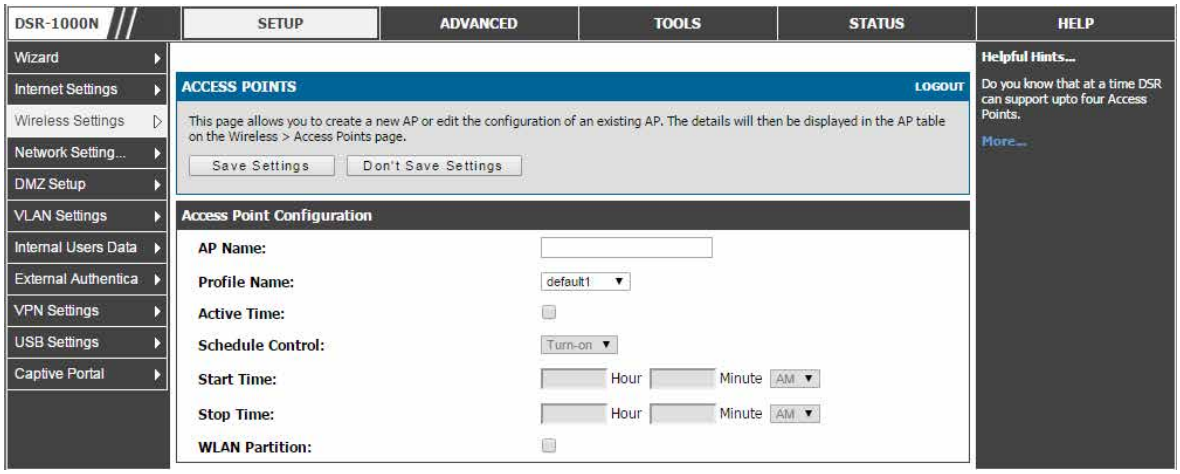


図 6-11　仮想 AP の設定

この AP に開始 / 停止時間の制御を行うことで節電ができます。未使用時には AP を無効にすることで無線電力を節約します。例えば、夕方や週末に、無線クライアントのいないことがわかっている場合には、開始時刻と終了時刻によりアクセスポイントを自動的に有効 / 無効にすることができます。

AP の設定後、**SETUP > Wireless Settings > Access Points** ページで周波数帯域上の AP を有効にする必要があります。AP が無線クライアントの受け入れを有効にすると「Status」欄は、「Enabled」に変更されます。AP が SSID（プロファイルパラメータ）をブロードキャストするように設定されると、ブロードキャストを示す緑色のチェックマークが「List of Available Access Points」に表示されます。

2. 以下の項目を設定します。

項目	説明
AP Name	アクセスポイント名。
Profile Name	設定済みプロファイルのプルダウンメニューからこの AP に接続するクライアントによって使用されるべき暗号化と認証方法を選択します。このリストは **SETUP > Wireless Settings > Profiles** ページでプロファイルを追加することで書き込まれます。
Active Time	この設定を有効にすると、続くスケジュール制御「Schedule Control」および「Start Time」/「Stop Time」欄を指定することができます。
Schedule Control	「Start Time」と「Stop Time」欄で指定された期間、クライアント AP を「Turn-on」（有効）/「Turn-off」（無効）にします。初期値は無効です。
Start Time	スケジュールを開始する時間（時、分、AM/PM）を設定します。
Stop Time	スケジュールを終了する時間（時、分、AM/PM）を設定します。
WLAN Partition	ボックスをチェックして、各無線接続に別々の仮想ネットワークを作成します。本機能が有効になると、各無線クライアントは自身の仮想ネットワークに存在し、他のクライアントと通信することができなくなります。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

VAP の統計情報表示

1. 「List of Available Access Points」で該当するアクセスポイントをチェック後、「Status」ボタンをクリックすることで、AP およびとその AP に接続するクライアントの現在の情報を表示します。

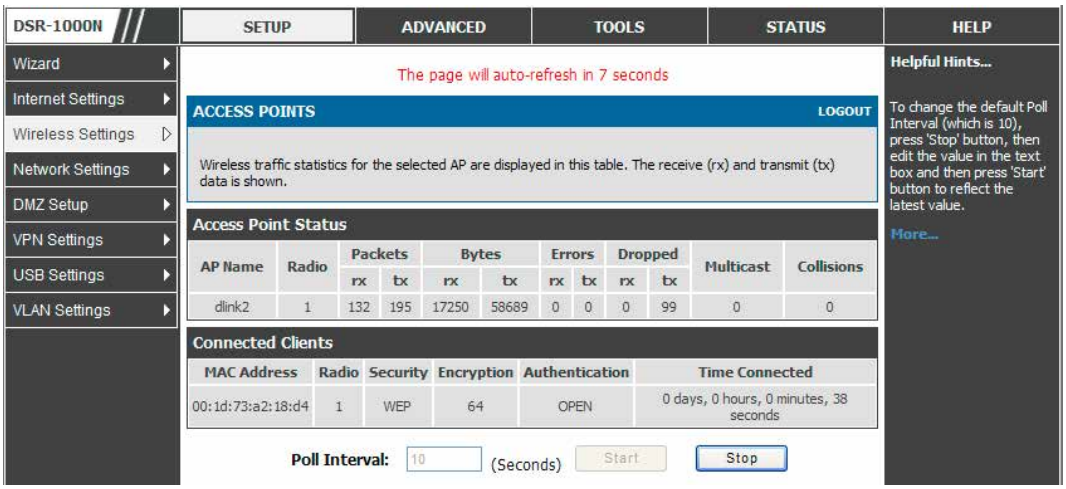


図 6-12　AP の状態

「Statistics」テーブルの各 AP のサマリ状態と比べて、トラフィックの統計情報は個別の AP に対して表示されます。接続するクライアントは、MAC アドレスでソートされて、この特定の AP に接続する時間ならびに無線リンクに使用されるセキュリティパラメータを示します。

「Start」ボタンをクリックすると、統計情報の収集を開始し、「Stop」ボタンをクリックすると、統計情報の収集を中断します。「Poll Interval」でこのページの情報を更新する間隔（秒）を変更することができます。

MAC フィルタ設定

• MAC フィルタの表示

1. 「List of Available Access Points」で該当するアクセスポイントをチェック後、「MAC Filter」ボタンをクリックすると、以下の画面が表示されます。

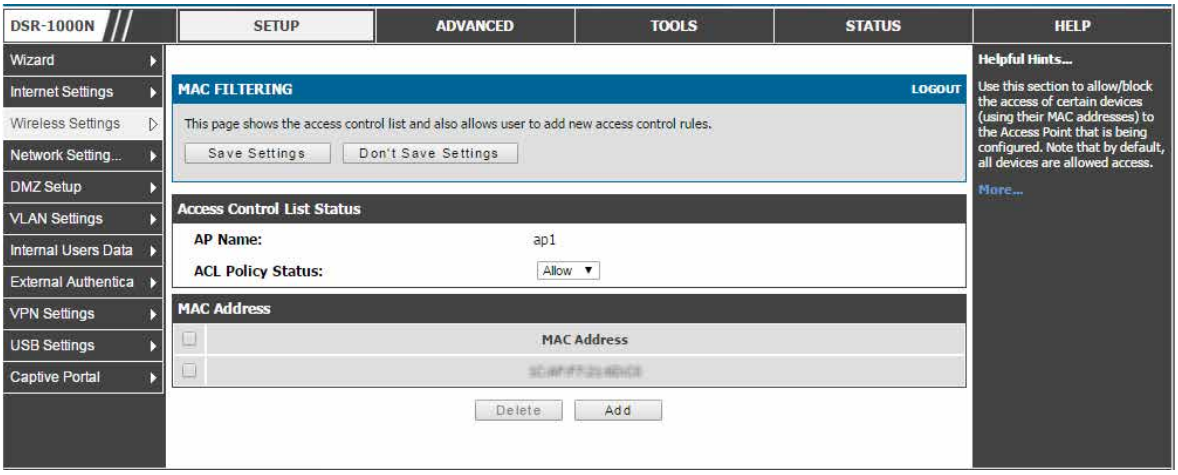


図 6-13　アクセスコントロールリスト表示画面

このページではアクセスコントロールリストを表示します。MAC アドレスを使用してアクセスポイントに特定のデバイスへのアクセスを許可 / ブロックすることができます。また、新しいアクセスコントロールルールの追加をすることができます。

2. 以下の項目を設定します。

項目	説明
Access Control List Status	
AP Name	プロファイル名。
ACL Policy Status	アクセスポリシーのタイプ（Open、Allow、Deny）を指定します。 • Allow - MAC アドレスがリストに表示されるクライアントによる接続を許可します。 • Deny - MAC アドレスがリストに表示されるクライアントによる接続を拒否します。 • Open - すべてのクライアントが接続することを許可して、リストに基づくアクセスをフィルタしません。（初期値）
MAC Address	
MAC アドレスのリストに追加したいクライアントの MAC アドレスを表示します。	
ボタン	
Add	フィルタする MAC アドレスを追加します。
Delete	チェックした MAC アドレスを削除します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

• MAC アドレスの追加

1. 「ACL Policy Status」で「Allow」または「Deny」を選択後、「Save Settings」ボタンをクリックします。

2. 「Add」ボタンをクリックして、以下の画面を表示します。

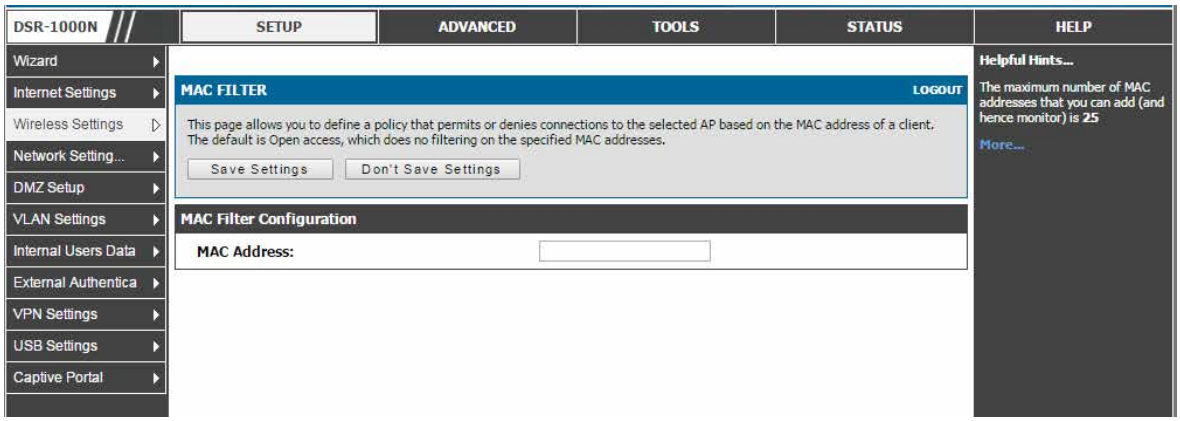


図 6-14　MAC フィルタ設定画面

3. MAC アドレスのリストに追加するクライアントの MAC アドレスを入力し、「Save Settings」ボタンをクリックして設定内容を保存および適用します。MAC アドレスの形式は XX:XX:XX:XX:XX:XX（X は 0-9 の数値、または A-F の英数字）です。

仮想 AP の利点

- 高スループット：
  802.11b、802.11g および 802.11n クライアントがこのルータ経由で LAN にアクセスするものとすると、3 つの VAP を作成することで各クライアントグループに管理またはトラフィックの絞り込みを行うことができます。802.11b クライアントのネットワークには固有の SSID を作成することができます。また、802.11n クライアントには別の SSID を割り当てることができます。それぞれが異なるセキュリティパラメータを持つことができます。リンクの SSID とセキュリティがプロファイルで決定されます。この方法により旧式のクライアントはより能力の高い 802.11n クライアントの総処理能力を低下させないでネットワークにアクセスできます。

- 高セキュリティ：
  多数のクライアントでは WPA2 セキュリティを使っている一方で、WEP セキュリティだけを利用するレガシークライアントを選択することをサポートする必要があるかもしれません。異なる SSID と異なるセキュリティパラメータで設定された 2 つの VAP を作成することで、両タイプのクライアントが LAN に接続できます。WPA2 がより安全であるため、この SSID をブロードキャストし、このシナリオ内ではレガシーデバイスは少ないため、WEP を使った VAP の SSID はブロードキャストしたくないかもしれません。

無線帯域の詳細設定の調整

SETUP > Wireless Settings > Radio Settings メニュー
ここでは本製品で有効である AP に有効なチャンネルと電力レベルを設定します。

ルータにはデュアルバンドの 802.11n 周波数帯域があり、2.4 GHz または 5 GHz 動作周波数のいずれかを選択できることを意味しています。（同時には選択できません。）選択した動作周波数に基づいて、モード選択では旧式の接続または 802.11n 接続のみ（または両方）が定義済み AP で受け付けられるかどうかを定義できます。

1. **SETUP > Wireless Settings > Radio Settings** の順にメニューをクリックし、以下の画面を表示します。

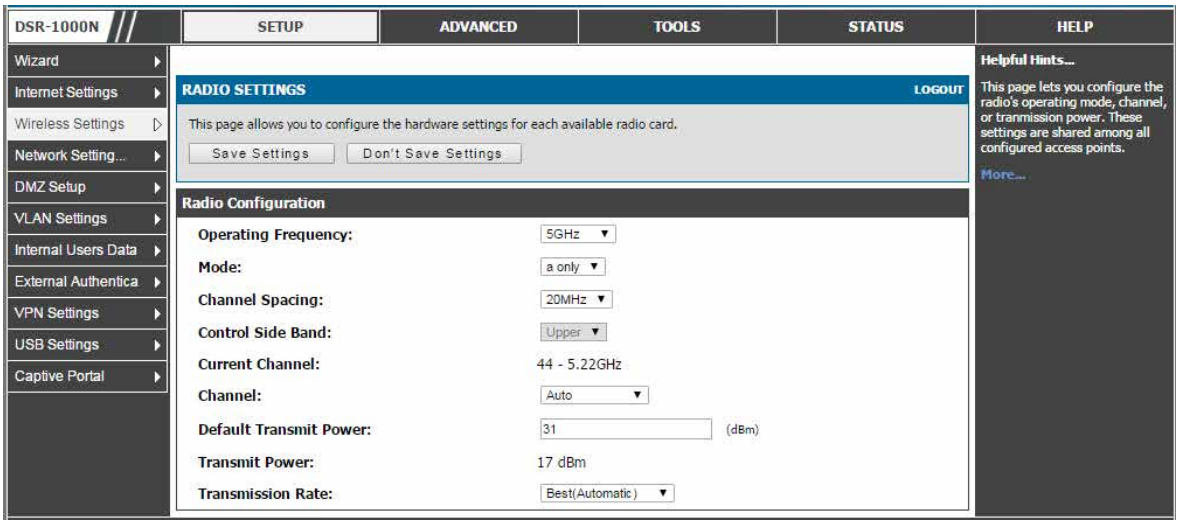


図 6-15　無線カード設定のオプション

この無線帯域で承認された 802.11n では適切なブロードキャスト（「na」または「ng」など）の選択が必要で、次に 802.11n トラフィックにチャンネル間隔と制御側の帯域を定義します。初期設定は多くのネットワークに適しています。例えば、チャンネル幅を 40MHz に変更すると、より速い 802.11n クライアントをサポートするように帯域幅を改善できます。

利用可能な伝送チャンネルは、ルータのリージョン設定に基づき規定上の制約によって管理されます。最大の送信電力は規制によって同様に管理されます。デフォルトの最大値から、周波数帯の出力強度を減らすためのオプションがあります。

WMM 設定

SETUP > Wireless Settings > WMM メニュー

WMM（Wi-Fi Multimedia）は、IEEE 802.11 ネットワークに基本的な QoS（Quality of Service）を提供します。WMM は、音声、ビデオ、ベストエフォート、およびバックグラウンドの 4 つの AC（Access Categories: アクセスカテゴリ）に従ってトラフィックを優先させます。

1. **SETUP > Wireless Settings > WMM** の順にメニューをクリックし、以下の画面を表示します。

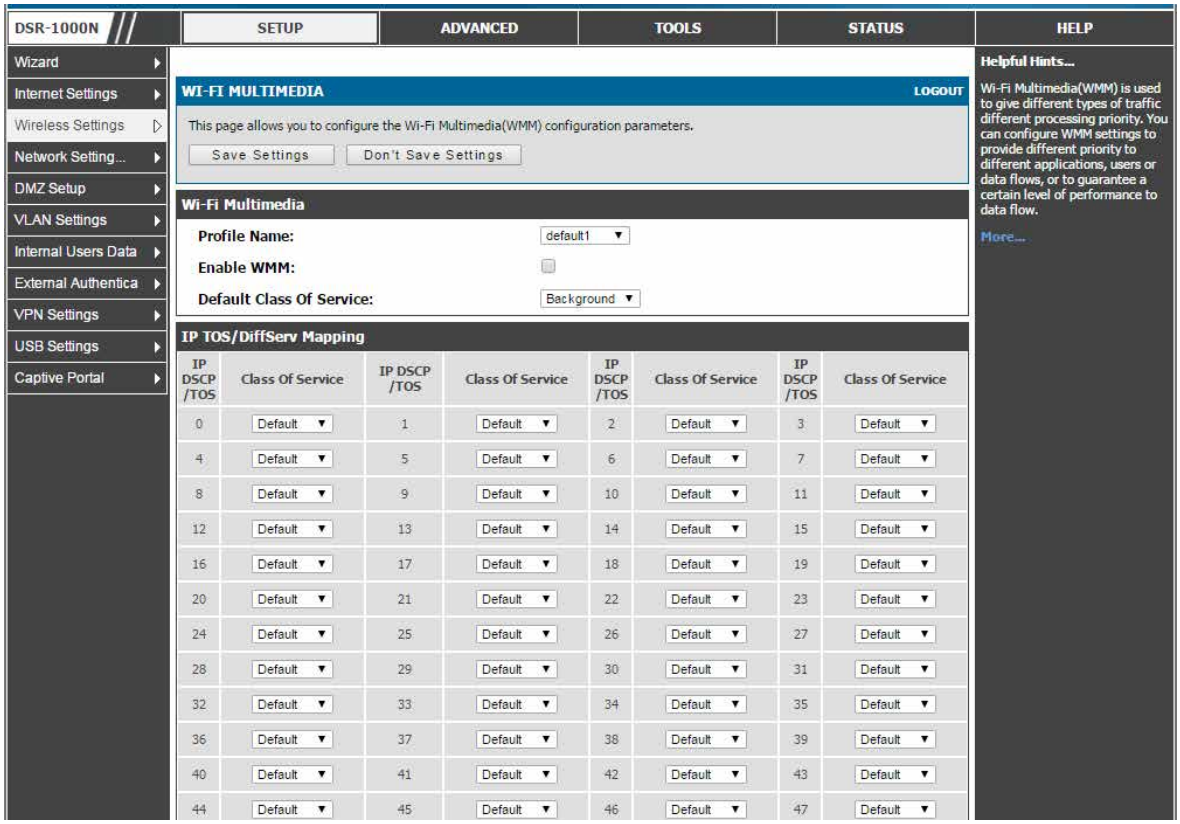


図 6-16　Wi-Fi Multimedia 画面

2. 以下の項目を設定します。

項目	説明
Wi-Fi Multimedia	
Profile Name	無線設定で利用可能なプロファイルを選択できます。
Enable WMM	マルチメディア伝送を改善するために WMM を有効にできます。
Default Class Of Service	利用可能なアクセスカテゴリ（Voice、Video、Best Effort および Background）を選択できます。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

WDS 設定

SETUP > Wireless Settings > WDS メニュー

WDS（Wireless Distribution System）は、ネットワークにおいてアクセスポイントの無線相互接続を有効にするシステムです。本機能は、同じタイプのデバイス間でのみ正常な動作を保証されます。

1. **SETUP > Wireless Settings > WDS** の順にメニューをクリックし、以下の画面を表示します。

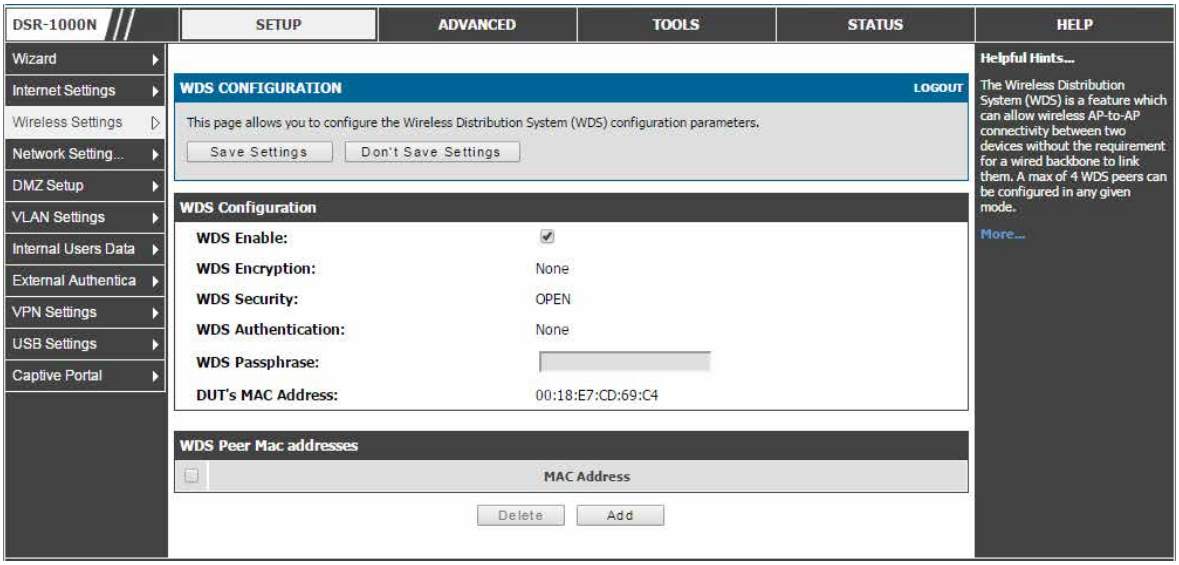


図 6-17　WDS CONFIGURATION 画面

注意 本機能は、同じタイプ（つまり、同じチップセット / ドライバを使用する）のデバイス間でのみ正常動作が保証されます。本シリーズでは DSR-1000N 間となります。

WDS リンクが有効である場合には、デフォルトアクセスポイントと同じセキュリティ設定を使用します。WDS リンクが適切な WPA/WPA2 をサポートしないと、WPA キーのハンドシェークが実行されません。代わりに、WDS Peer と共に使用されるセッションキーは、（WPA PMK を計算するのに使用するものと同じ）ハッシュ関数を使用して計算されます。本関数には、（WDS ページで管理者が設定可能な）PSK と（設定ができない）内部の「magic」文字列を入力します。

事実上は、WDS リンクは、デフォルト AP に設定された暗号化に従って TKIP/AES 暗号化を使用します。デフォルト AP の場合、暗号を組み合わせて使用します（TKIP+AES）。WDS リンクでは AES 暗号化方式を使用します。

注意 WDS リンクが適切に機能するためには、WDS ピアにおける無線帯域設定を同一にする必要があります。

WDS ページは 2 つのセクションから構成されています。

項目	説明
WDS Configuration	
すべての WDS ピアによって共有される一般的な WDS 設定を提供します。	
WDS Enable	ボックスをチェックします。
WDS Encryption	使用する暗号化のタイプを表示します。OPEN/64 ビット WEP/128 ビット WEP/TKIP/AES の 1 つです。ボックスを通過するのに使用されるパラメータ（CCMP または AES）です。
WDS Security	現在 WDS リンクで実行されているスキームを表示します。
WDS Authentication	現在 WDS リンクで実行されているスキームを表示します。
WDS Passphrase	これは選択した暗号化が TKIP/CCMP である場合に必要です。ASCII 文字列（8-63 文字）とします。WDS 設定ページでは、セキュリティを TKIP/AES モードに設定する場合、本欄は必須であり、2 つの WDS ピアは同一にある必要があります。WDS リンクは接続に PSK としてこれを使用します。
DUT's MAC Address	デバイスの MAC アドレスを表示します。これを本デバイスに接続する WDS ピアに指定するものとします。（同様に、2 つのデバイス間で WDS リンクを確立するために、WDS ピアの MAC アドレスを本デバイスに設定するものとします。）
WDS Peer Mac Addresses	
現在デバイスで設定されている WDS ピアのリストを表示します。「Add」/「Delete」ボタンを使用してピアエントリを追加 / 削除できます。最大 4 つまでの WDS ピアをいずれのモードでも設定することができます。	

注意 DSR に WDS 機能を設定する場合、各デバイスは同一の無線設定（無線モード、暗号化、認証方式、WDS パスフレーズ、WDS MAC アドレス、および無線 SSID）を持つ必要があります。

WDS ピアの設定

1. 「Add」ボタンをクリックして以下の画面を表示します。

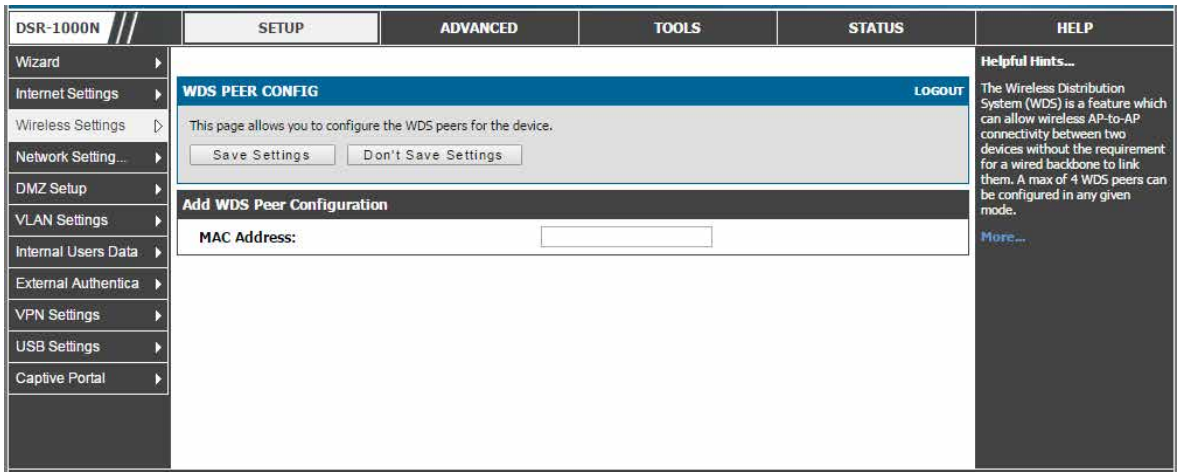


図 6-18　WDS ピアの追加

2. ピアの MAC アドレスを指定後、「Save Settings」ボタンをクリックします。

高度な無線設定

ADVANCED > Wireless Settings > Advanced Wireless メニュー
ここでは無線に詳細な設定を行います。

経験豊富な無線の管理者は本ページの 802.11 の通信パラメータを変更することができます。通常、初期設定は多くのネットワークに適しています。各設定パラメータの使用に関する詳細については GUI に統合しているヘルプを参照してください。

1. **ADVANCED > Wireless Settings > Advanced Wireless** の順にメニューをクリックし、以下の画面を表示します。

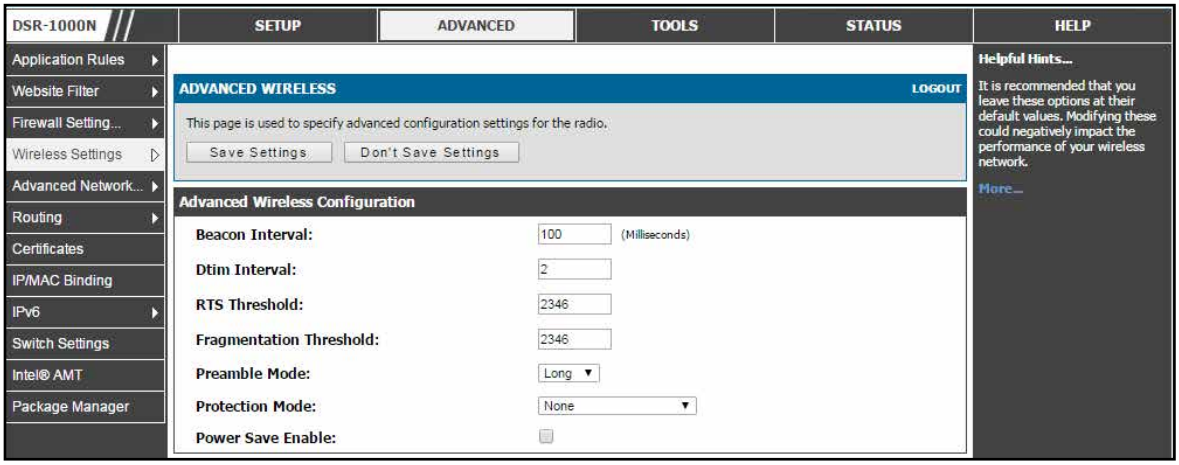


図 6-19　高度な無線通信設定

2. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

WPS 設定

ADVANCED > Wireless Settings > WPS メニュー
ここでは Wi-Fi Protected Setup（WPS）設定パラメータの定義と変更を行うことができます。

WPS はサポートする無線クライアントをネットワークに追加する簡単な方法であり、WPA または WPA2 セキュリティを使用する AP にだけ使用できます。

1. **ADVANCED > Wireless Settings > WPS** の順にメニューをクリックし、以下の画面を表示します。

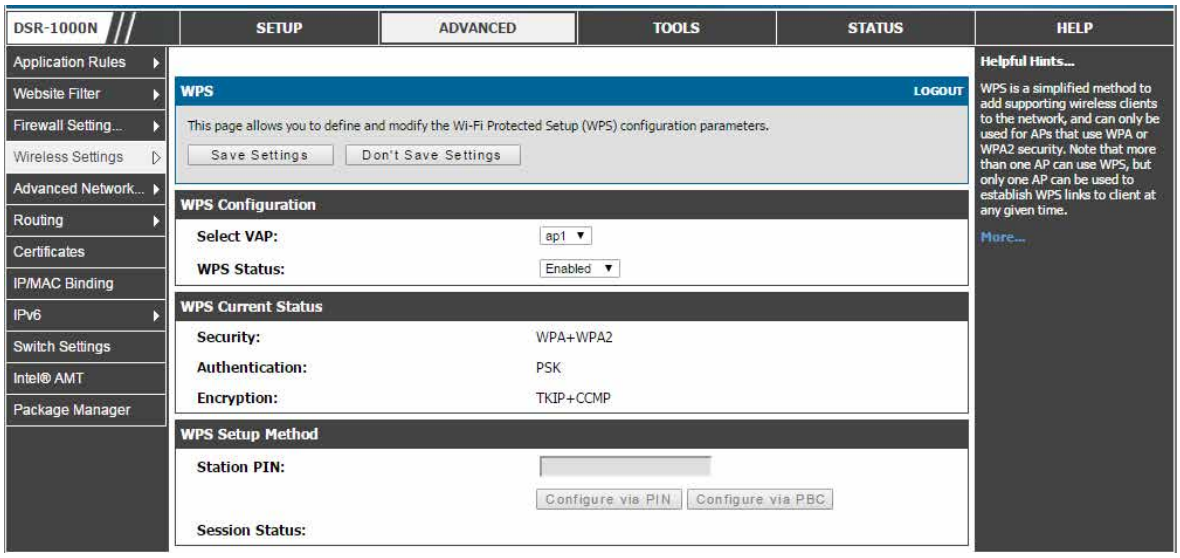


図 6-20　WPA/WPA2 プロファイルを持つ AP の WPS 設定

WPS を使用するためには、このセキュリティを使用して設定されている AP の「Select VAP」プルダウンメニューから適する VAP を選択して、「WPS Status」でこの AP の WPS ステータスを有効にします。

「WPS Current Status」セクションでは選択した AP のセキュリティ、認証、および暗号化設定について概説します。これらは AP のプロファイルと一致しています。WPS には利用可能な 2 つの設定オプションがあります。:

- PIN（Personal Identification Number）:
  WPS をサポートする無線デバイスが、英数字の PIN を持っている場合、この欄に PIN を入力します。ルータは「PIN」フィールドの下にある「Configure via PIN」ボタンを直ちにクリックした後、60 秒以内に接続します。クライアントが接続したことを示す LED 表示はありません。

- PBC（Push Button Configuration）:
  PBC をサポートする無線デバイスでは、このボタンを押したまま、2 分以内に「Configure via PBC」ボタンをクリックします。AP は、無線デバイスを検出して、クライアントとのリンクを確立します。

注意　1 つ以上の AP が WPS を使用できますが、どんな場合もクライアントとの WPS リンクを確立するのに 1 つの AP しか使用できません。

このルータには、インターネットへの接続を確立するのに使用する 2 つの WAN ポートがあり、次の ISP 接続タイプをサポートしています : DHCP、Static、PPPoE、PPTP、または L2TP。

ご使用のインターネットサービスプロバイダ（ISP）を使用したインターネットサービスが手配されているものとします。ルータをセットアップするのに必要である設定情報については ISP またはネットワーク管理者にご確認ください。

第 7 章　安全なプライベートネットワーク設定

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

設定項目	説明	参照ページ
ファイアウォールルール	ファイアウォールの設定について説明します。	100 ページ
ルールスケジュールの定義	ルールに割り当てるスケジュールの設定を行います。	102 ページ
ファイアウォールルールの設定手順	ファイアウォールの設定手順について説明します。	103 ページ
IPv6 ファイアウォールルールの設定手順	IPv6 ファイアウォールの設定手順について説明します。	107 ページ
ファイアウォールルール設定の例	ファイアウォールの設定例について説明します。	108 ページ
カスタムサービスにおけるセキュリティ	ファイアウォールルール設定で利用可能なサービスを追加します。	111 ページ
ALG サポート	アプリケーションレイヤプロトコルを選択します。	112 ページ
SMTP ALG 設定	メール ID または題名に基づいてメールをブロック / 許可します。	113 ページ
ファイアウォールのための VPN パススルー	VPN トラフィックを許可するようにファイアウォール設定を行います。	116 ページ
ブリッジモードのファイアウォール	ブリッジの一部である 2 つのポート間で適用されるファイアウォールルールを設定します。	117 ページ
アプリケーションルール	アプリケーションルールを設定します。	119 ページ
Web コンテンツフィルタリング	LAN と WAN 間に簡単に Web コンテンツをフィルタするアクセスポリシーを作成します。	120 ページ
IP/MAC バインディング	LAN ノードを照合する IP/MAC のバインドを行います。	123 ページ
IPS（Intrusion Protection シグネチャ）	スタティックな攻撃シグネチャを指定し、一般的な攻撃を検出して防御します。	125 ページ
インターネット攻撃からの保護	LAN と WAN ネットワークを一般的な攻撃から保護する設定を行います。	126 ページ
IGMP プロキシの設定	マルチキャストトラフィックを管理する IGMP プロキシを設定します。	127 ページ
Intel® AMT	Intel® AMT サービスを設定します。	128 ページ

内向きおよび外向きのインターネットトラフィックを選択的にブロックおよび許可するためには、ルータが使用するルールを作成および適用することによってネットワークを安全にすることができます。また、ルールを適用する方法、ルールを適用する人を指定します。そのためには、以下の項目を定義する必要があります。:

- サービスまたはトラフィックタイプ（例 : Web 閲覧、VoIP、他の標準的なサービス、およびユーザが定義するカスタムサービス）。
- トラフィックの送信元と送信先を指定することよるトラフィックの方向。これは、「From Zone」（LAN/WAN/DMZ）と「To Zone」（LAN/WAN/DMZ）を指定することによって、行われます。
- ルータがルールを適用するスケジュール。
- ルータが許可またはブロックするキーワード（ドメイン名内または Web ページの URL）。
- 指定スケジュールで指定サービスの内向きおよび外向きインターネットトラフィックを許可またはブロックするためのルール。
- インターネットにアクセスすべきでないデバイスの MAC アドレス。
- ポート番号によって定義されるような特定のサービスへのアクセスを許可またはブロックするために、ルータに通知するポートトリガ。
- ルータへの送信を希望するレポートとアラート。

例えば、時刻、Web アドレス、および Web アドレスキーワードに基づいたアクセスを制限するポリシーを設定することができます。チャットルームやゲームなどの LAN 上のアプリケーションとサービスによるインターネットアクセスをブロックすることができます。ご使用のネットワーク上における特定の PC グループが WAN またはパブリック DMZ ネットワークによってアクセスされるのを防ぐことができます。

ファイアウォールルール

デフォルト外向きポリシー

ADVANCED > Firewall Settings > Default Outbound Policy メニュー

ルータにデフォルト外向きポリシーを設定します。

1. **ADVANCED > Firewall Settings > Default Outbound Policy** の順にメニューをクリックし、以下の画面を表示します。

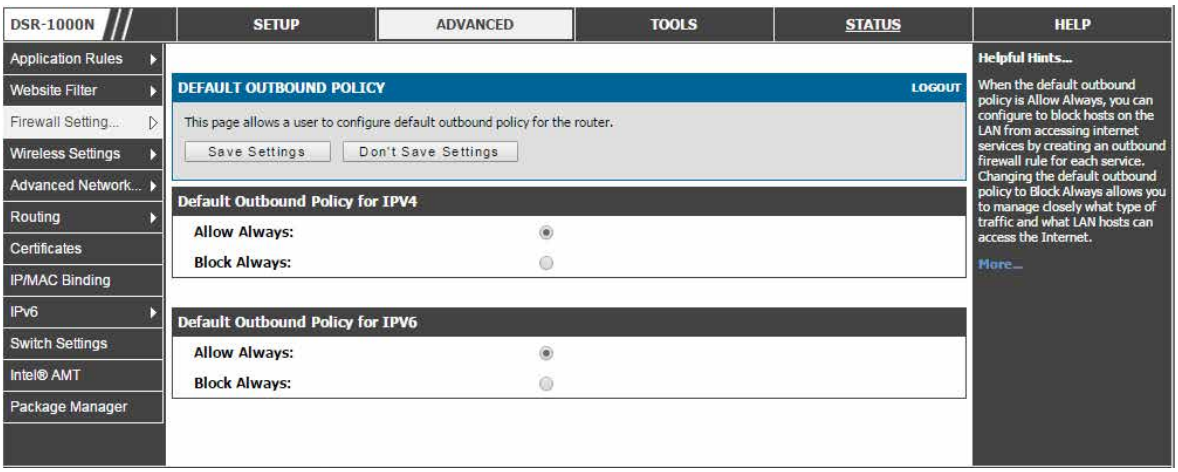


図 7-1　　内向きポリシーの設定

外向きポリシーが「Allow Always」（すべて許可）である場合、各サービスに外向きファイアウォールルールを作成することで、ホストのインターネットサービスへアクセスをブロックすることができます。デフォルトの外向きポリシーを「Block Always」（すべてブロック）に変更することで、どのトラフィックタイプおよび LAN ホストがインターネットサービスへアクセス可能かを細かく管理することができます。

2. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ファイアウォールルールの設定

ADVANCED > Firewall Settings > Firewall Rules メニュー

ファイアウォールは、ネットワーク管理者によって指定されたルールに従って、選択的に特定のタイプのトラフィックをブロックまたは許可するセキュリティメカニズムです。

ここではご使用のネットワークに対する、およびご使用のネットワークからのトラフィックを制御するファイアウォールルールを管理することができます。利用可能なファイアウォールルールのリストには本デバイス用のすべてのファイアウォールルールがあり、ファイアウォールルールにいくつかの操作を許可しています。

内向き（WAN から LAN/DMZ）ルールはご使用のネットワークに入力されるトラフィックに対してアクセス制限を行い、選択的に特定の外部ユーザのみ特定のローカルリソースにアクセスすることを許可することができます。初期値では、LAN または DMZ からの要求に応答する場合を除き、安全でない WAN 側からセキュアな LAN に対するすべてのアクセスをブロックします。外部のデバイスがセキュアな LAN 上のサービスにアクセスすることを許可するために、各サービスに内向きのファイアウォールルールを作成する必要があります。

入力トラフィックを許可したい場合、ルータの WAN ポートの IP アドレスをパブリックに知らせる必要があります。これを「ホストの可視化」と呼びます。アドレスを知らせる方法は WAN ポートの設定方法によって異なります。このルータでは、スタティックなアドレスを WAN ポートに割り当てる場合には IP アドレスを使用し、または、ご使用の WAN アドレスがダイナミックである場合は、DDNS（Dynamic DNS）名を使用できます。

外向き（LAN/DMZ から WAN）ルールはご使用のネットワークから出力するトラフィックに対してアクセス制限を行い、選択的に特定のローカルユーザのみ外部リソースにアクセスすることを許可することができます。外向きの初期ルールは、安全なゾーン（LAN）からパブリック DMZ または安全でない WAN のいずれかへのアクセスを許可するものです。また、DMZ から安全でない WAN までのアクセスも拒否するものです。**ADVANCED > Firewall Settings > Default Outbound Policy** ページでこの初期動作を変更することができます。デフォルトの内向きポリシーが「Allow Always」（すべて許可）である場合、各サービスに内向きファイアウォールルールを作成することで、ホストのインターネットサービスへアクセスをブロックすることができます。

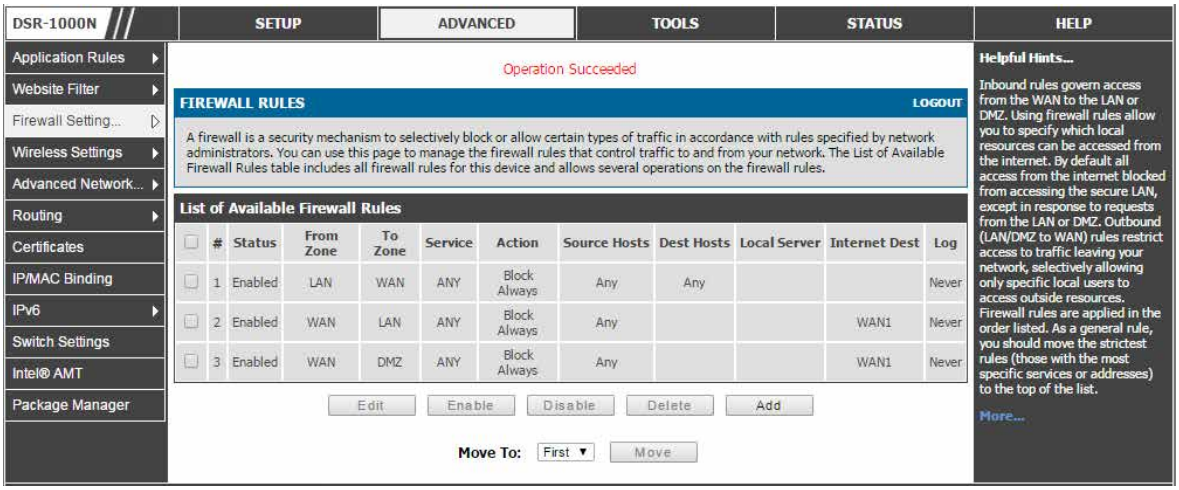


図 7-2　利用可能なファイアウォールルールのリスト

注意　ファイアウォールルール設定手順については、103 ページの「ファイアウォールルールの設定手順」を参照してください。

ファイアウォールルールに行うアクションは以下の通りです。

項目	説明
Edit	選択されたルールを編集するためにはファイアウォールルール設定ページをオープンします。
Enable	選択したファイアウォールルールを有効にします。
Disable	選択したファイアウォールルールを無効にします。
Delete	選択したファイアウォールルールを削除します。
Add	新しいファイアウォールルールを追加します。

ルールスケジュールの定義

TOOLS > Schedules メニュー
ここでは新しいスケジュールに曜日と時刻を定義することができます。

定義済みスケジュールに関連付けると、ファイアウォールルールを自動的に有効または無効にすることができます。ファイアウォールルール設定ページでこのスケジュールを選択することができます。

1. **TOOLS > Schedules** の順にメニューをクリックし、以下の画面を表示します。

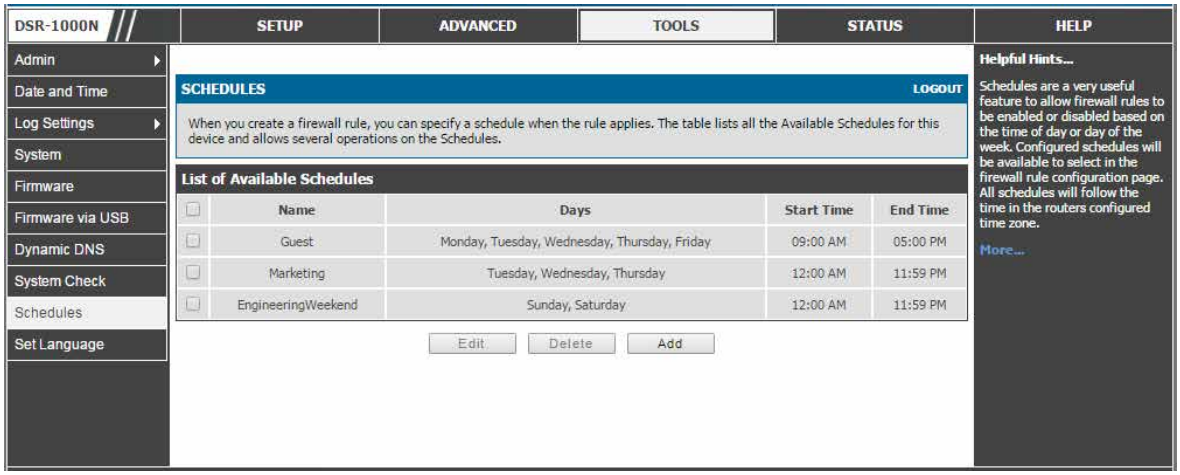


図 7-3　ファイアウォールにバインドする有効なスケジュールのリスト

注意 タイムゾーンが設定されているルータでは、すべてのスケジュールがその時間に従います。タイムゾーンの選択および NTP サーバの設定に関する詳細は各セクションを参照してください。

スケジュールの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

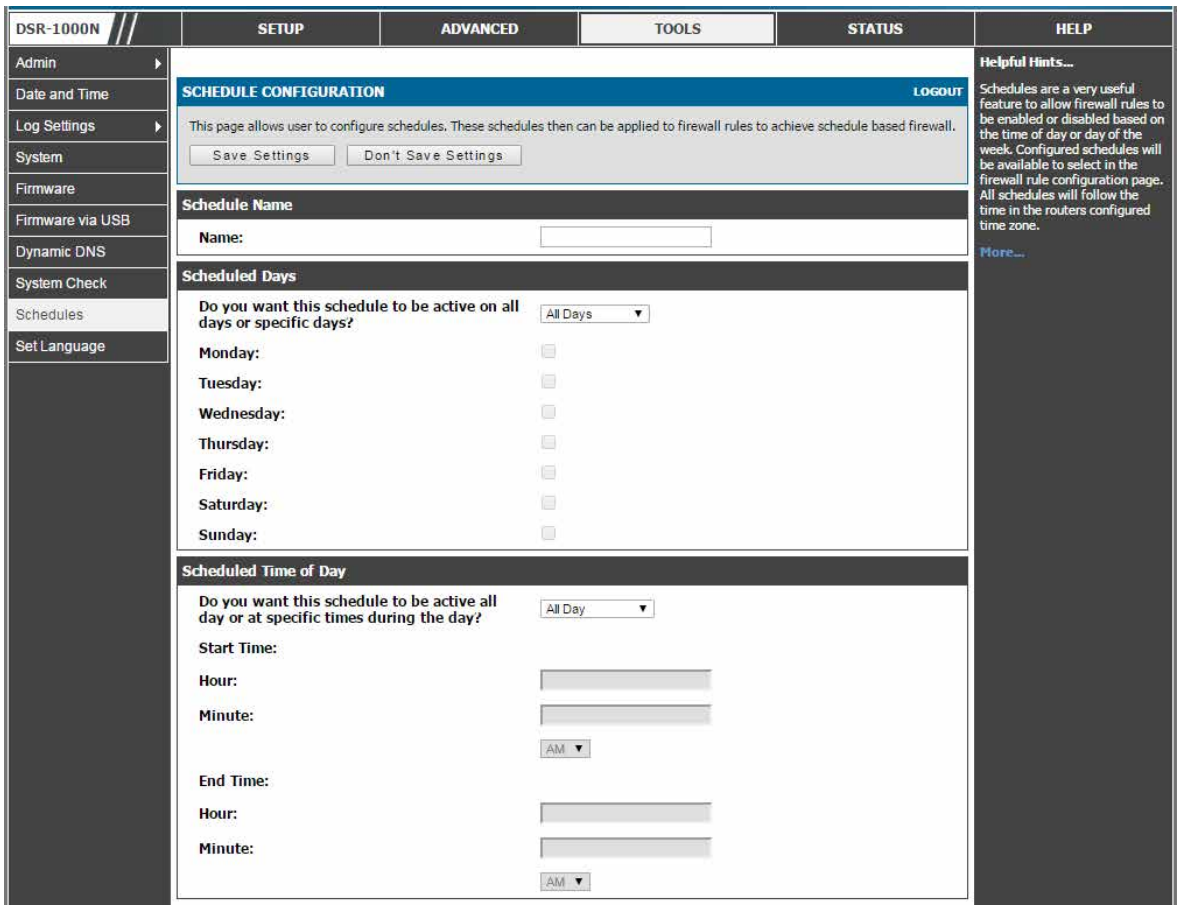


図 7-4　SCHEDULE CONFIGURATION 画面 - 追加

2. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ファイアウォールルールの設定手順

ADVANCED > Firewall Settings > Firewall Rules メニュー
ここではファイアウォールの設定手順を説明します。

ルータに関するすべての設定済みファイアウォールルールは「Firewall Rules」リストに表示されます。このリストは、ルールが有効（アクティブ）かどうかを示して、ルールが影響するサービスまたはユーザと共に From/To ゾーンの概要を表示します。

以下の手順に従って新しいファイアウォールルールを登録します。:

1. **ADVANCED > Firewall Settings > Firewall Rules** の順にメニューをクリックし、以下の画面を表示します。「List of Available Firewall Rules」テーブル内の既存のルールを参照します。

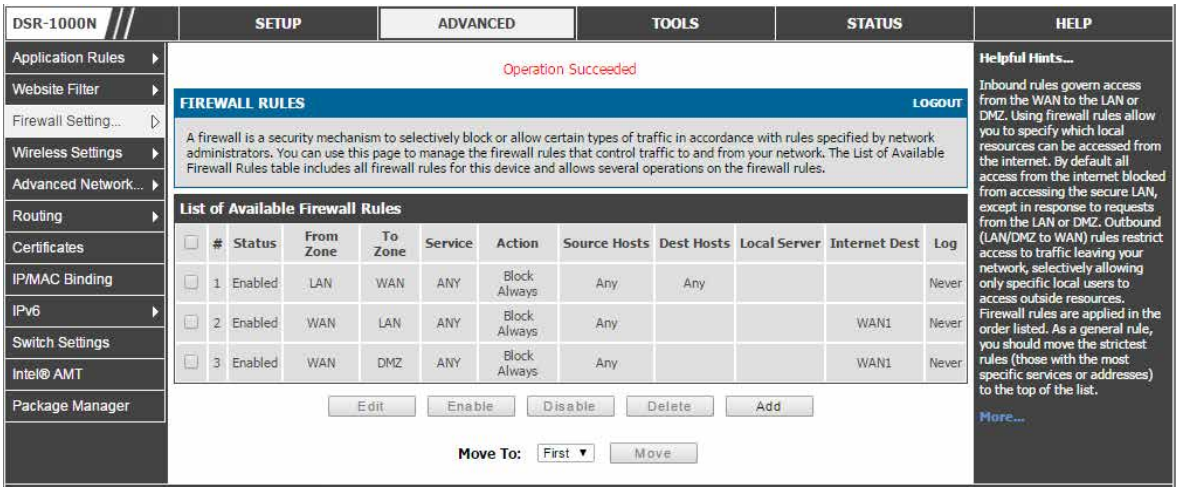


図 7-5　ファイアウォールルールリスト

2. 外向きまたは内向きサービスルールを編集、追加するためには、以下の手順を行います。:

- ルールを編集するためには、ルールの横にあるボックスをチェックして、「Edit」ボタンをクリックしてそのルールの設定ページにリンクします。
- 新しいルールを追加するためには、「Add」ボタンをクリックして新しいルールの設定ページにリンクします。一度作成されると、新しいルールは元々のテーブルに自動的に追加されます。

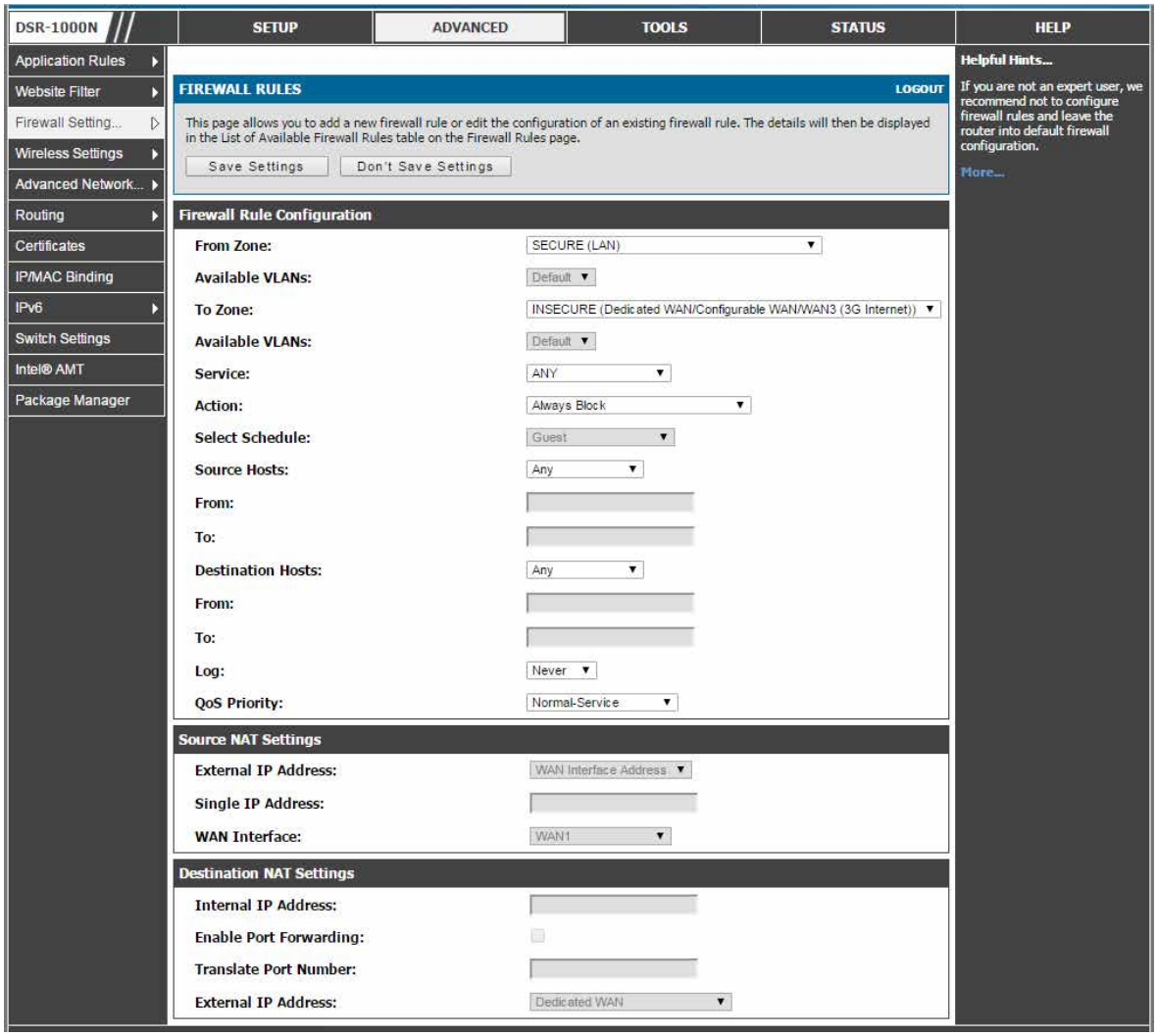


図 7-6　　ファイアウォールルール設定

「To/From Zone」、サービス、アクション、スケジュールを定義し、必要とされる送信元 / 送信先 IP アドレスを指定します。

3. トラフィックを生成するソースとなる「From Zone」を選択します。: SECURE（LAN）、DMZ、または INSECURE（WAN）。内向きルールでは、WAN が「From Zone」に選択される必要があります。

4. このルールでカバーされるトラフィックの宛先になる「To Zone」を選択します。「From Zone」が「WAN」であれば、「To Zone」は「DMZ」または「SECURE（LAN）」となります。同様に、「From Zone」が「LAN」であれば、「To Zone」は「DMZ」または「INSECURE（Dedicated WAN/Configurable WAN）」となります。

5. ファイアウォールルールを定義するパラメータには以下の項目があります。:

項目	説明
Service	「ANY」はすべてのトラフィックがこのルールの影響を受けることを意味しています。特定のサービスのために、プルダウンメニューには一般的なサービスが表示されます。またはカスタム定義サービスを選択できます。
Action	このルールが定義する以下の 4 つの操作から 1 つを選択します。: • Always Block（常にブロック） • Always Allow（常に許可） • Block by schedule, otherwise Allow（スケジュールによりブロック、その他は許可）。 • Allow by schedule, otherwise Block（スケジュールにより許可、その他はブロック）。 このルールに割り当てるためにはプルダウンメニューで利用可能となるようにスケジュールをあらかじめ設定する必要があります。
Source / Destination Hosts	それぞれの関連するカテゴリで、ルールを適用するユーザを選択します。: • Any（すべてのユーザ） • Single Address（IP アドレスを入力します。） • Address Range（適切な IP アドレス範囲を入力します。）

項目	説明
Log	このルールによってフィルタされるトラフィックをログに出力することができます。これには、別途ルータのログ出力機能を設定する必要があります。
QoS Priority	外向きルール（「To Zone」が「INSECURE（Dedicated WAN/Configurable WAN）」の場合）は、QoS のプライオリティタグでトラフィックをマークすることができます。以下のプライオリティレベルを選択します。: • Normal-Service : ToS=0（最も低い QoS） • Minimize-Cost : ToS=1 • Maximize-Reliability : ToS=2 • Maximize-Throughput : ToS=4 • Minimize-Delay : ToS=8（最も高い QoS）

6. 内向きルールは、WAN からのトラフィックを管理するのに、Destination NAT（DNAT）を使用することができます。「To Zone」が「DMZ」または「SECURE（LAN）」の場合に、Destination NAT は利用できます。

項目	説明
Internal IP Address	内向きの許可ルールの場合、選択されたサービスをホスティングしている内部サーバのアドレスを入力できます。
Enable Port Forwarding	ボックスをチェックすることによって、入力サービスの特定ルール（「From Zone」が「WAN」の場合）に対してポートフォワーディングを有効にすることができます。これにより、選択したサービスのトラフィックがポートフォワーディングルールを経由してインターネットから適切な LAN ポートに到達することができます。
Translate Port Number	ポートフォワーディングにより、入力トラフィックはここで入力するポート番号に送信します。
External IP address	入力トラフィックのための送信元 IP アドレスとして「Dedicated WAN」または「Configurable WAN」のいずれかを選択することによって、特定の WAN インタフェースにルールを割り当てることができます。

注意 本ルータは、マルチ NAT をサポートしているため、External IP アドレスを必ず WAN アドレスにする必要はありません。1 つの WAN インタフェースに複数のパブリック IP アドレスをサポートしています。ご契約の ISP が 1 つ以上のパブリック IP アドレスを割り当てる場合、これらのうち 1 つを WAN ポート上のプライマリ IP アドレスとして使用し、他の IP アドレスを LAN または DMZ 上のサーバに割り当てることができます。このようにして別名をつけたパブリック IP アドレスによってインターネットから LAN/DMZ サーバにアクセスすることができます。

7. ルールパラメータを照合するすべての LAN/DMZ トラフィックを特定の WAN インタフェースまたは外部 IP アドレス（通常、ご契約の ISP が提供）にスタティックにマップ（バインド）するために、外向きルールは Source NAT（SNAT）を使用することができます。

新しく、または編集したルールパラメータが保存されると、ファイアウォールルールのマスタリストに表示されます。ルールを有効または無効にするためには、ファイアウォールルールのリストにおいてルールの横にあるチェックボックスをクリックし、「Enable」または「Disable」ボタンを選択します。

注意 ルータは、リストにある順番でファイアウォールルールを適用します。一般的なルールでは、最も厳しいルール（多くの指定サービスまたはアドレスを持つ）をリストの先頭に移動させるべきです。ルールを再度整理するためには、ルールの横にあるチェックボックスをクリックして、「Move To」で順番を選択した後に「Move」ボタンをクリックします。

例 : 外部 IP アドレス（209.156.200.225）をプライベート DMZ IP アドレス（10.30.30.30）にマップするのに外向き SNAT ルールを使用する

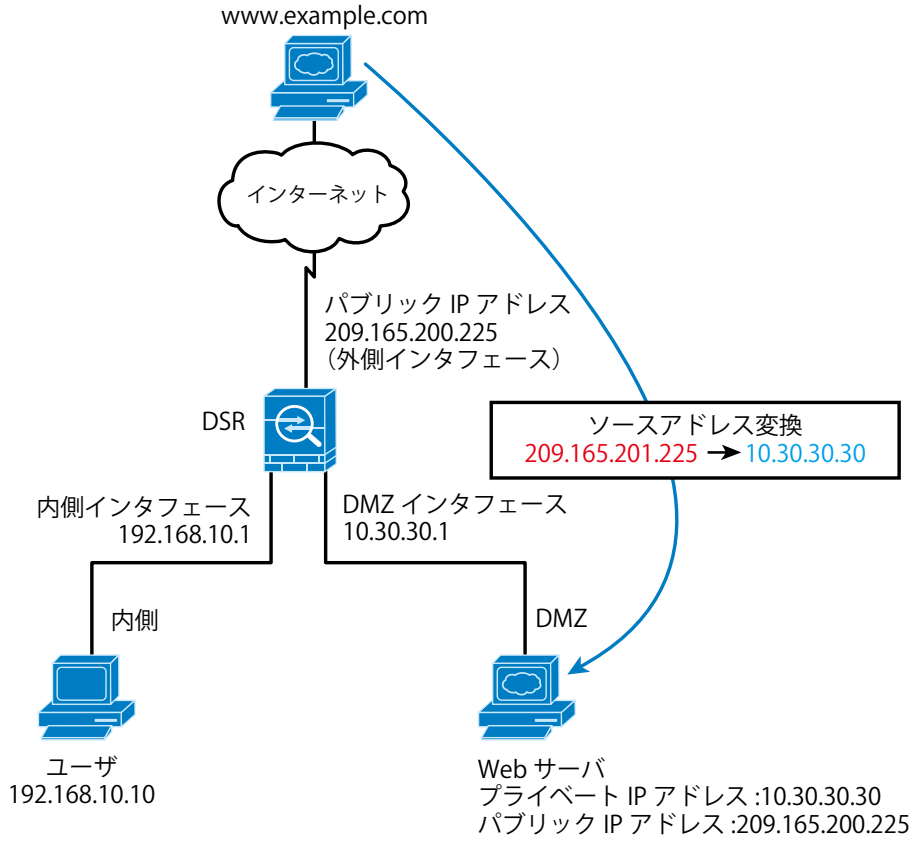


図 7-7　SNAT ルールの例

IPv6 ファイアウォールルールの設定手順

ADVANCED > Firewall Settings > IPv6 Firewall Rules メニュー

ルータに関するすべての設定済み IPv6 ファイアウォールルールは「Firewall Rules」リストに表示されます。

1. **ADVANCED > Firewall Settings > IPv6 Firewall Rules** の順にメニューをクリックし、以下の画面を表示します。

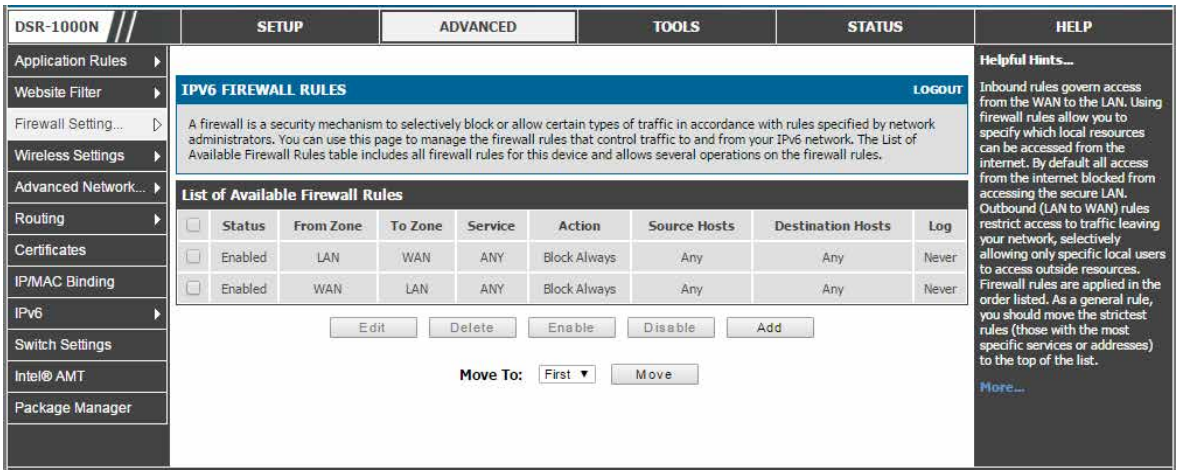


図 7-8　利用可能な IPv6 ファイアウォールルールのリスト画面

このリストは、ルールが有効 (アクティブ) かどうかを示して、ルールが影響するサービスまたはユーザと共に From/To ゾーンの概要を表示します。

ルールの設定

1. 「Add」ボタンをクリックして以下の画面を表示します。

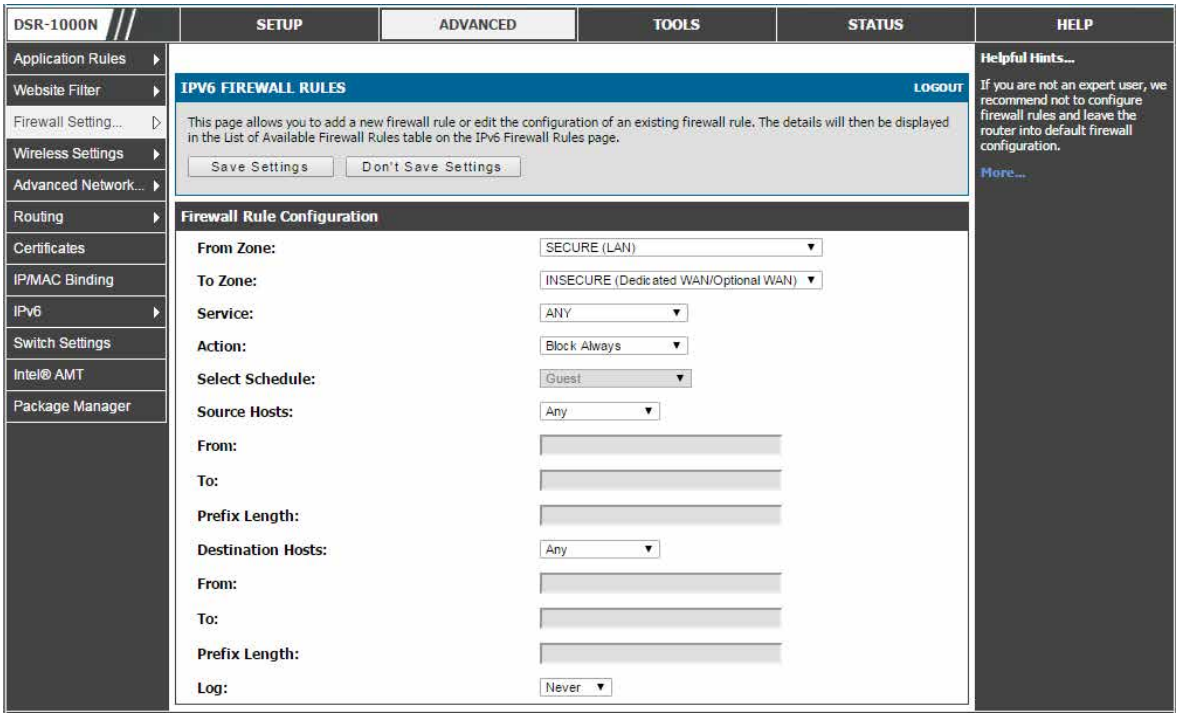


図 7-9　IPv6 ファイアウォールルール追加 画面

2. 「To/From Zone」、サービス、アクション、スケジュールを定義し、必要とされる送信元 / 送信先 IP アドレスを指定します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ファイアウォールルール設定の例

例 1 : DMZ に対する内向き HTTP トラフィックを許可する

状況 :

ローカルな DMZ ネットワークにおけるパブリック Web サーバをホスティングします。外部 IP アドレスからあなたの Web サーバの IP アドレスに対する内向き HTTP トラフィックを常に許可します。

ソリューション :

以下の通り、内向きルールを作成します。

項目	値
From Zone	INSECURE（WAN1 / WAN2）
To Zone	Public（DMZ）
Service	HTTP
Action	Always Allow
Send to Local Server（DNAT IP）	192.168.5.2（Web サーバの IP アドレス）
Destination Hosts	Any
Log	Never

例 2 : 外部の IP アドレス範囲からテレビ会議を許可する

状況 :

入力方向のテレビ会議が制限された外部の IP アドレス範囲（132.177.88.2 - 132.177.88.254）から（支店から）開始されることを希望するものとします。

ソリューション :

以下の通り、内向きルールを作成します。例えば、CUSeeMe（使用されるテレビ会議サービス）接続は指定範囲の外部 IP アドレスからだけ許可されます。

項目	値
From Zone	INSECURE（WAN1 / WAN2）
To Zone	SECURE（LAN）
Service	CU-SEEME:UDP
Action	Always Allow
Send to Local Server（DNAT IP）	192.168.10.11
Destination Hosts	Address Range
From	132.177.88.2
To	134.177.88.254
Enable Port Forwarding	Yes（有効）

例 3 : マルチ NAT 設定

状況 :

1 つの WAN ポートインタフェースに複数のパブリック IP アドレスをサポートするためにマルチ NAT の設定を希望します。

ソリューション :

追加のパブリック IP アドレスをホスティングするようにファイアウォールを設定する内向きルールを作成します。このアドレスを DMZ 上の Web サーバに関連付けます。使用するために 1 つ以上のパブリック IP アドレスを持つようにご契約の ISP に手配したら、追加のパブリック IP アドレスを使用して、ご使用の LAN でサーバにマップすることができます。これらのパブリック IP アドレスの 1 つはルータのプライマリ IP アドレスとして使用されます。このアドレスは、NAT を通じてご使用の LAN PC にインターネットアクセスを供給するのに使用されます。他のアドレスは、DMZ サーバにマップするために利用できます。

以下のアドレス指定案は、この手順を示すのに使用されます。:

- WAN IP アドレス : 10.1.0.118
- LAN IP アドレス : 192.168.10.1、サブネット 255.255.255.0
- DMZ における Web サーバホスト、IP アドレス : 192.168.12.222
- Web サーバへのアクセス : (シミュレートされた) パブリック IP アドレス 10.1.0.52

項目	値
From Zone	INSECURE（WAN1 / WAN2）
To Zone	Public（DMZ）
Service	HTTP
Action	Always Allow
Send to Local Server（DNAT IP）	192.168.12.222（Web サーバのローカル IP アドレス）
Destination Hosts	Single Address
From	10.1.0.52
WAN Users	Any
Log	Never

例 4 : 特定範囲のマシンから生成される場合に、トラフィックをスケジュールによってブロックする

使用するケース :

既知の IP アドレス範囲を持つ LAN 内の指定マシングループからリクエストが生成され、WAN からネットワーク経由で誰でもアクセス可能な場合（つまり、すべてのリモートユーザ）には、週末にすべての HTTP トラフィックをブロックします。

設定 :

1. スケジュールの設定 :

- 週末だけにトラフィックに作用するスケジュールを設定するためには、以下の設定を行います。
  セキュリティ : スケジュールを作成して、「Weekend」という名称をつけます。

- 土曜日朝の午前 12 時から月曜日朝の午前 12 時までを意味する「Weekend」（土曜と日曜の終日）を定義します。

- 「Scheduled Days」のボックス内に、「指定曜日」にアクティブにするものにチェックします。「Saturday」と「Sunday」を選択します。

- 「Scheduled Time of Day」で「All Day」（終日）を選択します。これは選択した曜日の午前 12 時から午後 11 時 59 分の間にスケジュールを適用します。

- 「Save Settings」をクリックします。これで、「Weekend」というスケジュールは 1 週間から土曜日と日曜日を隔離します。

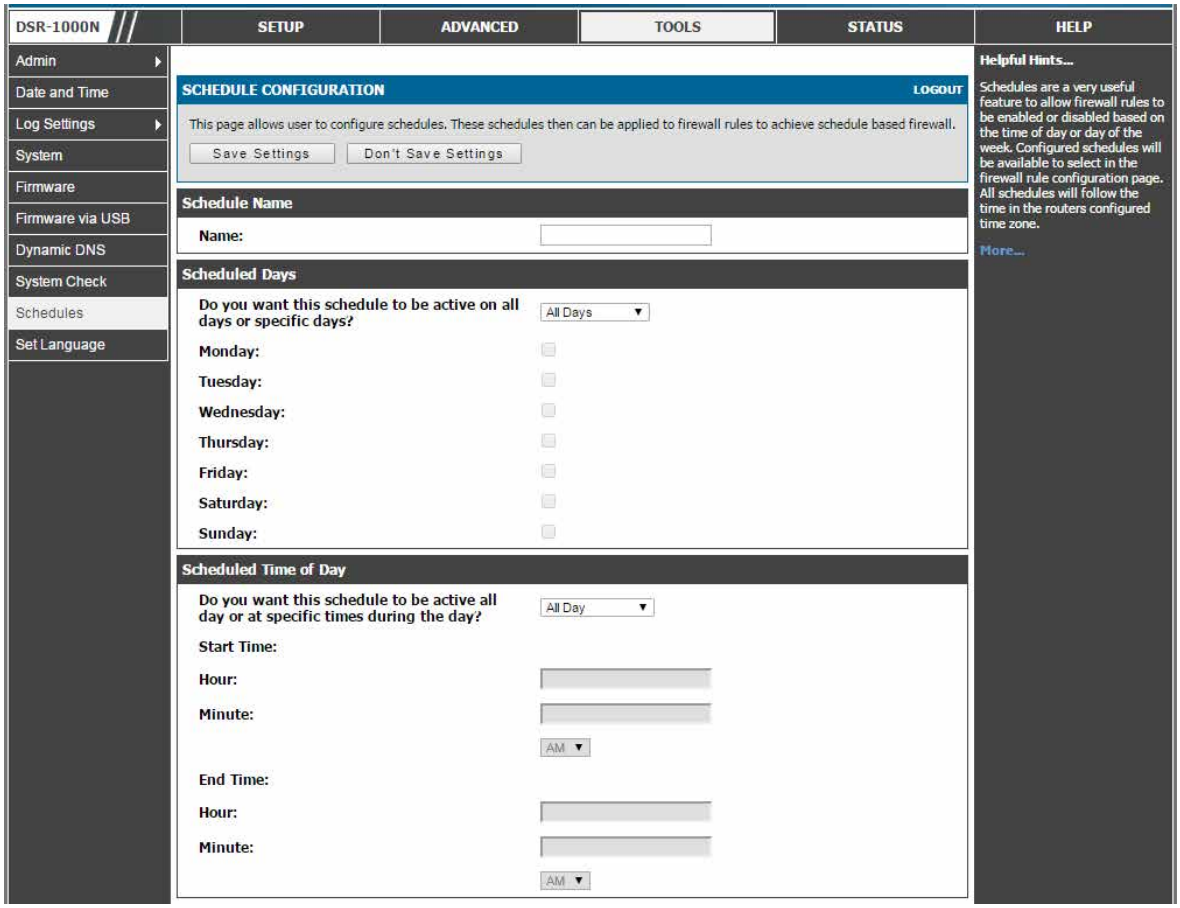


図 7-10　上記の例題のためのスケジュール設定

2. HTTP 要求をブロックしようとするため、これはスケジュール「Weekend」に従ってブロックされる「To Zone」が「INSECURE（WAN1 / WAN2 ）」であるサービスです。

3. 「Action」から「Block by schedule, otherwise Allow」（スケジュールに従いブロックし、その他は許可する）を選択します。これは、事前に定義したスケジュールを受け付けて、ルールが定義済みの曜日 / 時間においてブロックするルールであることを確実にします。スケジュール以外のすべての時間は、このファイアウォールのブロックルールの影響は受けません。

4. 「Weekend」というスケジュールを定義すると、プルダウンメニューでこれが利用可能になります。

5. 「Marketing」グループに割り当てた IP 範囲のブロックを行いたいとします。IP は「192.168.10.20」から「192.168.10.30」までとします。「Source Hosts」プルダウンメニューで、「Address Range」を選択して、「From/To」にこの IP アドレス範囲を追加します。

6. 安全でないゾーンに向かうすべてのサービスへの全 HTTP トラフィックをブロックしたいとします。「Destination Hosts」プルダウンメニューは「Any」とする必要があります。

7. QoS のデフォルト優先度またはログ出力を（希望しなければ）変更する必要はありません。「Save Settings」ボタンをクリックして、このファイアウォールルールをファイアウォールルールのリストに追加します。

8. 最後の手順は、このファイアウォールルールを有効にすることです。ルールを選択し、リストの下にある「Enable」ボタンをクリックしてファイアウォールルールをアクティブにします。

カスタムサービスにおけるセキュリティ

ADVANCED > Firewall Settings > Custom Services メニュー
ここではファイアウォールルールを定義するカスタムサービスを作成することができます。

ファイアウォールルールを作成する場合、ルールによって制御されるサービスを指定することができます。一般的なサービスタイプを選択して利用可能であり、自身のカスタムサービスを作成することもできます。

一般的なサービスは既知の TCP/UDP/ICMP ポートを使用しますが、多くのカスタムまたは一般的でないアプリケーションは LAN または WAN に存在します。カスタムサービス設定メニューでは、このサービスのためにポート範囲を定義して、トラフィックタイプ（TCP/UDP/ICMP）を確認することができます。定義されると、新しいサービスは「List OF Available Custom Services」テーブルおよび「ファイアウォールルール設定」メニューのサービスリストに表示されます。

1. **ADVANCED > Firewall Settings > Custom Services** の順にメニューをクリックし、以下の画面を表示します。

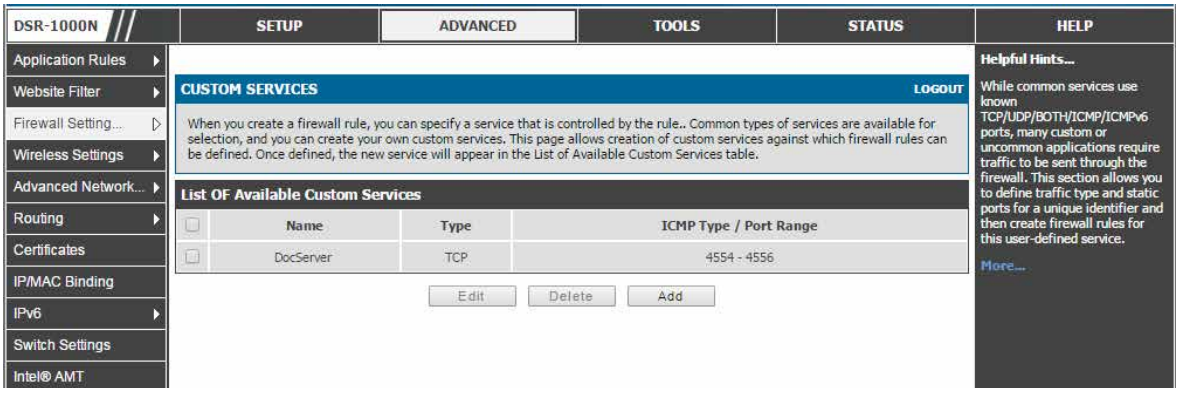


図 7-11　ユーザ定義サービスのリスト

サービスの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

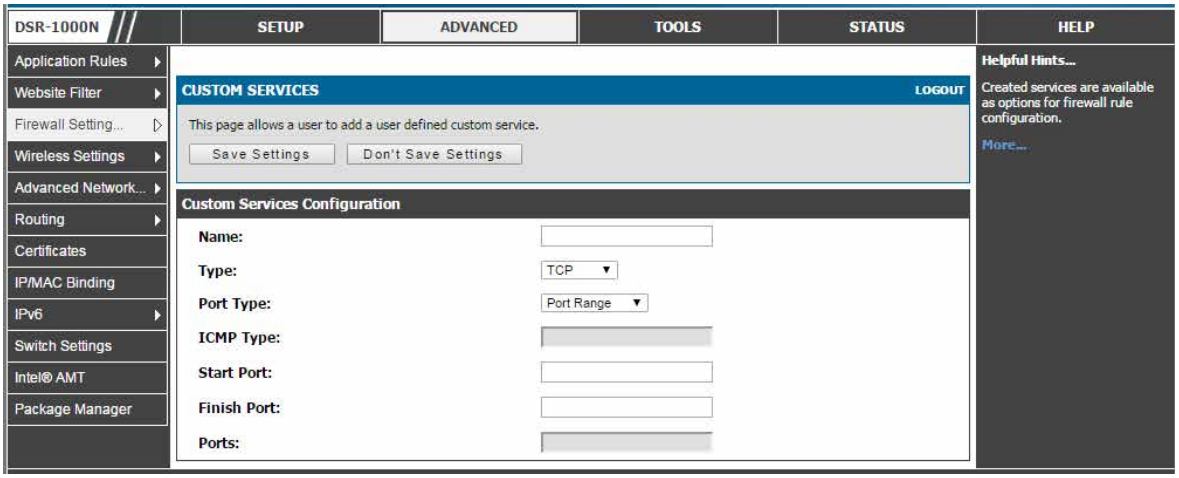


図 7-12　ユーザ定義サービスの追加

2. 作成したサービスをファイアウォールルール設定のオプションとして利用することができます。

項目	説明
Name	識別と管理目的のためのサービス名。
Types	サービスが使用するレイヤ 3 プロトコル。(TCP、UDP、Both、ICMP、または ICMPv6)
Port Type	本欄では「Port Range」または「Multiple Ports」を選択します。
ICMP Type	「Types」欄のレイヤ 3 プロトコルが「ICMP」または「ICMPv6」に選択されると本欄が有効になります。「ICMP」タイプは 0-40、「ICMPv6」タイプは 1-255 の数値です。ICMP タイプのリストについては、次の URL を参照してください。: http://www.iana.org/assignments/icmp-parameters
Start Port	サービスが使用する範囲の開始の TCP、UDP、または Both（両方）ポート。サービスが 1 つのポートだけを使用すると、「Start Port」（開始ポート）と「Finish Port」（終了ポート）は同じになります。
Finish Port	サービスが使用する終了レイヤ 3 プロトコル。サービスが 1 つのポートだけを使用すると、「Start Port」（開始ポート）と「Finish Port」（終了ポート）は同じになります。
Ports	サービスが使用するポート。

3. 各項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ALG サポート

ADVANCED > Firewall Settings > ALGs メニュー
ALG を有効 / 無効にします。

ALG（Application Level Gateways）は、シームレスにアプリケーションレイヤプロトコルをサポートするためにこのルータのファイアウォールと NAT サポートを機能強化するセキュリティコンポーネントです。

ALG により、カスタマイズされた NAT トラバーサルフィルタのゲートウェイへの挿入が可能となり、TFTP、SIP、RTSP、IPSec、PPTP など特定のアプリケーションレイヤの「コントロール / データ」プロトコルに対するアドレス変換およびポート変換をサポートすることができます。各 ALG は特定のプロトコルまたはアプリケーションに対する特別な処理を提供します。一般的なアプリケーションのための多くの ALG は初期値で有効とされています。

いくつかの場合では、管理者が同じサポートを実行するために大きなポート番号をオープンしなくても、ALG により、特定のクライアントアプリケーション（H.323 または RSTP など）が必要とする既知のポートと通信するために、ファイアウォールがダイナミックなエフェメラル TCP/UDP ポートを使用することができます。ALG は、それをサポートする特定のアプリケーションが使用するプロトコルを理解しているので、ルータのファイアウォールを通じたクライアントアプリケーションのサポートを導入する非常に安全で効率的な方法です。

1. **ADVANCED > Firewall Settings > ALGs** の順にメニューをクリックし、以下の画面を表示します。

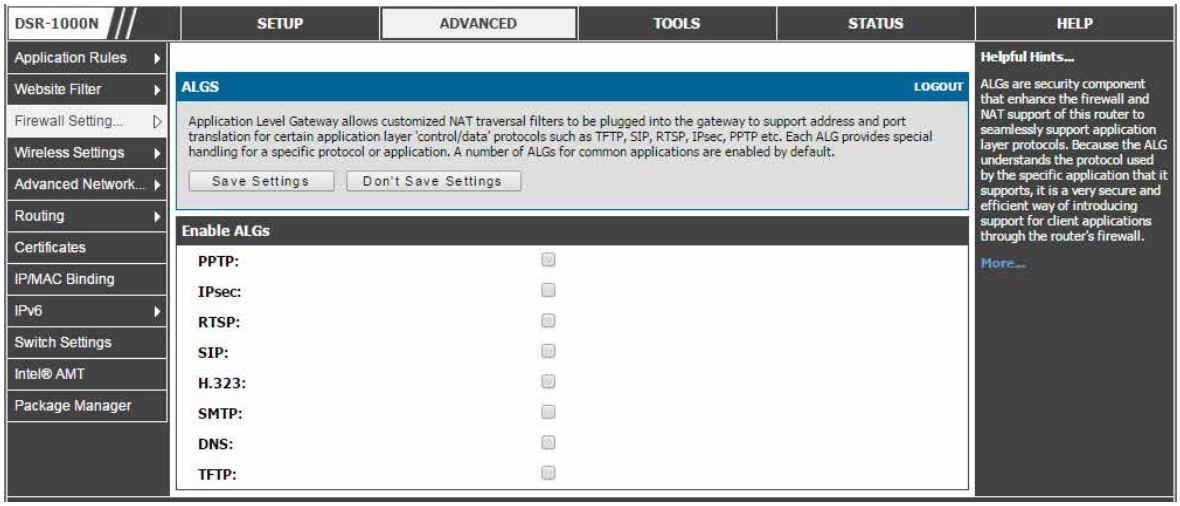


図 7-13　ルータにおける利用可能な ALG のでサポート

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

SMTP ALG 設定

SMTP ALG 設定

ADVANCED > Firewall Settings > SMTP ALG > SMTP ALG Configuration メニュー
SMTP ALG を有効にします。本機能は、メール ID または題名に基づいてメールをブロック / 許可するのを補助します。

1. **ADVANCED > Firewall Settings > SMTP ALG > SMTP ALG Configuration** の順にメニューをクリックし、以下の画面を表示します。

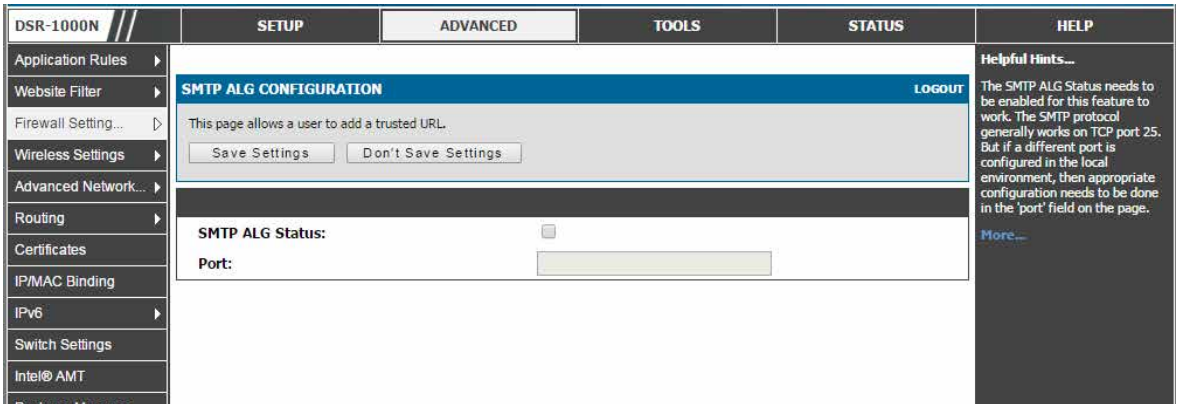


図 7-14　SMTP ALG 設定

2. 以下の項目を設定します。

項目	説明
SMTP ALG Status	他のオプションを設定するためには本オプションを有効にする必要があります。
Port	これは、SMTP パケットが予想されるポートです。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

承認されるメール ID

ADVANCED > Firewall Settings > SMTP ALG > Approved Mail Ids メニュー
許可するメール ID を設定します。

1. **ADVANCED > Firewall Settings > SMTP ALG > Approved Mail Ids** の順にメニューをクリックし、以下の画面を表示します。

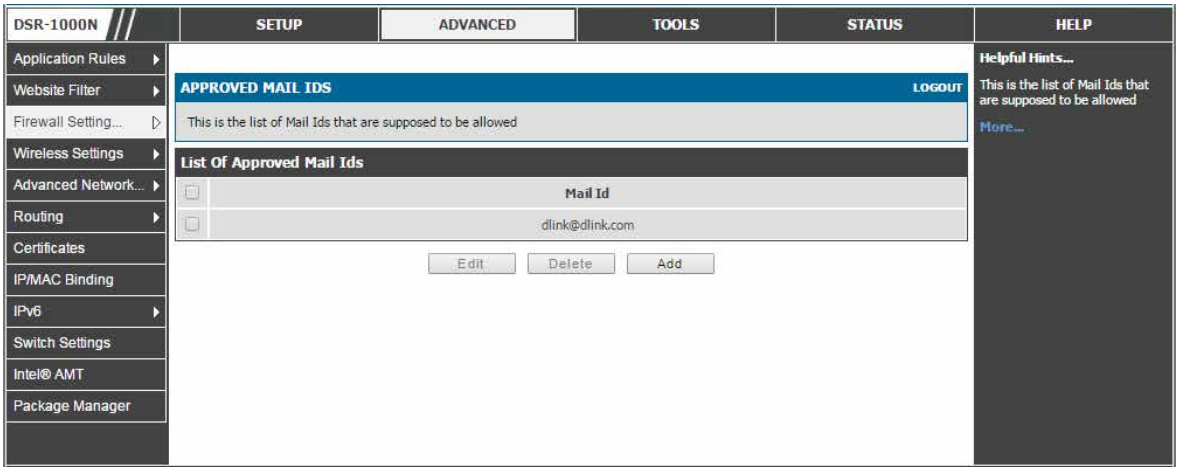


図 7-15　承認するメール ID 設定

ユーザが承認するメール ID のリストが表示されます。

メール ID の追加

1. 「Add」ボタンをクリックして以下の画面を表示します。

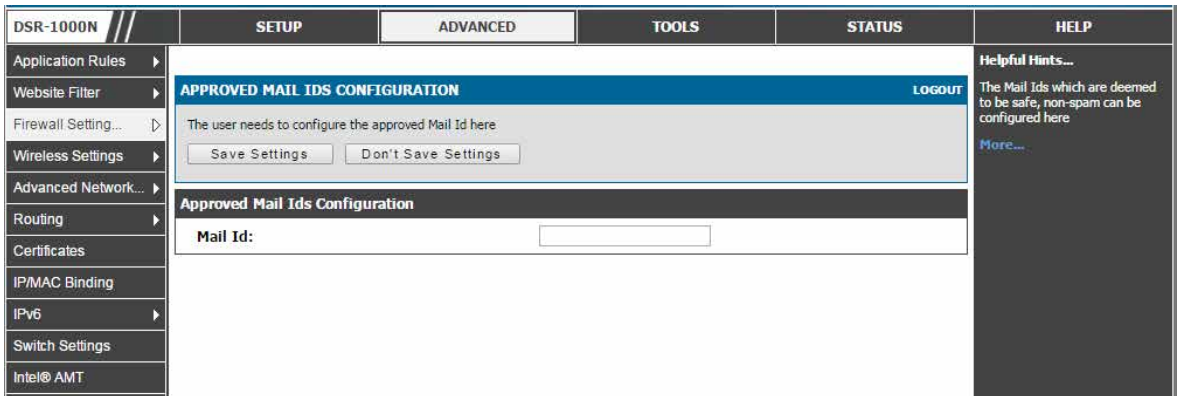


図 7-16　承認するメール ID 設定

2. 「Mail Id」に承認するメール ID を設定します。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ブロックされるメール ID のリスト

ADVANCED > Firewall Settings > SMTP ALG > Blocked Mail Ids メニュー

ブロックするメール ID を設定します。

1. **ADVANCED > Firewall Settings > SMTP ALG > Blocked Mail Ids** の順にメニューをクリックし、以下の画面を表示します。

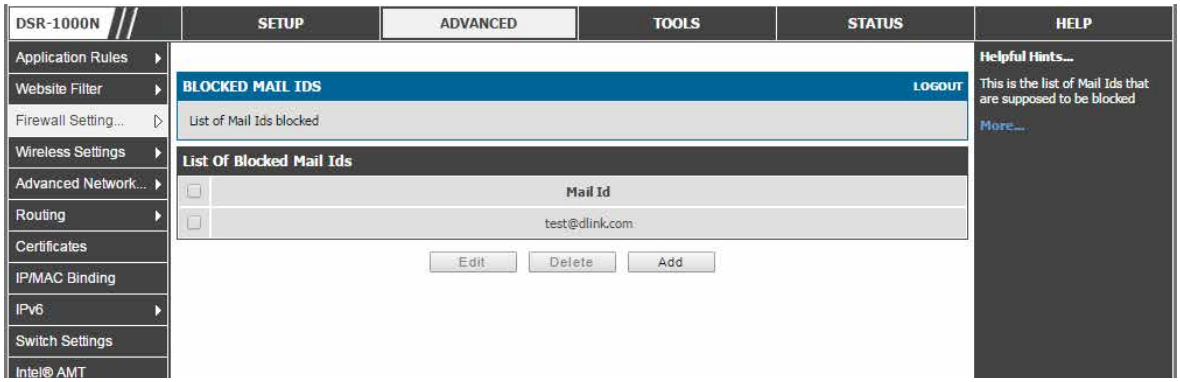


図 7-17　ブロックするメール ID 設定

ブロックするメール ID のリストが表示されます。

メール ID の追加

1. 「Add」ボタンをクリックして以下の画面を表示します。

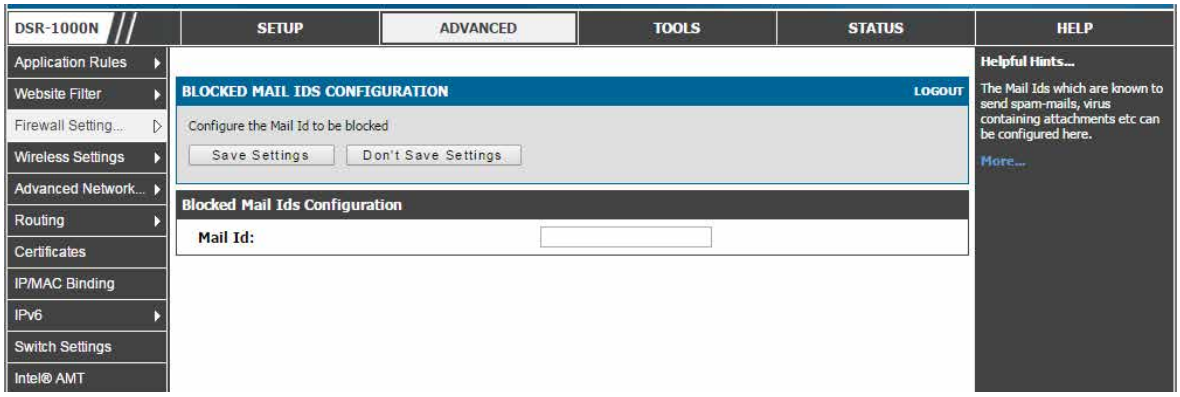


図 7-18　ブロックするメール ID 設定

2. 「Mail Id」にブロックするメール ID を設定します。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

題名リストの設定

ADVANCED > Firewall Settings > SMTP ALG > Subject List メニュー

「特定の題名」を持つ「特定のメール ID」から（へ）のメールへの操作を可能にします。ここに記載する操作は、メールに関連する他の設定すべてに優先度を設定します。

1. **ADVANCED > Firewall Settings > SMTP ALG > Subject List** の順にメニューをクリックし、以下の画面を表示します。

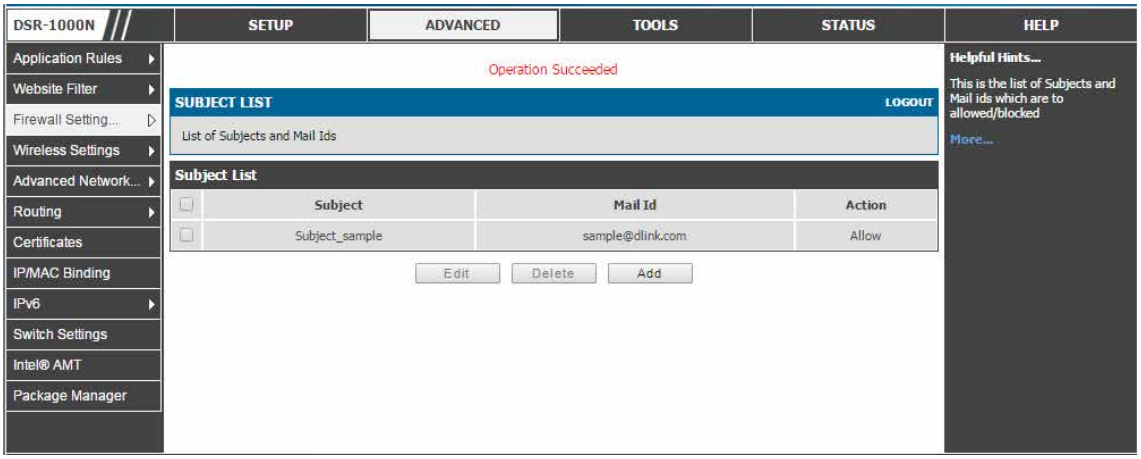


図 7-19　設定済みの題名

操作を行う題名を表示します。

項目	説明
Subject	操作を行うことになっている題名を表示します。
Mail Id	設定済みの題名がチェックされるべき送信元 / 送信先メール ID を表示します。
Action	実行する操作（ブロックまたは許可）を表示します。

題名の追加

1. 「Add」ボタンをクリックして以下の画面を表示します。

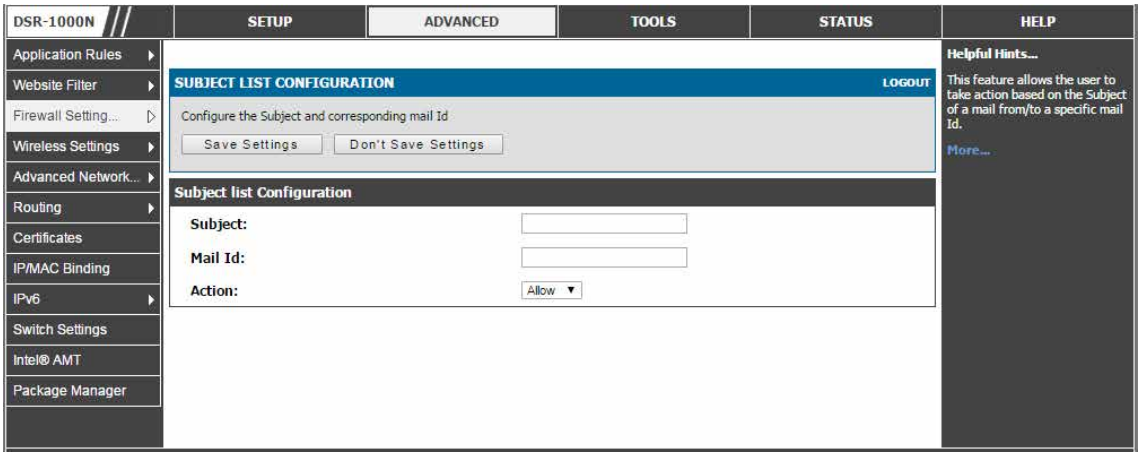


図 7-20　題名の登録

2. 以下の項目を設定します。

項目	説明
Subject	チェックの必要がある題名の文字列を完全に入力します。
Mail Id	受信 / 送信する送信元 / 送信先メール ID。
Action	メールを許可またはブロックします。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ファイアウォールのための VPN パススルー

ADVANCED > Firewall Settings > VPN Passthrough メニュー

LAN とインターネット間の IPSec、PPTP、および L2TP VPN トンネル接続用の暗号化された外向き VPN トラフィックを許可する（パススルー）ようにファイアウォール設定を行います。

特定のファイアウォールルールまたはサービスはこのパススルーを行うように設定されていません。そのため、「VPN PASSTHROUGH」（パススルーチェックボックス）を有効にすることで、同じサービスに基づくファイアウォールルールより高い優先度を持つことができます。

1. **ADVANCED > Firewall Settings > VPN Passthrough** の順にメニューをクリックし、以下の画面を表示します。

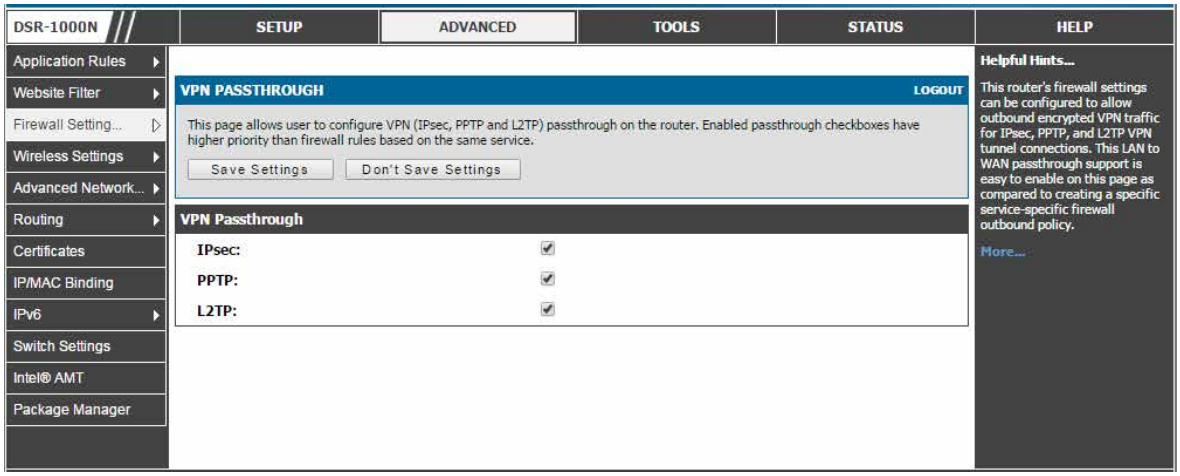


図 7-21　VPN トンネルのためのパススルーオプション

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ブリッジモードのファイアウォール

ADVANCED > Firewall Settings > Bridge Firewall Rules メニュー

ブリッジが選択したシステムのルーティングモードである場合、レイヤ 2 レベルのファイアウォールルールが、ネットワークトラフィックを管理するために利用可能です。これらのファイアウォールルールはブリッジの一部である 2 つのポート間で適用されます。: LAN1 と WAN2/DMZ 物理ポート

1. **ADVANCED > Firewall Settings > Bridge Firewall Rules** の順にメニューをクリックし、以下の画面を表示します。

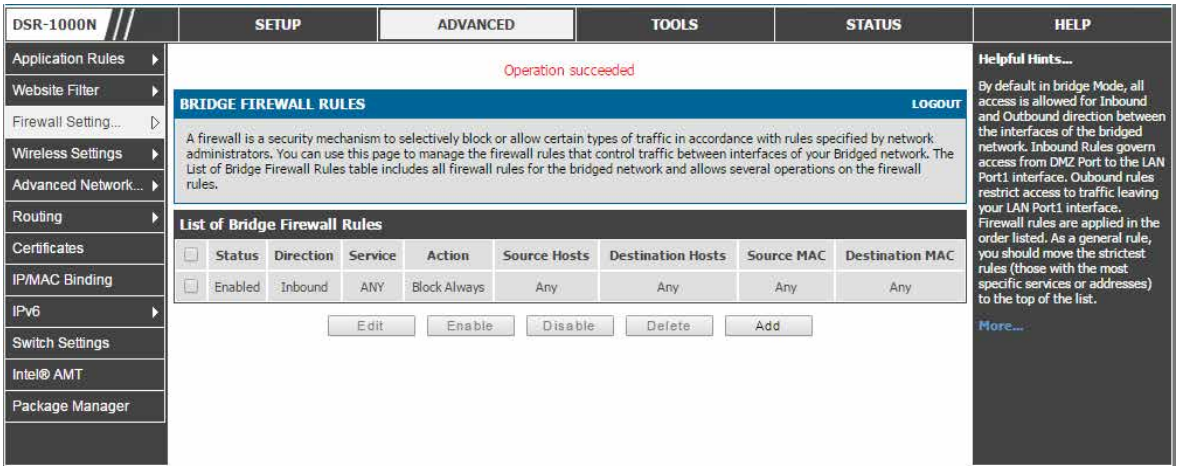


図 7-22　ブリッジファイアウォールルールのリスト

ブリッジ用に設定されたファイアウォールルールのリストを表示します。

ブリッジに設定されたファイアウォールルールは、プロトコル、ポートの外向き / 外向きの範囲に基づくトラフィックをフィルタします。L2 で処理は行われ、LAN1 ポートまたは WAN2/DMZ ポート（両方ではない）のいずれかに適用できます。

ブリッジファイアウォールルールの追加

1. 「Add」ボタンをクリックして以下の画面を表示します。

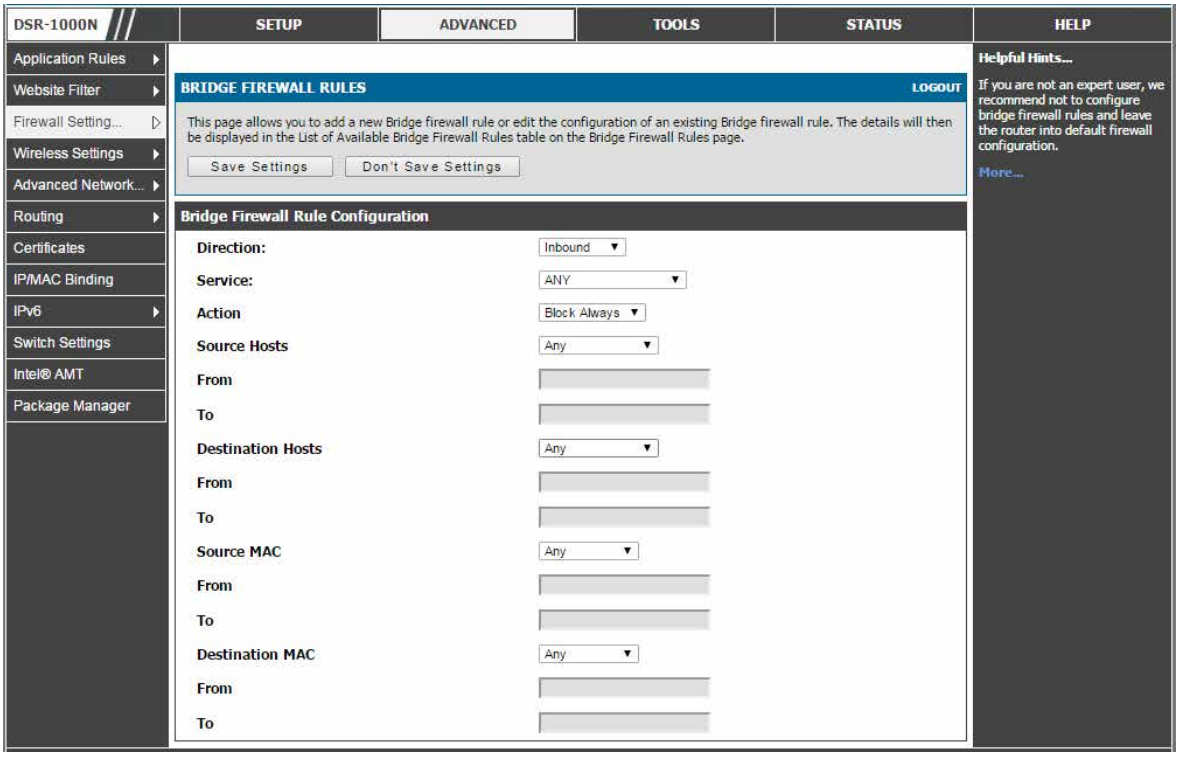


図 7-23　ブリッジファイアウォールルールの設定

2. 以下の項目を設定します。

項目	説明
Direction	このルールによって制御されるトラフィックの方向を設定します。 • Inbound - 内向き • Outbound - 外向き
Service	このルールによって制御されるサービスタイプを選択します。一般的なサービスはプルダウンメニューにあります。**ADVANCED > Firewall Settings > Custom Services** ページでサービスを追加することができます。
Action	行われるアクションを以下の通り選択します。 • Block Always - 選択したサービスを常にブロックします。 • Allow Always - 選択したサービスが常に通過することを許可します。
Source Hosts	以下の 1 つを選択します。 • Any - ブリッジネットワーク内のホストすべてから送られるトラフィックに適用するルールには本オプションを選択します。 • Single Address - 1 台のホストからのトラフィックに適用されるルールには本オプションを選択します。「From」ボックスにホストの IP アドレスを入力します。 • Address Range - IP アドレス範囲内のコンピュータ / デバイスのグループから来るトラフィックに適用されるルールには本オプションを選択します。範囲を指定するために、「From」ボックスに最初のアドレスを、「To」ボックスに最終アドレスを入力します。
Destination Hosts	以下の 1 つを選択します。 • Any - ブリッジネットワークのすべてのホストに到達するトラフィックに適用するルールに対するオプションを選択します。 • Single Address - 1 台のホストに到達するトラフィックに適用するルールに対する本オプションを選択します。「From」ボックスにホストの IP アドレスを入力します。 • Address Range - IP アドレス範囲内のコンピュータ / デバイスのグループに到達するトラフィックに適用されるルールには本オプションを選択します。範囲を指定するために、「From」ボックスに最初のアドレスを、「To」ボックスに最終アドレスを入力します。
Source MAC	以下の 1 つを選択します。 • Any - ブリッジネットワークに属するホストの全 MAC アドレスからのトラフィックに適用するルールに対してオプションを選択します。 • Single MAC - 1 つの MAC アドレスからのトラフィックに適用するルールに本オプションを選択します。「From」ボックスにホストの MAC アドレスを入力します。 • MAC Range - MAC アドレス範囲内のコンピュータ / デバイスのグループから来るトラフィックに適用されるルールには本オプションを選択します。範囲を指定するために、「From」ボックスに最初の MAC アドレスを、「To」ボックスに最終 MAC アドレスを入力します。
Destination MAC	以下の 1 つを選択します。 • Any - ブリッジネットワークに属するホストの全 MAC アドレスに到達するトラフィックに適用するルールに本オプションを選択します。 • Single MAC - 1 台の MAC アドレスに到達するトラフィックに適用するルールに本オプションを選択します。「From」ボックスにホストの MAC アドレスを入力します。 • MAC Range - MAC アドレス範囲内のコンピュータ / デバイスのグループに到達するトラフィックに適用されるルールに本オプションを選択します。範囲を指定するために、「From」ボックスに最初の MAC アドレスを、「To」ボックスに最終 MAC アドレスを入力します。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

アプリケーションルール

ADVANCED > Application Rules > Application Rules メニュー
ここでは利用可能な全トリガルールを表示し、ルールにいくつかの操作を許可します。

アプリケーションルールはポートトリガルールとも呼ばれます。本機能により、LAN または DMZ におけるデバイスは、それらに送信されるように 1 つ以上のポートを要求することができます。ポートトリガは、定義済みの出力ポートの 1 つにある LAN/DMZ からの外向き要求を待っており、特定のトラフィックタイプ用の入力ポートをオープンします。これは、アプリケーションがオープンした出力または入力ポートでデータを送信している間、ダイナミックなポートフォワーディングの形式として考えることができます。

ポートトリガを行うアプリケーションルールはファイアウォールルールの設定時に利用可能なオプションであるスタティックポートフォワーディングより柔軟性があります。これはポートトリガルールが特定の LAN IP または IP 範囲を参照する必要がないためです。その上、使用中でない場合でもポートはオープンされたままとなるため、その結果、ポートフォワーディングが提供しないセキュリティのレベルを提供します。

注意 入力ポートのオープン前に出力用の接続を行う LAN デバイスに依存するため、ポートトリガは LAN 上のサーバには適切ではありません。

いくつかのアプリケーションでは、外部デバイスがそれらに接続する場合に適切に機能するよう特定のポートまたはポート範囲にデータを受信することが必要です。ルータは必要とされるポートまたはポート範囲にあるアプリケーションだけにすべての入力データを送信する必要があります。ルータには、対応する外向き / 内向きのポートを持つ一般的なアプリケーションやゲームのリストがあり、オープンできます。また、有効になると、オープンすべきトラフィックタイプ（TCP または UDP）および入出力ポートの範囲を定義することでポートトリガルールを指定することができます。

1. **ADVANCED > Application Rules > Application Rules** の順にメニューをクリックし、以下の画面を表示します。

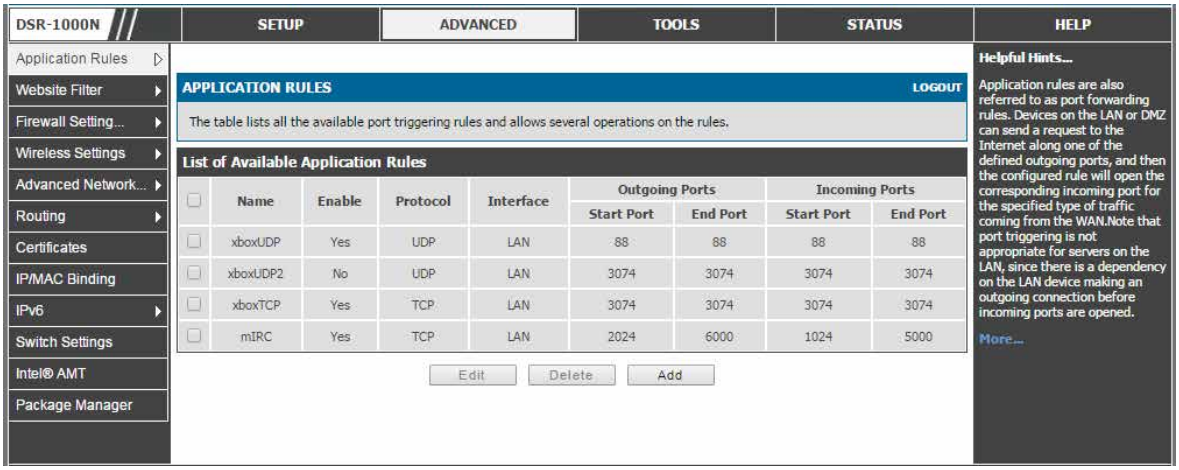


図 7-24　4 個のユニークなルールを表示する利用可能なアプリケーションルールのリスト

アプリケーションルールの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

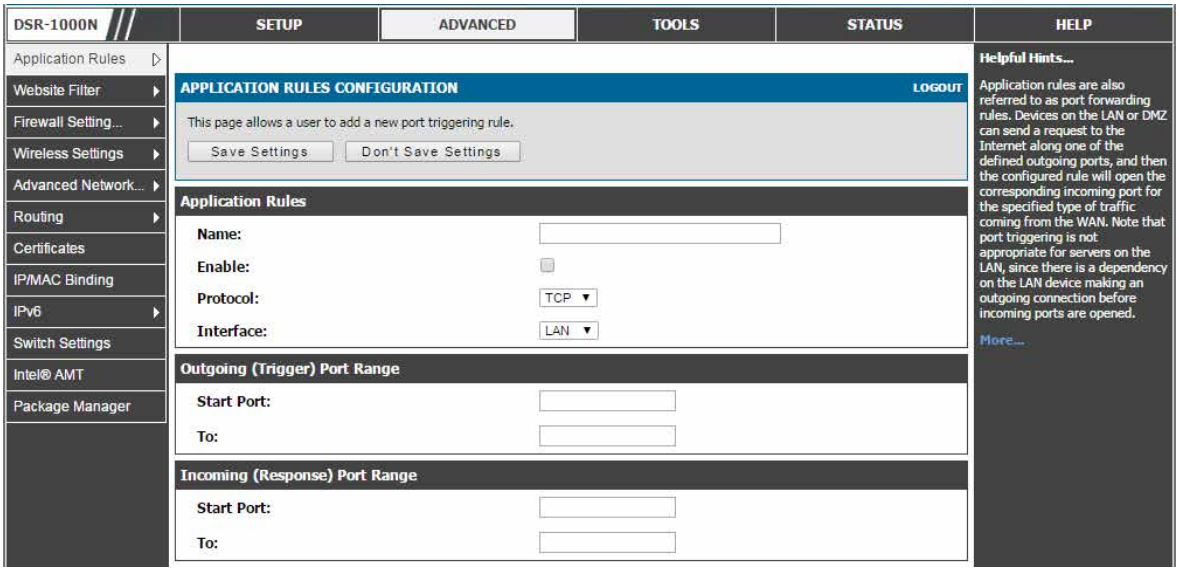


図 7-25　アプリケーションルールの追加

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ADVANCED > Application Rules > Application Rules Status ページではすべてのアクティブなルールを表示します。（つまり 定義済みの出力ポートからの外向きリクエストに基づいて始動する入力ポート）

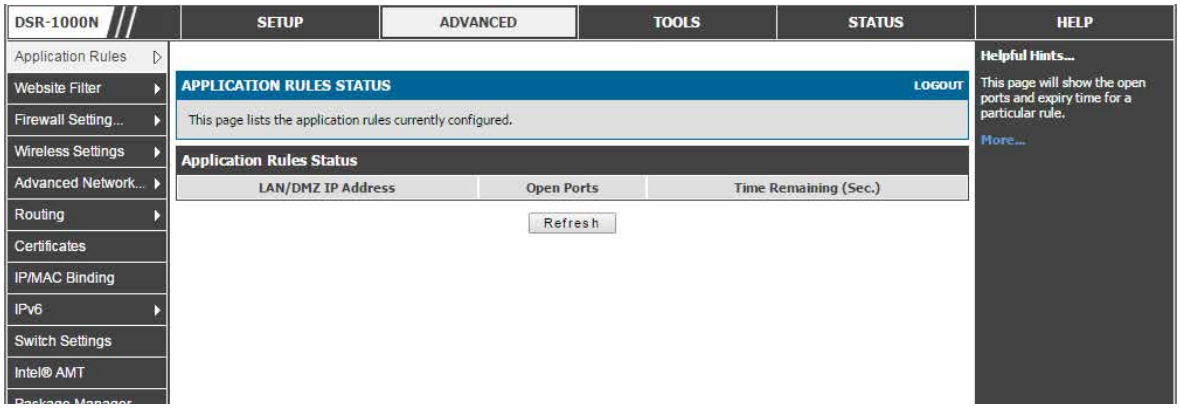


図 7-26　APPLICATION RULES STATUS 画面

Web コンテンツフィルタリング

ゲートウェイは、管理者が安全な LAN と安全でない WAN 間に簡単にアクセスポリシーを作成することができる標準的な Web フィルタリングオプションです。トラフィックタイプに基づいたポリシーを作成する代わりに（ファイアウォールルールを使用する場合など）、Web ベースコンテンツ自身がトラフィックが許可または破棄されるかを決定するために使用されます。

Content Filtering（コンテンツフィルタリング）

ADVANCED > Website Filter > Content Filtering メニュー

コンテンツフィルタリングオプションはユーザが特定のインターネットサイトにアクセスすることをブロックすることができます。

1. **ADVANCED > Website Filter > Content Filtering** の順にメニューをクリックし、以下の画面を表示します。

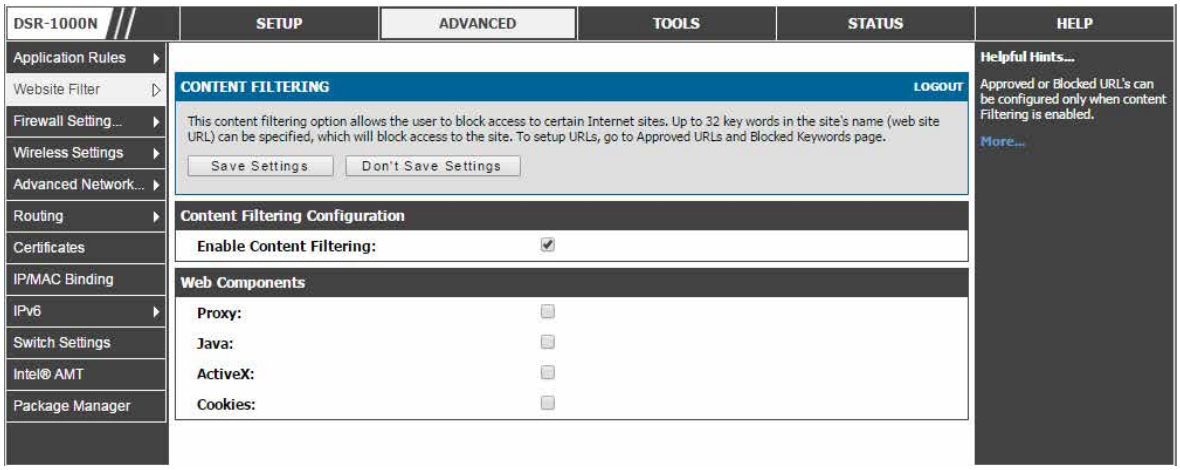


図 7-27　コンテンツフィルタリング設定

2. コンテンツフィルタリングは最初に「Enable Content Filtering」を有効とし、続く機能（トラストドメインのリスト、ブロックするキーワードにおけるフィルタリングなど）を設定および使用する必要があります。

3. 以下の項目を設定します。

項目	説明
Proxy	特定のファイアウォールルールを回避するために使用されるプロキシサーバは潜在的なセキュリティの隙間であり、すべての LAN インタフェースデバイスでブロックされます。
Java	Java アプレットはインターネットサイトからダウンロードされるのを防ぐことができます。
ActiveX	ゲートウェイは ActiveX コントロールがインターネットエクスプローラ経由でダウンロードされるのを防ぐことができます。
Cookies	プライベートネットワーク内の全デバイスのために、また、追加されたセキュリティクッキー（セッション情報を通常含む）をブロックすることができます。

4. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

Approved URLs（承認済み URL）

ADVANCED > Website Filter > Approved URLs メニュー
URL ドメイン名のための承認リストの表示および追加を行います。

このリストに追加されたドメインは、どんな形式でも許可されます。例えば、ドメイン「yahoo」がこのリストに追加されると、次の URL のすべてが LAN からのアクセスを許可されます。: www.yahoo.com、yahoo.co.uk など。また、CSV ファイルから Approved URL をインポートすることができます。

1. **ADVANCED > Website Filter > Content Filtering** の「Enable Content Filtering」を有効とします。

2. **ADVANCED > Website Filter > Approved URLs** の順にメニューをクリックし、以下の画面を表示します。

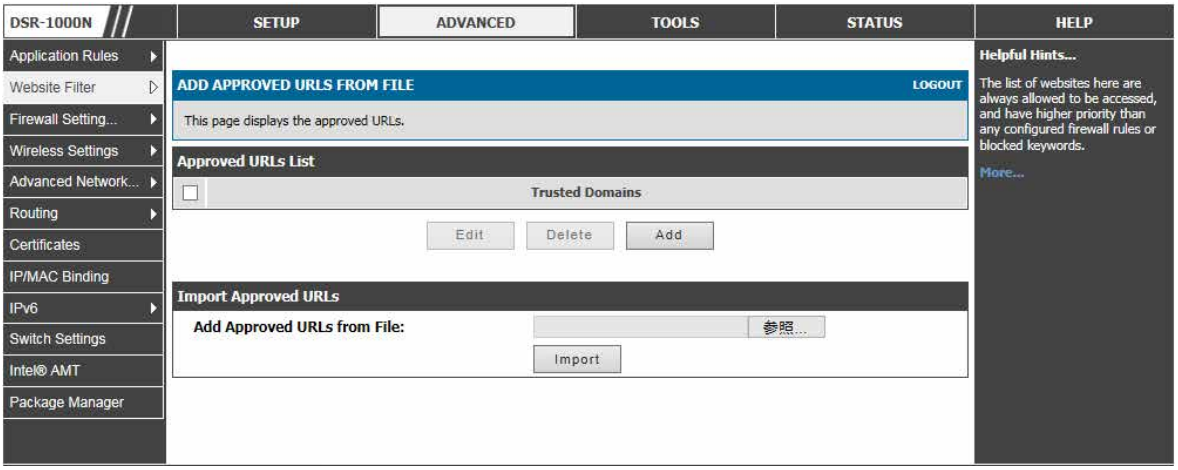


図 7-28　Approved URL List 画面

入力による URL の追加
1. 「Add」ボタンをクリックして、以下の画面を表示します。

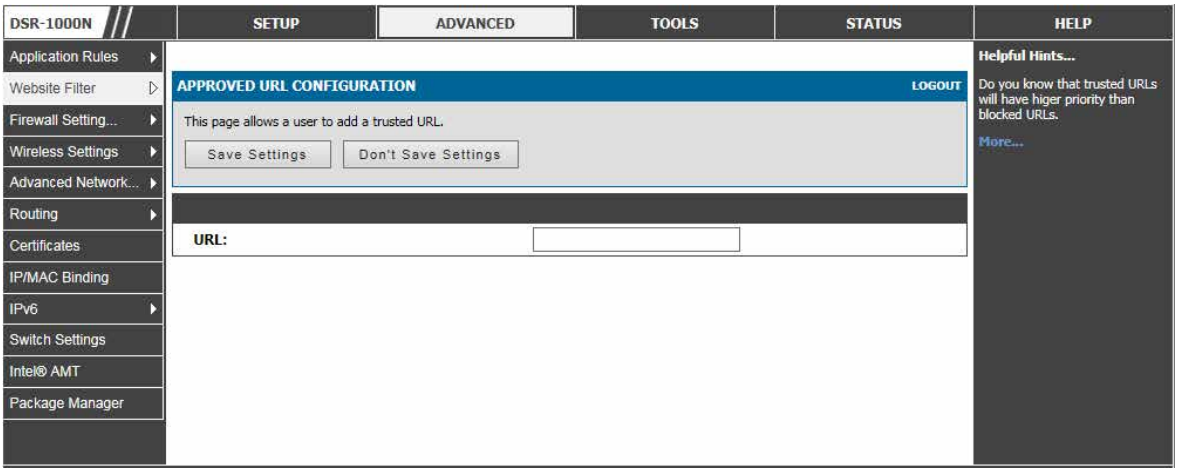


図 7-29　URL の追加

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ファイルによる URL の追加
1. 「Import Approved URLs」セクションで URL を含むローカルにある CSV ファイルボタンを選択します。

2. 「Import」ボタンをクリックして CSV ファイルを読み込みます。

Blocked Keywords（ブロックキーワード）

ADVANCED > Website Filter > Blocked Keywords メニュー

URL またはキーワードを入力することで、Web サイトへのアクセスをブロックします。

キーワードブロッキングでは、設定済みリスト内にあるキーワードを含むすべての Web サイトの URL またはサイトのコンテンツをブロックすることができます。これは「Approved URLs List」より低い優先度です。つまり、ブロックキーワードが「Approved URLs List」のトラストドメインによって許可されたサイトに存在している場合、そのサイトへのアクセスは許可されます。また、CSV ファイルから Blocked URL をインポートすることができます。

1. **ADVANCED > Website Filter > Content Filtering** の「Enable Content Filtering」を有効とします。

2. **ADVANCED > Website Filter > Blocked Keywords** の順にメニューをクリックし、以下の画面を表示します。

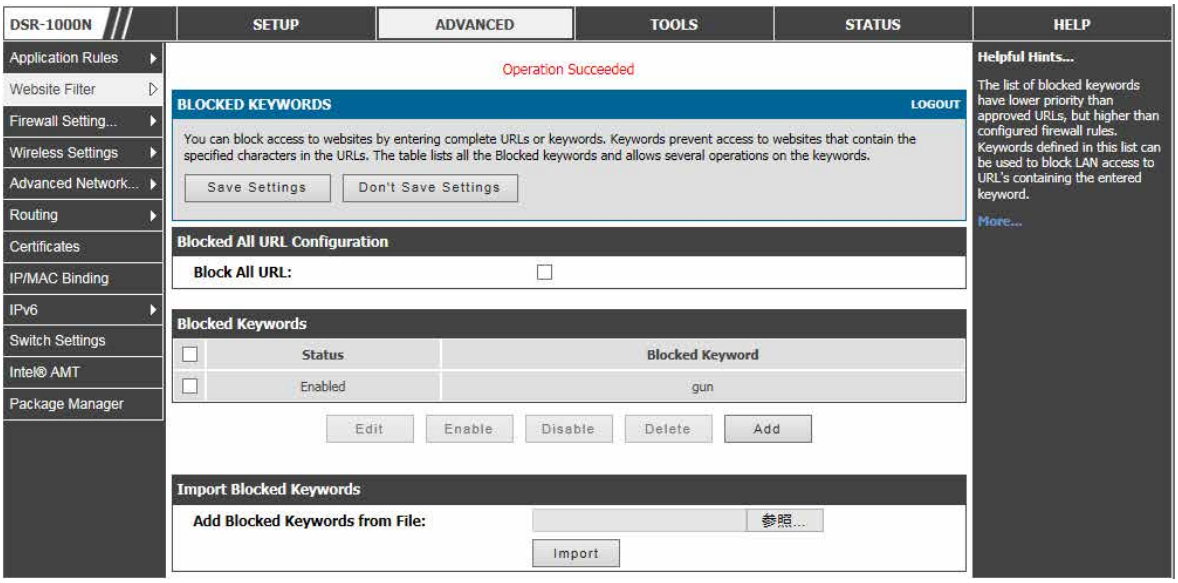


図 7-30　ブロックリストに追加されたキーワード

入力によるキーワードの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

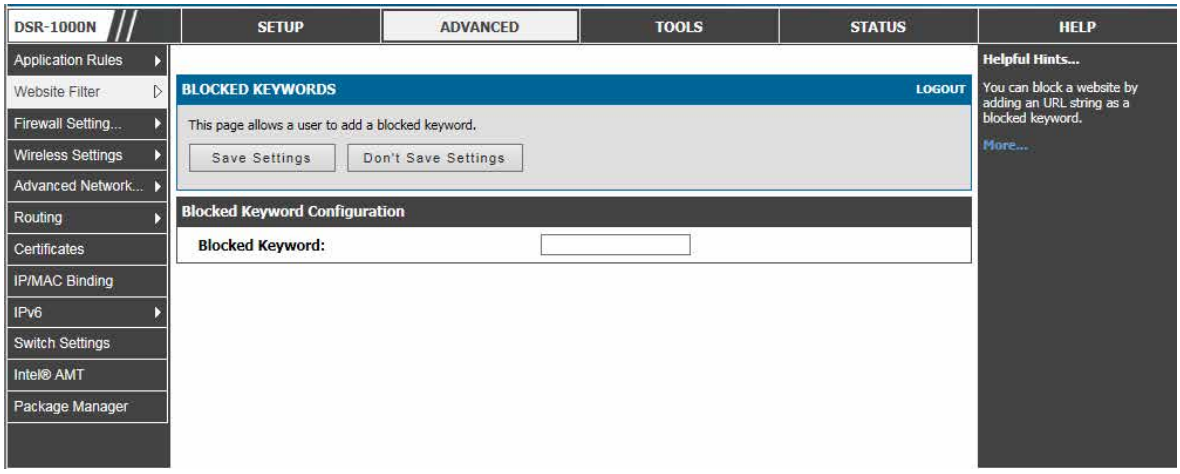


図 7-31　キーワードの追加

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ファイルによる URL の追加

1. 「Import Blocked URLs」セクションで URL を含むローカルにある CSV ファイルボタンを選択します。

2. 「Import」ボタンをクリックして CSV ファイルを読み込みます。

Web フィルタのエクスポート

ADVANCED > Website Filter > Export メニュー

許可する URL およびブロックするキーワードをエクスポートします。

1. **ADVANCED > Website Filter > Export** の順にメニューをクリックし、以下の画面を表示します。

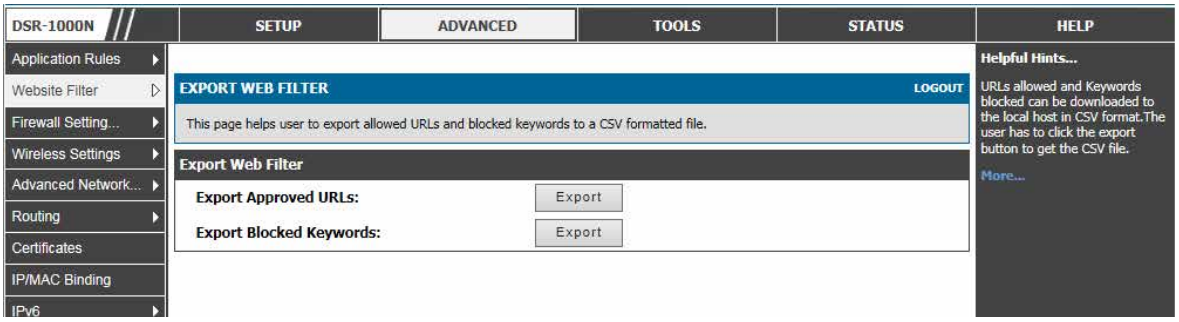


図 7-32　承認済み URL リストのエクスポート

2. 以下の項目を指定します。

項目	説明
Export Approved URLs	URL をローカルホストにダウンロードできる CSV ファイルにエクスポートします。「Export」ボタンをクリックして CSV ファイルを取得します。
Export Blocked Keywords	キーワードをローカルホストにダウンロードできる CSV ファイルにエクスポートします。「Export」ボタンをクリックして CSV ファイルを取得します。

IP/MAC バインディング

ADVANCED > IP/MAC Binding メニュー

現在定義済みの IP/MAC バインドルールを表示し、ルールにいくつかの操作を許可します。

LAN ノードがバインドされた MAC アドレスに一致する IP アドレスを持つ場合にだけ、別の利用可能なセキュリティ対策は（LAN から WAN までの）外向きトラフィックを許可することになっています。これは IP/MAC バインディングで、管理者はゲートウェイが設定済み LAN ノードの固有の MAC アドレスを持つ送信元トラフィックの IP アドレスを確認することで IP アドレスが偽造されないことを保証することができます。違反（すなわち、トラフィックの送信元 IP アドレスが同じ IP アドレスを持っていると思われた MAC アドレスに一致しない）の場合、パケットを破棄して診断のためにログに出力します。

1. **ADVANCED > IP/MAC Binding** の順にメニューをクリックし、以下の画面を表示します。

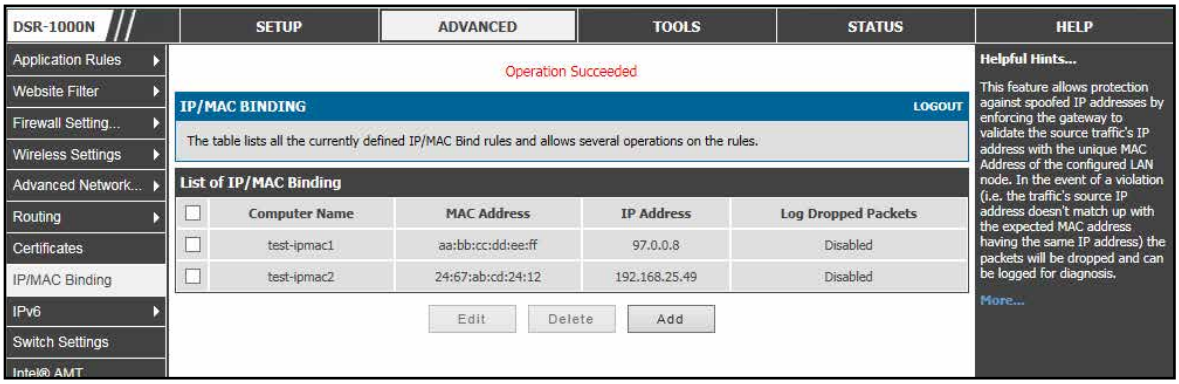


図 7-33　IP/MAC Binding 画面

上記の例では LAN ホストの MAC アドレスを IP アドレスに割り当てています。IP/MAC Binding の違反があると、違反パケットは破棄され、ログに出力されます。

2. 以下の項目を表示します。

項目	説明
Computer Name	本ルールのユーザ定義名を表示します。
MAC Address	本ルールの MAC アドレスを表示します。
IP Address	本ルールの IP アドレスを表示します。
Log Dropped Packets	本ルールのログ出力オプションを表示します。

IP/MAC バインディングの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

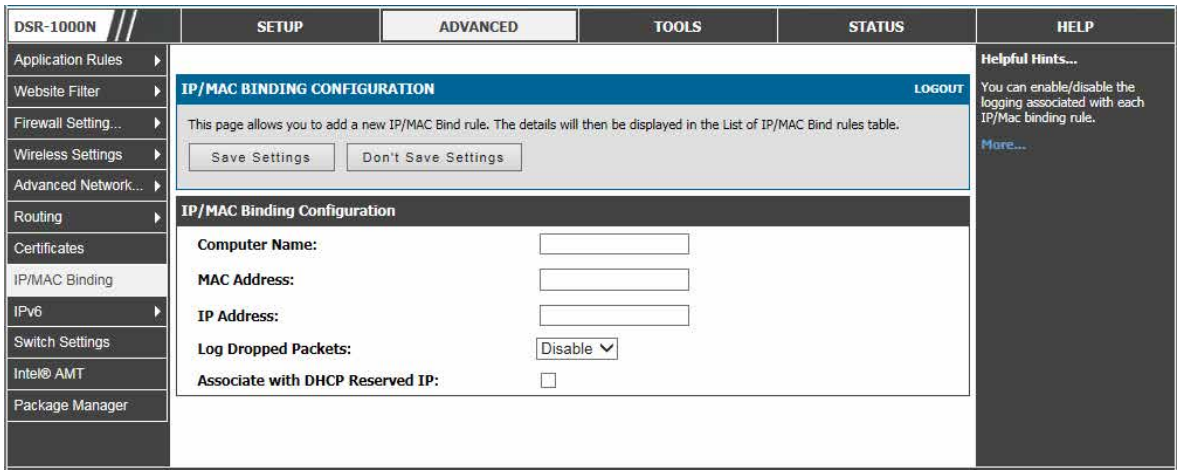


図 7-34　IP/MAC バインディングの追加

2. 以下の項目を指定します。

項目	説明
Computer Name	本ルールのユーザ定義名を指定します。
MAC Address	MAC アドレスを指定します。
IP Address	IP アドレスを指定します。
Log Dropped Packets	本ルールのログ出力オプションを指定します。有効にすると、パケットを破棄する前にログに出力されます。ルータは IP to MAC バインディングまたは MAC to IP バインディングのいずれかを侵害した破棄パケット数の合計を表示します。
Associated with DHCP Reserved IP	DHCP の予約 IP アドレスを使用したアソシエーションにする場合に指定します。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

IPS（Intrusion Protection シグネチャ）

ADVANCED > Advanced Network > IPS メニュー

ここではルータに侵入検知システム（IDS）および侵入防止システム（IPS）を設定することができます。

ゲートウェイの IPS は、インターネットからの悪意ある攻撃がプライベートネットワークにアクセスするのを防ぎます。デバイスにロードされたスタティックな攻撃シグネチャは、一般的な攻撃を検出して、防御することができます。WAN と DMZ または LAN 間でチェックを有効にすることができます。また、動作しているカウンタにより、管理者は WAN からの悪意ある侵入の試みが検出され、防御された数を参照することができます。

1. **ADVANCED > Advanced Network > IPS** の順にメニューをクリックし、以下の画面を表示します。

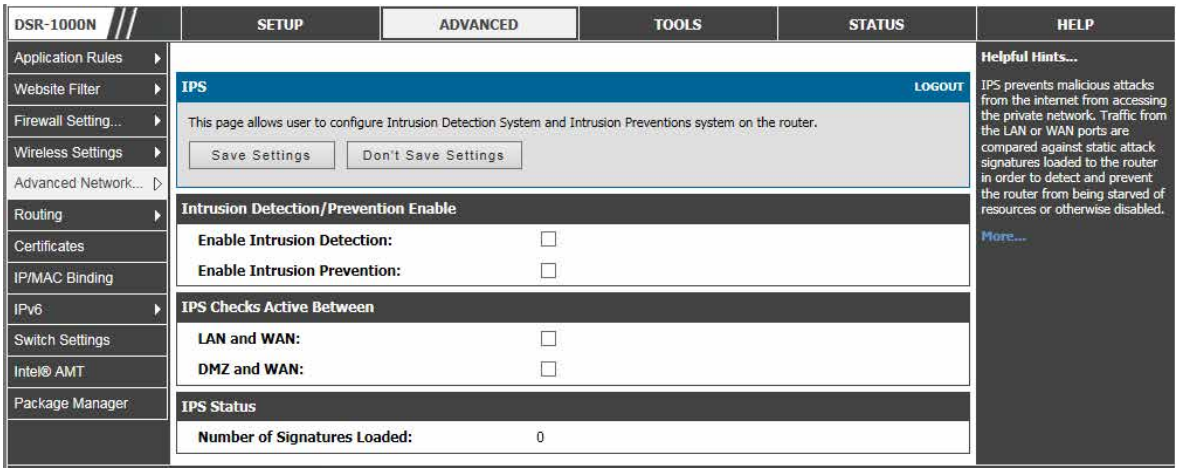


図 7-35　ルータにおける侵入防止機能

2. 以下の項目を指定します。

項目	説明
Intrusion Detection/Prevention Enable	
Enable Intrusion Detection	選択すると侵入イベントが検出されてログに出力されます。ゲートウェイへの各入力パケットはこのページで行った設定に基づいて潜在的な悪意ある攻撃のために調査されます。
Enable Intrusion Prevention	選択すると、デバイス侵入防止システムは WAN からインライントラフィックをモニタすることができますが、システム性能に影響します。
IPS Checks Active Between	
LAN and WAN	選択すると、セキュアな LAN とパブリック WAN 間の IPS を有効にします。
DMZ and WAN	選択すると、セキュアな DMZ とパブリック WAN 間の IPS を有効にします。
IPS Status	
Number of Signatures Loaded	ルータに保存される侵入のシグネチャ数で、IPS イベントの検出に使用されます。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

インターネット攻撃からの保護

ADVANCED > Advanced Network > Attack Checks メニュー
LAN と WAN ネットワークを一般的な攻撃から保護するか否かを指定します。

攻撃は、ルータを使用不能にする悪意あるセキュリティ違反または意図的ではないネットワーク問題であるかもしれません。攻撃のチェックにより連続する ping リクエストや ARP スキャンを経由するディスカバリなど WAN のセキュリティの脅威を管理することができます。TCP および UDP フラッド攻撃のチェックを有効にすると、WAN リソースの極端な利用を管理することができます。

さらに Denial-Of-Service（DoS）攻撃がブロックされます。率直に言うと、これらの攻撃は、処理能力と帯域幅を使い切り、通常、定期的なネットワークサービスの動作を妨げてしまいます。ICMP パケットフラッディング、SYN トラフィックフラッディング、および Echo ストームのしきい値は問題となるソースからのトラフィックを一時的に疑うために設定されます。

1. **ADVANCED > Advanced Network > Attack Checks** の順にメニューをクリックし、以下の画面を表示します。

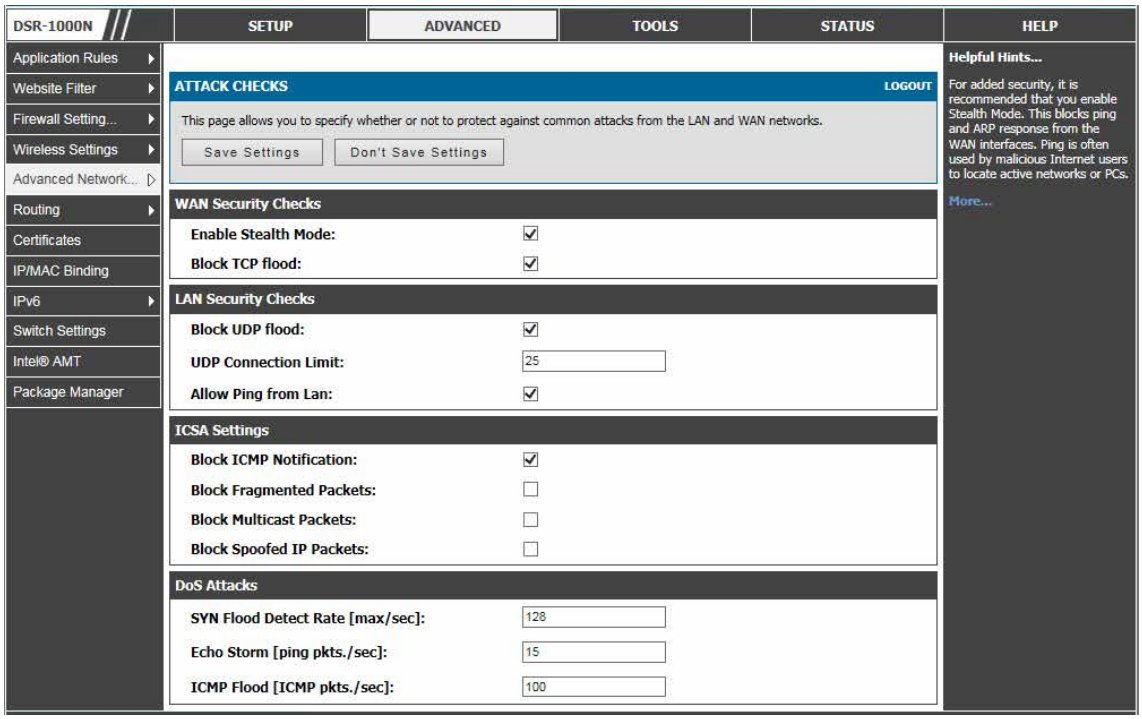


図 7-36　インターネット攻撃からルータと LAN を保護する

2. 以下の項目を指定します。

項目	説明
WAN Security Checks	
Enable Stealth Mode	「Stealth Mode」モードが有効になると、ルータは WAN からのポートスキャンに応答しません。これにより検出と攻撃による影響を低減します。
Block TCP Flood	本オプションを有効にすると、ルータは不正な TCP パケットをすべて破棄して、SYN フラッド攻撃から保護されます。
Allow Ping from Lan	本オプションを有効にすると、LAN からの ping に応答します。
LAN Security Checks	
Block UDP Flood	本オプションが有効になると、ルータは LAN 上の単一のコンピュータから同時に行われる 20 個以上のアクティブな UDP 接続を受け付けません。
UDP Connection Limit	LAN 上の 1 つのコンピュータから同時に受け付けられるアクティブな UDP 接続数を設定できます。初期値は 25 です。
ICSA Settings	
Block ICMP Notification	これを選択すると、ICMP パケットが特定されることを防止します。ICMP パケットは、特定されるとキャプチャされて Ping (ICMP) フラッド DoS 攻撃に使用されてしまいます。
Block Fragmented Packets	このオプションを選択すると、ゲートウェイを経由するどんなフラグメント化パケットも破棄します
Block Multicast Packets	このオプションを選択すると、ゲートウェイを経由するマルチキャストパケットを破棄します。
Block Spoofed IP Packets	このオプションを選択すると、IP スプーフィングパケットを破棄します。

項目	説明
DoS Attacks	
SYN Flood Detect Rate (max/sec)	SYN フラッドを検出できるレート。
Echo Storm (ping pkts/sec)	ルータが WAN からエコーストーム攻撃を検出して、その外部アドレスから更に ping トラフィックを防止する 1 秒あたりの ping パケット数。
ICMP Flood (ICMP pkts/sec)	ルータが WAN から ICMP フラッド攻撃を検出して、その外部アドレスから更に ICMP トラフィックを防止する 1 秒あたりの ICMP パケット数。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

注意 LAN インタフェースにおける ping は初期値では有効です。LAN ホストからデバイスの LAN/WAN ポートまでの ping 応答を無効にするには、「Allow Ping from Lan」オプションのチェックを外してください

IGMP プロキシの設定

ADVANCED > Advanced Network > IGMP Setup メニュー

IGMP Snooping では、ルータを通じた IGMP ネットワークトラフィックのリッスンを可能にします。また、ルータは、マルチキャストトラフィックをフィルタして、このストリームを必要とするホストだけに、これを送ることが可能になります。これは、すべての LAN ホストがこのマルチキャストトラフィックを受信する必要のないネットワーク (IPTV アプリケーションのため) に大量のマルチキャストトラフィックがある場合に役立ちます。IGMP Snooping を有効にすると、ルータがネットワーク上のマルチキャストトラフィックの量を規制して、すべての LAN ホストがフラッドすることを防止します。アクティブな IGMP Snooping は IGMP プロキシに参照され、ご使用のコントローラで利用可能となります。

1. **ADVANCED > Advanced Network > IGMP Setup** の順にメニューをクリックし、以下の画面を表示します。

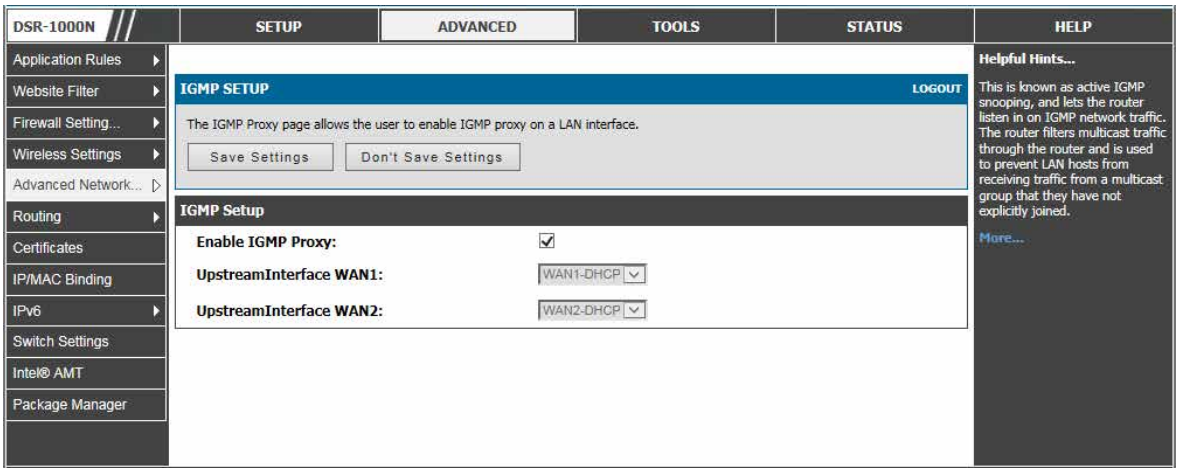


図 7-37　LAN への IGMP プロキシを有効にする

2. 以下の項目を指定します。

項目	説明
Enable IGMP Proxy	これを選択すると、ルータは、ネットワークを介する IGMP トラフィックをリッスンして、LAN に向かうマルチキャストストリームを管理することができます。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

Intel® AMT

ADVANCED > Intel AMT メニュー

Intel® AMT サービスを設定します。Intel® AMT サービスを有効にすると、Intel® AMT ポート、VNC ポート、および SNMP トラップポートへの適切な内向き / 外向きファイアウォールルールの追加をもたらします。すべてのファイアウォールルール内で、Intel® AMT ルールは最も高い優先度を持っています。Intel® AMT Reflector を有効にすると、内向き接続の選択ポートでサーバがリッスンするという結果になります。

Intel® アクティブ・マネジメント・テクノロジー (AMT) により IT 管理者はネットワークに接続するコンピュータのシステムごとにリモートでアクセスおよび管理できます。PC/ ノート PC の電源がオフまたは OS がクラッシュして OS やハードディスクが動作していない場合、PC/ ノート PC が電源およびネットワーク接続している間に電源をオフにしても可能です。Intel® AMT は個別にクライアントマシンで動作して、有線または無線ネットワークを通じて接続できる独立した管理プロセッサを使用しています。D-Link DSR ルータを使用して、AMT はインターネットをシームレスに通過し、インターネット経由の資産管理のために IT 管理者を補助する理想的なソリューションです。

1. **ADVANCED > Intel AMT** の順にメニューをクリックし、以下の画面を表示します。

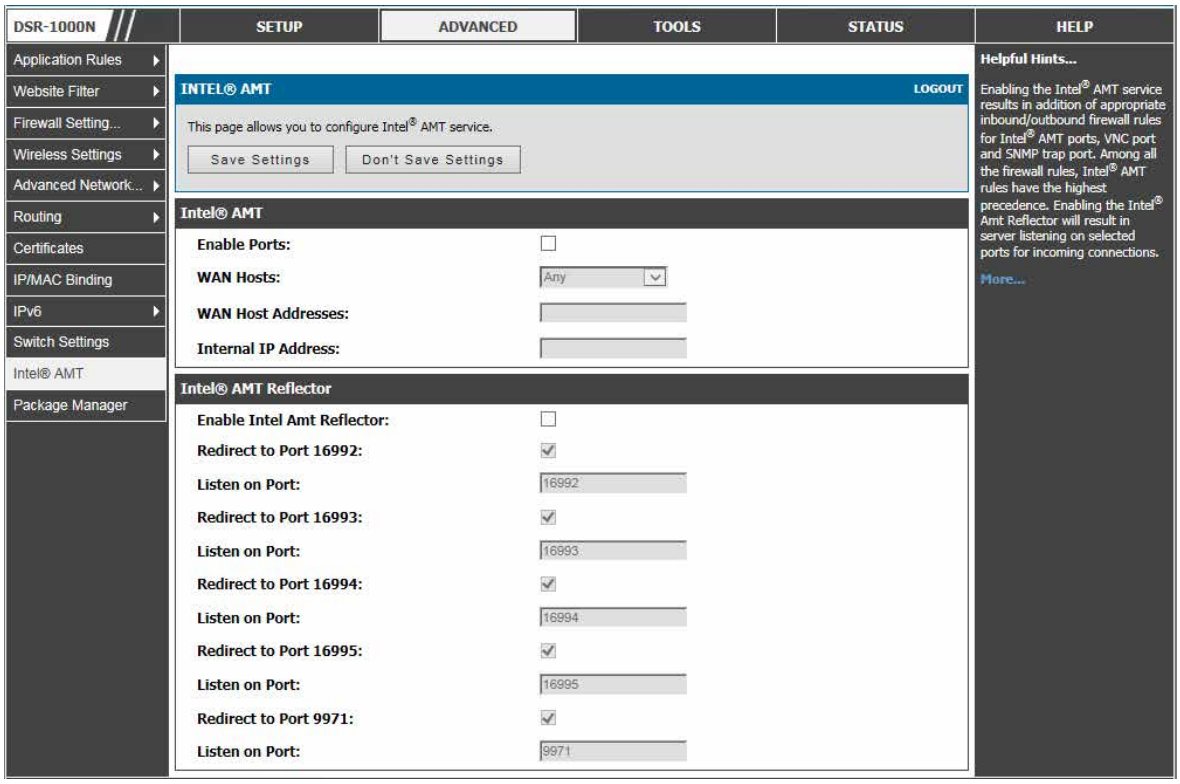


図 7-38　Intel® AMT 設定

2. 以下の項目を設定します。

項目	説明
Intel® AMT	
Enable Ports	有効にすると、特定のポートに対して Intel® AMT サービスを有効にするように、内向き / 外向きファイアウォールルールを追加することができます。
WAN Hosts	「Any」を選択すると、WAN 側の全ホストがローカルサーバへのアクセスを許可されます。「Specify WAN IPs」を選択した場合、ローカルサーバ（LAN ホスト）へのアクセスを許可される WAN ホストアドレスリストをカンマ「,」で分離して指定する必要があります。
WAN Host Addresses	プルダウンメニューで「Specify WAN IPs」を選択した場合には、ローカルユーザへのアクセス許可が必要な WAN IP アドレスのカンマ「,」で分離したリストを指定する必要があります。カンマ「,」だけが許可されており、カンマと IP アドレスの間にスペースを入れないでください。
Internal IP Address	LAN ホスト (ローカルサーバ) の 1 つの IP アドレスを指定します。

項目	説明
Intel® AMT Reflector	
Enable Intel® AMT Reflector	このボックスをチェックすると、クライアントが開始する接続に対して選択ポートのデータを反映します。
Redirect to Port 16992	このボックスをチェックすると、クライアントが開始する接続についてポート 16992 にリダイレクトします。
Listen on Port	サーバが内向き接続に対してリッスンすべきポートを入力します。
Redirect to Port 16993	このボックスをチェックすると、クライアントが開始する接続についてポート 16993 にリダイレクトします。
Listen on Port	サーバが内向き接続に対してリッスンすべきポートを入力します。
Redirect to Port 16994	このボックスをチェックすると、クライアントが開始する接続についてポート 16994 にリダイレクトします。
Listen on Port	サーバが内向き接続に対してリッスンすべきポートを入力します。
Redirect to Port 16995	このボックスをチェックすると、クライアントが開始する接続についてポート 16995 にリダイレクトします。
Listen on Port	サーバが内向き接続に対してリッスンすべきポートを入力します。
Redirect to Port 9971	このボックスをチェックすると、クライアントが開始する接続についてポート 9971 にリダイレクトします。
Listen on Port	サーバが内向き接続に対してリッスンすべきポートを入力します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

第 8 章　IPSec / PPTP / L2TP VPN 設定

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

設定項目	説明	参照ページ
VPN ウィザード	ウィザードを使用して VPN 設定を行います。	131 ページ
IPSec ポリシーの設定	IPSec ポリシーを作成します。	134 ページ
VPN クライアントの設定	VPN クライアントの設定について説明します。	140 ページ
PPTP / L2TP トンネル	PPTP または L2TP VPN トンネルを設定します。	140 ページ

VPN は 2 つのゲートウェイルータ間またはリモート PC クライアント間に安全な通信チャネル（「トンネル」）を提供します。以下のトンネルタイプを作成することができます。:

- Gateway-to-gateway VPN
  リモートサイト間のトラフィックを保証するために 2 つ以上のルータを接続します。

- リモートクライアント（client-to-gateway VPN トンネル）
  リモート PC クライアントの IP アドレスが事前に知られていない場合に、リモートクライアントが VPN トンネルを開始します。この場合、ゲートウェイは応答者として動作します。

- NAT ルータの背後のリモートクライアント
  クライアントはダイナミック IP アドレスを持ち、NAT ルータの背後にあります。リモート NAT ルータの IP アドレスが事前に知られていない場合に、NAT ルータにあるリモート PC が VPN トンネルを開始します。ゲートウェイの WAN ポートが応答者として動作します。

- LAN/WAN PPTP クライアント接続のための PPTP サーバ。

- LAN/WAN L2TP クライアント接続のための L2TP サーバ。

インターネットに接続する 2 つの DSR を使用した Gateway-to-Gateway IPSec VPN トンネルの例

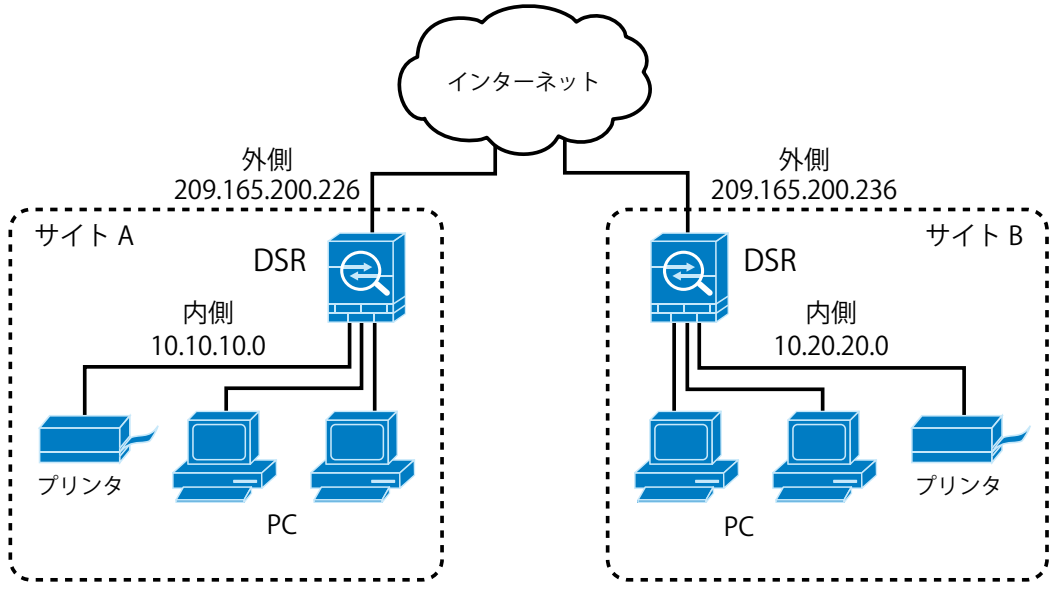


図 8-1　IPSec VPN トンネルの例

DSR IPSec ゲートウェイを通じて内部ネットワークに接続する 3 つの IPSec クライアントの例

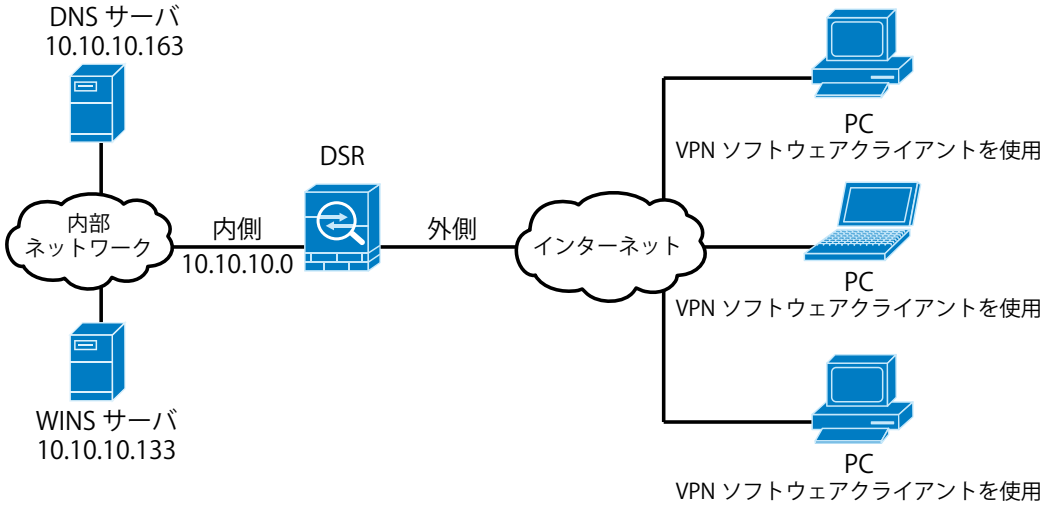


図 8-2　IPSec クライアントの例

VPN ウィザード

SETUP > Wizard > VPN Wizard メニュー

VPN ウィザードを使用して素早く IKE および VPN ポリシーの両方を作成することができます。IKE または VPN ポリシーの作成後、必要に応じてそれらを変更することができます。

1. **SETUP > Wizard > VPN Wizard** の順にメニューをクリックし、以下の画面を表示します。

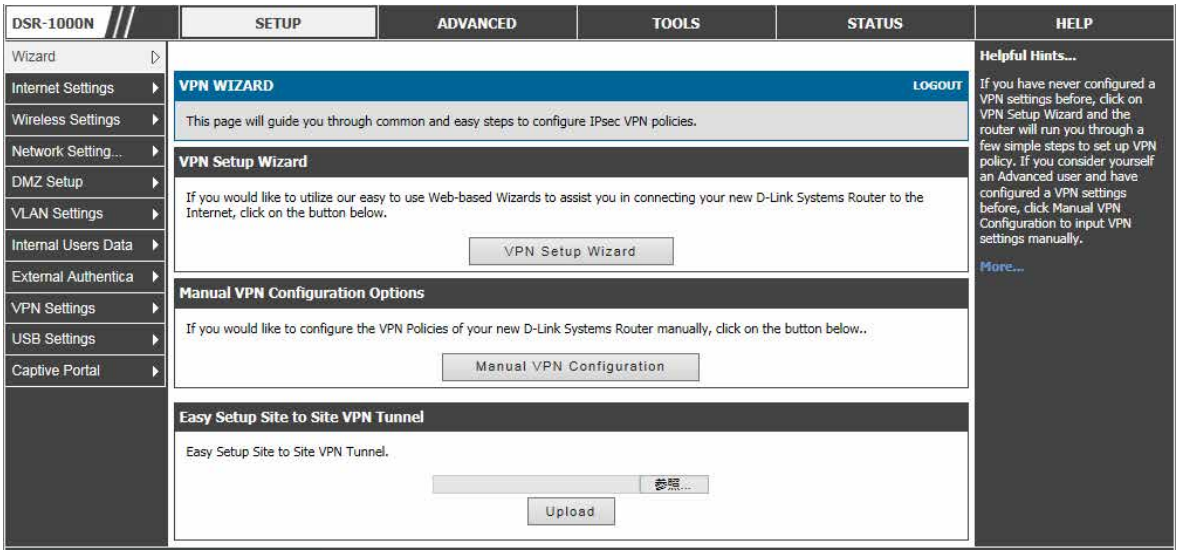


図 8-3　VPN ウィザードの開始画面

VPN Setup Wizard

以下の手順に従って VPN ウィザードを使用して簡単に VPN トンネルの確立を行います。:

1. 作成する VPN トンネルタイプをします。

「VPN Setup Wizard」ボタンをクリックして、以下の画面を表示します。

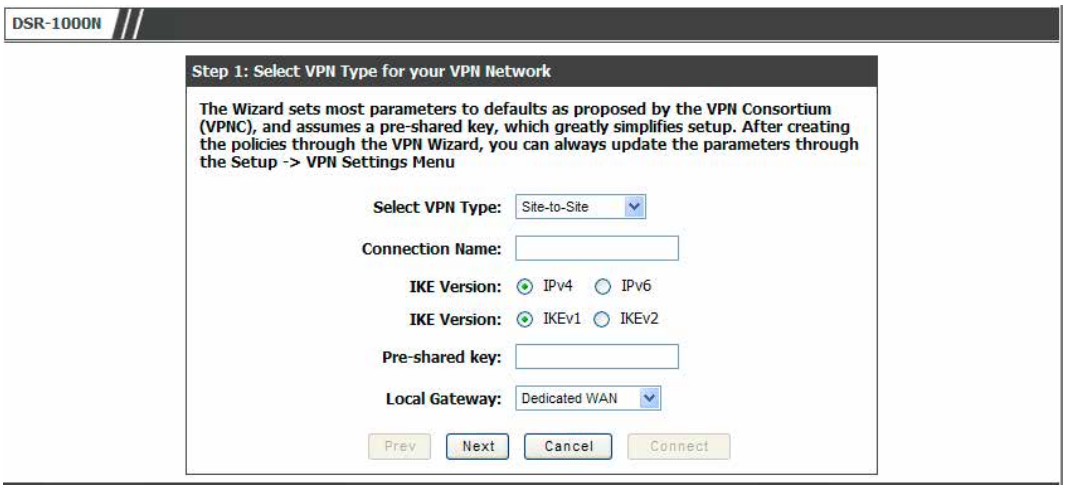


図 8-4　VPN ウィザード手順 1 画面

以下の項目を設定します。

項目	説明
Select VPN Type	トンネルは、gateway to gateway 接続（Site-to-Site）またはインターネット上のホストへのトンネル（Remote Access）のいずれかとすることができます。
Connection Name	管理に使用される接続名を設定します。
IKE Version	IP バージョン（IPv4 または IPv6）を選択します。
IKE Version	IKE バージョン（IKEv1 または IKEv2）を選択します。
Pre-Shared key	事前共有鍵（最大 64 桁）を設定します。事前共有鍵はトンネルを確立するために VPN クライアントまたはゲートウェイで必要です。
Local Gateway	このトンネルのためのローカルゲートウェイを決定します。1 つ以上の設定済み WAN がある場合、トンネルはゲートウェイのいずれかに対して設定されます。

「Next」ボタンをクリックします。

2. トンネルのエンドポイントにリモートおよびローカルの WAN アドレスを設定します。

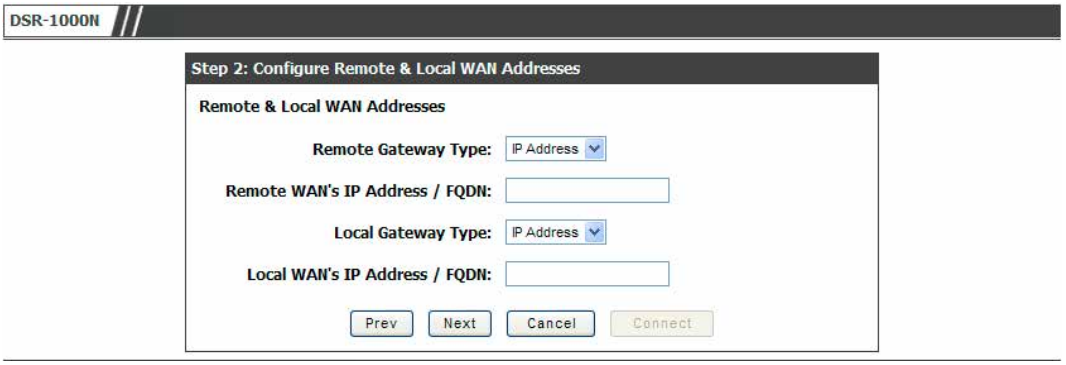


図 8-5　VPN ウィザード手順 2 画面

以下の項目を設定します。

項目	説明
Remote Gateway Type	FQDN またはスタティック IP アドレスによってトンネルのリモートエンドポイントを識別します。
Remote WAN's IP Address / FQDN	接続を試みるピアがゲートウェイである場合にだけ、本欄は有効にされます。VPN クライアントでは、クライアントから接続要求を受信する場合に、この IP アドレスまたはインターネット名が決定されます。
Local Gateway Type	FQDN またはスタティック IP アドレスによってトンネルのルータのエンドポイントを識別します。
Local WAN's IP Address / FQDN	異なる FQDN を使用していない場合、または WAN ポートの設定に 1 つ以上の IP アドレスが指定されている場合、本欄を空白のままにできます。

「Next」ボタンをクリックします。

3. リモートネットワークを識別するために「Secure Connection Remote Accessibility」欄を設定します。

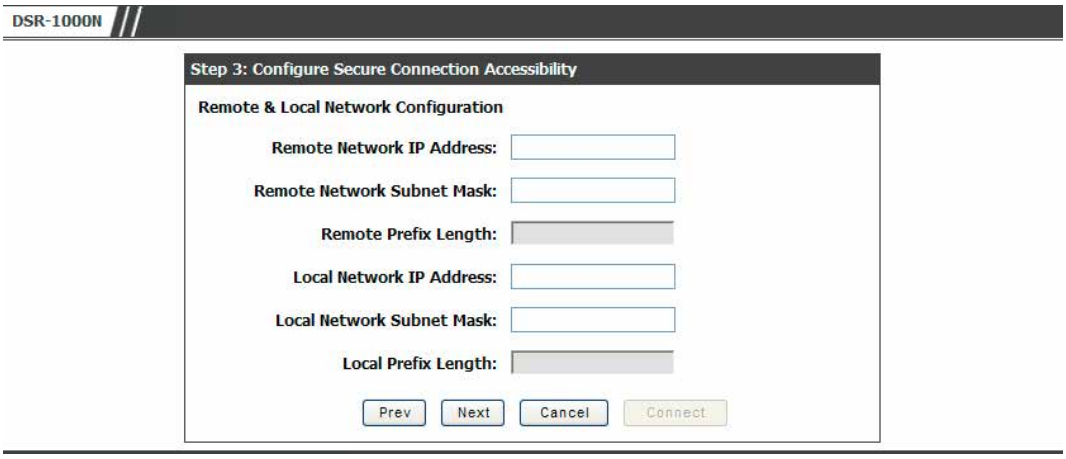


図 8-6　VPN ウィザード手順 3 画面

以下の項目を設定します。

項目	説明
Remote Network IP Address	リモート LAN の IP アドレス。
Remote Network Subnet Mask	リモート LAN のサブネットマスク。
Remote Prefix Length	リモート LAN のプレフィックス長。
Local Network IP Address	ローカル LAN の IP アドレス。
Local Network Subnet Mask	ローカル LAN のサブネットマスク。
Remote Prefix Length	ローカル LAN のプレフィックス長。

「Next」ボタンをクリックします。

注意 リモート LAN で使用される IP アドレス範囲は、ローカル LAN で使用される IP アドレス範囲と異なる必要はあります。

4. 設定を見直して、「Connect」ボタンをクリックしてトンネルを確立します。ウィザードは VPN クライアントまたはゲートウェイポリシーに以下の初期値を持つ自動 IPSec ポリシーを作成します。:

項目	ウィザードの初期値
交換モード	Aggressive（クライアントのポリシー）または Main（ゲートウェイのポリシー）
ID タイプ	FQDN
ローカル WAN ID	wan_local.com（クライアントのポリシーにだけ適用します。）
リモート WAN ID	wan_local.com（クライアントのポリシーにだけ適用します。）
暗号化アルゴリズム	3DES
認証アルゴリズム	SHA-1
認証方式	事前共有鍵（最大 64 桁）
PFS キーグループ	DH グループ 2（1024 ビット）
ライフライム（フェーズ 1）	24 時間
ライフライム（フェーズ 2）	8 時間
NETBIOS	Enabled（ゲートウェイポリシーにだけ適用します。）

注意 VPN ウィザードは自動 IPSec ポリシーに設定するお勧めの方法です。一度、ウィザードが、自動ポリシーに要求された一致する IKE および VPN ポリシーを作成すると、リストから選択して必要な欄を編集することができます。詳細についてはオンラインヘルプを参照してください。

Easy Setup Site to Site VPN Tunnel

VPN ウィザードを通じた VPN ポリシーの作成が困難である場合、「Easy Setup Site to Site VPN Tunnel」（サイト間 VPN トンネル簡単設定）を使用してください。これは、VPN ポリシーを含むファイルをインポートすることで VPN ポリシーを追加します。

ファイルを選択後、「Upload」ボタンをクリックします。

IPSec ポリシーの設定

外部 IPsec クライアントは、DHCP over IPsec を使用してルータへの VPN を形成し、どんなサーバにもアクセスするなどご使用の LAN にいるかのように動作することができます。DHCP over IPsec を使用して接続するためには、クライアントを許可するように DHCP を有効化にして IPSec ポリシーを作成します。また、接続クライアントは指定した範囲から IP アドレスを取得します。

IPSec VPN ポリシーの設定

SETUP > VPN Settings > IPsec > IPsec Policies メニュー

ここではルータに設定済みの IPSec VPN ポリシーのリストを表示します。さらに、IPsec VPN ポリシーの追加、削除、編集、および有効化 / 無効化ができます。

1. **SETUP > VPN Settings > IPsec > IPsec Policies** の順にメニューをクリックし、以下の画面を表示します。

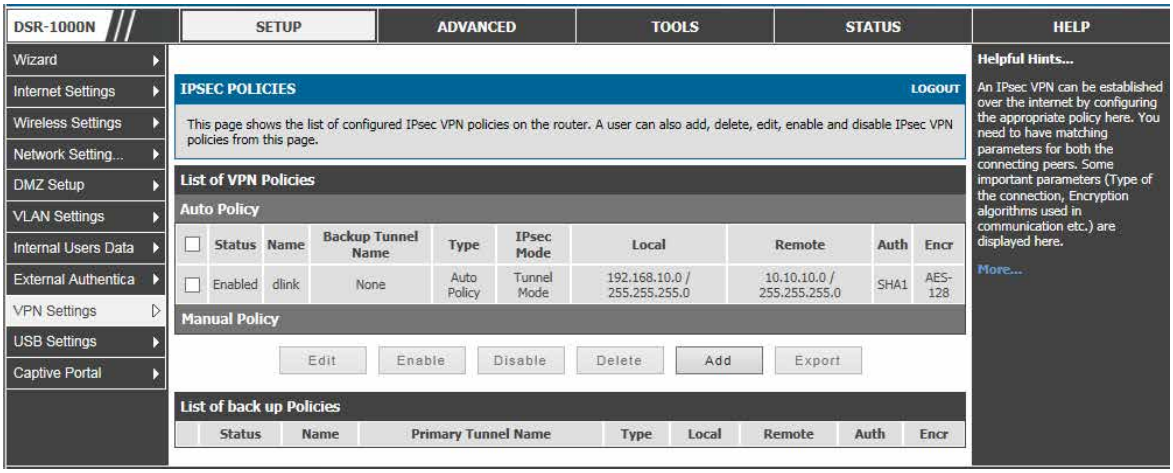


図 8-7　IPSec ポリシーリスト画面

IPSec ポリシーは本ルータと他のゲートウェイ間、または本ルータとリモートホストの IPSec クライアント間にあります。IPSec モードは、2 つのポリシーのエンドポイント間を横切るネットワークによって「Tunnel Mode」または「Transport Mode」になります。

- Transport Mode（転送モード）：
  これはこのルータとトンネルのエンドポイント（ホスト上の別の IPSec ゲートウェイまたは IPSec クライアントのいずれか）間の end-to-end 通信のために使用されます。データペイロードだけが暗号化されて、IP ヘッダは、変更または暗号化されません。

- Tunnel Mode（トンネルモード）：
  このモードはこのゲートウェイがトンネルの 1 つのエンドポイントである network-to-network IPSec トンネルに使用されます。このモードでは、ヘッダを含むすべての IP パケットは、暗号化と認証の両方、またはどちらかが行われています。

  トンネルモードを選択した場合、NetBIOS および DHCP over IPSec を有効にすることができます。DHCP over IPSec によりこのルータはリモート LAN のホストに IP リースをサービスすることができます。また、このモードでは、1 つの IP アドレス、IP アドレス範囲、またはトンネル上で通信できるローカルおよびリモート両方のプライベートネットワークにおけるサブネットを定義できます。

IPSec VPN ポリシーの追加

1. 「Add」ボタンをクリックし、以下の画面を表示します。

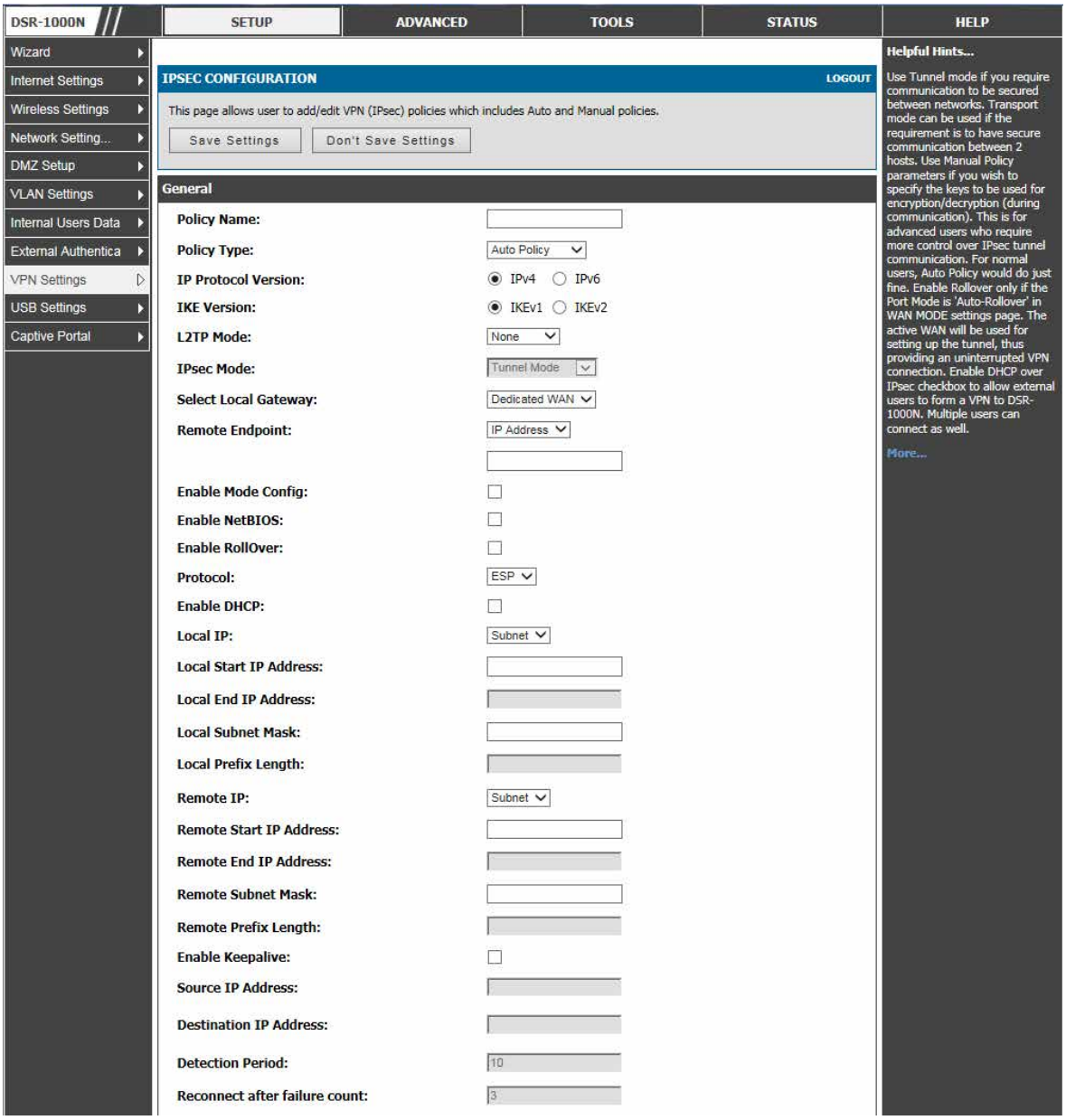


図 8-8　　IPSec ポリシー設定

トンネルタイプとトンネルのエンドポイントが定義されると、トンネルに使用するフェーズ 1/ フェーズ 2 のネゴシエーションを決定できます。ポリシーは、「Manual Policy」（手動ポリシー）または「Auto Policy」（自動ポリシー）とすることができるため、IPSec モード設定でこれに対応します。「Auto Policy」ポリシーでは、IKE（Internet Key Exchange）プロトコルは 2 つの IPSec ホスト間でダイナミックに鍵交換を行います。フェーズ 1 の IKE パラメータは、トンネルのセキュリティ関係の詳細を定義するのに使用されます。フェーズ 2 の「Auto Policy Parameters」セクションはフェーズ 2 のキーネゴシエーションに関するセキュリティ関係のライフタイムと暗号化 / 認証の詳細に対応しています。

VPN ポリシーは、自動 IPSec VPN トンネルを確立するのに必要とされる IKE/VPN ポリシーのペアの片方です。2 つの VPN エンドポイントにあるマシンの IP アドレスは、トンネルをセキュアにするために必要とされるポリシーパラメータと共にここで設定されます。

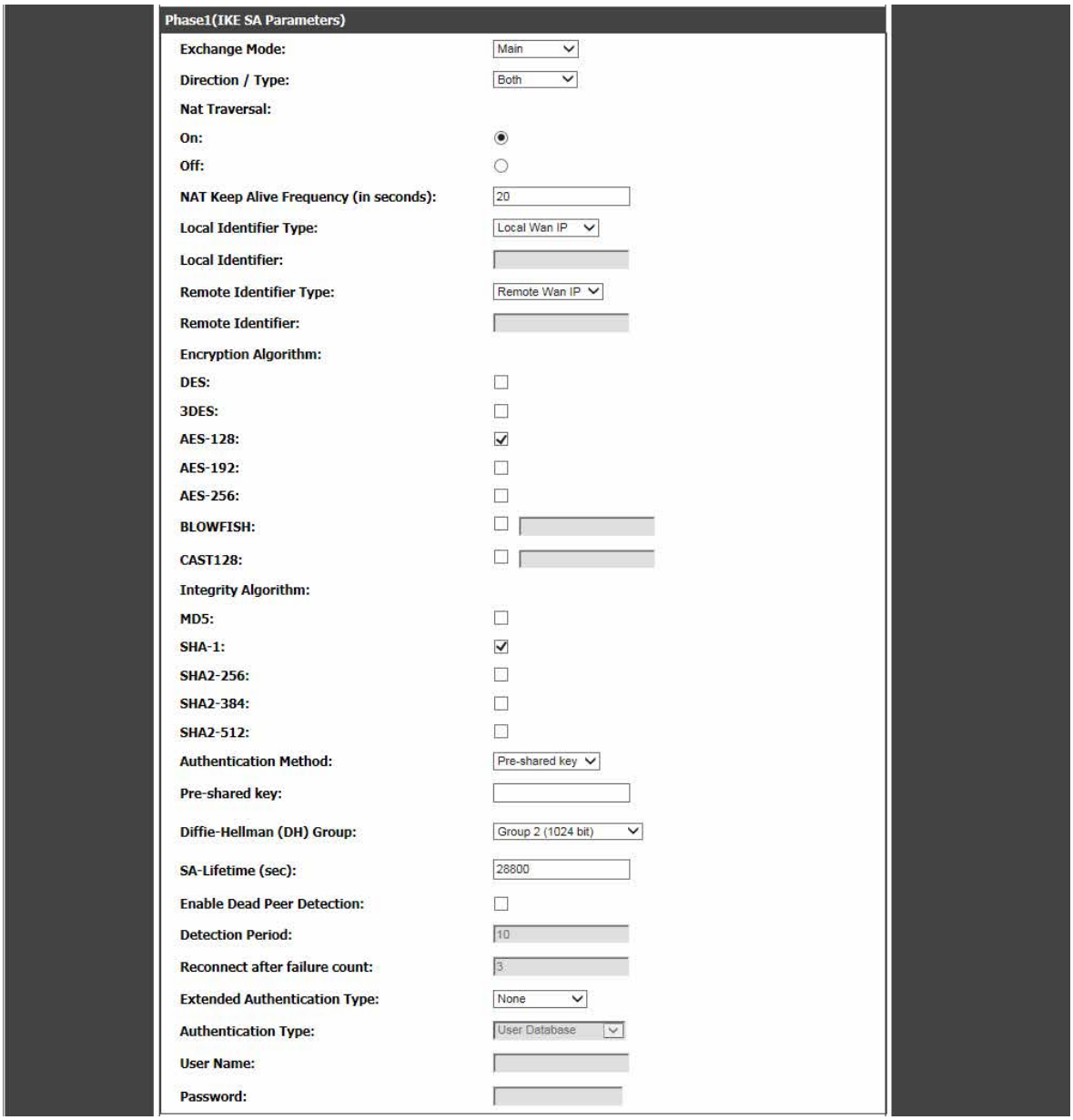


図 8-9　IPSec ポリシー設定（IKE を経由した自動ポリシー）

「Manual Policy」は、代わりに 2 つの IPSec ホスト間で認証パラメータを交換するために、IKE を使用しないで、代わりに手動のキー操作に依存します。リモートトンネルのエンドポイントで入出力する SPI（security parameter index）値を反映する必要があります。また、トンネルの確立に成功するためには、暗号化、保全アルゴリズム、およびキーはリモート IPSec ホストに一致する必要があります。SPI（security parameter index）値を各エンドポイントで変換する必要があるいくつかの IPSec の実行において IKE 経由をした「Auto Policy」を使用することが望ましいことに注意してください。

DSR は VPN ロールオーバ機能をサポートしています。これは、プライマリ WAN に設定されたポリシーがプライマリ WAN におけるリンク障害の場合にセカンダリ WAN にロールオーバすることを意味します。WAN が「Auto-Rollover」モードに設定されている場合にだけ、本機能を使用することができます 。

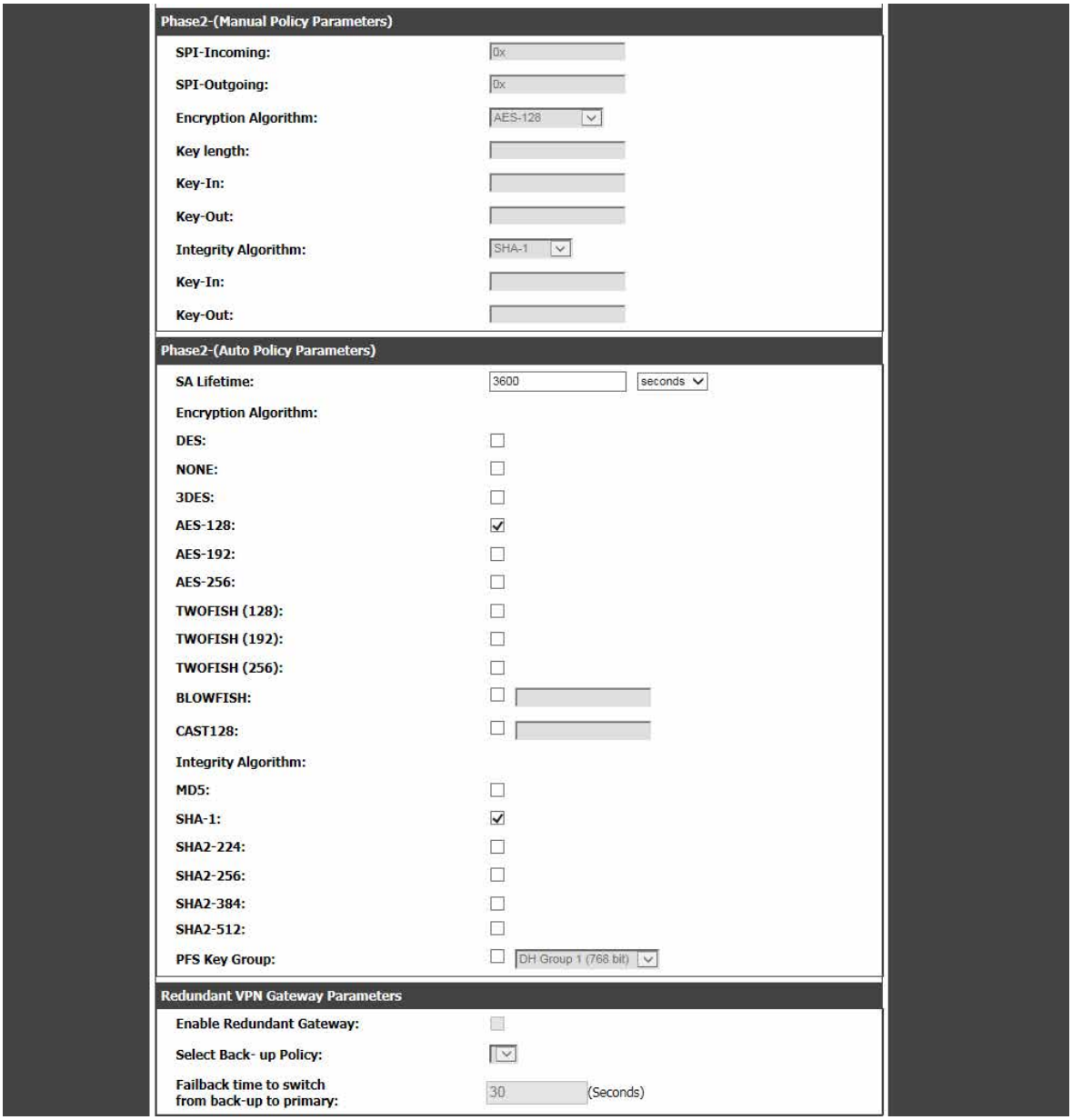


図 8-10　IPSec ポリシー設定（自動 / 手動フェーズ 2）

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

拡張認証（XAUTH）

さらに、拡張認証（XAUTH）を設定することができます。各ユーザにユニークな VPN ポリシーを設定するよりむしろ、保存されたユーザアカウントのリストから、または RADIUS サーバなどの外部認証サーバを使用してユーザの認証を行うために VPN ゲートウェイルータを設定することができます。ユーザデータベースを使用して、ルータに作成したユーザアカウントのユーザを認証するために使用します。

設定済み RADIUS サーバを使用して、ルータは、RADIUS サーバに接続し、VPN クライアントから受信する資格証明を承認します。サーバ（PAP または CHAP）によってサポートされる認証プロトコルを使用して、ルータと RADIUS サーバ間の接続を保証することができます。RADIUS PAP では、ルータは、最初に、ユーザ資格証明が利用可能であるかどうか確認するためにユーザデータベースをチェックします。利用可能でない場合、ルータは RADIUS サーバに接続します。

IPSec トンネル経由のインターネット

本機能では、すべてのトラフィックが VPN トンネルを通過して、リモートゲートウェイからパケットがインターネットに送信されます。リモートゲートウェイ側では、外向きのパケットが SNAT されます。

IP アドレス範囲の設定

SETUP > VPN Settings > IPsec > DHCP Range メニュー

DHCP over IPSec を使用して接続するクライアント用の IP アドレス範囲を定義します。

1. **SETUP > VPN Settings > IPsec > DHCP Range** の順にメニューをクリックし、以下の画面を表示します。

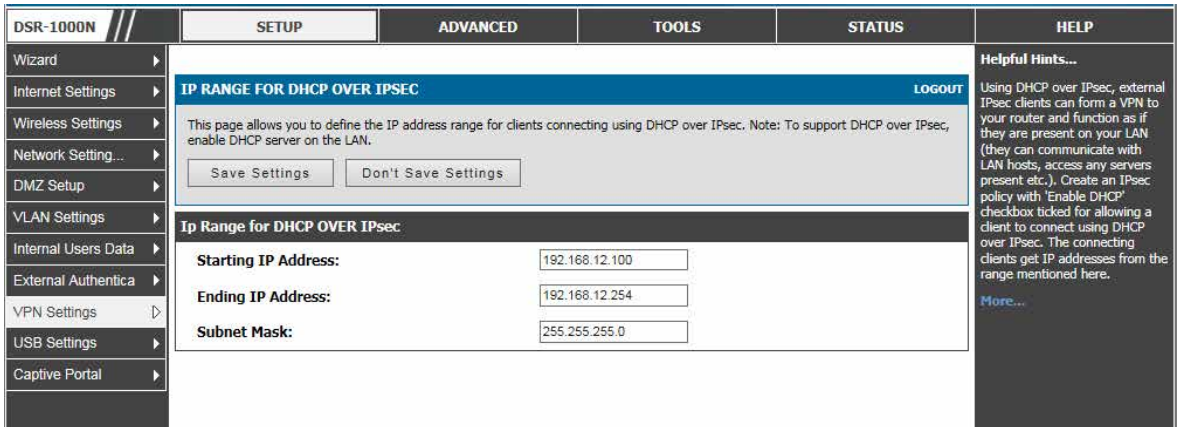


図 8-11　DHCP over IPSec 用の IP 範囲設定

2. 「Starting IP Address」および「Ending IP Address」に IP 範囲の開始および終了アドレスを入力し、「Subnet Mask」にサブネットマスクを指定します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

IPSec モードコンフィグ設定

SETUP > VPN Settings > IPsec > IPsec Mode Config メニュー

このページでは、IPSec モードコンフィグを使用して接続するクライアント用の IP アドレス範囲を定義できます。

1. **SETUP > VPN Settings > IPsec > IPsec Mode Config** の順にメニューをクリックし、以下の画面を表示します。

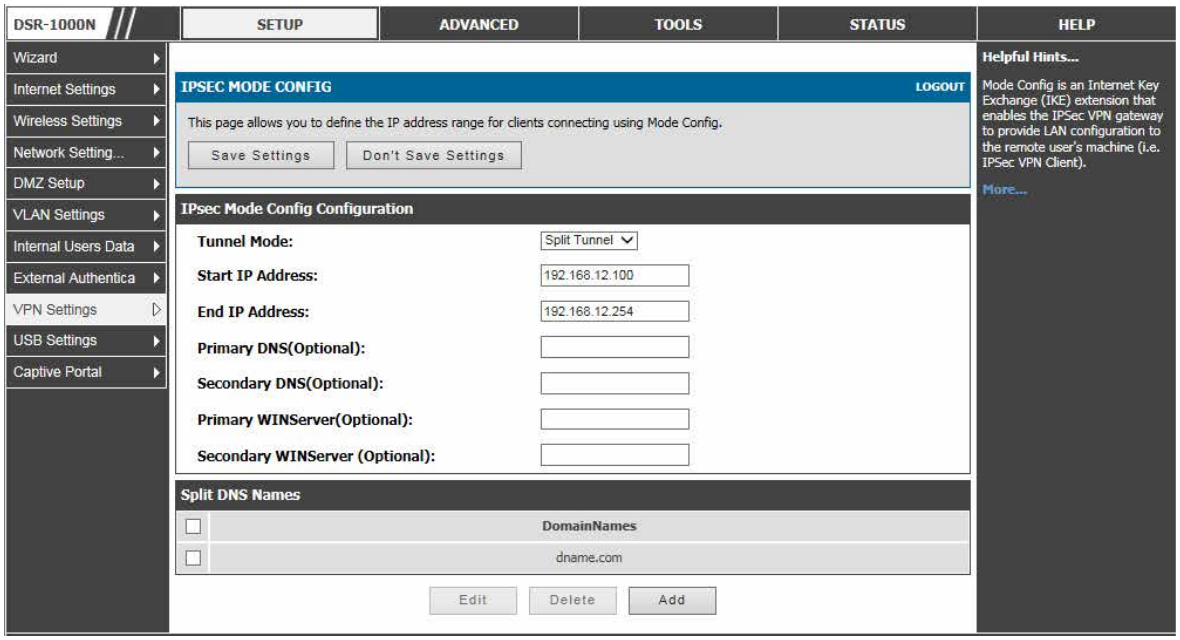


図 8-12　DHCP over IPSec 用の IPSec モードコンフィグ設定

2. 以下の項目を設定します。

項目	説明
IPsec Mode Config Configuration	
モードコンフィグを使用して接続している VPN クライアントには、IPsec Mode Config Configuration で定義したプールより IP アドレスが割り当てられます。	
Tunnel Mode	「Full Tunnel」（フルトンネル）または「Split Tunnel」（スプリットトンネル）。フルトンネルでは、すべてのパケット (インターネットまたはリモートサーバに向かう) が、スプリットトンネルのようなインターネットに向かうトラフィックを通過させないトンネルも通過します。
Start IP Address	このプールに割り当てられるべき最初のアドレス。
End IP Address	このプールに割り当てられるべき最後のアドレス。
Primary DNS	プライマリ DNS サーバは、ドメイン名を解決するためにこのルータに接続するクライアントに使用されます。トンネルモードがスプリットトンネルである場合、DNS サーバを内部のドメイン名サーバとするする必要があります。
Secondary DNS	セカンダリ DNS サーバは、ドメイン名を解決するためにこのルータに接続するクライアントに使用されます。トンネルモードがスプリットトンネルである場合、DNS サーバを内部のドメイン名サーバとするする必要があります。
Primary WINServer	NetBIOS 名を解決するのにクライアントが使用するされたプライマリ Windows NetBIOS ネームサーバ。
Secondary WINServer	NetBIOS 名を解決するのにクライアントが使用するセカンダリ Windows NetBIOS ネームサーバ。
Split DNS Names	
スプリット DNS インフラストラクチャでは、同じドメインに 2 つのゾーンを作成し、1 つは内部のネットワークに使用し、1 つは外部ネットワークに使用します。スプリット DNS は名前解決用に内部ドメイン名サーバに内部のホストを向け、外部ホストは名前解決用に外部のドメイン名サーバに向けます。	

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

スプリット DNS 名の追加

このデバイスに接続するクライアントは、ダイナミック IP 範囲ページで提供する DNS を使用して、このドメイン名を解決します。これはスプリットトンネルでのみ適用されます。

1. 「Split DNS Names」セクションの「Add」ボタンをクリックして以下の画面を表示します。

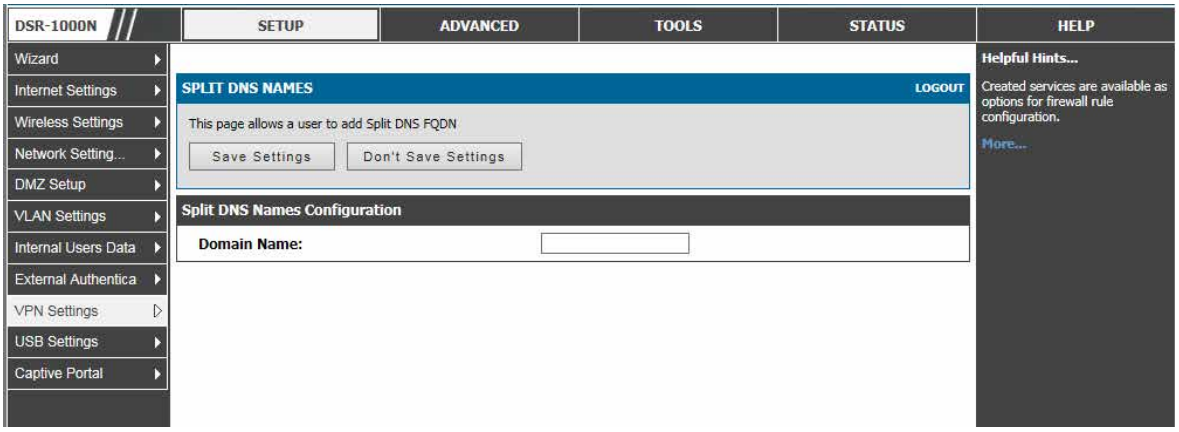


図 8-13　DHCP over IPSec 用の IP 範囲設定

2. 「Domain Name」にドメイン名を入力します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

VPN クライアントの設定

リモート VPN クライアントは、クライアントが使用を希望する VPN トンネルで使用されるのと同じ VPN ポリシーパラメータ（暗号化、認証、ライフタイム、および PFS はキーグループ）で設定する必要があります。これらの認証パラメータを確立する場合、VPN クライアントユーザデータベースにはトンネルへのユーザアクセス権を与えるアカウントをおく必要があります。

注意 VPN クライアントのソフトウェアが、ルータとリモートエンドポイント間で VPN トンネルを確立するために必要とされます。マイクロソフト IPSec VPN ソフトウェアをはじめとする（OpenVPN または Openswan などの）オープンソースソフトウェアは、IPSec VPN トンネルを確立するために必要な IKE ポリシーパラメータを使用して設定されます。ルータのオンラインヘルプと共にセットアップの細かい手順についてはクライアントソフトの説明書を参照してください。

ユーザデータベースには指定した VPN トンネルを使用することを認可される VPN ユーザアカウントのリストがあります。その代わりに、設定された RADIUS データベースを使用して、VPN トンネルユーザを認証することができます。ユーザデータベースへの移動、および / または、RADIUS 認証を設定する方法を決定するためにはオンラインヘルプを参照してください。

PPTP / L2TP トンネル

このルータは PPTP または L2TP ISP サーバから開始する VPN トンネルをサポートしています。ルータは、ISP のサーバが LAN VPN クライアントと VPN サーバ間の TCP 制御接続を作成できる仲介デバイスとして機能します。

PPTP トンネルのサポート

PPTP VPN クライアント設定

SETUP > VPN Settings > PPTP > PPTP Client メニュー
本ルータに PPTP VPN クライアントを設定します。

このクライアントを使用して、PPTP サーバに対してローカルであるリモートネットワークにアクセスできます。

1. **SETUP > VPN Settings > PPTP > PPTP Client** の順にメニューをクリックし、以下の画面を表示します。

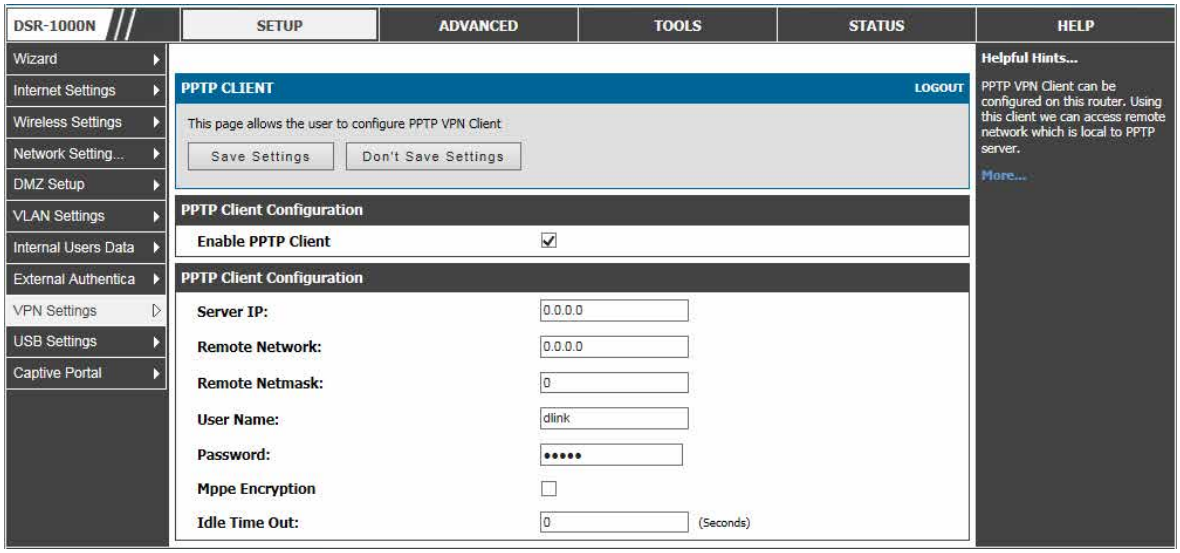


図 8-14　PPTP トンネル設定 - PPTP クライアント

クライアントが有効になると、ユーザは、**STATUS > Active VPNs** ページにアクセスし、「Connect」ボタンをクリックして PPTP VPN トンネルを確立します。トンネルを切断するには、「Disconnect」ボタンをクリックします。

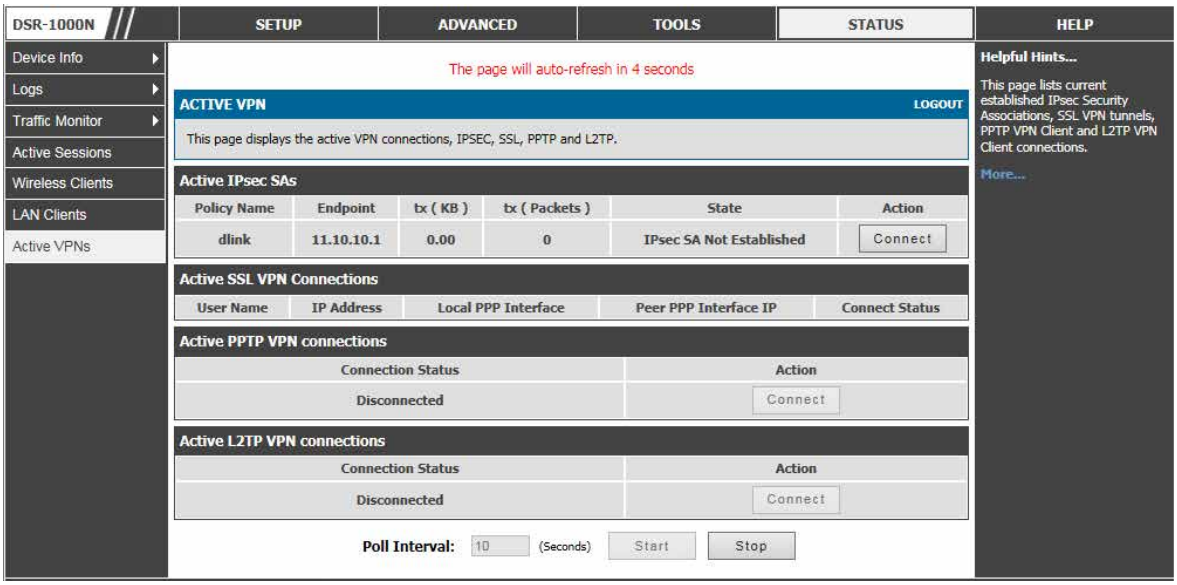


図 8-15　PPTP VPN 接続状態

PPTP VPN サーバ設定

SETUP > VPN Settings > PPTP > PPTP Server メニュー

ここでは、PPTP サーバの有効化 / 無効化、およびルータに接続するクライアントの IP アドレスの範囲を定義することができます。

PPTP によりインターネットを通して外部ユーザがこのルータに接続することができます。接続するクライアントは、LAN ホストと通信し、どんなサーバにもアクセスするなどご使用の LAN にいるかのように動作することができます

有効にされると、PPTP サーバは LAN および WAN PPTP クライアントユーザがアクセスするルータで利用可能になります。PPTP サーバが有効になると、許可されたクライアントの設定済み IP アドレス範囲内にある PPTP クライアントは、ルータの PPTP サーバに到達することができます。PPTP サーバ（トンネルのエンドポイント）によって一度認証されると、PPTP クライアントはルータが管理するネットワークにアクセスすることができます。

PPTP クライアントに割り当てる IP アドレス範囲は LAN サブネットと同じにできます。また、PPTP サーバは、ローカルな PPTP ユーザ認証をデフォルトとしますが、外部認証サーバを使用するように設定できます。

1. **SETUP > VPN Settings > PPTP > PPTP Server** の順にメニューをクリックし、以下の画面を表示します。

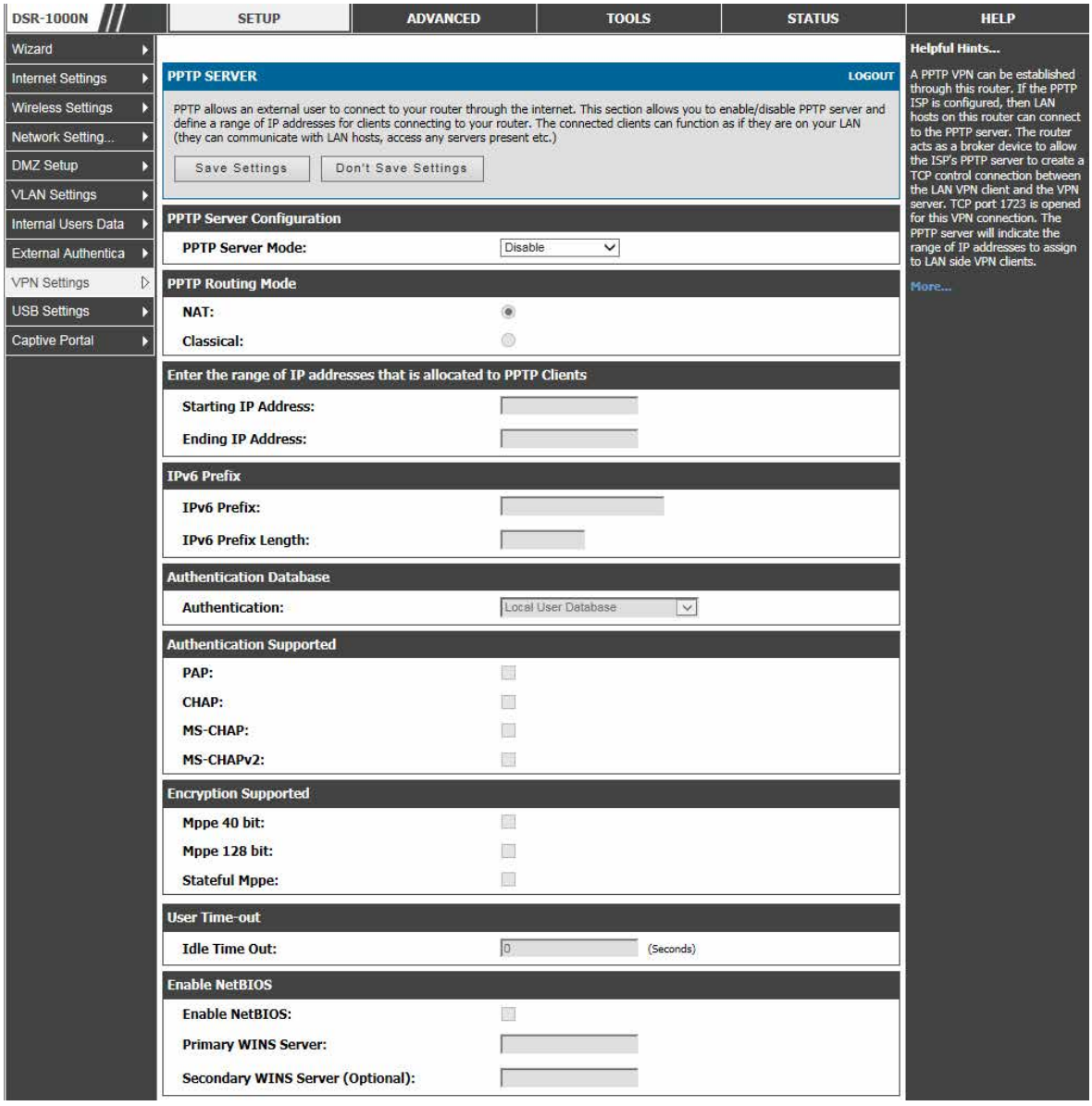


図 8-16　PPTP トンネル設定 - PPTP サーバ

2. 以下の項目を設定します。

項目	説明
PPTP Sever Configuration	
PPTP Server Mode	PPTP サーバを有効にするモードを選択します。: Enable IPv4（IPv4 のみ）、Enable IPv4/IPv6（IPv4/IPv6）、Disable（無効）
PPTP Routing Mode	
PPTP ルーティングモード（NAT/Classical）を有効または無効にします。	
Enter the range of IP addresses that is allocated to PPTP Clients	
Starting IP Address	接続するユーザに割り当てるべき IP アドレス範囲の開始の IP アドレスを入力します。この IP アドレスはサーバの IP アドレスとして使用され、範囲内の残りの IP アドレスはクライアントに割り当てられます。
Ending IP Address	接続するユーザに割り当てるべき IP アドレス範囲の終了の IP アドレスを入力します。
IPv6 Prefix	
IPv6 Prefix	PPTP サーバが IPv4/IPv6 モードである場合、グローバル IPv6 アドレスを PPTP クライアントに割り当てるために使用します。
IPv6 Prefix Length	IPv6 プレフィックス長（整数）。サーバが IPv4/IPv6 モードである場合にのみ入力します。
Authentication Database	
Authentication	認証データベース（ローカルユーザデータベースまたは外部 RADIUS サーバ）を選択します。「External RADIUS Server」（外部 RADIUS サーバ）を選択すると、有効状態にある RADIUS プロファイルにあるサーバの詳細設定を使用します。
Authentication Supported	
PAP	PAP 認証方式のサポートを有効にします。
CHAP	CHAP 認証方式のサポートを有効にします。
MS-CHAP	MS-CHAP 認証方式のサポートを有効にします。
MS-CHAPv2	MS-CHAPv2 認証方式のサポートを有効にします。
Encryption Supported	
Mppe 40 bit	Mppe 40 ビット暗号化を有効にします。（MS-CHAP および MS-CHAPv2 認証方式にだけ有効です。）
Mppe 128 bit	Mppe 128 ビット暗号化を有効にします。（MS-CHAP および MS-CHAPv2 認証方式にだけ有効です。）
Stateful Mppe	ステートフル Mppe 暗号化を有効にします。（MS-CHAP および MS-CHAPv2 認証方式にだけ有効です。）Mppe 暗号化のこのモードは、安全性は低いですが、互換のために使用することができます。
User Time-Out	
Idle Timeout	指定したタイムアウトを経過してもユーザからのトラフィックがない場合、接続は切断されます。
Enable Netbios	
Enable Netbios	チェックして、Netbios サポートを有効にします。
Primary WINS Server	プライマリ WINS サーバの IP アドレス
Secondary WINS Server (Optional)	オプション WINS サーバの IP アドレス

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

L2TP トンネルのサポート

L2TP VPN サーバ設定

SETUP > VPN Settings > L2TP > L2TP Server メニュー
ここでは L2TP サーバの有効化 / 無効化、およびルータに接続するクライアントの IP アドレスの範囲を定義することができます。

L2TP は、VPN を形成してインターネット経由で外部ユーザがこのルータに接続することができます。接続するクライアントは、LAN ホストと通信し、どんなサーバにもアクセスするなどご使用の LAN にいるかのように動作することができます

有効にされると、L2TP サーバは LAN および WAN L2TP クライアントユーザがアクセスするルータで利用可能になります。L2TP サーバが有効になると、許可されたクライアントの設定済み IP アドレス範囲内にある L2TP クライアントは、ルータの L2TP サーバに到達することができます。L2TP サーバ（トンネルのエンドポイント）によって一度認証されると、L2TP クライアントはルータが管理するネットワークにアクセスすることができます。

1. **SETUP > VPN Settings > L2TP > L2TP Server** の順にメニューをクリックし、以下の画面を表示します。

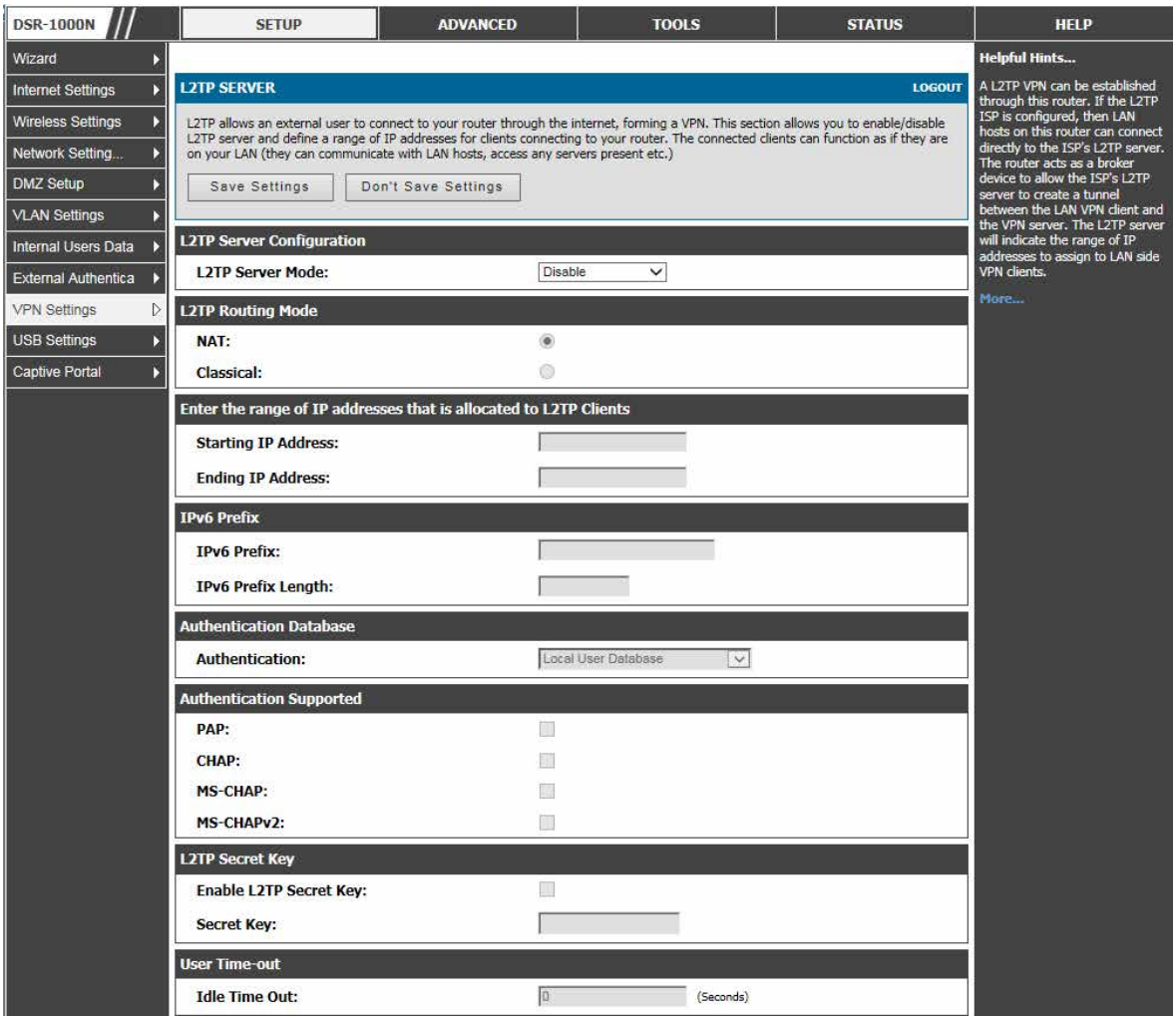


図 8-17　L2TP トンネル設定 - L2TP サーバ

2. 以下の項目を設定します。

項目	説明
L2TP Sever Configuration	
L2TP Server Mode	L2TP サーバを有効にするモードを選択します。: Enable IPv4（IPv4 のみ）、Enable IPv4/IPv6（IPv4/IPv6）、Disable（無効）
L2TP Routing Mode	
L2TP ルーティングモード（NAT/Classical）を有効または無効にします。	
Enter the range of IP addresses that is allocated to L2TP Clients	
Starting IP Address	接続するユーザに割り当てるべき IP アドレス範囲の開始の IP アドレスを入力します。この IP アドレスはサーバの IP アドレスとして使用され、範囲内の残りの IP アドレスはクライアントに割り当てられます。
Ending IP Address	接続するユーザに割り当てるべき IP アドレス範囲の終了の IP アドレスを入力します。
IPv6 Prefix	
IPv6 Prefix	L2TP サーバが IPv4/IPv6 モードである場合、グローバル IPv6 アドレスを L2TP クライアントに割り当てるために使用します。
IPv6 Prefix Length	IPv6 プレフィックス長（整数）。サーバが IPv4/IPv6 モードである場合にのみ入力します。
Authentication Database	
Authentication	認証データベース（ローカルユーザデータベースまたは外部 RADIUS サーバ）を選択します。「External RADIUS Server」（外部 RADIUS サーバ）を選択すると、有効状態にある RADIUS プロファイルにあるサーバの詳細設定を使用します。
Authentication Supported	
PAP	PAP 認証方式のサポートを有効にします。
CHAP	CHAP 認証方式のサポートを有効にします。
MS-CHAP	MS-CHAP 認証方式のサポートを有効にします。
MS-CHAPv2	MS-CHAPv2 認証方式のサポートを有効にします。
L2TP Secret Key	
Enable L2TP Secret Key	L2TP Secret キーを有効にします。
Secret Key	L2TP Secret キーを入力します。
User Time-Out	
Idle Timeout	指定したタイムアウトを経過してもユーザからのトラフィックがない場合、接続は切断されます。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

L2TP VPN クライアント設定

SETUP > VPN Settings > L2TP > L2TP Client メニュー

L2TP VPN クライアントを設定します。このクライアントを使用して、L2TP サーバに対してローカルであるリモートネットワークにアクセスできます。

1. **SETUP > VPN Settings > L2TP > L2TP Client** の順にメニューをクリックし、以下の画面を表示します。

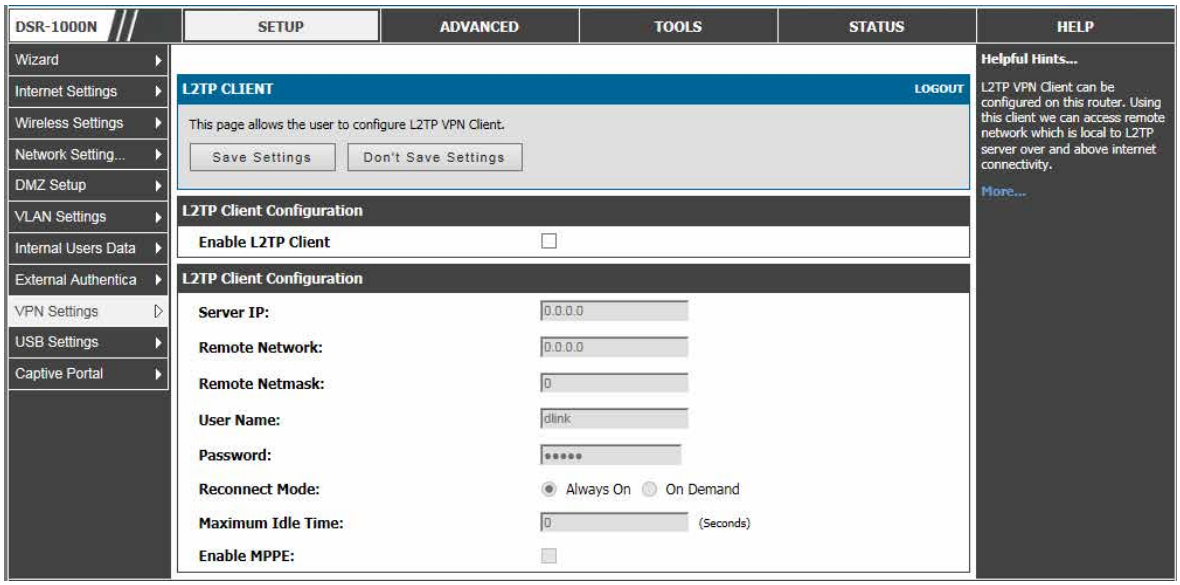


図 8-18　L2TP トンネル設定 - L2TP クライアント

クライアントが有効になると、ユーザは、**STATUS > Active VPNs** ページにアクセスし、「Connect」ボタンをクリックして L2TP VPN トンネルを確立できます。トンネルを切断するには、「Disconnect」ボタンをクリックします 。

このルータを通して L2TP VPN を確立することができます。有効にされると、L2TP サーバは LAN および WAN L2TP クライアントユーザがアクセスするルータで利用可能になります。一度、L2TP サーバが有効になると、リモートの L2TP ネットワークサーバ範囲（IP アドレスおよびネットマスク）で設定される L2TP クライアントは、エンドポイントルータの L2TP サーバに到達することができます。L2TP サーバ（トンネルのエンドポイント）によって一度認証されると、L2TP クライアントはルータが管理するローカルネットワークにアクセスすることができます。

GRE トンネルサポート

SETUP > VPN Settings > GRE Tunnels メニュー

GRE トンネルは、ルータの LAN においてブロードキャストトラフィックをインターネットに渡すこと、およびリモート LAN が受信することを許可します。GRE エンドポイントのローカルサブネット内のすべての LAN ホストが、ある LAN ホストからのブロードキャストトラフィックを受信することが D-Link Discovery Protocol（DDP）アプリケーションで最も有益です。

注意 以下に示す通り、製品ごとにサポートする GRE トンネル数の制限にご注意ください。

- DSR-500 : 15
- DSR-1000/1000N : 20

ルータの GRE トンネルを確立するのに以下の 2 つの手順があります。:

1. GUI から GRE トンネルを作成します。

2. GRE トンネルを使用して、リモートローカルネットワーク用のスタティックルートを設定します。

GRE トンネルの設定

1. **SETUP > VPN Settings > GRE Tunnels** の順にメニューをクリックし、以下の画面を表示します。

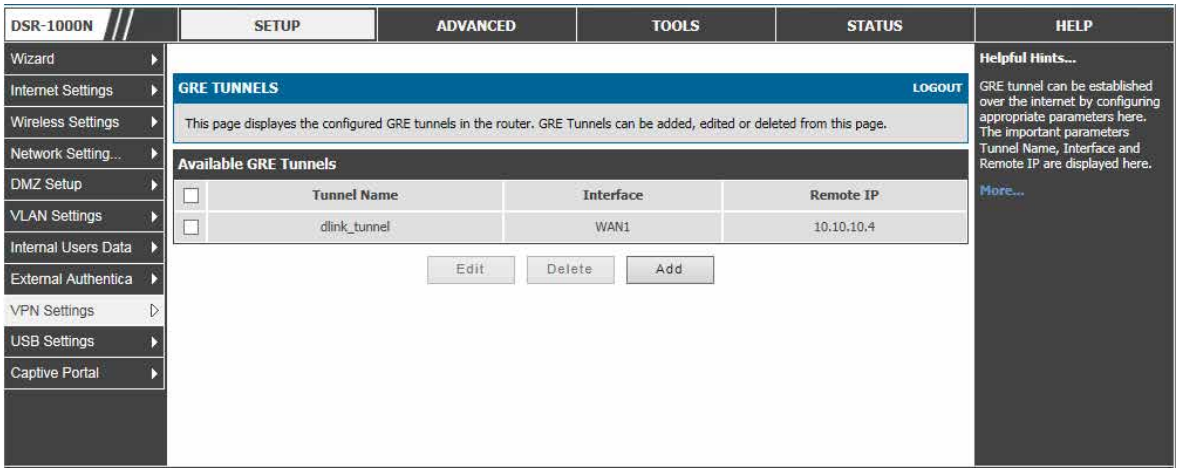


図 8-19　GRE トンネル設定

登録済みの GRE トンネルのリストが表示されます。

GRE トンネルの追加

1. 「**Add**」ボタンをクリックし、以下の画面を表示します。

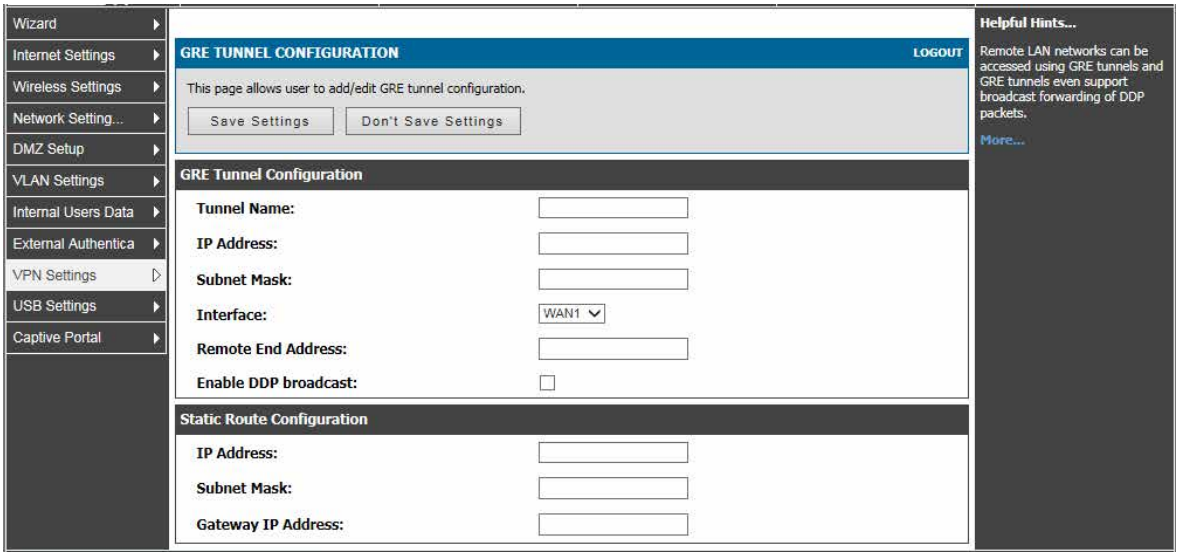


図 8-20　GRE トンネル設定

2. 以下の項目を設定します。

項目	説明
GRE Tunnels Configuration	
Tunnel Name	トンネル名。
IP Address	GRE トンネルインタフェースに割り当てる IPv4 アドレス。
Subnet Mask	GRE トンネルインタフェースに割り当てるサブネットマスク。
Interface	GRE トンネル設定に使用する IP インタフェース。
Remote End Address	GRE トンネルのリモートエンドの IP アドレス。
Enable DDP Broadcast	GRE トンネルのエンドから他のエンドへの DDP パケットの転送を有効にします。
Static Route Configuration	
IP Address	GRE トンネルのもう一方のエンドにある宛先ホストまたはネットワーク。
Subnet Mask	宛先 IP アドレスのサブネットマスク。
Gateway IP Address	宛先ホストまたはネットワークに到達できるゲートウェイの IP アドレス。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

GRE トンネルを作成する場合、IP アドレスは、その GRE トンネルのエンドポイントを特定する固有のアドレスとする必要があります。それはゲートウェイ IP アドレスとしてもう片方のルータのスタティックルートで参照されます。GRE トンネルの設定ページにおけるリモートエンドアドレスはもう片方のエンドポイントルータの WAN IP アドレスです。

1 度トンネルが確立されると、定義した GRE トンネル名に設定したインタフェースを使用することでルータのスタティックルートが作られます。スタティックルートの宛先 IP アドレスはリモート LAN のサブネットで、ルートのゲートウェイ IP アドレスは、終端にあるルータ（リモート LAN サブネットを管理する同じルータ）の GRE トンネル IP になります。一度、これらの 2 つの手順を完了すれば、すべての DDP ブロードキャストトラフィックが GRE トンネルを通じてリモート LAN サブネット間に流れます。

OpenVPN サポート

SETUP > VPN Settings > OpenVPN > OpenVPN Configuration メニュー

OpenVPN では、ピアが事前共有秘密鍵、証明書、またはユーザ名 / パスワードを使用することで相互に認証することができます。マルチクライアント - サーバ設定で使用されると、サーバはすべてのクライアントのために署名と CA（認証局）を使用して認証証明書をリリースすることができます。本ルータを通して OpenVPN を確立することができます。これをチェックまたはチェックを外し、「Save Settings」ボタンをクリックして OpenVPN サーバの起動 / 停止を行います。

1. **SETUP > VPN Settings > OpenVPN > OpenVPN Configuration** の順にメニューをクリックし、以下の画面を表示します。

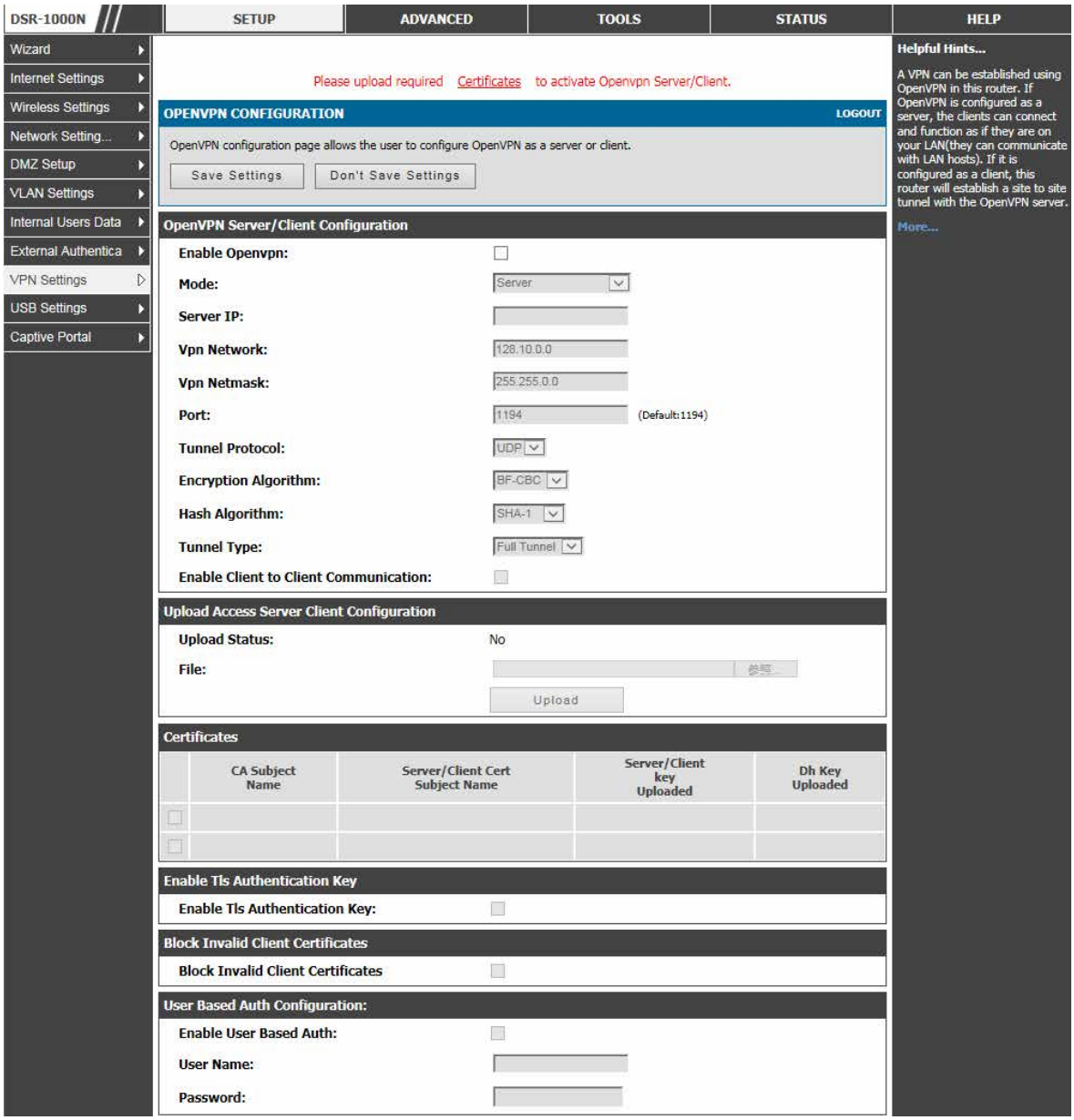


図 8-21　OpenVPN 設定

2. 以下の項目を設定または表示します。

項目	説明
OpenVPN Server/Client Configuration	
Mode	OpenVPN デーモンモード（Server、Client、Access Server Client）を指定します。「Access Server Client」モードでは、ユーザは、接続するために OpenVPN アクセスサーバから自動ログインプロファイルをダウンロードして、同じものをアップロードする必要があります。
Server IP	クライアントが（クライアントモードで適切に）接続する OpenVPN サーバ IP アドレス
VPN Network	仮想ネットワークアダプタのアドレス
VPN Netmask	仮想ネットワークのネットマスク
Port	OpenVPN サーバ（またはアクセスサーバ）を実行するポート番号
Tunnel Protocol	リモートホストと通信を行うために使用するプロトコル。例 :TCP、UDP。初期値は UDP です。
Encryption Algorithm	パケットが暗号化される方式。例 : BF-CBC、AES-128,AES-192 および AES-256。初期値は BF-CBC です。

項目	説明
Hash algorithm	パケット認証に使用されるメッセージダイジェストアルゴリズム。例 : SHA1、SHA256、および SHA512。初期値は SHA1 です。
Tunnel Type	• Full Tunnel - トンネルを通じてすべてのトラフィックをリダイレクトします。（初期値） • Split Tunnel - トンネルを通じて指定リソース（OpenVPN クライアントから追加されたルート）だけにトラフィックをリダイレクトします。
Enable Client to Client Communication	本機能を有効 にすると、「split tunnel」の場合に OpenVPN クライアント同士の通信を可能にします。初期値では無効です。
Upload Access Server Client Configuration	
本ルータを OpenVPN アクセスサーバに接続するには、自動ログインプロファイルのダウンロードを行い、ここでアップロードする必要があります。	
Certificates	
OpenVPN サーバが使用する証明書のセットを選択します。	
1 列目	サーバが使用する証明書とキーのセット。
2 列目	新たにアップロードされた証明書とキーのセット。
Enable Tls Authentication Key	
Enable Tls Authentication Key	本機能を有効にすると、認証の付加レイヤとして TIs 認証を追加します。TIs キーをアップロードする場合にだけチェックすることができます。初期値では無効です。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

OpenVPN リモートネットワーク設定

SETUP > VPN Settings > OpenVPN > OpenVPN Remote Network (Site-to- Site) メニュー

このネットワークに他の OpenVPN クライアントが到達できるリモートネットワークとネットマスクを追加 / 編集します。

1. **SETUP > VPN Settings > OpenVPN > OpenVPN Remote Network (Site-to- Site)** の順にメニューをクリックし、以下の画面を表示します。

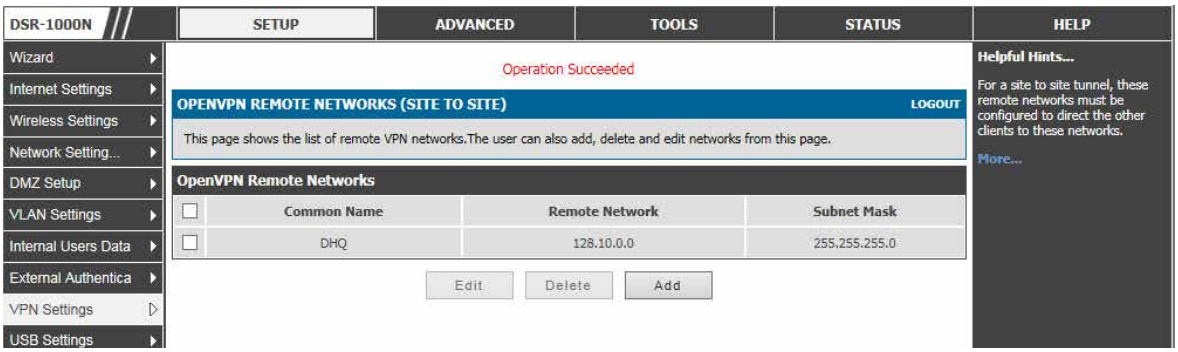


図 8-22　OpenVPN リモートネットワークリスト

OpenVPN リモートネットワークの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

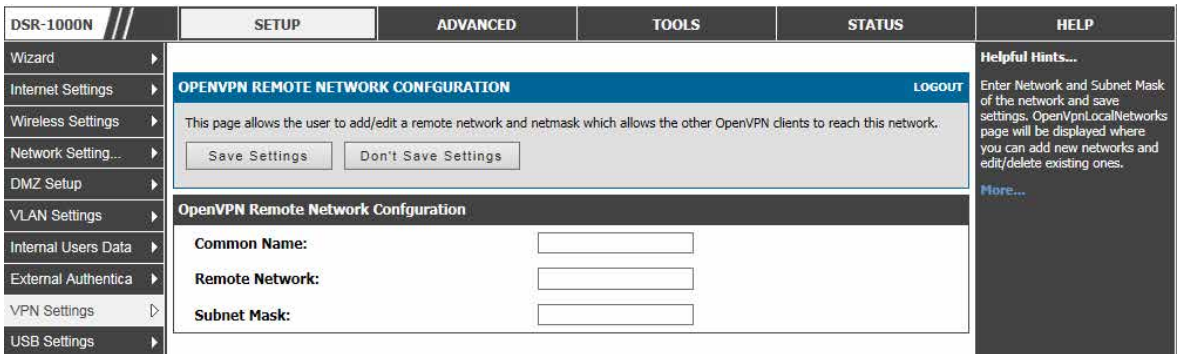


図 8-23　OpenVPN リモートネットワーク設定

2. 以下の項目を設定または表示します。

項目	説明
Common Name	OpenVPN クライアント証明書の一般名。
Remote Network	リモートリソースのネットワークアドレス。
Subnet Mask	リモートリソースのネットマスク。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

OpenVPN 認証

SETUP > VPN Settings > OpenVPN > OpenVPN Authentication メニュー

必要な証明書とキーをアップロードします。

1. **SETUP > VPN Settings > OpenVPN > OpenVPN Authentication** の順にメニューをクリックし、以下の画面を表示します。

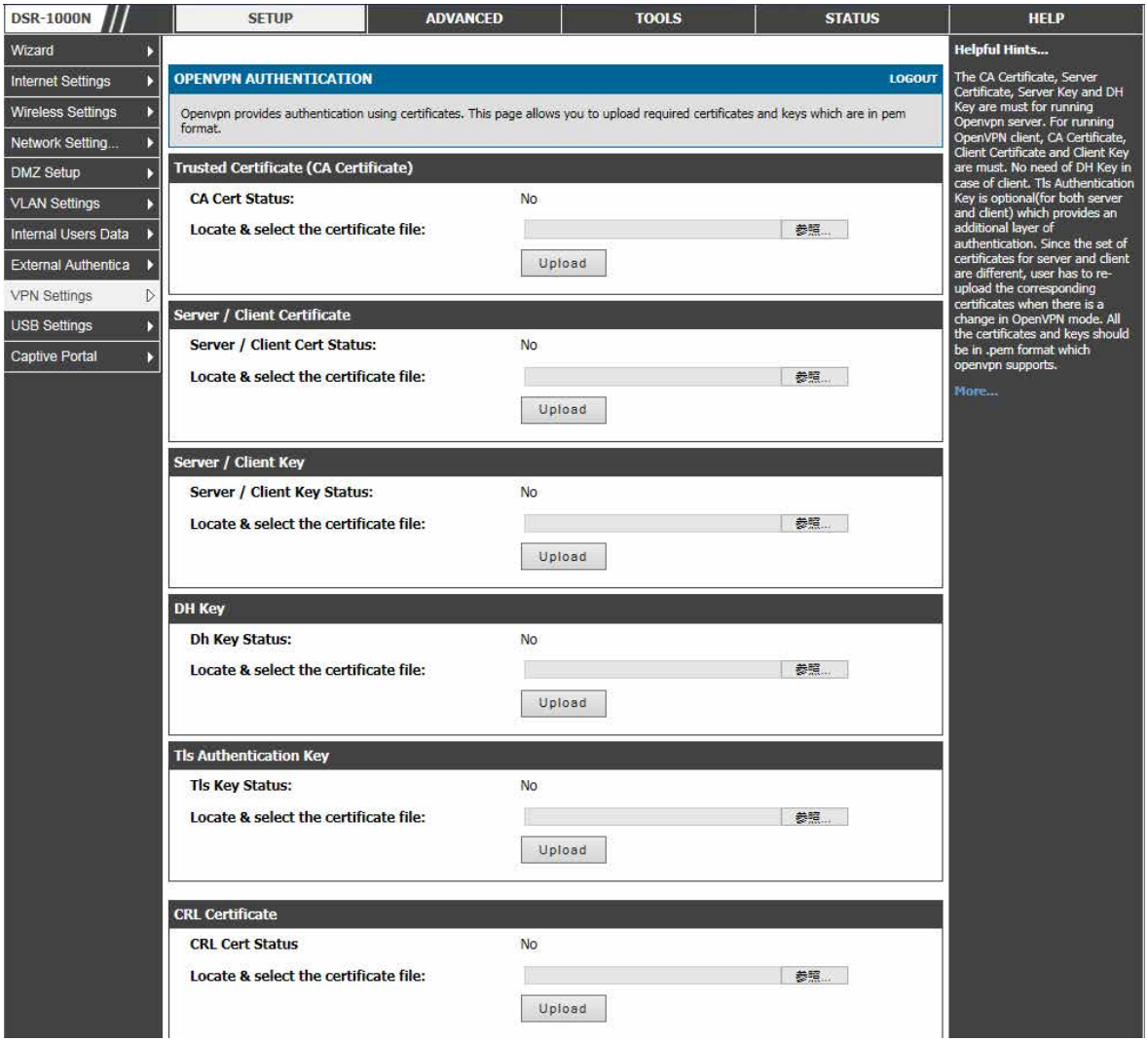


図 8-24　OpenVPN 認証

2. 以下の項目を設定または表示します。

項目	説明
Trust Certificate（CA Certificate）	PEM 形式の CA 証明書を検索して、アップロードします。
Server/Client Certificate	PEM 形式のサーバ / クライアント証明書を検索して、アップロードします。
Server/Client Key	PEM 形式のサーバ / クライアントキーを検索して、アップロードします。
DH Key	PEM 形式の Diffie Hellman キーを検索して、アップロードします。
Tls Authentication Key	PEM 形式の Tls 認証キーを検索して、アップロードします。
CRL Certificate	CRL リストを検索して、アップロードします。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

アクティブユーザの表示

SETUP > VPN Settings > PPTP > PPTP Active Users メニュー
SETUP > VPN Settings > L2TP > L2TP Active Users メニュー

PPTP サーバまたは L2TP サーバに現在接続するすべてのユーザを表示します。

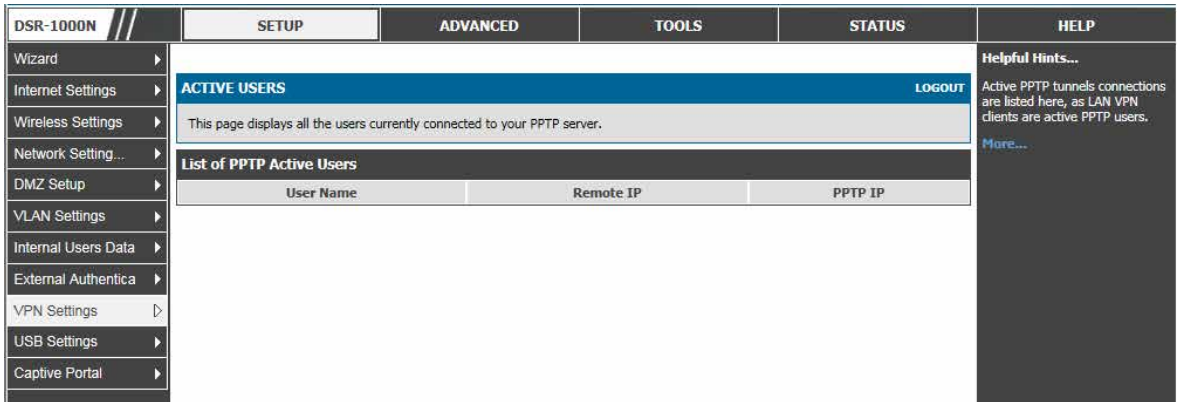


図 8-25　PPTP ユーザリスト

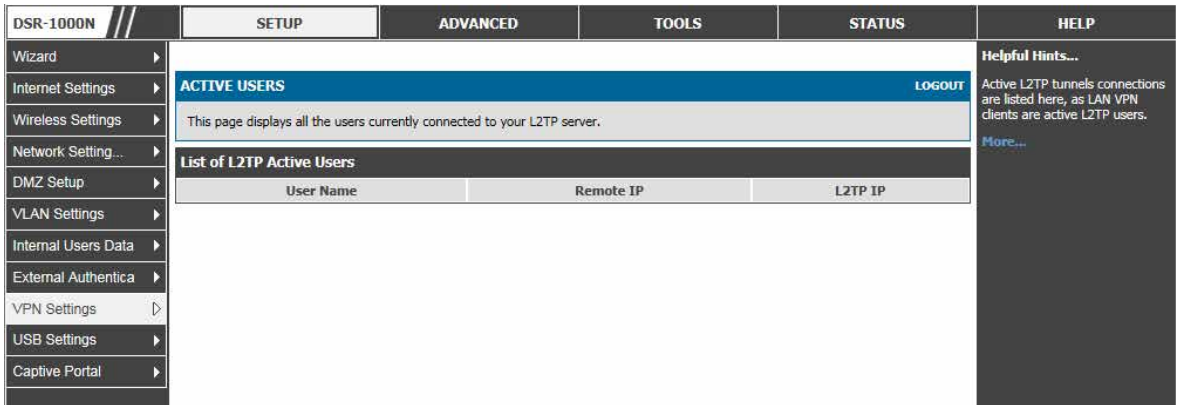


図 8-26　L2TP ユーザリスト

IPv6 トンネルステータス

ADVANCED > IPv6 > IPv6 Tunnels Status メニュー

トンネル名および IPv6 アドレスごとにアクティブな IPv6 トンネルを表示します。

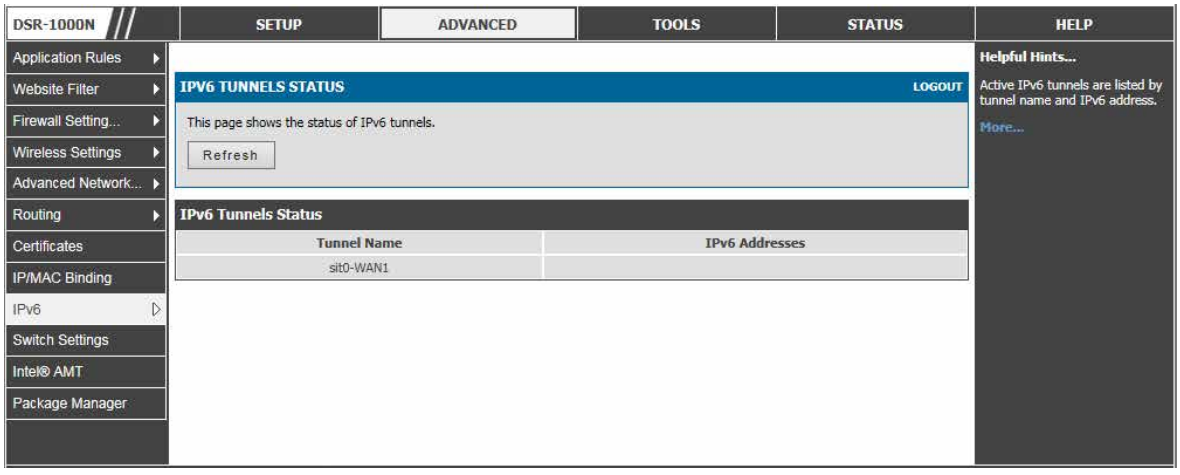


図 8-27　IPv6 トンネルステータス

第 9 章　SSL VPN 設定

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

設定項目	説明	参照ページ
グループとユーザ設定	ルータにログインする場合に必要なユーザ、グループを設定します。	154 ページ
SSL VPN ポリシー設定	SSL VPN ポリシーを設定します。	161 ページ
アプリケーションポートフォワーディング	アプリケーションに対してリモートユーザから SSL VPN ゲートウェイに送信されたデータを別ルートで送信します。	165 ページ
SSL VPN クライアント設定	SSL VPN トンネルクライアントを設定します。	167 ページ
ユーザポータル	SSL VPN ユーザポータルを設定します。	169 ページ

ルータは標準の IPSec VPN に代わるものとして固有の SSL VPN 機能を提供します。SSL VPN は、主としてリモートホストでプレインストールされた VPN クライアントの必要条件を削除するという点で、IPSec VPN とは異なっています。代わりに、ユーザは、標準の Web ブラウザを使用して SSL User Portal 経由で安全にログインし、コーポレート LAN に構成されたネットワークリソースにアクセスすることができます。ルータは、複数の同時セッションをサポートし、リモートユーザはカスタマイズ可能なユーザのポータルインタフェースを経由した暗号化済みリンク上の LAN にアクセス可能で、各 SSL VPN ユーザは固有の権限とネットワークリソースへのアクセスレベルを割り当てられます。

このルータを通じて SSL サービスのための様々なオプションをリモートユーザに提供できます。:

- VPN トンネル :
  リモートユーザの SSL が有効であるブラウザは、安全な VPN トンネルを確立するために、リモートホストの VPN クライアントに代わって使用されます。（Active-X または Java に基づいた）SSL VPN クライアントは、クライアントが事前に設定したアクセス / ポリシーの権限でコーポレート LAN に参加することを許可するためにリモートホストにインストールされます。ここで、仮想ネットワークインタフェースはユーザのホスト上に作成され、ルータからの IP アドレスと DNS サーバアドレスが割り当てられます。一度確立されると、ホストマシンは割り当てられたネットワークリソースにアクセスできます。

- ポートフォワーディング :
  Web ベース（ActiveX または Java）のクライアントが再度クライアントマシンにインストールされます。ポートフォワーディングサービスは、リモートユーザとルータ間の TCP 接続だけをサポートしていることに注意してください。ルータ管理者は、VPN トンネルのような完全な LAN へのアクセスの代わりにリモートポートフォワーディングが有効なサービスまたはアプリケーションをユーザに対して定義することができます。

注意 ActiveX クライアントは、インターネットエクスプローラブラウザを使用してリモートユーザがポータルにアクセスする場合に使用されます。Java クライアントは Mozilla Firefox、Netscape Navigator、Google Chrome、および Apple Safari のような他のブラウザで使用されます。

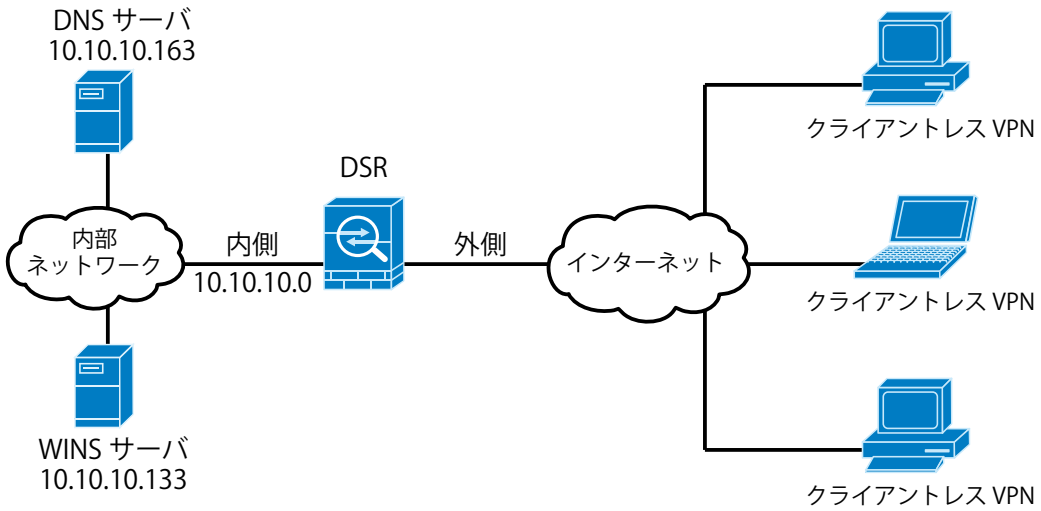


図 9-1　DSR へのクライアントレス SSL VPN 接続の例

グループとユーザ設定

グループ設定

SETUP > Internal Users Data > Groups メニュー

グループの作成、編集、および削除を行います。グループは一組のユーザタイプに割り当てられます。利用可能なグループのリストは「List of Groups」ページにグループ名とグループの説明文と共に表示されます。

1. **SETUP > Internal Users Data > Groups** の順にメニューをクリックし、以下の画面を表示します。

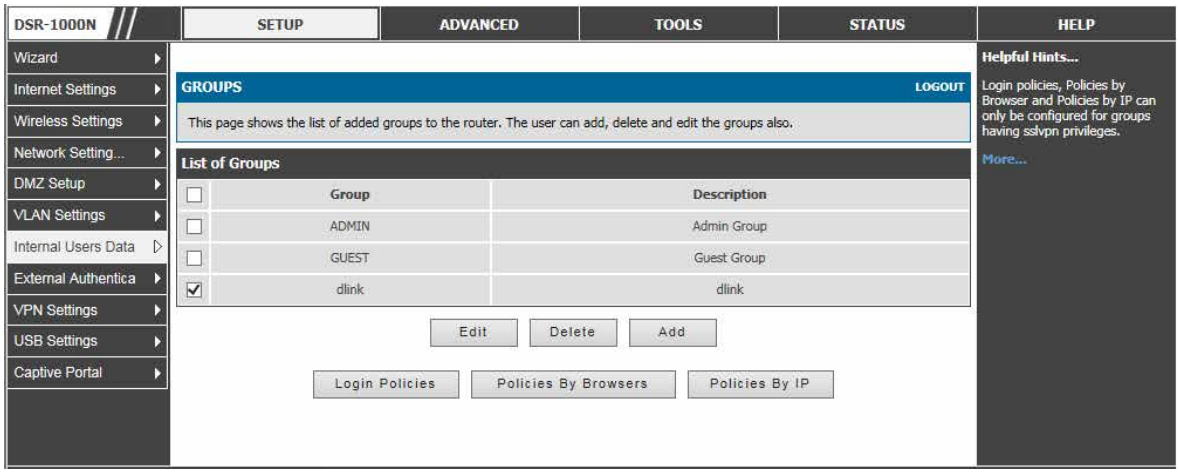


図 9-2　グループリスト

以下のアクションを行うことができます。

項目	説明
Add	新しいグループを作成します。
Edit	既存のグループを編集します。
Delete	既存のグループをクリアします。
Login Policies	ログインポリシーをグループに設定します。
Policies By Browsers	グループにブラウザポリシーを設定します。
Policies By IP	IP にグループポリシーを設定します。

グループの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

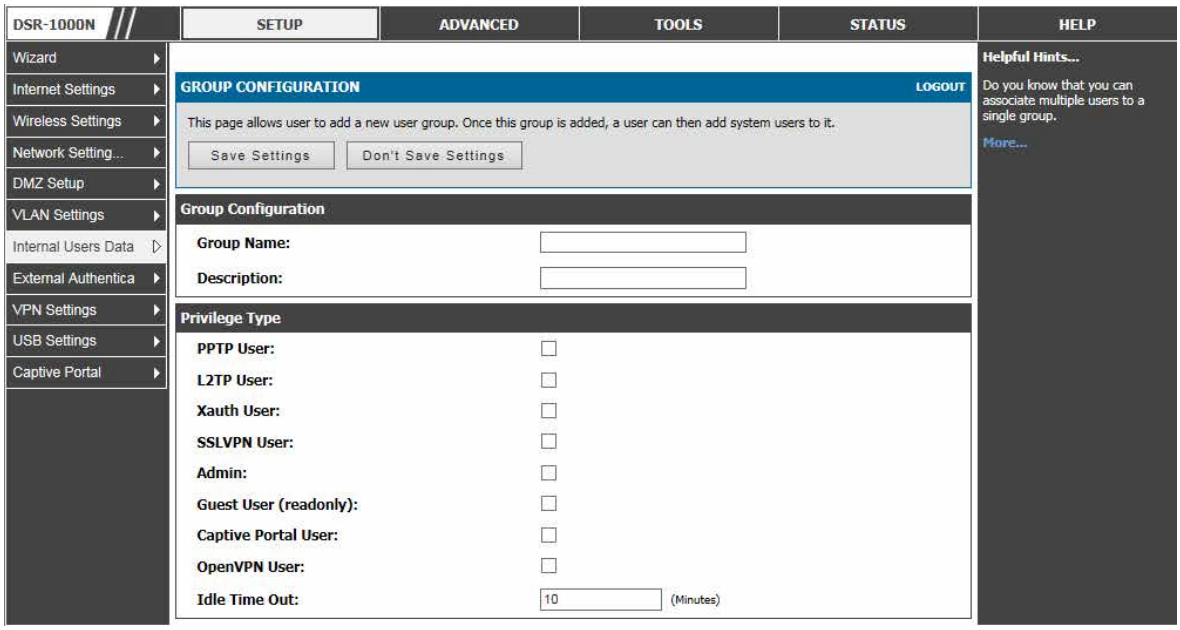


図 9-3　グループの設定画面

「Group Configuration」ページでは様々なユーザタイプのグループを作成できます。

2. グループの登録を行います。以下のユーザタイプがあります。

項目	説明
PPTP User	PPTP サーバを使用したトンネルを確立できる PPTP VPN トンネルの LAN ユーザです。
L2TP User	L2TP サーバを使用したトンネルを確立できる L2TP VPN トンネル LAN のユーザです。
Xauth User	このユーザの認証は外部的に設定された RADIUS または他のエンタープライズサーバによって実行されます。それはローカルユーザデータベースの一部ではありません。
SSLVPN User	このユーザはユーザがメンバであるグループポリシーと認証ドメインによって決定される SSL VPN サービスへのアクセス権を持っています。そのドメインが決定した SSL VPN ポータルは、このユーザタイプでログインする場合に表示されます。
Admin	ルータのスーパーユーザであり、ルータを管理して、SSL VPN を使用してネットワークリソースにアクセスし、Option 上の L2TP/PPTP サーバにログインすることができます。GUI には管理者ユーザの初期値が常にあります。
Guest User (readonly)	ゲストユーザは、コンフィグレーション設定を監視および見直しするために参照のみのアクセスを取得します。ゲストには、SSL VPN アクセスがありません。
Captive Portal User	これらのキャプティブポータルユーザは、ルータの承認によりインターネットアクセスを取得します。アクセスはキャプティブポータルポリシーに基づいて決定されます。
OpenVPN User	OpenVPN を使用するユーザです。
Idle Timeout	本グループのユーザ用のログインタイムアウト時間です。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

注意 最初にドメインを作成する必要があり、その後、新しいグループを作成してドメインに割り当てることができます。最後の手順は、特定の SSL VPN ユーザを設定済みのグループに追加することです。

4. グループの設定後、すべての定義済みグループのリストを表示します。

SSL VPN 設定

1. SSL VPN ユーザを選択した場合、SSL VPN 設定で取得される以下のパラメータと共に SSL VPN 設定は表示されます。

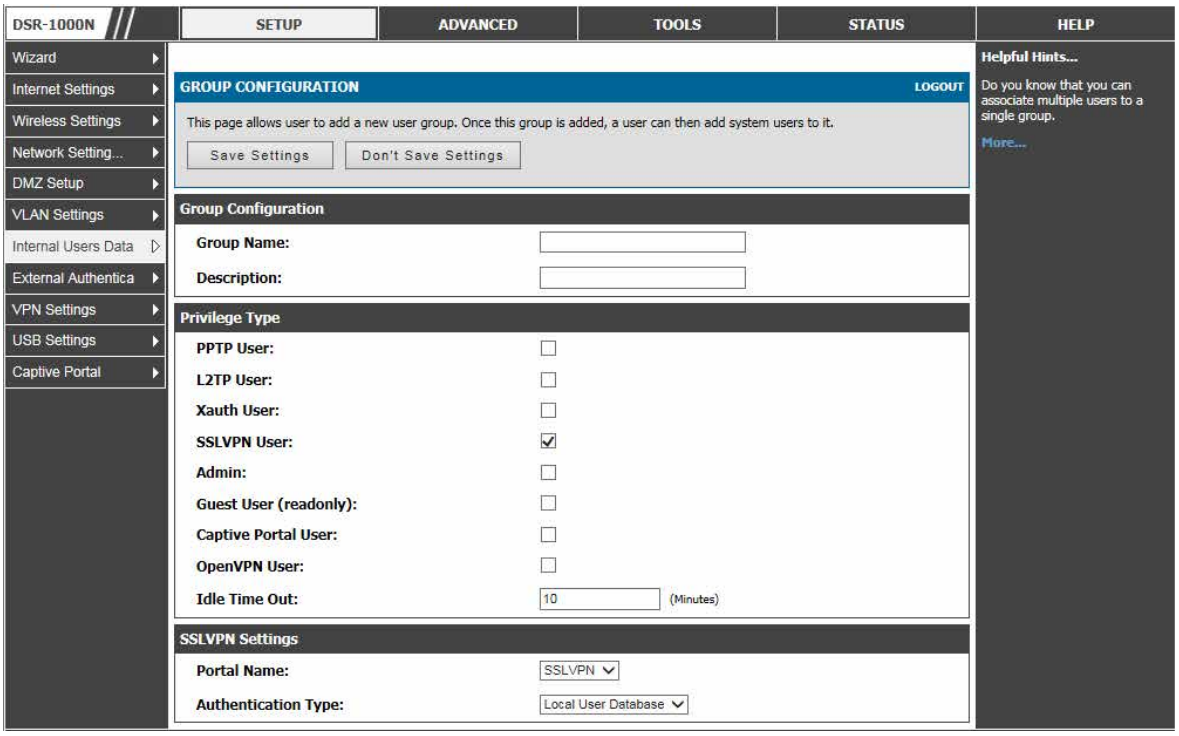


図 9-4　SSL VPN 設定

2. SSL VPN ユーザを選択した場合、SSL VPN 設定で取得される以下のパラメータと共に SSL VPN 設定は表示されます。SSL VPN の詳細を「Authentication Type」（認証タイプ）ごとに設定します。

項目	説明
Authentication Type	以下の 1 つの認証タイプを選択します。: Local User Database（初期値）、Radius-PAP、Radius-CHAP、Radius-MSCHAP、Radius-MSCHAPv2、NT Domain、Active Directory、LDAP、または POP3。
Authentication Secret	ドメインが RADIUS 認証を使用する場合、認証秘密が必要であり、これは RADIUS サーバに設定された秘密に一致する必要があります。
Workgroup	NT ドメイン認証に必要です。複数のワークグループがある場合、最大 2 個のワークグループの詳細を入力できます。
LDAP Base DN	LDAP 認証サーバのためのベースドメイン名です。複数の LDAP 認証サーバがある場合、最大 2 個の固有の LDAP Base DN の詳細を入力できます。

項目	説明
Active Directory Domain	ドメインがアクティブディレクトリが認証を使用する場合、本欄にアクティブなディレクトリドメイン名を入力する必要があります。それらのアクティブディレクトリのユーザ名とパスワードを使用することによって、アクティブディレクトリデータベースに登録されているユーザは、SSL VPN ポータルにアクセスすることができます。複数のアクティブディレクトリドメインがある場合、最大 2 個の認証ドメインの詳細を入力できます。
Timeout	認証サーバに到達するタイムアウト時間。
Retries	DSR が認証サーバへの到達を停止してから認証サーバによる認証を再試行する回数。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ログインポリシーの設定

ログインポリシーをグループに設定します。

1. **SETUP > Internal Users Data > Groups** で対応するグループを選択し、「Login Policies」ボタンをクリックして、以下の画面を表示します。

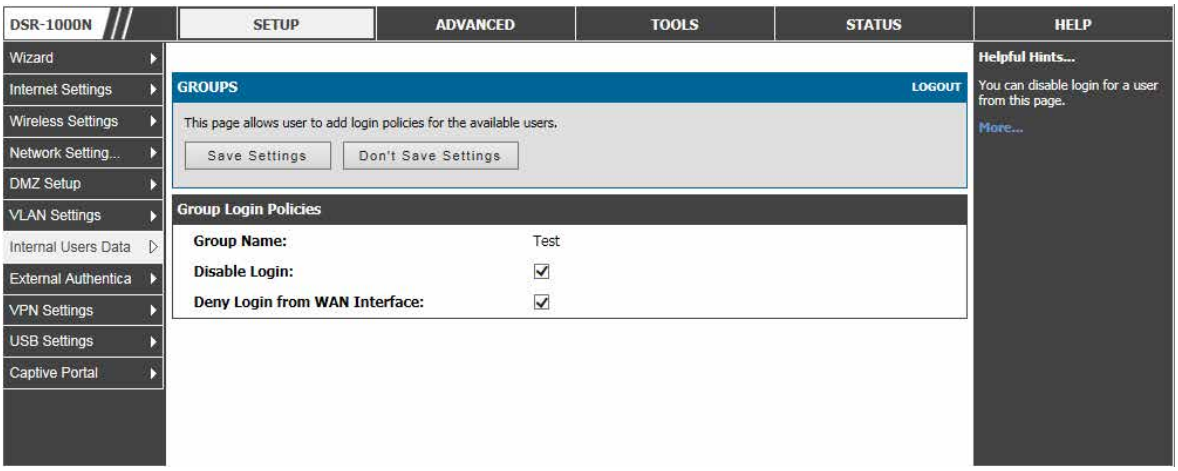


図 9-5　グループログインポリシーオプション

2. 以下の項目を設定します。

項目	説明
Group Name	ログインポリシーを編集できるグループ名を表示します。
Disable Login	チェックすると、本グループ内のユーザのデバイスにおける管理インタフェースへのログインを防止することができます。
Deny Login from WAN Interface	チェックすると、このグループのユーザが WAN（広域ネットワーク）インタフェースからログインするのを防止することができます。この場合、LAN を通したログインだけが許可されます。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ブラウザポリシーの設定

グループにブラウザポリシーを設定します。

1. **SETUP > Internal Users Data > Groups** で対応するグループを選択し、「Policies By Browsers」ボタンをクリックして、以下の画面を表示します。

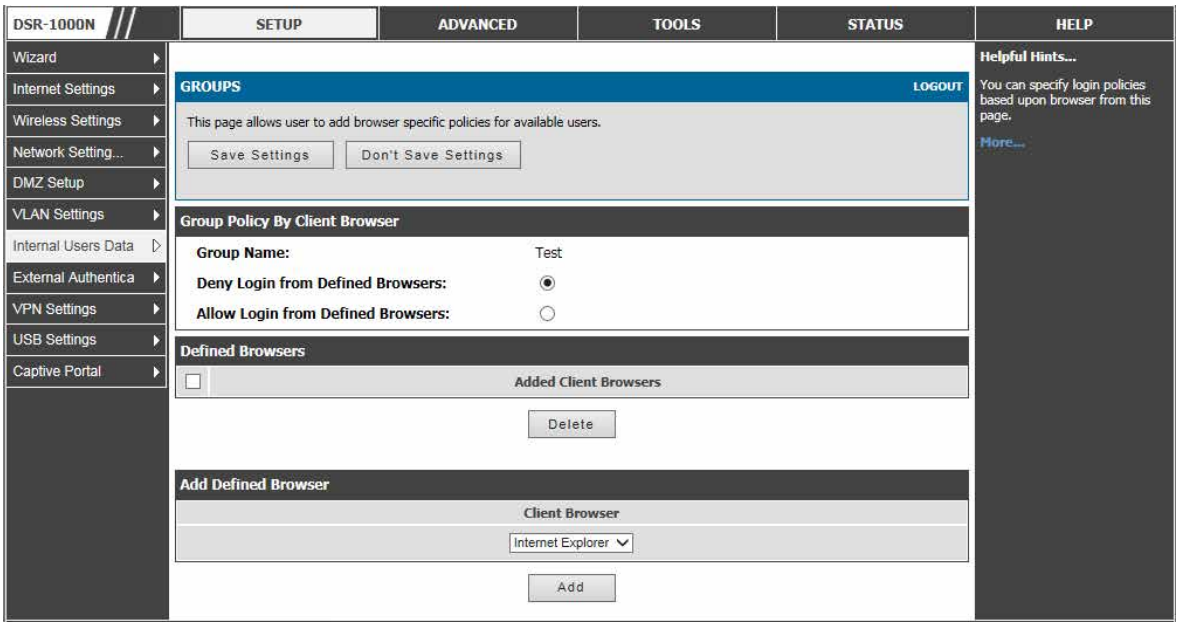


図 9-6　ブラウザポリシーオプション

2. 以下の項目を設定します。

項目	説明
Group Policy By Client Browser	
Group Name	ログインポリシーを編集できるグループ名を表示します。
Deny Login from Defined Browsers	定義済みブラウザのリストは、このグループのユーザがルータの GUI にログインすることを防ぐために使用されます。未定義ブラウザはすべてこのグループのユーザのログインを許可します。
Allow Login from Defined Browsers	定義済みブラウザのリストは、このグループのユーザがルータの GUI にログインすることを許可するために使用されます。未定義ブラウザはすべてこのグループのログインを拒否します。
Defined Browser	
このリストは、グループログインポリシーが定義できる定義済みブラウザ割り当てに追加された Web ブラウザを表示します。最初の列ヘッダのボックスをチェックすると、テーブル内のすべての定義済みブラウザを選択します。「Delete」ボタンをクリックして、選択したブラウザを削除します。	
Add Defined Browser	
プルダウンメニューからクライアントのブラウザを選択して、「Add」ボタンをクリックすることによって、「定義済みブラウザ」のリストに追加することができます。また、このブラウザは上記「Defined Browser」のリストに表示されます。	

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

IP ポリシーの設定

IP にグループにポリシーを設定します。

1. **SETUP > Internal Users Data > Groups** で対応するグループを選択し、「Policies By IP」ボタンをクリックして、以下の画面を表示します。

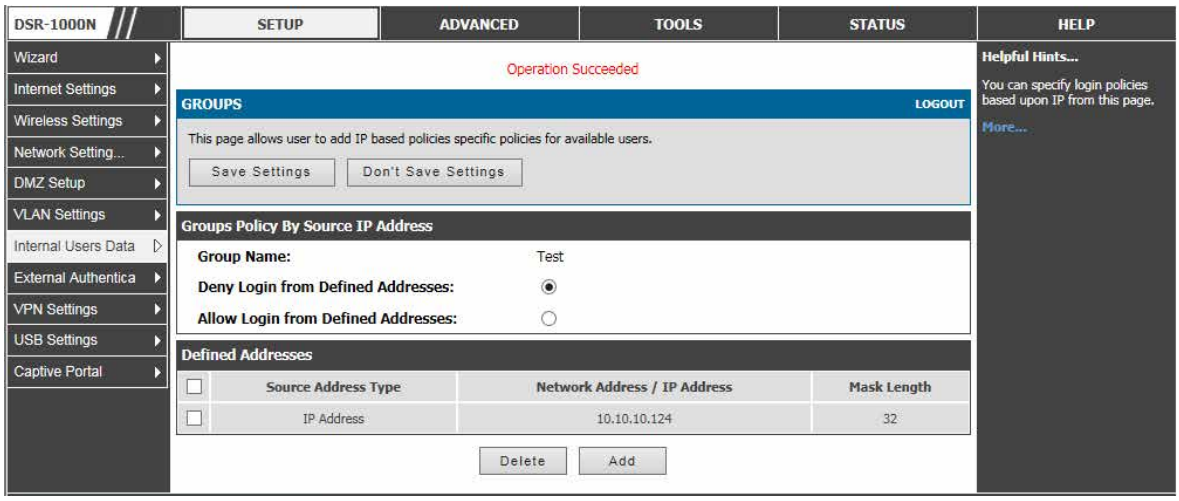


図 9-7　IP ポリシーオプション

2. 以下の項目を設定します。

項目	説明
Group Policy By Client IP Address	
Group Name	ログインポリシーを編集できるグループ名を表示します。
Deny Login from Defined Addresses	定義済みアドレスのリストは、このグループのユーザがルータの GUI にログインすることを防ぐために使用されます。未定義アドレスはすべてこのグループのユーザのログインを許可します。
Allow Login from Defined Addresses	以下の定義済みブラウザのリストは、このグループのユーザがルータの GUI にログインすることを許可するために使用されます。未定義アドレスはすべてこのグループのログインを拒否します。
Defined Addresses	
このリストは、グループログインポリシーが定義できる定義済みアドレスリストに追加されたアドレスを表示します。最初の列ヘッダのボックスをチェックすると、テーブル内のすべての定義済みアドレスを選択します。「Delete」ボタンをクリックして、選択したアドレスを削除します。「Add」ボタンをクリックすることによって、「定義済みアドレス」のリストに追加することができます。	

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

注意　「Login Policies」、「Policies By Browsers」、「Policies By IP」は SSL VPN ユーザ専用です。

アドレスの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

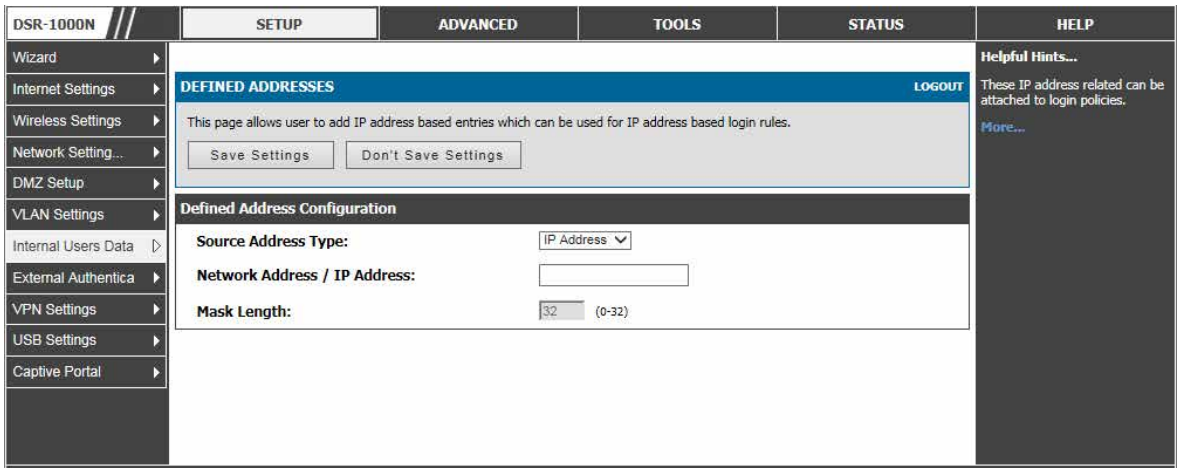


図 9-8　IP ポリシーオプション

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ユーザ設定

SETUP > Internal Users Data > Users メニュー

新しいグループの追加、既存グループの編集および削除を行います。各ユーザは定義済みグループに割り当てられます。

1. **SETUP > Internal Users Data > Users** の順にメニューをクリックし、以下の画面を表示します。

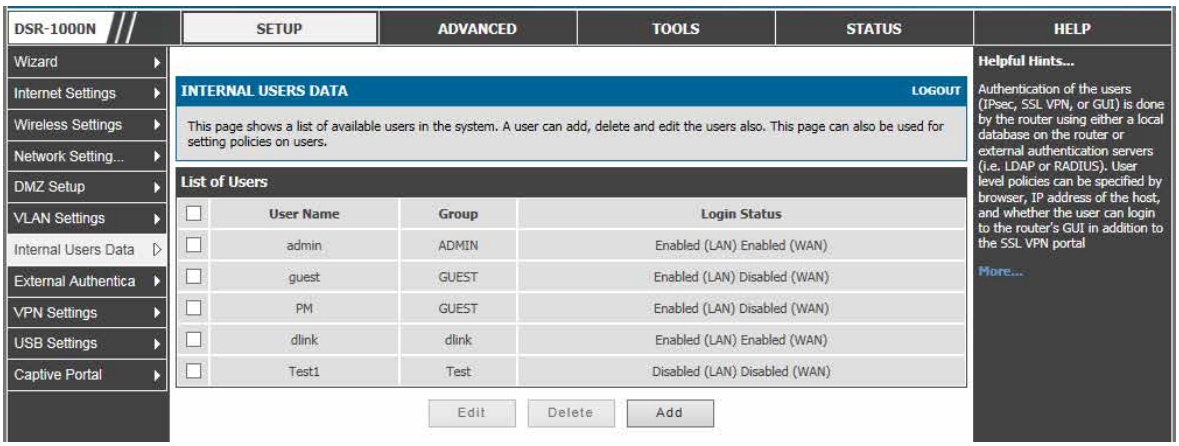


図 9-9　ログインステータスと関連するグループ / ドメインを持つ利用可能なユーザ

ユーザ名、関連グループ、およびログイン状態と共に「List of Users」ページに利用可能なユーザのリストを表示します。

- 「Add」ボタンをクリックして新しいユーザを作成します。
- 「Edit」ボタンをクリックして、既存のユーザを編集します。
- 「Delete」ボタンをクリックして、既存のユーザをクリアします。

ユーザタイプとパスワードの設定

グループに関連付けるユーザを作成します。

1. 「Add」ボタンをクリックして、以下の画面を表示します。

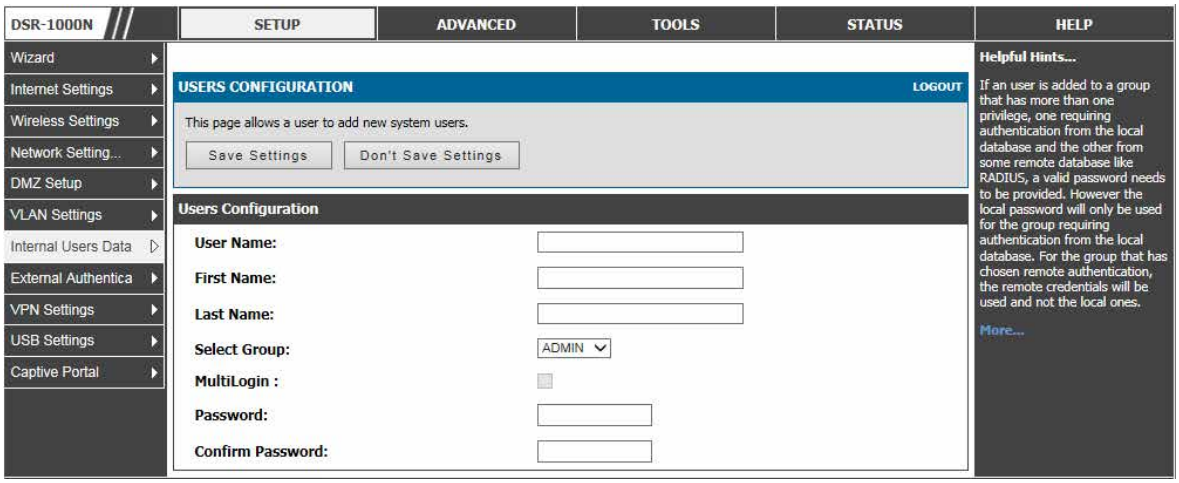


図 9-10　ユーザ設定オプション

2. ユーザ設定を行います。ユーザ設定には以下の主な項目があります。:

項目	説明
User Name	ユーザの固有な識別子。
First Name	ユーザの名前。
Last Name	ユーザの姓名。
Select Group	定義済みグループのリストからグループを選択します。
Password	ユーザ名に関連付けるパスワード。
Confirm Password	上記と同じパスワードを確認のために指定します。
Idle Time Out	ユーザのセッションタイムアウト。ユーザの設定後、すべての定義済みユーザのリストを表示します。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

パスワードがどんな言語の辞書の単語にも含まれず、文字（大文字と小文字の両方）、数字、および記号のシンボルを組み合わせたものであることをお勧めします。パスワードは 30 文字以内で指定します。

ユーザデータベースのインポート

SETUP > Internal Users Data > Import Users Database メニュー

DSR 管理者は適切な書式の CSV ファイルを使用して、直接、ローカルのデータベースにユーザを追加できます。本機能の利点は多くのユーザが 1 つの操作でシステムに追加されるのを可能にすることであり、必要に応じて複数の DSR デバイスに同じファイルをアップロードできます。一度アップロードすると、ローカルユーザデータベース内の特定のユーザは、必要に応じて GUI 経由で変更されます。

以下の手順でユーザデータベースに複数ユーザを持つ CSV ファイルをインポートします。

1. **SETUP > Internal Users Data > Import Users Database** の順にメニューをクリックし、以下の画面を表示します。

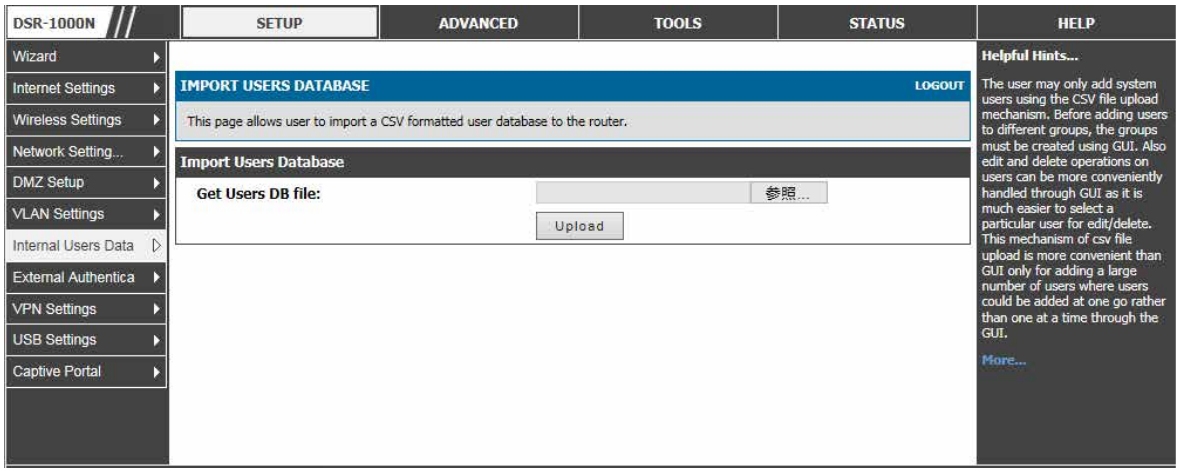


図 9-11　IMPORT USERS DATABASE 画面

2. 「Get Users DB file」にインポートするファイルを指定後、「Upload」ボタンをクリックします。

ユーザデータベースの CSV ファイルを定義するには、以下のパラメータを使用する必要があります。

1. 拡張子 .csv を持つ空のテキストファイルを作成します。

2. ファイルの各行は 1 つのユーザエントリに対応します。すべての行が CRLF（復帰改行）で終了する必要があります。このファイルにコメントまたは他のテキストを追加しないでください。

3. 形式のルール :
a) すべてのフィールドを 2 重引用符で囲む必要があります。
b) 連続したフィールドは「,」（カンマ）で区切ります。
c) 行の前後に空白を入れてはいけません。
d) フィールド間に空白を入れてはいけません。

CSV ユーザデータベースファイルの各行は次の形式に従う必要があります。:
「UserName」、「FirstName」、「LastName」、「GroupName」、「MultiLogin」、「Password」

上のサンプルには、以下の値を定義するフィールドがあります。

- Username（文字フィールド）: DSR のデータベースにおけるユーザと識別子で、ローカルユーザデータベースで固有である必要があります。
- FirstName（文字フィールド）: ユーザの詳細であり、固有である必要はありません。
- LastName（文字フィールド）: ユーザの詳細であり、固有である必要はありません。
- GroupName（文字フィールド）: このユーザに関連付けられるグループ。
- MultiLogSup（ブーリアン値）: これを有効（「1」）にすると、複数ユーザは単一のユーザ名とパスワードを共有できます。
- Password（文字フィールド）: このユーザ名に割り当てるパスワード。

注意　ユーザデータベースの CSV アップロードを動作する前に、GUI を使用してユーザに対応するグループ（CSV における「GroupName」）を作成する必要があります。

注意　ユーザデータベースの CSV では、上のフィールドのいずれも空または NULL とすることはできません。

SSL VPN ポリシー設定

SETUP > VPN Settings > SSL VPN Server > SSL VPN Policies メニュー
SSL VPN ポリシーを設定します。

ポリシーは、特定のネットワークリソース、IP アドレス、または IP ネットワークへのアクセスを許可または拒否するために役に立ちます。これらはユーザ、グループまたはグローバルなレベルで定義されます。初期値では、グローバルな「拒否」ポリシー (非表示) がすべてのアドレスとすべてのサービス / ポートに既に設定されています。

SSL VPN ポリシーはグローバル、グループまたはユーザレベルで作成されます。ユーザレベルポリシーはグループレベルポリシーより優先され、グループレベルポリシーはグローバルポリシーより優先されます。これらのポリシーは、LAN の特定のネットワークリソース、IP アドレスまたは範囲に、または、ルータによってサポートされる様々な SSL VPN サービスに適用できます。利用可能なポリシーのリストは、ユーザ、グループ、またはすべてのユーザ（グローバル）に適用するかどうかに基づいてフィルタされます。

注意 両方が同じユーザ / グループ / グローバルドメインに適用される場合、より特定のポリシーが一般的なポリシーより優先します。つまり、特定の IP アドレスのポリシーは既に参照された IP アドレスを含むアドレス範囲のポリシーより優先します。

注意 **TOOLS > Admin > Remote Management** メニューで「Enable Remote Management」（リモート管理を有効にする）をチェックしてください。

1. **SETUP > VPN Settings > SSL VPN Server > SSL VPN Policies** の順にメニューをクリックし、以下の画面を表示します。

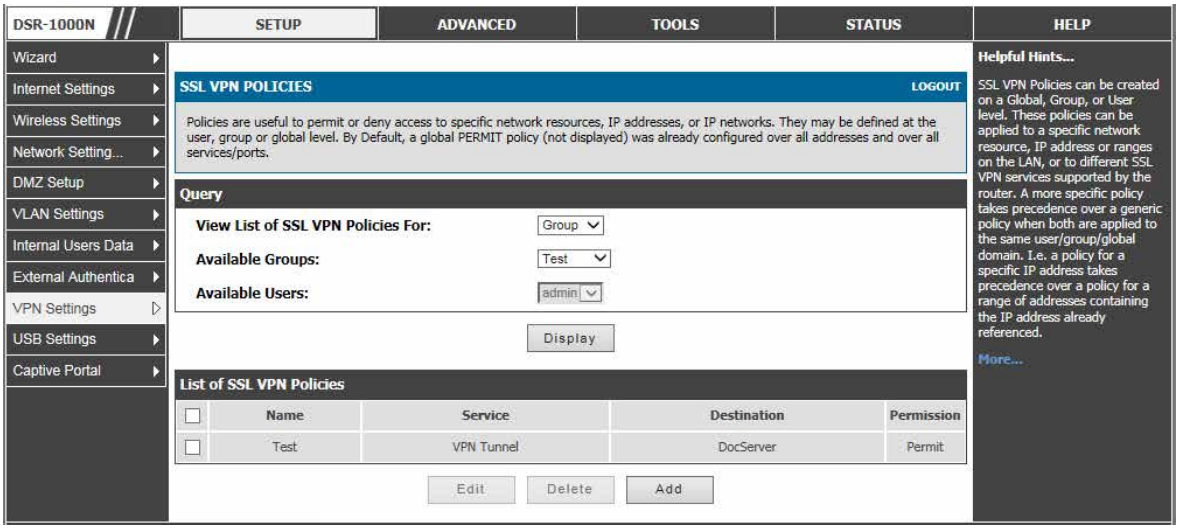


図 9-12　SSL VPN ポリシーのリスト（Group フィルタ）

SSL VPN ポリシーの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

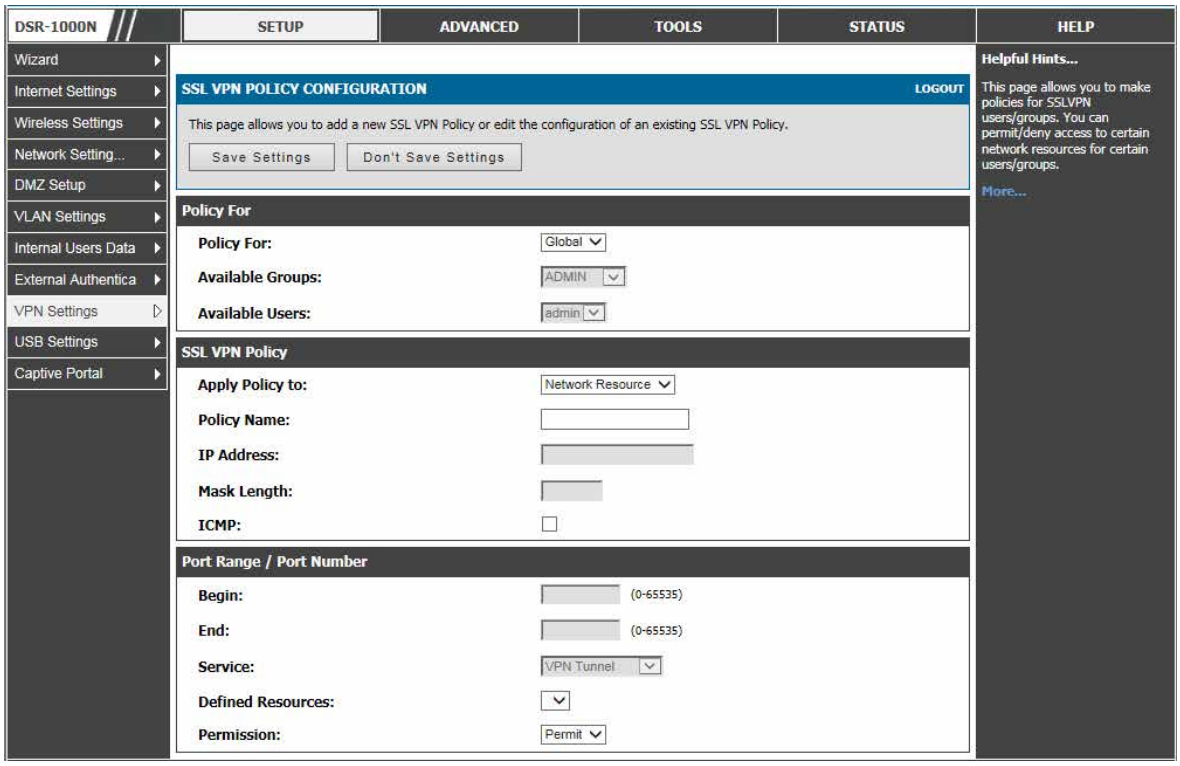


図 9-13　SSL VPN ポリシーの追加

最初にユーザ、グループ、またはグローバル（つまり、すべての SSL VPN ユーザに適用する）に割り当てる必要があります。ポリシーがグループ用であれば、利用可能な設定グループは、プルダウンメニューに表示され、1 つを選択する必要があります。同様に、ユーザ定義ポリシーには、設定済みユーザの使用可能リストから SSL VPN ユーザを選択する必要があります。

次に、ポリシーの詳細を定義します。ポリシー名はこのルールに固有の識別子です。ルータの LAN における特定のネットワークリソース（詳細は続くセクションに記述）、IP アドレス、IP ネットワーク、またはすべてのデバイスにポリシーを割り当てることができます。これら 4 つのオプションの 1 つの選択に基づいて、適切な設定欄が必要となります。（つまり、定義済みリソースのリストから行うネットワークリソースの選択、または IP アドレスの定義）。ポリシーをアドレスに適用するために、ポート範囲 / ポート番号を定義できます。

最後の手順では選択したアドレスまたはネットワークリソースへのアクセスを許可、または拒否するように設定するポリシーの許可が必要とされます。また、サポートしている SSL VPN サービス（VPN トンネル）のうち 1 つまたはすべてにポリシーを指定できます。

一度定義すると、ポリシーは直ちに実行されます。ポリシー名、適用する SSL サービス、送信先（ネットワークリソースまたは IP アドレス）、許可（許可 / 拒否）はルータに設定されたポリシーのリストに概説されています。

2. シングルユーザまたはユーザグループにポリシーを設定するためには、以下の情報を入力します。

項目	説明
Policy For	
Policy For	ユーザ、ユーザグループ、またはすべてのユーザ（グローバルポリシーとする）にポリシーを割り当てることができます。特定のユーザまたはグループ用にポリシーをカスタマイズするために、「Available Groups」および「Available Users」プルダウンメニューから選択できます。
SSL VPN Policy	
Apply Policy to	本ルータが管理する LAN リソースを参照し、ポリシーはネットワークリソース、IP アドレス、IP ネットワークなどへのアクセスを提供（または防止）することができます。
Policy Name	本欄は、ポリシーを識別する独自の名前です。
IP Address	管理されているリソースが IP アドレスまたはアドレス範囲により識別される場合に必要とされます。
Mask Length	管理されているリソースがサブネット内のアドレス範囲により識別される場合に必要とされます。
ICMP	チェックすると ICMP トラフィックをブロックします。

項目	説明
Port Range / Port Number	
Begin / End	ポリシーがトラフィックタイプを管理している場合、本欄は管理トラフィックに対応する TCP または UDP ポート番号の範囲を定義するために使用されます。開始 / 終了ポート範囲を空白のままにすると、すべての UDP および TCP トラフィックに対応します。
Service	本ポリシーによって利用可能な SSL VPN サービスです。提供されるサービスは、VPN トンネル、ポートフォワーディング、または両方です。
Defined Resources	このポリシーは特定のネットワークリソースへのアクセスを提供します。定義済みリソースとして選択できるようにポリシーを作成する前に、ネットワークリソースを設定する必要があります。ネットワークリソースは次のセクションで作成します。
Permission	このポリシーによって定義したリソースを、明示的に許可または拒否することができます。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ネットワークリソースの使用

SETUP > VPN Settings > SSL VPN Server > Resources メニュー

SSL VPN ポリシーを設定する場合に使用するリソースを設定します。テーブルには登録されたリソースが表示され、そのリソースにいくつかの操作を許可します。

ネットワークリソースは、SSL VPN ポリシーを簡単に作成および設定するのに使用される LAN IP アドレスのサービスまたはグループです。複数のリモート SSL VPN ユーザのために同様のポリシーを作成する場合、このショートカットが時間を節約します。

ネットワークリソースを追加する場合、リソースを識別する固有名を作成し、それにサポートする SSL サービスの 1 つまたはすべてを割り当てる必要があります。これが実行されると、作成済みのネットワークリソースの 1 つを編集することでサービスに関連しているオブジェクトタイプ（IP アドレスまたは IP 範囲のいずれか）を設定することができます。必要に応じてこのリソースにネットワークアドレス、マスク長、およびポート範囲 / ポート番号を定義できます。

1. **SETUP > VPN Settings > SSL VPN Server > Resources** の順にメニューをクリックし、以下の画面を表示します。

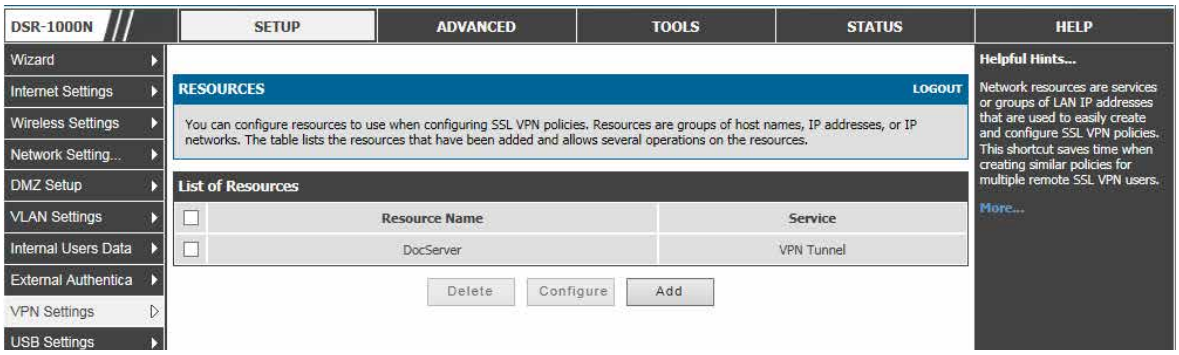


図 9-14　SSL VPN ポリシーに割り当てるために利用可能な設定済みリソースのリスト

リソースの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

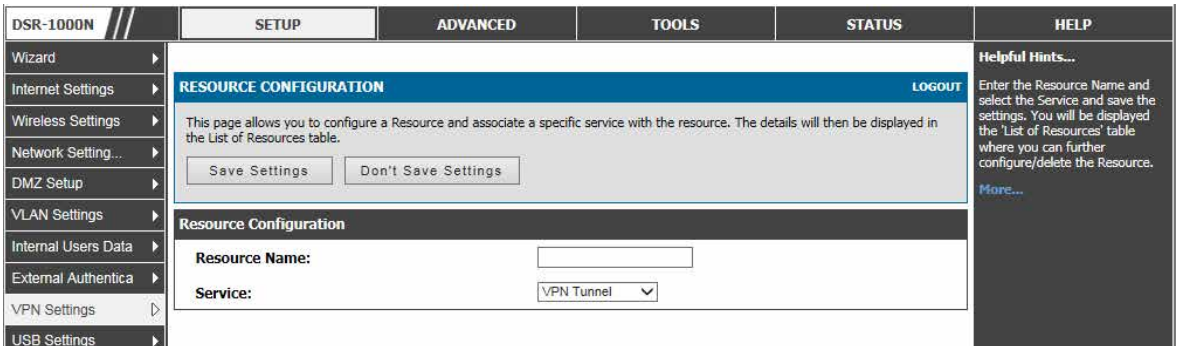


図 9-15　リソースの設定画面

2. ネットワークリソースを定義します。

項目	説明
Resource Name	リソースの独自の識別名
Service	リソース（VPN Tunnel、Port Forwarding、または All）に対応する SSL VPN サービス

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

リソースの詳細設定

1. リソースのリストで設定するリソースをチェックし、「Configure」ボタンをクリックして、以下の画面を表示します。

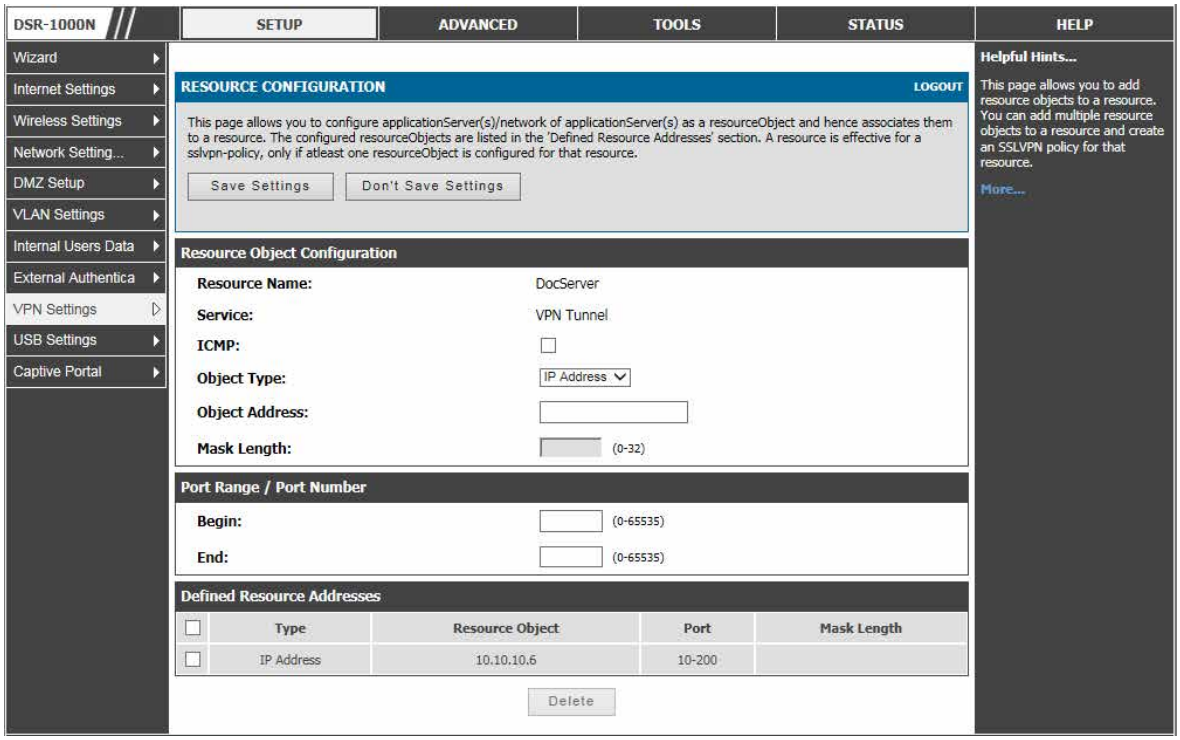


図 9-16　リソースの設定画面

2. ネットワークリソースのコンテンツを定義します。

項目	説明
Resource Object Config	
Resource Name	リソースの固有な識別子
Service	VPN トンネル、ポートフォワーディング、またはすべてのサービスなどの SSLVPN サービス
ICMP	このオプションを選択して、ICMP トラフィックを含めます。
Object Type	「IP Address」または「IP Network」を選択します。
Object Address	オブジェクトタイプによる IP アドレスまたはネットワークアドレス
Mask Length	ネットワーク先のマスク長
Port Range / Port Number	
リソースオブジェクトのポート範囲を指定します。	
Begin	リソースオブジェクトの開始のポート番号
End	リソースオブジェクトの終了のポート番号
Defined Resource Addresses	
リソースのために設定したリソースオブジェクトを示します。	
Type	リソースオブジェクトのオブジェクトタイプ
Resource Object	リソースオブジェクトのオブジェクトアドレス
Port	リソースオブジェクトのポート範囲
Mask Length	ネットワークのマスク長

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

アプリケーションポートフォワーディング

SETUP > VPN Settings > SSL VPN Server > Port Forwarding メニュー
ここでは、プライベートネットワークで動作する定義済みアプリケーションに対してリモートユーザから SSL VPN ゲートウェイに送信されたデータを、検出して、別ルートで送信します。

ポートフォワーディング機能により、リモート SSL ユーザはユーザポータルにログインしてポートフォワーディングを起動した後に、特定のネットワークアプリケーションにアクセスできます。リモートユーザからルータまでのトラフィックは、設定済みのポートフォワーディングルールに基づいて検出されて、別ルートで送信されます。

内部のホストサーバまたは TCP アプリケーションをリモートユーザにアクセスをできるように指定する必要があります。LAN サーバへのアクセスを許可するためには、ローカルサーバの IP アドレスとトンネルされるアプリケーションの TCP ポート番号の入力が必要です。以下の表では一般的なアプリケーションと対応する TCP ポート番号を示しています。:

TCP アプリケーション	ポート番号
FTP データ（通常、必要でない）	20
FTP コントロールプロトコル	21
SSH	22
Telnet	23
SMTP（メール送信）	25
HTTP（web）	80
POP3（メール受信）	110
NTP（ネットワーク時間プロトコル）	123
Citrix	1494
ターミナルサービス	3389
VNC（virtual network computing）	5900 または 5800

リモートユーザに便利なものとして、IP アドレスの解決を考慮したネットワークサーバのホスト名（FQDN）を設定できます。このホスト名解決は、SSL ユーザポータルを経由したポートフォワーディングサービスを利用する場合に、エラー傾向のある IP アドレスの代わりに TCP アプリケーションにアクセスするために、簡単に覚えられる FQDN を使用したものをユーザに提供します。

ポートフォワーディングを設定するためには、以下の項目が必要です。
- Local Server IP address - アプリケーションをホスティングするローカルサーバの IP アドレス。
- TCP port - アプリケーションの TCP ポート。

新しいアプリケーションを定義すると、「List of Configured Applications for Port Forwarding」（ポートフォワーディングの設定済みアプリケーションリスト）テーブルに表示します。

IP アドレスの代わりにホスト名を使用することによって、ユーザがプライベートネットワークサーバへのアクセスが可能となります。IP アドレスに対応する FQDN をポートフォワーディングホスト設定セクションで定義します。
- Local server IP address - アプリケーションをホスティングするローカルサーバの IP アドレス。アプリケーションはあらかじめ設定される必要があります。
- Fully qualified domain name - 内部サーバのドメイン名を指定します。

新しい FQDN の設定後、ポートフォワーディング用の定義済みホストのリストを表示します 。

注意 ポートフォワーディングのための最低限の必要条件が TCP アプリケーションとローカルサーバ IP アドレスを識別することである場合、ホスト名を定義するのはオプションです。構成されたホスト名のローカルサーバ IP アドレスはポートフォワーディングの構成されたアプリケーションの IP アドレスに一致する必要があります。

1. **SETUP > VPN Settings > SSL VPN Server > Port Forwarding** の順にメニューをクリックし、以下の画面を表示します。

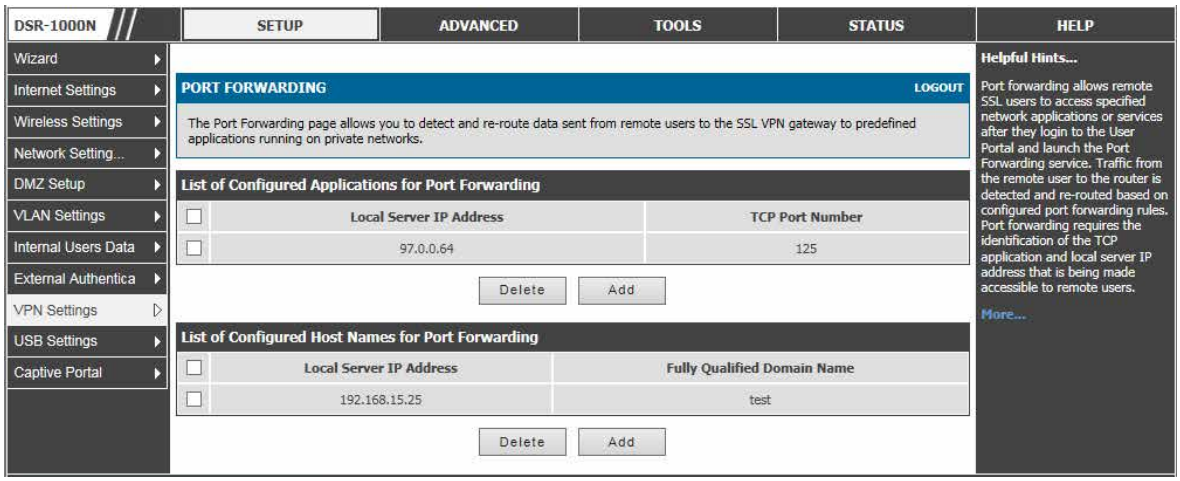


図 9-17　SSL ポートフォワーディングの使用可能なアプリケーションリスト

アプリケーションの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

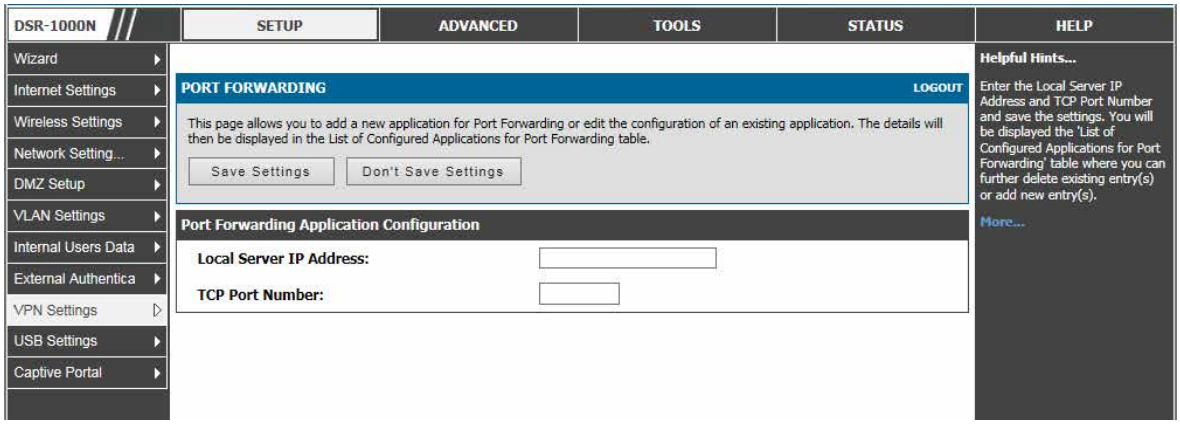


図 9-18　アプリケーションの設定画面

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

ホスト名の追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

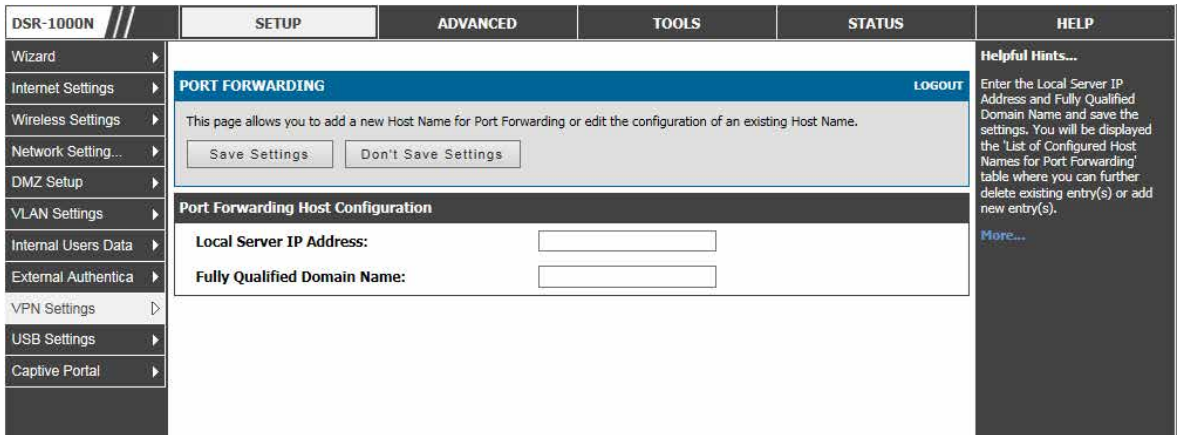


図 9-19　ホスト名の設定画面

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

SSL VPN クライアント設定

SSL VPN トンネルクライアント設定

SETUP > VPN Settings > SSL VPN Client > SSL VPN Client メニュー
SSL VPN トンネルクライアント設定を行います。

SSL VPN トンネルクライアントはブラウザ側マシンとこのルータ間のポイントツーポイント接続を提供します。SSL VPN クライアントがユーザポータルから起動される場合、企業のサブネットから IP アドレス、DNS、および WINS 設定を持つ「ネットワークアダプタ」が自動的に作成されます。これにより、リモート SSLVPN クライアントマシン上に特別なネットワーク設定をせずに、ローカルアプリケーションがプライベートネットワーク上のサービスにアクセスすることができます。

VPN トンネルクライアントの仮想（PPP）のインタフェースアドレスが LAN 上の物理デバイスと重複しないことを保証することが重要です。SSL VPN 仮想ネットワークアダプタ用の IP アドレス範囲は、コーポレート LAN と異なるサブネットまたは重複しない範囲とするべきです。

注意 クライアントのネットワークインタフェース（イーサネット、無線など）の IP アドレスは、SSL VPN トンネル経由でアクセスされている企業 LAN 上のルータの IP アドレスまたはサーバと一致することはできません。

1. **SETUP > VPN Settings > SSL VPN Client > SSL VPN Client** の順にメニューをクリックし、以下の画面を表示します。

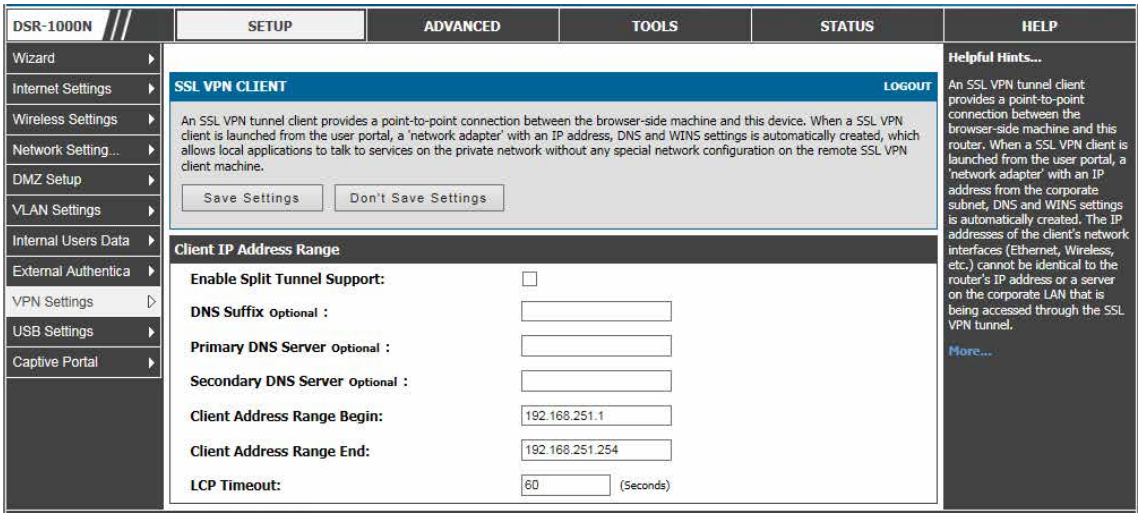


図 9-20　SSL VPN クライアントアダプタとアクセス設定

ルータは「Full tunnel」と「Split tunnel」のサポートを許可します。「Full tunnel」モードは VPN トンネル中のクライアントからルータにすべてのトラフィックを送信します。「Split tunnel」モードは事前に指定したクライアントのルートに基づいてプライベート LAN にトラフィックを送信します。これらのクライアントのルートは SSL クライアントに特定のプライベートネットワークへのアクセスを与えて、その結果、特定の LAN サービス上のアクセス制御を許可します。「Enable Split Tunnel Support」をチェックすると、「Split tunnel」が有効になります。

2. クライアントレベル設定を行います。

項目	説明
Enable Split Tunnel Support	Split トンネルを使用すると、クライアントルートが参照するリソースだけが VPN トンネル上でアクセスされます。Full トンネルを使用すると、（Split トンネルオプションが無効な場合、DSR は Full トンネルモードで動作します。）プライベートネットワークにおける全 IP アドレスが VPN トンネル上でアクセスされます。クライアントルートは必要とされません。
DNS Suffix	SSL VPN クライアントに付与される DNS サフィックス名。この設定はオプションです。
Primary DNS Server	クライアントホストに作成したネットワークアダプタに設定する DNS サーバの IP アドレス。本設定はオプションです。
Secondary DNS Server	この設定はオプションです。
Client Address Range Begin	トンネルに接続するクライアントは、この IP アドレスで開始するアドレスの範囲からネットワークアダプタに割り当てるために DHCP が配布する IP アドレスを取得します。
Client Address Range End	クライアントネットワークアダプタに配布する DHCP のアドレス範囲の終了 IP アドレス。
LCP Timeout	SSL VPN トンネルネゴシエーションのために待機する時間を設定します。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

SSL VPN トンネルの宛先ルートの表示、クライアントルートの追加

SETUP > VPN Settings > SSL VPN Client > Configured Client Routes メニュー

ここでは SSL VPN クライアントに設定されている宛先ルートの表示、クライアントルートの追加を行います。

コーポレートネットワークと異なるサブネットの IP アドレスを SSL VPN クライアントに割り当てる場合、VPN トンネルを通じたプライベート LAN へのアクセスを許可するためにクライアントルートを追加する必要があります。また、プライベート LAN のファイアウォール（通常このルータ）におけるスタティックルートが、VPN ファイアウォールを通じてプライベートトラフィックを送信する必要があります。Split トンネルモードが有効である場合、VPN トンネルクライアントにルートを設定する必要があります。

1. **SETUP > VPN Settings > SSL VPN Client > Configured Client Routes** の順にメニューをクリックし、以下の画面を表示します。

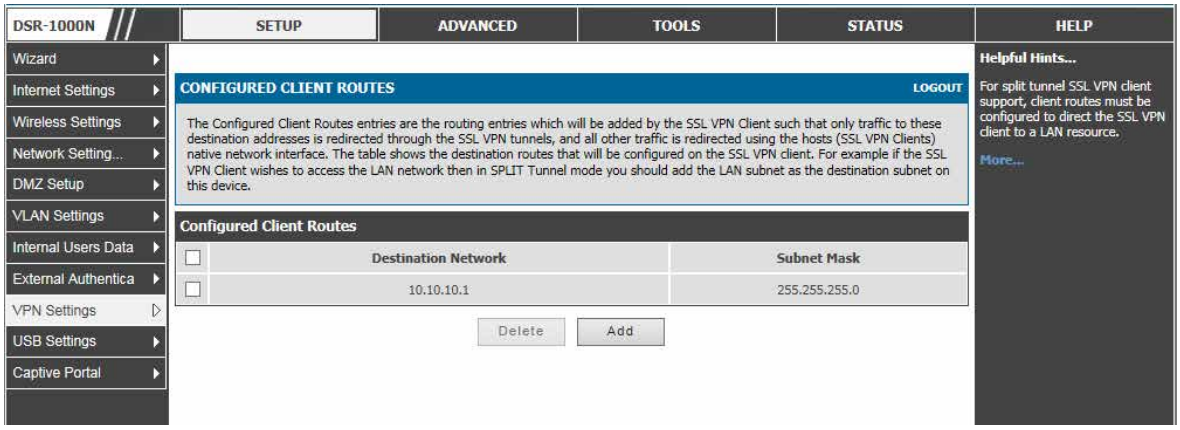


図 9-21　SSL VPN クライアントルートリスト

クライアントルートの追加

1. 「Add」ボタンをクリックして、以下の画面を表示します。

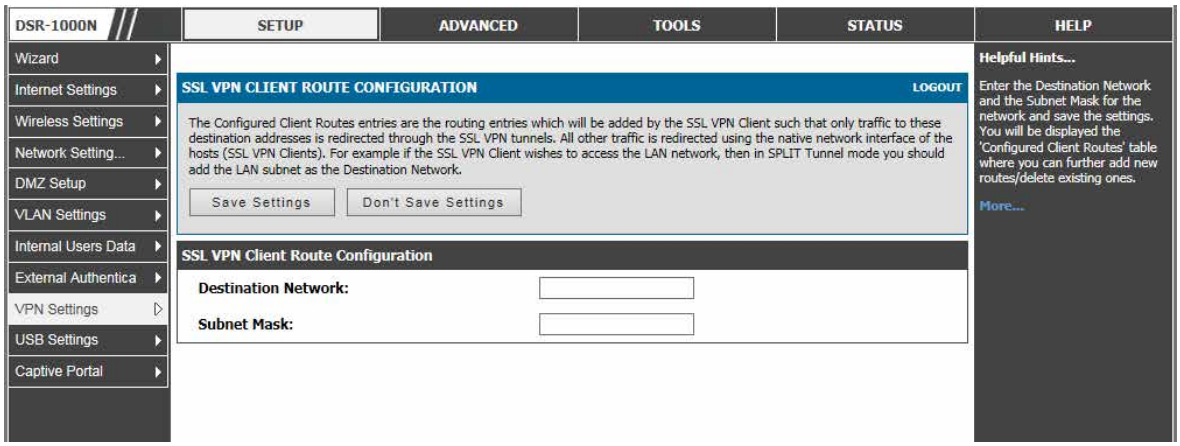


図 9-22　クライアントルートの設定画面

2. 以下の項目を設定します。

項目	説明
Destination Network	VPN トンネルクライアントから送信先ネットワークの LAN のネットワークアドレスまたはサブネット情報をここに設定します。
Subnet mask	送信先ネットワークのサブネット情報をここに設定します。

項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

注意　設定したクライアントルートは「split tunnel」モードでだけ適用されます。**SETUP > VPN Settings > SSL VPN Client > SSL VPN Client** メニューで「Enable Split Tunnel Support」をチェックする必要があります。

注意　**MAC OS における SSL VPN トンネルのインストール / アンインストール手順**

1. 端末をオープンし、root で visudo を実行し、sudoers ファイルをオープンします。
2. sudoers ファイルの末尾で「username ALL=NOPASSWD:/usr/sbin/chown,/bin/chmod,/bin/rm」を追加後、保存して、ファイルをクローズします。（ユーザ名は SSL VPN ユーザ名ではなく、MAC アカウントのユーザ名です。）

   SSL VPN トンネルをアンインストールする際にパスワードを要求された場合、root のパスワードまたは sslvpn ユーザのアカウントではなく MAC ユーザのアカウントのパスワードを入力します。

ユーザポータル

SSL VPN ポータルの設定

SETUP > VPN Settings > SSL VPN Server > Portal Layouts メニュー
本デバイスに設定された SSL ポータルレイアウトを表示し、ポータルレイアウトにいくつかの操作を許可します。

リモートユーザが SSL トンネル（ポートフォワーディングまたは VPN トンネルサービスのいずれかを使用して）経由でプライベートネットワークへのアクセスを希望する場合、ユーザポータルを通じてログインします。このポータルは、ルータ管理者が決定する適切なアクセスレベルと特権を提供する認証欄を用意しています。ユーザアカウントが保存されるドメインを指定する必要があります。また、ドメインは認証方式とリモートユーザを示すポータルレイアウト画面を決定します。

1. **SETUP > VPN Settings > SSL VPN Server > Portal Layouts** の順にメニューをクリックし、以下の画面を表示します。

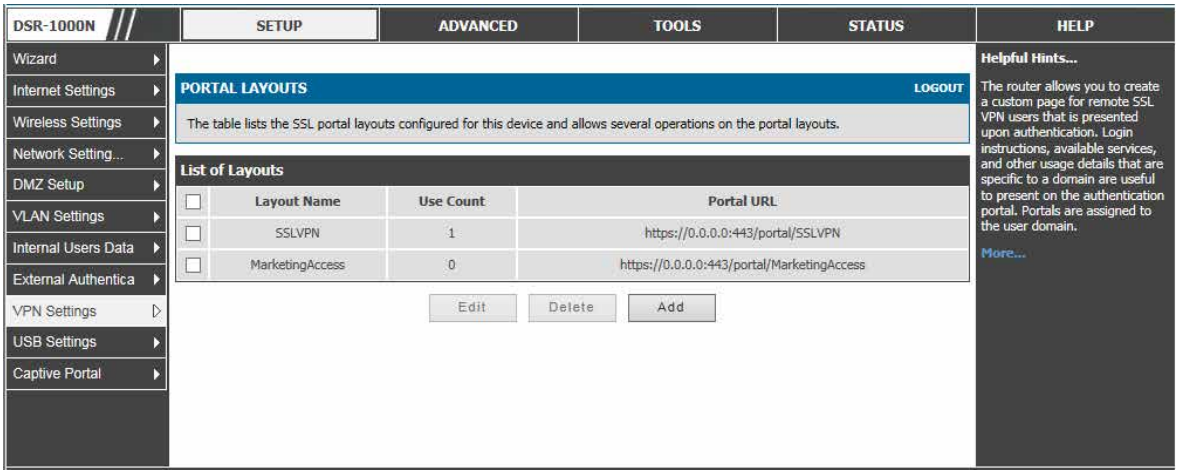


図 9-23　SSL VPN ポータルのリスト

設定したポータルは、認証ドメインに関連付けできます。

ポータルレイアウトの作成
ルータは、リモート SSL VPN ユーザに対して認証時に提示されるカスタムページを作成することができます。ドメインのためにカスタマイズ可能なポータルには様々な欄があり、これにより、ルータの管理者は、リモートユーザにポータルで目に見えるログインの手順、可能なサービス、およびその他利用の詳細などを通信することができます。ドメイン設定中、設定したポータルレイアウトを、そのドメインによって認証されるすべてのユーザのために選択できます。

注意　ポータル LAN の IP アドレスの初期値は https://192.168.10.1/scgibin/ userPortal/portal です。これは、「User Portal」リンクがルータ GUI の SSL VPN メニューでクリックされると開くページと同じです。

ルータ管理者は、SSL VPN メニューの設定ページでポータルレイアウトを作成および編集します。ポータル名、バナー名、およびバナーコンテンツをこのポータルの対象ユーザに対してカスタマイズすることができます。ポータル名は SSL VPN ポータルの URL に追加されます。また、このポータルに（認証ドメイン経由で）割り当てられたユーザは、「VPN Tunnel」ページまたは「Port Forwarding」ページなどのルータがサポートする 1 つ以上の SSL サービスで示されます。

1. 「Add」ボタンをクリックして以下の画面を表示します。

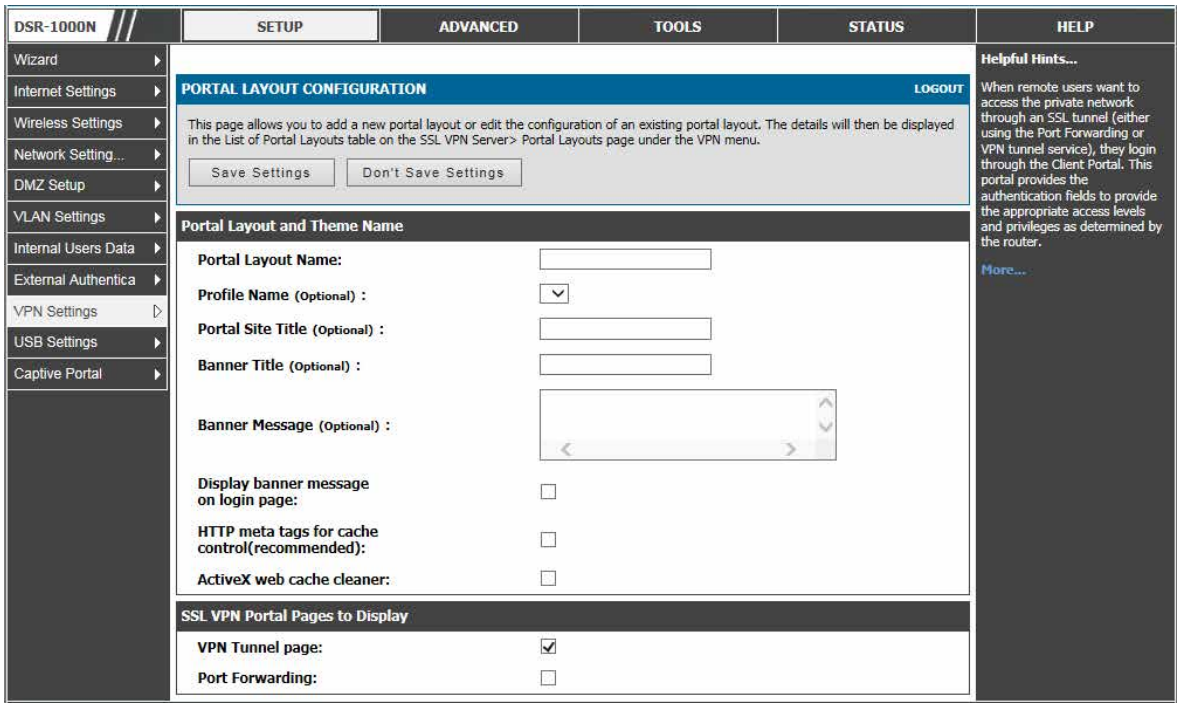


図 9-24　SSL VPN ポータル設定

2. ポータルレイアウトとテーマを設定するためには、以下の情報を設定します。

項目	説明
Portal Layout and Theme Name	
Portal layout Name	設定されているカスタムポータルの記述名。SSL ポータル URL の部分として使用されます。
Portal Name	（オプション）ポータル名を指定します。
Portal Site Title	（オプション）クライアントがこのポータルにアクセスする場合に表示されるポータル Web ブラウザ画面のタイトルです。
Banner Title	（オプション）ログイン前に SSL VPN クライアントに表示されるバナータイトル。
Banner Message	（オプション）ログイン前に SSL VPN クライアントに表示されるバナーメッセージ。
Display banner message on the login page	ログインページのバナーメッセージを表示または隠すオプションがあります。
HTTP meta tags for cache control	このセキュリティ機能は、期限切れの Web ページとデータがクライアントの Web ブラウザキャッシュに保存されるのを防ぎます。本オプションを選択することをお勧めします。
ActiveX web cache cleaner	ActiveX キャッシュ制御 Web クリーナ機能は、この SSL VPN ポータルにユーザがログインする時はいつも、ゲートウェイからクライアントのブラウザに対して実行されます。
SSL VPN Portal Page to Display	
このポータルに表する SSL サービスに従って「VPN Tunneled page」（VPN トンネルのページ）、「Port Forwarding」（ポートフォワーディング）、または両方を有効にすることができます。ポータル設定が行われると、新しく設定されたポータルは、ポータルレイアウトのリストに追加されます。	

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

第 10 章　高度な設定ツール

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

設定項目	説明	参照ページ
USB デバイスのセットアップ	USB ポートに接続した USB デバイスを設定します。	171 ページ
外部認証	各種認証サーバの設定を行います。	174 ページ
認証証明書	認証証明書の設定を行います。	180 ページ
高度なスイッチ設定	ルータの省電力およびジャンボフレーム設定を行います	181 ページ

USB デバイスのセットアップ

DSR サービスルータには、プリンタアクセス、ファイル共有のための USB インタフェースがあります。USB デバイスのサポートを有効にするために、GUI 上の設定は必要ありません。ご使用の USB ストレージデバイスまたはプリンタケーブルを挿入すると、DSR ルータは自動的に接続した周辺機器のタイプを検出します。

項目	説明
USB Mass Storage	「共有ポート」として参照されるため、LAN ユーザはネットワークドライブとして DSR に接続する USB ディスク上のファイルにアクセスできます。
USB Printer	DSR は USB を通して接続するプリンタへのアクセスを LAN に提供できます。プリンタドライバは LAN ホストにインストールされる必要があります。また、トラフィックは LAN とプリンタ間の DSR を通じて送信されます。

Windows マシンでプリンタを設定する

以下の手順を行います。:

1. デスクトップの「スタート」をクリックします。
2. 「プリンタと FAX」オプションを選択します。
3. 右クリックして「プリンタの追加」を選択するか、左のメニューにある「プリンタのインストール」をクリックします。
4. 「ネットワークプリンタ、またはほかのコンピュータに接続されているプリンタ」のラジオボタンを選択して、「次へ」ボタンをクリックします。（Windows7 の場合、「探しているプリンターはこの一覧にはありません」を選択します。）
5. 「インターネット上または自宅 / 会社のネットワーク上のプリンタに接続する」（Windows7 の場合、「共有プリンターを名前で選択する」を選択します。）を選択し、以下の URL を指定します。http://< ルータの IP アドレス >:631/printers/< モデル名 >（モデル名はルータの GUI の USB Status ページに表示されます。）
6. 「次へ」ボタンをクリックして、表示されたリストから適切なドライバを選択します。
7. 「次へ」ボタンをクリックして、プリンタの追加を完了します。

USB デバイスの検出

SETUP > USB Settings > USB Status メニュー

USB ポートに接続する USB デバイスに関する情報の表示、安全なデバイスの取り外しなど、USB デバイスに特定の設定を行うことができます。

1. **SETUP > USB Settings > USB Status** の順にメニューをクリックし、以下の画面を表示します。

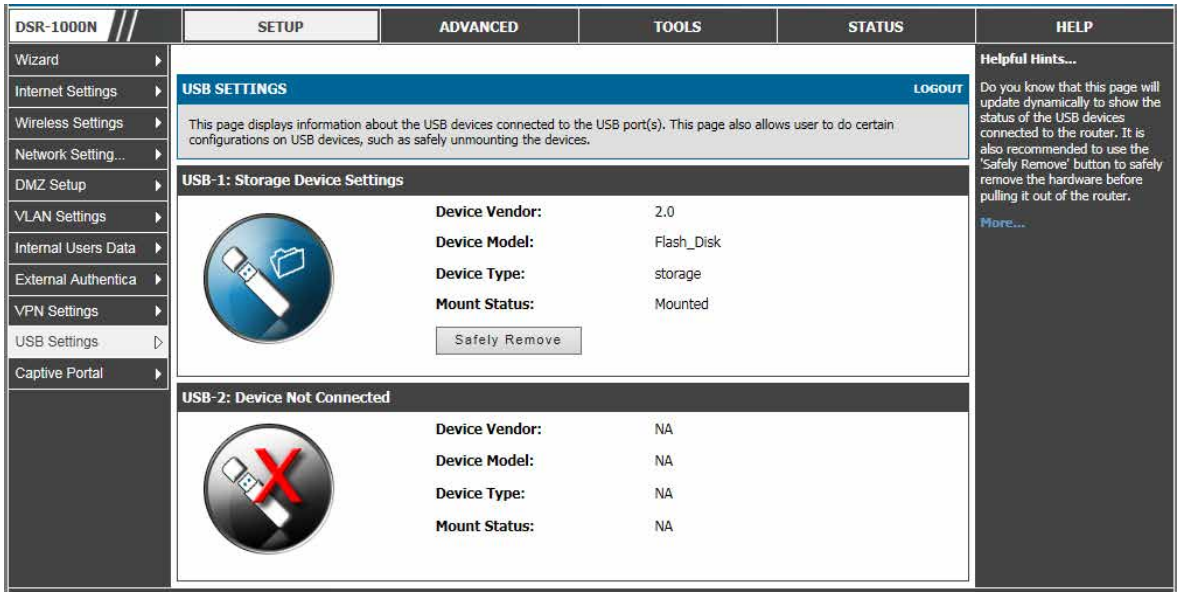


図 10-25 USB デバイスの状態

ルータからハードウェアを安全に取り外すために抜く前に「Safety Remove」ボタンをクリックすることをお勧めします。

USB 共有ポート

SETUP > USB Settings > USB SharePort メニュー

本ルータで利用可能な共有ポート機能を設定することができます。

1. **SETUP > USB Settings > USB SharePort** の順にメニューをクリックし、以下の画面を表示します。

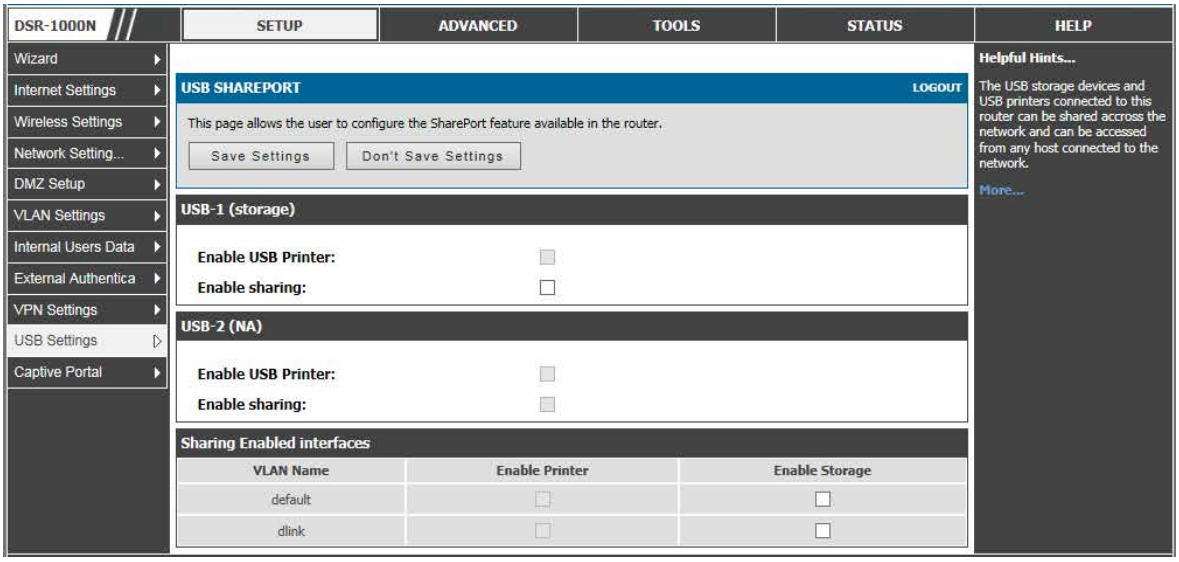


図 10-26　USB 共有ポートの設定

以下の項目があります。

項目	説明
USB-1 / USB-2	
Enable USB Printer	選択すると、ルータに接続する USB プリンタが、ネットワークを経由して共有できるようになります。 ホストの追加プリンタ画面で以下のコマンドを使用して、ルータに接続し、適切なインストール済みプリンタドライバを持つ LAN ホストは USB プリンタにアクセスします。http://< ルータ IP:631>/printers/< プリンタ名 > プリンタ名は USB 設定ページで確認できます。
Enable Sharing	選択すると、ルータに接続する USB ストレージが、ネットワークを経由して共有できるようになります。
Sharing Enabled interfaces	
USB 共有が有効な LAN インタフェースでは、少なくとも 1 つのインタフェースの共有を開始するために選択する必要があります。	
Enable Printer	選択インタフェースのプリンタ共有を有効にします。
Enable Storage	選択インタフェースのストレージ共有を有効にします。

2. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

外部認証

ルータ自身の現在のローカルユーザデータベースは、通常、GUI または CLI への管理アクセスを許可するのに使用されます。外部認証サーバは、一般的に安全であり、無線アクセスポイントの接続を許可するため、IPSec エンドポイントを認証するため、さらに、VLAN 上のキャプティブポータルを通じたアクセスを許可するために使用されます。本セクションでは、ルータで利用可能な認証サーバと設定の必要条件について説明します。

「Server Checking」ボタンは、すべての場合に設定したサーバへの接続性を検証するのに使用されます。

POP3 サーバ

POP3 は、TCP/IP 接続上でメールに最も一般的に使用されるアプリケーションレイヤのプロトコルです。暗号化トラフィックを POP3 サーバに送信するのに、ポート 995 経由の SSL 暗号化と共に認証サーバを使用します。POP3 サーバの証明書は、ユーザがアップロードした CA 証明書によって検証されます。SSL 暗号化が使用されない場合、ポート 110 は POP3 認証トラフィックに使用されます。

DSR ルータは、単に POP3 クライアントとして機能し、外部 POP3 サーバに接続することでユーザを認証します。この認証オプションは IPSec、PPTP/L2TP サーバ、およびキャプティブポータルユーザで利用可能です。PPTP/L2TP サーバ用の POP3 は、PAP でのみサポートしており、CHAP/MSCHAP/MSCHAPv2 暗号化ではサポートしていないことにご注意ください。

POP3 サーバの設定

SETUP > External Authentication > POP3 Settings > POP3 Server Configuration メニュー

1. **SETUP > External Authentication > POP3 Settings > POP3 Server Configuration** の順にメニューをクリックし、以下の画面を表示します。

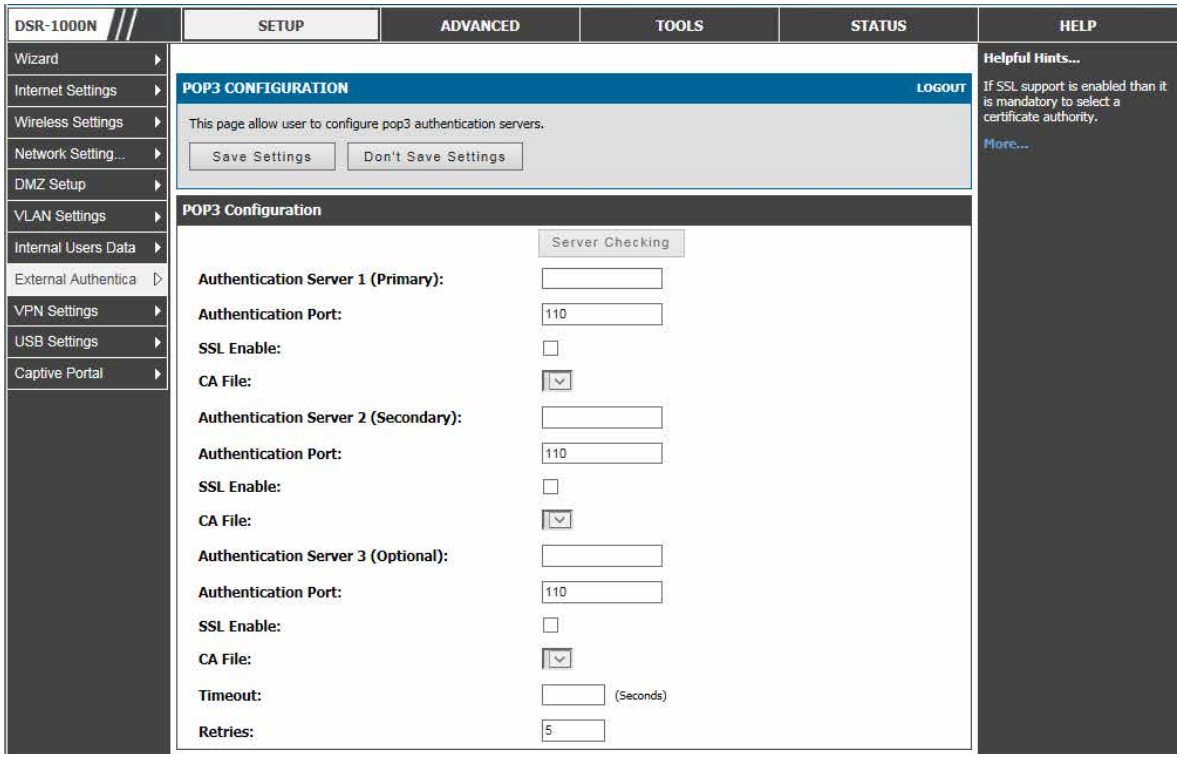


図 10-27 POP3 認証サーバ設定

2. 以下の項目を設定します。

項目	説明
Server Checking	設定したサーバの状態のチェック、およびサーバの稼働の有無をチェックします。
Authentication Server 1 (Primary)	プライマリ認証サーバの IP アドレス。
Authentication Server 2 (Secondary)	セカンダリ認証サーバの IP アドレス。
Authentication Server 3 (Optional)	サード（オプション）認証サーバの IP アドレス。
Authentication Port	それぞれの認証サーバの認証ポート。
SSL Enable	POP3 の SSL サポートを有効にします。本オプションが有効な場合、CA（認証局）を選択する必要があります。
CA File	POP3 サーバの証明書を検証する CA（認証局）。
Timeout	認証サーバからの応答に対するルータの待ち時間（秒）を設定します。
Retries	ルータが処理をやめる前に POP3 サーバに行うリトライ回数を決定します。

3. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

「Server Checking」ボタンは、設定したサーバへの接続性を検証するのに使用されます。設定した認証サーバの ID を検証するために、POP3 ネゴシエーションの一部として CA ファイルを使用します。3 つの設定サーバのそれぞれが、認証に使用する固有の CA を持てます。

POP3 CA ファイルのアップロード

SETUP > External Authentication > POP3 Settings > POP3 Trusted CA メニュー

1. **SETUP > External Authentication > POP3 Settings > POP3 Trusted CA** の順にメニューをクリックし、以下の画面を表示します。

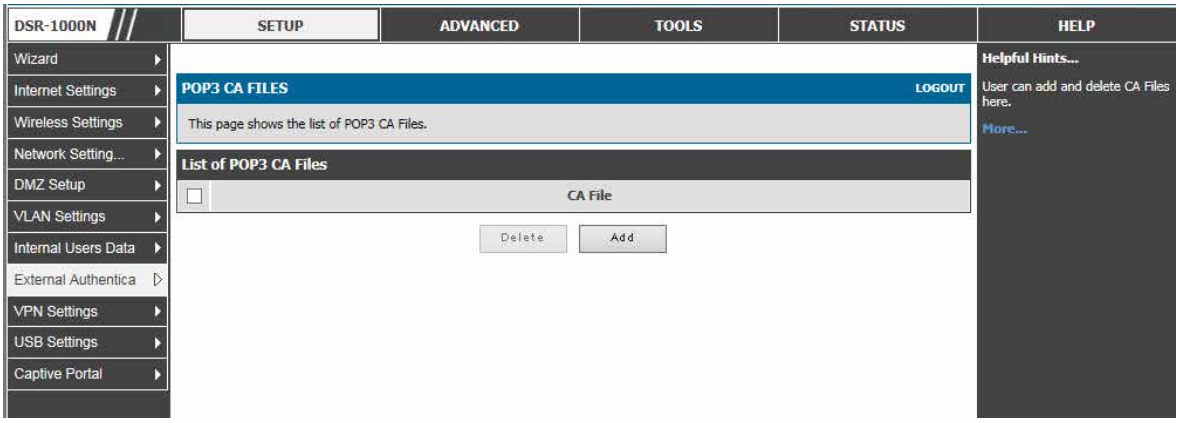


図 10-28 POP3 CA ファイルリスト

POP3 CA ファイルのリストが表示されます。

2. 「Add」ボタンをクリックし、以下の画面を表示します。

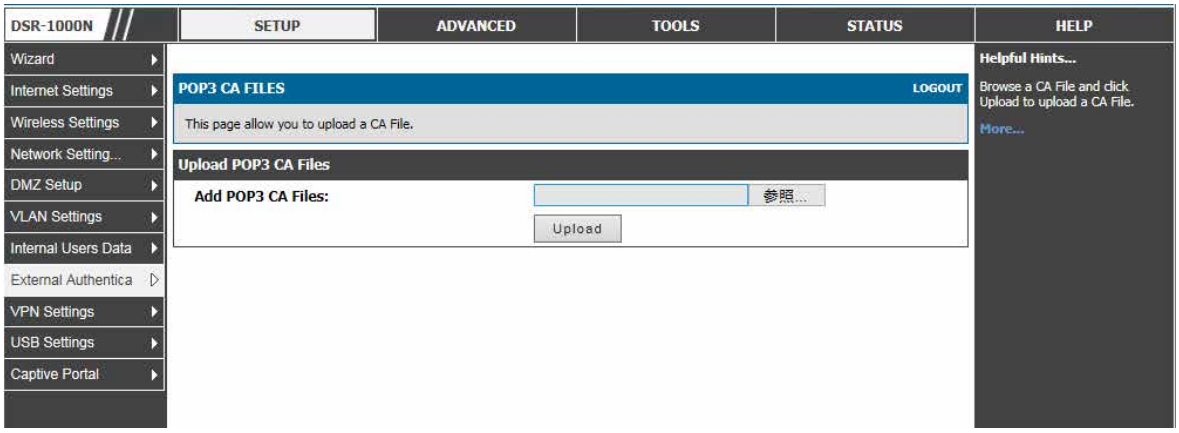


図 10-29 POP3 CA ファイルのアップロード

3. 設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

NT ドメインサーバ

SETUP > External Authentication > NT Domain Settings メニュー

NT ドメインサーバは、定義済みの「Workgroup」欄を通じてユーザとホストが自身の認証を行えるようにします。通常、Windows または Samba サーバを使用して、認定ユーザの統合管理ディレクトリに対する認証のドメインを管理します。

1. **SETUP > External Authentication > NT Domain Settings** の順にメニューをクリックし、以下の画面を表示します。

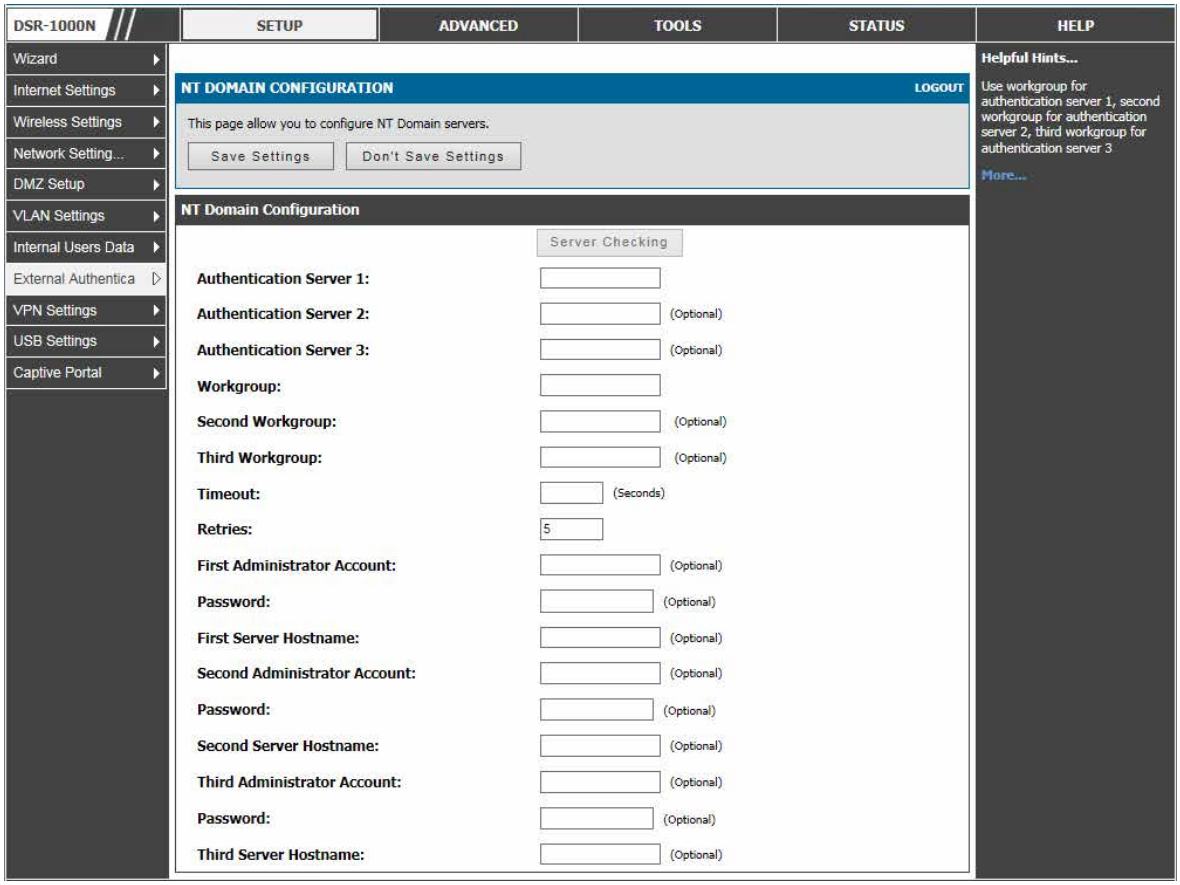


図 10-30 NT ドメイン認証サーバ設定

2. 以下の項目を設定します。

項目	説明
Server Checking	設定したサーバの状態のチェック、およびサーバの稼働の有無をチェックします。
Authentication Server 1 (Primary)	プライマリ認証サーバの IP アドレス。
Authentication Server 2 (Secondary)	セカンダリ認証サーバの IP アドレス。
Authentication Server 3 (Optional)	サード（オプション）認証サーバの IP アドレス。
Workgroup	認証サーバ 1 のワークグループ。認証の NT ドメインタイプは「Workgroup」欄を必要とします。NT ドメイン認証を設定するのに必要とされる Workgroup については管理者に問い合わせてください。
Second Workgroup (optional)	（オプション）認証サーバ 2 のワークグループ。
Third Workgroup (optional)	（オプション）認証サーバ 3 のワークグループ。
Timeout	認証サーバからの応答に対するルータの待ち時間（秒）を設定します。
Retries	ルータが処理をやめる前に POP3 サーバに行うリトライ回数を決定します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

RADIUS サーバ

SETUP > External Authentication > Radius Settings メニュー

無線セキュリティのエンタープライズモードは、WPA および / または WPA2 セキュリティに RADIUS サーバを使用します。RADIUS サーバは、RADIUS 認証を使用するプロファイルで有効にされた AP への無線クライアントの接続を認証するために設定されて、ルータがアクセスできる必要があります。

1. **SETUP > External Authentication > Radius Settings** の順にメニューをクリックし、以下の画面を表示します。

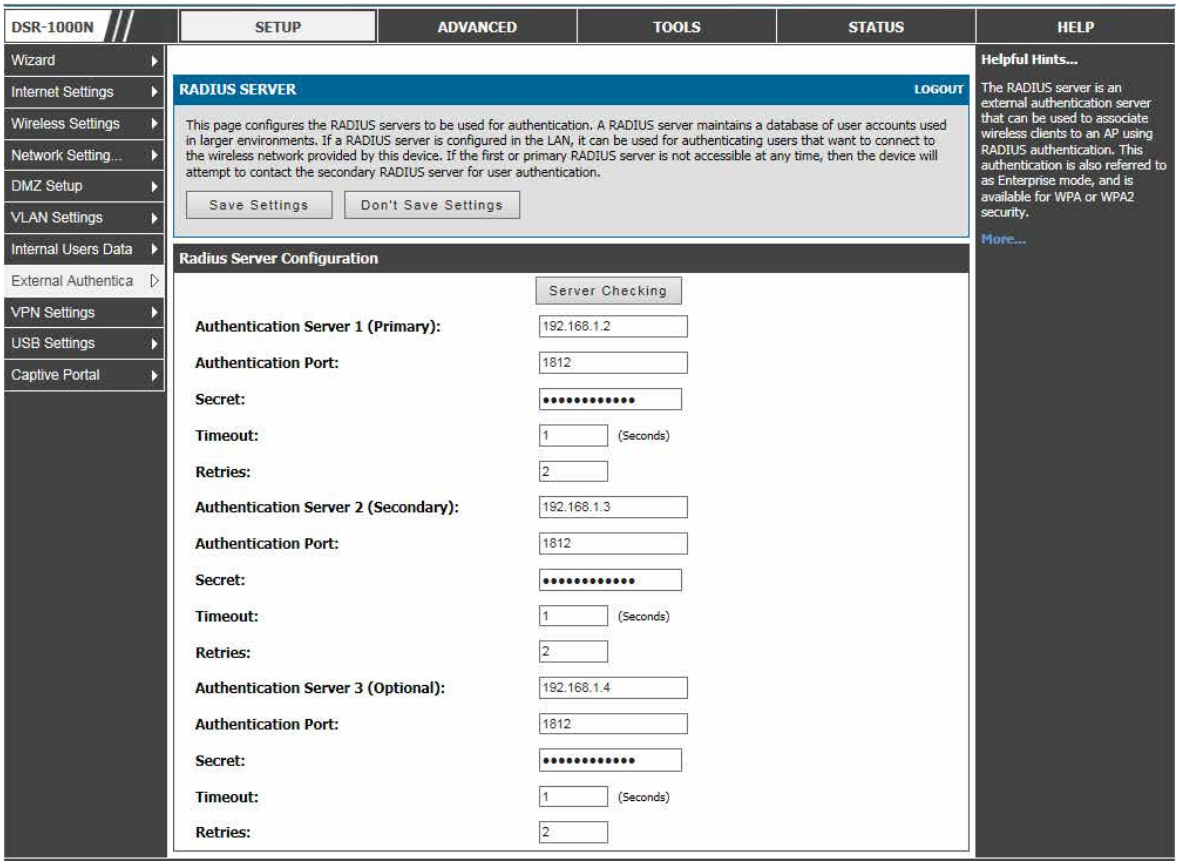


図 10-31 RADIUS サーバ設定

2. 以下の項目を設定します。

項目	説明
Server Checking	設定したサーバの状態のチェック、およびサーバの稼働の有無をチェックします。
Authentication Server IP Address	サーバを識別するために必要です。ルータがプライマリサーバに到達できない場合に必要に応じてセカンダリ RADIUS サーバが冗長性を提供します。
Authentication Port	RADIUS サーバ接続のためのポート
Secret	このルータが指定した RADIUS サーバへのログインを許可される共有シークレットを入力します。このキーは RADIUS サーバの秘密鍵に一致する必要があります。
Timeout / Retries	フィールドはプライマリに到達できない場合にセカンダリに移動するため、またはサーバとの通信が不能である場合に RADIUS 認証を試みるために使用されます。 • Timeout - 認証サーバからの応答に対するルータの待ち時間（秒）を設定します。 • Retries - ルータが処理をやめる前に POP3 サーバに行うリトライ回数を決定します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

Active Directory サーバ

SETUP > External Authentication > Active Directory Settings メニュー

Active Directory 認証は NT ドメイン認証を拡張したバージョンです。Kerberos プロトコルは、OU（Organizational Units：組織単位）でグループ化されるユーザの認証のために利用されます。特に、NT ドメインサーバは数千のユーザに制限されますが、Active Directory サーバでは、100 万以上の登録ユーザの構造化をサポートしています。

設定した認証サーバと Active Directory ドメインを使用して、外部の Windows ベースのサーバにあるユーザのディレクトリに連携するユーザを有効にします。本認証オプションも、SSL VPN クライアントユーザに共通であり、また、IPSec/PPTP/L2TP クライアント認証に役立ちます。

1. **SETUP > External Authentication > Active Directory Settings** の順にメニューをクリックし、以下の画面を表示します。

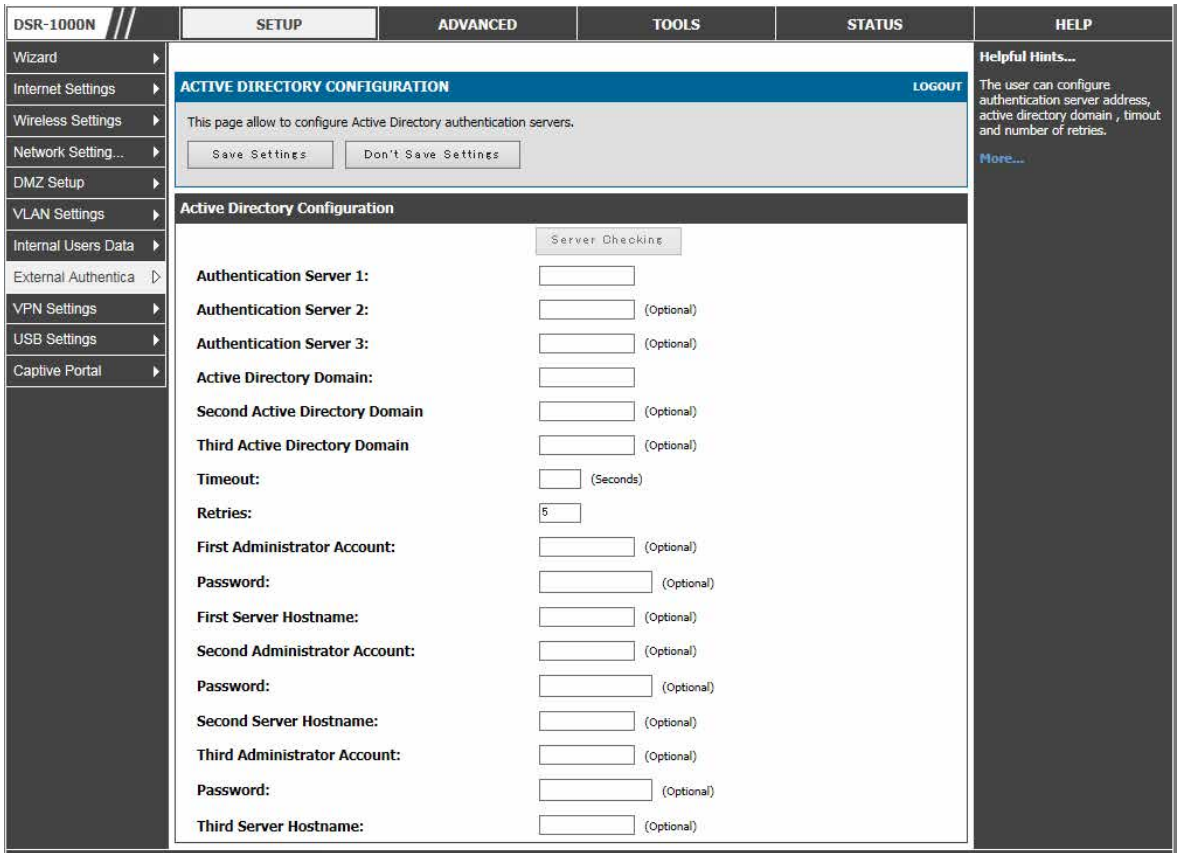


図 10-32　Active Directory 認証サーバ設定

2. 以下の項目を設定します。

項目	説明
Server Checking	設定したサーバの状態のチェック、およびサーバの稼働の有無をチェックします。
Authentication Server 1 (Primary)	プライマリ認証サーバの IP アドレス。
Authentication Server 2 (Secondary)	セカンダリ認証サーバの IP アドレス。
Authentication Server 3 (Optional)	サード（オプション）認証サーバの IP アドレス。
Active Directory Domain	アクティブディレクトリが認証タイプである場合、本欄にアクティブなディレクトリドメイン名を入力する必要があります。それらのアクティブディレクトリのユーザ名とパスワードを使用することによって、アクティブディレクトリデータベースに登録されているユーザは、SSL VPN ポータルにアクセスすることができます。
Second Active Directory Domain	（オプション）認証サーバ 2 のアクティブディレクトリドメイン。
Third Active Directory Domain	（オプション）認証サーバ 3 のアクティブディレクトリドメイン。
Timeout	認証サーバからの応答に対するルータの待ち時間（秒）を設定します。
Retries	ルータが処理をやめる前に POP3 サーバに行うリトライ回数を決定します。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

LDAP サーバ

SETUP > External Authentication > LDAP Settings メニュー

LDAP 認証方式は、ルータと外部サーバ間で認証証明書を交換するのに LDAP を使用します。LDAP サーバは、ディレクトリ構成内に大容量のユーザのデータベースを保持します。そのため、同じユーザ名でも異なるグループに所属するユーザは、ユーザ情報が階層的な方法に保存されることから、認証されます。なお、Windows における LDAP サーバまたは Linux サーバの設定は、ユーザ認証用の NT ドメインや Active Directory サーバの設定よりも格段に簡単になっています。

ルータに設定された詳細は、ルータとそのホストの認証を通過します。LDAP 属性、ドメイン名 (DN)、およびいくつかの場合では管理者アカウント & パスワードは、LDAP サーバにルータの認証を許可するキーフィールドです。

1. **SETUP > External Authentication > LDAP Settings** の順にメニューをクリックし、以下の画面を表示します。

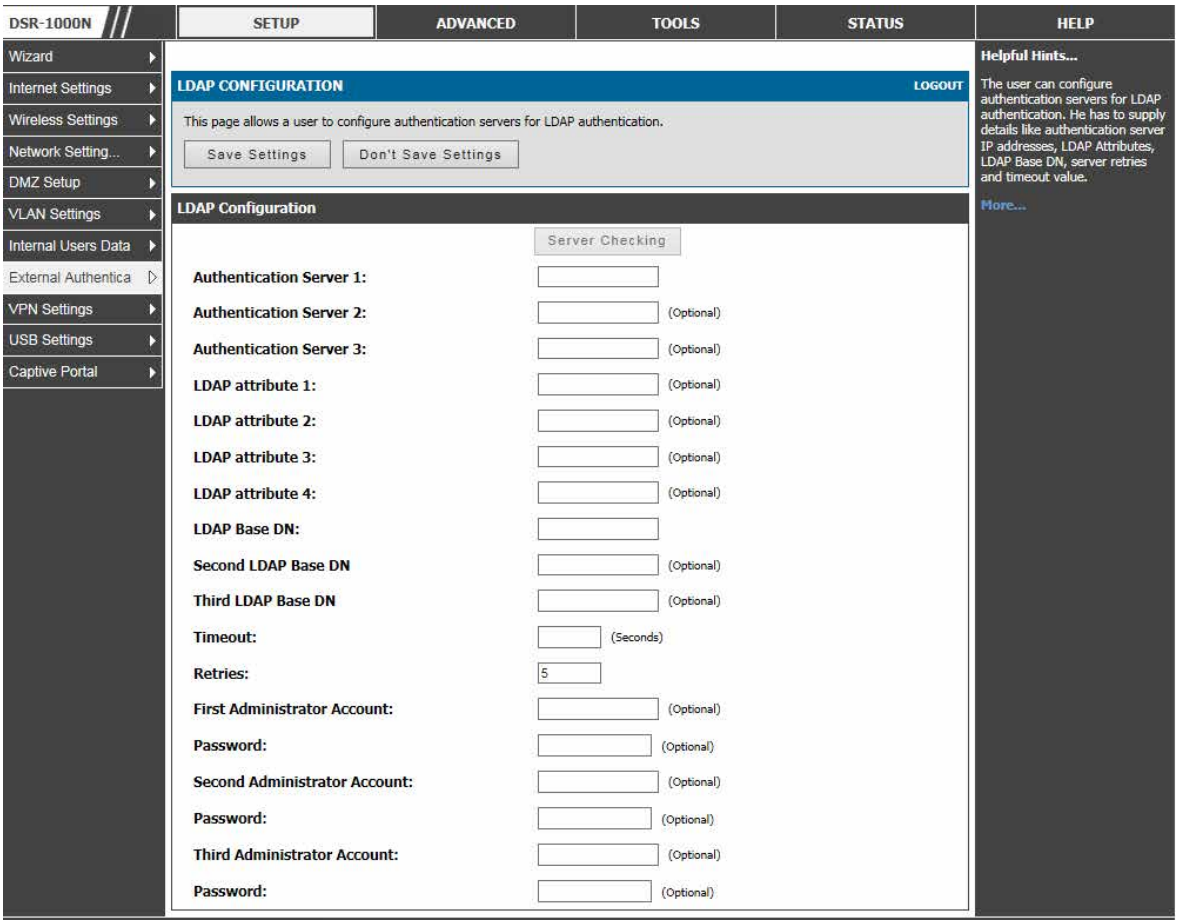


図 10-33 LDAP 認証サーバ設定

2. 以下の項目を設定します。

項目	説明
Server Checking	設定したサーバの状態のチェック、およびサーバの稼働の有無をチェックします。
Authentication Server 1 (Primary)	プライマリ認証サーバの IP アドレス。
Authentication Server 2 (Secondary)	セカンダリ認証サーバの IP アドレス。
Authentication Server 3 (Optional)	サード（オプション）認証サーバの IP アドレス。
LDAP attribute 1-4	LDAP サーバで設定された LDAP ユーザに関連する属性です。SAM アカウント名、Associated ドメイン名などの属性を含みます。同じユーザ名を持っていて異なるユーザを見分けるのにこれらを使用できます。
LDAP Base DN	LDAP 認証はベースドメイン名を必要とします。このドメインに LDAP 認証を使用するベース DN については管理者に問い合わせてください。
Second LDAP Base DN	（オプション）認証サーバ 2 のベースドメイン名。
Third LDAP Base DN	（オプション）認証サーバ 3 のベースドメイン名。
Timeout	認証サーバからの応答に対するルータの待ち時間（秒）を設定します。
Retries	ルータが処理をやめる前に POP3 サーバに行うリトライ回数を決定します。
First Administrator Account	PPTP/L2TP 接続に LDAP 認証が必要とされる時に使用される LDAP サーバのプライマリ管理アカウント。
Password	（オプション）プライマリ管理者パスワード。
Second Administrator Account	（オプション）PPTP/L2TP 接続に LDAP 認証が必要とされる時に使用される LDAP サーバのセカンダリ管理アカウント。

項目	説明
Password	（オプション）セカンド管理者パスワード。
Third Administrator Account	（オプション）PPTP/L2TP 接続に LDAP 認証が必要とされる時に使用されるサード LDAP サーバの管理アカウント。
Password	（オプション）サード管理者パスワード。

3. 「Save Settings」ボタンをクリックして設定内容を保存および適用します。

認証証明書

ADVANCED > Certificates メニュー

このゲートウェイは SSL 証明書（HTTPS と SSL VPN 認証用）と同様に IPSec VPN 認証にデジタル証明書を使用します。ベリサインなどのよく知られている認証局（CA）からデジタル証明書を入手するか、または、このゲートウェイで利用可能な機能を使用してあなた自身の証明書を生成および署名することができます。ゲートウェイには自己署名証明書があり、ご使用のネットワーク要件に応じて認証局によって署名されたものと交換することができます。CA 証明書がサーバのアイデンティティに関する強力な保証を提供しており、多くの企業ネットワーク VPN ソリューションの必要条件となっています。

1. **ADVANCED > Certificates** の順にメニューをクリックし、以下の画面を表示します。

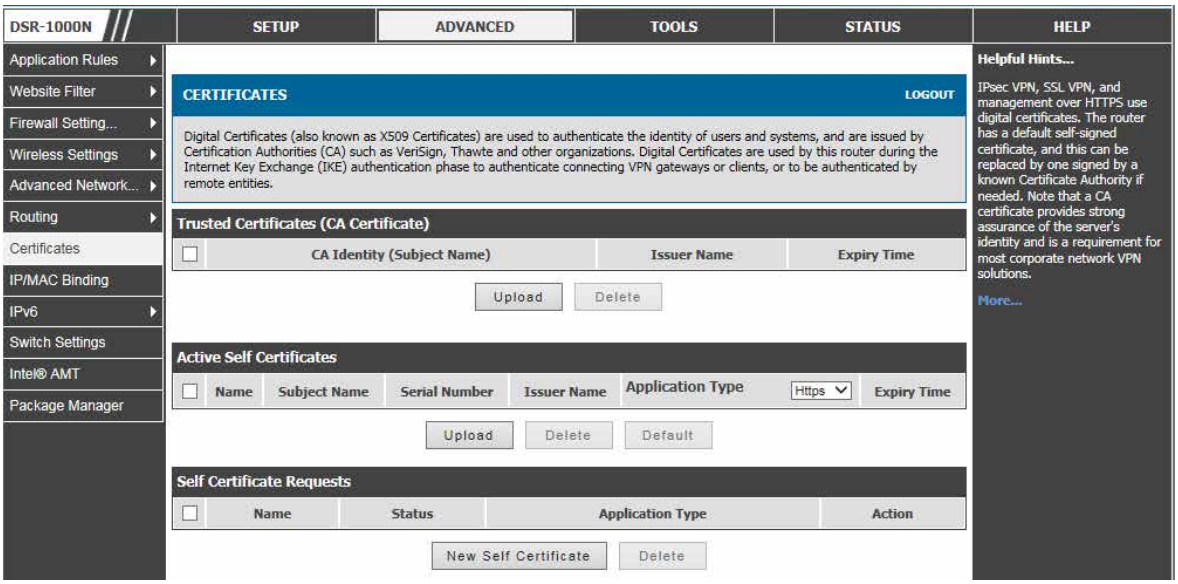


図 10-34 IPSec と HTTPS 管理のための証明書サマリ

証明書メニューでは、現在ゲートウェイにロードされている証明書（CA および自己署名の両方）のリストを参照することができます。トラスト（CA）証明書のリストには以下の証明書データが表示されます。:

項目	説明
CA Identity（サブジェクト名）	人または組織に証明書を発行します。
Issuer Name（発行者）	この証明書を発行した CA 名です。
Expiry Time（期限）	このトラスト証明書が無効になる日付。

自己証明書は、ご使用のデバイスを確認する CA によって発行された証明書です（または、CA のアイデンティティ保護が必要ない場合には自己署名証明書）。Active Self Certificate テーブルは現在ゲートウェイにロードされている自己証明書を表示します。各アップロードされている自己証明書に対して以下の情報が表示されます。:

項目	説明
Name（名称）	この証明書を特定するのに使用する名前であり、IPSec VPN ピアまたは SSL ユーザには表示されません。
Subject Name（サブジェクト名）	この証明書の所有者として表示される名前です。IPSec または SSL VPN ピアが本欄に表示されるため、これは公式に登録されるか会社名であるべきです。
Serial Number（シリアル番号）	シリアル番号は CA によって保持され、この署名された証明書を特定するために使用されます。
Issuer Name（発行者）	この証明書を発行した（署名した）CA 名です。
Expiry Time（期限）	署名証明書が無効になる日付。期限が切れる前に証明書を更新するべきです。

自己証明書を CA が署名するようにリクエストするためには、識別子パラメータの入力をすることによって、ゲートウェイから証明書署名要求（CSR）を生成することができます。そして、署名のためにそれを CA に渡します。署名されると、CA からのトラスト証明書と署名証明書がアップロードされ、ゲートウェイのアイデンティティを有効にする自己証明書をアクティベートすることができます。自己証明書は、ゲートウェイの真正性を有効にするのにピアとの IPSec および SSL 接続に使用されます。

高度なスイッチ設定

ADVANCED > Switch Settings メニュー

DSR では、実際の利用に基づいてハードウェアの消費電力を調整できます。ご使用の LAN スイッチに利用可能な 2 つの「グリーン」オプションはリンクステータス とケーブル長検知ステータスによる省電力です。また、高度なスイッチ設定としてジャンボフレームをサポートしています。ジャンボフレームは 1500 バイト以上のペイロードを持つイーサネットフレームです。このオプションが有効な場合、LAN デバイスはジャンボレートで情報を交換することができます。

ルータの省電力およびジャンボフレームの有効化 / 無効化が可能です。

1. **ADVANCED > Switch Settings** の順にメニューをクリックし、以下の画面を表示します。

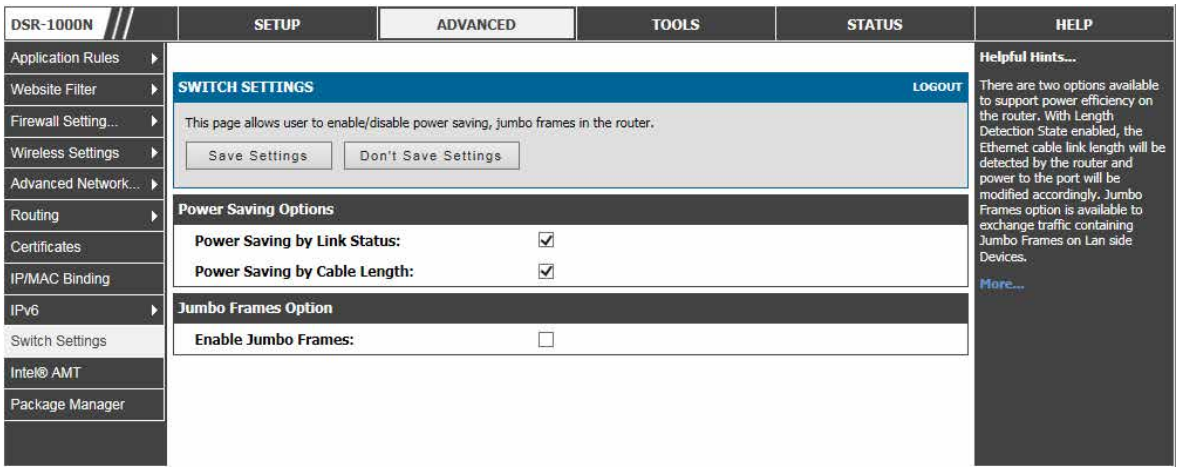


図 10-35　省電力およびジャンボフレーム設定 画面

2. 以下の項目を設定します。

項目	説明
Power Saving Options	
Power Saving by Link Status	有効にすると、LAN スイッチによる総消費電力は接続ポート数によって異なる機能となります。単一のポートが接続する場合、全体的な消費電流は全 LAN ポートが接続する場合より小さくなります。
Power Saving by Cable Length	有効にすると、LAN スイッチは短いケーブル長がそのポートに接続されている場合に LAN ポートに供給される全体的な消費電流を減少させます。
Jumbo Frames Options	
Enable Jumbo Frames	有効にすると、LAN 側デバイスはジャンボフレームを含むトラフィックを交換できます。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

第 11 章　システム管理

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

設定項目	説明	参照ページ
アクセスコントロールの設定	ユーザアクセスのコントロール設定をします。	182 ページ
SNMP 設定	SNMP 設定を行います。	184 ページ
タイムゾーンと NTP の設定	タイムゾーン、サマータイム、NTP サーバの設定をします。	186 ページ
ログ設定	ファイアウォール、VPN、および無線 AP を通じたトラフィックに対するログメッセージの取得と送信の設定を行います。	187 ページ
コンフィグレーションのバックアップと復元	コンフィグレーションファイルのバックアップと復元を行います。	193 ページ
DBGLOG の生成	ルータ問題を診断するためにデバッグログパッケージをダウンロードします。	194 ページ
ファームウェアのアップグレード	管理者 Web ページから新しいソフトウェアバージョンに更新します。	195 ページ
USB 経由のルータのファームウェア更新	USB メモリを使用したファームウェアのアップグレード、コンフィグレーションのバックアップと復元を行います。	196 ページ
ダイナミック DNS の設定	ダイナミック DNS サービスの設定を行います。	197 ページ
診断ツールの使用	診断ツールを使用して通信状態と総合的なネットワークの健全性を評価します。	198 ページ

アクセスコントロールの設定

プライマリは独立したブラウザの GUI を経由してこのゲートウェイを設定することを意味します。GUI はゲートウェイの LAN IP アドレスと HTTP を使用することで LAN ノードから、または、ゲートウェイの WAN IP アドレスと HTTPS（HTTP over SSL）を使用することで WAN から GUI にアクセスすることができます。

IP ポリシーの設定

IP にグループにポリシーを設定します。

1. **SETUP > Internal Users Data > Groups** で対応するグループを選択し、「Login Policies」ボタンをクリックして、以下の画面を表示します。

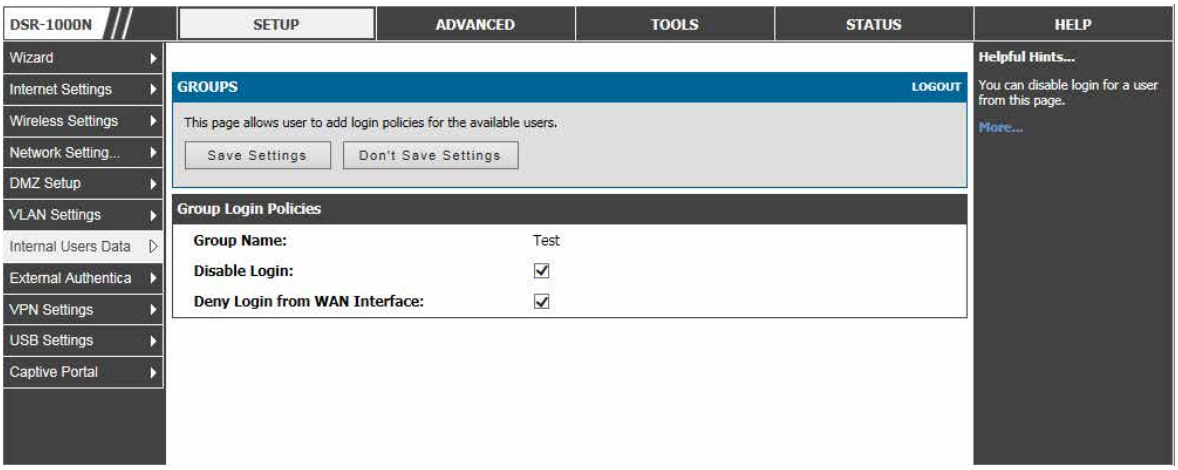


図 11-1　グループログインポリシーオプション

2. 以下の項目を設定します。

項目	説明
Group Name	ログインポリシーを編集できるグループ名を表示します。
Disable Login	チェックすると、本グループ内のユーザのデバイスにおける管理インタフェースへのログインを防止することができます。
Deny Login from WAN Interface	チェックすると、このグループのユーザが WAN（広域ネットワーク）インタフェースからログインするのを防止することができます。この場合、LAN を通したログインだけが許可されます。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

Admin 設定

TOOLS > Admin > Admin Settings メニュー

ルータの識別子名を設定します。

1. **TOOLS > Admin > Admin Settings** の順にメニューをクリックし、以下の画面を表示します。

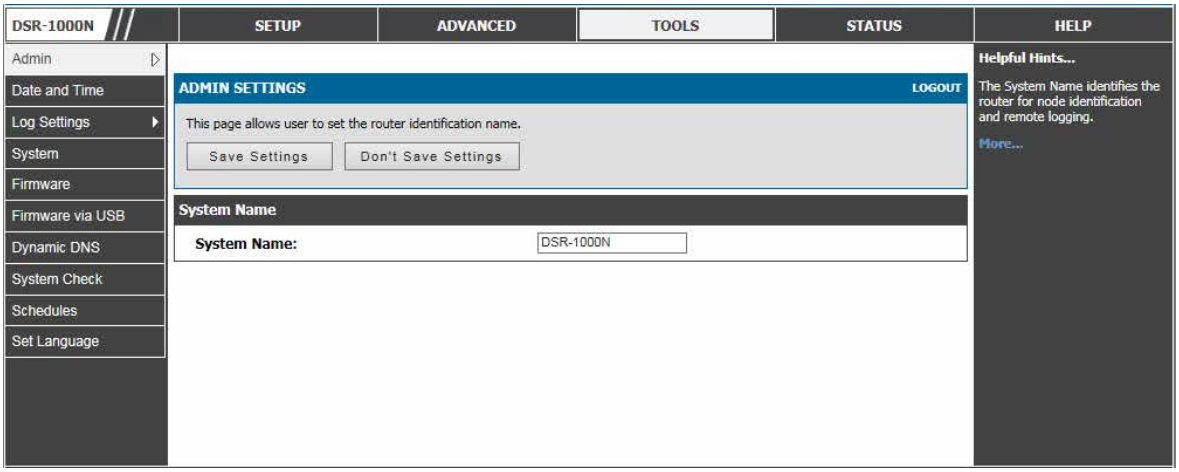


図 11-2　Admin Settings 画面

2. 以下の項目を設定および表示します。

項目	説明
System Name	これはルータの識別子であり、「status summary」ページに表示されます。

3. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

リモート管理

TOOLS > Admin > Remote Management メニュー

HTTPS と telnet アクセスの両方を IP アドレスのサブセットに制限します。

1. **TOOLS > Admin > Remote Management** の順にメニューをクリックし、以下の画面を表示します。

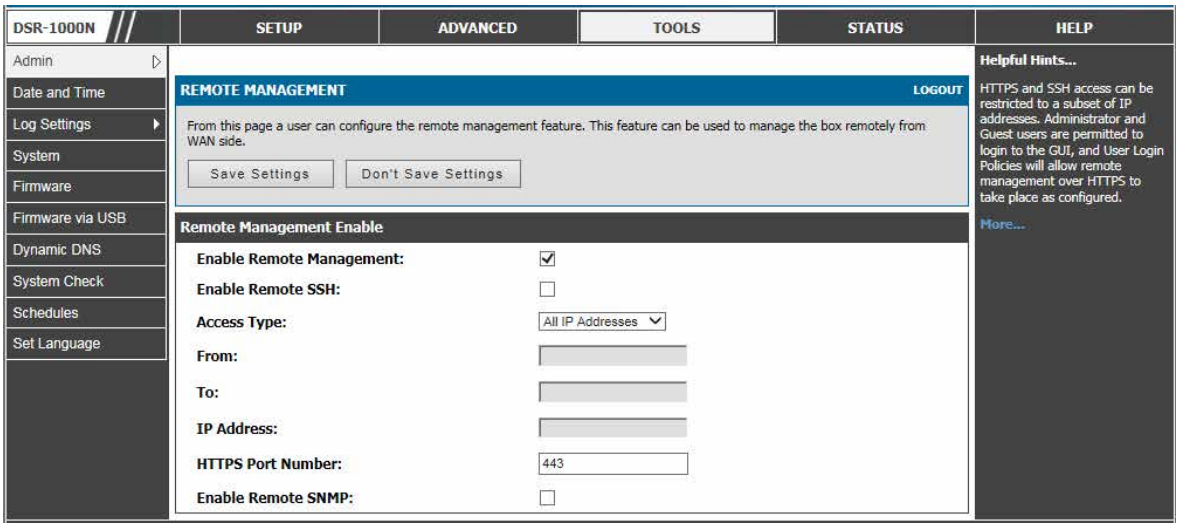


図 11-3　WAN からのリモート管理

ルータ管理者は HTTPS を使用して GUI にアクセスできる既知の PC、IP アドレスまたは IP アドレス範囲を定義できます。許可されるリモート管理の IP アドレス範囲を定義するのと同時に、SSL トラフィックのためにオープンされるポートを初期値の 443 から変更することができます。

CLI アクセス

Web ベースの GUI に加えて、ゲートウェイは、コマンドラインによる対話のために SSH と Telnet 管理をサポートしています。CLI ログイン証明書は管理者ユーザ用の GUI で共有されます。CLI にアクセスするためには、SSH またはコンソールのプロンプトで「cli」を入力し、管理者ユーザ権限でログインします。

SNMP 設定

TOOLS > Admin > SNMP メニュー

SNMP（Simple Network Management Protocol）により SNMP マネージャからルータをモニターおよび管理できます。SNMP はネットワーク装置をモニターおよび制御するため、また、設定、統計情報の収集、性能、およびセキュリティを管理するためのリモート手段を提供します。

SNMP は、ネットワーク内の複数のルータが中央のマスタシステムに管理されている場合に便利な管理ツールです。外部の SNMP マネージャにこのルータの MIB（Management Information Base）ファイルを提供する場合、マネージャは、構成パラメータの参照または更新のためにルータの階層変数を更新できます。管理されるデバイスとしてのルータは、マスタ（SNMP マネージャ）によって MIB 設定変数がアクセスされるのを許可する SNMP エージェントを搭載しています。ルータのアクセスコントロールリストは読み出し用または読み書き用の SNMP 権限を持つネットワーク内のマネージャを識別します。「Traps List」セクションはこのルータからの通知が SNMP コミュニティ（マネージャ）に提供されるポートとトラップ用の SNMP バージョン（v1、v2c、v3）について概説します。

1. **TOOLS > Admin > SNMP** の順にメニューをクリックし、以下の画面を表示します。

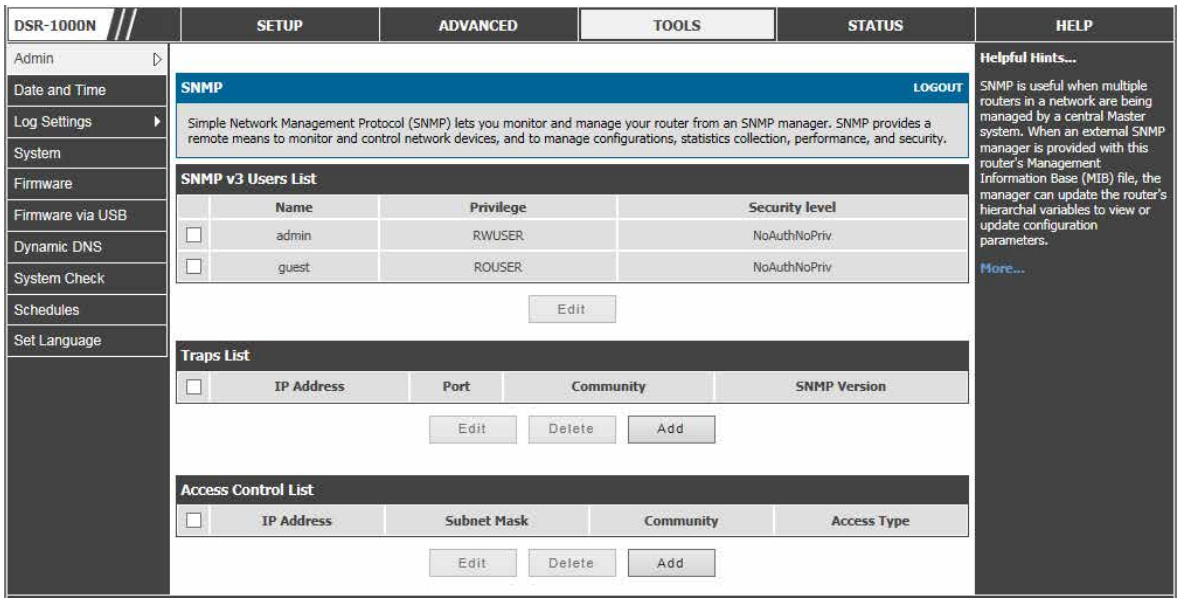


図 11-4　SNMP ユーザ、トラップ、およびアクセスコントロール

トラップの追加

1. 「Traps List」セクションの「Add」ボタンをクリックして、以下の画面を表示します。

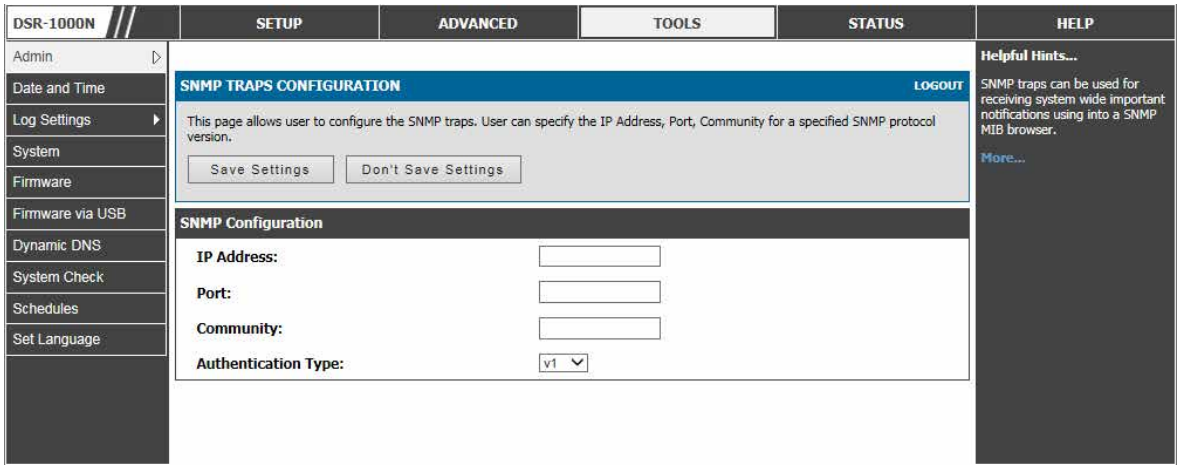


図 11-5　トラップの設定画面

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

アクセスコントロールリストの追加

1. 「Access Control List」セクションの「Add」ボタンをクリックして、以下の画面を表示します。

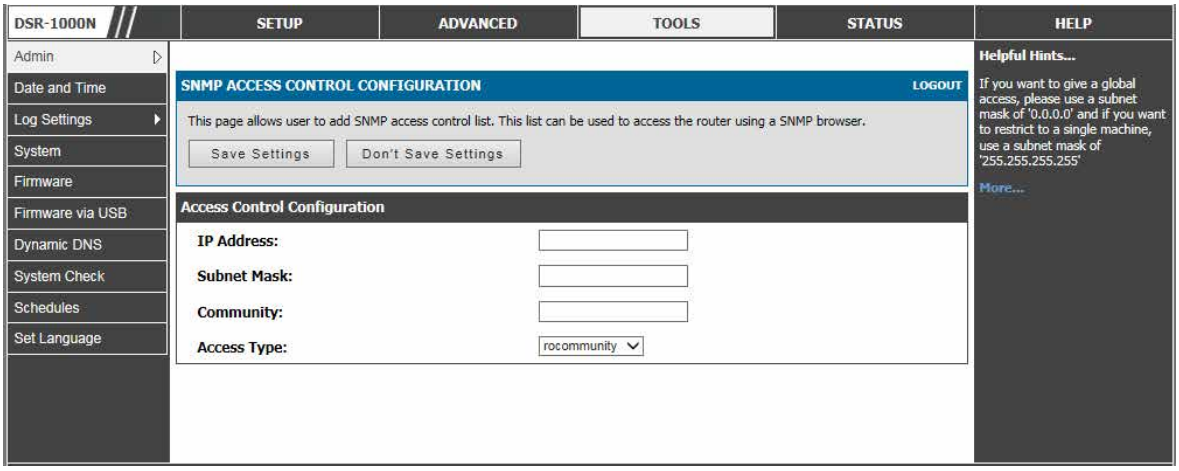


図 11-6　アクセスコントロールリストの設定画面

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

システム名の設定

TOOLS > Admin > SNMP System Info メニュー

ここではルータの現在の SNMP 設定を表示します。以下の SNMP（Simple Network Management Protocol）欄が表示され、ここで変更できます。

ルータはシステム情報を介して SNMP マネージャによって特定されます。また、ここで設定するシステム名は、SysLog 出力のためにルータを識別するために使用されます。

1. **TOOLS > Admin > SNMP System Info** の順にメニューをクリックし、以下の画面を表示します。

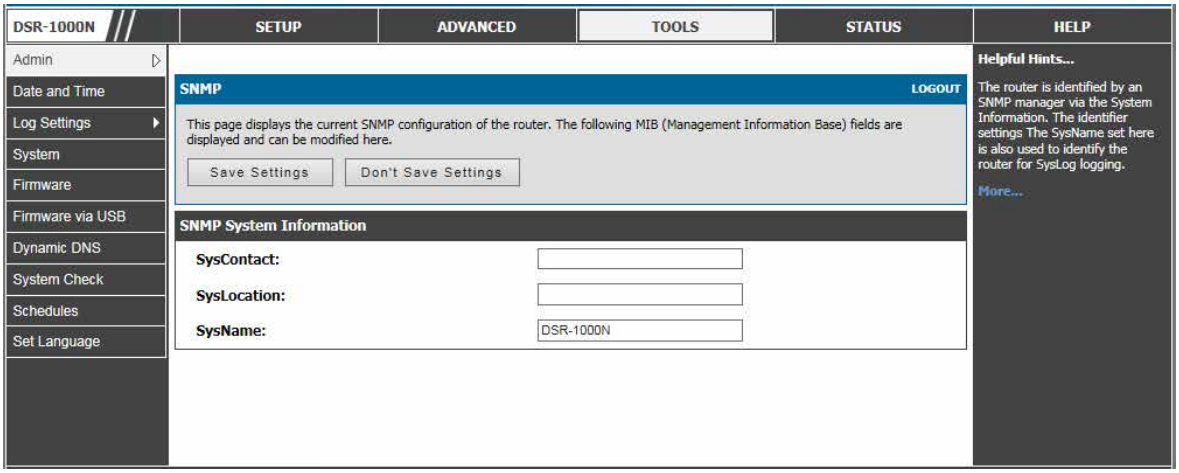


図 11-7　このルータの SNMP システム情報

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

タイムゾーンと NTP の設定

TOOLS > Date and Time メニュー

タイムゾーン、サマータイム（Daylight Savings Time）の調整の有無、日時を同期する NTP（Network Time Protocol）サーバの使用について設定することができます。手動設定で「日付と時間」を入力することもできます。これは、ルータの RTC（Real Time Clock）に情報を保存します。ルータがインターネットにアクセスする場合、ルータ時間を設定する最も正確なメカニズムは、NTP サーバ通信を有効にすることです。

注意 ルータの正確な日時はファイアウォールスケジュール、1 日の指定時間に AP を無効にする Wi-Fi 省電力サポート、および正確なログの出力のために非常に重要です。

以下の手順に従って NTP サーバを設定します。:

1. **TOOLS > Date and Time** の順にメニューをクリックし、以下の画面を表示します。

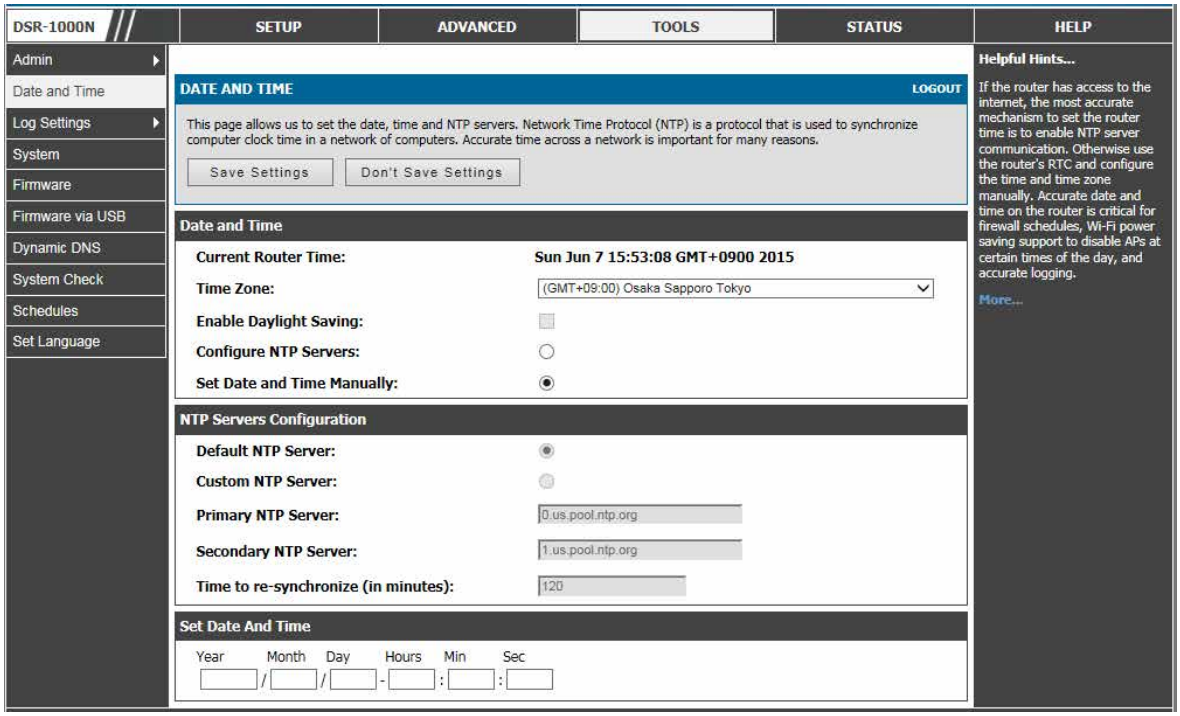


図 11-8　日付、時間、および NTP サーバ設定

2. グリニッジ標準時（GMT）に対するルータのタイムゾーンを選択します。

3. NTP サーバをサポートする場合、「Configure NTP Servers」をクリックします。

4. 「Default NTP Server」または「Custom NTP Server」の使用の有無を決定します。「Custom」の場合、サーバのアドレスまたは FQDN を入力します。

ログ設定

本ルータは、ファイアウォール、VPN、および無線 AP を通じたトラフィックに対するログメッセージを取得することができます。ログメッセージがルータによって検出されると、管理者として、ルータを通過するトラフィックタイプをモニターして、潜在的な攻撃またはエラーについて通知することができます。以下のセクションはログ構成設定とそれらのログにアクセスする方法を述べています。

ログに出力するものを定義する

TOOLS > Log Settings > Logs Facility メニュー

ルータから受信するログのレベルを決定することができます。

1. **TOOLS > Log Settings > Logs Facility** の順にメニューをクリックし、以下の画面を表示します。

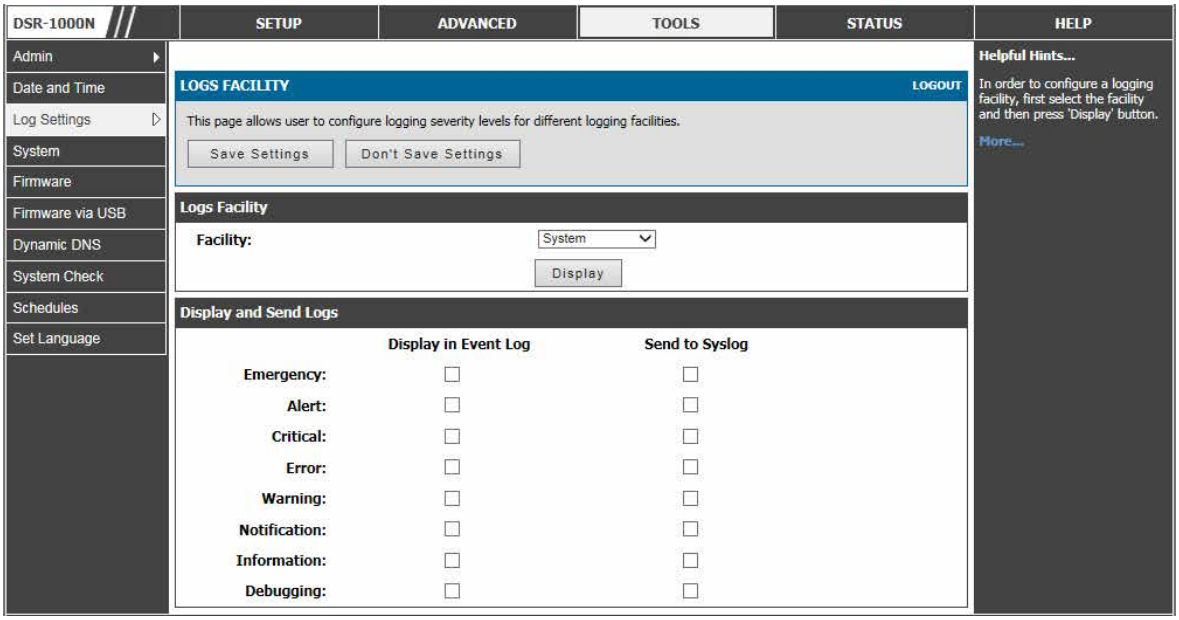


図 11-9　ログ出力のためのファシリティ設定

ファシリティとして参照されるルータのコアコンポーネントがあります。:

項目	説明
Kernel	Linux カーネルを参照します。このファシリティに対応するログメッセージは、ファイアウォールまたはネットワークスタックを通してトラフィックに対応します。
System	ユニット管理のために SSL VPN や管理者の変更を含む本ルータで利用可能なアプリケーションおよび管理レベル機能を参照します。
Local0-wireless	このファシリティは AP 機能をご使用のネットワークに提供するのに使用される 802.11 ドライバに対応します。
Local1-UTM	このファシリティは WAN からの悪意ある侵入攻撃を検知する IPS（Intrusion Prevention System）に対応しています。

各ファシリティにおいて、以下のイベント（セベリティの順）がログに出力されます。: Emergency、Alert、Critical、Error、Warning、Notification、Information、Debugging。セベリティレベルが選択される場合、選択されたセベリティ以上のセベリティを持つすべてのイベントがキャプチャされます。例えば Wireless ファシリティに CRITICAL レベルのログ出力が設定されていると、セベリティレベル CRITICAL、ALERT、および EMERGENCY を持つ 802.11 のログがログに出力されます。ログ出力に使用可能なセベリティレベルは以下の通りです。:

項目	説明
Emergency	システムは使用不能です。
Alert	すぐに、アクションを行う必要があります。
Critical	非常に危険な状態。
Error	エラー状態。
Warning	注意すべき状態。
Notification	標準ではあるが注意すべき状態。
Information	情報。
Debugging	デバッグレベルのメッセージ。

ログの表示は、後で確認するためにログが送信される場所、GUI 内のイベントログビューワ（**STATUS > Logs** ページにある）、またはリモート Syslog サーバのいずれかに基づいてカスタマイズされます。続くセクションで記述されるメールログは、Syslog サーバに設定されたログと同じ設定が続きます。

トラフィック対応の設定

IPv4 トラフィックのログ設定

TOOLS > Log Settings > Logs Configuration メニュー

ここでは Syslog、メールログ、イベントビューワへの表示のためにログ出力されるルータを通したトラフィックのタイプを決定することができます。DoS（Denial of Service）攻撃、一般的な攻撃情報、ログインの試み、破棄されたパケットなどのイベントを、IT 管理者による確認のために取得することができます。

ファイアウォールがパケットを受け付けたか、または破棄したかに基づいて各ネットワークセグメント（LAN、WAN、DMZ）を通じたトラフィックを追跡することができます。

受け付けたパケットは、対応するネットワークセグメント（LAN から WAN）を通じて転送に成功したものです。このオプションはデフォルトの外向きポリシーが「Always Block」（常にブロック）の場合に特に便利です。そのため、IT 管理者はファイアウォールを通過するトラフィックをモニターすることができます。

1. **TOOLS > Log Settings > Logs Configuration** の順にメニューをクリックし、以下の画面を表示します。

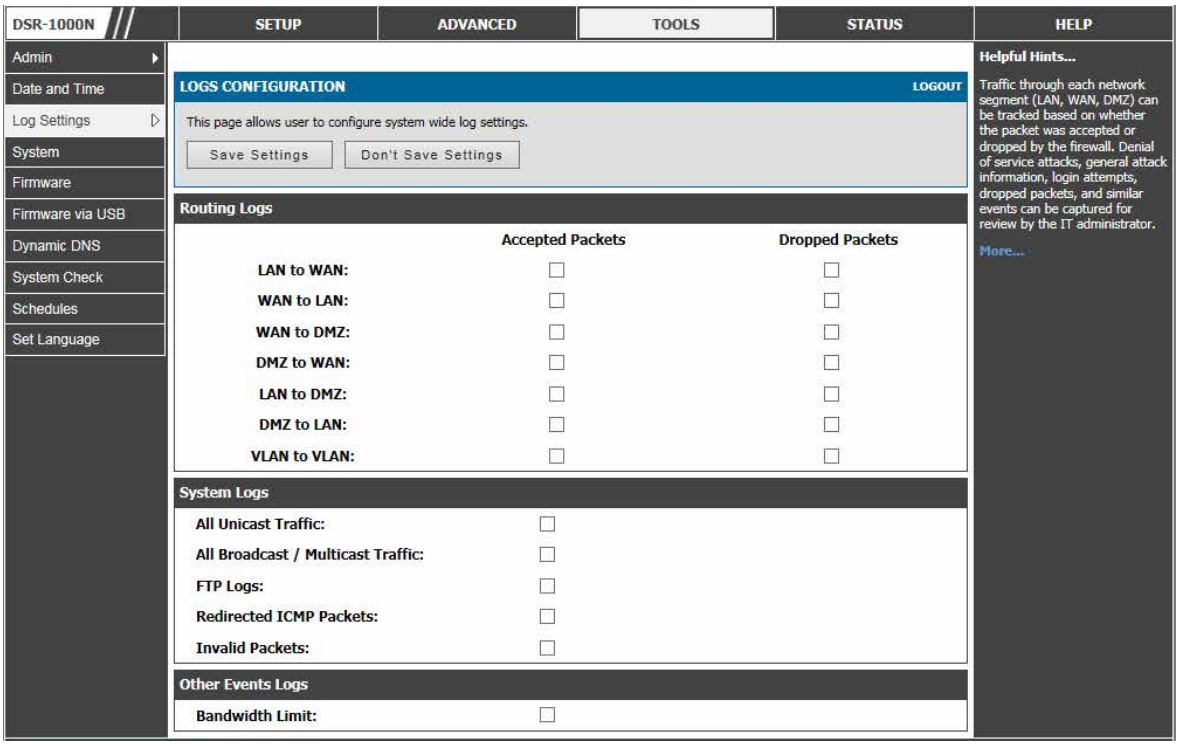


図 11-10　ルータを経由するトラフィックのためのログ設定オプション

例：

LAN から WAN までの「Accepted Packets」（パケットの許可）が有効にされて、LAN からの SSH トラフィックを許可するファイアウォールルールがあると、LAN マシンが SSH 接続を試みる場合にはいつも、それらのパケットを受け付けて、メッセージをログに出力します。（ログオプションが SSH ファイアウォールルールに対して「Allow」（許可する）に設定されているものとします。）

「Dropped Packets」は、対応するネットワークセグメント経由の転送から意図的にブロックされたパケットです。このオプションはデフォルトの外向きポリシーが「Allow Always」（常に許可）の場合に便利です。

例：

LAN から WAN までの「Dropped Packets」（パケットの破棄）が有効にされて、LAN からの SSH トラフィックをブロックするファイアウォールルールがあると、LAN マシンが SSH 接続を試みる場合にはいつも、それらのパケットを破棄して、メッセージをログに出力します。（ログオプションがこのファイアウォールルールに対して許可するように設定されていることを確認してください。）

注意　ファイアウォールを通じて受け付けるパケットのログ出力を有効にすると、典型的なネットワークトラフィックによって相当な量のログメッセージが生成される可能性があります。これはデバッグ目的だけとすることをお勧めします。

ネットワークセグメントのログ出力に加えて、ユニキャストおよびマルチキャストトラフィックをログに出力することができます。ユニキャストパケットはネットワークに単一の宛先を持っていますが、ブロードキャスト（マルチキャスト）パケットはすべての可能な宛先に同時に送信されます。
他の役に立つログ制御は、特定のインタフェース上に設定した帯域幅プロファイルのために破棄されるパケットをログに出力することです。このデータは、LAN ユーザに必要なインターネットトラフィックのためのアカウントに対する帯域幅プロファイルを変更する必要があるかどうかを管理者に示します。

IPv6 トラフィックのログ設定

TOOLS > Log Settings > IPv6 Logging メニュー
本ページでは、IPv6 ログの出力を設定できます。

1. **TOOLS > Log Settings > IPv6 Logging** の順にメニューをクリックし、以下の画面を表示します。

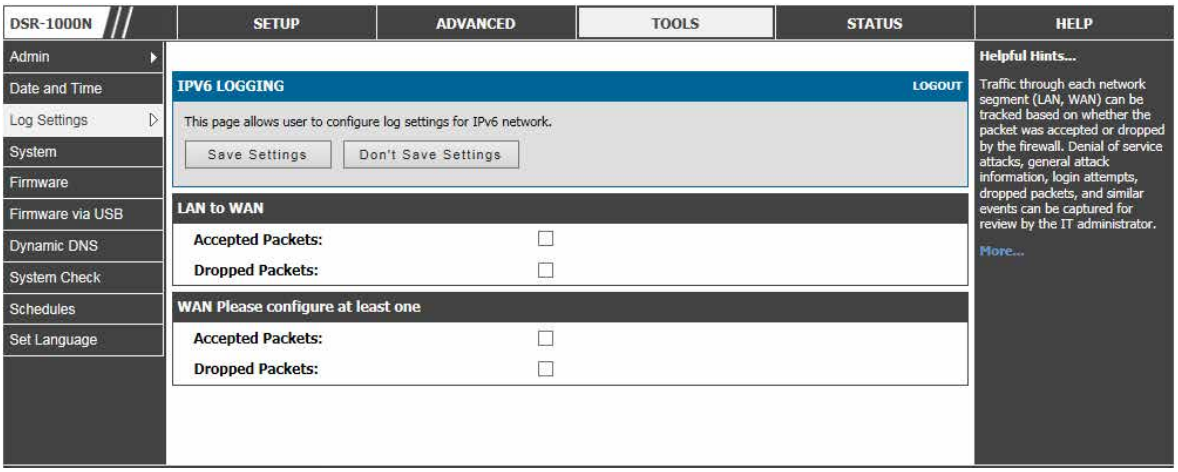


図 11-11　ルータを経由するトラフィックのための IPv6 ログ設定オプション

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

メールまたは Syslog に送信するログ

TOOLS > Log Settings > Remote Logging メニュー

ここでは、ルータにリモートログ出力オプションを設定することができます。

ルータに取得を希望するログのタイプを設定すると、ログは Syslog サーバまたはメールアドレスのどちらかに送信されます。

1. **TOOLS > Log Settings > Remote Logging** の順にメニューをクリックし、以下の画面を表示します。

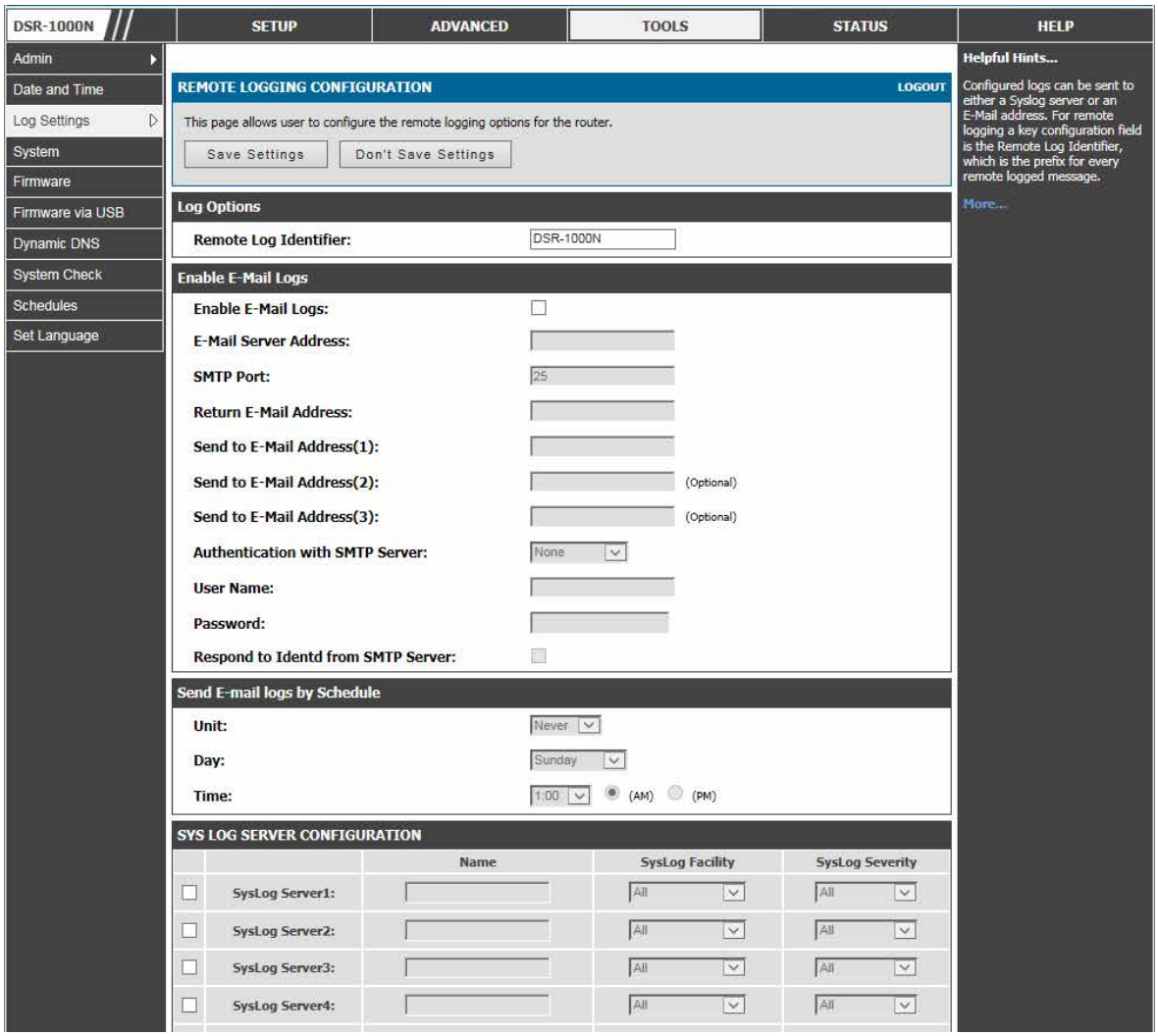


図 11-12　リモートログ出力オプションとしてのメール設定

リモートログ出力のための主要な構成欄は「Remote Log Identifier」（リモートログ識別子）です。1 つ以上のルータからログを受信する Syslog サーバまたはメールアドレスが、関連デバイスのログのためにソートできるように、すべてのログ出力メッセージには「Remote Log Identifier」の設定済みプレフィックスを含んでいます。

メールログに対してオプションを有効にしたら、SMTP サーバの E メールアドレス（IP アドレスまたは FQDN）を入力します。メールを設定したアドレスに送信する場合、ルータはこのサーバに接続します。SMTP ポートと返信メールアドレスは、ルータがログをパッケージして、設定した「Send-to」アドレスの 1 つが受け付ける有効なメールを送信するために必要な欄です。ログ受信者として最大 3 つのメールアドレスを設定できます。

設定された SMTP ポートとサーバで通信を確立するために、サーバの認証要求を定義します。ルータは、ユーザ名とパスワードデータを SMTP サーバに送信するために、「Login Plain」（暗号化しない）または「CRAM-MD5」（暗号化）をサポートしています。サーバにこの必要がない場合、認証を「None」（無効）にすることができます。いくつかの場合、SMTP サーバは IDENT 要求を出し、このルータでは、必要に応じてこの応答オプションを有効にすることができます。メールサーバと受信者の詳細が定義されると、ルータがログをいつ送信するべきであるかを決定することができます。最初に選択したユニットの定義済みログ送信スケジュールに基づいてメールのログを送信することができます。: Hourly（時間）、Daily（日）、または Weekly（週）。「Never」を選択するとログのメールを無効にしますが、メールサーバ設定は保存します。

外部の Syslog サーバは、ルータからログを集めて、保存するのにネットワーク管理者によって度々使用されます。このリモートデバイスは、通常、ルータの GUI にローカルなイベントビューワよりメモリの制限が少ないため、持続している期間は大量のログを収集することができます。通常、これは、デバッグネットワーク問題や長期間ルータトラフィックをモニターするために非常に役に立ちます。

このルータは並行して最大 8 つの Syslog サーバをサポートし、各サーバは様々なセベリティレベルのログファシリティメッセージを受信するために設定されます。Syslog サーバを有効にするために、Syslog サーバ欄横のボックスをチェックし、「Name」欄に IP アドレスまたは FQDN を割り当てます。この設定を保存すると、設定した（および有効にした）Syslog サーバに選択されたファシリティとセベリティレベルのメッセージを送信します。

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

GUI におけるイベントログビューワ

STATUS > Logs > View All Logs メニュー

「STATUS」メニューから設定したログメッセージをモニターできます。

ルータを通過する、またはルータに向かうトラフィックが **TOOLS > Log Settings > Logs Facility** または **TOOLS > Log Settings > Logs Configuration** ページで設定した内容に一致する場合、対応するログメッセージがタイムスタンプと共に本画面に表示されます。

1. **STATUS > Logs > View All Logs** の順にメニューをクリックし、以下の画面を表示します。

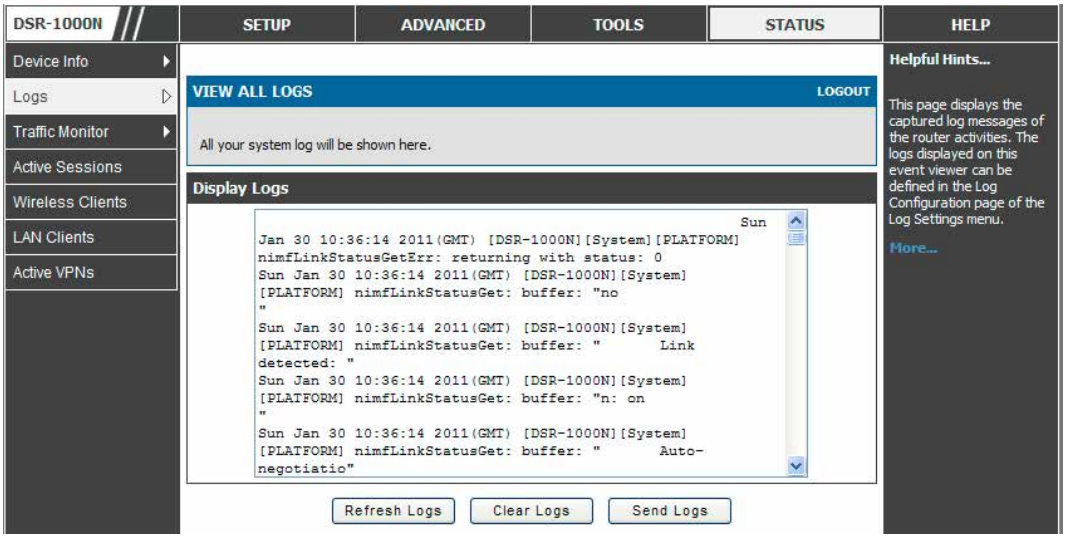


図 11-13 View All Logs 画面

注意 正確なシステム時間（マニュアル設定、または NTP サーバからの取得）を持つことが、ログメッセージを理解するために非常に重要です。

STATUS > Logs > VPN Logs メニュー

ファシリティおよびセベリティレベルの設定によって決定されるようなIPSec VPNログメッセージを表示します。このデータは、IPSec VPNトラフィックとトンネルの健全性を評価する場合に役に立ちます。

1. **STATUS > Logs > VPN Logs** の順にメニューをクリックし、以下の画面を表示します。

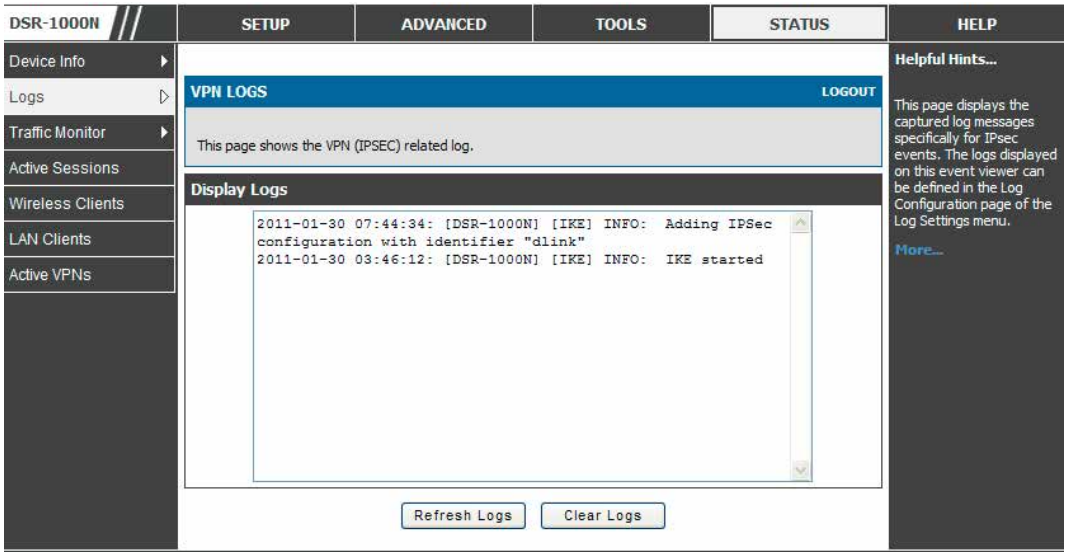


図 11-14 GUI イベントビューワに表示された VPN ログ

「Refresh Logs」ボタンをクリックして、ページがオープンした後に追加されたエントリを参照します。
「Clear Logs」ボタンをクリックして、「Display Logs」内のすべてのエントリをクリアします。

コンフィグレーションのバックアップと復元

TOOLS > System メニュー

コンフィグレーションのバックアップ、復元、および工場出荷時設定を含む構成に関連する操作をします。

ルータのカスタム構成設定をバックアップして、何らかの変更後に異なるデバイスまたは同じルータにそれらを復元することができます。バックアップ中、ご使用の設定はご使用のホストのファイルとして保存されます。同様にこのファイルからルータの保存された設定を復元できます。また、本ページでは工場出荷時設定の回復またはルータのソフトリブートを実行することができます。本ページでは、ルータ問題を診断するために D-Link サポートに有益なシステムステータス、統計情報、およびログをグループ化した dbglog パッケージのダウンロードや自動バックアップの設定もできます。

1. **TOOLS > System** の順にメニューをクリックし、以下の画面を表示します。

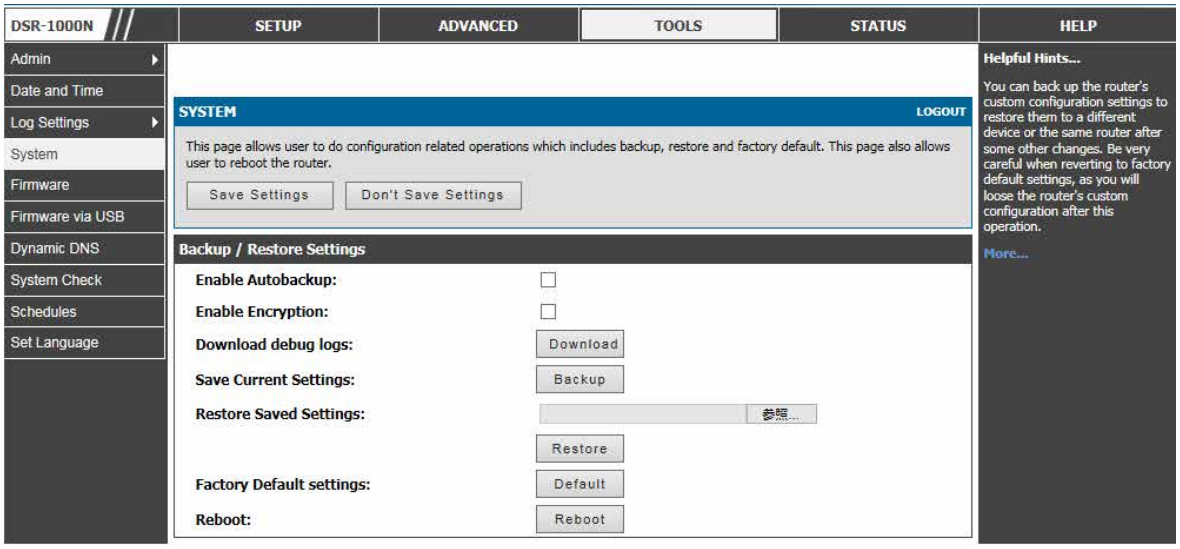


図 11-15　SYSTEM 画面

注意 復元操作の間、操作が完全に終了するまで、次の項目を守ってください。: オンラインにしない。ルータの電源を切らない。PC をシャットダウンしない。または、ルータに何もしないでください。これには約 1 分かかります。LED の消灯後、ルータが何かを実行するまで、もう数秒お待ちください。

コンフィグレーションのバックアップ、または保存済みコンフィグレーションの復元のためには、以下の手順に従います。:

1. 現在の設定のコピーを保存するために、「Save Current Settings」オプションで「Backup」ボタンをクリックします。ブラウザはコンフィグレーションファイルのエクスポートを開始して、ご使用のホストにファイルを保存するように入力を促します。

2. 現在システムに挿入されている USB ストレージデバイスがある場合、USB ファイルシステムへのコンフィグレーションファイルの自動バックアップを有効にできます。現在のコンフィグレーションのスナップショットは、USB ファイルシステムにアップロードされて、同じファイル名を持つどんなファイルも上書きします。（つまり、ここでバックアップされた以前のコンフィグレーションファイルがある場合）

3. バックアップファイルから保存した設定を復元するためには、「参照」ボタンをクリックしてホスト上のファイルの位置を示します。「Restore」ボタンをクリックした後に、ルータは保存されたコンフィグレーション設定のインポートを開始します。復元後、ルータは復元された設定で自動的に再起動されます。

4. 現在の設定を削除し、工場出荷時設定を回復するためには「Default」ボタンをクリックします。ルータは、次に、コンフィグレーション設定を工場出荷時設定に復元して、自動的に再起動されます。（ルータの工場出荷時設定パラメータについては付録 B を参照してください。）

暗号化が有効であると、バックアップ処理でコンフィグレーションファイルを暗号化できます。これは、システムユーザ名 / パスワードのような機密情報が権限を持たないソースによって参照できないことを保証します。本オプションを選択すると、USB ドライブをはじめとしてホストにバックアップされるコンフィグレーションファイルに適用されます。

DBGLOG の生成

Tools > System メニュー
ルータ問題を診断するために D-Link サポートに有益なシステムステータス、統計情報、およびログをグループ化したデバッグログ（dbglog）パッケージのダウンロードや自動バックアップの設定ができます

デバッグログのダウンロードリンクをクリックすると、このルータを管理するのに使用されるホストマシンにパッケージは保存されます。そして、このパッケージ (圧縮されたアーカイブ) を評価用に D-Link のサポートに送信することができます。

1. **TOOLS > System** の順にメニューをクリックし、以下の画面を表示します。

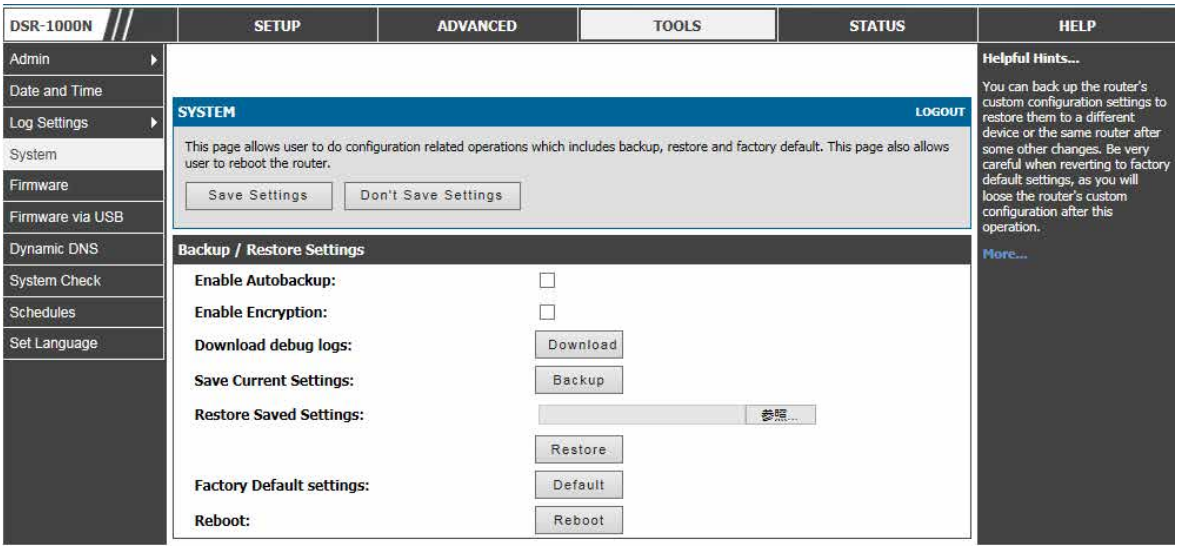


図 11-16　SYSTEM 画面

2. 「Download debug logs」で「Download」ボタンをクリックして、アーカイブファイルを保存します。

ファームウェアのアップグレード

ローカルまたは Web ページを利用したアップグレード

TOOLS > Firmware メニュー

管理者 Web ページから、新しいソフトウェアバージョンにアップグレードすることができます。

1. **TOOLS > Firmware** の順にメニューをクリックし、以下の画面を表示します。

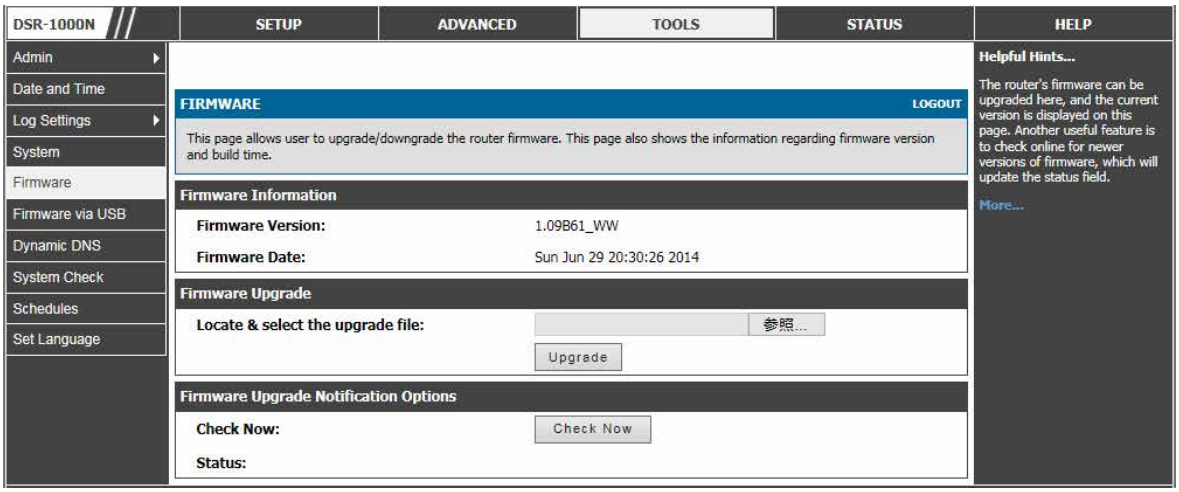


図 11-17　ファームウェアバージョン情報とアップグレードオプション

「Firmware Upgrade」セクションでは、ファームウェアをアップグレードするために、「参照」ボタンをクリックし、ホスト上のファームウェアイメージの場所を選択して「Upgrade」ボタンをクリックします。

新しいファームウェアイメージが有効にされた後に、新しいイメージはフラッシュメモリに書かれ、ルータは新しいファームウェアで自動的に再起動されます。「Firmware Information」および **STATUS > Device Info > Device Status** ページに新しいファームウェアバージョンを反映します。

注意 アップグレード操作の間、操作が完全に終了するまで、次の項目を守ってください。: オンラインにしない。ルータの電源を切らない。PC をシャットダウンしない。または、いずれにしろ処理を中断しないでください。これには再起動処理も含めて 1 分ほどかかります。フラッシュメモリは、（Web GUI を経由しないで）フラッシュのファームウェアを回復する低レベルの処理であるため、改悪されたり、ルータを無効にするように上書きされると、特定の時点でアップグレード処理を中断します。

また、このルータは、より新しいファームウェアバージョンがこのルータに利用可能であるかどうか判断するために自動通知をサポートしています。通知セクションで「Check Now」ボタンをクリックすると、このルータのファームウェアのより最新のバージョンが有効かどうかを参照するために D-Link サーバをチェックして、画面下にある「Status」欄を更新します。

注意 重要！

ファームウェア 1.04B13 以降で、新しいユーザデータベースアーキテクチャを導入しています。新しいユーザデータベースはセットアップがより簡単で、より直観的に使用できます。DSR のファームウェアを 1.04B13 以降にアップグレードする場合、DSR は古いデータベースのユーザを自動的に新しいデータベースに組み入れます。

しかし、ファームウェアを 1.04B13 から古いバージョン（例 1.03B43）にダウングレードすると、すべてのユーザデータベースが破棄されます。ファームウェアを古いものにダウンロードすると決定した後、今後の復元のためにユーザデータベースをバックアップしてください。

USB 経由のルータのファームウェア更新

USB メモリを利用したアップグレード

TOOLS > Firmware via USB メニュー

USB メモリを使用したファームウェアのアップグレード、コンフィグレーションのバックアップと復元を行うことができます。

1. **TOOLS > Firmware via USB** の順にメニューをクリックし、以下の画面を表示します。

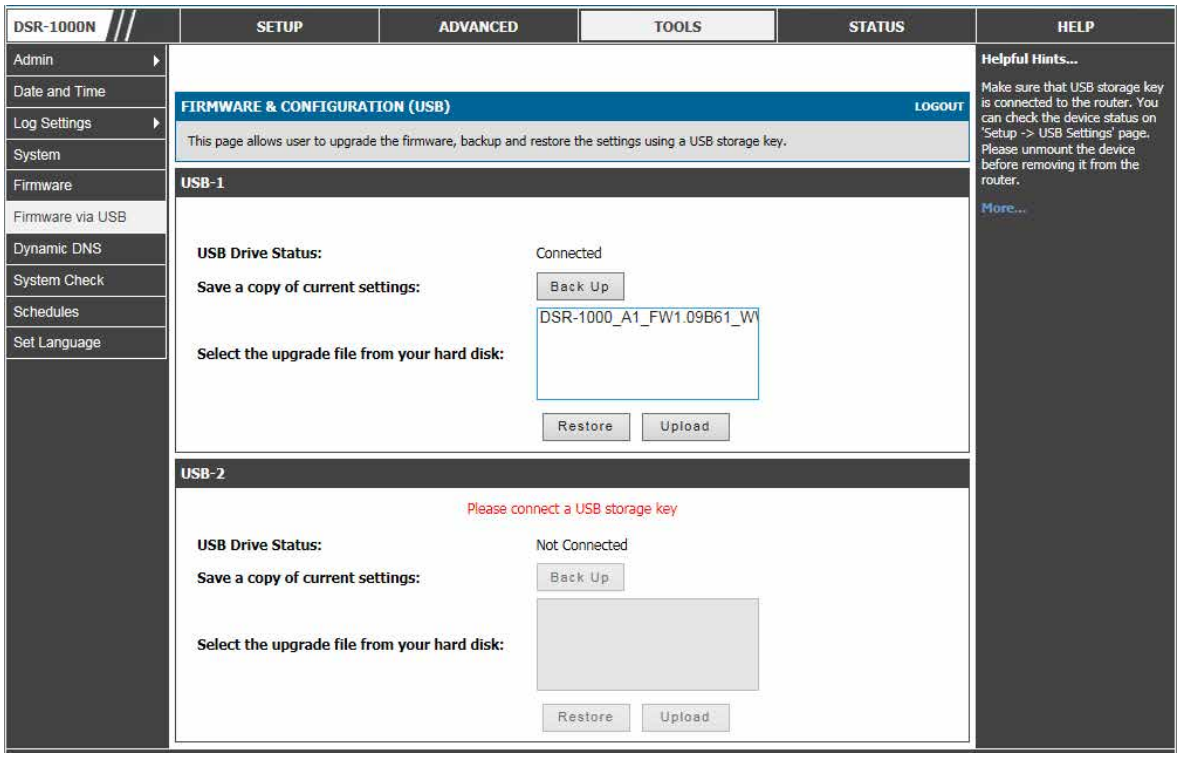


図 11-18 USB を使用したファームウェアバージョンとアップグレードオプション

注意 USB メモリがルータに接続していることを確認してください。**SETUP > USB Settings > USB Status** ページでデバイスのステータスをチェックすることができます。ルータからそれを取り外す前に、デバイスのマウントを解除してください。

2. 以下の項目を実行します。

項目	説明
Backup	コンフィグレーションが保存されます。
Restore	復元するファイルをフルパスで指定し、このボタンをクリックします。
Upload	更新するファームウェアファイルをフルパスで指定し、このボタンをクリックします。

3. 新しいファームウェアイメージが有効にされた後に、新しいイメージはフラッシュメモリに書かれ、ルータは新しいファームウェアで自動的に再起動されます。「Firmware Information」および **STATUS > Device Info > Device Status** ページに新しいファームウェアバージョンを反映します。

注意 アップグレード操作の間、操作が完全に終了するまで、次の項目を守ってください。: オンラインにしない。ルータの電源を切らない。PC をシャットダウンしない。または、いずれにしろ処理を中断しないでください。これには再起動処理も含めて 1 分ほどかかります。フラッシュメモリは、（Web GUI を経由しないで）フラッシュのファームウェアを回復する低レベルの処理であるため、改悪されたり、ルータを無効にするように上書きされると、特定の時点でアップグレード処理を中断します。

ダイナミック DNS の設定

TOOLS > Dynamic DNS メニュー
ダイナミック DNS を設定します。

ダイナミック DNS（DDNS）は、変化するパブリック IP アドレスを持つルータがインターネットのドメイン名を使用して設置できるインターネットのサービスです。DDNS を使用するためには、DynDNS.org、DlinkDDNS.com または Oray.net などの DDNS プロバイダでアカウントをセットアップする必要があります。必要であれば、各設定済み WAN は異なる DDNS サービスを持つことができます。

設定後、ルータは、FQDN 経由でルータの WAN にアクセスするのに依存する機能が正しい IP アドレスに向けられるように、WAN IP アドレスにおける DDNS サービスの変更を更新します。DDNS サービス、ホスト、およびドメイン名でアカウントをセットアップする場合、ユーザ名、パスワード、およびワイルドカードのサポートはアカウントプロバイダによって提供されます。

1. **TOOLS > Dynamic DNS** の順にメニューをクリックし、以下の画面を表示します。

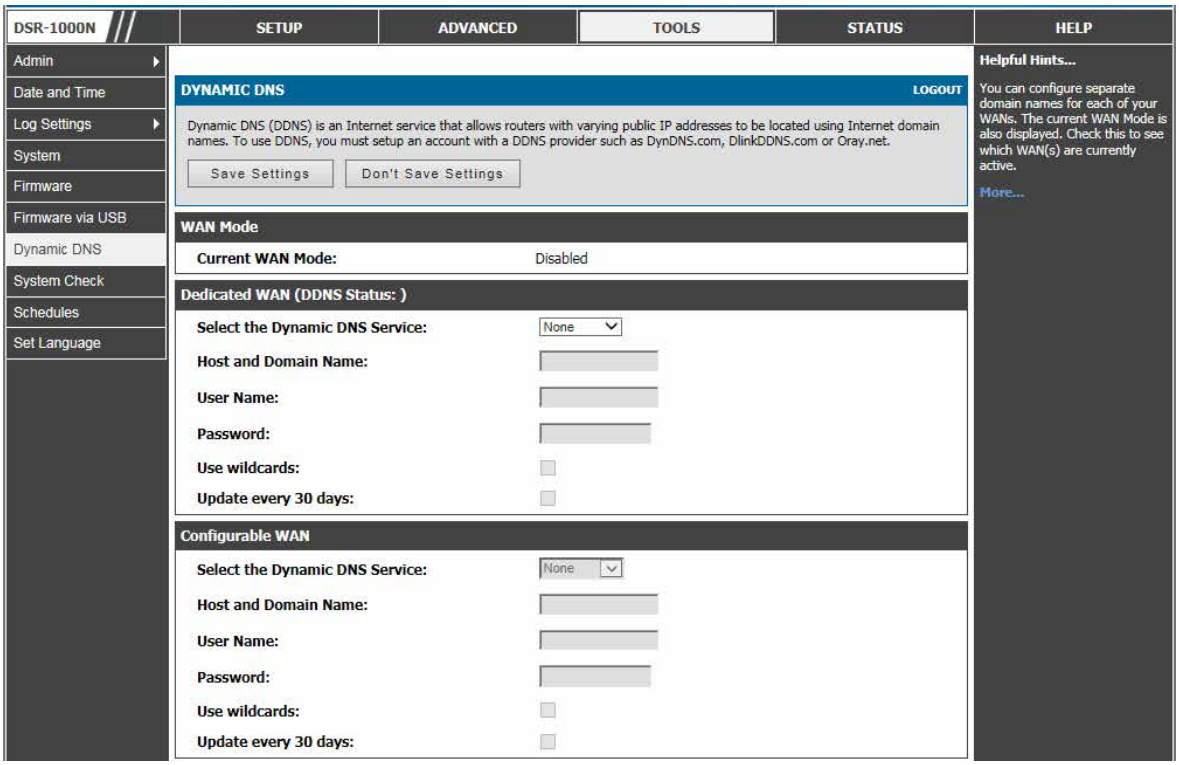


図 11-19 DYNAMIC DNS の設定

2. 項目を設定後、「Save Settings」ボタンをクリックして設定内容を保存および適用します。

診断ツールの使用

TOOLS > System Check メニュー
本ページは診断の目的で使用できます。

ルータには、管理者が通信ステータスと総合的なネットワークの健全性を評価できるツールが実装されています。

1. **TOOLS > System Check** の順にメニューをクリックし、以下の画面を表示します。

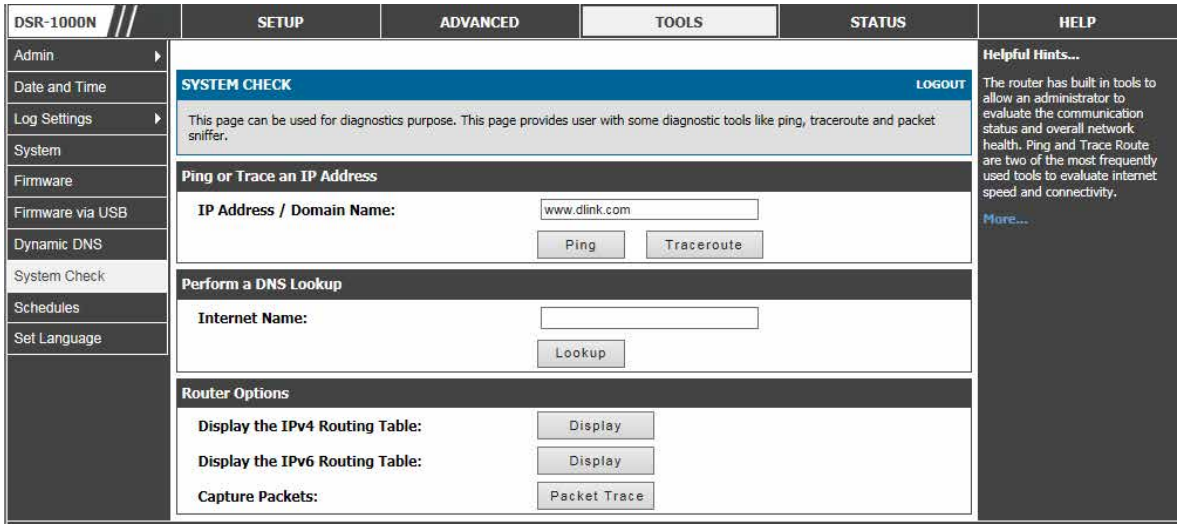


図 11-20 GUI で利用可能なルータ診断ツール

Ping

このユーティリティは、このルータとこれに接続するネットワーク上の別のデバイス間の接続性をテストするのに使用されます。IP アドレスを入力して、「Ping」ボタンをクリックします。コマンド出力は、ICMP エコーリクエストステータスを示しながら表示されます。

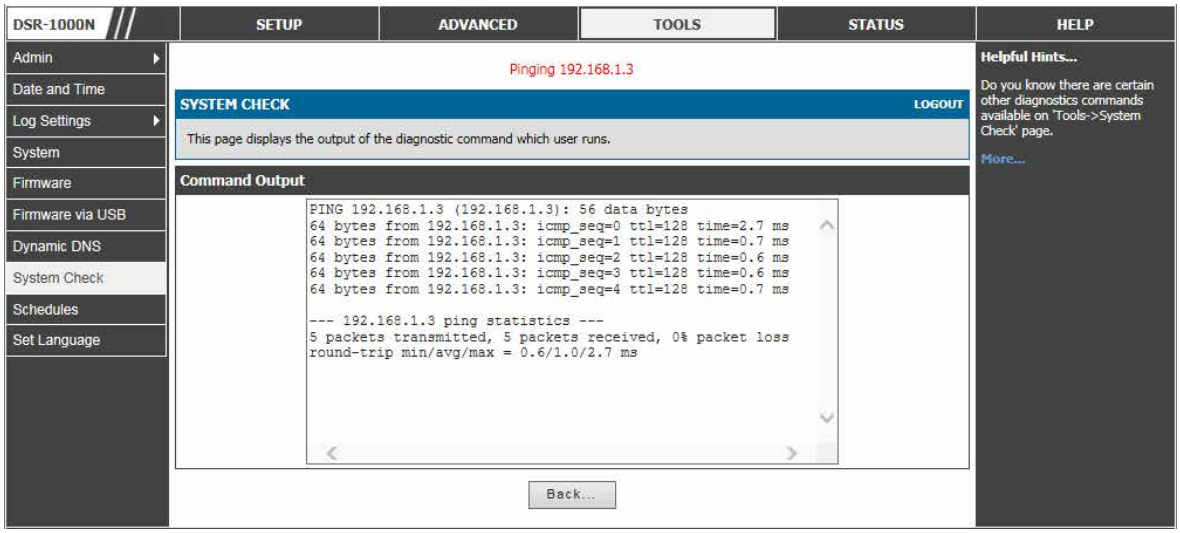


図 11-21 GUI で利用可能なルータ診断ツール - Ping

トレースルート

このユーティリティは、宛先 IP アドレスとこのルータ間に存在するすべてのルータを表示します。「Traceroute」ボタンをクリックして実行します。このルータと宛先の間にある最大 30「ホップ」(中間的ルータ) を表示します。

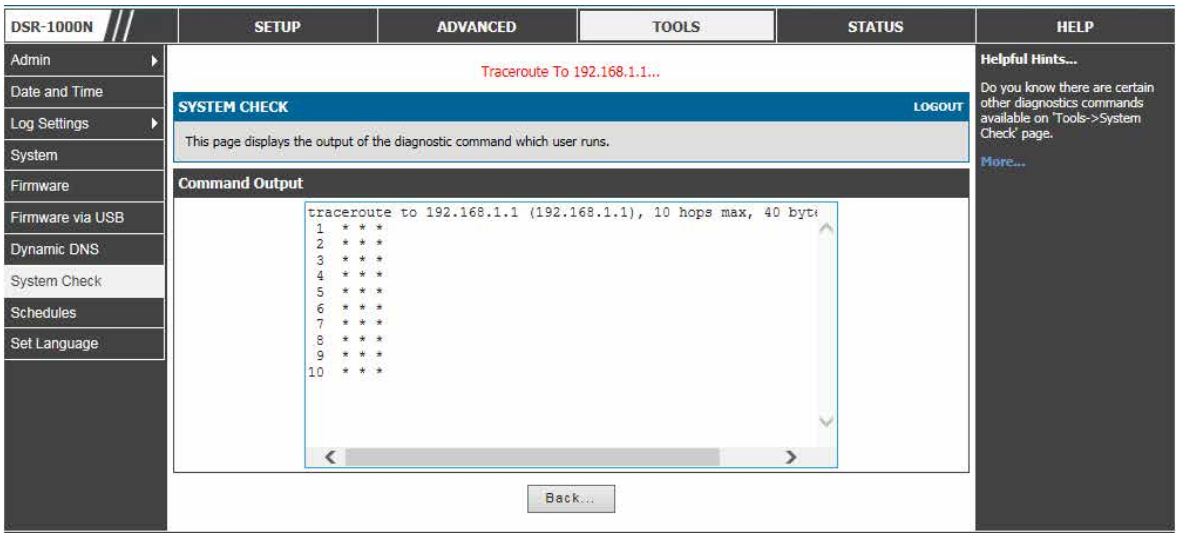


図 11-22　トレースルート出力

DNS ルックアップ

Web、FTP、メールまたはインターネットの他のサーバの IP アドレスを検索します。

「Internet Name」に「インターネット名」を入力し、「Lookup」ボタンをクリックします。ホストまたはドメインエントリが存在する場合、IP アドレスを持つ応答を参照します。「Unknown host」を示すメッセージは、特定のインターネット名が存在しないことを示します。

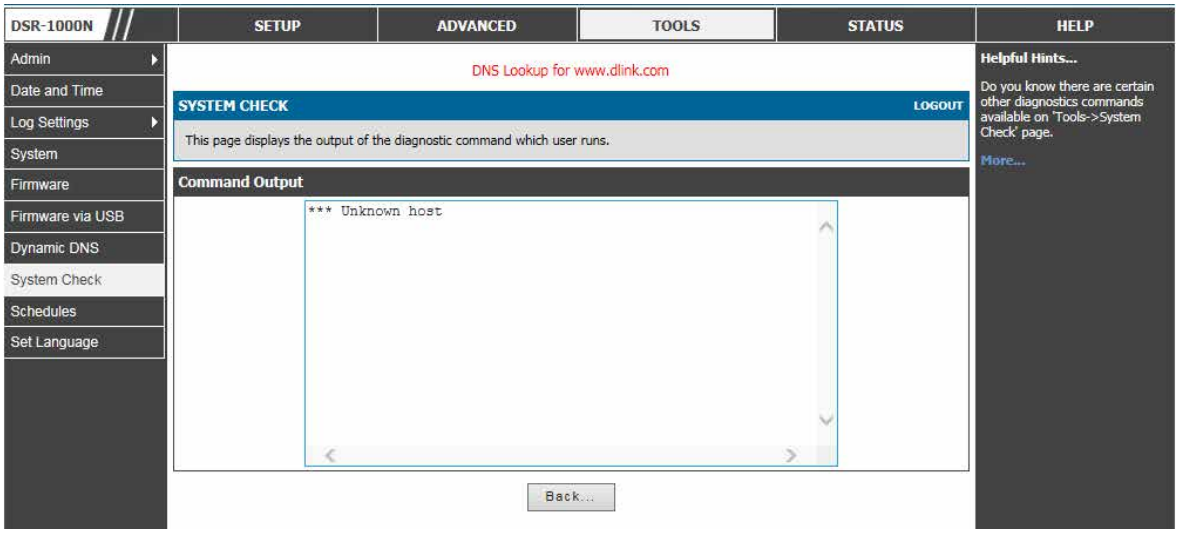


図 11-23　DNS ルックアップ出力

注意　この機能は、WAN リンクで利用可能なインターネットアクセスがあると仮定します。

ルータオプション

このルータで設定されたスタティックおよびダイナミックルートを対応するルーティングテーブルの「Display」ボタンをクリックすることで参照できます。

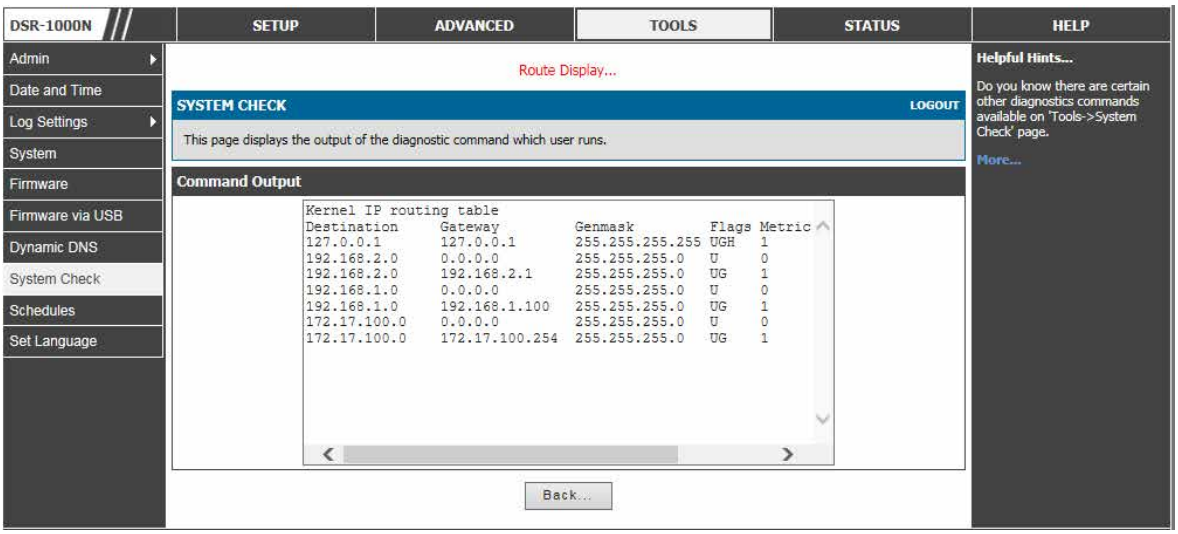


図 11-24 ルーティングテーブル出力

「Packet Trace」ボタンをクリックすると、ルータは、LAN と WAN インタフェース間のデバイスを経由してトラフィックを取得または表示します。この情報はデバッグトラフィックとルーティング問題の多くの場面で非常に役に立ちます。

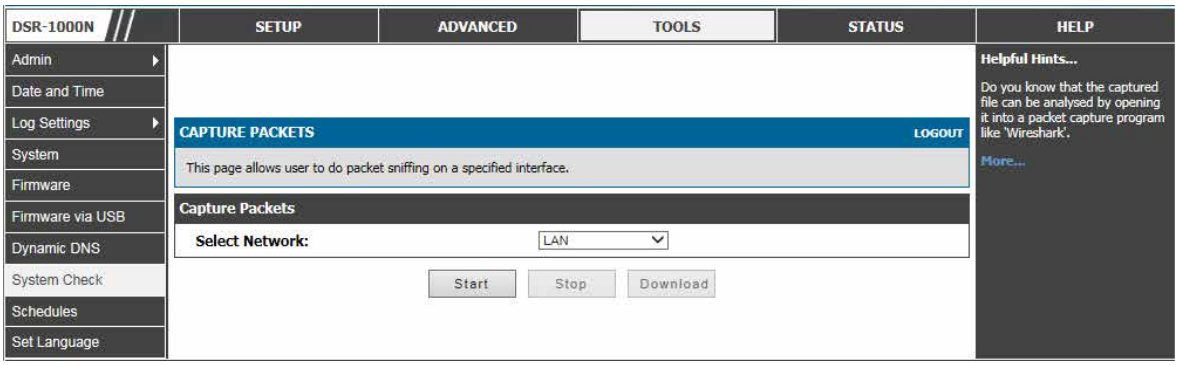


図 11-25 パケットキャプチャ

第 12 章　ルータステータスおよび統計情報

以下は本章の設定項目の説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

設定項目	説明	参照ページ
システム概要	現在のルータ状態および設定を表示します。	201 ページ
トラフィック統計情報	パケットの送受信情報などトラフィック情報を表示します。	205 ページ
アクティブな接続	アクティブなセッション情報を表示します。	206 ページ

システム概要

「STATUS」メニューでは、システム構成の詳細を取得することができます。有線 / 無線インタフェースの設定が「Device Status」ページに表示され、ハードウェアリソースの結果とルータの利用明細がルータのダッシュボードにまとめられます。

デバイスステータス

STATUS > Device Info > Device Status メニュー

ここでは「SETUP」と「ADVANCED」メニューで設定されたルータのコンフィグレーション設定を表示します。

スタティックなハードウェアシリアル番号と現在のファームウェアバージョンは「General」セクションに示されます。このページに表示された WAN/LAN インタフェース情報は、管理者の設定パラメータに基づいています。無線帯域幅とチャンネル設定は、本ルータで有効であるすべての設定済みでアクティブな AP と共に示されます。

1. STATUS > Device Info > Device Status の順にメニューをクリックし、以下の画面を表示します。

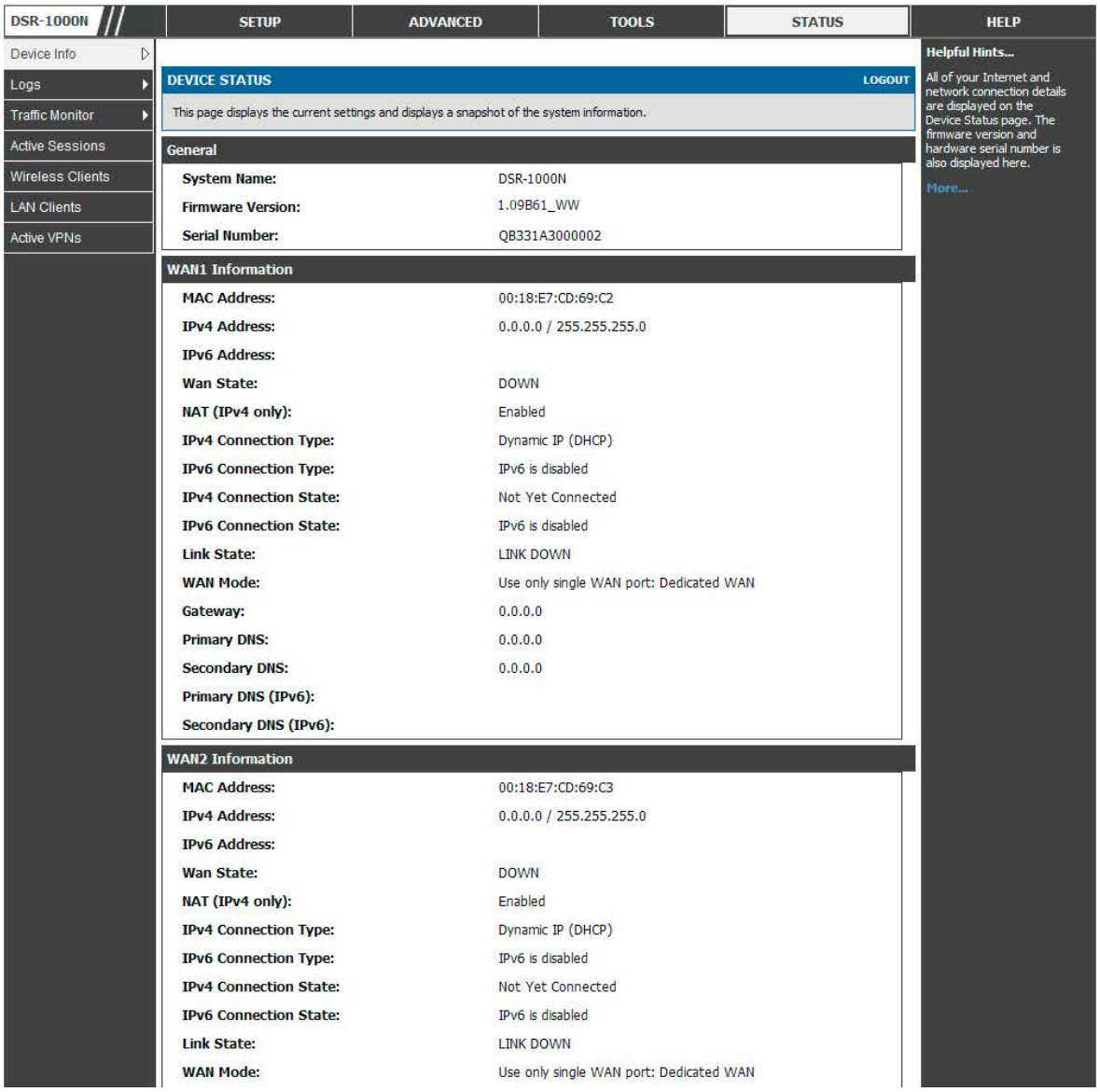


図 12-1　デバイスステータスの表示

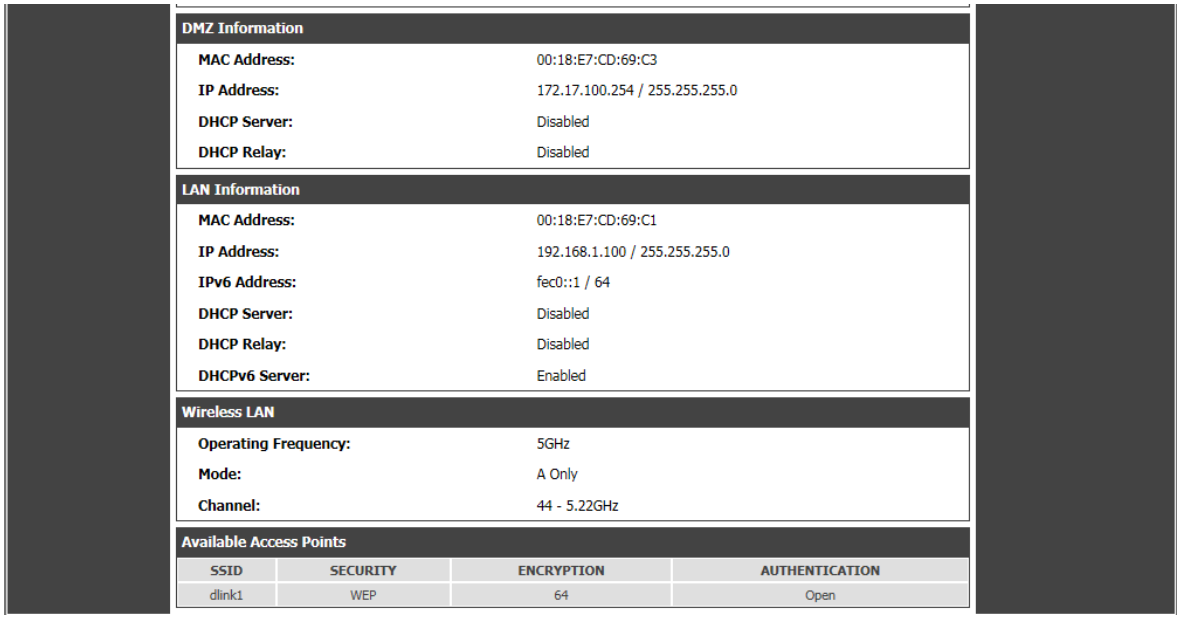


図 12-2　デバイスステータスの表示（続き）

注意　「Wireless LAN」セクションは DSR-1000N のみ表示されます。

リソースの利用

STATUS > Device Info > Dashboard メニュー

「Dashboard」ページではハードウェアと統計情報を提示します。

CPU とメモリの利用率はルータ経由で利用可能なハードウェア、現在の構成、およびトラフィックの機能です。有線接続（LAN、WAN1、WAN2/DMZ、VLAN）のインタフェースの統計情報では通過したパケットとインタフェースが破棄したパケットを表示します。「Refresh」をクリックして、このページは最新の統計情報を取得します。

1. **STATUS > Device Info > Dashboard** の順にメニューをクリックし、以下の画面を表示します。

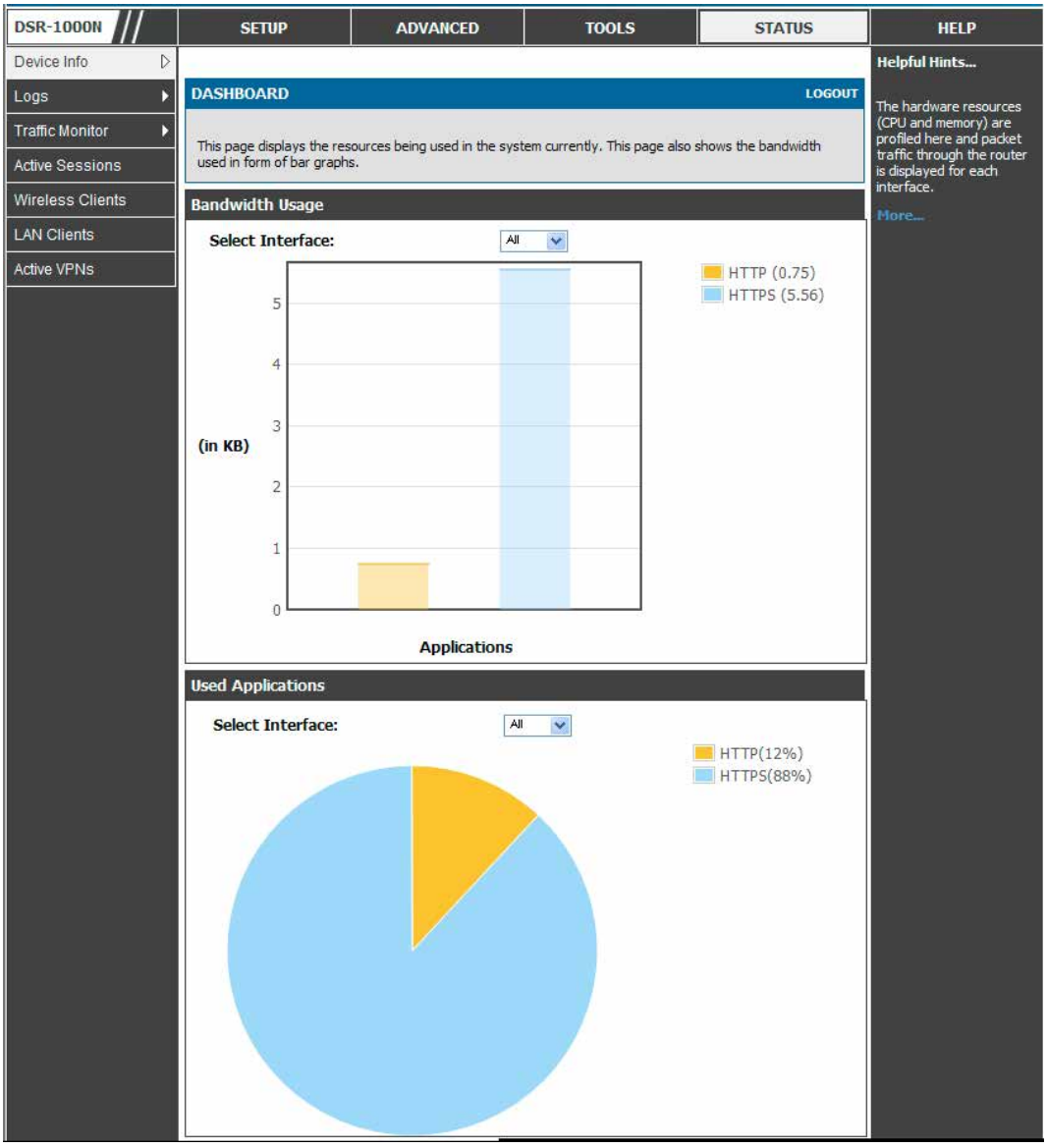
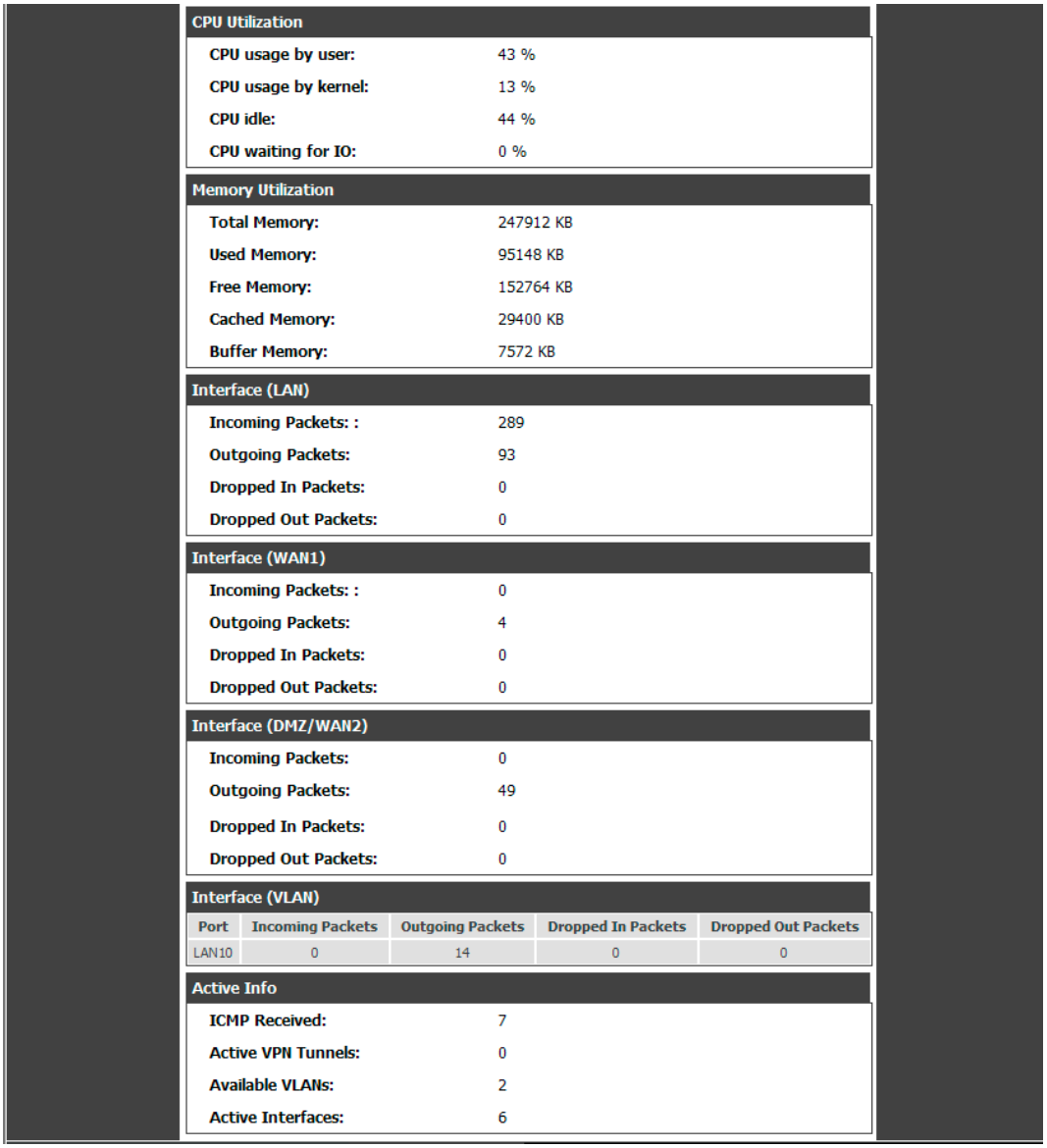


図 12-3　リソースの使用率の統計情報



CPU Utilization

CPU usage by user:	43 %
CPU usage by kernel:	13 %
CPU idle:	44 %
CPU waiting for IO:	0 %

Memory Utilization

Total Memory:	247912 KB
Used Memory:	95148 KB
Free Memory:	152764 KB
Cached Memory:	29400 KB
Buffer Memory:	7572 KB

Interface (LAN)

Incoming Packets: :	289
Outgoing Packets:	93
Dropped In Packets:	0
Dropped Out Packets:	0

Interface (WAN1)

Incoming Packets: :	0
Outgoing Packets:	4
Dropped In Packets:	0
Dropped Out Packets:	0

Interface (DMZ/WAN2)

Incoming Packets:	0
Outgoing Packets:	49
Dropped In Packets:	0
Dropped Out Packets:	0

Interface (VLAN)

Port	Incoming Packets	Outgoing Packets	Dropped In Packets	Dropped Out Packets
LAN10	0	14	0	0

Active Info

ICMP Received:	7
Active VPN Tunnels:	0
Available VLANs:	2
Active Interfaces:	6

図 12-4　リソース利用率データ（続き）

トラフィック統計情報

有線ポートの統計情報

STATUS > Traffic Monitor > Device Statistics メニュー

各物理ポートの詳しい送受信統計情報を表示します。

各インタフェース（WAN1、WAN2/DMZ、LAN、および VLAN）には、レビューのために提供される特定のパケットレベル情報があります。送受信パケット、ポートコリジョン、および送受信方向に対する累積バイト数 / 秒がポートの稼働時間と共に各インタフェースに提供されます。すべての有線ポート関する問題を疑う場合、このテーブルはポートが持つ稼働時間または送信レベル問題の診断を補助します。

統計情報テーブルには、各ページの更新時に最新のポートレベルデータの表示を可能にする自動更新制御があります。このページの自動更新の初期値は 10（秒）です。

1. **STATUS > Traffic Monitor > Device Statistics** の順にメニューをクリックし、以下の画面を表示します。

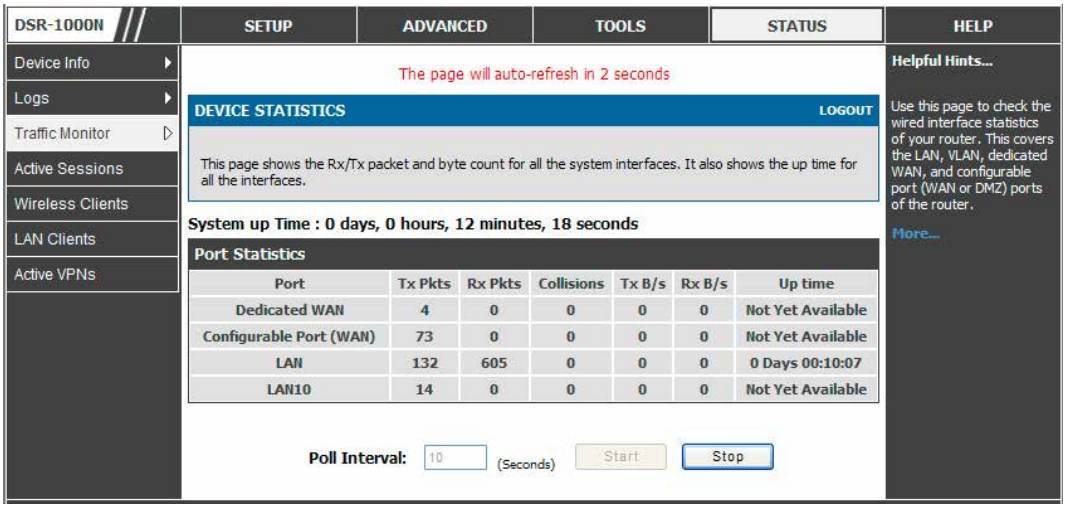


図 12-5　物理ポートの統計情報

無線ポートの統計情報（DSR-1000N のみ）

STATUS > Traffic Monitor > Wireless Statistics メニュー

各有効なアクセスポイントのトラフィック統計情報を表示します。

このページは各無線リンクに送信されたトラフィック量に関するスナップショットを提供します。無線帯域または VAP のダウンの可能性を疑う場合、このページでトラフィックが VAP 経由で送受信されているかどうかを確認します。

特定の AP に接続するクライアントは、**SETUP > Wireless Settings > Access Points** ページの AP リストの「Status」ボタンをクリックすることで表示されます。
「Statistics」テーブルの各 AP のサマリ状態と比べて、トラフィックの統計情報は個別の AP に対して表示されます。より頻繁なトラフィックとコリジョン統計情報を参照するために、ポーリング間隔（統計情報の更新レート）を変更できます。

1. **STATUS > Traffic Monitor > Wireless Statistics** の順にメニューをクリックし、以下の画面を表示します。

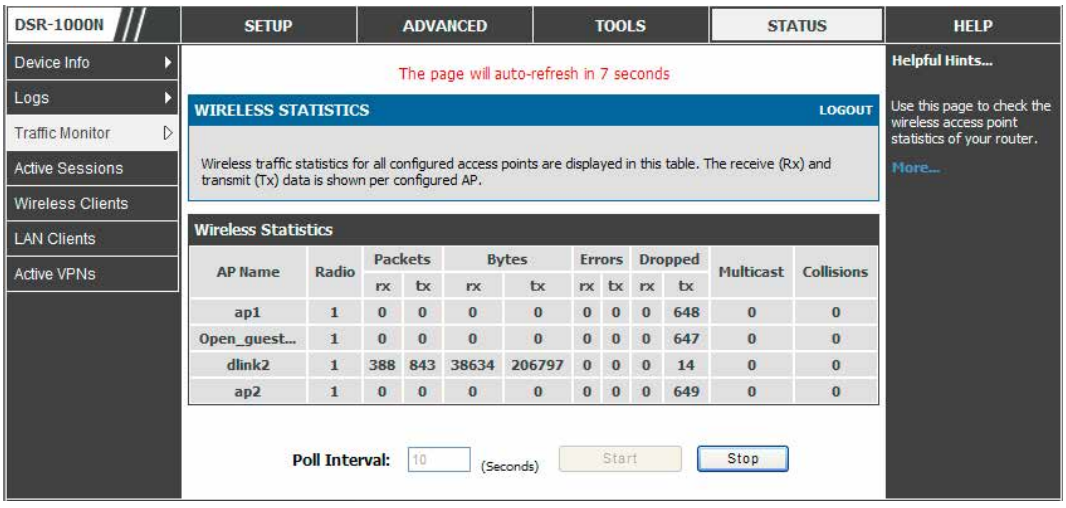


図 12-6　AP の特定の統計情報

アクティブな接続

ルータ経由のセッション

STATUS > Active Sessions メニュー

このテーブルはルータのファイアウォールを経由したアクティブなインターネットセッションを示します。セッションのプロトコル、状態、ローカルおよびリモート IP アドレスが表示されます。

1. **STATUS > Active Sessions** の順にメニューをクリックし、以下の画面を表示します。

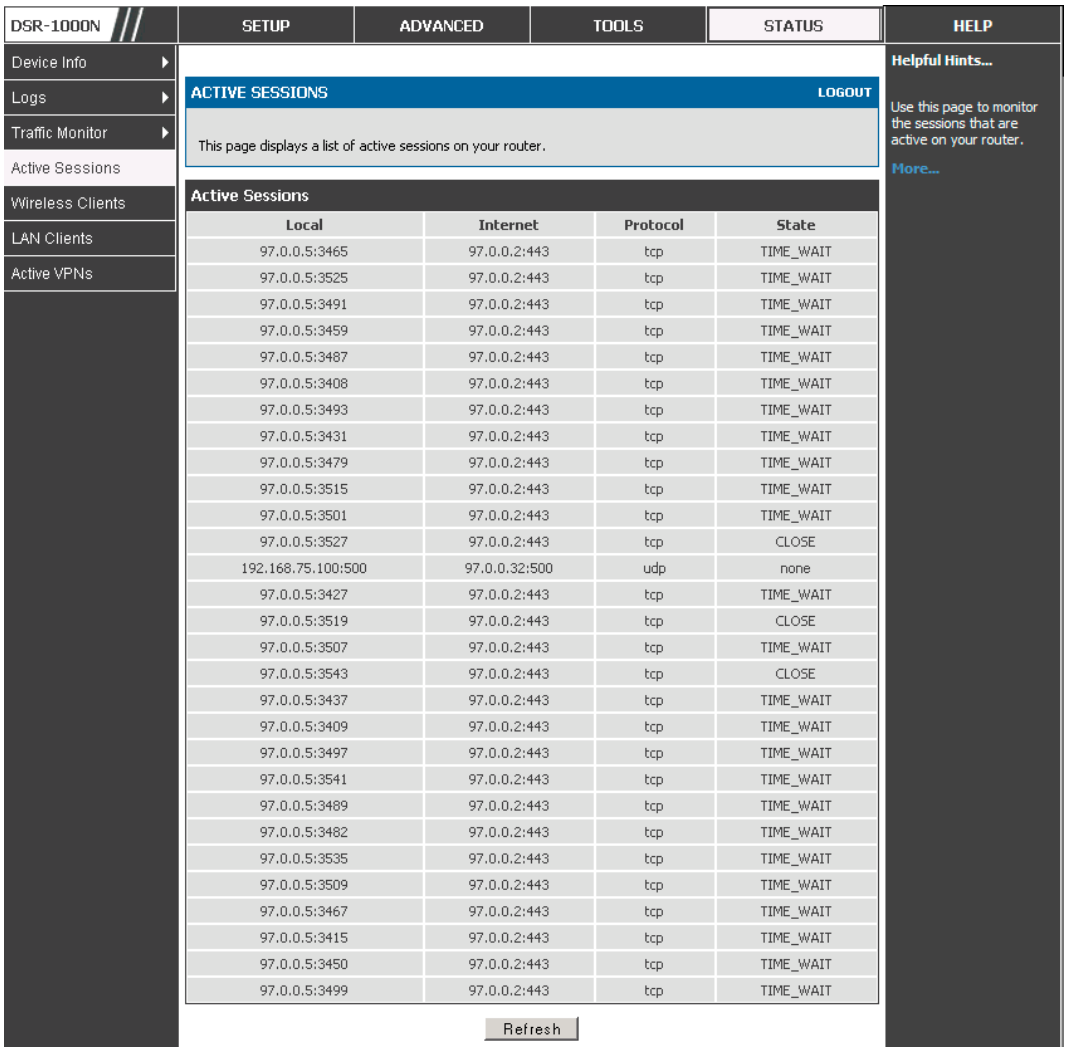


図 12-7　現在アクティブなファイアウォールセッションのリスト

無線クライアント（DSR-1000N のみ）

STATUS > Wireless Clients メニュー

特定の AP に接続するクライアントを表示します。

1. **STATUS > Wireless Clients** の順にメニューをクリックし、以下の画面を表示します。

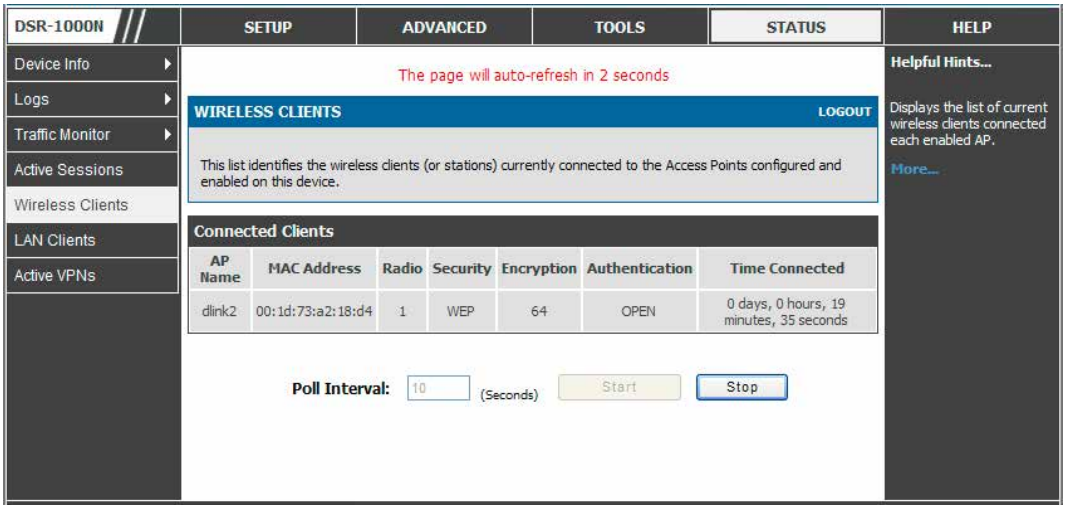


図 12-8　AP ごとに接続する 802.11 クライアントのリスト

接続するクライアントは、MAC アドレスでソートされて、対応する AP に接続する時間ならびに無線リンクに使用されるセキュリティパラメータを示します。

統計情報テーブルには、各ページの更新時に最新のポートレベルデータの表示を可能にする自動更新制御があります。このページの自動更新の初期値は 10（秒）です。

LAN クライアント

STATUS > LAN Clients メニュー

ルータに接続する LAN クライアントを LAN スイッチ経由の ARP スキャンによって識別します。検出された LAN ホストの NetBIOS 名（利用可能である場合）、IP アドレス、および MAC アドレスを表示します。

1. **STATUS > LAN Clients** の順にメニューをクリックし、以下の画面を表示します。

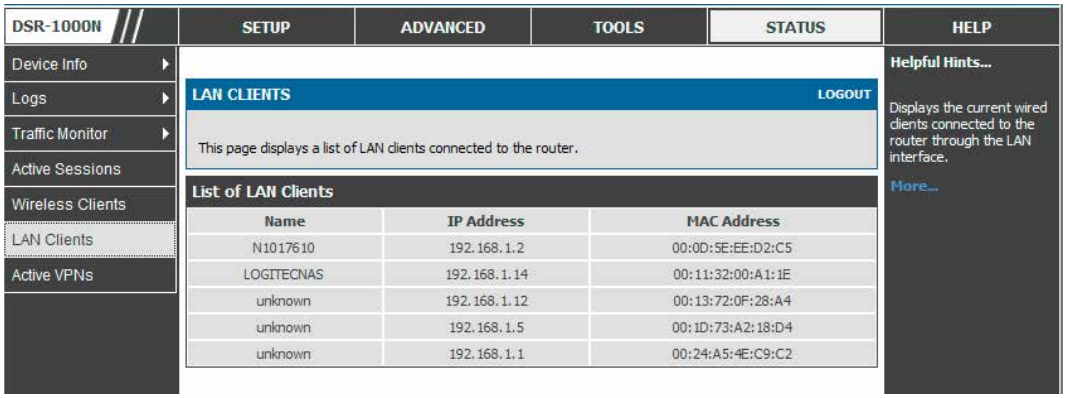


図 12-9　LAN ホストのリスト

アクティブな VPN トンネル

STATUS > Active VPNs メニュー

ルータの IPSec SA（セキュリティ結合）のステータス（接続または破棄）を参照および変更することができます。アクティブな IPSec SA（セキュリティ結合）がトラフィックの詳細とトンネル状態と共に示されます。トラフィックは、トンネル確立後の送受信パケットの累積または許可されたパケットの累積量です。

1. **STATUS > Active VPNs** の順にメニューをクリックし、以下の画面を表示します。

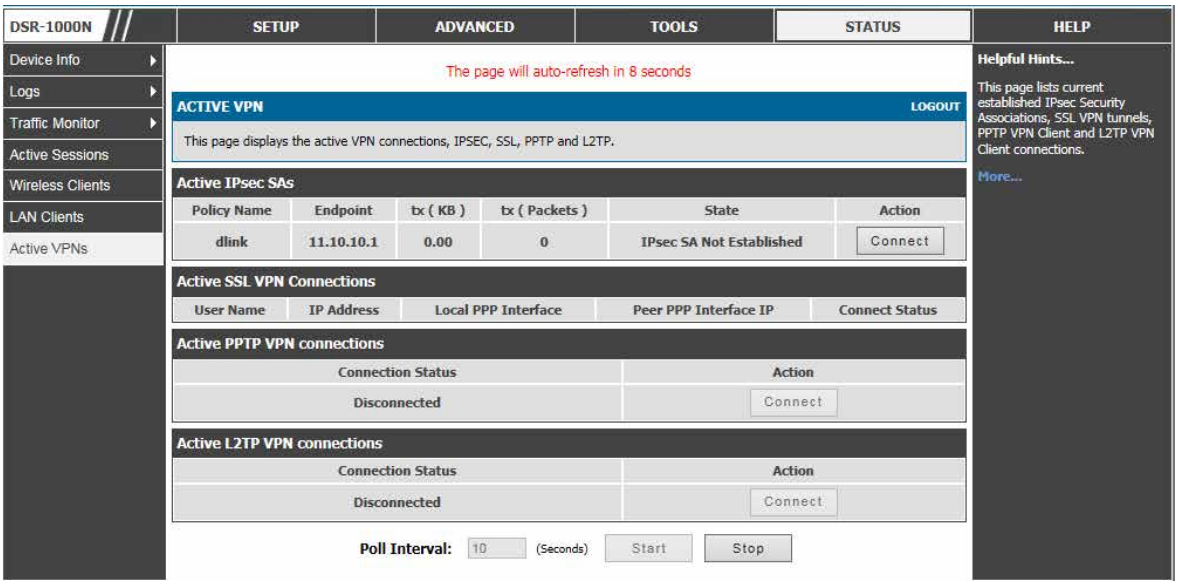


図 12-10　現在アクティブなセッションのリスト

Active IPSec SAs セクション

VPN ポリシー状態が「IPSec SA Not Established」であれば、対応するポリシー「Connect」ボタンをクリックすることによって、それを可能にすることができます。「Active IPSec SAs」テーブルはアクティブな IPSec SA のリストを表示します。テーブルの各フィールドは以下の通りです。

項目	設定
Policy Name	SA に関連付けられている IKE または VPN ポリシー名。
Endpoint	リモート VPN ゲートウェイまたはクライアントの IP アドレス。
tx（KB）	この SA が送信したデータ（Kbyte）。
tx（Packets）	この SA に受信した IP パケット数。
State	IKE ポリシーの SA のステータス：「Not Connected」（未接続）または「IPSec SA Established」（IPSec SA 確立済み）のどちらかです。

Active SSL VPN Connection セクション

VPN トンネルと VPN Port フォワーディングのためのすべてのアクティブな SSL VPN 接続が本ページに表示されます。テーブルの各フィールドは以下の通りです。

項目	設定
User Name	ルータにアクティブなトンネルまたはポートフォワーディングセッションを持つ SSL VPN ユーザ。
IP Address	リモート VPN クライアントの IP アドレス。
Local PPP Interface	セッションがアクティブであるインタフェース（WAN1 または WAN2）。
Peer PPP Interface IP	割り当てられた仮想ネットワークアダプタの IP アドレス。
Connect Status	このルータとリモート VPN クライアント間の SSL 接続のステータス：「Not Connected」（未接続）または「Connected」（接続済み。）

Active PPTP VPN connections セクション

このリストは PPTP VPN 接続のステータスを表示します。ここで PPTP VPN トンネルへの接続または切断を行うことができます。

項目	設定
Connection Status	トンネルの現在の状態を表示します。
Action	接続を確立するためには、「Connect」ボタンをクリックし、接続を終了するためには「Disconnect」ボタンをクリックします。

Active L2TP VPN connections セクション

このリストは L2TP VPN 接続のステータスを表示します。ここで L2TP VPN トンネルへの接続または切断を行うことができます。

項目	設定
Connection Status	トンネルの現在の状態を表示します。
Action	接続を確立するためには、「Connect」ボタンをクリックし、接続を終了するためには「Disconnect」ボタンをクリックします。

ページは VPN 接続の最新のステータスを表示するために自動的に更新します。ページ更新のための設定は以下の通りです。

項目	設定
Poll Interval	ページが自動的に再読込する時間（秒）
Start	自動ページ更新機能を有効にします。
Stop	自動ページ更新機能を無効にします。

第 13 章　トラブルシューティング

本製品のインストールと操作で発生する問題への解決策を提供します。

インターネット接続

症状 :

ご使用の LAN 上の PC からルータの Web 設定インタフェースにアクセスできない。

推奨される操作 :

1. PC とルータ間のイーサネット接続をチェックしてください。

2. ご使用の PC の IP アドレスがルータと同じサブネットにあることを確認してください。推奨されるアドレス指定の体系を使用している場合、ご使用の PC のアドレスは「192.168.10.2 - 192.168.10.254」の範囲にする必要があります。

3. PC の IP アドレスをチェックしてください。PC が DHCP サーバに到達できない場合、Windows と Mac OS のいくつかのバージョンでは IP アドレスを生成して、割り当てています。これらの自動生成アドレスは「169.254.x.x」の範囲にあります。IP アドレスがこの範囲にある場合、PC からファイアウォールまでの接続をチェックして、PC を再起動してください。

4. ご使用のルータの IP アドレスを変更して、それが何であるかを知らない場合には、ルータのコンフィグレーションを工場出荷時設定にリセットしてください（これはファイアウォールの IP アドレスを 192.168.10.1 に設定します）。

5. 工場出荷時設定にリセットしてコンフィグレーションを失いたくない場合、ルータを再起動して、再起動の間に送信されたパケットをキャプチャするためにパケットスニッファー（Ethereal など）を使用してください。ARP（Address Resolution Protocol）パケットを見て、ルータの LAN インタフェースアドレスの位置を見つけます。

6. ブラウザを起動し、Java、JavaScript、または ActiveX が有効であることを確認してください。Internet Explorer を使用している場合、「更新」をクリックして、Java アプレットがロードされていることを確認してください。ブラウザを閉じて、再度起動します。

7. 正しいログイン情報を使用していることを確認してください。工場出荷時のユーザ名とパスワードの初期値は「admin」です。この情報を入力する時、「CAPS LOCK」がオフであることを確認してください。

症状 :

ルータがコンフィグレーションの設定を保存しない。

推奨される操作 :

1. コンフィグレーション設定を入力する場合、別のメニューまたはタブに移行する前に「Save Settings」ボタンをクリックしてください。そうしないと行った変更は失われます。

2. ブラウザで「更新」または「リロード」をクリックしてください。変更が行われた可能性がありますが、ブラウザは古いコンフィグレーションをキャッシュしているかもしれません。

症状 :

ルータがインターネットにアクセスできない。

考えられる原因 :

ダイナミック IP アドレスを使用している場合、ご使用のルータが ISP に IP アドレスを要求していない可能性があります。

推奨される操作 :

1. ブラウザを起動して、www.google.com などの外部サイトに接続してください。
2. 「https://192.168.10.1」でファイアウォールコンフィグレーションのメインメニューにアクセスしてください。
3. **STATUS > Device Info > Device Status** を選択してください。
4. IP アドレスが WAN ポートに示されていること確認してください。「0.0.0.0」が示される場合、ファイアウォールはご契約の ISP から IP アドレスを取得していません。次の症状を参照してください。

症状 :

ルータが ISP から IP アドレスを取得できない。

推奨される操作 :

1. ケーブルまたは ADSL モデムの電源をオフにします。
2. ルータの電源をオフにします。
3. 5 分後にケーブルまたは ADSL モデムの電源を再度オンにします。
4. モデムの LED が、ISP に再度同期したことを示した後、ルータの電源を再度オンにします。ルータがまだ ISP のアドレスを取得できない場合、次の症状を参照してください。

症状 :

ルータがまだ ISP から IP アドレスを取得できない。

推奨される操作 :

1. ログインプログラムを必要とするかどうか ISP に問い合わせてください。 - PPP over Ethernet（PPPoE）または他のログインタイプ
2. もしそうであれば、設定したログイン名とパスワードが正しいことを確認してください。
3. ご使用の PC のホスト名をチェックするかどうか ISP に問い合わせてください。
4. もしそうであれば、**SETUP > Internet Settings > WAN Settings > WAN Setup** を選択して、アカウント名を ISP のアカウントの PC ホスト名に設定します。
5. 1 つのイーサネット MAC だけがインターネットに接続できるアドレスであり、そのため PC の MAC アドレスをチェックするかどうか ISP に問い合わせてください。
6. もしそうであれば、新しいネットワークデバイスを購入したことを ISP に知らせて、ファイアウォールの MAC アドレスを使用するように依頼してください。
7. または、**SETUP > Internet Settings > WAN Settings > WAN Setup** を選択して、ルータがご使用の PC の MAC アドレスになり代わるように設定してください。

症状 :

ルータは IP アドレスを取得できるが、PC はインターネットページをロードできない。

推奨される操作 :

1. 指定したドメインネームシステム（DNS）サーバのアドレスを ISP に問い合わせてください。PC がそれらのアドレスを認識するように設定してください。詳しくは、オペレーティングシステムのドキュメントを参照してください。

2. ご使用の PC に TCP/IP ゲートウェイであるルータを設定してください。

日付と時間

症状 :

表示される日付が、January 1, 1970（1970 年 1 月 1 日）である。

考えられる原因 :

ルータはまだネットワークタイムサーバ（NTS）への到達に成功していません。

推奨される操作 :

1. ルータを設定したばかりである場合、少なくとも 5 分間待ってから、**TOOLS > Date and Time** を選択して、日時を再確認してください。

2. インターネットアクセス設定を確認してください。

症状 :

時間が 1 時間遅れています。

考えられる原因 :

ルータは自動的にサマータイム（DST : Daylight Savings Time）の調整をしていません。

推奨される操作 :

1. **TOOLS > Date and Time** を選択して、現在の日付と時刻の設定を参照してください。

2. 「Enable Daylight Savings」をチェックするか、またはチェックを外して、「Save Settings」ボタンをクリックします。

LAN の接続性をテストするために Ping する

多くの TCP/IP 端末デバイスとファイアウォールには ICMP エコーリクエストパケットを指定したデバイスに送信する ping ユーティリティがあります。デバイスはエコーリプライで応答します。ご使用の PC またはワークステーションで ping ユーティリティを使用することによって、TCP/IP ネットワークの障害調査が非常に簡単になります。

ご使用の PC からルータまでの LAN パスをテストする

1. PC の Windows ツールバーから、「スタート」>「ファイル名を指定して実行」を選択します。

2. 「ping <IP アドレス >」とタイプしてください。<IP アドレス > はルータの IP アドレスです。例 : ping 192.168.10.1

3. 「OK」をクリックします。

4. 表示をモニタする :
- パス動作している場合、このメッセージシーケンスを参照します。:
  Pinging <IP アドレス > with 32 bytes of data
  Reply from <IP アドレス > : bytes=32 time=NN ms TTL=xxx
- パス動作していない場合、このメッセージシーケンスを参照します。:
  Pinging <IP アドレス > with 32 bytes of data Request timed out

5. パス動作していない場合、PC とルータ間の物理接続をテストしてください。
- LAN ポート LED が消灯している場合、15 ページの「LED 表示」セクションを参照してください。
- 対応するリンク LED がワークステーションとファイアウォールに接続するネットワークインタフェースカードおよびどんなハブポートに対しても点灯していることを確認してください。

6. パスがまだ動作していない場合、ネットワークのコンフィグレーションをテストしてください。:
- イーサネットカードのドライバソフトウェアと TCP/IP ソフトウェアが PC にインストールされて、設定済みであることを確認してください。
- ルータと PC の IP アドレスが正しく、同じサブネットにあることを確認してください。

ご使用の PC からリモートデバイスまでの LAN パスをテストする

1. PC の Windows ツールバーから、「スタート」>「ファイル名を指定して実行」を選択します。

2. 「ping-n10<IP アドレス >」とタイプしてください。「-n 10」は最大 10 回行うことを示し、<IP アドレス > はご契約の ISP の DNS サーバなどリモートデバイスの IP アドレスです。例 : ping -n 10 10.1.1.1

3. 「OK」をクリックして、表示をモニタします。(以前の手順を参照してください。)

4. パス動作していない場合、以下を行ってください :
- PC がデフォルトゲートウェイとして示されたファイアウォールの IP アドレスを持っているかをチェックしてください。(PC の IP 設定が DHCP によって割り当てられる場合、この情報は PC のネットワークコントロールパネルで見ることはできません。)
- PC のネットワーク (サブネット) アドレスがリモートデバイスのネットワークアドレスと異なることを確認してください。
- ケーブルまたは DSL モデムが接続されて、機能していることを確認してください。
- ご使用の PC にホスト名を割り当てたかどうか ISP に問い合わせてください。

  もしそうであれば、**SETUP > Internet Settings > WAN Settings > WAN Setup** を選択して、アカウント名を ISP のアカウント名として入力してください。
- ご使用の PC のすべてではなく、PC のうちの 1 つのイーサネット MAC アドレスを拒否するかどうかを ISP に問い合わせてください。

多くのブロードバンドの ISP が、ご使用のブロードバンドモデムにおける MAC アドレスからのトラフィックだけを許可することによって、アクセスを制限します。しかし、いくつかの ISP では、さらに、そのモデムに接続するただ 1 つの PC の MAC アドレスに対するアクセスを制限します。このケースの場合、ファイアウォールをクローンに設定するか、または MAC アドレスを認可された PC からのものになり代わるようにしてください。

工場出荷時コンフィグレーション設定を復元する

工場出荷時コンフィグレーション設定を復元するために、以下のいずれかを行います。:

1. アカウントのパスワードと IP アドレスをご存じですか？

- 知っている場合、**TOOLS > System** を選択し、「Default」ボタンをクリックします。

- 知らない場合、以下を行ってください。:
  ルータの背面パネルで、リセットボタンをテスト LED ライトが点灯し、次に点滅するまで 10 秒ほど押し続けます。ボタンを放して、ルータが再起動するのを待ってください。

2. ルータが自動的に再起動しない場合、手動で再起動を行い、初期設定を有効にしてください。

3. 工場出荷時設定に復元後に、コンフィグレーションインタフェースまたは「Reset」ボタンから開始されて以下の設定が適用されます。:

項目	設定
LAN IP アドレス	192.168.10.1
ユーザ名	admin
パスワード	admin
LAN の DHCP サーバ	enabled
WAN ポート設定	DHCP 経由で設定を取得

付録 A 用語解説

用語	説明
ARP	Address Resolution Protocol。IP アドレスを MAC アドレスにマップするブロードキャストプロトコル。
CHAP	Challenge-Handshake Authentication Protocol。ISP に対してユーザを認証するためのプロトコル。
DDNS	Dynamic DNS。リアルタイムでドメイン名を更新するシステム。ドメイン名がダイナミック IP アドレスを持つデバイスに割り当てられます。
DHCP	Dynamic Host Configuration Protocol。ホストがもう IP アドレスを必要としない時にアドレスを再利用できるようにダイナミックに IP アドレスを割り当てるプロトコル。
DNS	Domain Name System。H.323 ID、URL、またはメール ID を IP アドレスに変換するメカニズム。また、リモートゲートキーパの場所を見つけるのを補助して、IP アドレスを管理ドメインのホスト名にマップするために使用されます。
FQDN	FQDN(完全修飾ドメイン名)。ホスト部分を含むドメイン名を完成します。例 : serverA.companyA.com
FTP	File Transfer Protocol。ネットワークノード間でファイルを転送するプロトコル。
HTTP	Hypertext Transfer Protocol。ファイルの転送のために Web ブラウザと Web サーバに使用されるプロトコル。
IKE	Internet Key Exchange。VPN トンネルを構築する部分として ISAKMP で安全に暗号化鍵を交換するモード。
IPSec	IP security。データストリームにおける IP パケットの認証、または暗号化によって VPN トンネルを保証するプロトコルセット。IPSec は、「transport」モード (パケットヘッダではなく、ペイロードを暗号化する) または「tunnel」モード (ペイロードとパケットヘッダの両方を暗号化する) のいずれかで動作します。
ISAKMP	Internet Key Exchange Security Protocol。インターネットでセキュリティ結合と暗号鍵を確立するプロトコル。
ISP	Internet service provider（インターネットサービスプロバイダ）。
MAC Address	Media-access-control address。ネットワークアダプタに割り当てられている固有の物理アドレス識別子。
MTU	Maximum transmission unit。通過可能な最も大きいパケットサイズ（バイト）。イーサネットの MTU は 1500 バイトのパケットです。
NAT	Network Address Translation。ルータまたはファイアウォールを通過するパケットとして IP アドレスを書き換える処理。NAT は、LAN のゲートウェイルータにおける単一のパブリック IP アドレスを使用して、LAN 上の複数ホストがインターネットにアクセスするのを可能にします。
NetBIOS	ファイル共有、プリンタ共有、メッセージング、認証、および名前解決のためのマイクロソフトの Windows プロトコル。
NTP	Network Time Protocol。クロックマスタとして知られているルータをネットワークにおける単一のクロックに同期させるプロトコル。
PAP	Password Authentication Protocol。リモートアクセスサーバまたは ISP に対してユーザを認証するためのプロトコル。
PPPoE	Point-to-Point Protocol over Ethernet。ISP が IP アドレスの割り当てを管理することなくホストのネットワークを ISP に接続するためのプロトコル。
PPTP	Point-to-Point Tunneling Protocol。インターネット上のリモートクライアントからプライベートサーバまでの安全なデータ転送のために VPN を作成するプロトコル。
RADIUS	Remote Authentication Dial-In User Service。リモートユーザ認証とアカウンティングのためのプロトコル。ユーザ名とパスワードの集中管理を提供します。
RSA	Rivest-Shamir-Adleman。公開鍵 暗号化アルゴリズム。
TCP	Transmission Control Protocol。信頼性と順序通りの配信を保証したインターネットにおけるデータ送信のプロトコル。
UDP	User Data Protocol。信頼性と順序通りの配信を保証せずにインターネットにおけるデータを送信するプロトコル。
VPN	Virtual private network。あるネットワークから別のネットワークにトラフィックすべてを暗号化することによって IP トラフィックがパブリックな TCP/IP ネットワークに進むことを可能とするネットワーク。IP レベルで全情報を暗号化するためにトンネリングを使用します。
WINS	Windows Internet Name Service。名前解決のためのサービス。異なる IP サブネットのクライアントがブロードキャストを送信せずに、ダイナミックにアドレスの解決、自身の登録、およびネットワークのブラウズを行うことができます。
XAUTH	IKE Extended Authentication。IKE プロトコルに基づいてデバイス (IKE が認証する) だけではなく、ユーザも認証する方式。ユーザ認証はデバイス認証後と IPSec ネゴシエーション前に実行されます。

付録 B 工場出荷時設定

機能	説明	初期値
デバイスログイン	ユーザログイン	URL https://192.168.10.1
	ユーザ名（大文字小文字区別あり）	admin
	ログインパスワード（大文字小文字区別あり）	admin
インターネット接続	WAN MAC アドレス	初期アドレスを使用
	WAN MTU サイズ	1500
	ポート速度	オートセンス
ローカルエリアネットワーク（LAN）	IP アドレス	192.168.10.1
	IPv4 サブネットマスク	255.255.255.0
	RIP ディレクション	なし
	RIP バージョン	無効
	RIP 認証	無効
	DHCP サーバ	有効
	DHCP 開始 IP アドレス	192.168.10.2
	DHCP 終了 IP アドレス	192.168.10.100
	タイムゾーン	GMT
	DST 用に調整されるタイムゾーン	無効
	SNMP	無効
	リモート管理	無効
ファイアウォール	インターネットからの内向き通信	無効(HTTP ポートのポート 80 上のトラフィックを除く)
	インターネットへの外向き通信	有効（すべて）
	送信元 MAC フィルタ	無効
	ステルスモード	有効

付録 C ポートフォワーディングとファイアウォール設定に利用可能な標準サービス

ANY	ICMP-TYPE-8	RLOGIN
AIM	ICMP-TYPE-9	RTELNET
BGP	ICMP-TYPE-10	RTSP:TCP
BOOTP_CLIENT	ICMP-TYPE-11	RTSP:UDP
BOOTP_SERVER	ICMP-TYPE-13	SFTP
CU-SEEME:UDP	ICQ	SMTP
CU-SEEME:TCP	IMAP2	SNMP:TCP
DNS:UDP	IMAP3	SNMP:UDP
DNS:TCP	IRC	SNMP-TRAPS:TCP
FINGER	NEWS	SNMP-TRAPS:UDP
FTP	NFS	SQL-NET
HTTP	NNTP	SSH:TCP
HTTPS	PING	SSH:UDP
ICMP-TYPE-3	POP3	STRMWORKS
ICMP-TYPE-4	PPTP	TACACS
ICMP-TYPE-5	RCMD	TELNET
ICMP-TYPE-6	REAL-AUDIO	TFTP
ICMP-TYPE-7	REXEC	VDOLIVE

付録 D ログメッセージ

ファシリティ：システム（ネットワーク）

ログメッセージ	緊急度	ログメッセージ	緊急度
DBUpdate event: Table: %s opCode:%drowId:%d	DEBUG	BridgeConfig: too few arguments to command %s	ERROR
networkIntable.txt not found	DEBUG	BridgeConfig: too few arguments to command %s	ERROR
sqlite3QueryResGet failed	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Interface is already deleted in bridge	DEBUG	ddnsDisable failed	ERROR
removing %s from bridge %s... %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
adding %s to bridge %s... %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
stopping bridge...	DEBUG	ddnsDisable failed	ERROR
stopping bridge...	DEBUG	failed to call ddns enable	ERROR
stopping bridge...	DEBUG	ddnsDisable failed	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Wan is not up	DEBUG	Error in executing DB update handler	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
doDNS:failed	DEBUG	Illegal invocation of ddnsView (%s)	ERROR
doDNS:failed	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
doDNS:Result = FAILED	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
doDNS:Result SUCCESS	DEBUG	ddns: SQL error: %s	ERROR
Write Old Entry: %s %s %s: to %s	DEBUG	Illegal operation interface got deleted	ERROR
Write New Entry: %s %s #%s : to %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Write Old Entry: %s %s %s: to %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Write New Entry: %s %s #%s : to %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
ifStaticMgmtDBUpdateHandler: returning with "	DEBUG	ddnsDisable failed	ERROR
nimfLinkStatusGet: buffer: \	DEBUG	ddns: SQL error: %s	ERROR
nimfLinkStatusGetErr: returning with status: %d	DEBUG	Failed to call ddns enable	ERROR
nimfAdvOptSetWrap: current Mac Option: %d	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: current Port Speed Option: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfAdvOptSetWrap: current Mtu Option: %d	DEBUG	Failed to call ddns enable	ERROR
nimfAdvOptSetWrap: looks like we are reconnecting. "	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: Mtu Size: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: NIMF table is %s	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap:WAN_MODE TRIGGER	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfAdvOptSetWrap: MTU: %d	DEBUG	Failed to call ddns enable	ERROR
nimfAdvOptSetWrap: MacAddress: %s	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: old Mtu Flag: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: user has changed MTU option	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: MTU: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfAdvOptSetWrap: old MTU size: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfAdvOptSetWrap: old Port Speed Option: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: old Mac Address Option: %d	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: MacAddress: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Setting LED [%d]:[%d] For %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
l2tpEnable: command string: %s	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: handling reboot scenario	DEBUG	failed to call ddns enable	ERROR
nimfAdvOptSetWrap: INDICATOR = %d	DEBUG	ddns: SQL error: %s	ERROR
nimfAdvOptSetWrap: UpdateFlag: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: returning with status: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfGetUpdateMacFlag: MacTable Flag is: %d	DEBUG	Error in executing DB update handler	ERROR
nimfMacGet: Mac Option changed	DEBUG	Failed to open the resolv.conf file. Exiting./n	ERROR
nimfMacGet: Update Flag: %d	DEBUG	Could not write to the resolv.conf file. Exiting.	ERROR
nimfMacGet: MacAddress: %s	DEBUG	Error opening the lanUptime File	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
nimfMacGet: MacAddress: %s	DEBUG	Error Opening the lanUptime File.	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to open %s	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to open %s	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to query networkInterface table	ERROR
nimfMacGet:Mac option Not changed \	DEBUG	failed to query networkInterface table	ERROR
nimfMacGet: MacAddress: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to enable IPv6 forwarding	ERROR
nimfMacGet: MacAddress: %s	DEBUG	failed to set capabilities on the "	ERROR
nimfMacGet: returning with status: %s	DEBUG	failed to enable IPv6 forwarding	ERROR
Now in enableing LanBridge function	DEBUG	failed to set capabilities on the "	ERROR
sucessfully executed the command %s	DEBUG	failed to disable IPv6 forwarding	ERROR
Now in disableing LanBridge function	DEBUG	failed to set capabilities on the "	ERROR
sucessfully executed the command %s	DEBUG	failed to open %s	ERROR
configPortTblHandler:Now we are in Sqlite Update "	DEBUG	Could not create ISATAP Tunnel	ERROR
The Old Configuration of ConfiPort was:%s	DEBUG	Could not destroy ISATAP Tunnel	ERROR
The New Configuration of ConfiPort was:%s	DEBUG	Could not configure ISATAP Tunnel	ERROR
The user has deselected the configurable port	DEBUG	Could not de-configure ISATAP Tunnel	ERROR
failed query %s	DEBUG	nimfStatusUpdate: updating NimfStatus failed	ERROR
failed query %s	DEBUG	nimfStatusUpdate: updating NimfStatus failed	ERROR
failed query %s	DEBUG	nimfLinkStatusGet: determinig link's status failed	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	nimfLinkStatusGet: opening status file failed	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	Failed to commit	ERROR
%s:%d SIP ENABLE: %s	DEBUG	ifStatusDBUpdate: Failed to begin "	ERROR
sipTblHandler:failed to update ifStatic	DEBUG	%s: SQL error: %s	ERROR
sipTblHandler:failed to update Configport	DEBUG	%s: Failed to commit "	ERROR
%s:%d SIP DISABLE: %s	DEBUG	nimfNetIfaceTblHandler: unable to get LedPinId	ERROR
%s:%d SIP SET CONF: %s	DEBUG	nimfNetIfaceTblHandler: unable to get LedPinId	ERROR
Failed to open %s: %s	DEBUG	nimfNetIfaceTblHandler: unable to get LedPinId	ERROR
Failed to start sipalg	DEBUG	%s: unable to kill dhclient	ERROR
Failed to stop sipalg	DEBUG	nimfAdvOptSetWrap: unable to get current Mac Option	ERROR
Failed to get config info	DEBUG	nimfAdvOptSetWrap: unable to get current Port "	ERROR
Network Mask: 0x%x	DEBUG	nimfAdvOptSetWrap: unable to get current MTU Option	ERROR
RTP DSCP Value: 0x%x	DEBUG	nimfAdvOptSetWrap: error getting Mac Address from "	ERROR
Need more arguments	DEBUG	nimfAdvOptSetWrap: unable to get the MTU	ERROR
Invalid lanaddr	DEBUG	nimfAdvOptSetWrap: error setting interface advanced "	ERROR
Invalid lanmask	DEBUG	nimfAdvOptSetWrap: error getting MTU size	ERROR
Invalid option	DEBUG	nimfAdvOptSetWrap: unable to get Mac Address	ERROR
Failed to set config info	DEBUG	nimfAdvOptSetWrap: error setting interface advanced "	ERROR
Unknown option	DEBUG	nimfAdvOptSetWrap: failed to get old connectiontype	ERROR
sshdTblHandler	DEBUG	nimfAdvOptSetWrap: old connection type is: %s	ERROR
pPort: %s	DEBUG	nimfAdvOptSetWrap: failed to get old MTU Option	ERROR
pProtocol: %s	DEBUG	nimfAdvOptSetWrap: error getting MTU size	ERROR
pListerAddr: %s	DEBUG	nimfOldFieldValueGet: failed to get old "	ERROR
pKeyBits: %s	DEBUG	nimfOldFieldValueGet: user has changed MTU size	ERROR
pRootEnable: %s	DEBUG	nimfAdvOptSetWrap: failed to get old Port Speed "	ERROR
pRsaEnable: %s	DEBUG	nimfAdvOptSetWrap: user has changed Port Speed	ERROR
pDsaEnable: %s	DEBUG	nimfAdvOptSetWrap: failed to get old Mac Address "	ERROR
pPassEnable: %s	DEBUG	nimfAdvOptSetWrap: user has changed Mac Address "	ERROR
pEmptyPassEnable: %s	DEBUG	nimfAdvOptSetWrap: unable to get Mac Address	ERROR
pSftpEnable: %s	DEBUG	nimfAdvOptSetWrap:Failed to RESET the flag	ERROR
pScpEnable: %s	DEBUG	nimfAdvOptSetWrap: setting advanced options failed	ERROR
pSshdEnable: %s	DEBUG	nimfAdvOptSetWrap: interface advanced options applied	ERROR
pPrivSep: %s	DEBUG	nimfGetUpdateMacFlag: unable to get Flag from MacTable	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	nimfMacGet: Updating MAC address failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Re-Starting sshd daemon....	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
sshd re-started successfully.	DEBUG	error executing the command %s	ERROR
sshd stopped .	DEBUG	error executing the command %s	ERROR
failed query %s	DEBUG	error executing the command %s	ERROR
vlan disabled, not applying vlan configuration..	DEBUG	disableLan function is failed to disable ConfigPort"	ERROR
failed query %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
failed query %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
no ports present in this vlanId %d	DEBUG	Unable to Disable configurable port from	ERROR
failed query %s	DEBUG	configPortTblHandler has failed	ERROR
vlan disabled, not applying vlan configuration..	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
disabling vlan	DEBUG	Error in executing DB update handler	ERROR
enabling vlan	DEBUG	sqlite3QueryResGet failed	ERROR
vlan disabled, not applying vlan configuration..	DEBUG	Failed to execute switchConfig for port\	ERROR
no ports present in this vlanId %d	DEBUG	Failed to execute switchConfig for port enable	ERROR
failed query %s	DEBUG	Failed to execute ifconfig for port enable	ERROR
vlan disabled, not applying vlan configuration..	DEBUG	Failed to execute ethtool for\	ERROR
removing %s from bridge%s... %s	DEBUG	Failed to execute switchConfig for port disable	ERROR
adding %s to bridge%d... %s	DEBUG	Failed to execute ifconfig for port disable	ERROR
restarting bridge...	DEBUG	sqlite3QueryResGet failed	ERROR
[switchConfig] Ignoring event on port number %d	DEBUG	sqlite3_mprintf failed	ERROR
restarting bridge...	DEBUG	sqlite3QueryResGet failed	ERROR
executing %s ... %s	DEBUG	Failed to execute switchConfig for port mirroring	ERROR
removing %s from bridge%s... %s	DEBUG	Usage:%s <DB Name> <Entry Name> <logFile> <subject>	ERROR
adding %s to bridge%d... %s	DEBUG	sqlite3QueryResGet failed	ERROR
[switchConfig] Ignoring event on %s	DEBUG	Could not get all the required variables to email the Logs.	ERROR
restarting bridge...	DEBUG	runSmtpClient failed	ERROR
[switchConfig] Ignoring event on port number %d	DEBUG	getaddrinfo returned %s	ERROR
[switchConfig] executing %s ... %s	DEBUG	file not found	ERROR
restarting bridge...	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
UserName: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Password: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
IspName: %s	DEBUG	No memory to allocate	ERROR
DialNumber: %s	DEBUG	Failed to Open SSHD Configuration File	ERROR
Apn: %s	DEBUG	Ipaddress should be provided with accessoption 1	ERROR
GetDnsFromIsp: %s	DEBUG	Subnetaddress should be provided with accessoption 2	ERROR
IdleTimeOutFlag: %s	DEBUG	Failed to restart sshd	ERROR
IdleTimeOutValue: %d	DEBUG	unable to open the "	ERROR
AuthMetho: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
executing %s ... %s	DEBUG	Error in executing DB update handler	ERROR
removing %s from bridge%d... %s	DEBUG	Error in executing DB update handler	ERROR
adding %s to bridge%d... %s	DEBUG	unknown vlan state	ERROR
stopping bridge...	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
restarting bridge...	DEBUG	sqlite3_mprintf failed	ERROR
Could not configure 6to4 Tunnel Interface	DEBUG	Access port can be present only in single vlan	ERROR
Could not de-configure 6to4 Tunnel Interface	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
failed to restart 6to4 tunnel interfaces	DEBUG	unknown vlan state	ERROR
BridgeConfig: too few arguments to command %s	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
BridgeConfig: unsupported command %d	DEBUG	Failed to clear vlan for oldPVID %d	ERROR
BridgeConfig returned error=%d	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
sqlite3QueryResGet failed	DEBUG	Failed to clear vlan for %d	ERROR
Error in executing DB update handler	DEBUG	Failed to set vlan entry for vlan %d	ERROR
sqlite3QueryResGet failed	DEBUG	Failed to set vlan entries, while enabling \	ERROR
Failed to remove vlan Interface for vlanId \	DEBUG	sqlite3QueryResGet failed	ERROR
sqlite3QueryResGet failed	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Invalid oidp passed	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
Invalid oidp passed	DEBUG	Failed to enable vlan	ERROR
Failed to get oid from the tree	DEBUG	Failed to disable vlan	ERROR
threegEnable: Input to wrapper %s	DEBUG	Failed to set vlanPort table entries, while \	ERROR
threegEnable: spawning command %s	DEBUG	Failed to enable vlan	ERROR
threegMgmtHandler: query string: %s	DEBUG	unknown vlan state	ERROR
threegMgmtHandler: returning with status: %s	DEBUG	Error in executing DB update handler	ERROR
adding to dhcprealy ifgroup failed	DEBUG	unknown vlan state	ERROR
adding to ipset fwDhcpRelay failed	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
Disabling Firewall Rule for DHCP Relay Protocol	DEBUG	sqlite3_mprintf failed	ERROR
Enabling Firewall Rule for DHCP Relay Protocol	DEBUG	Access port can be present only in single vlan	ERROR
prerouting Firewall Rule add for Relay failed	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
prerouting Firewall Rule add for Relay failed	DEBUG	unknown vlan state	ERROR
%s: SQL get query: %s	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
%s: sqlite3QueryResGet failed	DEBUG	Failed to clear vlan for oldPVID %d	ERROR
%s: no result found	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
%s: buffer overflow	DEBUG	Failed to clear vlan for %d	ERROR
%s: value of %s in %s table is: %s	DEBUG	Failed to set vlan entry for vlan %d	ERROR
%s: returning with status: %s	DEBUG	Failed to set vlan entries, while enabling \	ERROR
dnsResolverConfigure: addressFamily: %d	DEBUG	Failed to execute vlanConfig binary for port number %d	ERROR
dnsResolverConfigure: LogicalIfName: %s	DEBUG	Failed to execute vlanConfig binary for vlanId %d	ERROR
chap-secrets File found	DEBUG	Failed to enable vlan	ERROR
PID File for xl2tpd found	DEBUG	Failed to disable vlan	ERROR
pid: %d	DEBUG	Failed to set vlanPort table entries, while \	ERROR
options.xl2tpd file found	DEBUG	Failed to enable vlan	ERROR
options.xl2tpd file not found	DEBUG	unknown vlan state	ERROR
Conf File for xl2tpd found	DEBUG	threegMgmtInit: unable to open the database file %s	ERROR
xl2tpd.conf not found	DEBUG	threegConnEnable: failed to get the WanMode	ERROR
Chap Secrets file found	DEBUG	threegEnable:spawning failed	ERROR
Chap Secrets file not found	DEBUG	threegDisable: unable to kill ppp daemon	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	threegMgmtHandler: Query: %s	ERROR
chap-secrets File found	DEBUG	threegMgmtHandler: error in executing database update	ERROR
PID File for pptpd found	DEBUG	Error in executing DB update handler	ERROR
pid: %d	DEBUG	are we getting invoked twice ??	ERROR
PID File for pptpd interface found	DEBUG	could not open %s to append	ERROR
pid: %d	DEBUG	could not write nameserver %s to %s	ERROR
options.pptpd file found	DEBUG	could not write nameserver %s to %s	ERROR
options.pptpd file not found	DEBUG	could not open %s to truncate	ERROR
Conf File for pptpd found	DEBUG	dnsResolverConfigMgmtInit: unable to open the "	ERROR
pptpd.conf not found	DEBUG	resolverConfigDBUpateHandler: sqlite3QueryResGet "	ERROR
Chap Secrets file found	DEBUG	could not configure DNS resolver	ERROR
Chap Secrets file not found	DEBUG	dnsResolverConfigure: could not write nameserver:%s,"	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	unboundMgmt: unable to open the "	ERROR
chap-secrets File found	DEBUG	ioctl call Failed-could not update active user Details	ERROR
pppoeMgmtTblHandler: MtuFlag: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pppoeMgmtTblHandler: Mtu: %d	DEBUG	Can't kill xl2tpd	ERROR
pppoeMgmtTblHandler: IdleTimeOutFlag: %d	DEBUG	xl2tpd restart failed	ERROR
pppoeMgmtTblHandler: IdleTimeOutValue: %d	DEBUG	failed to get field value	ERROR
pppoeMgmtTblHandler: UserName: %s	DEBUG	failed to get field value	ERROR
pppoeMgmtTblHandler: Password: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pppoeMgmtTblHandler: DNS specified: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pppoeMgmtTblHandler: Service: %s	DEBUG	unboundMgmt: unable to open the "	ERROR
pppoeMgmtTblHandler: StaticIp: %s	DEBUG	writing options.xl2tpd failed	ERROR
pppoeMgmtTblHandler: NetMask: %s	DEBUG	xl2tpdStop failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
pppoeMgmtTblHandler: AuthOpt: %d	DEBUG	writing xl2tpd.conf failed	ERROR
pppoeMgmtTblHandler: Satus: %d	DEBUG	writing options.xl2tpd failed	ERROR
pppoeEnable: ppp dial string: %s	DEBUG	xl2tpdStop failed	ERROR
pppoeMgmtDBUpdateHandler: returning with status: %s	DEBUG	xl2tpdStart failed	ERROR
pptpMgmtTblHandler: MtuFlag: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pptpMgmtTblHandler: Mtu: %d	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
pptpMgmtTblHandler: IdleTimeOutFlag: %d	DEBUG	xl2tpdStop failed	ERROR
pptpMgmtTblHandler: IdleTimeOutValue: %d	DEBUG	xl2tpdStart failed	ERROR
pptpMgmtTblHandler: GetDnsFromIsp: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pptpMgmtTblHandler: UserName: %s	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
pptpMgmtTblHandler: Password: %s	DEBUG	xl2tpdStop failed	ERROR
pptpMgmtTblHandler: dynamic MyIp configured	DEBUG	xl2tpdStart failed	ERROR
pptpMgmtTblHandler: MyIp: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pptpMgmtTblHandler: ServerIp: %s	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
pptpMgmtTblHandler: StaticIp: %s	DEBUG	Error in executing DB update handler	ERROR
pptpMgmtTblHandler: NetMask: %s	DEBUG	unboundMgmt: unable to open the "	ERROR
pptpMgmtTblHandler: MppeEncryptSupport: %s	DEBUG	Can't kill pptpd	ERROR
pptpMgmtTblHandler: SplitTunnel: %s	DEBUG	pptpd restart failed	ERROR
pptpEnable: ppp dial string: %s	DEBUG	Can't kill pptpd	ERROR
pptpEnable: spawning command %s	DEBUG	failed to get field value	ERROR
PID File for dhcpc found	DEBUG	failed to get field value	ERROR
pid: %d	DEBUG	unboundMgmt: unable to open the "	ERROR
pptpMgmtDBUpdateHandler: query string: %s	DEBUG	writing options.pptpd failed	ERROR
pptpMgmtDBUpdateHandler: returning with status: %s	DEBUG	pptpdStop failed	ERROR
dhcpcReleaseLease: dhcpc release command: %s	DEBUG	writing pptpd.conf failed	ERROR
dhcpcMgmtTblHandler: MtuFlag: %d	DEBUG	writing options.pptpd failed	ERROR
dhcpcMgmtTblHandler: Mtu: %d	DEBUG	pptpdStop failed	ERROR
DHCPv6 Server started successfully.	DEBUG	pptpdStart failed	ERROR
DHCPv6 Server stopped successfully	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
DHCPv6 Client started successfully.	DEBUG	Error in executing DB update handler	ERROR
DHCPv6 Client stopped successfully.	DEBUG	pppStatsUpdate: unable to get default MTU	ERROR
DHCPv6 Client Restart successful	DEBUG	pppoeMgmtInit: unable to open the database file %s	ERROR
l2tpMgmtTblHandler: MtuFlag: %d	DEBUG	pppoeDisable: unable to kill ppp daemon	ERROR
l2tpMgmtTblHandler: Mtu: %d	DEBUG	pppoeMultipleEnableDisable: pppoe enable failed	ERROR
l2tpMgmtTblHandler: IspName: %s	DEBUG	pppoeMultipleEnableDisable: pppoe disable failed	ERROR
l2tpMgmtTblHandler: UserName: %s	DEBUG	pppoeMgmtTblHandler: unable to get current Mtu Option	ERROR
l2tpMgmtTblHandler: Password: %s	DEBUG	pppoeMgmtTblHandler: unable to get the Mtu	ERROR
l2tpMgmtTblHandler: AccountName: %s	DEBUG	pppoeMgmtTblHandler: pppoe enable failed	ERROR
l2tpMgmtTblHandler: DomainName: %s	DEBUG	pppoeMgmtDBUpdateHandler: failed query: %s	ERROR
l2tpMgmtTblHandler: Secret: not specified	DEBUG	pppoeMgmtDBUpdateHandler: error in executing "	ERROR
l2tpMgmtTblHandler: Secret: %s	DEBUG	pptpMgmtInit: unable to open the database file %s	ERROR
l2tpMgmtTblHandler: dynamic MyIp configured	DEBUG	pptpEnable: error executing command: %s	ERROR
l2tpMgmtTblHandler: MyIp: %s	DEBUG	pptpEnable: unable to resolve address: %s	ERROR
l2tpMgmtTblHandler: ServerIp: %s	DEBUG	pptpEnable: inet_aton failed	ERROR
l2tpMgmtTblHandler: StaticIp: %s	DEBUG	pptpEnable: inet_aton failed	ERROR
l2tpMgmtTblHandler: NetMask: %s	DEBUG	pptpEnable:spawning failed	ERROR
l2tpMgmtTblHandler: SplitTunnel: %s	DEBUG	pptpDisable: unable to kill ppp daemon	ERROR
needToStartHealthMonitor: returning with status: %s	DEBUG	pptpMgmtTblHandler: unable to get current MTU Option	ERROR
l2tpEnable: command string: %s	DEBUG	pptpMgmtTblHandler: unable to get the Mtu	ERROR
l2tpEnable: command: %s	DEBUG	pptpMgmtTblHandler: dbRecordValueGet failed for %s "	ERROR
l2tpEnable: command string: %s	DEBUG	pptpMgmtTblHandler: pptp enable failed	ERROR
PID File for dhcpc found	DEBUG	pptpMgmtTblHandler: pptp disable failed	ERROR
pid: %d	DEBUG	pptpMgmtDBUpdateHandler: sqlite3QueryResGet "	ERROR
l2tpMgmtDBUpdateHandler: query string: %s	DEBUG	pptpMgmtDBUpdateHandler: error in executing "	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
l2tpMgmtDBUpdateHandler: returning with status: %s	DEBUG	Illegal invocation of dhcpConfig (%s)	ERROR
RADVD started successfully	DEBUG	dhcpLiblnit: unable to open the database file %s	ERROR
RADVD stopped successfully	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
empty update. nRows=%d nCols=%d	WARN	dhcpcMgmtInit: unable to open the database file %s	ERROR
Wan is not up or in load balencing mode	WARN	dhcpcReleaseLease: unable to release lease	ERROR
threegMgmtHandler: no row found. nRows = %d nCols = %d	WARN	dhcpcEnable: unable to kill dhclient	ERROR
pppoeMgmtDBUpdateHandler: empty update.	WARN	dhcpcEnable: enabling dhcpc failed on: %s	ERROR
dhcpcEnable: dhclient already running on: %s	WARN	dhcpcDisable: unable to kill dhclient	ERROR
dhcpcDisable: deleted dhclient.leases	WARN	dhcpcDisable: delete failed for dhclient.leases	ERROR
l2tpMgmtInit: unable to open the database file %s	ERROR	dhcpcDisable: failed to reset the ip	ERROR
l2tpEnable: unable to resolve address: %s	ERROR	dhcpcMgmtTblHandler: unable to get current Mtu Option	ERROR
l2tpEnable: inet_aton failed	ERROR	dhcpcMgmtTblHandler: unable to get the Mtu	ERROR
The Enable Command is %s	ERROR	dhcpcMgmtTblHandler: dhclient enable failed	ERROR
l2tpEnable:Executing the Command failed	ERROR	dhcpcMgmtTblHandler: dhcpc release failed	ERROR
l2tpDisable: command string: %s	ERROR	dhcpcMgmtTblHandler: dhcpc disable failed	ERROR
l2tpDisable: unable to stop l2tp session	ERROR	dhcpcMgmtDBUpdateHandler: failed query: %s	ERROR
l2tpMgmtTblHandler: unable to get current MTU option	ERROR	dhcpcMgmtDBUpdateHandler: error in executing "	ERROR
l2tpMgmtTblHandler: unable to get the Mtu	ERROR	DHCPv6 Client start failed.	ERROR
l2tpMgmtTblHandler: dbRecordValueGet failed for %s "	ERROR	DHCPv6 Client stop failed.	ERROR
l2tpMgmtTblHandler: l2tpEnable failed	ERROR	failed to create/open DHCPv6 client "	ERROR
l2tpMgmtTblHandler: disabling l2tp failed	ERROR	failed to write DHCPv6 client configuration file	ERROR
l2tpMgmtDBUpdateHandler: sqlite3QueryResGet "	ERROR	failed to restart DHCPv6 Client	ERROR
l2tpMgmtDBUpdateHandler: error in executing	ERROR	failed to create/open DHCPv6 Server "	ERROR
Illegal invocation of tcpdumpConfig (%s)	ERROR	Restoring old configuration..	ERROR
Failed to start tcpdump	ERROR	DHCPv6 Server configuration update failed	ERROR
Failed to stop tcpdump	ERROR	DHCPv6 Server Restart failed	ERROR
Invalid tcpdumpEnable value	ERROR	sqlite3QueryResGet failed.Query:%s	ERROR

ファシリティ：システム（**VPN**）

ログメッセージ	緊急度	ログメッセージ	緊急度
%d command not supported by eapAuth	DEBUG	PEAP key derive: ERROR	ERROR
pCtx NULL.	DEBUG	PEAP context is NULL: ERROR	ERROR
Current cert subject name= %s	DEBUG	Constructing P2 response: ERROR	ERROR
X509_STORE_CTX_get_ex_data failed.	DEBUG	innerEapRecv is NULL: ERROR	ERROR
Cannot get cipher, no session est.	DEBUG	Decrypting TLS data: ERROR	ERROR
%s: SSL_ERROR_WANT_X509_LOOKUP	DEBUG	Wrong identity size: ERROR	ERROR
err code = (%d) in %s	DEBUG	Wrong size for extensions packet: ERROR	ERROR
BIO_write: Error	DEBUG	innerEapRecv is NULL: ERROR.	ERROR
Decrypting: BIO reset failed	DEBUG	Inner EAP processing: ERROR	ERROR
Encrypting BIO reset: ERROR	DEBUG	TLS handshake: ERROR.	ERROR
BIO_read: Error	DEBUG	Sending P1 response: ERROR	ERROR
EAP state machine changed from %s to %s.	DEBUG	Unexpected tlsGlueContinue return value.	ERROR
EAP state machine changed from %s to %s.	DEBUG	No more fragments in message. ERROR	ERROR
Received EAP Packet with code %d	DEBUG	No phase 2 data or phase 2 data buffer NULL: ERROR	ERROR
Response ID %d	DEBUG	Allocating memory for PEAP Phase 2 payload: ERROR	ERROR
Response Method %d	DEBUG	TLS encrypting response: ERROR	ERROR
Created EAP/PEAP context: OK	DEBUG	Setting message in fragment buffer: ERROR	ERROR
Deleted EAP/PEAP context: OK	DEBUG	Allocating TLS read buffer is NULL: ERROR	ERROR
Upper EAP sent us: decision = %d method state = %d	DEBUG	Setting last fragment: ERROR	ERROR
P2 decision=(%d); methodState=(%d)	DEBUG	Getting message: ERROR	ERROR
Writing message to BIO: ERROR.	DEBUG	Processing PEAP message: ERROR	ERROR
Encrypted (%d) bytes for P2	DEBUG	Setting fragment: ERROR	ERROR
P2: sending fragment.	DEBUG	Creating receive buffer: ERROR	ERROR
P2: message size = %d	DEBUG	Setting first fragment: ERROR	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
P2: sending unfragmented message.	DEBUG	Sending P1 response: ERROR	ERROR
P1: Sending fragment.	DEBUG	NULL request (or response) PDU or NULL context: ERROR	ERROR
P1: Total TLS message size = (%d)	DEBUG	Expecting start packet, got something else: ERROR	ERROR
P1: sending unfragmented message.	DEBUG	Protocol version mismatch: ERROR	ERROR
peapFragFirstProcess: TLS record size to receive = (%d)	DEBUG	Processing PEAP message (from frag): ERROR	ERROR
Setting version %d	DEBUG	Processing PEAP message: ERROR	ERROR
PEAP pkt rcvd: data len=(%d) flags=(%d) version=(%d)	DEBUG	Processing PEAP message: ERROR	ERROR
Got PEAP/Start packet.	DEBUG	Indicated length not valid: ERROR	ERROR
Got first fragment	DEBUG	Did not get Acknowledged result: ERROR	ERROR
Got fragment (n)	DEBUG	Cannot understand AVP value: ERROR	ERROR
Got last fragment	DEBUG	eapExtResp is NULL: ERROR	ERROR
Got unfragmented message	DEBUG	eapWscCtxCreate: EAPAUTH_MALLOC failed.	ERROR
Got frag ack.	DEBUG	eapWscProcess: umiloctl req to WSC failed, status = %d	ERROR
Ext AVP parsed: flags=(0x%x)	DEBUG	eapWscCheck: Invalid frame	ERROR
Mandatory bit not set: WARNING	DEBUG	eapWscBuildReq: Invalid state %d	ERROR
Ext AVP parsed: type=(%d)	DEBUG	eapWscProcessWscResp: Invalid data recd pData = %p, dataLen"	ERROR
Ext AVP parsed: value=(%d)	DEBUG	Data received for invalid context, dropping it	ERROR
Got PEAPv0 success!	DEBUG	eapWscProcessWscResp: Build Request failed	ERROR
Got PEAPv0 failure!	DEBUG	eapWscProcessWscResp: Invalid state %d	ERROR
pCtx NULL.	DEBUG	eapWscProcessWscResp: Message processing failed 0x%X	ERROR
Authenticator response check: Error	DEBUG	eapWscProcessWscData: Invalid notification recd %d	ERROR
Authenticator response check: Failed	DEBUG	unable to initialize MD5	ERROR
MS-CHAP2 Response AVP size = %u	DEBUG	MDString: adpDigestInit for md5 failed	ERROR
Created EAP/MS-CHAP2 context: OK.	DEBUG	EAPAUTH_MALLOC failed.	ERROR
pCtx NULL.	DEBUG	EAPAUTH_MALLOC failed.	ERROR
Deleted EAP/MS-CHAPv2 context: OK	DEBUG	NULL context created: Error	ERROR
Not authenticated yet.	DEBUG	NULL context received: Error	ERROR
Authenticator response invalid	DEBUG	Authenticator ident invalid.	ERROR
EAP-MS-CHAPv2 password changed.	DEBUG	Success request message invalid: Error	ERROR
rcvd. opCode %d.	DEBUG	Plugin context is NULL	ERROR
pCtx NULL.	DEBUG	Deriving implicit challenge: Error	ERROR
TLS message len changed in the fragment, ignoring.	DEBUG	Generating NT response: Error	ERROR
no data to send while fragment ack received.	DEBUG	NULL in/out buffer: Error	ERROR
TLS handshake successful.	DEBUG	Incorrect vendor id.	ERROR
Created EAP/TTLS context: OK	DEBUG	Allocating memory for outBuff: ERROR	ERROR
Deleted EAP/TTLS context: OK	DEBUG	AVP code not recognized	ERROR
No more fragments in message. ERROR	DEBUG	EAPAUTH_MALLOC failed.	ERROR
Upper EAP sent us: method state = %d; decision = %d	DEBUG	Converting password to unicode: Error	ERROR
P2: sending fragment.	DEBUG	Generating password hash: Error.	ERROR
P2 send unfragmented message.	DEBUG	Generating password hash hash: Error.	ERROR
P1: sending fragment.	DEBUG	Generating master key: Error.	ERROR
P1: sending unfragmented message.	DEBUG	Generating first 16 bytes of session key: Error.n	ERROR
\tTLSMsgLen = 0x%x	DEBUG	Generating second 16 bytes of session key: Error.n	ERROR
Send req ptr = 0x%x; Send resp ptr = 0x%x	DEBUG	Converting password to unicode: Error	ERROR
P2 decision=(%d); methodState=(%d)	DEBUG	Constructing failure response: ERROR	ERROR
Default EAP: method state = %d; decision = %d	DEBUG	Error checking authenticator response.	ERROR
TTLS pkt: data len=(%d) flags=(0x%x)	DEBUG	Error generating NT response.	ERROR
Got start	DEBUG	Username string more than 256 ASCII characters: ERROR	ERROR
Got first fragment (n).	DEBUG	Invalid Value-Size.	ERROR
Got fragment (n).	DEBUG	Invalid MS-Length. Got (%d), expected (%d)	ERROR
Got last fragment	DEBUG	Error constructing response.	ERROR
Got unfragmented message.	DEBUG	Got type (%d), expecting (%d)	ERROR
Got frag ack.	DEBUG	Cannot handle message; opCode = %d	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Rcvd. AVP Code-%u: flags-0x%x: len- %u: vendorId-%u: "	DEBUG	EAPAUTH_MALLOC failed.	ERROR
MOD EAP: method state from upper = %d; decision = %d	DEBUG	tlsGlueCtxCreate failed.	ERROR
Got AVP len = %ul. Should be less than 16777215	DEBUG	client certificate must be set in the profile.	ERROR
AVP length extract: Error	DEBUG	received tls message length too big.	ERROR
pFB is NULL	DEBUG	total frags len > initial total tls length.	ERROR
Requesting message before assembly complete	DEBUG	total frags len > initial total tls length.	ERROR
pFB is NULL	DEBUG	total data rcvd(%d) doesnt match the initial "	ERROR
pFB is NULL	DEBUG	couldnt write %d data to TLS buffer.	ERROR
Buffer cannot hold message: ERROR	DEBUG	invalid flags %s passed to eapTlsBuildResp.	ERROR
pFB is NULL: Error	DEBUG	EAPAUTH_MALLOC failed.	ERROR
pFB is NULL	DEBUG	tlsGlueCtxCreate failed.	ERROR
TLS_FB* is NULL.	DEBUG	Context NULL: ERROR	ERROR
pFB->msgBuff is NULL.	DEBUG	Setting profile to glue layer: ERROR.	ERROR
Error calculating binary.	DEBUG	_eapCtxCreate failed.	ERROR
Error calculating binary.	DEBUG	%d authentication not enabled in the system.	ERROR
adpDigestInit for SHA1 failed.	DEBUG	Initializing inner non-EAP auth plugin: ERROR	ERROR
adpDigestInit for SHA1 failed.	DEBUG	TTLS key derive: ERROR	ERROR
E = %d	DEBUG	TTLS context from EAP plugin is NULL: ERROR	ERROR
R = %d	DEBUG	Allocating memory for TTLS Phase 2 payload: ERROR	ERROR
Could not initialize des-ecb	DEBUG	TLS Encrypting response: ERROR	ERROR
adpDigestInit for MD4 failed.	DEBUG	Allocating TLS read buffer is NULL: ERROR	ERROR
adpDigestInit for SHA1 failed.	DEBUG	Inner authentication (id: %d) unhandled	ERROR
adpDigestInit for SHA1 failed.	DEBUG	innerEapRecv is NULL: ERROR.	ERROR
Error converting received auth reponse to bin.	DEBUG	Decrypting TLS data: ERROR	ERROR
Gnerating challenge hash: Error	DEBUG	Processing Phase 2 method: Error	ERROR
Generating password hash: Error	DEBUG	Writing message to BIO: ERROR.	ERROR
Generating challenge response: Error	DEBUG	TLS handshake: ERROR.	ERROR
Conn cipher name=%s ver=%s: %s	DEBUG	Unexpected tlsGlueContinue return value.	ERROR
Send req ptr = 0x%x; Send resp ptr = 0x%x	DEBUG	NULL request (or response) PDU or NULL context	ERROR
Request ptr = 0x%x;	DEBUG	Protocol version mismatch: ERROR	ERROR
Response ptr = 0x%x	DEBUG	Creating receive buffer: ERROR	ERROR
Rcvd. AVP Code - %ul	DEBUG	Setting first fragment: ERROR	ERROR
Rcvd. AVP flags - 0x%02x	DEBUG	Setting fragment: ERROR	ERROR
Rcvd. AVP len - %ul	DEBUG	Setting last fragment: ERROR	ERROR
Rcvd. AVP vendor id - %ul	DEBUG	Getting message: ERROR	ERROR
\tCode = %d	DEBUG	Processing TTLS message: ERROR	ERROR
\tIdent = %d	DEBUG	Processing TTLS message: ERROR	ERROR
\tLen = %d	DEBUG	Processing TTLS message: ERROR	ERROR
\tType = %d	DEBUG	Decapsulating AVP: ERROR	ERROR
\tOpCode = %d	DEBUG	Processing EAP receive: Error	ERROR
\tMSID = %d	DEBUG	AVP code not EAP: Error	ERROR
\tmsLen = %d	DEBUG	Encapsulating AVP: ERROR	ERROR
\tvalSize = %d	DEBUG	profile %s doesnt exist.	ERROR
Frag Buffer bytes left = (%d)	DEBUG	profile %s is in use.	ERROR
Stripped username=(%s)	DEBUG	profile %s already exists.	ERROR
digestLen = %d.	DEBUG	EAPAUTH_MALLOC failed	ERROR
ClearText =	DEBUG	User not found.	ERROR
CipherText =	DEBUG	EAP-MD5 not enabled in system configuration.	ERROR
digestLen = %d.	DEBUG	EAP-MSCHAPV2 not enabled in system configuration.	ERROR
digestLen1 = %d.	DEBUG	EAP-TLS not enabled in system configuration.	ERROR
digestLen2 = %d.	DEBUG	EAP-TTLS not enabled in system configuration.	ERROR
password change is not allowed for this user	DEBUG	EAP-PEAP not enabled in system configuration.	ERROR
completed writing the policy	DEBUG	EAP-WSC not enabled in system configuration.	ERROR
completed writing the SA	DEBUG	PAP not enabled in system configuration.	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
completed writing the proposal block	DEBUG	CHAP not enabled in system configuration.	ERROR
cmdBuf: %s	DEBUG	MSCHAP not enabled in system configuration.	ERROR
X509_DEBUG : Invalid Certificate for the generated"	DEBUG	MSCHAPV2 not enabled in system configuration.	ERROR
X590_ERROR : Failed to create File '%s'	DEBUG	PAP/Token not enabled in system configuration.	ERROR
x509TblHandler	DEBUG	EAP-MD5 not enabled in system configuration.	ERROR
pCertType: %s	DEBUG	EAP-MSCHAPV2 not enabled in system config.	ERROR
pRowQueryStr: %s	DEBUG	EAP-TLS not enabled in system configuration.	ERROR
x509SelfCertTblHandler	DEBUG	EAP-TTLS and EAP-PEAP are not valid as inner"	ERROR
pRowQueryStr: %s	DEBUG	invalid innerAuth %d.	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	profile %s doesnt exist.	ERROR
umiRegister failed	ERROR	Re-assembling fragments incorrect size	ERROR
eapAuthHandler: Invalid data received	ERROR	Error creating cipher context.	ERROR
EAPAUTH_MALLOC failed.	ERROR	Error initializing cipher context.	ERROR
malloc failed.	ERROR	Error creating digest context.	ERROR
BIO_new_mem_buf failed.	ERROR	Error initializing digest context.	ERROR
malloc failed.	ERROR	Error initializing DES in Klite	ERROR
BIO_new_mem_buf failed.	ERROR	Error initializing MD4 in Klite	ERROR
SSL_CTX_new (TLSv1_client_method) failed.	ERROR	Error initializing RC4 in Klite	ERROR
unable to set user configured CIPHER list %s	ERROR	Error initializing SHA in Klite	ERROR
Certificate verification failed.	ERROR	Error cleaning cipher context.	ERROR
Server name match failed. Got (%s) expected "	ERROR	Error destroying cipher context.	ERROR
SSL_CTX_use_certificate_file (cert, PEM) failed.	ERROR	Error cleaning digest context.	ERROR
SSL_CTX_use_PrivateKey_file failed.	ERROR	Error destroying digest context.	ERROR
private key does not match public key	ERROR	Error stripping domain name.	ERROR
SSL_CTX_load_verify_locations failed	ERROR	Error cleaning digest context.	ERROR
SSL_new failed.	ERROR	Error cleaning digest context.	ERROR
Both SSL_VERIFY_PEER and SSL_VERIFY_NONE set: Error	ERROR	Challenge not present in failure packet.	ERROR
EAPAUTH_MALLOC failed.	ERROR	Wrong challenge length.	ERROR
EAPAUTH_MALLOC failed.	ERROR	Incorrect password change version value.	ERROR
eapTimerCreate failed.	ERROR	Error generating password hash.	ERROR
eapCtxDelete:pCtx == NULL	ERROR	Error generating password hash.	ERROR
eapRole != EAP_ROLE_PEER or EAP_ROLE_AUTHENTICATOR	ERROR	Error encrypting password hash with block	ERROR
pEapCtx == NULL or pPDU == NULL.	ERROR	Could not initialize des-ecb	ERROR
received EAP pdu bigger than EAP_MTU_SIZE.	ERROR	Error cleaning cipher context.	ERROR
received EAP pdu bigger than EAP_MTU_SIZE.	ERROR	Error cleaning cipher context.	ERROR
state machine is in invalid state.	ERROR	Error cleaning digest context.	ERROR
unable to create method context.	ERROR	Error cleaning digest context.	ERROR
method ctxCreate failed.	ERROR	adpDigestInit for SHA1 failed.	ERROR
method profile set failed.	ERROR	X509_ERROR : .Query:%s	ERROR
state machine is in invalid state.	ERROR	X509_ERROR : Invalid Certificate for the "	ERROR
Only StandAlone authenticator supported currently.	ERROR	invalid x509 certificate	ERROR
state machine is in invalid state.	ERROR	Couldn't get the x509 cert hash	ERROR
BuildReq operation failed	ERROR	Memory allocation failed	ERROR
No method ops defined for current method	ERROR	FileName too lengthy	ERROR
Process operation failed	ERROR	Couldn't execute command	ERROR
state machine is in invalid state.	ERROR	Memory allocation failed	ERROR
Packet length mismatch %d, %d	ERROR	Memory allocation failed	ERROR
eapAuthTypeToType: Invalid eapAuthType %d	ERROR	invalid certificate data	ERROR
eapTypeToAuthType: Invalid eapType %d	ERROR	.Query:%s	ERROR
unable to create method context.	ERROR	.Query:%s	ERROR
method ctxCreate failed.	ERROR	Memory allocation failed	ERROR
Invalid condition, methodState = %d, respMethod = %d	ERROR	X509_ERROR : Failed to validate the certficate "	ERROR
A EAP Ctx map already exists	ERROR	Memory allocation failed	ERROR
eapTimerCreate: Currently unsupported for Peer role	ERROR	.Query:%s	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
eapTimerStart: Currently unsupported for Peer role	ERROR	Invalid Sign Key Length : %d	ERROR
eapTimerDestroy: Currently unsupported for Peer role	ERROR	Invalid Hash Alg : %d	ERROR
eapTimerCancel: Currently unsupported for Peer role	ERROR	Invalid Sign Alg : %d	ERROR
eapTimerHandler: Currently unsupported for Peer role	ERROR	No Memory Available	ERROR
pCtx is NULL: ERROR	ERROR	Certificate Request Failed	ERROR
tlsGlueCtxCreate failed	ERROR	File Open Failed	ERROR
eapVars is NULL	ERROR	File is Empty	ERROR
Context NULL: ERROR	ERROR	Memory Allocation Failed	ERROR
Initializing inner EAP auth: ERROR	ERROR	File Open Failed	ERROR
pCtx is NULL: ERROR	ERROR	File is Empty	ERROR
Memory Allocation Failed	ERROR	Error in executing DB update handler	ERROR

ファシリティ：システム（Admin）

ログメッセージ	緊急度	ログメッセージ	緊急度
Usage:%s <DBFile>	DEBUG	unable to register to UMI	ERROR
Could not open database: %s	DEBUG	sqlite3QueryResGet failed	ERROR
CPU LOG File not found	DEBUG	radSendtoServer: socket: %s	ERROR
MEM LOG File not found	DEBUG	radSendtoServer: bind() Failed: %s: %s	ERROR
cpuMemUsageDBUpdateHandler: update query: %s	DEBUG	radRecvfromServer: recvfrom() Failed: %s	ERROR
Printing the whole list after inserting	DEBUG	radRecvfromServer: Packet too small from %s:%d: %s	ERROR
%s at %d(minute) %d(hour) %d(dayOfMonth) %d(month)"	DEBUG	radCheckMsgAuth: Invalid Message- Authenticator length in"	ERROR
adpCmdExec exited with return code=%d	DEBUG	radDictLoad: couldn't open dictionary %s: %s	ERROR
%s op=%d row=%d	DEBUG	radBuildAndSendReq: Invalid Request Code %d	ERROR
sqlite3_mprintf failed	DEBUG	radPairAssign: bad attribute value length	ERROR
sqlite3QueryResGet failed: query=%s	DEBUG	radPairAssign: unknown attribute type %d	ERROR
Printing the whole list after delete	DEBUG	radPairNew: unknown attribute %d	ERROR
%s at %d(minute) %d(hour) %d(dayOfMonth) %d(month)"	DEBUG	radPairGen: Attribute(%d) has invalid length	ERROR
Printing the whole list after inserting	DEBUG	radPairValue: unknown attribute type %d	ERROR
%s at %d(minute) %d(hour) %d(dayOfMonth) %d(month)"	DEBUG	radPairValueLen: unknown attribute type %d	ERROR
email logs: No logging events enabled	DEBUG	radPairLocate: Attribute(%d) has invalid length	ERROR
%s	DEBUG	radPairUnpackDefault: Unknown- Attribute[%d]:	ERROR
Mail sent and the Database is reset.	DEBUG	radConfigure: can't open %s: %s	ERROR
Disabled syslog server	DEBUG	radConfigure: %s: line %d: bogus format: %s	ERROR
Event logs are full, sending logs to email	DEBUG	radConfAssert: No AuthServer Specified	ERROR
Email logs sending failed	DEBUG	radConfAssert: No Default Timeout Specified	ERROR
Packing attribute: %s	DEBUG	radConfAssert: No Default Retry Count Specified	ERROR
Server found: %s, secret: %s	DEBUG	radExtractMppeKey: Invalid MSMPPE- Key Length	ERROR
Packed Auth. Reqest: code:%d, id:%d, len:%d	DEBUG	radVendorMessage: Invalid Length in Vendor Message	ERROR
Sending Packet to %x:%d	DEBUG	radVendorMessage: Unknown Vendor ID received:%d	ERROR
Receiving Reply Packet....	DEBUG	radVendorAttrGet: Invalid Length in Vendor Message	ERROR
Verified Reply Packet Integrity	DEBUG	radVendorAttrGet: Unknown Vendor ID:%d	ERROR
Generated Reply Attribute-Value pairs	DEBUG	radVendorMessagePack: Unknown Vendor ID:%d	ERROR
Verified Message-Authenticator	DEBUG	radGetIPByName: couldn't resolve hostname: %s	ERROR
Unloaded RADIUS Dictionary	DEBUG	radGetHostIP: couldn't get hostname	ERROR
Adding Dictionary Attribute %s	DEBUG	radGetHostIP: couldn't get host IP address	ERROR
Adding Dictionary Value %s	DEBUG	radius dictionary loading failed	ERROR
Loaded Dictionary %s	DEBUG	Failed to set default timeout value	ERROR
Adding Dictionary Attribute '%s'	DEBUG	Failed to set default retries value	ERROR
Adding Dictionary Value %s	DEBUG	ERROR: incomplete DB update information.	ERROR
Receiving attribute: %s	DEBUG	old values result does not contain 2 rows	ERROR
Processing attribute: %s	DEBUG	sqlite3QueryResGet failed	ERROR
Processing attribute: %s	DEBUG	empty update. nRows=%d nCols=%d	ERROR
Processing attribute: %s	DEBUG	Error in executing DB update handler	ERROR
Processing attribute: %s	DEBUG	sqlite3QueryResGet failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
radConfGet: "	DEBUG	Invalid SQLITE operation code - %d	ERROR
Added Server %s:%d with "	DEBUG	sqlite3QueryResGet failed	ERROR
Added Server %s:%d with "	DEBUG	empty result. nRows=%d nCols=%d	ERROR
Default Timeout Set to %d	DEBUG	sqlite3QueryResGet failed	ERROR
Default Retry Count Set to %d	DEBUG	empty result. nRows=%d nCols=%d	ERROR
%s - %s : %d	DEBUG	RADIUS Accounting Exchange Failed	ERROR
Deleting Server %s:%d with "	DEBUG	Unable to set debug for radAcct.	ERROR
Adding RowId:%d to Server %s:%d with "	DEBUG	Unable to set debug level for radAcct.	ERROR
rowIds: %d - %d	DEBUG	ERROR: option value not specified	ERROR
Deleting Server %s:%d with "	DEBUG	ERROR: option value not specified	ERROR
RADIUS Deconfigured	DEBUG	Unable to initialize radius	ERROR
Found Option %s on line %d of file %s	DEBUG	radEapMsgQueueAdd: Invalid EAP packet length(%d)	ERROR
Setting Option %s with value %s	DEBUG	radEapRecvTask: invalid EAP code:%d	ERROR
RADIUS Configured	DEBUG	radEapRecvTask: Packet length mismatch %d, %d	ERROR
%d : Server %s:%d with "	DEBUG	No attributes received in Access- Challenge message	ERROR
DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	No State Attribute in Access- Challenge message	ERROR
Host IP address: %s	DEBUG	radEapRecvTask: "	ERROR
Adding Packet for existing cookie:%p	DEBUG	failed to initialize UMI	ERROR
Adding Packet and cookie:%p	DEBUG	umiRegister failed. errno=%d	ERROR
Releasing Packet and cookie:%p	DEBUG	Invalid arguments to ioctl handler	ERROR
Releasing Packet with cookie:%p	DEBUG	radEapSendRtn: Invalid Arguments	ERROR
Received EAP-Identity from Pnac: %s	DEBUG	radEapSendRtn: failed to allocate buffer	ERROR
Filling User-Name: %s	DEBUG	umiloctl failed	ERROR
Filling State:	DEBUG	failed to initialize EAP message queue	ERROR
Filling EAP-Message:	DEBUG	Unable to set debug for radEap.	ERROR
Filling Service-Type: %d	DEBUG	Unable to set debug level for radEap.	ERROR
Filling Framed-MTU: %d	DEBUG	ERROR: option value not specified	ERROR
Received Access-Challenge from Server	DEBUG	ERROR: option value not specified	ERROR
Sending Reply EAP Packet to Pnac	DEBUG	could not initialize MGMT framework	ERROR
Error sending packet to Pnac	DEBUG	Unable to initialize radius	ERROR
RADIUS Authentication Failed; "	DEBUG	Unable to set debug for radEap.	ERROR
RADIUS Authentication Successful; "	DEBUG	Unable to set debug level for radEap.	ERROR
Got Packet with cookie:%p	DEBUG	ERROR: option value not specified	ERROR
Next DNS Retry after 1 min	DEBUG	Unable to initialize radius	ERROR
Next Synchronization after"	DEBUG	Invalid username or password	ERROR
Next Synchronization after"	DEBUG	Unable to set debug for radAuth.	ERROR
Next Synchronization after %d \	DEBUG	Unable to set debug level for radAuth.	ERROR
Primary is not available, "	DEBUG	ERROR: option value not specified	ERROR
Secondary is not available, "	DEBUG	Unable to initialize radius	ERROR
Invalid value for use default servers, "	DEBUG	Invalid username, challenge or response	ERROR
No server is configured, "	DEBUG	Unable to set debug for radAuth.	ERROR
Backing off for %d seconds	DEBUG	Unable to set debug level for radAuth.	ERROR
Requesting time from %s	DEBUG	ERROR: option value not specified	ERROR
Synchronized time with %s	DEBUG	Unable to initialize radius	ERROR
Received KOD packet from %s	DEBUG	Invalid username or password	ERROR
No suitable server found %s	DEBUG	usage : %s <DB fileName>	ERROR
Received Invalid Length packet from %s	DEBUG	ntpd : umi initialization failed	ERROR
Received Invalid Version packet from %s	DEBUG	ntpd : ntpInit failed	ERROR
Received Invalid Mode packet from %s	DEBUG	ntpd : ntpMgmtInit failed	ERROR
Request Timed out from %s	DEBUG	There was an error while getting the timeZoneChangeScript."	ERROR
Looking Up %s	DEBUG	unexpected reply from %d cmd=%d !	ERROR
Timezone difference :%d	DEBUG	cmd %d not supported. caller %d	ERROR
Could not open file: %s	DEBUG	default reached	ERROR
Could not read data from file	DEBUG	Unable to initialize ntpControl	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
ntpTblHandler	DEBUG	ntpMgmt : Couldn't open database %s	ERROR
status: %d	DEBUG	ERROR : incomplete DB update information	ERROR
tz: %d	DEBUG	empty update. nRows=%d nCols=%d	ERROR
DayLightsaving: %d	DEBUG	Error in executing DB update handler	ERROR
pNtpControl- >ServerNames[PRIMARY_SERVER]: %s	DEBUG	requestNtpTime: Invalid addr	ERROR
pNtpControl- >ServerNames[SECONDARY_SERVER] : %s	DEBUG	failed to take lock for compId: %d	ERROR
DS: %d	DEBUG	failed to convert ioctl args to buffer for"	ERROR
pPriServ %s	DEBUG	request timeout dst(%d) <-- src(%d)	ERROR
pSecServ %s	DEBUG	failed to take lock for compId: %d	ERROR
Making request from %d --> %d	DEBUG	umiIoctlArgsToBuf: failed to allocate memory	ERROR
sent request dst(%d) <-- src(%d) using option %d	DEBUG	umiRecvFrom: could not allocate memory	ERROR
received request too small!(%d bytes)	DEBUG	adpMalloc failed	ERROR
Received a UMI request from %d	DEBUG	context with ID: %d already registered	ERROR
sent a reply src(%d) ---> dst(%d)	DEBUG	Failed to allocate memory for creating UMI context	ERROR
umiRegister (%x,%x,%x,%x)	DEBUG	Failed to create recvSem for UMI context	ERROR
srcId=%d(%s) --> destId=%d(%s) cmd=%d inLen=%d outLen=%d	DEBUG	Failed to create mutex locks for UMI context	ERROR
waiting for reply...Giving Up	DEBUG	Failed to create mutex recvQLock for UMI context	ERROR
No request in the list after semTake	DEBUG	Invalid arguments to umiloctl	ERROR
reply timeout	DEBUG	could not find the destination context	ERROR
timeout after semTake	DEBUG	memPartAlloc for %d size failed	ERROR
srcId=%d(%s) <-- destId=%d(%s) cmd=%d	DEBUG	memPartAlloc for %d size failed	ERROR
Un-registerting component with Id %d	DEBUG	No Handler registered for this UMI context	ERROR
failed to send ioctl request: dst(%d) <--- src(%d)	DEBUG	Couldn't find component with ID (%d),"	ERROR
processed a reply dst(%d) <-- src(%d)	DEBUG	id=%d handler=%x	ERROR
request with no result option dst(%d) <-- src(%d)	DEBUG	Received NULL buffer in umiBufToIoctlArgs()	ERROR
cmd = %s	DEBUG	usbMgmtInit: unable to open the database file %s	ERROR
cmdstring is %s %s:%d	DEBUG	call to printConfig failed	ERROR
Calling printerConfig binary ...	DEBUG	Failed to Disable Network Storage" ERROR	
Calling unmount for USB ...	DEBUG	Some error occurred while removing device	ERROR
Calling mount for USB ...	DEBUG	Some error occurred while removing device	ERROR
usbdevice is %d %s:%d	DEBUG	Sqlite update failed	ERROR
Query string: %s	DEBUG	Failed to enable printer properly	ERROR
sqlite3QueryResGet failed.Query:%s	DEBUG	Failed to mount device on system	ERROR
%s: 1. usb is already disconnected for old usb type. "	DEBUG	Failed to enable network storage device"	ERROR
%s: 2.call disable for new usb type !	DEBUG	Failed to mount device on system	ERROR
%s: 3. usb is already disconnected for old usb type. "	DEBUG	Sqlite update failed	ERROR
%s: 4. Disabled old usb type . Now "	DEBUG	USB1 Touch failed	ERROR
usbdevice is %d %s:%d	DEBUG	USB2 Touch failed	ERROR
USB: failed to begin transaction: %s	DEBUG	Sqlite update failed	ERROR
USB: SQL error: %s pSetString = %s	DEBUG	Failed query: %s	ERROR
USB: failed to commit transaction: %s	DEBUG	Failed to execute usb database update handler	ERROR
USB: updated table: %s	DEBUG	Usage:%s <DBFile> <opType> <tblName> <rowId>	ERROR
USB: returning with status: %s	DEBUG	Illegal invocation of snmpConfig (%s)	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	Invalid Community Access Type	ERROR
executing %s status =%d	DEBUG	Invalid User Access Type	ERROR
executing %s	DEBUG	Invalid Security Level	ERROR
%s returned status=%d	DEBUG	Invalid Authentication Algorithm	ERROR
%s returned status=%d	DEBUG	Invalid Privacy Algorithm	ERROR
snmpd.conf not found	DEBUG	Invalid Argument	ERROR
[SNMP_DEBUG] : Fwrite Successful	DEBUG	Failed to allocate memory for engineID	ERROR
[SNMP_DEBUG] : Fwrite failed	DEBUG	[SNMP_DEBUG]: Failed to get host address	ERROR
radPairGen: received unknown attribute %d of length %d	WARN	[SNMP_DEBUG] : FOPEN failed	ERROR
radPairGen: %s has unknown type	WARN	sqlite3QueryResGet failed.Query:%s	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
radPairLocate: unknown attribute %ld of length %d	WARN	sqlite3QueryResGet failed.Query:%s	ERROR
radPairLocate: %s has unknown type	WARN	Invalid Security Level	ERROR
Illegal invocation of cpuMemUsage (%s)	ERROR	Invalid Authentication Algorithm	ERROR
cpuMemUsageDBUpdateHandler: SQL error: %s	ERROR	Invalid Privacy Algorithm	ERROR
unable to open the DB file %s	ERROR	Failed to Get Host Address	ERROR
umiInit failed	ERROR	Invalid version	ERROR
unable to register to UMI	ERROR	snmp v3 Trap Configuration Failed	ERROR
Error Reading from the Database.	ERROR	sqlite3QueryResGet failed query:%s	ERROR
short DB update event request!	ERROR	sqlite3QueryResGet failed.Query:%s	ERROR
Error in executing DB update handler	ERROR	Failed to Open Snmp Configuration File	ERROR
adpListNodeRemove : Returned with an error	ERROR	Failed to write access control entries	ERROR
command too long. Try increasing "	ERROR	Failed to write snmpv3 users entries	ERROR
failed to allocate memory for CRON_NODE	ERROR	Failed to write snmp trap entries	ERROR
sqlite3QueryResGet failed	ERROR	Failed to write system entries.	ERROR
There was an error while reading the schedules.	ERROR	Failed to restart snmp	ERROR
unable to register to UMI	ERROR	%s failed with status	ERROR
short DB update event request!	ERROR	Error in executing DB update handler	ERROR
malloc(DB_UPDATE_NODE) failed	ERROR	%s: Unable to open file: %s	ERROR
short ifDev event request!	ERROR	RADVD start failed	ERROR
sqlite3_mprintf failed	ERROR	RADVD stop failed	ERROR
no component id matching %s	ERROR	failed to create/open RADVD configuration file %s	ERROR
umiIoctl (%s, UMI_CMD_DB_UPDATE(%d)) failed.	ERROR	Restoring old configuration..	ERROR
sqlite3_mprintf failed	ERROR	failed to write/update RADVD configuration file	ERROR
sqlite3_mprintf failed	ERROR	upnpDisableFunc failed	ERROR
no component id matching %s	ERROR	upnpEnableFunc failed	ERROR
umiIoctl (%s, UMI_CMD_IFDEV_EVENT(%d)) failed.	ERROR	sqlite3QueryResGet failed.Query:%s	ERROR
klogctl(9) failed	ERROR	Error in executing DB update handler	ERROR
malloc failed for %d bytes	ERROR	unable to open the DB file %s	ERROR
klogctl(4) failed	ERROR	umiInit failed	ERROR
emailLogs: Invalid Number of Arguments!! Exiting.	ERROR	unable to register to UMI	ERROR
sqlite3QueryResGet failed	ERROR	short DB update event request!	ERROR
Could not execute the smtpClient.	ERROR	short ifDev event request!	ERROR
Error while cleaning the database.Exiting. %s	ERROR	sqlite3_mprintf failed	ERROR
		%s failed. status=%d	ERROR

ファシリティ：システム（**Firewall**）

ログメッセージ	緊急度	ログメッセージ	緊急度
Enabling rule for protocol binding.	DEBUG	Disable all NAT rules.	DEBUG
Disabling rule for protocol binding.	DEBUG	Enable all NAT rules.	DEBUG
Enabling Remote SNMP on WAN.	DEBUG	Enabling NAT URL filter rules.	DEBUG
Disabling Remote SNMP on WAN	DEBUG	Restarting all NAT rules.	DEBUG
wan traffic counters are restared	DEBUG	Deleting schedule based firewall rules.	DEBUG
Traffic limit has been reached	DEBUG	Deleting schedule based firewall rules from DB.	DEBUG
Traffic meter monthly limit has been changed to %d.	DEBUG	Update schedule based firewall rules in DB.	DEBUG
Enabling traffic meter for only dowload.	DEBUG	Restart schedule based firewall rules.	DEBUG
Enabling traffic meter for both directions.	DEBUG	inter vlan routing enabled	DEBUG
Enabling traffic meter with no limit.	DEBUG	inter vlan routing disabled	DEBUG
Email alert in traffic meter disabled.	DEBUG	Disabling Content Filter for %d	DEBUG
Email alert in traffic meter enabled.	DEBUG	Enabling Content Filter for %d	DEBUG
Traffic Meter:Monthly limit %d MB has been "	DEBUG	./src/firewall/linux/user/firewalld.c:59:#u ndef ADP_DEBUG2	DEBUG
Traffic Metering: Adding rule to drop all traffic	DEBUG	./src/firewall/linux/user/firewalld.c:61:#d efine ADP_DEBUG2 printf	DEBUG
Traffic Metering: %sabling Email traffic	DEBUG	Enabling Source MAC Filtering	DEBUG
Disabling attack checks for IPv6 rules.	DEBUG	Disabling Source MAC Filtering	DEBUG
Enabling attack checks for IPv6 rules.	DEBUG	Adding MAC Filter Policy for Block & Permit Rest	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
Configuring one to one NAT settings with %s private start IP "	DEBUG	Adding MAC Filter Policy for Permit & Block Rest	DEBUG
Deleting forward one to one NAT having setting %s private start"	DEBUG	Restarting Source MAC Address Policy	DEBUG
Disabling attack check for Block ping to WAN interface.	DEBUG	Disabling Firewall Rule for DHCP Relay Protocol	DEBUG
Disabling attack check for Stealth mode for tcp	DEBUG	Enabling Firewall Rule for DHCP Relay Protocol	DEBUG
Disabling attack check for Stealth mode for udp	DEBUG	prerouting Firewall Rule add for Relay failed	DEBUG
Disabling attack check for TCP Flood.	DEBUG	prerouting Firewall Rule add for Relay failed	DEBUG
Disabling attack check for UDP Flood.	DEBUG	Deleting MAC Filter Policy for Address %s	DEBUG
Disabling attack check for IPSec.	DEBUG	Adding MAC Filter Policy for Address %s	DEBUG
Disabling attack check for PPTP.	DEBUG	Disabling Firewall Rules for DMZ host	DEBUG
Disabling attack check for L2TP.	DEBUG	Enabling Firewall Rules for DMZ host	DEBUG
Disabling attack check for UDP Flood.	DEBUG	Disabling Firewall Rules for Spill Over Load Balancing	DEBUG
Disabling attack check for IPSec.	DEBUG	Disabling Firewall Rules for Load Balancing	DEBUG
Disabling attack check for PPTP.	DEBUG	Enabling Firewall Rules for Load Balancing	DEBUG
Disabling attack check for L2TP.	DEBUG	Enabling Firewall Rules for Spill Over Load Balancing	DEBUG
Enabling attack check for Block ping to WAN "	DEBUG	Enabling Firewall Rules for Auto Failover	DEBUG
Enabling attack check for Stealth Mode for tcp.	DEBUG	Enabling Firewall Rules for Load Balancing .	DEBUG
Enabling attack check for Stealth Mode for udp.	DEBUG	Enabling Firewall Rules for Spill Over Load Balancing .	DEBUG
Enabling attack check for TCP Flood.	DEBUG	Enabling Firewall Rules for Auto Failover	DEBUG
Enabling attack check for UDP Flood.	DEBUG	Deleting BlockSites Keyword \	DEBUG
Enabling attack check for IPSec.	DEBUG	Enabling BlockSites Keyword \	DEBUG
Enabling attack check for PPTP.	DEBUG	Disabling BlockSites Keyword \	DEBUG
Enabling attack check for L2TP.	DEBUG	Updating BlockSites Keyword from \	DEBUG
Enabling attack check for UDP Flood.	DEBUG	Inserting BlockSites Keyword \	DEBUG
Enabling attack check for IPSec.	DEBUG	Deleting Trusted Domain \	DEBUG
Enabling attack check for PPTP.	DEBUG	Adding Trusted Domain \	DEBUG
Enabling attack check for L2TP.	DEBUG	Restarting Schedule Based Firewall Rules	DEBUG
Enabling DoS attack check with %d SyncFlood detect rate, "	DEBUG	Enabling Remote SNMP	DEBUG
Disabling DoS attack check having %d SyncFlood detect rate,"	DEBUG	Disabling Remote SNMP	DEBUG
Enabling ICSA Notification Item for ICMP notification.	DEBUG	Enabling Remote SNMP	DEBUG
Enabling ICSA Notification Item for Fragmented Packets.	DEBUG	Disabling DOS Attacks	DEBUG
Enabling ICSA Notification Item for Multi cast Packets.	DEBUG	Enabling DOS Attacks	DEBUG
Disabling ICSA Notification Item for ICMP notification.	DEBUG	Enabling DOS Attacks	DEBUG
Disabling ICSA Notification Item for Fragmented Packets.	DEBUG	Restarting Firewall [%d]:[%d] For %s	DEBUG
Disabling ICSA Notification Item for Multicast Packets.	DEBUG	restartStatus = %d for LogicalIfName = %s	DEBUG
Adding IP/MAC binding rule for %s MAC address "	DEBUG	Deleting Lan Group %s	DEBUG
Deleting IP/MAC binding rule for %s MAC "	DEBUG	Adding Lan Group %s	DEBUG
./src/firewall/linux/user/firewalld.c:60:#un def ADP_DEBUG	DEBUG	Deleting lan host %s from group %s	DEBUG
./src/firewall/linux/user/firewalld.c:62:#def ine ADP_DEBUG printf	DEBUG	Adding lan host %s from group %s	DEBUG
Restarting traffic meter with %d mins, %d hours, "	DEBUG	Disabling Firewall Rule for IGMP Protocol	DEBUG
Updating traffic meter with %d mins, %d hours, "	DEBUG	Enabling Firewall Rule for IGMP Protocol	DEBUG
Deleting traffic meter.	DEBUG	Deleting IP/MAC Bind Rule for MAC address %s and IP "	DEBUG
Disabling block traffic for traffic meter.	DEBUG	Adding IP/MAC Bind Rule for MAC address %s and IP	DEBUG
Enabling traffic meter.	DEBUG	Deleting Protocol Bind Rule for Service %s	DEBUG
Adding lan group %s.	DEBUG	Deleting Protocol Bind Rule for Service %s	DEBUG
Deleting lan group %s.	DEBUG	Deleting Protocol Bind Rule for Service %s	DEBUG
Renaming lan group from %s to %s.	DEBUG	Adding Protocol Bind Rule for Service %s	DEBUG
Deleting host %s from %s group.	DEBUG	%s Session Settings	DEBUG
Adding host %s to %s group.	DEBUG	Restarting IPv6 Firewall Rules...	DEBUG
Enabling Keyword blocking for %s keyword.	DEBUG	Deleting Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Disabling keyword Blocking for %s keyword .	DEBUG	Deleting Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Deleting trusted domain with keyword %s.	DEBUG	Enabling Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Adding %s keyword to trusted domain.	DEBUG	Disabling Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
Enabling Management Access from Internet on port	DEBUG	Enabling Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Enabling remote access management for IP address range"	DEBUG	Disabling Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Enabling remote access management to only this PC.	DEBUG	Adding Port Trigger Rule for %d:%d:%d:%d:%d	DEBUG
Disabling Management Access from Internet on port %d	DEBUG	Enabling Content Filter	DEBUG
Disabling remote access management for IP address range"	DEBUG	Disabling Content Filter	DEBUG
Disabling remote access management only to this PC.	DEBUG	Enabling Content Filter	DEBUG
MAC Filtering %sabled for BLOCK and PERMIT REST.	DEBUG	Setting NAT mode for pLogicalIfName = %s	DEBUG
MAC Filtering %sabled for PERMIT and BLOCK REST.	DEBUG	Enabling DROP for INPUT	DEBUG
Enabling Content Filtering.	DEBUG	Enabling DROP for FORWARD	DEBUG
Disabling Content Filtering.	DEBUG	Enabling NAT based Firewall Rules	DEBUG
Deleting rule, port triggering for protocol TCP.	DEBUG	Setting transparent mode for pLogicalIfName \	DEBUG
Deleting rule, port triggering for protocol UDP.	DEBUG	Enabling Accept for INPUT	DEBUG
Deleting rule, port triggering for protocol TCP.	DEBUG	Enabling Accept for FORWARD	DEBUG
Deleting rule, port triggering for protocol UDP.	DEBUG	Setting Routing mode for pLogicalIfName \	DEBUG
Enabling rule, port triggering for protocol TCP.	DEBUG	Enabling DROP for INPUT	DEBUG
Enabling rule, port triggering for protocol UDP.	DEBUG	Enabling DROP for FORWARD	DEBUG
Enabling rule, port triggering for protocol TCP.	DEBUG	Disabling NAT based Firewall Rules	DEBUG
Enabling rule, port triggering for protocol UDP.	DEBUG	Enabling Firewall Rules for URL Filtering & "	DEBUG
Enabling DNS proxy.	DEBUG	Adding Firewall Rule for RIP Protocol	DEBUG
Restarting DNS proxy.	DEBUG	Restarting Schedule Based Firewall Rules	DEBUG
checking DNS proxy for Secure zone.	DEBUG	enabling IPS checks between %s and %s zones.	DEBUG
checking DNS proxy for Public zone.	DEBUG	disabling IPS checks between %s and %s zones.	DEBUG
Enabling Block traffic from %s zone.	DEBUG	Stopping IPS...%s	DEBUG
Configuring firewall session settings for "	DEBUG	IPS started.	DEBUG
Disabling DMZ	DEBUG	Route already exists	DEBUG
Disabling WAN-DMZ rules .	DEBUG	Route addition failed: Network Unreachable	DEBUG
Enabling WAN DMZ rules .	DEBUG	Route addition failed: Network is down	DEBUG
Restarting DMZ rule having %s address with %s address.	DEBUG	Route addition failed	DEBUG
Enabling LAN DHCP relay.	DEBUG	Failed to add rule in iptables	DEBUG
OneToOneNat configured successfully	DEBUG	Failed to delete rule from iptables	DEBUG
OneToOneNat configuration failed	DEBUG	fwLBSpillOverConfigure: Something going wrong here	ERROR
Deleting scheduled IPv6 rules.	DEBUG	fwLBSpillOverConfigure: unable to get interfaceName	ERROR
delete from FirewallRules6 where ScheduleName = '%s'.	DEBUG	fwLBSpillOverConfigure: Could not set PREROUTING rules	ERROR
Update FirewallRules6 where ScheduleName = '%s' to New "	DEBUG	fwLBSpillOverConfigure: Could not set POSTROUTING rules	ERROR
Dns proxy Restart failed	DEBUG	fwLBSpillOverConfigure: Something going wrong Here	ERROR
deleting interface to ifgroup failed	DEBUG	fwL2TPGenericRules.c: unable to open the database file "	ERROR
adding interface to ifgroup failed	DEBUG	fwL2TPGenericRules.c: inet_aton failed	ERROR
deleting interface pVirtIface %s from ifgroup %d"	DEBUG	fwPPTPGenericRules.c: unable to open the database file "	ERROR
adding interface pVirtIface %s to ifgroup %d failed	DEBUG	fwPPTPGenericRules.c: inet_aton failed	ERROR
Deleting IP address %s.	DEBUG	DNS proxy firewall rule add failed for %s	ERROR
Adding new IP address %s.	DEBUG	deleting interface %s from ifgroup %d failed	ERROR
Updating old IP address %s to new IP address %s.	DEBUG	adding interface %s to ifgroup %d failed	ERROR
Restarting Firewall For %s Address Update from %s:%s	DEBUG	nimfBridgeTblHandler: unable to get interfaceName	ERROR
Disabling Firewall Rule for MSS packet marking	DEBUG	nimfBridgeTblHandler: \	ERROR
Enabling Firewall Rule for MSS packet marking	DEBUG	nimfBridgeTblHandler: unable to get \	ERROR
Enabling packet marking rule for %s IDLE timer	DEBUG	Failed to %s traffic from %s to %s to IPS.	ERROR
Deleted firewall rule %s for service %s with action %s	DEBUG	Failed to %s traffic from %s to %s to IPS.	ERROR
%s firewall rule %s for service %s with action %s	DEBUG	failed to start IPS service.	ERROR
Added firewall rule %s for service %s with action %s	DEBUG	Timeout in waiting for IPS service to start.	ERROR
Deleting inbound(WAN-LAN) firewall rule.	DEBUG	Usage:%s <DBFile> <opType> <tblName> <rowId> "	ERROR
Deleting inbound(WAN-DMZ) firewall rule.	DEBUG	xlr8NatConfig: illegal invocation of (%s)	ERROR
RIPng disabled.	DEBUG	Illegal invocation of [%s]	ERROR
RIPng enabled.	DEBUG	xlr8NatMgmtTblHandler: failed query: %s	ERROR
Disable IPv6 firewall rule.	DEBUG	Could not open file: %s	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Enable IPv6 firewall rule.	DEBUG	Rip Error Command Too Long	ERROR
Deleting IGMP proxy rule.	DEBUG	No authentication for Ripv1	ERROR
Enable IGMP proxy rule.	DEBUG	Invalid Rip Direction	ERROR
Restarting IGMP rule.	DEBUG	Invalid Rip Version	ERROR
Traffic meter enabled with no limit type.	DEBUG	Invalid Password for 1st Key	ERROR
Traffic meter enabled for only download.	DEBUG	Invalid Time for 1st Key	ERROR
Traffic meter enabled for both directions.	DEBUG	Invalid Password for 2nd Key	ERROR
Deleted firewall rule %s for service %s with action %s	DEBUG	Invalid Time for 2nd Key	ERROR
%s firewall rule %s for service %s with action %s	DEBUG	Invalid First KeyId	ERROR
Added firewall rule %s for service %s with action %s	DEBUG	Invalid Second KeyId	ERROR
Enabling Inter VLAN routing.	DEBUG	Invalid Authentication Type	ERROR
Updating inter VLAN routing status.	DEBUG	ripDisable failed	ERROR
Deleting inter VLAN routing.	DEBUG	ripEnable failed	ERROR

ファシリティ：システム（無線）

ログメッセージ	緊急度	ログメッセージ	緊急度
(node=%s) setting %s to val = %d	DEBUG	sqlite3QueryResGet failed	ERROR
Custom wireless event: '%s'	DEBUG	sqlite3QueryResGet failed	ERROR
Wireless event: cmd=0x%x len=%d	DEBUG	VAP(%s) set beacon interval failed	ERROR
New Rogue AP (%02x:%02x:%02x:%02x:%02x:%02x) detected	DEBUG	VAP(%s) set DTIM interval failed	ERROR
WPS session in progress, ignoring enrolle assoc request	DEBUG	VAP(%s) set RTS Threshold failed	ERROR
ran query %s	DEBUG	VAP(%s) set Fragmentation Threshold failed	ERROR
DBUpdate event: Table: %s opCode:%d rowId:%d	DEBUG	VAP(%s) set Protection Mode failed	ERROR
%sing VAPs using profile %s	DEBUG	VAP(%s) set Tx Power failed	ERROR
%sing VAP %s	DEBUG	WDS Profile %s not found	ERROR
ran query %s	DEBUG	Failed to initalize WPS on %s	ERROR
%sing VAP instance %s	DEBUG	failed to get profile %s	ERROR
VAP(%s) set Short Preamble failed	DEBUG	could not initialize MGMT framework	ERROR
VAP(%s) set Short Retry failed	DEBUG	could not initialize MGMT framework	ERROR
VAP(%s) set Long Retry failed	DEBUG	dot11VapBssidUpdt SQL error: %s	ERROR
Decrypting context with key %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Unknown IAPP command %d received.	DEBUG	KDOT11_GET_PARAM(IEEE80211_I OC_CHANNEL) failed	ERROR
unexpected reply from %d cmd=%d !	DEBUG	Failed to get the channel setting for %s	ERROR
unexpected reply from %d cmd=%d !	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
Recvied DOT11_EAPOL_KEYMSG	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
shutting down AP:%s	DEBUG	profile %s not found	ERROR
APCtx Found	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
APCtx Not-Found	DEBUG	Interface name and policy must be specified	ERROR
node not found *:*:*:%x:%x:%x	DEBUG	Interface name and policy must be specified	ERROR
error installing unicast key for %s	DEBUG	invalid ACL type %d	ERROR
cmd =%d i_type =%d i_val=%d	DEBUG	interface name not specified	ERROR
join event for new node %s	DEBUG	interface name not specified	ERROR
wpa/rsn IE id %d/%d not supported	DEBUG	Invalid interface - %s specified	ERROR
wpa IE id %d not supported	DEBUG	buffer length not specified	ERROR
leave event for node %s	DEBUG	Invalid length(%d) specified	ERROR
NodeFree request for node : %s	DEBUG	failed created iappdLock	ERROR
installing key to index %d	DEBUG	failed to create cipher contexts.	ERROR
iReq.i_val : %d	DEBUG	unable to register to UMI	ERROR
pIfName : %s	DEBUG	iappSockInit() failed	ERROR
iReq.i_val : %d	DEBUG	iappInit got error, unregistering it with UMI	ERROR
setting mode: %d	DEBUG	umiIoctl(UMI_COMP_UDOT11,%d,%d) failed	ERROR
Global counter wrapped, re-generating...	DEBUG	umiIoctl(UMI_COMP_KDOT11,%d,%d) failed	ERROR
Got PNAC_EVENT_PREAUTH_SUCCESS event for : %s	DEBUG	UDP failed, received Length is %d	ERROR
event for non-existent node %s	DEBUG	umiIoctl(UMI_COMP_KDOT11,	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
PNAC_EVENT_EAPOL_START event received	DEBUG	umiloctl(UMI_COMP_UDOT11,%d,%d) \	ERROR
PNAC_EVENT_EAPOL_LOGOFF event received	DEBUG	umiloctl(UMI_COMP_KDOT11,%d,%d) \	ERROR
PNAC_EVENT_REAUTH event received	DEBUG	No IAPP Node found for req id %d	ERROR
PNAC_EVENT_AUTH_SUCCESS event received	DEBUG	umiloctl(UMI_COMP_UDOT11,%d,%d) \	ERROR
PNAC_EVENT_PORT_STATUS_CHAN GED event received	DEBUG	umiloctl(UMI_COMP_KDOT11,%d,%d) \	ERROR
unsupported event %d from PNAC	DEBUG	umiloctl(UMI_COMP_UDOT11,%d,%d) failed	ERROR
event for non-existent node %s. Create new node.	DEBUG	UDP socket is not created	ERROR
Add new node to DOT11 Node list	DEBUG	UDP send failed	ERROR
Update dot11STA database	DEBUG	IAPP: socket (SOCK_STREAM) failed.	ERROR
Add PMKSA to the list	DEBUG	IAPP: TCP connect failed to %s.	ERROR
eapolRecvAuthKeyMsg: received key message	DEBUG	cmd %d not supported.sender=%d	ERROR
node not found	DEBUG	umiloctl(UMI_COMP_KDOT11,%d,%d) failed	ERROR
eapolRecvKeyMsg: replay counter not incremented	DEBUG	IAPP-CACHE-NOTIFY-REQUEST send to	ERROR
eapolRecvKeyMsg: replay counter is not same	DEBUG	./src/dot11/iapp/iappLib.c:1314: ADP_ERROR (	ERROR
processing pairwise key message 2	DEBUG	BSSID value passed is NULL	ERROR
RSN IE matching: OK	DEBUG	reserved requestId is passed	ERROR
processing pairwise key message 4	DEBUG	interface name is NULL	ERROR
processing group key message 2	DEBUG	IP address value passed is NULL	ERROR
processing key request message from client	DEBUG	opening receive UDP socket failed	ERROR
WPA version %2x %2x not supported	DEBUG	enabling broadcast for UDP socket failed	ERROR
(%s) group cipher %2x doesn't match	DEBUG	opening receive TCP socket for new AP failed	ERROR
(%s)Pairwise cipher %s not supported	DEBUG	./src/dot11/iapp/iappLib.c:1784: ADP_ERROR(	ERROR
(%s) authentication method %d not supported	DEBUG	./src/dot11/iapp/iappLib.c:1794: ADP_ERROR(	ERROR
%s:Auth method=%s pairwise cipher=%s IE size=%d	DEBUG	./src/dot11/iapp/iappLib.c:1803: ADP_ERROR(	ERROR
WPA version %2x %2x not supported	DEBUG	failed created dot11dLock.	ERROR
Unable to obtain IE of type %d	DEBUG	failed initialize profile library.	ERROR
PTK state changed from %s to %s	DEBUG	failed to create cipher contexts.	ERROR
using PMKSA from cache	DEBUG	unable to register to UMI	ERROR
PTK GK state changed from %s to %s	DEBUG	could not create MIB tree	ERROR
GK state changed from %s to %s	DEBUG	unable to register to PNAC	ERROR
Sending PTK Msg1	DEBUG	Max registration attempts by DOT11 to PNAC exceeded	ERROR
Sending PTK Msg3	DEBUG	Creation of EAP WPS Profile Failed	ERROR
Sending GTK Msg1	DEBUG	umiloctl(UMI_COMP_IAPP,%d) failed	ERROR
sending EAPOL pdu to PNAC...	DEBUG	DOT11_RX_EAPOL_KEYMSG: unknown ifname %s	ERROR
creating pnac authenticator with values %d %d - %s	DEBUG	cmd %d not supported.sender=%d	ERROR
Profile %s does not exist	DEBUG	inteface name passed is NULL	ERROR
IAPP initialized.	DEBUG	BSSID passed is NULL	ERROR
Encrypting context key=%s for	DEBUG	inteface name passed is NULL	ERROR
could not find access point context for %s	DEBUG	unable to allocate memory for DOT11_CTX	ERROR
join event for existing node %s	DEBUG	unable to install wme mapping on %s	ERROR
failed to send PNAC_FORCE_AUTHORIZED "	DEBUG	unable to get %s mac address	ERROR
failed to send PNAC_AUTHORIZED "	DEBUG	Failed to set %s SSID	ERROR
failed to send PNAC_VAR_KEY_AVAILABLE (TRUE) "	DEBUG	Failed to set SSID broadcast status	ERROR
failed to send PNAC_VAR_KEY_TX_EN (TRUE) "	DEBUG	Failed to set PreAuth mode	ERROR
failed to send PNAC_VAR_KEY_TX_EN (FALSE) "	DEBUG	unable to install key	ERROR
failed to send PNAC_FORCE_AUTHORIZED "	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_AUTHMODE failed	ERROR
failed to send PNAC_AUTHORIZED "	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_PRIVACY failed	ERROR
mic verification: OK	DEBUG	wpaInit failed	ERROR
pnacIfConfig: Invalid supplicant"	DEBUG	dot11InstallProfile: unable to get interface index	ERROR
Failed to process user request	DEBUG	adpHmacInit(%s) failed	ERROR
Failed to process user request - %s(%d)	DEBUG	interface %s not found	ERROR
pnacIfConfigUmiloctl: umiloctl failed	DEBUG	AP not found on %s	ERROR
pnacIfConfigUmiloctl: usrPnac returned %d	DEBUG	keyLen > PNAC_KEY_MAX_SIZE	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
pnacIfConfigUmiloctl: usrPnac returned %d	DEBUG	Invalid profile name passed	ERROR
pnacIfConfigUmiloctl: usrPnac returned %d	DEBUG	Creation of WPS EAP Profile failed	ERROR
pnacKernNotifier: invalid PAE configuration "	DEBUG	unsupported command %d	ERROR
From pnacEapDemoAuthRecv: unsupported response "	DEBUG	device %s not found	ERROR
From pnacEapDemoAuthRecv: invalid codes received	DEBUG	unsupported command %d	ERROR
From pnacRadXlateDemoRecv: received unknown "	DEBUG	dot11NodeAlloc failed	ERROR
From pnacRadXlateDemoRecv: invalid codes received	DEBUG	Getting WPA IE failed for %s	ERROR
Error from pnacRadXlateDemoRecv: malloc failed	DEBUG	Getting WPS IE failed for %s	ERROR
From pnacRadXlateRadPktHandle: received a non-supported"	DEBUG	Failed initialize authenticator for node %s	ERROR
Only md5 authentication scheme currently supported. "	DEBUG	Failed to get the system up time while adding node %s	ERROR
Message from authenticator:	DEBUG	error creating PNAC port for node %s	ERROR
from pnacPDUXmit: bufsize = %d, pktType = %d,"	DEBUG	dot11NodeAlloc failed	ERROR
pnacPDUXmit: sending eap packet. code = %d, "	DEBUG	Invalid arguments.	ERROR
pnacRecvRtn: no corresponding pnac port pae found	DEBUG	umiloctl(UMI_COMP_IAPP,%d) failed	ERROR
sending unicast key	DEBUG	Invalid IE.	ERROR
sending broadcast key	DEBUG	umiloctl(UMI_COMP_KDOT11_VAP, %d) failed	ERROR
from pnacAuthPAEDisconnected: calling pnacTxCannedFail	DEBUG	umiloctl(UMI_COMP_KDOT11,%d ,%d) failed	ERROR
from pnacAuthPAEForceUnauth: calling pnacTxCannedFail	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME_CWMIN failed	ERROR
state changed from %s to %s	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME_CWMAX failed	ERROR
PNAC user comp id not set. dropping event %d	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME_AIFS failed	ERROR
sending event %d to %d	DEBUG	KDOT11_SET_PARAM:80211_IOC_WME_TXOPLIMIT failed	ERROR
requesting keys informantion from %d	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME_ACM failed	ERROR
pnacUmiPortPaeParamSet: error in getting port pae	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WME failed	ERROR
pnacUmiPortPaeParamSet: invalid param - %d	DEBUG	invalid group cipher %d	ERROR
pnacRecvASInfoMessage: Skey of length %d set	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_MCASTCIPHER failed	ERROR
pnacRecvASInfoMessage: reAuthPeriod set to: %d	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_MCASTKEYLEN failed	ERROR
pnacRecvASInfoMessage: suppTimeout set to: %d	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_UCASTCIPHERS failed	ERROR
PORT SUCCESSFULLY DESTROYED	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_KEYMGTALGS failed	ERROR
creating physical port for %s	DEBUG	KDOT11_SET_PARAM:IEEE80211_I OC_WPA failed	ERROR
pnacAuthInit: using defualt pnacAuthParams	DEBUG	unknow cipher type = %d	ERROR
pnacSuppInit: using defualt pnacSuppParams	DEBUG	umiloctl(UMI_COMP_IAPP,%d) failed	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	invalid media value=%d	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	invalid mediaOpt value=%d	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	invalid mode value=%d	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	dot11PnacIfCreate failed	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	wpaPRF failed	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	Error generating global key counter	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	wpaCalcMic: unsupported key descriptor version	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	integrity failed. need to stop all stations "	ERROR
Error from pnacCombinedStMachTriggerFunc: "	DEBUG	couldn't find AP context for %s interface	ERROR
received a pdu on %s	DEBUG	dot11Malloc failed	ERROR
pnacRecvMapi: protoType: %04x pPhyPort-> authToASSendRtn:%p	DEBUG	dot11Malloc failed	ERROR
port not found	DEBUG	eapolRecvKeyMsg: unknown descType =%d	ERROR
from pnacRecvMapi: pkt body len = %d, pktType = %d	DEBUG	eapolRecvKeyMsg: invalid descriptor version	ERROR
from pnacPDUProcess: received PNAC_EAP_PACKET	DEBUG	eapolRecvKeyMsg: incorrect descriptor version	ERROR
from pnacPDUProcess: currentId = %d	DEBUG	eapolRecvKeyMsg: Ack must not be set	ERROR
from pnacPDUProcess: code = %d, identifier = %d, "	DEBUG	eapolRecvKeyMsg: MIC bit must be set	ERROR
from pnacPDUProcess: setting rxResp true	DEBUG	wpaAuthRecvPTKMsg2: unexpected packet received	ERROR
from pnacPDUProcess: code = %d, identifier = %d, "	DEBUG	wpaAuthRecvPTKMsg2: mic check failed	ERROR
from pnacPDUProcess: received "	DEBUG	wpaAuthRecvPTKMsg2: rsn ie mismatch	ERROR
from pnacPDUProcess: received "	DEBUG	wpaAuthRecvPTKMsg4: unexpected packet received	ERROR
from pnacPDUProcess: received PNAC_EAPOL_KEY_PACKET	DEBUG	wpaAuthRecvPTKMsg4: keyDataLength not zero	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
doing pnacTxCannedFail	DEBUG	wpaAuthRecvPTKMsg4: mic check failed	ERROR
doing pnacTxCannedSuccess	DEBUG	wpaAuthRecvGTKMsg2: unexpected packet received	ERROR
doing pnacTxReqId	DEBUG	secureBit not set in GTK Msg2	ERROR
doing pnacTxReq	DEBUG	wpaAuthRecvGTKMsg2: keyDataLength not zero	ERROR
doing pnacTxStart	DEBUG	wpaAuthRecvGTKMsg2: mic check failed	ERROR
doing pnacTxLogoff	DEBUG	wpaAuthRecvKeyReq: unexpected packet received	ERROR
doing pnacTxRspId: 1st cond	DEBUG	wpaAuthRecvKeyReq: keyDataLength not zero	ERROR
doing pnacTxRspId: entering 2nd cond	DEBUG	wpaAuthRecvKeyReq: mic check failed	ERROR
from pnacTxRspId: code = %d, identifier = %d, length = %d, "	DEBUG	invalid OUI %x %x %x	ERROR
doing pnacTxRspId: 2nd cond	DEBUG	(%s) invalid OUI %x %x %x	ERROR
doing pnacTxRspAuth: 1st cond	DEBUG	[%s:%d] Cipher in WPA IE : %x	ERROR
doing pnacTxRspAuth: 2nd cond	DEBUG	(%s) invalid OUI %x %x %x	ERROR
message for unknown port PAE	DEBUG	short WPA IE (length = %d) received	ERROR
from pnacACToSuppRecvRtn: calling pnacEapPktRecord	DEBUG	PTK state machine in unknown state.	ERROR
from pnacEapPktRecord: code = %d, identifier = %d, "	DEBUG	dot11InstallKeys failed	ERROR
from pnacEapPktRecord: received success pkt	DEBUG	group state machine entered into WPA_AUTH_GTK_INIT	ERROR
from pnacEapPktRecord: received failure pkt	DEBUG	dot11Malloc failed	ERROR
from pnacEapPktRecord: received request pkt	DEBUG	dot11Malloc failed	ERROR
unknown EAP-code %d	DEBUG	dot11Malloc failed	ERROR
Authenticator[%d]:	DEBUG	aesWrap failed	ERROR
Auth PAE state = %s	DEBUG	unknown key descriptor version %d	ERROR
Auth Reauth state = %s	DEBUG	dot11Malloc failed	ERROR
Back auth state = %s	DEBUG	could not initialize AES128ECB	ERROR
Supplicant[%d]:	DEBUG	could not initialize AES-128-ECB	ERROR
Supp Pae state = %s	DEBUG	MD5 initialization failed	ERROR
from pnacBackAuthFail: calling pnacTxCannedFail	DEBUG	RC4 framework initialization failed	ERROR
%s returned ERROR	DEBUG	PNAC framework initialization failed	ERROR
pnacUmiloctlHandler: cmd: %s(%d)	DEBUG	ERROR: option value not specified	ERROR
%s not configured for 802.1x	DEBUG	ERROR: -u can be used only with -s	ERROR
could not process PDU received from the wire	DEBUG	ERROR: user-name not specified	ERROR
pnacPDUForward: failed to foward the received PDU	DEBUG	failed to enable debug	ERROR
Creating PHY port with AUTH backend : %s SendRtn: %p RecvRtn:%p	DEBUG	[%s]: failed to convert string to MAC "	ERROR
pnacUmiAuthConfig: %s not configured for 802.1x	DEBUG	failed to initialize UMI	ERROR
pnacSuppRegisterUserInfo: not a valid AC	DEBUG	pnacPhyPortParamSet:invalid arguments	ERROR
pnacIfConfig: autoAuth Enabled	DEBUG	pnacPhyPortParamSet:Failed to create socket	ERROR
pnacSendRtn: no pnac port pae found for "	DEBUG	Error from pnacPhyPortParamSet:%sdevice invalid	ERROR
sending portStatus: %s[%d] to dot11	DEBUG	Error from pnacPhyPortParamSet:%s- Getting MAC address "	ERROR
pnacRecvASInfoMessage: Rkey of length %d set	DEBUG	pnacPhyPortParamSet:Failed to add 802.1X multicast "	ERROR
ASSendRtn: %p ASToAuthRecv: %p	DEBUG	pnacIsInterfaceUp: failed to create a raw socket	ERROR
adpRand failed:unable to generate random unicast key	WARN	pnacIsInterfaceUp: failed to get interface flags	ERROR
using group key as unicast key	WARN	failed to allocate buffer	ERROR
Integrity check failed more than once in last 60 secs.	WARN	UMI initialization failed	ERROR
MIC failed twice in last 60 secs, taking countermeasures	WARN	UMI initialization failed	ERROR
Failed to set dot11 port status	WARN	Error from pnacEapDemoAuthLibInit: malloc failed	ERROR
PTK state machine in NO_STATE.	WARN	Error from pnacEapDemoAuthRecv: received null EAP pkt	ERROR
PTK state machine in NO_STATE!!	WARN	Error from pnacEapDemoAuthRecv: send "	ERROR
PMKSA refcount not 1	WARN	Error from pnacRadXlateASAdd: cannot open socket	ERROR
IV verification failednknown subtype>	WARN	Error from pnacRadXlateDemoRecv: received null EAP pkt	ERROR
pnacIfConfig: overwriting previous interface "	WARN	From pnacRadXlateDemoRecv: send "	ERROR
pnacIfConfig: overwriting previous "	WARN	Error from pnacRadXlateDemoRecv: radius "	ERROR
pnacIfConfig: overwriting previous username"	WARN	Error from pnacRadXlateDemoRecv: radius "	ERROR
pnacIfConfig: overwriting previous password"	WARN	Error from pnacRadXlateRadIdRespSend: send to failed	ERROR
%s: Failed to set port status	WARN	Error from pnacRadXlateRadNonIdRespSend: send to failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
%s: Failed to notify event to dot11	WARN	Error from pnacRadXlateRadRecvProc: recvfrom failed	ERROR
pnacLibDeinit: Failed to destroy the phyPort:%s	WARN	From pnacRadXlateRadPktIntegrityChk: no corresponding "	ERROR
pnacPortPaeDeconfig:kpnacPortPaeDec onfig failed	WARN	Error from pnacRadXlateRadPktIntegrityChk: no message "	ERROR
pnacPortPaeDeconfig:kpnacPortPaeDec onfig failed	WARN	Error from pnacRadXlateRadPktIntegrityChk: "	ERROR
pnacBackAuthSuccess: failed to notify the destination "	WARN	From pnacRadXlateRadChalPktHandle: no encapsulated eap "	ERROR
could not initialize MGMT framework	ERROR	Error from pnacRadXlateRadChalPktHandle: malloc for eap "	ERROR
umiInit failed	ERROR	Error from pnacEapDemoSuppUserInfoRegister: invalid "	ERROR
iappInit failed	ERROR	Error from pnacEapDemoSuppRecv: received null EAP pkt	ERROR
could not initialize IAPP MGMT.	ERROR	Error from pnacEapDemoSuppRecv: send ptr to pnac supplicant"	ERROR
dot11Malloc failed	ERROR	From pnacEapDemoSuppRecv: user info not entered yet	ERROR
buffer length not specified	ERROR	Error from pnacEapDemoSuppRecv: couldn't "	ERROR
Invalid length(%d) specified	ERROR	MDString: adpDigestInit for md5 failed	ERROR
Failed to get information about authorized AP list.	ERROR	pnacUmiInit: UMI initialization failed	ERROR
Recd IE data for non-existent AP %s	ERROR	could not start PNAC task	ERROR
Recd IE data for wrong AP %s	ERROR	invalid aruments	ERROR
Received Invalid IE data from WSC	ERROR	pnacIfNameToIndex failed	ERROR
Recd IE data for non-existent AP %s	ERROR	pnacPhyPortParamSet: device invalid %s%d	ERROR
Recd WSC Start command without interface name	ERROR	pnacPhyPortParamSet: EIOCGADDR ioctl failed	ERROR
Recd WSC start for non-existent AP %s	ERROR	pnacPhyPortParamSet: multicast addr add ioctl failed	ERROR
Recd WSC start for wrong AP %s	ERROR	pnacPhyPortParamUnset: multicast addr del ioctl failed	ERROR
Unable to send WSC_WLAN_CMD_PORT to WSC	ERROR	pnacPDUXmit: Invalid arguments	ERROR
Failed to get the ap context for %s	ERROR	pnacPDUXmit: failed to get M_BLK_ID	ERROR
WPS can only be applied to WPA/WPA2 security profiles	ERROR	from pnacIsInterfaceUp: device %s%d invalid	ERROR
wpsEnable: running wsccmd failed	ERROR	pnacRecvRtn: dropping received packet as port is"	ERROR
Failed to get the ap context for %s	ERROR	pnacSendRtn: Invalid arguments	ERROR
WPS conf. under non WPA/WPA2 security setting	ERROR	pnacSendRtn: no physical port corresponding to"	ERROR
Failed to reset the Beacon Frame IE in the driver	ERROR	pnacSendRtn: dropping packet as port"	ERROR
Failed to reset the Beacon Frame IE in the driver	ERROR	pnacAuthBuildRC4KeyDesc: adpEncryptInit(RC4) failed	ERROR
WPS method cannot be NULL	ERROR	pnacAuthBuildRC4KeyDesc: adpCipherContextCtrl"	ERROR
PIN value length should be a multiple of 4 !!	ERROR	pnacDot11UserSet: incorrect buffer length	ERROR
Failed to initiate PIN based association, PIN = %s	ERROR	PNAC user component id not set.	ERROR
Failed to initiate PBC based enrolle association	ERROR	pnacKeyInfoGet:failed to allocate buffer	ERROR
Invalid association mode. (Allowed modes : PIN/PBC)	ERROR	PNAC user comp id not set. dropping EAPOL key pkt	ERROR
wpsEnable: running wsccmd failed	ERROR	pnacUmiPortPaeParamSet: invalid buffer received	ERROR
Failed to send QUIT command to WSC from DOT11	ERROR	Error from pnacRecvASInfoMessage: "	ERROR
Failed to clear off the WPS process	ERROR	pnacRecvASInfoMessage: "	ERROR
missing profile name	ERROR	pnacRecvASInfoMessage: Bad info length	ERROR
A profile exists with the same name	ERROR	Error from pnacLibInit: malloc failed	ERROR
Error in allocating memory for profile	ERROR	could not create phy ports lock	ERROR
missing profile name	ERROR	could not create nodes ports lock	ERROR
missing profile name	ERROR	port exists for iface - %s	ERROR
Profile name and interface name must be specified	ERROR	pnacPhyPortCreate failed	ERROR
Profile %s does not exist	ERROR	kpnacPhyPortCreate failed	ERROR
Could not set profile %s on the interface %s	ERROR	invalid argument	ERROR
missing profile name	ERROR	pnacAuthConfig: maxAuth limit reached	ERROR
Profile %s does not exist	ERROR	pnacAuthConfig: malloc failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthConfig: pAsArg cannot be NULL	ERROR
SSID should not be longer than %d	ERROR	Error from pnacAuthConfig: receive routine hook "	ERROR
Profile %s does not exist	ERROR	pnacAuthConfig: pnacAuthInit failed	ERROR
Profile %s does not exist	ERROR	kpnacPortPaeConfig failed	ERROR
Profile %s does not exist	ERROR	Invalid arguments	ERROR
Profile %s does not exist	ERROR	Error from pnacSuppConfig: malloc failed	ERROR
Profile %s does not exist	ERROR	Error from pnacSuppConfig: receive routine hook "	ERROR
Profile %s does not exist	ERROR	Error from pnacSuppConfig: pnacSuppInit failed	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
SSID not set. SSID is needed to generate password hash	ERROR	kpnacPortPaeConfig failed	ERROR
Password string too big	ERROR	pnacAuthDeconfig failed: pPortPae NULL	ERROR
dot11Malloc failed	ERROR	Error from pnacPhyPortDestroy: port not configured	ERROR
Profile %s does not exist	ERROR	pnacPhyPortDestroy: Failed to deconfigure port	ERROR
Hex string should only have %d hex chars	ERROR	pnacPhyPortParamUnset FAILED	ERROR
dot11Malloc failed	ERROR	Error from pnacPhyPortCreate: malloc failed	ERROR
Profile %s does not exist	ERROR	Error from pnacPhyPortCreate: pnacPhyPortParamSet"	ERROR
invalid key index %d. key index should be 0-3.	ERROR	error from pnacPhyPortCreate: malloc failed	ERROR
wepKey length incorrect	ERROR	Error from pnacAuthInit: pnacPortTimersInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthInit: pnacAuthPAEInit failed	ERROR
Invalid Cipher type %d	ERROR	Error from pnacAuthInit: pnacAuthKeyTxInit failed	ERROR
Profile supports WEP stas,Group cipher must be WEP	ERROR	Error from pnacAuthInit: pnacReauthTimerInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthInit: pnacBackAuthInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthInit: pnacCtrlDirInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacAuthInit: pnacKeyRecvInit failed	ERROR
invalid pairwise cipher type %d	ERROR	Error from pnacSuppInit: malloc failed	ERROR
Cipher %s is already in the list.	ERROR	Error from pnacSuppInit: pnacPortTimersInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacSuppInit: pnacKeyRecvInit failed	ERROR
Invalid Cipher type %d	ERROR	Error from pnacSuppInit: pnacSuppKeyTxInit failed	ERROR
Cipher %s not found in the list.	ERROR	Error from pnacSuppInit: pnacSuppPAEInit failed	ERROR
Profile %s does not exist	ERROR	Error from pnacRecvRtn: invalid arguments	ERROR
Profile %s does not exist	ERROR	Error from pnacRecvMapi: unsupported PDU received	ERROR
Auth method %s is already in the list	ERROR	suppToACSendRtn returned not OK!	ERROR
Profile %s does not exist	ERROR	Error from pnacBasicPktCreate: malloc failed	ERROR
Auth method %s not found in the list.	ERROR	Error from pnacEAPPktCreate: basic pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacTxCannedFail: eap pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacTxCannedSuccess: eap pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacTxReqId: eap pkt create failed	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacTxReq: eap pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacSendRespToServer: malloc failed	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacSendRespToServer: no AS configured	ERROR
Profile %s does not exist	ERROR	Error from pnacTxStart: basic pkt create failed	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacTxStart: basic pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacTxRspId: eap pkt create failed	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacTxRspAuth: eap pkt create failed	ERROR
Profile %s does not exist	ERROR	Error from pnacEapPktRecord: EAP packet too"	ERROR
invalid type value %d. supported values are 1,2,3,4	ERROR	Error from pnacEapPktRecord: "	ERROR
Profile %s does not exist	ERROR	from pnacBackAuthTimeout: calling pnacTxCannedFail	ERROR
ERROR: incomplete DB update information.	ERROR	hmac_md5: adpHmacContextCreate failed	ERROR
old values result does not contain 2 rows	ERROR	hmac_md5:adpHmacInit failed	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiIoctlHandler: invalid cmd: %d	ERROR
Error in executing DB update handler	ERROR	pnacEapRadAuthSend: Invalid arguments	ERROR
sqlite3QueryResGet failed	ERROR	pnacEapRadAuthSend: failed to allocate inbuffer	ERROR
ERROR: incomplete DB update information.	ERROR	pnacXmit : umiloctl failed[%d]	ERROR
old values result does not contain 2 rows	ERROR	pnacPDUForward: Invalid input	ERROR
sqlite3QueryResGet failed	ERROR	pnacPDUForward: error in getting port pae information	ERROR
Error in executing DB update handler	ERROR	pnacPDUForward: error allocating memory	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmiIfMacAddrChange: %s not configured for 802.1x	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmiIfMacAddrChange: could not process PDU received"	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmiPhyPortConfig: Invalid config data	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmiPhyPortConfig: Invalid backend name specified	ERROR
startStopVap failed to stop %s	ERROR	pnacUmiPhyPortConfig: could not create PNAC physical"	ERROR
Invalid SQLITE operation code - %d	ERROR	pnacUmiAuthConfig: Invalid config data	ERROR
./src/dot11/mgmt/dot11Mgmt.c:1177: ADP_ERROR (	ERROR	pnacUmiAuthConfig: Invalid backend name specified	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
only delete event expected on dot11RogueAP.	ERROR	unable to create new EAP context.	ERROR
sqlite3QueryResGet failed	ERROR	unable to apply %s profile on the EAP context.	ERROR
unhandled database operation %d	ERROR	pnacUmiAuthConfig: could not configure PNAC PAE "	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiSuppConfig: Invalid config data	ERROR
failed to configure WPS on %s	ERROR	pnacUmiSuppConfig: Invalid backend name specified	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiSuppConfig: %s not configured for 802.1x	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiSuppConfig: could not PNAC port Access"	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiSuppConfig: Failed to register user information	ERROR
sqlite3QueryResGet failed	ERROR	pnacPortByMacDeconfig: port not found	ERROR
sqlite3QueryResGet failed	ERROR	pnacPortByMacDeconfig: port not found	ERROR
no VAP rows returned. expected one	ERROR	pnacUmiIfDown: Invalid config data	ERROR
multiple VAP rows returned. expected one	ERROR	pnacUmiIfDown: Invalid config data	ERROR
sqlite3QueryResGet failed	ERROR	Error from pnacPortDeconfig: port not configured	ERROR
invalid query result. ncols=%d nrows=%d	ERROR	pnacUmiIfDown: could not deconfigure port	ERROR
%s:VAP(%s) create failed	ERROR	pnacUmiPhyPortDestroy: Invalid config data	ERROR
sqlite3QueryResGet failed	ERROR	pnacUmiPhyPortDestroy: Invalid config data	ERROR
invalid query result. ncols=%d nrows=%d	ERROR	pnacUmiPhyPortDestroy: Failed to destroy the port	ERROR
Invalid config data	ERROR		

ファシリティ：システム（カーネル）

ログメッセージ	緊急度	ログメッセージ	緊急度
DNAT: multiple ranges no longer supported	DEBUG	%s: %s%s:%d -> %s:%d %s,	DEBUG
DNAT: Target size %u wrong for %u ranges,	DEBUG	%s: %s%s:%d %s,	DEBUG
DNAT: wrong table %s, tablename	DEBUG	%s: Failed to add WDS MAC: %s, dev- >name,	DEBUG
DNAT: hook mask 0x%x bad, hook_mask	DEBUG	%s: Device already has WDS mac address attached,	DEBUG
%s%d: resetting MPPC/MPPE compressor,	DEBUG	%s: Added WDS MAC: %s, dev- >name,	DEBUG
%s%d: wrong offset value: %d,	DEBUG	%s: WDS MAC address %s is not known by this interface,	DEBUG
%s%d: wrong length of match value: %d,	DEBUG	[madwifi] %s() : Not enough space., __FUNCTION__	DEBUG
%s%d: too big offset value: %d,	DEBUG	Returning to chan %d, ieeeChan	DEBUG
%s%d: cannot decode offset value,	DEBUG	WEP	DEBUG
%s%d: wrong length code: 0x%X,	DEBUG	AES	DEBUG
%s%d: short packet (len=%d), __FUNCTION__,	DEBUG	AES_CCM	DEBUG
%s%d: bad sequence number: %d, expected: %d,	DEBUG	CKIP	DEBUG
%s%d: bad sequence number: %d, expected: %d,	DEBUG	TKIP	DEBUG
PPPIOCDETACH file->f_count=%d,	DEBUG	%s: cannot map channel to mode; freq %u flags 0x%x,	DEBUG
PPP: outbound frame not passed	DEBUG	%s: %s, vap->iv_dev->name, buf	DEBUG
PPP: VJ decompression error	DEBUG	%s: [%s] %s, vap->iv_dev->name,	DEBUG
PPP: inbound frame not passed	DEBUG	%s: [%s] %s, vap->iv_dev->name, ether_sprintf(mac), buf	DEBUG
PPP: reconstructed packet	DEBUG	[%s:%s] discard %s frame, %s, vap- >iv_dev->name,	DEBUG
PPP: no memory for	DEBUG	[%s:%s] discard frame, %s, vap- >iv_dev->name,	DEBUG
missed pkts %u..%u,	DEBUG	[%s:%s] discard %s information element, %s,	DEBUG
%s%d: resetting MPPC/MPPE compressor,	DEBUG	[%s:%s] discard information element, %s,	DEBUG
%s%d: wrong offset value: %d,	DEBUG	[%s:%s] discard %s frame, %s, vap- >iv_dev->name,	DEBUG
%s%d: wrong length of match value: %d,	DEBUG	[%s:%s] discard frame, %s, vap- >iv_dev->name,	DEBUG
%s%d: too big offset value: %d,	DEBUG	ifmedia_add: null ifm	DEBUG
%s%d: cannot decode offset value,	DEBUG	Adding entry for	DEBUG
%s%d: wrong length code: 0x%X,	DEBUG	ifmedia_set: no match for 0x%x/0x%x,	DEBUG
%s%d: short packet (len=%d), __FUNCTION__,	DEBUG	ifmedia_set: target	DEBUG
%s%d: bad sequence number: %d, expected: %d,	DEBUG	ifmedia_set: setting to	DEBUG
%s%d: bad sequence number: %d, expected: %d,	DEBUG	ifmedia_ioctl: no media found for 0x%x,	DEBUG
PPPIOCDETACH file->f_count=%d,	DEBUG	ifmedia_ioctl: switching %s to , dev- >name	DEBUG
PPP: outbound frame not passed	DEBUG	ifmedia_match: multiple match for	DEBUG
PPP: VJ decompression error	DEBUG	<unknown type>	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
PPP: inbound frame not passed	DEBUG	desc->ifmt_string	DEBUG
PPP: reconstructed packet	DEBUG	mode %s, desc->ifmt_string	DEBUG
PPP: no memory for	DEBUG	<unknown subtype>	DEBUG
missed pkts %u..%u,	DEBUG	%s, desc->ifmt_string	DEBUG
%s: INC_USE_COUNT, now %d, __FUNCTION__, mod_use_count \	DEBUG	%s%s, seen_option++ ? , : ,	DEBUG
%s: DEC_USE_COUNT, now %d, __FUNCTION__, mod_use_count \	DEBUG	%s%s, seen_option++ ? , : ,	DEBUG
PPPOL2TP %s: _fmt,	DEBUG	%s, seen_option ? > :	DEBUG
PPPOL2TP: --> %s, __FUNCTION__)	DEBUG	%s: %s, dev->name, buf	DEBUG
PPPOL2TP: <-- %s, __FUNCTION__)	DEBUG	%s: no memory for sysctl table!, __func__	DEBUG
%s: recv: , tunnel->name	DEBUG	%s: no memory for VAP name!, __func__	DEBUG
%s: xmit:, session->name	DEBUG	%s: failed to register sysctls!, vap- >iv_dev->name	DEBUG
%s: xmit:, session->name	DEBUG	%s: no memory for new proc entry (%s)!, __func__,	DEBUG
%s: module use_count is %d, __FUNCTION__, mod_use_count	DEBUG	%s: 0x%p len %u, tag, p, len	DEBUG
PPPOL2TP %s: _fmt,	DEBUG	%03d:, i	DEBUG
PPPOL2TP: --> %s, __FUNCTION__)	DEBUG	%02x, ((u_int8_t *)p)[i]	DEBUG
PPPOL2TP: <-- %s, __FUNCTION__)	DEBUG	first difference at byte %u, i	DEBUG
%s: recv: , tunnel->name	DEBUG	%s: , t->name	DEBUG
%s: xmit:, session->name	DEBUG	FAIL: ieee80211_crypto_newkey failed	DEBUG
%s: xmit:, session->name	DEBUG	FAIL: ieee80211_crypto_setkey failed	DEBUG
PPPOL2TP %s: _fmt,	DEBUG	FAIL: unable to allocate skbuff	DEBUG
PPPOL2TP: --> %s, __FUNCTION__)	DEBUG	FAIL: wep decap failed	DEBUG
PPPOL2TP: <-- %s, __FUNCTION__)	DEBUG	FAIL: decap botch; length mismatch	DEBUG
%s: recv: , tunnel->name	DEBUG	FAIL: decap botch; data does not compare	DEBUG
%s: xmit:, session->name	DEBUG	FAIL: wep encap failed	DEBUG
%s: xmit:, session->name	DEBUG	FAIL: encap data length mismatch	DEBUG
IRQ 31 is triggered	DEBUG	FAIL: encrypt data does not compare	DEBUG
[%s:%d] , __func__, __LINE__\	DEBUG	PASS	DEBUG
\t[R%s %#0x %#0x 0x%08x%08x], (status == ERROR ? # :), page, addr, (uint32_t)(*pValue >> 32), (uint32_t)(*pValue & 0xffffffff)	DEBUG	%u of %u 802.11i WEP test vectors passed, pass, total	DEBUG
\t[W%s %#0x %#0x 0x%08x%08x], (status == ERROR ? # :), page, addr, (uint32_t)(value >> 32), (uint32_t)(value & 0xffffffff)	DEBUG	%s: 0x%p len %u, tag, p, len	DEBUG
%s: mac_add %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	%03d:, i	DEBUG
%s: mac_del %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	%02x, ((u_int8_t *)p)[i]	DEBUG
%s: mac_kick %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	first difference at byte %u, i	DEBUG
%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	%s: , t->name	DEBUG
%s: addr_add %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	FAIL: ieee80211_crypto_newkey failed	DEBUG
%s: addr_del %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	FAIL: ieee80211_crypto_setkey failed	DEBUG
%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X, dev->name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]	DEBUG	FAIL: unable to allocate skbuff	DEBUG
%s: set_float %d;%d,	DEBUG	FAIL: ccmp encap failed	DEBUG
IRQ 32 is triggered	DEBUG	FAIL: encap data length mismatch	DEBUG
ip_finish_output2: No header cache and no neighbour!	DEBUG	FAIL: encrypt data does not compare	DEBUG
a guy asks for address mask. Who is it?	DEBUG	FAIL: ccmp decap failed	DEBUG
icmp v4 hw csum failure)	DEBUG	FAIL: decap botch; length mismatch	DEBUG
expire>> %u %d %d %d, expire,	DEBUG	FAIL: decap botch; data does not compare	DEBUG
expire++ %u %d %d %d, expire,	DEBUG	PASS	DEBUG
rt_cache @%02x: %u.%u.%u.%u, hash,	DEBUG	%u of %u 802.11i AES-CCMP test vectors passed, pass, total	DEBUG
rt_bind_peer(0) @%p, NET_CALLER(iph)	DEBUG	%s: 0x%p len %u, tag, p, len	DEBUG
ip_rt_advice: redirect to	DEBUG	%03d:, i	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
ip_rt_bug: %u.%u.%u.%u -> %u.%u.%u.%u, %s,	DEBUG	%02x, ((u_int8_t *)p)[i]	DEBUG
udp cork app bug 2)	DEBUG	first difference at byte %u, i	DEBUG
udp cork app bug 3)	DEBUG	ieee80211_crypto_newkey failed	DEBUG
udp v4 hw csum failure.)	DEBUG	ieee80211_crypto_setkey failed	DEBUG
UDP: short packet: From %u.%u.%u.%u:%u %d/%d to %u.%u.%u.%u:%u,	DEBUG	unable to allocate skbuff	DEBUG
UDP: bad checksum. From %d.%d.%d.%d:%d to %d.%d.%d.%d:%d ulen %d,	DEBUG	tkip enmic failed	DEBUG
%s: lookup policy [list] found=%s,	DEBUG	enmic botch; length mismatch	DEBUG
%s: called: [output START], __FUNCTION__	DEBUG	enmic botch	DEBUG
%s: flow dst=%s, __FUNCTION__, XFRMSTRADDR(fl->fl4_dst, family)	DEBUG	tkip encap failed	DEBUG
%s: flow src=%s, __FUNCTION__, XFRMSTRADDR(fl->fl4_src, family)	DEBUG	encrypt phase1 botch	DEBUG
%s: flow dst=%s, __FUNCTION__, XFRMSTRADDR(fl->fl6_dst, family)	DEBUG	encrypt data length mismatch	DEBUG
%s: flow src=%s, __FUNCTION__, XFRMSTRADDR(fl->fl6_src, family)	DEBUG	encrypt data does not compare	DEBUG
a guy asks for address mask. Who is it?	DEBUG	tkip decap failed	DEBUG
icmp v4 hw csum failure)	DEBUG	decrypt phase1 botch	DEBUG
expire>> %u %d %d %d, expire,	DEBUG	decrypt data does not compare	DEBUG
expire++ %u %d %d %d, expire,	DEBUG	decap botch; length mismatch	DEBUG
rt_cache @%02x: %u.%u.%u.%u, hash,	DEBUG	decap botch; data does not compare	DEBUG
rt_bind_peer(0) @%p, NET_CALLER(iph)	DEBUG	tkip demic failed	DEBUG
ip_rt_advice: redirect to	DEBUG	802.11i TKIP test vectors passed	DEBUG
ip_rt_bug: %u.%u.%u.%u -> %u.%u.%u.%u, %s,	DEBUG	%s, buf	DEBUG
UDP: short packet: From %u.%u.%u.%u:%u %d/%d to %u.%u.%u.%u:%u,	DEBUG	Atheros HAL assertion failure: %s: line %u: %s,	DEBUG
UDP: bad checksum. From %d.%d.%d.%d:%d to %d.%d.%d.%d:%d ulen %d,	DEBUG	ath_hal: logging to %s %s, ath_hal_logfile,	DEBUG
a guy asks for address mask. Who is it?	DEBUG	ath_hal: logging disabled	DEBUG
fib_add_ifaddr: bug: prim == NULL	DEBUG	%s%s, sep, ath_hal_buildopts[i]	DEBUG
fib_del_ifaddr: bug: prim == NULL	DEBUG	ath_pci: No devices found, driver not installed.	DEBUG
expire>> %u %d %d %d, expire,	DEBUG	_fmt, __VA_ARGS__	DEBUG
expire++ %u %d %d %d, expire,	DEBUG	%s: Warning, using only %u entries in %u key cache,	DEBUG
rt_cache @%02x: %u.%u.%u.%u, hash,	DEBUG	%s: TX99 support enabled, dev->name	DEBUG
rt_bind_peer(0) @%p,	DEBUG	%s:grppoll Buf allocation failed ,__func__	DEBUG
ip_rt_advice: redirect to	DEBUG	%s: %s: unable to start recv logic,	DEBUG
ip_rt_bug: %u.%u.%u.%u -> %u.%u.%u.%u, %s,	DEBUG	%s: %s: unable to start recv logic,	DEBUG
%s: lookup policy [list] found=%s,	DEBUG	%s: no skbuff, __func__	DEBUG
%s: called: [output START], __FUNCTION__	DEBUG	%s: hardware error; resetting, dev- >name DEBUG	
%s: flow dst=%s, __FUNCTION__, XFRMSTRADDR(fl->fl4_dst, family)	DEBUG	%s: rx FIFO overrun; resetting, dev- >name	DEBUG
%s: flow src=%s, __FUNCTION__, XFRMSTRADDR(fl->fl4_src, family)	DEBUG	%s: unable to reset hardware: '%s' (HAL status %u)	DEBUG
%s: flow dst=%s, __FUNCTION__, XFRMSTRADDR(fl->fl6_dst, family)	DEBUG	%s: unable to start recv logic, dev- >name	DEBUG
%s: flow src=%s, __FUNCTION__, XFRMSTRADDR(fl->fl6_src, family)	DEBUG	%s: %s: unable to reset hardware: '%s' (HAL status %u),	DEBUG
a guy asks for address mask. Who is it?	DEBUG	%s: %s: unable to start recv logic,	DEBUG
icmp v4 hw csum failure)	DEBUG	ath_mgtstart: discard, no xmit buf	DEBUG
expire>> %u %d %d %d, expire,	DEBUG	%s: [%02u] %-7s , tag, ix, ciphers[hk- >kv_type]	DEBUG
expire++ %u %d %d %d, expire,	DEBUG	%02x, hk->kv_val[i]	DEBUG
rt_cache @%02x: %u.%u.%u.%u, hash,	DEBUG	mac %s, ether_sprintf(mac)	DEBUG
rt_bind_peer(0) @%p, NET_CALLER(iph)	DEBUG	%s , sc->sc_splitmic ? mic : rxmic	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
ip_rt_advice: redirect to	DEBUG	%02x, hk->kv_mic[i]	DEBUG
ip_rt_bug: %u.%u.%u.%u -> %u.%u.%u.%u, %s,	DEBUG	txmic	DEBUG
UDP: short packet: From %u.%u.%u.%u:%u %d/%d to %u.%u.%u.%u:%u,	DEBUG	%02x, hk->kv_txmic[i]	DEBUG
UDP: bad checksum. From %d.%d.%d.%d:%d to %d.%d.%d.%d:%d ulen %d,	DEBUG	%s: unable to update h/w beacon queue parameters,	DEBUG
REJECT: ECHOREPLY no longer supported.	DEBUG	%s: stuck beacon; resetting (bmiss count %u),	DEBUG
ipt_rpc: only valid for PRE_ROUTING, FORWARD, POST_ROUTING, LOCAL_IN and/or LOCAL_OUT targets.	DEBUG	move data from NORMAL to XR	DEBUG
ip_nat_init: can't setup rules.	DEBUG	moved %d buffers from NORMAL to XR, index	DEBUG
ip_nat_init: can't register in hook.	DEBUG	move buffers from XR to NORMAL	DEBUG
ip_nat_init: can't register out hook.	DEBUG	moved %d buffers from XR to NORMAL, count	DEBUG
ip_nat_init: can't register adjust in hook.	DEBUG	%s:%d %s, __FILE__, __LINE__, __func__	DEBUG
ip_nat_init: can't register adjust out hook.	DEBUG	%s:%d %s, __FILE__, __LINE__, __func__	DEBUG
ip_nat_init: can't register local out hook.	DEBUG	%s: no buffer (%s), dev->name, __func__	DEBUG
ip_nat_init: can't register local in hook.	DEBUG	%s: no skbuff (%s), dev->name, __func__	DEBUG
ipt_hook: happy cracking.	DEBUG	%s: HAL qnum %u out of range, max %u!,	DEBUG
ip_conntrack: can't register pre-routing defrag hook.	DEBUG	grppoll_start: grppoll Buf allocation failed	DEBUG
ip_conntrack: can't register local_out defrag hook.	DEBUG	%s: HAL qnum %u out of range, max %u!,	DEBUG
ip_conntrack: can't register pre-routing hook.	DEBUG	%s: AC %u out of range, max %u!,	DEBUG
ip_conntrack: can't register local out hook.	DEBUG	%s: unable to update hardware queue	DEBUG
ip_conntrack: can't register local in helper hook.	DEBUG	%s: bogus frame type 0x%x (%s), dev- >name,	DEBUG
ip_conntrack: can't register postrouting helper hook.	DEBUG	ath_stoprecv: rx queue 0x%x, link %p,	DEBUG
ip_conntrack: can't register post-routing hook.	DEBUG	%s: %s: unable to reset channel %u (%u MHz)	DEBUG
ip_conntrack: can't register local in hook.	DEBUG	%s: %s: unable to restart recv logic,	DEBUG
ip_conntrack: can't register to sysctl.	DEBUG	%s: unable to allocate channel table, dev->name	DEBUG
ip_conntrack_rtsp v IP_NF_RTSP_VERSION loading	DEBUG	%s: unable to allocate channel table, dev->name	DEBUG
ip_conntrack_rtsp: max_outstanding must be a positive integer	DEBUG	%s: unable to collect channel list from HAL;	DEBUG
ip_conntrack_rtsp: setup_timeout must be a positive integer	DEBUG	R (%p %llx) %08x %08x %08x %08x %08x %08x %c,	DEBUG
ip_conntrack_rtsp: ERROR registering port %d, ports[i]	DEBUG	T (%p %llx) %08x %08x %08x %08x %08x %08x %08x %08x %c,	DEBUG
ip_nat_rtsp v IP_NF_RTSP_VERSION loading	DEBUG	%s: no memory for sysctl table!, __func__	DEBUG
%s: Sorry! Cannot find this match option., __FILE__	DEBUG	%s: no memory for device name storage!, __func__	DEBUG
ipt_time loading	DEBUG	%s: failed to register sysctls!, sc- >sc_dev->name	DEBUG
ipt_time unloaded	DEBUG	%s: mac %d.%d phy %d.%d, dev- >name,	DEBUG
ip_conntrack_irc: max_dcc_channels must be a positive integer	DEBUG	5 GHz radio %d.%d 2 GHz radio %d.%d,	DEBUG
ip_conntrack_irc: ERROR registering port %d,	DEBUG	radio %d.%d, ah->ah_analog5GhzRev >> 4,	DEBUG
ip_nat_h323: ip_nat_mangle_tcp_packet	DEBUG	radio %d.%d, ah->ah_analog5GhzRev >> 4,	DEBUG
ip_nat_h323: ip_nat_mangle_udp_packet	DEBUG	%s: Use hw queue %u for %s traffic,	DEBUG
ip_nat_h323: out of expectations	DEBUG	%s: Use hw queue %u for CAB traffic, dev->name,	DEBUG
ip_nat_h323: out of RTP ports	DEBUG	%s: Use hw queue %u for beacons, dev->name,	DEBUG
ip_nat_h323: out of TCP ports	DEBUG	Could not find Board Configuration Data	DEBUG
ip_nat_q931: out of TCP ports	DEBUG	Could not find Radio Configuration data	DEBUG
ip_nat_ras: out of TCP ports	DEBUG	ath_ahb: No devices found, driver not installed.	DEBUG
ip_nat_q931: out of TCP ports	DEBUG	_fmt, __VA_ARGS__	DEBUG
ip_conntrack_core: Frag of proto %u.,	DEBUG	_fmt, __VA_ARGS__	DEBUG
Broadcast packet!	DEBUG	xlr8NatIpFinishOutput: Err.. skb2 == NULL !	DEBUG
Should bcast: %u.%u.%u.%u- >%u.%u.%u.%u (sk=%p, ptype=%u),	DEBUG	xlr8NatSoftCtxEnqueue: Calling xlr8NatIpFinishOutput () .., status	DEBUG
ip_conntrack version %s (%u buckets, %d max)	DEBUG	xlr8NatSoftCtxEnqueue: xlr8NatIpFinishOutput () returned [%d], status	DEBUG
ERROR registering port %d,	DEBUG	icmpExceptionHandler: Exception!	DEBUG
netfilter PSD loaded - (c) astaro AG	DEBUG	fragExceptionHandler: Exception!	DEBUG
netfilter PSD unloaded - (c) astaro AG	DEBUG	algExceptionHandler: Exception!	DEBUG
%s , SELF	DEBUG	dnsExceptionHandler: Exception!	DEBUG

ログメッセージ	緊急度	ログメッセージ	緊急度
%s , LAN	DEBUG	ipsecExceptionHandler: Exception!	DEBUG
%s , WAN	DEBUG	ESP Packet Src:%x Dest:%x Sport:%d dport:%d secure:%d spi:%d isr:%p,	DEBUG
TRUNCATED	DEBUG	xlr8NatConntrackPreHook: We found the valid context,	DEBUG
SRC=%u.%u.%u.%u DST=%u.%u.%u.%u ,	DEBUG	xlr8NatConntrackPreHook: Not a secured packet.	DEBUG
LEN=%u TOS=0x%02X PREC=0x%02X TTL=%u ID=%u ,	DEBUG	xlr8NatConntrackPreHook: isr=[%p], plsr	DEBUG
FRAG:%u , ntohs(ih->frag_off) & IP_OFFSET	DEBUG	xlr8NatConntrackPreHook: secure=[%d], secure	DEBUG
TRUNCATED	DEBUG	Context found for ESP %p,pFlowEntry- >post.plsr[0]	DEBUG
PROTO=TCP	DEBUG	xlr8NatConntrackPreHook: New connection.	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	xlr8NatConntrackPostHook: postSecure=[%d] postIsr=[%p %p],	DEBUG
SPT=%u DPT=%u ,	DEBUG	proto %d spi %d <-------> proto %d spi %d,pPktInfo->proto,pPktInfo->spi,	DEBUG
SEQ=%u ACK=%u ,	DEBUG	IPSEC_INF Clock skew detected	DEBUG
WINDOW=%u , ntohs(th->window)	DEBUG	IPSEC_ERR [%s:%d]: Max (%d) No of SA Limit reached,	DEBUG
RES=0x%02x , (u8)(ntohl(tcp_flag_word(th) & TCP_RESERVED_BITS) >> 22)	DEBUG	IPSEC_ERR [%s:%d]: Max (%d) No of SA Limit reached,	DEBUG
URGP=%u , ntohs(th->urg_ptr)	DEBUG	IPSEC_ERR [%s:%d]: time(secs): %u	DEBUG
TRUNCATED	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
%02X, op[i]	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PROTO=UDP	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
SPT=%u DPT=%u LEN=%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
SPT=%u DPT=%u LEN=%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PROTO=ICMP	DEBUG	unknown oid '%s', varName	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	could not find oid pointer for '%s', varName	DEBUG
TYPE=%u CODE=%u , ich->type, ich- >code	DEBUG	unRegistering ipsecMib	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
ID=%u SEQ=%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PARAMETER=%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
GATEWAY=%u.%u.%u.%u ,	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
MTU=%u , ntohs(ich->un.frag.mtu)	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PROTO=AH	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	unknown oid '%s', varName	DEBUG
SPI=0x%x , ntohl(ah->spi)	DEBUG	could not find oid pointer for '%s', varName	DEBUG
PROTO=ESP	DEBUG	unRegistering ipsecMib	DEBUG
INCOMPLETE [%u bytes] ,	DEBUG	. %u.%u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
SPI=0x%x , ntohl(eh->spi)	DEBUG	%02x, *p	DEBUG
PROTO=%u , ih->protocol	DEBUG	. %u.%u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
UID=%u , skb->sk->sk_socket->file- >f_uid	DEBUG	%02x, *p	DEBUG
<%d>%sIN=%s OUT=%s , loginfo- >u.log.level,	DEBUG	. %u.%u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
level_string	DEBUG	%02x, *p	DEBUG
%sIN=%s OUT=%s ,	DEBUG	. %u.%u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
%s , prefix == NULL ? loginfo->prefix : prefix	DEBUG	%02x, *p	DEBUG
IN=	DEBUG	unable to register vipsec kernel comp to UMI	DEBUG
OUT=	DEBUG	unregistering VIPSECK from UMI	DEBUG
PHYSIN=%s , physindev->name	DEBUG	in vipsecKIoctlHandler cmd - %d, cmd	DEBUG
PHYSOUT=%s , physoutdev->name	DEBUG	%s: Error. DST Refcount value less than 1 (%d),	DEBUG
MAC=	DEBUG	for %s DEVICE refcnt: %d ,pDst- >dev->name,	DEBUG
%02x%c, *p,	DEBUG	%s: Got Null m:%p *m:%p sa:%p *sa:%p,__func__,ppBufMgr,	DEBUG
NAT: no longer support implicit source local NAT	DEBUG	%s Got Deleted SA:%p state:%d,__func__,plpsecInfo,plpsecInfo->state	DEBUG
NAT: packet src %u.%u.%u.%u -> dst %u.%u.%u.%u,	DEBUG	%s: %s: fmt, __FILE__, __FUNCTION__ , ## args)	INFO
SNAT: multiple ranges no longer supported	DEBUG	%s: %s: fmt, __FILE__, __FUNCTION__ , ## args)	INFO
format,##args)	DEBUG	ipt_TIME: format, ## args)	INFO

ログメッセージ	緊急度	ログメッセージ	緊急度
version	DEBUG	IPT_ACCOUNT_NAME : checkentry() wrong parameters (not equals existing table parameters).	INFO
offset_before=%d, offset_after=%d, correction_pos=%u, x->offset_before, x- >offset_after, x->correction_pos	DEBUG	IPT_ACCOUNT_NAME : checkentry() too big netmask.	INFO
ip_ct_h323:	DEBUG	IPT_ACCOUNT_NAME : checkentry() failed to allocate %zu for new table %s., sizeof(struct t_ipt_account_table), info->name	INFO
ip_ct_h323: incomplete TPKT (fragmented?)	DEBUG	IPT_ACCOUNT_NAME : checkentry() wrong network/ netmask.	INFO
ip_ct_h245: decoding error: %s,	DEBUG	account: Wrong netmask given by netmask parameter (%i). Valid is 32 to 0., netmask	INFO
ip_ct_h245: packet dropped	DEBUG	IPT_ACCOUNT_NAME : checkentry() failed to create procfs entry.	INFO
ip_ct_q931: decoding error: %s,	DEBUG	IPT_ACCOUNT_NAME : checkentry() failed to register match.	INFO
ip_ct_q931: packet dropped	DEBUG	failed to create procfs entry .	INFO
ip_ct_ras: decoding error: %s,	DEBUG	MPPE/MPPC encryption/compression module registered	INFO
ip_ct_ras: packet dropped	DEBUG	MPPE/MPPC encryption/compression module unregistered	INFO
ERROR registering port %d,	DEBUG	PPP generic driver version PPP_VERSION	INFO
ERROR registering port %d,	DEBUG	MPPE/MPPC encryption/compression module registered	INFO
ipt_connlimit [%d]: src=%u.%u.%u.%u:%d dst=%u.%u.%u.%u:%d %s,	DEBUG	MPPE/MPPC encryption/compression module unregistered	INFO
ipt_connlimit [%d]: src=%u.%u.%u.%u:%d dst=%u.%u.%u.%u:%d new,	DEBUG	PPP generic driver version PPP_VERSION	INFO
ipt_connlimit: Oops: invalid ct state ?	DEBUG	PPPoL2TP kernel driver, %s,	INFO
ipt_connlimit: Hmm, kmalloc failed :-(	DEBUG	PPPoL2TP kernel driver, %s,	INFO
ipt_connlimit: src=%u.%u.%u.%u mask=%u.%u.%u.%u	DEBUG	PPPoL2TP kernel driver, %s,	INFO
_lvl PPPOL2TP: _fmt, ##args	DEBUG	failed to create procfs entry .	INFO
%02X, ptr[length]	DEBUG	proc dir not created ..	INFO
%02X, ((unsigned char *) m- >msg_iov[i].iov_base)[j]	DEBUG	Initialzing Product Data modules	INFO
%02X, skb->data[i]	DEBUG	De initializing by \	INFO
_lvl PPPOL2TP: _fmt, ##args	DEBUG	kernel UMI module loaded	INFO
%02X, ptr[length]	DEBUG	kernel UMI module unloaded	INFO
%02X, ((unsigned char *) m- >msg_iov[i].iov_base)[j]	DEBUG	Loading bridge module	INFO
%02X, skb->data[i]	DEBUG	Unloading bridge module	INFO
_lvl PPPOL2TP: _fmt, ##args	DEBUG	unsupported command %d, cmd	INFO
%02X, ptr[length]	DEBUG	Loading ifDev module	INFO
%02X, ((unsigned char *) m- >msg_iov[i].iov_base)[j]	DEBUG	Unloading ifDev module	INFO
%02X, skb->data[i]	DEBUG	ERROR#%d in alloc_chrdev_region, result	INFO
KERN_EMERG THE value read is %d,value*/	DEBUG	ERROR#%d in cdev_add, result	INFO
KERN_EMERG Factory Reset button is pressed	DEBUG	using bcm switch %s, bcmswitch	INFO
KERN_EMERG Returing error in INTR registration	DEBUG	privlegedID %d wanporttNo: %d, privlegedID,wanportNo	INFO
KERN_EMERG Initialzing Factory defaults modules	DEBUG	Loading mii	INFO
Failed to allocate memory for pSipListNode	DEBUG	Unloading mii	INFO
SIPALG: Memeory allocation failed for pSipNodeEntryTbl	DEBUG	%s: Version 0.1	INFO
pkt-err %s, pktInfo.error	DEBUG	%s: driver unloaded, dev_info	INFO
pkt-err %s, pktInfo.error	DEBUG	wlan: %s backend registered, be- >iab_name	INFO
pkt-err %s, pktInfo.error	DEBUG	wlan: %s backend unregistered,	INFO
%s Len=%d, msg, len	DEBUG	wlan: %s acl policy registered, iac- >iac_name	INFO
%02x , ((uint8_t *) ptr)[i]	DEBUG	wlan: %s acl policy unregistered, iac- >iac_name	INFO
End	DEBUG	%s, tmpbuf	INFO
CVM_MOD_EXP_BASE MISMATCH cmd=%x base=%x, cmd,	DEBUG	VLAN2	INFO
op->sizeofptr = %ld, op->sizeofptr	DEBUG	VLAN3	INFO
opcode cmd = %x, cmd	DEBUG	VLAN4 <%d %d>,	INFO
modexp opcode received	DEBUG	%s: %s, dev_info, version	INFO

ログメッセージ	緊急度	ログメッセージ	緊急度
Memory Allocation failed	DEBUG	%s: driver unloaded, dev_info	INFO
modexpcrt opcode received	DEBUG	%s, buf	INFO
kmalloc failed	DEBUG	%s: %s (, dev_info, ath_hal_version	INFO
kmalloc failed	DEBUG	%s: driver unloaded, dev_info	INFO
kmalloc failed	DEBUG	%s: %s: mem=0x%lx, irq=%d hw_base=0x%p,	INFO
kmalloc failed	DEBUG	%s: %s, dev_info, version	INFO
kmalloc Failed	DEBUG	%s: driver unloaded, dev_info	INFO
kmalloc failed	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
unknown cyrpto ioctl cmd received %x, cmd	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
register_chrdev returned ZERO	DEBUG	%s: %s, dev_info, version	INFO
const char *descr, krb5_keyblock *k) {	DEBUG	%s: driver unloaded, dev_info	INFO
F password, &pdata	DEBUG	%s, buf	INFO
test key, key	DEBUG	%s: %s (, dev_info, ath_hal_version	INFO
pre-hashed key, key	DEBUG	%s: driver unloaded, dev_info	INFO
const char *descr, krb5_keyblock *k) {	DEBUG	%s: driver unloaded, dev_info	INFO
AES 128-bit key, &key	DEBUG	%s: Version 2.0.0	INFO
const char *descr, krb5_keyblock *k) {	DEBUG	%s: driver unloaded, dev_info	INFO
test key, key	DEBUG	%s: driver unloaded, dev_info	INFO
pre-hashed key, key	DEBUG	wlan: %s backend registered, be- >iab_name	INFO
const char *descr, krb5_keyblock *k) {	DEBUG	wlan: %s backend unregistered,	INFO
128-bit AES key,&dk	DEBUG	wlan: %s acl policy registered, iac- >iac_name	INFO
256-bit AES key, &dk	DEBUG	wlan: %s acl policy unregistered, iac- >iac_name	INFO
WARNING:	DEBUG	%s: %s, dev_info, version	INFO
bwMonMultipathNxtHopSelect:: checking rates	DEBUG	%s: driver unloaded, dev_info	INFO
hop :%d dev:%s usableBwLimit = %d currBwShare = %d lastHopSelected = %d weightedHopPrefer = %d ,	DEBUG	%s: %s (, dev_info, ath_hal_version	INFO
1. selecting hop: %d lastHopSelected = %d , selHop, lastHopSelected	DEBUG	%s: driver unloaded, dev_info	INFO
4. hop :%d dev:%s usableBwLimit = %d currBwShare = %d lastHopSelected = %d weightedHopPrefer = %d ,	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
2. selecting hop: %d lastHopSelected = %d , selHop, lastHopSelected	DEBUG	%s: %s, dev_info, version	INFO
3. selecting hop: %d lastHopSelected = %d , selHop, lastHopSelected	DEBUG	%s: driver unloaded, dev_info	INFO
bwMonitor multipath selection enabled	DEBUG	ath_pci: switching rfkill capability %s,	INFO
bwMonitor multipath selection disabled	DEBUG	Unknown autocreate mode: %s,	INFO
weightedHopPrefer set to %d ,weightedHopPrefer	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
bwMonitor sysctl registration failed	DEBUG	%s: %s, dev_info, version	INFO
bwMonitor sysctl registered	DEBUG	%s: driver unloaded, dev_info	INFO
bwMonitor sysctl not registered	DEBUG	%s: %s, dev_info, version	INFO
Unregistered bwMonitor sysctl	DEBUG	%s: unloaded, dev_info	INFO
CONFIG_SYSCTL enabled ...	DEBUG	%s: %s, dev_info, version	INFO
Initialized bandwidth monitor ...	DEBUG	%s: unloaded, dev_info	INFO
Removed bandwidth monitor ...	DEBUG	%s: %s, dev_info, version	INFO
Oops.. AES_GCM_encrypt failed (keylen:%u),key->cvm_keylen	DEBUG	%s: unloaded, dev_info	INFO
Oops.. AES_GCM_decrypt failed (keylen:%u),key->cvm_keylen	DEBUG	failed to create procfs entry .	INFO
%s, msg	DEBUG	ICMP: %u.%u.%u.%u:	INFO
%02x%s, data[i],	DEBUG	ICMP: %u.%u.%u.%u: Source	INFO
Failed to set AES encrypt key	DEBUG	Wrong address mask %u.%u.%u.%u from	INFO
Failed to set AES encrypt key	DEBUG	Redirect from %u.%u.%u.%u on %s about INFO	
AES %s Encrypt Test Duration: %d:%d, hard ? Hard : Soft,	DEBUG	IP: routing cache hash table of %u buckets, %ldKbytes,	INFO
Failed to set AES encrypt key	DEBUG	source route option %u.%u.%u.%u -> %u.%u.%u.%u,	INFO
Failed to set AES encrypt key	DEBUG	ICMP: %u.%u.%u.%u:	INFO
AES %s Decrypt Test Duration: %d:%d, hard ? Hard : Soft,	DEBUG	ICMP: %u.%u.%u.%u: Source	INFO

ログメッセージ	緊急度	ログメッセージ	緊急度
Failed to set AES encrypt key	DEBUG	Wrong address mask %u.%u.%u.%u from	INFO
Failed to set AES encrypt key	DEBUG	Redirect from %u.%u.%u.%u on %s about	INFO
Failed to set AES encrypt key	DEBUG	IP: routing cache hash table of %u buckets, %ldKbytes,	INFO
Failed to set AES encrypt key	DEBUG	source route option %u.%u.%u.%u -> %u.%u.%u.%u,	INFO
Failed to set DES encrypt key[%d], i	DEBUG	Wrong address mask %u.%u.%u.%u from	INFO
Failed to set DES decrypt key[%d], i	DEBUG	Redirect from %u.%u.%u.%u on %s about	INFO
Failed to set DES encrypt key[%d], i	DEBUG	source route option	INFO
Failed to set DES decrypt key[%d], i	DEBUG	ICMP: %u.%u.%u.%u:	INFO
Failed to set DES encrypt key	DEBUG	ICMP: %u.%u.%u.%u: Source	INFO
Failed to set DES decrypt key	DEBUG	Wrong address mask %u.%u.%u.%u from	INFO
Failed to set DES encrypt key	DEBUG	Redirect from %u.%u.%u.%u on %s about	INFO
Failed to set DES decrypt key	DEBUG	IP: routing cache hash table of %u buckets, %ldKbytes,	INFO
AES Software Test:	DEBUG	source route option %u.%u.%u.%u -> %u.%u.%u.%u,	INFO
AES Software Test %s, aesSoftTest(0) ? Failed : Passed	DEBUG	IPsec: device unregistering: %s, dev- >name	INFO
AES Hardware Test:	DEBUG	IPsec: device down: %s, dev->name	INFO
AES Hardware Test %s, aesHardTest(0) ? Failed : Passed	DEBUG	mark: only supports 32bit mark	WARNING
3DES Software Test:	DEBUG	ipt_time: invalid argument	WARNING
3DES Software Test %s, des3SoftTest(0) ? Failed : Passed	DEBUG	ipt_time: IPT_DAY didn't matched	WARNING
3DES Hardware Test:	DEBUG	./Logs_kernel.txt:45:KERN_WARNING	WARNING
3DES Hardware Test %s, des3HardTest(0) ? Failed : Passed	DEBUG	./Logs_kernel.txt:59:KERN_WARNING	WARNING
DES Software Test:	DEBUG	ipt_LOG: not logging via system console	WARNING
DES Software Test %s, desSoftTest(0) ? Failed : Passed	DEBUG	%s: wrong options length: %u, fname, opt_len	WARNING
DES Hardware Test:	DEBUG	%s: options rejected: o[0]=%02x, o[1]=%02x,	WARNING
DES Hardware Test %s, desHardTest(0) ? Failed : Passed	DEBUG	%s: wrong options length: %u,	WARNING
SHA Software Test:	DEBUG	%s: options rejected: o[0]=%02x, o[1]=%02x,	WARNING
SHA Software Test %s, shaSoftTest(0) ? Failed : Passed	DEBUG	%s: don't know what to do: o[5]=%02x,	WARNING
SHA Hardware Test:	DEBUG	%s: wrong options length: %u, fname, opt_len	WARNING
SHA Hardware Test %s, shaHardTest(0) ? Failed : Passed	DEBUG	%s: options rejected: o[0]=%02x, o[1]=%02x,	WARNING
MD5 Software Test:	DEBUG	%s: wrong options length: %u,	WARNING
MD5 Software Test %s, md5SoftTest(0) ? Failed : Passed	DEBUG	%s: options rejected: o[0]=%02x, o[1]=%02x,	WARNING
MD5 Hardware Test:	DEBUG	%s: don't know what to do: o[5]=%02x,	WARNING
MD5 Hardware Test %s md5HardTest(0) ? Failed : Passed,	DEBUG	*** New port %d ***, ntohs(expinfo- >natport)	WARNING
AES Software Test: %d iterations, iter	DEBUG	** skb len %d, dlen %d,(*pskb)->len,	WARNING
AES Software Test Duration: %d:%d,	DEBUG	********** Non linear skb	WARNING
AES Hardware Test: %d iterations, iter	DEBUG	End of sdp %p, nexthdr	WARNING
AES Hardware Test Duration: %d:%d,	DEBUG	%s: unknown pairwise cipher %d,	WARNING
3DES Software Test: %d iterations, iter	DEBUG	%s: unknown group cipher %d,	WARNING
3DES Software Test Duration: %d:%d,	DEBUG	%s: unknown SIOCSIWAUTH flag %d,	WARNING
3DES Hardware Test: %d iterations, iter	DEBUG	%s: unknown SIOCGIWAUTH flag %d,	WARNING
3DES Hardware Test Duration: %d:%d,	DEBUG	%s: unknown algorithm %d,	WARNING
DES Software Test: %d iterations, iter	DEBUG	%s: key size %d is too large,	WARNING
DES Software Test Duration: %d:%d,	DEBUG	try_module_get failed \	WARNING
DES Hardware Test: %d iterations, iter	DEBUG	%s: request_irq failed, dev->name	WARNING
DES Hardware Test Duration: %d:%d,	DEBUG	try_module_get failed	WARNING
SHA Software Test: %d iterations, iter	DEBUG	try_module_get failed \	WARNING
SHA Software Test Duration: %d:%d,	DEBUG	%s: unknown pairwise cipher %d,	WARNING
SHA Hardware Test: %d iterations, iter	DEBUG	%s: unknown group cipher %d,	WARNING
SHA Hardware Test Duration: %d:%d,	DEBUG	%s: unknown SIOCSIWAUTH flag %d,	WARNING
MD5 Software Test: %d iterations, iter	DEBUG	%s: unknown SIOCGIWAUTH flag %d,	WARNING
MD5 Software Test Duration: %d:%d,	DEBUG	%s: unknown algorithm %d,	WARNING
MD5 Hardware Test: %d iterations, iter	DEBUG	%s: key size %d is too large,	WARNING
MD5 Hardware Test Duration: %d:%d,	DEBUG	unable to load %s, scan_modnames[mode]	WARNING
./pnac/src/pnac/linux/kernel/xcalibur.c:20 9:#define DEBUG_PRINTK printk	DEBUG	Failed to mkdir /proc/net/madwifi	WARNING

ログメッセージ	緊急度	ログメッセージ	緊急度
bcmDeviceInit: registration failed	DEBUG	try_module_get failed	WARNING
bcmDeviceInit: pCdev Add failed	DEBUG	%s: request_irq failed, dev->name	WARNING
REG Size == 8 Bit	DEBUG	too many virtual ap's (already got %d), sc->sc_nvaps	WARNING
Value = %x ::: At Page = %x : Addr = %x	DEBUG	%s: request_irq failed, dev->name	WARNING
REG Size == 16 Bit	DEBUG	rix %u (%u) bad ratekbps %u mode %u,	WARNING
Value = %x ::: At Page = %x : Addr = %x	DEBUG	cix %u (%u) bad ratekbps %u mode %u,	WARNING
REG Size == 32 Bit	DEBUG	%s: no rates for %s?,	WARNING
Value = %x ::: At Page = %x : Addr =%x	DEBUG	no rates yet! mode %u, sc- >sc_curmode	WARNING
REG Size == 64 Bit	DEBUG	%u.%u.%u.%u sent an invalid ICMP	WARNING
REG Size is not in 8/16/32/64	DEBUG	dst cache overflow	WARNING
Written Value = %x ::: At Page = %x : Addr = %x	DEBUG	Neighbour table overflow.	WARNING
bcm_ioctl :Unknown Ioctl Case :	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
==========Register Dump for Port Number # %d=========,port	DEBUG	martian destination %u.%u.%u.%u from	WARNING
%s : Read Status=%s data=%#x,regName[j],	DEBUG	martian source %u.%u.%u.%u from	WARNING
%s : Read Status=%s data=%#x,regName[j],	DEBUG	ll header:	WARNING
powerDeviceInit: device registration failed	DEBUG	%u.%u.%u.%u sent an invalid ICMP	WARNING
powerDeviceInit: adding device failed	DEBUG	dst cache overflow	WARNING
%s: Error: Big jump in pn number. TID=%d, from %x %x to %x %x.	DEBUG	Neighbour table overflow.	WARNING
%s: The MIC is corrupted. Drop this frame., __func__	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
%s: The MIC is OK. Still use this frame and update PN., __func__	DEBUG	martian destination %u.%u.%u.%u from	WARNING
ADDBA send failed: recipient is not a 11n node	DEBUG	martian source %u.%u.%u.%u from	WARNING
Cannot Set Rate: %x, value	DEBUG	ll header:	WARNING
Getting Rate Series: %x,vap- >iv_fixed_rate.series	DEBUG	%u.%u.%u.%u sent an invalid ICMP	WARNING
Getting Retry Series: %x,vap- >iv_fixed_rate.retries	DEBUG	dst cache overflow	WARNING
IC Name: %s,ic->ic_dev->name	DEBUG	Neighbour table overflow.	WARNING
usage: rtparams rt_idx <0|1> per <0..100> probe_intval <0..100>	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
usage: acparams ac <0|3> RTS <0|1> aggr scaling <0..4> min mbps <0..250>	DEBUG	martian source %u.%u.%u.%u from	WARNING
usage: hbrparams ac <2> enable <0|1> per_low <0..50>	DEBUG	ll header:	WARNING
%s(): ADDBA mode is AUTO, __func__	DEBUG	martian destination %u.%u.%u.%u from	WARNING
%s(): Invalid TID value, __func__	DEBUG	%u.%u.%u.%u sent an invalid ICMP	WARNING
%s(): ADDBA mode is AUTO, __func__	DEBUG	dst cache overflow	WARNING
%s(): Invalid TID value, __func__	DEBUG	Neighbour table overflow.	WARNING
%s(): Invalid TID value, __func__	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
Addba status IDLE	DEBUG	martian destination %u.%u.%u.%u from	WARNING
%s(): ADDBA mode is AUTO, __func__	DEBUG	martian source %u.%u.%u.%u from	WARNING
%s(): Invalid TID value, __func__	DEBUG	ll header:	WARNING
Error in ADD- no node available	DEBUG	Unable to create ip_set_list	ERROR
%s(): Channel capabilities do not match, chan flags 0x%x,	DEBUG	Unable to create ip_set_hash	ERROR
%s: cannot map channel to mode; freq %u flags 0x%x,	DEBUG	ip_conntrack_in: Frag of proto %u (hook=%u),	ERROR
ic_get_currentCountry not initialized yet	DEBUG	Unable to register netfilter socket option	ERROR
Country ie is %c%c%c,	DEBUG	Unable to create ip_conntrack_hash	ERROR
%s: wrong state transition from %d to %d,	DEBUG	Unable to create ip_conntrack slab cache	ERROR
%s: wrong state transition from %d to %d,	DEBUG	Unable to create ip_expect slab cache	ERROR
%s: wrong state transition from %d to %d,	DEBUG	Unable to create ip_set_iptreeb slab cache	ERROR
%s: wrong state transition from %d to %d,	DEBUG	Unable to create ip_set_iptreed slab cache	ERROR
%s: wrong state transition from %d to %d,	DEBUG	%s: cannot allocate space for %scompressor, fname,	ERROR
%s: wrong state transition from %d to %d,	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
ieee80211_deliver_l2uf: no buf available	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
%s: %s, vap->iv_dev->name, buf /* NB: no */	DEBUG	%s: cannot load ARC4 module, fname	ERROR
%s: [%s] %s, vap->iv_dev->name,	DEBUG	%s: cannot load SHA1 module, fname	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
%s: [%s] %s, vap->iv_dev->name, ether_sprintf(mac), buf	DEBUG	%s: CryptoAPI SHA1 digest size too small, fname	ERROR
[%s:%s] discard %s frame, %s, vap- >iv_dev->name,	DEBUG	%s: cannot allocate space for SHA1 digest, fname	ERROR
[%s:%s] discard frame, %s, vap- >iv_dev->name,	DEBUG	%s%d: trying to write outside history	ERROR
[%s:%s] discard %s information element, %s,	DEBUG	%s%d: trying to write outside history	ERROR
[%s:%s] discard information element, %s,	DEBUG	%s%d: trying to write outside history	ERROR
[%s:%s] discard %s frame, %s, vap- >iv_dev->name,	DEBUG	%s%d: too big uncompressed packet: %d,	ERROR
[%s:%s] discard frame, %s, vap- >iv_dev->name,	DEBUG	%s%d: encryption negotiated but not an	ERROR
HBR list dumpNode\tAddress\t\t\tState\tTrigger\tB lock	DEBUG	%s%d: error - not an MPPC or MPPE frame	ERROR
Nodes informationAddress\t\t\tBlock\t\tDroped Vl frames	DEBUG	Kernel doesn't provide ARC4 and/or SHA1 algorithms	ERROR
%d\t %2.2x:%2.2x:%2.2x:%2.2x:%2.2x:%2.2x \t%s\t%s\t%s,	DEBUG	PPP: not interface or channel??	ERROR
%2.2x:%2.2x:%2.2x:%2.2x:%2.2x:%2.2x \t%s\t\t%d,	DEBUG	PPP: no memory (VJ compressor)	ERROR
[%d]\tFunction\t%s, j, ni- >node_trace[i].funcp	DEBUG	failed to register PPP device (%d), err	ERROR
[%d]\tMacAddr\t%s, j,	DEBUG	PPP: no memory (VJ comp pkt)	ERROR
[%d]\tDescp\t\t%s, j, ni- >node_trace[i].descp	DEBUG	PPP: no memory (comp pkt)	ERROR
[%d]\tValue\t\t%llu(0x%llx), j, ni- >node_trace[i].value,	DEBUG	ppp: compressor dropped pkt	ERROR
ifmedia_add: null ifm	DEBUG	PPP: no memory (fragment)	ERROR
Adding entry for	DEBUG	PPP: VJ uncompressed error	ERROR
ifmedia_set: no match for 0x%x/0x%x,	DEBUG	ppp_decompress_frame: no memory	ERROR
ifmedia_set: target	DEBUG	ppp_mp_reconstruct bad seq %u < %u,	ERROR
ifmedia_set: setting to	DEBUG	PPP: couldn't register device %s (%d),	ERROR
ifmedia_ioctl: switching %s to , dev- >name	DEBUG	ppp: destroying ppp struct %p but dead=%d	ERROR
ifmedia_match: multiple match for	DEBUG	ppp: destroying undead channel %p !,	ERROR
<unknown type>	DEBUG	PPP: removing module but units remain!	ERROR
desc->ifmt_string	DEBUG	PPP: failed to unregister PPP device	ERROR
mode %s, desc->ifmt_string	DEBUG	%s: cannot allocate space for %scompressor, fname,	ERROR
<unknown subtype>	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
%s, desc->ifmt_string	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
%s%s, seen_option++ ? , : ,	DEBUG	%s: cannot load ARC4 module, fname	ERROR
%s%s, seen_option++ ? , : ,	DEBUG	%s: cannot load SHA1 module, fname	ERROR
%s, seen_option ? > :	DEBUG	%s: CryptoAPI SHA1 digest size too small, fname	ERROR
%s: %s, dev->name, buf	DEBUG	%s: cannot allocate space for SHA1 digest, fname	ERROR
%s: no memory for sysctl table!, __func__	DEBUG	%s%d: trying to write outside history	ERROR
%s: failed to register sysctls!, vap- >iv_dev->name	DEBUG	%s%d: trying to write outside history	ERROR
Atheros HAL assertion failure: %s: line %u: %s,	DEBUG	%s%d: trying to write outside history	ERROR
ath_hal: logging to %s %s, ath_hal_logfile,	DEBUG	%s%d: too big uncompressed packet: %d,	ERROR
ath_hal: logging disabled	DEBUG	%s%d: encryption negotiated but not an	ERROR
%s%s, sep, ath_hal_buildopts[i]	DEBUG	%s%d: error - not an MPPC or MPPE frame	ERROR
ath_pci: No devices found, driver not installed.	DEBUG	Kernel doesn't provide ARC4 and/or SHA1 algorithms	ERROR
---:%d pri:%d qd:%u ad:%u sd:%u tot:%u amp:%d %02x:%02x:%02x,	DEBUG	PPP: not interface or channel??	ERROR
SC Pushbutton Notify on %s::%s,dev- >name,vap->iv_dev->name	DEBUG	PPP: no memory (VJ compressor)	ERROR
Could not find Board Configuration Data	DEBUG	failed to register PPP device (%d), err	ERROR
Could not find Radio Configuration data	DEBUG	PPP: no memory (comp pkt)	ERROR
%s: No device, __func__	DEBUG	ppp: compressor dropped pkt	ERROR
ath_ahb: No devices found, driver not installed.	DEBUG	PPP: no memory (VJ comp pkt)	ERROR
PKTLOG_TAG %s:proc_dointvec failed, __FUNCTION__	DEBUG	PPP: no memory (comp pkt)	ERROR
PKTLOG_TAG %s:proc_dointvec failed, __FUNCTION__	DEBUG	PPP: no memory (fragment)	ERROR
%s: failed to register sysctls!, proc_name	DEBUG	PPP: VJ uncompressed error	ERROR
PKTLOG_TAG %s: proc_mkdir failed, __FUNCTION__	DEBUG	ppp_decompress_frame: no memory	ERROR
PKTLOG_TAG %s: pktlog_attach failed for %s,	DEBUG	ppp_mp_reconstruct bad seq %u < %u,	ERROR
PKTLOG_TAG %s:allocation failed for pl_info, __FUNCTION__	DEBUG	PPP: couldn't register device %s (%d),	ERROR
PKTLOG_TAG %s:allocation failed for pl_info, __FUNCTION__	DEBUG	ppp: destroying ppp struct %p but dead=%d	ERROR
PKTLOG_TAG %s: create_proc_entry failed for %s,	DEBUG	ppp: destroying undead channel %p !,	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
PKTLOG_TAG %s: sysctl register failed for %s,	DEBUG	PPP: removing module but units remain!	ERROR
PKTLOG_TAG %s: page fault out of range, __FUNCTION__	DEBUG	PPP: failed to unregister PPP device	ERROR
PKTLOG_TAG %s: page fault out of range, __FUNCTION__	DEBUG	JBD: bad block at offset %u,	ERROR
PKTLOG_TAG %s: Log buffer unavailable, __FUNCTION__	DEBUG	JBD: corrupted journal superblock	ERROR
PKTLOG_TAG	DEBUG	JBD: bad block at offset %u,	ERROR
Logging should be disabled before changing bufer size	DEBUG	JBD: Failed to read block at offset %u,	ERROR
%s:allocation failed for pl_info, __func__	DEBUG	JBD: error %d scanning journal, err	ERROR
%s: Unable to allocate buffer, __func__	DEBUG	JBD: IO error %d recovering block	ERROR
%s:allocation failed for pl_info, __func__	DEBUG	./Logs_kernel.txt:303:KERN_ERR	ERROR
%s: Unable to allocate buffer, __func__	DEBUG	./Logs_kernel.txt:304:KERN_ERR	ERROR
Atheros HAL assertion failure: %s: line %u: %s,	DEBUG	JBD: recovery pass %d ended at	ERROR
ath_hal: logging to %s %s, ath_hal_logfile,	DEBUG	%s: %s:%d: BAD SESSION MAGIC \	ERROR
ath_hal: logging disabled	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC \	ERROR
%s%s, sep, ath_hal_buildopts[i]	DEBUG	msg->msg_namelen wrong, %d, msg- >msg_namelen	ERROR
failed to allocate rx descriptors: %d, error	DEBUG	addr family wrong: %d, usin->sin_family	ERROR
ath_stoprecv: rx queue %p, link %p,	DEBUG	udp addr=%x/%hu, usin- >sin_addr.s_addr, usin->sin_port	ERROR
no mpdu (%s), __func__	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
Reset rx chain mask. Do internal reset. (%s), __func__	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
OS_CANCEL_TIMER failed!!	DEBUG	socki_lookup: socket file changed!	ERROR
%s: unable to allocate channel table, __func__	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
%s: unable to collect channel list from hal;	DEBUG	%s: %s:%d: BAD SESSION MAGIC \	ERROR
%s: cannot map channel to mode; freq %u flags 0x%x,	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC \	ERROR
%s: unable to reset channel %u (%uMhz)	DEBUG	msg->msg_namelen wrong, %d, msg- >msg_namelen	ERROR
%s: unable to restart recv logic,	DEBUG	addr family wrong: %d, usin->sin_family	ERROR
%s: start DFS WAIT period on channel %d, __func__,sc->sc_curchan.channel	DEBUG	udp addr=%x/%hu, usin- >sin_addr.s_addr, usin->sin_port	ERROR
%s: cancel DFS WAIT period on channel %d, __func__, sc- >sc_curchan.channel	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
Non-DFS channel, cancelling previous DFS wait timer channel %d, sc- >sc_curchan.channel	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
%s: unable to reset hardware; hal status %u	DEBUG	socki_lookup: socket file changed!	ERROR
%s: unable to start recv logic, __func__	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
%s: unable to start recv logic, __func__	DEBUG	%s: %s:%d: BAD SESSION MAGIC \	ERROR
%s: unable to reset hardware; hal status %u,	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC \	ERROR
hardware error; reseting	DEBUG	msg->msg_namelen wrong, %d, msg- >msg_namelen	ERROR
rx FIFO overrun; reseting	DEBUG	addr family wrong: %d, usin->sin_family	ERROR
%s: During Wow Sleep and got BMISS, __func__	DEBUG	udp addr=%x/%hu, usin- >sin_addr.s_addr, usin->sin_port	ERROR
AC\tRTS \tAggr Scaling\tMin Rate(Kbps)\tHBR \tPER LOW THRESHOLD	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
BE\t%s\t\t%d\t%6d\t\t%s\t%d,	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
BK\t%s\t\t%d\t%6d\t\t%s\t%d,	DEBUG	socki_lookup: socket file changed!	ERROR
VI\t%s\t\t%d\t%6d\t\t%s\t%d,	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
VO\t%s\t\t%d\t%6d\t\t%s\t%d,	DEBUG	rebootHook: null function pointer	ERROR
--%d,%p,%lu:0x%x 0x%x 0x%p 0x%x 0x%x 0x%x 0x%x,	DEBUG	Bad ioctl command	ERROR
bb state: 0x%08x 0x%08x, bbstate(sc, 4ul), bbstate(sc, 5ul)	DEBUG	fResetMod: Failed to configure gpio pin	ERROR
%08x %08x %08x %08x %08x %08x %08x %08x%08x %08x %08x %08x,	DEBUG	fResetMod: Failed to register interrupt handler	ERROR
noise floor: (%d, %d) (%d, %d) (%d, %d),	DEBUG	registering char device failed	ERROR
%p: %08x %08x %08x %08x %08x %08x %08x %08x %08x %08x %08x %08x,	DEBUG	unregistering char device failed	ERROR
--%d,%p,%lu:0x%x 0x%x 0x%p 0x%x 0x%x 0x%x 0x%x,	DEBUG	proc entry delete failed	ERROR
%08x %08x %08x %08x %08x %08x %08x %08x%08x %08x %08x %08x,	DEBUG	proc entry initialization failed	ERROR
%s: unable to allocate device object., __func__	DEBUG	testCompHandler: received %s from %d, (char *)pInBuf,	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
%s: unable to attach hardware; HAL status %u,	DEBUG	UMI proto registration failed %d,ret	ERROR
%s: HAL ABI msmatch;	DEBUG	AF_UMI registration failed %d,ret	ERROR
%s: Warning, using only %u entries in %u key cache,	DEBUG	umi initialization failed %d,ret	ERROR
unable to setup a beacon xmit queue!	DEBUG	kernel UMI registration failed!	ERROR
unable to setup CAB xmit queue!	DEBUG	./Logs_kernel.txt:447:KERN_ERR	ERROR
unable to setup xmit queue for BE traffic!	DEBUG	ERROR msm not found properly %d, len %d, msm,	ERROR
%s DFS attach failed, __func__	DEBUG	ModExp returned Error	ERROR
%s: Invalid interface id = %u, __func__, if_id	DEBUG	ModExp returned Error	ERROR
%s:grppoll Buf allocation failed ,__func__	DEBUG	%s: 0x%p len %u, tag, p, (unsigned int)len	ERROR
%s: unable to start recv logic,	DEBUG	%03d:, i	ERROR
%s: Invalid interface id = %u, __func__, if_id	DEBUG	%02x, ((unsigned char *)p)[i]	ERROR
%s: unable to allocate channel table, __func__	DEBUG	mic check failed	ERROR
%s: Tx Antenna Switch. Do internal reset., __func__	DEBUG	%s: 0x%p len %u, tag, p, (unsigned int)len	ERROR
Radar found on channel %d (%d MHz),	DEBUG	%03d:, i	ERROR
End of DFS wait period	DEBUG	%02x, ((unsigned char *)p)[i]	ERROR
%s error allocating beacon, __func__	DEBUG	mic check failed	ERROR
failed to allocate UAPSD QoS NULL tx descriptors: %d, error	DEBUG	[%s] Wrong parameters, __func__	ERROR
failed to allocate UAPSD QoS NULL wbuf	DEBUG	[%s] Wrong Key length, __func__	ERROR
%s: unable to allocate channel table, __func__	DEBUG	[%s] Wrong parameters, __func__	ERROR
%s: unable to update h/w beacon queue parameters,	DEBUG	[%s] Wrong Key length, __func__	ERROR
ALREADY ACTIVATED	DEBUG	[%s] Wrong parameters, __func__	ERROR
%s: missed %u consecutive beacons,	DEBUG	[%s] Wrong Key length, __func__	ERROR
%s: busy times: rx_clear=%d, rx_frame=%d, tx_frame=%d, __ func__, rx_clear, rx_frame, tx_frame	DEBUG	[%s] Wrong parameters, __func__	ERROR
%s: unable to obtain busy times, __func__	DEBUG	[%s] Wrong Key length, __func__	ERROR
%s: beacon is officially stuck,	DEBUG	[%s]: Wrong parameters, __func__	ERROR
Busy environment detected	DEBUG	[%s] Wrong Key Length %d, __func__, des_key_len	ERROR
Inteference detected	DEBUG	[%s] Wrong parameters %d, __func__, des_key_len	ERROR
rx_clear=%d, rx_frame=%d, tx_frame=%d,	DEBUG	[%s] Wrong Key Length %d, __func__, des_key_len	ERROR
%s: resume beacon xmit after %u misses,	DEBUG	[%s] Wrong parameters, __func__	ERROR
%s: stuck beacon; resetting (bmiss count %u),	DEBUG	[%s] Wrong Key Length, __func__	ERROR
EMPTY QUEUE	DEBUG	[%s] Wrong parameters, __func__	ERROR
SWRInfo: seqno %d isswRetry %d retryCnt %d,wh ? (*(u_int16_ t *)&wh- >i_seq[0]) >> 4 : 0, bf->bf_isswretry,bf- >bf_swretries	DEBUG	[%s] Wrong Key Length, __func__	ERROR
Buffer #%08X --> Next#%08X Prev#%08X Last#%08X,bf, TAILQ_NEXT(bf,bf_list),	DEBUG	[%s] Wrong parameters, __func__	ERROR
Stas#%08X flag#%08X Node#%08X, bf->bf_status, bf->bf_ flags, bf->bf_node	DEBUG	[%s] Wrong parameters, __func__	ERROR
Descr #%08X --> Next#%08X Data#%08X Ctl0#%08X Ctl1#%08X, bf- >bf_daddr, ds->ds_link, ds->ds_data, ds->ds_ ctl0, ds->ds_ctl1	DEBUG	[%s] Wrong parameters, __func__	ERROR
Ctl2#%08X Ctl3#%08X Sta0#%08X Sta1#%08X,ds->ds_hw[0], ds->ds_hw[1], lastds->ds_hw[2], lastds- >ds_hw[3]	DEBUG	[%s] Wrong parameters, __func__	ERROR
Error entering wow mode	DEBUG	device name=%s not found, pReq- >ifName	ERROR
Wakingup due to wow signal	DEBUG	unable to register KIFDEV to UMI	ERROR
%s, wowStatus = 0x%x, __func__, wowStatus	DEBUG	ERROR: %s: Timeout at page %#0x addr %#0x	ERROR
Pattern added already	DEBUG	ERROR: %s: Timeout at page %#0x addr %#0x	ERROR
Error : All the %d pattern are in use. Cannot add a new pattern , MAX_NUM_PATTERN	DEBUG	Invalid IOCTL %#08x, cmd	ERROR
Pattern added to entry %d ,i	DEBUG	%s: unable to register device, dev- >name	ERROR
Remove wake up pattern	DEBUG	ath_pci: 32-bit DMA not available	ERROR
mask = %p pat = %p ,maskBytes,patternBytes	DEBUG	ath_pci: cannot reserve PCI memory region	ERROR
mask = %x pat = %x ,(u_int32_t)maskBytes, (u_int32_t) patternBytes	DEBUG	ath_pci: cannot remap PCI memory region) ;	ERROR
Pattern Removed from entry %d ,i	DEBUG	ath_pci: no memory for device state	ERROR

ログメッセージ	緊急度	ログメッセージ	緊急度
Error : Pattern not found	DEBUG	%s: unable to register device, dev- >name	ERROR
PPM STATE ILLEGAL %x %x, forcePpmStateCur, afp->forceState	DEBUG	ath_dev_probe: no memory for device state	ERROR
FORCE_PPM %4d %6.6x %8.8x %8.8x %8.8x %3.3x %4.4x,	DEBUG	%s: no memory for device state, __func__	ERROR
failed to allocate tx descriptors: %d, error	DEBUG	kernel MIBCTL registration failed!	ERROR
failed to allocate beacon descripotrs: %d, error	DEBUG	Bad ioctl command	ERROR
failed to allocate UAPSD descripotrs: %d, error	DEBUG	WpsMod: Failed to configure gpio pin	ERROR
hal qnum %u out of range, max %u!,	DEBUG	WpsMod: Failed to register interrupt handler	ERROR
HAL AC %u out of range, max %zu!,	DEBUG	registering char device failed	ERROR
HAL AC %u out of range, max %zu!,	DEBUG	unregistering char device failed	ERROR
%s: unable to update hardware queue %u!,	DEBUG	%s:%d - ERROR: non-NULL node pointer in %p, %p<%s>!	ERROR
Multicast Q:	DEBUG	%s:%d - ERROR: non-NULL node pointer in %p, %p<%s>!	ERROR
%p , buf	DEBUG	can't alloc name %s, name	ERROR
buf flags - 0x%08x --------- , buf- >bf_flags	DEBUG	%s: unable to register device, dev- >name	ERROR
buf status - 0x%08x, buf->bf_status	DEBUG	failed to automatically load module: %s; \	ERROR
# frames in aggr - %d, length of aggregate - %d, length of frame - %d, sequence number - %d, tidno - %d,	DEBUG	Unable to load needed module: %s; no support for \	ERROR
isdata: %d isaggr: %d isampdu: %d ht: %d isretried: %d isxretried: %d shpreamble: %d isbar: %d ispspoll: %d aggrburst: %d calcairtime: %d qosnulleosp: %d,	DEBUG	Module \%s\ is not known, buf	ERROR
%p: 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x,	DEBUG	Error loading module \%s\, buf	ERROR
0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x,	DEBUG	Module \%s\ failed to initialize, buf	ERROR
0x%08x 0x%08x 0x%08x 0x%08x,	DEBUG	ath_pci: 32-bit DMA not available	ERROR
sc_txq[%d] : , i	DEBUG	ath_pci: cannot reserve PCI memory region	ERROR
tid %p pause %d : , tid, tid->paused	DEBUG	ath_pci: cannot remap PCI memory region) ;	ERROR
%d: %p , j, tid->tx_buf[j]	DEBUG	ath_pci: no memory for device state	ERROR
%p , buf	DEBUG	%s: unable to attach hardware: '%s' (HAL status %u),	ERROR
axq_q:	DEBUG	%s: HAL ABI mismatch;	ERROR
%s: unable to reset hardware; hal status %u, __func__, status	DEBUG	%s: failed to allocate descriptors: %d,	ERROR
****ASSERTION HIT****	DEBUG	%s: unable to setup a beacon xmit queue!,	ERROR
MacAddr=%s,	DEBUG	%s: unable to setup CAB xmit queue!,	ERROR
TxBufIdx=%d, i	DEBUG	%s: unable to setup xmit queue for %s traffic!,	ERROR
Tid=%d, tidno	DEBUG	%s: unable to register device, dev- >name	ERROR
AthBuf=%p, tid->tx_buf[i]	DEBUG	%s: autocreation of VAP failed: %d,	ERROR
%s: unable to reset hardware; hal status %u,	DEBUG	ath_dev_probe: no memory for device state	ERROR
%s: unable to reset hardware; hal status %u,	DEBUG	kdot11RogueAPEnable called with NULL argument.	ERROR
%s: unable to start recv logic,	DEBUG	kdot11RogueAPEnable: can not add more interfaces	ERROR
_fmt, __VA_ARGS__ \	DEBUG	kdot11RogueAPGetState called with NULL argument.	ERROR
sample_pri=%d is a multiple of refpri=%d, sample_pri, refpri	DEBUG	kdot11RogueAPDisable called with NULL argument.	ERROR
==========ft- >ft_numfilters=%u==========, ft->ft_numfilters	DEBUG	%s: SKB does not exist., __FUNCTION__	ERROR
filter[%d] filterID = %d rf_numpulses=%u; rf->rf_minpri=%u; rf->rf_maxpri=%u; rf->rf_threshold=%u; rf- >rf_filterlen=%u; rf->rf_mindur=%u; rf- >rf_maxdur=%u,j, rf->rf_pulseid,	DEBUG	%s: recvd invalid skb	ERROR
NOL	DEBUG	unable to register KIFDEV to UMI	ERROR
WARNING!!! 10 minute CAC period as channel is a weather radar channel	DEBUG	The system is going to factory defaults.....!!!	CRITICAL
%s disable detects, __func__	DEBUG	%s, msg	CRITICAL
%s enable detects, __func__	DEBUG	%02x, *(data + i)	CRITICAL
%s disable FFT val=0x%x , __func__, val	DEBUG	Inside crypt_open in driver ######	CRITICAL
%s enable FFT val=0x%x , __func__, val	DEBUG	Inside crypt_release in driver ######	CRITICAL
%s debug level now = 0x%x , __func__, dfs_debug_level	DEBUG	Inside crypt_init module in driver @@@@@@@@	CRITICAL
RateTable:%d, maxvalidrate:%d, ratemax:%d, pRc->rateTableSize,k,pRc- >rateMaxPhy	DEBUG	Inside crypt_cleanup module in driver @@@@@@@@	CRITICAL

ログメッセージ	緊急度	ログメッセージ	緊急度
%s: txRate value of 0x%x is bad., __FUNCTION__, txRate	DEBUG	SKB is null : %p ,skb	CRITICAL
Valid Rate Table:-	DEBUG	DST is null : %p ,dst	CRITICAL
Index:%d, value:%d, code:%x, rate:%d, flag:%x, i, (int) validRateIndex[i],	DEBUG	DEV is null %p %p ,dev,dst	CRITICAL
RateTable:%d, maxvalidrate:%d, ratemax:%d, pRc->rateTableSize,k,pRc- >rateMaxPhy	DEBUG	Packet is Fragmented %d,pBufMgr- >len	CRITICAL
Can't allocate memory for ath_vap.	DEBUG	Marked the packet proto:%d sip:%x dip:%x sport:%d dport:%d spi:%d,isr:%p:%p %p	CRITICAL
Unable to add an interface for ath_dev.	DEBUG	SAV CHECK FAILED IN DECRYPTION	CRITICAL
%s: [%02u] %-7s , tag, ix, ciphers[hk- >kv_type]	DEBUG	FAST PATH Breaks on BUF CHECK	CRITICAL
%02x, hk->kv_val[i]	DEBUG	FAST PATH Breaks on DST CHECK	CRITICAL
mac %02x-%02x-%02x-%02x-%02x-%02x, mac[0], mac[1], mac[2], mac[3], mac[4], mac[5]	DEBUG	FAST PATH Breaks on MTU %d %d %d, bufMgrLen(pBufMgr),mtu,dst_mtu(p Dst->path)	CRITICAL
mac 00-00-00-00-00-00	DEBUG	FAST PATH Breaks on MAX PACKET %d %d, bufMgrLen(pBufMgr),IP_MAX_PACKET	CRITICAL
%02x, hk->kv_mic[i]	DEBUG	SAV CHECK FAILED IN ENCRYPTION	CRITICAL
txmic	DEBUG	Match Found proto %d spi %d,pPktInfo->proto, pFlowEntry- >pre.spi	CRITICAL
%02x, hk->kv_txmic[i]	DEBUG	PRE: proto: %u srcip:%u.%u.%u.%u sport :%u dstip: %u.%u.%u.%u dport: %u,	CRITICAL
Cannot support setting tx and rx keys individually	DEBUG	POST: proto: %u srcip:%u.%u.%u.%u sport :%u dstip: %u.%u.%u.%u dport: %u,	CRITICAL
bogus frame type 0x%x (%s),	DEBUG	Clearing the ISR %p,p	CRITICAL
ERROR: ieee80211_encap ret NULL	DEBUG	PROTO:%d %u.%u.%u.%u--- >%u.%u.%u.%u,	CRITICAL
ERROR: ath_amsdu_attach not called	DEBUG	ESP-DONE: %p %p,sav,m	CRITICAL
%s: no memory for cwm attach, __func__	DEBUG	ESP-BAD: %p %p,sav,m	CRITICAL
%s: error - acw NULL. Possible attach failure, __func__	DEBUG	Bug in ip_route_input_slow().	CRITICAL
%s: unable to abort tx dma, __func__	DEBUG	Bug in ip_route_input_slow().	CRITICAL
%s: no memory for ff attach, __func__	DEBUG	Bug in ip_route_input \	CRITICAL
Failed to initiate PBC based enrolle association	DEBUG	Bug in ip_route_input_slow().	CRITICAL
KERN_EMERG Returing error in INTR registration	DEBUG	AH: Assigning the secure flags for sav :%p,sav	CRITICAL
KERN_EMERG Initialzing Wps module	DEBUG	ESP: Assigning the secure flags for sav :%p skb:%p src:%x dst:%x,sav,skb,ip- >ip_src.s_addr,ip->ip_dst.s_addr	CRITICAL
%s:%d %s, __FILE__, __LINE__, __func__	DEBUG	%s Buffer %d mtu %d path mtu %d header %d trailer %d,__func__,bufMgrLen(pBufMgr),mtu, dst_mtu(pDst->path),pDst- >header_len,pDst->trailer_len	CRITICAL