D-Link DSR-500/1000/1000AC Unified Services VPN Router





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。
▲ 危険 この表示を無視し、間違った使い方をすると	、死亡または重傷を負うおそれがあります。
▲警告 この表示を無視し、間違った使い方をすると	、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、間違った使い方をすると	、傷害または物的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。
	危険
 ☆ 止 火災、やけど、けが、感電などの原因となります。 かれた手でさわらない 	☆ 止 法気、湿気、埃の多い場所、高温になる場所や 熱のこもりやすい場所(火のそば、暖房器具のそば、 こたつや布団の中、直射日光の当たる場所、炎天下の車内、 風呂場など)、振動の激しい場所では、使用、保管、放置しない ☆ 、 かけば、はが、 東西、地防の原因したします
☆ 止 感電の原因となります。	欠災、やけど、けか、感電、故障の原因となります。 ○ 内部に全尾物や燃えやすいきのを入れたい
水をかけたり、ぬらしたりしない 素止 内部に水が入ると、火災、感電、故障の原因となります。	
水などの液体(飲料水、汗、海水、ペットの尿など) でぬれた状態で触ったり、電源を入れたりしない 火災、やけど、けが、感電、故障の原因となります。	砂や土、泥をかけたり、直に置いたりしない。 また、砂などが付着した手で触れない 火災、やけど、けが、感電、故障の原因となります。
各種端子やスロットに水などの液体(飲料水、汗、海水 ペットの尿など)をいれない。万が一、入ってしまった場合に 直ちに電源プラグをコンセントから抜く 火災、やけど、けが、感電、故障の原因となります。	電子レンジ、IH 調理器などの加熱調理機、 圧力釜など高圧容器に入れたり、近くに置いたりしない 火災、やけど、けが、感電、故障の原因となります。
	*** 11
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 故障の原因となります。	ガソリンスタンドなど引火性ガスが発生する可能性のある場所や 粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る 引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。
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 感電、火災の原因になります。 使用を止めて、ケーブルノコード類を抱いて、煙が出たくたって	★ カメラのレンズに直射日光などを長時間あてない 素子の退色、焼付きや、レンズの集光作用により、 火災、やけど、けがまたは故障の原因となります。
	無線製品は病院内で使用する場合は、 各医療機関の指示に従って使用する 電子機器や医療電気機器に悪影響を及ぼすおそれがあります。
<u>奈</u> 止火災、感電、または故障の原因となります。 <u>へ</u> たこ足配線禁止 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	本製品の周辺に放熱を妨げるようなもの (フィルムやシールでの装飾を含む)を置かない 火災、または故障の原因となります。
 ◎ () () () () () () () () () () () () ()	耳を本体から離してご使用ください 大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。
ア、火、 窓電、 まこは 叙障の原因となります。	無線製品をご使用の場合、医用電気機器などを 装着している場合は、医用電気機器メーカーもしくは、 販売業者に、電波による影響について確認の上使用する 医常要を増加に要認識を取ばされるおおにはす。
ケーブル/コード類や端子を破損させない 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、 または故障の原因となります。	医療電気機器に悪影響を及ぼすあてれいあります。 高精度な制御や微弱な信号を取り扱う 電子機器の近くでは使用しない 電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。
本製品付属のACアダプタもしくは電源ケーブルを 指定のコンセントに正しく接続して使用する 火災、感電、または故障の原因となります。	ディスプレイ部やカメラのレンズを破損した際は、 割れたガラスや露出した端末内部に注意する 破損部や露出部に触れると、やけど、けが、感電の原因となります。
会光源をのぞかない ☆ 止 光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED 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:	ペットなどが本機に噛みつかないように注意する 火災、やけど、けがなどの原因となります。
各種端子やスロットに導電性異物(金属片、鉛筆の芯など)を 接触させたり、ほこりが内部に入ったりしないようにする 火災、やけど、けが、感電または故障の原因となります。	スレセントに AC アダプタや電源ケーブルを 抜き差しするときは、金属類を接触させない 火災、やけど、感電または故障の原因となります。 マリングののでは、そのでは、そのでは、そのでは、そのでは、そのでは、そのでは、そのでは、
使用中に布団で覆ったり、包んだりしない 紫止 火災、やけどまたは故障の原因となります。	AC アダプタや電源ケーブルに 海外旅行用の変圧器等を使用しない 発火、発熱、感電または故障の原因となります。 ■



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。

この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起 こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

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。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 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。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは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、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、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本製品を保護するためには、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。踏みつけられたり躓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。
- 電源ケーブルや電源プラグを改造しないでください。
- 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おいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品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、本製品に触れる前に、身体から静電気を 逃がしてください。

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. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品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がしてください。
- 2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。
- 3. 静電気に敏感な機器の取り扱いは、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。

無線 LAN について

業界標準に基づく弊社の無線 LAN 製品は、ご家庭や職場または公共の施設において、使いやすく互換性の高い高速の無線接続を提供します。これ らを使用して時間や場所に関わらず必要なデータにアクセスすることができます。

WLAN は家庭やオフィス環境のみならず、空港やコーヒーショップ、または大学など公共の施設においても幅広く利用されるようになってきました。 この WLAN 技術を用いることにより、仕事やコミュニケーションがさらに効率的に行えるようになってきています。無線技術により可動性が増し、 配線や固定のインフラが減少したことでユーザに大きなメリットが生まれました。

ノート型やデスクトップ型 PC に使用する無線アダプタはイーサネットのアダプタカードと同じプロトコルをサポートしており、無線ユーザは有線 ネットワークと同じアプリケーションを利用できるようになりました。

WLAN 技術を利用するさまざまな理由

可動性

WLAN の動作範囲内のどこからでもデータにアクセス可能であり、生産性を向上します。また、リアルタイムな情報に基づく管理により作業効率が向上します。

低い実現コスト

WLAN は設置、管理、変更、移転のすべてが簡単です。このような WLAN の扱いやすさはネットワークの変更が頻繁に要求される環境に適しています。 WLAN は有線ネットワークでは困難であった場所へのネットワーク導入を可能にします

簡単な設置と拡張

煩わしい複雑なケーブル配線作業、特に壁や天井へのケーブル敷設の必要がないため、手早く簡単にシステムの設置を行うことができます。無線技 術は、ネットワークを家庭やオフィスを超えて拡張することで、さらなる多用途性を提供します。

低コストのソリューション

無線 LAN デバイスは、従来のイーサネット用機器とほぼ同等の価格設定となっています。本製品は設定可能な複数のモードで多機能性を提供し、 コスト削減を行います。

柔軟性

配置する無線LAN デバイスの数によって、ピアツーピアのネットワークが適している小さなユーザグループから大規模なインフラネットワークまで、 自由自在に構築することができます。

世界基準対応の技術

無線機器は、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n および IEEE 802.11ac に準拠しています。

• EEE 802.11ac 規格

IEEE 802.11ac 規格の無線通信速度は、最大 1300Mbps までと高速化されており、5GHz 帯の周波数と「OFDM」技術をサポートしています。

• EEE 802.11n 規格

IEEE 802.11n 規格は、従来の IEEE 802.11a、IEEE 802.11b および IEEE 802.11g の機能を拡張した規格です。無線通信速度は、最大 300Mbps までと高 速化され、2.4GHz 帯および 5GHz 帯の周波数を利用し、こちらも「OFDM」技術をサポートしています。

これらにより、多くの環境化において、無線サービスエリア内でネットワークによる大容量の送受信や遅延の少ない MPEG 形式の映像の視聴などが 可能になります。OFDM(Orthogonal Frequency Division Multiplexing) という技術により、この大容量のデジタルデータの高速伝送を無線で行うこ とができます。OFDM では、無線信号を小さいサブ信号に分割し、それらを同時に異なる周波数で送信します。OFDM により、信号伝送時のクロス トーク(干渉)の発生を抑えることが可能です。

IEEE 802.11n 規格は、「WPA」を含む現在最も先進的なネットワークセキュリティ機能を提供します。

WPA/WPA2 には企業向けの「Enterprise」とホームユーザ向けの「Personal」の2種類があります。「WPA-Personal」と「WPA2-Personal」はユーザ 認証に必要なサーバ機器を持たないホームユーザを対象としています。その認証方法は、無線ルータやアクセスポイントに「Pre-Shared Key(事前 共有鍵)」の定義を行うという点で WEP と似ています。クライアントとアクセスポイントの両方において、事前共有鍵が確認され条件が満たされた 時にアクセスが認められます。

「WPA-Enterprise」と「WPA2-Enterprise」は既にセキュリティ用にインフラが整備されている企業を対象としています。ネットワーク内のサーバを 中心にネットワーク管理とセキュリティの実施を行うような環境を想定しています。

ネットワーク管理者は、RADIUS サーバ上で 802.1X を使用し、無線 LAN へのアクセスを許可するユーザのリストを定義します。「WPA-Enterprise」 または「WPA2-Enterprise」を実装した無線 LAN にアクセスする場合、ユーザはユーザ名とパスワードの入力を要求されます。ユーザがネットワー ク管理者によってアクセスを許可されており、正しいユーザ名とパスワードを入力すると、ネットワークへのアクセスが可能になります。例えば、 ある社員が会社を辞めるというような場合、ネットワーク管理者がアクセス許可者のリストからその社員のデータを削除すれば、ネットワークを危 険にさらすことは避けることができます。

EAP (Extensible Authentication Protocol) は Windows OS に実装されています。802.1X の機能を使用する際には、ネットワークにおけるすべての デバイスの EAP タイプを同一にする必要があります。

重要

最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築 材料や工事、ネットワークオーバヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

無線に関するご注意

電波に関するご注意

本製品は、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。

本表的は、日本国内でのの反向でであり。

以下の注意をよくお読みになりご使用ください。

- 本製品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。
- ・ 電気製品、AV 機器、OA 機器などの磁気を帯びているところや電磁波が発生しているところで使用すると下記のような影響があります。
 - 時期や電気雑音の影響を受けると雑音が大きくなったり、通信ができなくなったりすることがあります。
 - テレビ、ラジオなどに近いと受信障害の原因となったり、テレビ画面が乱れたりすることがあります。
 - 近くに複数の無線 LAN アクセスポイントが存在し、同じチャネルを使用していると、正しく検索できない場合があります。
- 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。

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

本製品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。

- 本製品を使用する前に、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、本製品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、本製品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
想定干涉距離	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

5GHz 帯使用に関するご注意

無線 LAN の 5.2/5.3GHz(W52/W53)をご利用になる場合、電波法の定めにより屋外ではご利用になれません。

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。 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、および弊社 WEB に掲載された製品保証規程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。

製品保証規定は以下を参照ください。 https://www.dlink-jp.com/support/info/product-assurance-provision.html

- 本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。
- 弊社製品の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。
- 弊社は、予告なく本書の全体または一部を修正・改訂することがあります。
- 弊社は改良のため製品の仕様を予告なく変更することがあります。

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。 製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。 https://www.dlink-jp.com/support

警告 本書の内容の一部、または全部を無断で転載したり、複写することは固くお断りします。

E

「「「」「」「」「」「」「」「」「」「」「」「」「」「」」「」「」」「」「」」「」」「」」「」」「」」「」」	
安全にお使いいただくために	
ご使用上の注意	
静電気障害を防止するために	
電源の異常	
無線 LAN について	5
WLAN 技術を利用するさまざまな理由	5
無線に関するご注意	
けいめに	12
	12
本マニュアルの対象者	
表記規則について	
製品名 / 品番一覧	
第1章 本製品のご利用にあたって	14
制日梅田	14
我如似女 ギニ ↓	
が一 [
1 ED 主一	
LED 及小 悲声パラル	
月回ハイバレ	
第2章 製品の設置	<u> </u>
パッケージの中容	10
ハッケークの内容	10 10
イットソーソ 接続前の 午頭	
表記の設置	
10 インチョックへの取り付け	10
雪酒の投入	20
モネジススーー	20
第3章 基本設定について	21
Web GIII 画面へのログイン	21
Web Got 自由 KOT アイン	27
DHCP サーバの設定	23
日付 / 時刻の設定	23
インターネット接続設定	
ワイヤレスネットワーク接続(DSR-1000AC のみ)	28
ユーザアカウント作成	
セキュリティ / VPN ウィザード	
ダイナミック DNS ウィザード(DDNS)	
第 4 音 IAN 恐宁(Notwork)	24
第4章 LAN 設定(Network)	54
LAN(LAN 設定)	
LAN Settings(IPv4 ネットワーク用 LAN 設定)	
LAN DHCP Reserved IPs(LAN DHCP 予約 IP アドレスの設定)	
IP/MAC Binding(IP/MAC バインディング)	
IGMP Setup(IGMP 設定)	
UPnP Setup(UPnP 設定)	
VLAN(VLAN 設定)	
VLAN Settings(VLAN 設定)	
Port VLAN(ポート VLAN / ワイヤレス VLAN)	
第 5 章 ネットワーク設定(Network)	47
Internet(インターネット接続設定)	48
WAN1 Settings (WAN1 設定)	
WAN2 / DM7 Setting(WAN2 / DM7 設定)	59
WAN3 Setting(WAN3 / 3G インターネット設定(未サポート))	61
WAN Mode (WAN モード設定)	62
SIM Card Authentication (SIM カード認証 (未サポート))	
Routing Mode (ルーティングモード設定)	
IP Aliasing (IP エイリアス設定)	69
DMZ Settings(DMZ 設定)	
DMZ DHCP Reserved IPs(DMZ DHCP の予約 IP 設定)	
Dvnamic DNS (ダイナミック DNS 設定)	
Traffic Management (トラフィック管理)	73
	, , , , , , , , , , , , , , , , , , , ,

Ļμ

rБ

cŀ

n	
Jumbo Frames(ジャンホフレーム設定) Deution (リーニーマンド語中)	
Kouting (ルーテインク設定)	
Static Koutes (スタテイックルート)	
KIP (KIP 設定)	
OSPF(OSPF 設定)	
Protocol Binding (フロトコルハインテインク)	
IPv6 (IPv6 ネットリーク設定)	
IP Mode (IP モート設定)	
IPv6 Wan1 Settings(IPv6 ネットワークにおける WAN1 設定)	
IPV6 wanz Settings (IPV6 ネットワークにおける wanz 設定)	
Static Kouting (IPV6 スタテイックルーティンク設定)	
USPFV3(USPFV3 設定)	
6 to 4 Tunneling(6 to 4 トンネル設定)	
ISATAP TUNNEIS(ISATAP トンネル設定)	
Teredo Tunnei (Teredo トンネル改定)	
IPvo LAN Settings(IPvo LAN 設た)	95
IFVO Tullileis Status (IFVO ドノネルスナーダス)	
<u>第6章 無線設定(Wireless)(DSR-1000AC のみ)</u>	99
General(一般設定)	100
Access Points (アクセスポイント)	100
Access Forms (アクセスボリア)	103
Fiones (無線ドロックイル)	105
Radio Settings (無線形成の計幅改定)	107
Auvanced (周皮な政定)	107
WINI (WININ 改定)	108
Mbs (Wbs 設定)	109
WPS(WPS 設定)	
<u>第7章 VPN 設定(VPN)</u>	112
IPSec VPN(IPSec VPN の設定)	
Policies (IPSec VPN ポリシーの設定)	
Tunnel Mode $(\mathcal{V} \mathcal{V} \mathcal{V} \mathcal{V} \mathcal{V} \mathcal{V} \mathcal{V})$	
DHCP Range(IP アドレス範囲の設定)	
Certificate(認証証明書)	
Easy VPN Setup (VPN セットアップ)	
One To One Mapping (One To One マッピング)	
PPTP VPN(PPTP VPN 設定)	
PPTP Server (PPTP VPN サーバ設定)	
PPTP Client (PPTP クライアント)	
PPTP Active Users (PPTP アクティブユーザリスト)	125
L2TP VPN(L2TP VPN 設定)	
L2TP Server(L2TP VPN サーバ設定)	
L2TP Client(L2TP VPN クライアント)	
L2TP Active Users(L2TP アクティブユーザリスト)	
SSL VPN(SSL VPN 設定)	
SSL VPN 対応 OS/ ブラウザー覧	
SSL VPN Server Policy(SSL VPN ポリシー設定)	130
Portal Layouts(ポータルレイアウトの作成)	
Resources(ネットワークリソース)	
SSL VPN Client(SSL VPN クライアント設定)	
Client Routes(SSL VPN クライアントルート設定)	138
OpenVPN(OpenVPN 設定)	
OpenVPN 設定	139
OpenVPN Certificates(Open VPN 証明書)	141
OpenVPN Server Policy(Open VPN サーバポリシー)	145
Local Networks(ローカルネットワーク設定)	146
Remote Networks (リモートネットワーク設定)	147
OmniSSL Client Configuration(OmniSSL クライアント設定)	148
OmniSSL Portal Layouts(OmniSSL ポータルレイアウト)	149
GRE(GRE 設定)	150
	150

ch

<u>第8章 セキュリティ設定(Security)</u>	152
Authentication (認証設定)	
Internal User Database(内部ユーザデータベース)	
External Auth Server(外部認証)	
Radius Accounting(Radius アカウンティング設定)	
Login Profiles (ログインプロファイル)	
- Services Route Management(サービスルート管理)	
DUA External CP Web (DUA 外部キャプティブポータル Web サーバ)	
Web Content Filter(Web コンテンツフィルタリング)	
Static Filtering(スタティックフィルタリング)	
Dynamic Filtering(ダイナミックフィルタリング)	
URL Filtering ACL(URL フィルタリング ACL)	
Firewall(ファイアウォール設定)	
Firewall Rules(ファイアウォールルールの設定)	
Schedule(ファイアウォールスケジュール設定)	
Blocked Clients(クライアントブロック設定)	
Custom Services(カスタムサービスの設定)	
ALGs(ALG サポート)	
VPN Passthrough(VPN パススルー)	
Dynamic Port Forwarding(ダイナミックポートフォワーディング)	
Attack Checks(攻撃のチェック)	
Intel® AMT(インテル ® アクティブ・マネジメント・テクノロジー)	
IPS(侵入防止システム)	
App Control Policy(アプリケーションコントロールポリシー)	
Application Control(アプリケーションコントロール)	
<u>第9章</u> メンテナンス(Maintenance)	199
Administration(システム管理設定)	
System Setting(システム名の設定)	
Data and Time (システムの日時設定)	
Session Settings(セッションタイムアウトの設定)	
License Update(WCF ライセンスのアップデート)	
USB Share Ports(USB 共有ポートの設定)	
SMS Service (SMS サービス(未サポート))	
Package Manager(パッケージマネージャ)	
Set Language(言語設定)	
Web GUI Management(Web GUI 管理)	
Management(管理設定)	211
Remote Management(リモート管理)	
SNMP(SNMP の使用)	
Diagnostics (診断ツール)	
Power Saving(省エネ設定)	
DDP Client(DDP クライアント設定)	
Firmware & Config(ファームウェアとコンフィグ)	
Firmware Upgrade(ファームウェアアップグレード)	
Backup/Restore(コンフィグレーションのバックアップとリストア)	
Soft Reboot(再起動/工場出荷時設定の復元)	
Logs Settings(ログ設定)	231
Log Facilities(ログファシリティ)	231
Routing Logs(ルーティングログ)	
Sytem Log(System ログ)	
Remote Logging(リモートログ)	
SMS Logging(SMS ログ(未サポート))	

Lμ

rБ

<u>q</u>.[

cŀ

ĿЩ

<u>第 10 章 ステータス情報(Status)</u>	239
Dashboard (ダッシュボード画面)	
System Information(システム状態の参照)	
Device(デバイス状態の参照)	
All Logs(ログ)	
USB Status (USB ステータス)	
Network Information(ネットワーク情報の参照)	
DHCP クライアントの参照	
CaptivePortal Sessions(キャプティブポータルセッションの参照)	
Active Sessions(アクティブセッションの参照)	
Active VPNs(VPN セッションの参照)	
Interfaces Statistics(インタフェースの統計)	
Wireless Clients(無線クライアントの参照)	
Wireless Statistics (無線の統計情報)	
Device Statistics(デバイス統計情報)	
LAN Clients(LAN クライアント)	
Session Limiting Status(セッション制限ステータス)	
第 11 章 トラブルシューティング	258
インターネット接続	
日付と時間	
LAN の接続性をテストするために Ping する	
ご使用の PC からルータまでの LAN パスをテストする	
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	
工場出荷時設定へのリセット	
付録	262
【付録 A】用語解説	
【付録 B】工場出荷時設定	
【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	
【付録 D】ログメッセージ	

gJ

đ

гБ,

はじめに

本マニュアルでは、DSR-500/1000/1000ACの設置および操作方法について説明します。 各パラメータの説明については、本製品の Web GUI 上にあるオンラインヘルプ? もご参照ください。 「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 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 基本設定について」 - 製品を使用する上で必要な基本的設定について説明します。 「第4章 LAN 設定 (Network)」 - 本製品の LAN、WAN の設定方法について説明します。 「第5章 ネットワーク設定 (Network)」 - 本製品のインターネットへの接続、設定方法について説明します。 「第6章 無線設定(Wireless)(DSR-1000ACのみ)」 - 本製品の無線アクセスポイント設定、無線プロファイル、無線帯域設定、WMM、WDSなどについて説明します。 「第7章 VPN 設定 (VPN)」 - 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8章 セキュリティ設定 (Security)」 - 本製品のネットワークの安全を確保するための多くのセキュリティ機能について説明します。 「第9章 メンテナンス (Maintenance)」 - 本製品のメンテナンス作業について説明します。 「第 10 章 ステータス情報(Status)」

- 本製品とネットワークのステータス情報ついて説明します。

「第11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」

- 工場出荷時設定、ログメッセージなどを記載しています。

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。

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。

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。

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
Гј	Web GUI 上の UI 名を示します。	「OK」をクリックし、設定を適用します。
青字	参照先または URL を示します。	「Web GUI 画面へのログイン」をご参照ください。
Menu Name >	メニュー構造を示します。	Device > Port > Port Properties は、「Device」メニューの下
Menu Option		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。

^{1.} 製品名 / 品番一覧

製品名	品番
DSR-500	DSR-500/B1
DSR-1000	DSR-1000/B1
DSR-1000AC	DSR-1000AC

第1章 本製品のご利用にあたって

ここでは、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。

- 「製品概要」
- 「ポート」
- 「前面パネル」
- 「背面パネル」

製品概要

DSR-500/1000/1000AC は、SOHO などの小規模ビジネスにおいて、無線 LAN AP(1000AC のみ)と VPN をオールインワンで提供可能な 802.11ac 対応ワイヤレス VPN ルータです。高速ワイヤレス通信に対応する IEEE 802.11ac により、通常の有線ネットワーク通信と同等の通信環境を構築 することができます。最適なネットワークセキュリティは各種 VPN 機能、IPSecurity (IPSec)、Point-to-Point Tunneling Protocol (PPTP)、Layer2 Tunneling Protocol (L2TP)、そして Secure Sockets Layer (SSL)等の機能によって提供されています。さらに SSL VPN トンネル機能を利用して、時 間や場所を気にせずリモートアクセスすることが可能です。

多彩な管理機能

DSR-500/1000/1000AC は、ポリシーベースサービスマネージメント機能を提供するデュアル WAN ギガビットイーサネットを搭載しており、生産 性を最大に発揮します。フェイルオーバ機能はネットワーク通信を切断することなく、ネットワークトラフィックのデータを維持することができ、 WAN ロードバランシング機能は WAN インタフェースから送信されるトラフィックを調整し、システムパフォーマンスを最適化します。2 ポートあ るうちの 1 つの WAN ポートを DMZ のポートとして設定し、LAN からサーバを隔離することも可能です。

高速ワイヤレスネットワーク (DSR-1000AC)

DSR-1000AC は、IEEE802.11ac/a/b/g/n の無線標準規格に準拠しており、2.4GHz もしくは 5GHz の周波数帯域を使用することができ、既に構築済みのワイレスネットワークにも柔軟に対応することが可能です。最新の IEEE802.11ac に対応し、高速なワイヤレスネットワークを構築することができます。

優れた VPN 機能

Virtual Pivate Network (VPN)機能により、モバイル端末を使用しているユーザや支店からも安全にネットワークへ接続することができ、同時に15 (DSR-500)、25 (DSR-1000/1000AC)の SSL VPN トンネルをそれぞれに管理することができます。会社のデータベース等へ接続することができるリモートアクセス権限をモバイルユーザに割当てることで、瞬時に必要なデータを取得し、外出先で様々な対応を迅速にとることが可能となり、作業効率を上げていくことが可能です。

IPv6 対応

DSR-500/1000/1000ACは、IPv6/WAN ネットワークへの接続に対応するとともに、PPPoE(IPv6)や IPv6 スタティックルートなど様々な IPv6 機能を搭載し、IPv6 ネットワークへの移行に柔軟に対応できます。

D-Link Green 省電力機能

「D-Link Green 省電力機能」は、リンクダウン時とケーブル長に応じて、自動で消費電力を削減する仕組みです。これにより環境への配慮、製品寿命の延命化、発熱の抑制、運用時のコスト削減を実現します。

ポート

DSR シリーズは以下のポートを搭載しています。

ポート	DSR-500	DSR-1000	DSR-1000AC
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

前面パネル

前面パネルの各部名称と機能について説明します。

DSR-500





DSR-1000

D-Link DSR-1000		
UB81 ************************************		
ー USBポート & LED ー Power/Status LED	LAN ポート & LED	レーレー WAN ポート & LED
		コンソールポート

図 1-2 前面パネル (DSR-1000)

DSR-1000AC

D-Link DSR-1000AC		
Status 0 240 Status 0 240 USBポート & LED 2.4GHzモード LED Power/Status LED	1000100000000000000000000000000000000	1 WAN 2 ♪ WA CONSOL WAN ポート&LED コンソールポート

図 1-3 前面パネル (DSR-1000AC)

機能	説明
Power / Status LED	LED の点灯状態で本製品の状態を示します。
5GHz / 2.4GHz モード LED*	LED 表示については「」を参照してください。
USB ポート / LED	USB ポートには、USB2.0/USB1.1 対応フラッシュディスクやハードディスクを接続できます。
	注意 3G 機器は未サポートです。
LAN ポート	UTP ケーブルを使用し、スイッチやハブなどのイーサネットデバイスと接続します。
WAN ポート	UTP ケーブルを使用し、ケーブルモデムまたは DSL モデムに接続します。
	WAN2 ポートは、DMZ ポートとしても設定可能です。
コンソールポート	RJ45-to-DB9 コンソールケーブルを接続し、CLI (コマンドラインインタフェース) にアクセスします。

* DSR-1000AC のみ

LED 表示

本製品の LED 表示について説明します。





図 1-5 Power/Status、無線モード(5G/2.4G)LED



図 1-6 USB LED

LED	状態	色	状態説明
Power	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不具合が生じています。
	消灯	-	製品に電源が供給されていません。
Status	点灯	橙	製品の起動中です。
	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。
	消灯	-	製品が正常に動作しています。
5GHz*	点灯	緑	5GHz 無線 LAN による通信が可能な状態です。
(DSR-1000AC)	点滅	緑	5GHz 無線 LAN によりデータを送受信しています。
	消灯	-	5GHz 無線 LAN による通信が不可能な状態です。
2.4GHz*	点灯	緑	2.4GHz 無線 LAN による通信が可能な状態です。
(DSR-1000AC)	点滅	緑	2.4GHz 無線 LAN によりデータを送受信しています。
	消灯	-	2.4GHz 無線 LAN による通信が不可能な状態です。
リンクスピード	点灯	橙	1000Mbps でリンクが確立しています。
(WAN / LAN)	点灯	緑	100Mbps でリンクが確立しています。
	消灯	-	ポートは 10Mbps で動作中です。
TX/RX ステータス	点灯	(43	リンクが確立しています。
(WAN / LAN)	点滅	称下	データを送受信しています。
	消灯	-	リンクが確立していません。
USB	点灯	1	USB デバイスが接続しています。
	点滅	緑	USB デバイスとのデータ送受信を行っています。
	消灯]	USB デバイスが接続していません。

* DSR-1000AC のみ

背面パネル

背面パネルの各部名称と機能について説明します。

DSR-500/1000



DSR-1000AC



図 1-8 背面パネル図 (DSR-1000AC)

部位	機能
セキュリティスロット	市販のセキュリティロックの取り付けが可能です。
アース用端子	アース線を接続し、接地を行います。
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	電源の ON、OFF を行います。
アンテナ端子(DSR-1000AC)	DSR-1000AC に付属のアンテナを接続します。

第2章 製品の設置

- 「パッケージの内容」
- 「ネットワーク接続前の準備」
- 「製品の設置」
- 「電源の投入」
- 「ネットワークへの接続」

パッケージの内容

本製品を箱から取り出したら、以下の同梱物があることを確認してください。 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、ご購入いただいた代理店にお問い合わせください。

- 本体
- ・ AC 電源アダプタ
- ・ ネットワークケーブル
- RJ45/DB9 変換ケーブル
- ・ ラックマウントキット
- ・ ゴム足
- CD-ROM
- アンテナ×3 (DSR-1000ACのみ)
- ・ GNU GPL ライセンスノート
- ・PLシート

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。
- ・ 電源アダプタが 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、製品底面に同梱のゴム足を取り付けてください。ゴム製の足は製品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

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。
- 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 電源アダプタをご使用ください。

製品の設置

アンテナの取り付け (DSR-1000AC)



図 2-9 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 2-10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

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 2-11図 2-3 製品のラックへの設置

電源の投入

- 1. 電源アダプタを本製品の電源コネクタに接続します。電源アダプタのプラグを電源コンセントに接続します。
- 2. 本製品の電源スイッチを「ON」にします。本製品に電源が供給されると、Power LED が緑色に点灯します。

ネットワークへの接続

本製品の物理的なネットワークへの接続について説明します。

- 1. 外部ルータ、またはモデムと本製品の WAN ポートをイーサネットケーブルで接続します。WAN ポートは WAN のネットワークセグメントに属 することになります。
- 2. LAN セグメントに属するスイッチ、または PC と本製品の LAN ポートをイーサネットケーブルで接続します。
- 3. CLI での設定を行う場合は、付属のコンソールケーブルを使用し、コンソールポートを管理 PC を接続します。

第3章 基本設定について

Web GUI 画面へのログイン方法、IP アドレスの設定方法など、基本的な設定について説明します。

- ・「Web GUI 画面へのログイン」
- ・「LAN IP アドレスの設定」
- ・「DHCP サーバの設定」
- ・「日付/時刻の設定」
- ・「インターネット接続設定」
- ・「ワイヤレスネットワーク接続(DSR-1000ACのみ)」
- ・「ユーザアカウント作成」
- ・「セキュリティ / VPN ウィザード」
- ・「ダイナミック DNS ウィザード (DDNS)」

Web GUI 画面へのログイン

本製品の設定は、本製品と UTP ケーブルで接続した PC から行うことができます。Web ブラウザを使用して、本製品の Web GUI にアクセスしてく ださい。

対応している Web ブラウザ:Internet Explorer/Firefox/Chrome/Safari

- 1. UTP ケーブルを使用し、LAN ポートと設定用 PC を接続します。
- 2. 本製品と設定用 PC の IP アドレスが同じサブネット内にあることを確認します。(本製品の IP アドレスの初期値: 192.168.10.1)
- 3. Web ブラウザを起動します。
- 4. 本製品の IP アドレスをアドレスバーに入力し、Enter キーを押します。

፭ https://192.168.10.1/

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。

5. ログイン画面で「Username」と「Password」を入力します。

Please login to access D-Link Unified Services Router (DSR-1000AC) to manage and use the device. Login
Username Password Login
Supported Browsers: I.E 9+, Firefox 20+, Chrome 25+, Safari 5+

図 3-2 Login 画面

「Username」と「Password」の初期値は「admin」です。

Web GUI のログインパスワードを変更する場合は、Security > Authentication > Internal User Database > Users タブ画面で設定を行います。 詳細は「ユーザ情報の編集」を参照してください。

- 6. 「Login」をクリックします。
- 7. Status > Dashboard 画面がトップページとして表示されます。

LAN IP アドレスの設定

LAN IP アドレスの設定方法について説明します。

1. Network > LAN > LAN Settings をクリックし、以下の画面を表示します。

A Status	🛜 Wireless	💻 Network	A VPN	Security	Maintenance	
Network » LAN » LAN Settings						00
The LAN Configuration page all Server which runs on it and Cha the LAN IP address will require	ows you to configure th anges here affect all de all LAN hosts to be in	e LAN interface of t vices connected to t the same subnet and	he router including he router's LAN sw use the new addre	default behaviour fo itch and also wireles ss to access this GUI	or ping on LAN interfaces, s LAN clients. Note that a	the DHCP change to
LAN Settings						
LAN Ping						
Allow Ping from LAN						
IP Address Setup						
IP Address	1	92.168.10.1				
Subnet Mask	2	55.255.255.0				
DHCP Setup						
DHCP Mode	C	HCP Server	~			
Starting IP Address	1	92.168.10.100				
Ending IP Address	1	92.168.10.254				
Default Gateway	1	92.168.10.1				
Domain Name	C	Link				
Lease Time	2	4 [Range:	1 - 262800] Hours			
Configure DNS / WINS	C	OFF				

図 3-3 LAN Settings 画面 (IP Address Setup)

- 2. 「IP Address Setup」で、新しい IP アドレスを入力します。
- 3. 必要に応じて、サブネットマスクを変更します
- 4. 「Save」をクリックし、設定を適用します。

注意 IP アドレスを変更して「Save」をクリックすると、Web GUI が応答しなくなります。 変更後の IP アドレスを使用し、再度 Web GUI にログインしてください。

DHCP サーバの設定

DHCP サーバの設定方法について説明します。

1. Network > LAN > LAN Settings をクリックし、以下の画面を表示します。

🙆 Status	🛜 Wireless	Network	CA VPN	Security	🗢 Maintenance	
Network » LAN » LAN Settings						00
The LAN Configuration page allo Server which runs on it and Char the LAN IP address will require a	ws you to configure the L nges here affect all devic ill LAN hosts to be in the	AN interface of th es connected to th same subnet and	ne router including he router's LAN sw use the new addre	default behaviour tch and also wirele ss to access this Gl	for ping on LAN interfaces, ss LAN clients. Note that a II.	the DHCP change to
LAN Settings						
LAN Ping						
Allow Ping from LAN	ON					
IP Address Setup						
IP Address	192.	168.10.1				
Subnet Mask	255.	255.255.0				
DHCP Setup						
DHCP Mode	DHCF	Server	~			
Starting IP Address	192.	168.10.100				
Ending IP Address	192.	168.10.254				
Default Gateway	192.	168.10.1				
Domain Name	DLin	k				
Lease Time	24	[Range: 1	- 262800] Hours			
Configure DNS / WINS		OFF				

図 3-4 LAN Settings 画面(DHCP Setup)

- 2. 「DHCP Setup」セクションの「DHCP Mode」で、DHCP のモードを「None」「DHCP Server」「DHCP Relay」から選択します。
- 注意 「DHCP Relay」を選択すると、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。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。
- 3. 必要に応じて以下の項目を設定します。

項目	説明
Starting / Ending	DHCP アドレスプールの開始 IP アドレスと終了アドレスを入力します。
IP Address	LAN に参加する新規の DHCP クライアントには、「Starting IP Address」(開始 IP アドレス)と「Ending IP Address」(終了
	IP アドレス)で指定した範囲内の IP アドレスが割り当てられます。
	開始 IP アドレスと終了 IP アドレスは、ルータの LANIP アドレスと同じサブネット内である必要があります。
	・開始アドレスの初期値: 192.168.10.100
	・終了アドレスの初期値:192.168.10.254
Default Gateway	デフォルトゲートウェイを入力します。
	初期値はルータの LAN IP アドレス(192.168.10.1)です。
	ネットワークのゲートウェイがこのルータでない場合は、LAN サブネット内の任意の有効な IP に設定することができます。
	設定した IP アドレスはデフォルトゲートウェイとして DHCP サーバから DHCP クライアントに付与されます。
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。
Lease Time	IP アドレスがクライアントにリースされる期間を入力します。
	·設定可能範囲:1-262800(時)
	・初期値:24 (時)
Configure DNS/WINS	「ON」を選択した場合、DNS/WINS サーバの IP アドレスを入力します。

4. 「Save」をクリックし、設定を適用します。

日付/時刻の設定

日付/時刻の設定方法について説明します。

1. 「Wizard」をクリックします。



- 図 3-5
- **2.** 「Date and Time Wizard」内の「Run」をクリックします。

Nizards	
Internet Connection Wizard	Security Wizard
This wizard will guide you in connecting your new D-Link Unified	This wizard will guide you in configuring default Outbound Policy, VPN
Services Router to the Internet .	Passthrough and VPN Network Settings .
Run	Run
Date and Time Wizard	Users Wizard
This Wizard helps you in configuring Date and Time settings .	This Wizard guides you in creating a new user .
Run	Run
Dynamic DNS Wizard	Wireless Wizard
This Wizard helps in configuring Dynamic DNS WAN1 or WAN2 or WAN3	This wizard will guide you through common and easy steps to configure
settings.	your router's wireless interface .
Run	Run

図 3-6 Wizards 画面

- 3. 地図から設定する地域を選択 →「City」からタイムゾーンを選択します。
- サマータイムを有効にする場合は「Daylight Saving」を「ON」にします。 4.
- 「Next」をクリックします。 5.

Date and Time Wizard Current Time Zone is (GMT) Greenwic Lisbon Lor	th Mean Time : Dublin ndon	Edinburgh
Time Zone	Region City Daylight Saving	North America (GMT-08:00) Pacific Ti 🔻
Step: [1 of 2]		Previous Next



- 6. NTP サーバを使用する場合は「NTP Server」を「ON」にします。手動で時間と日付を指定する場合は「OFF」にします。
- 「ON」を選択した場合、「NTP Server Type」で「Default」または「Custom」を選択します。
 「Custom」を選択した場合、プライマリ / セカンダリ NTP サーバアドレスを入力します。
- 8. 「Time to Synchronize」で NTP サーバとの同期時間を指定します。

	Current NTP Server is ON	
Obtain Time from	Network	
NTP Server	ON	
NTP Server Type	Default	
Time to Synchronize	120	

- 9. 「Save」をクリックし、設定を適用します。
- 10. 確認画面が表示されます。確認後、「Finish」をクリックします。

インターネット接続設定

本製品は二つの WAN ポート保持しており、それらを使用してインターネット接続が利用できます。

ルータのインターネット接続には、現在使用しているインターネットサービスプロバイダ(ISP)からの情報が必要です。設定の際、必要な情報については ISP またはネットワーク管理者にご確認ください。

本製品がサポートしているインターネットの接続タイプは「DHCP」「Static IP Address」「PPPoE」「PPTP」「L2TP」「Japanese multiple PPPoE」「Russian dual PPPoE/PPTP/L2TP」です。本項目では「DHCP」または「Static IP Address」での接続方法を提示します。

- 1. ルータにログインします。
- 2. 手動でインターネットの設定を行う場合は「Wizard」をクリックします。



3. 「Internet Connection Wizard」内の「Run」をクリックします。

Wizards	
Internet Connection Wizard	Security Wizard
This wizard will guide you in connecting your new D-Link Unified	This wizard will guide you in configuring default Outbound Policy, VPN
Services Router to the Internet .	Passthrough and VPN Network Settings .
Run	Run
Date and Time Wizard	Users Wizard
This Wizard helps you in configuring Date and Time settings .	This Wizard guides you in creating a new user .
Run	Run
Dynamic DNS Wizard	Wireless Wizard
This Wizard helps in configuring Dynamic DNS WAN1 or WAN2 or WAN3	This wizard will guide you through common and easy steps to configure
settings.	your router's wireless interface .
Run	Run

図 3-10 Internet Connection Wizard ボックス 画面

4. 「DHCP」「Static IP Address」のいずれかを「ON」にし、「Next」をクリックします。

Internet Connection Wizard	8
Curr	rent Connection type DHCP
Internet Connection	
DHCP Choose this if your Internet connection automatically provides yo an IP Address. Most Cable Modems use this type of connection PPTP Choose this if your Internet connection requires PPTP username password to get online	ONL PPPoE OFF ou with Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection III OFF s and Static IP Address Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured
L2TP Choose this if your Internet connection requires L2TP username password to get online	and
Step : [1 of 2]	Previous Next

図 3-11 Internet Connection Wizard 画面

5. 「DHCP」を選択した場合、以下の画面で設定を行います。

nternet Connectio	n Wizard	X
	DHCP Connection Details	
DHCP Connection	Dynamic IP Address)	
MAC Address Source	Use Default Address 💌 Host Name	
DNS settings		
DNS Server Source	Get Dynamically from IS	

図 3-12 Internet Connection Wizard (DHCP) 画面

項目	説明
	DHCP Connection (Dynamic IP Address)
MAC Address Source	ご契約の ISP に認識される MAC アドレスを指定します。
	・「Use Default Address」:本ルータのデフォルト MAC アドレスを使用します。
	・「Clone your PC's MAC Address」:現在接続しているコンピュータの MAC アドレスを使用します。
	・「Use this MAC Address」:手動で MAC アドレスを設定します。
Host Name	ISP に提供する必要がある場合、ホスト名を入力します。
	DNS settings
DNS Server Source	DNS サーバを指定する方式を選択します。
	・「Get Dynamically from ISP」:ISP によって割り当てられた DNS サーバを使用します。
	・「Use These DNS Servers」:手動でプライマリ / セカンダリ DNS サーバの IP アドレスを設定します。

6. 「Static IP Address」を選択した場合、以下の画面で設定を行います。

nternet Connection Wi	zard		×
	Static IP Con	nection Details	
Static IP Address			
MAC Address Source	Use this MAC Address	IP Subnet Mask	
MAC Address			
IP Address			
Gateway IP Address			
DNS settings			
Primary DNS Server		Secondary DNS Server	

図 3-13 Internet Connection Wizard (Static IP Address) 画面

項目	説明
	Static IP Address
MAC Address Source	ご契約の ISP に認識される MAC アドレスを指定します。
	・「Use Default Address」:本ルータのデフォルト MAC アドレスを使用します。
	・「Clone your PC's MAC Address」:現在接続しているコンピュータの MAC アドレスを使用します。
	・「Use this MAC Address」:手動で MAC アドレスを設定します。
IP Address	ISP から割り振られた IP アドレスを指定します。
Gateway IP Address	ISP から割り振られたゲートウェイ IP アドレスを指定します。
IP Subnet Mask	ISP から割り振られたサブネットマスクを指定します。
	DNS settings
Primary DNS Server	ISP から割り振られたプライマリ DNS サーバの IP アドレスを指定します。
Secondary DNS Server	ISP から割り振られたセカンダリ DNS サーバ IP アドレスを指定します。

7. 「Save」をクリックし、設定を適用します。

インターネット接続のためルータが再起動します。接続まで数分お待ちください。

ワイヤレスネットワーク接続(DSR-1000ACのみ)

ワイヤレスネットワークのネットワーク名(SSID)とネットワークキー(事前共有鍵)の設定を行います。 SSID は、クライアントが AP を検出するための識別名です。本製品は、WPA / WPA2 セキュリティに TKIP+AES 暗号を使用します。クライアント側 のサポート状況によって、WPA または WPA2 を使用して AP に接続します。事前共有鍵の初期値は「passphrase」です。

1. 「Wizard」をクリックします。



図 3-14 Wizard 画面

2. 「Wireless Wizard」内の「Run」をクリックします。

Wizards	8
Internet Connection Wizard	Security Wizard
This wizard will guide you in connecting your new D-Link Unified	This wizard will guide you in configuring default Outbound Policy, VPN
Services Router to the Internet .	Passthrough and VPN Network Settings .
Run	Run
Date and Time Wizard	Users Wizard
This Wizard helps you in configuring Date and Time settings .	This Wizard guides you in creating a new user .
Run	Run
Dynamic DNS Wizard	Wireless Wizard
This Wizard helps in configuring Dynamic DNS WAN1 or WAN2 or WAN3	This wizard will guide you through common and easy steps to configure
settings.	your router's wireless interface .
Run	Run
Run	your routers wireless interiace . Run

図 3-15 Wireless Wizard ボックス 画面

3. 「Wireless Wizard」画面が表示されます。

Wireless Wizard			
	Wireless Wiza	ard Configuration	
Profile Name	default1 🔻	Network Key Type	Auto
Network Name (SSID)		Automatic: To prevent outsiders fro router will automatically assign a see	m accessing your network, the curity to your network .
		Manual: Use this options if you pref	er to create our own key .
Step : [1 of 1]			Previous Save



- **4.** 「Profile Name」でプロファイルを「default1」「default2」から指定します。
- 5. 「Network Name(SSID)」でワイヤレスネットワークの SSID を入力します。
- 6. 「Network Key Type」で「Manual」を指定します。
- 7. 「Wireless Security Password」にワイヤレスネットワークのパスワードを入力します。
- 8. 「Save」をクリックします。
- 9. 確認画面が表示されます。確認後、「Finish」をクリックします。

ユーザアカウント作成

ユーザアカウントの作成方法について説明します。ユーザアカウントはグループへの参加の際に必要となります。 参加するグループの作成方法については、「Groups (グループの設定)」を参照してください。

注意参加するグループを事前に作成する必要があります。詳しくは「グループ」をご参照ください。

- 1. ルータにログインします。
- 2. 「Wizard」をクリックします。



図 3-17 Wizard 画面

3. 「Users Wizard」内の「Run」をクリックします。

Wizards	8
Internet Connection Wizard	Security Wizard
This wizard will guide you in connecting your new D-Link Unified	This wizard will guide you in configuring default Outbound Policy, VPN
Services Router to the Internet .	Passthrough and VPN Network Settings .
Run	Run
Date and Time Wizard	Users Wizard
This Wizard helps you in configuring Date and Time settings .	This Wizard guides you in creating a new user .
Run	Run
Dynamic DNS Wizard	Wireless Wizard
This Wizard helps in configuring Dynamic DNS WAN1 or WAN2 or WAN3	This wizard will guide you through common and easy steps to configure
settings.	your router's wireless interface .
Run	Run

図 3-18 Users Wizard ボックス 画面

4. 「Users Wizard」画面が表示されます。

	Add a New User	
User Configuration		
New User Name	Group Type	ADMIN
New Password	Confirm Password	

- 5. 「New User Name」にユーザ名を入力します。
- 6. 「Group Type」で参加するグループを指定します。
- 7. 「New Password」でパスワードを入力 →「Confirm Password」で再度パスワードを入力します。
- 8. 「Save」をクリックし、設定を適用します。

セキュリティ / VPN ウィザード

VPN パススルーの有効化と VPN の作成について説明します。

1. 「Wizard」をクリックします。



図 3-20 Wizard 画面

2. 「Security Wizard」内の「Run」をクリックします。



図 3-21 Security Wizard ボックス 画面

3. 「Security Wizard」画面が表示されます。

ecurity Wizard)
Current Outbound Policy is Allow	
Default Outbound Policy for IPv4	
Always Allow 🔻	
VPN Passthrough	
IPSec ON	
Step : [1 of 3] Previous Next	

図 3-22 Security Wizard 画面(1/3)

- 4. 「Default Outbound Policy for IPv4」で「Allow」(許可)または「Block」(拒否)を選択します。
- 5. パススルーを許可する VPN の種類(「IPSec」「L2TP」「PPTP」)を「ON」にし、「Next」をクリックします。

6. 「IKE」「VPN」のポリシーを作成します。作成したポリシーは必要に応じて編集することが可能です。

Security Wizard			8
	Configure VPN Type and	d Remote & Local Addresses	
Select VPN Type for your VP	PN Network		
Select VPN Type	Site-to-Site 🔹	Connection Name	
IP Protocol Version	lpv4 ▼	Pre-Shared Key	
IKE Version	IKEv1	Local Gateway	Dedicated WAN
Remote & Local WAN Addres	sses		
Remote Gateway Type	IP Address 🔹	Remote WAN's IP Address / FQDN	
Local Gateway Type	IP Address 🔹	Local WAN's IP Address / FQDN	
Step : [2 of 3]			Previous Next
図 3-23 Security Wizard 画面	i (2/3)		

7.	以下の項目を設定後、	∣Next」 7	をクリックします。	

項目	説明		
	Select VPN Type for your VPN Network		
Select VPN Type	VPN の種類を「Site-to-Site」「Remote Access」から選択します。		
Connection Name	VPN 接続名を指定します。		
IP Protocol Version	IP プロトコルバージョンを「IPv4」または「IPv6」から選択します。「IPv6」は、IP モードを「IPv4&IPv6」に		
	設定した場合のみ表示されます。IP モードの設定については「IP Mode(IP モード設定)」を参照してください。		
Pre-Shared Key	Pre-Shared Key(事前共有鍵)を指定します。		
IKE Version	IKE のバージョンを選択します。		
Local Gateway	ローカルゲートウェイに使用する WAN ポートを指定します。		
	Remote & Local WAN Addresses		
Remote Gateway Type	リモートゲートウェイの種類を「IP Address」「FQDN」から選択します。		
Remote WAN's IP Address / FQDN	リモートゲートウェイで選択した「IP Address」または「FQDN」を入力します。		
Local Gateway Type	ローカルゲートウェイの種類を「IP Address」「FQDN」から選択します。		
Local WAN's IP Address / FQDN	ローカルゲートウェイで選択した「IP Address」または「FQDN」を入力します。		

第3章 基本設定について

8. 以下の画面で設定を行います。

Security Wizard		8
	Secure Connection Accessibility	
Configure Secure Connecti	n Accessibility	
Remote Network IP Address	Remote Network Subnet Mask	
Local Network IP Address	Local Network Subnet Mask	
Step:[3 of 3]		Previous Save

図 3-24 Security Wizard 画面 (3/3)

項目	説明		
Secure Connection Accessibility			
Remote Network IP Address	リモートネットワークの IP アドレスを入力します。		
Remote Network Subnet Mask	リモートネットワークのサブネットマスクを入力します。		
Local Network IP Address	ローカルネットワークの IP アドレスを入力します。		
Local Network Subnet Mask	ローカルネットワークのサブネットマスクを入力します。		

9. 「Save」をクリックし、設定を適用します。

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 の IP アドレス範囲と重複できません。

ダイナミック DNS ウィザード (DDNS)

ダイナミック DNS の設定方法について説明します。

ダイナミック DNS (DDNS) は、動的なパブリック 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接続することができるインター 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。ダイナミック DNS の詳細については、「Dynamic DNS (ダイナミック DNS 設定)」を参照してください。

1. 「Wizard」をクリックします。



図 3-25 Wizard 画面

2. 「Dynamic DNS Wizard」内の「Run」をクリックします。

Wizards	8
Internet Connection Wizard	Security Wizard
This wizard will guide you in connecting your new D-Link Unified	This wizard will guide you in configuring default Outbound Policy, VPN
Services Router to the Internet .	Passthrough and VPN Network Settings .
Run	Run
Date and Time Wizard	Users Wizard
This Wizard helps you in configuring Date and Time settings .	This Wizard guides you in creating a new user .
Run	Run
Dynamic DNS Wizard	Wireless Wizard
This Wizard helps in configuring Dynamic DNS WAN1 or WAN2 or WAN3	This wizard will guide you through common and easy steps to configure
settings.	your router's wireless interface .
Run	Run

図 3-26 Dynamic DNS Wizard ボックス画面

3. 「Dynamic DNS Wizard」画面が表示されます。

Dynamic DNS Wizard			×
	Currently WA	N1 is not configured	
Dynamic DNS			
Dynamic DNS	WAN1 T		
Dynamic DNS WAN1			
Dynamic DNS Service Type	DynDNS 🔻	Host Name	
User Name		Password	
Wildcard	OFF	Force Update Interval (1-30 Days)	
Step : [1 of 1]			Previous Save

図 3-27 Dynamic DNS Wizard 画面

- 4. 「Dynamic DNS」で、「WAN1」「WAN2」「WAN3」(DSR-1000AC のみ)を選択します。
- 5. 「Dynamic DNS Service Type」で DNS サーバタイプを指定します。
- 6. お使いの DDNS のサービスの内容に従い、「User Name」「Password」「Host Name」を入力します。
- 7. お使いの DDNS のサービスの内容に従い、「Wildcards」を「ON」にします。
- 8. 「Force Update Interval」で自動アップデートの間隔(1-30 日)を設定します。
- 9. 「Save」をクリックし、設定を適用します。

第4章 LAN 設定 (Network)

本製品の LAN および VLAN の設定方法について説明します。

設定項目	説明
「LAN(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。
「VLAN(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。

LAN (LAN 設定)

LAN Settings(IPv4 ネットワーク用 LAN 設定)

Network > LAN > LAN Settings 本製品の LAN 設定を行います。

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は、本製品の DHCP および TCP/IP 設定の初期値で動作可能です。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 モードを無効にします。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DNSプロキシを有効にすることができます。有効にした場合、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。無効にした場合、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。

	which runs on it ar	nd Changes here affe	ect all devices connec	ted to the route	r's LAN switch and a	lso wireless LAN clients.	Note t
change to th	ne LAN IP address w	ill require all LAN h	osts to be in the same	subnet and use	the new address to	access this GUI.	
LAN Settir	igs						
LAN Ping							
Allow Pi	ing from LAN	l	ON				
IP Addres	ss Setup	_					
IP Addr	ess		172.16.1.47				
Subnet	Mask		255.255.255.0				
DHCP Set	u p	-					
DHCP M	ode		None	•			
Domain	Name		DLink				
DNS Host	Name Mapping						
#	Host Name			IP Add	ress		
1							
2							
3							
4							
5							
6							
7							
8							
LAN Prox	У						
Activate	e DNS Proxy	l	ON				

1. Network > LAN > LAN 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 4-1 LAN Settings 画面

第4章 LAN設定(Network)

- 「LAN Ping」セクションで、「Allow Ping from LAN」の「ON」「OFF」を選択します。「ON」にした場合、LAN 内の Ping が許可されます。 2.
- 「IP Address Setup」セクションで、以下の項目を設定します。 3.
 - ・「IP Address」: IP アドレスを入力します。 初期値: 192.168.10.1
 - ・「Subnet Mask」:サブネットマスクを入力します。 初期値:255.255.255.0
- 4. 「DHCP Setup」セクションで、「DHCP Mode」を以下から選択します。
 - 「None」:
 - DHCP サーバ機能を無効にします。
 - 「DHCP Server」: ルータはネットワーク上で DHCP サーバとして動作します。「DHCP Server」を選択した場合の設定項目については、「DHCP Server (DHCP サー バ設定)」を参照してください。
 - 「DHCP Relay」: 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 アドレスリースを受け取ることができます。「DHCP Relay」を選択 した場合の設定項目については、「DHCP Relay (DHCP リレー設定)」を参照してください。
- 5. 「DNS Host Name Mapping」セクションで、「Host Name」「IP Address」にそれぞれマッピングするホスト名、IP アドレスを入力します。
- 6. 「LAN Proxy」セクションで、「Activate DNS Proxy」の「ON」/「OFF」を選択します。
 - ・「ON」: DNS プロキシを有効にします。
 - ・「OFF」: DNS プロキシを無効にします。

注意 IP アドレスを変更して「Save」をクリックすると、Web GUI が応答しなくなります。 変更後の IP アドレスを使用し、再度 WebGUI にログインしてください。

DHCP Server (DHCP サーバ設定)

1. 「DHCP Mode」で「DHCP Server」を選択します。

DHCP Mode	DUCD Course
Sher Mode	DHCP Server
Starting IP Address	192.168.10.100
Ending IP Address	192.168.10.254
Default Gateway	
Schudte Sutemay	192.100.10.1
Domain Name	DLink
Lease Time	24 [Range: 1 - 262800] Hours
Configure DNS / WINS	OFF

図 4-2 DHCP Server (DHCP Setup) 画面

2. 以下の項目を設定します。

項目	説明
Starting IP Address / Ending	DHCP アドレスプールの開始 IP アドレスと終了アドレスを入力します。
IP Address	LAN に参加する新規のDHCP クライアントには、「Starting IP Address」(開始 IP アドレス)と「Ending IP Address」(終
	了 IP アドレス)で指定した範囲内の IP アドレスが割り当てられます。
	開始 IP アドレスと終了 IP アドレスは、ルータの LANIP アドレスと同じサブネット内である必要があります。
Default Gateway	DHCP クライアントに割り当てるデフォルトゲートウェイの IP アドレスを入力します。通常、デフォルトゲート
	ウェイは本製品の LAN IP アドレス(初期値:192.168.10.1)となります。
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。
Lease Time	IP アドレスがクライアントにリースされる期間を入力します。
	・ 設定可能範囲:1-262800(時)
	 初期値:24(時)
Configure DNS/WINS	「ON」を選択した場合、DNS/WINS サーバの IP アドレスを入力します。「OFF」を選択した場合、本製品の LAN IP アド
	レスがクライアントに対しての DNS サーバの IP アドレスとしてアサインされ、本製品は ISP から DNS 情報を取得し
	ます。

^{3. 「}Save」をクリックし、設定を適用します。
DHCP Relay (DHCP リレー設定)

1. 「DHCP Mode」で「DHCP Relay」を選択します。

ner setup	
DHCP Mode	DHCP Relay
Domain Name	DLink
Gateway	

図 4-3 DHCP Relay (DHCP Setup) 画面

2. 以下の項目を設定します。

項目	説明
Domain Name	ネットワークのドメイン名を入力します。
Gateway	ゲートウェイのIPアドレスを入力します。

3. 「Save」をクリックし、設定を適用します。

LAN DHCP Reserved IPs(LAN DHCP 予約 IP アドレスの設定)

Network > LAN > LAN DHCP Reserved IPs $\checkmark = = =$

本機能では、クライアントのMACアドレス及び予約IPアドレスを追加することで、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 MAC アドレスとデータベース内の MAC アドレスリストが比較され ます。データベース内でそのコンピュータまたはデバイスに IP アドレスがすでに割り当てられている場合は、カスタマイズされた IP アドレスが設 定されます。それ以外の場合は、DHCP プールから自動的に IP アドレスがクライアントに割り当てられます。

1. Network > LAN > 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。

	🝘 Status	🛜 Wireless	🖳 Network	ഹം vpn	盈 Secur	ity 🔅 Maintena	ance
Network	» LAN » LAN DHCP I	Reserved IPs					00
This page receive t be assign	Add Status Wireless Metwork Cas VPN Security Maintenance Network » LAN N LAN DHCP Reserved IPs Image: Case VPN Image: Case VP						
LAN DH	CP Reserved IPs	List					
Show 1	o • entries [Right	click on record to get m	ore options]			(
Host N	ame	🔂 MAC Address	⇔	IP Address	⊖ II	∍/MAC Binding	θ
			No data a	vailable in table			
Showing	0 to 0 of 0 entries					H First A Previous	Next 🔰 Last 刘
Add N	ew DHCP Reserve	d IP					

図 4-4 LAN DHCP Reserved IPs 画面

2. 予約 IP アドレスを追加する場合は、「Add New DHCP Reserved IP」をクリックし以下の画面を表示します。

LAN DHCP Reserved IP Configur	ation	\bigotimes
Host Name		
IP Address		
MAC Address		
Associate with IP/MAC Binding	ON	
Log Dropped Packets	OFF	
		Save

図 4-5 LAN DHCP Reserved IP Configuration 画面

3. 以下の項目を設定します。

項目	説明
Host Name	デバイスのホスト名を入力します。スペースは使用できません。
IP Address	デバイスにわりあてる IP アドレスを入力します。この IP アドレスは、DHCP 設定の開始 IP アドレス/終了 IP アド
	レスの範囲内で設定する必要があります。
MAC Address	デバイスの MAC アドレスを入力します。大文字と小文字は区別されません。
Associate with IP/MAC Binding	「ON」にした場合、このデバイスの情報を IP/MAC バインディングに関連付けます。
Log Dropped Packets	「ON」にした場合、破棄パケットのログを取得します。

4. 「Save」をクリックし、設定を適用します。

追加した予約 IP アドレスは、LAN DHCP Reserved IPs 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

IP/MAC Binding(IP/MAC バインディング)

Network > LAN > IP/MAC Binding $\checkmark = \neg -$

IP/MAC バインディングリストの作成について説明します。

IP/MAC バインディングにより、ゲートウェイは送信トラフィックの IP アドレスを構成済み LAN ノード固有の MAC アドレスで検証します。 違反があった場合(トラフィックの送信元 IP アドレスが、同じ IP アドレスを持つ予想される MAC アドレスと一致しない場合)、パケットは破棄され、 診断のために記録される場合があります。

1. Network > LAN >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。

	🕜 Status		🖳 Network	Cas VPN			O Maintenance	
Network » L	AN » IP/MAC Bindin	g						00
The table lis addresses by violation (i.e and can be lo IP/MAC Bi	ts all the currently enforcing the gate: . the traffic's sourc ogged for diagnosis. nding List	defined IP/MAC Bind r way to validate the so e IP address doesn't n	ules and allows sever urce traffic's IP addre natch up with the exp	al operations on t ss with the uniqu ected MAC addres	he rules. e MAC Ada s having t	This feature dress of the he same IP	allows protection against configured LAN node. In th address) the packets will b	spoofed IP ne event of a ne dropped
Show 10	entries [Right cl	ick on record to get mo	re options J					٩
Host Nam	e 🗘	MAC Address	⊖ IP Ad	dress	⊖L	og Droppe	d Packets	€
			No data ava	ailable in table				
Showing 0 to	0 of 0 entries						First Previous Next	> Last >
Add New	IP/MAC Binding							

図 4-6 IP/MAC Binding 画面

2. 以下の項目が表示されます。

項目	説明
Host Name	ユーザが定義したルール名が表示されます。
MAC Address	MAC アドレスが表示されます。
IP Address	IP アドレスが表示されます。
Log Dropped Packets	ルールのログオプションが表示されます。

3. バインディングルールを追加する場合は、「Add New IP/MAC Binding」をクリックし以下の画面を表示します。

Host Name MAC Address IP Address Log Dropped Packets OFF	

図 4-7 IP/MAC Binding Configuration 画面

4. 以下の項目を設定します。

項目	説明
Host Name	デバイスのホスト名を入力します。スペースは使用できません。
MAC Address	デバイスの MAC アドレスを入力します。大文字と小文字は区別されません。
IP Address	デバイスにわりあてる IP アドレスを入力します。この IP アドレスは、DHCP 設定の開始 IP アドレス/終了 IP アド
	レスの範囲内で設定する必要があります。
Log Dropped Packets	「ON」にした場合、破棄パケットのログを取得します。

5. 「Save」をクリックし、設定を適用します。

追加したバインディングルールは、IP/MAC Binding 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

IGMP Setup(IGMP 設定)

Network > LAN > IGMP Setup

IGMP スヌーピングとは、IGMP パケットの中身を確認し、必要なホストにのみマルチキャストパケットを転送する機能です。 本機能は、ネットワーク上に大量のマルチキャストトラフィックが存在しているものの、すべての LAN ホストがこのトラフィックを受信する必要 がない場合に有用です。

1. Network > LAN > 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。

	🗥 Status	🛜 Wireless	📃 Network	CD VPN	Security	O° Maintenance	
Network » L	AN » IGMP Setup						00
The IGMP Pro configured. I nterfaces. IGMP Setu	xy page allows user t performs the host P	r to enable IGMP proxy. side of the IGMP protoc	The proxy contains ol on its upstream	many downstrean interface and the	n interfaces and a uni router side of the IG/	que upstream interface ex AP protocol on its downstr	cplicitly ream
IGMP Set	и р рху		OFF				
			Save	Cancel			
र्ष 4-8 ।	GMP Setup 画面						

2. 以下の項目を設定します。

項目	説明
IGMP Proxy	IGMP プロキシを「ON」または「OFF」に設定します。

3. 「Save」をクリックし、設定を適用します。

UPnP Setup (UPnP 設定)

Network > LAN > UPnP

UPnP の設定方法について説明します。

UPnP (Universal Plug and Play) は、ルータと通信可能な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 / 外部ポートを開放します。 UPnP を無効にした場合はデバイスの自動設定は行われません。アプリケーションを動作させるには、手動でポート開放を行います。

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

🐼 Status	🛜 Wireless	📃 Network	CA VPN	Security	O Maintenance	
vork » LAN » UPnP						0
P (Universal Plug and P ul for auto-configuring ned without user inter eby don't require corr	lay) is a feature that a application rules, whe vention. The UPnP Port esponding application	lows for automatic disc re internal/external po : Map Table has the de (port forwarding) rules	covery of devices th orts for the traffic tails of UPnP device to be configured.	at can communicate protocol required by s that respond to the	with this security applian a detected network device router's advertisements,	ce.UPn ce are , and
۱P						
PnP Setup						
Activate UPnP		ON THE				
LAN Segment		VLAN1	-			
Advertisement Period		1800 [Range:	1 - 86400] Seconds			
Advertisement Time T	o Live	4 IRange:	1 - 2551 Hops			
		Save	Cancel			
PnP Port Map List						
Show 10 💌 entries	[No right click option	ons]				Q
Active 🔂 IF	Address	⊖ Protocol	⊖ Internal Po	rt \varTheta	External Port	ę
		No data a	vailable in table			
Showing 0 to 0 of 0 entries				K) Fi	rst Previous Next >	Last
				N H	ISC 1 Previous Next >	Las

2. 以下の項目を設定します。

項目	説明
	UPnP Setup
Activate UPnP	UPnP を「ON」または「OFF」に設定します。
LAN Segment	UPnP を有効にする VLAN を選択します。
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を入力します。 大きい値を設定した場合ネットワークトラフィックが最小限になりますが、新規 UPnP デバイスのネットワークへの 識別は遅くなります。 - 設定可能範囲:1-86400(秒) - 初期値:1800(秒)
Advertisement Time to Live	パケットの TTL(生存時間)を設定します。 小さい値に設定した場合、UPnP ブロードキャスト範囲が制限されます。 スイッチの数が少ないネットワークでは、初期値の4に設定することが一般的です。 - 設定可能範囲:1-255(Hops) - 初期値:4(Hops)
	UPnP Port Map List
Active	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が表示されます。
IP Address	本製品が検出した UPnP デバイスの IP アドレスが表示されます。
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)が表示されます。
Internal Port	UPnP によってオープンされた内部ポートが表示されます。
External Port	UPnP によってオープンされた外部ポートが表示されます。

VLAN (VLAN 設定)

Network > VLAN

本製品は、VLAN を使用することで LAN 上に隔離した仮想ネットワークを構築できます。ネットワークデバイスに対し、VLAN 識別子で定義された サブネットワークと通信するように設定することができます。LAN ポートに固有の VLAN ID を割り当てることで、その物理ポートから送受信される トラフィックを通常の LAN から隔離することができます。

VLANフィルタリングは、大規模なネットワークにおけるデバイスのブロードキャストパケットを制限します。ルータのVLANは初期値では有効になっています。VLAN Settings 画面では、VLAN を有効にし、仮想ネットワークの設定を行います。

VLAN Settings(VLAN 設定)

Network > VLAN > VLAN Settings

VLAN の設定方法について説明します。

「VLAN List」には、設定済みの VLAN のリストが表示されます。リストの下にある「Add New VLAN」をクリックし、VLAN メンバシップを作成します。 VLAN メンバーシップエントリは、VLAN ID と、その VLAN メンバシップに割り当てられている数値の VLAN ID で構成されています。

VLAN ID の値は、2 ~ 4093 の任意の数字で設定できます。VLAN ID 1 は、デフォルト VLAN 用に予約されています。VLAN ID 1 は、インタフェースで 受信したタグなしフレームに使用されます。

1. Network > VLAN > VLAN 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。

		Status	🛜 Wireless	📮 Net	work 🖌	🔉 VPN 🛛 🔒 Secu	rity 🔅 Maintenance	
letwork »	VLAN »	 VLAN Settin 	ıgs					3 0
'he router Jefined by	support VLAN id	ts virtual net entifiers.	work isolation on t	he LAN with th	ne use of VLANs.	LAN devices can be conf	gured to communicate in a subnetw	rork
/LAN Co	nfigura	tion						
Vlan E	nable			ON				
				Save	Cance			
VLAN L	ist							
Show 1	0 🔻	entries [Righ	t click on record to ge	et more options]				
Name								
	U VI	LAN ID 🗧	IP Address	⊖ Subnet	Mask \varTheta	Captive Portal ↔	Authentication Server	÷
Default	ک ۷۱ 1	LANID 🤅	IP Address 172.16.1.53	⊖ Subnet 255.255.255	Mask ⊖ 5.0	Captive Portal → Free	Authentication Server None	÷
Default Showing	1 1;1to1of	LAN ID 🗧	HP Address	⊖ Subnet 255.255.25	Mask ↔	Captive Portal → Free	Authentication Server None	⊖ t)
Default Showing Add I	1 1 to 1 of New VLA	LAN ID 🗧 1 entries AN	 IP Address 172.16.1.53 	⊖ Subnet 255.255.25	Mask 🔤	Captive Portal ∂ Free	Authentication Server None	⊖ t)
Default Showing Add I	1 1 to 1 of New VLA	1 entries	IP Address 172.16.1.53	⊖ Subnet 255.255.25	Mask Ə	Captive Portal ∂ Free	Authentication Server None	⊖ t)

図 4-10 VLAN Settings 画面

- 2. 「VLAN Enable」を「ON」にし、VLAN を有効にします。
- **3.** 「Save」をクリックし、設定を適用します。

4. VLAN を追加する場合は、「Add New VLAN」をクリックし、以下の画面を表示します。

VLAN Configuration		×
VLAN ID	[Range: 2 - 4093]	^
Name		
Captive Portal Captive Portal	OFF	
Activate InterVLAN Routing	OFF	
Multi VLAN Subnet IP Address		
Subnet Mask		
DHCP		
DHCP Mode	● None ○ DHCP Server ○ DHCP Relay	
LAN Proxy		
Enable DNS Proxy	ON THE	
VLAN IPv6		
Enable VLAN IPv6	ON [11]	
LAN TCP/IP Setup		
IPv6 Address		
IPv6 Prefix Length	[Range: 0 - 128]	
DHCPv6		
Status	OFF	~
		Save

図 4-11 VLAN Configration 画面

5. 以下の項目を設定します。

項目	説明
VLAN ID	VLAN ID(2-4093)を指定します。
Name	VLAN 名を指定します。
	Captive Portal
Captive Portal	VLAN ごとにキャプティブポータルを「Enable」(有効)または「Disable」(無効)にします。
	有効にすると、「Captive Portal」セクション内で各項目を設定することができます。
Active InterVLAN Routing	複数の VLAN 間のルーティングを「ON」または「OFF」に設定します。
	Multi VLAN Subnet
IP Address	VLAN の IP アドレスを指定します。
Subnet Mask	VLAN のサブネットマスクを指定します。
	DHCP
DHCP Mode	以下から DHCP モードを指定します。
	・「None」:DHCP サーバ機能を VLAN に対して無効にします。
	・「DHCP Server」:ルータは DHCP サーバとして動作します。
	・「DHCP Relay」:有効にすると VLAN 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 アドレスのリースを受けることができます。
	LAN Proxy
Enable DNS Proxy	「ON」にするとルータがすべての DNS 要求に対するプロキシとして動作し、ISP の DNS サーバと通信します。
	VLAN IPv6
Enable VLAN IPv6	「ON」にした場合、VLAN の IPv6 アドレスが有効になります。
	LAN TCP/IP Setup
IPv6 Address	VLAN の IPv6 アドレスを入力します。
IPv6 Preficx Length	IPv6 プレフィックス長を入力します。
	- 設定可能範囲:0-128

項目	説明			
	DHCPv6			
Status	DHCPv6 のステータスを「ON」または「OFF」に設定します。有効にした場合、以降に表示される項目を設定してください。			
Mode	モードを「Stateless」または「Statefull」から選択します。			
Domain Name				
Server Preference	サーバの設定値を 10 進数で入力します。 設定値は、ステートレス DHCP で DHCP サーバの優先レベルを示すために使用されます。DHCPv6 クライアントは最 も高い設定値を持つ DHCPv6 サーバを選択します。 - 設定可能範囲:0-255 - 初期値:255			
DNS Servers	DNS サーバを以下から選択します。 - 「Use DNS Proxy」: DNS プロキシを使用します。 - 「Use Below」:以下で設定した「Primary DNS Server」「Secondary DNS Server」を使用します。 - 「Use DNS from ISP」: ISP が提供する DNS サーバを使用します。			
Primary DNS Server	「Use Below」を選択した場合、プライマリ DNS サーバを入力します。			
Secondary DNS Server	「Use Below」を選択した場合、セカンダリ DNS サーバを入力します。			
Lease / Rebind Time	 アドレスがクライアントにリースされる時間を設定します。 - 設定可能範囲:0-604800(秒) - 初期値:86400(秒) 			
Prefix Delegation	プレフィックス委任を「ON」または「OFF」に設定します。			

6. 「Save」をクリックし、設定を適用します。

Captive Portal(キャプティブポータル)

キャプティブポータルは、各 VLAN ごとに有効にできます。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します。 VLAN ごとに、固有の指示やブランド名を持つカスタマイズされたポータルにすることも可能です。本設定における最も重要な点は、認証サーバを 選択することです。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行う全てのユーザ (VLAN ホスト)が、指定のサーバ経由で認証されます。

- 1. Network > VLAN > VLAN Settings の順にメニューをクリックします。
- 2. 「Add New VLAN」をクリック、または既存の VLAN を右クリックして「Edit」を選択します。
- 3. 「VLAN Configuration」画面で「Captive Portal」セクションの設定を行います。

「Captive Portal Type」に「Internal CP Web」を選択した場合、以下の項目を設定します。

Captive Portal	
Captive Portal	ON THE
Captive Portal Type	Internal CP Web
Login Profile Name	default Create a Profile
Authentication Server	Local User Database
Redirect Type	
Activate InterVLAN	OFF
Routing	

図 4-12 Captive Portal 画面 -Internal CP Web

項目	説明
Captive Portal	キャプティブポータルを「ON」または「OFF」に設定します。
Captive Portal Type	キャプティブポータルのタイプを「Internal CP Web」に設定します。
Login Profile Name	ログインプロファイル名を指定します。 ドロップダウンメニューから選択、または「Create a Profile」をクリックし新しいプロファイルを指定します。
Authentication Server	この VLAN で利用できる認証サーバを表示します。 こ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、選択したサーバによって認証されます。
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。
Activate InterVLAN Routing	VLAN 間の通信を有効にする場合、「ON」にします。

「Captive Portal Type」に「DUA External CP Web」を選択した場合、以下の項目を設定します。

Captive Portal	
Captive Portal	ON III
Captive Portal Type	DUA External CP Web Enable DUA External Web Server
Enable Redirect	ON III
Original URL	ON
Activate InterVLAN	ON THE
Routing	

図 4-13 Captive Portal 画面 -DUA External CP Web

項目	説明
Captive Portal	キャプティブポータルを「ON」または「OFF」に設定します。
Captive Portal Type	キャプティブポータルのタイプを「DUA External CP Web」に設定します。
	「Enable DUA External Web Server」をクリックして DUA 外部 Web サーバを有効にできます。
Enable Redirect	リダイレクトを「ON」または「OFF」に設定します。
Original URL	「ON」にした場合、ユーザが入力したオリジナル URL へのリダイレクトが有効になります。
Activate InterVLAN Routing	VLAN 間の通信を有効にする場合、「ON」にします。

4. 「Save」をクリックし、設定を適用します。

Port VLAN(ポート VLAN / ワイヤレス VLAN)

Network > VLAN Settings > Port VLAN

VLAN ID が割り当てられた特定の LAN ポートを通過するすべてのトラフィックにタグ付けをするために、物理ポートと無線セグメントに対して VLAN を紐付けることができます。

本画面では、LAN 及び無線 LAN の VLAN メンバシッププロパティ情報の一覧を表示します。

- 「Port VLANs List」:「Port Name」「Mode」「PVID」「VLAN membership」の項目が表示されます。
- 「Wireless VLANs List」:4 つの物理ポートに関連付けられたアクセスポイントが表示されます。

物理ポートまたは構成済みのアクセスポイントを右クリックして「Edit」を選択し、設定画面を開くことができます。

1. Network > 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。

🙆 Status 🛜	Wireless	📃 Network 🛛 🤇	S VPN 🔒 S	Security 🔷 M	
Network » VLAN » Port VLAN					
This page allows user to configure the p specific LAN port with a VLAN ID, you o for that port and VLAN membership inf port	ort VLANs. A user an associate a VLA ormation. Go to th	can choose ports and AN to a physical port. Ne Available VLAN page	can add them into a The VLAN Port table e to configure a VLAN	VLAN. In order to tag displays the port ide I membership that cai	all traffic through a ntifier, the mode setting n then be associated with a
Port VLANs List					
					٩
Port Name 🔗	Mode	⊖ PVID	e VLAN Mer	nbership	:: 0
Port1	Access	1	1		1
Port2	Access	1	1		
Port3	Access	1	1		
Port4	Access	1	1		
Showing 1 to 4 of 4 entries					
Wireless VLAN List					
					٩
SSID 🕜 Mode	e pvid e	VLAN Membership	θ	Radio Type Descript	tion Θ
DSR-1000AC_2 Access	1	1		2.4 Ghz	
dsr1000ac Access	1	1		5 Ghz	
Showing 1 to 2 of 2 entries					

図 4-14 Port VLAN 画面

2. ポートを右クリック→「Edit」を選択し、設定画面を表示します。

選択したモードによって表示される画面が異なります。

Port VLAN Configuration	
Port Name Mode PVID	Port1 Access
図 4-15 Port VLAN - Edit「Access」画	面
Port VLAN Configuration	•
Port Name Mode PVID VLAN Membership Configuration VLAN Membership	Port1 General Default: 1, Range: 1 - 4093]
図 4-16 Port VLAN - Edit「General」 運	iā
Port VLAN Configuration	
Port Name Mode VLAN Membership Configuration VLAN Membership	Port1 Trunk T

図 4-17 Port VLAN - Edit「Trunk」 画面

3. 以下の項目を設定します。

項目	説明
Mode	VLAN のモードを以下から選択します。
	• 「General」
	ポートは任意の 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。受信データがアンタグの場合、定義済みの PVID が割り当てられます。
	<例>
	ポート 3 が PVID 3 を持つ「General」ポートである場合、ポート 3 で受信するデータには PVID 3 が割り当てられます。こ
	れと同じ 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はタグが取り外されます。これは通常、2つのイー
	サネットボートを持つ 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ボートに送信されるデータはタグ付け
	されます。接続するテバイスから電話を通過するテータはタクが取り外されます。
	ホートは単一の VLAN のメンハです。ホートで送受信する全てのテーダはダクなしとなります。 アクセスモートのホート
	を栓出するトラノイツクは、通常のイーサイツトノレームのように扱われます。 「Truck」
	・「IFUNK」 + _ トリバキの \/ \N わいわい トのマンバにたることができます。+ _ トで洋平信する公子のゴークがクガけけてわます。+
	小一下は仕息の VLAN セットのメンハになることができます。ホートで达文信する主てのナーダがダク的りされます。ホート 不必信する方をし ギーカけ ピート DVID-1 たけつマンクグのギフェルト VIAN た吟き転送されたけ トランクピー
	トビッピリタダクなしノーダは、ホート PVID=1 を持フアフダクのアフォルト VLAN を除き転送されません。トラフクホートは、同じ物理リンクトの複数 VLAN に対するトラフィックを多重化します
PVID	「General」モードを選択した場合、ホートの PVID を人力します。
VLAN Membership	VLAN メンバシップを選択します。

第5章 ネットワーク設定(Network)

本製品のネットワーク設定について説明します。

設定項目	説明
「Internet(インターネット接続設定)」	2 つの WAN ポートを使用したインターネット接続の設定を行います。
「Jumbo Frames(ジャンボフレーム設定)」	ジャンボフレーム設定を行います。
「Routing(ルーティング設定)」	スタティック / ダイナミックルーティングの設定を行います。
「IPv6(IPv6 ネットワーク設定)」	IPv6 の関連する LAN 設定を行います。

Internet (インターネット接続設定)

Network > Internet

```
本ルータにある2つのWANポートを使用し、インターネット接続を行うことができます。
設定には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必要です。通常これらの情報は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。
```

WAN1 Settings (WAN1 設定)

Network > Internet > WAN1 Settings

「WAN1」インタフェースの設定を行います。以下の画面の「Connection Type」で選択した項目によって、表示される画面が異なります。

2	Status	🛜 Wireless	📮 Network	ക vpn
Network » Internet	(IPv4) » WAN1	Settings		
This page allows you Account Information IPv4 WAN1 Setti	u to set up you n etc. This info ings	ir Internet conne Irmation is usually	ction. Ensure that you provided by your ISP (have the Internet or network adminis
WAN1 Setup				
Connection Ty	pe		Dynamic IP (DHCP)	•
Enable VLAN Ta	ag	l	ON III	
VLAN ID			0	

図 5-1 WAN1 Setup 画面

以下の項目を設定しま	す	0
------------	---	---

項目	説明
Connection Type	接続タイプを以下から選択します。
	・「Dynamic IP (DHCP)」:ご利用の ISP から自動的に IP アドレス、接続情報を取得します。
	・「Static IP」:手動で IP アドレスを含む接続設定を行います。
	・「PPPoE (Username/Password)」:ISP から提供される PPPoE 情報を元に接続設定を行います。
	・「PPTP (Username/Password)」:ISP から提供される PPTP 情報を元に接続設定を行います。
	・「L2TP (Username/Password)」:ISP から提供される L2TP 情報を元に接続設定を行います。
	・「Japanese multiple PPPoE」:ISP から提供される PPPoE 情報(日本向け)を元に接続設定を行います。
	・「Russian dual access PPPoE」:ISP から提供される PPPoE 情報(ロシア向け)を元に接続設定を行います。
	・「Russian dual access PPTP」:ISP から提供される PPTP 情報(ロシア向け)を元に接続設定を行います。
	・「Russian dual access L2TP」:ISP から提供される L2TP 情報(ロシア向け)を元に接続設定を行います。
Enable VLAN Tag	VLAN タグを「ON」または「OFF」にします。
VLAN ID	VLAN タグを「ON」にした場合、VLAN ID を入力します。

Dynamic IP (DHCP)(自動 IP アドレス設定)

「Connection Type」で「Dynamic IP (DHCP)」を選択した場合の設定です。

Dynamic IP (DHCP) Host Name	
DNS Servers (Domain Name System) DNS Server Source	● Get Dynamically from ISP – ● Use These DNS Servers
MAC Address MAC Address Source	● Use Default MAC
<i>Port Setup</i> MTU Size	● Default 🔍 Custom
Port Speed	Auto Sense
	Save Cancel

図 5-2 Dynamic IP (DHCP) 画面

以下の設定項目があります。

項目	説明	
Dynamic IP (DHCP)		
Host Name	ホスト名を指定します。	
	DNS Server (Domain Name System)	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。	
	・「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します。	
	・「Use These DNS Servers」:ご契約の ISP の指定したアドレスを使用します。	
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)	
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)	
	MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。	
	・「Use Default MAC」:WAN1 ポートの MAC アドレスを使用します。	
	・「Clone your PC's MAC」:現在接続しているコンピュータの MAC アドレスを使用します。	
	・「Use this MAC」:手動で MAC アドレスを指定します。	
MAC Address	ISP と紐付ける MAC アドレスを入力します。(「Use this MAC」 選択時)	
	Port Setup	
MTU Size	MTU Size MTU 値を「Default」(初期値:1500)または「Custom」に設定します。	
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。(「Custom」選択時)	
Port Speed	ポート速度を選択します。	
	・ 初期値:「Auto Sense」	

Static IP(スタティック IP アドレス設定)

「Connection Type」で「Static IP」を選択した場合の設定です。

Static IP	
IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Domain Name System (DNS) Servers	
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
MAC Address	
MAC Address Source	
MAC Address	00:00:00:00:00:00
Port Setup	
MTU Size	Default Custom
Custom MTU	1500 [Range: 1200 - 1500] Bytes
Port Speed	Auto Sense V
	Save Cancel

図 5-3 Static IP 画面

以下の設定項目があります。

説明		
Static IP		
ISP により提供された IP アドレスを入力します。		
ISP により提供されたサブネットマスクを入力します。		
ISP により提供されたゲートウェイ IP アドレスを入力します。		
Domain Name System(DNS) Servers		
プライマリ DNS サーバの IP アドレスを入力します。		
セカンダリ DNS サーバの IP アドレスを入力します。		
MAC Address		
ISP 側での識別に使用される MAC アドレスを設定します。		
・「Use Default MAC 」:WAN1 ポートの MAC アドレスを使用します。		
・「Clone your PC's MAC 」:現在接続しているコンピュータの MAC アドレスを使用します。		
・「Use this MAC」:手動で MAC アドレスを指定します。		
ISP と紐付ける MAC アドレスを入力します。(「Use this MAC」 選択時)		
Port Setup		
MTU 値を「Default」(初期値:1500)または「Custom」に設定します。		
MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。(「Custom」選択時)		
ポート速度を選択します。		
・ 初期値:「Auto Sense」		

PPPoE (Username/Password) (PPPoE 設定)

「Connection Type」で「PPPoE (Username/Password)」を選択した場合の設定です。

PPPoE Profile Configuration	
Address Mode	💿 Dynamic IP 🔍 Static IP
User Name	dlink
Password	••••
Service	Optional
Authentication Type	Auto-negotiate •
Reconnect Mode	🖲 Always On 🛛 🔍 On Demand
Domain Name System (DNS) Servers DNS Server Source	Get Dynamically from ISP O Use These DNS Servers
MAC Address MAC Address Source	◉ Use Default MAC ◎ Clone your PC's MAC ◎ Use this MAC
Port Setup MTU Size	🖲 Default 🔍 Custom
Port Speed	Auto Sense T
	Save Cancel

図 5-4 PPPoE (Username/Password) 画面

以	下の	設定項	目が	あり	ま	す	
---	----	-----	----	----	---	---	--

項目	説明
	PPPoE Profile Configuration
Address Mode	「Dynamic IP」または「Static IP」を選択します。
IP Address	ISP により提供された IP アドレスを入力します。(「Static IP」選択時)
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。(「Static IP」選択時)
User Name	PPPoE のユーザ名を入力します。
Password	PPPoE のパスワードを入力します。
Service	ISP により指示があった場合にサービス名を入力します。
Authentication Type	プロファイルが使用する認証タイプを指定します。
Reconnect Mode	インターネットの再接続モードを以下から選択します。
	・「Always On」:常にインターネットに接続している状態となります。
	・「On Demand」:インターネット接続を開始した場合のみ、ルータがインターネットに接続します。一定の時間アイド
	ル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。(「On Demand」選択時)
	Domain Name System (DNS) Servers
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。
	・「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します。
	・「Use These DNS Servers」:ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時)
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時)
	MAC Address
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。
	・「Use Default MAC」:WAN1 ポートの MAC アドレスを使用します。
	・「Clone your PC's MAC」:現在接続しているコンピュータの MAC アドレスを使用します。
	・「Use this MAC」:手動で MAC アドレスを指定します。
MAC Address	ISP と紐付ける MAC アドレスを入力します。(「Use this MAC」選択時)
	Port Setup
MTU Size	MTU 値を「Default」(初期値:1500)または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。(「Custom」選択時)
Port Speed	ポート速度を選択します。
	・ 初期値:「Auto Sense」

PPTP (Username/Password) (PPTP 設定)

「Connection Type」で「PPTP (Username/Password)」を選択した場合の設定です。

PPTP	
Address Mode	Oynamic IP Static IP
Server Address	0.0.0.0
User Name	dlink
Password	
Mppe Encryption	OFF
Split Tunnel	OFF
Reconnect Mode	Always On O Demand
Domain Name System (DNS) Serve	rs
DNS Server Source	Get Dynamically from ISP O Use These DNS Servers
MAC Address	
MAC Address Source	🖲 Use Default MAC 🔷 Clone your PC's MAC 🔗 Use this MAC
Port Setup	
MTU Size	Default O Custom
Port Speed	Auto Sense 🔻
	Save Cancel

図 5-5 PPTP (Username/Password) 画面

以下の設定項目があります。

項目	説明	
PPTP		
Address Mode	「Dynamic IP」または「Static IP」を選択します。	
IP Address	ISP により提供された IP アドレスを入力します。(「Static IP」 選択時)	
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。(「Static IP」選択時)	
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。(「Static IP」選択時)	
Server Address	PPTP サーバのアドレスを入力します。	
User Name	PPTP のユーザ名を入力します。	
Password	PPTP の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「ON」にします。	
Split Tunnel	スプリットトンネルを「ON」または「OFF」にします。	
	「ON」にすると、同じ物理接続を使用して VPN とインターネット両方の接続が可能になります。	
Reconnect Mode	インターネットの再接続モードを以下から選択します。	
	・「Always On」:常にインターネットに接続している状態となります。	
	・「On Demand」:インターネット接続を開始した場合のみ、ルータがインターネットに接続します。一定の時間アイド	
	ル状態が続くと、接続は自動的に終了します。	
Maximum Idle Time	アイドル時間の最大値を入力します。(「On Demand」選択時)	
	Domain Name System (DNS) Servers	
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。	
	・「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します。	
	・「Use These DNS Servers」:ご契約の ISP の指定したアドレスを使用します。	
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時)	
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時)	
	MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。	
	・「Use Default MAC」:WAN1 ポートの MAC アドレスを使用します。	
	・「Clone your PC's MAC」:現在接続しているコンピュータの MAC アドレスを使用します。	
	・「Use this MAC」:手動で MAC アドレスを指定します。	
MAC Address	ISP と紐付ける MAC アドレスを入力します。(「Use this MAC」選択時)	
	Port Setup	
MTU Size	MTU 値を「Default」(初期値:1500)または「Custom」に設定します。	
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。(「Custom」選択時)	
Port Speed	ポート速度を選択します。	
	・ 初期値:「Auto Sense」	

L2TP (Username/Password)(L2TP 設定)

「Connection Type」で「L2TP (Username/Password)」を選択した場合の設定です。

💿 Dynamic IP 🛛 🔍 Static IP
0.0.0.0
dlink
••••
Optional
OFF
💿 Always On 🛛 🔍 On Demand
● Get Dynamically from ISP 🛛 ● Use These DNS Servers
🖲 Use Default MAC 🛛 🔍 Clone your PC's MAC 🛛 🔍 Use this MAC
🖲 Default 🛛 Custom
Auto Sense
Save Cancel

図 5-6 L2TP (Username/Password) 画面

以下の設定項目があります。

項目	説明	
L2TP		
Address Mode	「Dynamic IP」または「Static IP」を選択します。	
IP Address	ISP により提供された IP アドレスを入力します。(「Static IP」 選択時)	
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。(「Static IP」選択時)	
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。(「Static IP」選択時)	
Server Address	L2TP サーバのアドレスを入力します。	
User Name	L2TP のユーザ名を入力します。	
Password	L2TP のパスワードを入力します。	
Secret	シークレットを入力します。	
Split Tunnel	スプリットトンネルを「ON」または「OFF」にします。 「ON」にすると、同じ物理接続を使用して VPN とインターネット両方の接続が可能になります。	
Reconnect Mode	インターネットの再接続モードを以下から選択します。 ・「Always On」:常にインターネットに接続している状態となります。 ・「On Demand」:インターネット接続を開始した場合のみ、ルータがインターネットに接続します。一定の時間アイド ル状態が続くと、接続は自動的に終了します。	
Maximum Idle Time	アイドル時間の最大値を入力します (「On Demand」選択時)	
	Domain Name System (DNS) Servers	
DNS Server Source	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 •「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します。 •「Use These DNS Servers」: ご契約の ISP の指定したアドレスを使用します。	
DNS Server Source Primary DNS Server	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 • 「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します。 • 「Use These DNS Servers」: ご契約の ISP の指定したアドレスを使用します。 プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)	
DNS Server Source Primary DNS Server Secondary DNS Server	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 • 「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します。 • 「Use These DNS Servers」: ご契約の ISP の指定したアドレスを使用します。 プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時) セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時)	
DNS Server Source Primary DNS Server Secondary DNS Server	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 •「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します。 •「Use These DNS Servers」: ご契約の ISP の指定したアドレスを使用します。 プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) MAC Address	
DNS Server Source Primary DNS Server Secondary DNS Server MAC Address Source	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 • 「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します。 プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) MAC Address ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」: WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC」: 現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」: 手動で MAC アドレスを指定します。	
DNS Server Source Primary DNS Server Secondary DNS Server MAC Address MAC Address	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 • 「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します。 ・「Use These DNS Servers」: ご契約の ISP の指定したアドレスを使用します。 プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) MAC Address ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」: WAN1 ポートの MAC アドレスを使用します。 • 「Use this MAC」: 現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」: 手動で MAC アドレスを指定します。 • 「Use this MAC」: 手動で MAC アドレスを指定します。	
DNS Server Source Primary DNS Server Secondary DNS Server MAC Address Source MAC Address	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 • 「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します。 ・「Use These DNS Servers」: ご契約の ISP の指定したアドレスを使用します。 プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) MAC Address ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」: WAN1 ポートの MAC アドレスを使用します。 • 「Clone your PC's MAC」: 現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」: 手動で MAC アドレスを指定します。 ISP と細付ける MAC アドレスを入力します。(「Use this MAC」選択時) Port Setup	
DNS Server Source Primary DNS Server Secondary DNS Server MAC Address Source MAC Address MTU Size	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 · 「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します。 · 「Use These DNS Servers」: ご契約の ISP の指定したアドレスを使用します。 プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時) セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時) MAC Address ISP 側での識別に使用される MAC アドレスを設定します。 · 「Use Default MAC」: WAN1 ポートの MAC アドレスを使用します。 · 「Clone your PC's MAC」: 現在接続しているコンピュータの MAC アドレスを使用します。 · 「Use this MAC」: 手動で MAC アドレスを指定します。 ISP と紐付ける MAC アドレスを入力します。(「Use this MAC」選択時) Port Setup MTU 値を「Default」(初期値: 1500) または「Custom」に設定します。	
DNS Server Source Primary DNS Server Secondary DNS Server MAC Address MAC Address MTU Size Custom MTU	Domain Name System (DNS) Servers DNS サーバの IP アドレス取得方法を以下から選択します。 • 「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します。 プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時) MAC Address ISP 側での識別に使用される MAC アドレスを設定します。 • 「Use Default MAC」: WAN1 ポートの MAC アドレスを使用します。 • 「Lose this MAC」: 現在接続しているコンピュータの MAC アドレスを使用します。 • 「Use this MAC」: 手動で MAC アドレスを指定します。 ISP と紐付ける MAC アドレスを入力します。(「Use this MAC」選択時) Port Setup MTU 値を「Default」(初期値: 1500) または「Custom」に設定します。(「Custom」選択時)	

Japanese multiple PPPoE(Japanese PPPoE 設定)

「Connection Type」で「Japanese multiple PPPoE」を選択した場合の設定です。

Japanese Multiple PPPoE	
Primary PPPoE Profile Configuration Address Mode	● Dynamic IP ○ Static IP
User Name	dlink
Password	••••
Service	Optional
Authentication Type	Auto-negotiate 🔻
Reconnect Mode	Always On On Demand
Primary PPPoE Domain Name System (DNS)	Servers
DNS Server Source	Get Dynamically from ISP Use These DNS Servers
Secondary PPPoE Profile Configuration	
Address Mode	🖲 Dynamic IP 🔍 Static IP
User Name	dlink
Password	•••••
Service	
Authentication Type	Auto-negotiate
Reconnect Mode	🖲 Always On 🗢 On Demand
Secondary PPPoE Domain Name System (DI	NS) Servers
DNS Server Source	🖲 Get Dynamically from ISP 🛛 🔍 Use These DNS Servers
MAC Address	
MAC Address Source	🖲 Use Default MAC 🛛 🔍 Clone your PC's MAC 👘 Use this MAC
Port Setup	
MTU Size	🖲 Default 🛛 Custom
Port Speed	Auto Sense V
	Save Cancel

図 5-7 Japanese Multiple PPPoE 画面

以下の設定項目があります。

項目	説明		
	Primary PPPoE Profile Configuration		
Address Mode	「Dynamic IP」または「Static IP」を選択します。		
IP Address	ISP により提供された IP アドレスを入力します。(「Static IP」 選択時)		
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。(「Static IP」選択時)		
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。(「Static IP」 選択時)		
User Name	PPPoE のユーザ名を入力します。		
Password	PPPoE のパスワードを入力します。		
Service	ISP により指示があった場合にサービス名を入力します。		
Authentication Type	プロファイルが使用する認証タイプを指定します。		
Reconnect Mode	インターネットの再接続モードを以下から選択します。		
	・「Always On 」:常にインターネットに接続している状態となります。		
	・「On Demand」:一定の時間アイドル状態が続くと、接続は自動的に終了します。		
Maximum Idle Time	アイドル時間の最大値を入力します。(「On Demand」選択時)		
	Primary PPPoE Domain Name System (DNS) Servers		
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。		
	・「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します。		
	・「Use These DNS Servers」:ご契約の ISP の指定したアドレスを使用します。		
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)		
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers 」選択時)		
Secondary PPPoE Profile Configuration			
Address Mode	「Dynamic IP」または「Static IP」を選択します。		
IP Address	ISP により提供された IP アドレスを入力します。(「Static IP」選択時)		
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。(「Static IP」選択時)		
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。(「Static IP」選択時)		
User Name	PPPoE のユーザ名を入力します。		

項目	説明
Password	PPPoE のパスワードを入力します。
Service	ISP により指示があった場合にサービス名を入力します。
Authentication Type	プロファイルが使用する認証タイプを指定します。
Reconnect Mode	インターネットの再接続モードを以下から選択します。
	・「Always On」: 常にインターネットに接続している状態となります。
	・「On Demand」:一定の時間アイドル状態が続くと、接続は自動的に終了します。
Maximum Idle Time	アイドル時間の最大値を入力します。(「On Demand」選択時)
	Secondary PPPoE Domain Name System (DNS) Servers
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。
	・「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します。
	・「Use These DNS Servers」:ご契約の ISP の指定したアドレスを使用します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)
MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。
	・「Use Default MAC」:WAN1 ポートの IP アドレスを使用します。
	・「Clone your PC's MAC」:現在接続しているコンピュータの MAC アドレスを使用します。
	・「Use this MAC」:手動で MAC アドレスを指定します。
MAC Address	MAC アドレスを入力します。(「Use this MAC」選択時)
Port Setup	
MTU Size	MTU 値を「Default」(初期値:1500)または「Custom」に設定します。
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。(「Custom」選択時)
Port Speed	ポート速度を選択します。
	・ 初期値:「Auto Sense」

「Save」をクリックし、設定を適用します。

Russian dual access PPPoE(Russian PPPoE 設定)

「Connection Type」で「Russian dual access PPPoE」を選択した場合の設定です。

Russian PPPoE	
Address Mode	💿 Dynamic IP 🛛 🔍 Static IP
User Name	dlink
Password	•••••
Service	Optional
Authentication Type	Auto-negotiate
Reconnect Mode	🖲 Always On 🔍 On Demand
Domain Name System (DNS) Servers DNS Server Source	Get Dynamically from ISP Use These DNS Servers
MAC Address	
MAC Address Source	💿 Use Default MAC 🛛 🔍 Clone your PC's MAC 🔍 Use this MAC
WAN Physical Settings	
Address Mode	💿 Dynamic IP 🛛 🔍 Static IP
WAN Physical Settings Domain Name Sys	tem
DNS Server Source	● Get Dynamically from ISP 🛛 🔍 Use These DNS Servers
Port Setup	
MTU Size	🖲 Default 🔷 Custom
Port Speed	Auto Sense
	Save Cancel

図 5-8 Russian dual access PPPoE 画面

以下の設定項目があります。

項目	説明	
Russian PPPoE		
Address Mode	「Dynamic IP」または「Static IP」を選択します。	
IP Address	ISP により提供された IP アドレスを入力します。(「Static IP 選択時)	
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。(「Static IP 選択時)	
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。(「Static IP 選択時)	
User Name	PPPoE のユーザ名を入力します。	
Password	PPPoE のパスワードを入力します。	
Service	ISP により指示があった場合にサービス名を入力します。	
Authentication Type	プロファイルが使用する認証タイプを指定します。	
	Domain Name System (DNS) Servers	
Reconnect Mode	インターネットの再接続モードを以下から選択します。	
	・「Always On 」:常にインターネットに接続している状態となります。	
	・「On Demand」:一定の時間アイドル状態が続くと、接続は自動的に終了します。	
Maximum Idle Time	アイドル時間の最大値を入力します。(「On Demand」選択時)	
DNS Server Source	DNSサーバのIPアドレス取得方法を以下から選択します。	
	 「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します。 	
	 Use These DNS Servers」: ご契約の ISP の指定したアドレスを使用します。 ニューロ DNS には、 バック Participation によう、 「ビース」、 DNS Community DNS Participation 	
Primary DNS Server	フライマリ DNS サーバの IP アドレスを入力します。(I Use These DNS Servers」)選択時	
Secondary DNS Server	セカンタリ DNS サーハの IP アドレスを入力します。(I Use These DNS Servers」)選択時	
	MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。	
	 Use Default MAC」・WANT ホートの MAC アドレスを使用します。 「Cloppyour DC's MAC」・現在控結しているコンピュータの MAC アドレスを使用します。 	
	・「Clotle your FC's MAC」・現在後続しているコンビュータの MAC アドレスを使用しより。 ・「Lise this MAC」・毛動で MAC アドレスを指定します	
MAC Address	MAC アドレスを入力します。(「Use this MAC」 選択時)	
IVIAC AUGIESS IVIAC / 「レスをハノ」しより。(I USE II IIS IVIAC」医抗団/		
Address Mode	「Dvnamic IP」または「Static IP」を選択します。	
WAN Physical Setting Domain Name System		
DNS Server Source	DNS サーバの IP アドレス取得方法を以下から選択します。	
	・「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します。	
	・「Use These DNS Servers」:ご契約の ISP の指定したアドレスを使用します。	
Primary DNS Server		
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)	
	Port Setup	
MTU Size		
Custom MTU	MTU 値を指定し、ご利用の ISP の通信におけるパフォーマンスを最適化します。	
Port Speed	オート速度を選択します。	
	・ 初期値:「Auto Sense」	

Russian dual access PPTP(PPTP 設定)

「Connection Type」で「Russian dual access PPTP」を選択した場合の設定です。

🖲 Dynamic IP 🛛 Static IP
0.0.0.0
dlink
•••••
OFF
OFF
🖲 Always On 🛛 🔍 On Demand
● Get Dynamically from ISP 🛛 🔍 Use These DNS Servers
● Use Default MAC 🛛 Clone your PC's MAC 🔍 Use this MAC
🖲 Default 🔍 Custom
Auto Sense 🔹
Save Cancel

図 5-9 Russian dual access PPTP 画面

以下の設定項目があります。

項目	説明	
Russian PPTP		
Address Mode	「Dynamic IP」または「Static IP」を選択します。	
IP Address	ISP により提供された IP アドレスを入力します。(「Static IP」選択時)	
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。(「Static IP」選択時)	
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。(「Static IP」 選択時)	
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	PPTP のユーザ名を入力します。	
Password	PPTP の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「ON」にします。	
Split Tunnel	スプリットトンネルを「ON」または「OFF」にします。	
	「ON」にすると、同じ物理接続を使用して VPN とインターネット両方の接続が可能になります。	
Reconnect Mode	インターネットの再接続モードを以下から選択します。	
	・「Always On」:常にインターネットに接続している状態となります。	
	・「On Demand」:一定の時間アイドル状態が続くと、接続は自動的に終了します。	
Maximum Idle Time	アイドル時間の最大値を入力します。(「On Demand」選択時)	
	Domain Name System (DNS) Servers	
DNS Server Source	DNSサーバのIPアドレス取得方法を以下から選択します。	
	・「Get Dynamically from ISP」:ご契約の ISP から目動的に DNS サーバアドレスを取得します。	
	・ 「Use These DNS Servers」、ご契約の ISP の指定したアドレスを使用します。	
Primary DNS Server	ノライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」 選択時)	
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(I Use These DNS Servers」選択時)	
	MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。	
	・ 「Use Default MAC」:WAN1 ボートの MAC アドレスを使用します。	
	・「Clone your PC's MAC」:現任接続しているコンビュータの MAC アドレスを使用します。	
	 Ose Unis MAC」、手動でMACアドレスを指定します。 	
MAC Address	MAC アトレスを入力します。	
	MIU 個を「Delduit」(初期値・ISUU) よたは「CUSTOM」に設定しより。	
	MIU 個を指定し、ご利用の ISP の通信におけるハフォーマノスを最適化します。(I CUSTOM」選択時)	
Port Speed	示一下迷度を選択します。初期他:「Auto Sense」	
「Save」をクリックし、	設定を適用します。	

57

Russian dual access L2TP(Russian L2TP 設定)

「Connection Type」で「Russian dual access L2TP」を選択した場合の設定です。

Russian L2TP	
Address Mode	🖲 Dynamic IP 🔍 Static IP
Server Address	0.0.0.0
User Name	dlink
Password	•••••
Secret	Optional
Split Tunnel	OFF
Reconnect Mode	💿 Always On 🔍 On Demand
Domain Name System (DNS) Servers DNS Server Source	● Get Dynamically from ISP 🛛 ● Use These DNS Servers
MAC Address MAC Address Source	● Use Default MAC 🛛 Clone your PC's MAC 🔍 Use this MAC
<i>Port Setup</i> MTU Size	● Default ○ Custom
Port Speed	Auto Sense 🔻
	Save Cancel

図 5-10 Russian dual access L2TP 画面

以下の設定項目があります。

項目	説明	
Russian L2TP		
Address Mode	「Dynamic IP」または「Static IP」を選択します。	
IP Address	ISP により提供された IP アドレスを入力します。(「Static IP 」選択時)	
IP Subnet Mask	ISP により提供されたサブネットマスクを入力します。(「Static IP 」選択時)	
IP Gateway	ISP により提供されたゲートウェイアドレスを入力します。(「Static IP 」選択時)	
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	L2TP のユーザ名を入力します。	
Password	L2TP のパスワードを入力します。	
Secret	シークレットを入力します。	
Split Tunnel	スプリットトンネルを「ON」または「OFF」にします。	
	「ON」にすると、同じ物理接続を使用して VPN とインターネット両方の接続が可能になります。	
Reconnect Mode	インターネットの再接続モードを以下から選択します。	
	・「Always On」:常にインターネットに接続している状態となります。	
	・「On Demand」:一定の時間アイドル状態が続くと、接続は自動的に終了します。	
Maximum Idle Time	アイドル時間の最大値を入力します。(「On Demand」選択時)	
	Domain Name System (DNS) Servers	
DNS Server Source	DNSサーバのIPアドレス取得方法を以下から選択します。	
	 「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します。 	
	・「Use These DNS Servers」:ご契約の ISP の指定したアドレスを使用します。	
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」)選択時	
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)	
	MAC Address	
MAC Address Source	ISP 側での識別に使用される MAC アドレスを設定します。	
	 Use Default MAC」: WAN1 ボートの MAC アドレスを使用します。 	
	 「Clone your PC's MAC」: 現在接続しているコンビュータの MAC アドレスを使用します。 「リーリー・MAC」・エチェス MACコンド・スキャウト キキ 	
	 ・ Use this MAC」・手動 ぐ MAC アドレスを指定します。 	
MAC Address	MAC アドレスを入力します。(I Use this MAC」選択時)	
	Port Setup	
MIU Size	MIU 値を「Default」(初期値:1500)または「Custom」に設定します。	
Custom MTU	MIU 値を指定し、ご利用の ISP の通信におけるバフォーマンスを最適化します。	
Port Speed	ボート速度を選択します。初期値:「Auto Sense」	

WAN2 / DMZ Setting (WAN2 / DMZ 設定)

Network > Internet > WAN2 / DMZ Setting

WAN2 ポートに対して、WAN2 または DMZ の設定を行います。

WAN2 に設定する場合、設定内容は WAN1 の設定項目と同等です。DMZ(DeMilitarized Zone)は、外部ネットワークと社内ネットワークの中間 につくられるネットワーク上のセグメントです。外部ネットワークからも内部ネットワークからもファイアウォールなどによって隔離されるため、 DMZ 内にサーバを設置するなどしてセキュリティの強化を図ることができます。

1. Network > Internet > IPv4 WAN2/ DMZ Setting 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 5-11 IPv4 WAN2 / DMZ Setting「Configurable Port Setup」画面

2. 「WAN」または「DMZ」を選択します。

「WAN」:WAN2 ポートに対して WAN の設定を行います。WAN の設定内容については「WAN1」での設定項目と同等になります。 「DMZ」:WAN2 ポートに対して DMZ の設定を行います。

3. 選択後、表示される各項目の設定を行います。

WAN (WAN 設定 /WAN2)

「Configurable Port」で「WAN」を選択した場合、以下の画面が表示されます。

	2 Status	🛜 Wireless	🚽 Network	CA VPN	🔒 Security	O Maintenance	
Network » II	nternet » WAN2 / DA	Z Setting					0 0
This page all Information e	ows you to set up yo etc. This information . / DMZ Setting	ur Internet connection. E is usually provided by yc	nsure that you ha our ISP or networ	ave the Internet co k administrator.	onnection informatio	n such as the IP Addresses	, Account
Configura	able Port Setup						
Configur	able Port	• w/	AN O DMZ				
WAN2 Se	tup						
Connec	tion Type	Dynam	ic IP (DHCP)	~			
Enable	VLAN Tag		OFF				
Dynamic	IP (DHCP)						
Host N	ame			Optional			
DNS Ser	vers (Domain Nam	e System)					
DNS Se	rver Source	• G	et Dynamically fr	om ISP O Use	These DNS Servers		
MAC Add	dress						
MAC A	ddress Source	• Us	e Default MAC	O Clone your PC	C's MAC O Use thi	s MAC	
Port Set	up						
MTU Si	ze	• De	efault O Cust	om			
Port Sp	peed	Auto S	iense	\checkmark			
			Save	Cancel			

図 5-12 IPv4 WAN2 / DMZ Setting 画面

注意 「WAN2 / DMZ Setting」での「WAN」の設定項目については「WAN1 Settings(WAN1 設定)」と同等となります。WAN2 ポートにおける WAN の設定を行うには「WAN1 Settings(WAN1 設定)」を参照してください。

DMZ(DMZ 設定/WAN2)

本製品の WAN2 ポートは、セカンダリ WAN イーサネットポート、または DMZ ポートとして設定できます。

DMZ (DeMilitarized Zone) は、パブリックにオープンでありながらファイアウォールに保護されたサブネットワークです。 DMZ により、「特定のポート/サービスによるインターネットへのアクセスは許可しても、ネットワーク (LAN) にはアクセスさせない」というセキュ リティレイヤを提供できます。

Web サーバやメールサーバなど、インターネットへのアクセスを必要とするホストを DMZ ネットワークに配置することが推奨されます。

ファイアウォールのルールでは、LAN 及び WAN 両方からの DMZ 上の指定サービス / 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 への攻撃イベントが発生した場合、必ずしも LAN が脆弱になるという訳ではありません。

DMZ設定はLAN設定と同等です。DMZポートに対しては、ゲートウェイのIPアドレスと同等のIPアドレスを付与すること以外、IPアドレス/サブネッ トマスクの設定に関する制限はありません。

1. 「IPv4 WAN2 / DMZ Setting」画面の「Configurable Port」で「DMZ」を選択します。

0		🛜 Wireless	💂 Network	CA VPN	Security	O Maintenance	
twork » Intern	net » WAN2/E	OMZ Setting					
is page allows count Informa	you to set up ation etc. This i	your Internet conne information is usually	ction. Ensure that you provided by your ISP	have the Internet or network adminis	connection informati strator.	on such as the IP Addresses,	
v4 WAN2 /	DMZ Setting						
Configurable	Port Setup						
Configurable	e Port		🔍 WAN 🔘 DMZ				

図 5-13 IPv4 WAN2 / DMZ Setting 画面

2. 「Save」をクリックし、設定を適用します。

「WAN2 / DMZ Setting」で DMZ を有効にした場合、DMZ の設定を行う必要があります。WAN2 ポートにおける DMZ の設定を行うには「DMZ 注意 Settings (DMZ 設定)」を参照してください。

WAN3 Setting (WAN3 / 3G インターネット設定(未サポート))

Network > Internet > WAN3 Settings

注意 本項目(WAN3 Settings)は未サポートです。

本ルータは 3G インターネットアクセスをサポートしています。DSR シリーズ用 3G USB モデムを使用して、携帯電話用 3G インターネットアクセ スが利用できます。実際の接続を行うには通信会社から提供される 3G データプランからの認証要件を満たす必要があります。通信会社から提供 される電話番号と APN が固有に存在します。接続種類を設定・保存した後、WAN ステータスのページ(Status > System Information > Device > WAN3)から、WAN3 リンクを有効にして 3G 接続を確立することが可能です。

1. Network > Internet > 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。

	🝘 Status	🛜 Wireless	💻 Netv	vork 🖌				© ^o Maintenance	
Network <mark>»</mark> Ir	etwork » Internet » WAN3 Settings								
This page allo Information->	ows user to configur USB Status page.	e the ISP settings for	connecting to	a Mobile Inte	rnet servio	e. Please	check the l	JSB card status on Status	->System
WAN3 Sett	ings								
WAN3 (Ma Reconne	o bile Internet) ct Mode	C	Always On	• On Deman	ł				
Maximun	n Idle Time	5	[Range: 1 - 999]					
Mobile In	ternet Connection	n Type							
User Nar	ne				Optional				
Password	d				Optional				
Dial-In N	lumber	**	99#						
Authenti	ication Protocol	N	one	~					
APN Req	uired								
APN		w	ap.isp.com						
Domain N	ame System (DNS)	Servers							
DNS Serv	ver Source	C	Get Dynamic	ally from ISP	• Use T	hese DNS	Servers		
Primary	DNS Server	0	.0.0.0						
Seconda	ry DNS Server	0	.0.0.0						
Port Setu	p								
MTU Size	2	C	Default	Custom					
Custom /	мти	1	500 [Range: 1200 - 15	00] Bytes				
			Save	Cance	el				

図 5-14 WAN3 Settings 画面

2. 以下の項目を設定します。

項目	説明					
	WAN3 (Mobile Internet)					
Reconnect Mode	以下のオプションの1つを選択します。					
	・「Always On」:常にインターネットに接続している状態となります。					
	・「On Demand」:一定の時間アイドル状態が続くと、接続は自動的に終了します。					
Maximum Idle Time	アイドル時間の最大値を入力します。(「On Demand」選択時)					
	Mobile Internet Connection Type					
User Name	3G アカウントのユーザ名を入力します。					
Password	3G アカウントのパスワードを入力します。					
Dial-In Number	インターネットへのアクセスに使用するダイヤル番号を入力します。					
Authentication Protocol	認証プロトコルを指定します。「None」「PAP」「CHAP」から指定できます。					
APN Required	お使いの ISP 接続に APN を要件としている場合「ON」にします。					
APN	ISP から提供される APN (アクセスポイント名) を入力します。					
	Domain Name System (DNS) Servers					
DNS Server Source	DNS サーバ情報の設定方法を「Get Dynamically from ISP」「Use These DNS Servers」から指定します。					
Primary DNS Server	プライマリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)					
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを入力します。(「Use These DNS Servers」選択時)					
	Port Setup					
MTU Size	MTU 値を「Default」(初期値:1500)または「Custom」に設定します。					
Custom MTU	ISP とのパフォーマンスを最適にする MTU 値を指定します。(「Custom」選択時)					

WAN Mode(WAN モード設定)

Network > Internet > WAN Mode

本製品は、複数のWANリンクをサポートしています。一つのポートでWAN接続が不安定になった場合でも、フェイルオーバ機能およびロードバランシング機能により、インターネットを利用する特定のサービスを優先的に処理することができます。

オート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。これにはインターネット 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(ユーザ定義)への ping といった検知設定が含まれています。必要に応じて、リン クが切断していることが疑われる場合のリトライ回数や、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. Network > Internet > 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。

	🗥 Status	🛜 Wireless	📮 Network	S VPN	Security	O ^o Maintenance	
Network » Ir	nternet » WAN Mode	e					00
This page allo router to acc excessively o fails for any i WAN Mode	ows user to configui ess the internet. Lo verloaded. Auto-Ro reason.	re the policies on the bad balancing allows t llover uses a backup li	three WAN ports for 'affic to and from th nk to preserve inter	Internet connecti e internet to be s net connectivity f	on.By configuring bot hared across both con or the LAN if the mair	h WANs, there are two way figured links to ensure on n ISP configured on the pri	ys for the e ISP is not imary WAN
WAN Mod	e Setup						
WAN Mod	le	s	ingle WAN port	\checkmark			
Single WA	N port						
Use only	single WAN port		WAN1 O WAN2	O WAN3			
			Save	Cancel			
0							

図 5-15 WAN Mode 画面

2. 「WAN Mode Setup」の「WAN Mode」で WAN リンクの種類を選択します。

Single WAN Port(シングル WAN ポート)

- オートフェイルオーバまたはロードバランシングを使用しない場合、「Single WAN Port」を選択します。
- 1. 「WAN Mode」で「Single WAN Port」を選択します。

🕋 Status	(î:		💻 Network	CB VPN	Security	OP Maintenance	
Network » Internet » WAN A	Node						00
This page allows user to conf router to access the internet excessively overloaded. Auto fails for any reason. WAN Mode	igure the p . Load bala -Rollover u	policies on the ancing allows tr ises a backup li	three WAN ports for affic to and from th nk to preserve inter	Internet connection in internet to be si net connectivity fo	on.By configuring bot ared across both con or the LAN if the main	h WANs, there are two way ifigured links to ensure one n ISP configured on the pri	vs for the E ISP is not mary WAN
WAN Mode Setup							
WAN Mode		Si	ngle WAN port	\checkmark			
Single WAN port							
Use only single WAN por	rt	۲	WAN1 O WAN2	O WAN3			
			Save	Cancel			

図 5-16 WAN Mode (Single WAN Port) 画面

- 2. 対象の WAN ポートを「WAN1」「WAN2」「WAN3」から選択します。
- 3. 「Save」をクリックし、設定を適用します。

Auto-Rollover using WAN port (WAN ポートを使用したオートロールオーバ)

本項目では、1 つの WAN ポートをインターネットトラフィック用のプライマリインターネットリンクとして設定し、もう1 つの WAN ポートをセ カンダリインターネットリンクとして設定します。セカンダリインターネットリンクは、なんらかの理由でプライマリリンクがダウンした場合の冗 長用として使用されます。本機能を有効にする前に、プライマリ WAN ポート / セカンダリ WAN ポートともに接続用の ISP 情報を設定しておく必要 があります。セカンダリ WAN ポートは、プライマリ WAN ポートがダウンした場合のみ接続されます。いずれのポートもプライマリとして使用す ることができます。オートフェイルオーバモードで設定を行った場合、プライマリ WAN ポートはリンクダウン検知で設定した期間に従いリンクス テータスをチェックされます。

1. 「WAN Mode」で「Auto-Rollover Using WAN IP」を選択します。

🕐 Status 🤶	Wireless 📃 N	Network 🚯 VPN	Security	🗢 Maintenance	
Network » Internet » WAN Mode					0 0
This page allows user to configure the p router to access the internet. Load bala excessively overloaded. Auto-Rollover u fails for any reason.	olicies on the three WAN ncing allows traffic to a ses a backup link to pres	N ports for Internet connect and from the internet to be serve internet connectivity	tion.By configuring both shared across both conf for the LAN if the main	WANs, there are two way igured links to ensure on ISP configured on the pri	ys for the e ISP is not imary WAN
WAN Mode					
WAN Mode Setup					
WAN Mode	Auto-Rollover	using WAN port			
Auto-Rollover using WAN port					
Use Primary WAN port	WAN1	O WAN2 O WAN3			
Use Secondary WAN port	WAN2	\checkmark			
WAN health check	WAN DNS Ser	rvers			
Retry Interval is	30	[Default: 30, Range: 5 - 999]	Seconds		
Failover After	4] [Default: 4, Range: 2 - 999]	Failures		
	Save	Cancel			
	n <mark>60</mark>				

図 5-17 WAN Mode (Auto-Rollover Using WAN port) 画面

2. 以下の項目を設定します。

項目	説明
Use Primary WAN Port	プライマリリンクとしての WAN ポートを指定します。
Use Secondary WAN Port	プライマ WAN ポートがダウンした場合に使用されるセカンダリリンクとしての WAN ポートを指定します。
WAN health check	WAN ポートに対するステータスチェックの種類を以下から選択します。
	・「WAN DNS Servers」:
	DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。
	「DNS Servers」:
	カスタム DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。
	FPing These IP Addresses」:
	定期的な Ping を実行してプライマリ WAN の接続性をチェックします。
WAN1/WAN2/WAN3	「DNS Servers」または「Ping These IP Addresses」を選択した場合、Ping を実行する DNS サーバまたは IP アドレスを
	指定します。WAN3 は未サポートです。
Retry Interval is	「WAN health check」をルータが実行する頻度を指定します。
	・ 設定可能範囲:5-999 (秒)
	 初期値:30(秒)
Failover After	フェイルオーバが有効になるまでのリンク不具合の回数を設定します。
	・ 設定可能範囲:2-999(回)
	 初期値:4(回)

Load Balancing(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、複数の ISP) を使用することができます。WAN ポートを複数設定した後、ロードバランシング オプションにより、2 つ以上のリンクにトラフィックを送信するように設定することができます。また、インターネットフロー管理において、各プ ロトコルサービスを各 WAN ポートに振り分けるために、プロトコルバインディングが使用されます。ロードバランシングモードが設定されている 場合、定義した障害検出方式が、すべての設定済み WAN ポート上で定期的に実行されます。

本ルータは、以下のアルゴリズムをサポートしています。

Round Robin

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、遅延の少ないサービス(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。

Spill Over

定義したしきい値に達するまで、プライマリ WAN が専用リンクとして機能します。しきい値に達した後、セカンダリ WAN が新しい接続に使用 されます。スピルオーバロジックにより、プライマリからセカンダリ WAN に移動するアウトバウンド通信が管理されるため、セカンダリ WAN におけるインバウンド接続は、本モードで許可されます。スピルオーバモードでは次のオプションを設定することができます。

- Load Tolerance: この最大帯域幅(%)を超えた場合、プライマリ WAN からセカンダリ WAN に切り替わります。

- Max Bandwidth:アウトバウンド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。

アウトバウンドトラフィックのリンク帯域がロードトレランス最大帯域を上回ると、ルータは次の接続をセカンダリ WAN に切り替えます。

例 : プライマリ WAN の最大帯域幅 :1Kbps、ロードトレランス :70 の場合

ある接続数で帯域幅が1Kbpsの70%に到達すると、新規のアウトバウンド接続はセカンダリWANに切り替えられます。

ロードバランシングは、1 つの WAN ポートの接続速度が他と大きく異なる場合に特に役に立ちます。この場合、低遅延のサービス (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。

Round Robin (ラウンドロビン)

1. 「WAN Mode」で「Load Balancing」を選択 →「Round Robin」を選択し以下の画面を表示します。

	🕋 Status		📮 Network	C VPN	Security	O Maintenance	
Network » I	nternet » WAN Mod	e					00
This page all router to acc excessively o fails for any WAN Mode	ows user to configu ess the internet. Lo verloaded. Auto-Ro reason.	re the policies on the oad balancing allows tı llover uses a backup li	three WAN ports for affic to and from the nk to preserve interr	Internet connection e internet to be sine thet connectivity for	on.By configuring botl nared across both con or the LAN if the main	h WANs, there are two way figured links to ensure one ISP configured on the pri	s for the ISP is not mary WAN
WAN Mod	e Setup						
WAN Mo	de	Lo	ad Balancing	\checkmark			
Load Bala	ncing Setup						
Load Ba	ancing	۲	Round Robin	Spillover Mode			
WAN hea	alth check	N	DNe	~			
			Save	Cancel			

- 図 5-18 Load Balancing (Round Robin) 画面
- 2. 以下の項目を設定します。

項目	説明
Load Balancing	「Round Robin」を選択します。
WAN health check	 WAN ポートに対するステータスチェックの種類を以下から選択します。 「WAN DNS Servers」: DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 「DNS Servers」: カスタム DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 「Ping these IP addresses」: 定期的な Ping を実行してプライマリ WAN の接続性をチェックします。
WAN1/WAN2/WAN3	「DNS Servers」または「Ping These IP Addresses」を選択した場合、Ping を実行する DNS サーバまたは IP アドレスを指定します。WAN3 は未サポートです。
Retry Interval is	 「WAN health check」をルータが実行する頻度を指定します。 ・ 設定可能範囲: 5-999(秒) / 初期値: 30(秒)
Failover After	フェイルオーバが有効になるまでのリンク不具合の回数を設定します。 • 設定可能範囲:2-999(回) / 初期値:4(回)

Spillover Mode	(スピルオーバー	Eード)					
1. WAN Mode	」で「Load Balanc	:ing」を選択 →「S	pillover Mode	」を選択し、	以下の画面を表示	≂ します。	
注意 スピルオ	-ーバモードを使用	する場合、ハード	ウェアオフロ	ードが無効にフ	なるため、パフォ	ーマンスが低下す	る場合があります。
1	🕜 Status	🛜 Wireless	📃 Network	A VPN	🔒 Security	🍄 Maintenance	
Network This pag router t excessiv fails for WAN N	» Internet » WAN Mod e allows user to configu o access the internet. L ely overloaded. Auto-Re any reason. Mode	le ure the policies on the th oad balancing allows tra ollover uses a backup lin	rree WAN ports for ffic to and from t k to preserve inte	Internet connecti ne internet to be si rnet connectivity fi	on.By configuring both hared across both coni or the LAN if the main	WANs, there are two wa rigured links to ensure on ISP configured on the pr	iys for the te ISP is not timary WAN
WAN	<i>Mode Setup</i> N Mode	Loa	d Balancing				
Load Loa	Balancing Setup	0	Round Robin	Spillover Mode			
WA	N health check	WA	N DNS Servers	~			
Ret	ry Interval is	30	[Default	: 30, Range: 5 - 999] S	Seconds		
Fai	lover After	4	[Default	: 4, Range: 2 - 999] Fa	ailures		
Spille	over Configuration Se	etup					
Loa	d Tolerance	80	[Default	: 80, Range: 20 - 80]			
Max	< Bandwidth	819	2 bps		(Max. 1000 Mbps)		
			Save	Cancel			

図 5-19 Load Balancing (Spillover Mode) 画面

2. 以下の項目を設定します。

項目	説明				
	Load Balancing Setup				
Load Balancing	「Spillover Mode」を選択します。				
WAN health check	 WAN ポートに対するステータスチェックの種類を以下から選択します。 「WAN DNS Servers」: DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 「DNS Servers」: カスタム DNS サーバの DNS ルックアップを使用してプライマリ WAN の接続性をチェックします。 「Ping These IP Addresses」: 定期的な Ping を実行してプライマリ WAN の接続性をチェックします。 				
WAN1/WAN2/WAN3	「DNS Servers」または「Ping These IP Addresses」を選択した場合、Ping を実行する DNS サーバまたは IP アドレスを指定します。WAN3 は未サポートです。				
Retry Interval is	 「WAN health check」をルータが実行する頻度を指定します。 ・ 設定可能範囲:5-999(秒) ・ 初期値:30(秒) 				
Failover After	フェイルオーバが有効になるまでのリンク不具合の回数を設定します。 ・ 設定可能範囲:2-999(回) ・ 初期値:4(回)				
	Spillover Configuration Setup				
Load Tolerance	ルータがセカンダリ WAN に切り替わる最大帯域幅(%)を指定します。				
Max Bandwidth	プライマリ WAN で許可される最大の帯域幅を設定します。 帯域幅の単位は「bps」「Mbps」「Kbps」から指定します。				

SIM Card Authentication(SIM カード認証(未サポート))

Network > Internet > SIM Card Authentication

本ルータは SIM カードをサポートしています。SIM カードのスロットにより携帯電話のモジュールと統合されます。SIM カードの種類によって、3G と 4G がサポートされます。インターネットの利用を開始するには、スロットに SIM カードを挿入し、PIN コードを入力して SIM を解除します。



🗟 本項目は未サポートです。

1. Network > Internet > SIM Card 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。

🗥 Status	🛜 Wireless 🔄	Network	CA VPN	Security	🏟 Maintenance	
Network » Internet » SIM Card A	Authentication					00
	51 N	obile Interne	et is not avai	lable		
This page allows you to unlock t SIM Card Settings	he SIM card by entering the	SIM PIN				
SIM						
SIM Card Status	Not Avai	lable				

図 5-20 SIM Card Authentication 画面

2. 以下の項目を設定します	0
項目	説明
SIM Card Status	SIM カードのステータス(ロック / ロック解除 / ブロック)が表示されます。
Enter SIM PIN	SIM カードがロックされている場合に表示されます。PIN コード(4-8 桁の数字)を入力して SIM カードを解除します。 SIM カードがロックされている場合、全てのネットワークサービスがブロックされます。モバイルインターネット及び SMS サービスを利用するには SIM カードのロックを解除する必要があります。

Routing Mode (ルーティングモード設定)

Network > Internet > Routing Mode

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で受信す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

以下のルーティングモードについて説明します。

「NAT or Classical」 「Transparent」 「Bridge」

■ NAT or Classical (NAT/ クラシカルモード)の設定

Classical ルーティングでは、適切なファイアウォールの設定がなされている場合、LAN 上のデバイスはパブリック IP アドレスでインターネット上 から直接アクセスする事が可能です。ご利用の ISP からコンピュータ/デバイス用に IP アドレスが割り当てられている場合は、「Classical」を選択し ます。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。NAT によって接続の共有が可能になるほか、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すことができます。ISP により割り当てられた IP アドレスが 1 個だけの場合、NAT が必要にな ります。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必要があります。

	🕐 Status	🛜 Wireless	🖳 Network	CA VPN	Security	O° Maintenance	
Network »	nternet » Routing						0 0
This page al traffic is hau internal LAN Mode traffic Routing M	lows user to configu ndled when received IP addresses from i between LAN1 and V ode	re different routing mo I on one physical interf nternet devices. Transj WAN2 is bridged and NA	des like NAT or Clas ace. NAT or Classica varent mode does no T will be done for N	ssical, Transparen al is the most com ot perform NAT an WAN1 and rest of 1	t and Bridge Routing.T mon application for m d lets you bridge traff he LAN ports.	The Routing mode determin ost routers, and allows yo fic between the LAN and W	nes how u to hide /AN.In Bridge
Routing	Settings						
Routing	Settings	۲	NAT or Classical	O Transparent			
NAT vs (Classical routing f	for each WAN					
NAT wi	th WAN1		N				
NAT wi	th WAN2	C	N				
			Save	Cancel			

図 5-21 Routing Mode - NAT or Classical 画面

以下の項目を設定します。

項目	説明
Routing Settings	MAT/ クラシカルモードを有効にするには、「NAT or Classical」を選択します。
NAT with WAN1/	WAN1/WAN2のNATを「ON」または「OFF」(Classical)にします。
NAT with WAN2	

■ Transparent (透過モード)の設定

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。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、LAN インタフェースに到着するブロードキャスト / マルチキャストパケットは WAN にスイッチされます。逆の場合 も同様です。LAN と WAN が同じブロードキャストドメインにある場合は、透過モードを選択します。これにより、ルータで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。LAN と WAN が同じブロードキャストドメインにある場合、本製品のすべての機能が透過モードでサポートされます。

	🗥 Status	🛜 Wireless	📮 Network	C VPN	Security	🏩 Maintenance	
Network »	Internet » Routing						0 0
This page al traffic is ha internal LAN Mode traffic Routing N	lows user to configu ndled when received I IP addresses from i : between LAN1 and ' Node	re different routing m I on one physical inter nternet devices. Trans WAN2 is bridged and N	odes like NAT or Cla face. NAT or Classic sparent mode does n IAT will be done for	assical, Transparen al is the most com ot perform NAT an WAN1 and rest of t	and Bridge Routing. non application for n d lets you bridge traf he LAN ports.	The Routing mode determ nost routers, and allows y fic between the LAN and	ines how ou to hide WAN.In Bridge
Routing	Settings						
Routing	s Settings	C	ONAT or Classical	• Transparent			
			Save	Cancel			

図 5-22 Routing Mode - Transparent 画面

以下の項目を設定します。

項目	説明
Routing Settings	透過モードを有効にするには、「Transparent」を選択します。

「Save」をクリックし、設定を適用します。

■ Bridge(ブリッジモード)の設定

ブリッジモードルーティングが有効になると、最初の物理LAN ポートとセカンダリWAN / DMZ(ポート2)インタフェースがレイヤ2でブリッジされ、 集約ネットワークが作成されます。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いため、ルータはこれらの他のポー トに対する NAT デバイスとして要求します。LAN ポート1およびWAN2 / DMZ インタフェースのブリッジモードでは、L2 / L3 ブロードキャストト ラフィックと ARP / RARP パケットが通過します。WAN 2 がタグ付きトラフィックを受信すると、パケットが LAN ポート1インタフェースに転送さ れる前にタグ情報が削除されます。

🙆 Status 🛜 Wirele	s 🖳 Network 🏾 🕻	<mark>ស</mark> VPN	🚊 Security	🐡 Maintenance	
Network » Internet (IPv4) » Routing					00
This page allows user to configure different ro traffic is handled when received on one physi internal LAN IP addresses from internet device Bridge Mode traffic between LAN1 and WAN2 i Routing Mode	uting modes like NAT or Classical al interface. NAT or Classical is t s. Transparent mode does not pe bridged and NAT will be done fo	, Transparent a the most common rform NAT and r WAN1 and res	and Bridge Routing.T on application for m lets you bridge trafi st of the LAN ports.	The Routing mode determ ost routers, and allows y fic between theLAN and	ines how ou to hide Option.In
Pouting Sottings					
Routing Settings	NAT or Classical I Br	idge			
Bridge Mode Setup					
Bridge Interface IP Address	0.0.0.0]			
DMZ interface IP Address	172.17.100.254]			
Subnet Mask	255.255.255.255]			
NAT vs Classical routing for each WAN NAT with WAN1	ON				
	Save Canci	el			

図 5-23 Routing Mode - Bridge 画面

注意 Network > Internet > WAN2 / DMZ Setting 画面で DMZ を選択した場合のみ、「Bridge」の項目が表示されます。

以下の項目を設定します。

項目	説明				
	Routing Settings				
Routing Settings	ブリッジモードを有効にするには、「Bridge」を選択します。ブリッジモードルーティングが有効である場合、物理 LAN ポート 1 とセカンダリ WAN/DMZ インタフェースにおいてトラフィックがブリッジされ、WAN1 と他の LAN ポー トに対しては NAT が実行されます。				
	注意 ルーティングモード(NAT or Classical、Transparent、Bridge)を変更した場合、すべてのインバウンドファ イアウォールルールが削除されます。				
	Bridge Mode Setup				
Bridge Interface IP Address	ブリッジインタフェースの IP アドレスを入力します。				
DMZ Interface IP Address	DMZ インタフェースの IP アドレスを入力します。				
Subnet Mask	サブネットマスクを入力します。				
	NAT vs Classical routing for each VLAN				
NAT with WAN1	WAN1のNATを「ON」または「OFF」(Classical)にします。				

「Save」をクリックし、設定を適用します。

IP Aliasing(IP エイリアス設定)

Network > Internet > IP Aliasing

IP エイリアスアドレスを設定します。

ポートにエイリアスを追加することで、単一の WAN イーサネットポートに複数の IP アドレスでアクセスできます。

1. Network > Internet > 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。

	🙆 Status	🛜 Wireless	🖳 Network	🎧 VPN	Security	O Maintenance
Network >	» Internet » IP Alias	ing				0 0
This page can be ac	displays the configu cessed via multiple	ured IP Aliases on Opti IP addresses by adding	on interfaces . User ca a alias to the port. Th	an also add, de his is done by	elete and edit the IP Ali configuring IP Alias.	as also.A single Option Ethernet port
IP Aliasi	ing List					
Show 10	entries	[Right click on record to	get more options]			٩
Port	¢	IP Address		€ 9	Subnet Mask	⇔
			No data ava	ilable in table		
Showing (0 to 0 of 0 entries					First Previous Next > Last >
Add N	lew IP Aliasing					

図 5-24 IP Aliasing 画面

2. IP エイリアスを追加する場合は、「Add New IP Aliasing」をクリックし以下の画面を表示します。

IP Aliasing Configuration		×
Interface IP Address Subnet Mask	wan1 wan2	

図 5-25 IP Aliasing Configuration 画面

3. 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「WAN1」「WAN2」から選択します。
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。

4. 「Save」をクリックし、設定を適用します。

追加した予約 IP エイリアスは、IP Aliasing 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

DMZ Settings(DMZ 設定)

Network > Internet > DMZ Settings

WAN2 ポートを DMZ に設定している場合、本項目で DMZ の設定を行う必要があります。

注意

DMZ ポートを設定するためには、**Network > Internet > WAN2 Settings / DMZ Setting** で WAN2 ポートに対して「DMZ」を有効にする必 要があります。「IPv4 WAN2 / DMZ Setting」画面の「Configurable Port Setup」で、WAN2 ポートの設定に「DMZ」を選択します。

1. Network > Internet > DMZ 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。

🕐 Status	Wireless 📃 Network	CAS VPN	Security	O Maintenance	
Network » Internet » DMZ Settings					00
The De-Militarized Zone (DMZ) is a netw servers and give public access to them, and firewall/VPN policies can be custor FTP or mail servers.	vork which, when compared to the LA1 DMZ setup is similar to the LAN TCP/I nized for the DMZ. The DMZ is typicall	N, has fewer fire P options. The ne ly used for netwo	wall restrictions, by d etwork subnet for the ork devices that you w	efault. This zone can be DMZ can be different fro ish to expose to the inte	used to host m the LAN, rnet, such as
DMZ Settings					
DMZ IP Address					
IP Address	172.17.100.254				
Subnet Mask	255.255.255.0				
DHCP for DMZ					
DHCP Mode	O None O DHCP Ser	ver O DHCP F	Relay		
Starting IP Address	172.17.100.100				
Ending IP Address	172.17.100.253				
Default Gateway	172.17.100.254				
Domain Name	DLink				
Lease Time	24 [Paper 1 -	2628001 Hours			
Primary DNS Server	[Nunger (202000] (10013			
Frimary DNS Server					
Secondary DNS Server					
WINS Server					
Enable DNS Proxy	ON IIII.				
- 1921 (1929) 	Save	ancel			

図 5-26 DMZ Settings 画面

2. 以下の項目を設定します。

項目	説明			
DMZ IP Address				
IP Address	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を入力します。			
DHCP for DMZ				
DHCP Mode	 「None」: DHCP 機能を無効化します。 「DHCP Server」: ネットワーク上で本ルータを DHCP サーバとして使用します。DHCP サーバ情報を設定します。 「DHCP Relay」: ネットワーク上の DHCP クライアントは、異なるサブネットの DHCP サーバから IP アドレスを取得することができます。DHCP Relay を選択した場合は、リレーゲートウェイ情報を入力します。 			
Starting IP Address	アドレス範囲の開始 IP アドレスを入力します。 DMZ に参加する新しい DHCP クライアントは、このアドレス範囲内で IP アドレスが付与されます。			
Ending IP Address	アドレス範囲の終了 IP アドレスを入力します。 DMZ に参加する新しい DHCP クライアントは、このアドレス範囲内で IP アドレスが付与されます。			
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。			
Domain Name	ドメイン名を入力します。			
Lease Time	IP アドレスがクライアントにリースされる期間(単位:時間)を指定します。			
Gateway	「DHCP Relay」選択時に表示されます。「DHCP Relay」のゲートウェイを指定します。			
Primary DNS Server	DNS プロキシが有効化されている場合は、プライマリ DNS サーバの IP アドレスを入力します。			
Secondary DNS Server	DNS プロキシが有効化されている場合は、セカンダリ DNS サーバ IP アドレスを入力します。			
WINS Server	DNS プロキシが有効化されている場合は、WINS サーバの IP アドレス を入力します。			
Enable DNS Proxy	「ON」にして、DNS 及び(または)WINS サーバ IP アドレスを手動で設定します。 無効化した場合、本ルータの LAN IP アドレスがクライアントの DNS サーバとして割り当てられ、ルータは ISP から DNS 情報を取得します。			

DMZ DHCP Reserved IPs (DMZ DHCP の予約 IP 設定)

Network > Internet > DMZ DHCP Reserved IPs

DHCP サーバでは、ネットワーク上の DMZ クライアントに対し、クライアントの MAC アドレス及び割り当て IP アドレスを設定して予約 IP 設定を 行うことができます。クライアントからのリクエストを受けたルータは、データベースの MAC アドレスリストとクライアントの MAC アドレスを確 認します。データベース内でそのコンピュータまたはデバイスに IP アドレスがすでに割り当てられている場合は、カスタマイズされた IP アドレス が設定されます。それ以外の場合は、DMZ DHCP プールから自動的に IP アドレスがクライアントに割り当てられます

1. Network > Internet > 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。

	🙆 Status	🛜 Wireless	📮 Network	A VPN	🔒 Security	🍄 Maintenance	
Network >	» Internet » DMZ DF	ICP Reserved IPs				0	0
This page receive th only be as DMZ DHO Show 10	allows user to confi ne same IP address v ssigned to the match CP Reserved IPs entries	igure the reserved IP A when DHCP is enabled o hing MAC address. List [Right click on record to	ddresses for the DHCI n the DMZ, bind the get more options]	P Server configura DMZ device's MAC	tion.In order to ensur address to a preferred	e certain DMZ devices always d IP address. This IP address wil	٩
IP Addr	ess	Ó	MAC Address		⇔	Status	⊜
			No data av	ailable in table			
Showing () to 0 of 0 entries				И	First I Previous Next > Last	K
Add N	lew DMZ DHCP Re	served IP					

図 5-27 DMZ DHCP Reserved IPs 画面

2. 「Add New DMZ DHCP Reserved IP」をクリックして以下の画面を表示します。

DMZ DHCP Reserved IPs Confi	guration	×
DMZ DHCP Reserved IP Enable IP Address MAC Address		
		Save

図 5-28 DMZ DHCP Reserved IP Configuration 画面

3. 以下の項目を設定します。

項目	説明
DMZ DHCP Reserved IP	「ON」にして DMZ DHCP 予約 IP アドレスの登録を有効にします。
Enable	
IP Address	デバイスにわりあてる IP アドレスを入力します。この IP アドレスは、DHCP 設定の開始 IP アドレス/終了 IP アドレ
	スの範囲内で設定する必要があります。
MAC Address	デバイスの MAC アドレスを入力します。(xx:xx:xx:xx:xx 形式)

4. 「Save」をクリックし、設定を適用します。

追加した予約 IP アドレスは、DMZ DHCP Reserved IPs 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Dynamic DNS (ダイナミック DNS 設定)

Network > Internet > Dynamic DNS

ダイナミック DNS の設定について説明します。

ダイナミックDNS (DDNS) は、動的なパブリック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接続することができるインター 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。

必要に応じて、各WAN に異なる DDNS サービスを設定できます。設定が完了すると、WAN IP アドレスにおける DDNS サービスの変更が更新されます。 これにより、FQDN 経由でルータの WAN に接続する機能が正しい IP アドレスを向くように設定されます。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がアカウントプロバイダによって提供されます。



🐼 Status 🦻	🕈 Wireless 📃 I	Network 🚯 VPN	Security	O ^o Maintenance		
Network » Internet » Dynamic DNS » Dynamic DNS WAN1 Settings						
Dynamic DNS WAN1 Settings	Oynamic DNS WAN2 Setti	ngs Dynamic DNS WAN3	Settings			
Dynamic DNS (DDNS) is an Internet ser you must setup an account with a DDM	rvice that allow routers w IS provider such as DynDN	ith varying public IP addres S, D-Link DDNS, Oray etc.	ses to be located using	g Internet domain names. T	o use DDNS,	
Dynamic DNS WAN1 Settings						
Status						
Current WAN Mode	use only sin	gle WAN port WAN1				
DDNS Status	DDNS is disa	DDNS is disabled				
WAN1						
Dynamic DNS Service Type	DynDNS	~				
User Name						
Password						
Host Name						
Туре	Dynamic	~				
Wildcard	OFF	OFF				
Use external (NAT router's) IP a	ddress OFF					
Force Update Interval	10	[Range	e: 1 - 30, Default: 10 Days]			
	Save	Cancel				

図 5-29 Dynamic DNS > Dynamic DNS WAN1 Settings タブ画面

- 2. DDNS を設定する WAN のタブを「Dynamic DNS WAN1 Settings」「Dynamic DNS WAN2 Settings」「Dynamic DNS WAN3 Settings」から選択します。
- 3. 「Dynamic DNS Service Type」から DDNS の種類を選択します。「Dynamic DNS Service Type」以下に表示される項目は、選択した DDNS により 異なります。
- 4. 以下の項目を設定します。

項目	説明		
Status			
Current WAN Mode	現在の WAN モードについて表示します。		
DDNS Status	現在の接続状況を表示します。		
WAN1			
Dynamic DNS Service Type	ダイナミック DNS サービスのタイプを以下から選択します。 「DynDNS」「D-Link DDNS」「FreeDNS」「NO-IP」「3322.org」「Custom」「Oray」		
User Name	DDNS のユーザ名を入力します。		
Password	DDNS のパスワードを入力します。		
Host Name	DDNS のホスト名を入力します。		
Туре	ホストの種類を指定します。		
Wildcards	ワイルドカードを許可します。		
Use external (NAT router's)	外部(NAT ルータ)の IP アドレスを指定します。		
IP address			
Force Update Interval	定期的な自動アップデート間隔(単位:日)を指定します。		
URL	DDNS のカスタム URL を指定します。		
Additional DDNS Options	追加の DDNS オプションを指定します。		
Oray UserType	Oray のユーザ名が表示されます。		
Oray Domain	Oray のドメインが表示されます。		
Traffic Management (トラフィック管理)

Network > Internet > Traffic Management

トラフィック管理の設定を行います。

Bandwidth Profiles(帯域幅プロファイル)

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。本機能は、コスト節減または帯域幅優先度の 割り当てを目的として、低優先度の LAN ユーザ(ゲストまたは HTTP サービスなど)が 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による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。その後、プロファ イルをトラフィックセレクタに関連付けることができます。これにより、セレクタと一致するトラフィックに対して帯域幅プロファイルが適用され ます。「セレクタ」とは、定義済みの帯域規則をトリガする、IP アドレスやサービスといった要素を意味します。

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

work » Internet » Traffic Management » Bandwidth Profiles Eandwidth Profiles Traffic Shaping Bridge Bandwidth Profiles Enable Bandwidth Profiles Enable Bandwidth Profiles Save Cancel Andwidth Profiles List Show 10 • entries [Right click on record to get more options] Name Bandwidth Rate / Priority AAA Low BBB Medium CCC High Showing 1 to 3 of 3 entries Add New Bandwidth Profile			🛜 Wireless	📮 Network	ଜ VPN	🔒 Security	💭 Maintenance	
Bandwidth Profiles Traffic Shaping Bridge Bandwidth Profiles Session Limiting Indwidth Profiles Enable Bandwidth Profiles Save Cancel andwidth Profiles List Show 10 • entries Right click on record to get more options] • Name Bandwidth Rate / Priority • AAA Low BBB Medium Ccc High Showing 1 to 3 of 3 entries Add New Bandwidth Profile	rork » Internet »	» Traffic Mana	gement » Bandw	idth Profiles				00
Add Midth Profiles Enable Bandwidth Profiles Enable Bandwidth Profiles andwidth Profiles List Show 10 entries [Right click on record to get more options] Name AAA Low BBB Medium CCC High Showing 1 to 3 of 3 entries Add New Bandwidth Profile	Bandwidth Profil	es Traffic !	Shaping Bridge	Bandwidth Profile	s Bridge Traffi	c Selectors Sessi	on Limiting	
Enable Bandwidth Profiles List andwidth Profiles List Show 10 entries [Right click record to get more options] Aname Bandwidth Rate / Priority AAA Low BBB Medium CCC High Showing 1 to 3 of 3 entries I like	dwidth Profiles	s						
AAA Low BBB Medium CCC High to 3 of 3 entries I to 3 ent	Enable Bandwidth	Profiles						
andwidth Profiles List Show 10 entries [Right click on record to get more options] Name Bandwidth Rate / Priority Image: Clark of the state				Sava	Cancel			
andwidth Profiles List Show 10 entries [Right click on record to get more options] Name Bandwidth Rate / Priority AAA Low BBB Medium CCC High Showing 1 to 3 of 3 entries Add New Bandwidth Profile				Jave	Calicer			
Show 10 entries [Right click on record to get more options] Name Image: Comparis and Comparison an								
Name Bandwidth Rate / Priority AAA Low BBB Medium CCC High Showing 1 to 3 of 3 entries Interview	indwidth Profile	s List						
AAA Low BBB Medium CCC High Showing 1 to 3 of 3 entries Add New Bandwidth Profile	indwidth Profile	es List ies [Right clic	sk on record to ge	t more options]				٩
BBB Medium CCC High Showing 1 to 3 of 3 entries I Next > Last >	ndwidth Profile how 10 ▼ entri Name	⊳s <i>List</i> ies [Right clic	ok on record to ge	t more options] ate / Priority				<u>م</u> 0
CCC High Showing 1 to 3 of 3 entries Add New Bandwidth Profile	ndwidth Profile how 10 • entri Name MAA	es List ies [Right click	bk on record to ge Bandwidth R Low	t more options] ate / Priority				<u>२</u> Ө
Showing 1 to 3 of 3 entries INext > Last > Add New Bandwidth Profile	nndwidth Profile how 10 ▼ entri Name MAA 38B	es List ies (Right clic) Bandwidth R Low Medium	t more options] ate / Priority				<u>२</u> Ә
Add New Bandwidth Profile	nndwidth Profile how 10 Tentri Name MAA 388 388 5000	es List ies [Right clic	k on record to ge Bandwidth R Low Medium High	t more options] ate / Priority				२) Ө
Add New Bandwidth Profile	Indwidth Profile how 10 • entri Name NAA 388 388 300 300 300 300 300 300	rs List ies (Right clic C	 k on record to ge Bandwidth R Low Medium High 	t more options] ate / Priority		[] Firs	t Previous 1 Next >	Q O Last X
	Indwidth Profile how 10 • entri Name AAA 388 388 5000 5000 howing 1 to 3 of 3 en	rs List ies [Right clic c	k on record to ge Bandwidth R Low Medium High	t more options] ate / Priority		∭ Firs	t J Previous 1 Next >	ع € Last)
	Indwidth Profile how 10 • entri Name MAA BBB CCCC howing 1 to 3 of 3 en Add New Bandy	es List ies [Right olid res ntries width Profile	k on record to ge Bandwidth R Low Medium High	t more options] ate / Priority		<u>(</u>) Firs	t / Previous 1 Next >	Q) Ø

図 5-30 Bandwidth Profiles > Bandwidth Profiles タブ画面

- 2. 帯域幅プロファイルを有効にする場合は、「Enable Bandwidth Profiles」を「ON」にします。
- 3. 「Save」をクリックし、設定を適用します。

Add New Bandwidth Profile(新しい帯域幅プロファイルの作成)

1. 「Add New Bandwidth Profile」をクリックして以下の画面を表示します。

Bandwidth Profile Configuration		X
Name Policy Type WAN Interface Profile Type Minimum Bandwidth Rate Maximum Bandwidth Rate	Outbound Image: 1 Dedicated WAN Image: 1 Rate Image: 1 (Range: 1 - Max Bandwidth) Kbps (Range: 100 - 1000000) Kbps	
	Save	

図 5-31 Bandwidth Profile Configuration 画面

2. 以下の項目を設定します。

項目	説明
Name	プロファイル名を入力します。
	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」(アウトバウンド)または「Inbound」(インバウンド)を選択します。
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。
Profile Type	「Priority」(優先度)または「Rate」(レート)を選択します。
Priority	「Profile Type」で「Priority」(優先度)を選択した場合、「Low」(低)、「Medium」(中)、「High」(高)から選択します。
Minimum / Maximum	「Profile Type」で「Rate」(レート)を選択した場合、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指定します。
Bandwidth Rate	

3. 「Save」をクリックし、設定を適用します。

追加した帯域幅プロファイルは、**Bandwidth Profiles > Bandwidth Profiles タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Traffic Shaping(トラフィックシェーピング)

作成したプロファイルは、LAN から WAN へのトラフィックフローに関連付けることができます。 トラフィックセレクタの設定により、帯域幅プロファイルに対して LAN トラフィックのタイプやソースの紐付けを行います。

1. Network > Internet > Traffic Management > Traffic Shaping タブの順にメニューをクリックし、以下の画面を表示します。

	🕋 Status		📮 Network	S VPN	🔒 Securit	/ 🗘 Maintenance	
Network »	Internet » Traffic I	Management » Traff	fic Shaping				00
Bandwie	dth Profiles Traf	fic Shaping Brid	ge Bandwidth Profile:	Bridge Traffic	: Selectors Se	ssion Limiting	
This page sho	ows a list of traffic	selectors. Traffic s	selectors are service b	ased rules to whic	ch user can atta	ch bandwidth profiles.	
Traffic Sel	ectors List						
	1000						
Show 10	• entries [Right c	lick on record to ge	t more options]				٩
Show 10	 entries [Right of Contract of	lick on record to ge	t more options] ch Type		⊖ Band	vidth Profile	<u>२</u> 0
Show 10 Service ANY	entries (Right of the second	ilick on record to ge	t more options] ch Type		e Band AAA	vidth Profile	<i>۹</i> 0
Show 10 Service ANY Showing 1 to	entries [Right c Tra IP 1 of 1 entries	ilick on record to ge	t more options] ch Type		- ⊖ Band AAA	width Profile	ع e

図 5-32 Traffic Management > Traffic Shaping タブ画面

Add New Traffic Selector(トラフィックセレクタの作成)

1. 「Add New Traffic Selector」をクリックし、以下の画面を表示します。

affic Selector Configuration		
Available Profiles	AAA	
ervice	ANY	
raffic Selector Match Type	IP V	
P Address		
ubnet Mask		

図 5-33 Traffic Selector Configuration 画面

2. 以下の項目を設定します。

項目	説明
Available Profiles	定義済みの帯域幅プロファイルを選択します。
Service	適用するサービスを選択します。
Traffic Selector Match	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)を定義します。
Туре	
IP Address	「Traffic Selector Match Type」に「IP」を選択した場合、プロファイルに紐付けるソース IP アドレスを入力します。
Subnet Mask	「Traffic Selector Match Type」に「IP」を選択した場合、サブネットマスクを入力します。
MAC Address	「Traffic Selector Match Type」に「MAC Address」を選択した場合、プロファイルに紐付けるソース 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、プロファイルに紐付けるポートを選択します。
VLAN	「Traffic Selector Match Type」に「VLAN」を選択した場合、プロファイルに紐付ける VLAN を選択します。

Bridge Bandwidth Profiles(ブリッジ帯域幅プロファイル)

本項目ではブリッジ帯域幅プロファイルの設定を行います。これらのプロファイルは「Bridge Traffic Selectors」の設定時に使用されます。 ブリッジトラフィックを制御することで、低優先値のユーザがブリッジ帯域幅を独占しないようにします。

注意
ブリッジ帯域幅プロファイル機能を使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

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

	» Traffic Management » E	Bridge Bandwidth Profiles				00
Bandwidth Prof	iles Traffic Shaping B	ridge Bandwidth Profile	es Bridge Traffi	c Selectors Sessi	on Limiting	
s page shows the I adwidth profiles yo dge bandwidth for idge Bandwidth	list of configured bridge ba ou can shape and regulate t cost-savings or bandwidth n Profiles	andwidth profiles. These p the bridge traffic. This is n-priority-allocation purp	profiles then can b useful to ensure t oses.	e used with the bridg that low priority user	ge traffic selectors. With rs do not monopolize the a	Bridge available
Enable Bridge Ba	andwidth Profiles	Save	Cancel			
Bridge Bandwidt.	h Profiles List					
Show 10 🔻 ent	tries [Right click on record	to get more options]				٩
Name	😔 🛛 Bridge Bandv	width Rate / Priority				÷
	Low					
AAA	entries			Firs	t Previous 1 Next >	Last 刘
AAA Showing 1 to 1 of 1 e						

図 5-34 Traffic Management > Bridge Bandwidth Profiles タブ画面

- 2. 帯域幅プロファイルを有効にする場合は、「Enable Bandwidth Profiles」を「ON」にします。
- 3. 「Save」をクリックし、設定を適用します。

Add New Bridge Bandwidth Profile(ブリッジ帯域幅プロファイルの追加)

1. 「Add New Bridge Bandwidth Profile」をクリックし、以下の画面を表示します。

Bridge Bandwidth Profile Configurat	ion 🛞
Name	
Policy Type	Outbound
Profile Type	Priority
Priority	Low

図 5-35 Bridge Bandwidth Profile Configuration 画面

2. 以下の項目を設定します。

項目	説明
Name	プロファイル名を入力します。
Policy Type	「Outbound」(アウトバウンド)または「Inbound」(インバウンド)を選択します。
Profile Type	「Priority」(優先度)または「Rate」(レート)を選択します。
Priority	「Profile Type」に「Priority」(優先度)を選択した場合、「Low」(低)、「Medium」(中)、「High」(高)から選択できます。
Minimum / Maximum	「Profile Type」に「Rate」(レート)を選択した場合、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指定します。
Bandwidth Rate	

3. 「Save」をクリックし、設定を適用します。

Bridge Traffic Selectors(ブリッジトラフィックセレクタ)

作成したブリッジ帯域幅プロファイルは、「LANPort-1」から「DMZ」へのトラフィックフローと関連づけることができます。 トラフィックセレクタの設定により、帯域幅プロファイルに対してブリッジトラフィックのタイプやソースの紐付けを行います。

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

	🕋 Status	🛜 Wireless	📃 Network	ର VPN	🔒 Seci	urity 🔷 🗢 Mair	ntenance
Network » I	Internet » Traffic M	lanagement » Brid	lge Traffic Selectors				0 0
Bandwid	ith Profiles Traf	fic Shaping Brid	ge Bandwidth Profile:	Bridge Traff	ic Selectors	Session Limiting	
This page sho static routes menu will sho associated w outbound tra Bridge Traf	wes the list of stati Be sure to enter w all available conf ith a traffic flow fr ffic to be regulated iffic Selectors Li	c routes configure a destination addr igured wired interf om the LANPort-1 d. st	d on the router. User c ess, subnet mask, gate faces on the router as a toDMZ. Bridge traffic s	an also add, dele way and metric f options. Once a l electors are elen	ete and edit th foreach config pridge bandwin nents like IP a	ne configured routes. ured static route. Th dth profile has been c ddresses or services	Use this page to define e Interface dropdown reated it can then be that require their
Show 10	• entries [Right c	lick on record to ge	et more options]				٩
Service	🗘 Traffi	c Selector Match	Туре	θ	Bridge Ban	dwidth Profile	θ
ANY	IP				AAA		
Showing 1 to	1 of 1 entries					First Previou	us 1 Next > Last >
Add New	Bridge Traffic Se	elector					

図 5-36 Traffic Management > Bridge Traffic Selectors タブ画面

Add New Bridge Traffic Selector(ブリッジトラフィックセレクタの作成)

1. 「Add New Bridge Traffic Selector」をクリックし、以下の画面を表示します。

Bridge Traffic Selector Configuration		8
Available Profiles	AAA	
Service	ANY	
Traffic Selector Match Type	IP 💌	
IP Address		
Subnet Mask		
		Save

図 5-37 Bridge Traffic Selector Configuration 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	定義済みの帯域幅プロファイルを選択します。
Service	適用するサービスを選択します。
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」または「MAC」)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。
IP Address	「Traffic Selector Match Type」に「IP」を選択した場合、プロファイルに紐付けるソース IP アドレスを入力します。
	「Traffic Selector Match Type」に「IP」を選択した場合、サブネットマスクを入力します。
MAC Address	「Traffic Selector Match Type」に「MAC Address」を選択した場合、プロファイルに紐付けるソース MAC アドレスを入力 します。

Session Limiting(セッション制限)

セッション制限画面では、設定したセッション制限プロファイルの一覧を表示します。セッションの制限は、IPアドレス、IPアドレス範囲、インタフェースごとに行うことができます。また、セッションが上限に達した際の警告メッセージも設定可能です。本設定にはプロファイル名、ソースタイプ、IPアドレス、最大セッション数などが含まれます。

1. Network > Internet > Traffic Management > Session Limiting タブの順にメニューをクリックし、以下の画面を表示します。

rork » Internet » Traffic Managen	ent » Session Limit		
Bandwidth Profiles Traffic Sha	oing Bridge Bandwidth Profiles Bridge Traffic	Selectors Session Limiting	
page shows the list of configured : interface.	ession limiting Profiles. It allows user to limit number	of sessions through the device per an IP/range of	
sion Limiting			
Warning Message	You have reached maximum number of permitted internet sessions. Please close one or more applications to allow further interne access. Contact system administrator for more information Characters left: 69 Save Cancel	* * 5	
ssion Limiting Profiles List	a record to get more entions 1		0
now 10 • entries [Right click o	n recora to get more options j		٩
Profile Name 🛛 O S	ource Type 🛛 🖯 Maximum Sessions((Per IP Address)	-
howing 0 to 0 of 0 entries		First Previous Next > Last	×
Add Session Limiting			

図 5-38 Traffic Management > Session Limiting タブ画面

Warning Message(警告メッセージ)の設定

1. 「Warning Message」を入力します。

∀arning Message	You have reached maximum number of permitted internet sessions. Please close one or more applications to allow further internet access. Contact system administrator for	
	Characters left: 65	
	Save Cancel	

図 5-39 Warning Message 画面

Add Session Limiting(セッション制限の追加)

1. 「Add Session Limiting」をクリックし、以下の画面を表示します。

Session Limiting Configuration		×
Profile Name Source Type		
Maximum Sessions Enable Schedules	100 [Range: 1 - 999]	
	Save	

図 5-40 Session Limiting Configuration 画面

2. 以下の項目を設定します。

項目	説明
Profile Name	特定のソースタイプに適用するプロファイル名を入力します。
Source Type	プロファイルのソースタイプを「IP」「Range」「Interface」から指定します。
IP Address	「Source Type」に「IP」を選択した場合、セッション制限プロファイルで制御されるクライアント / ホストの IP アドレス を入力します。
Start IP Address	「Source Type」に「Range」を選択した場合、セッション制限プロファイルで制御されるクライアントの IP アドレス範囲の開始 IP アドレスを入力します。
End IP Address	「Source Type」に「Range」を選択した場合、セッション制限プロファイルで制御されるクライアントの IP アドレス範囲の終了 IP アドレスを入力します。
Interface	「Source Type」に「Interface」を選択した場合、セッション制限プロファイルで制御されるネットワークのインタフェースを選択します。
Maximum Sessions	「Souce Type」に対し許可される最大セッション数を指定します。セッション数の上限に達すると、セッション制限プロファイル におけるいかなる種類のセッション / トラフィックも受け付けません。 ・ 設定可能範囲:1-999
Enable Schedules	スケジュールを有効化して、セッション制限プロファイルを特定の曜日や時間帯などに適用するように設定します。
Schedule Profile	セッション制限プロファイルに紐付けるスケジュールプロファイルを選択します。

Jumbo Frames (ジャンボフレーム設定)

Network > Internet > Jumbo Frames

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フレームレートで情報を交換することができます。

注意
ジャンボフレームを使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

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

🖾 Statu	s 🛜 Wirel	ess 📮 Network	CA VPN	Security	O° Maintenance	
twork » LAN » Jumb	o Frame					00
is page allows user to ffic containing Jumbo	enable/disable juml Frames on LAN side	o frames and set MTU for Devices.	jumbo frames in the	router.Jumbo Frames	option is available to exch	ange
mbo Frame						
Activate Jumbo Fra	mes					
		Save	Cancel			

図 5-41 Jumbo Frame 画面

2. 以下の項目を設定します。

項目	説明
Activate Jumbo Frames	「ON」にしてジャンボフレームを有効にします。

Routing (ルーティング設定)

Network > Routing

ルーティングの設定を行います。

Static Routes (スタティックルート)

Network > Routing > Static Routes

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。 本ルータに手動でスタティックルートを追加することにより、異なるインタフェース間のトラフィック経路の選択を定義できます。本ルータと他の デバイス間で、経路の変更を説明するための通信はありません。ルートが設定されると、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 ティブで有効となります。

1. Network > Routing > Static 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。

etwork » Routing » Static Routes his page shows the list of static routes configured on the router. User can also add, delete and edit the configured routes.Use this page to atic routes. Be sure to enter a destination address, subnet mask, gateway and metric for each configured static route. The Interface drop enu will show all available configured wired interfaces on the router as options. tatic Routes List Show 10 • entries [Right click on record to get more options] Name ① Destination ④ Subnet Mask ④ Gateway ④ Interface ④ Metric ④ Active ④ Privat No data available in table Showing 0 to 0 of 0 entries	🖾 Stat	us 🋜	Wireless	<u>п</u>	letwork	ക	VPN	🔒 Se	curity	0	• Main	tenan	ice	
his page shows the list of static routes configured on the router. User can also add, delete and edit the configured routes.Use this page to attic routes. Be sure to enter a destination address, subnet mask, gateway and metric for each configured static route. The Interface drop enu will show all available configured wired interfaces on the router as options. tatic Routes List Show 10	etwork » Routing » :	Static Routes											2	e
10 → entries [Right click on record to get more options] Name O Destination O Subnet Mask O Gateway O Interface O Metric O Active O Private No data available in table No data available in table Interface O Metric O Active O Private Showing 0 to 0 of 0 entries Image: Click of the state	is page shows the lis atic routes. Be sure enu will show all avail catic Routes List	t of static rou to enter a des able configure	ites configured itination addres ed wired interfa	on the ro s, subnet aces on th	uter. User car mask, gateway ie router as op	n also a y and m otions.	dd, delete an etric for eacl	id edit t h config	the config ured stat	gured ro ic route	utes.Us . The In	e this iterfac	page to d ce dropdo	efin wn
Name O Destination	how 10 💌 entries	[Right c	click on record to	get more o	options]							1 1 1 1		٩
No data available in table	Name 🕜 Destin	ation \varTheta	Subnet Mas	k ⊖	Gateway	⊜	Interface	⇔	Metric	⊖ A	ctive	⊜	Private	8
ihowing 0 to 0 of 0 entries					No data availa	able in ta	ible							
	Showing 0 to 0 of 0 entrie	25								First	Previo	us Ne	ext > La	t)
Add New Static Route	Add Now Static D													

図 5-42 Static Routes 画面

Add New Static Route(スタティックルートの追加)

1. 「Add New Static Route」をクリックして以下の画面を表示します。

Static Route Configuration		
Route Name Active Private Destination IP Address IP Subnet Mask Interface Gateway IP Address Metric	OFF OFF Dedicated WAN Image: 2 -15]	
		Save

図 5-43 Static Route Configuration 画面

2. 以下の項目を設定します。

項目	説明
Route Name	ルート名を入力します。
Active	「ON」にしてルートを有効、または「OFF」にして無効にします。
Private	「ON」にしてルートを「プライベート」に設定します。「プライベート」に設定した場合、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。
Destination IP Address	ルートの宛先 IP アドレスを指定します。
IP Subnet Mask	ルートのサブネットマスクを指定します。
Interface	物理ネットワークインタフェースを指定します。このインタフェースを介して本ルートがアクセス可能になります。
Gateway IP Address	ゲートウェイの IP アドレスを指定します。このゲートウェイを介して宛先ホストまたはネットワークに到達することがで
	きます。
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」をクリックし、設定を適用します。

RIP (RIP 設定)

Network > Routing > RIP

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。 RIP を使用すると、LAN 内の他のルータとルーティング情報を交換できます。

また、動的なルーティングテーブルの更新を行い、トラフィックフローを中断せずに LAN 内の変更を適用することができます。

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

🖾 Status	🛜 Wireless	📃 Network	A VPN	Security	O Maintenance	
Network » Routing » RIP						0 0
This page allows to configure	the RIP (Routing Info	mation Protocol).				
RIP						
RIP Setup						
Direction		None O In Only	Out Only	© Both		
Version		RIP-1	•			
		Save	ancol			
	0	Jave	Jancer			

図 5-44 RIP 画面

2. 以下の項目を設定します。

項目	説明
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」: ルータは自身のルーティングテーブルをブロードキャストし、また、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。RIP は実質的に無効になります。
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 が無効化されている場合に設定します。 「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。
	3. RIP-2B または RIP-2M を選択した場合、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。LAN 上で検出されたルータとのルーティング情 報交換が確実に行われるように、認証キーの有効期間を設定できます。

OSPF (OSPF 設定)

Network > Routing > OSPF

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 IGP (Interior Gateway Protocols) です。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。OSPFv2 は、RFC2328-OSPF バージョン 2 に記述されているルーティ ングプロトコルです。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ています。

1. Network > 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。

	Status Sta	🛜 Wireless	🖳 🖳 Netwo	rk 🕼 VPN			O° Maintenanc	
letwork » This page sl DSPFv2 L	Routing » OSPF hows the OSPFv2 paramet ist	ers configured	d on the router.User	can also edit the O	SPFv2 cor	figured paramete	rs.	00
Show 10	entries [Right click o	n record to get	more options]					٩
Status 🗘	Port \varTheta Area Ə	Priority ⊖	Hello Interval ↔	Dead Interval ⊖	Cost⊖	Authentication Type	D ⊖ LAN Ro Exchar	ute o
Disabled	LAN	1	10	40	10	None	N/A	
Disabled	WAN1	1	10	40	10	None	Enabled	
Disabled Disabled	WAN1 WAN2	1	10 10	40 40	10 10	None None	Enabled	
Disabled Disabled Disabled	WAN1 WAN2 WAN3	1 1 1	10 10 10	40 40 40	10 10 10	None None None	Enabled Enabled Enabled	

図 5-45 OSPFv2 Configuration 画面

2. 変更するインタフェース (LAN/WAN1/WAN2/WAN3/L2TPoverIPSEC) で右クリック → 「Edit」を選択し、以下の画面を表示します。

OSPFv2 Configuration			\bigotimes
OSPFv2 Enable	ON 111)	^
Interface	WAN1		
Area		[Range: 0 - 200]	
Priority	1	[Default:1, Range: 0 - 255]	
Hello Interval	10	[Default:10, Range: 1 - 65535]	
Dead Interval	40	[Default:40, Range: 1 - 65535]	
Cost	10	[Default:10, Range: 1 - 65535]	
Authentication Type	MD5		
MD5 Key ID		[Range: 1 - 255]	
MD5 Authentication Key			
LAN Route Exchange	ON		
NSSA	OFF		~
			Save

図 5-46 OSPFv2 Configuration 画面

3. 以下の項目を設定します。

項目	説明
OSPFv2 Enable	OSPF を有効にします。
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を表示します。
Area	インタフェースが所属するエリアを入力します。2つのルータが共通のセグメントを持っている場合、インタフェース はセグメント同じエリアに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	ネットワークにおける OSPFv2 代表ルータの選出に使用されます。高い優先度を持つルータが、代表ルータとして、より適格であるとみなされます。値を0に設定すると、ルータは代表ルータとして不適格となります。低い番号ほど高い 優先度を意味します。 ・ 初期値:1
Hello Interval	Hello インターバルタイマの値(秒)を入力します。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:10(秒)
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)を入力します。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。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。 ・ 初期値:40(秒)
Cost	OSPFv2 インタフェースでパケットを送信するコストを入力します。
Authentication Type	OSPFv2 に使用する認証タイプを選択します。 ・「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」を選択した場合、認証キーを入力します。
MD5 Key ID	認証タイプに「MD5」を選択した場合、MD5 キー ID を入力します。
MD5 Authentication Key	認証タイプに「MD5」を選択した場合、MD5 認証キーを入力します。
LAN Route Exchange	WAN/LAN インタフェース上で LAN/WAN 経路情報の交換を行います。
NSSA	NSSA を ON または OFF に設定します。

4. 「Save」をクリックし、設定を適用します。

L2TP over IPsec でサポートされる OSPF

LAN/WAN1/WAN2 の他に、L2TP over OSPF を使用してルートの変更を行うことができます。OSPF では L2TP over IPsec チャンネルで作成された仮 想インタフェースがサポートされています。追加されたスタティックルートはそれらのインタフェースで交換される必要があります。 L2TP over IPsec では IPsec におけるデータリンク層をカプセル化します。プレーンな IPsec では単にネットワークレイヤの暗号化のみ行います。 L2TP over IPsec の設定が保存された後、トンネルイニシエーションが自動的に開始されますが、トンネルの確立はクライアント側とサーバ側の設定 及びサーバの応答に依存します。OSPF を有効化する前に、IPsec 上の L2TP トンネルが確立されていることを確認してください。

Protocol Binding(プロトコルバインディング)

Network > Routing > Protocol Binding

IP/MAC バインドルールの表示とルールの設定を行います。

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。設定済みサービスまたはユーザ定義サービスのリストから選択して、 利用可能な WAN ポートの1つだけを通過するように、トラフィックの種類を割り当てることができます。柔軟性を高めるため、送信元のネットワー ク/端末と送信先のネットワーク/端末を指定できます。たとえば、ある LAN IP アドレスへの VoIP トラフィックを1つの WAN に割り当て、残りの IP アドレスからの VoIP トラフィックをもう1つの WAN リンクに割り当てることができます。

プロトコルバインディングは、ロードバランシングモードが有効で、複数の WAN が設定されている場合にのみ適用できます。

1. Network > Routing > Protocol 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。

() ()	🙆 Status	🛜 Wireless	📃 Networ	k 🕼 VPN	🔒 Secu	rity 🗘 🍄 Maintenanc	e
Network	» Routing » Protocol	l Binding					0 0
This pag required service t Protoco Show 1	e shows the configure when the Load Balan to a particular Option ol Bindings List	ed protocol bindin icing feature is in link to ensure the Right click on recor	gs. A user can also a use, and are only ap a high priority servic d to get more options]	dd, delete, edit, enab Jlicable when two Op es are sent to the mo	le or disable th tion links are co re reliable or le	e protocol bindings.Protocol I nfigured. This feature lets yo ss expensive ISP.	oindings are u assign a
Status	Service	⊖ Local Ga	teway A	Source Network	A	Destination Network	
			No d	ata available in table			
Showing	0 to 0 of 0 entries					H First H Previous Nex	t > Last >
Add	New Protocol Bindir	ng					

図 5-47 Protocol Binding 画面

2. プロトコルバインディングを追加する場合は、「Add New Protocol Binding」をクリックし以下の画面を表示します。

Protocol Bindings Configurat	ion	×
Service	ANY	
Local Gateway	● WAN1 ◎ WAN2 ◎ WAN3	
Source Network	Any Single Address Address range	
Start Address		
End Address		
Destination Network	O Any O Single Address O Address range	
Start Address		

図 5-48 Protocol Bindings Configuration 画面

3. 以下の項目を設定します。

項目	説明
Service	プロトコルバインディングを設定するサービスを選択します。
Local Gateway	WAN インタフェースを選択します。
Source Network	送信元ネットワークとして以下のいずれかを選択します。 ・「Any」:ネットワークの指定は不要です。
	 「Single Address」: 1 台のコンピュータを指定します。 「Address range」: IP アドレス範囲を指定します。
Destination Network	送信先ネットワークとして以下のいずれかを選択します。「Single Address」「Addres Range」を選択した場合は IP アドレス /IP ア ドレス範囲を指定します。 ・「Any」:ネットワークの指定は不要です。 ・「Single Address」: 1 台のコンピュータに制限します。 ・「Address range」: IP アドレス範囲を指定します。

4. 「Save」をクリックし、設定を適用します。

追加したプロトコルバインディングは、Protocol Bindings 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

IPv6 (IPv6 ネットワーク設定)

Network > IPv6

ここでは IPv6 の関連する LAN 設定を行います。

IP Mode (IP モード設定)

Network > IPv6 > IP Mode

本項目では使用する IP プロトコルのバージョンを設定します。お使いのネットワークで IPv6 を使用する場合、「IPv4 & IPv6」モードに指定する必要 があります。このモードに設定すると、本ルータを通して IPv4 ノードと IPv6 デバイスの通信が可能になります。

1. Network > 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。

🖾 Status	🛜 Wireless	📃 Network	A VPN	Security	🌮 Maintenance
letwork » IPv6 » IP Mode his page allows user to co e in IPv4 / IPv6 mode. This P Mode	nfigure the IP protocol ; mode will allow IPv4 nc	version to be used on des to communicate v	the router.In orde vith IPv6 devices th	r to support IPv6 on 1 rough this router.	the LAN, you must set the router
IP Mode		© IPv4 Only ● IP• Save	v4 & IPv6 Cancel		

図 5-49 IP Mode 画面

- 2. 「IPv4」または「IPv4&IPv6」をチェックします。
- 3. 「Save」をクリックし、設定を適用します。
- 注意 IP モードの設定変更を行うと本製品は再起動します。電源を切らずそのままお待ちください。IP モードの設定変更は、 VLAN 設定画面(Network > VLAN > VLAN Settings)の設定項目に影響します。

IPv6 Wan1 Settings (IPv6 ネットワークにおける WAN1 設定)

Network > IPv6 > IPv6 Wan1 Settings

本ルータは、スタティック IPv6 アドレスを設定する、または DHCPv6 クライアントとして接続情報を受信することによって、IPv6 WAN に接続でき ます。インターネット接続用に ISP から固定のアドレスを付与されている場合、スタティック IP アドレスの設定を完了させる必要があります。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なります。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 を介した WAN IP 設定の取得が ISP から許可されている場合、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 クライアントは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ている場合、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 側の DHCPv6 サーバは不要であり、このゲー トウェイから ICMPv6 検出メッセージが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ことも可能です。

1. Network > IPv6 > IPv6 Wan1 Settings の順にメニューをクリックします。「Connection Type」で選択する接続タイプにより表示される画面が異な ります。

	🝘 Status	🛜 Wireless	📮 Network	r vpn	盈 Security	🗢 Maintenance	
Network » II	Þνó » IPνó Wan1 Set	ttings					0 0
This page all configured a stateful. If a be a DHCPv6 IPv6 Wan1	ows user to IPv6 re s a DHCPv6 client o stateful client is s server available at Settings	lated WAN1 configura r connect to ISP usir elected the gateway the ISP, rather ICMPv	tions. This router car g username and pass will connect to the I 6 discover messages	n have a static IPv word (PPPoE). The SP's DHCPv6 serve will originate from	6 address or receive 9 DHCPv6 client on th r for a leased addres 9 this gateway and wi	connection information ne gateway can be either s. For stateless DHCP the ill be used for auto confi	when stateless or re need not guration.
IP∨6 WAN	1 Setup						
Connect	ion Type	C	HCPv6	•			
DHCPv6							
DHC Pv6	Auto Configuration	. @	🖲 Stateless Address	○ Stateful Add	ress		
Prefix D	elegation		OFF				
			Save	Cancel			

図 5-50 IPv6 Wan1 Settings (DHCPv6) 画面

🐼 Status 🛜 V	Wireless 📃 Network	ക vpn	💂 Security	🗢 Maintenance	
Network » IPv6 » IPv6 Wan1 Settings					0 0
This page allows user to IPv6 related WAM configured as a DHCPv6 client or connect stateful. If a stateful client is selected to be a DHCPv6 server available at the ISP, r IPv6 Wan1 Settings	11 configurations.This router ca : to ISP using username and pas: ne gateway will connect to the ather ICMPv6 discover messages	n have a static IPv6 : sword (PPPoE). The D ISP's DHCPv6 server f will originate from t	address or receive OHCPv6 client on th for a leased address this gateway and wil	connection information of e gateway can be either . For stateless DHCP the Il be used for auto confi	when stateless or re need not guration.
IPv6 WAN1 Setup					
Connection Type	Static	T			
Static					
IPv6 Address					
IPv6 Prefix Length	[Default:	64, Range: 1 - 128]			
Default IPv6 Gateway					
Primary DNS Server					
Secondary DNS Server					
	Save	Cancel			

図 5-51 IPv6 Wan1 Settings (Static) 画面

😰 Status	🛜 Wireless	📮 Network	A VPN	Security	O Maintenance	
Network » IPv6 » IPv6 Wan1 Se	ttings					00
This page allows user to IPv6 rei as a DHCPv6 client or connect to stateful client is selected the g server available at the ISP, rath IPv6 Wan1 Settings	lated WAN1 configurati o ISP using username ar ateway will connect to er ICMPv6 discover mes	ons.This router can d password (PPPoE the ISP's DHCPv6 se sages will originate	have a static IPv6). The DHCPv6 clie erver for a leased a e from this gatewa	address or receive co nt on the gateway ca ddress. For stateless y and will be used for	onnection information whe n be either stateless or sta DHCP there need not be a auto configuration.	n configured ateful. If a DHCPv6
IPv6 WAN1 Setup						
Connection Type	PF	PoE	\checkmark			
PPPOE Sessions	۲	Separate Session f	for IPv6 O Com	mon Session for IPv4 a	and IPv6	
PPPoE						
User Name						
Password						
Authentication Type	Au	to-negotiate	\checkmark			
DHCPv6 Options	Dis	able DHCPv6	~			
Primary DNS Server						
Secondary DNS Server						
		Save	Cancel			

図 5-52 IPv6 Wan1 Settings (PPPoE) 画面

2. 以下の項目を設定します。

項目	説明
	IPv6 WAN 1 Setup
Connection Type	接続タイプを以下から選択します。 ・「DHCPv6」 ・「Static」 ・「PPPoE」
	DHCPv6
DHCPv6 Auto Configuration	「Stateless Address 」または「Stateful Address」を選択します。
Prefix Delegation	ルーター広告プレフィックスを要求するには、このオプションを選択します。取得されたプレフィックスは、 LAN 側で広告されたプレフィックスに更新されます。 このオプションは、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できます。
	Static
IPv6 Address	ISP から提供された IP アドレスを指定します。
IPv6 Prefix Length	ISP から提供された IPv6 プレフィックス長を指定します。
Default IPv6 Gateway	ISP から提供された IPv6 ゲートウェイのアドレスを指定します。
Primary DNS Server	プライマリ DNS サーバの IP アドレスを指定します。
Secondary DNS Server	セカンダリ DNS サーバの IP アドレスを指定します。
	PPPoE
PPPoE Sessions	「Separate sessions for IPv6」または「Common sessions for IPv4 and IPv6」を選択します。 ・「Separate Session for IPv6」:IPv4/IPV6 の個別 PPPoE セッションを処理します。 ・「Common Session for IPV4 and IPv6」:IPv4/IPV6 の共有 PPPoE セッションを処理します。
User Name	PPPoE ユーザ名を入力します。
Password	PPPoE 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を以下から選択します。 「Auto-negotiate」「PAP」「CHAP」「MS-CHAP」「MS-CHAPv2」
DHCPv6 Options	DHCPv6 クライアントが開始されるモードを以下から選択します。 「Disable DHCPv6」「Stateless DHCPv6」「Stateful DHCPv6」「Stateless dhcpv6 with Prefix delegation」 「Statelfull dhcpv6 with Prefix delegation」
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 サーバの IP アドレスを入力します。

IPv6 Wan2 Settings (IPv6 ネットワークにおける WAN2 設定)

Network > IPv6 > IPv6 Wan2 Settings

本項目では IPv6 に関する WAN2 設定を行うことができます。

注意	「IPv6 Wan2 Settings」の設定項目は、	「IPv6 Wan1 Settings」と同等です。
	設定項目については「WAN1 Settings	(WAN1 設定)」を参照してください。

Static Routing (IPv6 スタティックルーティング設定)

Network > IPv6 > Static Routing

ルータに設定済みのスタティックルートのリストが表示されます。また、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、特定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。本ルータと他のデバイス間で、経路の変更を構成するため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有効となります。

スタティックルートの一覧には、管理者によって手動で追加されたすべてのルートが表示されます。

1. Network > 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。

	🖾 Status	🛜 Wireless	📮 Network	4	B VPN	🔒 Secur	ity 4	Maintenance	
Network >	» IPv6 » Static Rout	ing							00
This page	shows a list of IPv6	static routes added. A	A user can add, delete	e and (edit the routes	s also.			
IPv6 Sta	tic Routing List								
Show 10	▼ entries	[Right click on record to	get more options]						٩
Name	Destina	tion Θ	Gateway	⊜	Interface	⇔	Metric	⊖ Active	⊜
			No data a	vailable	in table				
Showing () to 0 of 0 entries						First	Previous Next >	Last 刘
6		_							
Add N	lew IPv6 Static Ro	ute							

図 5-53 Static Routing 画面

2. IPv6 スタティックルートを追加する場合、「Add New IPv6 Static Route」をクリックし以下の画面を表示します。

Pv6 Static Routing Configura	ion	X
Route Name		
Active	OFF	
IPv6 Destination		
IPv6 Prefix Length	[Range: 0 - 128]	
Interface	WAN1 Osit0 Tunnel-WAN1 OLAN	
	O WAN2 Osit0 Tunnel-WAN2	
IPv6 Gateway		
Metric	[Range: 2 - 15]	

図 5-54 IPv6 Static Routing Configuration 画面

3. 以下の項目を設定します。

項目	説明
Route Name	ルート名を入力します。
Active	「ON」:スタティックルートを有効にします。
	「OFF」:スタティックルートを無効にします。
IPv6 Destination	スタティックルートの宛先 IPv6 アドレスを指定します。
IPv6 Prefix Length	スタティックルートの 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 を以下から選択します。
	「WAN1」「sit0 Tunnel-WAN1」「LAN」「WAN2」「sit0 Tunnel-WAN2」
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 アドレスを指定します。
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。

4. 「Save」をクリックし、設定を適用します。

追加したスタティックルートは、Static Routing 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

OSPFv3 (OSPFv3 設定)

Network > IPv6 > OSPFv3

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。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。

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. Network > IPv6 > OSPFv3 の順にメニューをクリックし、以下の画面を表示します。

ter.User can also edit the O cribed in RFC2740.OSPF is a th RIP, OSPF can provide sca s]	SPFv3 configured parameters.OSI in IGP (Interior Gateway Protocol alable network support and faster	PF(Open Shortest Path First)) used to distribute routing r convergence times.OSPF can
ter.User can also edit the O cribed in RFC2740.OSPF is a th RIP, OSPF can provide sca s]	SPFv3 configured parameters.OS in IGP (Interior Gateway Protocol alable network support and faster interior for the support of the support interior for the support of the support interior for the support of the support interior for the support	PF(Open Shortest Path First)) used to distribute routing r convergence times.OSPF can
[2		4
	The second second second second second second	
Hello Interval	😌 Dead Interval	⊖ Cost €
10	40	10
10	40	10
10	40	10
	10	10 40

図 5-55 OSPFv3 画面

2. 変更するインタフェース (LAN/WAN1/WAN2) で右クリックし、「Edit」をクリックします。以下の画面が表示されます。

OSPFv3 Configuration			×
OSPFv3 Enable	ON THE		
Interface	WAN1		
Priority	1	[Default:1, Range: 0 - 255]	
Hello Interval	10	[Default:10, Range: 1 - 65535]	
Dead Interval	40	[Default:40, Range: 1 - 65535]	
Cost	10	[Default:10, Range: 1 - 65535]	

図 5-56 OSPFv3 Configuration 画面

3. 以下の項目を設定します。

項目	説明
OSPFv3 Enable	OSPFv3 を「ON」または「OFF」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が表示されます。
Priority	ネットワークの OSPFv3 代表ルータの決定に使用されます。高い優先度を持つルータが、より代表ルータとして適格であるとみなされます。値を0に設定すると、ルータは代表ルータとして不適格となります。低い番号ほど高い優先度を意味します。 ・ 初期値:1
Hello Interval	Hello インターバルタイマの値(秒)を入力します。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:10(秒)
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)を指定します。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。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。 ・ 初期値:40(秒)
Cost	OSPFv3 インタフェースでパケットを送信するコストを指定します。

6 to 4 Tunneling (6 to 4 トンネル設定)

Network > IPv6 > 6 to 4 Tunneling

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 トンネリング機能は、IPv4 を IPv6 に移行するためのインターネット移行メカニズムです。IPv6 パケットの IPv4 ネットワークへの転送を可能 にします。本画面では「Activate Auto Tunneling」を有効にし、IPv6 LAN からのトラフィックを IPv4 オプションでリモート IPv6 ネットワークに到 達するように設定できます。

1. Network > 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。

	🖾 Status	🛜 Wireless	📃 Network	a vpn	Security	O Maintenance
letwork This page AN. This Pv6 to	» IPv6 » 6 to 4 Tunn allows user to enab option is very comm IPv4 Tunneling	le/disable the 6 to 4 t ion in network that us	unneling.With this op1 e both IPv4 and IPv6 n	tion enabled IPv4 ac odes.	Idress information is	embedded in IPv6 addresses on ti
Acti	vate Auto Tunneling	1	on m Save	Cancel		

図 5-57 6 to 4 Tunneling 画面

- 2. 6 to 4 トンネルを有効にする場合は、「Activate Auto Tunneling」を「ON」にします。
- 3. 「Save」をクリックし、設定を適用します。

ISATAP Tunnels(ISATAP トンネル設定)

Network > IPv6 > ISATAP Tunnels

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で 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 の操作を決定します。

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。

1. Network > 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。

	A Status	🛜 Wireless	💂 Netw	vork 🕼 VPN	Security	O ^o Maintenance	
Network >	» IPv6 » ISATAP Tun	nels					0
This page connectiv	shows the list of av ity between IPv6 no	ailable ISATAP tunnels. des within the LAN, as	A user can als it treats the I	so add, delete and edit IS IPv4 network as a single II	ATAP tunnels from thi Pv6 local link.	s page.ISATAP is available to	provide
ISATAP	Tunnels List						
Show 10	entries	[Right click on record to	get more option	ns]			٩
Local E	ndpoint		<u>ن</u> ا	SATAP Subnet Prefix			⇔
			No	o data available in table			
Showing (0 to 0 of 0 entries					First V Previous Next >	Last 刘
Add N	lew ISATAP Tunne	el					

図 5-58 ISATAP Tunnels 画面

第5章 ネットワーク設定(Network)

2. ISATAP トンネルを追加する場合は、「Add New ISATAP Tunnel」をクリックして以下の画面を表示します。

ATAP Tunnels Configuratio	n	(
ISATAP Subnet Prefix End Point Address	O LAN Other IP	
IPv4 Address		
		Sava

図 5-59 ISATAP Tunnels Configuration 画面

3. 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 ISATAP 論理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 を元に設定します。
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 です(LAN が IPv4 ネットワークであると想定)。 ・「Other IP」:特定の LAN IPv4 アドレスを指定します。
IPv4 Address	エンドポイントアドレスで「Other IP」を指定した場合、ローカルのエンドポイントアドレスを指定します。

4. 「Save」をクリックし、設定を適用します。

追加した ISATAP トンネルは ISATAP Tunnels 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Teredo Tunnel (Teredo トンネル設定)

Network > IPv6 > Teredo Tunnel

Teredo トンネルの設定をします。

「Teredo Tunnelling」を有効にすると、所属するネットワークにおいて IPv6 接続のない IPv6 が有効なホストに対して IPv6 接続を提供します。

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

🝘 Status	🛜 Wireless	📮 Network	r VPN	Security	O Maintenance	
Network » IPv6 » Tereod Tunnel						00
Teredo Tunnelling						
Activate Teredo Tunnelling Primary Server Secondary Server	te	redo-deblan.remlab.n redo.lpv6.microsoft.c Save	et om Cancel			

図 5-60 Teredo Tunnelling 画面

- 2. 「Activate Teredo Tunnelling」を「ON」に指定します。
- 3. 以下の項目を設定します。

項目	説明
Primary Server /	Teredo サーバのプライマリ / セカンダリサーバを指定します。
Secondary Server	

^{4. 「}Save」をクリックし、設定を適用します。

IPv6 LAN Settings(IPv6 LAN 設定)

Network > IPv6 > IPv6 LAN Settings

本項目では IPv6 に関する LAN 設定を行います。

IPv6 LAN Settings(IPv6 LAN 設定)

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。本機能を有効にすると、DHCPv6 サーバによって、LAN に割り当てられたプレフィックス長とともに設定済みアドレスプールから IPv6 アドレスが提供されます。

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は、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。

1. Network > IPv6 > IPv6 LAN Settings > IPv6 LAN Settings タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🛜 Wirele	ss 📮 Network	ക VPN	🚨 Security	🗢 Maintenance	
Network » IPvó » IPvó LAN Settings					00
IPv6 LAN Settings IPv6 Address Pools	Prefixes for Prefix Delegat	ion Router Adv	ertisement Adve	rtisement Prefixes	
This page allows user to IPv6 related LAN confi common among all LAN hosts. Changes here affi will require all LAN hosts to be in the same net IPv6 LAN Settings	gurations.The IPv6 address is sot all devices connected to work prefix and use the new	128 bits, with a c the router's LAN address to acces	default 64 bit prefix switch. Note that : ss this GUI.	that defines the netwo a change to the defaul L	rk and is AN IP address
LAN TCP/IP Setup					
IPv6 Address	fec0::1				
IPv6 Prefix Length	64 [Range: 0 - 12	28]			
DHCPv6					
Status	ON				
Mode	🖲 Stateless 🛛 🔍 Statef	ful			
Domain Name	dlink.com				
Server Preference	255 [Range: 0 - 2	55]			
DNS Servers	Use DNS Proxy	•			
Lease / Rebind Time	86400 [Range: 0 - 6	04800] Seconds			
Prefix Delegation	OFF				
	Save Ca	ancel			

図 5-61 IPv6 LAN Settings > IPv6 LAN Settings タブ画面

2. 以下の項目を設定します。

項目	説明
	LAN TCP/IP Setup
IPv6 Address	ルータの IPv6 アドレスを入力します。
IPv6 Prefix Length	IPv6 プリフィクス長を入力します。
	DHCPv6
Status	DHCPv6 機能を有効にします。有効にすると以下の項目が指定できます。
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ため、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: 255
DNS Servers	 「Use Below」: DNS サーバの詳細を手動で設定します。(Primary/Secondary DNS Server オプション) 「Use DNS from ISP」: LAN DHCP クライアントは、ISP から直接 DNS サーバの詳細を受信します。 「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)
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 委任を有効にします。 本項目は、DHCPv6 の「Mode」を「Stateless」に設定した場合のみ表示されます。

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 委任プレフィックスを定義できます。委任プレフィックスを 使用すると、LAN 内の他のネットワーク装置に対して、割り当てられたプレフィックス固有の DHCP 情報を通知する処理を自動化できます。

1. Network > IPv6 > IPv6 LAN Settings > IPv6 Address Pools タブの順にメニューをクリックし、以下の画面を表示します。

	🕋 Status	🛜 Wireless	💻 Netwo	rk 🟠 VPN	Security	O Maintenance	
Network » IF	∿6 » IPv6 LAN Sett	ings » IPv6 Address Poo	ıls				0 0
IPv6 LAN	I Settings IPv6 A	ddress Pools Prefix	es for Prefix D	elegation Router	Advertisement Ad	vertisement Prefixes	
This Page allo	ow user to create/a	add/delete/edit Addres	s Pools List for	IPv6 configuration.			
IPv6 Addre	ss Pools List						
Show 10	✓ entries [Right cl	lick on record to get mor	e options]				0
							~
Start Addr	ess 🤇	End Address	⊖ Pre	fix Length	⊖ Interface	⊖ IPv6 Status	•
Start Addr	ess 🤇	End Address		fix Length ata available in table	⊖ Interface	⊖ IPv6 Status	÷
Showing 0 to 0	ess C	End Address	⊖ Pre No d	r <mark>fix Length</mark> ata available in table	⊖ Interface	IPv6 Status First Previous Next	e X Last X

図 5-62 IPv6 LAN Settings > IPv6 Address Pools タブ画面

2. アドレスプールを追加する場合は、「Add New Address Pool」をクリックし以下の画面を表示します。

IPv6 Address Pools Configuration		8
Start IPv6 Address End IPv6 Address Prefix Length VLAN Interface	[Range: 1 - 128]	
		Save

図 5-63 IPv6 Address Pools Configuration 画面

3. 以下の項目を設定します。

項目	説明
Start IPv6 Address	開始 IPv6 LAN アドレスを入力します。
End IPv6 Address	終了 IPv6 LAN アドレスを入力します。
Prefix Length	プレフィックス長を入力します。
VLAN Interface	VLAN インタフェースを指定します。

4. 「Save」をクリックし、設定を適用します。

追加した IPv6 プールは、**IPv6 LAN Settings > IPv6 Address Pools タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Prefixes for Prefix Delegation (IPv6 プレフィックス委任)

IPv6 プレフィックス長の追加 / 編集 / 削除を行います。

1. Network > IPv6 > LAN Settings > Prefixes for Prefix Delegation タブの順にメニューをクリックし、以下の画面を表示します。

Car) Status	🛜 Wireless	📃 Network 🏠	VPN	Security	O ^o Maintenance	
etwork » IPv6 » IPv6 LAN S	Settings » Prefixes for Prefix	Delegation				00
IPv6 LAN Settings IPve	6 Address Pools Prefixes	s for Prefix Delegation	outer Advertisen	nent Advert	tisement Prefixes	
his Page allow user to create	e/add/delete/edit Prefix D	elegaion Pools List for IPv6	configuration.			
ist of Prefixes for Pre	fix Delegation					
Show 10 🗸 entries [Right	t click on record to get more	options]				٩
Show 10 v entries [Right	t click on record to get more	options]	Interface		Ə IPv6 Status	٩ (
Show 10 v entries [Righ	t click on record to get more	options] ngth é No data available in f	able		€ IPv6 Status	م ج
Show 10 v entries [Righ Prefix Address Showing 0 to 0 of 0 entries	t click on record to get more	options] ngth e No data available in f	able		IPv6 Status First Previous	Q G Kt X Last X
Show 10 I entries [Righ Prefix Address Showing 0 to 0 of 0 entries	t click on record to get more	options] ngth é No data available in f) Interface able		IPv6 Status First Previous Nez	Q € et) Last)i

図 5-64 IPv6 LAN Settings>Prefixes for Prefix Delegation タブ 画面

2. プレフィックスを追加する場合は、「Add New Prefix Delegation」をクリックし以下の画面を表示します。

IPv6 Prefix Delegation Configuration		
Prefix Address Prefix Length VLAN Interface	[Range: 1 - 128] Default	
		Save

図 5-65 IPv6 Prefix Delegation Configuration 画面

3. 以下の項目を設定します。

項目	説明
Prefix Address	プレフィックスアドレスを入力します。
Prefix Length	プレフィックス長を入力します。
VLAN Interface	VLAN インタフェースを指定します。

4. 「Save」をクリックし、設定を適用します。

追加したプレフィックスは、**IPv6 LAN Settings > Prefixes for Prefix Delegation タブ** 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Router Advertisement(IPv6 ルータ通知)

RA (ルータ通知) は LAN クライアントに対する IPv4 DHCP 割り当てと類似する機能です。IP アドレスやサポートするネットワーク情報といった情報を受け付けるように設定されたデバイスに対してそれらの情報を通知します。

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。ルータ通知デーモンを設定することにより、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。

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

	A Status	🛜 Wireless	🖳 Network	CB VPN	🔒 Security	🍄 Maintenance	
Network » I	Pv6 » IPv6 LAN Sett	ings » Router Advertisem	ent				00
IPv6 LA	N Settings IPv6 A	ddress Pools Prefixe	s for Prefix Delega	ation Router Ad	vertisement Adv	ertisement Prefixes	
This page all assignments network info will listen or Router Ad	ows user to configu for LAN clients. Wit rmation to devices the LAN for router vertisement	re Router Advertisement h this the router will pe that are configured to a solicitations and respon	Daemon (RADVD) r rform stateless aut ccept such details. Id to these LAN hos	elated configurati co configuration of By configuring the ts with router advo	ons.Router Advertis LAN nodes by assig Router Advertisem ertisements.	ements are analogous to ning an IP address and suj ent Daemon on this route	Pv4 DHCP oporting r, the device
Show 10	✓ entries [Right cl	ick on record to get more	options]				٩
Status			🗘 Interf	ace			⇔
Disabled			Default				
Showing 1 to	1 of 1 entries					First J Previous 1 Ne	xt > Last >

図 5-66 IPv6 LAN Settings > Router Advertisement タブ 画面

2. ルータ通知を編集する場合、エントリ上で右クリック→「Edit」を選択し、以下の画面を表示します。

Router Advertisement Configur	ation	×
<i>Router Advertisement</i> Advertise Mode Advertise Interval	Unsolicited Multicast O Unicast Only IRange: 10 - 1800]	
RA Flags Managed Other Router Preference	OFF	
MTU Router Lifetime	1500 [Range: 1280 - 1500] 3600 Seconds	

図 5-67 Router Advertisement Configuration 画面

```
3. 以下の項目を設定します。
```

項目	説明
	Router Advertisement
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軽減させます。
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、本値のその 1/3 の値の間のランダムな値となります。 ・ 初期値: 30 (秒)
	RA Flags
Managed	「ON」にすると、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	「ON」にすると(アドレス以外の)他の情報の自動設定に管理/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る優先度を「Low/Medium/High」から選択します。LAN 上に RADVD が有効な他のデ バイスがある場合、IPv6 クライアントに対して重複を回避するために本機能を使用します。
MTU	 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対して、ルータ通知はこの MTU (Maximum Transmission Unit) 値を設定します。 ・ 設定可能範囲:1280-1500 ・ 初期値:1500
Router Lifetime	この値は RA に含まれ、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。 この期限に到達した際は、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。 ・ 初期値:3600(秒)

Advertisement Prefixes (通知のプレフィックス)

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。 ルータ通知にはサブネットプレフィックスのリストが含まれています。これによりネイバを決定し、そのホストがルータと同じリンク上に存在する かどうかを識別できます。

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

	🕜 Status	🛜 Wirel	less 🧕	🖵 Network	ക	/PN	🔒 Secu	rity 🗢	Maintenance	
Network » I	Pvő » IPvő LAN Set	tings » Advertis	ement Prefixe	es						00
				Radvd i	s not En	abled	b.			
IPv6 LAI	N Settings IPv6 .	Address Pools	Prefixes fo	or Prefix Delega	tion Ro	uter Ad	lvertisement	Advertiseme	nt Prefixes	
This page all prefixes allo that allow th Advertiser	ows user to config w this router to inf ne router to determ ment Prefixes L	ure IPv6 prefixe form hosts how f nine neighbors a L ist	s which will to perform s nd whether	be used while a stateless address the host is on th	dvertiseme auto conf e same lin	nt.The iguratio k as the	router adverti on. Router adve e router.	sements config ertisements con	ured with adverti tain a list of sub	isement net prefixes
Show 10	entries [Right o	click on record to	get more opt	tions]						٩
IPv6 Prefi	x	O IPv6 Pre	fix Length			⊖ Li	ife Time	⊖	Interface	⇔
				No data av	ailable in ta	ble				
Showing 0 to	0 of 0 entries							[] First	Previous Nex	d > Last >
Add New	Advertisement F	Prefix								

図 5-68 IPv6 LAN Settings >Advertisement Prefixes タブ 画面

2. プレフィックスを追加する場合、「Add New Advertisement Prefix」をクリックし以下の画面を表示します。

Advertisement Prefix Configuration		×
IPv6 Prefix Type SLA ID Prefix Lifetime VLAN Interface	Global /Local/ISATAP [Range: 0 - 999] [Range: 5 - 65536] Seconds	
	Save	

図 5-69 Advertisement Prefix Configuration 画面

3. 以下の項目を設定します。

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 とする必要があります。
IPv6 Prefix	「Global/Local/ISATAP」プレフィックスを使用する場合、本ルータが通知する IPv6 ネットワークを定義します。
IPv6 Prefix Length	「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を指定します。通常は 64 を指定します。
Prefix Lifetime	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
	タイムと類似の機能です。
VLAN Interface	VLAN インタフェースを指定します。

4. 「Save」をクリックし、設定を適用します。

追加したプレフィックスは、IPv6 LAN Settings > Advertisement Prefixes タブ画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

IPv6 Tunnels Status (IPv6 トンネルステータス)

Network > IPv6 > IPv6 Tunnels Status

IPv6 トンネルのステータスを表示します。

1. Network > IPv6 > IPv6 Tunnels 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。

	🕢 Status	🛜 Wireless	💂 Network	I VPN	🔒 Security	O ^o Maintenance	
Network »	IPvő » IPvő Tunneb	s Status					00
This page sh	ows the status of I	Pv6 tunnels.					
IPv6 Tunn	els Status						
Show 10	• entries [No right	nt click options]					٩
Tunnel Na	ame		0	IPv6 Addresses			Θ
sitO-WAN1							
sito-WAN2							
Showing 1 to	2 of 2 entries				KIF	irst A Previous 1 Next	> Last >

図 5-70 IPv6 Tunnels Status 画面

第6章 無線設定(Wireless)(DSR-1000ACのみ)

本製品の無線設定について説明します。 無線設定はウィザードを使用して行うこともできます。 ウィザードを開始するには、「ワイヤレスネットワーク接続(DSR-1000AC のみ)」を参照してください。

項目	説明
「General(一般設定)」	DSR-1000AC の無線ネットワークおける一般的な設定(AP 追加、プロファイル、帯域設定など)をします。
「Advanced(高度な設定)」	DSR-1000AC の無線ネットワークおける高度な設定(WMM、WDS、WPS など)をします。

General (一般設定)

Wireless > General

DSR-1000AC 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/ac 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 設定メニューで設定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。各仮想 AP 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。



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。

Access Points (アクセスポイント)

Wireless > General > Access Points

無線 LAN アクセスポイントを設定、表示します。

1. Wireless > General > 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。

	🗥 Status	🛜 Wir	eless 📃		CB VPN	Seci		🌻 Maintenan	ce
Wireless » (General » Access	Points							0 0
The List of A radios) can b Access Po	wailable Access P be reviewed and A ints List	oints table lists AP parameter co	the configured Anniguration setting	Access Points (AP) ngs can be access	for this device. ed.	From this	summary lis	t, the status of e	ach AP (over all
Show 10	entries [Right	t click on record I	o get more option	15]					٩
Status 🗘	Virtual AP ⊖	SSID ⊖	Broadcast ⊖	Profile Name	Active Time	e 🕀 Sta	rt Time 😌	Stop Time ⊖	Radio Mode 🕀
Enabled	ap1	DSR-1000AC_1	Enabled	default1	No (Turn-off)	-		2	5 Ghz
Enabled	ap5	DSR-1000AC_2	Enabled	default2	No (Turn-off)	-		-	2.4 Ghz
Showing 1 to	2 of 2 entries						First	Previous 1	Next 🔪 Last 刘
Add New	Access Point								

図 6-1 Access Points 画面

- 2. エントリで右クリックすると、以下のメニューが表示されます。
 - ・「Edit」:アクセスポイントの追加、編集を行います。
 - ・「Disable」:アクセスポイントを無効にします。
 - ・「MAC Filter」:MAC フィルタリングを行います。
 - ・「Status」:ステータスを表示します。
 - ・「Delete」:アクセスポイントを削除します。

Add New Access Point(アクセスポイントの追加 / 編集)

1. 「Add New Access Point」をクリック、または既存のエントリ上で右クリック→「Edit」を選択し、以下の画面を表示します。

Access Point Configuration		X
AP Name	ap 1	
Profile Name	default 1	
Active Time	ON THE	
Schedule Control	OFF	
Start Time	Hour Minute AM	
Stop Time	Hour Minute AM	
WLAN Partition	OFF	
		Save

図 6-2 Access Point Configuration 画面

2. 以下の項目を設定します。

項目	説明
AP Name	仮想アクセスポイント名を入力します。
Profile Name	プルダウンメニューからこのアクセスポイントに紐付けるプロファイルを選択します。Wireless > General > Profiles 画面 で追加したプロファイルが選択肢として表示されます。
Active Time	アクセスポイントとしての機能を有効にします。 以下「Schedule Control」および「Start Time」/「Stop Time」欄を指定することができます。
Schedule Control	アクセスポイントのスケジュール制御を有効にします。 「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	「ON」に設定すると、各無線クライアントは他のクライアントと通信することができなくなります。

MAC Filter(アクセスポイントの MAC フィルタリング)

1. 既存のエントリ上で右クリック→「MAC Filter」を選択し、以下の画面を表示します。

👔 Status 🛜 Wireless	📃 Network 🙆 VPN	Security	O° Maintenance	
Wireless » General » Access Points » MAC Fitter				00
This page shows the access control list and also al	ows user to add new access control	rules.		
MAC Filter				
Access Control List Status				
AP Name	ap1 🔻			
ACL Policy Status	Open 🔻			
	Save Cancel			
MAC Filter List				
Show 10 Tentries [Right click on record to	get more options]			٩
MAC Address				٥
	No data available in table			
Showing 0 to 0 of 0 entries			First 🔄 Previous 🛛 Next 🗲	Last 刘
Add New MAC Filter				

図 6-3 MAC Filter 画面

2. 以下の項目を設定します。

項目	説明			
Access Control List Status				
AP Name	アクセスポイントを選択します。			
ACL Policy Status	アクセスコントロールリストのステータスを選択します。			
MAC Filter List				
MAC Address	アクセスポイントへの接続が許可または拒否されている MAC アドレスのリストが表示されます。			

- 3. MAC アドレスを追加する場合は、「Add New MAC Filter」をクリックし、MAC アドレスを入力します。
- 4. 「Save」をクリックし、設定を適用します。

Status(アクセスポイントのステータス確認)

1. 既存のエントリ上で右クリック→「Status」を選択し、以下の画面を表示します。

cess P	oints									
ccess F	Points Sta	itus								
AP Name	Radio	Packets rx	Packets tx	Bytes rx	Bytes tx	Errors rx	Errors tx	Dropped rx	Dropped tx	MultiCas
ap1	1	3413	6160	445421	4882238	0	0	0	0	0
onnect	ed Client	.5								
MAC Ad	ldress	Radio	Secur	ty	Encryption	n i i	Authentica	tion	Time Conno	ected
				N	o data availab	le in table				

図 6-4 MAC Filter 画面

2. アクセスポイントのステータスと接続しているクライアントの情報を確認します。

Profiles(無線プロファイル)

Wireless > General > Profiles

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。

プロファイルを作成することにより、APと無線クライアントの通信で使用するセキュリティタイプ、暗号化、および認証を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。このモードでは、すべての互換性のある無線クライアントが AP に接続できるため安全ではありません。

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を有効化した場合、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。

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することができます。

1. Wireless > General > 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。

	孢 Status	، پ	Vireless	<u>-</u> N		CA VPN	S 🔒		O° Maintenan	
Wireless » Genera	al » Profile	s								0 0
A profile is a grou Configuration pag Profiles List	ping of wire e. The profi	eless settings ile allows for	which can be s easy duplicatio	hared a n of SSI	cross multipl IDs, security	e APs. AP s settings, er	pecific setting cryption meth	s are configu ods, client ai	red on the Access F uthentication, etc.	Point across APs.
Profile Name	SS	ID 6	Broadcast		Security	e Encr	vption 🕀	Authentic	ation \ominus Ra	udio Mode 🛛 🖯
default1	DSF	R-1000AC_1	Enabled		WPA+WPA2	TKIP+	ССМР	PSK	5 0	ihz
default2	DSF	R-1000AC_2	Enabled		OPEN	None		None	2.4	Ghz
Showing 1 to 2 of 2	entries							K Fir	st Previous 1	Next > Last >
Add Now Dro										

図 6-5 Profiles 画面

|注意| DSR-1000AC は 2.4GHz と 5GHz の両方の帯域をサポートしています。デフォルトプロファイルについても編集することができます。

2. プロファイルを追加する場合、「Add New Profile」をクリックし以下の画面を表示します。

Profile Configuration		8
Profile Name		
SSID		[Length: 1 -32]
Broadcast SSID	ON	
Security	OPEN 🗸	
Radio Mode	2.4 Ghz	
		Save

図 6-6 Profile Configuration 画面

3. 以下の項目を設定します。

項目	説明
Profile Name	プロファイル名を入力します。
SSID	SSID を入力します。
Broadcast SSID	SSID をブロードキャストにオープンする場合「ON」にします。「OFF」にすると非表示になります。
Security	 セキュリティ方式を以下から選択します。 「OPEN」:パブリックに「オープン」なネットワークを作成し、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。 「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。
Authentication	暗号の種類を指定したセキュリティ方式に従い、以下から選択します。 ・「WEP」:「Open System」または「Shared Key」を選択します。 ・「WPA2/WPA+WPA2」:「PSK」(パスフレーズ)、「RADIUS」(RADIUS サーバ)、「PSK+RADIUS」から指定します。
Encryption	認証方式を指定したセキュリティ方式に従い、以下から選択します。 ・「WEP」: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。 ・「WPA2」:「CCMP」のみ選択可能です。 ・「WPA+WPA2」:「TKIP+CCMP」のみ選択可能です。
WEP Passphrase/ WEP Key1-4	WEP を選択した場合、パスフレーズまたは 16 進数方式のキーを指定します。 「WEP Passphrase」を入力し、「Generate Key」をクリックすると自動的に「WEP Key」が生成されます。
WPA Password	「WPA2」、「WPA+WPA2」を選択した場合、WPA パスワードを指定します。
Protect Management Frame	「PSK」「PSK+RADIUS」を選択した場合に表示されます。「ON」にすると管理フレームの保護を有効にします。
Enable Pre-Authentication	「WPA2」で「RADIUS」を選択した場合に表示されます。「ON」にすると事前認証を有効にします。
Radio Mode	適用する無線帯域を指定します。「2.4GHz」「5GHz」「Both」(両方)から選択します。

4. 「Save」をクリックし、設定を適用します。

追加したプロファイルは、Profiles 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Wireless > General > Access Points 画面では、新しいアクセスポイントの作成とプロファイルの紐付けを行います。

本製品は複数のアクセスポイントをサポートしており、これは仮想アクセスポイント(VAP)と呼ばれます。固有の SSID を持つ各仮想 AP は、クラ イアント側から見てそれぞれ独立した1台のアクセスポイントのように見えます。こうした仕組みにより、ユーザ要件に沿ってユーザグループに対 してセキュリティとスループットの最適化を行うことで、ルータの無線設定を行うことが可能です。VAP の作成手順は、「Access Points(アクセス ポイント)」を参照してください。

Radio Settings (無線帯域の詳細設定)

Wireless > General > Radio Settings

DSR-1000AC の無線設定について説明します。

DSR-1000AC では、2.4 GHz または 5 GHz のいずれかの周波数帯を選択できます。 選択した周波数帯に基づき、モードの種類とチャネル幅を設定します。

2.4 GHz(2.4 GHz 設定)

2.4GHz 帯域での無線機能について説明します。

1. Wireless > General > Radio Settings > 2.4GHz タブの順にメニューをクリックし、以下の画面を表示します。

🐼 Status	🛜 Wireless	💻 Network	Ca VPN	Security	O Maintenance	
Wireless » General » Radio Setti	ngs » 2.4 GHz					0 0
2.4 GHz 5 GHz						
This page allows you to configure	the hardware setting	gs for each available	radio card.			
Radio Settings - 2.4 GHz						
Mode	ng	1	~			
Channel Spacing	20	OMHz	~			
Current Channel	6 -	2.437GHz				
Channel	6	- 2.437GHz	\checkmark			
Default Transmit Power	10	00 [Range: 1	I - 100] %			
Transmission Rate	В	est(Automatic)	\checkmark			
		Davis	Concel			
		Save	Cancel			

図 6-7 Radio Settings (2.4GHz) 画面

2. 以下の項目を設定します。

項目	説明
Mode	802.11 モードを「g and b」「g only」「b only」「ng」「n only」から選択します。
Channel Spacing	 チャネル幅を選択します。 ・「20/40 MHz」(初期値) 802.11n 対応の無線機器と 802.11n 非対応の無線機器がネットワークに混在する場合に選択します。「Mode」が「ng」「n only」の場合に選択できます。 ・「20MHz」 802.11n 対応の無線機器を使用しない場合、選択します。「Mode」が「g and b」「g only」「b only」の場合に選択できます。
Control Side Band	「Upper」または「Lower」を選択します。チャネル幅が「20/40 MHz」の場合のみ選択できます。
Current Channel	現在のチャネルを表示します。
Channel	使用するチャネルを選択します。
Default Transmit Power	初期設定の発信強度(単位:%)を指定します。
Transmission Rate	ドロップダウンメニューより送信レートを選択します。 これにより無線接続の送信レートは固定されます。 ・ 推奨設定:「Best (Automatic)」

5 GHz(5 GHz 設定)

本項目では 5GHz 帯域での無線機能について説明します。

5GHz帯のみで使用可能な「802.11AC」を使用すると、最大 80MHz までチャンネル帯域を指定することが可能となり、データスループットは「802.11n」 に比べて大きく向上します。使用できるチャネルや帯域は DSR-1000AC が使用される国によって制限がある場合があります。「802.11AC」では、 5GHz 無線の新しいデザインによる拡張機能を使用し、無線フレームアグリゲーション経由でより多くのデータを単一パケットに乗せて送信するこ とが可能です。

1. Wireless > General >Radio Settings > 5 GHz タブの順にメニューをクリックし、以下の画面を表示します。

🖽 Status	🛜 Wireless	💻 Network	CA VPN	Security	O Maintenance	
Wireless » General » Radio Se	ttings » 5 GHz					0 0
2.4 GHz 5 GHz						
This page allows you to configu	ire the hardware setting	s for each available	radio card.			
Radio Settings 5 GHz						
Mode	a	n/ac	V			
Channel Spacing	2)/40MHz	\checkmark			
Control Side Band	U	pper	\checkmark			
Current Channel	40	- 5.2GHz				
Channel	A	uto	~			
Default Transmit Power	5	4 [Range:	1 - 100] %			
Transmission Rate	в	est(Automatic)	~			
		Save	Cancel			
	_		ounou			

図 6-8 Radio Settings > 5GHz タブ画面

2. 以下の項目を設定します。

項目	説明			
Mode	「a only」「n only」「ac only」「na」「a/n/ac」から選択します。			
Channel Spacing	 チャンネル幅を選択します。 ・「20/40 MHz」: Mode が「n only」「ac only」「na」「a/n/ac」の場合、選択可能です。 ・「20MHz」: 全モードで選択可能です。 ・「80MHz」: Mode が「ac only」「a/n/ac」の場合、選択可能です。 			
Control Side Band	「Upper」または「Lower」を選択します。「20/40 MHz」選択時のみ有効です。			
Current Channel	現在のチャネルを表示します。			
Channel	使用するチャネルを選択します。			
Default Transmit Power	初期設定の発信強度(単位:%)を指定します。			
Transmission Rate	ドロップダウンメニューより送信レートを選択します。 これにより無線接続の送信レートは固定されます。推奨設定:「Best (Automatic)」			

Advanced(高度な設定)

Wireless > Advanced

無線設定における高度な設定を行います。

WMM (WMM 設定)

Wireless > Advanced > WMM

WMM (Wi-Fi Multimedia) は、IEEE 802.11 ネットワークに基本的な QoS (Quality of Service)機能を提供します。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. Wireless > Advanced > 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。

🖾 Status 🛜 Wire	less 📃 Network	A VPN	Security	O ^o Maintenance	
eless » Advanced » WMM					0
s page allows you to configure the Wi-Fi	Multimedia(WMM) configura	ation parameters.			
AM Settings					
Profile Name	default1	•			
Enable WMM	OFF				
Default Class Of Service	Background	•			
P TOS/DiffServ Mapping					
Show 10 entries [No right di	ck options]				0
					4
IP DSCP / TOS	Ŷ	Class Of Service			0
0		Default			
1		Default			
2		Default			
3		Default			
4		Default			
5		Default			
6		Default			
7		Default			
8		Default			
9		Default			
Showing 1 to 10 of 64 entries			First J Previous	1 2 3 4 5 Next >	Last 刘
	Save	Cancel			

図 6-9 WMM 画面

2. 以下の項目を設定します。

項目	説明
Profile Name	本設定に関連付けるプロファイルを選択します。
Enable WMM	「ON」にすると WMM 機能が有効になります。
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) を選択します。
IP DSCP / TOS	「Class Of Service」毎にサービスを選択し、「IP DSCP / TOS」とのマッピングを設定します。

WDS (WDS 設定)

Wireless > Advanced > WDS

WDS (Wireless Distribution System) は、ネットワーク上のアクセスポイント同士で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(同じチップセット / ドライバを使用している場合など)でのみ正常な動作が保証されます。

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 キーのハンドシェイ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 設定ページで管理者による設定が可能な) PSK と(設定不可の)内部の「magic」文字列が、入力値として使用されます。

実際には、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。Default AP で TKIP + AES が選択されている 場合、WDS リンクでは AES 暗号化方式が使用されます。

WDS 設定は各帯域(5GHz/2.4GHz)でタブで切り替えて設定を行います。表示される項目は同一です。

1. Wireless > Advanced > WDS > 2.4 GHz タブ / 5GHz タブの順にメニューをクリックし、以下の画面を表示します。

🐼 Status	Wireless	💻 Network	ക vpn	盈 Security	🐡 Maintenance		
Wireless » Advanced » WDS » 2.4	GHz					?	0
2.4 GHz 5 GHz							
This page allows you to configure t	he Wireless Distrib	ution System (WDS)	configuration param	eters.			
WDS Settings 2.4 GHz							
WDS Enable	- 11	OFF					
WDS Encryption	Nor	ne					
WDS Security	OPI	EN					
WDS Authentication	Nor	ne					
System MAC Address	10	INCOMPTO INCOME					
		Save	Cancel				
WDS Peer MAC Address List							
Show 10 • entries [Right clic	k on record to get m	ore options]					
MAC Address							÷
		No data avi	ailable in table				
Showing 0 to 0 of 0 entries				K Fir	st 🚽 Previous Next 🗲	Last 刘	

図 6-10 WDS > 2.4 GHz タブ画面

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。

2. 以下の項目を設定します。

項目	説明
WDS Enable	「ON」にして WDS を有効にします。
WDS Encryption	現在 WDS リンクで使用されている暗号化のタイプを表示します。
WDS Security	現在 WDS リンクで使用されているセキュリティを表示します。
WDS Authentication	現在 WDS リンクで使用されている認証方法を表示します。
WDS Passphrase	WDS のパスフレーズを入力します。本項目は、WEP、WPA、WPA2、WPA+WPA2 が有効で、「WDS Enable」を「ON」 にした場合のみ表示されます。
System MAC Address	システム MAC アドレスを表示します。
Advanced Settings(詳細設定)

Wireless > Advanced > Advanced Settings

ここでは無線の詳細な設定を行います。

802.11 の通信パラメータを変更することができます。通常、多くのネットワークでは初期設定が適しています。 Advanced Settings(詳細設定)は各帯域(5GHz/2.4GHz)でタブで切り替えて設定を行います。表示される項目は一部を除き同じです。

1. Wireless > Advanced > Advanced Settings > 2.4 GHz タブ / 5GHz タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status	🛜 Wireless	💻 Network	A VPN	Security	O Maintenance	
Wireless » Advanced » Advan	ced Settings » 2.4 GHz					00
2.4 GHz 5 GHz						
This page is used to specify ad	lvanced configuration se	ttings for the radio.				
Advanced Wireless Setti	ings 2.4 GHz					
Beacon Interval	1	00 [Default:	100, Range: 40 - 350	0] Milliseconds		
Dtim Interval	2	[Default:	2, Range: 1 - 255]			
Enable RTS Threshold		OFF				
Fragmentation Threshold	2	346 [Range: 2	257 - 2346]			
Protection Mode	N	lone	~			
Tx Antenna	A	uto	~			
Rx Antenna	A	uto	\checkmark			
AMPDU		N NO				
Power Save Enable		OFF				
Multi To Unicast		OFF				
		Save	Cancel			
	-					

図 6-11 Advanced Settings 画面(2.4GHz) 画面

🙆 Status 🛜	Wireless 📃 N	letwork 🕼 VPN 🚊 Security 💇 Maintenance	
Wireless » Advanced » Advanced Settings	» 2.4 GHz		0 0
2.4 GHz 5 GHz			
This page is used to specify advanced con	figuration settings for	Web ページからのメッセージ	
Advanced Wireless Settings 2.4 (GHz		
Beacon Interval	100	Converting multicast traffic to unicast will lead to performance drop for multicast traffic over the wired LAN. It will also disable	
Dtim Interval	2	the WDS. Are you sure you want to proceed?	
Enable RTS Threshold	OFF		
Fragmentation Threshold	2346	OK キャンセル	
Protection Mode	None		
Tx Antenna	Auto		
Rx Antenna	Auto		
AMPDU	ON THIR		
Power Save Enable	OFF		
Multi To Unicast	ON		
	Save	Cancel	

図 6-12 Advanced Settings 画面(2.4GHz)(Multi To Unicast 有効化時) 画面

項目	説明
Beacon Interval	「ビーコン」は無線ネットワークに同期するためにアクセスポイントから送信されるパケットです。初期値は 100 です。
Dtim Interval	ビーコンに含まれる DTIM(Delivery Traffic Information Message)の周期を設定します。
	省電力モードの無線クライアントに対して、送信待ちのデータがあることを伝えます。
	• 初期值:2
Enable RTS Threshold	RTS しきい値を指定します。送信データがこのパケットサイズ(Byte)よりも大きい場合、無線クライアントへ RTS(Request
	To Send:送信要求)信号を送信します。値を小さくすると RTS パケットの送信頻度が高くなり、ネットワーク帯域を消費し
	てスループットの低下を招く可能性があります。初期値の 2432 のままとしておくことを推奨します。
Fragmentation Threshold	フラグメンテーションしきい値を設定します。設定のしきい値を超えたパケットを送信前にフラグ化します。
(2.4GHz のみ)	・ 初期値:2346
Preamble Mode	プリアンブルモードを「Long」「Short」から選択します。アクセスポイントとローミング無線アダプタ間の通信におい
(5GHz のみ)	て、CRC (Cyclic Redundancy Check) ブロックの長さを定義します。ネットワークのトラフィックが多い場所では「Short」
	を選択します。
Protection Mode	プロテクションモードを「None」「CTS-to-Self Protection」から選択します。
(2.4GHz のみ)	「CTS-to-Self Protection」を選択すると 802.11b と g が混在した環境下でのステーション同士のコリジョン(衝突)を軽減す
	る「CTS-to-Self」防御メカニズムが有効になります。
	・ 初期値:「None」
Tx/Rx Antenna	送信(Tx)、受信(Rx)におけるアンテナへの割り当てを指定します。
AMPDU	AMPDU(aggregation MAC protocol data unit)を有効にします。MAC ヘッダを含んだフレーム集約を行います。
Power Save Enable	省電力機能を有効にします。「ON」にすると U-APSD(WMM Power Save)によって無線の電力消費が抑制されます。
Multi To Unicast	外部から受信したコンテンツプロバイダのマルチキャスト宛先アドレスを有効にし、ユニキャスト宛先アドレスに変換
	します。

3. 「Save」をクリックし、設定を適用します。

WPS (WPS 設定)

Wireless > Advanced > WPS

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 はサポートされる無線クライアントをネットワークに追加するシンプルな方法であり、WPA または WPA2 セキュリティが設定された AP で使用することができます。WPS を使用するには、これらのセキュリティが設定されている AP をドロップダウンメニューから選択し、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の概要が表示されます。 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) :
- 4. 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」をクリックした後、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) :
- 5. PBC をサポートする無線デバイスに対しては、2 秒間「Configure via PBC」を押し続けます。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。

1. Wireless > Advanced > 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。

Status	🛜 Wireless	💻 Network	CA VPN	Security	O° Maintenance	
Wireless » Advanced » WPS						0 0
This page allows you to define an	d modify the Wi-Fi Pi	otected Setup (WP	5) configuration par	ameters.		
WPS Settings						
WPS Configuration						
Select VAP	at	5	\checkmark			
WPS Status		OFF				
WPS Current Status						
Security	W	PA+WPA2				
Authentication	PS	к				
Encryption	тк	IP+CCMP				
		Save	Cancel			
	_					
<u> </u>						

図 6-13 WPS 画面

- 2. 「Select VAP」で WPS を使用する VAP をドロップダウンメニューから選択します。
- 3. 「WPS Status」を「ON」にして、設定を適用します。
- 4. WPS が有効になると以下の画面が表示されます。

Wireless » Advanced » WPS		0
	Operation Succeeded	
This page allows you to define and mo	dify the Wi-Fi Protected Setup (WPS) configuration parameters.	
WPS Settings		
WPS Configuration		
Select VAP	ap5	
WPS Status	ON THE	
WPS Current Status		
Security	WPA+WPA2	
Authentication	PSK	
Encryption	ТКІР+ССМР	
WPS Setup Method		
Station PIN		
	Configure Via PIN Configure Via PBC	
Session Status		

図 6-14 WPS(ON) 画面

- 5. 「WPS Setup Method」で WPS の方法として、「Configure Via PIN」(PIN 入力)または「Configure Via PIN」(WPS ボタン押下)を選択します。
- 6. 「PIN」を使用する場合、「Station PIN」に無線クライアントのピンコードを入力し、「Configure Via PIN」(PIN 入力)をクリックします。
- 7. プッシュボタン方式を使用する場合、「Configure Via PBC」をクリックします。これにより WPS セッションが起動され、無線クライアントの WPS ボタンを 1 分以内に押す(またはインタフェース上で開始する)必要があります。
- 8. 接続には約2分程度かかります。「Session Status」で正常に接続されたことを確認します。

第7章 VPN 設定(VPN)

VPN (Virtual Private Network)の設定について説明します。

設定項目	説明
「IPSec VPN (IPSec VPN の設定)」	IPSec VPN の設定を行います。
「PPTP VPN (PPTP VPN 設定)」	PPTP VPN の設定を行います。
「L2TP VPN(L2TP VPN 設定)」	L2TP VPN の設定を行います。
「SSL VPN(SSL VPN 設定)」	SSL VPN の設定を行います。
「OpenVPN(OpenVPN 設定)」	OpenVPN の設定を行います。
「GRE(GRE 設定)」	GRE の設定を行います。

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。 以下のタイプのトンネル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 ルータの後方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 ルータの後方にあります。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

IPSec VPN (IPSec VPN の設定)

VPN > IPSec VPN

Policies (IPSec VPN ポリシーの設定)

VPN > IPSec VPN > Policies

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。

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 クライアント間の通信に適用されます。IPSec モード は、ポリシーの 2 つのエンドポイント間を横切るネットワークに応じて「Tunnel Mode」または「Transport Mode」のどちらかになります。

• Transport (転送モード) :

このモードは、本ルータとトンネルのエンドポイント(別の IPsec ゲートウェイまたはホスト上の IPSec VPN クライアントのいずれか)間の endto-end 通信のために使用されます。データペイロードのみが暗号化され、IP ヘッダは、変更または暗号化されません。

Tunnel (トンネルモード):

このモードは network-to-network IPSec トンネルに使用されます。このゲートウェイがトンネルの一方のエンドポイントとなります。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 リースを提供することができます。また、このモードでは、ローカル及びリモートのプライベートネットワークの両方に対し、 IP アドレスや IP アドレス範囲、サブネットを定義してトンネル経由の通信を許可することも可能です。

1. VPN > IPSec 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。

	2 Status	*	ኛ Wireless		💻 Netwo	rk Ca	B VP	אי 🔒	Security	O °	Maintenance		
VPN » IPSec	VPN » Policies											?	0
This page sho from this pag Note: Policy IPSec Polic	ows the list of co ge. with '*' represent cies List	nfigure ts a Clie	d IPsec VPN po ent Policy.	licies (on the router	r. A user cai	n also	add, delete, e	dit, enable,	disable a	nd export IPsed	: VPN pol	icies
Show 10	✓ entries [Right]	click o	n record to get i	more of	otions]					(1	٩	
Status	∆ Name	0	Backup Tunnel Name	⇔ Т	ype Ə	IPSec Mode	÷	Local	Remote	⇔	Auth 😔	Encr	Ð
					No da	ata available i	in table	9					
Showing 0 to	0 of 0 entries									First	Previous Ne	xt 👂 🛛 Las	st >
Add New	IPSec Policy												
Backup Po	licies List												
Show 10	entries [No ri	ght clic	k options]							(٩	
Status	O Name	0	Primary Funnel Name	()	буре ⊖	IPSec Mode	⇔	Local	Remote	÷	Auth 😔	Encr	⇔
					No da	ata available i	in table	9					
Showing 0 to	0 of 0 entries									First	Previous Ne	xt 🔪 Las	st >

図 7-1 Policies 画面

Add New IPSec Policy(IPSec VPN ポリシーの追加)

1. 「Add New IPSec Policy」をクリックし、以下の画面を表示します。

IPSec Policy Configuration		×
General		^
Policy Name		
Policy Type	Auto Policy	
IP Protocol Version	IPv4	
IKE Version	IKEv1	
L2TP Mode	None	
IPSec Mode	Tunnel Mode	
Select Local Gateway	Dedicated WAN	
Remote Endpoint	IP Address	
IP Address / FQDN		
Enable Mode Config	OFF	
Enable NetBIOS	OFF	
Enable RollOver	OFF	
Protocol	ESP	
Enable DHCP	OFF	
Local IP	Subnet	
Local Start IP Address		
Local Subnet Mask		
Remote IP	Subnet 🔽	
Remote Start IP Address		
Remote Subnet Mask		
Enable Keepalive	OFF	~
		Save

図 7-2 IPSec Policy Configuration 画面

2. 以下の項目を設定します。

項目	説明
Policy Name	VPN ポリシー名を入力します。これはリモート WAN/ クライアントの識別名とはなりません。
Policy Type	 VPN ポリシーの種類を「Manual Policy」「Auto Policy」から指定します。 ・「Manual Policy」:各エンドポイントに対し、キーなども含め VPN トンネルのすべての設定を手動で行います。第三 者機関サーバや組織などは含まれません。
	 「Auto Policy」: VPN トンネルのいくつかのパラメータは自動的に生成されます。これには二つの VPN エンドボイン ト間での IKE プロトコルを使用したネゴシエーションが必要になります。
IP Protocol Version	IP バージョン を「IPv4」または「IPv6」から選択します。
IKE Version	IKE バージョン を「IKEv1」または「IKEv2」から選択します。
L2TP Mode	L2TP モードを「None」「Client」「Gateway」から指定します。
IPSec Mode	IPSec モードの状態を「Tunnel Mode」「Transport Mode」で表示します。 IPsec トンネルモードは信頼性の低いネットワークを通過するトラフィックを保護する際に有効です。相互運用性を目的と して、主に「L2TP/IPsec」「PPTP」接続などをサポートしていないゲートウェイやエンドシステムなどにおいて、トンネルモー ドが使用されます。「トランスポートモード」は IPSec の初期モードであり、end-to-end 通信に使用されます。(例:クラ イアント / サーバ間など)
Select Local Gateway	IPSec トンネルのためのローカルゲートウェイを指定します。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。
Remote Endpoint	FQDN または 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。L2TP モードに「Client」を選択し た場合は表示されません。
IP Address / FQDN	ルータの識別子を入力します。
Enable Mode Config	「ON」で「Mode Config」を有効にします。 「Mode Config」は、DHCP 機能のようにリモートの VPN クライアントに IP アドレスをアサインする機能です。
Enable NetBIOS	「ON」で VPN トンネルにおける「NetBIOS」ブロードキャストの通過を許可します。
Enable RollOver	「ON」で VPN ロールオーバを有効にします。WAN モードを「Rollover」に指定する必要があります。

項目	説明
Protocol	プロトコルを選択します。
Enable DHCP	「ON」にすると、IPsec 経由でルータに接続している VPN クライアントが、DHCP による割り当て IP アドレスを取得でき るようになります。
Remote IP / Local IP	「Enable DHCP」を「OFF」にした場合、エンドポイント用の識別の種類を指定します。 ・「Any」:ポリシーは、ローカル/リモートのエンドポイントからのトラフィックに適用されます。 ・「Single」:ポリシーの適用を1台のホストのみに限定します。入力したホストのIPアドレスがVPNの一部になります。 ・「Range」:VPNへの接続を許可するIPアドレスの範囲を指定します。開始IPアドレスと終了IPアドレスを入力します。 ・「Subnet」:VPNへの接続を許可するサブネットを指定します。ネットワークアドレスとサブネットマスクを入力します。
Enable Keepalive	「ON」にした場合、以下の項目を入力します。 ・ Source IP Address ・ Destination IP Address ・ Detection Period [Range: 10 - 999] ・ Reconnect After Failure

トンネルのトンネルタイプとエンドポイントが定義されたら、トンネルに使用するフェーズ1/フェーズ2ネゴシエーションを決定できます。 ポリシーは手動または自動で設定することができます。自動ポリシーの場合、インターネットキー交換(IKE)プロトコルは2つの IPsec ホスト間で キーを動的に交換します。

3. 「Phase1(IKE SA Parameters)」「Phase2(Auto Policy Parameters)」の設定を行います。

			X
OFF			
			^
Main	~		
Both	~		
ON			
Local Wan I	P		
Remote Wa	n IP		
OFF	3DES	ON THE	
ON THE	AES-192	OFF	
OFF			
OFF			
	Main Both CN Local Wan I Remote Wa	Main Both Cot Local Wan IP Cot Remote Wan IP Cot AES-192 COFF COFF	Main V Both V Both V Local Wan IP V Remote Wan IP V AES-192 OFF

図 7-3 IPSec Policy Configuration 画面 - Phase 1/Phase 2 画面

フェーズ1の「IKE SA Parameter」セクションでは、トンネルのセキュリティアソシエーションの詳細を定義します。 フェーズ2の「Auto Policy Parameter」セクションでは、フェーズ2キーネゴシエーションのセキュリティアソシエーションの有効期間と暗号化/ 認証の詳細を設定します。

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。

「Manual Policy」では、IKE を使用せず、2 つの IPsec ホスト間での認証パラメータ交換を手動で行います。 送受信される SPI(Security Parameter Index)値は、リモートのトンネルエンドポイントに反映される必要があります。

また、トンネルを確立するためには、暗号化、整合性アルゴリズム、およびキーがリモート IPSec ホストに一致する必要があります。 一部の IPsec では、SPI(Security Parameter Index)値が各エンドポイントで変換を必要とするため、「Auto Policy」で IKE を使用することが推奨されます。

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 におけるリンク障害の場合にプライマリ WAN に設定されたポリシーがプ 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のみ本機能を使用することができます。

4. 項目を設定後、「Save」をクリックして設定内容を適用します。



注意

L2TP over IPSec 設定を適用後、両端(サーバとエンドポイント)が正しく設定されサーバが応答中である場合は、トンネルイニシエーションが自動的に開始されます。

Tunnel Mode(トンネルモード)

VPN > IPSec VPN > Tunnel Mode

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。

本ルータは「Full Tunnel」(フルトンネル)と「Split Tunnel」(スプリットトンネル)をサポートしています。 「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。

Tunnel Mode(トンネルモード)

1. VPN > IPSec VPN > Tunnel Mode > Tunnel Mode タブの順にメニューをクリックし、以下の画面を表示します。

🖾 Status 🎅	Wireless 📃 Network	A VPN	Security	Maintenance	
PN » IPSec VPN » Tunnel Mode					00
Tunnel Mode Split DNS Names					
his page allows you to define the IP a	ddress range for clients connectin	ng using Mode Confi	g.		
lode Config					
Tunnel Mode	Full Tunnel O S	Split Tunnel			
Start IP Address	192.168.12.100				
End IP Address	192.168.12.254				
Primary DNS					
Secondary DNS					
Primary WINServer					
Secondary WINServer					
	Save	Cancel			

図 7-4 Tunnel Mode > Tunnel Mode タブ画面

2. 以下の項目を設定します。

項目	説明
Tunnel Mode	「Full Tunnel」(フルトンネル)または「Split Tunnel」(スプリットトンネル)を選択します。フルトンネルでは(インター
	ネットまたはリモートサーバに向かう)すべてのパケットがトンネルを通過しますが、スプリットトンネルではインター
	ネットに向かうトラフィックはトンネルを通過しません。
Start IP Address	このプールに割り当てられる最初のアドレスを入力します。
End IP Address	このプールに割り当てられる最後のアドレスを入力します。
Primary DNS	プライマリ DNS サーバは、このルータに接続するクライアントがドメイン名を解決するために使用します。 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必要があります。
Secondary DNS	セカンダリ DNS サーバは、このルータに接続するクライアントがドメイン名を解決するために使用します。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必要があります。
Primary WIN Server	プライマリ WIN サーバを設定します。
Secondary WIN Server	セカンダリ WIN サーバを設定します。

3. 「Save」をクリックし、設定を適用します。

Split DNS Names(スプリット DNS 名)

スプリット DNS では同一のドメインに2つのゾーンを作成できます。1つは内部ネットワークに使用し、もう1つは外部ネットワークに使用します。 スプリット DNS では、名前解決の際に内部ホストは内部ドメインネームサーバに、外部ホストは外部ドメインネームサーバに向かうように処理さ れます。

1. VPN > IPSec VPN > Tunnel Mode > Split DNS Names タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status	🛜 Wireless	💻 Network	CB VPN	Security	O° Maintenance	
N » IPSec VPN » Tunnel M	ode » Split DNS Names					
Tunnel Mode Split DN	S Names is device use the DNS pr	rovided in Dynamic IP	Range page to res	olve this domain name	.This is applicable only in cas	se of
lit tunnel. plit DNS Names List						
Show 10 💌 entries	[Right click on record to	get more options]				٩
Domain Names						ç
		No data av	ailable in table			
Showing 0 to 0 of 0 entries					First I Previous Next > L	ast 🕅
Add New Split DNS Nar	ne					

図 7-5 Tunnel Mode > Split DNS Names タブ 画面

2. 「Add New Split DNS Name」をクリックして以下の画面を表示します。

Split DNS Names Configuration	×
Domain Name	
	Save

図 7-6 Split DNS Names Configuration 画面

- 3. 「Domain Name」にドメイン名を入力します。
- 4. 「Save」をクリックし、設定を適用します。

DHCP Range (IP アドレス範囲の設定)

VPN > IPSec VPN > DHCP Range

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。 初期値は 192.168.12.0 サブネットの範囲です。

1. VPN > IPSec VPN > 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。

🕜 Status	🛜 Wireless	💻 Network	CB VPN	Security	O Maintenance	
VPN » IPSec VPN » DHCP Rang	e					00
This page allows you to define server on the LAN.	the IP address range	for clients connectin	g using DHCP over	IPsec. Note: To suppo	ort DHCP over IPsec, enabl	e DHCP
DHCP Range						
Starting IP Address	[192.168.12.100				
Ending IP Address	[192.168.12.254				
Subnet Mask	[255.255.255.0				
		Save	Cancel			

図 7-7 DHCP Range 画面

- 2. 「Starting IP Address」「Ending IP Address」に IP アドレスを入力し、 IP アドレス範囲を指定します。
- 3. 「Subnet Mask」でサブネットマスクを指定します。
- 4. 「Save」をクリックし、設定を適用します。

Certificate(認証証明書)

VPN > IPSec VPN > Certificate

本ルータは IPSec VPN 認証にデジタル証明書を使用します。VeriSign(ベリサイン)などの認証局(CA)からデジタル証明書を入手するか、または、 本ゲートウェイで利用可能な機能を使用して自己署名証明書を生成することができます。

本ルータには自己署名証明書が存在し、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置き換えることができます。CA 証明 書は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 ソリューションにおいて必要条件となっています。

Trusted Certificates(トラスト証明書)

現在ルータ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 (Subject Name)	証明書発行先の人物または組織です。
Issuer Name	この証明書を発行した CA 名です。
Expiry Date & Time	このトラスト証明書が無効になる日付です。

1. VPN > IPSec VPN > Certificate > Trusted Certificates タブの順にメニューをクリックし、以下の画面を表示します。

Jacus	🛜 Wireless	💻 Network	A VPN	Security	O Maintenance	
PN » IPSec VPN » Certificate	es » Trusted Certificates					00
Trusted Certificates	ctive Self Certificates	Self Certificate	Requests			
ent presents a digital certi e Trusted CA certificates a rusted Certificates (CA	ficate, the authenticati re used in this authenti A Certificate) List	ion process verifies ication process.	that the presente	d certificate is issued	by one of the trusted at	uthorities.
ihow 10 👻 entries	[Right click on record to g	get more options]				Q
how 10 • entries	[Right click on record to g	get more optionsj	uer Name	A Evoiry Dat	in 9 Time	٩
Show 10 💽 entries	[Right click on record to g ie)	Q Iss No data	uer Name available in table	⊖ Expiry Dat	e & Time	م (
ihow 10 💽 entries CA Identity (Subject Nam ihowing 0 to 0 of 0 entries	[Right click on record to g	O Iss No data	uer Name available in table	⊖ Expiry Dat	First J Previous Next	م و کے Last
Show 10 • entries CA Identity (Subject Nam Showing 0 to 0 of 0 entries	[Right click on record to g	No data	uer Name available in table	⊖ Expiry Dat	e & Time First 📢 Previous Next	م () [Last]

図 7-8 Certificate > Trusted Certificates タブ画面

- 2. 「Upload New CA Certificate」をクリックします。
- 3. 以下の画面で「参照 /Browse」をクリック → 証明書の場所を指定し「Save」をクリックします。

Trusted Certificates (CA	Certificate) Configuration	×
Certificate File	参照	
		Save



Active Self Certificates(自己証明書)

自己証明書は、CA によって発行された、ご使用のデバイスを保障する証明書です。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 書を使用します。Active Self Certificate タブでは、現在ルータにロードされている自己証明書を表示します。

項目	説明
Name	この証明書の名前(識別名)です。
Subject Name	この証明書の所有者として表示される名前です。通常、公式に登録されたビジネスまたは会社名です。
Serial Number	シリアル番号は CA によって証明書を識別するために使用されます。
Issuer Name	この証明書を発行した (署名した) CA 名です。
Expiry Time	署名証明書が無効になる日付です。期限が切れる前に証明書を更新する必要があります。

アップロードされている各自己証明書に対して、以下の情報が表示されます。

1. VPN > IPSec VPN > Certificate > Active Self Certificates タブの順にメニューをクリックし、以下の画面を表示します。

	🙆 Status	🛜 Wireless	💻 Network	CB VPN	🔒 Security	O° Maintenar	nce
PN » IP	Sec VPN » Certificate	es » Active Self Certifica	ates				00
Trust	ted Certificates	Active Self Certificate	Self Certificate R	lequests			
nis table	lists the contificat			hasities (CAs)	and available for proce	station to remote IKE	The The
emote IK	E server validates th	his router using these	certificates. For each	certificate, th	e following data is disp	layed:	servers. The
emote IK Active S Show 10	E server validates the certificates	List [Right click on record to	ertificates. For each	certificate, th	e following data is disp	layed:	ervers. The
emote IK active S Show 10 Name	E server validates th Self Certificates • • entries • Subject	List [Right click on record to Name	get more options]	certificate, th	Issuer Name	eaved: ∂ Expiry Time	ervers. The م
emote IK Active S Show 10 Name	Self Certificates	es issued to you by tru his router using these List [Right click on record to Name Θ	get more options] Serial Number No data av	ertificate, th	Issuer Name	θ Expiry Time	ervers. The ۹
emote IK active S Show 10 Name Showing (e server varidates the certificates e entries C Subject 1 to 0 of 0 entries	es issued to you by tru is router using these - List [Right click on record to Name ⊖	sted Certification Au certificates. For each get more options] Serial Number No data av	ertificate, th	ling available for prese e following data is disp Issuer Name	B Expiry Time Image: State	ext > Last >)
emote IK ctive S Show 10 Name Showing (Self Certificates entries C Subject 1 0 to 0 of 0 entries	es issued to you by tru his router using these List [Right click on record to Name Θ	get more options] Serial Number No data av	ertificate, th	Issuer Name	O Expiry Time Ising the second seco	ور و ext کے لیود کا

図 7-10 Certificate > Active Self Certificates タブ画面

- 2. 「Upload New Self Certificate」をクリックします。
- 3. 以下の画面で「参照 /Browse」をクリック → 自己証明書の場所を指定し「Upload」をクリックします。

Upload Active Self Certificate		×
Certificate File	Browse No file selected.	
		Upload

図 7-11 Upload Active Self Certificate 画面

Self Certificate Requests(自己証明書リクエスト)

自己証明書を CA で署名してもらうには、ルータで識別子パラメータを入力して証明書署名要求(CSR)を生成し、生成したファイルを CA に提出し ます。CA のトラスト証明書及び CA によって署名されたサーバ証明書をアップロードし、ゲートウェイの正当性を証明する自己証明書をアクティブ にすることができます。自己証明書は、ピアとの IPsec および SSL 接続でゲートウェイの信頼性を検証するために使用されます。

1. VPN > IPSec VPN > Certificate > Self Certificate Requests タブの順にメニューをクリックし、以下の画面を表示します。

æ		🛜 Wireless	💻 Network	CA VPN	Security	O° Maintenance
PN » IPSec VPN	» Certificates	s » Self Certificate Requ	ests			0 0
Trusted Certi	ificates Ac	tive Self Certificates	Self Certificate R	equests		
ie Self Certificat	te Requests	table displays a list of	all the certificate re	quests made.		
elf Certificate	e Requests	s List				
show 10 💌 er	ntries	[Right click on record to g	get more options]			٩
Name			<u>ن</u> د	tatus		
			No data av	ailable in table		
Showing 0 to 0 of 0	entries					First Previous Next > Last >
New Celf Cert	-					
New Self Cert	incate					

図 7-12 Certificate > Self Certificate Requests タブ画面

2. 自己証明書を追加する場合、「New Self Certificate」をクリックし以下の画面を表示します。

Generate Self Certificate Request		8
Name Subject		
Hash Algorithm	MD5	
Signature Key Length	512	
Application Type	HTTPS	
IP Address		Optional
Domain Name		Optional
Email Address		Optional
		Save

図 7-13 Generate Self Certificate Request 画面

3. 以下の項目を設定します。

項目	説明
Name	証明書の名前(識別子)を入力します。
Subject	生成される証明書の CN (Common Name) エントリが含まれます。サブジェクト名は通常次のフォーマットによっ て定義されます。 CN= <device name="" デバイス名="">, OU=<department 部署="">, O=<organization 組織="">, L=<city 市町="">,</city></organization></department></device>
	(例:CN=router1, OU=my_company, O=mydept, L=SFO, C=US.)
Hash Algorithm	アルゴリズムを以下から指定します。 「MD5」「SHA1」「SHA256」「SHA384」「SHA512」
Signature Key Length	シグニチャキーの長さを「512」「1024」「2048」から指定します。
Application Type	アプリケーションの種類を「HTTPS」「IPSec」から指定します。
IP Address	IP アドレスを入力します。本項目はオプションです。
Domain Name	ドメイン名を入力します。本項目はオプションです。
Email Address	メールアドレスを入力します。本項目はオプションです。

4. 「Save」をクリックし、設定を適用します。

追加した自己証明書は Certificate > Self Certificate Requests タブ画面に表示されます。

右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Easy VPN Setup (VPN セットアップ)

VPN > IPSec VPN > Easy VPN Setup

エクスポートされた IPSec VPN ポリシーをアップロードします。

- 1. VPN > IPSec VPN > Easy VPN Setup の順にメニューをクリックします。
- 2. 以下の画面で「参照 /Browse」をクリック → ポリシーの場所を指定し「Upload」をクリックします。

	🗥 Status		💻 Network	CA VPN	Security	O ^o Maintenance	
VPN » IPSec	VPN » Easy VPN Set	tup					00
This page wil	l guide you through	common and easy ste	ps to configure IPSec	VPN policies.			
Easy Setup	Site To Site V	PN Tunnel					
Easy Setu	p Site To Site VP	N Tunnel					
Easy VPM	l Setup	Г	参)	照			
			Upload				
図 7-14 F	asy VPN Setun	面面					

アップロード後、VPN > IPSec VPN > Policies 画面に読み込まれた VPN が表示されます。 右クリックし「Edit」(編集)、「Delete」(削除)を実行できます。

One To One Mapping (One To One マッピング)

VPN > IPSec VPN > Certificate > One To One Mapping

設定済みの「IPsec One To One マッピング」のリストを表示します。また、「One To One マッピング」の追加、編集、削除を行うことができます。

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

	🝘 Status	🛜 Wireless	💻 Network	🗥 VPN	💂 Security	🗘 Maintenance			
VPN » IPSec	VPN » IPSec VPN » One To One Mapping								
This page sho	ows the list of conf	igured IPsec One To	One Mapping, A user	can also add, ed	it and delete IPsec O	ne To One Mapping from	this page.		
IPSec One	To One Mappin	g List							
Show 10	 entries [Right c 	lick on record to get mo	re options]				٩		
Source IP	Range Start	🔂 Mapped	IP Range Start	😔 Ran	ge Length 🗧 🤅	B IPSec Policy Name	⇔		
			No data ava	ilable in table					
Showing O to	0 of 0 entries					First Previous Next	> Last >		
Add New	One To One Map	ping							

図 7-15 One To One Mapping 画面

2. マッピングリストを追加する場合、「Add New One To One Mapping」をクリックし以下の画面を表示します。

IPSec One To One Mapping Configur	ation	
Source IP Range Start Mapped IP Range Start Range Length IPSec Policy Name	[Range: 1 - 254]	

項目	説明
Source IP Range Start	One to One マッピングルールの開始 IP アドレスになる、プライベート(LAN) IP サブネットの IP アドレスを入力 します。
Mapped IP Range Start	プライベート LAN IP サブネットへの One to One マッピングサブネットの、マッピング範囲開始 IP として機能する IP アドレスを入力します。 この IP は、リモートホストからのトラフィックをローカル LAN ホスト / LAN ホストのサブネットにマッピングする ために使用されます。ローカルデバイスの IPSec ポリシーの「ローカル開始 IP アドレス」およびリモートデバイス の IPSec ポリシーの「リモート開始 IP アドレス」と同じである必要があります。
Range Length	プライベート / パブリックアドレスの One to One マッピング範囲を入力します。 設定可能範囲:1-254
IPSec Policy Name	One To One マッピングルールに紐付ける IPSec ポリシーを選択します。

4. 「Save」をクリックし、設定を適用します。

PPTP VPN (PPTP VPN 設定)

VPN > PPTP VPN

PPTP Server (PPTP VPN サーバ設定)

VPN > PPTP VPN > PPTP Server

本ルータを介して PPTP VPN 接続を確立することができます。PPTP を有効にし、LAN/WAN PPTP クライアントユーザが接続するためのサーバの設 定を行います。PPTP サーバが有効化されると、許可された IP 範囲に存在する PPTP クライアントは、ルータの PPTP サーバに到達できるようになり ます。その後、PPTP サーバ(トンネルのエンドポイント)によって認証されると、PPTP クライアントはルータによって管理されたネットワークに 接続可能となります。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することができます。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ことも可能です。

1. VPN > PPTP VPN > 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。

🝘 Status	🛜 Wireless	💻 Network	🕼 VPN	🚨 Security	🗢 Maintenance	
VPN » PPTP VPN » PPTP Server						00
PPTP allows an external user to range of IP addresses for clien with LAN hosts, access any ser only.	o connect to your route ts connecting to your ro vers present etc.MSCHAF	through the inter uter. The connect Authentication wi	net. This section ad clients can fu ll work with eith	allows you to enable nction as if they are er of MPPE 128-bit or	e/disable PPTP server and on your LAN (they can co Stateful MPPE Encryptio	define a ommunicate n methods
PPTP Server						
Server Setup Enable PPTP Server	Enal	ile IPv4	•			
PPTP Routing Mode	۲	IAT 🔍 Classical				
Range of IP Addresses (A Starting IP Address	llocated to PPTP Clier	ts)				
Ending IP Address						
Authentication Database Authentication	Loc	al User Database	•			
Authentication Supporte	d					
PAP		OFF				
СНАР	. 111	OFF				
MS-CHAP	111	OFF				
MS-CHAPv2	111	OFF				
User Time-out						
Idle Timeout	0	[Range: 30	0 - 1800] Seconds			
Netbios Setup						
Netbios		OFF				
		Save (ancel			

図 7-17 PPTP Server 画面

項目	説明					
Server Setup						
Enable PPTP Server	PPTP サーバを有効にするモードを選択します。: Enable IPv4 (IPv4)、Enable IPv6 (IPv6)、Disable(無効)					
PPTP Routing Mode	PPTP ルーティングモード を「NAT」または「Classical」から選択します。					
	Range of IP Addresses (Allocated to PPTP Client)					
Starting IP Address	PPTP クライアントに割り当てる IP アドレス範囲の開始 IP アドレスを入力します。					
Ending IP Address	PPTP クライアントに割り当てる IP アドレス範囲の終了 IP アドレスを入力します。					
IPv6 Prefix	IPv6 モードを選択した場合、IPv6 プレフィックスを入力します。					
IPv6 Prefix Length	IPv6 モードを選択した場合、IPv6 プレフィックス長を入力します。					
	Authentication Database					
Authentication	認証タイプを選択します。					
	Authentication Supported					
РАР	PAP 認証方式のサポートを有効にします。					
СНАР	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。					
	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。					
	Netbios Setup					
Netbios	「ON」にすると、VPN トンネルにおける NetBIOS ブロードキャストの通過を許可します。					

3. 「Save」をクリックし、設定を適用します。

PPTP Client(PPTP クライアント)

VPN > PPTP VPN > PPTP Client

本ルータに PPTP VPN クライアントを設定します。PPTP クライアントを使用し、PPTP サーバの存在するリモートネットワークに接続します。 クライアント有効化後、**Status > Active VPNs** 画面で PPTP VPN トンネルの接続を確立します。

1. VPN > PPTP VPN > 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。

🕐 Status 🛜 Wireless	💂 Network 🏠 VPN 🔒 Security 🗘 Maintenance
VPN » PPTP VPN » PPTP Client	0 0
PPTP VPN Client can be configured on this router. L	Using this client we can access remote network which is local to PPTP server.
PPTP Client	
Client	
Server IP	0.0.0.0
Tunnel Type	OFull Tunnel
Remote Network	0.0.0
Remote Netmask	0 [Range: 0 - 32]
Username	dlink
Password	•••••
Mppe Encryption	
Idle Timeout	0 [Range: 300 - 1800] Seconds
Auto Connect	ON THE
Time	2 [Range: 2 - 30] Minutes
	Save Cancel

図 7-18 PPTP Client 画面

項目	説明					
Client	PPTP クライアントを有効にします。					
Server IP	する PPTP サーバの IP アドレスを指定します。					
Tunnel Type	トンネルタイプを「Full Tunnel」(フルトンネル)または「Split Tunnel」(スプリットトンネル)から選択します。					
Remote Network	PPTP サーバにとってローカルとなるリモートネットワークアドレスを指定します。トンネルタイプに「Split Tunnel」を選択した場合のみ表示されます。					
Remote Netmask	リモートネットワークのサブネットマスクを指定します。トンネルタイプに「Split Tunnel」を選択した場合のみ 表示されます。					
Username	PPTP ユーザ名を指定します。					
Password	PPTP パスワードを指定します。					
Mppe Encryption	「ON」にして Microsoft Point-to-Point Encryption (MPPE) を有効にします。					
Idle Timeout	 マイドル状態時に PPTP サーバから切断するまでの時間を指定します。 ・ 設定可能範囲: 300-1800(秒) ・ 初期値: 0(秒) 					
Auto Connect	自動接続機能を有効または無効にします。 クライアントが切断された後、「Time」で指定した時間を過ぎると再度サーバへの接続を自動的に試します。					
Time	 再接続までの時間を入力します。 クライアントが切断された後、「Time」で指定した時間を過ぎると再度サーバへの接続を自動的に試行します。 ・ 設定可能範囲: 2-30(分) ・ 初期値: 2(分) 					

3. 「Save」をクリックし、設定を適用します。

PPTP Active Users (PPTP アクティブユーザリスト)

VPN > PPTP VPN > PPTP Active Users

PPTP の接続状況について表示します。

	🕋 Status		💻 Network	A VPN	Securit	у 🗢 м		
VPN » PPTP	VPN » PPTP Active	Users						00
Active PPTP	tunnels connections	are listed here, as LA	N VPN clients are ac	tive PPTP users.				
PPTP Acti	ve Users List							
Show 10	entries [No right	t click options]						٩
User Nam	2	0	Remote IP		€	PPTP IP		÷
			No data a	vailable in table				
Showing 0 to	0 of 0 entries					K First	Previous Next	> Last >

図 7-19 PPTP Active Users List 画面

項目	説明
User Name	現在接続中のユーザ名が表示されます。'*'が表示されている場合は、認証なしで接続中のユーザを意味します。
Remote IP	PPTP サーバによってユーザに割り当てられている IP アドレスが表示されます。
PPTP IP	サーバのローカル IP が表示されます。

PPTP サーバと L2TP サーバのトンネル数の上限値は以下のとおりです。

	DSR-1000/1000AC	DSR-500
PPTP トンネル数	25	15
L2TP トンネル数	25	15
合計	50	30

L2TP VPN(L2TP VPN 設定)

VPN > L2TP VPN

L2TP Server(L2TP VPN サーバ設定)

VPN > L2TP VPN > L2TP Server

本ルータを介して L2TP VPN 接続を確立することができます。

L2TP を有効にし、LAN/WAN L2TP クライアントユーザが接続するためのサーバの設定を行います。

L2TP サーバが有効化されると、許可された IP 範囲に存在する L2TP クライアントは、ルータの L2TP サーバに到達できるようになります。 その後、L2TP サーバ(トンネルのエンドポイント)によって認証されると、L2TP クライアントはルータによって管理されたネットワークに接続可 能となります。

L2TP 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することはできません。 また、L2TP サーバはローカルな L2TP 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ことも可能です。

1. VPN > L2TP VPN > 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。

🗥 Status 🛜 Wireles	s 💂 Network 🏠 VPN 💂 Security 🔅 Maintenance
VPN » L2TP VPN » L2TP Server	0 0
L2TP allows an external user to connect to your and define a range of IP addresses for clients co communicate with LAN hosts, access any servers L2TP Server	router through the internet, forming a VPN. This section allows you to enable/disable L2TP server innecting to your router. The connected clients can function as if they are on your LAN (they can present etc.).
Server Setup	
Enable L2TP Server	Enable IPv4
L2TP Routing Mode	NAT Classical
Range of IP Addresses (Allocated to L2TF Starting IP Address Ending IP Address	<pre> Clients) [</pre>
Authentication Database	
Authentication	Local User Database
Authentication Supported	
PAP	OFF
СНАР	OFF
MS-CHAP	OFF
MS-CHAPv2	OFF
Encryption	
Secret Key	ON
User Time-out	
Idle Timeout	0 [Range: 300 - 1800] Seconds
	Save Cancel

図 7-20 L2TP Server 画面

2. 以下の項目を設定します。

項目	説明				
	Server Setup				
Enable L2TP Server	L2TP サーバを IPv4 また IPv6 で有効、または無効にします。 - 「Enable IPv4」(IPv4 で有効) - 「Enable IPv6」(IPv6 で有効) - 「Disable」(無効)				
L2TP Routing Mode	L2TP ルーティングモードを「NAT または「Classical」から選択します。				
	Range of IP Addresses (Allocated to PPTP Client)				
Starting IP Address	L2TP クライアントに割り当てる IP アドレス範囲の開始 IP アドレスを入力します。				
Ending IP Address	L2TP クライアントに割り当てる IP アドレス範囲の終了 IP アドレスを入力します。				
IPv6 Prefix	IPv6 モードを選択した場合、IPv6 プレフィックスを入力します。				
IPv6 Prefix Length	IPv6 モードを選択した場合、IPv6 プレフィックス長を入力します。				
	Authentication Database				
Authentication	認証タイプを選択します。				
	Authentication Supported				

項目	説明				
PAP	PAP 認証方式のサポートを有効にします。				
СНАР	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				
Secret Key	暗号鍵(暗号キー)を指定します。				
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。				
	F適用します。				

L2TP Client (L2TP VPN クライアント)

VPN > L2TP VPN > L2TP Client

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。 クライアント有効化後、Status > Active VPNs 画面で L2TP VPN トンネルの接続を確率します。

1. VPN > L2TP VPN > 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。

🗥 Status 🗧	Wireless 📃 Netv	work Cas VPN	Security	O Maintenance	
VPN » L2TP VPN » L2TP Client					00
L2TP VPN Client can be configured on	his router. Using this client v	we can access remote net	work which is local t	o L2TP server.	
L2TP Client					
Client	ON STITE				
Server IP	0.0.0.0				
Tunnel Type	OFull Tunnel	Split Tunnel			
Remote Network	0.0.0				
Remote Netmask	0	Range: 0 - 32]			
Username	dlink				
Password	•••••				
Reconnect Mode	Always On	O On Demand			
Enable MPPE	ON THE				
Auto Connect	ON THE				
Time	2	Range: 2 - 30] Minutes			
	Save	Cancel			

図 7-21 L2TP Client 画面

2. 以下の項目を設定します。

項目	説明
Client	L2TP クライアントを有効にします。
Server IP	接続する L2TP サーバの IP アドレスを指定します。
Tunnel Type	トンネルタイプを「Full Tunnel」(フルトンネル)または「Split Tunnel」(スプリットトンネル)から選択します。
Remote Network	L2TP サーバにとってローカルとなるリモートネットワークアドレスを指定します。トンネルタイプに「Split
	Tunnel」を選択した場合のみ表示されます。
Remote Netmask	リモートネットワークのサブネットマスクを指定します。トンネルタイプに「Split Tunnel」を選択した場合のみ
	表示されます。
Username	L2TP ユーザ名を指定します。
Password	L2TP パスワードを指定します。
Reconnect Mode	再接続モードを指定します。「Always On」「On Demand」から選択できます。
Maximum Idle Time	「On Demand」を選択した場合、アイドル状態時に L2TP サーバから切断するまでの時間を指定します。(単位:秒)
Enable MPPE	「ON」にして Microsoft Point-to-Point Encryption (MPPE) を有効にします。
Auto Connect	自動接続機能を有効または無効にします。
	クライアントが切断された後、「Time」で指定した時間を過ぎると再度サーバへの接続を自動的に試します。
Time	「Auto Connect」を有効にした場合、自動接続を行うまでの時間(単位:分)を指定します。

3. 「Save」をクリックし、設定を適用します。

注意 L2TP クライアントが適切に設定・保存され L2TP サーバが起動すると、トンネルイニシエーションが自動的に開始されます。

L2TP Active Users(L2TP アクティブユーザリスト)

L2TP の接続状況について表示します。

	🝘 Status	🛜 Wireless	💻 Network	🕼 VPN	🔒 Security	🐡 Maintenance	
VPN » L2TP VP	N » L2TP Active	Users					00
Active L2TP tur	nnels connection	s are listed here, as l	AN VPN clients are a.	ctive L2TP users.			
L2TP Active	Users List						
Show 10 🔻	entries [No righ	it click options]					٩
User Name		â	Remote IP		⊖ L2	TP IP	⇔
			No data ava	ilable in table			
Showing 0 to 0 d	of 0 entries					K First A Previous Next	t 🗲 Last 🕅

図 7-22 L2TP Active Users 画面

項目	説明
User Name	現在接続中のユーザ名が表示されます。'*'が表示されている場合は、認証なしで接続中のユーザを意味します。
Remote IP	PPTP サーバによってユーザに割り当てられている IP アドレスが表示されます。
L2TP IP	サーバのローカル IP が表示されます。

PPTP サーバと L2TP サーバのトンネル数の上限値は以下のとおりです。

	DSR-1000/1000AC	DSR-500
PPTP トンネル数	25	15
L2TP トンネル数	25	15
合計	50	30

SSL VPN (SSL VPN 設定)

VPN > SSL VPN

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できます。

各ポリシーの優先度は、高いほうからユーザレベルポリシー > グループレベルポリシー > グローバルポリシーの順です。

これらのポリシーは、LAN の特定のネットワークリソースや IP アドレス /IP 範囲、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、ポリシータイプ(ユーザ、グループ、すべてのユーザ(グローバル))によってフィルタ可能です。

設定は以下の流れで行います。

(1)

SSL VPN ポリシーを追加するにあたり、ポリシーの適用先をユーザ、グループ、またはグローバル(すべての SSL VPN ユーザに適用)から指定します。 グループに適用する場合は、プルダウンメニューで利用可能な定義済みグループを選択します。 ユーザに適用する場合は、利用可能な定義済みユーザのリストから SSL VPN ユーザを選択します。

(2)

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となります。

ルータの LAN における特定のネットワークリソース、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つオプションごとに異なる設定フィールドが表示されます。

(例:定義済みリソースのリストからのネットワークリソースの選択、または IP アドレスの定義など)。

ポリシーをアドレスに適用する場合、ポート範囲 / ポート番号を定義できます。

(3)

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 / 拒否する Permission 設定を行います。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。

ポリシーは定義後にすぐに有効となります。

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)、Permission 設定は、ルータの定義済みポリシー一覧の概要で確認することができます

注意 本機能を設定するには、Maintenance > Management > Remote Management 画面でリモート管理を有効にする必要があります。

SSL VPN 対応 OS/ ブラウザー覧

SSL VPN 接続が可能な Windows OS、ブラウザー覧は以下の通りです。

OS	ブラウザ
Windows 7 (32bit)	IE9.0/11、Firefox 47.0.1
Windows 7 (64bit)	IE9.0
Windows 8 (32bit)	IE10.0、Firefox 47.0.1
Windows 8 (64bit)	IE10.0
Windows 8.1 (32bit) *	IE11、Firefox 47.0.1
Windows 8.1 (64bit) 💥	IE11

※ Windows 8.1 上での IE11 ブラウザ経由の SSL VPN スプリットトンネル接続には対応していません。

SSL VPN Server Policy (SSL VPN ポリシー設定)

VPN > SSL VPN > SSL VPN Server Policy $\checkmark = = =$

SSL VPN ポリシーを設定します。

1. VPN > SSL VPN > SSL VPN Server 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。

	🖾 Status	🛜 Wireless	💻 Network	යි VPN	<u> Security</u>	🍄 Maintenance		
VPN » S	/PN » SSL VPN » SSL VPN Server Policy							
This SSLV resource: was alrea SSL VPN	This SSLVPN Enable feature enables Option users to use SSLVPN functionality.Policies are useful to permit or deny access to specific network resources, IP addresses, or IP networks. They may be defined at the user, group or global level. By Default, a global PERMIT policy (not displayed) was already configured over all addresses and over all services/ports SSL VPN Server Policies List							
Show 10	entries	[Right click on record to	o get more options]				٩	
Name	♦ Servi	ice ⊖	Destination	⇔	Permission	⊖ Scope	θ	
			No data ava	ailable in table				
Showing	Showing 0 to 0 of 0 entries Next > Last >						Last 刘	
Add N	New SSL VPN Serv	ver Policy						

図 7-23 SSL VPN Server Policy 画面

SSL VPN ポリシーの追加

1. 「Add New SSL VPN Server Policy」をクリックして、以下の画面を表示します。

SSL VPN Server Policies Configuration		9
Policy Type SSL VPN Policy Apply Policy to Policy Name	Global O Group O User Network Resource	
ICMP	OFF	
Port Range / Port Number		
Defined Resources Permission	Permit Deny	

図 7-24 SSL VPN Server Policies Configuration (Network Resource) 画面

SSL VPN Server Policies Configuration	on	x
Policy Type	● Global [©] Group [©] User	
SSL VPN Policy Apply Policy to	IP Address	
Policy Name		
IP Address	or	
Port Range / Port Number		
Begin	[Range: 0 - 65535]	
End	[Range: 0 - 65535]	
Permission	 Permit Deny 	

図 7-25 SSL VPN Server Policies Configuration (IP Address) 画面

項目	説明
Policy Type	ポリシータイプを以下から選択します。
	・「Global」: ポリシーをすべての SSL VPN ユーザに適用します。
	・「Group」:ポリシーを選択したグループに適用します。
	・「User」: ポリシーを選択したユーザに適用します。
	SSL VPN Policy
Apply Policy to	ポリシーの適用先を以下から選択します。
Policy Name	ボリシーの識別名を指定します。
IP Address	ポリシーを「IPAddress」(IP アドレス)または「IP Netrwork」(IP ネットワーク)に適用する場合、IP アドレスを入力します。
Mask Length	ポリシーを「IP Netrwork」(IP ネットワーク)に適用する場合、マスク長(0-32)を入力します。
ICMP	ICMP トラフィックを含める場合は、「ON」に設定します。
	Port Range / Port Number
Begin / End	ポート範囲を入力します。すべての TCP/UDP ポートを含める場合は空欄にします。「Network Resource」を選択した場合は本 設定は不要です。
Service	「VPN Tunnel」(VPN トンネル)、「Port Forwarding」(ポートフォワーディング)、または「All」(両方)を選択します。ネットワー クリソースを選択した場合は本設定は不要です。
Defined Resources	「Network Resource」を選択した場合、プルダウンメニューから定義済みリソースを選択します。リソースが作成されていない場合は、「Resources(ネットワークリソース)」の手順を参照し、定義済みリソースを作成してください。
Permission	本ポリシーによって定義したリソースを「Permit」(許可)または「Deny」(拒否)に設定します。

3. 「Save」をクリックし、設定を適用します。

Portal Layouts(ポータルレイアウトの作成)

リモート VPN ユーザの認証時に表示される、カスタムページを作成することができます。 カスタムページには、ログイン手順やサービス等の情報を記載することが可能です。

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

	A Status	🛜 Wireless	💻 Network	B VPN	Security	O Maintenance	
VPN » SSL V	/PN » Portal Layouts						00
The table lis custom page specific to a SSL VPN P Show 10	ts the SSL portal lay for remote SSL VPN domain are useful t ortal Layouts Li	routs configured for t users that is present o present on the aut st ick on record to get mo	this device and allows se ted upon authentication. hentication portal. Porta	veral operatior Login instruct als are assigned	is on the portal layout ions, available service I to the user domain.	s. The router allows you t s, and other usage detail:	o create a s that are
Lavout Na	ime	O Use Cou	unt é	Portal URI			•
SSLVPN		0		https://0.0.0	.0:443/portal/SSLVPN		
Showing 1 to	1 of 1 entries				L1	First J Previous 1 Next	t 🔀 Last 刘
Add New	SSL VPN Portal	Layout					

図 7-26 Portal Layouts 画面

2. レイアウトを追加する場合は、「Add New SSL VPN Portal Layout」をクリックし以下の画面を表示します。

Portal Layout and Theme Name	
Portal Layout Name	
Login Profile Name	default
Portal Site Title	
Banner Title	
Banner Message	
Display Banner Message	OFF
on Login Page	
HTTP Meta Tags for Cache	OFF
Control (Recommended)	
ActiveX Web Cache Cleaner	OFF
SSL VPN Portal Authentication	
Authentication Type	Local User Database
Group	None
SSL VPN Portal Pages to Display	
VPN Tunnel page	OFF
Port Forwarding	OFF

図 7-27 SSL VPN Portal Layout Configuration 画面

- 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、ルータの Web GUI の SSL VPN メニュー で「Portal URL」リンクをクリックしたときに開くページと同じです。
- 3. 以下の項目を設定します。

項目	説明
Portal Layout Name	ポータル名を英数字で入力します。ポータル名は、SSL ポータル URL パスの一部として使用されます。
Login Profile Name	ログインプロファイル名を指定します。
Portal Site Title	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。 この項目はオプションです。この項目はオプションです。
Banner Title	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です。この項目はオプションです。
Banner Message	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です。この項目はオプションです。
Display Banner Message on Login Page	ログインページのバナータイトル及びメッセージの表示を「ON」(表示)または「OFF」(非表示)に設定します。
HTTP Meta Tags for Cache Control (Recommended)	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。 推奨される設定:「ON」
ActiveX Web Cache Cleaner	SSL VPN ポータルにユーザがログインする毎に、ActiveX キャッシュ制御 Web クリーナ機能がゲートウェイか らクライアントのブラウザに対して実行されます。
Authentication Type	ドロップダウンメニューで認証の種類を選択します。
Group	ドロップダウンメニューで所属するグループを選択します。
VPN Tunnel Page	リモートユーザによる VPN トンネルページの閲覧を許可します。
Port Forwarding	リモートユーザによるポートフォワーディングページの閲覧を許可します。

4. 「Save」をクリックし、設定を適用します。

追加したレイアウトは Portal Layouts 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Resources (ネットワークリソース)

VPN > SSL VPN > Resources $\checkmark = = =$

ネットワークリソースは、LAN IP アドレスのサービスまたはグループです。 SSL VPN ポリシーを簡単に作成、設定するために使用します。 複数のリモート SSL VPN ユーザを対象に同様のポリシーを作成する場合、本機能によって設定時間を短縮できます。

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、サポートする SSL サービスのうちの 1 つまたはすべてを割り当てます。 作成したネットワークリソースを編集し、サービスに紐づくオブジェクトタイプ(IP アドレスまたは IP 範囲)を設定することも可能です。 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、ポート範囲 / ポート番号を定義できます。

ネットワークリソースの追加

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

	🖾 Status	후 Wir		🖳 Network	CAS VPN	Security	ф ^о м		
VPN » SSL	VPN » Resources								00
Network re when crea or services re-routed that is bei SSL VPN	esources are servic ting similar policie: s after they login t based on configure ng made accessible Resources List	es or groups s for multiple o the User Po d port forwa to remote u	of LAN IP a remote SS ortal and la rding rules sers.	uddresses that are us L VPN users. Port for unch the Port Forwa , Port forwarding req	ed to easily creat warding allows re rding service. Tra uires the identifi	e and configure S mote SSL users to ffic from the remo cation of the TCP	SL VPN policies. access specifie te user to the application and	This shortcut d network app router is dete local server I	t saves time blications cted and P address
Show 10	▼ entries	[Right click o	n record to g	et more options]					٩
Name	Service	θ	Туре	e Resource Ob	ect	e Port	e Mask I	ength	θ
			11.14.4.4.5.5. 	No data ava	ilable in table	and the second second			
Showing 0	to 0 of 0 entries						J. First Pr	evious Next >	Last 🕅
Add N	ew Resource								
Port For	warding List for	Configure	d Applic	ations					
Show 10	• entries							(٩
Local Se	erver IP Address				О ТСР	Port Number			Θ
				No data ava	ilable in table				
Showing 0	to 0 of 0 entries						First	evious Next >	Last 刘
Add N	ew Rule								
Port For	warding List for	Configure	d Host N	ames					
Show 10	▼ entries								٩
Local Se	erver IP Address			🗘 Full	y Qualified Dom	ain Name			θ
				No data ava	ilable in table				
Showing 0	to 0 of 0 entries						First I Pr	evious Next >	Last 刘
Add No	ew Rule								

図 7-28 Resources 画面

2. 「Add New Resource」をクリックして、以下の画面を表示します。

SSL VPN Resources		
Resource Name		
Service	VPN Tunnel Port Forwarding All A	
Resource Object Configuration		
ICMP	OFF	
Object Type	IP Network	
Object Address		
Mask Length	[Range: 0 - 32]	
Port Range / Port Number		
Begin	[Range: 0 - 65535]	
End	[Range: 0 - 65535]	
		Serve

3. 以下の項目を設定します。

項目	説明
	SSL VPN Resource
Resource Name	リソースに固有の名称を設定します。
Service	リソースの SSL VPN サービスを「VPN Tunnel」「Port Forwarding」「All」からを選択します。
	Resource Object Configurarion
ICMP	「ON」にして ICMP トラフィックを有効にします。
Object Type	オブジェクトのタイプを「IP Address」「IP Network」から選択します。
Object Address	IP アドレスを入力します。
Mask Length	オブジェクトのタイプを「IP Network」に設定した場合、マスク長を指定します。 ・設定可能範囲:0-32
	Port Range / Port Number
Begin / End	オブジェクトのポート範囲(開始 / 終了)を指定します。

4. 「Save」をクリックし、設定を適用します。

追加したネットワークリソースは、Resources 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

ポートフォワーディングルールの追加

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サービスを起動すると、リモート SSL ユーザは特定のネットワークアプリケーションまたは サービスにアクセスできます。

リモートユーザからルータへのトラフィックは、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、再ルーティングされます。

内部ホストサーバまたは TCP アプリケーションは、リモートユーザがアクセス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には、トンネリングするアプリケーションのローカルサーバの IP アドレスと TCP ポート番号を入力します。

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

	atus	The Wireless	🖳 Network	C VPN	Security	O ^o Maintenance	
N » SSL VPN » R	lesources						•
twork resources a en creating simila services after the routed based on it is being made a	are services of r policies fo by login to th configured p ccessible to	or groups of LAN I or multiple remote he User Portal and port forwarding rul remote users.	P addresses that are us SSL VPN users. Port for launch the Port Forwa es. Port forwarding rec	ed to easily create a warding allows remot rding service. Traffic juires the identificati	nd configure SSL e SSL users to ac from the remote on of the TCP ap	VPN policies. This shortcut cess specified network app user to the router is dete plication and local server If	saves dicatio cted a Paddro
now 10 💌 entri	ies [Ri	ight click on record t	o get more options]				
ame O	Service		A Resource Ob	iect	A Port		
		A CARLES AND A CARLES	No data avi	silable in table		and the second se	
owing 0 to 0 of 0 en	tries					First Previous Next	Last
						Tress Christian Howe X	
ow 10 💌 entri	ies						
I AL SHIVEL IP A	TITLE MALE				rt Number		
ocal Server IP A	duress		No data avi	ailable in table	rt Number		
owing 0 to 0 of 0 en	ntries		No data avi	O TCP Por silable in table	rt Number	First Previous Next 🗦	Last
owing 0 to 0 of 0 en Add New Rule	ntries		No data avi	O TCP Po	rt Number	() First 🔤 🖞 Previous 🛛 Next 🗦	Las
Notes Server IP A Notes Server IP A Add New Rule rt Forwarding	utries List for Co	onfigured Host	No data avi	O TCP Po	rt Number	L] First 🔄 Previous Next 🗦	Last
Add New Rule rt Forv/arding 10 10 10 10 entri	utries List for Co	onfigured Host	No data avi	O TCP Por	rt Number	l First Previous Next >	Last
Add New Rule rt Forwarding now 10 • entri ocal Server IP A	utries List for Co ies ddress	onfigured Host	No data av Names	Q TCP Por silable in table	Name	L First Previous Next >	Last
Add New Rule rt Forwarding now 10 • entri ocal Server IP A	List for Co	onfigured Host	No data av Names O Fut No data av	y Qualified Domain vilable in table	Name	L First Previous Next >	Last
Add New Rule Add New Rule rt Forwarding tow 10 re entri ocal Server IP A towing 0 to 0 of 0 en	List for Co ddress ddress	onfigured Host	No data avi Names O Full No data avi	Qualified Domain ilable in table	Name	First Previous Next >	Last
Add New Rule iowing 0 to 0 of 0 en Add New Rule rt Forwarding iow 10 • entri ocal Server IP A owing 0 to 0 of 0 en	List for Co ies iddress	onfigured Host	No data avi Names No data avi	CP Por silable in table y Qualified Domain silable in table	Name	L First / Previous Next >	Last

図 7-30 Resources 画面

2. 「Port Forwarding List for Configured Applications」または「Port Forwarding List for Configured Host Names」内にある「Add New Rule」をクリックします。

how 10 💌 entries		
ocal Server IP Address	TCP Port Number	
	No data available in table	
howing 0 to 0 of 0 entries		First Previous Next > Last
Add New Rule		
ort Forwarding List for Configured H	Host Names	
nt Forwarding List for Configured H	Host Names	
ort Forwarding List for Configured H how 10 v entries .ocal Server IP Address	Host Names O Fully Qualified Domain Name	,
ort Forwarding List for Configured H how 10 v entries .ocal Server IP Address	Host Names O Fully Qualified Domain Name No data available in table	
rt Forwarding List for Configured H now 10 • entries ocal Server IP Address nowing 0 to 0 of 0 entries	Host Names O Fully Qualified Domain Name No data available in table	I First J Previous Next > Last

図 7-31 Port Forwarding List for Configured Applications/Host Names 画面

3. 以下の画面で設定を行います。

Port Forwarding List for Conf	gured Applications	X
Local Server IP Address TCP Port Number	[Range: 0 - 65535]	

図 7-32 Port Forwarding List for Configured Applications 画面 「Local Server IP Address」: ローカルサーバの IP アドレスを入力します。 「TCP Port Number TCP」: ポート番号を入力します。

Port Forwarding List for Host Con	figuration	×
Local Server IP Address		
Fully Qualified Domain Name		
In T-33 Port Forwarding List for Ho	t Configuration 画页	

図 7-55 For Forwarding List for Host Configuration 画面 「Local Server IP Address」: ローカルサーバの IP アドレスを入力します。 「Fully Qualified Domain Name」: ドメイン名(FQDN)を入力します。

4. 「Save」をクリックし、設定を適用します。

SSL VPN Client(SSL VPN クライアント設定)

VPN > SSL VPN > SSL VPN Client $\checkmark = = =$

SSL VPN トンネルクライアントにより、本ルータとブラウザ側マシンとのポイントツーポイント接続が可能となります。 SSL VPN クライアントがユーザポータルから起動されると、企業サブネット内の 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、 UFTート SSLVDN クライアントのマシントで特別たきットワーク設定をせずに、 ローカルアプリケーションをプライベートきットワーク

これにより、リモート SSLVPN クライアントのマシン上で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をプライベートネットワー ク上のサービスにアクセスさせることができます。

VPN トンネルクライアントの仮想(PPP)インタフェースアドレスは、LAN 上の物理デバイスと重複しないようにしてください。 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に設定します。

本ルータは「Full Tunnel」(フルトンネル)と「Split Tunnel」(スプリットトンネル)をサポートしています。 フルトンネルモードでは、VPN トンネル経由で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。 スプリットトンネルモードでは、事前に指定したクライアントルートに基づいて、プライベート LAN ヘトラフィックを送信します。 これらのクライアントルートは、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許可し、特定の LAN サービスに対するアクセ ス制御を可能にします。

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

SSL VPN tunnel client provides a point	to-point connection	between the browser-s	ide machine and this o	levice. When a SSL VPN client is	
nched from the user portal, a "network lications to talk to services on the priv	adapter" with an IP ate network without	address, DNS and WINS any special network co	settings is automatical onfiguration on the re	ly created, which allows local mote SSL VPN client machine.	
VPN Client					
Full Tuppel Support					
DNS Suffix					
Drimary DNC Server					
Secondary UNS Server					
Client Address Range Begin	192.168.251	1			
Client Address Range End	192.168.251	254			
LCP Timeout	60	[Range: 1 - 999999] Secon	nds		

図 7-34 SSL VPN Client 画面

2. 以下の項目を設定します。

項目	説明
Full Tunnel Support	フルトンネルを「ON」または「OFF」にします。
DNS Suffix	SSL VPN クライアントに付与される DNS サフィックス名を入力します。本項目はオプションです。
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 アドレスを入力します。本項目は オプションです。
Secondary 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セカンダリ DNS サーバの IP アドレスを入力します。 本項目はオプションです。
Client Address Range Begin	クライアントに割り当てる IP アドレス範囲の開始 IP アドレスを入力します。
Client Address Range End	クライアントに割り当てる IP アドレス範囲の終了 IP アドレスを入力します。
LCP Timeout	LCP ECHO の送信間隔を入力します。(単位:秒)

3. 「Save」をクリックし、設定を適用します。

Client Routes (SSL VPN クライアントルート設定)

VPN > SSL VPN > Client Routes

SSL VPN クライアントルートの設定を行います。

SSL VPN クライアントが企業ネットワークと異なるサブネット内の IP アドレスをアサインされた場合、VPN トンネルを通じてプライベート LAN に アクセスできるようにクライアントルートを追加します。同様に、VPN ファイアウォールを通じてリモート SSL VPN クライアントにプライベートト ラフィックを送信できるように、プライベート LAN のファイアウォール(通常はこのルータ)上にスタティックルートを設定する必要があります。

スプリット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。

・宛先ネットワーク:VPN トンネルクライアントから見た LAN のネットワークアドレスまたは宛先ネットワークのサブネット情報を設定します。 ・サブネットマスク:宛先ネットワークのサブネット情報を指定します。

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

	🙆 Status	🛜 Wireless	💻 Network	CA VPN	Security	O Maintenance
/PN » SSL	VPN » Client Route	25				00
The Config Iddresses i The table : network th	ured Client Routes is redirected throu shows the destinati ien in SPLIT Tunnel Client Routes L	entries are the routin gh the SSL VPN tunnel: on routes that will be mode you should add ist	g entries which will b s, and all other traffic configured on the SSI the LAN subnet as the	e added by the SS c is redirected usi L VPN client. For e destination subn	L VPN Client such tha ng the hosts (SSL VPN example if the SSL VPI et on this device.	at only traffic to these destination I Clients) native network interface. N Client wishes to access the LAN
Show 10	▼ entries	[Right click on record to	get more options]			٩
Destinat	tion Network			Ŷ	Subnet Mask	0
			No data av	ailable in table		
Showing 0	to 0 of 0 entries					First Previous Next > Last >
Add Ne	ew Client Route	,				

図 7-35 Client Routes 画面

クライアントルートの追加

1. 「Add New Client Route」をクリックして、以下の画面を表示します。

SSL VPN Client Route Configuration	8
Destination Network Subnet Mask	
	Save

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見た LAN のネットワークアドレスまたは宛先ネットワークのサブネット情報を設定します。
Subnet Mask	宛先ネットワークのサブネット情報を指定します。

^{3. 「}Save」をクリックし、設定を適用します。

OpenVPN(**OpenVPN** 設定)

VPN > OpenVPN メニュー

Open VPN の設定を行います。

OpenVPN は、VPN を構築するためのアプリケーションです。VPN を利用することにより、インターネット上に仮想的にネットワークを構築し、場所の離れた拠点間、またモバイル環境とオフィス内 LAN の間などを安全に接続することができます。 また、SSL VPN 機能の代替となる OmniSSL 機能の設定方法についても説明します。

OpenVPN 設定

VPN > OpenVPN > OpenVPN Settings $\checkmark = = =$

OpenVPN では、証明書やユーザ名 / パスワードを使用したピアの相互認証が可能です。マルチクライアント - サーバ設定で利用した場合、サーバは 署名と CA(認証局)を使用して、すべてのクライアントに対して認証証明書をリリースすることができます。OpenVPN は、本ルータを介して確立 することができます。

OpenVPN のモードを「Server」モード、「Client」モード、「Access Server Client」モードから選択します。アクセスサーバクライアントモードで接 続するには、「OpenVPN Access Server」から自動ログインプロファイルをダウンロードし、本ルータにアップロードする必要があります。

1. VPN > OpenVPN > OpenVPN 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。

	nfiguration page allows the user to conf	figure OpenVPN as a server or client				
IIVPN	seccings					
OpenVP	N	ON THE				
Mode		Server O Client O Acces	s Server Client			
VPN Net	twork	128.10.0.0				
VPN Net	tmask	255.255.0.0				
Duplica	te CN	OFF				
Port		1194 [Default: 1194, Range: 1024 - 65535]				
ſunnel	Protocol	O TCP UDP				
Encrypt	ion Algorithm	AES-128				
lash Al	gorithm	SHA1				
funnel	Туре	Full Tunnel O Split Tunnel				
Isos Pa	red Auth					
ortific	sed Auth	DISABLE				
ertific	ace verification					
	rome	default				
Certs P	CLC LL LL	Server Cert Subject Name	Client Cert Subject Name	Туре	CA key Status	
Certs Pr	CA Subject Name					
lerts Pi	C=TW, ST=Taiwan, L=Taipei, O=D-Link Cor	C=TW, ST=Taiwan, L=Taipei, O=D-Lin	C=TW, ST=Taiwan, L=Taipei, O=D-Lin	Default:Serv		
ame efault	CA SUBJECT Name C=TW, ST=Taiwan, L=Taipei, O=D-Link Cor poration, OU=Certificate for DSR (Self-Sign	C=TW, ST=Taiwan, L=Taipei, O=D-Lin k Corporation, OU=Certificate for DSR	C=TW, ST=Taiwan, L=Taipei, O=D-Lin k Corporation, OU=Certificate for DSR	Default:Serv er & Client	Available	
ame	CA Subject Name C=TW, ST=Taiwan, L=Taipei, O=D-Link Cor poration, OU=Certificate for DSR (Self-Sign ed), CN=D-Link Corporation CA	C=TW, ST=Taiwan, L=Taipei, O=D-Lin k Corporation, OU=Certificate for DSR (Self-Signed), CN=server	C=TW, ST=Taiwan, L=Taipei, O=D-Lin k Corporation, OU=Certificate for DSR (Self-Signed), CN=client	Default:Serv er & Client	Available	

図 7-37 OpenVPN Settings (Server) 画面

2. 以下の項目を設定します。

項目	説明
Open VPN	Open VPN を「ON」または「OFF」にします。
Mode	モードを以下から選択します。
	・「Server」:サーバモード
	・「Client」:クライアントモード
	・「Access Server Client」:アクセスサーバクライアントモード
	選択したモードによって、画面に表示される項目が異なります。
	Server
VPN Network	VPN の IP ネットワークを入力します。
VPN Netmask	ネットマスクを入力します。
Duplicate CN	有効にすると、複数のクライアントに同じ認証を使用することが可能になります。

項目	説明
Port	使用するポート番号を入力します。初期値:1194
Tunnel Protocol	「TCP」または「UDP」を選択します。初期値:UDP
Encryption Algorithm	暗号化方式を選択します。
Hash Algorithm	ハッシュアルゴリズムを選択します。
Tunnel Type	トンネルタイプを以下から選択します。
	・「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、事前定義されたクライアントルートに基づくプライベート LAN のみにトラ フィックをリダイレクトします。
Client to Client	有効にした場合、スプリットトンネルにおいて Open VPN クライアント同士の相互通信が可能になります。トンネル
Communication	タイプに「Split Tunnel」を選択した場合のみ表示されます。 • 初期値:無効
User Based Auth	ユーザ名 / パスワードを使用した追加の認証方式を有効化 / 無効化します。
Certificate Verification	本機能を有効化した場合、クライアント証明書が必要になります。無効化した場合、クライアントはユーザ名/パスワードのみを使用して認証を行います。 ・ 初期値:有効
Certs Profile	設定されたサーバ / クライアント用に証明書がアップロードされているプロファイルを選択します。 初期値では、サーバ証明書とクライアント証明書の両方を持つデフォルトプロファイルが選択されています。
TLS Authentication Key	TLS 認証を有効化し、追加の認証レイヤを追加します。TLS キーがアップロードされた場合にだけチェックされます ・ 初期値:無効
Invalid Client Certificate	 不正なクライアント証明書をブロックするファシリティを追加します。ブロックされるクライアント証明書のリスト を含む CRL 形式の証明書が必要です。 初期値: 無効
	Client
Server IP	クライアントが接続する OpenVPN サーバ IP アドレスを入力します。
Failover Server IP	フェイルオーバ IP アドレスを入力します。
Port	使用するポート番号を入力します。初期値 : 1194
Tunnel Protocol	「TCP」または「UDP」を選択します。初期値 : UDP
Encryption Algorithm	暗号化方式を選択します。
Hash algorithm	ハッシュアルゴリズムを選択します。
Auto Connect	自動接続を有効または無効にします。
	有効にした場合、自動的に再接続を試行するまでの間隔を設定します。
	Status > Network Information > Active VPNs > OpenVPN Connections 画面でもサーバへの接続または切断を設定できます。
Interval	自動的に再接続を試行するまでの間隔を設定します。(単位:分)
User Based Auth	ユーザ名 / パスワードを使用した追加の認証方式を有効化 / 無効化します。
Certificate Verification	本機能を有効化した場合、クライアント証明書が必要になります。無効化した場合、クライアントはユーザ名/パスワードのみを使用して認証を行います。 ・ 初期値:有効
Certs Profile	設定されたサーバ / クライアント用に証明書がアップロードされているプロファイルを選択します。
	初期値では、サーバ証明書とクライアント証明書の両方を持つデフォルトプロファイルが選択されています。
TLS Authentication Key	TLS 認証を有効化し、追加の認証レイヤを追加します。TLS キーがアップロードされた場合にだけチェックされます ・ 初期値:無効
	Access Server Client
Port	使用するポート番号を入力します。初期値:1194
Enable Private Tunnel	「ON」にした場合、安全なアクセス接続を提供する www.privatetunnel.com に接続します。 初期値:「OFF」
	以下の項目は「Enanle Private Tunnel」を「ON」にした場合のみ表示されます。
	・「Email Address」:www.privatetunnel.com に登録する Email アドレスを入力します。
	 Password」:ハスワードを人力します。ハスワードには央徴学を使用可能です。 「VDN Cluster L: VDN クラスタのタイプを選択します
Auto Connact	・「VPN Cluster」、VPN ソフスタのタイフを迭折します。
	日期が変形でで行対ようには無対応とします。行対応とした場合、日期的に円接続を試行するよどの前隔を設定します。 Status > Network Information > Active VPNs > OpenVPN Connections 画面でもサーバへの接続または切断を設定でき ます。
Interval	自動的に再接続を試行するまでの間隔を設定します。(単位:分)
Upload Status	設定ファイルのアップロード状況について表示します。
File	「Browse/参照」をクリックし、設定ファイルをアップロードします。

3. 「Save」をクリックし、設定を適用します。

OpenVPN Certificates(Open VPN 証明書)

VPN > OpenVPN > OpenVPN Certificates メニュー Open VPN では、証明書を使用した認証を行うことができます。 pem 形式の証明書とキーのアップロード方法について説明します

OpenVPN Certificates (Open VPN 証明書)

1. VPN > Open VPN > OpenVPN Certificates > OpenVPN Certificates タブの順にメニューをクリックし、以下の画面を表示します。

	🖾 Status		ess 📃 Net	work 🏠	VPN	Security	🗘 Main		
VPN » Ope	enVPN » OpenVPN Cert	tificates							00
OpenV	OpenVPN Certificates TLS Key CRL Certificates								
Openvpn pr	ovides authentication	using certifica	tes. This page allow	ws you to upload	required OpenVF	'N certificates	and keys.		
OpenVPN	Certificates List								
Show 10	✓ entries [Right cli	ck on record to g	et more options]						٩
Name 🗘	CA Subject Name	θ	Server Cert Sub Name	ject ⊖	Client Cert Sub Name	ject \varTheta	Туре 🕀	CA key Status ⊖	Status ⊖
default	C=TW, ST=Taiwan, L=Ta Corporation, OU=Certifi If-Signed), CN=D-Link Co	ipei, O=D-Link cate for DSR (Se orporation CA	C=TW, ST=Taiwan, L ink Corporation, OU: DSR (Self-Signed), Cl	=Taipei, O=D-L (=Certificate for i N=server I	=TW, ST=Taiwan, L nk Corporation, OU ISR (Self-Signed), C	=Taipei, O=D-L =Certificate for N=client	Default:Ser ver & Client	Available	Active
Showing 1 to 1 of 1 entries 1 Next > Last >									
Upload	OpenVPN Certs	Generate C	penVPN Certs						

図 7-38 OpenVPN Certificates > OpenVPN Certificates タブ 画面

項目	説明
Name	プロファイル名が表示されます。
CA Subject Name	CA証明書のサブジェクト名が表示されます。
	名則には、C、SI、L、O、OU、CN、Eなどのコンテンツからまれます。CN は CA 証明書のコモンネームです。
Server Cert Subject Name	サーバ証明書のサブジェクト名が表示されます。
	名前には、C、ST、L、O、OU、CN、E などのコンテンツが含まれます。CN は CA 証明書のコモンネームです。
	サーバ証明書が存在しない場合、「N/A」と表示されます。
Client Cert Subject Name	クライアント証明書のサブジェクト名が表示されます。
	名前には、C、ST、L、O、OU、CN、E などのコンテンツが含まれます。CN は CA 証明書のコモンネームです。
	クライアント証明書が存在しない場合、「N/A」と表示されます。
Туре	プロファイルのタイプが表示されます。
	タイプは、証明書(Generated/Uploaded/Default)と設定したモード(Server/Client/Server & Client)の組み合わせです。
CA Key Status	CA キーのステータスが表示されます。
	・「N/A」:CA キーが存在しません。
	・「Available」:CA キーが使用可能です。
Status	プロファイルのステータスが表示されます。
Upload OpenVPN Certs	クリックすると、Server/Client Certificate Configuration 画面が表示されます。
Generate OpenVPN Certs	クリックすると、OpenVPN Certificate Configuration 画面が表示されます。

■ Open VPN 証明書のアップロード

1. 「Upload OpenVPN Certs」をクリックし、以下の画面を表示します。

Server/Client Certificate Configur	ation	×
Name		
Mode	Server OClient OServer & Client	
Trusted Certificate (CA Certificate)	参照… Upload	
CA Key	参照 Upload Optional	
Server Certificate	参照… Upload	
Server Key	参照… Upload	
DH Key	参照… Upload	
	Save	

図 7-39 Server/Client Certificate Configuration 画面

2. 以下の項目を設定します。

項目	説明
Name	プロファイル名が表示されます。
Mode	モードを以下から選択します。
	「Server」「Client」「Server & Client」
	選択したモードによって、以降に表示される項目が異なります。
Trusted Certificate (CA Certificate)	「Browse」をクリックし、pem 形式の CA 証明書をアップロードします。
СА Кеу	「Browse」をクリックし、pem 形式の CA キーをアップロードします。
Server Certificate	「Browse」をクリックし、pem 形式のサーバ証明書をアップロードします。
Server Key	「Browse」をクリックし、pem 形式のサーバキーをアップロードします。
Client Certificate	「Browse」をクリックし、pem 形式のクライアント証明書をアップロードします。
Client Key	「Browse」をクリックし、pem 形式のクライアントキーをアップロードします。
DH Key	「Browse」をクリックし、pem 形式の Diffie Hellman キーをアップロードします。

3. 「Save」をクリックし、設定を適用します。

■ Open VPN 証明書の生成

1. 「Generate OpenVPN Certs」をクリックし、以下の画面を表示します。

OpenVPN Certificate Configurat	ion Astro	\bigotimes
Name		^
Country Name (C)		
State or Province Name (ST)		
Locality Name (L)		
Organization Name (O)		
Organizational Unit Name (OU)		
CA Certificate CN		
Email Name (E)		
Key Encryption Length	1024	
Valid Through	10 [Range: 1 - 20] years	
Server Certificate CN		
Client Certificate CN		
Hash Algorithm	SHA1	
		*
		Save

図 7-40 OpenVPN Certificate Configuration 画面

項目	説明			
Name	プロファイル名が表示されます。			
Country Name (C)	ISO 形式の 2 文字の国名コードを入力します。日本の場合は「JP」です。			
State or Province Name (ST)	都道府県名を入力します。			
Locality Name (L)	市区町村名を入力します。			
Organizational Name (O)	企業名などの組織名を入力します。組織名は、公的機関に登録されている正式名称を入力してください。			
Organizational Unit Name (OU)	組織内の部門を区別するため、証明書を取り扱う組織のユニット名を入力します。			
CA Certificate CN	CA 証明書の CN(コモンネーム)を入力します。			
	コモンネームは、サーバの DNS ルックアップに使用されるドメイン名です。(例:www.mydomain.com)			
	ブラウザは、ウェブサイトを識別するためにこの情報を使用します。お使いのホスト名を変更した場合、別のデジ			
	タル ID を要求する必要があります。			
	ホストに接続しているクライアントブラウザは、デジタル ID のコモンネームと URL が一致しているか確認します。			
Email Name (E)	組織への連絡に使用する E メールアドレスを入力します			
Key Encryption Length	接続の暗号化に使用される暗号化キーの長さを選択します。			
Valid Through	証明書の有効期間を入力します。(単位:年)			
Server Certificate CN	使用するサーバ証明書のコモンネームを入力します。			
Client Certificate CN	使用するクライアント証明書のコモンネームを入力します。			
Hash Algorithm	証明書で使用するハッシュアルゴリズムを、「SHA1」または「SHA256」から選択します。			

3. 「Save」をクリックし、設定を適用します。

TLS Key(TLS キー)

pem 形式の TLS キーをアップロードします。

1. VPN > Open VPN > OpenVPN Certificates > TLS Key タブの順にメニューをクリックし、以下の画面を表示します。

	Characteristics		📃 Network	⇔ vpn	🔒 Security	Maintenance	
/PN » Oper	nVPN » OpenVPN Cer	tificates » TLS Key					00
OpenVF	PN Certificates	S Key CRL Certific	ates				
)penvpn pro	ovides tls authenticat	tion using tls key. Thi	s page allows you to i	upload required ce	ertificates.		
LS Key L	.ist						
Show 10	✓ entries [Right cli	ick on record to get mor	re options]				٩
Name		٥	TLS Uploaded				. 6
		2000 	No data av	ailable in table			
Showing 0 to	0 of 0 entries					First Previous Next	> Last >

図 7-41 OpenVPN Certificates > TLSKey タブ 画面

2. 「Add TLS Key」をクリックします。

TLS Key Configuration	8
Name TLS Authentication Key	参照
図 7-42 TLS Key Configuration 画面	

- 3. TLS キーの名前を入力します。OpenVPN Setting 画面で識別可能とするためです。
- 4. 「Browse/参照」をクリックし、pem 形式の TLS キーをアップロードします。
- 5. 「Save」をクリックし、設定を適用します。

CRL Certificate(CRL 証明書)

Open VPN では、CRL 証明書を使用した CRL 認証が可能です。 必要な証明書のアップロード方法について説明します。

1. VPN > Open VPN > OpenVPN Certificates > CRL Certificate タブの順にメニューをクリックし、以下の画面を表示します。

	🙆 Status		📃 Network	🚯 VPN	🔒 Security	O ^o Maintenance	
VPN » Open	VPN » OpenVPN Cer	rtificates » CRL Certific	cate				0 0
OpenVP	N Certificates TI	LS Key CRL Certific	ates				
Openvpn pro	vides crl authentica	ation using crl certific	ate. This page allows	you to upload req	uired certificates.		
CRL Certif	ricate List						
Show 10	✓ entries [Right cl	lick on record to get mo	re options]				٩
Name		۵	CRL Uploaded				θ
No data available in table							
Showing 0 to	0 of 0 entries					First Previous Next	t 🔪 Last 💥
Add CRL	Certificate						

図 7-43 OpenVPN Certificates > CRL Certificate タブ画面

2. 「Add CRL Certificate」をクリックします。

CRL Certificate Configuration		X
Name		
CRL Certificate	参照	

図 7-44 CRL Certificate Configuration 画面

- 3. CRL 証明書の名前を入力します。OpenVPN Setting 画面で識別可能とするためです。
- 4. 「Browse/参照」をクリックし、pem 形式の CRL 証明書をアップロードします。クライアント証明書は無効になります。
- 5. 「Save」をクリックし、設定を適用します。
OpenVPN Server Policy(Open VPN サーバポリシー)

VPN > OpenVPN > OpenVPN Server Policy $\checkmark = \neg -$

Open VPN サーバポリシーの設定方法について説明します。Open VPN サーバポリシーは、SSL VPN サーバポリシーの代替となるものです。

1. VPN > OpenVPN > OpenVPN Server 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。

	🙆 Status		💻 Network	C∰ VPN	Security	¢°		
VPN » Open	VPN » OpenVPN Ser	rver Policy						0 0
Policies are policies appl	useful to permit or y for only user base	deny access to specified authentication and o	c IP addresses, or IP ne duplicate cn enabled co	tworks. They ma onfiguration.	ay be defined at the u	iser or gl	obal level. Op	penVPN server
OpenVPN	Server Policies	List						
Show 10	entries [Right cl	lick on record to get mor	re options]					٩
Name	<u>۲</u>	Destination	θ	Permission		θ	Scope	θ
			No data avail	able in table				
Showing 0 to	0 of 0 entries					First	I Previous	Next > Last >
Add New	OpenVPN Serve	r Policy						

図 7-45 OpenVPN Server Policy 画面

2. Open VPN サーバポリシーを追加する場合、「Add New OpenVPN Server Policy」をクリックし以下の画面を表示します。

OpenVPN Server Policies Co	onfiguration	X
Policy Type	Slobal O User	
OpenVPN Policy		
Apply Policy to	IP Address	
Policy Name		
IP Address		
ICMP	OFF	
Port Range / Port Number		
Begin	[Range: 0 - 65535]	
End	[Range: 0 - 65535]	
Permission	Permit O Deny	
		Save

図 7-46 OpenVPN Sever Policies Configuration 画面

3. 以下の項目を設定します。

項目	説明
Policy Type	ポリシータイプを以下から選択します。
	・「Global」: すべてのユーザにポリシーを適用します。
	・「User」:特定のユーザにポリシーを適用します。「User」を選択した場合は、「Available Users」でユーザを選択
	します。
	OpenVPN Policy
Apply Policy To	ポリシーの適用先を以下から選択します。
	・「IP Address」: ポリシーを IP アドレスに対して適用します。
	・「IP Network」: ポリシーを IP ネットワークに対して適用します。
Policy Name	ポリシー名を入力します。
ICMP	IPCMP を「ON または「OFF」に設定します。
	・「ON」:ICMP トラフィックをサポートします。
	・「OFF」:ICMP トラフィックをサポートしません。
IP Address	IPアドレスを入力します。
Mask Length	「IP Network」を選択した場合、マスク長を入力します。
	Port Range / Port NUmber
Begin / End	適用するポート番号の範囲を入力します。
Permission	「Permit」:ポリシーを許可します。
	「Deny」:ポリシーを拒否します。

Local Networks (ローカルネットワーク設定)

Open VPN のローカルネットワークの作成方法について説明します。

ローカルネットワークの作成は、VPN > OpenVPN > OpenVPN Settings 画面でトンネルタイプにスプリットトンネルを選択した場合に行います。

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

can status	🛜 Wireless	💻 Network	CAS VPN	Security	O Maintenance
PN » OpenVPN » Local N	etworks				@ (
	🛞 Pleas	e select Split Tun	nel and config	ure this page.	
nis page shows the list of dit networks from this pa penVPN Local Netwo	configured OpenVPN LAN ge. orks List	I networks. Clients ha	ve access to only	these local networks.	The user can also add, delete ar
his page shows the list of dit networks from this pa OpenVPN Local Netwo Show 10 • entries	configured OpenVPN LAN ge. orks List [Right click on record to	I networks. Clients ha	ve access to only	these local networks.	The user can also add, delete ar
his page shows the list of dit networks from this pa penVPN Local Network Show 10 entries Local Network	configured OpenVPN LAN ge. orks List [Right click on record to	I networks. Clients ha	Subnet Ma	these local networks. sk	The user can also add, delete ar
his page shows the list of dit networks from this pa OpenVPN Local Network Show 10 • entries Local Network	configured OpenVPN LAN ge. orks List [Right click on record to	I networks. Clients ha get more options] No data av	Ve access to only O Subnet Maailable in table	these local networks. sk	The user can also add, delete ar

図 7-47 Local Networks 画面

2. 「Add New OpenVPN Local Network」をクリックし以下の画面を表示します。

OpenVPN Local Network Cor	figuration	8
Local Network Subnet Mask		
		Save

図 7-48 OpenVPN Local Network Configuration 画面

3. 以下の項目を設定します。

項目	説明
Local Network	ローカル IP ネットワークを入力します。
Subnet Mask	サブネットマスクを入力します。

Remote Networks (リモートネットワーク設定)

VPN > OpenVPN > Remote Networks $\prec = = -$

Open VPN のリモートネットワークの作成方法について説明します。

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

🖾 Status	🛜 Wireless	📃 Network	CAS VPN	🔒 Secu	rity 🗘 🗘	
VPN » OpenVPN » Remote I	Networks					0 0
This page shows the list of D DpenVPN Remote Netv Show 10 • entries	remote VPN networks.] vorks List [Right click on record 1	The user can also add, o	delete and edit net	tworks from th	is page.	9
Common Name	0	Remote Network		θ	Subnet Mask	•
a second s	1996 B	No data av	ailable in table		Contraction of the State of the	
Showing 0 to 0 of 0 entries					() First	Previous Next > Last >
Add New OpenVPN Re	emote Network					

図 7-49 Remote Networks 画面

2. 「Add New OpenVPN Local Network」をクリックし以下の画面を表示します。

OpenVPN Remote Network O	onfiguration	8
Common Name Remote Network Subnet Mask		
		Save

図 7-50 OpenVPN Remote Network Configuration 画面

3. 以下の項目を設定します。

項目	説明
Common Name	リモートネットワークの名前を指定します。
Remote Network	リモート IP ネットワークを入力します。
Subnet Mask	サブネットマスクを入力します。

4. 「Save」をクリックし、設定を適用します。

作成したネットワークは Remote Networks 画面に表示されます。 右クリックで「Edit」(編集)、「Delete」(削除)を実行できます。

OmniSSL Client Configuration (OmniSSL クライアント設定)

VPN > OpenVPN > OmniSSL Client Configuration $\checkmark = \neg -$

本ルータは多くの SSL VPN 機能をサポートする一方で、SSL VPN 機能の代替となる OmniSSL 機能も提供しています。

OmniSSL により、ポータル画面を通じたデバイスからのクライアントインストールが容易になり、既存の OpenVPN 機能を強化することができます。 さらに、この VPN ツールはモバイルデバイス経由で使用することが可能であるため、SSL VPN ソリューションで発生するブラウザ・Java 依存の問 題を解決します。

OmniSSL は、様々な OS でインストールが可能です。本画面では、クライアント設定を生成できます。

1. VPN > OpenVPN > OmniSSL Client 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。

	🕜 Status	🛜 Wireless	💻 Network	A VPN	Security	O Maintenance	
VPN » Open	VPN » OmniSSL Clie	nt Configuration					0 0
OpenVpn pro	vides support to ger	nerate client configur	ation. This page allow	rs to generate clie	ent configuration.		
OmniSSL C	lient Configura	tion List					
Show 10	✓ entries						٩
Name							٥
client							
Showing 1 to	1 of 1 entries					First Previous 1 Next	t > Last >
Add New	Client Configurat	tion					

図 7-51 OmniSSL Client Configuration 画面

2. クライアントを右クリックすると、以下のメニューが表示されます。

Select All	
E View	
Download	
Download with custom CN	
× Delete	

図 7-52 OmniSSL Client Configuration Menu 画面

項目	説明
Select All	リストに表示されたすべてのクライアント設定を選択します。
View	クライアント名と、クライアント設定ファイルの詳細を表示します。
Download	選択した設定をダウンロードします。ポータル以外のユーザおよび OS 固有のものであり、IP/FQDN 固有のオプショ
	ンは維持されません(例:dev、設定内のリモートオプション)。
Download with custom CN	テキストボックスに表示されたカスタムクライアント名で設定をダウンロードします。
Delete	選択したクライアントを削除します。デフォルトのクライアントは削除できません。
注音 いきのまたつ、デー	

注意 CA 証明書をアップロードした後は、クライアント設定を再生成してください。

3. 新しいクライアント設定を追加する場合は、「Add New Client Configuration」をクリックし以下の画面を表示します。

OmniSSL Client Configuration		3
Client List	Other Client	
Configuration Name		

図 7-53 OmniSSL Client Configuration 画面

4. 以下の項目を設定します。

項目	説明
Client List	設定した OpenVPN ユーザ、または「Other Client」(その他のクライアント)を選択してください。
Configuration Name	設定名を入力します。
Configuration Name	設定名を入力します。

OmniSSL Portal Layouts (OmniSSL ポータルレイアウト)

VPN > OpenVPN > OmniSSL Portal Layouts メニュー

リモート OmniSSL ユーザの認証時に表示される、カスタムページを作成します。

1. VPN > OpenVPN > OmniSSL 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。

	🕜 Status	🛜 Wireless	💻 Network	🎧 VPN	Security	🍄 Maintenance		
VPN » Open	PN » OpenVPN » OmniSSL Portal Layouts							
The table lis a custom pag	ts the OmniSSL port e for remote OmniS	al layouts configured SL users that is prese	for this device and al nted upon authenticat	lows several operation.	tions on the portal	ayouts.The router allows y	ou to create	
OmniSSL F	ortal Layout Li	st						
Show 10	✓ entries [Right cl	ick on record to get mo	re options]				٩	
Layout Na	me				🔂 Status		÷	
OMNISSL					Active			
Showing 1 to	1 of 1 entries					First Previous 1 Next	> Last >	
Add Omr	niSSL Portal Layo	ut						

図 7-54 OmniSSL Portal Layouts 画面

2. 「Add OmniSSL Portal Layout」をクリックし以下の画面を表示します。

tai Layout and Theme Name				
ortal Layout Name				
ogin Profile Name	default	\checkmark		
ortal Site Title				
anner Title				
anner Message				
			Ť	
isplay Banner Message on Login Page	OFF			
Portal Authentication Type	Level User Detabase			

図 7-55 OmniSSL Portal Layout Configuration 画面

3. 以下の項目を設定します。

項目	説明
Portal Layout Name	ポータルレイアウトの名称を英字で入力します。
Login Profile Name	ログインプロファイルを選択します。
Portal Site Title	ポータルサイトのタイトルを入力します。本項目はポータルの Web ブラウザウィンドウのタイトルとして表示されま
	す。
Banner Title	ポータルにログインする前に表示されるバナータイトルを入力します。
Banner Message	バナーメッセージを入力します。
	バナーメッセージはバナータイトルと共に表示されます。
Display Banner Message on	「ON」:バナータイトルとバナーメッセージをログイン画面に表示します。
Login Page	「OFF」:バナータイトルとバナーメッセージをログイン画面に表示しません。
Portal Authentication Type	OmniSSL ポータルユーザの認証方法を以下から選択します。
	[Local User Database] [Radius-PAP, Radius-CHAP] [Radius-MSCHAP] [Radius-MSCHAPv2] [NT Domain] [Active
	Directory」「LDAP」「POP3」

4. 「Save」をクリックし、設定を適用します。

追加したポータルレイアウトは OmniSSL Portal Layouts 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

GRE(GRE 設定)

VPN > GRE メニュー

GRE Tunnels(Gre トンネル設定)

GRE(Generic Routing Encapsulation)は、トンネルプロトコルの1つです。パケットを別のプロトコルでカプセル化して伝送を行います。GREトンネルを作成すると、トンネルを介してマルチキャストパケットの送受信が可能となります。

GRE トンネルは、D-Link Discovery Protocol (DDP) のブロードキャストトラフィックをリモート LAN サブネット間で送受信する場合に使用できます。

注意 設定できる GRE トンネル数は製品によって異なります。

- DSR-500:15
- DSR-1000/1000AC:25

以下の手順で GRE トンネルを確立します。

- 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 トンネルを作成する場合、GRE トンネルのエンドポイントに固有の IP アドレスを設定します。 この IP アドレスは、もう一方ルータのスタティックルートでゲートウェイ IP アドレスとして参照されます。 GRE Tunnels Configuration 画面の「Remote End Address」には、エンドポイントルータの WAN IP アドレスを入力します。

トンネル確立後、GRE トンネル名に対して設定されたインタフェースを使用し、ルータ上にスタティックルートを作成します。

スタティックルートの宛先 IP アドレスはリモート LAN のサブネットです。

スタティックルートのゲートウェイ IP アドレスは、終端ルータ(リモート LAN サブネットを管理しているルータ)の GRE トンネル IP になります。 これらの手順が完了すると、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。

1. VPN > GRE > 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。

	🕜 Status	🛜 Wireless	💻 Network	A VPN	🔒 See	curity	O Maintenance	
VPN » G This page GRE TU	RE » GRE Tunnels e allows user to add/ nnels List	/edit GRE tunnel configur	ation.					00
Show 1	0 💌 entries	[Right click on record to ge	et more options]					٩
Tunnel	Name		Interface		Θ	Remote IP		θ
			No data av	ailable in table				
Showing	0 to 0 of 0 entries					[] Firs	t 🔄 Previous Next)	Last 刘
Add 1	New GRE Tunnel	l .						

図 7-56 GRE Tunnels 画面

2. GRE トンネルを追加する場合、「Add New GRE Tunnel」をクリックし以下の画面を表示します。

GRE Tunnels Configuration		\bigotimes
GRE Tunnel Name IP Address Subnet Mask Interface Remote End Address	WAN1	
Enable DDP Broadcast Static Route Configuration IP Address Subnet Mask Gateway IP Address		
		Save

図 7-57 GRE Tunnels Configuration 画面

3. 以下の項目を設定します。

項目	説明
GRE Tunnel Name	トンネル名を入力します。
IP Address	本エンドポイントのIPアドレスを入力します。ゲートウェイIPアドレスとして他のルータのスタティックルートで参
	照されます。
Subnet Mask	サブネットマスクを入力します。
Interface	GRE トンネル設定に使用する IP インタフェースを選択します。
Remote End Address	エンドポイントルータの WAN IP アドレスを入力します。
Enable DDP Broadcast	DDP ブロードキャストを有効にします。
	Static Route Configuration
IP Address	スタティックルートにおけるリモート LAN サブネットの宛先 IP アドレスを入力します。
Subnet Mask	宛先 IP アドレスのサブネットマスクを入力します。
Gateway IP Address	終端ルータのIPアドレスを入力します。

4. 「Save」をクリックし、設定を適用します。

追加した GRE トンネルは GRE Tunnels 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

第8章 セキュリティ設定 (Security)

ご使用のネットワークの安全を確保する、セキュリティ機能の設定について説明します。

設定項目	説明
「Authentication(認証設定)」	本ルータの認証に関する設定を行います。
「Web Content Filter (Web コンテ	Webのコンテンツを対象としたアクセスポリシーを作成、適用する、Webフィルタリング機能の設定を行います。
ンツフィルタリング)」	
「Firewall(ファイアウォール設	本ルータのファイアウォールの設定を行います。
定)」	
「App Control Policy(アプリケー	アプリケーションのトラフィックのコントロールを行います。
ションコントロールポリシー)」	

注意 ネットワークの概念と専門用語を理解している熟練したユーザのみ本章の手順を実行してください。

Authentication(認証設定)

Security > Authentication $\rtimes = \neg -$

Internal User Database (内部ユーザデータベース)

Security > Authentication > Internal User Database メニュー 内部ユーザデータベースの管理方法について説明します。 ユーザグループを作成後、グループに適用するポリシーを設定し、ユーザをグループに追加します。

Groups (グループの設定)

ユーザグループは同じ特権を共有するユーザの集まりです。作成したユーザグループについて、ログインポリシー、ブラウザポリシー、IP ポリシー を設定することができます。 作成したグループ及びポリシーは Internal User Database > Groups タブ画面に表示されます。

右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

■ ユーザグループの追加

1. Security > Authentication > Internal User Database > Groups タブの順にメニューをクリックし、以下の画面を表示します。

curity » Authentication » Internal User Database » Groups	2
Get User DB Groups Users	
Policies can only be configured for groups having admin and sslvpn privile	eges.
snow to get more options]	۹
Group Name	Description
Group Name	Description Admin Group
Group Name	Description Admin Group Guest Group
Group Name	Contraction Admin Group Guest Group I First J Previous 1 Next > Last

図 8-1 Internal User Database > Groups タブ画面

2. 「Add New Group」をクリックし、以下の画面を表示します。

Group Configuration		×
Group Name Description		19
User Type		
User Type	🔿 Admin 💿 Network 🔿 Guest	
PPTP User	OFF	
L2TP User	OFF	
Xauth User	OFF	
OpenVPN User	OFF	
SSLVPN User	OFF	Ī
Captive Portal User	OFF	
Idle Timeout	10 [Default: 10, Range: 1 - 999] Minutes	
	Save	

図 8-2 Group Configuration 画面

3. 以下の項目を設定します。

項目	説明
Group Name	グループ名を入力します。
Description	本ユーザグループの説明文を入力します。
	User Type
User Type	 ユーザの種類を選択します。 「Admin」: このグループのすべてのユーザには、スーパーユーザ権限が付与されます。初期値では、Admin ユーザが1つ 登録されています。 「Network」: Admin の次に高いレベルの権限を付与されます。 「Guest」: このグループのユーザには、閲覧権限のみが付与されます。 「Network」または「Admin」ユーザを選択した場合、「PPTP」「L2TP」「Xauth (Network グループのみ)」「SSLVPN」「Captive Portal」を有効にすることができます。
PPTP User	PPTP User を有効 / 無効にします。
L2TP User	L2TP User を有効 / 無効にします。
Xauth User	Xauth User を有効 / 無効にします。
OpenVPN User	OpenVPN User を有効 / 無効にします。
SSL VPN User	SSL VPN User を有効 / 無効にします。
Captive Portal User	Captive Portal User を有効 / 無効にします。
Idle Timeout	ユーザグループ内のユーザが Web 管理セッションを自動的にログアウトするまでの無通信の時間を入力します。「0」を設定 した場合、ログアウトしません。

4. 「Save」をクリックし、設定を適用します。

■ ログインポリシーの設定

ユーザグループに対して、Web GUI へのログインアクセスを許可または拒否することができます。

1. Security > Authentication > Internal User Database > 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。

Show 10 v entries			٩
Group	٥	Status	
ADMIN		Allow	
GUEST		Deny	
Showing 1 to 2 of 2 entries			LETT Dravious 1 Novt Last

図 8-3 Login Policies 画面

2. エントリを右クリックして「Edit」を選択すると、以下の画面が表示されます。

Login Policies Configurati	on	×
Group Name Disable Login Deny Login from WAN Interface	ADMIN OFF OFF	
		Save

3. 以下の項目を設定します。

項目	説明
Group Name	グループ名が表示されます。
Disable Login	選択したグループ内の全ユーザに対して Web GUI へのログインアクセスを許可または拒否します。
	・「ON」:ログインアクセスを無効にします。
	・「OFF」:ログインアクセスを有効にします。
Deny Login from WAN	選択したグループ内の全ユーザに対して WAN2/DMZ ポートからの Web GUI へのログインアクセスを許可または
Interface	拒否します。
	・「ON」:ログインアクセスを無効にします。
	・「OFF」:ログインアクセスを有効にします。

4. 「Save」をクリックし、設定を適用します。

■ ブラウザポリシーの設定

Web ブラウザから本製品の Web GUI にログインすることを許可または拒否することができます。

1. Security > Authentication > Internal User Database > 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。

Browser Policies					
Show 10 <pre> entries</pre>					
Group	÷	Added Client Browsers	⇔	Status	÷
		No data available in table			
Showing 0 to 0 of 0 entries			K First	I Previous	Next 🔰 Last 刘
Add Browser Policies					

図 8-5 Browser Policies 画面

2. 「Add Browser Policies」をクリックし、以下の画面を表示します。

Browser Policies Configuration		
Group Name	ADMIN	•
Add Defined Browser Client Browser	Internet Explorer]

図 8-6 Browser Policies Configuration 画面

3. 以下の項目を設定します。

項目	説明
Group Name	プルダウンメニューからグループ名を選択します。
Client Browser	プルダウンメニューから Web ブラウザを選択します。

IP ポリシーの設定

ユーザグループに IP の詳細なポリシーを設定します。

ユーザグループ内のユーザが、特定のネットワークまたは IP アドレスから本製品の Web GUI にログインすることを許可または拒否することができます。

1. Security > Authentication > Internal User Database > 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。

P Policies			
Show 10 • entries			٩
Group 🔂 Source Address Type	Network Address / IP Address	⊖ Mask Length ⊖ Sta	atus ⊖
	No data available in table		
Showing 0 to 0 of 0 entries		First Previous Next	Last 刘
Add IP Policies			

図 8-7 IP Policies 画面

2. 「Add IP Policies」をクリックし、以下の画面を表示します。

IP Policies Configuration		×
Group Name	ADMIN	
Defined Address Configuration Source Address Type Network Address / IP Address	IP Network	
Mask Length	32 [Default:32, Range 0 - 32]	
	1	Save

図 8-8 IP Policies Configuration 画面

3. 以下の項目を設定します。

項目	説明
Group Name	プルダウンメニューからグループ名を選択します。
Source Address Type	ソースアドレスのタイプを選択します。 ・「IP Address」:特定の IP アドレスを指定します。 ・「IP Network」:特定の IP ネットワークを指定します。
Network Address / IP Address	ネットワークまたは IP アドレスを入力します。
Mask Length	サブネットマスク長を入力します。(「IP Network」選択時)

Users (ユーザの追加)

- ユーザグループの作成後、グループにユーザを追加します。ユーザは個別または CSV 形式のファイルで一括インポートすることが可能です。
- 1. Security > Authentication > Internal User Database > Users タブの順にメニューをクリックし、以下の画面を表示します。

🖓 Status 🛜	Wireless 🖳 Network	ക	VPN	🚊 Security	O° Maintenance	
Security » Authentication » Internal Use	er Database » Users					00
Get User DB Groups Users						
This page shows a list of available user on users.	s in the system. A user can add, del	ete and	edit the u	users also. This pag	e can also be used for se	tting policies
Users List						
Show 10 • entries [Right click on r	ecord to get more options]					٩
User Name 🔂	Group Name	⇔	Login Sta	atus		⇔
admin	ADMIN		Enabled (LA	N) Enabled (WAN)		
guest	GUEST		Disabled (L4	AN) Disabled (WAN)		
Showing 1 to 2 of 2 entries				И	First 🚽 Previous 1 Next	> Last >
Add New User						

図 8-9 Internal User Database > Users タブ画面

2. 「Add New User」をクリックし、以下の画面を表示します。

er Configuration		
User Name		
First Name		
Last Name		
Select Group	ADMIN T	
Password		
Confirm Password		
		Savo

図 8-10 User Configuration 画面

3. 以下の項目を設定します。

項目	説明
User Name	固有の識別名となるユーザ名を入力します。
First Name	ユーザの名前を入力します。
Last Name	ユーザの名字を入力します。
Select Group	ユーザが所属するグループを選択します。
Password	ユーザが Web GUI にアクセスする際に指定するログインパスワード (大文字と小文字を区別) を入力します。セキュリ ティのために、入力したパスワード文字は、「・」で表示されます。
Confirm Password	確認のため、再度パスワードを入力します。

4. 「Save」をクリックし、設定を適用します。

追加したユーザは **Internal User Database > Users タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

■ ユーザ情報の編集

管理者およびユーザのグループ、Web GUI のログインパスワードを変更することができます。

- 1. Security > Authentication > Internal User Database > Users タブの順にメニューをクリック → 編集したいユーザ上で右クリックし、「Edit」(編
 - 集)を選択します。

	🕜 Status	🛜 Wireless	💻 Network	ഹ് ലം vi	PN	Security	© ^o Maintenance	
Security » Au Get User	Get User DB Groups Users							
This page show users. Users List	ws a list of availabl	e users in the system	. A user can add, delet	e and edit	t the users	also. This page	can also be used for setti	ing policies on
Show 10	entries [Right cli	ck on record to get mor	e options]					٩
User Name		Group Name	9	€L	ogin Statu	IS		÷
admin	Select All	ADMIN		E	nabled (LAN)	Enabled (WAN)		
guest	Select All	GUEST		D	isabled (LAN)	Disabled (WAN)		
Showing 1 to	X Delete					И	First Previous 1 Nex	xt > Last >
Add New	User							

図 8-11 Internal User Database > Users タブ画面

2. 以下の画面が表示されます。ログインパスワードを変更する場合は、「Edit Password」を「ON」にします。

User Configuration		\otimes
User Name	admin	
First Name	admin	
Last Name	ssi	
Select Group	ADMIN	
Edit Password		
Current Logged In Administrator Password		
New Password	••••	
Confirm New Password	••••	
		Save

- 図 8-12 User Configuration 画面
- 3. 以下の項目を設定します。

項目	説明
User Name	固有の識別名となるユーザ名を入力します。
First Name	ユーザの名前を入力します。
Last Name	ユーザの名字を入力します。
Select Group	ユーザが所属するグループを選択します。
Edit Password	Web GUI のログインパスワードを変更する場合は「ON」にします。
Current Logged In	現在設定されている Web GUI のログインパスワードを入力します。
Administrator Password	
New Password	Web GUIの新しいログインパスワード (大文字と小文字を区別) を入力します。セキュリティのために、入力したパスワー
	ド文字は、「・」で表示されます。
Confirm New Password	確認のため、再度新しいログインパスワードを入力します。

4. 「Save」をクリックし、設定を適用します。



Web GUI のログインパスワードを変更した場合、「Save」をクリックすると一旦 Web GUI からログアウトします。 ログイン画面が表示されますので、新しいパスワードを入力して再度ログインしてください。

Get User DB(ユーザデータベースのインポート)

DSR の管理者は、適切な形式の CSV(Comma separated value)ファイルをインポートすることにより、内部ローカルデータベースに直接ユーザを 追加することができます。本機能を使用することで、システムに多数のユーザを一括で追加することが可能です。また、必要に応じて同じファイル を別の DSR デバイスにアップロードすることもできます。ローカルユーザデータベースにアップロードされたユーザは、Web GUI で編集すること ができます。

1. Security > Authentication > Internal User Database > Get User DB の順にメニューをクリックし、以下の画面を表示します。

🕢 Status	🛜 Wireless	💻 Network	பல் VPN	🔒 Security	🐡 Maintenance			
Security » Authentication » Internal User Database » Get User DB								
Get User DB Groups Us	sers							
This page allows user to import	a CSV formatted user	database to the rout	er.					
Get User DB								
Select User DB File		7ァイルを選択 選択さ…ませ	t X 0					
		Upload						
		Upload						

図 8-13 Internal User Database > Get User DB タブ画面

- 2. 「参照 /Browse」をクリックします。
- 3. CSV ファイルの場所に移動して、ファイルを選択し、「開く (Open)」をクリックします。
- 4. 「Upload」をクリックします。

■ ユーザデータベースの作成(CSV ファイル)

- 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 や他のテキストを追加しないでください。
- 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","Password","MultiLogin"

以下の値を定義するフィールドがあります。

- ・ Username (文字列フィールド): DSR のデータベースにおけるユーザ (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 (文字列フィールド):ユーザの詳細であり、固有である必要はありません。
- ・ LastName (文字列フィールド):ユーザの詳細であり、固有である必要はありません。
- ・ GroupName (文字列フィールド): このユーザに関連付けられるグループ。
- ・ MultiLogSup (ブーリアン値):本項目を有効(「1」)にすると、複数のユーザで単一のユーザ名とパスワードを共有できます。
- Password (文字列フィールド): 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 アップロードを行う前に、Web 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。



External Auth Server (外部認証)

Security > Authentication > External Auth Server $\rtimes \Box \Box -$

外部認証を行うサーバの設定について説明します。設定は以下のタブごとに行います。 「RADIUS Server」「POP3 Server」「POP3 Trusted CA」「LDAP Server」「AD Server」「NT Domain Server」

Radius Server (RADIUS サーバの設定)

クライアント接続の際に、RADIUS サーバによる認証を行います。 RADIUS サーバはユーザアカウントのデータベースを保持しており、ネットワークにアクセスしようとするユーザの認証を行います。プライマリ RADIUS サーバにアクセスできない場合は、セカンダリ / ターシャリ RADIUS サーバが認証を行います。

1. Security > Authentication > External Auth Server > RADIUS Server タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🛜 Wirele	ss 💂 Network 🕼 VPN 🤮 Security 🗇 Maintenance							
Security » Authentication » External Auth Server	» Radius Server							
Radius Server POP3 Server POP3 Trus	ted CA LDAP Server AD Server NT Domain							
This page configures the RADIUS servers to be used for authentication. A RADIUS server maintains a database of user accounts used in larger environments. If a RADIUS server is configured in the LAN, it can be used for authenticating users that want to connect to the IPSec,L2TP,PPTP,SSL VPN and wireless networks provided by this device. If the first/primary RADIUS server is not accessible at any time, then the device will attempt to contact the secondary RADIUS server for user authentication.								
Server Check	Server Checking							
Authentication Server1 (Primary)	192.168.1.2							
Authentication Port	1812 [Range: 0 - 65535]							
Secret								
Timeout	1 (Seconds)							
Retries	2							
Authentication Server2 (Secondary)	192.168.1.3							
Authentication Port	1812 [Range: 0 - 65535]							
Secret								
Timeout	1 (Seconds)							
Retries	2							
Authentication Server 3 (Tertiary)	192.168.1.4							
Authentication Port	1812 [Range: 0 - 65535]							
Secret								
Timeout	1 (Seconds)							
Retries	2							
	Save Cancel							

図 8-14 External Auth Server > RADIUS Server タブ画面

2. 以下の項目を設定し	ょ	す	0
--------------	---	---	---

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	RADIUS 認証サーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。
	「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
Authentication Port	RADIUS 認証サーバのポートを指定します。
Secret	デバイスが設定済みの RADIUS サーバにログインするための秘密鍵を指定します。これは RADIUS サーバの秘密鍵に一致す
	る必要があります。
Timeout	RADIUS 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	RADIUS サーバへの接続試行回数を指定します。

POP3 Server (POP3 サーバ)

POP3 は、TCP/IP 接続におけるメール通信で最も一般的に使用されるアプリケーション層のプロトコルです。暗号化トラフィックを POP3 サーバに 送信する際に、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 が POP3 認証トラフィックに使用されます。

1. Security > Authentication > External Auth Server > POP3 Server タブの順にメニューをクリックし、以下の画面を表示します。

🖾 Status 🛜 Wireless	💻 Network	ക vpn	🔒 Security	🗘 Maintenance	
Security » Authentication » External Auth Server »	POP3 Server				00
Radius Server POP3 Server POP3 Truste	d CA LDAP Server A	D Server NT Doi	main		
This page allow user to configure pop3 authentic:	ition servers.				
POP3 Server Configuration					
Server Check	Server Checking				
Authentication Server1 (Primary)					
Authentication Port	110 [Default: 1	10, Range: 1 - 65535]			
SSL Enable	OFF				
Authentication Server2 (Secondary)		Optional			
Authentication Port	110 [Default: 1	10, Range 1 - 65535]			
SSL Enable	OFF				
Authentication Server 3 (Tertiary)		Optional			
Authentication Port	110 [Default: 1	10, Range 1 - 65535]			
SSL Enable	OFF				
Timeout	(Seconds)				
Retries	5				
	Save	Cancel			

図 8-15 External Auth Server > POP3 Server タブ画面

2.	以下の項目を設定します	す。
----	-------------	----

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	POP3 認証サーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。 「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
Authentication Port	RADIUS 認証サーバのポートを指定します。 ・ 設定可能範囲:1-65535 ・ 初期値:110
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)を指定します。
Timeout	POP3 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	POP3 サーバへの接続試行回数を指定します。

POP3 Trusted CA(POP3 トラスト CA)

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 ファイルが使用されます。 3 つの設定サーバごとに、認証に使用する固有の CA を持つことができます。

1. Security > Authentication > External Auth Server > POP3 Trusted CA タブの順にメニューをクリックし、以下の画面を表示します。

	🗥 Status	🛜 Wireless	💻 Network	A VPN	Security	O Maintenance	
Security »	• Authentication »	External Auth Server »	POP3 Trusted CA				00
Radiu	IS Server POP3 S	erver POP3 Trusted	CA LDAP Server	AD Server NT Do	main		
This page POP3 CA	shows the list of P A Files List	OP3 CA Files.					
Show 10	▼ entries	[Right click on record to	get more options]				٩
CA File							Û
			No data av	ailable in table			
Showing () to 0 of 0 entries					First Previous Next >	Last 刘
Add C	A File						

図 8-16 External Auth Server > POP3 Trusted CA タブ

2. 「Add CA File」をクリックして、CA ファイルを追加します。

CA File Configuration		x
CA File	ファイルを選択 No file selected.	
	Upload	

図 8-17 CA File Configuration 画面

3. 「参照 /Browse」をクリックして、CA ファイルを参照します。ファイルを選択後、「Upload」をクリックします。

LDAP Server (LDAP サーバ)

LDAP サーバは、ディレクトリ構造により大容量のユーザデータベースを保持します。ディレクトリ構造ではユーザ情報が階層的に保存されるため、 同じユーザ名で異なるグループに所属するユーザを認証することができます。なお、WindowsまたはLinuxサーバにおけるLDAP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シンプルになっています。

ルータに設定された詳細情報は、ルータとそのホストの認証のために送信されます。LDAP サーバがルータを認証する上で、LDAP 属性、ドメイン 名 (DN)、場合によっては管理者アカウントとパスワードがキーフィールドとなります。

1. Security > Authentication > External Auth Server > LDAP Server タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🛜 Wire	less 💻 Network	🚯 VPN 🔒	Security	🌻 Maintenance	
surity » Authentication » External Auth Serve	r » LDAP Server				00
Radius Server POP3 Server POP3 Tru	isted CA LDAP Server AD Ser	rver NT Domain			
is page allows a user to configure authentica	ation servers for LDAP authentica	tion.			
Server Check	Server Checking				
Authentication Server1 (Primary)					
Authentication Server2 (Secondary)		Optional			
Authentication Server 3 (Tertiary)		Optional			
LDAP Attribute 1		Optional			
LDAP Attribute 2		Optional			
LDAP Attribute 3		Optional			
LDAP Attribute 4		Optional			
LDAP Base DN]			
Second LDAP Base DN		Optional			
Third LDAP Base DN		Optional			
Timeout	(Seconds)				
Retries	5 [Range: 5 - 9]				
First Administrator Account	admin	Orthogol			
Password		Optional			
Second Administrator Account		Optional			
Password		Optional			
T1. 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.		Optional			
inira Administrator Account		Optional			
Password		Optional			
	Save Can	cel			

図 8-18 External Auth Server > LDAP Server タブ画面

2. 以下の項目を設定します。

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	LDAP 認証サーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。
	[Authentication Server 1 (Primary)] [Authentication Server 2 (Secondary)] [Authentication Server 3 (Tertiary)]
LDAP Attribute	LDAP サーバで設定された LDAP ユーザに関連する属性を指定します。これらは、SAM アカウント名、対応するドメイン
	名などの属性を含みます。同じユーザ名を持つ異なるユーザを識別するために使用されます。
LDAP Base DN	LDAP 認証におけるベースドメイン名を指定します。
Timeout	ルータが LDAP サーバからの応答を待つ待機時間 (秒) を設定します。
Retries	ルータから LDAP サーバへの接続試行回数を決定します。
Administrator Account	PPTP/L2TP 接続で LDAP 認証が必要な場合に使用される管理者アカウント情報を入力します。「First Administrator
	Account」「Second Administrator Account」「Third Administrator Account」の3つを設定可能です。
Password	管理パスワードを入力します。

AD Server (アクティブディレクトリサーバ)

アクティブディレクトリ認証は、NT ドメイン認証の高機能バージョンです。

Organizational Units (OUs) 内でグループ化されているユーザの認証に Kerberos プロトコルが使用されます。NT ドメインサーバでサポートされるユー ザは数千程度ですが、Active Directory サーバは通常百万単位のユーザをサポートすることができるストラクチャを有しています。 設定された認証サーバと Active Directory ドメインは、外部の Windows ベースサーバのユーザディレクトリを使用して、ユーザを認証します。この 認証方法は「SSL VPN」クライアントで一般的であり、「IPSec」「PPTP」「L2TP」クライアント認証などでも有効です。

1. Security > Authentication > External Auth Server > AD Server タブの順にメニューをクリックし、以下の画面を表示します。

ity » Authentication » External Auth Serve	r » AD Server			2
Radius Server POP3 Server POP3 Tru	sted CA LDAP Server AD Se	rver NT Domain		
page allow to configure Active Directory a	uthentication servers.			
ve Directory Configuration				
Server Check				
	Server Checking			
Authentication Server1 (Primary)				
Authentication Server2 (Secondary)		Optional		
Authentication Server 3 (Tertiary)		Optional		
Active Directory Domain				
Second Active Directory Domain		Optional		
Third Active Directory Domain		Optional		
Timeout	(Seconds)			
Retries	5 [Range: 5 - 9]			
First Administrator Account		Optional		
Password		Optional		
First Server Hostname				
Second Administrator Account		Optional		
Password		Optional		
Second Server Hestname		Optional		
		Optional		
inird Administrator Account		Optional		
Password		Optional		
Third Server Hostname		Optional		

図 8-19 External Auth Server > AD Server タブ画面

2. 以下の項目を設定します。

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	AD サーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。
	「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
Active Directory Domain	アクティブディレクトリドメイン名を入力します。オプションとして「Second Active Directory Domain」「Third Active
	Directory Domain」も設定可能です。
Timeout	AD サーバからの応答を待つ待機時間(秒)を指定します。
Retries	ルータから認証サーバへの認証試行回数を指定します。
Administrator Account	PPTP/L2TP 接続で認証が必要な場合に使用される管理者アカウント情報を入力します。
	「First Administrator Account」「Second Administrator Account」「Third Administrator Account」の3つを設定可能です。

NT Domain Server(NT ドメインサーバ)

NT ドメインサーバは事前に設定済みのワークグループフィールドを経由したユーザとホストの認証を行います。通常、認証ユーザのディレクトリ 集約のため、認証ドメインの管理には Windows サーバまたは Samba サーバが使用されます。

1. Security > Authentication > External Auth Server > NT Domain タブの順にメニューをクリックし、以下の画面を表示します。

Radius Server POP3 Server POP3 Tru	sted CA LDAP Server AD Ser	ver NT Domain	
page allow you to configure NT Domain se	rvers.		
Domain Configuration			
Server Check	Server Checking		
Authentication Server 1 (Primary)		2	
Authentication Server 2 (Secondary)		Optional	
Authentication Server 3 (Tertiary)		Optional	
Workgroup]	
Second Workgroup		Optional	
Third Workgroup		Optional	
Timeout	(Seconds)		
Retries	5 [Range: 5 - 9]		
First Administrator Account		Optional	
Password		Optional	
First Server Hostname		Optional	
Second Administrator Account		Optional	
Password		Optional	
Second Server Hostname		Optional	
Third Administrator Account		Optional	
Password		Optional	
Third Server Hostname		Optional	

図 8-20 External Auth Server > NT Domain タブ画面

2. 以下の項目を設定します。

項目	説明
Server Check	「Server Checking」をクリックして、サーバとの接続をテストします。
Authentication Server	NT ドメインサーバの IP アドレスを指定します。サーバは以下の 3 つを登録できます。
	「Authentication Server 1 (Primary)」「Authentication Server 2 (Secondary)」「Authentication Server 3 (Tertiary)」
Workgroup	NT ドメイン認証に必要なワークグループを入力します。
	「Second Workgroup」「Third Workgroup」まで設定可能です。
Timeout	NT ドメインサーバからの応答を待つ待機時間(秒)を指定します。
Retries	NT ドメインサーバへの認証試行回数を指定します。
Administrator Account	PTP/L2TP 接続で認証が必要な場合に使用される管理者アカウント情報を入力します。
	「First Administrator Account」「Second Administrator Account」「Third Administrator Account」の 3 つを設定可能です。
Password	管理パスワードを入力します。
Server Hostname	サーバのホスト名を入力します。「First Server Hostname」「Second Server Hostname」「Third Server Hostname」の3
	つを設定可能です。

Radius Accounting (Radius アカウンティング設定)

Security > Authentication > Radius Accounting $\checkmark = \neg -$

本画面では、ユーザの Radius アカウンティング認証の有効化 / 無効化を行います。また、定義済み Radius サーバに対してアカウンティングメッセージ内でセッションのトラフィック統計が送信される間隔(Accounting Interim Interval)の設定が可能です。

Radius Accounting (Radius アカウンティング)

以下の手順に従って Radius サーバへの接続設定を行います。

1. Security > Authentication > Radius Accounting > Radius Accounting タブの順にメニューをクリックし、以下の画面を表示します。

	🝘 Status		ess 💻		A VPN	Security	O Maintenance	
Security » A	uthentication » Rac	lius Accounting						00
Radius A	Accounting Radiu	IS Accounting S	erver					
This page all the device se	ows user to enable ends the traffic stat	or disable the F istics of a sessi	adius Account on in accounti	ing for a feat ng messages	ure and also to co to the Radius serv	onfigure the Accounti er configured.	ng Interim Interval in seco	nds at which
Radius Acc	counting Config	uration						
Captive Radius A	Portal Accounting Interim	Interval	300	[Range: 3	800 - 3600] Seconds			
			Sav	/e	Cancel			

図 8-21 Radius Accounting > Radius Accounting タブ画面

2. 以下の項目を設定します。

項目	説明
Captive Portal	「ON」: キャプティブポータルの Radius アカウンティング機能を有効にします。
	「OFF」: キャプティブポータルの Radius アカウンティング機能を無効にします。
Radius Accounting	デバイスから Radius Accounting(Interim-Update)パケットが送信される間隔を設定します。
Interim Interval	・ 設定可能範囲:300-3600(秒)
	・ 初期値:300(秒)

Radius Accounting Server (Radius アカウンティングサーバ)

RADIUS アカウンティングサーバの設定について説明します。プライマリ RADIUS サーバに接続できない場合、デバイスはセカンダリ RADIUS サーバに対してアカウンティングリクエスト送信のコンタクトを試行します。

1. Security > Authentication > Radius Accounting > Radius Accounting Server タブの順にメニューをクリックし、以下の画面を表示します。

	Status		💻 Network	CA VPN	Security	O Maintenance	
Security » A	uthentication » Rad	ius Accounting » Radiu	us Accounting Server				00
Radius A	ccounting Radiu	s Accounting Server					
This page allo time, then th	ows user to configu e device will attem	e the Radius Account pt to contact the sec	ing Server configur ondary Radius serve	ation on the router er for sending accou	.If the first/primary R Inting requests.	adius server is not accessi	ible at any
Radius Acc	ounting Server	Configuration		5	5 1		
Account	ing Server (Primary) 1	92.168.1.2				
Account	ing Port	1	813 [Range	e: 0 - 65535]			
Secret		•	•••••				
Account	ing Server 2 (Secon	dary) 1	92.168.1.3				
Account	ing Port	1	813 [Range	e: 0 - 65535]			
Secret		•	•••••				
Account	ing Server 3 (Tertia	ury) 1	92.168.1.4				
Account	ing Port	1	813 [Range	e: 0 - 65535]			
Secret		•	•••••				
			Save	Cancel			
				ouncer			

図 8-22 Radius Accounting > Radius Accounting Server タブ画面

2. 以下の項目を設定します。

項目	説明
Accounting Server	RADIUS アカウンティングサーバの IP アドレスを入力します。サーバは以下の 3 つを登録できます。
	「Accounting Server (Primary)」「Accounting Server 2 (Secondary)」「Accounting Server 3 (Tertiary)」
Accounting Port	Radius アカウンティングサーバのポート番号を入力します。
	・ 設定可能範囲:0-65535
	 初期値:1813
Secret	デバイスが設定済みの RADIUS サーバにログインするための秘密鍵を指定します。これは RADIUS サーバの秘密鍵に一致す
	る必要があります。

Login Profiles (ログインプロファイル)

Security> Authentication> Login Profiles $\checkmark = = = -$

無線クライアントがアクセスポイントの SSID や VLAN に接続する際、ログイン画面が表示されます。 本項目では、ログイン画面のカスタマイズ方法について説明します。

1. Security > Authentication > Login 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。

	🕋 Status		💻 Network	A VPN	🔒 Security	O° Ma		
Security » A	uthentication » Log	in Profiles						00
This table lis available on Login Prof	ts all the login page the device) sessions iles List	e profiles available in	the system. These lo	gin page profiles	are used for authentio	cating SSL \	/PN and Captive I	Portal (if
Show 10	entries [Right cl	ick on record to get more	e options]					٩
Profile Na	me	🗘 Brov	wser Title			😔 Sta	tus	0
default		D-link	Unified Services Router	i.		SSLV	/PN,test	
default2		D-link	Unified Services Router			Not	In Use	
Showing 1 to	2 of 2 entries					First 🔄 Pre	evious 1 Next	Last 刘
Add New	Login Profile							

図 8-23 Login Profiles 画面

2. 「Add New Login Profile」をクリックし、以下の画面を表示します。

Login Profile Configuratio	n	×
General Details Profile Name Browser Title Background	 Image Color 	^
Page Background Image	Default Add Add Add Add	
Minimal Page for Mobile Devices		
Header Details		
Background	● Image ○ Color	~
		Save

図 8-24 Login Profile Configuration 画面

3. 以下の項目を設定します。

項目	説明
	General Details
Profile Name	キャプティブポータルプロファイルの名称を入力します。他のプロファイルと区別できる名前を設定します。
Browser Title	キャプティブポータルセッション中にブラウザのタイトルとして表示される文字列を入力します。
Background	キャプティブポータルセッション中に表示されるログインページの背景として、画像またはカラーを選択します。 「Image」:ページの背景として画像を表示します。「Page Background Image」フィールドを使用して、背景 画像を選択します。 「Color」:ページの背景色を設定します。プルダウンメニューから色を選択します。
Page Background Image	「Background」に「Image」を選択した場合、キャプティブポータルセッション中に表示されるページの背景画像を選択します。新しく画像ファイルをアップロードするには、「Add」をクリックします。
Page Background Upload	画像ファイルをアップロードします。「Page Background Image」で「Add」クリックすると、本項目が表示されます。 画像ファイルを指定後、「Upload」をクリックします。アップロードできる画像の最大サイズは 100KByte です。
Page Background Color	「Background」に「Color」を選択した場合、キャプティブポータルセッション中に表示されるページの背景色を プルダウンメニューから選択します。
Custom Color	「Page Background Color」に「Custom」を選択した場合、HTML のカラーコードを入力します。
Minimal Page for Mobile Devices	モバイル端末で Web ページを適切に表示させる機能です。
	Header Details
Background	 キャプティブポータルセッション中に表示されるログインページのヘッダーとして、画像またはカラーを選択します。 「Image」:ページの背景として画像を表示します。「Header Background Image」フィールドを使用して、背景画像を選択します。 「Color」:ページの背景色を設定します。プルダウンメニューから色を選択します。
Header Background Image	「Background」に「Image」を選択した場合、キャプティブポータルセッション中に表示されるページのヘッダー 画像を選択します。新しく画像ファイルをアップロードするには、「Add」をクリックします。
Header Background Upload	画像ファイルをアップロードします。「Page Background Image」で「Add」クリックすると、本項目が表示されます。 画像ファイルを指定後、「Upload」をクリックします。アップロードできる画像の最大サイズは 100KByte です。
Header Background Color	「Background」に「Color」を選択した場合、キャプティブポータルセッション中に表示されるページのヘッダー 色をプルダウンメニューから選択します。
Custom Color	「Header Background Color」に「Custom」を選択した場合、HTML のカラーコードを入力します。
Header Caption	キャプティブポータルセッション中にログインページのヘッダに表示されるテキストを入力します。
Caption Font	ヘッダテキストのフォントを選択します。
Font Size	ヘッダテキストのフォントサイズを選択します。
Font Color	ヘッダテキストのフォント色を選択します。
	Login Details
Login Section Title	キャプティブポータルセッションへのログイン時に表示されるログインボックスのタイトルに表示されるテキストを入力します。 本項目はオプションです。
Welcome Message	キャプティブセッションへのログインに成功した場合に表示されるウェルカムメッセージを入力します。 本項目はオプションです。
Error Message	キャプティブセッションへのログインに失敗した場合に表示されるエラーメッセージを入力します。 本項目はオプションです。
	Advertisement Details
Enable Advertisement	広告の表示の有無を指定します。
Ad Place	広告の表示箇所を指定します。「Top」「Bottom」から指定できます。
Ad Content	広告の内容を指定します。
Font	広告のフォントを指定します。
Font Size	広告のフォントサイズを指定します。
Font Color	広告のフォント色を指定します。
	Footer Details
Change Footer Content	ログインページのフッターコンテンツへの変更を有効または無効にします。
Footer Content	「Change Footer Content」をチェックした場合、フッターに表示されるテキストを入力します。
Footer Font Color	「Change Footer Content」がチェックした場合、フッターに表示される色を入力します。

Services Route Management (サービスルート管理)

Security > Authentication > Services Route Management $\varkappa = \neg -$

サービスルート管理機能では、認証でサービストラフィックが送信されるインタフェースを設定することができます。また、認証用としてトンネルのリモート LAN ネットワーク上の Radius サーバを利用することも可能です。

1. Security > Authentication > Services Route 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。

	🕢 Status		💻 Network	C VPN	Security	O ^o Maintenance				
Security » A	Security » Authentication » Services Route Management									
This table li	sts all the service ro	outes on which we are	interested to send th	netraffic of partic	ular service.					
Services R	oute Manageme	nt List								
Show 10	Show 10 vertices [Right click on record to get more options]									
Service	۵	Service Interface		⇔	Routing Interface		⇔			
			No data av	ailable in table						
Showing 0 to	0 of 0 entries					K First A Previous Ne	ext 🔰 Last 划			
Add Serv	vice Route									

図 8-25 Services Route Management 画面

2. 「Add Service Route」をクリックし、以下の画面を表示します。

Service Route Management Con	figuration	\otimes
Service Name	Radius]
Service Interface	Primary Auth]
Route Interface	VLAN 🗸]
VLAN Name	Default]
		Save

図 8-26 Service Route Management Configuration 画面

3. 以下の項目を設定します。

項目	説明
Service Name	サービスを選択します。
Service Interface	サービスのインタフェースを選択します。
Route Interface	トラフィックが送信されるインタフェースを選択します。「VLAN」または「IPSec」から選択します。
VLAN Name	「Route Interface」で「VLAN」を選択した場合、ルートの VLAN を選択します。 この VLAN 上でトラフィックが送信されます。
Policy Name	「Route Interface」で「IPSec」を選択した場合、ルートの IPSec ポリシーを選択します。このポリシー上でトラフィックが送信されます。

DUA External CP Web(DUA 外部キャプティブポータル Web サーバ)

Security > Authentication > DUA External CP Web $\prec = = =$

DUA 外部キャプティブポータル Web サーバの設定方法について説明します。

1. Security > Authentication > DUA External CP Web の順にメニューをクリックし、以下の画面を表示します。

	🕐 Status		💻 Network	A VPN	Security	O ^o Maintenance	
Security » A	uthentication » DUA	External CP Web					0 0
This page all	ows user to configur	e DUA External Captiv	e Portal Web Server.				
DUA Exter	nal CP Web Serv	ver Configuration					
Enable DUA Ext DUA CP Shared S Server S	ernal CP URL Logout IP jecret tatus	1 1 5 0 0	11.1 12.168.10.219/cpweb 1.1.1 ccret wn Save	Cancel			

図 8-27 DUA External CP Web 画面

2. 以下の項目を設定します。

項目	説明
Enable	DUA 外部キャプティブポータル Web サーバを有効または無効にします。
DUA External CP URL	DUA 外部サーバの URL を入力します。
DUA CP Logout IP	設定する CP ログアウト IP を入力します。
Shared Secret	DUA 外部サーバに対して設定する共有シークレットを入力します。
Server Status	DUA 外部 Web サーバの現在のステータスが表示されます。

Web Content Filter (Web コンテンツフィルタリング)

Security > Web Content Filter $\prec = \neg -$

Web コンテンツフィルタリングは、特定のインターネットサービスへの接続をブロックする機能です。 スタティックフィルタリング、ダイナミックフィルタリング、URL フィルタリング ACL の設定方法について説明します。

Static Filtering(スタティックフィルタリング)

Security > Web Content Filter > Static Filtering $\forall = \neg -$

スタティックフィルタリングにより、Web プロキシや Java など、特定のインターネットサービスをブロックすることができます。「Static Filtering」 タブでブロックするサービスを選択します。

また、「Approved URL」タブと「Blocked URL」タブでは許可または拒否する URL のリストを登録できます。

Static Filtering(スタティックフィルタリング)

1. Security > Web Content Filter > Static Filtering > Static Filtering タブの順にメニューをクリックし、以下の画面を表示します。

	🕋 Status		📃 Network	A VPN	🔒 Security	O Maintenance	
Security » V	/eb Content Filter »	Static Filtering					00
Static F	iltering Approved	d URL Blocked URL					
This content specified, wh	filtering option allo nich will block acces	ows the user to block ss to the site. To setu	access to certain Inte p URLs, go to Approv	ernet sites. Up to a ed URLs and Block	32 key words in the s ed URLs page.	ite's name (web site URL)	can be
Static Filt	ering						
Content	Filtering		ON CIT				
Web Pro	ху		OFF				
Java			OFF				
ActiveX			OFF				
Browser	Cookies		OFF				
			Save	Cancel			

図 8-28 Static Filtering > Static Filtering タブ画面

2. 以下の項目を設定します。

項目	説明
Content Filtering	コンテンツフィルタリングを「ON」または「OFF」にします。
Web Proxy	「ON」にした場合、プロキシサーバがブロックされます。 プロキシサーバを介した通信では、特定のファイアウォールルールを回避した状態で通信が行われます。例えば、ファイアウォー ルによって特定の IP アドレスへの通信がブロックされている場合であっても、プロキシを経由してリクエストが転送されるとい う状況が考えられます。
Java	「ON」にした場合、Java アプレットをブロックします。 Java アプレットは Web ページに組み込まれた小さなプログラムであり、ページの動的処理を行います。コンピュータへの不正ア クセスや感染を目的として不正なアプレットが使用されることがあります。
ActiveX	「ON」にした場合、ActiveX のダウンロードがブロックされます。 ActiveX コントロールは、Java アプレットと同様に Internet Explorer 実行中に Windows コンピュータにインストールされます。 コンピュータへの不正アクセスや感染を目的として不正な ActiveX が使用されることがあります。
Browser Cookies	「ON」にした場合、Web サイトによるクッキーの作成がブロックされます。 クッキーは、Web サイトによって保存されるセッション情報であり、主にログイン時に使用されます。Web サイトによっては情 報の追跡と閲覧習慣のために保存することもあります。

^{3. 「}Save」をクリックし、設定を適用します。

Approved URL(承認済み URL)

URL ドメイン名の承認リストを作成します。 承認リストに登録されたドメインは、どの形式でもアクセスを許可されます。 例:ドメイン「dlink」を登録した場合 LAN からのアクセスを許可される URL → www.dlink.com, support.dlink.com など

承認リストはテキストまたは CSV ファイルでインポート/エクスポートできます。

1. Security > Web Content Filter > Static Filtering > Approved URL の順にメニューをクリックし、以下の画面を表示します。

🙆 Sta	atus 🛜	Wireless	💂 Network	CB VPN	Security	0°
Security » Web Conter	nt Filter » Static	Filtering » Approv	ed URL			
Static Filtering	Approved URL	Blocked Keyword	is			
This page displays the firewall rules or block Approved URLs Li	e approved URLs. ked keywords. st	The list of website	es here are alway	s allowed to be ac	cessed, and have high	her prior
	F [Dight cli					
Show 10 - entrie	is [Kight ch	ick on record to get r	nore options]			
Show 10 entrie	is [Kight Gi	ck on record to get r	nore options]			
Show 10 entrie	is [Kigiit di	ck on record to get r	nore options] No data av	ailable in table		

図 8-29 Static Filtering > Approved URL タブ画面

■ URL のインポート / アップロード

- 1. テキスト /CSV ファイルからインポートする場合は、「Upload URLs List from File」をクリックします。
- 2. CSV ファイルを参照し、「Upload」をクリックして URL をインポートします。

■ URL のエクスポート

1. 現在のリストをエクスポートする場合は、「Export URLs List to File」をクリックします。

■ URL の追加

1. 「Add New Approved URL」をクリックして、以下の画面を表示します。

Approved URLs Configuration		×
URL		
		Save

図 8-30 Approved URLs Configuration 画面

Blocked URL(ブロック URL)

指定した URL へのアクセスをブロックします。

ブロック URL では、指定した URL 含むすべての Web サイトの URL 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。 例えば、ブロック URL が「Approved URLs List」の信頼されたドメインによって許可されたサイト内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。Blocked URL はテキストまたは CSV ファイルでインポート / エクスポートすることができます。

1. Security > Web Content Filter > Static Filtering > Blocked URL の順にメニューをクリックし、以下の画面を表示します。

🕐 Status 🎅 Wireless	Network	CB VPN	🔒 Security	O Maintenance	
Security » Web Content Filter » Static Filtering » Blocke	ed Keywords				0
Static Filtering Approved URL Blocked URL					
This page displays the blocked URLs. The list of website	s here are always bloc	cked.			
Blocked All URL Configuration Block All URL	off Save Ca	ncel			
Blocked URL List					
Show 10 V entries [Right click on record to get more	options]				٩
URL	🔂 Status				€
	No data availa	able in table			
Showing 0 to 0 of 0 entries				First I Previous Nex	t 🔰 Last 刘
Add New URL Upload URLs list from File	Export URLs Li	ist to File			

図 8-31 Static Filtering > Blocked URL タブ画面

■ ブロック URL の有効化

- 1. 「Blocked All URL Configuration」の「Block All URL」を「ON」にします。
- 2. 「Save」をクリックし、設定を適用します。
- URL リストのインポート / アップロード
- 1. テキスト /CSV ファイルからインポートする場合は、「Upload URLs List from File」をクリックします。
- 2. CSV ファイルを選択→「Upload」をクリックし URL リストをインポートします。
- URL リストのエクスポート
- 1. 現在のリストをエクスポートする場合は、「Export URLs List to File」をクリックします。

■ URL の追加

1. 「Add New URL」をクリックして、以下の画面を表示します。

図 8-32 Blocked URLs Configuration 画面

- 2. URL を入力します。
- 3. 「Save」をクリックし、設定を適用します。

Dynamic Filtering(ダイナミックフィルタリング)

Security > Web Content Filter > Dynamic Filtering $\varkappa = \neg -$

注意 本機能を使用するには WCF ライセンスが必要です。

WCF ライセンスのアクティブ化については、「License Update (WCF ライセンスのアップデート)」を参照してください。

ダイナミックフィルタリングは、カテゴリリストに基づきコンテンツのフィルタリングを行う機能です。

ルータを WCF ライセンスでアップグレードしてから、フィルタリングするカテゴリを選択します。ブロック対象のカテゴリに属する Web サイトへ アクセスした場合は、エラー画面が表示されます。

1. Security > Web Content Filter > Dynamic 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。

🖾 Status	🛜 Wireless	💻 Network 🗸	🚯 VPN 🖉	Security O ^o Main	tenance
Security » Web Content Filter »	Dynamic Filtering				3
This page displays the list of cate Dynamic Filtering	gories to be bloc	ked.			
Non-Managed Action		Allow			
Override Timeout		300	[Range: 60 - 360	0] Seconds	
Update on Access		ON			
Adult	OFF	News	OFF	Job Search	OLL
Gambling	OFF	Travel / Tourism	OFF	Shopping	OFF
Entertainment	OFF	Chat Rooms / IMs	OFF	Dating Sites	OFF
Game Sites	OFF	Investment Sites	OFF	E-Banking	OFF
Crime Terrorism	OFF	Personal Beliefs/Cults	OFF	Politics	OFF
Sports	OFF	www-E-Mail Sites	OFF	Violence / Undesirable	OFF
Malicious	OFF	Search Sites	OFF	Health Sites	OFF
Clubs and Societies	OFF	Music / Video	OFF	Business Oriented	OFF
Government Blocking List	OFF	Educational	OFF	Advertising	OFF
Drugs / Alcohol	OFF	Computing / IT	OFF	Swimsuit / Lingerie / Models	OFF
Remote Control / Desktop	OFF	Save Cano	cel		

図 8-33 Dynamic Filtering 画面

2. 以下の項目を設定します。

項目	説明
Non-Managed	管理対象外サイトに対して実行されるアクションを「Allow」(許可)または「Block」(拒否)から選択します。
Action	・ 初期値:「Allow」
Allow Override	「ON」にした場合、ブロックするカテゴリに分類されたサイトを許可します。
Override	ブロック対象のカテゴリが「Allow Override」によって許可される時間(秒)を指定します。
Timeout	
Update on	ブロック対象のカテゴリへの新しいアクセス毎に Override(上書き)タイマを再起動します。タイムアウトするまで接続は許可
Access	されます。
Adult	性的なコンテンツ、ヌードを提供するサイトなど。
News	ニュースや最近の時事情報を提供するサイト。新聞、放送局、その他出版社など。
Job Search	仕事の情報、インタビューコーチング、その他雇用に関するサービスを提供するサイト。
Gambling	オンラインギャンブルやギャンブルに関する情報のサイト。
Travel/Tourism	旅や旅行情報のサイト。シティマップや旅程、バス / 電車 / 航空の予約、ホテルの予約など。
Shopping	オンラインショッピング、カタログ、オークションサイトや広告など。
Entertainment	テレビ、映画、エンタメニュースなどのサイト及び映画の映像コンテンツやテレビ配信を提供するサイト。
Chat rooms/IMs	ソーシャルネットワークサイト。チャットルームやインスタントメッセージサイト。
Dating Sites	オンラインデート、結婚の仲介、交際アドバイス、個人広告、結婚に関連する Web サイト。
Game Sites	オンラインゲーム、MORPG、コンピュータゲームの情報やチートコードなどを提供するサイト。
Investment	仲買、信託、保険、その他組織に関連した投資のサイト。
Sites	

項目	説明
E-banking	金融機関によるオンライン銀行サービスを提供するサイト。
Crime/Terrorism	殺人や破壊活動、爆撃など反社会的行動に関する情報を提供するサイト。
Personal	宗教、礼拝所、宗教グループ、カルトに関するサイト。
Bellets/Cults	
Politics	政治、選挙、法律のサイト及び政治家や政党のノロモーションを行うサイト。
Sports	スボーツチームやファンクラフなどスボーツに関するサイト。
www-E-mail Sites	Web アクセス可能な E メールアカウントを使用して送信 / 受信する Web サイト。
Violence/ Undesirable	暴力、闘争、ヘイト、人種差別を促進または残虐な情報を含むサイト。
Malicious	マルウェアに感染またはマルウェアを広めるためにチャンネルとして使用されているサイト。
Search Sites	Web やその他のコンテンツを検索する検索エンジンサイト。
Health Sites	医師の検索や病気の回復などに関する情報を含む、個人の健康や医療サービスに関連したサイト。
Clubs and	コミュニティ、掲示板、クラブのサイト。
Societies	
Music/Video	インターネットラジオ、配信メディア、ミュージシャン、バンド、MP3 ダウンロードサイト。
Business	大企業、事業、中小ビジネスのサイト。
Concented	
Blocking List	Australian Broadcasting Authorities (ABA) のクロックリスト。
Educational	教育組織の Web サイト、教育に関するコンテンツや辞書・百科事典を含む参照資料を提供しているサイト。
Advertising	広告を提供するサイト。広告フィルタではなく広告サーバの識別とブロックのためのカテゴリです。
Drugs/Alcohol	アルコール飲料の販売促進や販売を行うサイト、カクテルレシピなどの作成方法を提供するサイト。
Computing/IT	コンピュータ、ソフトウェア、ハードウェア、テクノロジに関するサイト。技術製品を提供する会社のウェブサイト。
Swimsuit/ Lingerie/Models	下着やビキニ等を表示・販売するサイト。
Remote Control/ Desktop	リモートコントロール / リモートデスクトップのサイト。

URL Filtering ACL(URL フィルタリング ACL)

Security > Web Content Filter > URL Filtering ACL $\rtimes =$ = =

URLフィルタリング ACL の設定方法について説明します。 アクセスコントロールリスト(ACL)を使用すると、承認されたユーザのみが特定のリソースにアクセスできるため、ネットワークリソースへの不 正なアクセスを阻止できます。

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

🕜 Status	🛜 Wireless	📃 Network	C VPN	Security	©° Maintenance	
Security » Web Content Filter »	URL Filtering ACL					00
This page allows the user to ena LAN clients or users from the co	able or disable the URL Infigured static or dyna	. Filtering AccessCor amic filtering rules.	itrol feature and to	configure the profile	s for blacklisting or white	elisting the
URL Filtering Access Cont	trol					
Enable URL Filtering ACL						
Action	В	ilack List	\checkmark			
		Save	Cancel			
IIRI Filtering Access Cont	rol List					
Show 10 v entries [Right	t click on record to get n	nore options]				٩
Profile Name		🔄 Тур	e	⊖ Network		⇔
		No data a	vailable in table			1
Showing 0 to 0 of 0 entries					First Previous Next >	Last 刘
Add New Profile						

図 8-34 URL Filtering ACL 画面

- 2. アクセスコントロールリストを有効化する場合は、「Enable URL Filtering ACL」を「ON」にします。
- 「Action」でポリシーを「White List」(ホワイトリスト)、「Black List」(ブラックリスト)から指定し、「Save」をクリックします。 ブラックリストに指定されたクライアントはスタティック/ダイナミックルールで制御されます。ホワイトリストに指定されたクライアントは スタティック/ダイナミックルールで制御されません。
- 4. ルールを編集、削除するにはエントリ上で右クリックし、「Edit」または「Delete」を選択します。
- 5. 新しいルールを追加する場合は、「Add New Profile」をクリックし、以下の画面を表示します。

L Filtering ACL Config	uration	X
Profile Name		
Туре	Single IP	
IP Address		

図 8-35 URL Filtering ACL Configuration 画面画面

6. 以下の項目を設定します。

項目	説明
Profile Name	プロファイル名を入力します。
Туре	プロファイルのタイプを「Single IP」「Range」「Interface」から選択します。
IP Address	「Type」で「Single IP」を選択した場合、制御するクライアントの IP アドレスを指定します。
Start Address	「Type」で「Range」を選択した場合、制御するクライアントの IP アドレス範囲の開始アドレスを指定します。
End Address	「Type」で「Range」を選択した場合、制御するクライアントの IP アドレス範囲の終了アドレスを指定します。
Interface	「Type」で「Interface」を選択した場合、制御するネットワークのインタフェースを選択します。

Firewall(ファイアウォール設定)

Security > Firewall メニュー

ファイアウォールの設定方法について説明します。

Firewall Rules (ファイアウォールルールの設定)

Security > Firewall > Firewall Rules $\prec = = =$

インバウンド (WAN から LAN/DMZ) ルールでは、ご利用のネットワークに到達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、各サービスにインバウンドのファイアウォールルールを作成する必要があります。

ご利用のネットワークに到達するトラフィックを許可する場合、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。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す。使用の WAN アドレスがダイナミックで

このルータでは、スタティックなアドレスを WAN ホートに割り当てる場合には IP アドレスを使用します。使用の WAN アドレスかタイナミックで ある場合は、DDNS(Dynamic DNS)名を使用できます。

アウトバウンド (LAN/DMZ から WAN) ルールでは、ご利用のネットワークから送出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。アウトバウンドの初期ルールは、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。アウトバウンド初期ルールは、一方で、DMZ から安全でな い WAN までのアクセスを拒否するものです。「Default Outbound Policy」画面 (Security > Firewall > Firewall Rules > IPv4/IPv6 Firewall Rules) で 初期ルールの設定を変更することができます。デフォルトのインバウンドポリシーが「Always Allow」である場合、各サービスにインバウンドファ イアウォールルールを作成することで、インターネットサービスからの LAN ホストへのアクセスをブロックすることができます。

IPv4/IPv6 Firewall Rules (IPv4/IPv6 ファイアウォールルール)

1. Security > Firewall > Firewall Rules > IPv4 Firewall Rules タブ、または IPv6 Firewall Rules タブの順にメニューをクリックし、以下の画面を表示します。

🕢 Status	🛜 Wireless	💻 Network	CB VPN	Security	🗘 Maintenance	
Security » Firewall » Firewall R	ules » IPv4 Firewall Rul	es				00
IPv4 Firewall Rules IPv6	Firewall Rules Brid	ge Firewall Rules				
A firewall is a security mechanis You can use this page to manage firewall rules for this device and Firewall Rules	m to selectively block the firewall rules that allows several operat	or allow certain type t control traffic to ar ions on the firewall r	es of traffic in acc nd from your netw rules.	ordance with rules s ork. The List of Avai	pecified by network adm lable Firewall Rules tabl	inistrators. e includes all
Default Outbound Policy f	or IPv4					
Always	۲	Allow O Block				
		Save	Cancel			
IPv4 Firewall Rules List						
Show 10 v entries [Right	click on record to get m	ore options]				٩
Status ↔ From ↔ To Zone Zone	Service ⊖ Bloc Allo	w 9 Source ⊖ Hosts 9	Destination ⊖ Hosts	Local Server 😌 Interne Destin	et ⊖ Log _⊖ Rule	Priority 🕀
		No data ava	ailable in table			7
Showing 0 to 0 of 0 entries					First I Previous Next	> Last >
Add New IPv4 Firewall F	Rule					

図 8-36 IPv4 Firewall Rules/IPv6 Firewall Rules タブ画面

2. 「Default Outbound Policy for IPv4/IPv6」でポリシーを「Allow」「Block」から指定し、「Save」をクリックします。

3. 新しいルールを追加するには、「Add New IPv4/IPv6 Firewall Rule」をクリックし、以下の画面を表示します。

Pv4 Firewall Rules Configu	ration	×
From Zone	SECURE (LAN)	
To Zone	INSECURE (Dedicated WAN/Co	
Service	ANY	
Action	Always Block	
Source Hosts	Any O Single Address O Address range	
Destination Hosts	Any O Single Address O Address range Address range	
Log	Never O Always	
QoS Priority	Normal-Service	

図 8-37 IPv4 Firewall Rules Configuration 画面

4. 以下の項目を設定します。

項目	説明
From Zone	トラフィックの送信元を以下から選択します。
	IPv4 設定時:「SECURE(LAN)」「SECURE(VLAN)」「INSECURE (WAN1/WAN2/WAN3 (Mobile Internet))」「DMZ」
	IPv6 設定時:「SECURE(LAN)」「INSECURE (Dedicated WAN/Optional WAN)」
Available VLANs	「From Zone」で「SECURE(VLAN)」を選択した場合、VLAN を指定します。
To Zone	トラフィックの送信先を選択します。
Service	トラフィックを適用するサービスを選択します。
	ANY」を選択した場合、すべてのトラフィックにこのルールが適用されます。
Action	プルダウンメニューからアクションを選択します。
	 Always Block」:常にフロック 「Always Block」:常にフロック
	・ 「Always Allow」、常に計り 「Pleade by cabedula L: ス たジェール に たい ブロック
	・「BIOCK by schedule」、スケシュールによりノロック
Select Schedule	スケンユールを選択します。 Action] ぐ Block by schedule」または Allow by schedule」を選択した場合のみ衣示されます。 スケジュールの設定については「Schodulo(ファイアウォールスケジュール設定)」を参照 スイださい
Source Hosts/Destination	メデシュールのの設定については「Schedule(デディアジオールスデジュール設定)」を必然しててたとい。 洋信売 / 応失ホストを指定します
Host	\bullet [Anv]: d (70 π Z k
	・「Single Address」:IP アドレスを入力します。
	 「Address Range」:IP アドレス範囲を入力します。
Log	ファイアウォールトラフィックのログ出力を設定します。
QoS Priority	アウトバウンドルールの場合は、QoS のプライオリティを選択します。IPv6 Firewall Rules Configuration 画面では表
(IPv4 時のみ)	示されません。
	・「Normal-Service」: ToS=0(最も低い QoS)
	・「Minimize-Cost」: ToS=1
	• 「Maximize-Reliability」: ToS=2
	Maximize-Throughput J: ToS=4
	・「Minimize-Delay」: ToS=16(最も高い QoS)
External IP Address	「From Zone」で「INSECURE (WAN1/WAN2/WAN3 (Mobile Internet))」を選択した場合、宛先 NAT 設定として外部 IP
	Source NAT Settings
SNAT (Source Network Add	% 9 る場合に表示される項目で 9 。 dress Translation)は、受け取ったパケットの送信元 IP アドレスを別の IP アドレスに変換します。
External IP Address	外部IPアドレスを選択します。
	Destination NAT Settings
インバウンドルールを作成	する場合に表示される項目です。
DNAT (Destination Networ	k Address Translation)は、送信するパケットの宛先 IP アドレスを別の IP アドレスに変換します。
Internal IP Address	サーバを保持しているローカルネットワークのマシンの IP アドレスを指定します。
Enable Port Forwarding	「ON」:ポートフォワーディングを有効にします。有効にした場合、「Translate Port Number」を設定します。
	「OFF」:ポートフォワーディングを無効にします。
Translate Port Number	ポートフォワーディングに使用するポート番号を入力します。
External IP Address	外部IPアドレスを選択します。

5. 「Save」をクリックし、設定を適用します。

追加したルールは IPv4 Firewall Rules/IPv6 Firewall Rules タブ画面に表示されます。

右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Bridge Firewall Rules(ブリッジファイアウォールルール)

Security > Firewall Rules > Bridge Firewall Rules タブ

ブリッジネットワークにおけるファイアウォールの設定について説明します。

初期設定では、ブリッジネットワークのインタフェース間で、すべてのアクセスがインバウンド/アウトバウンドの双方向に許可されています。 インバウンドルールは DMZ ポートから LAN ポート 1 へのアクセスについて管理します。アウトバウンドは LAN ポート 1 から送信されるトラフィッ クのアクセスを制御します。

ファイアウォールルールは最も制御の厳しいルールがリストの上部に表示され、リストの順で適用されます。

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

	🕜 Status		💻 Networ	k 🝙 VPN	Security	O° Maintenance	
Security » F	irewall » Firewall R	tules » Bridge Firewal	l Rules				00
IPv4 Fir	ewall Rules IPv6	Firewall Rules Br	idge Firewall Rule	25			
A firewall is You can use table include allowed for I interface. Ou should move	a security mechani: this page to manage sall firewall rules nbound and Outbou ubound rules restric the strictest rules dge Firewall Ru	sm to selectively bloc the firewall rules th for the bridged netw nd direction between t access to traffic le (those with the most lles	ck or allow certain nat control traffic ork and allows sevi i the interfaces of aving your LAN Por specific services o	types of traffic in between interface eral operations or the bridged netw. t1 interface. Fire r addresses) to th	n accordance with rules es of your Bridged netwo t he firewall rules.By do rok. Inbound Rules gover wall rules are applied in e top of the list.	specified by network admin rk. The List of Bridge Firev efault in bridge Mode, all a n access from DMZ Port to the order listed. As a gen	nistrators. wall Rules iccess is the LAN Port1 eral rule, you
Show 10	✓ entries [Right cl	lick on record to get m	ore options]				٩
Status	6 Direction	⊖ Service e	⊖ Action ⊖	Source Hosts ⊖	Destination Hosts ⊖	Source MAC \ominus Destina MAC	tion \ominus
1			No dat	a available in table			
Showing 0 to	0 of 0 entries					K First Previous Next	t 🔰 Last 刘
Add New	Bridge Firewall I	Rule					

図 8-38 Firewall Rules > Bridge Firewall Rules タブ画面

2. 「Add New Bridge Firewall Rule」をクリックし、ルールを追加します。

Bridge Firewall Rule Configurati	ion	×
Direction	Inbound	
Service	ANY	
Action	Block Always	
Source Hosts	Any O Single Address O Address range	
Destination Hosts	Any O Single Address O Address range	
Source MAC	Any O Single MAC O MAC Range	
Destination MAC	● Any ○ Single MAC ○ MAC Range	

図 8-39 Bridge Firewall Rule Configuration 画面

3. 以下の項目を設定します。

項目	説明			
Direction	トラフィックの方向を「Inbound」または「Outbound」から選択します。			
Service	トラフィックを適用するサービスを選択します。			
	「ANY」を選択した場合、すべてのトラフィックにこのルールが適用されます。			
Action	プルダウンメニューからアクションを選択します。			
	・「Always Block」:常にブロック			
	・「Always Allow」:常に許可			
Source Hosts/Destination	送信元 / 宛先ホストを指定します。			
Host	・「Any」:すべてのホスト			
	・「Single Address」:IP アドレスを入力します。			
	・「Address Range」:IP アドレス範囲を入力します。			
Source Mac/Destination	送信元 / 宛先 MAC アドレスを指定します。			
Мас	・「Any」:すべての MAC			
	・「Single MAC」:MAC アドレスを入力します。			
	・「MAC Range」:MAC アドレス範囲を入力します。			

4. 「Save」をクリックし、設定を適用します。

追加したルールは Firewall Rules > Bridge Firewall Rules タブ画面に表示されます。

っ 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。
Schedule(ファイアウォールスケジュール設定)

Security > Firewall > Schedules $\prec = = =$

ファイアウォールのルールは関連付けられたスケジュールに基づき、自動的に有効/無効に指定することが可能です。スケジュール設定ページでは 曜日/時刻の単位で新しくスケジュールを設定することが可能です。設定したスケジュールを Security > Firewall > Firewall Rules 画面で選択して適用します。

I	洧	Ē		f.
ų	-	-	1.0	-

全てのスケジュールはルータで設定された時刻とタイムゾーンを基準としています。時刻、タイムゾーンの設定については「Data and Time (システムの日時設定)」を参照してください。

1. Security > Firewall > 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。

0		🛜 Wireless		Network	CA VPN	£	Secur	ity 🗘°		
Security » Firew	all » Schedul	es								00
When you create Illows several op	e a firewall ru erations on t t	le, you can specify a he Schedules.	schedule	when the rul	e applies. The	table list	all the A	wailable Schedu	ules for this dev	ice and
Show 10 💌	entries	[Right click on record to	get more	options]						٩
Name	٥	Day(s)	θ	Start Time			Θ	End Time		(
				No data ava	ilable in table					
Showing 0 to 0 of	0 entries							First	Previous Next	Last 🕅
Add New Sci	hedule									
8-40 Sche	edules 画面	Ī								

2. 「Add New Schedule」をクリックし、スケジュールを追加します。

Schedules Configuration		\bigotimes
Name		^
Scheduled Days Do you want this schedule to be active on all days or specific days?	O All Days Specific Days	
Monday	ON Tuesday	OFF
Wednesday	Thursday	OFF
Friday	Saturday	OFF
Sunday	OFF	
Scheduled Time of Day Do you want this schedule to be active all day or at Specific Times during the day?	O All Day • specific times	N
Start Time Start Time	HH MM AM/PM	
End Time End Time	12:08 AM HH MM AM/PM 12 08 AM 12 08 AM	~
		Save

図 8-41 Schedules Configuration 画面

第8章 セキュリティ設定(Security)

3. 以下の項目を設定します。

項目	説明
Name	スケジュール名を入力します。
Scheduled Days	「All Days」(毎日)または「Specific Days」(指定日)を選択します。
Monday - Sunday	「Specific Days」を選択した場合、有効にする曜日を「ON」にします。
Scheduled Time of Day	「All Day」(終日)または「specific times」(指定時間)を選択します。
Start Time/End Time	「specific times」を選択した場合、開始時刻(Start Time)と終了時刻(End Time)を指定します。

4. 「Save」をクリックし、設定を適用します。

追加したスケジュールは Schedules 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Blocked Clients(クライアントブロック設定)

Security > Firewall > Blocked Clients $\prec = \neg -$

クライアントブロック設定では、指定した MAC アドレスのクライアントをブロックすることができます。 ブロックするクライアントの追加方法について説明します。

1. Security > Firewall > Blocked 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。

	🕜 Status	🛜 Wireless	💻 Network	A VPN	🚊 Security	O Maintenance			
Security » F	irewall » Blocked Cl	ients					0 0		
This page shows a list of clients MAC addresses blocked by admin. Block MAC Clients List									
Show 10 v entries [Right click on record to get more options]									
MAC Addre	ess			Description	n	- ⊖			
			No data av	ailable in table					
Showing 0 to 0 of 0 entries Next > Last						Last X			
Add New	Add New Blocked Clients								

図 8-42 Blocked Clients 画面

2. 「Add New Blocked Clients」をクリックし、クライアントを追加します。

Blocked MAC Profile Configuration	8
MAC Address Description	

図 8-43 Blocked MAC Profile Configuration 画面

3. 以下の項目を設定します。

項目	説明
MAC Address	ブロックするクライアントの MAC アドレスを入力します。
Description	ブロックするクライアントの概要について入力します。

4. 「Save」をクリックし、設定を適用します。

追加したクライアントのリストは Blocked Clients 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Custom Services(カスタムサービスの設定)

Security > Firewall > Custom Services $\prec = = =$

ファイアウォールルールを定義するカスタムサービスの設定方法について説明します。 一般的なサービスは 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が LAN または WAN に存在します。 カスタムサービス設定では、ポート範囲を定義し、トラフィックタイプ(TCP/UDP/ICMP など)を指定することができます。 本画面で定義したサービスは、Security > Firewall > Firewall Rules 画面のサービスリストに表示されます。

1. Security > Firewall > 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。

	🕢 Status		💻 Network	CA VPN	🔒 Security	O Maintenance				
Security » F	Security » Firewall » Custom Services									
When you create a firewall rule, you can specify a service that is controlled by the rule Common types of services are available for selection, and you can create your own custom services. This page allows creation of custom services against which firewall rules can be defined. Once defined, the new service will appear in the List of Available Custom Services table.										
Custom Se	rvices List									
Show 10	✓ entries [Right cl	lick on record to get mor	re options]				٩			
Name	🗘 Туре	⊖ Source Port Rar	nge G	ICMP Type /	Destination Port R	ange	÷			
			No data ava	ilable in table						
Showing 0 to	0 of 0 entries					H First A Previous Next	> Last >			
Add New	Add New Custom Service									
	Justom Sonvico	。面面								

図 8-44 Custom Services 画面

2. 「Add New Custom Service」をクリックし、カスタムサービスを追加します。

Custom Services Configuration		×
Name Type Port Type	TCP • Port Range • Multiple Ports	
Source Start Port Source Finish Port Destination Start Port Destination Finish Port	[Range: 1 - 65535] [Range: 1 - 65535] [Range: 1 - 65535] [Range: 1 - 65535]	
	Save	

図 8-45 Custom Services Configuration 画面

3. 以下の項目を設定します。

項目	説明
Name	カスタムサービス名を入力します。
Туре	サービスが使用するL3 プロトコルを以下から選択します。
	TTCP」「UDP」「BOTH」「ICMP」「ICMPv6」
Port Type	ポートタイプを以下から選択します。
	「Port Range」「Multiple Ports」
Source / Destination	「Port Range」を選択した場合、サービスに使用する送信元 / 宛先開始ポートを指定します。
Start Port	
Source / Destination	「Port Range」を選択した場合、サービスに使用する送信元 / 宛先終了ポートを指定します。
Finish Port	
Source / Destination	「Multiple Port」を選択した場合、サービスに使用する送信元 / 宛先の複数ポートを「,」(コンマ)で区切り指定します。
Ports	
ICMP/ICMPv6 Type	「ICMP/ICMPv6 Type」を選択した場合、適用する数値を指定します。
	・ICMP の設定可能範囲:0-40
	・ICMPv6 の設定可能範囲:1-255

4. 「Save」をクリックし、設定を適用します。

追加したカスタムサービスは Custom Servce 画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

ALGs(ALG サポート)

Security > Firewall > ALGs $\prec = = =$

ALG(Application Level Gateways)は、本ルータのファイアウォールと NAT サポートを強化し、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セキュリティコンポーネントです。

ALG の有効化により、特定のクライアントアプリケーション(H.323、RSTP など)が既知のポートと通信する際、ファイウォールで動的なエフェメ ラル TCP/UDP ポートを使用することができます。そのため、管理者が多数のポートをオープンする必要がなくなります。

ALG は、サポートされる特定のアプリケーションが使用するプロトコルを認識することができるため、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となっています。

ALGs

ALG 機能において、ルータへの通過を許可するプロトコルを選択します。

1. Security > Firewall > ALGs タブをクリックして、以下の画面を表示します。

🙆 Status	🛜 Wireless	Retwork	CA VPN	Security	O ^o Maintenance
curity <mark>» Firewall »</mark> ALGs	2				0
ALGS SMTP ALGS A	opproved Mail IDs Blo	cked Mail IDs 🛛 Mail F	iltering		
oplication Level Gateway a plication layer "control/d umber of ALGs for common LGS	ullows customized NAT t lata" protocols such as applications are enable	raversal filters to be p TFTP, SIP, RTSP etc. E ed by default.	lugged into the gat ich ALG provides sp	eway to support addro ecial handling for a s	ess and port translation for cert pecific protocol or application.
RTSP		OFF			
SIP		OFF			
H.323		OFF			
TFTP		Off			
		Save	Cancel		

図 8-46 ALG > ALGs タブ画面

- 2. ルータへの通過を許可するプロトコルを「ON」にします。
- 3. 「Save」をクリックし、設定を適用します。

SMTP ALGs

Simple Mail Transfer Protocol(SMTP)は、インターネット経由で E-mail を送信するために使用されるテキストベースのプロトコルです。通常、ロー カル SMTP サーバは DMZ に置かれ、リモート SMTP サーバから送信されたメールがルータを横断してローカルサーバに届くように構成されます。ロー カルユーザは、E-mail のクライアントソフトウェアを使用してローカルの SMTP サーバから E-mail を取得します。また、SMTP はクライアントが Eメー ルを送信する際に使用され、クライアント・サーバ双方からの SMTP トラフィックをモニタするために SMTP ALG を使用することも可能です。

注意 SMTP ALG 機能を使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

1. Security > Firewall > ALGs > SMTP ALGs タブをクリックして、以下の画面を表示します。

	🕋 Status		💻 Network	A VPN	Security	🗢 Maintenance				
Security » F	iecurity » Firewall » ALGs » SMTP ALGs									
ALGs	SMTP ALGs Appro	oved Mail IDs Block	ed Mail IDs 🛛 Mail Fi	ltering						
This page all	ows the user to ena	ble the SMTP ALG.								
SMTP ALG										
Status	Status									
			Save	Cancel						

図 8-47 ALGs > SMTP ALGs タブ

- 2. 「Status」を「ON」にし、SMTP パケットを検査するポートを指定します。
- 3. 「Save」をクリックし、設定を適用します。

Approved Mail ID(許可メール ID)

メール ID を追加し、該当するメールを許可することができます。

1. Security > Firewall > ALGs > Approved Mail IDs タブをクリックして、以下の画面を表示します。

	🙆 Status	🛜 Wireless	💻 Network	CAS VPN	Security	O° Maintenance	
curity »	Firewall » ALGs	 Approved Mail IDs 					00
ALGs	SMTP ALGS AP	proved Mail IDs Bloc	ked Mail IDs 🕇 Mail F	Filtering			
nis table	lists all the availab	le Mail Ids that are sup	posed to be allowed	in the system.			
pprove	d Mail IDs List						
Show 10	• entries	[Right click on record to	get more options]				٩
Mail ID							C
			No data av	ailable in table			
Showing 0	to 0 of 0 entries				11	First J Previous Next	> Last >
Add N	ew Approved Mail	ID					

図 8-48 ALGs > Approved Mail IDs タブ画面

2. 「Add New Approved Mail ID」をクリックし、許可するメール ID を追加します。

Approved Mail IDs Configuration	8
Mail ID	
	Save

図 8-49 Approved Mail IDs Configuration 画面

3. 「Save」をクリックし、設定を適用します。

追加したメール ID は **ALGs > Approved Mail IDs タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Blocked Mail IDs(拒否メール ID)

メール ID を追加し、該当するメールを拒否することができます。

1. Security > Firewall > ALGs > Blocked Mail IDs タブをクリックして、以下の画面を表示します。

	🖾 Status	🛜 Wireless	🖳 Network	CB VPN	Security	O Maintenance	
Security	» Firewall » ALGs »	 Blocked Mail IDs 					00
ALG	SMTP ALGS AP	proved Mail IDs Blo	cked Mail IDs Mail F	iltering			
^{This tabl}	le lists all the availab d Mail IDs List	le Mail Ids that are su	oposed to be blocked	in <mark>the</mark> system.			
Show 1	0 entries	[Right click on record to	get more options]				٩
Mail I)						0
			No data av	ailable in table			
Showing	0 to 0 of 0 entries					First Previous Next	Last 刘
Add	New Blocked Mail II	D					

図 8-50 ALGs > Blocked Mail IDs タブ画面

2. 「Add New Blocked Mail ID」をクリックし、拒否するメール ID を追加します。

Blocked	Mail IDs Configuration			8
Mail II)]	
				Save
図 8-51	ALGs > Mail Filtering タブ画面	0		

3. 「Save」をクリックし、設定を適用します。

追加したメール ID は **ALGs > Blocked Mail IDs タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Mail Filtering(メールフィルタリング)

Security > Firewall > ALGs > Mail Filtering $\vartheta \vec{J}$

メールフィルタリングの設定について説明します。

1. Security > Firewall > ALGs > Mail Filtering タブをクリックして、以下の画面を表示します。

	A Status	🛜 Wireless	🖳 Network	CAS VPN	🔒 Se	curity	O Maintenance	
ecurity »	• Firewall » ALGs	» Mail Filtering						00
ALGs	SMTP ALGS AP	proved Mail IDs Blo	cked Mail IDs Mail F	iltering				
he table	lists all the Subjec	ts and Mail ids which a	re to allowed/blocked					
Show 10	tering List	Right dick on record to	get more options]					
511044	• entries	Inight click on record to	Sectione options]					q
Subject	t	(Mail ID		Θ	Action		e
			No data av	ailable in table				
Showing (0 to 0 of 0 entries						First Previous Next >	Last 刘
	Iow Mail Filter							
	rew wan ritter							

図 8-52 ALGs > Mail Filtering タブ画面

2. 「Add New Mail Filter」をクリックし、メールフィルタを追加します。

Mail Filtering Configura	tion	×
Subject Mail ID		
Action	Allow O Block	
		Save

図 8-53 Mail Filtering Configuration 画面

- 3. 「Subject」と「Mail ID」を指定し、「Action」を「Allow」(許可)または「Deny」(拒否)から選択します。
- 4. 「Save」をクリックし、設定を適用します。

追加したメールフィルタは **ALGs > Mail Filtering タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

VPN Passthrough (VPN パススルー)

Security > Firewall > VPN Passthrough メニュー VPN パススルーの設定方法について説明します。

VPN パススルーは、LAN 内のプライベートアドレスを持った VPN クライアントのパケットをインターネット側に通過させる機能です。

1. Security > Firewall > 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。

	🖾 Status	🛜 Wireless	💻 Network	S VPN	Security	O Maintenance
ecurity »	Firewall » VPN Pa	ssthrough				0
his page a rewall rul	llows user to conf es based on the sa	igure VPN (IPsec, PPTP me service.	and L2TP) passthrou	gh on the router. E	nabled passthrough c	neckboxes have higher priority
PN Pass	through					
IPSec		1	ON			
PPTP		1	ON			
L2TP		1	ON IME			
			Save	Cancel		

図 8-54 VPN Passthrough 画面

- 2. 許可する VPN プロトコルを「ON」にします。
- 3. 「Save」をクリックし、設定を適用します。

Dynamic Port Forwarding(ダイナミックポートフォワーディング)

Security > Firewall > Dynamic Port Forwarding $\forall = \neg -$

ダイナミックポートフォワーディングの設定方法について説明します。 Application Rules タブでアプリケーションルールの設定を行います。設定したルールのステータスは、Application Rules Status タブに表示されます。

Application Rules (アプリケーションルール設定)

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 上のデバイス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 からのアウトバウンドのリクエストを待ち、その後、その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。この動作は、オープンした出力または入力ポートでアプリケーションがデータを送信している間のダイナミックなポートフォワーディングの形式と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、特定の LAN IP または IP 範囲を参照する必要がないため、スタティックポートフォワーディングよりも柔軟性があります。また、使用されていないポートはオープンの状態にされないため、セキュリティのレベルを向上できます。

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。

アプリケーションによっては、機能が適切に動作するために、外部デバイスから接続される際に特定のポートまたはポート範囲でデータを受信する 必要があります。ルータは、必要なポートまたはポート範囲のみでそのアプリケーションの全受信データを送信する必要があります。ルータは一般 的なアプリケーションやゲームのアウトバウンド/インバウンドポートの一覧を保持しており、オープンすることができます。また、トラフィック タイプ (TCP や UDP) 及びオープンするインバウンド/アウトバウンドポートの範囲を定義して、ポートトリガルールを指定することもできます。

1. Security > Firewall > Dynamic Port Forwarding > Application Rules タブの順にメニューをクリックし、以下の画面を表示します。

		🛜 Wireles	s 📃 Netv		CAS VPN	🔒 s	ecurity	O ° M		enance	
ecurity » Firewal	l » Dynami	ic Port Forwarding								0	0
Application R	ules Appi	lication Rules Sta	tus								
he table lists all	the availabl	e port triggering	rules and allows se	everal oper	ations on the	rules.					
Application Ru	les List										
Show 10 👻 er	ntries	[Right click on reco	rd to get more optio	ons]							٩
Name O St.	atus 🖯	Protocol O	Interface	⊖ Outgo	ing ⊖ Port ⊖	Outgoing End Port	Θ	Incoming Start Port	Θ	Incoming End Port	e
			- N	No data availa	ble in table						
Showing 0 to 0 of 0	entries							J First J P	revious	Next > La	t >

図 8-55 Dynamic Port Forwarding > Application Rules タブ画面

2. アプリケーションルールを追加する場合は、「Add New Application Rule」をクリックし以下の画面を表示します。

Application Rules	-			
Name				
Enable	OFF			
Protocol	• тср	0	UDP	
Interface	EAN	0	DMZ	
Outgoing (Trigger) Port Range		_		
Start Port			[Range: 0 - 65535]	
То			[Range: 0 - 65535]	
Incoming (Response) Port Range		_		
Start Port			[Range: 0 - 65535]	
То			[Range: 0 - 65535]	

図 8-56 Application Rules Configuration 画面

3. 以下の項目を設定します。

項目	説明
Name	ルール名を入力します。
Enable	「ON」にしてルールを有効にします。
Protocol	プロトコルを「TCP」「UDP」から選択します。
Interface	インタフェースを「LAN」「DMZ」から選択します。
Outgoing (Trigger) Port Range	トリガポート範囲の開始 / 終了ポートを指定します。
Incoming (Response) Port Range	受信ポートを範囲の開始 / 終了ポートを指定します。

4. 「Save」をクリックし、設定を適用します。

追加したルールは **Dynamic Port Forwarding > Application Rules タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Application Rules Status (アプリケーションルールステータス)

アプリケーションルールのステータスが表示されます。

1. Security > Firewall > Dynamic Port Forwarding > Application Rules Status タブの順にメニューをクリックし、以下の画面を表示します。

	🙆 Status		💂 Network	CAS VPN	Security	O° Maintenance	
Security »	Firewall » Dynam	ic Port Forwarding » App	plication Rules Status				00
Applic	ation Rules App	lication Rules Status					
This page li Applicati	ists the application	n rules containing statu s <mark>List</mark>	us, open ports and exp	piry time for a par	rticular rule.		
Show 10	▼ entries	[No right click options]					٩
LAN / DA	WZ IP Address		O Open Ports	Θ	Time Remaining (Se	ec.)	Θ
			No data ava	ilable in table			
	to 0 of 0 option						

図 8-57 Application Rules > Application Rules タブ画面

2. 以下の項目を確認します。

項目	説明
LAN / DMZ IP Address	アプリケーションルールがアクティブになり、応答ポートが開かれるトリガとなった内部ネットワーク IP アドレスが表示
	されます。
Open Ports	内部デバイスのリクエストにより、このファイアウォールを通過してオープンになった応答ポートが表示されます。
Time Remaining (Sec.)	開いているポートが外部トラフィックを許可する時間(単位:秒)が表示されます。
	この時間は、トラフィックが LAN / DMZ からトリガポートに送信されるたびにリセットされます。

Attack Checks(攻撃のチェック)

Security > Firewall > Attack Checks $\prec = \neg -$

攻撃(アタック)とは、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の問題を意味します。攻撃を確認 することにより、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 におけるセキュリティの脅威を管理できます。 また、TCP フラッド、UDP フラッド、Dos 攻撃など、帯域幅を消費し通常のネットワークサービスの動作を妨げる攻撃をブロックすることが可能です。

1. Security > Firewall > 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。

🕢 Status	🛜 Wireless	💻 Network	CA VPN	Security	O Maintenance	
Security » Firewall » Attack C	hecks					00
This page allows you to specify	whether or not to prot	ect against common a	ittacks from the L	AN and WAN network	5.	
Attack Checks						
WAN Security Checks						
Stealth Mode		DN III				
Block TCP Flood						
TCP Filter Check						
Filter Check		DN THE				
LAN Security Checks						
Block UDP Flood		25	[Range: 25 - 500]			
ICSA Settings						
Block ICMP Notification		DN THE				
Block Fragmented Packet	s 🚺					
Block Multicast Packets						
Block Spoofed IP Packets		N CARL				
DoS Attacks						
SYN Flood Detect Rate	1	28 [Range: 1	- 10000] max/sec			
Echo Storm	1	[Range: 1	- 10000] Ping pkts./:	sec		
ICMP Flood	1	[Range: 1	- 10000] ICMP pkts./	sec		
		Save	Cancel			

図 8-58 Attack Checks 画面

2. 以下の項目を設定します。

項目	説明				
	WAN Security Checks				
Stealth Mode	「ON」にした場合、ルータは WAN からのポートスキャンに応答しません。検出と攻撃による影響が低減されます。				
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。				
	TCP Filter Check				
Filter Check	本オプションを有効にすると、不正な TCP パケット(FIN、RST や ACK)は SNAT とともに破棄され、接続は遮断 されます。「TCP OUT-OF-WINDOW」のようなパケットは不正として判断されます。				
	LAN Security Checks				
Block UDP Flood	「ON」にした場合、UDP フラッドをブロックします。 LAN 上の単一コンピュータからの、設定した数を超えたアクティブな UDP 接続を受け付けません。 • 設定可能範囲: 25-500 • 初期値: 25				
	ICSA Settings				
Block ICMP Notification	本オプションを有効にすると、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 攻撃に使用される可能性があります。				
Block Fragmented Packets	本オプションを有効にすると、ゲートウェイを経由する全てのフラグメント化パケットを破棄します。				
Block Multicast Packets	本オプションを有効にすると、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。ルータ経由または ルータへのスプーフィング攻撃の可能性があります。				
Block Spoofed IP Packets	本オプションを有効にすると、IP スプーフィングパケットを破棄します。				
	DoS Attacks				
SYN Flood Detect Rate	SYN フラッドを検出できるレートを指定します。				
Echo Storm	ルータが WAN からのエコーストーム攻撃を検出して、その外部アドレスからの ping トラフィックを防止する 1 秒あたりの ping パケット数を指定します。				
ICMP Flood	ルータが WAN からの ICMP フラッド攻撃を検出して、その外部アドレスからの ICMP トラフィックを防止する 1 秒あたりの ICMP パケット数を指定します。				

Intel® AMT(インテル®アクティブ・マネジメント・テクノロジー)

Security > Firewall > Intel AMT $\checkmark =$ $\neg -$

インテル®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にリモートでアクセスし管理できます。PCが電源およびネットワーク接続している限り、電源がオフの場合またはOSやハードディスクが動作していない場合でも制御することが可能です。インテル®AMTは、クライアントマシンで独立して動作する、有線または無線ネットワークを通じて接続できる個別の管理プロセッサを使用しています。

1. Security > Firewall > 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。

surity » Firewall » Intel® AMT				
e table lists all the available intelAmi tel® AMT	tin the system.			
Intel® AMT Setup				
Ports	ON COM			
WAN Host	Any O Specify	WAN IPs		
Internal IP Address				
ntel® AMT Reflector				
Reflector	ON THE			
Redirect to Port 16992	Listen on Po	ort 16992	[Range : 1 - 65535]	
Redirect to Port 16993	CN Listen on Po	ort 16993	[Range : 1 - 65535]	
Redirect to Port 16994	ON Listen on Po	ort 16994	[Range : 1 - 65535]	
Redirect to Port 16995	Listen on Po	ort 16995	[Range : 1 - 65535]	
Redirect to Port 9971	Listen on Po	ort 9971	[Range : 1 - 65535]	

- 図 8-59 Intel AMT 画面
- 2. 以下の項目を設定します。

項目	説明						
	Intel® AMT Setup						
Ports	本項目を有効にすると、特定のポートに対してインバウンド/アウトバウンドファイアウォールルールを追加して、インテル®AMTサービスを有効にします。						
WAN Hosts	「Any」を選択すると、WAN 側の全ホストに対してローカルサーバへのアクセスが許可されます。「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指定します。 アドレスはカンマ「,」で区切って指定する必要があります。						
WAN Host Addresses	「Specify WAN IPs」を選択した場合、ローカルユーザへのアクセス許可が必要な WAN IP アドレスリストをカンマ「,」 で区切って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 アドレスの間に空白を入れないでく ださい。						
Internal IP Address	LAN ホスト(ローカルサーバ)の IP アドレスを指定します。						
	Intel® AMT Reflector						
Reflector	「ON」にしてリフレクターを有効にします。指定したポートでクライアントに対してデータを送り返します。						
Redirect to Port 16992	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port:サーバがインバウンド通信をリッスンするポートを指定します。						
Redirect to Port 16993	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port:サーバがインバウンド通信をリッスンするポートを指定します。						
Redirect to Port 16994	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port:サーバがインバウンド通信をリッスンするポートを指定します。						
Redirect to Port 16995	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port:サーバがインバウンド通信をリッスンするポートを指定します。						
Redirect to Port 9971	有効にすると、インバウンド接続用に本ポートでリッスンします。 Listen on Port:サーバがインバウンド通信をリッスンするポートを指定します。						

IPS(侵入防止システム)

Security > Firewall > IPS $\prec = \neg -$

IPS(Intrusion Prevention System)/ ルーター侵入防止システムは、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。ルータに保存されたスタティックな攻撃シグニチャにより、一般的な攻撃を検出して防止することが可能です。また、管理者は WAN からの悪意のある侵入の試みが防止された回数を確認できます。

注意 IPS 機能を使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

1. Security > Firewall > 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。

	🕋 Status		💻 Network	යි VPN	🔒 Security	O Maintenance				
Security » Fi	curity » Firewall » IPS									
This page allo	ows user to configu	re Intrusion Detection	System and Intrusio	n Preventions syst	em on the router.					
IPS										
Intrusion	Detection/Preve	ntion Enable								
Enable I	ntrusion Detection		OFF							
Enable II	ntrusion Preventior	۰ E	OFF							
IPS/IDS CI	hecks Active Betv	veen								
LAN and	WAN		OFF							
DMZ and	WAN		OFF							
IPS Status										
Number	of Signatures Load	ed 0								
			Save	Cancel						

図 8-60 IPS 画面

2. 以下の項目を設定します。

項目	説明					
	Intrusion Detection/Prevention Enable					
Enable Intrusion Detection	「ON」にして侵入の検出を有効にします。					
Enable Intrusion Prevention	「ON」にして侵入の防止を有効にします。					
	IPS/IDS Checks Active Between					
LAN and WAN	「LAN / WAN」間での IPS を有効にします。					
DMZ and WAN	「DMZ / WAN」間での IPS を有効にします。					
IPS Status						
Number of Signatures Loaded	シグネチャの読み込み回数が表示されます。					

App Control Policy (アプリケーションコントロールポリシー)

Application Control (アプリケーションコントロール)

Security > App Control Policy > Application Control $\checkmark = = = -$

処理中のアプリケーションのトラフィックをネットワーク管理者が許可、ブロック、またはコントロールすることができます。

注意 アプリケーションコントロール機能を使用する場合、ハードウェアオフロードが無効になるため、パフォーマンスが低下する場合があります。

Policies(ポリシー設定)

グループを作成し、管理するアプリケーションを選択します。また、アプリケーション管理のポリシーを設定することも可能です。 1. Security > App Control Policy > Application Control > Policies タブの順にメニューをクリックし、以下の画面を表示します。

CA Status	🛜 Wireless	💂 Network 🎧 VP	N 🔒 Security	O Maintenance
ecurity » App Control Policy »	Application Control » P	olicies		(
Policios Notwork Profile				
Policies Network Profile				
pplication Control feature allo pplication Control feature will inctions related to the feature ore options to administrators ontrol feature should be enabl	ws network administrat be license based subsc User can select partic to set up policies to coi ed to configure Default	tors to allow or block or control t rription. Administrator needs to e cular app or can select group to r ntrol access to the applications f : Policy, Group and Policy setting	the traffic of applications the mable Application Control lio manage the applications asso or selected network users or s	at is transacting the traffic. ense in device to get visibilit ciated with that group. This a IP's or network segments.App
pplication Control Polic	ies			
Enable Application Control		OFF		
		Save Cancel		
Default Policy	-	2		
Always	۲	Allow OBlock		
		Save Cancel		
	_			
Application Control Gro	oup List			
Show 10 v entries [Right	t click on record to get m	ore options]		
Group Name		App List	⊖ St	atus
		No data available in table		
Showing 0 to 0 of 0 entries			K] F	rst I Previous Next > Last
Showing 0 to 0 of 0 entries			KI F	rst A Previous Next > Last
Showing 0 to 0 of 0 entries Add New Group			<u>H</u> F	rst J Previous Next > Last
Showing 0 to 0 of 0 entries Add New Group			KI F	rst - Previous Next > Last
Showing 0 to 0 of 0 entries Add New Group Application Control Pol	icy List		KI F	rst - Previous Next -> Last
Add New Group Add New Group Application Control Pol Show 10 🕑 entries	icy List		KI F	rst Previous Next > Last
Add New Group Add New Group Application Control Pol Show 10 v entries Policy Name	icy List	⊖ Policy Type	APP/Group S	rst (Previous Next) Last
Add New Group Add New Group Application Control Pol Show 10 v entries Policy Name	icy List	Policy Type No data available in table	ti F :∂ APP/Group S	rst (Previous Next) Last
Add New Group Add New Group Application Control Pol Show 10 v entries Policy Name Showing 0 to 0 of 0 entries	icy List		APP/Group S	rst (Previous Next) Last
Showing 0 to 0 of 0 entries Add New Group Application Control Pol Show 10 v entries Policy Name Showing 0 to 0 of 0 entries	icy List	O Policy Type No data available in table	ि APP/Group S	rst Previous Next > Last

図 8-61 Application Control > Policies タブ画面

2. 「Enable Application Control」を「ON」または「OFF」に設定 →「Save」をクリックします。(初期値:「OFF」)

3. 以下の項目を設定します。

項目	説明					
	Default Policy					
Always	作成したグループに対するデフォルトポリシーを以下から選択します。 ・「Allow」:グループのアプリケーションを常に許可します。 ・「Deny」:グループのアプリケーションを常にブロックします。					
	Application Control Group List					
Group Name	グループ名が表示されます。					
App List	選択したアプリケーションが表示されます。					
Status	選択したアプリケーションのステータスが表示されます。					
	Application Control Policy List					
Policy Name	ポリシー名が表示されます。					
Action	ポリシールールのアクションが表示されます。					
Policy Type	ポリシータイプが表示されます。					
APP/Group Status	アプリケーションおよびグループのステータスが表示されます。					

4. 「Save」をクリックし、設定を適用します。

■ グループの追加

「Enable Application Control」を「ON」にした場合のみグループの追加を行うことができます。

1. 「Add New Group」をクリックし、グループを追加します。



図 8-62 Group Configuration 画面

2. 以下の項目を設定します。

項目	説明
Group Name	グループ名を入力します。
Supported Apps	サポートされているアプリケーションが表示されます。
Selected Apps	「Supported Apps」からアプリケーションを選択します。
	選択したアプリケーションが「Selected Apps」のボックスに表示されます。

3. 「Save」をクリックし、設定を適用します。

追加したグループは **Application Control > Policies タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

■ ポリシーの追加

「Enable Application Control」を「ON」にした場合のみポリシーの追加を行うことができます。

1. 「Add New Application Policy」をクリックし、アプリケーションポリシーを追加します。

Application Control Policy Config	uration	×
Policy Name		
Application Type	● Group ○ APP	
Group Name	AudioVideo	
Action	Always Allow	
Log	OFF	
Policy Type	● Global ○ Feature	

図 8-63 Application Control Policy Configuration 画面

2. 以下の項目を設定します。

項目	説明
Policy Name	ポリシー名を入力します。
Application Type	アプリケーションタイプを「Group」または「APP」から選択します。
Group Name	グループ名を選択します。
APP Name	アプリケーション名を選択します。
Action	ポリシーのアクションを以下から選択します。 「Always Allow」:常に許可 「Always Block」: 常にブロック
	 「Allow by schedule」: スケジュールにより許可 「Block by schedule」: スケジュールによりブロック
Select Schedule	「Action」で「Allow by schedule」「Block by schedule」を選択した場合、スケジュールを選択します。 スケジュールは、Security > Firewall > Schedules 画面で登録します。
Log	「ON」にした場合、統計のログを取得します。
Policy Type	ポリシータイプを以下から選択します。 ・「Global」:選択したアプリケーションに該当するすべてのトラフィックにポリシーを適用します。 ・「Feature」:以降に表示される項目でポリシーを設定します。
Network Profiles	ネットワークプロファイルを選択します。
Captive Portal User	キャプティブポータルを「ON」または「OFF」にします。「ON」にした場合、すべてのキャプティブポータルクライアン トがこのポリシーに従います。
User DB	ユーザデータベースを「ON」または「OFF」にします。ユーザデータベースは、選択したアプリケーションを制御するネットワークユーザを選択するために使用します。
Network Type	ネットワークタイプを「Groups」または「Users」から選択します。
Available Groups/ Available Users	アプリケーションを管理するグループまたはユーザを選択します。
QoS	QoS を「ON」または「OFF」にします。 選択したアプリケーションを介してアクセスするトラフィックの帯域幅レートまたは優先順位を選択できます。 「Action」で「Always Allow」「Allow by schedule」を選択した場合のみ表示されます。
Profile Type	プロファイルのタイプを「Rate」または「Priority」から選択します。 QoS を有効にした場合のみ表示されます。
Priority	プロファイルのタイプを「Priority」にした場合、優先度を以下から選択します。 「High」「Medium」「Low」
Minimum Bandwidth Rate	プロファイルのタイプを「Rate」にした場合、最小の帯域幅を入力します。
Maximum Bandwidth Rate	プロファイルのタイプを「Rate」にした場合、最大の帯域幅を入力します。
VPN Traffic	VPN トラフィックを「ON」または「OFF」にします。 「ON」にした場合、以下の項目の「ON」「OFF」を選択します。 ・「PPTP」「L2TP」「OpenVPN」「SSL VPN」「IPSec」

「Network Profiles」以降の項目は、「Policy Type」で「Feature」を選択した場合にのみ表示されます。

3. 「Save」をクリックし、設定を適用します。

追加したポリシーは **Application Control > Policies タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Network Profiles(ネットワークプロファイル設定)

アプリケーションポリシーの設定時に使用する、ネットワークプロファイルの追加方法について説明します。

1. Security > App Control Policy > Application Control > Network Profiles タブの順にメニューをクリックし、以下の画面を表示します。

	🕐 Status	🛜 Wireless	💻 Network	Ca VPN	🔒 See	curity	🗘° Maintenance			
Security » A	Security » App Control Policy » Application Control » Network Profiles									
Policies	Network Profile	es Auto Upgrade								
This page will allow admin to create Network profiles that can be selected during Policy creation.Application Control feature should be enabled to configure Network profile settings.										
Network P	rofile List									
Show 10	✓ entries [Right c	lick on record to get mo	re options]					٩		
Profile Na	ime		🗘 VLAN		€	Network		θ		
i i			No data av	ailable in table						
Showing 0 to	0 of 0 entries						First I Previous Nex	t 🗲 Last 🕅		
Add New	Network Profile									

図 8-64 Application Control > Network Profiles タブ画面

2. 「Add New Network Profile」をクリックし、以下の画面を表示します。

Network Profile Configuration		×
Profile Name		
VLAN		
VLAN ID	1	
IP Network Type	Single	
IP Address		
		Save

図 8-65 Network Profile Configuration 画面

3. 以下の項目を設定します。

項目	説明
Profile Name	プロファイル名を入力します。
VLAN	VLAN を「ON」または「OFF」にします。
VLAN ID	VLAN を「ON」にした場合、VLAN ID を選択します。
IP Network Type	IP ネットワークのタイプを以下から選択します。
	「None」「Single」「Network」「Range」
	選択したタイプに応じて、以降に表示される項目を設定します。
IP Address	IP アドレスを入力します。
Subnet Mask	サブネットマスクを入力します。
Start IP Address	IP アドレス範囲の開始 IP アドレスを入力します。
End IP Address	IP アドレス範囲の終了 IP アドレスを入力します。

4. 「Save」をクリックし設定を適用します。

追加したプロファイルは、**Application Control > Network Profiles タブ**画面に表示されます。 右クリックし、「Edit」(編集)、「Delete」(削除)を実行できます。

Auto Upgrade(オートアップグレード設定)

パッケージのオートアップグレード設定について説明します。

1. Security > App Control Policy > Application Control > Auto Upgrade タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🎅 W	/ireless 📃 N	letwork	CA VPN	🔒 Security	O° Maintenance	
Security » App Control Policy » Application	Control » Auto Upgrad	de				0 0
Policies Network Profiles Auto U	pgrade					
This page will provide information about Pa configure Autoupgrade settings.	ackage and to allow c	onfigure Auto	Upgrade relate	d fields.Application (Control feature should be	enabled to
Auto Upgrade						
Package Version	0.0.0.16					
Auto Upgrade	ON					
Time Interval		[Range: 60 -4	43200] Minutes			
Reboot (if required)	Manual	O Auto				
	Save	Ca	ancel			

図 8-66 Application Control > Auto Upgrade タブ画面

2. 以下の項目を設定します。

項目	説明
Package Version	現在のパッケージバージョンが表示されます。
Auto Upgrade	オートアップグレードを「ON」または「OFF」にします。 「ON」にした場合、アプリケーションコントロールのパッケージは自動でアップグレードされます。
Time Interval	サーバ上に新しいパッケージが存在するか確認する間隔を設定します。 ・ 設定可能範囲:60-43200(分)

第9章 メンテナンス (Maintenance)

本章では、フ	⁷ アームウェアアップ	プデートなど、	本製品のメンテナン	/ス作業につい	、て説明します。
--------	------------------------	---------	-----------	---------	----------

設定項目	説明
「Administration(システム管理設	システム名、日時、言語、Web GUI 設定やライセンス更新などの設定を行います。
定)」	
「Management(管理設定)」	リモート管理、SNMP、診断ツールなどの設定を行います。
「Firmware & Config(ファームウェ	ファームウェアアップデート、コンフィグレーションのバックアップ/リストアなどの設定を行います。
アとコンフィグ)」	
「Logs Settings(ログ設定)」	トラフィックの追跡 / ルーティングログ、Syslog、リモートログ、イベントログなどの設定を行います。

Administration(システム管理設定)

Maintenance > Administration $\varkappa = \neg -$

System Setting (システム名の設定)

Maintenance > Administration > System Setting $\times = -$

ルータのシステム名を変更することができます。

1. Maintenance > Administration > System Setting の順にメニューをクリックし、以下の画面を表示します。

🙆 Stati	ıs 🛜 Wireless	💂 Network	പ്പം vpn	🔒 Security	🔅 Maintenance	
Maintenance » Administratio	m » System Setting					00
This page allows user to se	t the router identificatio	n name.				
System Setting						
Current System Name New Name for System		R-1000AC SR-1000AC Save	Cancel			

図 9-1 System Setting 画面

- 2. 「New Name for System」に新しいシステム名を入力します。
- 3. 「Save」をクリックし、設定を適用します。

Data and Time (システムの日時設定)

Maintenance > Administration > Date and Time $\prec = -$

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します。 また、手動で日時を入力することも可能です。手動の場合、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可能な場合、NTP サーバ通信を有効すると最も正確に日時を設定できます。

1. Maintenance > Administration > 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。

🙆 Status	🛜 Wireless	💻 Network	CB VPN	Security	O Maintenance
Maintenance » Administration » This page allows us to set the o time in a network of computers Date and Time	Date and Time date, time and NTP s . Accurate time acr	ervers. Network Time oss a network is impo	Protocol (NTP) is rtant for many reas	a protocol that is used sons.	d to synchronize computer clock
Current Device Time Time Zone Daylight Saving NTP Servers NTP Server Type Primary NTP Server Secondary NTP Server Time to re-synchronize		Ved Jan 05 04:55:54 ((GMT) Greenwich Mean ON Default © Cus Ous.pool.ntp.org 1.us.pool.ntp.org 120 [Default Save	Ime ▼ tom : 120, Range: 5 - 1440]. Cancel	Minutes	

図 9-2 Date and Time 画面

2. 以下の項目を設定しま

項目	説明
Current Device Time	ルータの現在の日時を表示します。
Time Zone	プルダウンメニューからタイムゾーンを選択します。
Daylight Saving	「ON」にしてサマータイムを有効にします。
NTP Servers	「ON」にするとインターネット上の NTP サーバを使用します。
NTP Server Type	「Default」または「Custom」を選択します。 「Custom」を選択した場合は NTP サーバのアドレスを入力します。
Primary NTP Server	NTP サーバの種類で「Custom」を選択した場合、プライマリ NTP サーバのアドレスを入力します。
Secondary NTP Server	NTP サーバの種類で「Custom」を選択した場合、セカンダリ NTP サーバのアドレスを入力します。
Time to re-synchronize	NTP サーバと同期する間隔(分)を指定します。

3. 「Save」をクリックし、設定を適用します。

Session Settings(セッションタイムアウトの設定)

Maintenance > Administration > Session Settings $\prec = \neg -$

管理者およびゲストアカウントに対してタイムアウト設定を行います。

1. Maintenance > Administration > Session 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。

iaius	😴 Wireless	🖳 Network	Ca5 VPN	😸 Security	Maintenance	
dministration »	Session Settings					0 9
he user to set	session timeout value	for administrator an	d guest users.			
gs						
r	9	99 [Default: 1	10, Range: 0 - 999] <i>N</i>	linutes		
	9	99 [Default: 1	10, Range: 0 - 999] <i>N</i>	linutes		
		Save	Cancel			
• •	dministration » :he user to set ngs or	dministration » Session Settings the user to set session timeout value ngs or 93	dministration » Session Settings the user to set session timeout value for administrator an ngs pr 999 [Default: : 999 [Default: : Save	dministration » Session Settings the user to set session timeout value for administrator and guest users. ngs pr 999 [Default: 10, Range: 0 - 999] M 999 [Default: 10, Range: 0 - 999] M Save Cancel	dministration » Session Settings the user to set session timeout value for administrator and guest users. ngs pr 999 [Default: 10, Range: 0 - 999] Minutes 998 [Default: 10, Range: 0 - 999] Minutes Save Cancel	dministration » Session Settings the user to set session timeout value for administrator and guest users. ngs pr 999 [Default: 10, Range: 0 - 999] Minutes 998 [Default: 10, Range: 0 - 999] Minutes Save Cancel

図 9-3 Session Settings 画面

2. 以下の項目を設定します。

項目	説明
Administrator	管理者ユーザのセッションタイムアウト値を入力します。
Guest	ゲストユーザのセッションタイムアウト値を入力します。

License Update(WCF ライセンスのアップデート)

Maintenance > Administration > License Update $\checkmark = = =$

Web Content Filter(Web コンテンツフィルタリング)機能を使用するには、別途購入した WCF ライセンスが必要です。 本項目ではライセンスをアクティブ化する方法について説明します。

- 1. D-Link からアクティベーションキーを取得します。
 - a. デバイスの底面にある本製品のシリアル番号を探します。
 - b. ライセンスの購入後に、D-Link からライセンスキーを取得します。
 - c. Web ブラウザを開き、https://register.dlink.com アクセスします。
 - d. アカウントがない場合、新しいアカウントを登録します。
 - e. 登録したユーザ名とパスワードでログインします。
 - f. D-Link Global Registration ポータル Web サイトで「ライセンスキーのアクティベーション」をクリックします。
 - g. 指示に従って、アクティベーションコードを受信します。
- 2. アクティベーションキーを取得後、Maintenance > Administration > License Update の順にメニューをクリックし、以下の画面を表示します。

🙆 Status	🛜 Wireless	💻 Network	🚯 VPN	盈 Security	🜻 Maintenance	
Maintenance » Administration	» License Update					00
This page shows the list of ac License Update	tivated licenses and als	o can be used for ac	tivating new WCF li	censes.		
Licenses List						
Show 10 Y entries	[No right click options]					٩
License Model		Activation Cod	le	e	Expires	⇔
		No data ava	ailable in table			
Showing 0 to 0 of 0 entries				KI Fi	rst 🔄 Previous 🗌 Next >	Last 刘
Activation Setup License Activation Code		Activate				

図 9-4 License Update 画面

- 3. 「Activation Setup」 セクションの「License Activation Code」に、アクティブ化したいライセンスに対して D-Link が供給したコードを入力します。
- 4. 「Activate」をクリックします。アクティベーションコードはリストに表示されます。
- 5. ライセンスを有効にするには、本製品を再起動します。

USB Share Ports(USB 共有ポートの設定)

Maintenance > Administration > USB Share Ports $\prec = = =$

デバイスに USB 共有機能を設定します。

1. Maintenance > Administration > USB Share Ports の順にメニューをクリックし、以下の画面を表示します。

🙆 Status	🛜 Wireless	💻 Network	C VPN	盈 Security	🗘° Maintenance	
Maintenance » Administration	» USB Share Ports					00
This page allows the user to c	onfigure the SharePo	rt feature available in	the device.			
USB Share Ports						
USB1 Share Port Setup						
Enable USB Printer		OFF				
Enable sharing	1	ON				
USB2 Share Port Setup						
Enable USB Printer	1	OFF				
Enable sharing)	OFF				
Printer Enabled Interfac	es List					
Interface Name		Enable Printer		Enable Stor	age	
default		OFF		ON		
	[Save	Cancel			

図 9-5 USB Share Ports 画面

2. 以下の項目を設定します。

項目	説明							
	USB1/2 Share Port Setup							
Enable USB Printer	「ON」にすると、当該 USB ポートに接続するプリンタをネットワークを経由して共有できるようになります。							
Enable Sharing	「ON」にすると、当該 USB ポートに接続する USB デバイスをネットワークを経由して共有できるようになります。							
	Printer Enabled Interfaces List							
Interface Name	プリンタのインタフェース名が表示されます。							
Enable Printer	インタフェースのプリンタを「ON」または「OFF」にします。							
Enable Storage	インタフェースのストレージを「ON」または「OFF」にします。							

SMS Service (SMS サービス(未サポート))

Maintenance > Administration > SMS Service メニュー SMS サービス機能を設定します。

注意 本機能は未サポートです。

本ルータでは USB インタフェースに 3G モデムを差し込みショートメールサービス(SMS)の送受信を行うことが可能です。受信したメッセージは「Inbox」に格納され、また新しいショートメッセージ(SMS)を作成、送信することが可能です。「WAN3」が WAN モード、ロードバランシングモードとして使用されている場合、または 3G USB モデムが接続されていない場合は、本項目は表示されません。

Inbox (受信箱)

受信した SMS を表示します。

1. Maintenance > Administration > SMS Service > Inbox タブの順にメニューをクリックし、以下の画面を表示します。

	🕋 Status		💻 Network	CA VPN	Security	O Maintenance			
Maintenance	aintenance » Administration » SMS Service » Inbox								
	Mobile Internet is not available								
Inbox	Create SMS								
This page all	ows the users to ch	eck received messages	in the Inbox and also	to create new m	essages.				
Inbox									
Show 10	entries [Right cl	ick on record to get mor	e options]				٩		
S.No	<u> </u>	Sender	⊖ Time	Stamp		⊖ Text	⇔		
			No data ava	ilable in table					
Showing 0 to	0 of 0 entries					H First Previous Next	Last 刘		

図 9-6 SMS Service > Inbox タブ画面

2. 以下の項目が表示されます。

項目	説明
S. No	SMS のシリアル番号を表示します。
Sender	SMS の送信者を表示します。
Time Stamp	SMS の送信時間を表示します。
Text	SMS の本文を表示します。

エントリを右クリックすると、以下のメニューを選択できます。

- 「Delete」:削除
- 「Refresh」:更新
- 「Reply」:返信
- 「Forward」:転送

Create SMS(SMS 作成)

SMS の作成と送信を行います。

注意 本機能は未サポートです。

1. Maintenance > Administration > SMS Service > Create SMS タブの順にメニューをクリックし、以下の画面を表示します。

	🕜 Status	🛜 Wireless	💻 Network	C VPN	Security	O Maintenance	
Maintenance »	Administration »	SMS Service » Create	SMS				00
		102	Mobile Interi	net is not avai	ilable		
Inbox C	reate SMS						
This page will	allow users to cre	ate a new SMS and ser	nd it to a particular i	umber.			
Receiver				_			
Text Mess	age				~		
					~		
			Send Message	Cancel			

図 9-7 SMS Service > Create SMS タブ画面

2. 以下の項目で設定を行います。 項目 説明 Receiver 受信者の電話番号を指定します。 メッセージ本文を作成します。 Text Message Send Message クリックしてメッセージを送信します。 メッセージの送信をキャンセルします。 Cancel

Package Manager (パッケージマネージャ)

Maintenance > Administration > Package Manager $\prec = \neg -$

「Package(パッケージ)」はルータによって D-Link リポジトリからインストールされるファイルの集合体です。本機能では、サポートされる USB デバイス用のドライバや、ルータ管理画面の多言語サポートを有効にする言語パックなどをダウンロードします。

パッケージマネージャによる多言語サポートでは、ルータのユーザインタフェースで使用されている全テキストを選択した言語で表示させます。ド ライバと言語の言語パックはそれぞれ1種類ずつルータ上に保存することができます。ドライバおよび言語パックは、ルータの再起動後に使用可能 となります。

以下2種類のインストール方法があります。

1. 手動インストール(Manual Installation): 手動インストールを行う場合は、まずパッケージをダウンロードする必要があります。ダウンロード したパッケージは GUI で表示され、選択することができるようになります。

注意 D-Link からの提供されるドライバのみ選択できます。検証プロセスはインストール中に行われます。

- 2. 自動インストール(Auto Installation):表示されるリンク "click here"をクリックすることで自動インストール対応のパッケージリストが表示 されます。有効なドライバ/言語パックのリストが表示されている画面からオプションを指定し、インストールを行います。このタイプのイン ストールでは、リポジトリサーバからパッケージをダウンロードするため、ルータは常にインターネットに接続されている必要があります。
- 1. Maintenance > Administration > Package Manager の順にメニューをクリックし、以下の画面を表示します。

	🕐 Status	🛜 Wireless	📃 Network	CD VPN	Security	Maintenance	
Maintenance	» Administration »	Package Manager					00
This page sho	ows the list of availa	able drivers. User can	install or uninstall t	he drivers.			
Device Dri	vers						
List of De	fault Drivers						
Show 10	✓ entries						٩
Driver	Descript	ion				⊖ Installed	⇔
cdc-acm	D-Link (DW	M-156 A5, DWM-156 A6, D	WM-157 A1)			• 0.9	
GobiNet	D-Link (DW	M-221 & 222)				• 0.9	
option	D-Link (DW	M-152 A1, DWM-152 A2, D	WM-152 A3, DWM-156 A1	1, DWM		0.9	
Showing 1	to 3 of 3 entries				[] Fir	st Previous 1 Next	Last 刘
Driver for yo	ur device not listed? <u>cli</u>	ick here to see if updates	or new drivers are availa	able			
Manual Ir	astall						
Select D	river	Γ		照			
			Install				
Install Hi	story						
Install H	listory				~		
					~		

図 9-8 Package Manager 画面

2. 以下の項目を設定します。

項目	説明
List of Default Drivers	インストールされている初期ドライバを表示します。
Click Here	クリックしてダウンロード可能なパッケージー覧を表示します。インターネットに接続している必要があります。パッケー
	ジー覧からアップデート/インストールするドライバを選択します。
Manual Install	パッケージをダウンロード済みの場合、以下の手順でインストール行います。
	(1)「Browse/ 参照」をクリックしパッケージを選択
	(2)「Opem/ 開く」をクリックします。
	(3)「Install」をクリックします。
Install History	インストール履歴を表示します。

日本語言語パック(Japanese Language Installation Pack)の設定

日本語言語パック(Japanese Language Installation Pack)のダウンロード、インストールについて説明します。

1. Maintenance > Administration > Package Manager の順にメニューをクリックし、以下の画面の「click here」をクリックします。

<i>a</i>) Status 🛜 Wireless	💻 Network	PN 🕞	盈 Security	🜻 Maintenance	
Maintenance » Admi	nistration » Package Manager					0 0
This page shows the	list of available drivers. User c	an install or uninstall t	he drivers.			
Device Drivers						
List of Default	Drivers					0
Driver G	Description				⊖ Installed	÷
cdc-acm	D-Link (DWM-156 A5, DWM-156 A6,	DW/M-157 A1)			🔴 0.9	
option	D-Link (DWM-152 A1, DWM-152 A2,	DWAA-152 A3, DWAA-156 A1,	DW:M		🔵 0.9	
Showing 1 to 2 of 2	2 entries			∬ First	I Next >	Last 刘
Driver for your devic Manual Install	e not listed ^e <u>click here</u> to see if upda	tes or new drivers are ava	ilable			
🗵 9-9 🛛 Packag	ge Manager 画面(ダウン	/ロード)				
	項目				説明	
Driver for your o	device not listed?	Ļ	ストに希望の)ドライバーがな(い場合、「click here	」をクリ
click here to see	e if updates or new drivers	s are available 有	前効なドライバ	、 のアップデート [;]	をご確認ください。	

2. インストール可能なドライバの一覧が表示されます。

「List of Device Drivers」から「Japanese Language Installation Pack」を選択 → 右クリックし「🕢 Install 」を選択します。

Device Drivers		
List of Device D	rivers	
Show 10 🔻 er	itries	٩
Driver 合	Description	⊖ Installed ⊖
cdc-acm	D-Link (DWM-156 A5, DWM-156 A6, DWM-157 A1)	1.0
DE	German Language Installation Pack Version 1.0	1.0
ES	Spanish Language Installation Pack Version 1.0	• 1.0
FR	French Language Installation Pack Version 1.0	• 1.0
	Italian Language Installation Pack Version 1.0	• 1.0
JP	Japanese Language Installation Pack Version 1.0	• 1.0
option	D-Link (DWM-152 A1, DWM-152 A2, DWM-152 A3, DWM-156 A1, DWM	• 1.0
RU	Russian Language Installation Pack Version 1.0	• 1.0
тс	Chinese (Traditional) Language Installation Pack Version 1.0	• 1.0
Showing 1 to 9 of 9	entries	H First Previous 1 Next Last

図 9-10 Japanese Language Installation Pack 画面

3. 上部に「Operation Succeeded」と表示され、「Japanese Language Installation Pack」の「Installed」の項目が緑になっていると、言語パックが 正しくインストールされたことを意味します。

2	Status 🛜 Wireless	💻 Network	🚯 VPN	읊 Security	😳° Maintenance	
ntenance » Admin	istration » Package Manager					00
	691	Operatio	on Succeeded			
page shows the	list of available drivers. User ca	n install or uninstall t	he drivers.			
vice Drivers						
ist of Device Dr	ivers					
Show 10 • en	tries					٩
Driver 🔂	Description				⊖ Installed	⇔
cdc-acm	D-Link (DWM-156 A5, DWM-156 A6, D	WM-157 A1)			🔴 1.0	
DE	German Language Installation Pack	/ersion 1.0			🔴 1.0	
ES	Spanish Language Installation Pack \	/ersion 1.0			🔴 1.0	
FR	French Language Installation Pack V	ersion 1.0			🔴 1.0	
IT	Italian Language Installation Pack Ve	ersion 1.0			🔴 1.0	
JP	Japanese Language Installation Pack	Version 1.0			🔵 1.0	
option	D-Link (DWM-152 A1, DWM-152 A2, D	WM-152 A3, DWM-156 A1,	DWM		1.0	
RU	Russian Language Installation Pack Version 1.0				🔶 1.0	
тс	Chinese (Traditional) Language Insta	llation Pack Version 1.0			🔴 1.0	
Showing 1 to 9 of 9	entries			Firs	t 👌 Previous 1 Next 🗲	Last 刘

図 9-11 Japanese Language Installation Pack 画面(インストール済み)

次に、Maintenance > Administration > Set Language の順にメニューをクリックし、「Set Language」(言語設定)を表示します。
 「Set Language」のドロップダウンメニューで「Japanese」を選択→「Save」をクリックし、設定を適用します。

	🝘 Status	🛜 Wireless	💻 Network	ഹ് VPN	盈 Security	😍 Maintenance				
Maintenance >	Maintenance » Administration » Set Language									
		; in package								
This page sho Language S	ws the list of avail ettings	lable languages.								
Set Lang	nage	E	nglish nglish apanese	· · · · ·						

図 9-12 Set Language 画面(選択)

5. 上部に「操作に成功しました」と表示されます。

	🙆 ステータス	🛜 ७२७७८	💂 ネットワーク	ക vpn	🔒 セキュリティ	ᅌ メンテナンス
×	ンテナンス » 管理 » 言語	を設定				00
		(9	操作に成功	しました		
TI	nis page shows the list of	available languages.				
	語設定					
ſ	言語を設定		Japanese	Y		
l			保存 キャン	・セル		
 义	9-13 Set Languag	ge 画面(日本語)				

Set Language(言語設定)

Maintenance > Administration > Set Language $\prec = = =$

「Package Manager」で取得した言語パックの設定を行います。

1. Maintenance > Administration > Set Language の順にメニューをクリックし、以下の画面を表示します。

3 Status	🛜 Wireless	💻 Network	S VPN	🔒 Security	Maintenance	
Maintenance » Administration »	 Set Language 					0
	Plea	ase install driver n	rs for language nanager	s in package		
This page shows the list of avai	ilable languages.					
Language Settings						
Set Language	E	inglish	\checkmark			
		Save	Cancel			

図 9-14 Set Language 画面

2. 以下の項目を設定します。

項目	説明
Set Language	ドロップダウンメニューから言語を選択します。

注意 Web GUI の日本語化を行う場合は、「日本語言語パック(Japanese Language Installation Pack)の設定」を参照してください。

Web GUI Management (Web GUI 管理)

Maintenance > Administration > Web GUI Management メニュー Web GUI へのアクセスを許可する IP アドレスまたは VLAN を指定します。

1. Maintenance > Administration > Web GUI 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。

	🕋 Status		💻 Network	CA VPN	🔒 Security	OP Maintenance		
Maintenance >	Administration *	Web GUI Management					00	
This page allo Web GUI M	ows the user to man	age Device GUI acces	s/deny permissions to	VLAN host/ VLAN	Network.			
Enable List of Al	lowed IP Address	/ Vlan Network	Save	Cancel				
Show 10	✓ entries [Right	click on record to get r	nore options]				٩	
Name	Act	cess Type	↔ IP A No data ava	Address / Vlan I ilable in table	Network		θ	
Showing 0 t	Showing 0 to 0 of 0 entries Next > Last >							
Add Ne	w Configuration	l						

図 9-15 Web GUI Management 画面

- 2. 「Enable」を「ON」にし、「Save」をクリックします。
- 3. 「Add New Configuration」をクリックし、新しい設定を追加します。

Web GUI Management Configuration		
Name Access Type Single IP Address	Single IP Address	
	Save	

図 9-16 Web GUI Management Configuration 画面

4. 以下の項目を設定します。

項目	説明
Name	設定名を指定します。
Access Type	アクセスタイプを「Single IP Address」または「VLAN Network」から選択します。
Single IP Address	Web GUI へのアクセスを許可するコンピュータ / デバイスの IP アドレスを指定します。
VLAN Network	Web GUI へのアクセスを許可するコンピュータ / デバイスの VLAN ID を指定します。

5. 「Save」をクリックし、設定を適用します。

エントリの編集

編集するエントリを右クリックし、「Edit」を選択します。 設定変更後、「Save」をクリックします。

エントリの削除

削除するエントリを右クリックし、「Delete」を選択します。 すべてのエントリを削除する場合は、右クリックして「Select All」をチェックし、「Delete」を選択します。

Management(管理設定)

Maintenance > Management $\prec = \neg -$

Remote Management (リモート管理)

Maintenance > Management > Remote Management $\prec = \neg -$

HTTPS または Telnet を使用した本製品のリモート管理を有効にできます。IP アドレスのサブネットに対し、HTTPS と Telnet 両方の接続を制限する ことができます。ルータの管理者は、お使いの PC、IP アドレス /IP アドレス範囲で HTTPS 経由での GUI ヘアクセスを制限できます。リモート IP ア ドレス範囲の許可設定と同時に、SSL トラフィックのオープンポートを初期値である 443 から変更することも可能です。

1. Maintenance > Management > 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。

	🕜 Status	🛜 Wireless	💻 Network	රබු VPN	Security	Maintenance	
Maintenance	» Management » R	emote Management					0 0
rom this pag	e a user can config	ure the remote mana	gement feature. Th	is feature can be us	ed to manage the bo	x remotely from WAN side.	
Remote Ma	anagement						
Remote M	anagement Setur						
Enable R	emote Management	t [ON THE				
HTTPS P	ort No	4	43 [Range	: 1 - 65535]			
SSH			ON THE				
SNMP			ON TITLE				
Access Co	ontrol Setup						
Access	Туре	(All IP Addresses	O IP Address Rai	nge O Only Selec	ted PC	
WAN Ping							
Respond	to Ping						
Device LA	N IP Access via W	AN					
LAN IP A	ccess		ON THE				
		I	Save	Cancel			

図 9-17 Remote Management 画面

2. 以下の項目を設定します。

項目	説明
Enable Remote	「ON」にしてリモート管理を有効にします。
Management	
HTTPS Port No	HTTPS 接続のポート番号を指定します。
	 初期値:443
SSH	「ON」にして SSH(Secure Shell)プロトコルを有効にします。SSH は、リモートホストからのネットワークを介した CLI ア
	クセスで使用されます。
SNMP	「ON」にして SNMP でのリモート管理を有効にします。
Access Type	アクセスのタイプを以下から選択します。
	「All IP Addresses」(全 IP アドレス)、「IP Address Range」(IP アドレス範囲)、「Only Selected PC」(選択したデバイス)
	・「IP Address Range」(IP アドレス範囲)選択時は「From IP Address」と「To IP Address」で IP アドレス範囲を指定します。
	・「Only Selected PC」(選択したデバイス)選択時はデバイスの IP アドレスを指定します。
Respond to Ping	「ON」にして WAN からの Ping リクエストへの応答を許可します。
LAN IP Access	「ON」にして WAN 側からの LAN IP アクセスを有効にします。

SNMP (SNMP の使用)

Maintenance > Management > SNMP $\times = = =$

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追加の管理ツールです。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、Read-Only または Read-Write 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。トラップリストでは、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) について概要が表示されます。

注意 本製品の SNMP 機能は読み取り専用となります。そのため、ユーザに割り当てる本製品へのアクセス権は「読み取り」のみです。

SNMP(SNMPv3 ユーザリストの設定)

SNMP v3 ユーザリストを設定します。

1. Maintenance > Management > SNMP > SNMP タブの順にメニューをクリックし、以下の画面を表示します。

	🙆 Status	🛜 Wireless	💻 Network	CB VPN	Security	Maintenance	
Maintenance	» Management »	SNMP					0
SNMP	SNMP Trap List	Access Control List	SNMP System Info				
Simple Netv monitor and SNMP v3 1	vork Management control network Jser List	Protocol (SNMP) lets y devices, and to manag	ou monitor and manage e configurations, stati	your router fror stics collection, p	n an SNMP manager. Si berformance, and secu	NMP provides a remote means rrity.	to
Name		Privilege		Security	r Level		
admin		RWUSER		No-Auth N	o-Priv		
guest		ROUSER		No-Auth N	o-Priv		

図 9-18 SNMP > SNMP タブ画面

2. 「admin」または「guest」を右クリック→「Edit」を選択し、以下の画面を表示します。

SNMP User	×
Username Access Privilege Security Level	guest ROUSER No-Auth No-Priv
図 9-19 SNMP User 画面(quest)	

3. 以下の項目を設定します。

項目	説明
Username	SNMPv3 マネージャのユーザ名を表示します。
Access Privilege	アクセス権限が表示されます。
Security Level	このユーザの認証とプライバシー設定を定義します。 - 「No-Auth No-Priv」:認証にユーザ名の一致のみを必要とします。 - 「Auth No-Priv」: MD5 または SHA アルゴリズムに基づいた認証を提供します。 - 「AuthPriv」: DES-256 ビットを使用した暗号プライバシーと、MD5 または SHA アルゴリズムに基づいた認証を提供し ます。

SNMP Trap List(SNMP トラップリスト)

ルータがトラップメッセージを送信する SNMP エージェントの IP アドレスを設定および表示します。

1. Maintenance > Management > SNMP > SNMP Trap List タブの順にメニューをクリックし、以下の画面を表示します

🗥 Status	🛜 Wireless	💻 Network	C C VPN		Security	O ^o Maintenance	
Maintenance » Management	» SNMP » SNMP Trap Li	st					00
SNMP SNMP Trap Lis	Access Control List	SNMP System II	nfo				
The table lists all IP addres	ses of SNMP agents to v	vhich the router w	ill send trap message	es.			
Show 10 💌 entries	[Right click on record t	o get more options]					٩
IP Address	🔂 Port	⊖ Commu	inity	€	SNMP Version		⇔
		No da	ta available in table				
Showing 0 to 0 of 0 entries					First	Previous Next >	Last 刘
Add SNMP Trap							

図 9-20 SNMP > SNMP Trap List タブ画面

2. トラップを追加する場合は、「Add SNMP Trap」をクリックし画面を表示します。

SNMP Trap Configuration	8
IP Address Port	[Range: 0 - 65535]
Community	
Autoentication Type	
	Save

図 9-21 SNMP Trap Configuration 画面

3. 以下の項目を設定します。

項目		
IP Address	SNMP トラップエージェントの IP アドレスを入力します。	
Port	トラップメッセージが送信される宛先 SNMP トラップポートを指定します。	
Community	エージェントが所属するコミュニティストリングを指定します。多くのエージェントは、Public コミュニティでト	
	ラップにリッスンするように設定されます。	
Authentication Type	トラップエージェントが使用する SNMP バージョン (v1、v2c、または v3)を選択します。	

4. 「Save」をクリックし、設定を適用します。

エントリの編集

編集するエントリを右クリックし、「Edit」を選択します。 設定変更後、「Save」をクリックします。

エントリの削除

削除するエントリを右クリックし、「Delete」を選択します。 すべてのエントリを削除する場合は、右クリックして「Select All」をチェックし、「Delete」を選択します。

Access Control List (SNMP アクセスコントロールリストの設定)

SNMP アクセスコントロールリストを設定します。

1. Maintenance > Management > SNMP > Access Control List タブの順にメニューをクリックし、以下の画面を表示します

	🙆 Status	🛜 Wireless	💻 Network	A VPN	Security	O° Maintena	nce
Maintenanc	e » Management »	SNMP » Access Contro	l <mark>List</mark>				00
SNMP	SNMP Trap List	Access Control List	SNMP System Int	io			
The table	lists all IP addresse	s of SNMP agents to w	hich the router wil	l allows several oper	rations on the SNMP ag	gents.	
Access (Control List						
Show 10	▼ entries	[Right click on record to	get more options]				٩
Name	🗘 Sub	net Mask	⊖C	ommunity	⊖ Acc	ess Type	θ
			No data	available in table			
Showing 0) to 0 of 0 entries					First Previous M	lext > Last >
Add A	ccess Control						

図 9-22 ASNMP > Access Control List タブ画面

- 2. エントリを右クリックして「Edit」「Delete」を行います。
- 3. 新しくアクセスコントロールを作成するには、「Add Access Control」をクリックします。

IP Address	Access Control List		\mathbf{x}
Save	IP Address Subnet Mask Community Access Type	rocommunity	
			Save

4. 以下の項目を設定します。

項目	説明
IP Address	SNMP トラップエージェントの IP アドレスを入力します。
Subnet Mask	許可される SNMP マネージャリストを決定するために使用されるネットワークマスクを入力します。
Community	エージェントが所属するコミュニティストリングを入力します。多くのエージェントは、Public コミュニティでト
	ラップにリッスンするように設定されます。
Access Type	アクセスの種類として、読取専用 (rocommunity) または読み書き (rwcommunity) を選択します。

5. 「Save」をクリックし、設定を適用します。

エントリの編集

編集するエントリを右クリックし、「Edit」を選択します。 設定変更後、「Save」をクリックします。

エントリの削除

削除するエントリを右クリックし、「Delete」を選択します。

すべてのエントリを削除する場合は、右クリックして「Select All」をチェックし、「Delete」を選択します。

SNMP System Info(SNMP システム情報の設定)

ルータの SNMP システム情報を設定します。

1. Maintenance > Management > SNMP > SNMP System Info タブの順にメニューをクリックし、以下の画面を表示します

		🝘 Status	🛜 Wireless	💻 Network	ക vpn	🔒 Security	🐡 Maintenance	
Ma	intenance »	Management »	SNMP » SNMP System I	nfo				00
_	SNMP	NMP Trap List	Access Control List	SNMP System Info				
Th ^r mo	is page disp dified here	lays the current	SNMP configuration o	of the router. The foll	owing MIB (Mana;	gement Information B	ase) fields are displayed :	and can be
SN	MP Syste	m Info						
	SysConta	ct						
	SysLocat	ion						
	SysName		C	SR-1000AC				
			I	Save	Cancel			

図 9-24 SNMP > SNMP System Info タブ画面

2. 以下の項目を設定します。

項目	説明
SysContact	本ルータの連絡窓口の名前を入力します。例 : admin、 John Doe
SysLocation	ルータの物理的な位置を入力します。 例 : Rack#2,4th Floor
SysName	ルータの簡単な識別名を入力します。

Diagnostics (診断ツール)

Maintenance > Management > Diagnostics $\prec = \neg -$

ルータの診断機能を実行します。

Network Tools (ネットワークツール)

Network Tools タブでは、ネットワークやインターネット上で本製品と他のデバイス間の接続性をテストすることができます。

■ Ping の送信

1. Maintenance > Management > Diagnostics > Network Tools タブの順にメニューをクリックし、以下の画面を表示します。

🕜 Status		💻 Network	Ca VPN	Security	O Maintenance				
Maintenance » Management » Diagnostics » Network Tools									
Network Tools Capture Pac	kets System Chec	ĸ							
This page can be used for diagnosti	cs purpose. This page	e provides user with	some diagnostic	tools like ping, dns lo	ookup and traceroute.				
Network Tools									
Command Output for Ping an IP Address / Domain Name	d Traceroute	w.dlink.com							
Command Output		Ping Tra	aceroute		^				
					~				

図 9-25 Diagnostics > Network Tools タブ画面

- 2. 「Command Output for Ping and Traceroute」セクションの「IP Address / Domain Name」に、IP アドレスまたはドメイン名を入力します。
- 3. 「Ping」をクリックすると、「Command Output」に結果が表示されます。

🙆 Status	🛜 Wireless	💻 Network	ക vpn	盈 Security	😳 Maintenance	
Maintenance » Management » I	Diagnostics » Network	ែ០៤				00
	•	Operatio	on Succeeded			
Network Tools Capture	Packets System Che	ck				
This page can be used for diag Network Tools	nostics purpose. This	page provides user w	ith some diagnost	ic tools like ping, dn	s lookup and traceroute.	
Command Output for Ping	g and Traceroute					
IP Address / Domain Name		ww.dlink.com				
		Ping Tr	aceroute			
Command Output	P 6 6 6 - 5 5 r	ING www.dlink.com 4 bytes from 12.1 4 bytes from 12.1 4 bytes from 12.1 4 bytes from 12.1 4 bytes from 12.1 www.dlink.com packets transmit ound-trip min/awg	(12.130.207.1 30.207.110: se 30.207.110: se 30.207.110: se 30.207.110: se 30.207.110: se ping statistic ted, 5 packets /max = 108.515	10): 56 data byte q=0 ttl=46 time=1 q=2 ttl=46 time=1 q=2 ttl=46 time=1 q=3 ttl=46 time=1 s received, 0% pac /109.231/110.223	s 09.040 ms 005.515 ms 09.151 ms 09.228 ms 10.223 ms ket loss ms	

図 9-26 Diagnostics > Network Tools タブ画面
■ Traceroute の使用

本ルータは、ネットワークのパスをパブリックホストにマップさせる Traceroute 機能を提供します。 本ルータと宛先の間に位置する最大 30 個までのルータ(または「ホップ」)が表示されます。

1. Maintenance > Management > Diagnostics > Network Tools タブの順にメニューをクリックし、以下の画面を表示します

🙆 Status 🤻	Wireless	💻 Network	CAS VPN	Security	Maintenance	
Maintenance » Management » Diagno	stics » Network Too	ls				00
Network Tools Capture Packe	ets System Check					
This page can be used for diagnostics	purpose. This page	provides user with	h some diagnostic 1	tools like ping, dns l	ookup and traceroute.	
Network Tools						
Command Output for Ping and	Traceroute					
IP Address / Domain Name	www	v.dlink.com				
		Ping Ti	raceroute			
Command Output					~	
					~	

図 9-27 Diagnostics > Network Tools タブ画面

- 2. 「Command Output for Ping and Traceroute」にある「IP Address/Domain Name」に IP アドレスまたはドメイン名を入力します。
- 3. 「Traceroute」をクリックすると、「Command Output」に結果が表示されます。

🙆 Status	🛜 Wireless	💻 Network	ക VPN	🚨 Security	🐡 Maintenance	
Maintenance » Management » Dia	gnostics » Network T	ools				00
		Operatio	on Succeeded			
Network Tools Capture Pa	ckets System Che	ck				
This page can be used for diagno: Network Tools	stics purpose. This p	nage provides user w	ith some diagnost	ic tools like ping, dr	ns lookup and traceroute.	
Command Output for Ping a	nd Traceroute					
IP Address / Domain Name	W	ww.dlink.com				
		Ping Tr	aceroute			
Command Output		Taceroute to www. te packets + + + + + + +	dlink.com (12.:	130.207.110), 10	hops max, 40	

図 9-28 Diagnostics > Network Tools タブ画面

■ DNS 検索の実行

本製品は、インターネット上の Web、FTP、メール、またはその他のサーバの IP アドレスも検索できる DNS 索引機能を提供します。

1. Maintenance > Management > Diagnostics > Network Tools タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🎅 Wireless	s 📃 Network	A VPN	Security	Maintenance	
Maintenance » Management » Diagnostics » Netwo	ork Tools				00
Network Tools Capture Packets System	Check				
This page can be used for diagnostics purpose. This	s page provides user w	ith some diagnosti	c tools like ping, dns l	ookup and traceroute.	
Command Output for Ping and Traceroute	www.dlink.com				
	www.uninc.com				
	Ping	Traceroute			
Command Output				~	
				~	
Dura la la					
Domain Name					
	Соокар				
Command Output				~	
				\sim	
(A)					

図 9-29 Diagnostics > Network Tools タブ画面

2. 「DNS Lookup」セクションの「Domain Name」に、インターネット名を入力します。

3. 「Lookup」をクリックすると、「Command Output」に結果が表示されます。ホストまたはドメインエントリが存在する場合、IP アドレスと共 に応答を表示します。「Host Unknown」メッセージ表示された場合、そのインターネット名は存在しません。

Markan Status Status	s 📃 Network	A VPN	Security	🜮 Maintenance	
Maintenance » Management » Diagnostics » Netw	rork Tools				00
•	Operati	on Succeeded			
Network Tools Capture Packets System	Check				
This page can be used for diagnostics purpose. T	This page provides user w	rith some diagnosti	ic tools like ping, dn	s lookup and traceroute.	
Network Tools					
Command Output for Ping and Traceroute	2				
IP Address / Domain Name	www.dlink.com				
	Ping	aceroute			
Command Output					
	4			• 1	
Domain Name					
	Lookup				
Command Output	Server:	1.0			
	Address 1:	adm.djp.loo	ral		

図 9-30 Diagnostics > Network Tools タブ画面

Capture Packets (パケットのキャプチャ)

本ルータではLAN インタフェースを通過するすべてのパケットをキャプチャすることができます。パケットのトレースはキャプチャセッションあたり 1MB のデータに制限されます。キャプチャファイルサイズが1MB を超えると、自動的に削除されて新しいキャプチャファイルが作成されます。

1. Maintenance > Management > Diagnostics > Capture Packets タブの順にメニューをクリックし、以下の画面を表示します

	🝘 Status	🛜 Wireless	💻 Networl	k 🕼 VP	N 🤮 Seci	urity 🔅 🔅 Ma	aintenance			
Maintenance >	Management » [Diagnostics » Capture P	ackets				0 9			
Network	Tools Capture	Packets System Ch	eck							
This page pro	This page provides user packet sniffer as a diagnostic tool.									
Capture Pa	ckets									
Interfac	U.	L	AN	•						
			Start Trace	Stop Trace	Download					

図 9-31 Diagnostics > Capture Packets タブ画面

2. 「Interface」のプルダウンメニューからインタフェースを選択します。

3. 「Start Trace」をクリックすると、パケットのキャプチャが開始されます。

🙆 Status	🛜 Wireless	💻 Network	ക vpn	🔒 Security	Maintenance					
Maintenance » Management »	Diagnostics » Capture Pa	ckets				00				
	Packet Capturing started. Click the Stop button to stop packet tracing									
Network Tools Capture	Network Tools Capture Packets System Check									
This page provides user packet	t sniffer as a diagnostic	tool.								
Capture Packets										
Interface	LA	.N	•							
		Start Trace St	op Trace	Download						

図 9-32 Diagnostics > Capture Packets タブ画面

4. パケットのキャプチャを停止するには「Stop Trace」をクリックします。

	🝘 Status	🛜 Wireless	💻 Network	A VPN	🔒 Security	Maintenance	
Maintenance	» Management » [Diagnostics » Capture Pa	ackets				0
Network	Tools Capture I	Packets System Che	ck				
This page pro	vides user packet	sniffer as a diagnostic	tool.				
Capture Pa	ckets						
Interfac	э	L	AN	×			
			Start Trace S	top Trace	Download		

図 9-33 Diagnostics > Capture Packets タブ画面

5. 「Download」をクリックすると、トレース結果がブラウザのデフォルトのダウンロードフォルダに保存されます。

System Check (システムチェック)

- ルータの診断機能の一部として、IPv4/IPv6の両方についてスタティック/ダイナミックルートを表示することができます。
- 1. Maintenance > Management > Diagnostics > System Check タブの順にメニューをクリックし、以下の画面を表示します

	🝘 Status	🛜 Wireless	💻 Network	ക vpn	🔒 Security	🐡 Maintenance			
Maintenance	» Management » [Diagnostics » System C	neck				00		
Network	. Tools Capture A	Packets System Ch	eck						
This page display the router's static and dynamic routes.									
System Ch	eck								
Comman	d Output		Display IPv4 Table	Display IP	v6 Table				

図 9-34 Diagnostics > System Check タブ画面

注意

IPv4 & IPv6 モードに設定されている場合、「Display IPv6 Table」が表示されます。

2. 「Display IPv4 Table」または「Display IPv6 Table」をクリックすると、「Command Output」に結果が表示されます。

	🕜 Status	🛜 Wireless	💻 Network	CA VPN	🔒 Securi	ty 🔅 Mai	ntenance
Maintenance »	Management » D	iagnostics » System Ch	eck				0 0
		69	Operati	on Succeeded			
Network	Fools Capture I	ackets System Che	ck				
This page disp	ay the router's st	atic and dynamic route	95.				
System Che	ck						
			Display IPv4 Table	Display IP	v6 Table		
Command	Output	D	estination Gat ef Use Iface	ceway Ge	Kernel IP nmask	? routing table Flags Metric	^
		201	.0.0.0 0.0 0 bdg10	0.0.0 25	5.0.0.0	U 0	
		0	0 bdg1 72.17.100.0 0.0 0 eth0	0.0.0 25	5.255.255.0	а 0	

図 9-35 Diagnostics > System Check タブ画面 (IPv4)

	🕜 Status	🛜 Wireless	💻 Netwo	ork	ഹം∨	PN	Security	O° Maintenan	ice
tenance >	» Management » D	Diagnostics » System	Check						?
		•	Оре	ration	Succe	eded			
Network	Tools Capture I	Packets System Cl	heck						
page dis	play the router's st	atic and dynamic rou	utes.						
tem Ch	eck								
			Display IPv4	Tablo	Die	olay IDv6	Table		
6	1.0		Display in V4		Dis				
Comman	α σατρατ		Destination				Next	icing table	~
			Hop			F	lags Metric Ref	Use Iface	
			::1/120	U	0	150	1 10		
			fe80::/128			101	11		
			fe80/128	U	0	0	1 10		
			100011/100	TT	0	0	1 10		
				0		0			
			fe80::/128		0	0	1.1.		
			fe80::/128	U	0	0	1 10		

図 9-36 Diagnostics > System Check タブ画面 (IPv6)

3. Network > Routing > Static Routes > Static Route Configuration 画面でルートが private に設定されている場合、「Display IPv4 Table」をクリッ クすると"Private ルートテーブル"が表示されます。

🙆 Status 🎅 Wireless	💂 Network 🖓 VP	N 🔒 Security	Maintenance	
Maintenance » Management » Diagnostics » Sys	tem Check			0 0
•	Operation Succee	ded		
Network Tools Capture Packets System C	Check			
This page display the router's static and dynamic ro	utes.			
System Check				
	Display IPv4 Table			
Command Output	Destination Gateway Ref Use Iface	Kernel IP ro Genmask Fl	uting table ags Metric	
	2.0.0.0 192.168.10.1 0 0 bdg1 192.168.10.0 0.0.0.0 0 0 bdg1	255.0.0.0 UG 255.255.255.0 U	0	
	Private routes table <destination netmask=""> via <ga <metric></metric></ga </destination>	teway> dev <interface< td=""><td>> metric</td><td></td></interface<>	> metric	
		. bdað samala m	.d	

図 9-37 Diagnostics > System Check タブ画面 (IPv4 - Private)

Power Saving(省エネ設定)

Maintenance > Management > Power Saving $\checkmark = \neg -$

本製品は、実際のハードウェアの状況に基づいて電力を調整することができます。 リンクステータスまたはケーブルの長さに応じて、消費電力を調整します。

1. Maintenance > Management > Power Saving の順にメニューをクリックし、以下の画面を表示します。

	🝘 Status	🛜 Wireless	💻 Network	ക vpn	盈 Security	🜻 Maintenance	
Maintenance >	» Management » P	Power Saving					00
This page allo	ows user to enable	/disable power saving	in the router.				
Power Sav	ing						
By Link S	Status						
By Cable	Length Detection						
			Save	Cancel			

図 9-38 Power Saving 画面

2. 有効にする機能を「ON」に指定します。

項目	説明
By Link Status	本オプションを有効にすると、消費電力は接続ポート数に依存するようになります。すべての有効な LAN ポートがアクティ ブなイーサネット接続を行っている状態よりも、単一ポートのみ接続状態にある方が、電力消費を抑えられます。
By Cable Length Detection	本オプションを有効にすると、短いケーブルに接続した LAN ポートの消費電力を抑えることができます。

DDP Client(DDP クライアント設定)

Maintenance > Management > DDP Client メニュー DDP クライアントを有効または無効に設定します。

1. Maintenance > Management > DDP 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。

	🗥 Status		💻 Network	A VPN	Security	ᅇ Maintenance	
Maintenance	» Management » D	DP Client					0 0
This page allo	ows user to enable/	disable DDP client in	the router.				
DDP Client							
DDP Clie	nt						
			Save	Cancel			
-							

図 9-39 DDP Client 画面

- 2. DDP クライアントを「ON」または「OFF」に設定します。
- 3. 「Save」をクリックし、設定を適用します。

Firmware & Config (ファームウェアとコンフィグ)

Maintenance > Firmware & Config X = 2 -

ファームウェアのアップグレード方法と、コンフィグレーションのバックアップ/リストア方法について説明します。

Firmware Upgrade(ファームウェアアップグレード)

Maintenance > Firmware & Config > Firmware Upgrade $\neq = = =$

本画面では新しいファームウェアにアップグレードすることができます。「Firmware Upgrade」セクションでファイルを選択し、「Upgrade」をクリッ クしてアップグレードを実施します。新しいファームウェアファイルが検証された後、新しいイメージがフラッシュに書き込まれ、ルータは新しい ファームウェアで自動的に再起動します。

■ ユニバーサルファームウェアの命名規則

新しいファームウェアの命名規則は「DSR_<Modelname>_<Hardware>x_FW <Version number>_<WW>」となります。各ハードウェア(A、B、C など)のすべてのバージョン(1、2、3など)に使用されるファームウェアファイルは1種類のみです。例えば、新しいファームウェアファイル 名が「DSR_500_Ax_FW3.12_WW」である場合、このファームウェアは A2/A3/A4 などのハードウェアバージョンにおけるアップグレードで使用す ることができます。

注意 ファームウェアのアップグレード中は、オンライン接続・DSR の電源切断・PC のシャットダウンなど、処理を中断するアクションは行わ ないでください。アップグレードは再起動まで含めて数分程度で完了します。フラッシュ書き込み中にアップグレード処理が中断される と、フラッシュメモリが破損し、Web GUI を経由せずにフラッシュファームウェアをリストアしなければ使用することができなくなりま す。

Check Update(アップデートチェック)

新しいバージョンの利用可能なファームウェアがあるかチェックを行います。

注意 日本で使用する場合は、ディーリンクジャパンのサイト(https://www.dlink-jp.com/)からダウンロードしたファームウェアのみをご利用くだ さい。

1. Maintenance > Firmware & Config > Firmware Upgrade > Check Update タブの順にメニューをクリックし、以下の画面を表示します。

		🛜 Wireless	💻 Network	CB VPN	Security	Maintenance	
Maintenance » Firmw	vare & Config »	Firmware Upgrade ᠉	Check Update				00
Using System (F	PC) Using USB	Check Update					
This page is used for	checking the av	vailability of newer fi	rmware. Once yo	u press the checkno	w button, the device	e will tell you if you are r	equired to
Check Update							
Check Now		Ch	eck Now				
Status							

図 9-40 Firmware Upgrade > Check Update タブ画面

2. 「Check Now」をクリックすると、「Status」欄に新しいファームウェアの有無が表示されます。

```
Using System (PC) (PC を使用したファームウェアアップグレード)
```

- 1. D-Link Web サイトから新しいファームウェアをダウンロードします。
- 2. 本製品の Web GUI で、Maintenance > Firmware & Config > Firmware Upgrade > Using System (PC) タブの順にメニューをクリックし、以下の 画面を表示します。

🐼 Sta		🛜 Wireless	💻 N		C VPN	Security	Maintenance		
Maintenance » Firmware 8	£ Config »	Firmware Upgrad	• » Using Sy	stem (PC)				?	0
Using System (PC)	Using US	B Check Upda	e						
This page allows user to u	upgrade/de	owngrade the rou	ter firmware	e. This page	also shows the ir	formation regarding	firmware version and buil	d time.	
Current Firmware In	oformatio	n							
Firmware Version			3.14_WW						
Firmware Date			Wed Apr 10 1	8:46:01 20	19				
Firmware Upgrade									
Browse Firmware			Upgrade	*	R				

図 9-41 Firmware Upgrade > Using System (PC) タブ画面

- 3. 「Browse Firmware」の「参照 /Browse」をクリックします。
- 4. ファームウェアを選択後、「開く (Open)」をクリックします。
- 5. 「Upgrade」をクリックします。



Using USB(USB ドライブを使用したファームウェアアップグレード)

- 1. D-Link Web サイトから新しいファームウェアをダウンロードし、USB ドライブにコピーします。
- 2. USB ドライブを本ルータの USB ポートに接続します。
- 3. 本製品の Web GUI で、Maintenance > Firmware & Config > Firmware Upgrade > Using USB タブの順にメニューをクリックし、以下の画面を 表示します。

🙆 Status	🕈 Wireless 📃 Ne	twork 🖓 VPN	Security	ô Maintenance	
Maintenance » Firmware & Config » Fi	rmware Upgrade » Using USB				00
	Please Co	onnect a USB Storage	e Device!		
Using System (PC) Using USB	Check Update				
Using USB					
USB Port 1 USB Device Status Select Firmware	Disconnected				
USB Port 2 USB Device Status Select Firmware	Disconnected				

図 9-42 Firmware Upgrade > Using USB タブ画面

- 4. 一覧からファイルを選択し、「Upgrade」をクリックします。
- 注意 アップグレードのプロセスには数分かかります。アップグレードを中止したり、システムをオフにしたりしないでください。アップグレードが中断された場合、ファームウェアが破損する場合があります。ブラウザで他のサイトを参照せずに、アップグレードが完了するまでお 待ちください。

Backup/Restore (コンフィグレーションのバックアップとリストア)

Maintenance > Firmware & Config > Backup/Restore $\prec = = =$

本製品の設定後、設定内容をコンフィグレーションファイルとしてバックアップする方法について説明します。何らかの理由で不具合が生じた場合、 バックアップしたファイルを使用して設定を復元することができます。 また、同じモデルの別のルータにコンフィグレーションファイルをアップロードすることも可能です。

Backup(コンフィグレーションのバックアップ)

コンフィグレーションのバックアップ方法について説明します。

1. Maintenance > Firmware & Config > Backup/Restore > Backup/Restore タブの順にメニューをクリックし、以下の画面を表示します。

🗥 Status 🛜 Wirele	ss 📃 Network	🕼 VPN 🔮	Security	🔅 Maintenance	
Maintenance » Firmware & Config » Backup / Rest	ore				00
Backup / Restore Backup Settings					
This page allows user to do configuration relate	d operations which inclu	des backup and restore	э.		
Backup / Restore					
Download Debug Logs					
	Download				
Config File Backup					
	Save to System (P	C) Save to USB	Port 1 S	ave to USB Port 2	
Restore Config File from System (PC)					
Browse Saved Configurations	ファイルを選択 選択さ	. せん			
	Restore				
Restore Config File from USB Port 1					

図 9-43 Backup/Restore > Backup/Restore タブ画面

- 2. 「Download Debug Logs」で「Download」をクリックすることにより、デバッグログをダウンロードします。
- 3. バックアップを保存する場所によって、「Save to System (PC)」、「Save to USB Port 1」、または「Save to USB Port 2」をクリックします。ファイ ル名には「.cfg」という拡張子が付加されます。

Restore (コンフィグレーションのリストア)

保存したコンフィグレーションファイルのリストア方法について説明します。リストアすることにより、設定が復元されます。

1. Maintenance > Firmware & Config > Backup/Restore > Backup/Restore タブの順にメニューをクリックし、以下の画面を表示します。

🖽 Status 🎅 Wirele	ss 📃 Network 🕼 VPN 🔒 Security 🐓 Maintenance	
Maintenance » Firmware & Config » Backup / Rest	ore	00
Backup / Restore Backup Settings		
This page allows user to do configuration relate	d operations which includes backup and restore.	
Backup / Restore		
Download Debug Logs		
	Download	
Config File Backup		
	Save to System (PC) Save to USB Port 1 Save to USB Port 2	
Restore Config File from System (PC)		
Browse Saved Configurations	ファイルを選択 選択さ… せん	
	Restore	
Restore Config File from USB Port 1		
USB Device Status	disconnected	
Select File	^ _	
	×	
	Restore	
Restore Config File from USB Port 2		
USB Device Status	disconnected	
566667116		
	Destare	
	Restore	J

図 9-44 Backup/Restore > Backup/Restore タブ画面

- 2. 「Restore Config File from System (PC)」セクションで、「参照 /Browse」をクリックします。バックアップファイルを選択して、「開く (Open)」をクリック、 次に「Restore」をクリックします。
- 3. 「Restore Config File from USB Port 1」「Restore Config File from USB Port 2」に表示される、各 USB ポートに接続した USB デバイスにあるコンフィ グレーションファイルを選択、復元することも可能です。
- 4. 「Restore」をクリックすると、選択したファイルからコンフィグレーションを復元します。

Restori	ng configuration	
	Router will be up in 138 Seconds	
		_

図 9-45 Restoring Configuration 画面

5. 完了するまでしばらくお待ちください。リストアが完了すると、ログイン画面が表示されます。



コンフィグレーションのリストア後に「電源を切る」もしくは「再起動する」場合は、復元完了後のログイン画面が表示されてから3分以 上経過してから実行してください。

Backup Settings (バックアップ設定)

コンフィグレーションのバックアップ方法について説明します。ルータに USB ストレージデバイスが接続されている場合、自動バックアップ(Auto-Backup)機能を使用することが可能です。現在のコンフィグレーションが USB ストレージデバイスに保存され、同様のファイル名が存在する場合は 上書きされます。(以前にバックアップファイルを保存したことがある場合など)。また、コンフィグレーションファイルの暗号化も可能です。

1. Maintenance > Firmware & Config > Backup / Restore > Backup Settings タブの順にメニューをクリックし、以下の画面を表示します

🙆 Status 🛜 Wirele	ss 📃 Network	ഹ vpn	盈 Security	ᅌ Maintenance	
Maintenance » Firmware & Config » Backup / Rest	ore » Backup Settings				0
Backup / Restore Backup Settings					
This page allows user to do configuration relate	d operations which incl	udes backup config	uration.		
Backup / Restore Configuration Setting	gs				
Backup Configuration to USB Automatically	OFF				
Encrypt Configuration File	OFF				
	Save	Cancel			

図 9-46 Backup/Restore > Backup Settings タブ

- 2. 「Backup Configuration to USB Automatically」を「ON」にすると自動的にコンフィグレーションが USB ストレージにファイルとして保存されます。
- 「Encrypt Configuration File」を「ON」にするとコンフィグレーションファイルが暗号化されます。これによりシステムユーザ名/パスワード などの機密情報が未認証のソースなどから閲覧されることはありません。USBドライブ及びホスト上のコンフィグバックアップファイルに適用 されます。

Soft Reboot(再起動/工場出荷時設定の復元)

Maintenance > Firmware & Config > Soft Reboot $\forall = a - b$

Soft Reboot (再起動)

本製品を再起動します。再起動は、電源の切断と投入を実行しますが、初期状態から変更した設定については保持します。

1. Maintenance > Firmware & Config > Soft Reboot の順にメニューをクリックし、以下の画面を表示します。

	🕋 Status	🛜 Wireless	📮 Network	ക vpn	盈 Security	🔅 Maintenance	
Maintenance →	Firmware & Config	» Soft Reboot					3 0
This page allo	ws user to Reboot	: and Reboot with Fac	tory Default the rou	ter.			
Soft Reboo	t						
Soft Reb	oot		Soft Reboot				
Reboot v	vith Factory Defau	ult	Default				

図 9-47 Soft Reboot 画面

2. 「Soft Reboot」の「Soft Reboot」をクリックして、ルータを再起動します。「Cancel」をクリックすると、再起動はキャンセルされます。

Reset to Factory Default Settings(工場出荷時設定へのリセット)

本製品を工場出荷時設定にリセットする方法について説明します。

工場出荷時設定にリセットすると、すべての設定が購入時の状態に戻ります。ログインパスワード、SSID、IP アドレスや無線セキュリティキーなど、 インターネット接続を行うために必要とされる重要な項目もすべてリセットされます。

1. Maintenance > Firmware & Config > Soft Reboot の順にメニューをクリックし、以下の画面を表示します。

	🕋 Status	🛜 Wireless	💻 Network	🚯 VPN	🚊 Security	🔅 Maintenance	
Maintenance »	Firmware & Config	» Soft Reboot					00
This page allo	ws user to Reboot	and Reboot with Fa	actory Default the rout	ter.			
Soft Reboo	t						
Soft Reb	oot		Soft Reboot				
Reboot v	ith Factory Defau	ult	Default				

図 9-48 Soft Reboot 画面

2. 「Reboot with Factory Default」の「Default」をクリックすると、工場出荷時の設定で再起動します。

本製品の工場出荷時の IP アドレス、ログインユーザ名、パスワードは以下の通りです。 IP アドレス: 192.168.10.1 / ログインユーザ名: admin / パスワード: admin

Logs Settings(ログ設定)

Maintenance > Logs Settings $\checkmark = \neg =$

本ルータでは、ログメッセージを取得することができます。ルータを追加するトラフィックの種類をモニタして、潜在的な攻撃やエラーの検出時に通知 を受け取ることができます。以下のセクションはログ構成設定とこれらのログにアクセスする方法を説明しています。

Log Facilities (ログファシリティ)

Maintenance > Logs Settings > Log Facilities $\forall = \neg -$

ファシリティは、ログの種類を意味します。

「Facilities」でログの種類を選択し、「Configuration Options」でログを取得するイベントのセベリティを選択します。

1. Maintenance > Logs Settings > Log Facilities の順にメニューをクリックし、以下の画面を表示します。

🕋 Status	🛜 Wireless	💻 Network	ക vpn	盈 Security	🔅 Maintenance	
Maintenance » Logs Settings »	Log Facilities					00
This page allows user to config	ure logging severity le	evels for different logg	ing facilities.			
Log Facilities						
Facilities						
Select Facility	к	(ernel	•			
Configuration Options						
	Se	end to Event Log	Send to Syslog			
Emergency		OFF	OFF			
Alert		OFF	OFF			
Critical		OFF	OFF			
Error		OFF	OFF			
Warning		OFF	OFF			
Notification		OFF	OFF			
Information		OFF	OFF			
Debugging		OFF	OFF			
		Save C	ancel			

図 9-49 Log Facilities 画面

2. 「Facility」セクションでログの種類を選択→「Configuration Options」セクションでログを取得するイベントのセベリティを選択します。

項目	説明				
	Facilities				
Select Facility	 ログの種類を以下から選択します。 「Kernel」:カーネル関連のログです。 「System」:アプリケーションまたは管理レベルの機能、またはユニット管理に関する管理者による変更に対応 するログです。 「Wireless」:無線(AP)関連の設定と動作に関するログです。 「Network」:ネットワーク関連のログです。 「VPN」:「sslvpn」「openvpn」「ipsec」など VPN 関連のログです。 「Firewall」:ファイアウォール関連のログです。 				
Configuration Options					
ログの送信方法を以下から選択します。 「Send to Event Log」:設定した以上のセベリティのイベントが発生した場合、イベントがキャプチャされデバイスに保存されます。 「Send to Syslog」:設定した以上のセベリティのイベントが発生した場合、イベントがキャプチャされ Syslog サーバに転送されます。 					
Emergency	システムは使用不能				
Alert	すぐになんらかの対処が必要				
Critical	クリティカルな状態				
Error	エラー状態				
Warning	警告状態				
Notification	正常だが注意を要する状態				
Information	情報メッセージ				
Debugging	デバッグッセージ				

特定のセベリティレベルが選択された場合、それと同等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」ファシリティに対し「CRITICAL」レベルのログを設定した場合、CRITICAL、ALERT、EMERGENCYレベルの 802.11 のログが出力されます。

Web 内のイベントログビューア (Status > System Information > All Logs > Current Logs 画面)、またはリモート Syslog サーバのどちらでログを閲 覧するかによって、ログ表示をカスタマイズすることができます。以降のセクションで説明するメールログは、Syslog サーバに設定されたログと同 じ設定が適用されます。

Routing Logs(ルーティングログ)

Maintenance > Logs Settings > Routing Logs $\forall = a - b$

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よってトラフィックを追跡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、閲覧・確認することができます。

注意 ログオプションを有効にすると、大量のログメッセージを生成する可能性があるため、デバッグ目的だけに使用することをお勧めします。

各ネットワークセグメント(LAN、WAN、DMZ)を通過するトラフィックは、ファイアウォールによるパケットの許可 / 破棄の処理に基づいて追跡 することができます。Accepted Packets (許可パケット) は各ネットワークセグメントにおいて送信成功を意味します。本オプションは特に「Default Outbound Policy」が「Always Block」(常にブロック)の時に有効で、ファイアウォールを通過するトラフィックをモニタすることができます。 Dropped Packet(破棄パケット) は、各ネットワークセグメントにおいて送信がブロックされたことを意味します。本オプションは特に「Default Outbound Policy」が「Always Allow」(常に許可)の時に有効で、ファイアウォールを通過するトラフィックをモニタすることができます。

IPv4

1. Maintenance > Logs Settings > Routing Logs > IPv4 タブの順にメニューをクリックし、以下の画面を表示します。

🕋 Status	🛜 Wireless 🛛 💻	Network 🕼 VPN	🔒 Security	🗘 Maintenance	
Maintenance » Logs Settings » R	Routing Logs » IPv4				00
IPv4 IPv6					
The table lists all the available i	routing Logs in the system.				
IPv4 Routing Log Configur	ation				
Routing Log					
	Accepted F	Packets Dropped Pack	ets		
LAN to WAN	OFF	OFF			
WAN to LAN	OFF	OFF			
WAN to DMZ	OFF	OFF			
DMAZ to WAN	OFF	OFF			
LAN to DMZ	OFF	OFF			
DMZ to LAN	OFF	OFF			
VLAN to VLAN	OFF	OFF			
Category Filtering	OFF	OFF			
	Save	Cancel			

図 9-50 Routing Logs > IPv4 タブ画面

2. 「Accepted Packets」または「Dropped Packets」について、以下のイベントの「ON」「OFF」を選択します。

「LAN to WAN」	DMZ to WAN	「VLAN to VLAN」
「WAN to LAN」	□ LAN to DMZ	「Category Filtering」
「WAN to DMZ」	DMZ to LAN	

- Accepted Packets

セグメント間で正常に転送されたパケットをログ出力します。

「Default Outbound Policy」が「Always Block」(常にブロック)の時に役に立ちます。

Dropped Packets

セグメント間でブロックされたパケットをログ出力します。

「Default Outbound Policy」が「Always Allow」(常に許可)の時に役に立ちます。

3. 「Save」をクリックし、設定を適用します。

「Cancel」をクリックした場合は、変更前の設定に戻ります。

IPv6

1. Maintenance > Logs Settings > Routing Logs > IPv6 タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🏾 🎅 Wire	less 📃 Network	ക vpn	🔒 Security	💇 Maintenance	
Maintenance » Logs Settings » Routing Logs »	IPv6				00
IPv4 IPv6					
This page allows user to configure log setting	s for IPv6 network.				
IPv6 Routing Log Configuration					
LAN to WAN					
Accepted Packets	OFF				
Dropped Packets	OFF				
WAN Please configure at least one					
Accepted Packets	OFF				
Dropped Packets	OFF				
	Save	Cancel			

図 9-51 Routing Logs > IPv6 タブ画面

- 2. 「LAN to WAN」セクションで、「Accepted Packets」「Dropped Packets」を「ON」または「OFF」にします。
- 3. 「WAN (Please configure at least one)」セクションで、「Accepted Packets」「Dropped Packets」を「ON」または「OFF」にします。
 - Accepted Packets

セグメント間で正常に転送されたパケットをログ出力します。

「Default Outbound Policy」が「Always Block」(常にブロック)の時に役に立ちます。

- Dropped Packets
 セグメント間でブロックされたパケットをログ出力します。
 「Default Outbound Policy」が「Always Allow」(常に許可)の時に役に立ちます。
- 4. 「Save」をクリックし、設定を適用します。

「Cancel」をクリックした場合は、変更前の設定に戻ります。

Sytem Log(System ログ)

Maintenance > Logs Settings > System Logs メニュー

ネットワークセグメントのログの他に、ユニキャストとマルチキャストトラフィックのログを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上に単一の宛先を持っており、一方で、ブロードキャスト(またはマルチキャスト)パケットは、到達可能な すべての宛先に同時に送信されます。もう1つの有用なログの設定として、設定済みの帯域プロファイルによって特定のインタフェース上で破棄さ れたパケットをログ出力することもできます。これらのデータを元に、LANユーザにとって望ましいインターネットトラフィックになるように、帯 域プロファイルの変更する必要があるかどうか検討することができます。

1. Maintenance > Logs Settings > System 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。

🙆 Status 🛜 Wirele	ss 💂 Network 🏠 VPN	🔒 Security	🔅 Maintenance	
aintenance » Logs Settings » System Logs				
This page allows user to configure system wide	log settings.			
System Logs				
All Unicast Traffic	OFF			
All Broadcast / Multicast Traffic	OFF			
FTP Log	OFF			
Redirected ICMP Packets	OFF			
Invalid Packets	OFF			
Bandwidth Limit	OFF			
	Save Cancel			

図 9-52 System Logs 画面

2. 以下の項目を設定します。

項目	説明
All Unicast Traffic	有効にするとルータに向けたパケットを追跡します。
All Broadcast / Multicast Traffic	有効にするとルータに向けたすべてのブロードキャストまたはマルチキャストパケットを追跡します。
FTP Log	有効にするとログ情報を FTP ログに送信します。
Redirected ICMP Packets	有効にするとリダイレクトされた ICMP (Internet Control Message Protocol) パケット数を追跡します。
Invalid Packets	有効にすると受信した無効なパケット数を追跡します。
Bandwidth Limit	有効にすると帯域制限に関連した無線クライアントの情報をログに出力します。

Remote Logging (リモートログ)

Maintenance > Logs Settings > Remote Logging $\prec = -$

ルータが収集するログの種類を設定後、Syslog または E-Mail アドレスにログを送信するように設定できます。 リモートログにおけるキーコンフィグレーションフィールドは、Remote Log Identifier です。各ログメッセージには設定された Remote Log Identifier のプレフィックスが含まれているため、1 台以上のルータからログを受信したシスログサーバやメールサーバは関連デバイスのログをソー トすることが可能です。

メールログに対してオプションを有効にした後、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。ルータがログをパッケージ化して "send-to" アドレスの1つで受信される E メールを送信するために、SMTP ポートと返信メールアドレスが必要となります。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、SMTP サーバに送信されるユーザ名とパスワードデータに使用される「LoginPlain」(暗号化しない)または「CRAM-MD5」(暗号化)をサポートしています。サーバ側で認証が不要な場合、認証を「None」(無効)にすることもできます。SMTP サーバは IDENT 要求を送信することがありますが、本ルータでは、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、ルータによるログの送信タイミングを決定することができます。ログを送信する際のユニット(頻度 など)を選択し、そこで指定した定義済みスケジュールに従って E メールログが送信されます。「Never」を選択した場合、E メールログが無効化さ れますが、メールサーバの設定は保存されます。

Email

1. Maintenance > Logs Settings > Remote Logging > Email タブの順にメニューをクリックし、以下の画面を表示します。

🗥 Status 🛜 Wirele:	ss 📃 Network	ക VPN	盈 Security	🗢 Maintenance	
Maintenance » Logs Settings » Remote Logging »	Email				0
Email Syslog					
This page allows user to configure the remote le Email Log Configuration	ogging options for the rou	ter.			
Remote Log Identifier	DSR-1000AC				
E-Mail Log	ON				
E-Mail Server Address					
SMTP Port	[Range: 1	65535]			
Return E-Mail Address					
Send to E-Mail Address (1)					
Send to E-Mail Address (2)		Optional			
Send to E-Mail Address (3)		Optional			
Authentication with SMTP	🔍 None 💿 Plain Lo	igin OCRAM-	WD5		
User Name					
Password					
Enable Tis	OFF				
Respond to Identd from SMTP	OFF				
E-Mail log by schedule					
Unit	🖲 Never 🛛 🔍 Hourly	O Daily	Weekly		
	Save	Cancel			

図 9-53 Remote Logging > Email タブ画面

2. 以下の項目を設定します。

項目	説明				
Remote Log Identifier	メッセージの送信元を識別するのに使用されるプレフィックスを入力します。この識別子はメールと Syslog メッセージ両方の先頭に付けられています。				
E-Mail Log	<ールログを有効、または無効にします。 ・「ON」:E メールログを有効にします。有効にした場合、以降の項目を設定します。 ・「OFF」:E メールログを無効にします。				
E-Mail Server Address	「E-Mail Log」を「ON」にした場合、SMTP (Simple Mail Transfer Protocol) サーバの IP アドレスまたはネットワーク アドレスを入力します。要求があった場合に、ルータはこのサーバに接続してメールログを送信します。SNMP サー バで E メール通知が受信可能に設定されている必要があります。				
SMTP Port	「E-Mail Log」を「ON」にした場合、メールサーバの SMTP ポートを入力します。				
Return E-Mail Address	「E-Mail Log」を「ON」にした場合、SMTP サーバからの応答が送信されるメールアドレスを入力します。(失敗メッ セージ送信時に必要)				
Send to E-mail Address (1-3)	「E-Mail Log」を「ON」にした場合、ログ、警告が送信されるメールアドレスを最大 3 つまで入力します。				
Authentication with SMTP	「E-Mail Log」を「ON」にした場合、接続を受け入れる前に SMTP サーバ側で認証を必要とする場合、認証の種類を 選択します。 ・「None」:認証は使用されません。「User Name」および「Password」フィールドは利用できません。				
	 「Login Plain」:非暗号化の通信セッション上で Base64 によりコード化されたパスワードを使用してログインするのに使用される認証。Base64 でコード化されたパスワードでは暗号の保護を提供しないため、攻撃の被害を受けやすくなります。 「CRAM-MD5」: HMAC-MD5 MAC アルゴリズムに基づき RFC 2195 で定義されたチャレンジレスポンス認証メカニズム。「CRAM-MD5」は、「Login Plain」よりも高いレベルの認証を提供します。 				
User Name	「Authentication with SMTP」で「Login Plain」または「CRAM-MD5」を設定した場合、認証に使用するユーザ名を 入力します。				
Password	「Authentication with SMTP」で「Login Plain」または「CRAM-MD5」を設定した場合、認証に使用するパスワード(大 文字、小文字の区別あり)を入力します。				
Enable TIs	「Authentication with SMTP」で「Plain Login」または「CRAM-MD5」を選択した場合、TLS を有効にすることが可能です。				
Respond to Identd from SMTP	「E-Mail Log」を有効にした場合、ルータが SMTP サーバからの IDENT 要求に応答するかどうかを指定します。 ・「ON 」:ルータは SMTP サーバからの IDENT 要求に応答します。 ・「OFF 」:ルータは SMTP サーバからの IDENT 要求を無視します。				
	E-Mail log by schedule				
スケジュールに基づいてメー,	ルログを受信するためには、スケジュール設定を行います。				
Unit	ログを送信する間隔を選択します。ログの定期送信を無効化した場合でも、Status > System Information > All Logs > Current Logs 画面で「Send Log」をクリックし、ログを送信することができます。 ・「Never」:ログの送信を無効にします。 ・「Hourly」:1時間ごとにログを送信します。 ・「Daily」:毎日指定した時間にログを送信します。 ・「Weekly」:毎週指定した曜日と時間にログを送信します。				
Day	「Unit」を「Weekly」に設定した場合、ログを送信する曜日を選択します。				
Time	「Unit」を「Daily」または「Weekly」に設定した場合、ログを送信する時間を選択します。				

Syslog

ルータからログを収集して保存する場合、一般的に Syslog サーバが使用されます。そのようなリモートデバイスでは、通常、ルータのローカルメ モリよりも容量制限の影響が少なくなっています。多くのログを収集することができるため、長期間に渡ってネットワーク問題のデバッグを実施し たり、ルータトラフィックをモニターする際に役に立ちます。

本画面の設定を使用して、各サーバに対してセベリティの異なる様々なログファシリティメッセージを受信するように設定することができます。 ログの定義については、「Log Facilities(ログファシリティ)」を参照してください。

1. Maintenance > Logs Settings > Remote Logging > Syslog タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🛜 Wirele	ess 📃 Network	🝙 VPN 🔮 Security	Maintenance
Maintenance » Logs Settings » Remote Logging »	Syslog		9 0
Email Syslog			
This page allows user to configure the syslog ser	rver logging options for the	router.	
System server configuration			
Syslog Server 1	ON THE		
FQDN / IP Address			
Facility	All	V	
Severity	All	V	
Syslog Server 2	OFF	J	
Syslog Server 3	OFF		
Syslog Server 4	OFF		
Syslog Server 5	OFF		
Syslog Server 6	OFF		
Syslog Server 7	OFF		
Syslog Server 8	OFF		
Syslog Server 9	OFF		
Syslog Server 10	OFF		
	Save	Cancel	

図 9-54 Remote Logging > Syslog タブ画面

2. 以下の項目を設定します。

項目	説明			
Syslog Server	Syslog サーバを「ON」または「OFF」に設定します。			
	サポートしている Syslog サーバの数は製品によって異なります。			
	• DSR-1000/1000AC : 10			
	• DSR-500 : 7			
FQDN/IP Address	Syslog サーバのインターネット名 /IP アドレスを指定します。			
Facility	コグ出力のファシリティ(「All」「Kernel」「System」「Network」「VPN」「Firewall」)を選択します。			
Severity	ログ出力のセベリティを選択します。			
	• 「Log Debug」			
	• 「Log Info」			
	「Log Notice」			
	• 「Log Warning」			
	• 「Log Error」			
	• 「Log Critical」			
	• 「Log Alert」			
	FLog Emerg J			

SMS Logging (SMS ログ (未サポート))

Maintenance > Logs Settings > SMS Logging $\prec = a - a$

「WAN」「VPN」「CPU/Memory」に関するログ情報を指定の携帯端末番号へ SMS で送信します。

注意 本機能は未サポートです。

1. Maintenance > Logs Settings > SMS 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。

	🝘 Status	🛜 Wireless	💻 Network	r vpn	욢 Security	😳 Maintenance	
Maintenance » Logs Settings » SMS Logging							00
			3G is n	ot available			
This page allo	ows user to get eve	ent based SMS on con	figured mobile numb	er.			
SMS Loggir	ig Configuration	n					
Receiver							
Mobile N	lumber						
Events							
WAN UP/	Down		OFF				
VPN Con	nect/Disconnect		OFF				
CPU/Me	nory usage reache	s Max limit	OFF				
			Save	Cancel			

図 9-55 SMS Logging 画面

2. 以下の項目を設定します。	
項目	説明
Mobile Number	ログを送信する SMS の携帯端末番号を入力します。
WAN UP/Down	WAN の有効 / 無効に関するログについて SMS 送信を行います。
VPN Connect/Disconnect	VPN の接続 / 切断に関するログについて SMS 送信を行います。
CPU/Memory usage reaches	CPU 使用率が 50%、Memory 使用率が 80% に到達したときに SMS 送信を行います。
Max limit	

第10章 ステータス情報 (Status)

本製品のステータス情報と統計情報を表示する、以下のページについて説明します。

メニュー	説明
「Dashboard (ダッシュボード画面)」	ルータは、システムが使用しているリソースについて表示するダッシュボードを提供します。
「System Information(システム状態の参照)」	ルータのシステム情報について参照します。
「Network Information (ネットワーク情報の参照)」	ルータのネットワーク情報について参照します。

Dashboard (ダッシュボード画面)

Status > Dashboard $\prec = \neg -$

ダッシュボード画面では、WAN ポートや VPN の使用状況やトラフィックの量など、本製品のリソースを確認できます。 各項目にある「Detail」をクリックすると、より詳細な情報が表示されます。

🝘 Status <table-cell> 🛜 Wir</table-cell>	reless 📃 I	Network 🙆 VPN	🔒 Security	🔅 Maintenance	
Status » Dashboard					0 0
The Traffic Overview, WAN Ports, Bandwidth	Usage, VPNs and	packet traffic through the i	router is displayed f	or each interface.	
Dashboard				Manage	Dashboard
Traffic Overview	WAN Port	:5	Bandw	ridth Usage	ALL 🔻
HTTP 2.33% HTTPS 96.08% Email 0% DNS 1.6%	10 8 4 2 0 MB 6:30	3 6:45 7:0 7:15 7:30	30 22.5 15 7.5	1 2 3 4	5
		0.00 MB/s 0.00 MB/s 0.00 MB/s	III HTT III DNS III Oth Total B	P 0.53 M HTTP: 0.37 SNMP er 0.00 andwidth Usage: 22.92 MB	22.02
Details		Det	ails	l	Details
VPNs	CPU Utiliz	ation	Memo	ry Utilization	
10 8 6 4 2 0		User Kernel Idle Time	6% 300 2% 200 92% 0		
6:53 7:0 7:13 7:30 7:36 GIVE Connected FIPSec Gateway 0/0 Tunnels Connected FIPSec Client 0/0 Tunnels Connected		IOs	0% 🔟 Use	d 129.96 Ma Free hed 35.84 Ma Buffer	351.58 s 0.00
SSL VPN 0/1 Tunnels Connected		Det	Total //	lemory Usage: 481.54 MB	Details
Fraffic Information					
Traffic	LAN	WAN1	WAN2	WAN3	
Incoming	134742	117445	0	0	
Outgoing	34000	4353	0	0	
Dropped Outgoing	0	0	0	0	

図 10-1 Dashboard 画面

項目	説明
Traffic Overview	各インタフェースのサービス毎のトラフィック概要についてグラフを表示します。
WAN Ports	WAN トラフィックのパケット情報や帯域についてグラフを表示します。
Bandwidth Usage	「WLAN」や「LAN」などのネットワークセグメントに使用された帯域の使用率を表示します。データは「HTTP」「HTTPS」「DNS」 「SNMP」などのアプリケーションサービス毎に表示されます。
VPNs	帯域やトンネル数など VPN トラフィックについてのチャートを表示します。
Memory Utilization	メモリの使用率について表示します。
CPU Utilization	CPU の使用率について表示します。
Traffic Information	各インタフェースのトラフィック統計を表示します。
Active Information	受信 ICMP パケット数、利用可能な VLAN、アクティブなインタフェースの情報を表示します。

■ ダッシュボードの管理

ダッシュボードに表示する項目を選択できます。

1. 「Manage Dashboard」をクリックします。



2. 以下の画面で、各項目の「ON」「OFF」を選択します。

Manage Dashboard				×
Traffic Overview	ON	WAN Ports	ON	
Bandwidth Usage	ON III	VPNs	ON	
CPU Utilization	ON	Memory Utilization	ON III	
			Sav	/e
		18(4)	LINE THE STREET	

図 10-3 Managed Dashboard 画面

- 3. 「ON」にした項目がダッシュボード画面に表示されます。
- 4. 「Save」をクリックし、設定を適用します。

System Information(システム状態の参照)

Status > System Information $\checkmark = \neg -$

Device (デバイス状態の参照)

Status > System Information > Device $\times = = =$

本製品の状態について表示します。

System (システム)

本製品のシステムや LAN、WAN などの状態を確認できます。

1. Status > System Information > Device > System タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status		💻 Network	CA VPN	🔒 Security	O ^o Maintenance	
Status » System Information »	Device » System					00
System LAN WAN1	WAN2 WAN3 Wirel	ess				
All of your Internet and netwo displayed here. System Information	rk connection details a	re displayed on the D	evice Status page.	The firmware version	n and hardware serial num	ıber is also
General						
System Name	D	5R-1000AC				
Firmware Version	3	14_WW				
Hardware Version	A	1				
Serial Number	s	37R1F6000013				

図 10-4 System > System タブ画面

項目	説明
	General
System Name	ルータ名が表示されます。
Firmware Version	現在使用しているファームウェアのバージョンが表示されます。
Hardware Version	ハードウェアバージョンが表示されます。
Serial Number	シリアル番号が表示されます。

LAN

本製品の MAC アドレス、IP アドレスやリンクステータスなど LAN 状態について表示します。

1. Status > System Information > Device > LAN タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🛜 Wire	less 💂 Network	🕼 VPN	💂 Security	Maintenance		
Status » System Information » Device » LAN					00	
System LAN WAN1 WAN2 WAN3	Wireless					
All of your LAN network connection details a	re displayed on the Device St	tatus page.				
LAN Information						
Description	LAN Info					
MAC Address	94 80 6A 71 (K 28					
IPv4 Address	IPw4 Address 172.16.1.47 / 255.255.255.0					
IPv6 Address	IPv6 Address fe80::56b8:aff:fe71:be28 / 64, fec0::1 / 64					
Status UP						
DHCP Server	Disabled					
DHCP Relay	Disabled					
図 10-5 Device > LAN タブ画面						

WAN1

本製品の WAN1 ポートの状態について表示します。

1. Status > System Information > Device > WAN1 タブの順にメニューをクリックし、以下の画面を表示します。

🝘 Status 🛜 Wireless 💂 Netwo	ork 🕼 VPN 🤮 Security 🔅 Maintenance
Status » System Information » Device » WAN1	0
System LAN WAN1 WAN2 WAN3 Wireless	
All of your WAN1 network connection details are displayed on the D	evice Status page.
WAN1 Information	
Description	WAN1 Info
MAC Address	54 WebA710629
IPv4 Address	0.0.0.0 / 255.255.255.0
IPv6 Address / Prefix	
Status	DOWN
IPv6 Connection Type	Dynamic IP (DHCPv6)
IPv6 Connection State	Not Yet Connected
NAT (IPv4 Only)	Enabled
IPv4 Connection Type	Dynamic IP (DHCP)
IPv4 Connection State	Not Yet Connected
Link State	LINK DOWN
WAN Mode	Use only single port: WAN1
Gateway	0.0.0
Primary DNS	0.0.0
Secondary DNS	0.0.0
Renew	Release

図 10-6 Device > WAN1 タブ画面

「Renew」:表示情報を更新します。

「Release」:インターネット接続設定の更新を行います。

WAN2

本製品の WAN2 ポートの状態について表示します。

1. Status > System Information > Device > WAN2 タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🛜 Wireless 💂 Netwo	rk 🕼 VPN 🤮 Security 🔅 Maintenance			
Status » System Information » Device » WAN2	0 9			
System LAN WAN1 WAN2 WAN3 Wireless				
All of your WAN2 network connection details are displayed on the De	avice Status page.			
WAN2 Information				
Description	WAN2 Info			
MAC Address	North do 11 milito			
IPv4 Address	0.0.0.0 / 255.255.255.0			
IPv6 Address				
Status	DOWN			
IPv6 Connection Type	Dynamic IP (DHCPv6)			
IPv6 Connection State	Not Yet Connected			
Prefix Obtained				
NAT (IPv4 Only)	Enabled			
IPv4 Connection Type	dhepe			
IPv4 Connection State	Not Yet Connected			
Link State	LINK DOWN			
WAN Mode Use only single port: WAN1				
Gateway	0.0.0			
Primary DNS	0.0.0.0			
Secondary DNS	0.0.0			
Disable				

図 10-7 Device > WAN2 タブ画面

「Disable」:WAN2 ポートを無効にします。

WAN3

本製品の WAN3 ポートの状態について表示します。

1. Status > System Information > Device > WAN3 タブの順にメニューをクリックし、以下の画面を表示します。

🙆 Status 🛜 Wireless 💂 Netwo	rk 🙃 VPN 🎡 Security 🍄 Maintenance
Status » System Information » Device » WAN3	0 9
System LAN WAN1 WAN2 WAN3 Wireless	
All of your WAN3 network connection details are displayed on the D	evice Status page.
WAN3 Information	
Description	WAN3 Info
MAC Address	00:00:00:00:00
IPv4 Address	0.0.0.0 / 255.255.255.0
IPv6 Address / Prefix	N/A
Status	DOWN
IPv6 Connection Type	N/A
IPv6 Connection State	N/A
NAT (IPv4 Only)	Enabled
IPv4 Connection Type	Mobile Internet
IPv4 Connection State	Not Yet Connected
Link State	LINK DOWN
WAN Mode	Use only single port: WAN1
Gateway	0.0.0
Primary DNS	0.0.0
Secondary DNS	0.0.0
Disable	

図 10-8 Device > WAN3 タブ画面

「Disable」:WAN3 ポートを無効にします。

Wireless(無線ネットワーク)

本製品の無線ネットワーク設定について表示します。

1. Status > System Information > Device > Wireless タブの順にメニューをクリックし、以下の画面を表示します。

🝘 Status	🛜 Wireless 🖳	Network	S VPN	Security	🗢 Maintenance			
Status » System Information » Device » Wireless								
System LAN WAN1 WA	System LAN WAN1 WAN2 WAN3 Wireless							
All of your wireless network con	nection details are displayed	d on the Device Sta	tus page.					
Wireless Lan Information								
Description			Wireless LAN					
Operating Frequency			5GHz					
Mode			A/N/AC-Mixed					
Channel			40 - 5.2GHz					
Wireless LAN Information f	or Radio-2							
Description			Wireless LAN					
Operating Frequency			2.4GHz					
Mode			N/G-Mixed					
Channel	Channel 6 - 2.437GHz							
Available Access Points								
SSID	Security	Encryption		Authent	ication			
DSR-1000AC_1	OPEN	NONE		NONE				
DSR-1000AC_2	OPEN	NONE		NONE				

図 10-9 Device > Wireless タブ画面

All Logs (ログ)

Status > System Information > All Logs $\rtimes =$ =

ルータで設定したログメッセージを表示します。各ログは、ルータの設定時刻に従って定められたタイムスタンプと共に表示されます。Syslog サーバやメールログ出力などのリモートログ出力が設定されると、ここに表示されるだけでなく、同じログをリモートインタフェースにも送信します。

1. Status > System Information > 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。

🕐 Status 🗧	🔋 Wireless 🛛 💻 Net	work 🕼 VPN	Security	©° Maintenance	
Status » System Information » All Log	» Current Logs				00
This page displays the captured log m Current Logs	essages of the router activiti	es.			
Facility Level	All	\checkmark			
Category	ALL	~			
Severity Level	All	~			
List of Current Logs	on record to get more options]				٩
Facility	🗘 Severity		⊖ Message		θ
	1	lo data available in table			
Showing 0 to 0 of 0 entries				J First J Previous Next >	Last 刘
Clear All Send Logs	Export Logs				

図 10-10 Current Logs 画面

2. 以下の項目を設定します。

項目	説明
Facility Level	 ログの定義を以下から選択します。 「Kernel」:カーネル関連のログです。 「System」:アプリケーションまたは管理レベルの機能、またはユニット管理に関する管理者による変更に対応 するログです。 「Wireless」:無線(AP)関連の設定と動作に関するログです。 「Network」:ネットワーク関連のログです。 「VPN」:「sslvpn」「openvpn」「ipsec」など VPN 関連のログです。 「Firewall」:ファイアウォール関連のログです。
Category	表示するログのカテゴリを指定します。
Severity Level	 表示するログのセベリティレベルを以下から選択します。 「Emergency」:システムは使用不能 「Alert」:即時処理が必要 「Critical」:クリティカルな状態 「Error」:エラー状態 「Warning」:警告状態 「Notification」:正常だが注意を要する状態 「Information」:情報メッセージ 「Debugging」:デバッグッセージ

3. 以下のいずれかを実行します。

・「Clear All」:画面内のすべてのエントリをクリアします。

・「Send Logs」:画面内のすべてのエントリを設定済みのメール受信者に送信します。

・「Export Logs」:画面内のすべてのエントリを TXT ファイル形式でエクスポートします。

USB Status (USB ステータス)

Status > System Information > USB Status $\rtimes = = =$

ルータに接続する USB デバイスの情報について概要を表示しています。ルータには、USB プリンタや USB ストレージ デバイス を直接接続できます。

1. Status > System Information > 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。

🖚 Status 🛜 🕅	Wireless 📃 Network	🕼 VPN 🔒 Se	curity 🔅 Maintenance	
Status » System Information » USB Status				00
This page displays information about the devices connected to the router.	USB devices connected to the l	JSB port(s).This page will upd	ate dynamically to show the statu	s of the USB
Description	USB Port 1		USB Port 2	
Status	Disconnected		Disconnected	
Vendor	NA		NA	
Model	NA		NA	
Туре	NA		NA	
Mount Status	NA		NA	
図 10-11 USB Status 画面				

2. 以下の項目が表示されます。

項目	説明
Status	接続 / 切断されたデバイスの状態を表示します。
Vendor	ルータに接続する USB デバイスのベンダ名を表示します。
Model	ルータに接続する USB デバイスのモデル名を表示します。
Туре	ルータは、USB ディスクドライブ (メモリスティック) デバイス、インターネット USB モデム(アダプタ)、または USB プリンタに接続するインタフェースをサポートしています。
Mount Status	ルータに接続する USB デバイスのマウント状態を表示します。
USB Port 1	USB ポート1に接続するデバイスに関する情報を表示します。
USB Port 2	USB ポート 2 に接続するデバイスに関する情報を表示します。

Network Information (ネットワーク情報の参照)

Status > Network Information $\mathcal{I} = \mathcal{I}$

DHCP リースクライアント情報や VPN の接続状況など、ネットワーク情報の確認を行います。

DHCP クライアントの参照

Status > Network Information > DHCP Leased Clients $\checkmark = = =$

ルータから IP をリースしているクライアントのリストを表示します。

リストには以下の種類があります。

- ・ LAN リースクライアント
- ・ IPv6 リースクライアント
- ・ DMZ リースクライアント

LAN Leased Clients(LAN リースクライアント)

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

	🕜 Status	🛜 Wireless	📃 Network	CA VPN	盈 Security	O ^o Maintenance	
Status » Net	work Information »	DHCP Leased Clients »	LAN Leased Clients				0
LAN Lea	sed Clients IPv6	Leased Clients DM	Z Leased Clients				
This table di addresses, th	splays the list of D is table will show	HCP clients connected the list of DHCP client	to the LAN DHCP Se ts for the router's LA	erver and to whom DHCR N DHCP server.	9 Server has given	leases.If the LAN is serv	ing DHCP
LAN Lease	d Clients List						
Show 10	entries [No right]	nt click options]					٩
Host Name	e	e IP	Address	e	MAC Address		÷
			No data a	available in table			
Showing 0 to	0 of 0 entries					K First A Previous Net	xt 🔰 Last 刘

図 10-12 DHCP Leased Clients > LAN Leased Clients タブ画面

2. 以下の項目が表示されます。

項目	説明
Host Name	接続しているクライアントのホスト名が表示されます。
IP Address	予約 IP リストに一致するクライアントの LAN IP アドレスが表示されます。
MAC Addresses	設定済みの IP アドレス予約を持つ LAN クライアントの MAC アドレスが表示されます。

IPv6 Leased Clients (IPv6 リースクライアント)

1. Status > Network Information > DHCP Leased Clients > IPv6 Leased Clients タブの順にメニューをクリックし、以下の画面を表示します。

	🝘 Status	🛜 Wireless	💻 Network	ഹ VPN	🔒 Security	🗘 Maintenance	
Status » Net	work Information »	DHCP Leased Clients »	IPvó Leased Clients				00
LAN Lea	sed Clients IPv6	Leased Clients DA	4Z Leased Clients				
This table dis DHCPV6 addr	plays the list of DH esses, this table wi	HCPv6 clients connect Il show the list of DH	ted to the LAN DHCF CPv6 clients for the	^D v6 Server and to v router's LAN DHCF	vhom DHCPv6 Server Vv6 server.	has given leases.If the LAI	N is serving
IPv6 Lease	d Clients List						
Show 10	• entries [No righ	it click options]					٩
IP Address			🔂 DI	UID	⇔	IAID	⇔
			No data a	vailable in table			
Showing O to	0 of 0 entries					First J Previous Next	> Last >

図 10-13 DHCP Leased Clients > IPv6 Leased Clients タブ画面

2. 以下の項目が表示されます。

項目	説明
IP Address	予約 IP リストに一致するクライアントの LAN IPv6 アドレスが表示されます。
DUID	設定済みの IPv6 アドレス予約を持つ LAN クライアントの DUID(DHCP Unique Identifier)が表示されます。
IAID	設定済みの IPv6 アドレス予約を持つ LAN クライアントの IAID(Identity Association Identifier)が表示されます。

DMZ Leased Clients(DMZ リースクライアント)

1. Status > Network Information > DHCP Leased Clients > DMZ Leased Clients タブの順にメニューをクリックし、以下の画面を表示します。

	🝘 Status	🛜 Wireless	💻 Network	ഹ് VPN	🔒 Security	🗘 Maintenance	
Status » Net	work Information »	DHCP Leased Clients »	DMZ Leased Clients				00
LAN Lea	sed Clients IPv6	Leased Clients	MZ Leased Clients				
This table dis addresses, th	plays the list of Di is table will show t	HCP clients connecte the list of DHCP clier	d to the DMZ DHCP S its for the router's D/	erver and to who MZ DHCP server.	m DHCP Server has giv	ven leases.If the LAN is s	erving DHCP
DMZ Lease	d Clients List						
Show 10	 entries [No right 	nt click options]					٩
IP Address				AC Address			⇔
			No data av	ailable in table			
Showing O to	0 of 0 entries					First Previous Next	: > Last >

図 10-14 DHCP Leased Clients > DMZ Leased Clients タブ画面

2. 以下の項目が表示されます。

項目	説明
IP Address	予約 IP リストに一致するホストの LAN IP アドレスが表示されます。
MAC Address	定義済みの IP アドレスの予約を持つ LAN ホストの MAC アドレスが表示されます。

CaptivePortal Sessions (キャプティブポータルセッションの参照)

Status > Network Information > CaptivePortal Sessions $\checkmark = =$

キャプティブポータルセッションについての情報を表示します。

1. Status > Network Information > CaptivePortal 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。

00
٩
⇔
t 🔪 Last 🕅

図 10-15 CaptivePortal Sessions 画面

2. 以下の項目が表示されます。

項目	説明
User Name	キャプティブポータルにログイン中のユーザ名が表示されます。
IP Address	キャプティブポータルにログイン中のユーザの IP アドレスが表示されます。

キャプティブポータルセッションのエントリを右クリックし、以下のアクションを実行することができます。

- ・「Block」: ユーザ名と IP アドレスをブロックします。
- ・「Disconnect」: 選択したユーザの現在のセッションを削除します。

Active Sessions(アクティブセッションの参照)

Status > Network Information > Active Sessions $\checkmark = \neg -$

アクティブセッションでは、ルータのファイアウォール経由のアクティブなインターネットセッションについて、以下の項目の情報を表示します。

- •「Source」:送信元
- •「Destination」:宛先
- 「Protocol」: プロトコル
- ・「State」:状態
- 1. Status > Network Information > 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。

tive on your router.				1	00
			(
Destination	0	Protocol	⊖	State	٩
192.168.0.1:53		udp		none	
192.168.0.1:53		udp		none	
192.168.0.1:53		udp		none	
192.168.0.1:53		udp		none	
192.168.0.1:53		udp		none	
192.168.10.100:68		udp		none	
	Destination 192.168.0.1:53 192.168.0.1:53 192.168.0.1:53 192.168.0.1:53 192.168.0.1:53 192.168.0.1:53 192.168.10.100:68	Destination Image: Comparison of the state of the sta	Destination Protocol 192.168.0.1:53 udp 192.168.0.1:53 udp	Destination Protocol P 192.168.0.1:53 udp 192.168.0.1:53 udp	Destination ♥ Protocol ♥ State 192.168.0.1:53 udp none 192.168.10.100:68 udp none

図 10-16 Active Sessions 画面

Active VPNs (VPN セッションの参照)

Status > Network Information > Active VPNs $\prec = = =$

ルータの VPN 接続に関するステータス(接続 / 破棄)について表示、変更します。アクティブな VPN 接続のトラフィック詳細やトンネル状態についてリスト化しています。トラフィックについてはトンネル確立後の送受信パケットの累積総量で表示されます。

表示する VPN セッションの内容を以下のタブから選択します。

- IPSec SAs
- SSL VPN Connections
- PPTP Connections
- Open VPN Connections
- L2TP VPN Connections
- GRE Tunnel Sessions

IPSec SAs

1. Status > Network Information > Active VPNs > IPSec SAs タブの順にメニューをクリックし、以下の画面を表示します。

		🝘 Status	I.	Wireless	💻 Netv	vork 🕋		🔒 Security	🗢 Mai		
Status » Network Information » Active VPNs » IPsec SAs											
IPsec SAs SSL VPN Connections PPTP VPN Connections Open VPN Connections L2TP VPN Connections GRE Tunnel Status											
This page lists current established IPsec Security Associations.											
Active IPSec SAs List											
SI	now 10	 entries [Righ 	it click or	n record to get m	ore options]						٩
P	olicy Nam	e	Ŷ	Endpoint	⇔	t× (KB)	⇔	tx (Packets)		⊖ State	⊜
	No data available in table										
SI	nowing () to (of 0 entries							H First A P	revious Next	t 🔪 Last 刘

図 10-17 Active VPNs > IPsec SAs タブ画面

SSL VPN Connections

1. Status > Network Information > Active VPNs > SSL VPN Connections タブの順にメニューをクリックし、以下の画面を表示します。

	🝘 Status	🛜 Wireles	ss 📃 Network	ଜ ଜ ଏ	PN 🔮 Security	🔅 Maintenance				
Status » Network Information » Active VPNs » SSL VPN Connections										
IPsec SAs SSL VPN Connections PPTP VPN Connections Open VPN Connections L2TP VPN Connections GRE Tunnel Status										
This page lists current established SSL VPN tunnels.										
Active SSL VPN Connections										
Show 10 🔹 entries [Right click on record to get more options]										
User Name	🔂 IP Ado	iress 😔 L	ocal PPP Interface	÷	Peer PPP Interface	⊖ Connect Status	; ⊖			
No data available in table										
Showing 0 to 0 of 0 entries Next > Last >										
図 10-18 Active VPNs > SSL VPN Connections タブ画面										

PPTP VPN Connections

1. Status > Network Information > Active VPNs > PPTP VPN Connections タブの順にメニューをクリックし、以下の画面を表示します。

	🕐 Status	🛜 Wireless	💻 Network	A VPN	읊 Security	🗘 Maintenance				
Status » Network Information » Active VPNs » PPTP VPN Connections										
IPsec SA	s SSL VPN Conn	ections PPTP VPN C	onnections Open V	PN Connections	L2TP VPN Connect	ions GRE Tunnel Status				
This page lists current established PPTP VPN tunnels.										
Active PPTP VPN Connections										
Show 10 • entries [Right click on record to get more options]										
Connection Status										
Disconnected										
Showing 1 to 1 of 1 entries 1 Next > Last >										

図 10-19 Active VPNs > PPTP VPN Connections タブ画面

Open VPN Connections

1. Status > Network Information > Active VPNs > Open VPN Connections タブの順にメニューをクリックし、以下の画面を表示します。

	🝘 Status	🛜 Wireless	💻 Network	ഹം VPN	盈 Security	🗘 Maintenance				
Status » Network Information » Active VPNs » Open VPN Connections										
IPsec SAs SSL VPN Connections PPTP VPN Connections Open VPN Connections L2TP VPN Connections GRE Tunnel Status										
The table lists all the available Active OpenVPN Connections in the system.										
Active OpenVPN Connections										
Show 10 • entries [No right click options]										
Common N	ame	🔂 Client II	P ↔	Bytes Received		⊖ Bytes Sent	⇔			
No data available in table										
Showing 0 to 0 of 0 entries Next > Last >										

図 10-20 Active VPNs > OpenVPN Connections タブ画面
L2TP VPN Connections

1. Status > Network Information > Active VPNs > L2TP VPN Connections タブの順にメニューをクリックし、以下の画面を表示します。

	🕋 Status	🛜 Wireless	💻 Netwo	ork 🙆 VPN	🔒 Security	🗢 Maintenance	
Status » Netv	vork Information »	Active VPNs » L2TP VI	PN Connections				00
IPsec SA	s SSL VPN Conn	ections PPTP VPN C	onnections C)pen VPN Connectior	s L2TP VPN Connec	tions GRE Tunnel Status	
This page list	s current establish	ned L2TP VPN tunnels.					
Active L2T	P VPN Connect	ions					
Show 10	• entries [Right c	click on record to get mo	re options]				٩
Connectio	n Status						÷
Disconnected							
Showing 1 to	1 of 1 entries				Н	First A Previous 1 Next	> Last >

図 10-21 Active VPNs > L2TP VPN Connections タブ画面

GRE Tunnel Status

1. Status > Network Information > Active VPNs > GRE Tunnel Status タブの順にメニューをクリックし、以下の画面を表示します。

	🕋 Status	🛜 Wireless	💻 Network	ക vpn	🚨 Security	🐡 Maintenance	
Status » Netv	vork Information »	Active VPNs » GRE Tu	nnel Status				00
IPsec SA	s SSL VPN Conn	ections PPTP VPN C	Connections Open V	PN Connections	L2TP VPN Connect	ions GRE Tunnel Status	
This page list	s current GRE tun	nels.					
Active GRE	Tunnels						
Show 10	• entries [No rig	ht click options]					٩
Tunnel Na	ne	🔂 Loc	al IP	⊖ Remote	IP		⇔
			No data ava	ilable in table			
Showing O to) of 0 entries					K First Previous Next	> Last >

図 10-22 Active VPNs > GRE Tunnel Status タブ画面

Interfaces Statistics (インタフェースの統計)

Status > Network Information > Interfaces Statistics $\varkappa \Box \Box -$

LAN、VLAN および WLAN インタフェースにおけるパケット情報を表示します。

1. Status > Network Information > Interfaces 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。

us » Network Information » Interfac	es Statistics			0 (
profiled and packet traffic through	the router is display	ed for each interface	ο.	
erfaces Statistics				
AN	100000000	Lawrences	L'active provider and	Commission Commission
Description	LAN	WAN1	WANZ / DMZ	WAN3
Incoming Packets	17151	0	0	0
Outgoing Packets	14687	0	0	0
Dropped In Packets	0	0	0	0
Dropped Out Packets	0	0	0	0
LAN				
Show 10 💟 entries [No right click	options]			٩
Port O Incoming Packets	Outgoing F	Packets 0	Dropped In Packets	Θ Dropped Out Packets Θ
Port O Incoming Packets LAN10 0 Showing 1 to 1 of 1 entries	Outgoing F	Packets 0	Dropped in Packets	Oropped Out Packets O 0 0 First (Provious 1 Next > Last))
Port O Incoming Packets LANIO 0 Showing 1 to 1 of 1 entries /LAN	0 Outgoing F	Packets Θ (Dropped in Packets	Dropped Out Packets O 0 0 First (] Previous 1 Next >
Port O Incoming Packets LANIO 0 Showing I to 1 of 1 entries /LAN Data Information	θ Outgoing F 0	Packets 0 1	Dropped in Packets	B Dropped Out Packets O 0 0 First () Previous 1 Next > Last >) Bytes 0
Port O Incoming Packets LANIO 0 Showing 1 to 1 of 1 entries /LAN Data Information Transmitted	Outgoing F	Packets 0 1	Dropped in Packets	Byperform Dropped Out Packets Out 0 0 First (Provious 1 Next > Last >) Bytes 0 0
Port O Incoming Packets LANIO 0 Showing 1 to 1 of 1 entries /LAN Data Information Transmitted Received	Outgoing F	Packets 0 1	Dropped in Packets	Bytes 0 0 0
Port O Incoming Packets LAN10 0 Showing 1 to 1 of 1 entries //LAN Data Information Transmitted Received Transmit Dropped	Outgoing F	Packets 0 1	Dropped in Packets	Bytes 0
Port O Incoming Packets LAN10 0 Showing 1 to 1 of 1 entries //LAN Data Information Transmitted Received Transmit Dropped Receive Dropped	Outgoing F	Packets 0 1	Dropped in Packets	Bytes 0 Bytes 0 0 2505 0
Port O Incoming Packets LAN10 0 Showing 1 to 1 of 1 entries /LAN Data Information Transmitted Received Transmit Dropped Receive Dropped Transmit Errors	Outgoing F	Packets 6	Dropped in Packets	Bytes 0 Bytes 0 0 2505 0 N/A
Port Incoming Packets LANIO 0 Showing 1 to 1 of 1 entries /LAN Data Information Transmitted Received Transmit Dropped Receive Dropped Transmit Errors Receive Errors	0 Outgoing F	Packets 6 1 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Dropped in Packets	Bytes 0 Bytes 0 Bytes 0 <th< td=""></th<>
Port O Incoming Packets LANIO 0 Showing 1 to 1 of 1 entries LANN Data Information Transmitted Received Transmit Dropped Receive Dropped Transmit Errors Receive Errors	0 Outgoing F	Packets 6 6	Dropped in Packets	Bytes 0 Bytes 0 Bytes 0 <th< td=""></th<>
Port O Incoming Packets LAN10 0 Showing 1 to 1 of 1 entries LANN Data Information Transmitted Received Transmit Dropped Receive Dropped Transmit Errors Receive Errors Receive Info	Outgoing F 0	Packets 6	Dropped in Packets 0 sckets 0	Bytes 0 Bytes 0 Bytes 0
Port Incoming Packets LAN10 0 Showing 1 to 1 of 1 entries ZAN Data Information Transmitted Received Dropped Transmit Errors Receive Errors ctive Info Description	0 Outgoing F	Packets 6	Dropped in Packets 0 Inckets 05 Count	Bytes 0 Bytes 0 Bytes 0
Incoming Packets IAN10 0 Showing 1 to 1 of 1 entries IANN Data Information Transmitted Received Dropped Transmit Errors Receive Frors ctive Info Description	Θ Outgoing F 0	Packets 6 1	Dropped in Packets 0 count Count 45	Bytes 0 Bytes 0 Bytes 0
Port Incoming Packets LAN10 0 Showing 1 to 1 of 1 entries /LAN Data Information Transmitted Received Transmit Dropped Receive Dropped Transmit Errors Receive Errors ctive Info Description ICMP Received Active VPN Tunnets	0 Outgoing F	Packets 6 1	Dropped in Packets 0 count 45 0	Bytes 0 Bytes 0 Bytes 0

図 10-23 Interfaces Statistics 画面

2. 以下の項目が表示されます。

項目	説明
	LAN
Incoming Packets	ポートに入力する IP パケット数が表示されます。
Outgoing Packets	ポートから出力するパケット数が表示されます。
Dropped In Packets	インタフェースのインバウンド方向で破棄されたパケットが表示されます。
Dropped Out Packets	インタフェースのアウトバウンド方向で破棄されたパケットが表示されます。
	VLAN
Port	VLAN に対応するポート番号が表示されます。
Incoming Packet	ポートに入力する IP パケット数が表示されます。
Outgoing Packet	ポートから出力するパケット数が表示されます。
Dropped In Packet	インタフェースのインバウンド方向で破棄されたパケットが表示されます。
Dropped Out Packet	インタフェースのアウトバウンド方向で破棄されたパケットが表示されます。
	WLAN
Transmitted	ルータの管理下にあるすべてのアクセスポイントが送信したパケット数が表示されます。
Received	ルータの管理下にあるすべてのアクセスポイントが受信したパケット数が表示されます。
Transmit Dropped	ルータの管理下にあるすべてのアクセスポイントが送信し、破棄された総パケット数が表示されます。
Receive Dropped	ルータの管理下にあるすべてのアクセスポイントが受信し、破棄された総パケット数が表示されます。
Transmit Errors	ルータの管理下にあるすべてのアクセスポイントが送信し、エラーが発生した総パケット数が表示されます。
Receive Errors	ルータの管理下にあるすべてのアクセスポイントが受信し、エラーが発生した総パケット数が表示されます。

項目	説明
	Active Info
ICMP Received	インタフェースで受信した ICMP パケットの総数が表示されます。
Active VPN Tunnels	現在のアクティブな VPN トンネルセッション数が表示されます。
Available VLAN	現在のアクティブな有効 VLAN インタフェース数が表示されます。
Active Interfaces	有効なインタフェースの数が表示されます。

Wireless Clients(無線クライアントの参照)

Status > Network Information > Wireless Clients $\prec = = -$

AP に接続するクライアントについて表示します。接続クライアントは MAC アドレスによってソートされ、対応する AP への接続時間や、無線リン クで使用されるセキュリティパラメータが表示されます。統計テーブルには、ページが更新されるたびに最新のデータを表示できるようにする自動 更新機能があります。自動更新は 10 秒ごとに行われます。

本項目は DSR-1000AC でのみ表示されます。

Status > Network Information > 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。

	🕜 Status		s <u>I</u>	📃 Network	S VPN		Security	\$ ° ^	Naintenance	
Status » Net	work Information »	Wireless Clients								00
This list iden	tifies the wireless o	clients (or station	s) curren	tly connected	to the Access Poin	ts con	figured and enab	led on this	s device.	
Wireless C	lients									
Show 10	entries [No right	click options]								٩
AP Name	MAC Addre	ss \varTheta Radi	• ÷	Security 6	Encryption	€	Authentication	•	Time Connect	ed \varTheta
				No data	available in table					
Showing 0 to	0 of 0 entries							First	J Previous Next	> Last >
図 10-24 \	Nireless Clients	画面								

Wireless Statistics (無線の統計情報)

Status > Network Information > Wireless Statistics $\prec = \neg -$

本画面では、有効化された各アクセスポイントについて、トラフィック統計を表示します。各無線リンクで送信されるトラフィック量を確認することができます。無線帯域または VAP の不具合が発生している場合、本項目でトラフィックが VAP 経由で送受信されているかどうかを確認します。

本項目は DSR-1000AC でのみ表示されます。

1. Status > Network Information > 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。

	🕜 Stat	us 🔶 🐨	'ireless		CA VPN	I 🔒 Se		🗘° Maintenanc	e
Status » Netv	vork Informati	on » Wireless Sta	tistics						00
Wireless traff AP.	ic statistics	for all configured	l access points ar	e displayed in	this table. Th	e receive (Rx) a	and transmit (T	x) data is shown p	oer configured
Wireless St	atistics								
Show 10	entries [N	lo right click option	ns]						٩
AP Name 🕯	Radio 🕀	Packets rx ⊕	Packets tx ⊖	Bytes rx ⊖	Bytes tx ⊖	Errors rx 🕀	Errors tx ⊖	Dropped rx ⊖	Dropped tx ⊖
ap1	5 Ghz	0	0	0	0	0	0	0	0
ap5	2.4 Ghz	0	0	0	0	0	0	0	250
Showing 1 to 2	of 2 entries), First	Previous 1	Next 🍾 Last 💥

図 10-25 Wireless Statistics 画面

Device Statistics(デバイス統計情報)

Status > Network Information > Device Statistics $\prec = \neg -$

本製品の物理ポートの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、確認のために提供されている、ポート固有のパケットレベル情報があります。 送信/受信パケット、ポートの衝突、および送信/受信方向の累積バイト/秒が、ポートの稼働時間とともに各インタフェースに提供されます。有線ポートに問題があると思われる場合は、この表を参照し、アップタイムまたはポートの伝送レベルの問題を診断してください。 統計テーブルには、画面が更新されるたびに最新のデータを表示できるようにする自動更新機能があります。自動更新は 10 秒ごとに行われます。

1. Status > Network Information > 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。

🕐 Stat	us	Wireless	💻 Networ	k 🖓 VPN	🔒 Security	🗘 Mai	ntenance
Status » Network Information	on » Devic	e Statistics					0 0
This page shows the Rx/Tx	packet an	d byte count for	all the system int	erfaces. It also shows	the up time for a	ll the interfaces	•
Device Statistics							
Show 10 v entries [N	o right click	options]					٩
Port	T 🕤	'x Pkts ⊖	Rx Pkts 🛛 🖯	Collisions Θ	Tx B/s ⊖	Rx B/s ⊖	Up time Θ
Configurable Port (WAN)	0	i.	0	0	0	0	Not Yet Available
Dedicated WAN	0		0	0	0	0	Not Yet Available
LAN	6	67	736	0	0	33	0 Days 00:05:06
Showing 1 to 3 of 3 entries						H First H Previ	ious 1 Next > Last >
⊠ 10-26 Device Sta	tistics 面	Ť					

LAN Clients(LAN クライアント)

Status > Network Information > LAN Clients $\checkmark = = = -$

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 > Network Information > 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。

	🕜 Status		💻 Network	CA VPN	Security	🗘° Maintenance	
Status » Net	work Information »	LAN Clients					00
This page dis	plays a list of LAN	clients connected to th	e router.				
LAN Client	s List						
Show 10	entries [No right]	t click options]					٩
IP Address		٢	MAC Address		÷	Туре	⇔
192.168.10.1	0		d4aar52ic11an1c			Static	
Showing 1 to	Showing 1 to 1 of 1 entries 1 Next > Last >						

図 10-27 LAN Clients 画面

Session Limiting Status (セッション制限ステータス)

Status > Network Information > Session Limiting Status $\checkmark =$ =

セッション制限のステータスが表示されます。

1. Status > Network Information > Session Limiting 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。

	🕜 Status		💻 Network	S VPN	Security	O ^o Maintenance		
Status » Net	itus » Network Information » Session Limiting Status							
Use this page Configured in Session Lir	to monitor the run the Profile with Pr niting Status	itime authentication o rofile Name and Source	r current sessions ti e.	hat are active on p	articular session limit	ing Profile with total Sess	ions	
	• encres [rught ct	ick on record to get mor	le options J					
Profile Na	me	Source Type	÷	Current Session	s / Session Limit		⇔	
			No data a	available in table				
Showing 0 to 0 of 0 entries Next > Last >								

図 10-28 Session Limiting Status 画面

第11章 トラブルシューティング

本製品の操作時にトラブルが発生した場合、本章をご参照ください。

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 アドレスを変更した後、IP アドレスを忘れた場合には、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 (リセットにより、ファイアウォールの IP アドレスが 192.168.10.1 に設定されます)。
- 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、パケットスニッファー(Ethereal など)を使用して、ルータの再起 動時に送信されたパケットをキャプチャしてください。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」をクリックしてください。 「Save」をクリックしない場合、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. ステータス画面で IP アドレスが WAN ポートに表示されていることを確認してください。「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. ログインプログラムが必要な場合、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.** チェックが行われる場合、Network Configuration > WAN Settings > Ethernet ISP Settings 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. ご使用のイーサネット MAC アドレスが検証され、許可された MAC アドレス 1 つだけがインターネットに接続できるのかどうか ISP に問い合わ せてください。
- **6.** MAC アドレスの検証が行われる場合、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、Network Configuration > WAN Settings > Ethernet ISP Settings 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 で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. 指定の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 でルータが TCP/IP ゲートウェイとなるように設定します。

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、5 分以上待ってから Maintenance > Administration > Date and Time メニューで日付を確認してください。

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)の調整をしません。

■ 推奨される操作:

- 2. 「Daylight Saving」を「ON」または「OFF」にします。
- 3. 「Save」をクリックし、設定を適用します。

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 ping ユーティリティが備わっており、ICMP エコーリクエストパケットを指定したデバイスに 送信することができます。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、「cmd」を入力して Enter キーを押します。
- 2. コマンドプロンプトで「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. Enter キーを押します。
- 4. 表示をモニタする:
 - パスが動作している場合、以下のメッセージシーケンスが表示されます。
 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
 - パスが動作していない場合、以下のメッセージシーケンスが表示されます。
 Pinging <IP アドレス > with 32 bytes of data Request timed out
- パスが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、「」を参照してください。
 - 対応するリンクの 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ハブポートについ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、「cmd」を入力して Enter キーを押します。
- 2. コマンドプロンプトで「ping-n10 <IP アドレス >」と入力してください。「-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. Enter キーを押して、表示をモニタします。(前述の手順を参照してください。)
- 4. パスが動作していない場合、以下を確認してください。
 - ・ PC にファイアウォールの IP アドレスがデフォルトゲートウェイとして設定され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ている場合、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。

ホスト名が割り当てられている場合、Network Configuration > WAN Settings > Ethernet ISP Settings を選択して、そのホスト名を ISP のア カウント名として入力してください。

・特定の PC のイーサネット MAC アドレス以外が拒否される仕様かどうかを ISP に問い合わせてください。

ブロードバンドの ISP の多くは、ユーザが利用する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。ISP によっては、さらにそのモデムに接続する特定の PC の MAC アドレスに対するアクセスを制限します。 そのような場合は、ファイアウォールをクローンに設定するか、認可された PC からの MAC アドレスになり代わるようにしてください。

工場出荷時設定へのリセット

工場出荷時のコンフィグレーション設定を復元するには、以下のいずれかの手順を実施します。

- 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、Maintenance > Firmware & Config > Soft Reboot を選択し、「Default」をクリックします。
 - ・ 知らない場合、以下の手順を行ってください。

ルータの背面パネルで、リセットボタンを 10 秒程度押し続けます。全ての LED ライトが点灯し、点滅したらボタンを離して、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. コンフィグレーションインタフェースまたは「Reset」から工場出荷時設定に復元した後、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 【付録 A】用語解説

付録

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。
СНАР	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 IP アドレスを必要としなくなった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)。ホスト部分を含む完全なドメイン名。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処理の中で、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。
РРТР	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。
ТСР	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。異なるネットワーク間の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 ネットワークを安全に通過する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(IKE が認証する)デバイスだけではなく、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	Auto Sense
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
	サマータイム	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インバウンド通信	無効(HTTP 80 番ポートを除く)
	インターネットへのアウトバウンド通信	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	РРТР	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:%drowld:%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	DEBUG	sglite3QueryResGet failed.Query:%s	ERROR
opCode:%d rowld:%d			
Wan is not up	DEBUG	Error in executing DB update handler	ERROR
%s:DBUpdate event: Table: %s	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
opCode:%d rowld:%d			
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	sglite3QueryResGet 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	sglite3QueryResGet 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	sglite3OuervResGet failed.Ouerv:%s	ERROR
Setting LED [%d]:[%d] For %s	DEBUG	sglite3OuervResGet failed.Ouerv:%s	ERROR
I2tpEnable: command string: %s	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: handling reboot scenario	DEBUG	failed to call ddns enable	ERROR
nimfAdvOptSetWrap: INDICATOR = %d	DEBUG	ddns: SOL error: %s	ERROR
nimfAdvOptSetWrap: UpdateFlag: %d	DEBUG	ddnsDisable failed	ERROR
nimfAdvOptSetWrap: returning with status: %s	DEBUG	sglite3QueryResGet failed.Querv:%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. Exitina.	ERROR
nimfMacGet: MacAddress: %s	DEBUG	Error opening the lanUptime File	ERROR

ログメッカージ	 	ログメッセージ	
nimfMacGet: MacAddress: %s		Error Opening the land Intime File	FRROR
nimfMacGet: MacAddress: %s	DEBUG	failed to open %s	
nimfMacGet: MacAddress: %s	DEBUG	failed to open %s	
nimfMacGet: MacAddress: %s	DEBUG	failed to query networkInterface table	
nimfMacGet: Mac option Not changed \	DEBUG	failed to query networkInterface table	
nimfMacGet: MacAddress: %s		solite3OuervBesGet failed Ouerv%s	
nimfMacGet: MacAddress: %s	DEBUG	failed to enable IPv6 forwarding	
nimfMacGet: MacAddress: %s	DEBUG	failed to set capabilities on the "	
nimfMacGet: returning with status: %s	DEBUG	failed to enable IPv6 forwarding	
Now in enableing LanBridge function	DEBUG	failed to set capabilities on the "	
successfully executed the command %s	DEBUG	failed to disable IPv6 forwarding	
Now in disableing LanBridge function		failed to set capabilities on the "	
successfully executed the command %s	DEBUG	failed to open %s	
configPortThlHandler:Now we are in Salite Lindate "	DEBUG		
The Old Configuration of ConfiPort was %s	DEBUG		
The New Configuration of ConfiPort was://s	DEBUG		
The user has deselected the configurable port			
failed guony %c	DEBUG	nimfStatus Indato: undating NimfStatus failed	
failed query %s		nimfStatus Update: updating NimfStatus failed	
failed query %s		nimfl inkStatusCot: dotorminig link's status failed	
%s:DBLIndate event: Table: %s opCode:%d rowld:%d		nimfLinkStatusGet: determining link's status failed	
%s:DBUpdate event: Table: %s opCode:%d rowld:%d			
		ifStatucDPU Indato: Eailed to begin "	
%S.%U SIF LINADLL. %S		Instatusebopdate. Failed to begin	
sip i bli landler failed to update listatic		%S. SQL EITOL %S	
		vos. Failed to commit	
WS: WU SIP DISABLE: WS			
%S.%d SIP SET CONF. %S		nimfNetlfaceTbHandler: unable to get LedPinid	
Failed to open %s. %s			
Failed to start sipalg		%S. Unable to Kill Unclient	
Failed to stop sipalg		nimiAdvOptSetWrap, unable to get current Mac Option	
Notwork Mask: 0x%x		nimiAdvOptSetWrap: unable to get current MTU Option	
		nimfAdvOptSetWrap: drable to get current who Option	
Nic DSCr Value. 0X90X		nimiAdvOptSetWrap: unable to get the MTU	
		himiAdvOptSetWrap: driable to get the Wro	
		nimiAdvOptSetWrap: unable to get Mac Address	
Eailed to set config info		himiAdvOptSetWrap: drable to get Mac Address	
		nimfAdvOptSetWrap: failed to get old connectiontype	
schdTblHandlor		nimfAdvOptSetWrap: alled to get old connectiontype	
nPort- %s		nimfAdvOptSetWrap: failed to get old MTLLOption	
pProtocol: %s		nimfAdvOptSetWrap: arror gotting MTLL size	
philotocol. 705		nimiAdvopisetwiap. enorgetting who size	
	DEBUG	nimfOldFieldValueGet: user bas changed MTU size	
nBootEnable: %s		nimf@dvOptSetWrap: failed to get old Port Speed "	
nRsaEnable: %s	DEBUG	nimfAdvOptSetWrap: user has changed Port Speed	
nDsaEnable: %s	DEBUG	nimfAdvOptSetWrap: date has changed for Speed	
pDsaEnable: //s	DEBUG	himfAdvOptSetWrap: user has changed Mac Address "	
nEmptyPassEnable: %s		nimfAdvOptSetWrap: upable to get Mac Address	
nSftnEnable: %c		nimfAdy(OntSat)(/rap:Epiled to DECET the floa	
nSchdEnable: %s		nimfAdvOptSetWrap: interface advanced options railed	
		nimfGetUndateMacElag: upable to get Elag from MacTable	
prinzep. 705		nimfMacGat: Updating MAC address failed	
ws.obopuate event. Table. %S opcode:%d towid:%d	DEDUG	רווידוויאמכשבו. טףטמנוויץ זאר <i>י</i> כ מטטופגא זמוופט	

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 vlanld %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 vlanld %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></subject></logfile></entry></db>	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: guery 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	sglite3_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 guery: %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: LogicallfName: %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 rowld:%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 rowld:%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: Staticlp: %s	DEBUG	writing options.xl2tpd failed	ERROR
pppoeMgmtTblHandler: NetMask: %s	DEBUG	xl2tpdStop failed	ERROR

pppppher/TbHandler Saus (%d) PFR/G writing at/pit.cm/talled PFR/G ppppet/mbleppde/data/sector_returning with starus (%d) DFR/G writing at/pit.cm/talled ERROR ppppet/mbleppde/data/sector_returning with starus (%d) DEBLG st2pd5top failed ERROR ppppet/mbleppde/mblepde/mbleppde/mbleppde/mbleppde/mbleppde/mblepde/mbl	ログメッセージ	緊急度	ログメッセージ	緊急度
ppppb/gmt1bitundler: staus: %d DEU/G witting potions/Etg/failed EROR pppbo/gmt2bity: ppp dial string: %d DEU/G xitzpidstart failed EROR pppb/gmt2bitundler: structing with struce. %d DEU/G xitzpidstart failed EROR pppb/gmt2bitundler: Mur Kid DEU/G xitzpidstart failed EROR pppb/gmt2bitundler: Mur Kid DEU/G xitzpidstart failed EROR pppb/gmt2bitundler: Mur Kid DEU/G xitzpidstart failed EROR pppb/gmt2bitundler: Sitzpidstart failed DEROR EROR EROR pppb/gmt2bitundler: Sitzpidstart failed DEROR DEROR EROR	pppoeMgmtTblHandler: AuthOpt: %d	DEBUG	writing xl2tpd.conf failed	ERROR
poppedable ppd di string %s DEBUG xi2pdSop Piled ERICR poppedAgmtDiblopders/Indier Multigrim DEBUG xi2pdSop Piled ERICR poppedAgmtDiblopders/Indier Multigrim DEBUG xi1pdSop Piled ERICR pripAgmtDiblopders/Indier Multigrim ERICR ERICR ERICR pripAgmtDiblopders Multigrim DEBUG xi1pdSop Piled ERICR pripAgmtDiblopders / Malligrim DEBUG xi1pdSop Piled ERICR pripAgmtDiblopders / Common / Malligrim DEBUG xi1pdSop Piled ERICR pripAgmtDiblopders / Common / Malligrim DEBUG xi1pdSop Piled ERICR pripAgmtDiblopders / Common / Malligrim DEBUG xi1pdSop Piled ERICR pripAgmtDiblopders / Malligrim DEBUG Can't III ppd ERICR pripAgmtDiblopders / Malligrim DEBUG Can't III ppd ERICR	pppoeMgmtTblHandler: Satus: %d	DEBUG	writing options.xl2tpd failed	ERROR
pppppAgmCBUpdateHandler etuning with status % DESUG ski2pdSortPlated EROR ppppAgmCBUpdateHandler, Muridag %d DESUG sqlteSQueyResGet ShiledQuey%a EROR pppMgmCBUpdateHandler, Muridag %d DESUG sqlteSQueyResGet ShiledQuey%a EROR pppMgmCBUpdateHandler, Muridag DEBUG XVtpdStop Tailed EROR pppMgmCBUpdateHandler, Muridag DEBUG XVtpdStop Tailed EROR pppMgmCBUpdateFatemStremStar DEBUG XVtpdStop Tailed EROR pptMgmCBUpdateFatemStremStar DEBUG WittingChapsecrets/RapSecrets failed EROR pptMgmCBUpdateFatemStremStar DEBUG WittingChapsecrets/RapSecrets failed EROR pptMgmCBUpdateFatemStremStar DEBUG WittingChapsecrets/RapSecrets failed EROR pptMgmCBUpdateFatemStremStar DEBUG Cront necessaring Datasetters/RapSecrets failed EROR pptMgmCBUpdateFatemStremStar DEBUG Cront necessaring Datasetters/RapSecrets failed EROR pptMgmCBUpdateFatemStar DEBUG Cront NapDetates Tailed EROR pptMgmCBUpdateFatemStar DEBUG Cront NapDetates Tailed EROR <td>pppoeEnable: ppp dial string: %s</td> <td>DEBUG</td> <td>xl2tpdStop failed</td> <td>ERROR</td>	pppoeEnable: ppp dial string: %s	DEBUG	xl2tpdStop failed	ERROR
pppMgmtTbH lander: Murling: %d DEBUG splites/QueryResGet failed/QueryRes EBROR pppMgmtTbHeander: Murling: %d DEBUG writing: Chapacerest/Pap-Secret salled EBROR pppMgmtTbHeander: IdeTimeOutValue %d DEBUG StypStster tailed EBROR pppMgmtTbHeander: IdeTimeOutValue %d DEBUG StypStster tailed EBROR pptMgmtTbHeander: GetDimForms %d DEBUG StypStster tailed EBROR pptMgmtTbHeander: UsenName %s DEBUG StypStster tailed EBROR pptMgmtTbHeander: Myperantigueed DEBUG StypStster tailed EBROR pptMgmtTbHeander: StypMgmtTbHeander: Styp	pppoeMgmtDBUpdateHandler: returning with status: %s	DEBUG	xl2tpdStart failed	ERROR
pppMgmtTbHander:Mursid DEBUG writing Chap secrets/Pap Secrets failed DEROR pppMgmtTbHander:IdETImeOutFlag:Wid DEBUG M2tpStop failed EROR pppMgmtTbHander.IdETImeOutFlag:Wid DEBUG M2tpStop failed EROR pppMgmtTbHander.GetDimSroniss; %d DEBUG writing Chap-Secrets/Rap-	pptpMgmtTblHandler: MtuFlag: %d	DEBUG	sqlite3QueryResGet failed.Query:%s	ERROR
pppAgmit bilandle: clebinecoursaux sed DBBUG si2tpdStap failed ERROR pppAgmit bilandle: CdEbin Froncoursaux sed DBBUG si2tpdStap failed ERROR pppAgmit bilandle: CdEbin Froncoursaux sed DBBUG si2tpdStap failed ERROR pppAgmit bilandle: CdEbin Froncoursaux sed DBBUG si2tpdStap failed ERROR pppAgmit bilandle: Devande K% DBBUG si2tpdStap failed ERROR pppAgmit bilandle: Asword sed DBBUG si2tpdStap failed ERROR ERROR pppAgmit bilandle: Scorarig kis DBBUG Error in executing DB update handler ERROR pppAgmit bilandle: Scorarig kis DBBUG Error in executing DB update handler ERROR pppAgmit bilandle: Scorarig kis DBBUG Error in executing DB update handler ERROR pppAgmit bilandle: Scorarig kis DBBUG Can't kll pptad ERROR pppAgmit bilandle: Scorarig kis DBBUG Can't kll pptad ERROR pppAgmit bilandle: sed DBBUG Can't kll pptad ERROR pppAgmit bilandle: sed DBBUG Can't kll pptad ERROR	pptpMgmtTblHandler: Mtu: %d	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
ppppAgent biskandler, idle ineQuitValue, %id DFBUG slitpdStart failed ERKR pppAgent biskandler, Skethamer %in DFBUG sqitbdStappeRsecrets/Pag-Secrests/Pag-Secrests/Pag-Secrets/Pag-Secrets/Pag-Secrets/Pag-Secrets	pptpMgmtTblHandler: IdleTimeOutFlag: %d	DEBUG	xl2tpdStop failed	ERROR
ppppMgmtTbHandler, GetDnsFromisp: %d DEBUG sqlte3QueryResGet failed QueryRes ERROR pppMgmtTbHandler, Password: %s DEBUG writing Chap-secrets/Pas-Secrets failed ERROR pppMgmtTbHandler, Password: %s DEBUG st2pd5tagn tabled ERROR pppMgmtTbHandler, Password: %s DEBUG st2pd5tagn tabled ERROR pptMgmtTbHandler, Severigr, %s DEBUG st2pd5tagn tabled ERROR pptMgmtTbHandler, Severigr, %s DEBUG Error in executing D8 update handler ERROR pptMgmtTbHandler, Severigr, %s DEBUG Can't kill pptd ERROR pptMgmtTbHandler, Severigr, %s DE	pptpMgmtTblHandler: IdleTimeOutValue: %d	DEBUG	xl2tpdStart failed	ERROR
pppt/gem/Tbillandler, Name, MA DEBUG writing Chap secret/Pap Secrets failed ERROR ppt/gem/Tbillandler, Synamic Myle contigured DEBUG M2/pdStrp failed ERROR ppt/gem/Tbillandler, Synamic Myle contigured DEBUG Satito SQueryKis ERROR ppt/gem/Tbillandler, Synamic Myle contigured DEBUG Satito SQueryKis ERROR ppt/gem/Tbillandler, Staticity, %is DEBUG Error in executing OB update handler ERROR ppt/gem/Tbillandler, Staticity, %is DEBUG Carr's Ill pptrof ERROR ERROR ppt/gem/Tbillandler, Mperinceppt/support; %is DEBUG Carr's Ill pptrof ERROR ERROR ppt/gem/Tbillandler, Staticity, %is DEBUG Laled to get field value ERROR ERROR ppt/gem/Tbillandler, Staticity, %is DEBUG Laled to get field value ERROR ERROR ppt/gem/Tbillandler, Muellandler, Russiang, 7%is DEBUG writing options ppt/gem/Tbillandler, Russiang, 7%is EBROR ppt/gem/Tbillandler, Muellag, 7Md DEBUG writing options ppt/gem/Tbillandler ERROR ppt/gem/Tbillandler, Muellag, 7Md DEBUG writing options, pptpd faile	pptpMgmtTblHandler: GetDnsFromIsp: %d	DEBUG	sglite3QueryResGet failed.Query:%s	ERROR
ppptpMgmtTbHandler: Password:%s DEBUG xi2tpdStop failed ERROR pptpMgmtTbHandler: Myrb configured DEBUG xi2tpdStop failed ERROR pptpMgmtTbHandler: Myrb configured DEBUG xitptogCaseStatiledQuery%s ERROR pptpMgmtTbHandler: Statil.op:%s DEBUG Error in executing DB update handler ERROR pptpMgmtTbHandler: NetWask %s DEBUG Error in executing DB update handler ERROR pptpMgmtTbHandler: Split Junnel: %s DEBUG Can't kill pptpd ERROR pptpMgmtTbHandler: Split Junnel: %s DEBUG Can't kill pptpd ERROR pptpTable: ppt failed intring: %s DEBUG Galext tog effeld value ERROR pptpTable: ppt failed intring: %s DEBUG Galext tog effeld value ERROR pptpMgmtTbHandler: Augestrating: %s DEBUG winting options.pptpd failed ERROR pptpMgmtTbHandler: Muring: %s DEBUG winting options.pptpd failed ERROR pptpMgmtTbHandler: Muring: %s DEBUG winting options.pptpd failed ERROR disped/mgmtTbHandler: Muring: %s DEBUG winting options.pptpd failed ERROR	pptpMgmtTblHandler: UserName: %s	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
pppMgmtTbHandler.dynamic Mylp configured DEBUG xl2tpdStart failed ERROR pppMgmtTbHandler.Sevelp.% DEBUG sqlite3QueryResGet failed QueryNis ERROR pppMgmtTbHandler.Sevelp.% DEBUG tron in executing D8 update handler ERROR pppMgmtTbHandler.Staticlp.% DEBUG unto conservertyRap-Secrets failed ERROR pppMgmtTbHandler.MpeEncryptSupport.% DEBUG Can't kill pppd ERROR pptMgmtTbHandler.MpeEncryptSupport.% DEBUG Can't kill pppd ERROR pptMgmtTbHandler.MpeEncryptSupport.% DEBUG Can't kill pptd ERROR pptfDable.sppanning command %s DEBUG failed to get field value ERROR PID Fie for dhcpc found DEBUG inition gotions.pptpd failed ERROR pptMgmtTBHandler.spwming command %s DEBUG writing options.pptpd failed ERROR pptMgmtTBHandler.spwming command %s DEBUG writing options.pptpd failed ERROR pptMgmtTBHandler.Mullagi %d DEBUG pptpdStopTailed ERROR dicpcMgmtTBHandler.Mullagi %d DEBUG pptpdStopTailed ERROR l	pptpMgmtTblHandler: Password: %s	DEBUG	xl2tpdStop failed	ERROR
pppMgmtTbitAndler: Mylp: % DFBUG sqite3QueyResGet tailed,QueyResGet tailed,ResGR FRROR pppMgmtTbitAndler: NetMask: % DFBUG Cran't kill pppd FRROR pptMgmtTbitAndler: NetMask: % DFBUG Can't kill pppd FRROR pptMgmtTbitAndler: NetMask: % DEBUG Can't kill pppd FRROR pptMgmtTbitAndler: SplitTunnel: %s DEBUG Can't kill pppd FRROR pptMgmtTbitAndler: SplitTunnel: %s DEBUG Can't kill pppd FRROR pptMgmtTbitAndler: SplitTunnel: %s DEBUG failed to get field value ERROR pptMgmtTbitAndler: Muray %si DEBUG urbitaget field value ERROR pptMgmtTbitAndler: Muray %si DEBUG writing options pptpd failed ERROR pptMgmtTbitAndler: Muray %si DEBUG writing options pptpd failed ERROR pptMgmtTbitAndler: Muray %si DEBUG writing options pptpd failed ERROR dipceMeastExest choper release command; %s DEBUG pptpdSyntTbitandler	pptpMgmtTblHandler: dynamic Mylp configured	DEBUG	xl2tpdStart failed	ERROR
pripMgmTbHandler: Servelp: %s DEBUG writing Chap-secrets/Pap-Secrets failed ERROR pripMgmTbHandler: Networks: %s DEBUG unbound/mm: unable to open the ' ERROR pripMgmTbHandler: Networks: %s DEBUG Can't kill pptpd ERROR ERROR pripMgmTbHandler: Networks: %s DEBUG Can't kill pptpd ERROR ERROR pripTohole: pptg olid string: %s DEBUG Can't kill pptpd ERROR ERROR pripTohole: pptg olid string: %s DEBUG Can't kill pptpd ERROR ERROR PID File for dhttp: found DEBUG failed to get field value ERROR ERROR pripTohole: pptg DEBUG failed to get field value ERROR ERROR pripMgmtDBUpdateHandler: returning with status: %s DEBUG writing options.pptpd failed ERROR dhcpcReivasid: exe dhcpc release: command: %s DEBUG pripdSomtDBUpdateHandler: Rut %d DEBUG pripdSomtDBUpdateHandler: Rut %d DEBUG pripdSomtDBUpdateHandler: Rut %d ERROR DFCMoS converstred Serverstred DEBUG propdSop failed ERROR DF	pptpMgmtTblHandler: Mvlp: %s	DEBUG	sglite3OuervResGet failed.Ouerv:%s	ERROR
pppMgmTDHandler. Staticly % DEBUG Error in executing DB update handler ERROR pppMgmTDHLandler. NetMask.%is DFBUG Can't kli pppd ERROR pptMgmTDHLandler. NpeEncryptUpport.%is DEBUG Can't kli pptpd ERROR pptMgmTDHLandler. SplitUmmet.%is DEBUG Can't kli pptpd ERROR pptpLonable: ppa dial string: %is DEBUG failed to get field value ERROR pptpLonable: ppa dial string: %is DEBUG failed to get field value ERROR pptMgmTDHLandler: query string: %is DEBUG writing options.pptpd failed ERROR pptMgmTDHLandler: Murplag: %id DEBUG intig options.pptpd failed ERROR dhcpcMgmTDHLandler: Murplag: %id DEBUG intig options.pptpd failed ERROR dhcpcMgmTDHLandler: Murplag: %id DEBUG intig options.pptpd failed ERROR dhcpcMgmTDHLandler: Murplag: %id DEBUG intig options.pptpd failed ERROR DHCMvG Client stared successfully. DEBUG intig options.pptpd failed ERROR DHCMvG Client stared successfully. DEBUG intig options.pptpd failed ERROR </td <td>pptpMgmtTblHandler: ServerIp: %s</td> <td>DEBUG</td> <td>writing Chap-secrets/Pap-Secrets failed</td> <td>ERROR</td>	pptpMgmtTblHandler: ServerIp: %s	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
pripMigmtTbHandler. NetMask: %s DEBUG unboundMgmt: inable to open the " ERNOR pripMigmtTbHandler. Splitfumet %s DEBUG port kill porpd ERNOR ERNOR pptMigmtTbHandler. Splitfumet %s DEBUG Can't kill porpd ERNOR ERNOR pptMigmtTbHandler. Splitfumet %s DEBUG Can't kill porpd ERNOR ERNOR pptMigmtTbHandler. Splitfumet %s DEBUG Failed to get field value ERNOR ERNOR pitAgmtTbHandler. SplitfumtTbHandler. Query string: %s DEBUG field to get field value ERNOR pptMigmtTbHandler. Murely: %d DEBUG pripMigmtTbHandler. Murely: %d DEBUG writing options.pptpd failed ERNOR dhcpcMgmtTbHandler. Murely: %d DEBUG pripMigmtTbHandler. Murely: %d DEBUG pripMigmtTbHandler. Murely: %d ERNOR DHCPV6 Server stanted successfully. DEBUG pripMigmtTbHandler. Murely: %d ERNOR ERNOR DHCPV6 Server stanted successfully. DEBUG pripMigmtTbHandler. Murely: %d ERNOR DHCPV6 Clenx stopped successfully. DEBUG pripMigmtTbHandler. Murely: %d ERNOR D	pptpMgmtTblHandler: Staticlp: %s	DEBUG	Error in executing DB update handler	ERROR
DPD/MgmTbHandler: MppeFncyptSupport: %s DEBUG Can't kill potpd ERKOR pptpMgmTbHandler: SplitTunnet: %s DEBUG pptpd restart failed ERKOR pptpEnable: ppp dial string: %s DEBUG failed to get field value ERKOR pptpEnable: spawning command %s DEBUG failed to get field value ERKOR PID File for dhcpc found DEBUG failed to get field value ERKOR pptpMgmtDBUpdateHandler: returning with status: %s DEBUG writing options.pptpd failed ERKOR pptpMgmtDBUpdateHandler: returning with status: %s DEBUG writing options.pptpd failed ERKOR dhcpcMgmtDBUpdateHandler: Mtu:%d DEBUG writing options.pptpd failed ERKOR dhcpcMgmtDBUpdateHandler: Mtu:%d DEBUG pptpdSart failed ERKOR DHCPv6 Server started successfully. DEBUG pptpdSart failed ERKOR DHCPv6 Client stoped successfully. DEBUG pptpdSart failed ERKOR DHCPv6 Client stoped successfully. DEBUG pptpodWgmtTibHandler: Mtu/Hag: %d DEBUG pptpodWgmtTibHandler: Mtu/Hag: %d DEBUG DHCPv6 Client stoped successfully. </td <td>pptpMgmtTblHandler: NetMask: %s</td> <td>DEBUG</td> <td>unboundMamt: unable to open the "</td> <td>ERROR</td>	pptpMgmtTblHandler: NetMask: %s	DEBUG	unboundMamt: unable to open the "	ERROR
DFDV DEBUG DPDV DEBUG DEBUG ERROR DPptpMamTbHandler: SplitTunnel: %s DEBUG Can't kill potpd ERROR DP1File or dhepc found DEBUG failed to get field value ERROR DP1File or dhepc found DEBUG failed to get field value ERROR pptpMamDBUpdateHandler: query string: %s DEBUG unboundMgmt: unable to open the * ERROR pptpMamDBUpdateHandler: returning with status: %s DEBUG writing options.pptpd failed ERROR dhcpcMgmtTbHandler: Muti%g DEBUG writing options.pptpd failed ERROR dhcpcMgmtTbHandler: Muti%d DEBUG writing options.pptpd failed ERROR DICMo Server stored successfully. DEBUG writing Chapescrets/Pap-Secrets failed ERROR DICMo Server stored successfully. DEBUG pptpotstat/pate: unable to get hed atlates ERROR DICMo Server stored successfully. DEBUG pptpotstat/pate: unable to get hed atlates ERROR DICMo Server stored successfully. DEBUG pppcoMgmtTbHandler.Mtu?Mate ERROR DICMo Server stored successfully. DEBUG	pptpMgmtTblHandler: MppeEncryptSupport: %s	DEBUG	Can't kill pptpd	ERROR
Deptipertable Deptiperable Deptipera	pptpMgmtTblHandler: SplitTunnel: %s	DEBUG	pptpd restart failed	ERROR
Protect DEBUG Failed to get field value ERROR PID File for dhcpc found DEBUG failed to get field value ERROR PID File for dhcpc found DEBUG unboundMgmt: unable to open the " ERROR pitd %d DEBUG writing options.ptpdfofaild ERROR pptpMgmtDBUpdateHandler: returning with status: %s DEBUG writing options.pptpdfaild ERROR dhcpcMgmtDHLandler. MtuFlag: %d DEBUG writing options.pptpd failed ERROR dhcpcMgmtDHLandler. MtuFlag: %d DEBUG writing options.pptpd failed ERROR DHCPVo Server started successfully. DEBUG pptpdStabt failed ERROR DHCPvo Client started successfully. DEBUG pptpdStabt failed ERROR DHCPvo Client started successfully. DEBUG pppeoMgmtDHLandler: MuTU ERROR DHCPvo Client started successfully. DEBUG pppeoMgmtDHLandler: MuTU ERROR DtPVo Client started successfully. DEBUG pppeoMgmtDHLandler: MuTU ERROR DtPMgmtDHLandler: MuFlag: %d DEBUG pppeoMgmtDHLandler: MuTU ERROR DtPMgmtDHLan	pptpEnable: ppp dial string: %s	DEBUG	Can't kill pptpd	FRROR
Profile Profile <t< td=""><td>pptpEnable: spawning command %s</td><td>DEBUG</td><td>failed to get field value</td><td>ERROR</td></t<>	pptpEnable: spawning command %s	DEBUG	failed to get field value	ERROR
pid:%id DEBUG UnboundMgmt unable to open the * ERROR pptpMgmtDBUpdateHandler:querystring:%s DEBUG writing options.pptpd failed ERROR pptpMgmtDBUpdateHandler:reuerystring:%s DEBUG writing options.pptpd failed ERROR dhcpcReleaseLease: dhcpc release command: %s DEBUG writing options.pptpd failed ERROR dhcpcMgmtTDIHandler: MtuFlag:%d DEBUG writing options.pptpd failed ERROR dhcpcMgmtTDIHandler: MtuFlag:%d DEBUG pptpdStor failed ERROR DHCPv6 Server started successfully. DEBUG pptpdStor failed ERROR DHCPv6 Client started successfully. DEBUG pptpfattpdate: unable to open the database file %s ERROR DHCPv6 Client storped successfully. DEBUG pppoeMgmtTiHuable: to apen the database file %s ERROR DHCPv6 Client storped successfully. DEBUG pppoeMgmtTiHuable: unable to apen the database file %s ERROR DtPv6 Client Restar successful DEBUG pppoeMgmtTiHuable: unable to apen the database file %s ERROR DtPv6 Glient Starte: not specified DEBUG pppoeMgmtTiHuable: unable to apen the database file %s ERROR DtpMgmtTiHandler: Muri%d DEBUG pppoeMgmtTiHuable: unable to apen the database file %s ERROR DtpMgmtTiHandler: Seret: mos specified DEBUG <t< td=""><td>PID File for dhopc found</td><td>DEBUG</td><td>failed to get field value</td><td>ERROR</td></t<>	PID File for dhopc found	DEBUG	failed to get field value	ERROR
ptptMgmtD8UpdateHandler: query string: %s DEBUG writing options.pptpd failed ERROR pptpMgmtD8UpdateHandler: returning with status: %s DEBUG pptpdStop failed ERROR dhcpcMgmtTbHandler: NurFlag: %d DEBUG writing options.pptpd failed ERROR dhcpcMgmtTbHandler: MurFlag: %d DEBUG writing options.pptpd failed ERROR dhcpcMgmtTbHandler: MurFlag: %d DEBUG pptpdStop failed ERROR DHCPv6 Server started successfully. DEBUG pptpdStatt failed ERROR DHCPv6 Client started successfully. DEBUG pptpdStatt failed ERROR DHCPv6 Client Restart successfull DEBUG pppoeMgmtInit: unable to get default MTU ERROR DHCPv6 Client Restart successful DEBUG pppoeMultipleEnableDisable: pppoe anable failed ERROR DtpMgmtTbHandler: Mur %d DEBUG pppoeMultipleEnableDisable: pppoe disable failed ERROR DtpMgmtTbHandler: Start successfull DEBUG pppoeMultipleEnableDisable: pppoe disable failed ERROR DtpMgmtTbHandler: Mur %d DEBUG pppoeMgmtTbHandler: unable to get the Mtu ERROR DtpMgmtTbHandler: Start: %s	pid: %d	DEBUG	unboundMamt: unable to open the "	ERROR
printprintprintprintprintprintprintprintprintprintprintprintdhcpcKeleaseLease: dhcpc release command: %sDEBUGwriting pptid.conf failedERRORdhcpcKgmtTblHandler: MtuFlag: %dDEBUGprinting pptid.conf failedERRORdhcpcKgmtTblHandler: MtuFlag: %dDEBUGpptidStop failedERRORDHCPv6 Server started successfully.DEBUGpptidStaft failedERRORDHCPv6 Client started successfully.DEBUGpror or executing DB update handlerERRORDHCPv6 Client stopped successfully.DEBUGpppoeMgmthit: unable to ogen the database file %sERRORDHCPv6 Client stopped successfulDEBUGpppoeMgmthit: unable to kill ppt daemonERRORDHCPv6 Client stopped successfulDEBUGpppoeMgmthit: unable to kill ppt daemonERRORDtCPv6 Client stopped successfulDEBUGpppoeMgmthit: unable to kill ppt daemonERRORDtPv6 Client stopped successfulDEBUGpppoeMgmthit: unable to get uternt Mtu OptionERRORDtpMgmtTblHandler: Nurs%dDEBUGpppoeMgmtTblHandler: unable to get uternt Mtu OptionERRORDtpMgmtTblHandler: SpName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERRORDtpMgmtTblHandler: SpName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERRORDtpMgmtTblHandler: SpName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERRORDtpMgmtTblHandler: SpName: %sDEBUGppppeMgmtTblHandler: SpName: %sERRO	pptpMgmtDBUpdateHandler: guery string: %s	DEBUG	writing options optiod failed	FRROR
processprocessprocessprocessprocessdhcpcMeaseLease:dhcpcMgmtTblHandler:Mturing options.pptpd failedERRORdhcpcMgmtTblHandler:MturingDEBUGpytpdStorp failedERRORDHCPv6 Server started successfully.DEBUGpptpdStart failedERRORDHCPv6 Server storped successfully.DEBUGprotedStorp failedERRORDHCPv6 Client started successfully.DEBUGprotedStorp failedERRORDHCPv6 Client storped successfully.DEBUGprotedStart failedERRORDHCPv6 Client storped successfully.DEBUGprotedStart unable to get default MTUERRORDHCPv6 Client storped successfully.DEBUGpppceMgmtThitunable to get default MTUERRORDtpMgmtTDiHandler:IspName: %sDEBUGpppceMgmtTbiHandler: unable to get defaultERRORDtpMgmtTDiHandler:IspName: %sDEBUGpppceMgmtTbiHandler: unable to get the MtuERRORDtpMgmtTDiHandler:Secret: not specifiedDEBUGpppceMgmtTbiHandler: represenable failedERRORDtpMgmtTDiHandler:Secret: not specifiedDEBUGpppceMgmtTbiHandler: represenable failedERRORDtpMgmtTDiHandler:Secret: not specifiedDEBUGpppceMgmtTbiHandler: r	pptpMgmtDBUpdateHandler: returning with status: %s	DEBUG	pptpdStop failed	ERROR
dispeckgmtTbHandler: MturBag: %dDEBUGwriting options.pptpd failedERRORdispeckgmtTbHandler: Mtur %dDEBUGpptpdStop failedERRORDHCPv6 Server started successfully.DEBUGpptpdStart failedERRORDHCPv6 Server started successfully.DEBUGpptpdStart failedERRORDHCPv6 Client started successfully.DEBUGpror in executing DB update handlerERRORDHCPv6 Client started successfully.DEBUGpppoeMgmtInit: unable to get default MTUERRORDHCPv6 Client Restart successfulDEBUGpppoeMgmtInit: unable to get default MTUERRORDHCPv6 Client Restart successfulDEBUGpppoeMgmtInit: unable to get default MTUERROR12tpMgmtTbHandler: MtuFlag: %dDEBUGpppoeMgmtInit: unable to get default MTUERROR12tpMgmtTbHandler: MturBag: %dDEBUGpppoeMultiplEEnableDisable: pppoe enable failedERROR12tpMgmtTbHandler: Sture %dDEBUGpppoeMgmtTbHandler: unable to get current Mtu OptionERROR12tpMgmtTbHandler: AccountName: %sDEBUGpppoeMgmtTbHandler: unable to get the MtuERROR12tpMgmtTbHandler: AccountName: %sDEBUGpppoeMgmtDBHpdateHandler: failed query: %sERROR12tpMgmtTbHandler: Secret: %sDEBUGpppoeMgmtDBHpdateHandler: failed query: %sERROR12tpMgmtTbHandler: Secret: %sDEBUGpptpEnable: error executing command: %sERROR12tpMgmtTbHandler: Secret: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTbHandler: Secret: %sDEBUGpptpEnable: error executing	dhcpcBeleasel ease: dhcpc release command: %s	DEBUG	writing pptpd conf failed	FRROR
InterportDescDescDescDescDHCPv6 Server started successfully.DEBUGpptpdStart failedERRORDHCPv6 Server storped successfully.DEBUGpptpdStart failedERRORDHCPv6 Client started successfully.DEBUGError in executing DB update handlerERRORDHCPv6 Client started successfully.DEBUGpppotatsupdate: unable to get default MTUERRORDHCPv6 Client storped successfully.DEBUGpppoeMymthit: unable to get default MTUERRORDHCPv6 Client storped successfully.DEBUGpppoeMymthit: unable to get default MTUERRORDHCPv6 Client storped successfully.DEBUGpppoeMymthit: unable to get default MTUERRORDtCPv6 Client storped successfully.DEBUGpppoeMymthit: unable to get default MTUERRORDtQmgmTbHandler: Nursign.NoDEBUGpppoeMymthit: unable to get default MTUERRORDtpMgmTbHandler: IspName: %sDEBUGpppoeMymthitieEnableDisable: pppoe enable failedERRORDtpMgmTbHandler: AccountName: %sDEBUGpppoeMymtTbHandler: unable to get current Mtu OptionERRORDtpMgmTbHandler: AccountName: %sDEBUGpppoeMymtTbHandler: failed query. %sERRORDtpMgmtTbHandler: Secret: not specifiedDEBUGpptptpmable: error error in executing *ERRORDtpMgmtTbHandler: dynamic Mylp configuredDEBUGpptpEnable: error executing command: %sERRORDtpMgmtTbHandler: serverip: %sDEBUGpptptpmable: inteaton failedERRORDtpMgmtTbHandler: NetMask: %sDEBUGpptptp	dhcpcMgmtTblHandler: MtuFlag: %d	DEBUG	writing options option failed	FRROR
DHCPv6 Server started successfully. DEBUG pptpdStart failed ERROR DHCPv6 Server started successfully. DEBUG writing Chap-secrets/Pap-Secrets failed ERROR DHCPv6 Client started successfully. DEBUG provine executing DB update handler ERROR DHCPv6 Client started successfully. DEBUG ppopelytatsUpdate: unable to get default MTU ERROR DHCPv6 Client started successfully. DEBUG pppoeMgmthit: unable to open the database file %s ERROR DHCPv6 Client started successfully. DEBUG pppoeMgmthit: unable to open the database file %s ERROR 12tpMgmtTDlHandler: Mtu:%d DEBUG pppoeMultipleEnableDisable: pppoe disable failed ERROR 12tpMgmtTDlHandler: UserName: %s DEBUG pppoeMgmtTblHandler: unable to get urrent Mtu Option ERROR 12tpMgmtTDlHandler: SpName: %s DEBUG pppoeMgmtTblHandler: unable to get the Mtu ERROR 12tpMgmtTDlHandler: Secret: %s DEBUG pppoeMgmtTblHandler: unable to get the Mtu ERROR 12tpMgmtTDlHandler: Secret: not specified DEBUG pppoeMgmtTblHandler: unable to get the Mtu ERROR 12tpMgmtTDlHandler: Secret: %s DEBUG pppoeMgmtTblHandler: unable to get the Mtu ERROR 12tpMgmtTDlHandler: Secret: %s DEBUG pppoeMgmtTblHandler: error in executing "ERROR 12tpMgmtTDlHandler: Secret: %s DEBUG pppoeMgmtTblHandler: error in executing "ERROR 12tpMgmtTDlHandler: Secret: %s DEBUG pppoeMgmtTblHandler: error in executing "ERROR 12tpMgmtTDlHandler: Secret: %s DEBUG pptpEnable: error executing command: %s ERROR 12tpMgmtTDlHandler: Secret: %s DEBUG pptpEnable: error executing command: %s ERROR 12tpMgmtTDlHandler: SplitTunnet: %s DEBUG pptpEnable: inet_aton failed ERROR 12tpMgmtTDlHandler: %s DEBUG pptpEnable: inet_aton failed ERROR 12tpMgmtTDlHandler: SplitTunnet: %s DEBUG pptpMgmtTDlHandler: unable to get the Mtu ERROR 12tpMgmtTDlHandler: SplitTunnet: %s DEBUG pptpMgmtTDlHandler: unable to get turnet Mtu Option ERRO	dhcpcMgmtTblHandler: Mtu: %d	DEBUG	pptpdStop failed	FRROR
DHCPv6 Server stopped successfully DHCPv6 Client started successfully. DHCPv6 Client started successfully. DHCPv6 Client started successfully. DHCPv6 Client stopped successfully. DHCPv6 Client stopped successfull. DHCPv6 Client festart successful DHCPv6 Client Restart successful DHCPv6 DepeedMultipleEnableDisable: pppoe enable failed ERROR DHCPv6 DepeedMultipleEnable: Pappoe Restart Successful DHCPv6 DepeedMultipleEnable: Pappoe Restart Successful DHCPv6 DepeedMultipleEnable: Pappoe Restart Successful DHCPv6 DepeedMultipleEnable: Pappoe Restart Successful DHCPv6 DepeedMultipleEnable: Successful DHCPv6 DepeedMul	DHCPv6 Server started successfully	DEBUG	pptpdStart failed	FRROR
DHCPv6 Client started successfully.DEBUGError in executing DB update handlerERRORDHCPv6 Client started successfully.DEBUGpppStatsUpdate: unable to get default MTUERRORDHCPv6 Client Restart successfulDEBUGpppoeMgmtInit: unable to open the database file %sERROR12tpMgmtTblHandler: MtuFlag: %dDEBUGpppoeMgmtInit: unable to set with unable to set with unable to get default MTUERROR12tpMgmtTblHandler: Mtu: %dDEBUGpppoeMultipleEnableDisable: pppoe enable failedERROR12tpMgmtTblHandler: IspName: %sDEBUGpppoeMgmtTblHandler: unable to get current Mtu OptionERROR12tpMgmtTblHandler: DerName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERROR12tpMgmtTblHandler: DomainName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERROR12tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtTblUpdateHandler. failed query: %sERROR12tpMgmtTblHandler: Secret: not specifiedDEBUGpptpeMgmtInit: unable to open the database file %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpEnable: error executing command: %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpEnable: unable to resolve address: %sERROR12tpMgmtTblHandler: NetWask:	DHCPv6 Server stopped successfully	DEBUG	writing Chap-secrets/Pap-Secrets failed	ERROR
DHCv6 Client stopped successfully.DEBUGpppStatsUpdate: unable to get default MTUERRORDHCv6 Client Restart successfulDEBUGpppoeMgmtInit: unable to open the database file %sERROR12tpMgmtTblHandler: MtuFlag: %dDEBUGpppoeMultipleEnableDisable: pppoe enable failedERROR12tpMgmtTblHandler: Mtu: %dDEBUGpppoeMultipleEnableDisable: pppoe enable failedERROR12tpMgmtTblHandler: IspName: %sDEBUGpppoeMultipleEnableDisable: pppoe disable failedERROR12tpMgmtTblHandler: UserName: %sDEBUGpppoeMgmtTblHandler: unable to get current Mtu OptionERROR12tpMgmtTblHandler: Sasword: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERROR12tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtTblHandler: nuable to get the MtuERROR12tpMgmtTblHandler: Secret: %sDEBUGpppoeMgmtDBUpdateHandler. failed query: %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpeMgmtInit: unable to open the database file %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptptEnable: error executing command: %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptptEnable: unable to resolve address: %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptptEnable: unable to get urrent Mtu OptionERROR12tpMgmtTblHandler: Secret: %sDEBUGpptptEnable: unable to resolve address: %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptptEnable: unable to resolve address: %sERROR12tpMgmtTblHandler: Staticlp: %sDEBUGpptptEnabl	DHCPv6 Client started successfully.	DEBUG	Error in executing DB update handler	ERROR
DHCPv6 Client Restart successfulDEBUGpppoeMgmtnit: unable to open the database file %sERROR12tpMgmtTblHandler: MtuFlag: %dDEBUGpppoeMgmtnit: unable to open the database file %sERROR12tpMgmtTblHandler: MtuFlag: %dDEBUGpppoeMgmtnit: unable to open the database file %sERROR12tpMgmtTblHandler: Mtu: %dDEBUGpppoeMgmtIplEnableDisable: pppoe enable failedERROR12tpMgmtTblHandler: UserName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERROR12tpMgmtTblHandler: Password: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERROR12tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtTblHandler: failed query: %sERROR12tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtDBUpdateHandler: failed query: %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpeMgmtDBUpdateHandler: reror in executing "ERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpeMgmtDBUpdateHandler: failed query: %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpEnable: error executing command: %sERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler:	DHCPv6 Client stopped successfully.	DEBUG	ppStatsUpdate: unable to get default MTU	ERROR
I2tpMgmtTblHandler: MtuFlag: %dDEBUGpppoeDisable: unable to kill ppp daemonERRORI2tpMgmtTblHandler: Mtu: %dDEBUGpppoeMultipleEnableDisable: pppoe enable failedERRORI2tpMgmtTblHandler: IspName: %sDEBUGpppoeMultipleEnableDisable: pppoe disable failedERRORI2tpMgmtTblHandler: UserName: %sDEBUGpppoeMgmtTblHandler: unable to get current Mtu OptionERRORI2tpMgmtTblHandler: Password: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERRORI2tpMgmtTblHandler: ComainName: %sDEBUGpppoeMgmtTblHandler: pppoe enable failedERRORI2tpMgmtTblHandler: DomainName: %sDEBUGpppoeMgmtTblHandler: pppoe enable failedERRORI2tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtTblHandler: error in executing "ERRORI2tpMgmtTblHandler: Secret: %sDEBUGpptpEnable: error executing command: %sERRORI2tpMgmtTblHandler: Secret: %sDEBUGpptpEnable: unable to resolve address: %sERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpfnable: inet_aton failedERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpfnable: inet_aton failedERRORI2tpMgmtTblHandler: Serverlp: %s<	DHCPv6 Client Bestart successful	DEBUG	pppoeMgmtInit: unable to open the database file %s	ERROR
DipportDipportDipportDipportDipportDEBUGpppoeMultipleEnableDisable: pppoe disable failedERROR12tpMgmtTblHandler: UserName: %sDEBUGpppoeMultipleEnableDisable: pppoe disable failedERROR12tpMgmtTblHandler: UserName: %sDEBUGpppoeMgmtTblHandler: unable to get current Mtu OptionERROR12tpMgmtTblHandler: AccountName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERROR12tpMgmtTblHandler: ComainName: %sDEBUGpppoeMgmtTblHandler: pppoe enable failedERROR12tpMgmtTblHandler: ComainName: %sDEBUGpppoeMgmtDBUpdateHandler: failed query: %sERROR12tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtDBUpdateHandler: error in executing "ERROR12tpMgmtTblHandler: dynamic Mylp configuredDEBUGpptpEnable: error executing command: %sERROR12tpMgmtTblHandler: Mylp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: Mylp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: ServerIp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: Staticip: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: ServerIp: %sDEBUGpptpEnable: nable to get current MTU OptionERROR12tpMgmtTblHandler: Staticip: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERROR12tpMgmtTblHandler: Staticip: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERROR12tpMgmtTblHandler: ServerIp: %sDEBUGpptpMgmt	12tpMgmtTblHandler: MtuElag: %d	DEBUG	pppoeDisable: unable to kill ppp daemon	ERROR
DEBUGPPPOPMUTPLEJ2tpMgmtTblHandler: IspName: %sDEBUGpppoeMultipleEnableDisable: pppoe disable failedERRORI2tpMgmtTblHandler: UserName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERRORI2tpMgmtTblHandler: AccountName: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERRORI2tpMgmtTblHandler: DomainName: %sDEBUGpppoeMgmtTblHandler: pppoe enable failedERRORI2tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtDBUpdateHandler: failed query: %sERRORI2tpMgmtTblHandler: Secret: %sDEBUGpptpeMgmtTblHandler: error in executing "ERRORI2tpMgmtTblHandler: dynamic Mylp configuredDEBUGpptpEnable: error executing command: %sERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpIngmtTblHandler: unable to get turnet MtU OptionERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpMgmtTblHandler: unable to	12tpMgmtTblHandler: Mtu: %d	DEBUG	pppoeMultipleEnableDisable: pppoe enable failed	ERROR
Izpmgmt But Ander Spreak and the second se	12tpMgmtTb Handler: IspName: %s	DEBUG	pppoeMultipleEnableDisable: pppoe disable failed	FRROR
IzppgrtruitDEBUGpppoeMgmtTblHandler: unable to get the MtuERRORIzppMgmtTblHandler: Password: %sDEBUGpppoeMgmtTblHandler: unable to get the MtuERRORIzpMgmtTblHandler: DomainName: %sDEBUGpppoeMgmtTblHandler: failed query: %sERRORIzpMgmtTblHandler: DomainName: %sDEBUGpppoeMgmtDBUpdateHandler: failed query: %sERRORIzpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtDBUpdateHandler: error in executing "ERRORIzpMgmtTblHandler: Secret: %sDEBUGpptptmgmtnit: unable to open the database file %sERRORIzpMgmtTblHandler: dynamic Mylp configuredDEBUGpptptnable: error executing command: %sERRORIzpMgmtTblHandler: Mylp: %sDEBUGpptptnable: unable to resolve address: %sERRORIzpMgmtTblHandler: Severlp: %sDEBUGpptptnable: inet_aton failedERRORIzpMgmtTblHandler: NetMask: %sDEBUGpptptnable: inet_aton failedERRORIzpMgmtTblHandler: NetMask: %sDEBUGpptptnable: inet_aton failedERRORIzpMgmtTblHandler: NetMask: %sDEBUGpptptnable: nuable to kill ppt daemonERRORIzpMgmtTblHandler: NetMask: %sDEBUGpptptnable: nuable to get current MTU OptionERRORIzpMgmtTblHandler: Serverlp: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORIzpMgmtTblHandler: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERRORIzpMgmtTblHandler: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORIzpMgmtTblHandler: %sDEBUG <td< td=""><td>12tpMgmtTblHandler: UserName: %s</td><td>DEBUG</td><td>pppoeMantTblHandler: unable to get current Mtu Option</td><td>FRROR</td></td<>	12tpMgmtTblHandler: UserName: %s	DEBUG	pppoeMantTblHandler: unable to get current Mtu Option	FRROR
IztpMgmtTblHandler: AccountName: %sDEBUGpppoeMgmtTblHandler: pppoe able failedERRORIztpMgmtTblHandler: DomainName: %sDEBUGpppoeMgmtDBUpdateHandler: failed query: %sERRORIztpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtDBUpdateHandler: error in executing "ERRORIztpMgmtTblHandler: Secret: %sDEBUGpptpoeMgmtDBUpdateHandler: error in executing "ERRORIztpMgmtTblHandler: dynamic Mylp configuredDEBUGpptpEnable: error executing command: %sERRORIztpMgmtTblHandler: Mylp: %sDEBUGpptpEnable: unable to resolve address: %sERRORIztpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORIztpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: inet_aton failedERRORIztpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: unable to kill ppt daemonERRORIztpMgmtTblHandler: SplitTunnel: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERRORIztpMgmtTblHandler: SplitTunnel: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORIztpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORIztpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORIztpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORIztpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORIztpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERROR<	12tpMgmtTblHandler: Password: %s	DEBUG	pppoeMamtTblHandler: unable to get the Mtu	ERROR
12tpMgmtTblHandler: DomainName: %sDEBUGpppoeMgmtDBUpdateHandler: failed query: %sERROR12tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtDBUpdateHandler: error in executing "ERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpMgmtInt: unable to open the database file %sERROR12tpMgmtTblHandler: dynamic Mylp configuredDEBUGpptpEnable: error executing command: %sERROR12tpMgmtTblHandler: Mylp: %sDEBUGpptpEnable: unable to resolve address: %sERROR12tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: Nation: Setticlp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpEnable: unable to kill ppp daemonERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERROR12tpEnable: command: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERROR12tpEnable: command: %sD	12tpMgmtTblHandler: AccountName: %s	DEBUG	pppoeMgmtTblHandler: pppoe enable failed	ERROR
12tpMgmtTblHandler: Secret: not specifiedDEBUGpppoeMgmtDBUpdateHandler: error in executing "ERROR12tpMgmtTblHandler: Secret: %sDEBUGpptpMgmtInit: unable to open the database file %sERROR12tpMgmtTblHandler: dynamic Mylp configuredDEBUGpptpEnable: error executing command: %sERROR12tpMgmtTblHandler: Mylp: %sDEBUGpptpEnable: unable to resolve address: %sERROR12tpMgmtTblHandler: ServerIp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: Staticlp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpEnable: unable to kill ppp daemonERROR12tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: date failed for %s "ERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: splite3QueryResGet "ERROR12tpEnable:	12tpMgmtTblHandler: DomainName: %s	DEBUG	pppoeMamtDBUpdateHandler: failed query: %s	ERROR
I2tpMgmtTblHandler: Secret: %sDEBUGpptpMgmtInit: unable to open the database file %sERRORI2tpMgmtTblHandler: dynamic Mylp configuredDEBUGpptpEnable: error executing command: %sERRORI2tpMgmtTblHandler: Mylp: %sDEBUGpptpEnable: unable to resolve address: %sERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Staticlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpEnable: unable to kill ppp daemonERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERRORI2tpEnable: command: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERRORI2tpEnable: command string: %s <td>12tpMgmtTblHandler: Secret: not specified</td> <td>DEBUG</td> <td>pppoeMamtDBUpdateHandler: error in executing "</td> <td>ERROR</td>	12tpMgmtTblHandler: Secret: not specified	DEBUG	pppoeMamtDBUpdateHandler: error in executing "	ERROR
12tpMgmtTblHandler: dynamic Mylp configuredDEBUGpptpEnable: error executing command: %sERROR12tpMgmtTblHandler: Mylp: %sDEBUGpptpEnable: unable to resolve address: %sERROR12tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: Staticlp: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: inet_aton failedERROR12tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpDisable: unable to kill ppp daemonERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: duRecordValueGet failed for %s "ERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: duRecordValueGet failed for %s "ERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERROR12tpMgmtDBlUpdateHandler: guter string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERROR12tpEna	I2tpMgmtTblHandler: Secret: %s	DEBUG	pptpMgmtInit: unable to open the database file %s	ERROR
I2tpMgmtTblHandler: Mylp: %sDEBUGpptpEnable: unable to resolve address: %sERRORI2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Staticlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: spawning failedERRORI2tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpDisable: unable to kill ppp daemonERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: dbRecordValueGet failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: dbRecordValueGet failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERRORI2tpMgmtTblHandler: pptp disable	12tpMgmtTblHandler: dynamic Mylp configured	DEBUG	pptpEnable: error executing command: %s	ERROR
I2tpMgmtTblHandler: Serverlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: Staticlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: spawning failedERRORI2tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpDisable: unable to kill ppp daemonERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: dbRecordValueGet failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: dbRecordValueGet failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: spltp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERRORI2tpMgmtDBUpdateHandler: ouery string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERRORI2tpMgmtDBUpdateHandler: ouery string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERRORI2tpMgmtDBUpdateHandler: ouery string: %sDEBUGpptpMgmtDBUpdateHandler: splte3QueryResGet "ERROR </td <td>12tpMgmtTblHandler: Mylp: %s</td> <td>DEBUG</td> <td>pptpEnable: unable to resolve address: %s</td> <td>ERROR</td>	12tpMgmtTblHandler: Mylp: %s	DEBUG	pptpEnable: unable to resolve address: %s	ERROR
I2tpMgmtTblHandler: Staticlp: %sDEBUGpptpEnable: inet_aton failedERRORI2tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable: spawning failedERRORI2tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpDisable: unable to kill ppp daemonERRORI2tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpDisable: unable to get current MTU OptionERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: optp enable failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp disable failedERRORPID File for dhcpc foundDEBUGpptpMgmtTblHandler: pptp disable failedERRORpid: %dDEBUGpptpMgmtDBUpdateHandler: sqlite3QueryResGet "ERRORI2tpMgmtDBUpdateHandler: guery string: %sDEBUGpptpMgmtDBUpdateHandler: error in executing "ERROR	12tpMgmtTblHandler: ServerIp: %s	DEBUG	pptpEnable: inet_aton failed	ERROR
I2tpMgmtTblHandler: NetMask: %sDEBUGpptpEnable:spawning failedERRORI2tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpDisable: unable to kill ppp daemonERRORI2tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: optp enable failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORPID File for dhcpc foundDEBUGpptpMgmtTblHandler: pptp disable failedERRORpid: %dDEBUGpptpMgmtDBUpdateHandler: sqlite3QueryResGet "ERRORI2tpMgmtDBUpdateHandler: guery string: %sDEBUGpptpMgmtDBUpdateHandler: sqlite3QueryResGet "ERROR	12tpMgmtTblHandler: Staticlp: %s	DEBUG	pptpEnable: inet_aton failed	ERROR
I2tpMgmtTblHandler: SplitTunnel: %sDEBUGpptpDisable: unable to kill ppp daemonERRORneedToStartHealthMonitor: returning with status: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORPID File for dhcpc foundDEBUGpptpMgmtTblHandler: pptp disable failedERRORpid: %dDEBUGpptpMgmtDBUpdateHandler: sqlite3QueryResGet "ERRORI2tpMgmtDBUpdateHandler: query string: %sDEBUGpptpMgmtDBUpdateHandler: error in executing "ERROR	12tpMgmtTblHandler: NetMask: %s	DEBUG	pptpEnable:spawning failed	ERROR
needToStartHealthMonitor: returning with status: %sDEBUGpptpMgmtTblHandler: unable to get current MTU OptionERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERROR12tpEnable: command: %sDEBUGpptpMgmtTblHandler: dbRecordValueGet failed for %s "ERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failed for %s "ERROR12tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORPID File for dhcpc foundDEBUGpptpMgmtTblHandler: pptp disable failedERRORpid: %dDEBUGpptpMgmtDBUpdateHandler: sqlite3QueryResGet "ERROR12tpMgmtDBUpdateHandler: guery string: %sDEBUGpptpMgmtDBUpdateHandler: error in executing "ERROR	l2tpMgmtTblHandler: SplitTunnel: %s	DEBUG	pptpDisable: unable to kill ppp daemon	ERROR
I2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: unable to get the MtuERRORI2tpEnable: command: %sDEBUGpptpMgmtTblHandler: dbRecordValueGet failed for %s "ERRORI2tpEnable: command string: %sDEBUGpptpMgmtTblHandler: pptp enable failedERRORPID File for dhcpc foundDEBUGpptpMgmtTblHandler: pptp disable failedERRORpid: %dDEBUGpptpMgmtTblHandler: sqlite3QueryResGet "ERRORI2tpMgmtDBUpdateHandler: guery string: %sDEBUGpptpMgmtDBUpdateHandler: error in executing "ERROR	needToStartHealthMonitor: returning with status: %s	DEBUG	pptpMgmtTblHandler: unable to get current MTU Option	ERROR
I2tpEnable: command: %s DEBUG pptpMgmtTblHandler: dbRecordValueGet failed for %s " ERROR I2tpEnable: 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 I2tpMgmtDBUpdateHandler: query string: %s DEBUG pptpMgmtDBUpdateHandler: error in executing " ERROR	I2tpEnable: command string: %s	DEBUG	pptpMgmtTblHandler: unable to get the Mtu	ERROR
I2tpEnable: 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 I2tpMgmtDBUpdateHandler: guery string: %s DEBUG pptpMgmtDBUpdateHandler: error in executing " ERROR	12tpEnable: command: %s	DEBUG	pptpMgmtTblHandler: dbRecordValueGet failed for %s "	ERROR
PID File for dhcpc found DEBUG pptpMgmtTblHandler: pptp disable failed ERROR pid: %d DEBUG pptpMgmtDBUpdateHandler: sqlite3QueryResGet " ERROR l2tpMgmtDBUpdateHandler: guery string: %s DEBUG pptpMgmtDBUpdateHandler: error in executing " ERROR	12tpEnable: command string: %s	DEBUG	pptpMgmtTblHandler: pptp enable failed	ERROR
pid: %d DEBUG pptpMgmtDBUpdateHandler: sqlite3QueryResGet " ERROR 12tpMgmtDBUpdateHandler: guery string: %s DEBUG pptpMgmtDBUpdateHandler: error in executing " ERROR	PID File for dhcpc found	DEBUG	pptpMgmtTblHandler: pptp disable failed	ERROR
I2tpMgmtDBUpdateHandler: guery string: %s DFRUG ppppmgmt2 = ppater and en optice gaes into optice g	pid: %d	DEBUG	pptpMgmtDBUpdateHandler: sglite3OuervResGet "	ERROR
Teres a second decidence and the second seco	i2tpMgmtDBUpdateHandler: 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
I2tpMgmtTblHandler: disabling I2tp 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

ログメッヤージ	緊急度	ログメッヤージ	婜急度
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
peapEragEirstProcess: 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 reg to WSC failed, status = %d	ERROR
Ext AVP parsed: flags=(0x%x)	DEBUG	eapWscCheck: Invalid frame	ERROR
Mandatory bit not set: WARNING	DEBUG	eapWscBuildReg: 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: Eailed	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 FAP/MS-CHAPv2 context: OK	DEBUG	NULL context created: Error	FRROR
Not authenticated vet	DEBUG	NULL context received: Error	FRROR
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: vendorld-%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
\tldent = %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 rowld:%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></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 Rowld:%d to Server %s:%d with "	DEBUG	Unable to set debug level for radAcct.	ERROR
rowlds: %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 rowld:%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=""></db>	ERROR
Received Invalid Length packet from %s	DEBUG	ntpd : umi initialization failed	ERROR
Received Invalid Version packet from %s	DEBUG	ntpd : ntplnit 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

ログメッヤージ	堅急度	ログメッヤージ	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
Davl johtsaving: %d	DEBUG	Error in executing DB update handler	FRROR
pNtpControl->ServerNames[PRIMARY_SERVER]: %s	DEBUG	requestNtpTime: Invalid addr	ERROR
pNtpControl->ServerNames[SECONDARY_SERVER] · %s	DEBUG	failed to take lock for compld: %d	FRROR
DS: %d	DEBUG	failed to convert joctl args to buffer for"	FRROR
pPriServ %s	DEBUG	request timeout dst(%d) < src(%d)	ERROR
pSecServ %s	DEBUG	failed to take lock for compld: %d	ERROR
Making request from %d> %d	DEBUG	umiloctlArgsToBuf: failed to allocate memory	FRROR
sent request dst(%d) < src(%d) using option %d	DEBUG	umiRecvFrom: could not allocate memory	FRROR
received request too small(%d bytes)	DEBUG	adpMalloc failed	FRROR
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	FRROR
umiBegister (%x.%x.%x)	DEBUG	Failed to create recySem for UMI context	ERROR
srcld=%d(%s)> destId=%d(%s) cmd=%d inLen=%d	DEBUG	Failed to create mutex locks for UMI context	ERROR
outLen=%d			
waiting for replyGiving 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 umiBufToloctlArgs()	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></rowid></tblname></optype></dbfile>	ERROR
USB: returning with status: %s	DEBUG	Illegal invocation of snmpConfig (%s)	ERROR
%s:DBUpdate event: Table: %s opCode:%d rowld:%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 enginelD	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
umilnit 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
umiloctl (%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
umiloctl (%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	umilnit 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

ログメッヤージ	緊急度	ログメッヤージ	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 LogicallfName = %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	DEBUG
Disabling keyword Blocking for %s keyword .	DEBUG	Deleting Port Trigger Rule for %d:%d:%d:%d	DEBUG
Deleting trusted domain with keyword %s.	DEBUG	Enabling Port Trigger Rule for %d:%d:%d:%d	DEBUG
Adding %s keyword to trusted domain.	DEBUG	Disabling Port Trigger Rule for %d:%d:%d:%d	DEBUG

ログメッカージ	取刍由		取刍奋
Enabling Management Access from Internet on port	<u>糸芯反</u> DFRUG	Enabling Port Trigger Bule for %d·%d·%d·%d·%d	<u>条志反</u> DEBUG
Enabling management vices mont internet on port	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	
Disabling remote access management for IP address range"	DEBUG	Disabling Content Filter	DEBUG
Disabling remote access management only to this PC		Enabling Content Filter	
MAC Eiltering %sabled for BLOCK and PERMIT PEST		Setting NAT mode for pl ogicallfName – %s	
MAC Filtering %sabled for DEDUCK and PLINIT REST.		Enabling DPOP for INDUT	
Enabling Content Elitering			
Disabling Content Filtering.			
Disability Content Filtering.		Enabling IVAT based Filewall Rules	
Deleting rule, port triggering for protocol TCP.			
Deleting rule, port triggering for protocol UDP.	DEBUG		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 pLogicalifiname \	DEBUG
Enabling rule, port triggering for protocol TCP.	DEBUG		DEBUG
Enabling rule, port triggering for protocol UDP.	DEBUG		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 pVirtlface %s from ifgroup %d"	DEBUG	fwPPTPGenericRules.c: unable to open the database file "	ERROR
adding interface pVirtlface %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> "</rowid></tblname></optype></dbfile>	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	xIr8NatMgmtTblHandler: failed guery: %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 Keyld	ERROR
Added firewall rule %s for service %s with action %s	DEBUG	Invalid Second Keyld	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 rowld:%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
plfName : %s	DEBUG	iappSockInit() failed	ERROR
iReq.i_val : %d	DEBUG	iappInit got error, unregistering it with UMI	ERROR
setting mode: %d	DEBUG	umiloctl(UMI_COMP_UDOT11,%d,%d) failed	ERROR
Global counter wrapped, re-generating	DEBUG	umiloctl(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	umiloctl(UMI_COMP_KDOT11,	ERROR

ログメッヤージ	堅急度	ログメッセージ	堅急度
PNAC EVENT EAPOL START event received	DEBUG	umiloctl(UMLCOMP_UDOT11.%d.%d))	ERROR
PNAC_EVENT_EAPOL_LOGOFE event received	DEBUG	umiloctI(UMI_COMP_KDOT11.%d.%d.)	ERROR
PNAC EVENT REAUTH event received	DEBUG	No IAPP Node found for reg 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
eapolRecvAuthKevMsg: received key message	DEBUG	cmd %d not supported.sender=%d	ERROR
node not found	DEBUG	umiloctl(UMI_COMP_KDOT11,%d,%d) failed	ERROR
eapolRecyKeyMsg: replay counter not incremented	DEBUG	IAPP-CACHE-NOTIFY-REQUEST send to	ERROR
eapolBecyKeyMsg: replay counter is not same	DEBUG	/src/dot11/iapp/iappl ib c:1314: ADP_ERBOR (FRROR
processing pairwise key message 2	DEBUG	BSSID value passed is NULL	FRROR
RSN IF matching: OK	DEBUG	reserved requestid is passed	FRROR
processing pairwise key message 4	DEBUG	interface name is NULL	FRROR
processing group key message 2	DEBUG	IP address value passed is NULL	FRROR
processing key request message from client	DEBUG	opening receive UDP socket failed	FRROR
WPA version %2x %2x not supported	DEBUG	enabling broadcast for UDP socket failed	FRROR
(%s) group cipher %2x doesn't match	DEBUG	opening receive TCP socket for new AP failed	FRROR
(%s)Pairwise cipher %s not supported	DEBUG	/src/dot11/iapp/iappl ib c:1784: ADP_ERBOR(FRROR
(%s) authentication method %d not supported	DEBUG	/src/dot11/iapp/iapplib.c.1794: ADP_ERBOR(
%:Auth method=%s pairwise cipher=%s IE size=%d	DEBUG	/src/dot11/iapp/iappLib.c.1791;701 _Enrich(FRROR
WPA version %2x %2x not supported	DEBUG	failed created dot11dl ock	
Unable to obtain IE of type %d	DEBUG	failed initialize profile library	FRROR
PTK state changed from %s to %s	DEBUG	failed to create cipher contexts	FRROR
using PMKSA from cache	DEBUG	unable to register to UMI	FRROR
PTK GK state changed from %s to %s	DEBUG	could not create MIB tree	FRROR
GK state changed from %s to %s	DEBUG	unable to register to PNAC	FRROR
Sending PTK Msg1	DEBUG	Max registration attempts by DOT11 to PNAC exceeded	FRROR
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_BX_EAPOL_KEYMSG: unknown ifname %s	ERROR
creating phac 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
ioin 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 OC AUTHMODE failed	ERROR
failed to send PNAC_AUTHORIZED "	DEBUG	KDOT11 SET PARAM:IEEE80211 LOC PRIVACY failed	ERROR
mic verification: OK	DEBUG	wpalnit failed	ERROR
pnaclfConfig: 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
pnaclfConfigUmiloctl: umiloctl failed	DEBUG	AP not found on %s	ERROR
pnaclfConfigUmiloctl: 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
pnaclfConfigUmiloctl: usrPnac returned %d	DEBUG	Invalid profile name passed	ERROR
pnaclfConfigUmiloctl: 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 pnacRadXlateDemoRecy: 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 LOC WME CWMIN failed	ERROR
state changed from %s to %s	DEBUG	KDOT11 SET PARAM:IEEE80211 LOC WME CWMAX failed	ERROR
PNAC user comp id not set, dropping event %d	DEBUG	KDOT11 SET PARAM:IEEE80211 LOC 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 LOC WME ACM failed	ERROR
pnacUmiPortPaeParamSet: error in getting port pae	DEBUG	KDOT11 SET PARAM:IEEE80211 LOC WME failed	ERROR
pnacUmiPortPaeParamSet: invalid param - %d	DEBUG	invalid group cipher %d	ERROR
pnacRecvASInfoMessage: Skey of length %d set	DEBUG	KDOT11 SET PARAM: IEEE80211 LOC 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	dot11PnaclfCreate 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->	DEBUG	dot11Malloc failed	ERROR
authToASSendRtn:%p			
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 pnacTxReg	DEBUG	wpaAuthRecvGTKMsg2: keyDataLength not zero	ERROR
doing pnacTxStart	DEBUG	wpaAuthRecvGTKMsg2: mic check failed	ERROR
doing pnacTxLogoff	DEBUG	wpaAuthRecvKeyReg: unexpected packet received	ERROR
doing pnacTxRspld: 1st cond	DEBUG	wpaAuthRecvKeyReq: keyDataLength not zero	ERROR
doing pnacTxRspld: entering 2nd cond	DEBUG	wpaAuthRecvKeyReg: mic check failed	ERROR
from pnacTxRspld: code = %d, identifier = %d, length = %d, "	DEBUG	invalid OUI %x %x %x	ERROR
doing pnacTxRspld: 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
pnaclfConfig: 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	pnaclsInterfaceUp: failed to create a raw socket	ERROR
adpRand failed:unable to generate random unicast key	WARN	pnaclsInterfaceUp: 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
pnaclfConfig: overwriting previous interface "	WARN	From pnacRadXlateDemoRecv: send "	ERROR
pnaclfConfig: overwriting previous "	WARN	Error from pnacRadXlateDemoRecv: radius "	ERROR
pnaclfConfig: overwriting previous username"	WARN	Error from pnacRadXlateDemoRecv: radius "	ERROR
pnaclfConfig: 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
umilnit 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	pnacUmilnit: 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	pnaclfNameToIndex 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 pnaclsInterfaceUp: 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 pnacSupplnit: 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 pnacTxRspld: 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	pnacUmiloctlHandler: 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	pnacUmilfMacAddrChange: %s not configured for 802.1x	ERROR
sqlite3QueryResGet failed.Query:%s	ERROR	pnacUmilfMacAddrChange: 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	pnacUmilfDown: Invalid config data	ERROR
multiple VAP rows returned. expected one	ERROR	pnacUmilfDown: Invalid config data	ERROR
sqlite3QueryResGet failed	ERROR	Error from pnacPortDeconfig: port not configured	ERROR
invalid query result. ncols=%d nrows=%d	ERROR	pnacUmilfDown: 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	ТКІР	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=""></unknown>	DEBUG

PPH-Induced packet DLBUG dots > fm_string DLBUG PPR-commemory for DEBUG mode %a des > fm_string DLBUG PPR-commemory for DEBUG %anknown subtypes DEBUG MKNUES_COUNT_now %aRINCTONmod_use_county DPRUG %ester	ログメッセージ	緊急度	ログメッセージ	緊急度
PPP: constructed packet DEBUG mode Bits descripting string DEBUG PPP: no memory for DEBUG studiewon subsysse DEBUG PPP: no memory for DEBUG Studiewon subsysse DEBUG Rei MC_LES_CONT_now MdEINCTIONmod_use_rount DEBUG Studies seen_option 7 - 1. DEBUG PPPOL2TP: wisfmit, DEBUG Studies seen_option 7 - 1. DEBUG Studies seen_option 7 - 1. DEBUG Studies and the studies set set set set set set set set set s	PPP: inbound frame not passed	DEBUG	desc->ifmt_string	DEBUG
PPP normanop for DEBUG stanknown abbypes DEBUG missed pkis Suu Sku DEBUG Sku Sko Skin, string DEBUG Min ML, DE, COUNT, row Kd, _=NNCTONmod_use_count DEBUG Sku Sko Skin, pprion++ 7, DEBUG Min ML, String, Think, Tow Kd, _=NNCTONmod_use_count DEBUG Sko Skon, pprion++ 7, DEBUG PPO2.7P -sks,UNCTON DEBUG Sko skon, pprion++ 7, DEBUG PPO2.7P -sks,UNCTON DEBUG Sko rom memory for VAP namel,func DEBUG Sko scon, proston stame DEBUG Sko rom memory for VAP namel,func DEBUG Sko scon, proston stame DEBUG Sko rom scon stame procentry (RMC,tunc DEBUG Sko scon, scon stame DEBUG Sko rom stame stame DEBUG Sko rom stame stame DEBUG PPO2.7P sko,fmi DEBUG Sko rom stame stame DEBUG Sko rom stame stame DEBUG PPO2.7P sko, _fmi DEBUG Fills Sko rom stame stame DEBUG PPO2.7P sko, _fmi DEBUG Fills Sko rom stame stame stame stame DEBUG PPO2.7P	PPP: reconstructed packet	DEBUG	mode %s, desc->ifmt_string	DEBUG
missed pikes yuu, yuu DCBUG %6. disc.: Princ, string DCBUG %6. NGL: USL: COUNT, reversing,	PPP: no memory for	DEBUG	<ur><unknown subtype=""></unknown></ur>	DEBUG
%EINC.USC.COM/I.now/#dUNCTONmod_usc.com/ DEBUG %6x% secn_ppion+1?.; DEBUG %EDE_USE.COM/I.now/#dUNCTONmod_usc.com/ DEBUG %6x% secn_ppion+1?.; DEBUG %EDE_USE.COM/I.now/#dUNCTONmOd_usc.com/ DEBUG %6x% secn_point>1?.; DEBUG %PPOLZTP->%KUNCTON DEBUG %cs.mc.pbin7>5: DEBUG %sc.rom.encory for ysecitable!nnc DEBUG %cs.ncm.encory for ysecitable!nnc DEBUG %sc.rom.encory for ysecitable!nnc DEBUG %cs.ncm.encory for ysecitable!nnc DEBUG %sc.rom.encory for ysecitable!nnc DEBUG %cs.ncm.encory for ysecitable!nnc DEBUG %sc.rom.ession name DEBUG %cs.field to registar special with ysis	missed pkts %u%u,	DEBUG	%s, desc->ifmt_string	DEBUG
Stor DECUSE_COUNT_Now %6(FUNCTION	%s: INC_USE_COUNT, now %d,FUNCTION, mod_use_count \	DEBUG	%s%s, seen_option++?,:,	DEBUG
PPP0.17P av_fmt DPB/G %s, sen_prion 7 >: DPB/G PPP0.17P>%s_FUNCTION	%s: DEC_USE_COUNT, now %d,FUNCTION, mod_use_count \	DEBUG	%s%s, seen_option++?,:,	DEBUG
PPPOL2TP:->KaFUNCTIONDEBUG Visc %s. dev=name.buf DEBUG PPOL2TP:->KaFUNCTIONDEBUG %s. no memory for syscit table!funcDEBUG Ms. no memory for syscit table!funcDEBUG %s. rmls.session-name DEBUG %s. no memory for syscit table!funcDEBUG %s. rmls.session-name DEBUG %s. no memory for new proc entry (%s]uncDEBUG %s. rmls.session-name DEBUG %s. no memory for new proc entry (%s]uncDEBUG PPOL2TP:%smt, DEBUG %s. none_uncNoNo	PPPOL2TP %s: _fmt,	DEBUG	%s, seen_option ? > :	DEBUG
PPPOL2TP: C=NsFUNCTION	PPPOL2TP:> %s,FUNCTION)	DEBUG	%s: %s, dev->name, buf	DEBUG
Site recv., tunnel->name DEBUG %s: no memory for VAP name!funcDEBUG Ms: no memory for VAP name!funcDEBUG %s: mith, session->name DEBUG %s: not memory for New procentiny (%s), _funcDEBUG DEBUG %s: mith, session->name DEBUG %s: not memory for New procentiny (%s), _funcDEBUG DEBUG PPO.12P %c _fmt, DEBUG %s: not memory for New procentiny (%s), _funcDEBUG DEBUG %s: cront, sead, _FUNCTION	PPPOL2TP: < %s,FUNCTION)	DEBUG	%s: no memory for sysctl table!,func	DEBUG
Miss xmlt, session->name DEBUG %s: failed to register systEll, vap.>iv_dev>name DEBUG Miss xmlt, session->name DEBUG Net. nomemory for new proc entry (Net),	%s: recv: , tunnel->name	DEBUG	%s: no memory for VAP name!,func	DEBUG
Nax.mlt.session->name DEBUG %s: no memory for new procentry (%s)(func) DEBUG %s: module use_count is Ma_FUNCTON_med_use_count DEBUG %s: no memory for new procentry (%s)(func) DEBUG PPPOL279: fmc_mt, DDBUG %d3d; 1 DDBUG PPOL27P: fmc_mt, DDBUG %d3d; 1 DDBUG PPOL27P: fmc_mt, DDBUG fmcd inference at byte %u, 1 DDBUG %s: rcrcv_tinnel >name DDBUG FML idee80211_crypto_newkey failed DEBUG %s: rcrcv_tinnel >name DDBUG FAIL idee80211_crypto_serkey failed DEBUG PPOL27P:>-%sFUNCTION DEBUG FAIL idee80211_crypto_serkey failed DEBUG PPOL27P:>-%sFUNCTION DEBUG FAIL ideeap botch; lead bot	%s: xmit:, session->name	DEBUG	%s: failed to register sysctls!, vap- >iv_dev->name	DEBUG
%sc madule use_count is %idFUNCTON mod_use_count DEBUG %sc bulkpip len %u, tag, p, len DEBUG PPPO.2TP: %sfmt, DEBUG %d32, (iINB_1*p)[I] DEBUG PPPO.2TP: %sfmt, DEBUG Md32, (iINB_1*p)[I] DEBUG %sc recv; tunnel name DFBUG %dx2, (iINB_1*p)[I] DEBUG %sc recv; tunnel name DFBUG %dx, (iINB_1*p)[I] DEBUG %sc mit; session name DFBUG FAL: see80211_crypto_newkey failed DEBUG PPPO.2TP: %dx_fmt, DEBUG FAL: see80211_crypto_setkpt failed DFBUG PPPO.2TP: %dx_fmt, DEBUG FAL: see80211_crypto_setkpt failed DEBUG PPPO.2TP: %dx_fmt, DEBUG FAL: see80211_crypto_setkpt failed DEBUG PPPO.2TP: %dx_fmt, DEBUG FAL: see80211_crypto_setkpt failed DEBUG PPO.2TP: %dx_fmt, DEBUG FAL: see80211_crypto_table fails fails setspecification DEBUG PPO.2TP: %dx_fmt, DEBUG FAL: see80211_crypto_table fails DEBUG PRO.2TP Ks_fmt, DEBUG FAL: see80211_crypto_table fails DEBUG Msc mite, session name	%s: xmit:, session->name	DEBUG	%s: no memory for new proc entry (%s)!,func,	DEBUG
PPPOLZTP %x:_fmt, DEBUG %03d, i DEBUG PPPOLZTP ~> %x:_FUNCTON	%s: module use_count is %d,FUNCTION, mod_use_count	DEBUG	%s: 0x%p len %u, tag, p, len	DEBUG
PPPOLZTP: -> %kFUNCTION_) DEBUG %02x_((u_im8_t**)p)(i) DEBUG PPPOLZTP: -> %kFUNCTION_) DEBUG %irst difference at byte %ki, i DEBUG %irs crev, tunnel-name DEBUG %irst difference at byte %ki, i DEBUG %irs crev, tunnel-name DEBUG %irst isession->name DEBUG FAIL isee80211_crypto_newkey failed DEBUG %irs crev, tunnel-name DEBUG FAIL isee80211_crypto_restley failed DEBUG PPOLZTP: ~- %sFUNCTION_) DEBUG FAIL isee80211_crypto_restley failed DEBUG PPOLZTP: <- %sFUNCTION_)	PPPOL2TP %s: _fmt,	DEBUG	%03d:, i	DEBUG
PPPOL2TP: <-%s, _FUNCTION_) DEBUG first difference at byte %u, i DEBUG first difference at byte %u, i DEBUG West, I>name DEBUG %s: xmip: sexion:>name DEBUG FML: eneopol 11_crypto_setkey failed DEBUG %s: xmip: sexion:>name DEBUG FAIL: eneopol 11_crypto_setkey failed DEBUG %s: xmip: sexion:>name DEBUG FAIL: eneopol 11_crypto_setkey failed DEBUG PPPOL2TP: >%sFUNCTION_) DEBUG FAIL: decap botch; leagt batch; data does not compare DEBUG %s: xmip: sexion:>name DEBUG FAIL: encopt data does not compare DEBUG %s: xmip: sexion:>name DEBUG FAIL: encopt data does not compare DEBUG %s: whit; session->name DEBUG FAIL: encopt data does not compare DEBUG %s: whit; session->name DEBUG FAIL: encopt data does not compare DEBUG %s: whit; session->name DEBUG %so of %so 2000 DEBUG Mession: %s: whit; session->name DEBUG FAIL: encopt data ength mismatch DEBUG DEBUG Mession: DEBUG	PPPOL2TP:> %s,FUNCTION)	DEBUG	%02x, ((u_int8_t *)p)[i]	DEBUG
%s: recv., tunnel->name DEBUG %s:, t->name DEBUG %s: mic, session >-name DEBUG FAL: ieee80211_crypto_newkey failed DEBUG PPPOL2TP %s: _fmt, DEBUG FAL: ieee80211_crypto_setkey failed DEBUG PPPOL2TP %s: _fmt, DEBUG FAL: unable to allocate skbuff DEBUG PPPOL2TP: ~> %sFUNCTION DEBUG FAL: weep decap failed DEBUG PPPOL2TP: ~> %sFUNCTION DEBUG FAL: decap botch; length mismatch DEBUG %s: xmit; session->name DEBUG FAL: decap botch; length mismatch DEBUG %s: xmit; session->name DEBUG FAL: encap data length mismatch DEBUG %s: xmit; session->name DEBUG FAL: encap data length mismatch DEBUG %s: xmit; session->name DEBUG FAL: encap data length mismatch DEBUG %s: xmit; session->name DEBUG FAL: encap data length mismatch DEBUG %s: xmit; session->name DEBUG PASS DEBUG %s: xmit; session->name DEBUG %so dist isst isst isst isst isst isst isst	PPPOL2TP: < %s,FUNCTION)	DEBUG	first difference at byte %u, i	DEBUG
%%xmit, session > name DEBUG FAIL: icee80211_crypto_newkey failed DEBUG %%xmit, session > name DEBUG FAIL: icee80211_crypto_setkey failed DEBUG PPPOLZTP: < %s, _FUNCTION	%s: recv: , tunnel->name	DEBUG	%s:,t->name	DEBUG
%is:xmlit;session->name DEBUG FAIL: incee80211_crypto_setkey failed DEBUG PPPOL2TP %is:_fmt, DEBUG FAIL: wable to allocate skbuff DEBUG PPPOL2TP :-> %is,_FUNCTON_) DEBUG FAIL: wable to allocate skbuff DEBUG PPPOL2TP:-> %is,_FUNCTON_) DEBUG FAIL: decap botch; data does not compare DEBUG %is: xmlit;session->name DEBUG FAIL: decap botch; data does not compare DEBUG %is: xmlit;session->name DEBUG FAIL: encypt data does not compare DEBUG Mis: xmlit;session->name DEBUG FAIL: encypt data does not compare DEBUG Mis: xmlit;session->name DEBUG FAIL: encypt data does not compare DEBUG Mis: wdit, xdwlox wdwloxkki, (status == ERROR ? # :), page DEBUG %is: 04(pi len 4/u, tag, p, len DEBUG ymme, addr(0), addr(1), addr(1), addr(4), addr(5) DEBUG %is: 040p len 4/u, tag, p, len DEBUG ymme, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) DEBUG %is: x+-name DEBUG ymme, addr(0), addr(1), addr(1), addr(1), addr(1), addr(1), addr(1), a	%s: xmit:, session->name	DEBUG	FAIL: ieee80211_crypto_newkey failed	DEBUG
PPPOL2TP %s: _mt, 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 Sis recv, funnel->name DEBUG FAIL: decap botch; length mismatch DEBUG %s: xmit; session->name DEBUG FAIL: encrypt data idees not compare DEBUG %s: xmit; session->name DEBUG FAIL: encrypt data idees not compare DEBUG %s: xmit; session->name DEBUG FAIL: encrypt data idees not compare DEBUG (%s: xMit; session->name DEBUG PAIL: encrypt data idees not compare DEBUG (%s: xMit; session->name DEBUG %s: ox/kp len %u, tag, p, len DEBUG (WW%s \$Wr0: XM00X%002X%002X%002X; dev- DEBUG %s: ox/kp len %u, tag, p, len DEBUG yname, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) %s: ox/kp len %u, tag, p, len DEBUG yname, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) %s: ox/kp len %u, i DEBUG yname, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) %s: x - name DEBUG	%s: xmit:, session->name	DEBUG	FAIL: ieee80211_crypto_setkey failed	DEBUG
PPPDL2TP:-> %s, _FUNCTION_) DEBUG FAIL: wep decap failed DEBUG PPPDL2TP: <- %s, _FUNCTION_)	PPPOL2TP %s: _fmt,	DEBUG	FAIL: unable to allocate skbuff	DEBUG
PPPOL2TP: <- %s,FUNCTION DEBUG FAIL: decap botch; length mismatch DEBUG %s: xmit; session ->name DEBUG FAIL: decap botch; data does not compare DEBUG %s: xmit; session ->name DEBUG FAIL: encap data length mismatch DEBUG Nex xmit; session ->name DEBUG FAIL: encap data length mismatch DEBUG NRS %ERX: %800: 0x%08X%08X% (status == ERROR 7 ±); ngae; DEBUG %s: 0x%p len %u, tag, p, len DEBUG YMR% %EXX: %02X%02X%02X%02X%02X%02X%02X%02X%02X%02X	PPPOL2TP:> %s,FUNCTION)	DEBUG	FAIL: wep decap failed	DEBUG
%s: recv. tunnel->name DEBUG FAIL: decap botch; data does not compare DEBUG %s: xmit; session->name DEBUG FAIL: encap data length mismatch DEBUG %s: xmit; session->name DEBUG FAIL: encap data length mismatch DEBUG WQ3 Is triggered DEBUG FAIL: encapt data does not compare DEBUG W(R%s %M0X %M0X %M0X %M0X%) (status == ERROR 7 # :), page, page, addr, (uin32_1)(*palue >> 32), (uin32_1)(*palue & 0xfffffff) DEBUG %s: 0x%p len %u, tag, p, len DEBUG yame, add %02X%M02X%M02X%M02X%M02X, dov- >name, addr(0, addr(1), addr(1), addr(1), addr(1) DEBUG %s: 0x%p len %u, tag, p, len DEBUG %s: mac_udel %02X%02X%02X%02X%02X%02X, dov- >name, addr(0), addr(1), addr(1), addr(1) DEBUG %03dr, i DEBUG %s: mac_udel %02X%02X%02X%02X%02X%02X, dev- >name, addr(0), addr(1), addr(1), addr(1) DEBUG first difference at byte %u, i DEBUG %s: mac_undefined %02X%02X%02X%02X%02X%02X DEBUG first difference at byte %u, i DEBUG %s: mac_undefined %02X%02X%02X%02X%02X%02X DEBUG first difference at byte %u, i DEBUG %s: addr_add w02X%02X%02X%02X%02X%02X%02X%02X DEBUG first difference at byte %u, i DEBUG	PPPOL2TP: < %s,FUNCTION)	DEBUG	FAIL: decap botch; length mismatch	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: encap data length mismatch DEBUG [Rq 31 is triggered DEBUG FAIL: encap data length mismatch DEBUG [Rq 31 is triggered DEBUG FAIL: encap data length mismatch DEBUG [Ws:%dr], funcLINE_\ DEBUG Will of %u 000, %u00, %u00, %u00, %u00, %u00, %u10, %u11, %u10, %u12, %u12, %u10, %u12, %u10, %u12, %u12, %u10, %u12, %u12, %u10, %u12, %u10, %u12, %u12, %u10, %u12, %u12, %u12, %u12, %u10, %u12, %u	%s: recv: , tunnel->name	DEBUG	FAIL: decap botch; data does not compare	DEBUG
%s: xmlt, session:>name DEBUG FAIL: encap data length mismatch DEBUG IRQ 31 is triggered DEBUG FAIL: encap data length mismatch DEBUG [%s;%d],funcLINE_\ DEBUG PASS DEBUG (WR%s %d0, %eb0x (%s0x) (status == ERROR 7 # :), DeBUG %s0 of %u 802.111 WEP test vectors passed, pass, total DEBUG addr, (uint32_1)(*pValue >> 32), (uint32_1)(*pValue & 0xfffffff) DEBUG %s0 x%bp len %u, tag, p, len DEBUG page, addr, (uint32_1)(xaddr[3], addr[4], addr[5] DEBUG %o3d, i DEBUG %s: mac_add %02X%02X%02X%02X%02X, dev- DEBUG %03d, i DEBUG >name, addr[0], addr[1], addr[2], addr[4], addr[5] DEBUG %o2x, ((u_int8_t *)p)[1] DEBUG >name, addr[0], addr[1], addr[2], addr[4], addr[5] DEBUG first difference at byte %u, i DEBUG >name, addr[0], addr[1], addr[2], addr[4], addr[5] Ms:, t->name DEBUG >name, addr[0], addr[1], addr[2], addr[4], addr[5] Ms:, t->name DEBUG >name, addr[0], addr[1], addr[2], addr[4], addr[5] Ms:, t->name DEBUG >name, addr[0], addr[1], addr[2], addr[4], addr[5] Ms:, t->name DEBUG %s: addr_add %02X%02X%02X%02X%02X, dev- DEBUG FAIL: iece80211_crypto_newkey failed DEBUG >name, addr[0], addr[1], addr[2], addr[4], addr[5] MS: trippered	%s: xmit:, session->name	DEBUG	FAIL: wep encap failed	DEBUG
IRQ 31 is triggered DEBUG FAIL: encrypt data does not compare DEBUG [%55%d],funcLINE\ DEBUG PASS DEBUG [%55%d],funcLINE\ DEBUG %SS DEBUG [%55%d],funcLINE\ DEBUG %SS DEBUG addr, (uint32_1)(*pValue >>32), (uint32_1)(*pValue & 0xfffffff) %SS %SS MSS mare_add %02X%02X%02X%02X%02X%02X DEBUG %SS MSS %SS mare_add %02X%02X%02X%02X%02X%02X DEBUG %O3d, i >name_addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) DEBUG %O2X, ((u_int8_t *)p)(I) DEBUG >name_addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) DEBUG frst difference at byte %u, i DEBUG >name_addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) DEBUG frst difference at byte %u, i DEBUG >name_addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) DEBUG frst. tifference at byte %u, i DEBUG >name_addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) DEBUG FAIL: ieee80211_crypto_newkey failed DEBUG >name_addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) DEBUG FAIL: ieee80211_crypto_setkey failed DEBUG >name_addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) DEBUG FAIL: ieee80211_crypto_setkey failed D	%s: xmit:, session->name	DEBUG	FAIL: encap data length mismatch	DEBUG
(%s%d),funcLINE\ DEBUG PASS DEBUG (%s%d),funcLINE\ DEBUG %u of %u 802.111 WEP test vectors passed, pass, total DEBUG addr, (uint32_1)(*pValue >> 32), (uin32_t)(*pValue & 0xfffffff) %s: 0x %o %o fen %u, tag, p, len DEBUG %s: mac_add %02X%002X%002X%02X%02X, dev- DEBUG %s: 0x %o fen %u, tag, p, len DEBUG >name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) %s: mac_del %02X%02X%02X%02X%02X, dev- DEBUG %o2x, ((u_int8_t *)p)[i] DEBUG >name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) ms: mac_del %02X%02X%02X%02X%02X, dev- DEBUG first difference at byte %u, i DEBUG >name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) ms: mac_undefined %02X%02X%02X%02X%02X, dev- DEBUG first difference at byte %u, i DEBUG >name, addr(0), addr(1), addr(1), addr(1), addr(1), addr(1) DEBUG first difference at byte %u, i DEBUG >name, addr(0), addr(1), addr(1), addr(1), addr(1) DEBUG first difference at byte %u, i DEBUG >name, addr(0), addr(1), addr(1), addr(1), addr(1) DEBUG first difference at byte %u, i DEBUG >name, addr(0), addr(1), addr(1), addr(1), addr(1) ddr(1) ddr(1) DEBUG first difference at byte %u, i >name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5) first difference at byte %u, i	IRQ 31 is triggered	DEBUG	FAIL: encrypt data does not compare	DEBUG
\ttps://ttps://ttps://ttps://ttps://ttps/alue & 0.stfffffff DEBUG %u of %u of %u 802.111 WEP test vectors passed, pass, total DEBUG addr, (uint32_1)(*pvalue >> 32), (uint32_t)(*pvalue & 0.stfffffff) DEBUG %s: 0x%p len %u, tag, p, len DEBUG %s: mac_add %02X%02X%02X%02X%02X%02X, dev- DEBUG %s: 0x%p len %u, tag, p, len DEBUG >name, addr(01, addr(11, addr(2), addr(3), addr(4), addr(5) %003d, i DEBUG %s: 0x%p len %u, tag, p, len %s: macadd %02X%02X%02X%02X%02X%02X%02X, dev- DEBUG %002x, ((u_int8_t *)p)[i] DEBUG >name, addr(10, addr(11, addr(2), addr(3), addr(4), addr(5) Most of %02X%02X%02X%02X%02X%02X%02X%02X%02X%02X	[%s:%d] ,func,LINE\	DEBUG	PASS	DEBUG
addr, (uint32_t)(*pValue >> 32), (uint32_t)(*pValue & 0xfffffff) Image (triangle (tria	\t[R%s %#0x %#0x 0x%08x%08x], (status == ERROR ? # :), page,	DEBUG	%u of %u 802.11i WEP test vectors passed, pass, total	DEBUG
\ttp://www.settox.vs/wowwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww	addr, (uint32_t)(*pValue >> 32), (uint32_t)(*pValue & 0xfffffff)			
page, addr. (uint32_1)(value &> 32). (uint32_1)(value & 0.4fffffff)MeanDeBUGWordst; iDeBUG	\t[W%s %#0x %#0x 0x%08x%08x], (status == ERROR ? # :),	DEBUG	%s: 0x%p len %u, tag, p, len	DEBUG
%s: mac_add %02X%02X%02X%02X%02X, dev- >name, addr[0], addr[1], addr[2], addr[4], addr[5] DEBUG %03d; i DEBUG %s: mac_add %02X%02X%02X%02X%02X, dev- >name, addr[0], addr[1], addr[2], addr[4], addr[5] DEBUG %02x, ((u_int8_t *)p)[i] DEBUG %s: mac_undefined %02X%02X%02X%02X%02X, dev- >name, addr[0], addr[1], addr[2], 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[4], addr[5] DEBUG %s: , t->name DEBUG %s: mac_undefined %02X%02X%02X%02X%02X%02X DEBUG fs: , t->name DEBUG >name, addr[0], addr[1], addr[2], addr[4], addr[5] DEBUG fs: , t->name DEBUG %s: addr_add %02X%02X%02X%02X%02X%02X, dev- >name, addr[0], addr[1], addr[2], addr[4], addr[5] DEBUG FAlL: ieee80211_crypto_newkey failed DEBUG %s: addr_add %02X%02X%02X%02X%02X%02X, dev- >name, addr[0], addr[1], addr[2], addr[4], addr[5] DEBUG FAlL: inable to allocate skbuff DEBUG %s: set_float %dy%d, DEBUG FAlL: crop encap failed DEBUG DEBUG IBUG %s: set_float %dy%d, DEBUG FAlL: encrypt data dees not compare DEBUG IBUG IBUG IBUG IBUG IBUG IBUG IBUG IBUG </td <td>page, addr, (uint32_t)(value >> 32), (uint32_t)(value & 0xfffffff)</td> <td></td> <td></td> <td>ļ </td>	page, addr, (uint32_t)(value >> 32), (uint32_t)(value & 0xfffffff)			ļ
%s: mac_del %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, iDEBUG personal%s: mac_kick %02X:%02X:%02X:%02X:%02X:%02X; dev- >name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUG %s: , t > nameMestionDEBUG%s: addr_add %02X:%02X:%02X:%02X:%02X:%02X:%02X; dev- >name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUG personal%s: , t > nameDEBUG%s: addr_add %02X:%02X:%02X:%02X:%02X:%02X; dev- >name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUG personalFAIL: ieee80211_crypto_newkey failedDEBUG%s: addr_adel %02X:%02X:%02X:%02X:%02X:%02X; dev- >name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X:%02X:%02X:	%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
>name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5)DEBUGfirst difference at byte %u, iDEBUG>name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5)DEBUGfirst difference at byte %u, iDEBUG%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X;%02XDEBUG%s: rt>name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5)DEBUG%s: addr_add %02X:%02X:%02X:%02X:%02X:%02X.DEBUGFAIL: ieee80211_crypto_newkey failedDEBUG>name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5)DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: addr_add %02X:%02X:%02X:%02X:%02X.DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG>name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5)DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: mac_undefined %02X:%02X:%02X:%02X:%02X.DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG>name, addr(0), addr(1), addr(2), addr(3), addr(4), addr(5)DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: set_float %d;%d,DEBUGFAIL: crmp encap failedDEBUGip_fnish_output2: No header cache and no neighbour!DEBUGFAIL: encrypt data does not compareDEBUGigy asks for address mask. Who is it?DEBUGFAIL: ccmp decap failedDEBUGicmp v4 hw csum failure)DEBUGFAIL: decap botch; length mismatchDEBUGexpire>> %u% d%d %d, expire,DEBUGFAIL: decap botch; lengt mismatchDEBUGexpire>> %u% d%d %d, expire,DEBUGFAIL: decap botch; lengt mismatchDEBUGexpire++%u% d%d %d, expi	%s: mac_del %02X:%02X:%02X:%02X:%02X:%02X, dev-	DEBUG	%02x, ((u_int8_t *)p)[i]	DEBUG
%s: mac_kick %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, iDEBUG first difference at byte %u, iDEBUG 	>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]			
%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X;%02XDEBUG%s: st->nameDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_newkey failedDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: addr_del %02X:%02X:%02X:%02X:%02X:%02X; dev- >name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: mac_undefined %02X:%02X:%02X:%02X:%02X; dev- >name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: mac_undefined %02X:%02X:%02X:%02X:%02X; dev- >name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: inable to allocate skbuffDEBUG%s: set_float %d;%d,DEBUGFAIL: ccmp encap failedDEBUGing_finish_output2: No header cache and no neighbour!DEBUGFAIL: encrypt data does not compareDEBUGaguy asks for address mask. Who is it?DEBUGFAIL: ccmp decap failedDEBUGicmp v4 hw csum failure)DEBUGFAIL: decap botch; length mismatchDEBUGexpire+> %u %d %d %d, expire,DEBUGPASSDEBUGrt_cache @%02x: %u, %u, %u, hash,DEBUG%u of %u 802.111 AES-CCMP test vectors passed, pass, totalDEBUGin_t_divice redirect toDEBUG%u of %u 802.111 AES-CCMP test vectors passed, pass, totalDEBUGin_t_divice redirect toDEBUG%u of %u 802.111 AES-CCMP test vectors passed, pass, totalDEBUG	%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
>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]Image: add addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_newkey failedDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: unable to allocate skbuffDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: crmp encap failedDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: encap data length mismatchDEBUGNS: set_float %d;%d,DEBUGDEBUGFAIL: encrypt data does not compareDEBUGip_finish_output2: No header cache and no neighbour!DEBUGFAIL: ccmp decap failedDEBUGicmp v4 hw csum failure)DEBUGFAIL: dcap botch; length mismatchDEBUGexpire>>%u %d %d %d, expire,DEBUGFAIL: dcap botch; data does not compareDEBUGexpire++ %u %d %d %d, expire,DEBUGPASSDEBUGrt_cache @%02x: %u.wu.wu.wu, hash,DEBUG%u of %u 802.11i AES-CCMP test vectors passed, pass, totalDEBUGip_t divice: redirect toDEBUG%s: 0x%p len %u, tag, p, lenDEBUGip_t divice: redirect toDEBUG%s: 0x%p len %u, tag, p, lenDEBUG	%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X, dev-	DEBUG	%s: , t->name	DEBUG
%s: addr_add %02X:%02X:%02X:%02X:%02X:%02X;DEBUGFAIL: ieee80211_crypto_newkey failedDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: addr_del %02X:%02X:%02X:%02X:%02X:%02X;DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: ieee80211_crypto_setkey failedDEBUG%s: mac_undefined %02X:%02X:%02X:%02X:%02X;DEBUGFAIL: unable to allocate skbuffDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAIL: crmp encap failedDEBUG%s: set_float %d;%d,DEBUGDEBUGFAIL: encap data length mismatchDEBUGIRQ 32 is triggeredDEBUGFAIL: encryp to data does not compareDEBUGa guy asks for address mask. Who is it?DEBUGFAIL: ccmp decap failedDEBUGicmp v4 hw csum failure)DEBUGFAIL: decap botch; length mismatchDEBUGexpire>>%u %d %d %d, expire,DEBUGFAIL: decap botch; length mismatchDEBUGexpire++ %u %d %d %d, expire,DEBUGFAIL: decap botch; length mismatchDEBUGrt_cache @%02x: %u.%u.%u.%u, hash,DEBUG%u of %u of %u 802.111 AES-CCMP test vectors passed, pass, totalDEBUGrt_bind_peer(0) @%p, NET_CALLER(iph)DEBUG%u of %u 3dv. iDEBUGDEBUGin. rt_advice: redirect toDEBUG%u of %u 3dv. iDEBUG	>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]			
%s: addr_del %02X:%02X:%02X:%02X:%02X:%02X;DEBUGFAlL: ieee80211_crypto_setkey failedDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAlL: unable to allocate skbuffDEBUG%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X;DEBUGFAlL: unable to allocate skbuffDEBUG>name, addr[0], addr[1], addr[2], addr[3], addr[4], addr[5]DEBUGFAlL: ccmp encap failedDEBUG%s: set_float %d;%d,DEBUGFAlL: encap data length mismatchDEBUGIRQ 32 is triggeredDEBUGFAlL: encrypt data does not compareDEBUGa guy asks for address mask. Who is it?DEBUGFAlL: ccmp decap failedDEBUGicmp v4 hw csum failure)DEBUGFAlL: decap botch; length mismatchDEBUGexpire>> %u %d %d, expire,DEBUGFAlL: decap botch; length mismatchDEBUGexpire++ %u %d %d %d, expire,DEBUGPASSDEBUGrt_cache @%02x: %u.%u.%u.%u, hash,DEBUG%u of %u 802.11i AES-CCMP test vectors passed, pass, totalDEBUGrt_bind_peer(0) @%p, NET_CALLER(iph)DEBUG%s: 0x%p len %u, tag, p, lenDEBUGDEBUG	%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: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X;%02X;%02X;%02X;%02X;%02X:%02X:%02X:%02X:%02X:%02X:%02X:%02X:	%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
Name, addr(U), addr(1), addr(2), addr(4), addr(5)DEBUGFAIL: ccmp encap failedDEBUG%s: set_float %d;%d,DEBUGFAIL: encap data length mismatchDEBUGIRQ 32 is triggeredDEBUGFAIL: encap data length mismatchDEBUGip_finish_output2: No header cache and no neighbour!DEBUGFAIL: encrypt data does not compareDEBUGa guy asks for address mask. Who is it?DEBUGFAIL: ccmp decap failedDEBUGicmp v4 hw csum failure)DEBUGFAIL: decap botch; length mismatchDEBUGexpire>> %u %d %d %d, expire,DEBUGFAIL: decap botch; data does not compareDEBUGexpire++ %u %d %d %d, expire,DEBUGFAIL: decap botch; data does not compareDEBUGrt_cache @%02x: %u.%u.%u, hash,DEBUG%u of %u 802.11i AES-CCMP test vectors passed, pass, totalDEBUGrt_bind_peer(0) @%p, NET_CALLER(iph)DEBUG%s: 0x%p len %u, tag, p, lenDEBUGDEBUG	%s: mac_undefined %02X:%02X:%02X:%02X:%02X:%02X, dev-	DEBUG	FAIL: unable to allocate skbuff	DEBUG
Wast set_indat %0, %0, %0, %0, %0, %0, %0, %0, %0, %0,	>name, addr[U], addr[T], addr[2], addr[3], addr[4], addr[5]		EAll - comp op cap failed	
InclusionDEBOGPAIL: encapidata length mismatchDEBOGip_finish_output2: No header cache and no neighbour!DEBUGFAIL: encrypt data does not compareDEBUGa guy asks for address mask. Who is it?DEBUGFAIL: ccmp decap failedDEBUGicmp v4 hw csum failure)DEBUGFAIL: decap botch; length mismatchDEBUGexpire>> %u %d %d %d, expire,DEBUGFAIL: decap botch; data does not compareDEBUGexpire++ %u %d %d %d, expire,DEBUGFAIL: decap botch; data does not compareDEBUGrt_cache @%02x: %u.%u.%u.hash,DEBUG%u of %u 802.11i AES-CCMP test vectors passed, pass, totalDEBUGrt_bind_peer(0) @%p, NET_CALLER(iph)DEBUG%os: 0x%p len %u, tag, p, lenDEBUGip_rt_advice: redirect toDEBUG%03 ch iDEBUG			FAIL: encap data longth micmatch	
a guy asks for address mask. Who is it?DEBUGFAIL: encrypt data does not compareDEBUGicmp v4 hw csum failure)DEBUGFAIL: dccap botch; length mismatchDEBUGexpire>> %u %d %d %d, expire,DEBUGFAIL: decap botch; data does not compareDEBUGexpire++ %u %d %d %d, expire,DEBUGPASSDEBUGrt_cache @%02x: %u.%u.%u.%u, hash,DEBUG%u of %u 802.11i AES-CCMP test vectors passed, pass, totalDEBUGrt_bind_peer(0) @%p, NET_CALLER(iph)DEBUG%s: 0x%p len %u, tag, p, lenDEBUG	in finish output?: No boador cacho and no noighbourl		FAIL: encap data length mismatch	
a guy ass for address mask, who is it:DEBUGPALL Chip decap failedDEBUGicmp v4 hw csum failure)DEBUGFAIL: decap botch; length mismatchDEBUGexpire>> %u %d %d %d, expire,DEBUGFAIL: decap botch; data does not compareDEBUGexpire++ %u %d %d %d, expire,DEBUGPASSDEBUGrt_cache @%02x: %u.%u.%u.%u, hash,DEBUG%u of %u 802.11i AES-CCMP test vectors passed, pass, totalDEBUGrt_bind_peer(0) @%p, NET_CALLER(iph)DEBUG%s: 0x%p len %u, tag, p, lenDEBUGip. rt_advice: redirect toDEBUG%03d: iDEBUG	a guy asks for address mask. Who is it?		FAIL: encrypt data does not compare	
InterpretativeDEBUGPALL decap botch, height mismatchDEBUGexpire>> %u %d %d %d, expire,DEBUGFAIL: decap botch; data does not compareDEBUGexpire++ %u %d %d %d, expire,DEBUGPASSDEBUGrt_cache @%02x: %u.%u.%u.%u, hash,DEBUG%u of %u 802.11i AES-CCMP test vectors passed, pass, totalDEBUGrt_bind_peer(0) @%p, NET_CALLER(iph)DEBUG%s: 0x%p len %u, tag, p, lenDEBUGip, rt_advice: redirect toDEBUG%03d: iDEBUG	a guy asks for address mask. Who is it?		FAIL: CCTIP decap failed	
Expire/> You			FAIL: decap botch; deta dess not compare	
PEBUG PEBUG PAS 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	expire you you you you, expire,			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	$rt_cache @%02y. \%1. \%1. \%1. \%1. \%2$		Mu of Mu 802 11; AES-CCMP tast vectors passed pass total	DERLIC
in tradvice redirect to DERLIG 0603d+ i	$rt_cache @ 7002A, 700.700.700.700, Hash,$		/ 100 01 700 002.111 ALS-CENT LEST VECTOTS PASSED, PASS, LOLAI	DERLIC
	in_t_advice: redirect to	DEBUG	%03d· i	DEBLIG

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	DEBUG	unable to allocate skbuff	DEBUG
UDP: bad checksum. From %d.%d.%d.%d:%d to	DEBUG	tkip enmic failed	DEBUG
%d.%d.%d.%d Wen %d,	DEDLIC		
%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	DEBOG
%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 guv 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.NFT_CALLER(iph)	DEBUG	tkip demic failed	DEBUG
ip_rt_advice: redirect to	DEBUG	802 11i TKIP test vectors passed	DEBUG
ip rt bua: %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	DEBUG	Atheros HAL assertion failure: %s: line %u: %s.	DEBUG
%u.%u.%u.%u;%u,			
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 guv 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	%: 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:gropoll Buf allocation failedfunc	DEBUG
ip rt advice: redirect to	DEBUG	%s: %s: unable to start recy logic.	DEBUG
ip rt bug: %u.%u.%u.%u -> %u.%u.%u.%u.%s.	DEBUG	%s: %s: unable to start recy 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,	DEBUG	%s: unable to start recv logic, dev- >name	DEBUG
%: flow src=%s,FUNCTION_, XFRIVISTRADDR(fl->flo_src, family)	DEBUG	%s: %s: unable to reset nardware: %s (HAL status %u),	DEBOG
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	DEBUG	move data from NORMAL to XR	DEBUG
ROUTING, LOCAL_IN and/or LOCAL_OUT targets.			
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	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	xlr8NatlpFinishOutput: Err skb2 == NULL !	DEBUG
Should bcast: %u.%u.%u.%u- >%u.%u.%u.%u (sk=%p,	DEBUG	xlr8NatSoftCtxEnqueue: Calling xlr8NatIpFinishOutput (), status	DEBUG
ptype=%u),			
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	DEBUG
		spi:%d isr:%p,	
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_RITS) >> 22)	DEBUG	IPSEC_ERR [%s:%d]: Max (%d) No of SA Limit reached,	DEBUG
$UBGP=$ %u_ntohs(th->urg_ntr)	DEBUG	IPSEC_ERR [%s·%d]: time(secs): %u	DEBUG
	DEBUG	EBROR: Failed to add entry to insec sa table	DEBUG
%02X op[i]		EBROR: Failed to add entry to ipsec sa table	
		EBROR: Failed to add entry to insec sa table	
INCOMPLETE [%] bytes]	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
SPT=%u DPT=%u EN=%u		EBROR: Failed to add entry to insec sa table	
SPT=%u DPT=%u LEN=%u	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
PROTO=ICMP		unknown oid '%s' varName	
		could not find oid pointer for '%s' varName	DEBUG
TYPE-%u CODE-%u ich->type ich->code			
		EBBOR: Failed to add entry to insec sa table	DEBUG
	DEBUG	EBROR: Failed to add entry to insec sa table	DEBUG
PARAMETER=%u	DEBUG	ERROR: Failed to add entry to ipsec sa table	DEBUG
GATEWAY=%u %u %u %u	DEBUG	EBROR: 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, NIPQUAD(trt->rt_dst)	DEBUG
SPI=0x%x , ntohl(eh->spi)	DEBUG	%02x,*p	DEBUG
PROTO=%u, ih->protocol	DEBUG	. %u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
UID=%u,skb->sk_socket->file->f_uid	DEBUG	%02x,*p	DEBUG
<pre></pre>	DEBUG	. %u.%u.%u, NIPQUAD(trt->rt_dst)	DEBUG
level_string	DEBUG	%02x,*p	DEBUG
%sIN=%s OUT=%s ,	DEBUG	. %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 vipsecKloctlHandler 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,plpsecInf o->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	INFO
		equals existing table parameters).	
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	INFO
		for new table %s., sizeof(struct t_ipt_account_table), info-	
		>name	
ip_ct_h323: incomplete TPKT (fragmented?)	DEBUG	IPT_ACCOUNT_NAME : checkentry() wrong network/	INFO
		netmask.	
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	DEBUG	PPP generic driver version PPP_VERSION	INFO
dst=%u.%u.%u.%u:%d new,	02000		
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

ログメッカージ	取刍由	ログイッカージ	取刍由
Memory Allocation failed	<u>条志</u> 反	%: driver uploaded dev info	<u>条芯反</u>
modevport opcode received		%s huf	
		%: %s (day, info ath, hal, version	
kmalloc failed		%: driver unloaded day, info	
		%s. %s. mem-0x%ix, inq-%u nw_base-0x%p,	
		%S: %S, dev_INIO, version	
Killalloc Idlied		%5. %5. mem=0x%ix, irq=%d,	
unknown cyrpto locu chia received %x, chia	DEBUG	%S: %S: mem=0x%ix, irq=%d,	
register_chraev returned ZERO	DEBUG	%S: %S, dev_Into, version	
	DEBUG		
F password, &pdata	DEBUG	%S, DUT	
test key, key	DEBUG	%s: %s (, dev_info, atn_nai_version	
pre-hashed key, key	DEBUG	%s: driver unloaded, dev_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	DEBUG	%s: %s: mem=0x%lx, irq=%d,	INFO
2 selecting here: %d lastHanSelected = %d, selHan		%: % day info varsion	
lastHopSelected	DEBOG		
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:	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:	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_	DEBUG	Failed to mkdir /proc/net/madwifi	WARNING
PRINTK printk			

ログメッヤージ	緊急度	ログメッヤージ	緊急度
bcmDeviceInit: registration failed	DEBUG	try module get failed	WARNING
bcmDeviceInit: pCdev Add failed	DEBUG	%s: request_irg 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_irg 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 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 loctl Case :	DEBUG	host %u.%u.%u/if%d ignores	WARNING
=======Register Dump for Port Number #	DEBUG	martian destination %u.%u.%u from	WARNING
%d======,port			
%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	DEBUG	Neighbour table overflow.	WARNING
%x.			
%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	II header:	WARNING
Getting Rate Series: %x,vap- >iv_fixed_rate.series	DEBUG	%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 <0100> probe_intval <0100>	DEBUG	host %u.%u.%u.%u/if%d ignores	WARNING
usage: acparams ac <0 3> RTS <0 1> aggr scaling <04> min mbps <0250>	DEBUG	martian source %u.%u.%u.%u from	WARNING
usage: hbrparams ac <2> enable <0 1> per_low <050>	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/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

	一一一日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日		取名去
ロジメッセーシ %s: [%s] %s vap siv dov spame other sprintf(mas) buf		ロクメッセーシ We: Churto ADI SHA1 digart size too small fname	
%. [%] %, vap->iv_dev->iaine, ether_spinit(inac), but		%s: cappet allocate space for SHA1 digest frame	
		%s. calliot allocate space for STAT digest, marine	
[%c:%c] discard %c information element %c		%s%d: trying to write outside history	
[%s:%s] discard information element, %s,	DEBUG	%s%d: trying to write outside history	
		%s%d: trying to write outside history	
		%s%d: too big uncompressed packet. %d,	
LAD list dumpNodo\+Addross\t\t\tStato\tTriggor\tP lock		%s%d: encryption negotiated but not an	
Nodes information Address \t\t\tBlock\t\tDrened \ll frames	DEBUG	Kernel deesn't provide APC4 and/or SHA1 algorithms	
% %		PDP: not interface or channel?	ERROR
%00 \L %02.2X.%02.2X.%02.2X.%02.2X.%02.2X. %00 \L %05.12%.%02.2X.%02.2X.%02.2X.%02.2X. %00 \L %05.12%.%02.2X.%02.2X.%02.2X.	DEBUG	PPP: no momony (//L compressor)	
[0/d])+Eupstion)+0/s i ni > podo trace[i] funce		failed to register DDD dovise (0/d) orr	
[%d]\tPunction\t%s, J, h= >node_trace[i].tuncp		PPD: no momony (//L comp pkt)	
[%d]\tMdCAdd1\t%s, j,			
[%d]\tDescp\t\t%s, J, h=>hode_trace[i].descp		PPP: no memory (comp pkt)	
[%d]/tvalde/t/t%lld(0x%llx), J, II->Hode_trace[i].valde,		ppp. compressor dropped pkt	
Adding optry for			
ifmedia, setupo match for 0x00x /0x00x	DEBUG	PPP: VJ uncompressed error	
imedia_set. no match for 0x%x/0x%x,		ppp_decompress_frame: no memory	
ifmedia_set: target	DEBUG	ppp_mp_reconstruct bad seq %u < %u,	
ifmedia_set: setting to	DEBUG	PPP: couldn't register device %s (%d),	
ifmedia_locti: switching %s to , dev- >name	DEBUG	ppp: destroying ppp struct %p but dead=%d	ERROR
If media_match: multiple match for	DEBUG	ppp: destroying undead channel %p !,	ERROR
<unknown type=""></unknown>	DEBUG	PPP: removing module but units remain!	ERROR
desc->Imt_string	DEBUG	PPP: failed to unregister PPP device	ERROR
mode %s, desc->Irmt_string	DEBUG	%s: cannot allocate space for %scompressor, mame,	ERROR
<unknown subtype=""></unknown>	DEBUG	%s: cannot allocate space for MPPC history,	ERROR
%s, desc->Imt_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 SHAT module, fname	ERROR
%s, seen_option ? > :	DEBUG	%S: CryptoAPI SHAT digest size too small, fname	ERROR
%s: %s, dev->name, but	DEBUG	%s: cannot allocate space for SHAT digest, mame	ERROR
%s: no memory for syscti table!,tunc	DEBUG	%\$%d: trying to write outside history	ERROR
%s: failed to register sysctis!, vap- >iv_dev->name	DEBUG	%\$%d: trying to write outside history	ERROR
Atheros HAL assertion failure: %s: line %u: %s,	DEBUG	%\$%d: trying to write outside history	ERROR
atn_nal: logging to %s %s, atn_nal_logfile,	DEBUG	%\$%d: too big uncompressed packet: %d,	ERROR
atn_nal: logging disabled	DEBUG	%\$%d: encryption negotiated but not an	ERROR
	DEBUG	%\$%d: error - not an MPPC or MPPE frame	ERROR
ath_pci: No devices found, driver not installed.	DEBUG	Rernel doesn't provide ARC4 and/or SHAT algorithms	ERROR
:%a pri:%a qa:%u aa:%u sa:%u tot:%u amp:%a %02x:%02x:%02x,	DEBUG	PPP: not interface of 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 rangeEUNCTION	DEBUG	IBD: bad block at offset %u	FRROR
PKTI OG TAG %: Log buffer unavailable. FUNCTION	DEBUG	IBD: corrupted journal superblock	FRROR
PKTLOG TAG	DEBUG	JBD: bad block at offset %u	FRROR
Logging should be disabled before changing bufer size	DEBUG	IBD: Failed to read block at offset %u	FRROR
%sallocation failed for pl_infofunc	DEBUG	IBD: error %d scanning journal err	FRROR
%: Unable to allocate bufferfunc	DEBUG	IBD: IQ error %d recovering block	
%sallocation failed for pl_infofunc	DEBUG	/Logs_kernel_txt+303;KERN_ERR	
%: Unable to allocate bufferfunc	DEBUG	/logs_kerneltxt:304:KERN_ERR	
Atheros HAL assertion failure: %s: line %u: %s	DEBUG	IBD: recovery pass %d ended at	
ath ball logging to %s %s ath ball logfile		%: %: %d: BAD SESSION MAGIC \	
atti_nal. logging to /03 /03, atti_nal_logine,			
% see at hal buildents[i]		msg. >msg. pamolon wrong %d msg. >msg. pamolon	
foiled to allocate ry descriptors: %d error		addr family wrong: %d usin >sin_family	
ather to anotate ix descriptors. 700, enor		addr anning wrong, 700, usin > sin addr a addr usin > sin port	
Poset ry chain mask. Do internal reset (0/c) func			
		705. 705.700. BAD TONNEL MAGIC	
US_CANCEL_TIMER Talled!!			
%: unable to allocate channel table,unc			
%s: unable to collect channel list from hal;	DEBUG		
%s: cannot map channel to mode; freq %u flags 0x%x,	DEBUG	%S: %S:%d: BAD TUNNEL MAGIC \	
%s: unable to reset channel %u (%ulvinz)	DEBUG	msg->msg_namelen wrong, %d, msg- >msg_namelen	
%s: unable to restart recv logic,	DEBUG	addr family wrong: %d, usin->sin_family	
%s: start DFS WAIT period on channel %d,tunc,sc->sc_	DEBUG	udp addr=%x/%nu, usin->sin_addr.s_addr, usin->sin_port	ERROR
%s: cancel DES WAIT period on channel %d func sc->sc	DEBUG	s: %s:%d: BAD TUNNEL MAGIC	FRROR
curchan.channel			
Non-DFS channel, cancelling previous DFS wait timer	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
channel %d, sc- >sc_curchan.channel			
%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	DEBUG	%s: %s:%d: BAD TUNNEL MAGIC	ERROR
THRESHOLD			
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	DEBUG	fResetMod: Failed to register interrupt handler	ERROR
%08x %08x,			
noise floor: (%d, %d) (%d, %d) (%d, %d),	DEBUG	registering char device failed	ERROR
%p: %08x %08x %08x %08x %08x %08x %08x %08x	DEBUG	unregistering char device failed	ERROR
%08x %08x %08x,			ļ
%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	DEBUG	proc entry initialization failed	ERROR
%08x %08x,			ļ
%s: unable to allocate device object.,func	DEBUG	testCompHandler: received %s from %d, (char *)pInBuf,	ERROR

ログメッセージ	婜刍咹	ログメッセージ	
%s: unable to attach hardware: HAL status %u	DERLIG	UMI proto registration failed %d ret	来态反 ERR∩R
%s: HAL ABI msmatch:		AE LIMI registration failed %d ret	
905: MAL ADITISTIALCH,		umi initialization failed %d ret	
vos. Warning, using only vou entries in vou key cache,			
unable to setup vmit queue for PE traffic		FROD mem not found property (%d lop (%d mem	
Unable to setup xinit queue for be trainc:		ModEve returned Error	
% DFS attach failed,			
%s: Invalid Interface id = %u,runc, II_id		Modexp returned Error	
%s.grppoil but allocation failed ,func			
%s: unable to start recv logic,	DEBUG	%03d:, 0(02): ((((((((((((((((((((((((((((((((((((ERROR
%s: Invalid interface id = %u,func, if_id	DEBUG	%U2x, ((unsigned char ^)p)[i]	ERROR
%s: unable to allocate channel table,tunc	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:,	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,	DEBUG	[%s] Wrong parameters,func	ERROR
func, rx_clear, rx_frame, tx_frame			
%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_	DEBUG	[%s] Wrong Key Length,func	ERROR
t *)&wh->i_seq[0]) >> 4:0, bf->bf_isswretry,bf->bf_swretries			
Buffer #%08X> Next#%08X Prev#%08X Last#%08X,bf,	DEBUG	[%s] Wrong parameters,func	ERROR
TAILQ_NEXT(bf,bf_list),			
Stas#%08X flag#%08X Node#%08X, bf->bf_status, bf->bf_	DEBUG	[%s] Wrong parameters,func	ERROR
Descr #%08X> Next#%08X Data#%08X CtiU#%08X Ctil#%08X bf $>$ bf daddr ds $>$ ds link ds $>$ ds $>$ ds $>$ ds	DEBUG	[%s] wrong parameters,runc	ERKOR
ctl0 ds->ds_ctl1			
Ctl2#%08X Ctl3#%08X Sta0#%08X Sta1#%08X ds->ds_bw[0]	DEBLIG	[%s] Wrong parametersfunc	FRROR
ds->ds_hw[1], lastds->ds_hw[2], lastds- >ds_hw[3]	DEDOG		Ennon
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	DEBUG	Invalid IOCTL %#08x, cmd	ERROR
pattern , MAX_NUM_PATTERN			
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)	DEBUG	ath_pci: cannot remap PCI memory region) ;	ERROR
patternBytes			
Pattern Removed from entry %d ,i	DEBUG	ath_pci: no memory for device state	ERROR

ログメッヤージ	緊急度	ログメッヤージ	緊急度
Error : Pattern not found	DEBUG	%: 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 gnum %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	DEBUG	Unable to load needed module: %s; no support for \	ERROR
frame - %d, sequence number - %d, tidno - %d,			
isdata: %d isaggr: %d isampdu: %d ht: %d isretried: %d	DEBUG	Module \%s\ is not known, buf	ERROR
isxretried: %d shpreamble: %d isbar: %d ispspoll: %d			
aggrburst: %d calcairtime: %d qosnulleosp: %d,			
%p: 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,	0.5011.6		
0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x 0x%08x	DEBUG	Module \%s\ failed to initialize, buf	ERROR
		ath nois 22 hit DMA not available	
		ath_pci: s2-bit DiviA hot available	
Sc_txq[%d]:, I		ath_pci: cannot reserve PCI memory region	
%d:%p_i_tid_>tx_buffil		ath_pci. callificitienap PCI memory region) ,	
		%: upable to attach hardware: '%s' (HAL status %u)	
		%: HAL ABL mismatch:	
%: unable to reset hardware: hal status %u func status		%: failed to allocate descriptors: %d	
		%: unable to setup a beacon ymit queuel	
MacAddr-%s		%: unable to setup CAB ymit queuel	
TxBufldx=%d i	DEBUG	%: unable to setup xmit queue for %s traffic!	FRROR
Tid=%d tidno	DEBUG	%: unable to register device dev->name	FRROR
AthBuf=%p, tid->tx_buf[i]	DEBUG	%: 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-	DEBUG	%s: SKB does not exist.,FUNCTION	ERROR
>ft_numfilters			
filter[%d] filterID = %d rf_numpulses=%u; rf->rf_minpri=%u; rf-	DEBUG	%s: recvd invalid skb	ERROR
>rf_maxpri=%u; rf->rf_threshold=%u; rf- >rf_filterlen=%u; rf-			
>rf_mindur=%u; rf->rf_maxdur=%u,j, rf->rf_pulseid,			
NOL	DEBUG	unable to register KIFDEV to UMI	ERROR
WARNING!!! 10 minute CAC period as channel is a weather	DEBUG	The system is going to factory defaults!!!	CRITICAL
radar channel	DEDUC		
%s disable detects,tunc	DEBUG	%s, msg	
Yos eriable detects,TUNC	DEBUG	youzx, "(data + I)	
	DEBUG	Inside crypt_open in driver ######	
Yos eriable FFT Val=UX%X ,TUNC, Val	DEBUG	Inside crypt_release in driver ######	
%s debug level now = UX%X ,runc, dfs_debug_level	DEBUG	Inside crypt_init module in driver @@@@@@@@@	
nale rable:%u, maxvallurale:%u, ralemax:%u, pKC-	DEBUG	Inside crypt_cleanup module in driver @@@@@@@@@	

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	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