D-Link®
Building Networks for People

# Unified Services Router
# User Manual

DSR-250N / 500 / 500N / 1000 / 1000N

Ver. 1.03

Small Business Gateway Solution http://security.dlink.com

# User Manual

## *Unified Services Router*

D-Link Corporation
Copyright © 2011.

http://www.dlink.com

# User Manual

## DSR-250N / DSR-500 / 500N / 1000 / 1000N
## Unified Services Router
## Version 1.03

Copyright © 2011

### Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

### Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

### Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

# Table of Contents

# List of Figures

# Chapter 1. Introduction

D-Link Unified Services Routers offer a secure, high performance networking solution to address the growing needs of small and medium businesses. Integrated high-speed IEEE 802.11n and 3G wireless technologies offer comparable performance to traditional wired networks, but with fewer limitations. Optimal network security is provided via features such as virtual private network (VPN) tunnels, IP Security (IPsec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Secure Sockets Layer (SSL). Empower your road warriors with clientless remote access anywhere and anytime using SSL VPN tunnels.

With the D-Link Unified Services Router you are able to experience a diverse set of benefits:

- Comprehensive Management Capabilities

  The DSR-500, DSR-500N, DSR-1000 and DSR-1000N include dual-WAN Gigabit Ethernet which provides policy-based service management ensuring maximum productivity for your business operations. The failover feature maintains data traffic without disconnecting when a landline connection is lost. The Outbound Load Balancing feature adjusts outgoing traffic across two WAN interfaces and optimizes the system performance resulting in high availability. The second WAN port can be configured as a DMZ port allowing you to isolate servers from your LAN.

DSR-250N has a single WAN interface, and thus it does not support Auto Failover and Load Balancing scenarios.

- Superior Wireless Performance

  Designed to deliver superior wireless performance, the DSR-500N and DSR-1000N include 802.11 a/b/g/n, allowing for operation on either the 2.4 GHz or 5 GHz radio bands. Multiple In Multiple Out (MIMO) technology allows the DSR-500N and DSR-1000N to provide high data rates with minimal “dead spots” throughout the wireless coverage area.

DSR-250N and DSR-500N supports the 2.4GHz radio band only.

- Flexible Deployment Options

  The DSR-1000 / 1000N supports Third Generation (3G) Networks via an extendable USB 3G dongle. This 3G network capability offers an additional secure data connection for networks that provide critical services. The DSR-1000N can be configured to automatically switch to a 3G network whenever a physical link is lost.

- Robust VPN features

  A fully featured virtual private network (VPN) provides your mobile workers and branch offices with a secure link to your network. The DSR-250N, DSR-500, DSR-500N, DSR-1000 and DSR-1000N are capable of simultaneously managing 5, 10, 20 Secure Sockets Layer (SSL) VPN tunnels respectively,

empowering your mobile users by providing remote access to a central corporate database. Site-to-site VPN tunnels use IP Security (IPsec) Protocol, Point-to-Point Tunneling Protocol (PPTP), or Layer 2 Tunneling Protocol (L2TP) to facilitate branch office connectivity through encrypted virtual links. The DSR-250N, DSR-500(N) and DSR-1000(N) support 25, 35 and 75 simultaneous IPSec VPN tunnels respectively.

- Efficient D-Link Green Technology

  As a concerned member of the global community, D-Link is devoted to providing eco-friendly products. D-Link Green WiFi and D-Link Green Ethernet save power and prevent waste. The D-Link Green WLAN scheduler reduces wireless power automatically during off-peak hours. Likewise the D-Link Green Ethernet program adjusts power usage based on the detected cable length and link status. In addition, compliance with RoHS (Restriction of Hazardous Substances) and WEEE (Waste Electrical and Electronic Equipment) directives make D-Link Green certified devices the environmentally responsible choice.

Support for the 3G wireless WAN USB dongle is only available for DSR-1000 and DSR-1000N.

## 1.1 About this User Manual

This document is a high level manual to allow new D-Link Unified Services Router users to configure connectivity, setup VPN tunnels, establish firewall rules and perform general administrative tasks. Typical deployment and use case scenarios are described in each section. For more detailed setup instructions and explanations of each configuration parameter, refer to the online help that can be accessed from each page in the router GUI.

## 1.2 Typographical Conventions

The following is a list of the various terms, followed by an example of how that term is represented in this document:

- Product Name – D-Link Unified Services Router.
  - Model numbers DSR-500/500N/1000/1000N
- GUI Menu Path/GUI Navigation – ***Monitoring > Router Status***
- Important note –

# Chapter 2. Configuring Your Network: LAN Setup

It is assumed that the user has a machine for management connected to the LAN to the router. The LAN connection may be through the wired Ethernet ports available on the router, or once the initial setup is complete, the DSR may also be managed through its wireless interface as it is bridged with the LAN. Access the router's graphical user interface (GUI) for management by using any web browser, such as Microsoft Internet Explorer or Mozilla Firefox:

- Go to **http://192.168.10.1** (default IP address) to display the router's management login screen.
- Default login credentials for the management GUI:
  - Username: **admin**
  - Password: **admin**

If the router's LAN IP address was changed, use that IP address in the navigation bar of the browser to access the router's management UI.

## 2.1 LAN Configuration

***Setup > Network Settings > LAN Configuration***

By default, the router functions as a Dynamic Host Configuration Protocol (DHCP) server to the hosts on the WLAN or LAN network. With DHCP, PCs and other LAN devices can be assigned IP addresses as well as addresses for DNS servers, Windows Internet Name Service (WINS) servers, and the default gateway. With the DHCP server enabled the router's IP address serves as the gateway address for LAN and WLAN clients. The PCs in the LAN are assigned IP addresses from a pool of addresses specified in this procedure. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications the default DHCP and TCP/IP settings are satisfactory. If you want another PC on your network to be the DHCP server or if you are manually configuring the network settings of all of your PCs, set the DHCP mode to 'none'. DHCP relay can be used to forward DHCP lease information from another LAN device that is the network's DHCP server; this is particularly useful for wireless clients.

Instead of using a DNS server, you can use a Windows Internet Naming Service (WINS) server. A WINS server is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. The router includes the WINS server IP address in the DHCP configuration when acknowledging a DHCP request from a DHCP client.

You can also enable DNS proxy for the LAN. When this is enabled the router then as a proxy for all DNS requests and communicates with the ISP's DNS servers. When disabled all DHCP clients receive the DNS IP addresses of the ISP.

To configure LAN Connectivity, please follow the steps below:

1. In the LAN Setup page, enter the following information for your router:

    - IP address (factory default: 192.168.10.1).

> If you change the IP address and click Save Settings, the GUI will not respond. Open a new connection to the new IP address and log in again. Be sure the LAN host (the machine used to manage the router) has obtained IP address from newly assigned pool (or has a static IP address in the router's LAN subnet) before accessing the router via changed IP address.

    - Subnet mask (factory default: 255.255.255.0).

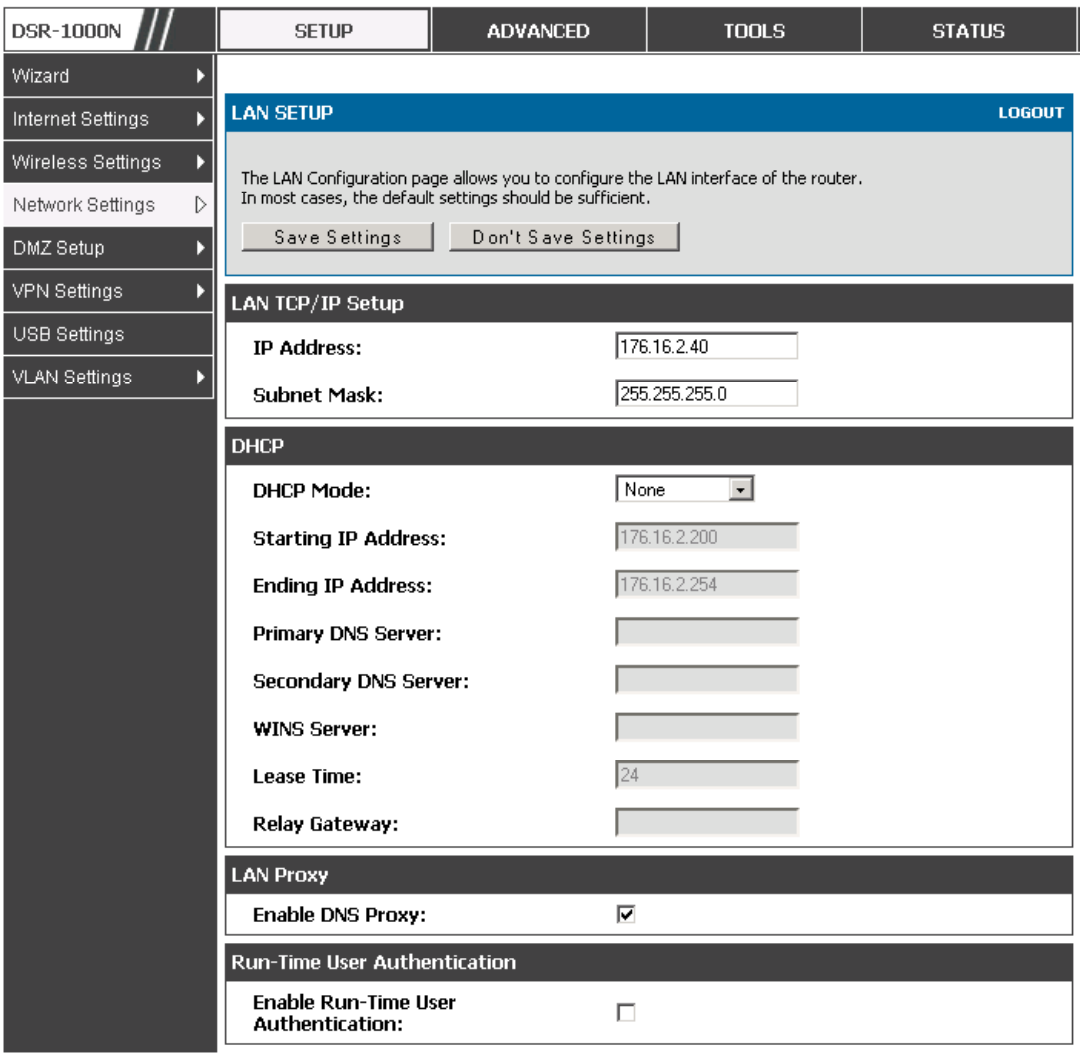
2. In the DHCP section, select the DHCP mode:

    - None: the router's DHCP server is disabled for the LAN
    - DHCP Server. With this option the router assigns an IP address within the specified range plus additional specified information to any LAN device that requests DHCP served addresses.
    - DHCP Relay: With this option enabled, DHCP clients on the LAN can receive IP address leases and corresponding information from a DHCP server on a different subnet. Specify the Relay Gateway, and when LAN clients make a DHCP request it will be passed along to the server accessible via the Relay Gateway IP address.
    - If DHCP is being enabled, enter the following DHCP server parameters:
    - Starting and Ending IP Addresses: Enter the first and last continuous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address in this range. The default starting address is 192.168.10.2. The default ending address is 192.168.10.100. These addresses should be in the same IP address subnet as the router's LAN IP address. You may wish to save part of the subnet range for devices with statically assigned IP addresses in the LAN.
    - Primary and Secondary DNS servers: If configured domain name system (DNS) servers are available on the LAN enter their IP addresses here.
    - WINS Server (optional): Enter the IP address for the WINS server or, if present in your network, the Windows NetBios server.

- Lease Time: Enter the time, in hours, for which IP addresses are leased to clients.
- Enable DNS Proxy: To enable the router to act as a proxy for all DNS requests and communicate with the ISP's DNS servers, click the checkbox.

3. Click Save Settings to apply all changes.

**Figure 1: Setup page for LAN TCP/IP settings**



## 2.1.1 LAN Configuration in an IPv6 Network

***Advanced > IPv6 > IPv6 LAN > IPv6 LAN Config***

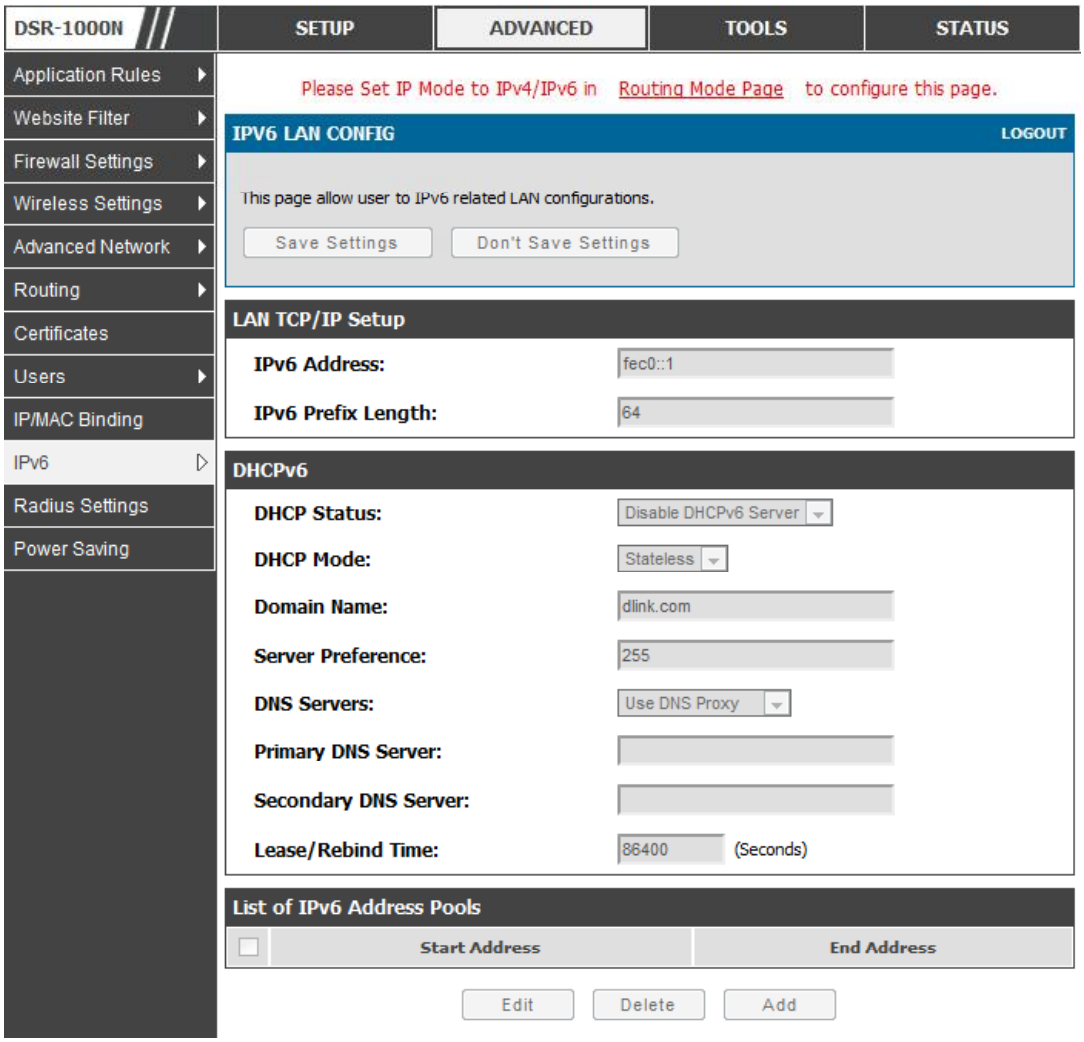
In IPv6 mode, the LAN DHCP server is enabled by default (similar to IPv4 mode). The DHCPv6 server will serve IPv6 addresses from configured address pools with the IPv6 Prefix Length assigned to the LAN.

IPv4 / IPv6 mode must be enabled in the ***Advanced > IPv6 > IP mode*** to enable IPv6 configuration options.

### LAN Settings

The default IPv6 LAN address for the router is **fec0::1**. You can change this 128 bit IPv6 address based on your network requirements. The other field that defines the LAN settings for the router is the prefix length. The IPv6 network (subnet) is identified by the initial bits of the address called the prefix. By default this is **64** bits long. All hosts in the network have common initial bits for their IPv6 address; the number of common initial bits in the network's addresses is set by the prefix length field.

**Figure 2: IPv6 LAN and DHCPv6 configuration**




If you change the IP address and click Save Settings, the GUI will not respond. Open a new connection to the new IP address and log in again. Be sure the LAN host (the machine used to manage the router) has obtained IP address from newly assigned pool (or has a static IP address in the router's LAN subnet) before accessing the router via changed IP address.

As with an IPv4 LAN network, the router has a DHCPv6 server. If enabled, the router assigns an IP address within the specified range plus additional specified information to any LAN PC that requests DHCP served addresses.

The following settings are used to configure the DHCPv6 server:

- DHCP Mode: The IPv6 DHCP server is either stateless or stateful. If stateless is selected an external IPv6 DHCP server is not required as the IPv6 LAN hosts are auto-configured by this router. In this case the router advertisement daemon (RADVD) must be configured on this device and ICMPv6 router discovery messages are used by the host for auto-configuration. There are no managed addresses to serve the LAN nodes. If stateful is selected the IPv6 LAN host will rely on an external DHCPv6 server to provide required configuration settings
- The domain name of the DHCPv6 server is an optional setting
- Server Preference is used to indicate the preference level of this DHCP server. DHCP advertise messages with the highest server preference value to a LAN host are preferred over other DHCP server advertise messages. The default is 255.
- The DNS server details can be manually entered here (primary/secondary options. An alternative is to allow the LAN DHCP client to receive the DNS server details from the ISP directly. By selecting Use DNS proxy, this router acts as a proxy for all DNS requests and communicates with the ISP's DNS servers (a WAN configuration parameter).
- Primary and Secondary DNS servers: If there are configured domain name system (DNS) servers available on the LAN enter the IP addresses here.
- Lease/Rebind time sets the duration of the DHCPv6 lease from this router to the LAN client.

### IPv6 Address Pools

This feature allows you to define the IPv6 delegation prefix for a range of IP addresses to be served by the gateway's DHCPv6 server. Using a delegation prefix you can automate the process of informing other networking equipment on the LAN of DHCP information specific for the assigned prefix.

## 2.1.2 Configuring IPv6 Router Advertisements

Router Advertisements are analogous to IPv4 DHCP assignments for LAN clients, in that the router will assign an IP address and supporting network information to devices that are configured to accept such details. Router Advertisement is required in an IPv6 network is required for stateless auto configuration of the IPv6 LAN. By configuring the Router Advertisement Daemon on this router, the DSR will listen on the LAN for router solicitations and respond to these LAN hosts with router advisements.

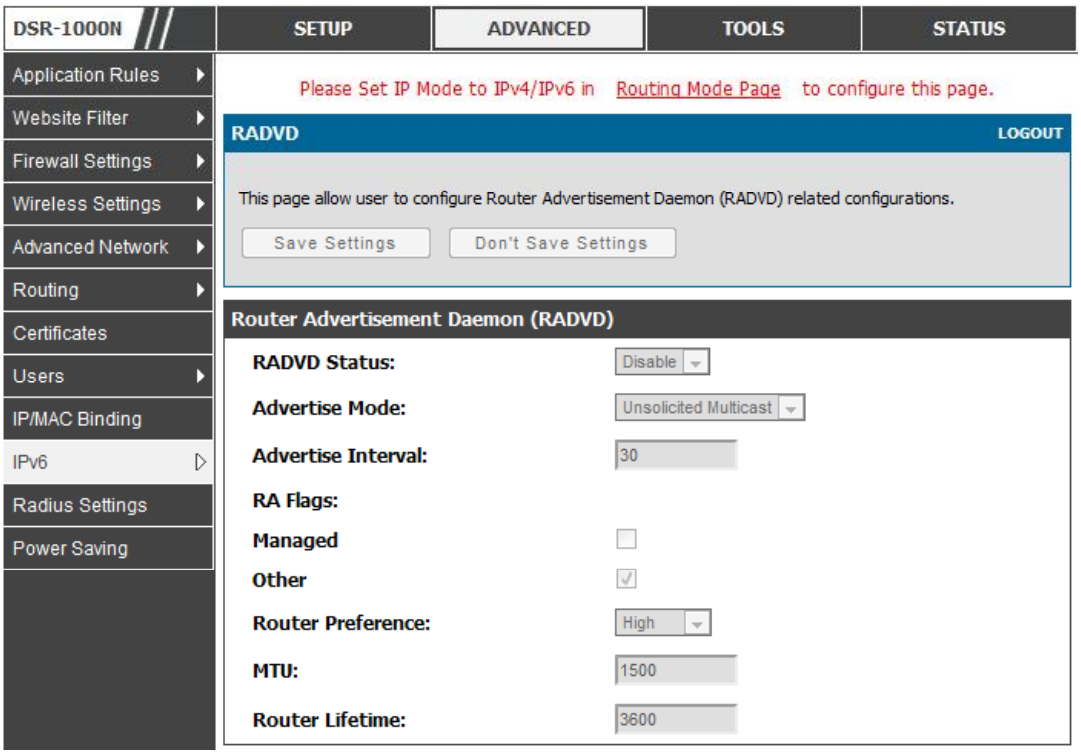
## RADVD

### *Advanced > IPv6 > IPv6 LAN > Router Advertisement*

To support stateless IPv6 auto configuration on the LAN, set the RADVD status to Enable. The following settings are used to configure RADVD:

- Advertise Mode: Select Unsolicited Multicast to send router advertisements (RA's) to all interfaces in the multicast group. To restrict RA's to well known IPv6 addresses on the LAN, and thereby reduce overall network traffic, select Unicast only.
- Advertise Interval: When advertisements are unsolicited multicast packets, this interval sets the maximum time between advertisements from the interface. The actual duration between advertisements is a random value between one third of this field and this field. The default is 30 seconds.
- RA Flags: The router advertisements (RA's) can be sent with one or both of these flags. Chose Managed to use the administered /stateful protocol for address auto configuration. If the Other flag is selected the host uses administered/stateful protocol for non-address auto configuration.
- Router Preference: this low/medium/high parameter determines the preference associated with the RADVD process of the router. This is useful if there are other RADVD enabled devices on the LAN as it helps avoid conflicts for IPv6 clients.
- MTU: The router advertisement will set this maximum transmission unit (MTU) value for all nodes in the LAN that are autoconfigured by the router. The default is 1500.
- Router Lifetime: This value is present in RA's and indicates the usefulness of this router as a default router for the interface. The default is 3600 seconds. Upon expiration of this value, a new RADVD exchange must take place between the host and this router.

**Figure 3: Configuring the Router Advertisement Daemon**




## Advertisement Prefixes

### *Advanced > IPv6 > IPv6 LAN > Advertisement Prefixes*

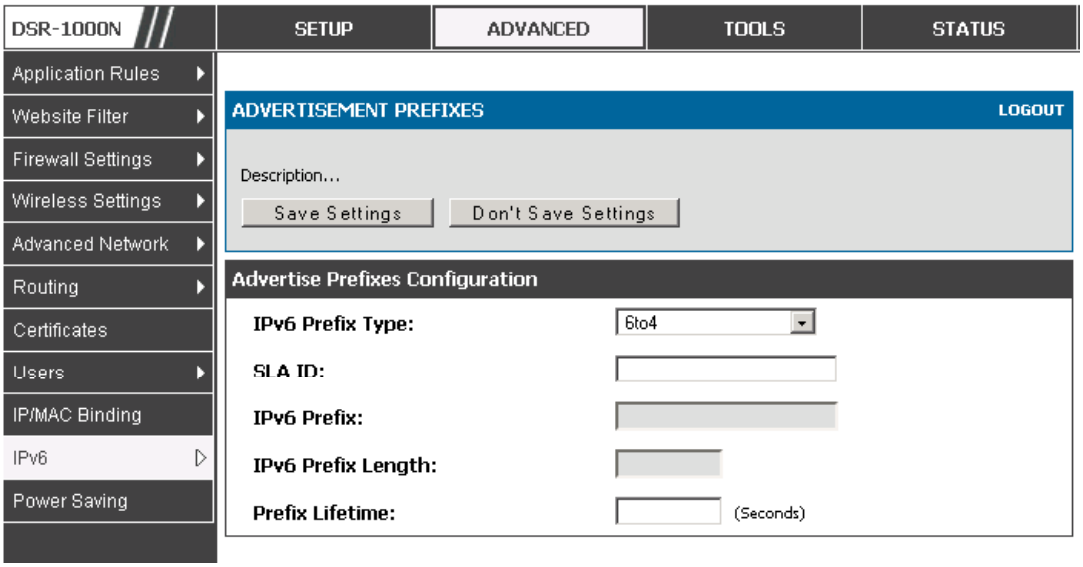
The router advertisements configured with advertisement prefixes allow this router to inform hosts how to perform stateless address auto configuration. Router advertisements contain a list of subnet prefixes that allow the router to determine neighbors and whether the host is on the same link as the router.

The following prefix options are available for the router advertisements:

- IPv6 Prefix Type: To ensure hosts support IPv6 to IPv4 tunnel select the 6to4 prefix type. Selecting Global/Local/ISATAP will allow the nodes to support all other IPv6 routing options
- SLA ID: The SLA ID (Site-Level Aggregation Identifier) is available when 6to4 Prefixes are selected. This should be the interface ID of the router's LAN interface used for router advertisements.
- IPv6 Prefix: When using Global/Local/ISATAP prefixes, this field is used to define the IPv6 network advertised by this router.

- IPv6 Prefix Length: This value indicates the number contiguous, higher order bits of the IPv6 address that define up the network portion of the address. Typically this is 64.
- Prefix Lifetime: This defines the duration (in seconds) that the requesting node is allowed to use the advertised prefix. It is analogous to DHCP lease time in an IPv4 network.

**Figure 4: IPv6 Advertisement Prefix settings**




# 2.2 VLAN Configuration

The router supports virtual network isolation on the LAN with the use of VLANs. LAN devices can be configured to communicate in a subnetwork defined by VLAN identifiers. LAN ports can be assigned unique VLAN IDs so that traffic to and from that physical port can be isolated from the general LAN. VLAN filtering is particularly useful to limit broadcast packets of a device in a large network

VLAN support is disabled by default in the router. In the VLAN Configuration page, enable VLAN support on the router and then proceed to the next section to define the virtual network.

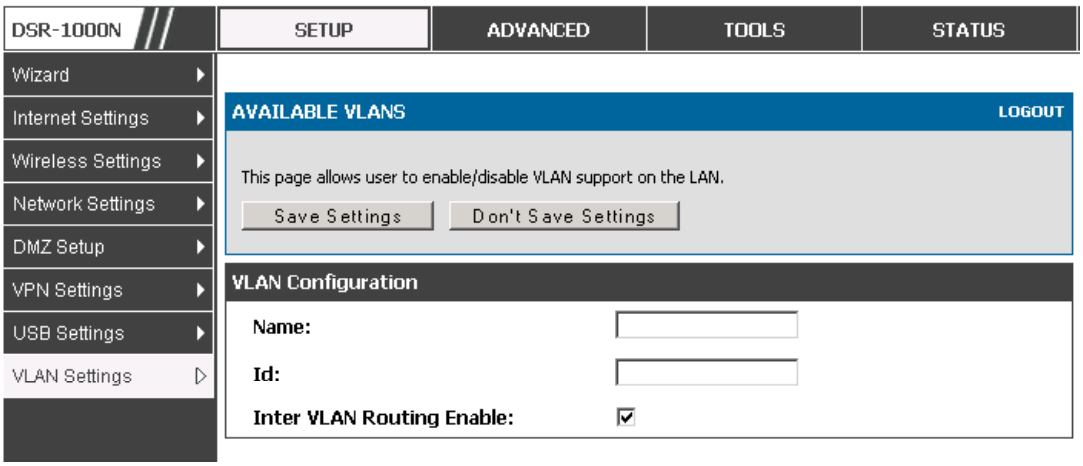
### *Setup > VLAN Settings > Available VLAN*

The Available VLAN page shows a list of configured VLANs by name and VLAN ID. A VLAN membership can be created by clicking the Add button below the List of Available VLANs.

A VLAN membership entry consists of a VLAN identifier and the numerical VLAN ID which is assigned to the VLAN membership. The VLAN ID value can be any number from 2 to 4091. VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. By enabling Inter VLAN Routing, you

will allow traffic from LAN hosts belonging to this VLAN ID to pass through to other configured VLAN IDs that have Inter VLAN Routing enabled.

**Figure 5: Adding VLAN memberships to the LAN**




## 2.2.1 Associating VLANs to ports

In order to tag all traffic through a specific LAN port with a VLAN ID, you can associate a VLAN to a physical port.

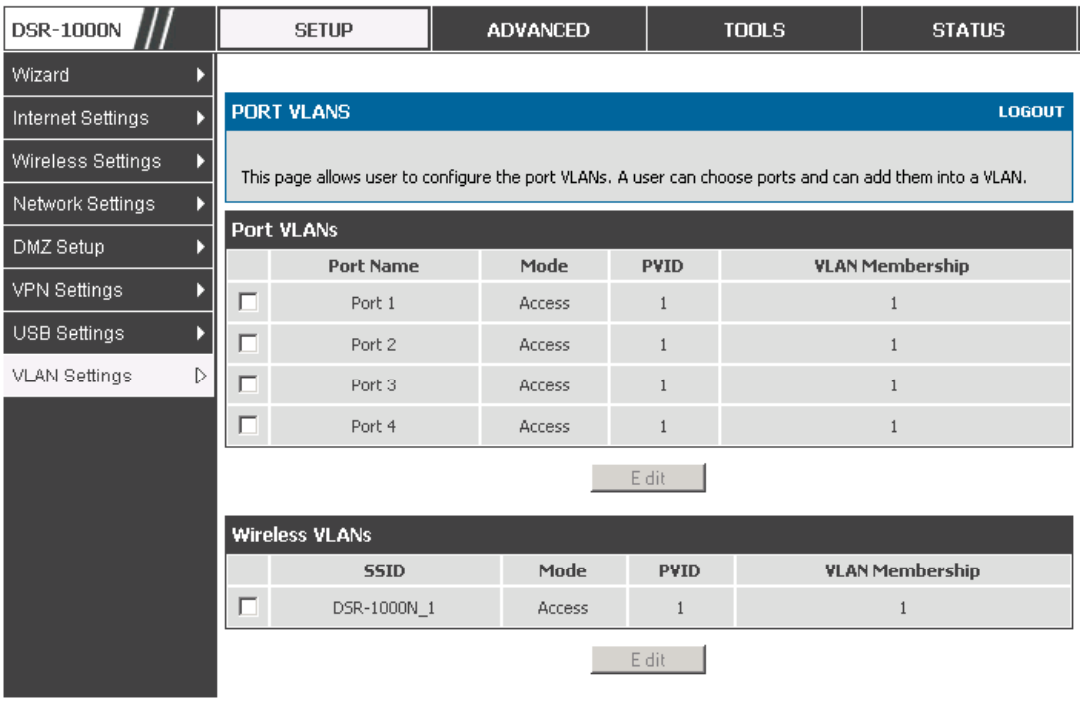
### *Setup > VLAN Settings > Port VLAN*

VLAN membership properties for the LAN and wireless LAN are listed on this page. The VLAN Port table displays the port identifier, the mode setting for that port and VLAN membership information. The configuration page is accessed by selecting one of the four physical ports or a configured access point and clicking Edit.

The edit page offers the following configuration options:

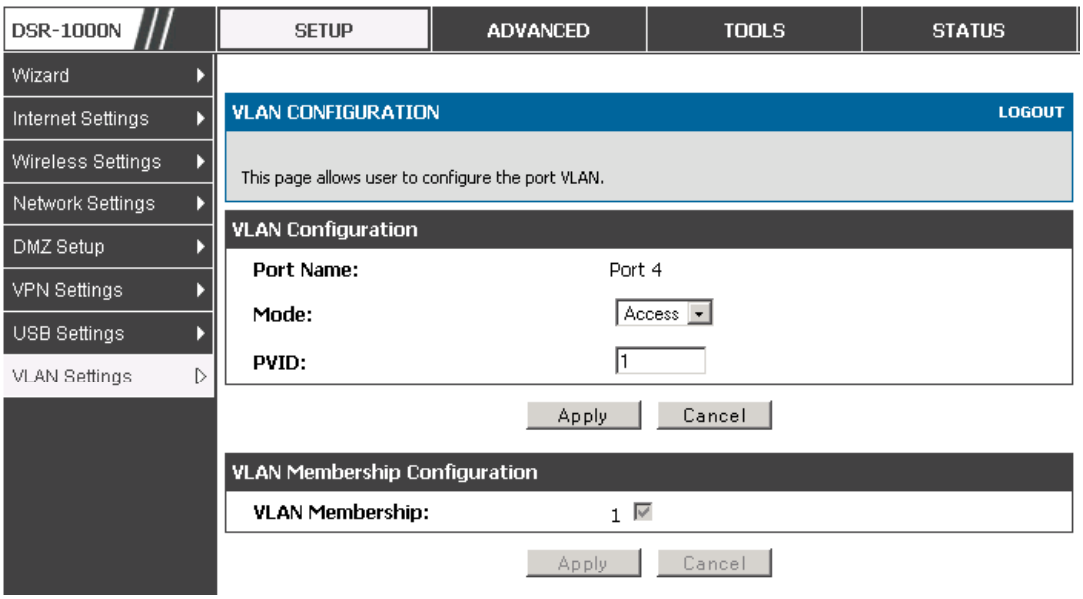
- Mode: The mode of this VLAN can be General, Access, or Trunk. The default is access.
- In General mode the port is a member of a user selectable set of VLANs. The port sends and receives data that is tagged or untagged with a VLAN ID. If the data into the port is untagged, it is assigned the defined PVID. In the configuration from Figure 4, Port 3 is a General port with PVID 3, so untagged data into Port 3 will be assigned PVID 3. All tagged data sent out of the port with the same PVID will be untagged. This is mode is typically used with IP Phones that have dual Ethernet ports. Data coming from phone to the switch port on the router will be tagged. Data passing through the phone from a connected device will be untagged.

**Figure 6: Port VLAN list**




- In Access mode the port is a member of a single VLAN (and only one). All data going into and out of the port is untagged. Traffic through a port in access mode looks like any other Ethernet frame.
- In Trunk mode the port is a member of a user selectable set of VLANs. All data going into and out of the port is tagged. Untagged coming into the port is not forwarded, except for the default VLAN with PVID=1, which is untagged. Trunk ports multiplex traffic for multiple VLANs over the same physical link.
- Select PVID for the port when the General mode is selected.
- Configured VLAN memberships will be displayed on the VLAN Membership Configuration for the port. By selecting one more VLAN membership options for a General or Trunk port, traffic can be routed between the selected VLAN membership IDs

**Figure 7: Configuring VLAN membership for a port**




# 2.3 Configurable Port: DMZ Setup

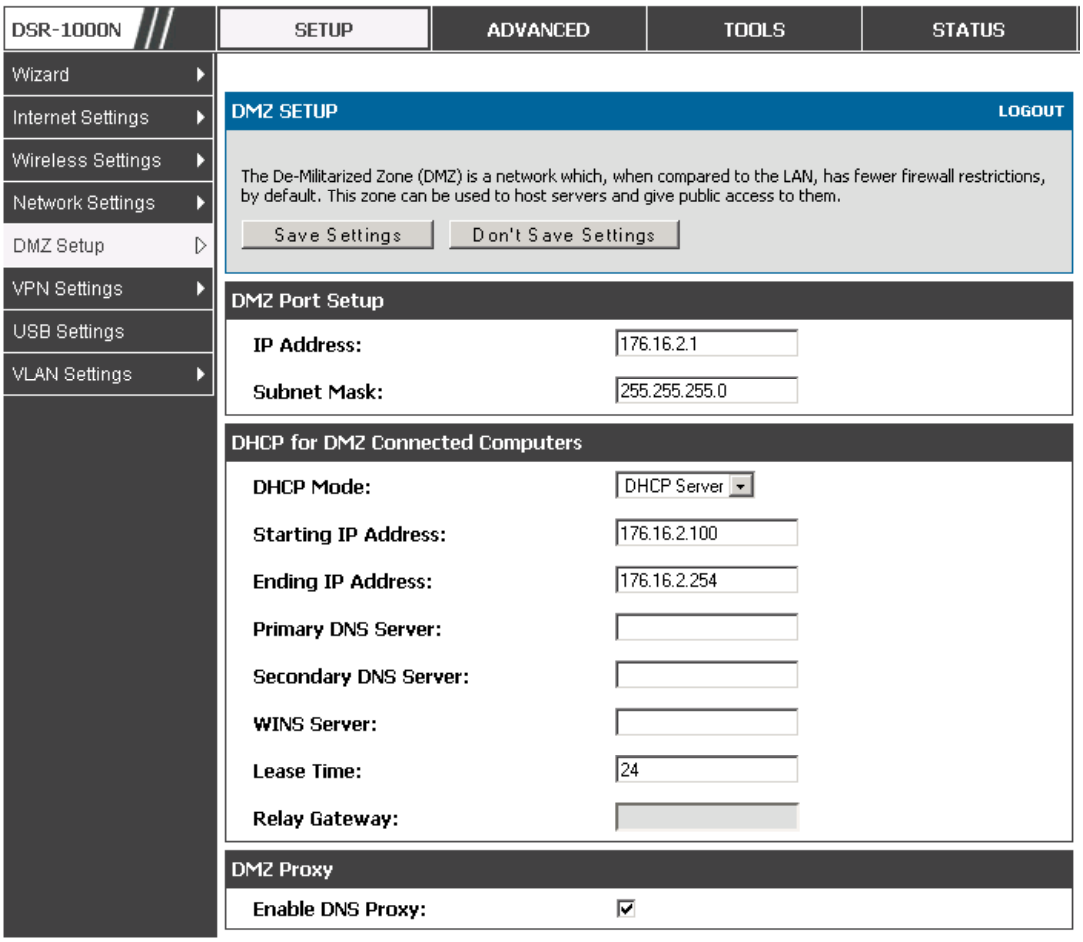
> DSR-250N does not have a configurable port – there is no DMZ support.

This router supports one of the physical ports to be configured as a secondary WAN Ethernet port or a dedicated DMZ port. A DMZ is a subnetwork that is open to the public but behind the firewall. The DMZ adds an additional layer of security to the LAN, as specific services/ports that are exposed to the internet on the DMZ do not have to be exposed on the LAN. It is recommended that hosts that must be exposed to the internet (such as web or email servers) be placed in the DMZ network. Firewall rules can be allowed to permit access specific services/ports to the DMZ from both the LAN or WAN. In the event of an attack to any of the DMZ nodes, the LAN is not necessarily vulnerable as well.

### *Setup > DMZ Setup > DMZ Setup Configuration*

DMZ configuration is identical to the LAN configuration. There are no restrictions on the IP address or subnet assigned to the DMZ port, other than the fact that it cannot be identical to the IP address given to the LAN interface of this gateway.

**Figure 8: DMZ configuration**




> In order to configure a DMZ port, the router's configurable port must be set to DMZ in the ***Setup > Internet Settings > Configurable Port*** page.

# 2.4 Universal Plug and Play (UPnP)

***Advanced > Advanced Network > UPnP***

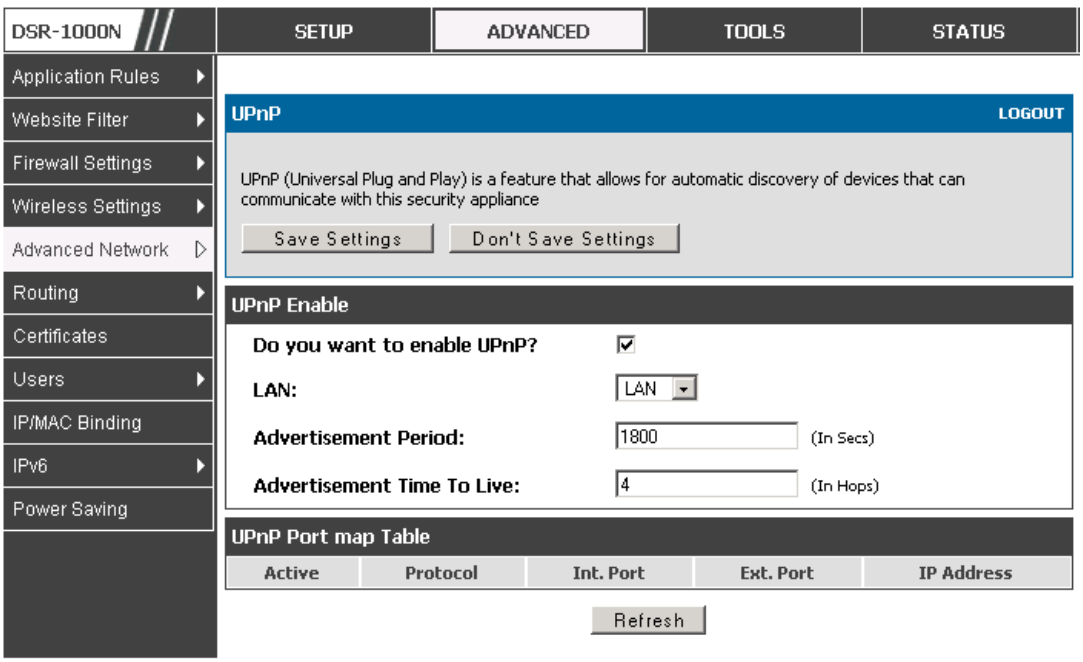
Universal Plug and Play (UPnP) is a feature that allows the router to discovery devices on the network that can communicate with the router and allow for auto configuration. If a network device is detected by UPnP, the router can open internal or external ports for the traffic protocol required by that network device.

Once UPnP is enabled, you can configure the router to detect UPnP-supporting devices on the LAN (or a configured VLAN). If disabled, the router will not allow for automatic device configuration.

Configure the following settings to use UPnP:

- Advertisement Period: This is the frequency that the router broadcasts UPnP information over the network. A large value will minimize network traffic but cause delays in identifying new UPnP devices to the network.
- Advertisement Time to Live: This is expressed in hops for each UPnP packet. This is the number of steps a packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range. A default of 4 is typical for networks with few switches.

**Figure 9: UPnP Configuration**




UPnP Port map Table

The UPnP Port map Table has the details of UPnP devices that respond to the router's advertisements. The following information is displayed for each detected device:

- Active: A yes/no indicating whether the port of the UPnP device that established a connection is currently active
- Protocol: The network protocol (i.e. HTTP, FTP, etc.) used by the DSR
- Int. Port (Internal Port): The internal ports opened by UPnP (if any)
- Ext. Port (External Port): The external ports opened by UPnP (if any)

- IP Address: The IP address of the UPnP device detected by this router

Click Refresh to refresh the portmap table and search for any new UPnP devices.

# 2.5 Captive Portal

DSR-250N does not have support for the Captive Portal feature.

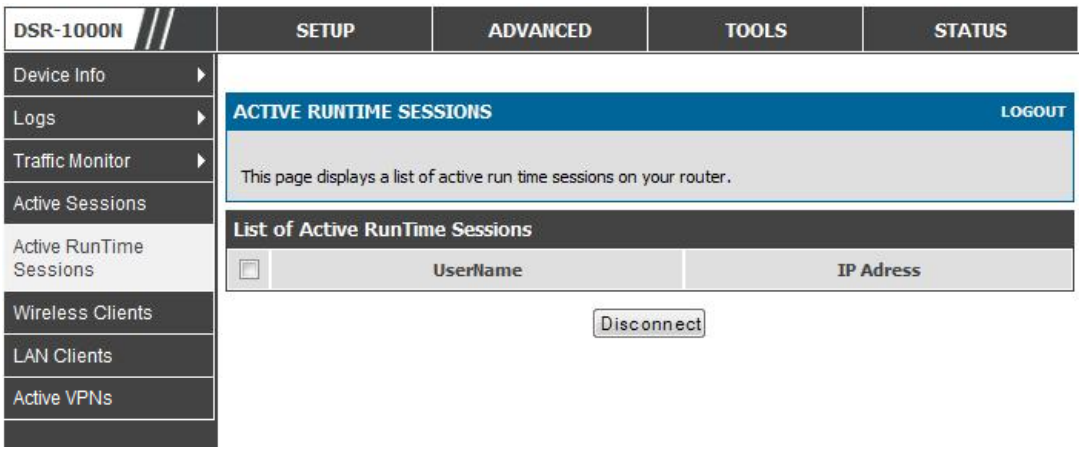
LAN users can gain internet access via web portal authentication with the DSR. Also referred to as Run-Time Authentication, a Captive Portal is ideal for a web café scenario where users initiate HTTP connection requests for web access but are not interested in accessing any LAN services. Firewall policies underneath will define which users require authentication for HTTP access, and when a matching user request is made the DSR will intercept the request and prompt for a username / password. The login credentials are compared against the RunTimeAuth users in user database prior to granting HTTP access.

Captive Portal is available for LAN users only and not for DMZ hosts.

### *Status > Active RunTime Sessions*

The Active Runtime internet sessions through the router's firewall are listed in the below table. These users are present in the local or external user database and have had their login credentials approved for internet access. A 'Disconnect' button allows the DSR admin to selectively drop an authenticated user.

**Figure 10: Active Runtime sessions**



# Chapter 3. Connecting to the Internet: WAN Setup

This router has two WAN ports that can be used to establish a connection to the internet. The following ISP connection types are supported: DHCP, Static, PPPoE, PPTP, L2TP, 3G Internet (via USB modem).

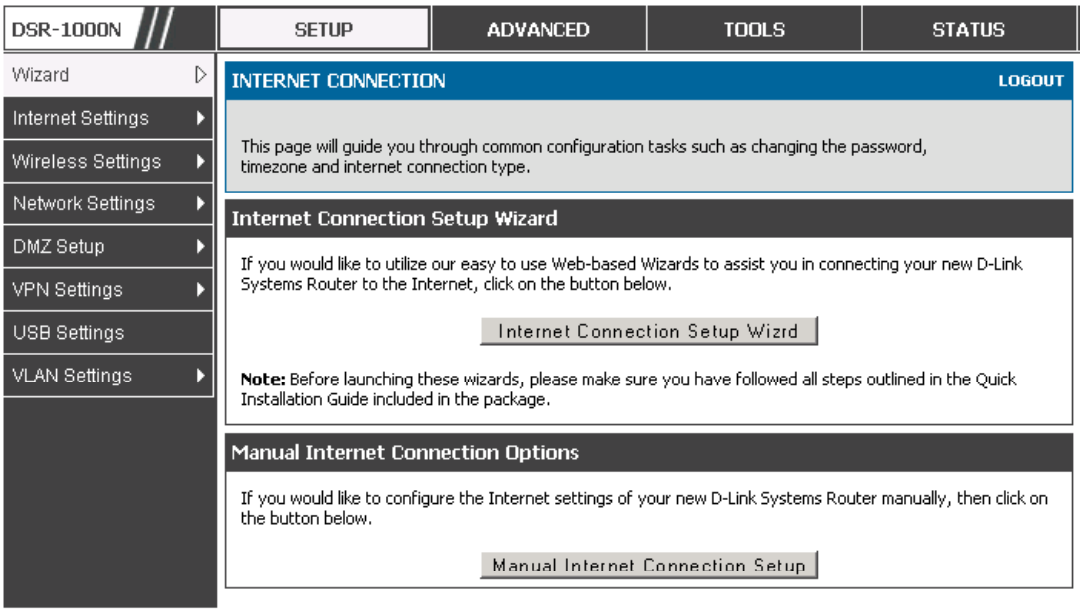
It is assumed that you have arranged for internet service with your Internet Service Provider (ISP). Please contact your ISP or network administrator for the configuration information that will be required to setup the router.

## 3.1 Internet Setup Wizard

***Setup > Wizard > Internet***

The Internet Connection Setup Wizard is available for users new to networking. By going through a few straightforward configuration pages you can take the information provided by your ISP to get your WAN connection up and enable internet access for your network.

**Figure 11: Internet Connection Setup Wizard**




You can start using the Wizard by logging in with the administrator password for the router. Once authenticated set the time zone that you are located in, and then choose the type of ISP connection type: DHCP, Static, PPPoE, PPTP, L2TP. Depending on the connection type a username/password may be required to register this router with the ISP. In most cases the default settings can be used if the ISP did not specify that parameter. The last step in the Wizard is to click the Connect button, which confirms the settings by establishing a link with the ISP. Once connected, you can move on and configure other features in this router.

> 3G Internet access with a USB modem is supported on the secondary WAN port (WAN2). The Internet Connection Setup Wizard assists with the primary WAN port (WAN1) configuration only.

# 3.2 WAN Configuration

***Setup > Internet Settings > WAN1 Setup***

You must either allow the router to detect WAN connection type automatically or configure manually the following basic settings to enable Internet connectivity:

- ISP Connection type: Based on the ISP you have selected for the primary WAN link for this router, choose Static IP address, DHCP client, Point-to-Point Tunneling Protocol (PPTP), Point-to-Point Protocol over Ethernet (PPPoE), Layer 2 Tunneling Protocol (L2TP). Required fields for the selected ISP type become highlighted. Enter the following information as needed and as provided by your ISP:
- PPPoE Profile Name. This menu lists configured PPPoE profiles, particularly useful when configuring multiple PPPoE connections (i.e. for Japan ISPs that have multiple PPPoE support).
- ISP login information. This is required for PPTP and L2TP ISPs.
    - User Name
    - Password
    - Secret (required for L2TP only)
- MPPE Encryption: For PPTP links, your ISP may require you to enable Microsoft Point-to-Point Encryption (MPPE).
- Split Tunnel (supported for PPTP and L2TP connection). This setting allows your LAN hosts to access internet sites over this WAN link while still permitting VPN traffic to be directed to a VPN configured on this WAN port.

> If split tunnel is enabled, DSR won't expect a default route from the ISP server. In such case, user has to take care of routing manually by configuting the routing from Static Routing page.

- Connectivity Type: To keep the connection always on, click Keep Connected. To log out after the connection is idle for a period of time (useful if your ISP costs are based on logon times), click Idle Timeout and enter the time, in minutes, to wait before disconnecting in the Idle Time field.

- My IP Address: Enter the IP address assigned to you by the ISP.
- Server IP Address: Enter the IP address of the PPTP or L2TP server.

DSR-250N doesn't have a dual WAN support.

## 3.2.1 WAN Port IP address

Your ISP assigns you an IP address that is either dynamic (newly generated each time you log in) or static (permanent). The IP Address Source option allows you to define whether the address is statically provided by the ISP or should be received dynamically at each login. If static, enter your IP address, IPv4 subnet mask, and the ISP gateway's IP address. PPTP and L2TP ISPs also can provide a static IP address and subnet to configure, however the default is to receive that information dynamically from the ISP.

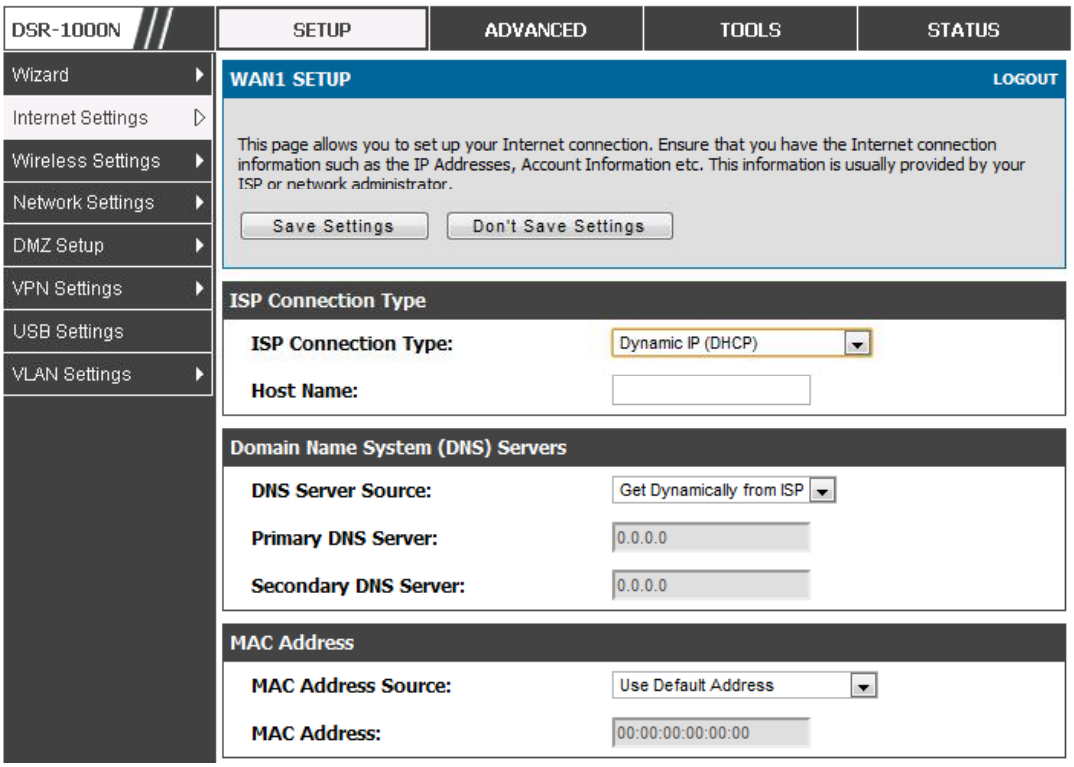
## 3.2.2 WAN DNS Servers

The IP Addresses of WAN Domain Name Servers (DNS) are typically provided dynamically from the ISP but in some cases you can define the static IP addresses of the DNS servers. DNS servers map Internet domain names (example: www.google.com) to IP addresses. Click to indicate whether to get DNS server addresses automatically from your ISP or to use ISP-specified addresses. If its latter, enter addresses for the primary and secondary DNS servers. To avoid connectivity problems, ensure that you enter the addresses correctly.

## 3.2.3 DHCP WAN

For DHCP client connections, you can choose the MAC address of the router to register with the ISP. In some cases you may need to clone the LAN host's MAC address if the ISP is registered with that LAN host.

**Figure 12: Manual WAN configuration**

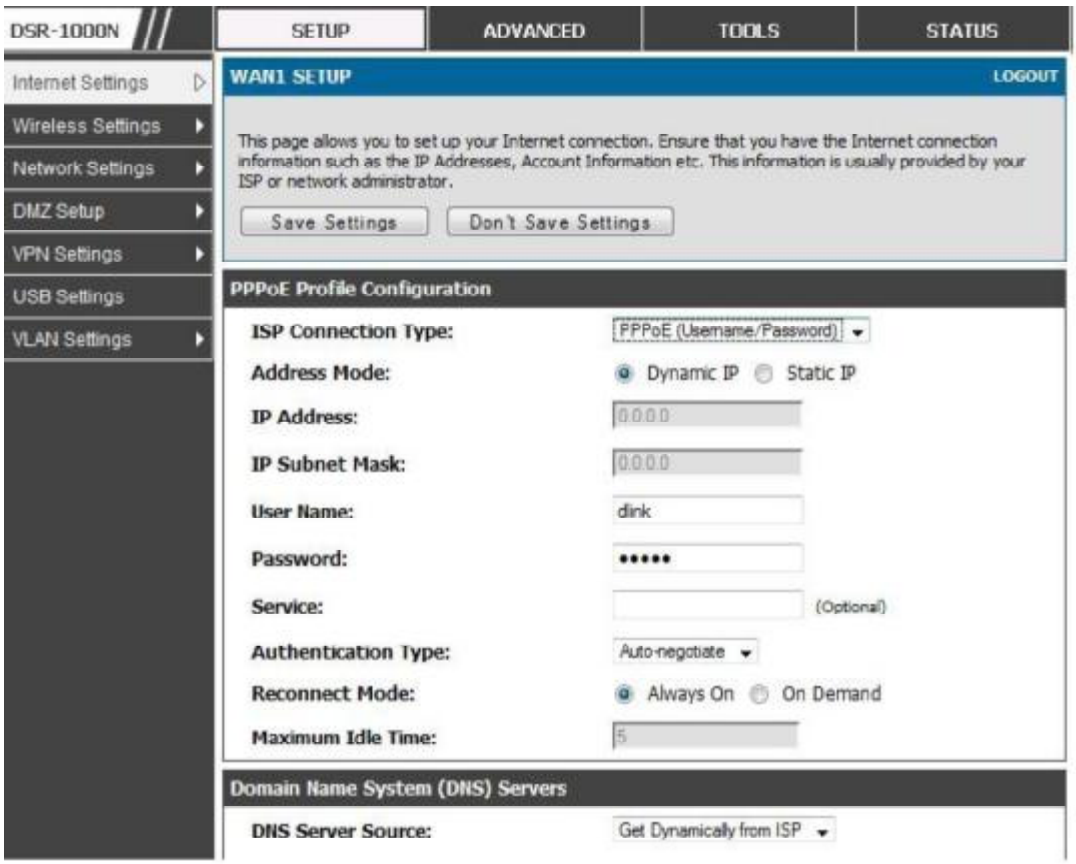



## 3.2.4 PPPoE

***Setup > Internet Settings***

The PPPoE ISP settings are defined on the WAN Configuration page. There are two types of PPPoE ISP's supported by the DSR: the standard username/password PPPoE and Japan Multiple PPPoE.

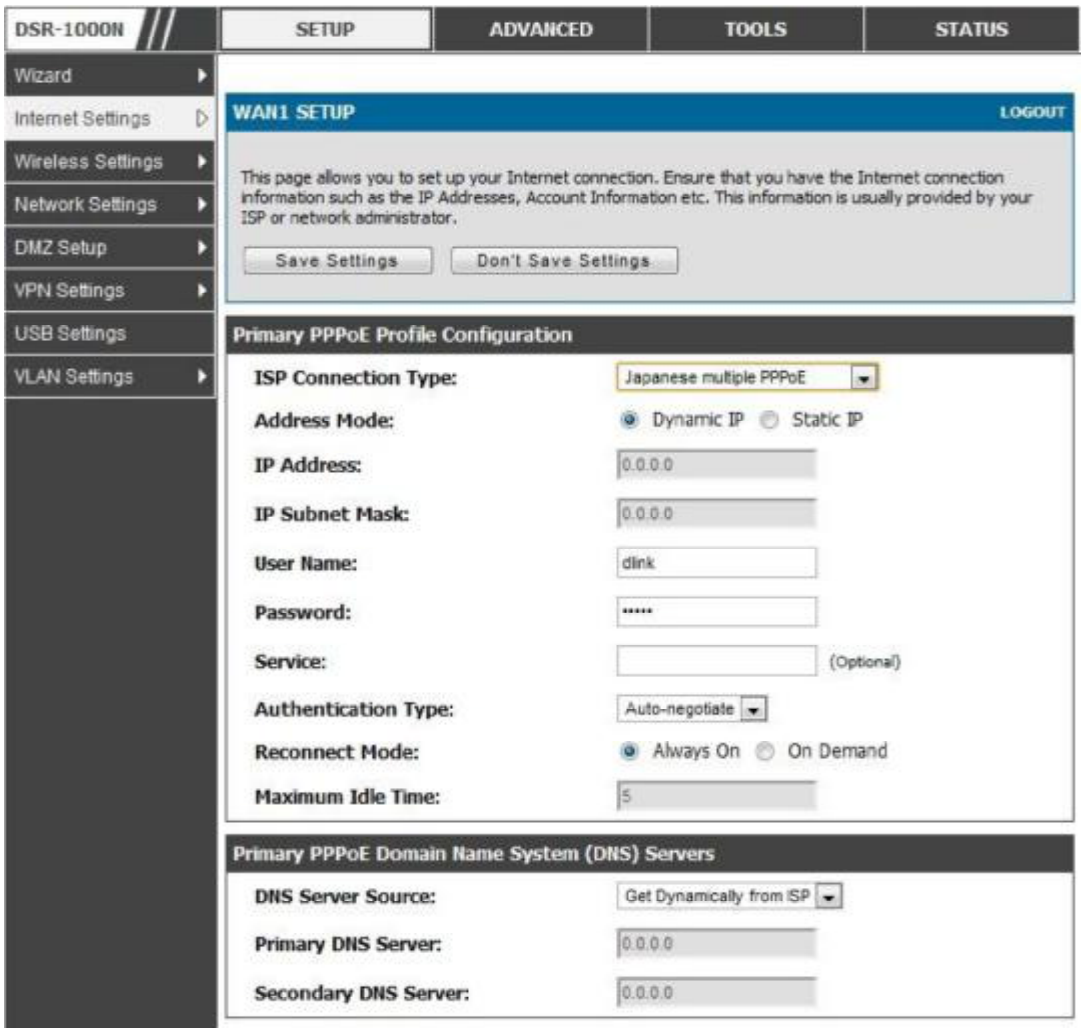
**Figure 13: PPPoE configuration for standard ISPs**




Most PPPoE ISP's use a single control and data connection, and require username / password credentials to login and authenticate the DSR with the ISP. The ISP connection type for this case is "PPPoE (Username/Password)". The GUI will prompt you for authentication, service, and connection settings in order to establish the PPPoE link.

For some ISP's, most popular in Japan, the use of "Japanese Multiple PPPoE" is required in order to establish concurrent primary and secondary PPPoE connections between the DSR and the ISP. The Primary connection is used for the bulk of data and internet traffic and the Secondary PPPoE connection carries ISP specific (i.e. control) traffic between the DSR and the ISP.

**Figure 14: WAN configuration for Japanese Multiple PPPoE (part 1)**

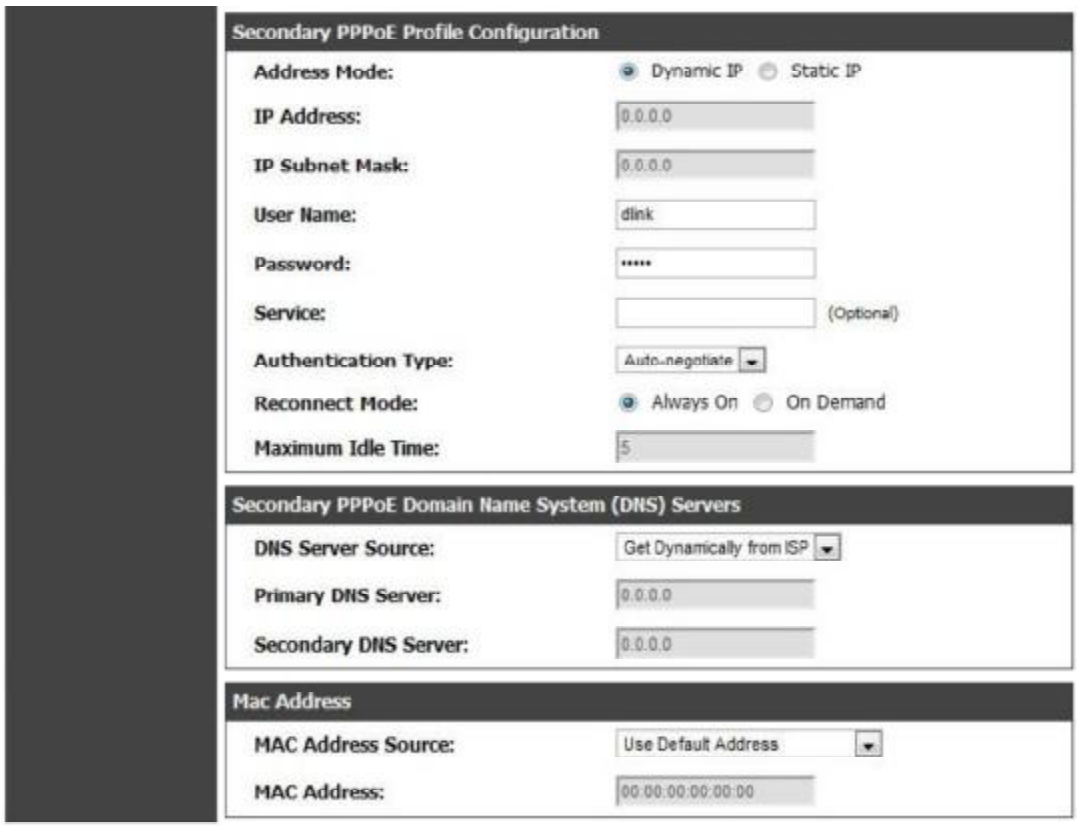



There are a few key elements of a multiple PPPoE connection:

- Primary and secondary connections are concurrent
- Each session has a DNS server source for domain name lookup, this can be assigned by the ISP or configured through the GUI
- The DSR acts as a DNS proxy for LAN users
- Only HTTP requests that specifically identify the secondary connection's domain name (for example *.flets) will use the secondary profile to access the content available through this secondary PPPoE terminal. All other HTTP / HTTPS requests go through the primary PPPoE connection.

When Japanese multiple PPPoE is configured and secondary connection is up, some predefined routes are added on that interface. These routes are needed to access the internal domain of the ISP where he hosts various services. These routes can even be configured through the static routing page as well.

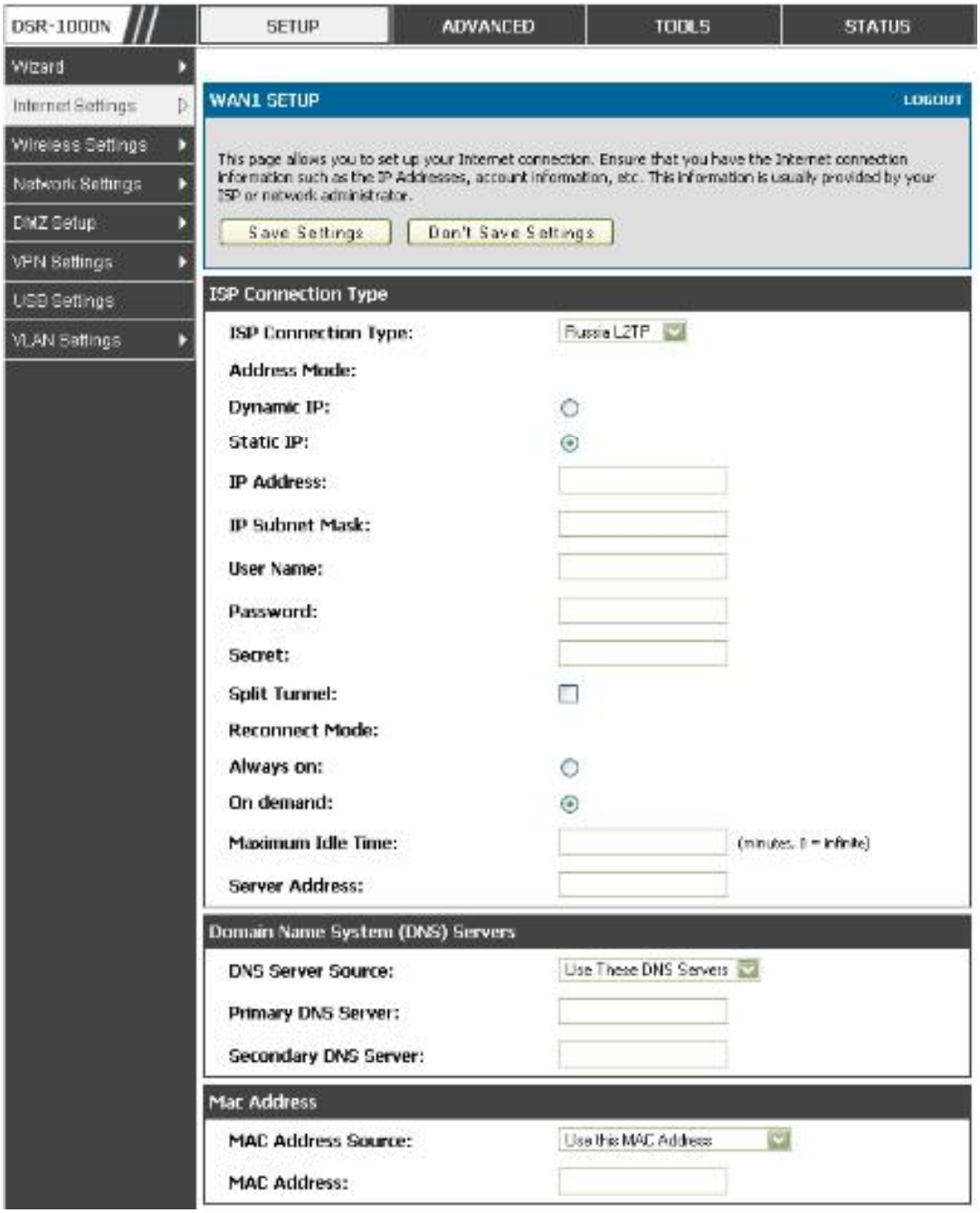
**Figure 15: WAN configuration for Multiple PPPoE (part 2)**




## 3.2.5 Russia L2TP and PPTP WAN

For Russia L2TP WAN connections, you can choose the address mode of the connection to get an IP address from the ISP or configure a static IP address provided by the ISP. For DHCP client connections, you can choose the MAC address of the router to register with the ISP. In some cases you may need to clone the LAN host's MAC address if the ISP is registered with that LAN host.

**Figure 16: Russia L2TP ISP configuration**



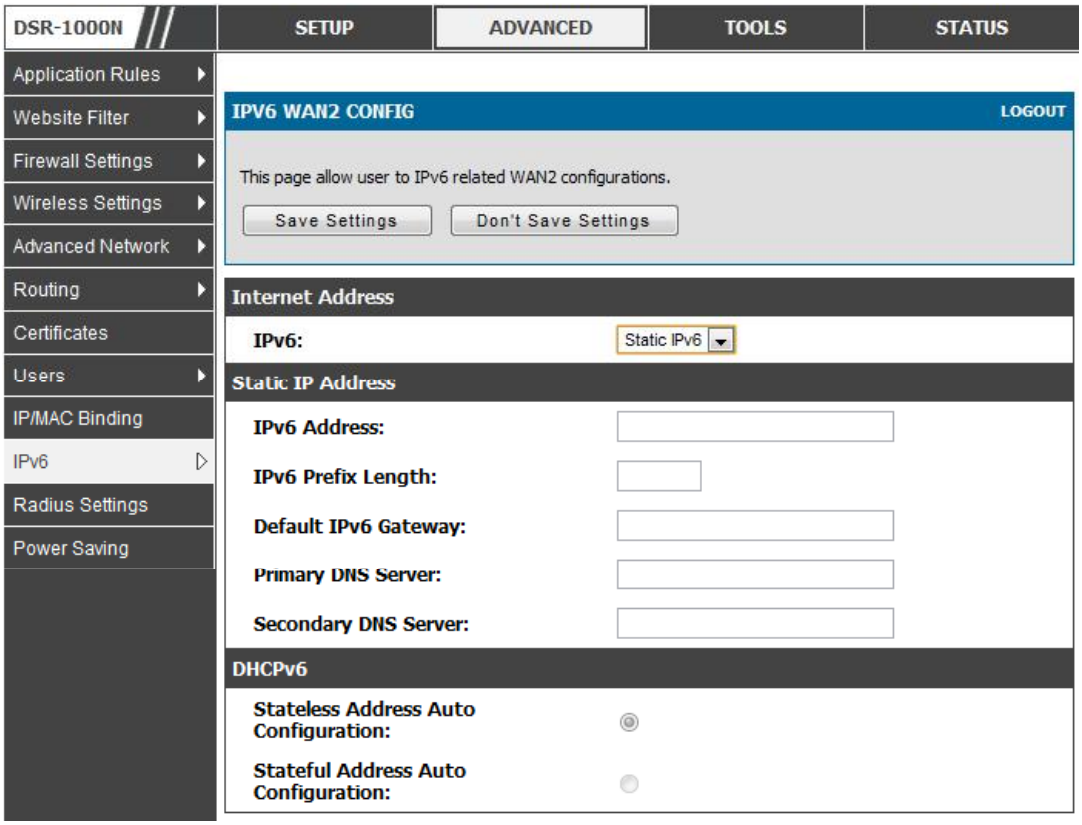

## 3.2.6 WAN Configuration in an IPv6 Network

***Setup > IPv6 > IPv6 WAN1 Config***

For IPv6 WAN connections, this router can have a static IPv6 address or receive connection information when configured as a DHCPv6 client. In the case where the ISP assigns you a fixed address to access the internet, the static configuration settings must be completed. In addition to the IPv6 address assigned to your router, the IPv6 prefix length defined by the ISP is needed. The default IPv6 Gateway address is the server at the ISP that this router will connect to for accessing the internet. The primary and secondary DNS servers on the ISP's IPv6 network are used for resolving internet addresses, and these are provided along with the static IP address and prefix length from the ISP.

When the ISP allows you to obtain the WAN IP settings via DHCP, you need to provide details for the DHCPv6 client configuration. The DHCPv6 client on the gateway can be either stateless or stateful. If a stateful client is selected the gateway will connect to the ISP's DHCPv6 server for a leased address. For stateless DHCP there need not be a DHCPv6 server available at the ISP, rather ICMPv6 discover messages will originate from this gateway and will be used for auto configuration. A third option to specify the IP address and prefix length of a preferred DHCPv6 server is available as well.

**Figure 17: IPv6 WAN Setup page**



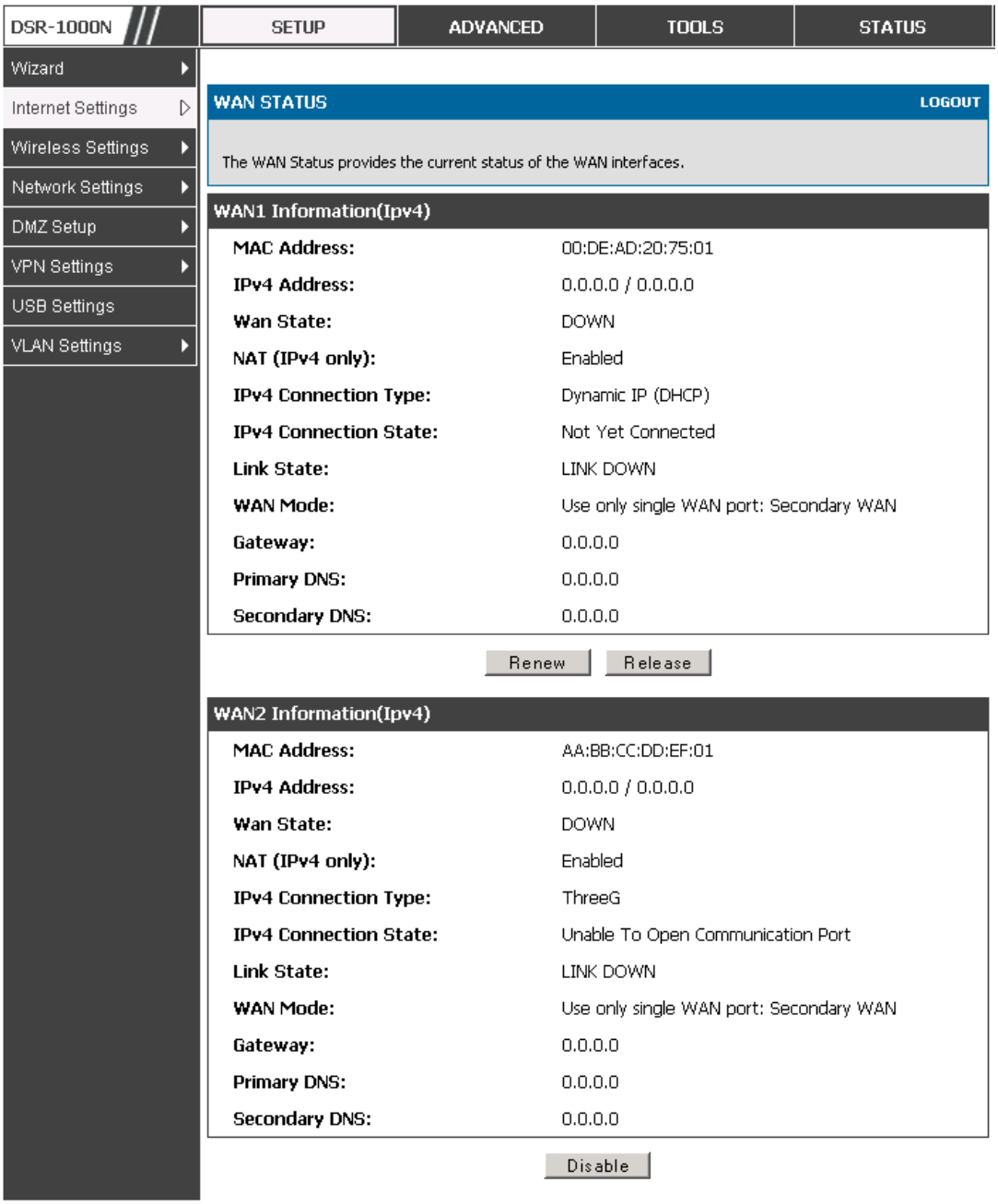

## 3.2.7 Checking WAN Status

***Setup > Internet Settings > WAN Status***

The status and summary of configured settings for both WAN1 and WAN2 are available on the WAN Status page. You can view the following key connection status information for each WAN port:

- Connection time: The connection uptime
- Connection type: Dynamic IP or Static IP
- Connection state: This is whether the WAN is connected or disconnected to an ISP. The Link State is whether the physical WAN connection in place; the Link State can be UP (i.e. cable inserted) while the WAN Connection State is down.
- IP address / subnet mask: IP Address assigned
- Gateway IP address: WAN Gateway Address

**Figure 18: Connection Status information for both WAN ports**




The WAN status page allows you to Enable or Disable static WAN links. For WAN settings that are dynamically received from the ISP, you can Renew or Release the link parameters if required.

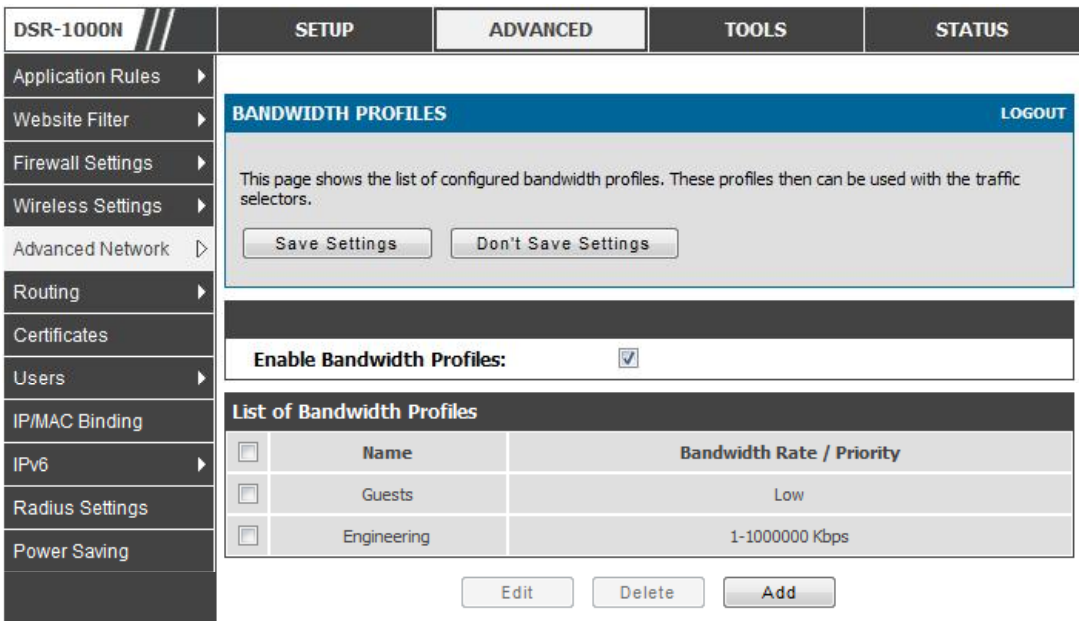
# 3.3 Bandwidth Controls

***Advanced > Advanced Network > Traffic Management > Bandwidth Profiles***

Bandwidth profiles allow you to regulate the traffic flow from the LAN to WAN 1 or WAN 2. This is useful to ensure that low priority LAN users (like guests or HTTP service) do not monopolize the available WAN's bandwidth for cost-savings or bandwidth-priority-allocation purposes.

Bandwidth profiles configuration consists of enabling the bandwidth control feature from the GUI and adding a profile which defines the control parameters. The profile can then be associated with a traffic selector, so that bandwidth profile can be applied to the traffic matching the selectors. Selectors are elements like IP addresses or services that would trigger the configured bandwidth regulation.

**Figure 19: List of Configured Bandwidth Profiles**



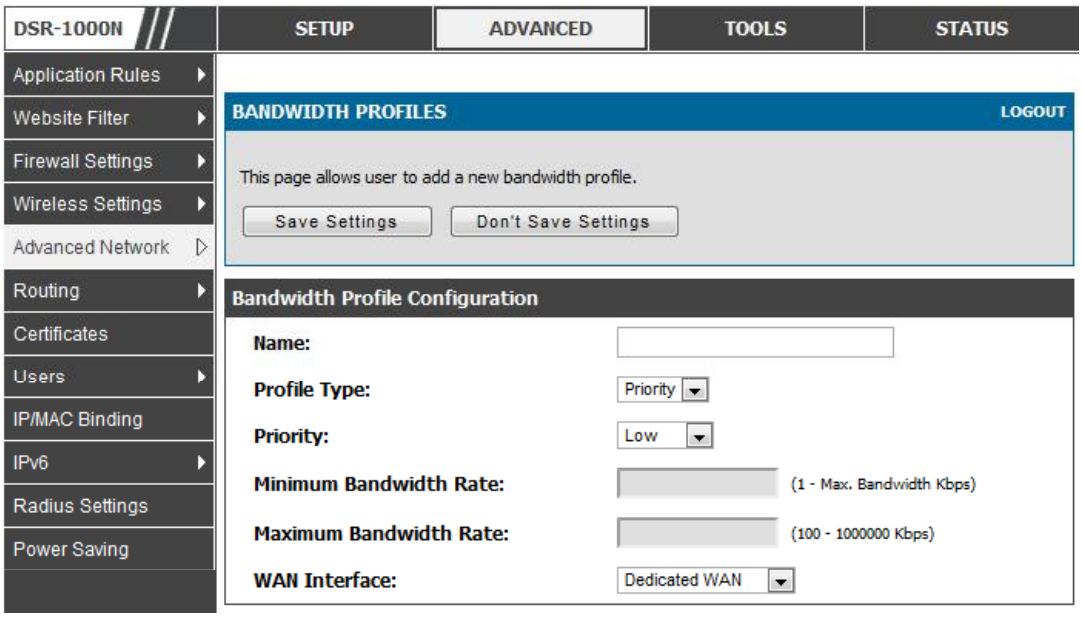

To create a new bandwidth profile, click Add in the List of Bandwidth Profiles. The following configuration parameters are used to define a bandwidth profile:

- Profile Name: This identifier is used to associate the configured profile to the traffic selector
- You can choose to limit the bandwidth either using priority or rate.
    - If using priority "Low", "High", "Medium" can be selected. If there is a low priority profile associated with traffic selector A and a high priority profile associated with traffic selector B, then the WAN bandwidth allocation preference will be to traffic selector B packets.

- For finer control, the Rate profile type can be used. With this option the minimum and maximum bandwidth allowed by this profile can be limited.

- Choose the WAN interface that the profile should be associated with.

**Figure 20: Bandwidth Profile Configuration page**

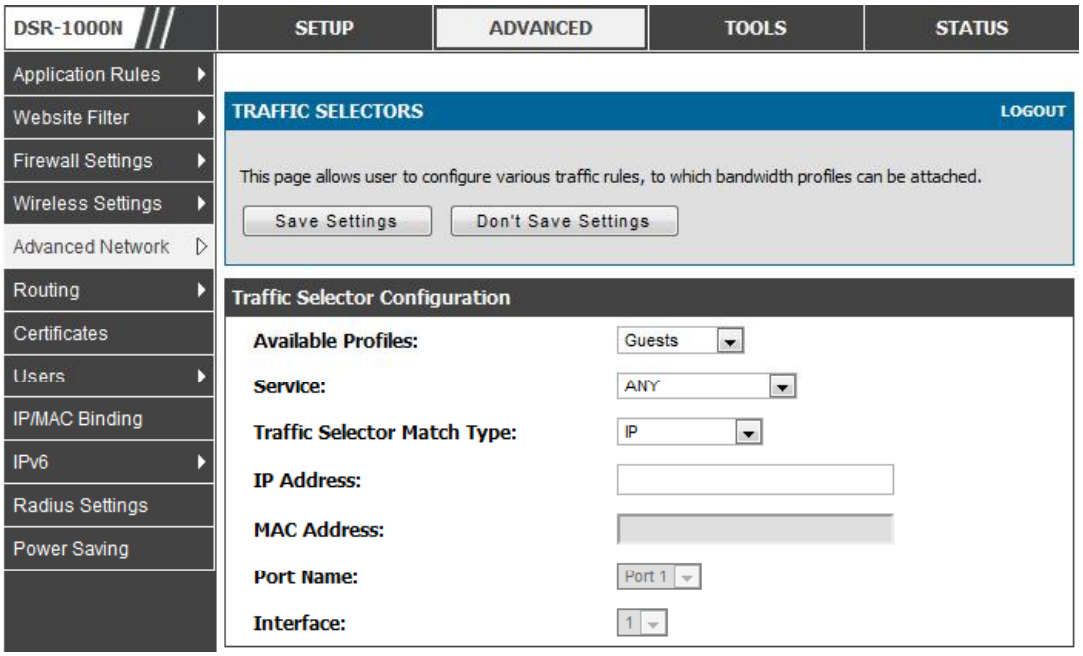



### *Advanced > Advanced Network > Traffic Management > Traffic Selectors*

Once a profile has been created it can then be associated with a traffic flow from the LAN to WAN. To create a traffic selector, click Add on the Traffic Selectors page. Traffic selector configuration binds a bandwidth profile to a type or source of LAN traffic with the following settings:

- Available profiles: Assign one of the defined bandwidth profiles
- Service: You can have the selected bandwidth regulation apply to a specific service (i.e. FTP) from the LAN. If you do not see a service that you want, you can configure a custom service through the ***Advanced > Firewall Settings > Custom Services*** page. To have the profile apply to all services, select ANY.
- Traffic Selector Match Type: this defines the parameter to filter against when applying the bandwidth profile. A specific machine on the LAN can be identified via IP address or MAC address, or the profile can apply to a LAN port or VLAN group. As well a wireless network can be selected by its BSSID for bandwidth shaping.

**Figure 21: Traffic Selector Configuration**




# 3.4 Features with Multiple WAN Links

This router supports multiple WAN links. This allows you to take advantage of failover and load balancing features to ensure certain internet dependent services are prioritized in the event of unstable WAN connectivity on one of the ports.

***Setup > Internet Settings > WAN Mode***

To use Auto Failover or Load Balancing, WAN link failure detection must be configured. This involves accessing DNS servers on the internet or ping to an internet address (user defined). If required, you can configure the number of retry attempts when the link seems to be disconnected or the threshold of failures that determines if a WAN port is down.

## 3.4.1 Auto Failover

In this case one of your WAN ports is assigned as the primary internet link for all internet traffic. The secondary WAN port is used for redundancy in case the primary link goes down for any reason. Both WAN ports (primary and secondary) must be configured to connect to the respective ISP's before enabling this feature. The secondary WAN port will remain unconnected until a failure is detected on the primary link (either port can be assigned as the primary). In the event of a failure on the primary port, all internet traffic will be rolled over to the backup port. When configured in Auto Failover mode, the link status of the primary WAN port is checked at regular intervals as defined by the failure detection settings.

Note that both WAN1 and WAN2 can be configured as the primary internet link.

- Auto-Rollover using WAN port-WAN1: WAN1 is the primary internet link.
- Auto-Rollover using WAN port-WAN2: WAN2 is the primary internet link.

Failover Detection Settings: To check connectivity of the primary internet link, one of the following failure detection methods can be selected:

- DNS lookup using WAN DNS Servers: DNS Lookup of the DNS Servers of the primary link are used to detect primary WAN connectivity.
- DNS lookup using DNS Servers: DNS Lookup of the custom DNS Servers can be specified to check the connectivity of the primary link.
- Ping these IP addresses: These IP's will be pinged at regular intervals to check the connectivity of the primary link.
- Retry Interval is: The number tells the router how often it should run the above configured failure detection method.
- Failover after: This sets the number of retries after which failover is initiated.

## 3.4.2 Load Balancing

This feature allows you to use multiple WAN links (and presumably multiple ISP's) simultaneously. After configuring more than one WAN port, the load balancing option is available to carry traffic over more than one link. Protocol bindings are used to segregate and assign services over one WAN port in order to manage internet flow. The configured failure detection method is used at regular intervals on all configured WAN ports when in Load Balancing mode.

DSR currently support three algorithms for Load Balancing:

**Round Robin**: This algorithm is particularly useful when the connection speed of one WAN port greatly differs from another. In this case you can define protocol bindings to route low-latency services (such as VOIP) over the higher-speed link and let low-volume background traffic (such as SMTP) go over the lower speed link. Protocol binding is explained in next section.

**Spill Over**: If Spill Over method is selected, WAN1 acts as a dedicated link till a threshold is reached. After this, WAN2 will be used for new connections. You can configure spill-over mode by using folloing options:

- Load Tolerance: It is the percentage of bandwidth after which the router switches to seconday WAN.
- Max Bandwidth: This sets the maximum bandwidth tolerable by the primary WAN.

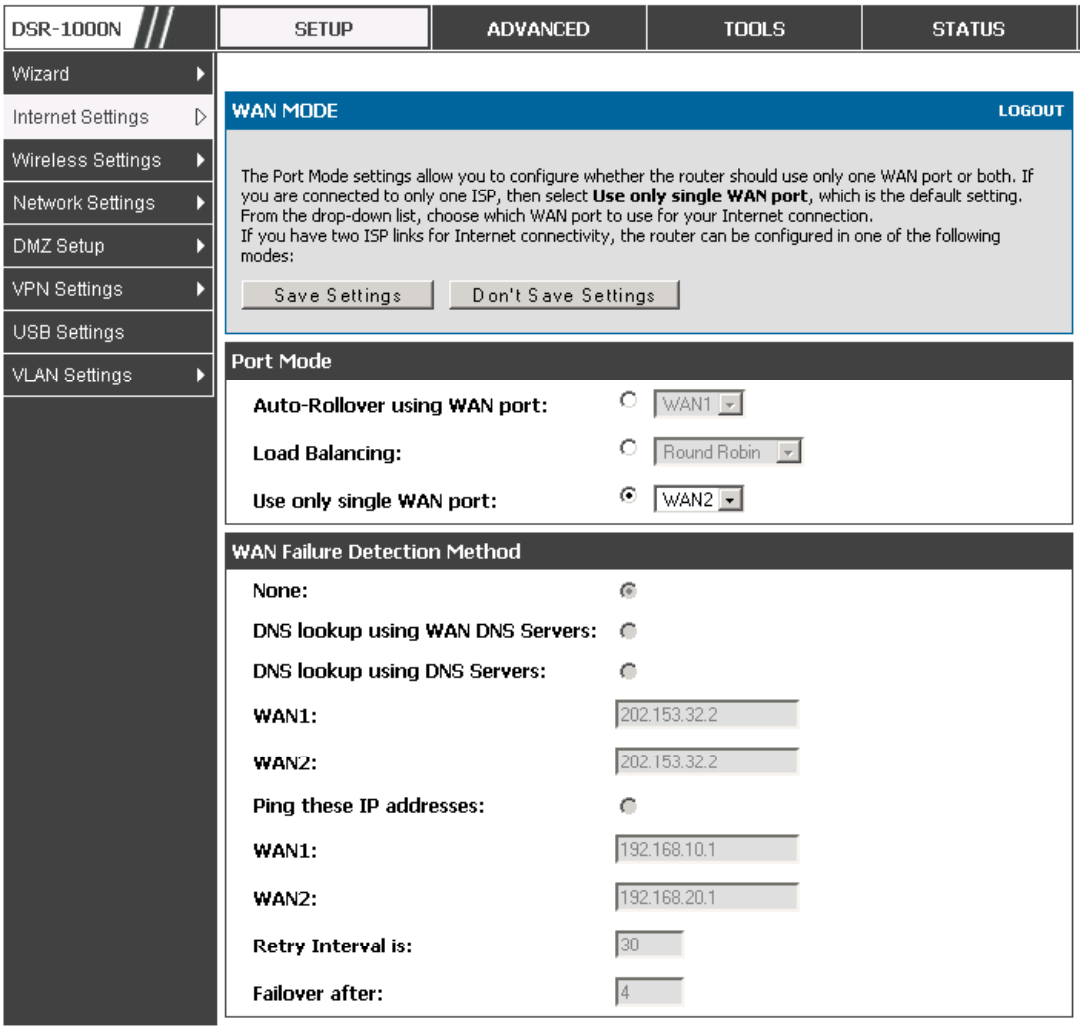
If the link bandwidth goes above the load tolerance value of max bandwidth, the router will spill-over the next connections to secondary WAN.

For example, if the maximum bandwidth of primary WAN is 1 Kbps and the load tolerance is set to 70. Now everytime a new connection is established the bandwidth increases. After a certain number of connections say bandwidth reached 70% of 1Kbps, the new connections will be spilled-over to secondary WAN. The maximum value of load tolerance is 80 and the least is 20.

**Protocol Bindings**: Refer Section 3.4.3 for details

Load balancing is particularly useful when the connection speed of one WAN port greatly differs from another. In this case you can define protocol bindings to route low-latency services (such as VOIP) over the higher-speed link and let low-volume background traffic (such as SMTP) go over the lower speed link.

**Figure 22: Load Balancing is available when multiple WAN ports are configured and Protocol Bindings have been defined**



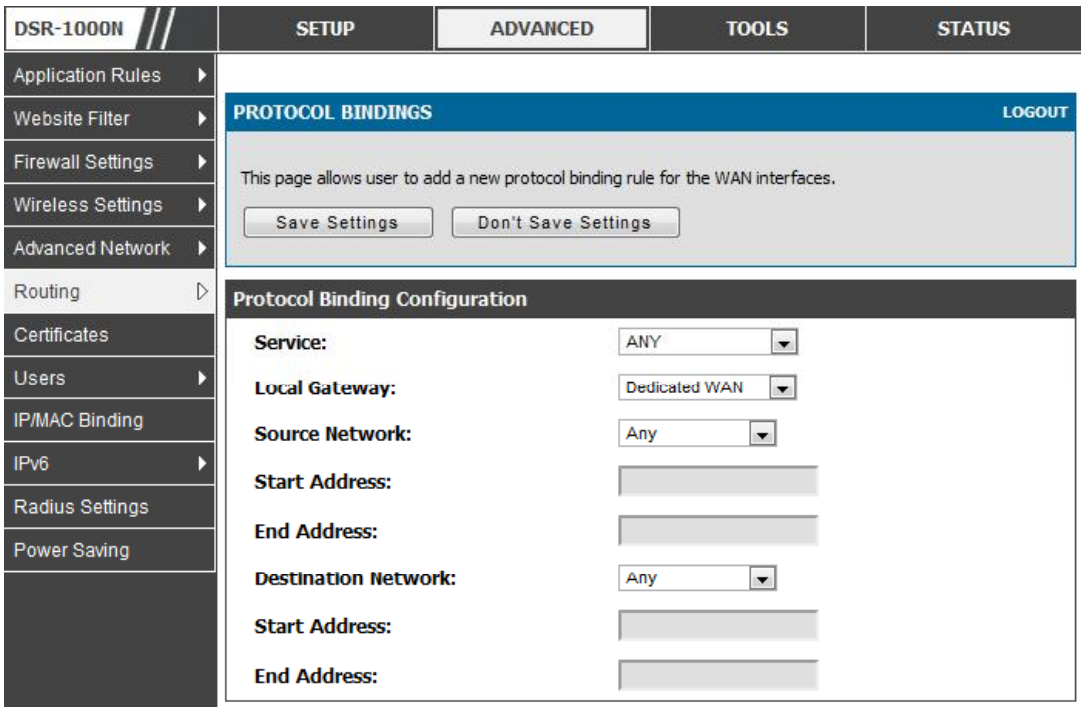

## 3.4.3 Protocol Bindings

***Advanced > Routing > Protocol Bindings***

Protocol bindings are required when the Load Balancing feature is in use. Choosing from a list of configured services or any of the user-defined services, the type of traffic can be assigned to go over only one of the available WAN ports. For increased flexibility the source network or machines can be specified as well as the destination network or machines. For example the VOIP traffic for a set of LAN IP addresses can be assigned to one WAN and any VOIP traffic from the remaining IP

addresses can be assigned to the other WAN link. Protocol bindings are only applicable when load balancing mode is enabled and more than one WAN is configured.

**Figure 23: Protocol binding setup to associate a service and/or LAN source to a WAN and/or destination network**




# 3.5 Routing Configuration

Routing between the LAN and WAN will impact the way this router handles traffic that is received on any of its physical interfaces. The routing mode of the gateway is core to the behavior of the traffic flow between the secure LAN and the internet.

## 3.5.1 Routing Mode

***Setup > Internet Settings > Routing Mode***

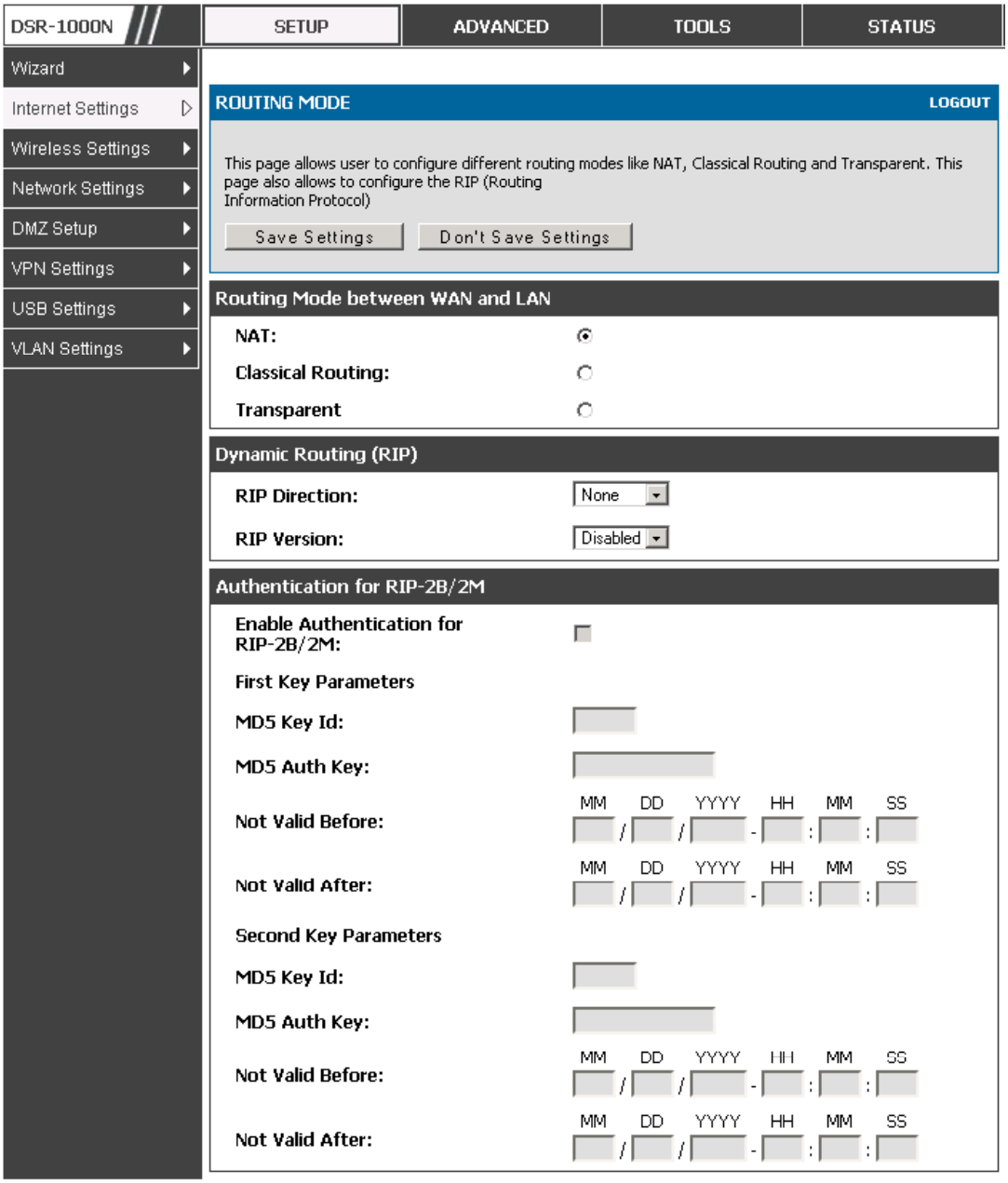
This device supports classical routing, network address translation (NAT), and transport mode routing.

- With classical routing, devices on the LAN can be directly accessed from the internet by their public IP addresses (assuming appropriate firewall settings). If your ISP has assigned an IP address for each of the computers that you use, select Classic Routing.

- NAT is a technique which allows several computers on a LAN to share an Internet connection. The computers on the LAN use a "private" IP address range while the WAN port on the router is configured with a single "public" IP address. Along with connection sharing, NAT also hides internal IP addresses from the computers on the Internet. NAT is required if your ISP has assigned only one IP address to you. The computers that connect through the router will need to be assigned IP addresses from a private subnet.
- Transparent routing between the LAN and WAN does not perform NAT. Broadcast and multicast packets that arrive on the LAN interface are switched to the WAN and vice versa, if they do not get filtered by firewall or VPN policies. To maintain the LAN and WAN in the same broadcast domain select Transparent mode, which allows bridging of traffic from LAN to WAN and vice versa, except for router-terminated traffic and other management traffic. All DSR features (such as 3G modem support) are supported in transparent mode assuming the LAN and WAN are configured to be in the same broadcast domain.

NAT routing has a feature called “NAT Hair-pinning” that allows internal network users on the LAN and DMZ to access internal servers (eg. an internal FTP server) using their externally-known domain name. This is also referred to as “NAT loopback” since LAN generated traffic is redirected through the firewall to reach LAN servers by their external name.

**Figure 24: Routing Mode is used to configure traffic routing between WAN and LAN, as well as Dynamic routing (RIP)**




## 3.5.2 Dynamic Routing (RIP)

DSR-250N does not support RIP.

***Setup > Internet Settings > Routing Mode***

Dynamic routing using the Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) that is common in LANs. With RIP this router can exchange routing information with other supported routers in the LAN and allow for dynamic adjustment of routing tables in order to adapt to modifications in the LAN without interrupting traffic flow.

The RIP direction will define how this router sends and receives RIP packets. Choose between:

- Both: The router both broadcasts its routing table and also processes RIP information received from other routers. This is the recommended setting in order to fully utilize RIP capabilities.
- Out Only: The router broadcasts its routing table periodically but does not accept RIP information from other routers.
- In Only: The router accepts RIP information from other routers, but does not broadcast its routing table.
- None: The router neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.
    - The RIP version is dependent on the RIP support of other routing devices in the LAN.
- Disabled: This is the setting when RIP is disabled.
- RIP-1 is a class-based routing version that does not include subnet information. This is the most commonly supported version.
- RIP-2 includes all the functionality of RIPv1 plus it supports subnet information. Though the data is sent in RIP-2 format for both RIP-2B and RIP-2M, the mode in which packets are sent is different. RIP-2B broadcasts data in the entire subnet while RIP-2M sends data to multicast addresses.

If RIP-2B or RIP-2M is the selected version, authentication between this router and other routers (configured with the same RIP version) is required. MD5 authentication is used in a first/second key exchange process. The authentication key validity lifetimes are configurable to ensure that the routing information exchange is with current and supported routers detected on the LAN.

## 3.5.3 Static Routing

***Advanced > Routing > Static Routing***

***Advanced > IPv6 > IPv6 Static Routing***

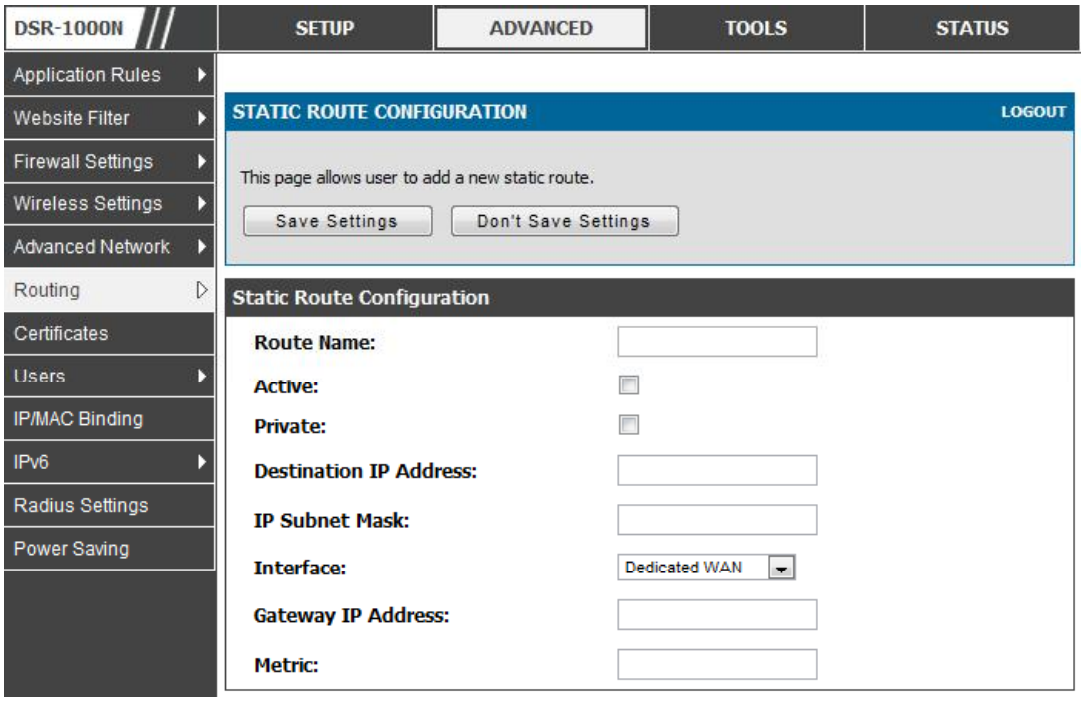
Manually adding static routes to this device allows you to define the path selection of traffic from one interface to another. There is no communication between this

router and other devices to account for changes in the path; once configured the static route will be active and effective until the network changes.

The List of Static Routes displays all routes that have been added manually by an administrator and allows several operations on the static routes. The List of IPv4 Static Routes and List of IPv6 Static Routes share the same fields (with one exception):

- Name: Name of the route, for identification and management.
- Active: Determines whether the route is active or inactive. A route can be added to the table and made inactive, if not needed. This allows routes to be used as needed without deleting and re-adding the entry. An inactive route is not broadcast if RIP is enabled.
- Private: Determines whether the route can be shared with other routers when RIP is enabled. If the route is made private, then the route will not be shared in a RIP broadcast or multicast. This is only applicable for IPv4 static routes.
- Destination: the route will lead to this destination host or IP address.
- IP Subnet Mask: This is valid for IPv4 networks only, and identifies the subnet that is affected by this static route
- Interface: The physical network interface (WAN1, WAN2, DMZ or LAN), through which this route is accessible.
- Gateway: IP address of the gateway through which the destination host or network can be reached.
- Metric: Determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen.

**Figure 25: Static route configuration fields**




# 3.6 Configurable Port - WAN Option

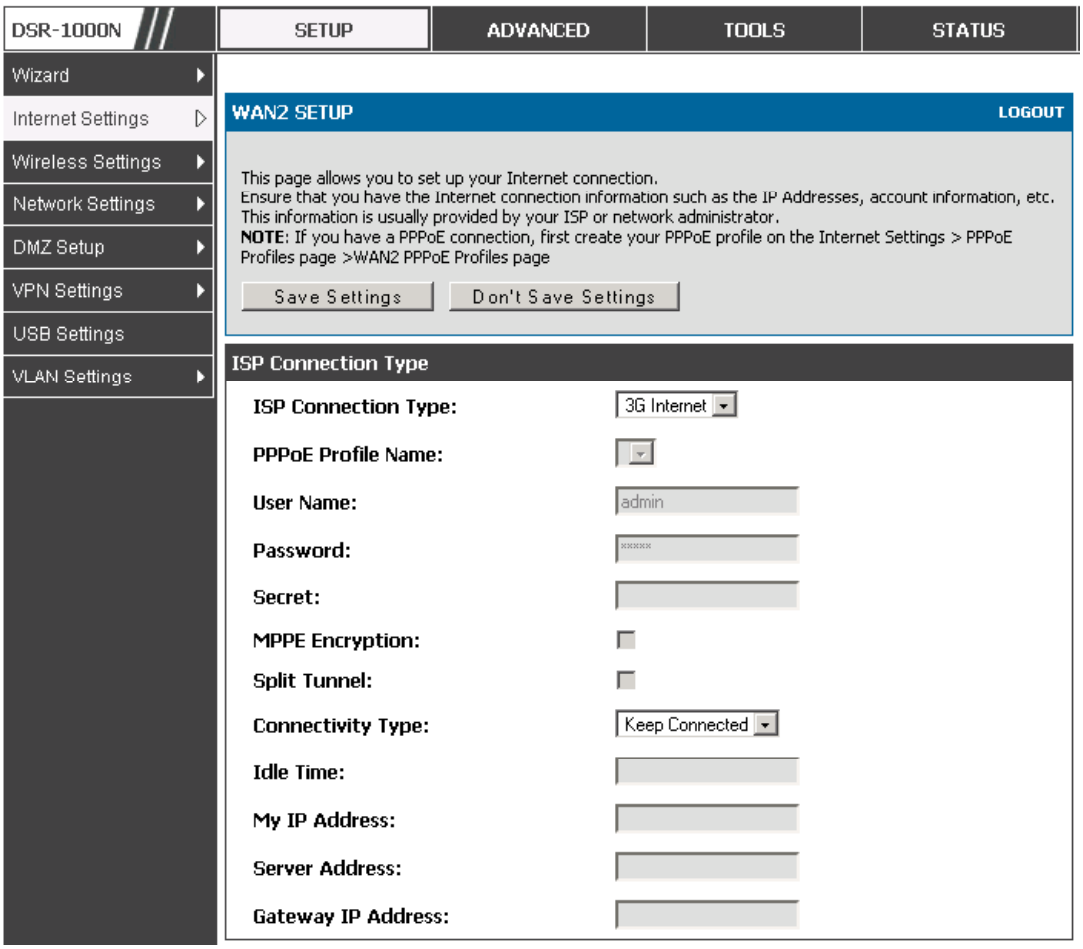
This router supports one of the physical ports to be configured as a secondary WAN Ethernet port or a dedicated DMZ port. If the port is selected to be a secondary WAN interface, all configuration pages relating to WAN2 are enabled.

### *Setup > Internet Settings > WAN2 Setup*

WAN2 configuration is identical to the WAN1 configuration with one significant exception: configuration for the 3G USB modem is available only on WAN2.

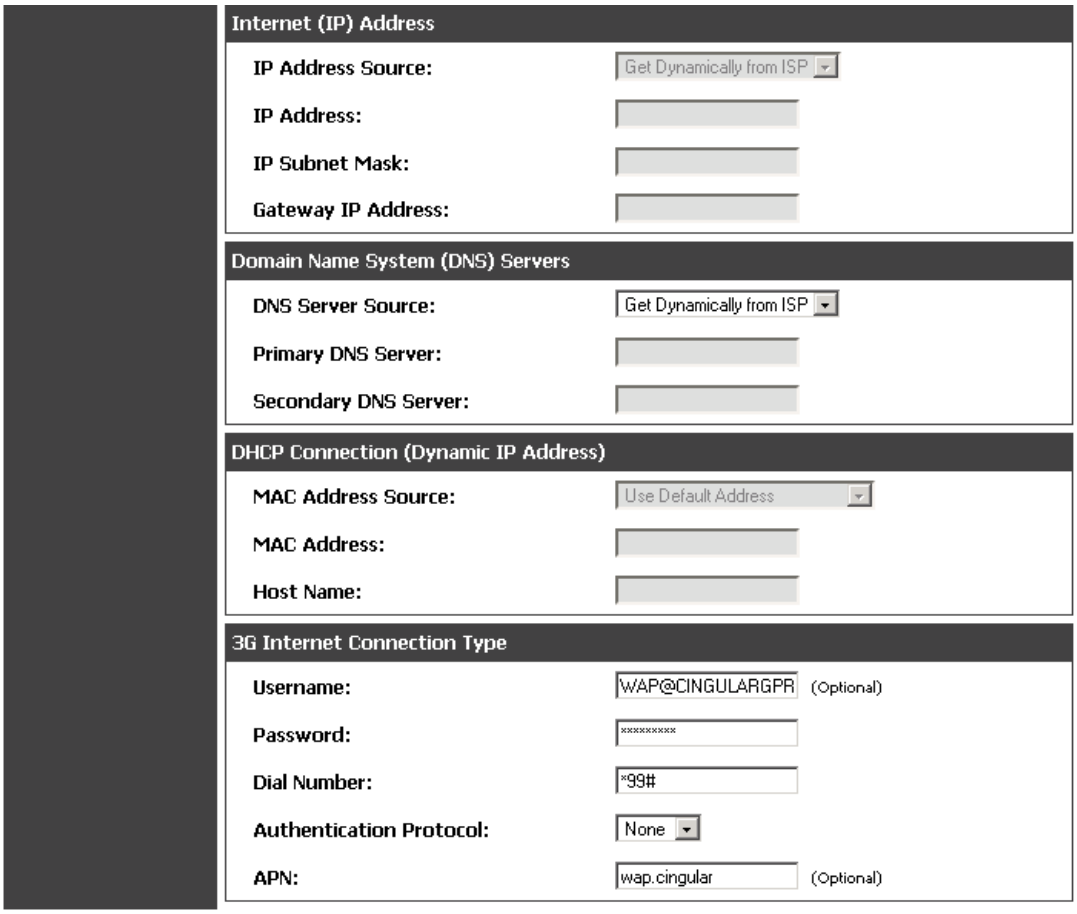
> 3G WAN support is available on the dual WAN products: DSR-1000 and DSR-1000N.

**Figure 26: WAN2 configuration for 3G internet (part 1)**




Cellular 3G internet access is available on WAN2 via a 3G USB modem for DSR-1000 and DSR-1000N. The cellular ISP that provides the 3G data plan will provide the authentication requirements to establish a connection. The dial Number and APN are specific to the cellular carriers. Once the connection type settings are configured and saved, navigate to the WAN status page (***Setup > Internet Settings > WAN Status***) and Enable the WAN2 link to establish the 3G connection.

**Figure 27: WAN2 configuration for 3G internet (part 2)**




# 3.7 WAN Port Settings

***Advanced > Advanced Network > WAN Port Setup***

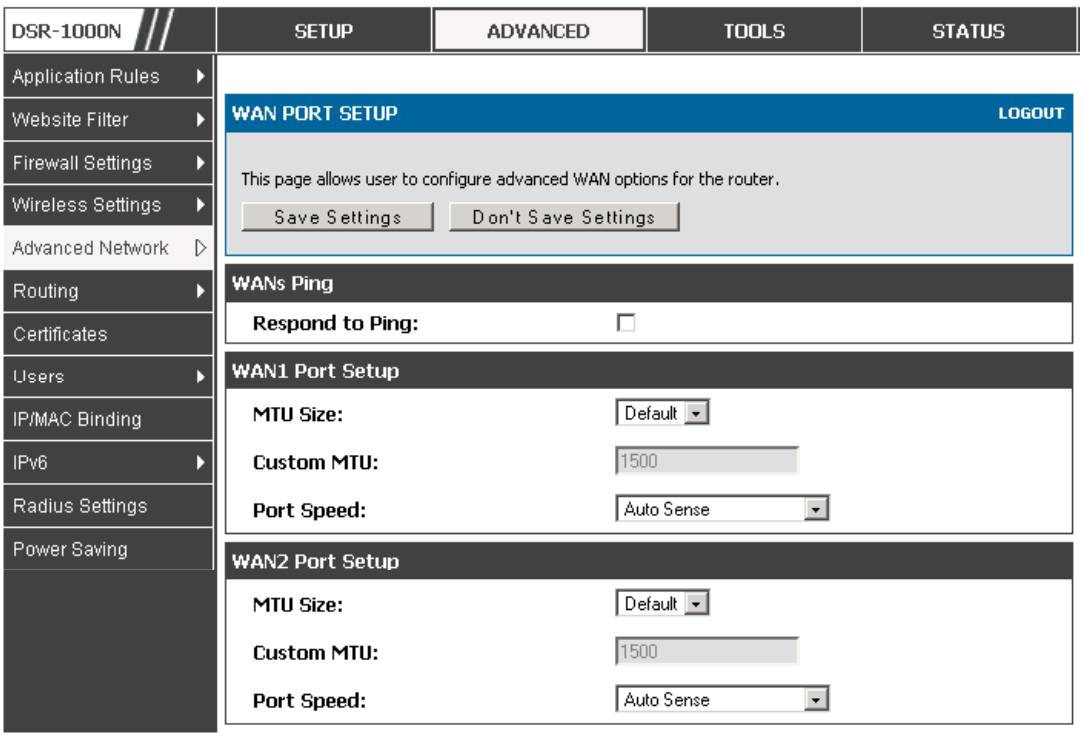
The physical port settings for each WAN link can be defined here. If your ISP account defines the WAN port speed or is associated with a MAC address, this information is required by the router to ensure a smooth connection with the network.

The default MTU size supported by all ports is 1500. This is the largest packet size that can pass through the interface without fragmentation. This size can be increased, however large packets can introduce network lag and bring down the interface speed. Note that a 1500 byte size packet is the largest allowed by the Ethernet protocol at the network layer.

The port speed can be sensed by the router when Auto is selected. With this option the optimal port settings are determined by the router and network. The duplex (half or full) can be defined based on the port support, as well as one of three port speeds: 10 Mbps, 100 Mbps and 1000 Mbps (i.e. 1 Gbps). The default setting is 100 Mbps for all ports.

The default MAC address is defined during the manufacturing process for the interfaces, and can uniquely identify this router. You can customize each WAN port's MAC address as needed, either by letting the WAN port assume the current LAN host's MAC address or by entering a MAC address manually.

**Figure 28: Physical WAN port settings**



# Chapter 4. Wireless Access Point Setup

This router has an integrated 802.11n radio that allows you to create an access point for wireless LAN clients. The security/encryption/authentication options are grouped in a wireless Profile, and each configured profile will be available for selection in the AP configuration menu. The profile defines various parameters for the AP, including the security between the wireless client and the AP, and can be shared between multiple APs instances on the same device when needed.

> The content in this section is applicable to the DSR-500N and DSR-1000N products.

Up to four unique wireless networks can be created by configuring multiple "virtual" APs. Each such virtual AP appears as an independent AP (unique SSID) to supported clients in the environment, but is actually running on the same physical radio integrated with this router.

You will need the following information to configure your wireless network:

- Types of devices expected to access the wireless network and their supported Wi-Fi™ modes
- The router's geographical region
- The security settings to use for securing the wireless network.

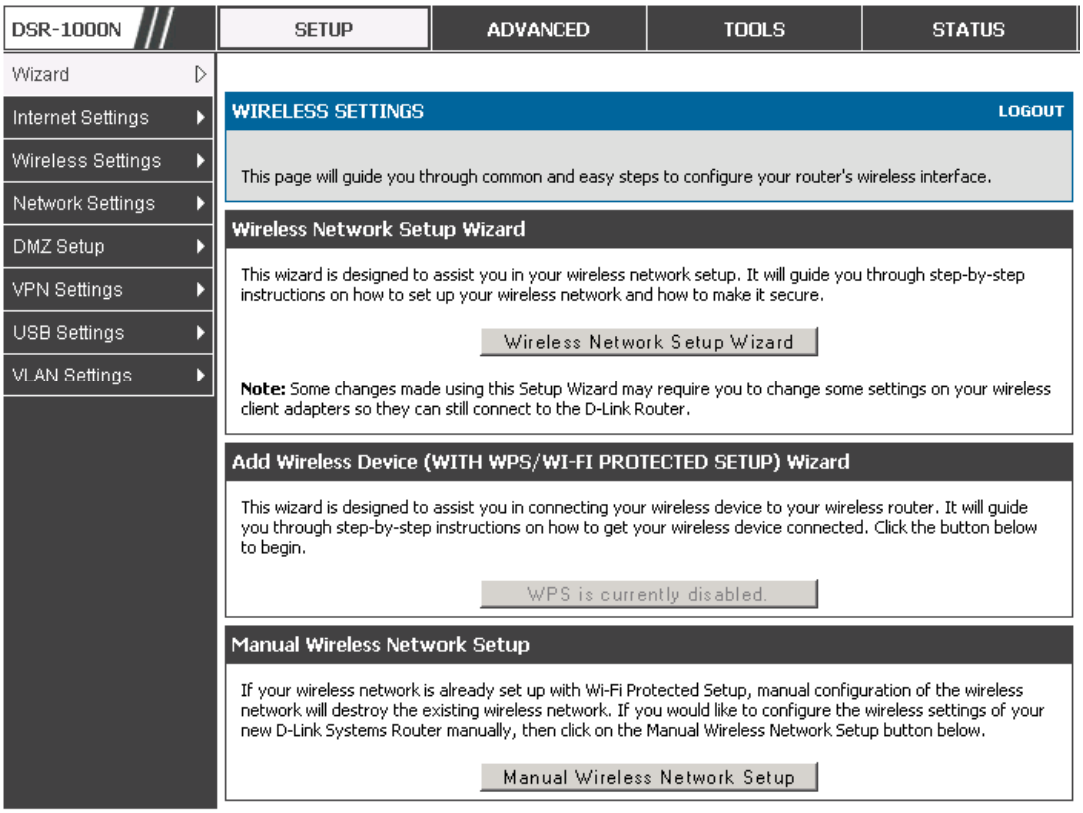
> Profiles may be thought of as a grouping of AP parameters that can then be applied to not just one but multiple AP instances (SSIDs), thus avoiding duplication if the same parameters are to be used on multiple AP instances or SSIDs.

## 4.1 Wireless Settings Wizard

***Setup > Wizard > Wireless Settings***

The Wireless Network Setup Wizard is available for users new to networking. By going through a few straightforward configuration pages you can enable a Wi-Fi™ network on your LAN and allow supported 802.11 clients to connect to the configured Access Point.

**Figure 29: Wireless Network Setup Wizards**




## 4.1.1 Wireless Network Setup Wizard

This wizard provides a step-by-step guide to create and secure a new access point on the router. The network name (SSID) is the AP identifier that will be detected by supported clients. The Wizard uses a TKIP+AES cipher for WPA / WPA2 security; depending on support on the client side, devices associate with this AP using either WPA or WPA2 security with the same pre-shared key.

The wizard has the option to automatically generate a network key for the AP. This key is the pre-shared key for WPA or WPA2 type security. Supported clients that have been given this PSK can associate with this AP. The default (auto-assigned) PSK is “passphrase”.

The last step in the Wizard is to click the Connect button, which confirms the settings and enables this AP to broadcast its availability in the LAN.

## 4.1.2 Add Wireless Device with WPS

With WPS enabled on your router, the selected access point allows supported WPS clients to join the network very easily. When the Auto option for connecting a wireless device is chose, you will be presented with two common WPS setup options:

- **Personal Identification Number (PIN):** The wireless device that supports WPS may have an alphanumeric PIN, and if entered in this field the AP will establish a link to the client. Click Connect to complete setup and connect to the client.
- **Push Button Configuration (PBC):** for wireless devices that support PBC, press and hold down on this button and within 2 minutes, click the PBC connect button. The AP will detect the wireless device and establish a link to the client.

> You need to enable at least one AP with WPA/WPA2 security and also enable WPS in the ***Advanced > Wireless Settings > WPS*** page to use the WPS wizard.

### 4.1.3 Manual Wireless Network Setup

This button on the Wizard page will link to the ***Setup> Wireless Settings> Access Points*** page. The manual options allow you to create new APs or modify the parameters of APs created by the Wizard.

## 4.2 Wireless Profiles

***Setup > Wireless Settings > Profiles***

The profile allows you to assign the security type, encryption and authentication to use when connecting the AP to a wireless client. The default mode is "open", i.e. no security. This mode is insecure as it allows any compatible wireless clients to connect to an AP configured with this security profile.

To create a new profile, use a unique profile name to identify the combination of settings. Configure a unique SSID that will be the identifier used by the clients to communicate to the AP using this profile. By choosing to broadcast the SSID, compatible wireless clients within range of the AP can detect this profile's availability.

The AP offers all advanced 802.11 security modes, including WEP, WPA, WPA2 and WPA+WPA2 options. The security of the Access point is configured by the Wireless Security Type section:

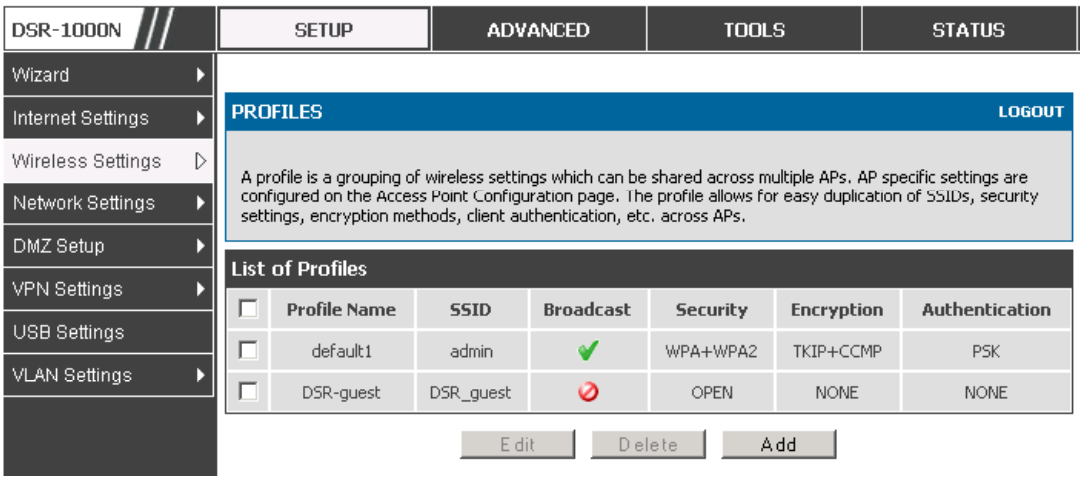
- Open: select this option to create a public "open" network to allow unauthenticated devices to access this wireless gateway.
- WEP (Wired Equivalent Privacy): this option requires a static (pre-shared) key to be shared between the AP and wireless client. Note that WEP does not support 802.11n data rates; is it appropriate for legacy 802.11 connections.
- WPA (Wi-Fi Protected Access): For stronger wireless security than WEP, choose this option. The encryption for WPA will use TKIP and also CCMP if required. The authentication can be a pre-shared key (PSK), Enterprise mode with RADIUS

server, or both. Note that WPA does not support 802.11n data rates; is it appropriate for legacy 802.11 connections.

- WPA2: this security type uses CCMP encryption (and the option to add TKIP encryption) on either PSK (pre-shared key) or Enterprise (RADIUS Server) authentication.
- WPA + WPA2: this uses both encryption algorithms, TKIP and CCMP. WPA clients will use TKIP and WPA2 clients will use CCMP encryption algorithms.

> "WPA+WPA2" is a security option that allows devices to connect to an AP using the strongest security that it supports. This mode allows legacy devices that only support WPA2 keys (such as an older wireless printer) to connect to a secure AP where all the other wireless clients are using WPA2.

**Figure 30: List of Available Profiles shows the options available to secure the wireless link**



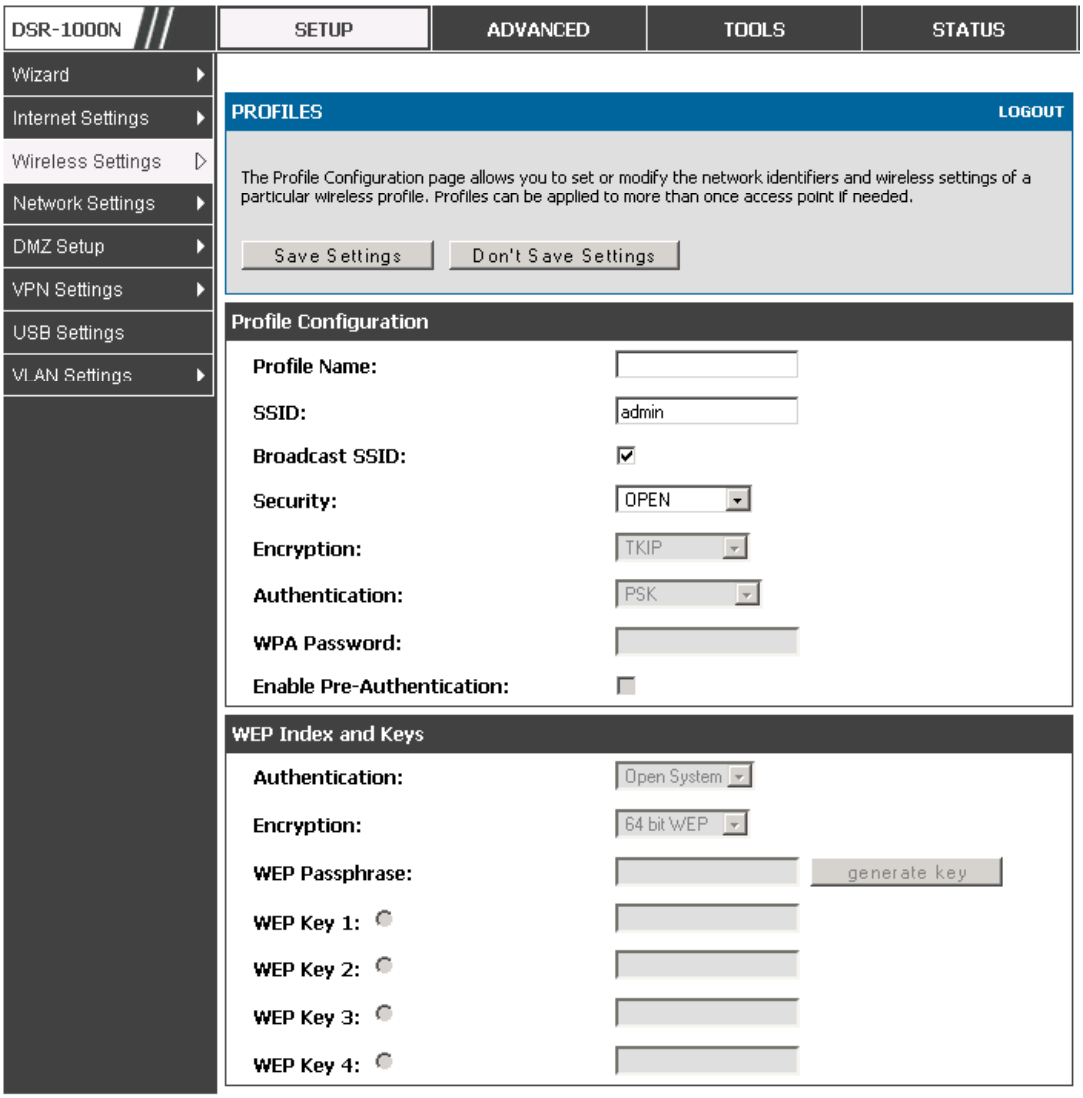

## 4.2.1 WEP Security

If WEP is the chosen security option, you must set a unique static key to be shared with clients that wish to access this secured wireless network. This static key can be generated from an easy-to-remember passphrase and the selected encryption length.

- Authentication: select between Open System, or Shared Key schemes
- Encryption: select the encryption key size -- 64 bit WEP or 128 bit WEP. The larger size keys provide stronger encryption, thus making the key more difficult to crack
- WEP Passphrase: enter a alphanumeric phrase and click Generate Key to generate 4 unique WEP keys with length determined by the encryption key

size. Next choose one of the keys to be used for authentication. The selected key must be shared with wireless clients to connect to this device.

**Figure 31: Profile configuration to set network security**




## 4.2.2 WPA or WPA2 with PSK

A pre-shared key (PSK) is a known passphrase configured on the AP and client both and is used to authenticate the wireless client. An acceptable passphrase is between 8 to 63 characters in length.

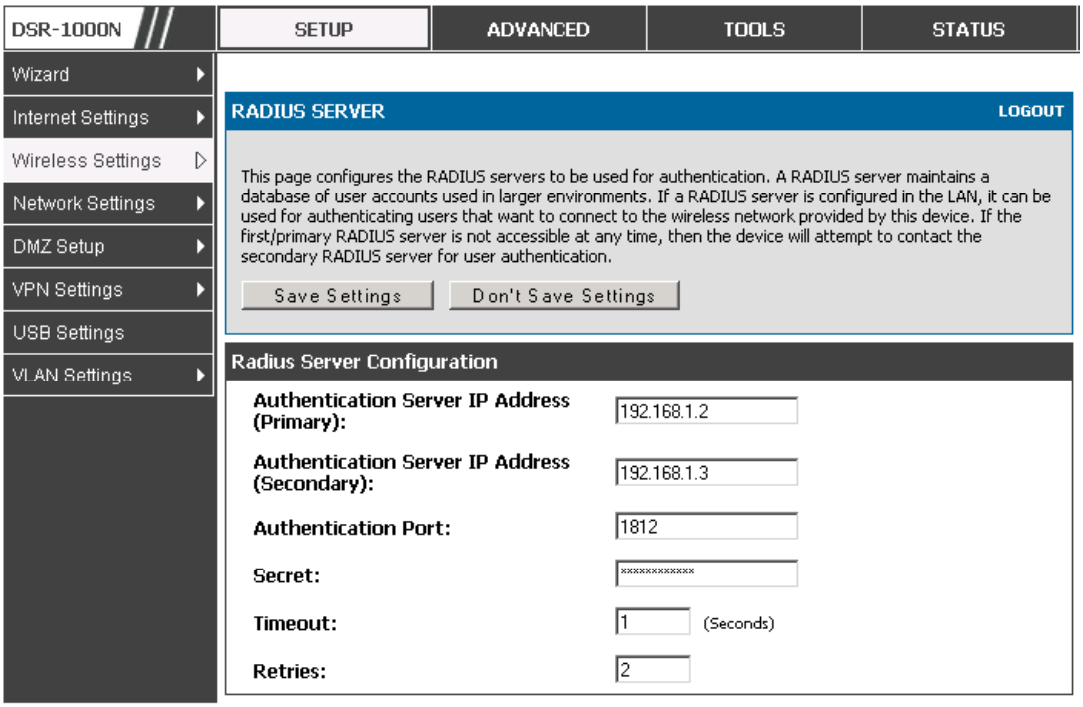
## 4.2.3 RADIUS Authentication

***Setup > Wireless Settings > RADIUS Settings***

Enterprise Mode uses a RADIUS Server for WPA and/or WPA2 security. A RADIUS server must be configured and accessible by the router to authenticate wireless client connections to an AP enabled with a profile that uses RADIUS authentication.

- The Authentication IP Address is required to identify the server. A secondary RADIUS server provides redundancy in the event that the primary server cannot be reached by the router when needed.
- Authentication Port: the port for the RADIUS server connection
- Secret: enter the shared secret that allows this router to log into the specified RADIUS server(s). This key must match the shared secret on the RADIUS Server.
- The Timeout and Retries fields are used to either move to a secondary server if the primary cannot be reached, or to give up the RADIUS authentication attempt if communication with the server is not possible.

**Figure 32: RADIUS server (External Authentication) configuration**




# 4.3 Creating and Using Access Points

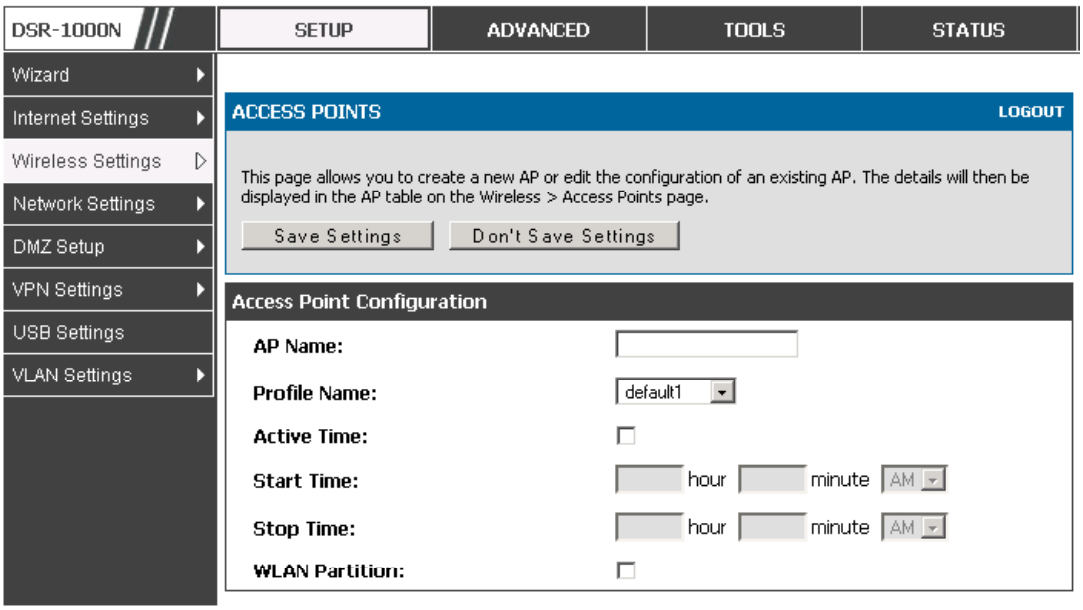
***Setup > Wireless Settings > Access Points***

Once a profile (a group of security settings) is created, it can be assigned to an AP on the router. The AP SSID can be configured to broadcast its availability to the 802.11 environment can be used to establish a WLAN network.

The AP configuration page allows you to create a new AP and link to it one of the available profiles. This router supports multiple AP's referred to as virtual access points (VAPs). Each virtual AP that has a unique SSIDs appears as an independent access point to clients. This valuable feature allows the router's radio to be configured in a way to optimize security and throughput for a group of clients as required by the user. To create a VAP, click the "add" button on the ***Setup > Wireless Settings > Access Points*** page. After setting the AP name, the profile dropdown menu is used to select one of the configured profiles.

The AP Name is a unique identifier used to manage the AP from the GUI, and is not the SSID that is detected by clients when the AP has broadcast enabled.

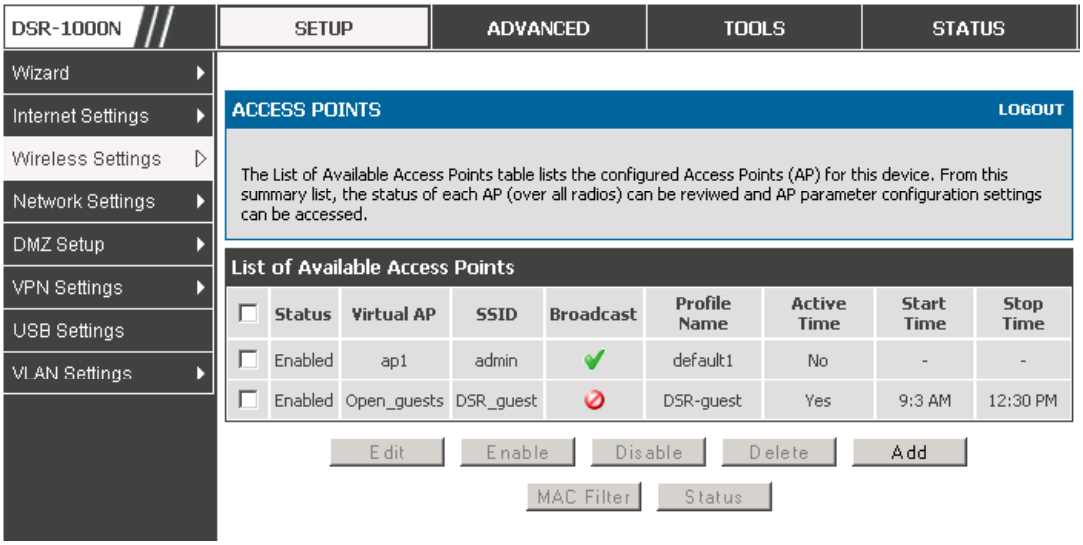
**Figure 33: Virtual AP configuration**




A valuable power saving feature is the start and stop time control for this AP. You can conserve on the radio power by disabling the AP when it is not in use. For example on evenings and weekends if you know there are no wireless clients, the start and stop time will enable/disable the access point automatically.

Once the AP settings are configured, you must enable the AP on the radio on the ***Setup > Wireless Settings > Access Points*** page. The status field changes to "Enabled" if the AP is available to accept wireless clients. If the AP is configured to broadcast its SSID (a profile parameter), a green check mark indicating it is broadcasting will be shown in the List of Available Access points.

**Figure 34: List of configured access points (Virtual APs) shows one enabled access point on the radio, broadcasting its SSID**




The clients connected to a particular AP can be viewed by using the Status Button on the List of Available Access Points. Traffic statistics are shown for that individual AP, as compared to the summary stats for each AP on the Statistics table. Connected clients are sorted by the MAC address and indicate the security parameters used by the wireless link, as well as the time connected to this particular AP. Clicking the Details button next to the connected client will give the detailed send and receive traffic statistics for the wireless link between this AP and the client.

## 4.3.1 Primary benefits of Virtual APs:

- Optimize throughput: if 802.11b, 802.11 g, and 802.11n clients are expected to access the LAN via this router, creating 3 VAPs will allow you to manage or shape traffic for each group of clients. A unique SSID can be created for the network of 802.11b clients and another SSID can be assigned for the 802.11n clients. Each can have different security parameters – remember, the SSID and security of the link is determined by the profile. In this way legacy clients can access the network without bringing down the overall throughput of more capable 802.11n clients.
- Optimize security: you may wish to support select legacy clients that only offer WEP security while using WPA2 security for the majority of clients for the radio. By creating two VAPs configured with different SSIDs and different security parameters, both types of clients can connect to the LAN. Since WPA2 is more secure, you may want to broadcast this SSID and not

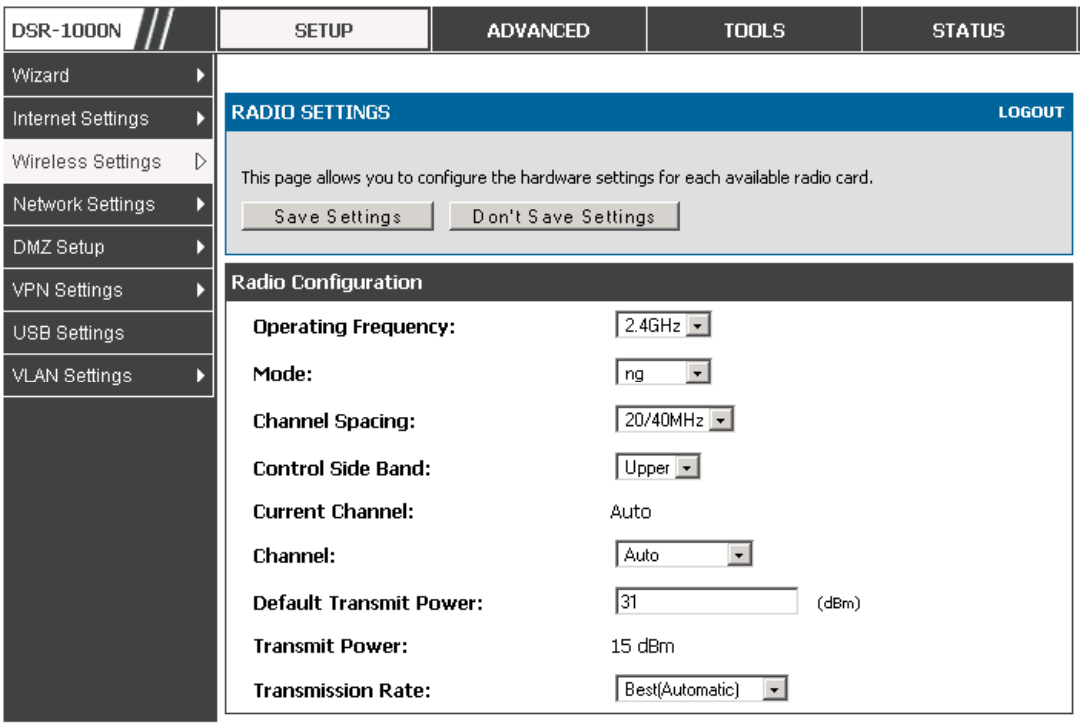
broadcast the SSID for the VAP with WEP since it is meant to be used for a few legacy devices in this scenario.

# 4.4 Tuning Radio Specific Settings

***Setup > Wireless Settings > Radio Settings***

The Radio Settings page lets you configure the channels and power levels available for the AP's enabled on the DSR. The router has a dual band 802.11n radio, meaning either 2.4 GHz or 5 GHz frequency of operation can be selected (not concurrently though). Based on the selected operating frequency, the mode selection will let you define whether legacy connections or only 802.11n connections (or both) are accepted on configured APs.

**Figure 35: Radio card configuration options**




The ratified 802.11n support on this radio requires selecting the appropriate broadcast (NA or NG etc.) mode, and then defining the channel spacing and control side band for 802.11n traffic. The default settings are appropriate for most networks. For example, changing the channel spacing to 40 MHz can improve bandwidth at the expense of supporting earlier 802.11n clients.

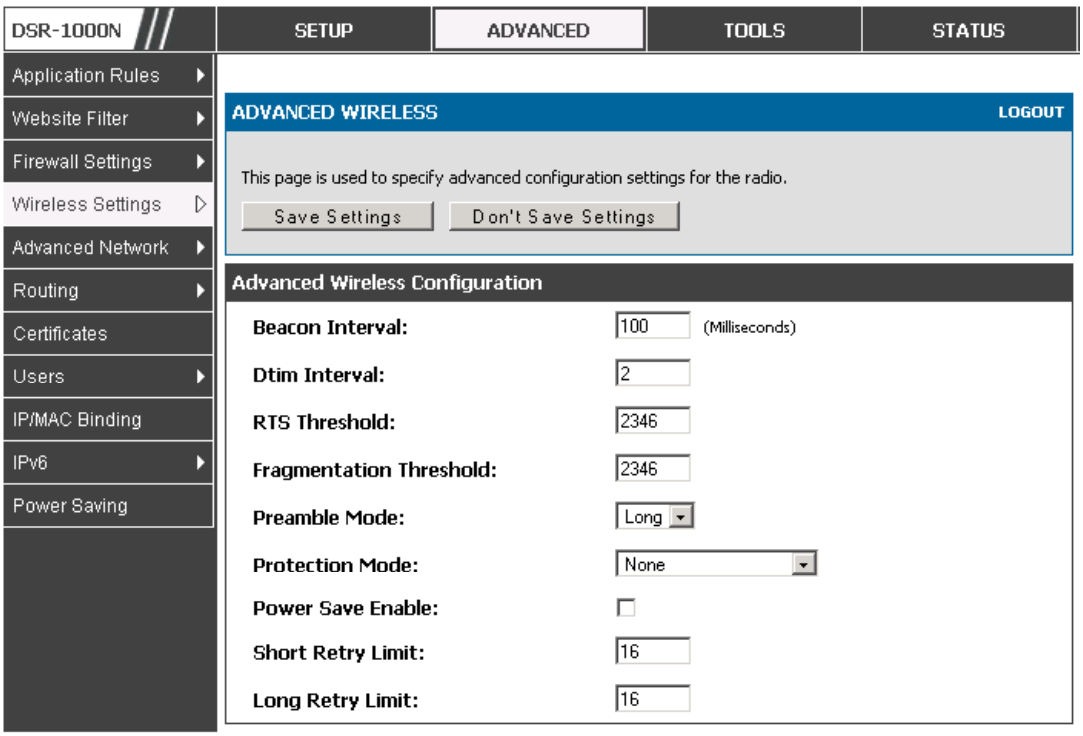
The available transmission channels are governed by regulatory constraints based on the region setting of the router. The maximum transmission power is similarly governed by regulatory limits; you have the option to decrease from the default maximum to reduce the signal strength of traffic out of the radio.

# 4.5 Advanced Wireless Settings

***Advanced > Wireless Settings > Advanced Wireless***

Sophisticated wireless administrators can modify the 802.11 communication parameters in this page. Generally, the default settings are appropriate for most networks. Please refer to the GUI integrated help text for further details on the use of each configuration parameter.

**Figure 36: Advanced Wireless communication settings**




# 4.6 Wi-Fi Protected Setup (WPS)

***Advanced > Wireless Settings > WPS***

WPS is a simplified method to add supporting wireless clients to the network. WPS is only applicable for APs that employ WPA or WPA2 security. To use WPS, select the eligible VAPs from the dropdown list of APs that have been configured with this security and enable WPS status for this AP.

The WPS Current Status section outlines the security, authentication, and encryption settings of the selected AP. These are consistent with the AP's profile. There are two setup options available for WPS:

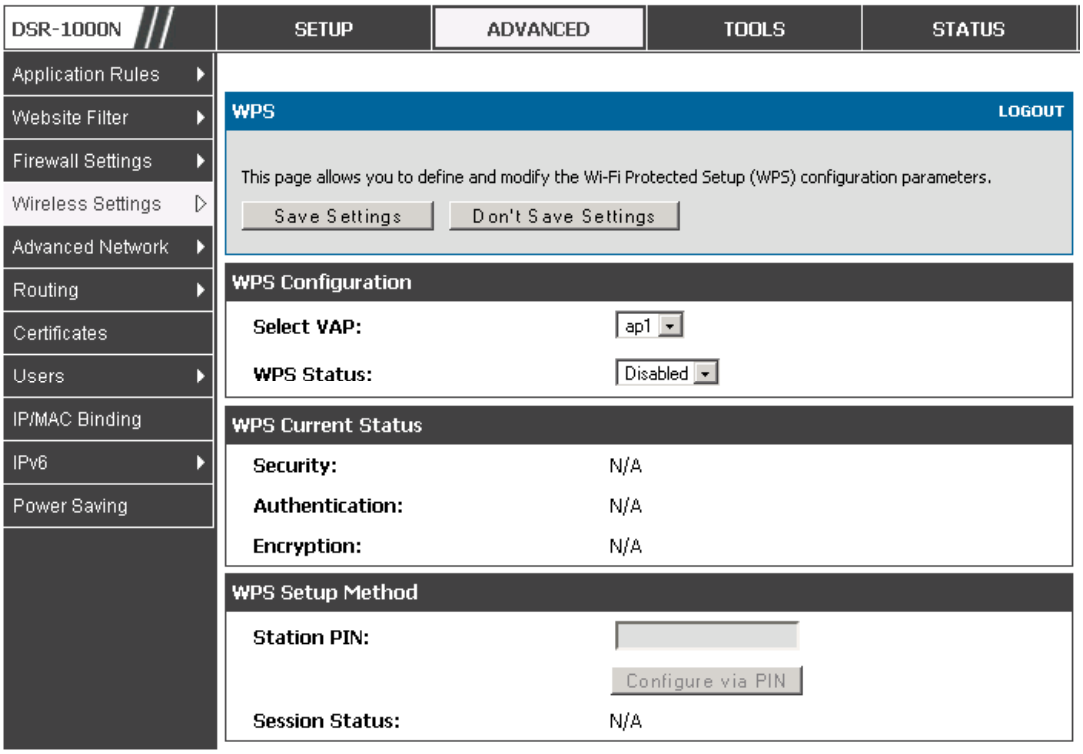
- **Personal Identification Number (PIN):** The wireless device that supports WPS may have an alphanumeric PIN, if so add the PIN in this field. The router will

connect within 60 seconds of clicking the "Configure via PIN" button immediately below the PIN field. There is no LED indication that a client has connected.

- **Push Button Configuration (PBC):** for wireless devices that support PBC, press and hold down on this button and within 2 minutes click the PBC connect button. The AP will detect the wireless device and establish a link to the client.

> More than one AP can use WPS, but only one AP can be used to establish WPS links to client at any given time.

**Figure 37: WPS configuration for an AP with WPA/WPA2 profile**



# Chapter 5. Securing the Private Network

You can secure your network by creating and applying rules that your router uses to selectively block and allow inbound and outbound Internet traffic. You then specify how and to whom the rules apply. To do so, you must define the following:

- Services or traffic types (examples: web browsing, VoIP, other standard services and also custom services that you define)
- Direction for the traffic by specifying the source and destination of traffic; this is done by specifying the "From Zone" (LAN/WAN/DMZ) and "To Zone" (LAN/WAN/DMZ)
- Schedules as to when the router should apply rules
- Any Keywords (in a domain name or on a URL of a web page) that the router should allow or block
- Rules for allowing or blocking inbound and outbound Internet traffic for specified services on specified schedules
- MAC addresses of devices that should not access the internet
- Port triggers that signal the router to allow or block access to specified services as defined by port number
- Reports and alerts that you want the router to send to you

You can, for example, establish restricted-access policies based on time-of-day, web addresses, and web address keywords. You can block Internet access by applications and services on the LAN, such as chat rooms or games. You can block just certain groups of PCs on your network from being accessed by the WAN or public DMZ network.

## 5.1 Firewall Rules

***Advanced > Firewall Settings > Firewall Rules***

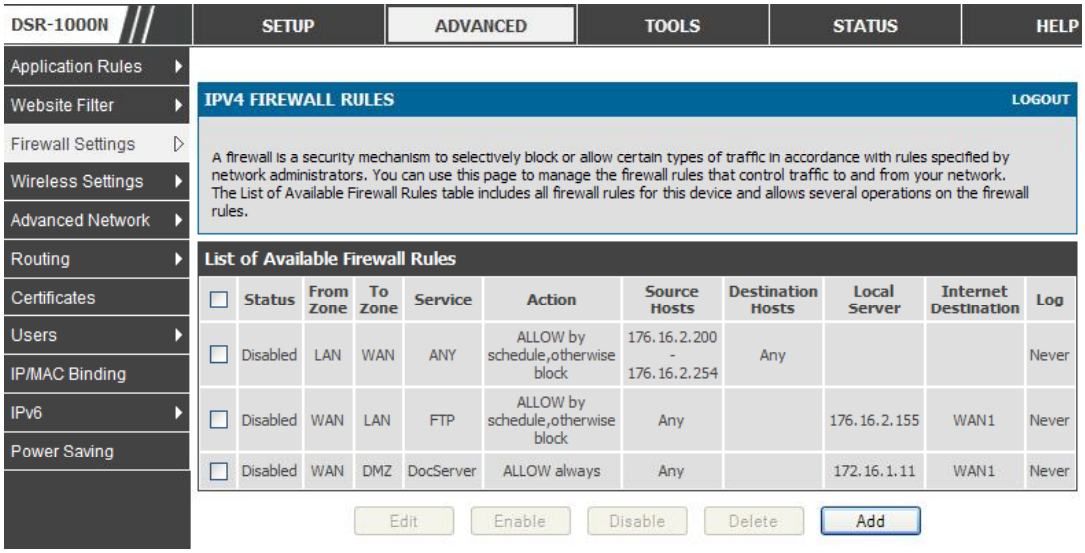
Inbound (WAN to LAN/DMZ) rules restrict access to traffic entering your network, selectively allowing only specific outside users to access specific local resources. By default all access from the insecure WAN side are blocked from accessing the secure LAN, except in response to requests from the LAN or DMZ. To allow outside devices to access services on the secure LAN, you must create an inbound firewall rule for each service.

If you want to allow incoming traffic, you must make the router's WAN port IP address known to the public. This is called "exposing your host." How you make your address known depends on how the WAN ports are configured; for this router you

may use the IP address if a static address is assigned to the WAN port, or if your WAN address is dynamic a DDNS (Dynamic DNS) name can be used.

Outbound (LAN/DMZ to WAN) rules restrict access to traffic leaving your network, selectively allowing only specific local users to access specific outside resources. The default outbound rule is to allow access from the secure zone (LAN) to either the public DMZ or insecure WAN. You can change this default behavior in the ***Firewall Settings > Default Outbound Policy*** page. When the default outbound policy is allow always, you can to block hosts on the LAN from accessing internet services by creating an outbound firewall rule for each service.

**Figure 38: List of Available Firewall Rules**



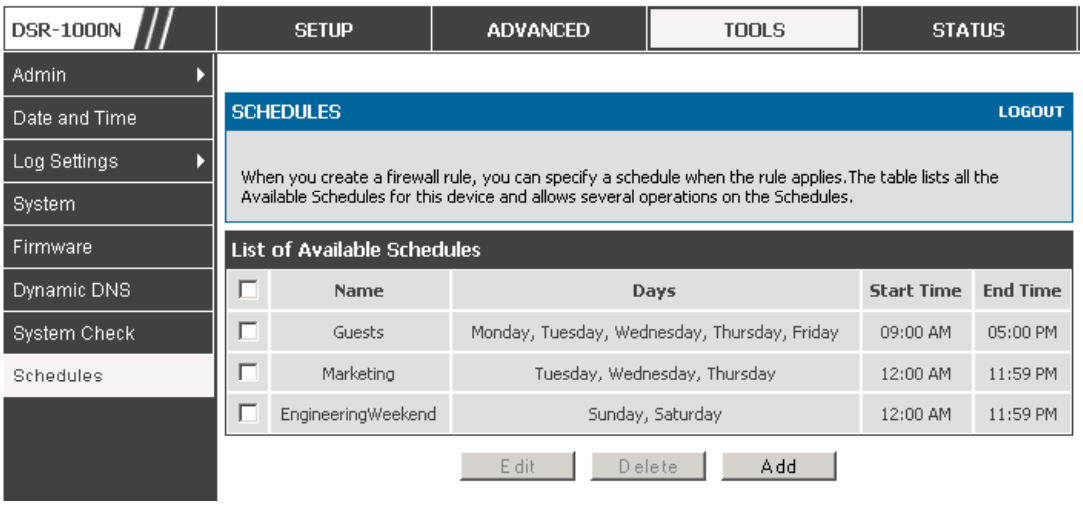

# 5.2 Defining Rule Schedules

### *Tools > Schedules*

Firewall rules can be enabled or disabled automatically if they are associated with a configured schedule. The schedule configuration page allows you to define days of the week and the time of day for a new schedule, and then this schedule can be selected in the firewall rule configuration page.

> All schedules will follow the time in the routers configured time zone. Refer to the section on choosing your Time Zone and configuring NTP servers for more information.

**Figure 39: List of Available Schedules to bind to a firewall rule**




# 5.3 Configuring Firewall Rules

***Advanced > Firewall Settings > Firewall Rules***

All configured firewall rules on the router are displayed in the Firewall Rules list. This list also indicates whether the rule is enabled (active) or not, and gives a summary of the From/To zone as well as the services or users that the rule affects.

To create a new firewall rules, follow the steps below:

1. View the existing rules in the List of Available Firewall Rules table.
2. To edit or add an outbound or inbound services rule, do the following:

- To edit a rule, click the checkbox next to the rule and click Edit to reach that rule's configuration page.
- To add a new rule, click Add to be taken to a new rule's configuration page. Once created, the new rule is automatically added to the original table.

3. Chose the From Zone to be the source of originating traffic: either the secure LAN, public DMZ, or insecure WAN. For an inbound rule WAN should be selected as the From Zone.
4. Choose the To Zone to be the destination of traffic covered by this rule. If the From Zone is the WAN, the To Zone can be the public DMZ or secure LAN. Similarly if the From Zone is the LAN, then the To Zone can be the public DMZ or insecure WAN.
5. Parameters that define the firewall rule include the following:

- Service: ANY means all traffic is affected by this rule. For a specific service the drop down list has common services, or you can select a custom defined service.
- Action & Schedule: Select one of the 4 actions that this rule defines: BLOCK always, ALLOW always, BLOCK by schedule otherwise ALLOW, or ALLOW by schedule otherwise BLOCK. A schedule must be preconfigured in order for it to be available in the dropdown list to assign to this rule.
  - Source & Destination users: For each relevant category, select the users to which the rule applies:
    - Any (all users)
    - Single Address (enter an IP address)
    - Address Range (enter the appropriate IP address range)
  - Log: traffic that is filtered by this rule can be logged; this requires configuring the router's logging feature separately.
  - QoS Priority: Outbound rules (where To Zone = insecure WAN only) can have the traffic marked with a QoS priority tag. Select a priority level:
    - Normal-Service: ToS=0 (lowest QoS)
    - Minimize-Cost: ToS=1
    - Maximize-Reliability: ToS=2
    - Maximize-Throughput: ToS=4
  - Minimize-Delay: ToS=8 (highest QoS)

6. Inbound rules can use Destination NAT (DNAT) for managing traffic from the WAN. Destination NAT is available when the To Zone = DMZ or secure LAN.
   - With an inbound allow rule you can enter the internal server address that is hosting the selected service.
   - You can enable port forwarding for an incoming service specific rule (From Zone = WAN) by selecting the appropriate checkbox. This will allow the selected service traffic from the internet to reach the appropriate LAN port via a port forwarding rule.
   - Translate Port Number: With port forwarding, the incoming traffic to be forwarded to the port number entered here.

- External IP address: The rule can be bound to a specific WAN interface by selecting either the primary WAN or configurable port WAN as the source IP address for incoming traffic.

> This router supports multi-NAT and so the External IP address does not necessarily have to be the WAN address. On a single WAN interface, multiple public IP addresses are supported. If your ISP assigns you more than one public IP address, one of these can be used as your primary IP address on the WAN port, and the others can be assigned to servers on the LAN or DMZ. In this way the LAN/DMZ server can be accessed from the internet by its aliased public IP address.

7. Outbound rules can use Source NAT (SNAT) in order to map (bind) all LAN/DMZ traffic matching the rule parameters to a specific WAN interface or external IP address (usually provided by your ISP).

Once the new or modified rule parameters are saved, it appears in the master list of firewall rules. To enable or disable a rule, click the checkbox next to the rule in the list of firewall rules and choose Enable or Disable.

> The router applies firewall rules in the order listed. As a general rule, you should move the strictest rules (those with the most specific services or addresses) to the top of the list. To reorder rules, click the checkbox next to a rule and click up or down.

**Figure 40: Example where an outbound SNAT rule is used to map an external IP address (209.156.200.225) to a private DMZ IP address (10.30.30.30)**

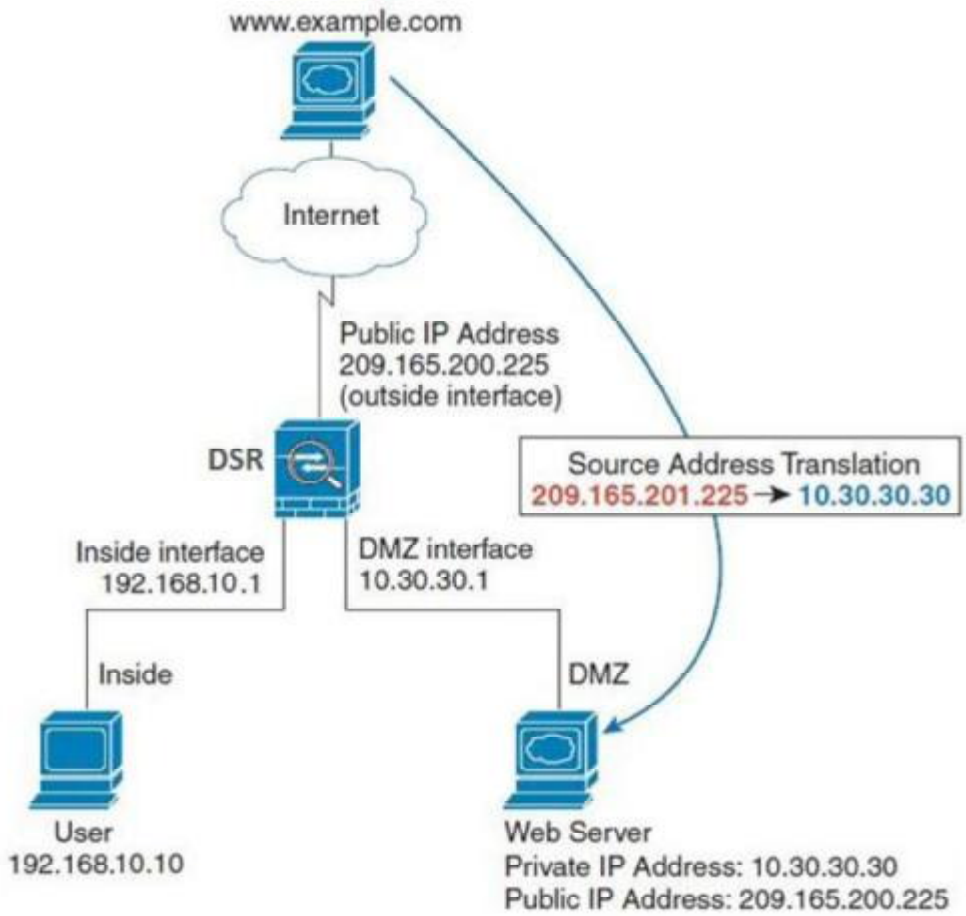
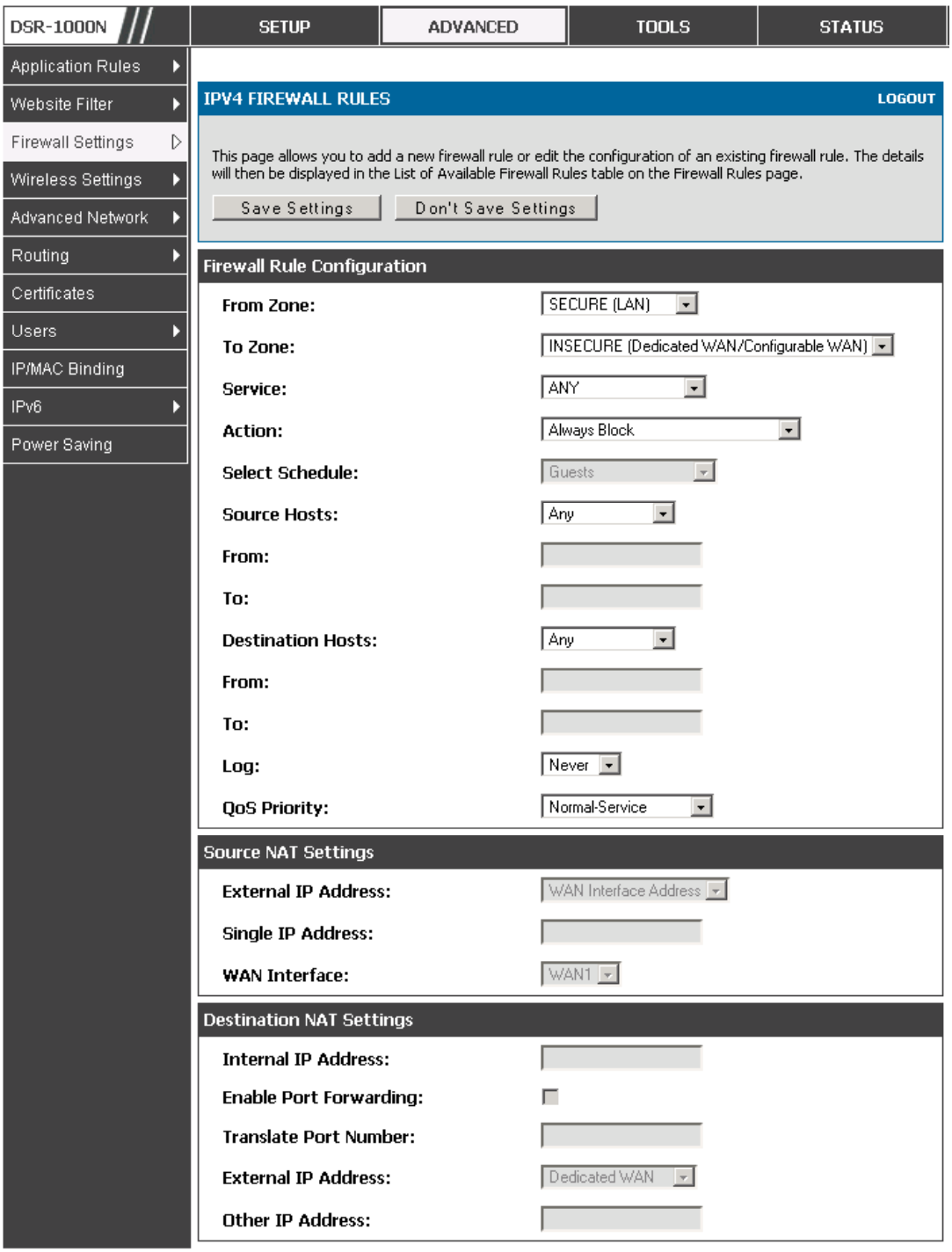


**Figure 41: The firewall rule configuration page allows you to define the To/From zone, service, action, schedules, and specify source/destination IP addresses as needed.**



## 5.3.1 Firewall Rule Configuration Examples

**Example 1:** Allow inbound HTTP traffic to the DMZ

**Situation:** You host a public web server on your local DMZ network. You want to allow inbound HTTP requests from any outside IP address to the IP address of your web server at any time of day.

**Solution:** Create an inbound rule as follows.

| Parameter | Value |
|---|---|
| From Zone | Insecure (WAN1/WAN2) |
| To Zone | Public (DMZ) |
| Service | HTTP |
| Action | ALLOW always |
| Send to Local Server (DNAT IP) | 192.168.5.2 (web server IP address) |
| Destination Users | Any |
| Log | Never |

**Example 2:** Allow videoconferencing from range of outside IP addresses

**Situation:** You want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses (132.177.88.2 - 132.177.88.254), from a branch office.

**Solution:** Create an inbound rule as follows. In the example, CUSeeMe (the video conference service used) connections are allowed only from a specified range of external IP addresses.

| Parameter | Value |
|---|---|
| From Zone | Insecure (WAN1/WAN2) |
| To Zone | Secure (LAN) |
| Service | CU-SEEME:UDP |
| Action | ALLOW always |
| Send to Local Server (DNAT IP) | 192.168.10.11 |
| Destination Users | Address Range |
| From | 132.177.88.2 |
| To | 134.177.88.254 |
| Enable Port Forwarding | Yes (enabled) |

**Example 3:** Multi-NAT configuration

**Situation:** You want to configure multi-NAT to support multiple public IP addresses on one WAN port interface.

**Solution:** Create an inbound rule that configures the firewall to host an additional public IP address. Associate this address with a web server on the DMZ. If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN. One of these public IP addresses is used as the primary IP address of the router. This address is used to provide Internet access to your LAN PCs through NAT. The other addresses are available to map to your DMZ servers.

The following addressing scheme is used to illustrate this procedure:

- WAN IP address: 10.1.0.118
- LAN IP address: 192.168.10.1; subnet 255.255.255.0
- Web server host in the DMZ, IP address: 192.168.12.222
- Access to Web server: (simulated) public IP address 10.1.0.52

| Parameter | Value |
|---|---|
| From Zone | Insecure (WAN1/WAN2) |
| To Zone | Public (DMZ) |
| Service | HTTP |
| Action | ALLOW always |
| Send to Local Server (DNAT IP) | 192.168.12.222 ( web server local IP address) |
| Destination Users | Single Address |
| From | 10.1.0.52 |
| WAN Users | Any |
| Log | Never |

**Example 4:** Block traffic by schedule if generated from specific range of machines

**Use Case:** Block all HTTP traffic on the weekends if the request originates from a specific group of machines in the LAN having a known range of IP addresses, and anyone coming in through the Network from the WAN (i.e. all remote users).

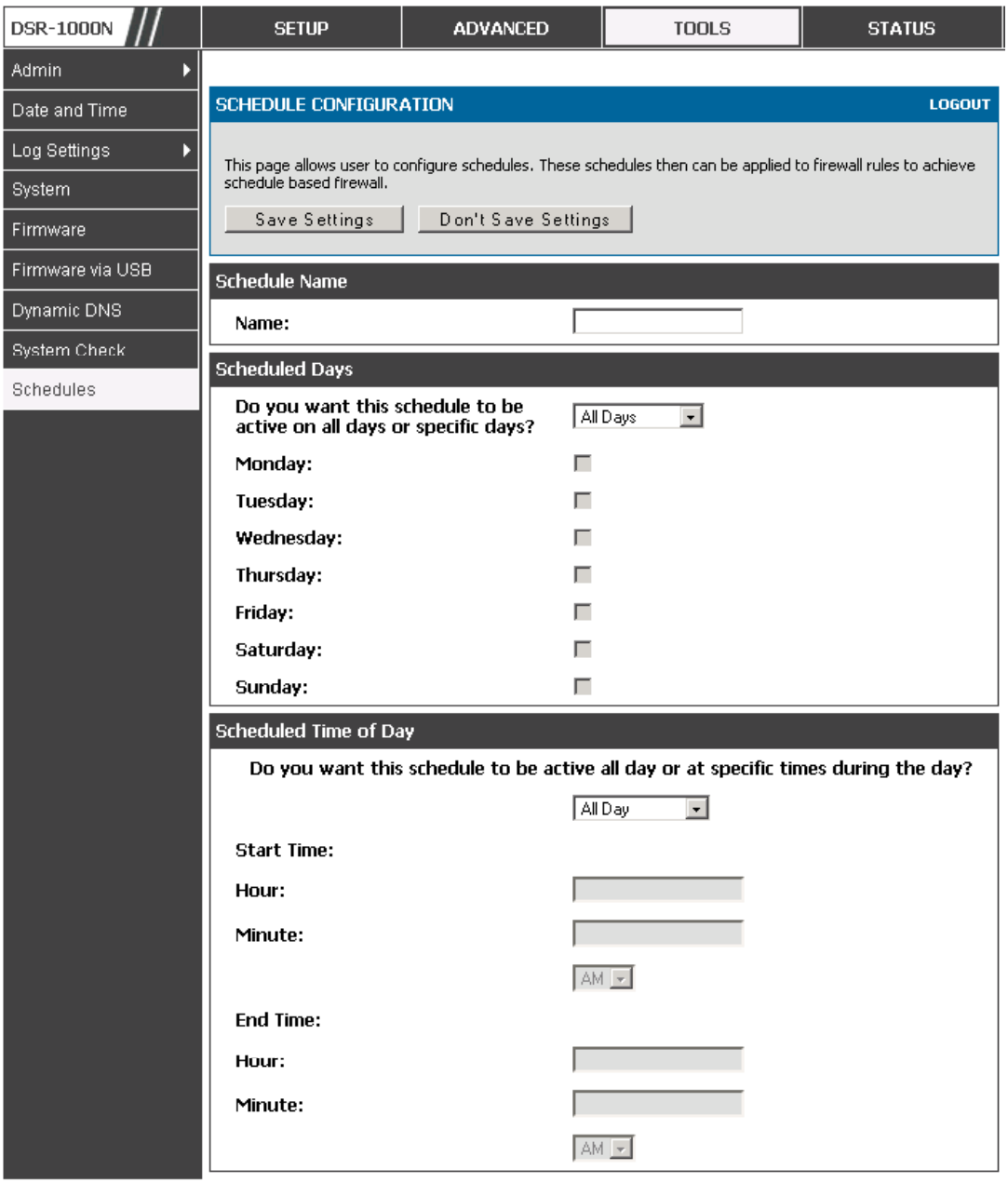
**Configuration:**

1. Setup a schedule:

- To setup a schedule that affects traffic on weekends only, navigate to Security: Schedule, and name the schedule “Weekend”
- Define “weekend” to mean 12 am Saturday morning to 12 am Monday morning – all day Saturday & Sunday

- In the Scheduled days box, check that you want the schedule to be active for "specific days". Select "Saturday" and "Sunday"
- In the scheduled time of day, select "all day" – this will apply the schedule between 12 am to 11:59 pm of the selected day.
- Click apply – now schedule "Weekend" isolates all day Saturday and Sunday from the rest of the week.

**Figure 42: Schedule configuration for the above example.**




2. Since we are trying to block HTTP requests, it is a service with To Zone: Insecure (WAN1/WAN2) that is to be blocked according to schedule "Weekend".

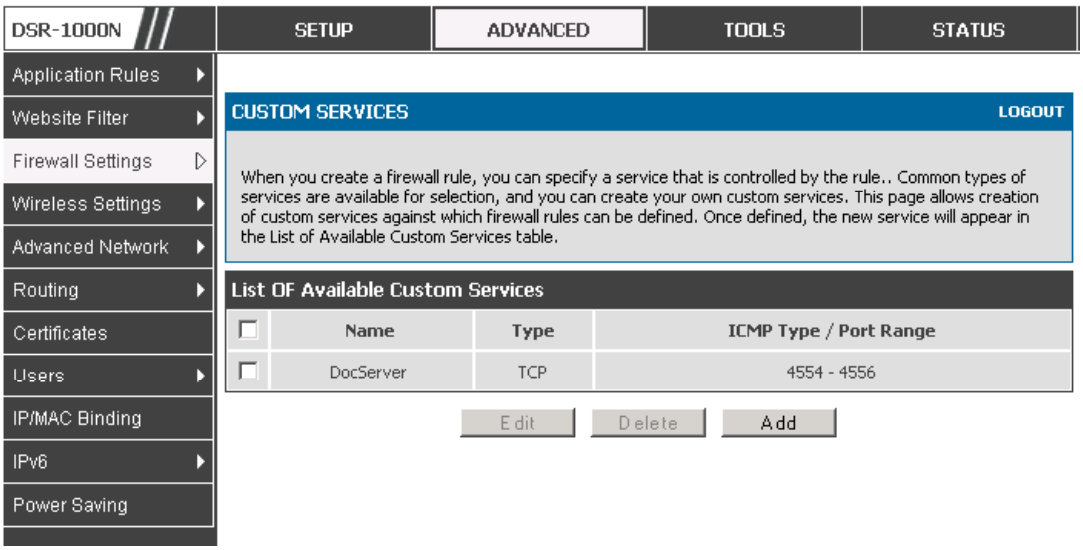
3. Select the Action to "Block by Schedule, otherwise allow". This will take a predefined schedule and make sure the rule is a blocking rule during the defined dates/times. All other times outside the schedule will not be affected by this firewall blocking rule
4. As we defined our schedule in schedule "Weekend", this is available in the dropdown menu
5. We want to block the IP range assigned to the marketing group. Let's say they have IP 192.168.10.20 to 192.168.10.30. On the Source Users dropdown, select Address Range and add this IP range as the From and To IP addresses.
6. We want to block all HTTP traffic to any services going to the insecure zone. The Destination Users dropdown should be "any".
7. We don't need to change default QoS priority or Logging (unless desired) – clicking apply will add this firewall rule to the list of firewall rules.
8. The last step is to enable this firewall rule. Select the rule, and click "enable" below the list to make sure the firewall rule is active

# 5.4 Security on Custom Services

***Advanced > Firewall Settings > Custom Services***

Custom services can be defined to add to the list of services available during firewall rule configuration. While common services have known TCP/UDP/ICMP ports for traffic, many custom or uncommon applications exist in the LAN or WAN. In the custom service configuration menu you can define a range of ports and identify the traffic type (TCP/UDP/ICMP) for this service. Once defined, the new service will appear in the services list of the firewall rules configuration menu.

**Figure 43: List of user defined services.**

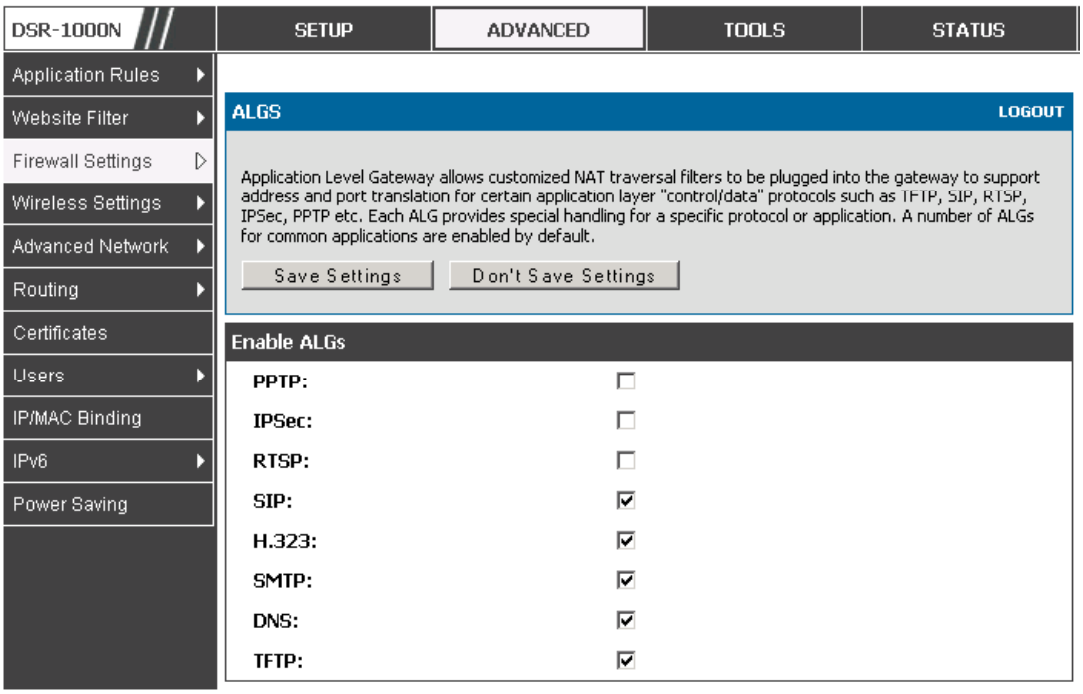



# 5.5 ALG support

***Advanced > Firewall Settings > ALGs***

Application Level Gateways (ALGs) are security component that enhance the firewall and NAT support of this router to seamlessly support application layer protocols. In some cases enabling the ALG will allow the firewall to use dynamic ephemeral TCP/ UDP ports to communicate with the known ports a particular client application (such as H.323 or RTSP) requires, without which the admin would have to open large number of ports to accomplish the same support. Because the ALG understands the protocol used by the specific application that it supports, it is a very secure and efficient way of introducing support for client applications through the router's firewall.

**Figure 44: Available ALG support on the router.**

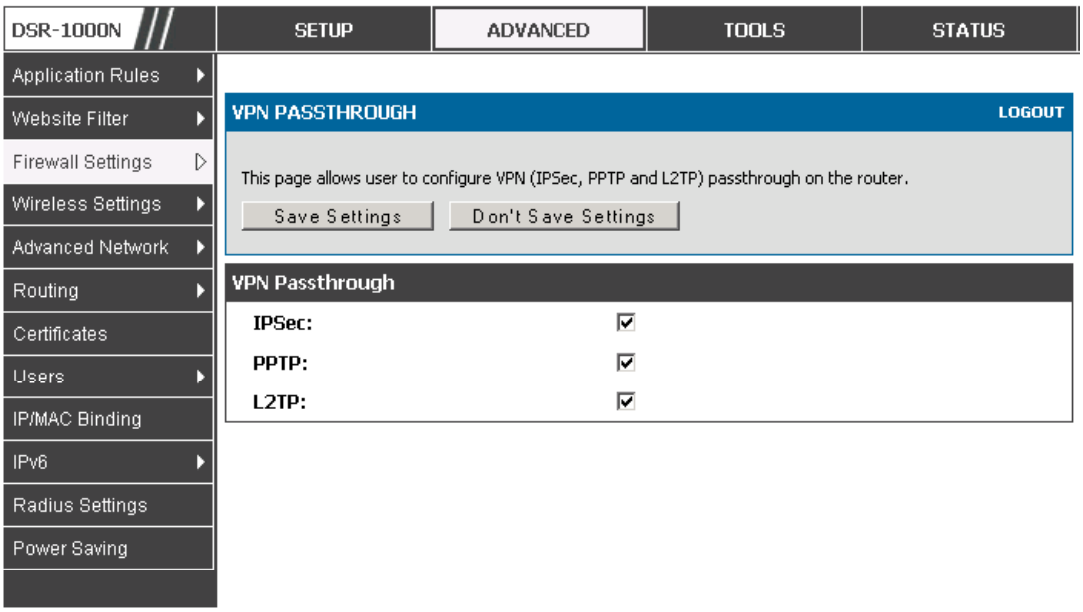



# 5.6 VPN Passthrough for Firewall

***Advanced > Firewall Settings > VPN Passthrough***

This router's firewall settings can be configured to allow encrypted VPN traffic for IPsec, PPTP, and L2TP VPN tunnel connections between the LAN and internet. A specific firewall rule or service is not appropriate to introduce this passthrough support; instead the appropriate check boxes in the VPN Passthrough page must be enabled.

**Figure 45: Passthrough options for VPN tunnels**




# 5.7 Application Rules

***Advanced > Application Rules > Application Rules***

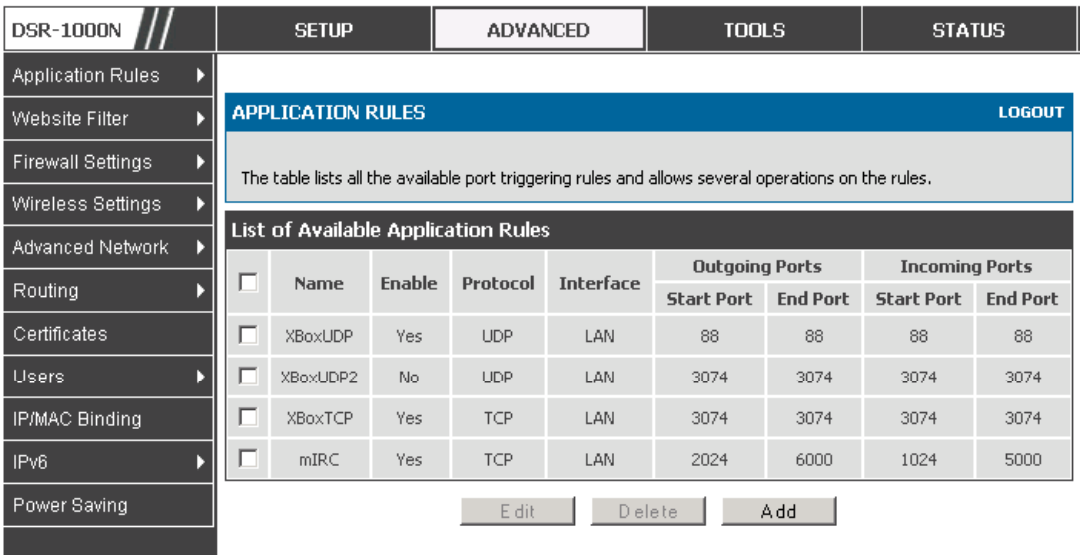
Application rules are also referred to as port triggering. This feature allows devices on the LAN or DMZ to request one or more ports to be forwarded to them. Port triggering waits for an outbound request from the LAN/DMZ on one of the defined outgoing ports, and then opens an incoming port for that specified type of traffic. This can be thought of as a form of dynamic port forwarding while an application is transmitting data over the opened outgoing or incoming port(s).

Port triggering application rules are more flexible than static port forwarding that is an available option when configuring firewall rules. This is because a port triggering rule does not have to reference a specific LAN IP or IP range. As well ports are not left open when not in use, thereby providing a level of security that port forwarding does not offer.

Port triggering is not appropriate for servers on the LAN, since there is a dependency on the LAN device making an outgoing connection before incoming ports are opened.

Some applications require that when external devices connect to them, they receive data on a specific port or range of ports in order to function properly. The router must send all incoming data for that application only on the required port or range of ports. The router has a list of common applications and games with corresponding outbound and inbound ports to open. You can also specify a port triggering rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled.

**Figure 46: List of Available Application Rules showing 4 unique rules**




The application rule status page will list any active rules, i.e. incoming ports that are being triggered based on outbound requests from a defined outgoing port.

# 5.8 Web Content Filtering

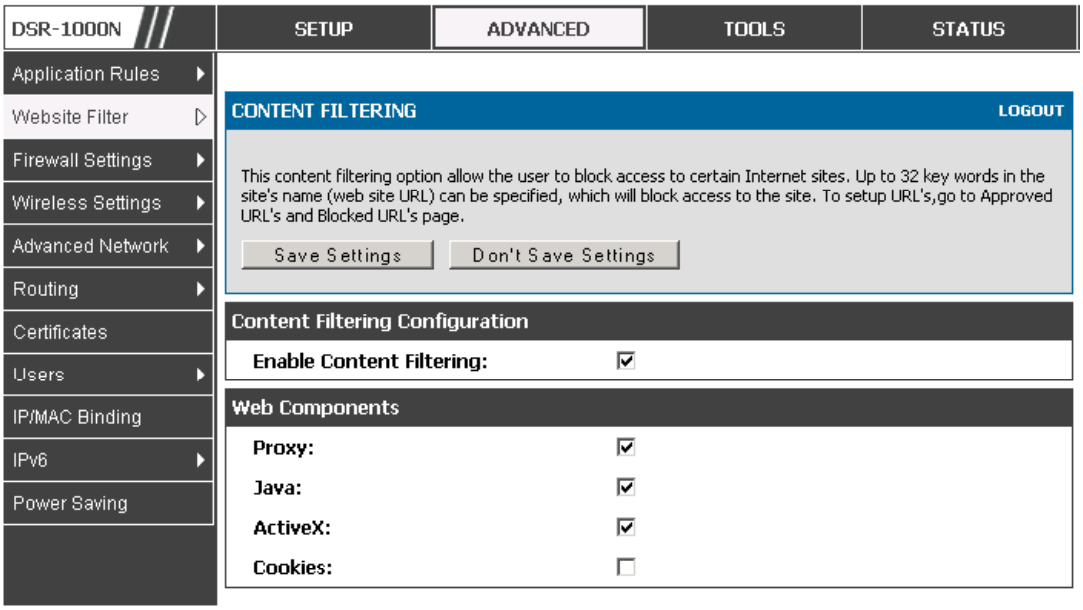
The gateway offers some standard web filtering options to allow the admin to easily create internet access policies between the secure LAN and insecure WAN. Instead of creating policies based on the type of traffic (as is the case when using firewall rules), web based content itself can be used to determine if traffic is allowed or dropped.

## 5.8.1 Content Filtering

***Advanced > Website Filter > Content Filtering***

Content filtering must be enabled to configure and use the subsequent features (list of Trusted Domains, filtering on Blocked Keywords, etc.). Proxy servers, which can be used to circumvent certain firewall rules and thus a potential security gap, can be blocked for all LAN devices. Java applets can be prevented from being downloaded from internet sites, and similarly the gateway can prevent ActiveX controls from being downloaded via Internet Explorer. For added security cookies, which typically contain session information, can be blocked as well for all devices on the private network.

**Figure 47: Content Filtering used to block access to proxy servers and prevent ActiveX controls from being downloaded**

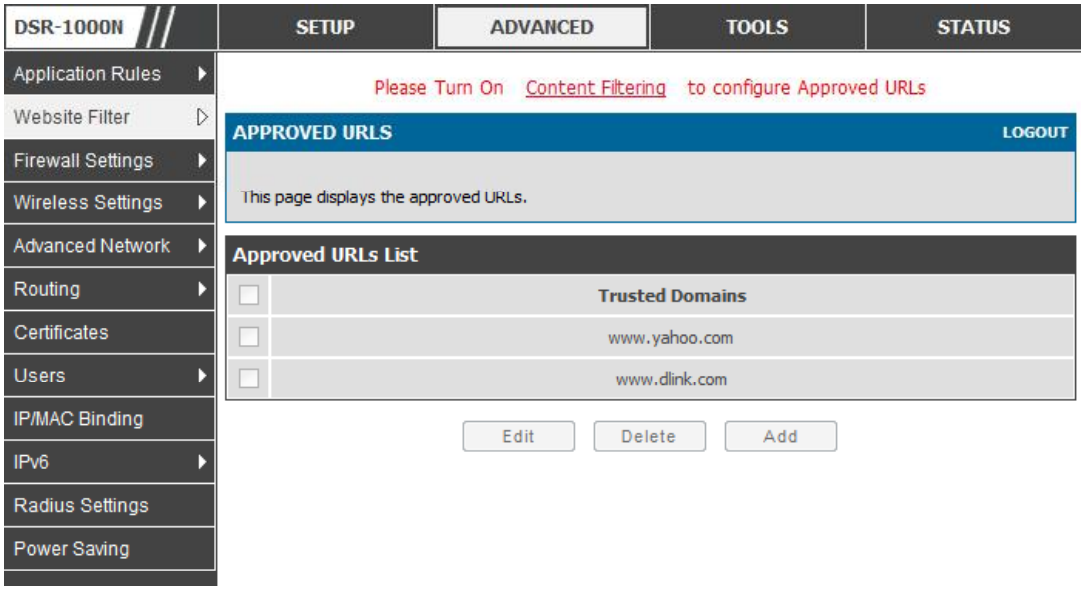



## 5.8.2 Approved URLs

***Advanced > Website Filter > Approved URLs***

The Approved URLs is an acceptance list for all URL domain names. Domains added to this list are allowed in any form. For example, if the domain "yahoo" is added to this list then all of the following URL's are permitted access from the LAN: www.yahoo.com, yahoo.co.uk, etc.

**Figure 48: Two trusted domains added to the Approved URLs List**

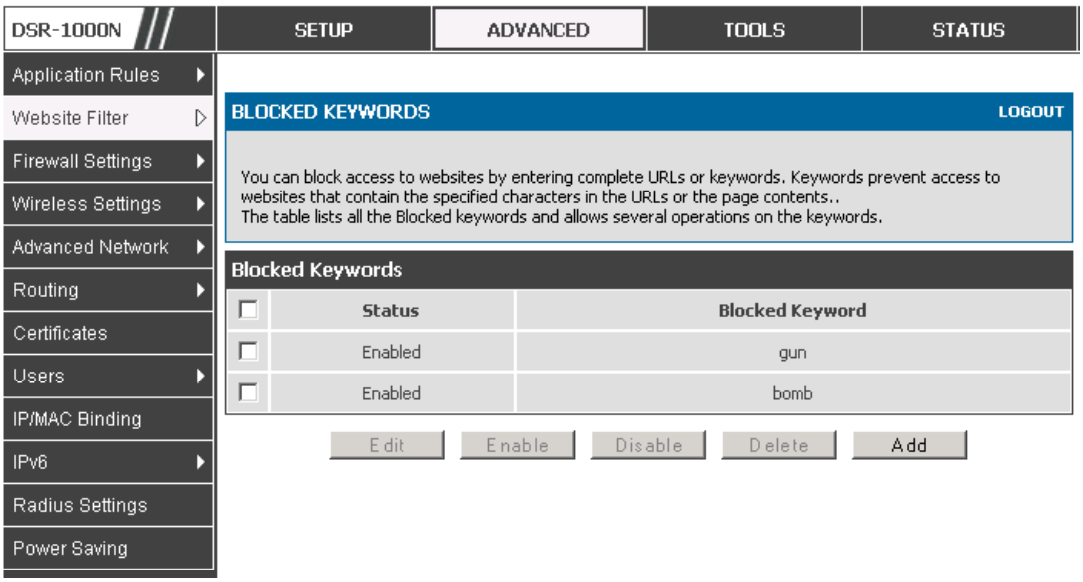



## 5.8.3 Blocked Keywords

***Advanced > Website Filter > Blocked Keywords***

Keyword blocking allows you to block all website URL's or site content that contains the keywords in the configured list. This is lower priority than the Approved URL List; i.e. if the blocked keyword is present in a site allowed by a Trusted Domain in the Approved URL List, then access to that site will be allowed. Import/export from a text or CSV file for keyword blocking is also supported.

**Figure 49: Two keywords added to the block list**

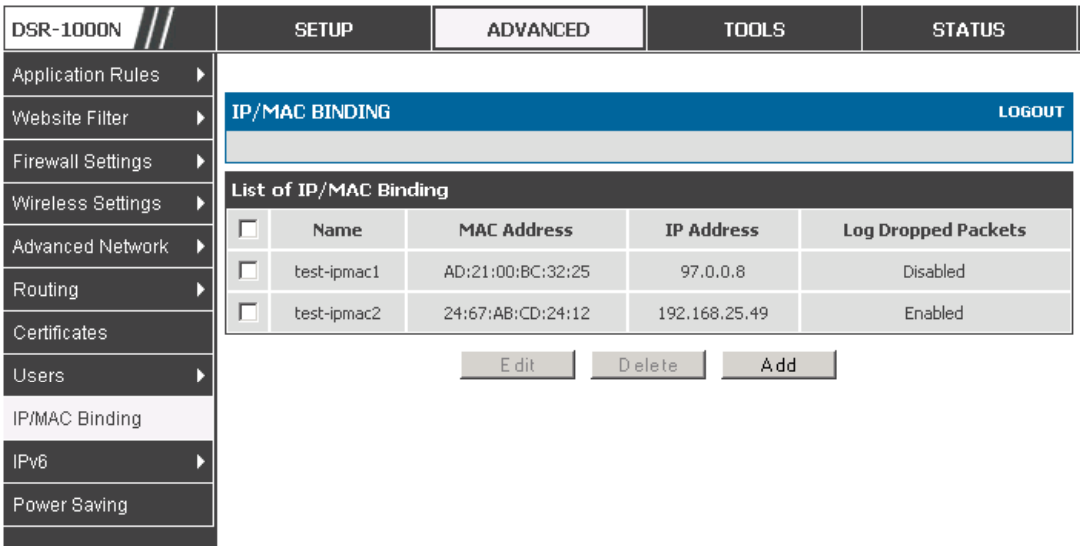



# 5.9 IP/MAC Binding

### *Advanced > IP/MAC Binding*

Another available security measure is to only allow outbound traffic (from the LAN to WAN) when the LAN node has an IP address matching the MAC address bound to it. This is IP/MAC Binding, and by enforcing the gateway to validate the source traffic's IP address with the unique MAC Address of the configured LAN node, the administrator can ensure traffic from that IP address is not spoofed. In the event of a violation (i.e. the traffic's source IP address doesn't match up with the expected MAC address having the same IP address) the packets will be dropped and can be logged for diagnosis.

**Figure 50: The following example binds a LAN host's MAC Address to an IP address served by DSR. If there is an IP/MAC Binding violation, the violating packet will be dropped and logs will be captured**

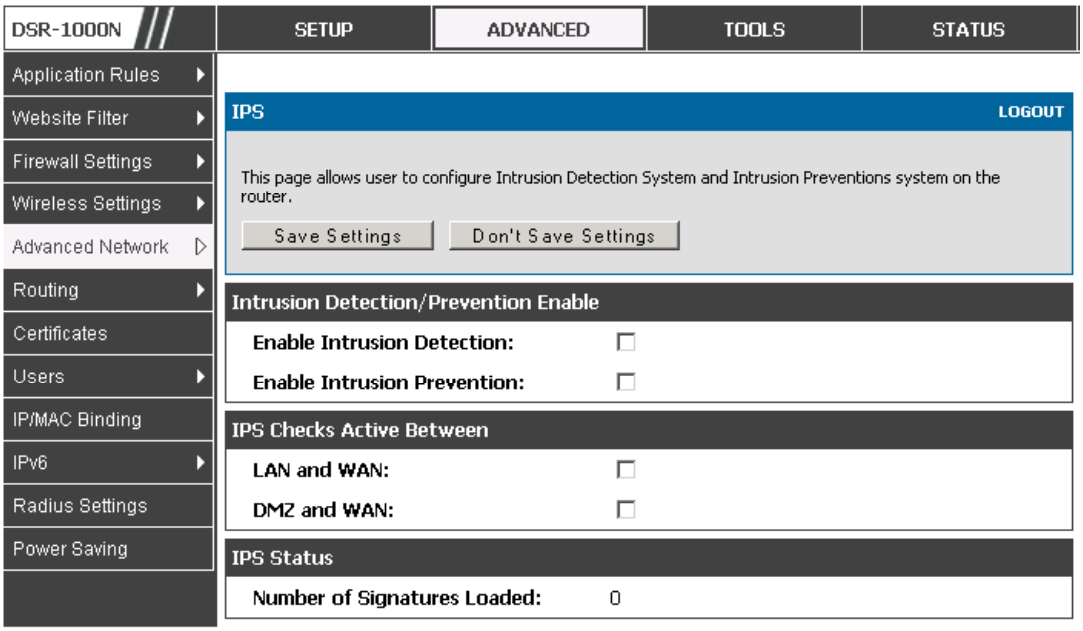



# 5.10 Intrusion Prevention (IPS)

### *Advanced > Advanced Network > IPS*

The gateway's Intrusion Prevention System (IPS) prevents malicious attacks from the internet from accessing the private network. Static attack signatures loaded to the DSR allow common attacks to be detected and prevented. The checks can be enabled between the WAN and DMZ or LAN, and a running counter will allow the administrator to see how many malicious intrusion attempts from the WAN have been detected and prevented.

**Figure 51: Intrusion Prevention features on the router**



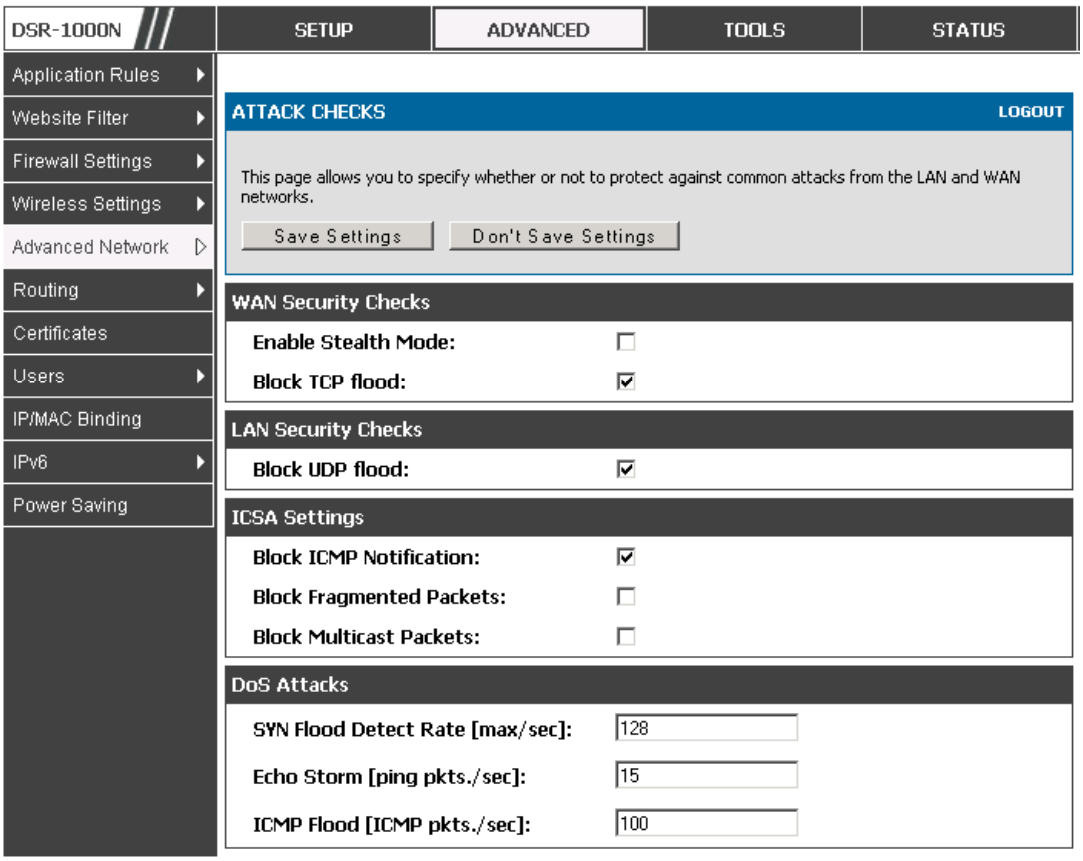

# 5.11 Protecting from Internet Attacks

### *Advanced > Advanced Network > Attack Checks*

Attacks can be malicious security breaches or unintentional network issues that render the router unusable. Attack checks allow you to manage WAN security threats such as continual ping requests and discovery via ARP scans. TCP and UDP flood attack checks can be enabled to manage extreme usage of WAN resources.

Additionally certain Denial-of-Service (DoS) attacks can be blocked. These attacks, if uninhibited, can use up processing power and bandwidth and prevent regular network services from running normally. ICMP packet flooding, SYN traffic flooding, and Echo storm thresholds can be configured to temporarily suspect traffic from the offending source.

**Figure 52: Protecting the router and LAN from internet attacks**



# Chapter 6. IPsec / PPTP / L2TP VPN

A VPN provides a secure communication channel ("tunnel") between two gateway routers or a remote PC client. The following types of tunnels can be created:

- Gateway-to-gateway VPN: to connect two or more routers to secure traffic between remote sites.
- Remote Client (client-to-gateway VPN tunnel): A remote client initiates a VPN tunnel as the IP address of the remote PC client is not known in advance. The gateway in this case acts as a responder.
- Remote client behind a NAT router: The client has a dynamic IP address and is behind a NAT Router. The remote PC client at the NAT router initiates a VPN tunnel as the IP address of the remote NAT router is not known in advance. The gateway WAN port acts as responder.
- PPTP server for LAN / WAN PPTP client connections.
- L2TP server for LAN / WAN L2TP client connections.

**Figure 53: Example of Gateway-to-Gateway IPsec VPN tunnel using two DSR routers connected to the Internet**

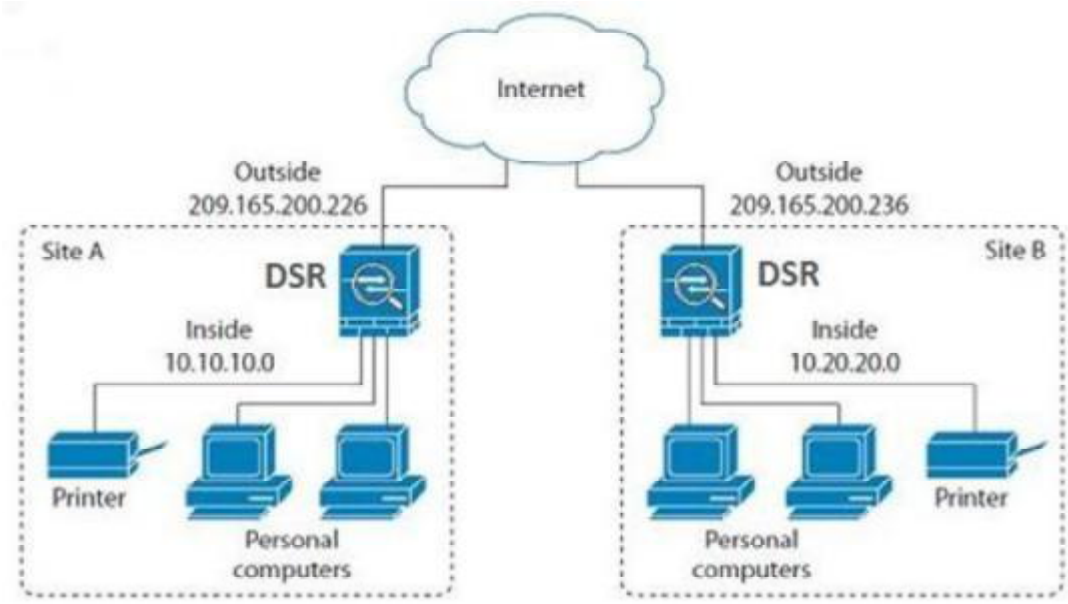
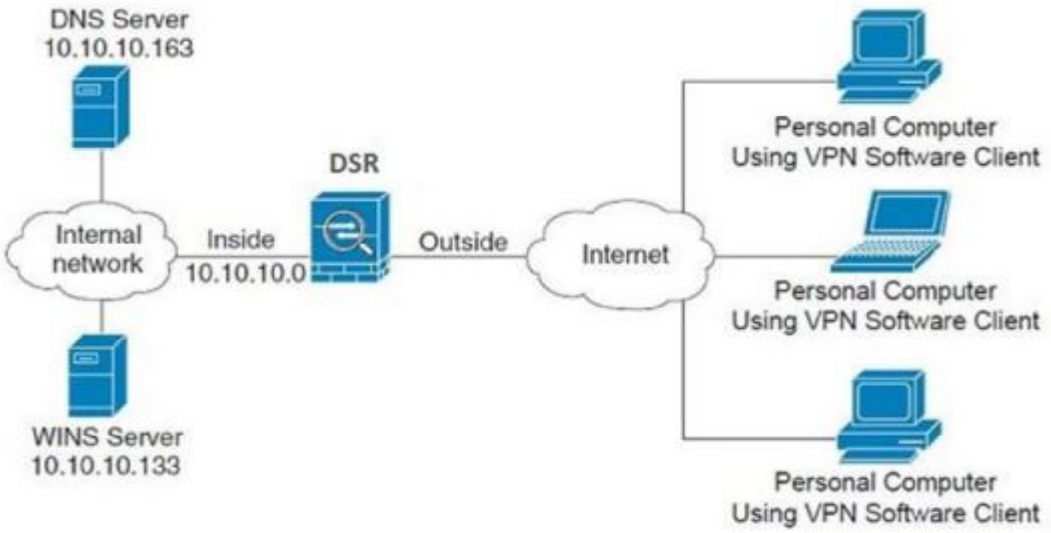


**Figure 54: Example of three IPsec client connections to the internal network through the DSR IPsec gateway**

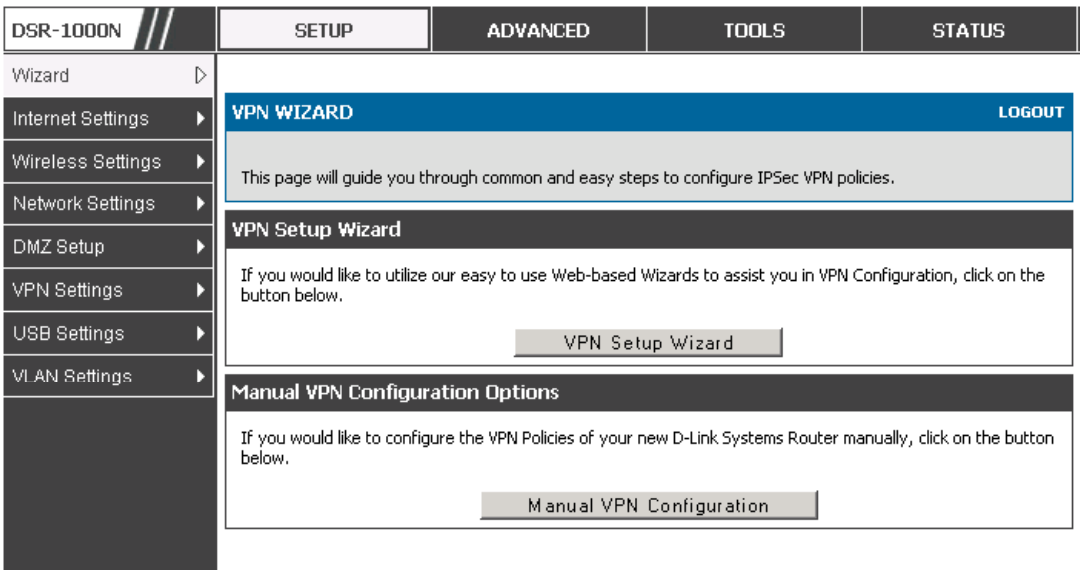



# 6.1 VPN Wizard

***Setup > Wizard > VPN Wizard***

You can use the VPN wizard to quickly create both IKE and VPN policies. Once the IKE or VPN policy is created, you can modify it as required.

**Figure 55: VPN Wizard launch screen**




To easily establish a VPN tunnel using VPN Wizard, follow the steps below:

1. Select the VPN tunnel type to create

- The tunnel can either be a gateway to gateway connection (site-to-site) or a tunnel to a host on the internet (remote access).
- Set the Connection Name and pre-shared key: the connection name is used for management, and the pre-shared key will be required on the VPN client or gateway to establish the tunnel
- Determine the local gateway for this tunnel; if there is more than 1 WAN configured the tunnel can be configured for either of the gateways.

2. Configure Remote and Local WAN address for the tunnel endpoints

- Remote Gateway Type: identify the remote endpoint of the tunnel by FQDN or static IP address
- Remote WAN IP address / FQDN: This field is enabled only if the peer you are trying to connect to is a Gateway. For VPN Clients, this IP address or Internet Name is determined when a connection request is received from a client.
- Local Gateway Type: identify this router's endpoint of the tunnel by FQDN or static IP address

- Local WAN IP address / FQDN: This field can be left blank if you are not using a different FQDN or IP address than the one specified in the WAN port's configuration.

3. Configure the Secure Connection Remote Accessibility fields to identify the remote network:

- Remote LAN IP address: address of the LAN behind the peer gateway
- Remote LAN Subnet Mask: the subnet mask of the LAN behind the peer

> **Note:** The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

4. Review the settings and click Connect to establish the tunnel.

The Wizard will create a Auto IPsec policy with the following default values for a VPN Client or Gateway policy (these can be accessed from a link on the Wizard page):

| Parameter | Default value from Wizard |
|---|---|
| Exchange Mode | Aggressive (Client policy ) or Main (Gateway policy) |
| ID Type | FQDN |
| Local WAN ID | wan_local.com (only applies to Client policies) |
| Remote WAN ID | wan_remote.com (only applies to Client policies) |
| Encryption Algorithm | 3DES |
| Authentication Algorithm | SHA-1 |
| Authentication Method | Pre-shared Key |
| PFS Key-Group | DH-Group 2(1024 bit) |
| Life Time (Phase 1) | 24 hours |
| Life Time (Phase 2) | 8 hours |
| NETBIOS | Enabled (only applies to Gateway policies) |

> The VPN Wizard is the recommended method to set up an Auto IPsec policy. Once the Wizard creates the matching IKE and VPN policies required by the Auto policy, one can modify the required fields through the edit link. Refer to the online help for details.

# 6.2 Configuring IPsec Policies

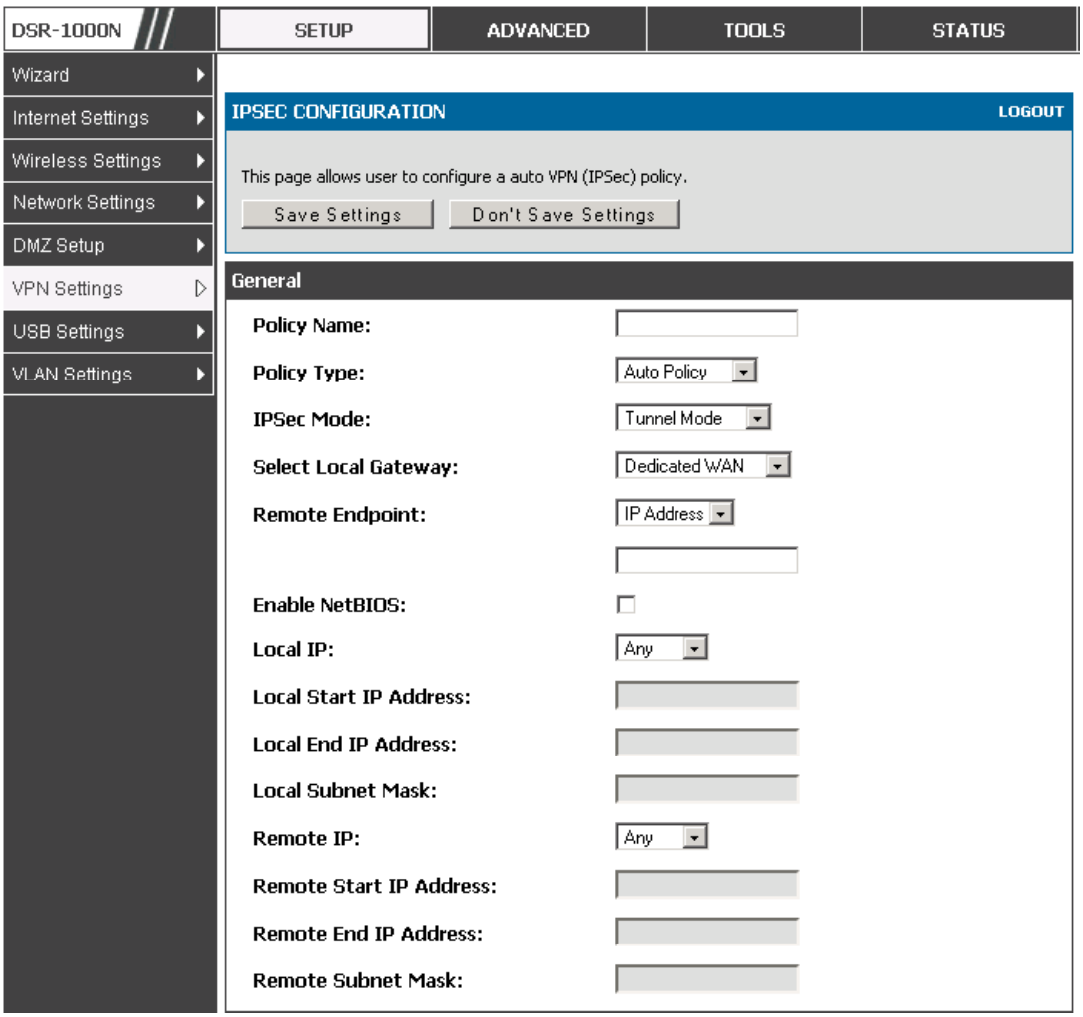
***Setup > VPN Settings > IPsec > IPsec Policies***

An IPsec policy is between this router and another gateway or this router and a IPsec client on a remote host. The IPsec mode can be either tunnel or transport depending on the network being traversed between the two policy endpoints.

- Transport: This is used for end-to-end communication between this router and the tunnel endpoint, either another IPsec gateway or an IPsec VPN client on a host. Only the data payload is encrypted and the IP header is not modified or encrypted.
- Tunnel: This mode is used for network-to-network IPsec tunnels where this gateway is one endpoint of the tunnel. In this mode the entire IP packet including the header is encrypted and/or authenticated.

When tunnel mode is selected, you can enable NetBIOS and DHCP over IPsec. DHCP over IPsec allows this router to serve IP leases to hosts on the remote LAN. As well in this mode you can define the single IP address, range of IPs, or subnet on both the local and remote private networks that can communicate over the tunnel.

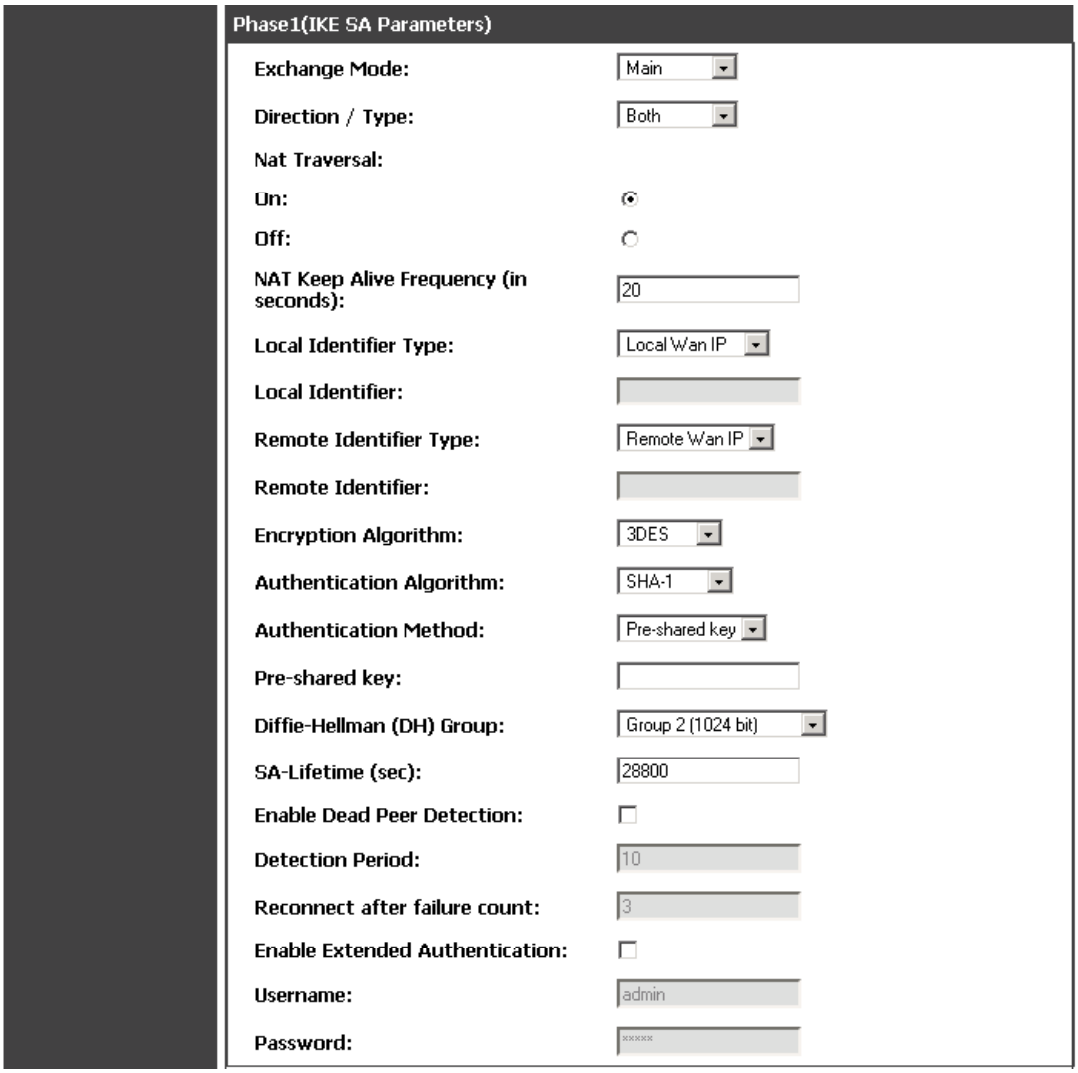
**Figure 56: IPsec policy configuration**




Once the tunnel type and endpoints of the tunnel are defined you can determine the Phase 1 / Phase 2 negotiation to use for the tunnel. This is covered in the IPsec mode setting, as the policy can be Manual or Auto. For Auto policies, the Internet Key Exchange (IKE) protocol dynamically exchanges keys between two IPsec hosts. The Phase 1 IKE parameters are used to define the tunnel's security association details. The Phase 2 Auto policy parameters cover the security association lifetime and encryption/authentication details of the phase 2 key negotiation.

The VPN policy is one half of the IKE/VPN policy pair required to establish an Auto IPsec VPN tunnel. The IP addresses of the machine or machines on the two VPN endpoints are configured here, along with the policy parameters required to secure the tunnel

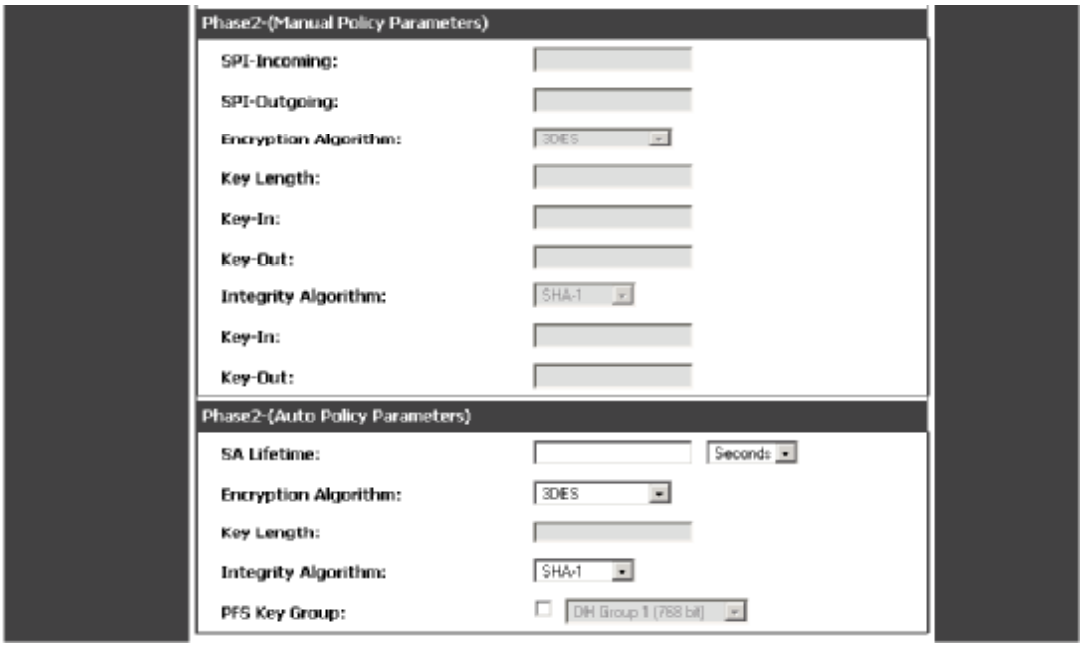
**Figure 57: IPsec policy configuration continued (Auto policy via IKE)**




A Manual policy does not use IKE and instead relies on manual keying to exchange authentication parameters between the two IPsec hosts. The incoming and outgoing security parameter index (SPI) values must be mirrored on the remote tunnel endpoint. As well the encryption and integrity algorithms and keys must match on the remote IPsec host exactly in order for the tunnel to establish successfully. Note that using Auto policies with IKE are preferred as in some IPsec implementations the SPI (security parameter index) values require conversion at each endpoint.

DSR supports VPN roll-over feature. This means that policies configured on primary WAN will rollover to the seconday WAN incase of a link failure on a primary WAN. This feature can be used only if your WAN is configured in Auto-Rolleover mode.

**Figure 58: IPsec policy configuration continued (Auto / Manual Phase 2)**




## 6.2.1 Extended Authentication (XAUTH)

You can also configure extended authentication (XAUTH). Rather than configure a unique VPN policy for each user, you can configure the VPN gateway router to authenticate users from a stored list of user accounts or with an external authentication server such as a RADIUS server. With a user database, user accounts created in the router are used to authenticate users.

With a configured RADIUS server, the router connects to a RADIUS server and passes to it the credentials that it receives from the VPN client. You can secure the connection between the router and the RADIUS server with the authentication protocol supported by the server (PAP or CHAP). For RADIUS – PAP, the router first checks in the user database to see if the user credentials are available; if they are not, the router connects to the RADIUS server.

## 6.2.2 Internet over IPSec tunnel

In this feature all the traffic will pass through the VPN Tunnel and from the Remote Gateway the packet will be routed to Internet. On the remote gateway side, the outgoing packet will be SNAT'ed.

# 6.3 Configuring VPN clients

Remote VPN clients must be configured with the same VPN policy parameters used in the VPN tunnel that the client wishes to use: encryption, authentication, life time, and PFS key-group. Upon establishing these authentication parameters, the VPN Client user database must also be populated with an account to give a user access to the tunnel.

> VPN client software is required to establish a VPN tunnel between the router and remote endpoint. Open source software (such as OpenVPN or Openswan) as well as Microsoft IPsec VPN software can be configured with the required IKE policy parameters to establish an IPsec VPN tunnel. Refer to the client software guide for detailed instructions on setup as well as the router's online help.

The user database contains the list of VPN user accounts that are authorized to use a given VPN tunnel. Alternatively VPN tunnel users can be authenticated using a configured Radius database. Refer to the online help to determine how to populate the user database and/or configure RADIUS authentication.

# 6.4 PPTP / L2TP Tunnels

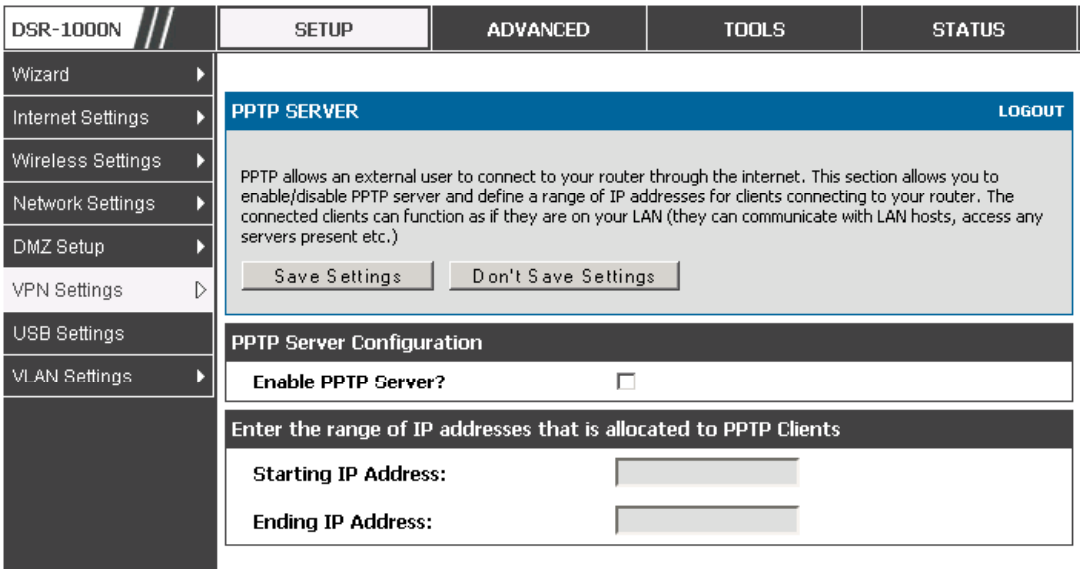
This router supports VPN tunnels from either PPTP or L2TP ISP servers. The router acts as a broker device to allow the ISP's server to create a TCP control connection between the LAN VPN client and the VPN server.

## 6.4.1 PPTP Tunnel Support

***Setup > VPN Settings > PPTP > PPTP Server***

A PPTP VPN can be established through this router. Once enabled a PPTP server is available on the router for LAN and WAN PPTP client users to access. Once the PPTP server is enabled, PPTP clients that are within the range of configured IP addresses of allowed clients can reach the router's PPTP server. Once authenticated by the PPTP server (the tunnel endpoint), PPTP clients have access to the network managed by the router.

**Figure 59: PPTP tunnel configuration – PPTP Server**

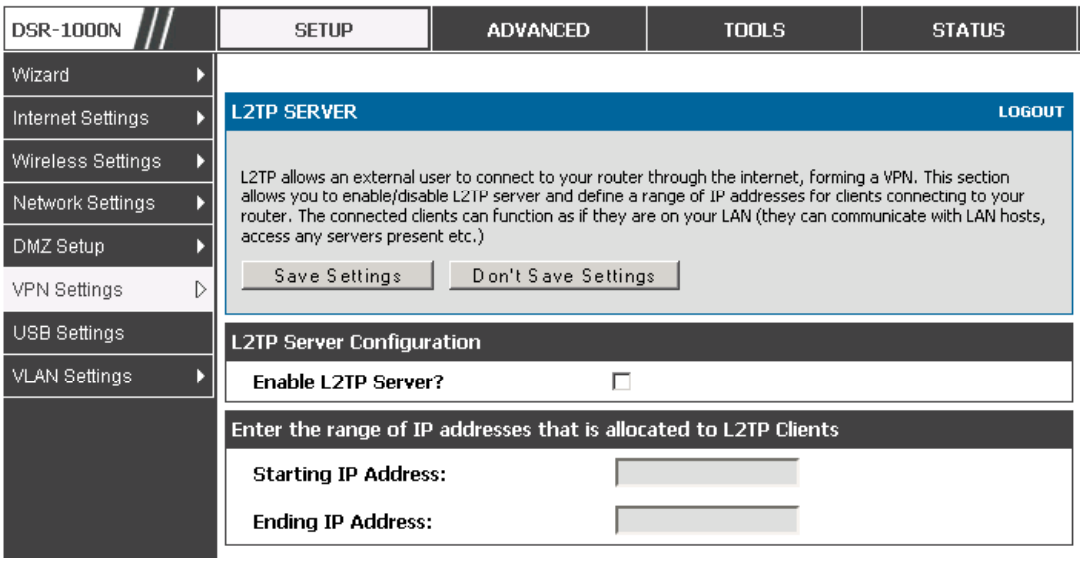



## 6.4.2 L2TP Tunnel Support

***Setup > VPN Settings > L2TP > L2TP Server***

A L2TP VPN can be established through this router. Once enabled a L2TP server is available on the router for LAN and WAN L2TP client users to access. Once the L2TP server is enabled, L2TP clients that are within the range of configured IP addresses of allowed clients can reach the router's L2TP server. Once authenticated by the L2TP server (the tunnel endpoint), L2TP clients have access to the network managed by the router.

**Figure 60: L2TP tunnel configuration – L2TP Server**



# Chapter 7. SSL VPN

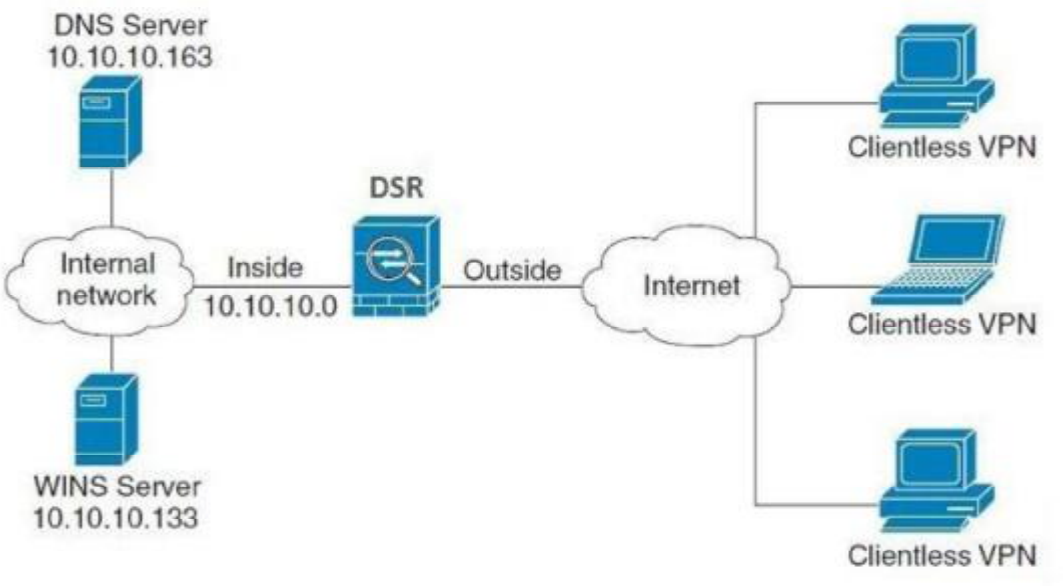
The router provides an intrinsic SSL VPN feature as an alternate to the standard IPsec VPN. SSL VPN differs from IPsec VPN mainly by removing the requirement of a pre-installed VPN client on the remote host. Instead, users can securely login through the SSL User Portal using a standard web browser and receive access to configured network resources within the corporate LAN. The router supports multiple concurrent sessions to allow remote users to access the LAN over an encrypted link through a customizable user portal interface, and each SSL VPN user can be assigned unique privileges and network resource access levels.

The remote user can be provided different options for SSL service through this router:

- **VPN Tunnel**: The remote user's SSL enabled browser is used in place of a VPN client on the remote host to establish a secure VPN tunnel. A SSL VPN client (Active-X or Java based) is installed in the remote host to allow the client to join the corporate LAN with pre-configured access/policy privileges. At this point a virtual network interface is created on the user's host and this will be assigned an IP address and DNS server address from the router. Once established, the host machine can access allocated network resources.
- **Port Forwarding**: A web-based (ActiveX or Java) client is installed on the client machine again. Note that Port Forwarding service only supports TCP connections between the remote user and the router. The router administrator can define specific services or applications that are available to remote port forwarding users instead of access to the full LAN like the VPN tunnel.

ActiveX clients are used when the remote user accesses the portal using the Internet Explorer browser. The Java client is used for other browsers like Mozilla Firefox, Netscape Navigator, Google Chrome, and Apple Safari.

**Figure 61: Example of clientless SSL VPN connections to the DSR**




# 7.1 Users, Groups, and Domains

***Advanced > Users > Users***

Authentication of the users (IPsec, SSL VPN, or GUI) is done by the router using either a local database on the router or external authentication servers (i.e. LDAP or RADIUS). The remote user must specify the user, group and domain when logging in to the router. One or more users are members of a Group. One or more Groups belong to an authentication Domain.

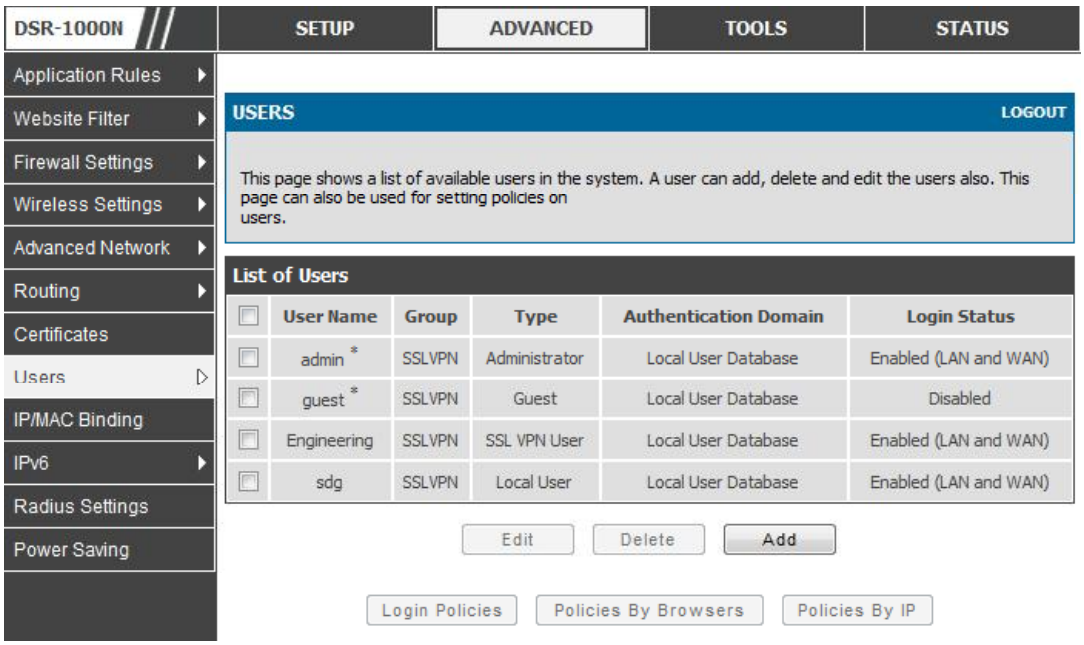
The user settings contain the following:

- User Name: This is unique identifier of the user.
- First Name: This is the user's first name
- Last Name: This is the user's last name
- User Type: The user's access privileges are defined as an SSL VPN User, administrator, guest, XAUTH user, L2TP user, PPTP user, Local User. The SSL VPN User or administrator user should be selected.
- Select Group: A group is chosen from a list of configured groups.
- Password: The password associated with the user name.
- Confirm Password: The same password as above is required to mitigate against typing errors.

- Idle Timeout: The session timeout for the user.

Once the user is configured, the DSR will display a list of all configured users.

**Figure 62: Available Users with login status and associated Group/Domain**




### *Advanced > Users > Domains*

The Domain determines the authentication method (local user database, external server) to be used when validating the remote user's connection. As well the Domain determines the portal layout presented to the remote SSL user. Since the portal layout assigns access to SSL VPN tunnel and/or SSL VPN Port Forwarding features, the domain is essential in defining the authentication and features exposed to SSL users.

The following information is used to configure a domain:

- Domain Name: The unique identifier of the domain.
- Authentication Type: The authentication type can be one of the following: Local User Database, Radius-PAP, Radius-CHAP, Radius-MSCHAP, Radius-MSCHAPv2, NT Domain, Active Directory, and LDAP.
- Authentication Server: If the SSL VPN connection will use an authentication method other than the Local User Database (such as a RADIUS server), then the sever access details are needed. If there are multiple authentication servers, user can enter the details for upto three authentication servers.
- Authentication Secret: If the domain uses RADIUS authentication then the authentication secret is required (and this has to match the secret configured on the RADIUS server).

- Timeout: The timeout period for reaching the authentication server.
- Retries: The number of retries to authenticate with the authentication server after which the DSR stops trying to reach the server.
- Workgroup: This is required is for NT domain authentication. If there are multiple workgroups, user can enter the details for upto two workgroups.
- LDAP Base DN: This is the base domain name for the LDAP authentication server. If there are multiple LDAP authentication servers, user can enter the details for upto two LDAP Base DN.
- Active Directory Domain: If the domain uses the Active Directory authentication, the Active Directory domain name is required. Users configured in the Active Directory database are given access to the SSL VPN portal with their Active Directory username and password. If there are multiple Active Directory domains, user can enter the details for upto two authentication domains.

Once the domain is configured, the DSR will display a list of all configured domains.

***Advanced > Users > Groups***

Groups are used to assign access policies to a set of SSL users within a domain. Groups are domain subsets that can be seen as types of SSL users; some groups require access to all available network resources and some can be provided access to a select few. With groups, a very secure hierarchy of SSL VPN remote access can be created for all types of users with minimal number of policies to configure.

To configure a group in the DSR, enter the following information:

- Name: This is a unique identifier for a group name.
- Domain: This is the authenticating domain the group is attached to.
- Idle timeout: This is the log in timeout period for users of this group.

Once the group is defined the DSR will display a list of all configured groups.

You must create a Domain first, and then a new Group can be created and assigned to the Domain. The last step is to add specific SSL VPN users to an already-configured Group.

## 7.1.1 User Types and Passwords

***Advanced > Users > Users***

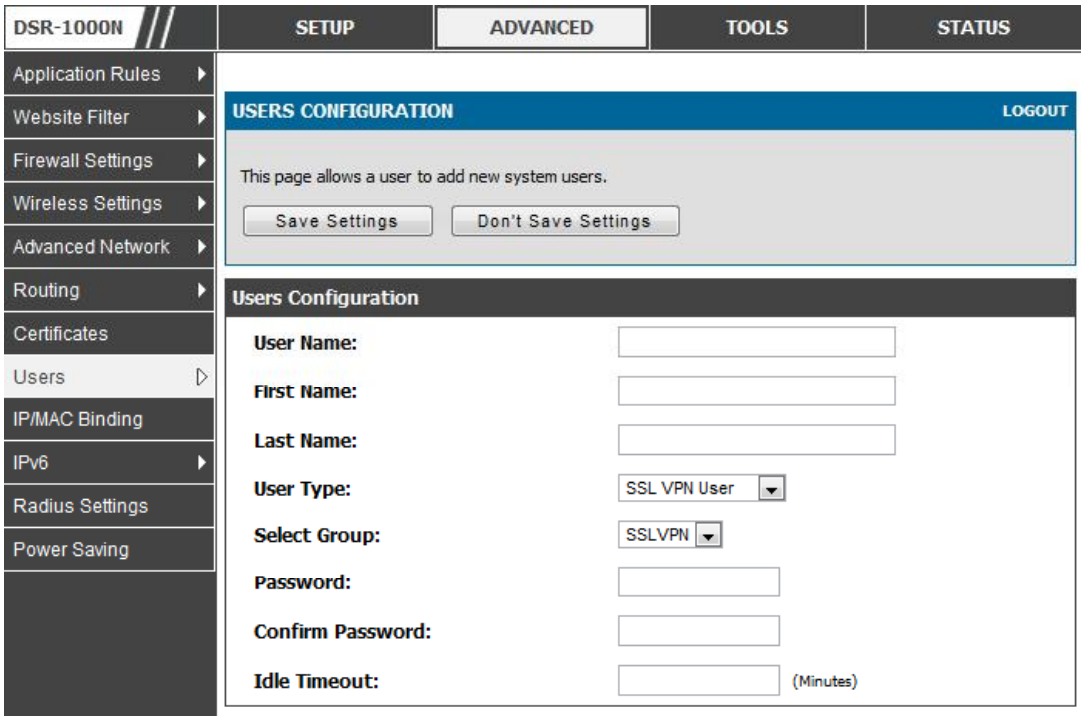
User level policies can be specified by browser, IP address of the host, and whether the user can login to the router's GUI in addition to the SSL VPN portal. The following user types are assigned to a user that reaches the GUI login screen from the LAN or WAN:

- Administrator: This is the router's super-user, and can manage the router, use SSL VPN to access network resources, and login to L2TP/PPTP servers on the WAN. There will always be one default administrator user for the GUI.

- Guest (read only): The guest user gains read only access to the GUI to observe and review configuration settings. The guest does not have SSL VPN access.
- SSL VPN User: This user has access to the SSL VPN services as determined by the group policies and authentication domain of which it is a member. The domain-determined SSL VPN portal will be displayed when logging in with this user type.
- XAuth User: This user's authentication is performed by an externally configured RADIUS or other Enterprise server. It is not part of the local user database.
- L2TP User: These are L2TP VPN tunnel LAN users that can establish a tunnel with the L2TP server on the WAN.
- PPTP User: These are PPTP VPN tunnel LAN users that can establish a tunnel with the PPTP server on the WAN.
- Local User: This user's authentication domain is located on the router itself.

Once the user type is determined, you can define/modify the password and idle login timeout for the user. It is recommended that passwords contains no dictionary words from any language, and is a mixture of letters (both uppercase and lowercase), numbers, and symbols. The password can be up to 30 characters.

**Figure 63: User configuration options**



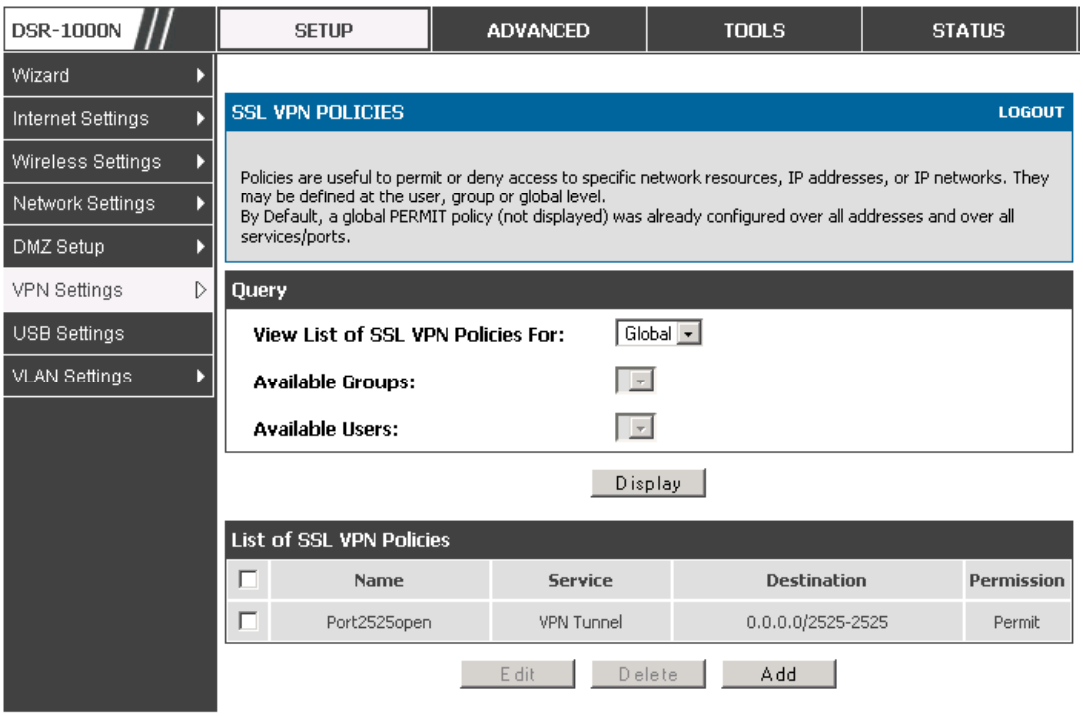

# 7.2 Using SSL VPN Policies

***Setup > VPN Settings > SSL VPN Server > SSL VPN Policies***

SSL VPN Policies can be created on a Global, Group, or User level. User level policies take precedence over Group level policies and Group level policies take precedence over Global policies. These policies can be applied to a specific network resource, IP address or ranges on the LAN, or to different SSL VPN services supported by the router. The List of Available Policies can be filtered based on whether it applies to a user, group, or all users (global).

A more specific policy takes precedence over a generic policy when both are applied to the same user/group/global domain. I.e. a policy for a specific IP address takes precedence over a policy for a range of addresses containing the IP address already referenced.

**Figure 64: List of SSL VPN polices (Global filter)**



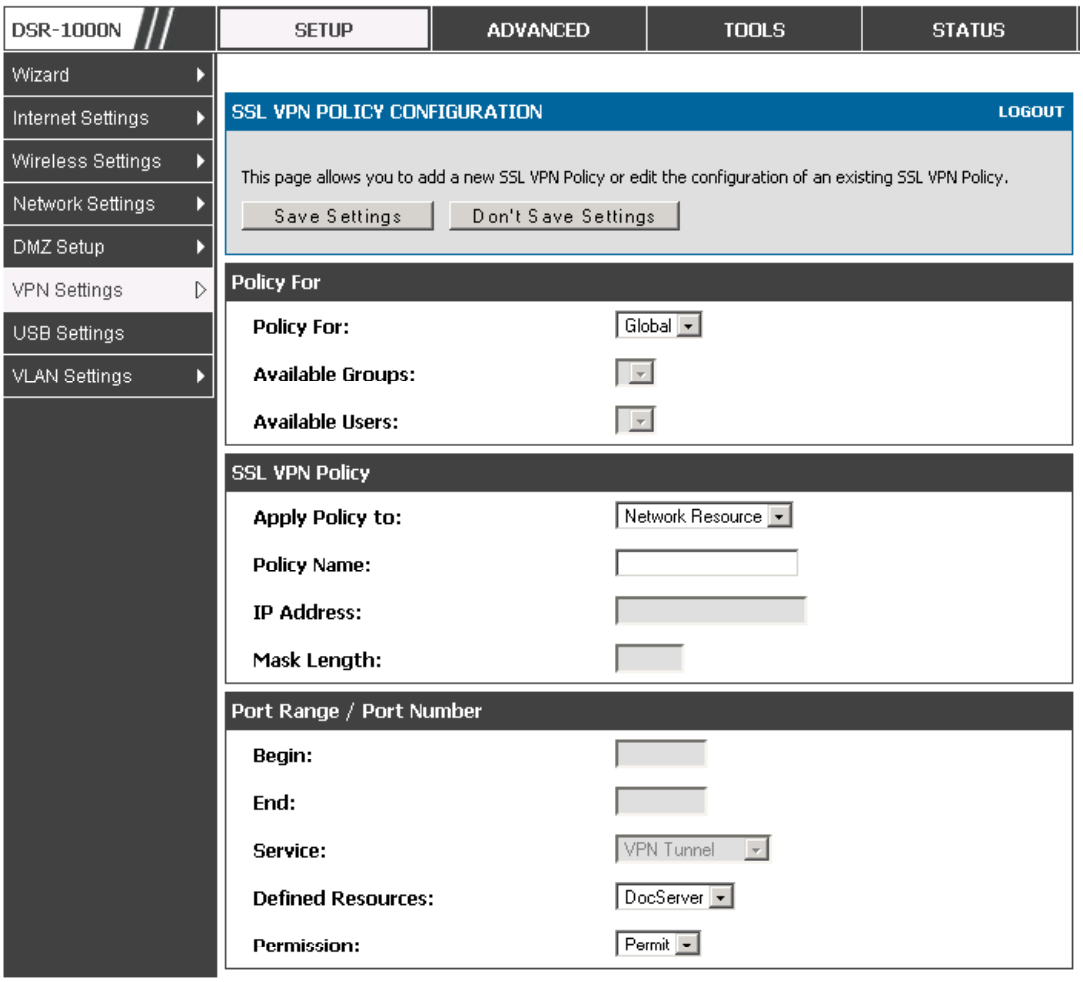

To add a SSL VPN policy, you must first assign it to a user, group, or make it global (i.e. applicable to all SSL VPN users). If the policy is for a group, the available configured groups are shown in a drop down menu and one must be selected. Similarly, for a user defined policy a SSL VPN user must be chosen from the available list of configured users.

The next step is to define the policy details. The policy name is a unique identifier for this rule. The policy can be assigned to a specific Network Resource (details follow in the subsequent section), IP address, IP network, or all devices on the LAN of the router. Based on the selection of one of these four options, the appropriate configuration fields are required (i.e. choosing the network resources from a list of defined resources, or defining the IP addresses). For applying the policy to addresses the port range/port number can be defined.

The final steps require the policy permission to be set to either permit or deny access to the selected addresses or network resources. As well the policy can be specified for one or all of the supported SSL VPN services (i.e. VPN tunnel)

Once defined, the policy goes into effect immediately. The policy name, SSL service it applies to, destination (network resource or IP addresses) and permission (deny/permit) is outlined in a list of configured policies for the router.

**Figure 65: SSL VPN policy configuration**




To configure a policy for a single user or group of users, enter the following information:

- Policy for: The policy can be assigned to a group of users, a single user, or all users (making it a global policy). To customize the policy for specific users or groups, the user can select from the Available Groups and Available Users drop down.
- Apply policy to: This refers to the LAN resources managed by the DSR, and the policy can provide (or prevent) access to network resources, IP address, IP network, etc.
- Policy name: This field is a unique name for identifying the policy. IP address: Required when the governed resource is identified by its IP address or range of addresses.
- Mask Length: Required when the governed resource is identified by a range of addresses within a subnet.

- Port range: If the policy governs a type of traffic, this field is used for defining TCP or UDP port number(s) corresponding to the governed traffic. Leaving the starting and ending port range blank corresponds to all UDP and TCP traffic.
- Service: This is the SSL VPN service made available by this policy. The services offered are VPN tunnel, port forwarding or both.
- Defined resources: This policy can provide access to specific network resources. Network resources must be configured in advance of creating the policy to make them available for selection as a defined resource. Network resources are created with the following information
- Permission: The assigned resources defined by this policy can be explicitly permitted or denied.

## 7.2.1 Using Network Resources

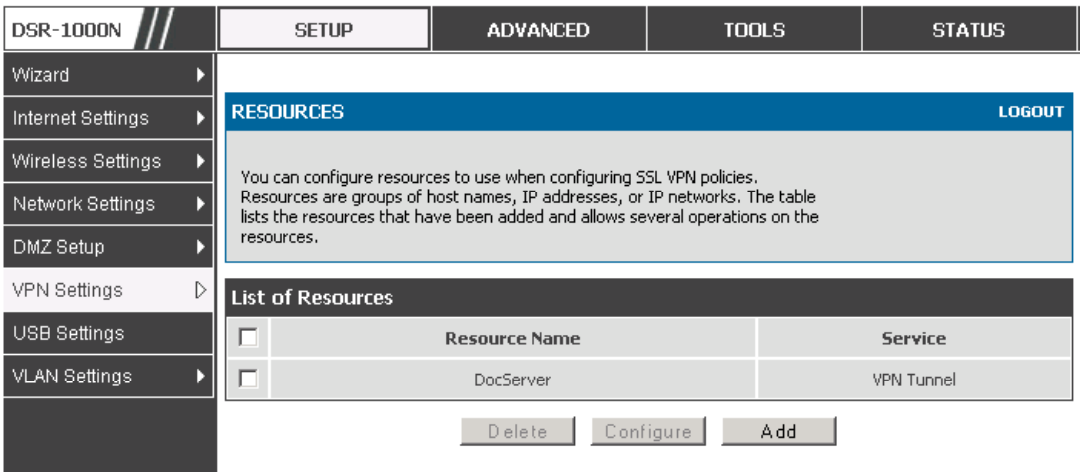
***Setup > VPN Settings > SSL VPN Server > Resources***

Network resources are services or groups of LAN IP addresses that are used to easily create and configure SSL VPN policies. This shortcut saves time when creating similar policies for multiple remote SSL VPN users.

Adding a Network Resource involves creating a unique name to identify the resource and assigning it to one or all of the supported SSL services. Once this is done, editing one of the created network resources allows you to configure the object type (either IP address or IP range) associated with the service. The Network Address, Mask Length, and Port Range/Port Number can all be defined for this resource as required. A network resource can be defined by configuring the following in the GUI:

- Resource name: A unique identifier name for the resource.
- Service: The SSL VPN service corresponding to the resource (VPN tunnel, Port Forwarding or All).

**Figure 66: List of configured resources, which are available to assign to SSL VPN policies**




# 7.3 Application Port Forwarding

***Setup > VPN Settings > SSL VPN Server > Port Forwarding***

Port forwarding allows remote SSL users to access specified network applications or services after they login to the User Portal and launch the Port Forwarding service. Traffic from the remote user to the router is detected and re-routed based on configured port forwarding rules.

Internal host servers or TCP applications must be specified as being made accessible to remote users. Allowing access to a LAN server requires entering the local server IP address and TCP port number of the application to be tunneled. The table below lists some common applications and corresponding TCP port numbers:

| TCP Application | Port Number |
|---|---|
| FTP Data (usually not needed) | 20 |
| FTP Control Protocol | 21 |
| SSH | 22 |
| Telnet | 23 |
| SMTP (send mail) | 25 |
| HTTP (web) | 80 |
| POP3 (receive mail) | 110 |
| NTP (network time protocol) | 123 |
| Citrix | 1494 |
| Terminal Services | 3389 |
| VNC (virtual network computing) | 5900 or 5800 |

As a convenience for remote users, the hostname (FQDN) of the network server can be configured to allow for IP address resolution. This host name resolution provides users with easy-to-remember FQDN's to access TCP applications instead of error-prone IP addresses when using the Port Forwarding service through the SSL User Portal.

To configure port forwarding, following are required:

- Local Server IP address: The IP address of the local server which is hosting the application.
- TCP port: The TCP port of the application

Once the new application is defined it is displayed in a list of configured applications for port forwarding.

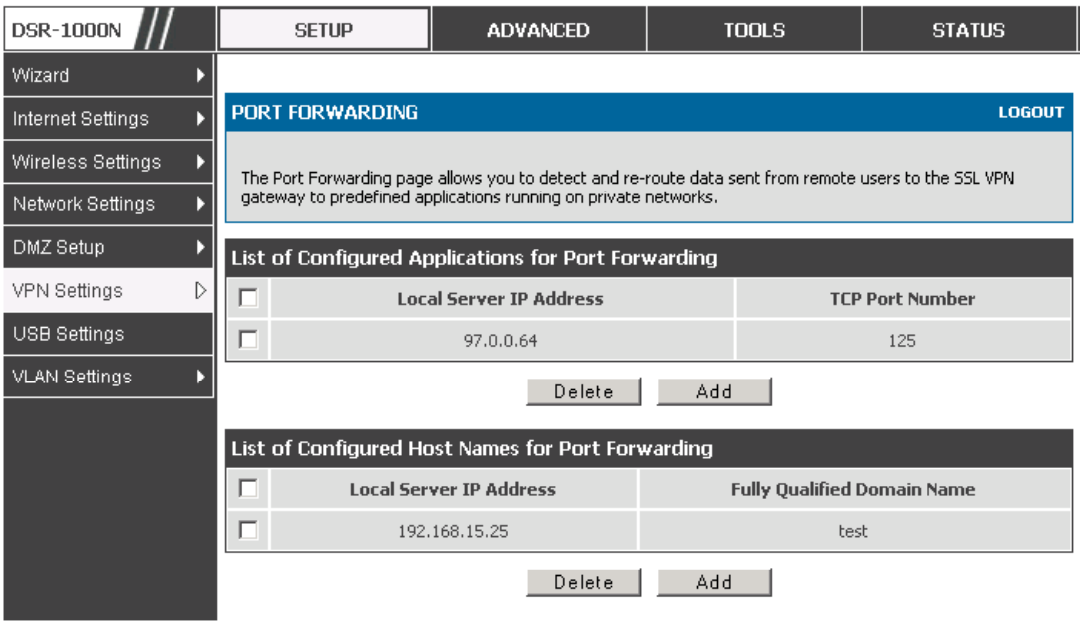
allow users to access the private network servers by using a hostname instead of an IP address, the FQDN corresponding to the IP address is defined in the port forwarding host configuration section.

- Local server IP address: The IP address of the local server hosting the application. The application should be configured in advance.
- Fully qualified domain name: The domain name of the internal server is to be specified

Once the new FQDN is configured, it is displayed in a list of configured hosts for port forwarding.

Defining the hostname is optional as minimum requirement for port forwarding is identifying the TCP application and local server IP address. The local server IP address of the configured hostname must match the IP address of the configured application for port forwarding.

**Figure 67: List of Available Applications for SSL Port Forwarding**




# 7.4 SSL VPN Client Configuration

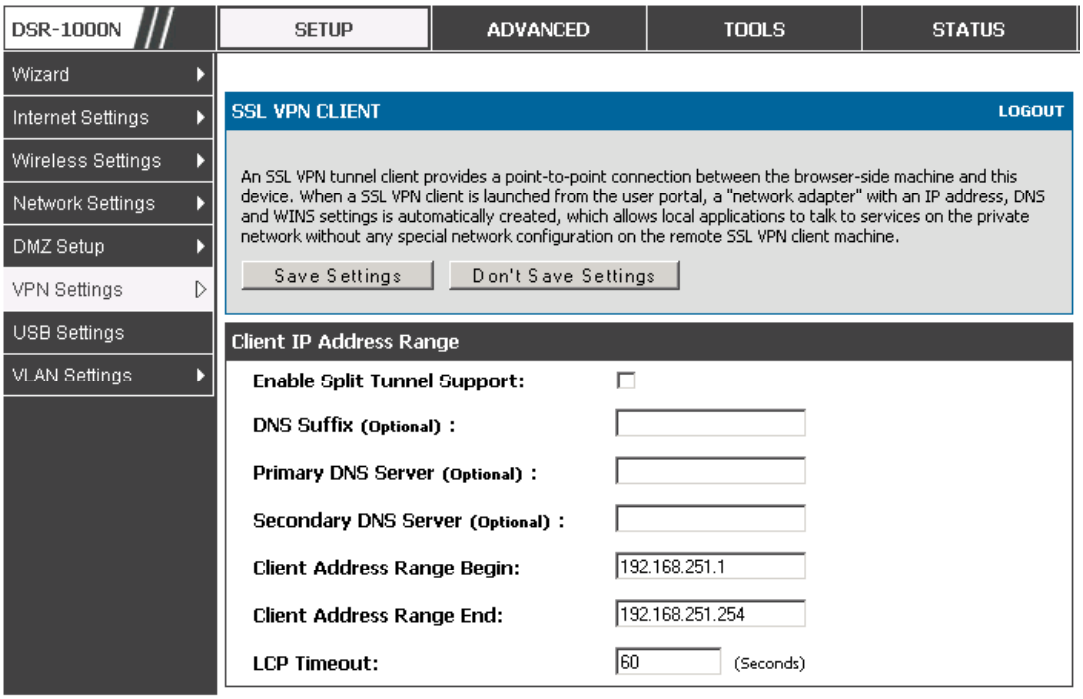
***Setup > VPN Settings > SSL VPN Client > SSL VPN Client***

An SSL VPN tunnel client provides a point-to-point connection between the browser-side machine and this router. When a SSL VPN client is launched from the user portal, a "network adapter" with an IP address from the corporate subnet, DNS and WINS settings is automatically created. This allows local applications to access services on the private network without any special network configuration on the remote SSL VPN client machine.

It is important to ensure that the virtual (PPP) interface address of the VPN tunnel client does not conflict with physical devices on the LAN. The IP address range for the SSL VPN virtual network adapter should be either in a different subnet or non-overlapping range as the corporate LAN.

The IP addresses of the client's network interfaces (Ethernet, Wireless, etc.) cannot be identical to the router's IP address or a server on the corporate LAN that is being accessed through the SSL VPN tunnel.

**Figure 68: SSL VPN client adapter and access configuration**




The router allows full tunnel and split tunnel support. Full tunnel mode just sends all traffic from the client across the VPN tunnel to the router. Split tunnel mode only sends traffic to the private LAN based on pre-specified client routes. These client routes give the SSL client access to specific private networks, thereby allowing access control over specific LAN services.

Client level configuration supports the following:

- Enable Split Tunnel Support: With a split tunnel, only resources which are referenced by client routes can be accessed over the VPN tunnel. With full tunnel support (if the split tunnel option is disabled the DSR acts in full tunnel mode) all addresses on the private network are accessible over the VPN tunnel. Client routes are not required.
- DNS Suffix: The DNS suffix name which will be given to the SSL VPN client. This configuration is optional.
- Primary DNS Server: DNS server IP address to set on the network adaptor created on the client host. This configuration is optional.
- Secondary DNS Server: Secondary DNS server IP address to set on the network adaptor created on the client host. This configuration is optional.
- Client Address Range Begin: Clients who connect to the tunnel get a DHCP served IP address assigned to the network adaptor from the range of addresses beginning with this IP address

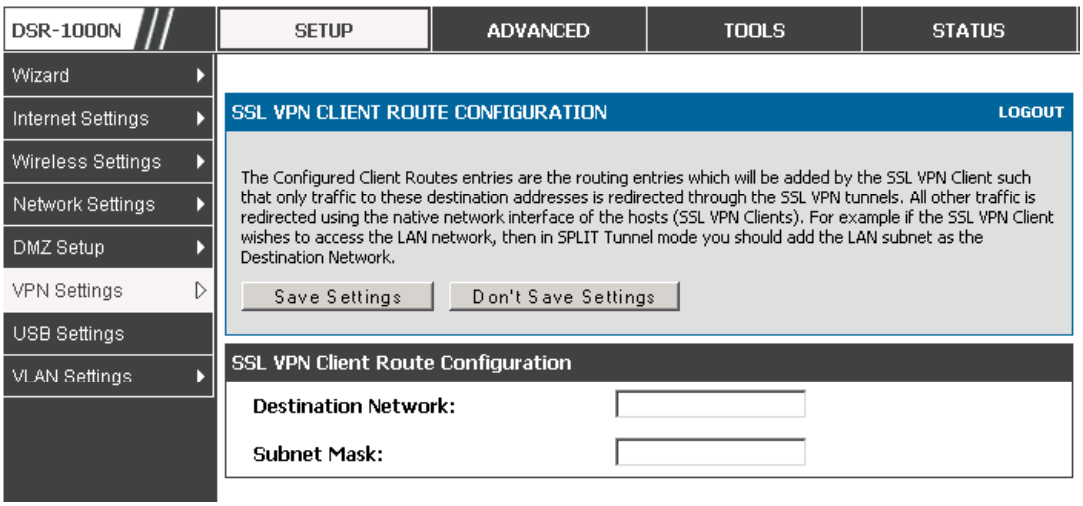
  Client Address Range End: The ending IP address of the DHCP range of addresses served to the client network adaptor.

### *Setup > VPN Settings > SSL VPN Client > Configured Client Routes*

If the SSL VPN client is assigned an IP address in a different subnet than the corporate network, a client route must be added to allow access to the private LAN through the VPN tunnel. As well a static route on the private LAN's firewall (typically this router) is needed to forward private traffic through the VPN Firewall to the remote SSL VPN client. When split tunnel mode is enabled, the user is required to to configure routes for VPN tunnel clients:

- Destination network: The network address of the LAN or the subnet information of the destination network from the VPN tunnel clients' perspective is set here.
- Subnet mask: The subnet information of the destination network is set here.

**Figure 69: Configured client routes only apply in split tunnel mode**

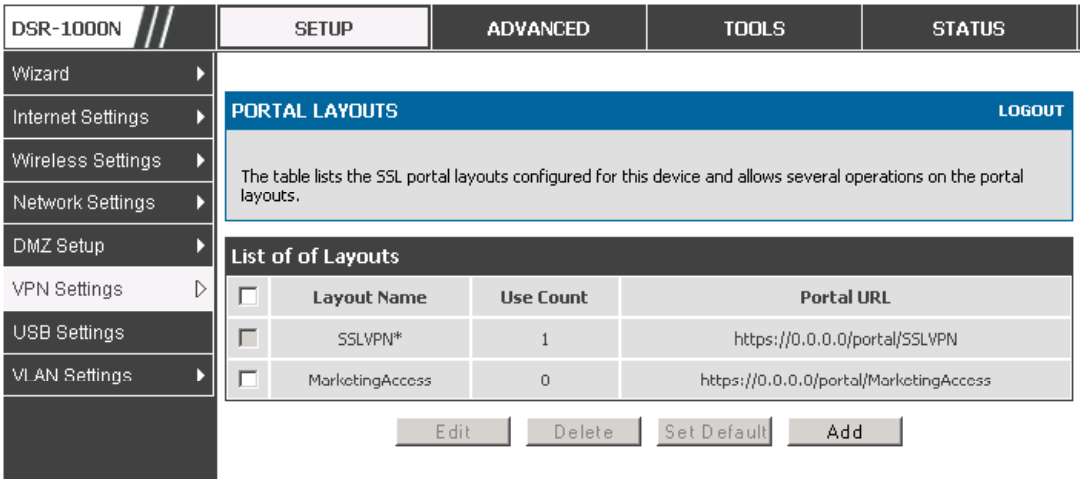



# 7.5 User Portal

### *Setup > VPN Settings > SSL VPN Client > SSL VPN Client Portal*

When remote users want to access the private network through an SSL tunnel (either using the Port Forwarding or VPN tunnel service), they login through a user portal. This portal provides the authentication fields to provide the appropriate access levels and privileges as determined by the router administrator. The domain where the user account is stored must be specified, and the domain determines the authentication method and portal layout screen presented to the remote user.

**Figure 70: List of configured SSL VPN portals. The configured portal can then be associated with an authentication domain**




## 7.5.1 Creating Portal Layouts

***Setup > VPN Settings > SSL VPN Server > Portal Layouts***

The router allows you to create a custom page for remote SSL VPN users that is presented upon authentication. There are various fields in the portal that are customizable for the domain, and this allows the router administrator to communicate details such as login instructions, available services, and other usage details in the portal visible to remote users. During domain setup, configured portal layouts are available to select for all users authenticated by the domain.

The default portal LAN IP address is https://192.168.10.1/scgi-bin/userPortal/portal. This is the same page that opens when the "User Portal" link is clicked on the SSL VPN menu of the router GUI.

The router administrator creates and edits portal layouts from the configuration pages in the SSL VPN menu. The portal name, title, banner name, and banner contents are all customizable to the intended users for this portal. The portal name is appended to the SSL VPN portal URL. As well, the users assigned to this portal (through their authentication domain) can be presented with one or more of the router's supported SSL services such as the VPN Tunnel page or Port Forwarding page.

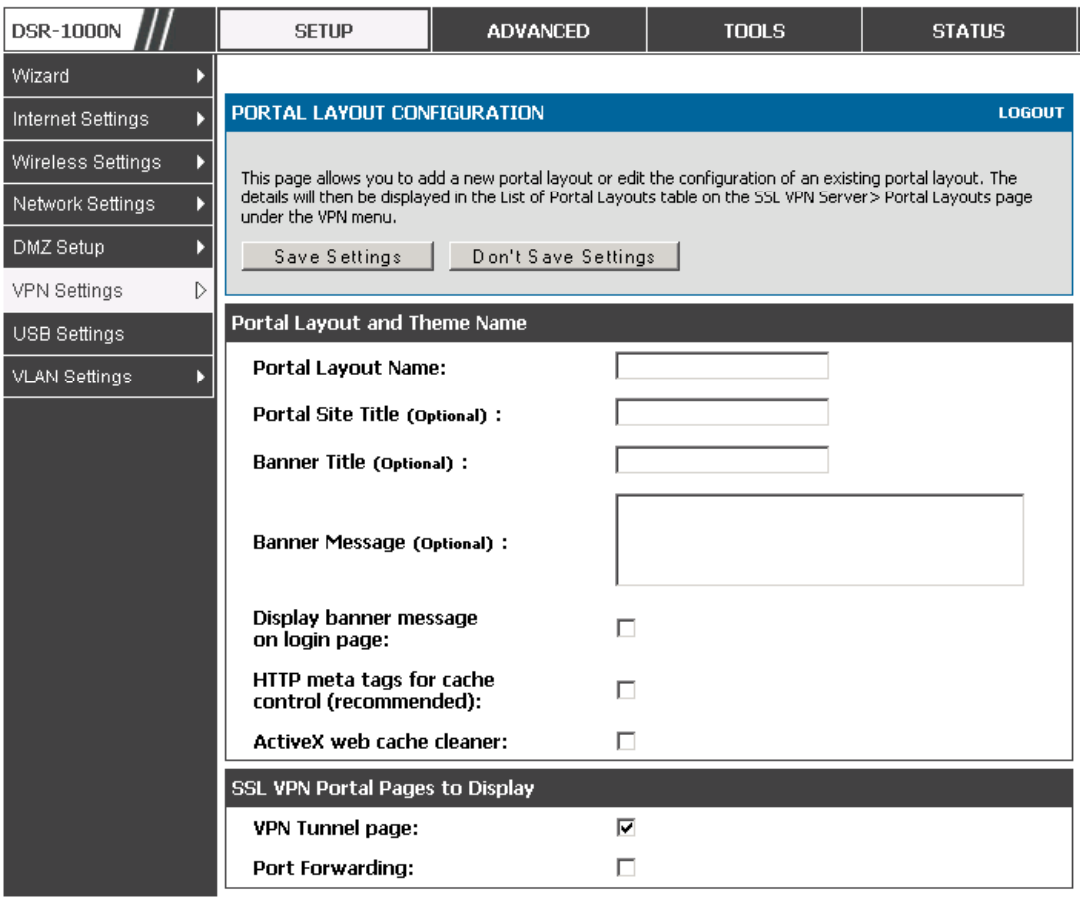
To configure a portal layout and theme, following information is needed:

- Portal layout name: A descriptive name for the custom portal that is being configured. It is used as part of the SSL portal URL.
- Portal site title: The portal web browser window title that appears when the client accesses this portal. This field is optional.
- Banner title: The banner title that is displayed to SSL VPN clients prior to login. This field is optional.

- Banner message: The banner message that is displayed to SSL VPN clients prior to login. This field is optional.
- Display banner message on the login page: The user has the option to either display or hide the banner message in the login page.
- HTTP meta tags for cache control: This security feature prevents expired web pages and data from being stored in the client's web browser cache. It is recommended that the user selects this option.
- ActiveX web cache cleaner: An ActiveX cache control web cleaner can be pushed from the gateway to the client browser whenever users login to this SSL VPN portal.
- SSL VPN portal page to display: The User can either enable VPN tunnel page or Port Forwarding, or both depending on the SSL services to display on this portal.

Once the portal settings are configured, the newly configured portal is added to the list of portal layouts.

**Figure 71: SSL VPN Portal configuration**



# Chapter 8. Advanced Configuration Tools

## 8.1 USB Device Setup

***Setup > USB Settings***

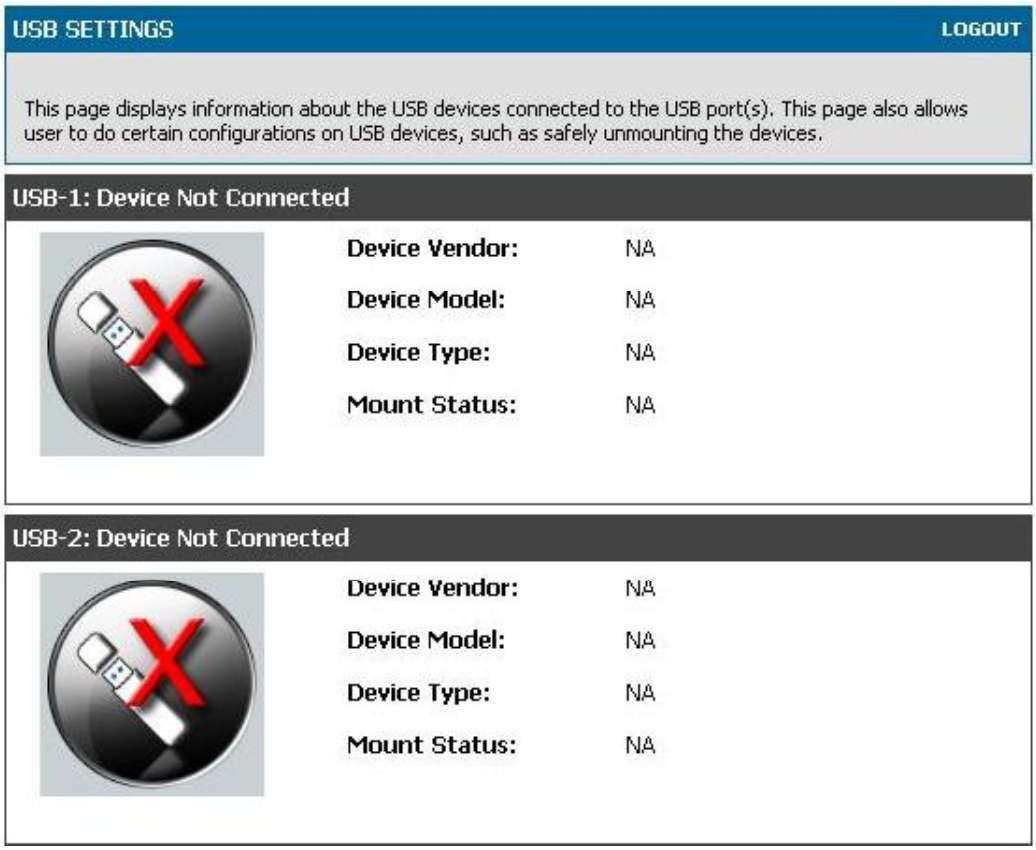
The DSR Unified Services Router has a USB interface for printer access, file sharing and on the DSR-1000 / DSR-1000N models 3G modem support. There is no configuration on the GUI to enable USB device support. Upon inserting your USB storage device, printer cable or 3G modem the DSR router will automatically detect the type of connected peripheral.

- USB Mass Storage: also refered to as a “share port”, files on a USB disk connected to the DSR can be accessed by LAN users as a network drive.
- USB Printer: The DSR can provide the LAN with access to printers connected through the USB. The printer driver will have to be installed on the LAN host and traffic will be routed through the DSR between the LAN and printer.
- USB 3G modem: A 3G modem dongle can be plugged in and used as a secondary WAN. Load balancing, auto-failover, or primary WAN access can be configured through the 3G interface.

To configure printer on a Windows machine, follow below given steps:

- Click 'Start' on the desktop.
- Select ‘Printers and faxes’ option.
- Right click and select 'add printer' or click on 'Add printer' present at the left menu.
- Select the 'Network Printer' radio button and click next (select "device isn't listed in case of Windows7").
- Select the 'Connect to printer using URL' radio button ('Select a shared printer by name'in case of Windows 7) and give the following URL http://<Router's LAN IP address>:631/printers/<Model Name> (Model Name can be found in the USB status page of router's GUI).
- Click 'next' and select the appropriate driver from the displayed list.
- Click on 'next' and 'finish' to complete adding the printer.

**Figure 72: USB Device Detection**




# 8.2 Authentication Certificates

***Advanced > Certificates***

This gateway uses digital certificates for IPsec VPN authentication as well as SSL validation (for HTTPS and SSL VPN authentication). You can obtain a digital certificate from a well known Certificate Authority (CA) such as VeriSign, or generate and sign your own certificate using functionality available on this gateway. The gateway comes with a self-signed certificate, and this can be replaced by one signed by a CA as per your networking requirements. A CA certificate provides strong assurance of the server's identity and is a requirement for most corporate network VPN solutions.

The certificates menu allows you to view a list of certificates (both from a CA and self-signed) currently loaded on the gateway. The following certificate data is displayed in the list of Trusted (CA) certificates:

CA Identity (Subject Name): The certificate is issued to this person or organization

Issuer Name: This is the CA name that issued this certificate

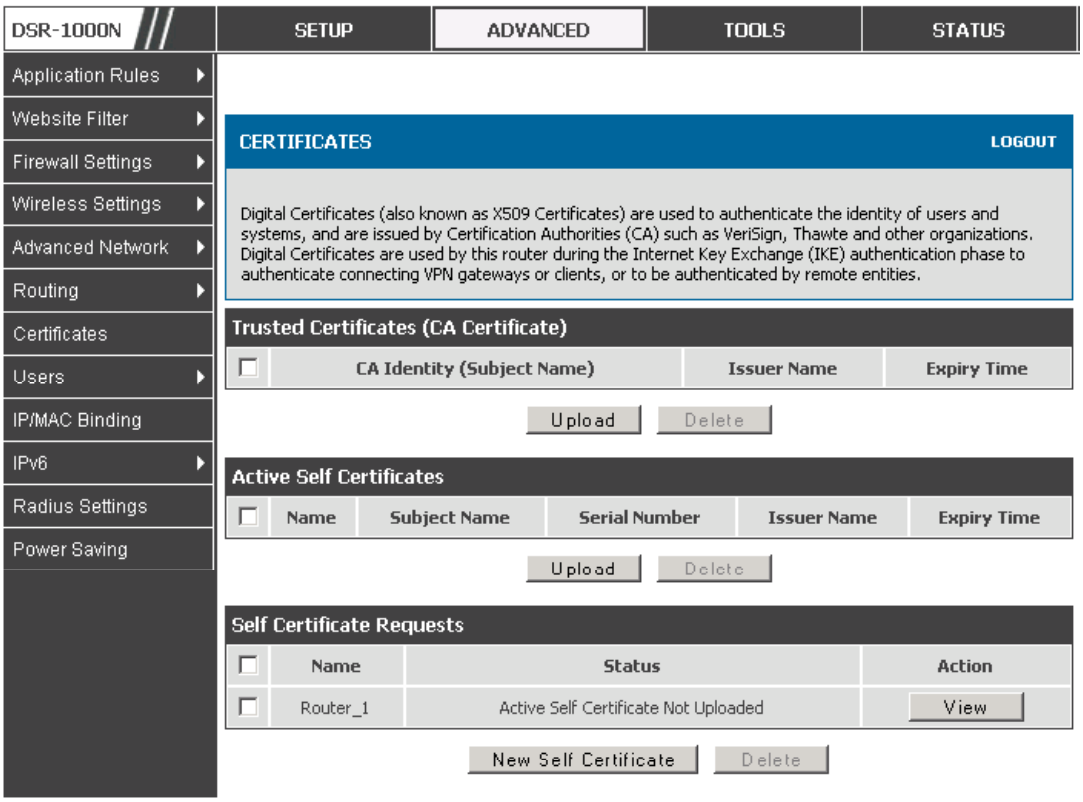
Expiry Time: The date after which this Trusted certificate becomes invalid

A self certificate is a certificate issued by a CA identifying your device (or self-signed if you don't want the identity protection of a CA). The Active Self Certificate table lists the self certificates currently loaded on the gateway. The following information is displayed for each uploaded self certificate:

- Name: The name you use to identify this certificate, it is not displayed to IPsec VPN peers or SSL users.
- Subject Name: This is the name that will be displayed as the owner of this certificate. This should be your official registered or company name, as IPsec or SSL VPN peers are shown this field.
- Serial Number: The serial number is maintained by the CA and used to identify this signed certificate.
- Issuer Name: This is the CA name that issued (signed) this certificate
- Expiry Time: The date after which this signed certificate becomes invalid – you should renew the certificate before it expires.

To request a self certificate to be signed by a CA, you can generate a Certificate Signing Request from the gateway by entering identification parameters and passing it along to the CA for signing. Once signed, the CA's Trusted Certificate and signed certificate from the CA are uploaded to activate the self-certificate validating the identity of this gateway. The self certificate is then used in IPsec and SSL connections with peers to validate the gateway's authenticity.

**Figure 73: Certificate summary for IPsec and HTTPS management**

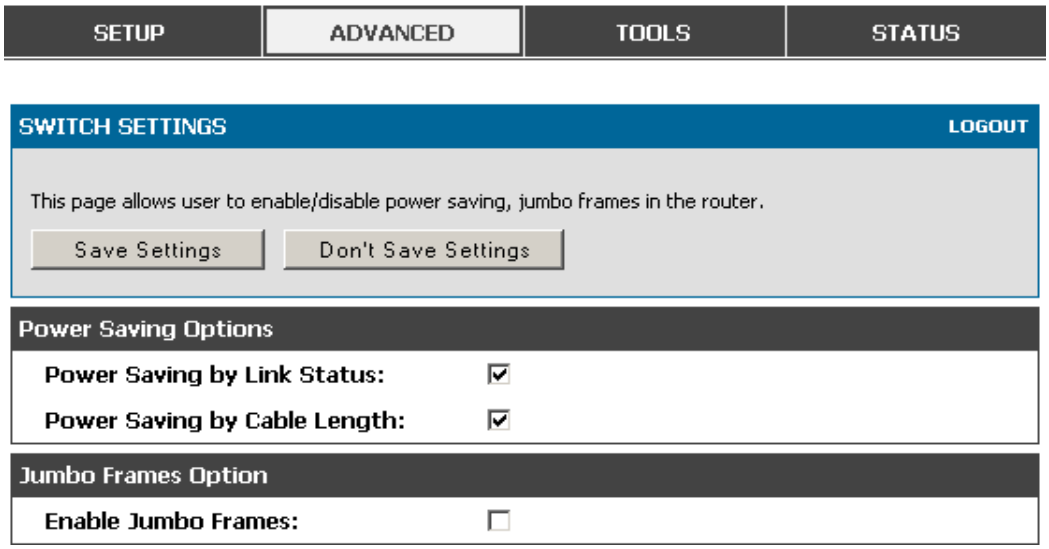



# 8.3 Advanced Switch Configuration

The DSR allows you to adjust the power consumption of the hardware based on your actual usage. The two "green" options available for your LAN switch are Power Saving by Link Status and Length Detection State. With "Power Saving by Link Status" option enabled, the total power consumption by the LAN switch is dependent function of on the number of connected ports. The overall current draw when a single port is connected is less than when all the ports are connected. With "Length Detection State" option enabled, the overall current supplied to a LAN port is reduced when a smaller cable length is connected on a LAN port.

Jumbo Frames support can be configured as an advanced switch configuration. Jumbo frames are Ethernet frames with more than 1500 bytes of payload. When this option is enabled, the LAN devices can exchange information at Jumbo frames rate.

**Figure 74: Advanced Switch Settings**



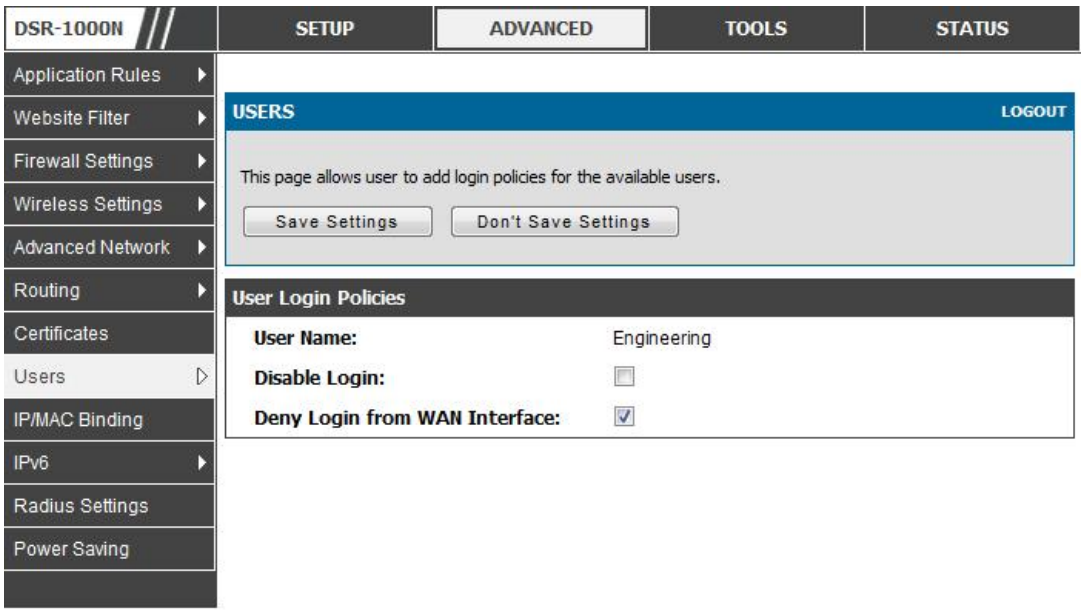
# Chapter 9. Administration & Management

## 9.1 Configuration Access Control

The primary means to configure this gateway via the browser-independent GUI. The GUI can be accessed from LAN node by using the gateway's LAN IP address and HTTP, or from the WAN by using the gateway's WAN IP address and HTTPS (HTTP over SSL).

Administrator and Guest users are permitted to login to the router's management interface. The user type is set in the ***Advanced > Users > Users*** page. The Admin or Guest user can be configured to access the router GUI from the LAN or the Internet (WAN) by enabling the corresponding Login Policy.

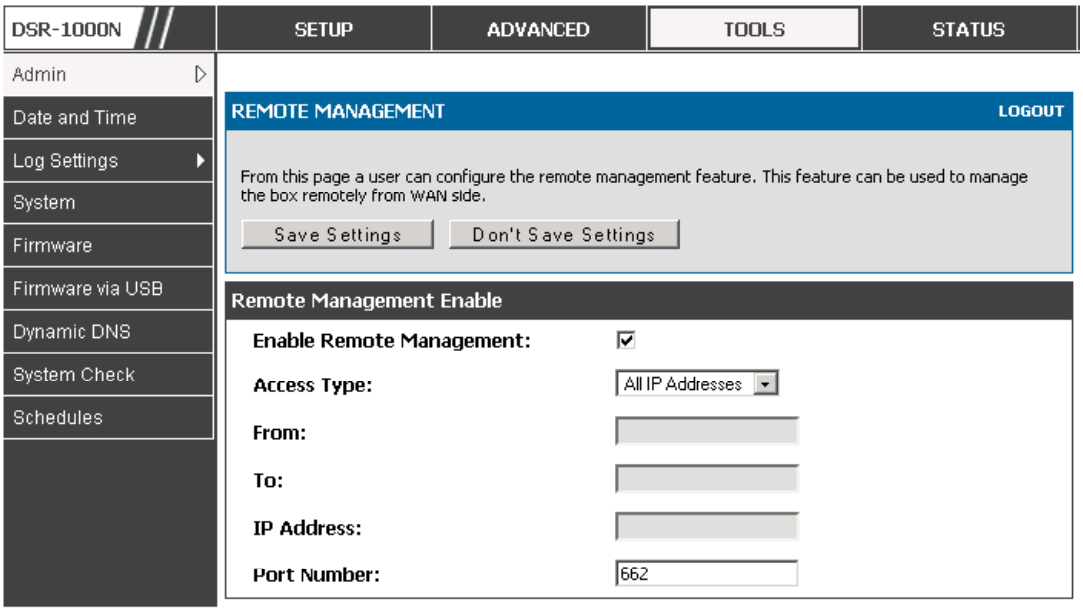
**Figure 75: User Login policy configuration**




### 9.1.1 Remote Management

Both HTTPS and telnet access can be restricted to a subset of IP addresses. The router administrator can define a known PC, single IP address or range of IP addresses that are allowed to access the GUI with HTTPS. The opened port for SSL traffic can be changed from the default of 443 at the same time as defining the allowed remote management IP address range.

**Figure 76: Remote Management from the WAN**




## 9.1.2 CLI Access

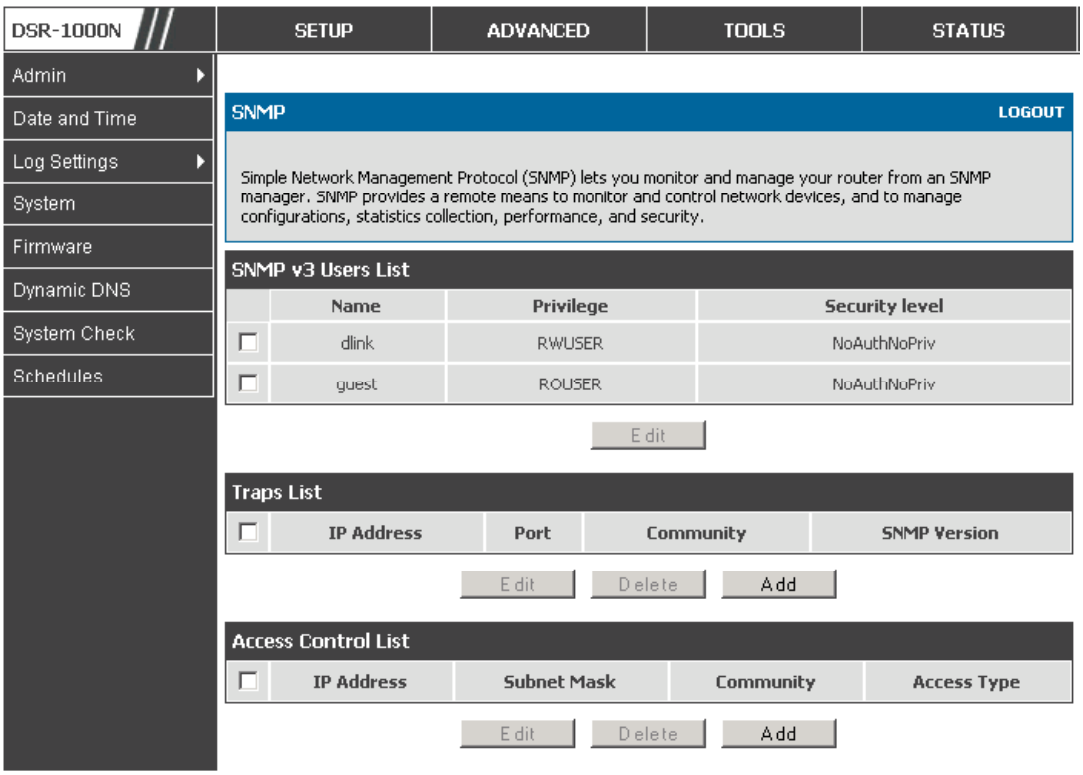
In addition to the web-based GUI, the gateway supports SSH and Telnet management for command-line interaction. The CLI login credentials are shared with the GUI for administrator users. To access the CLI, type "cli" in the SSH or console prompt and login with administrator user credentials.

# 9.2 SNMP Configuration

***Tools > Admin > SNMP***

SNMP is an additional management tool that is useful when multiple routers in a network are being managed by a central Master system. When an external SNMP manager is provided with this router's Management Information Base (MIB) file, the manager can update the router's hierarchal variables to view or update configuration parameters. The router as a managed device has an SNMP agent that allows the MIB configuration variables to be accessed by the Master (the SNMP manager). The Access Control List on the router identifies managers in the network that have read-only or read-write SNMP credentials. The Traps List outlines the port over which notifications from this router are provided to the SNMP community (managers) and also the SNMP version (v1, v2c, v3) for the trap.

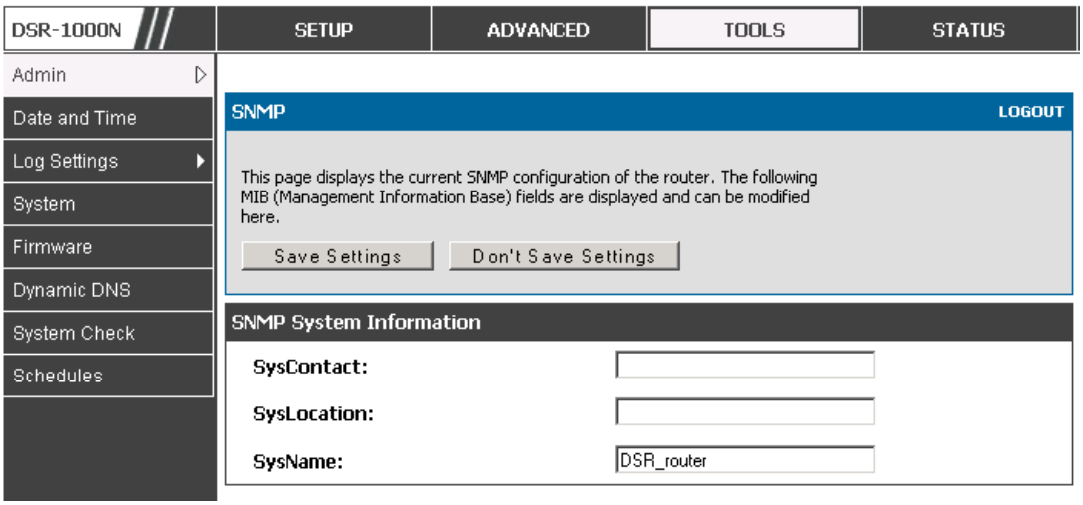
**Figure 77: SNMP Users, Traps, and Access Control**




### *Tools > Admin > SNMP System Info*

The router is identified by an SNMP manager via the System Information. The identifier settings The SysName set here is also used to identify the router for SysLog logging.

**Figure 78: SNMP system information for this router**




# 9.3 Configuring Time Zone and NTP

***Tools > Date and Time***

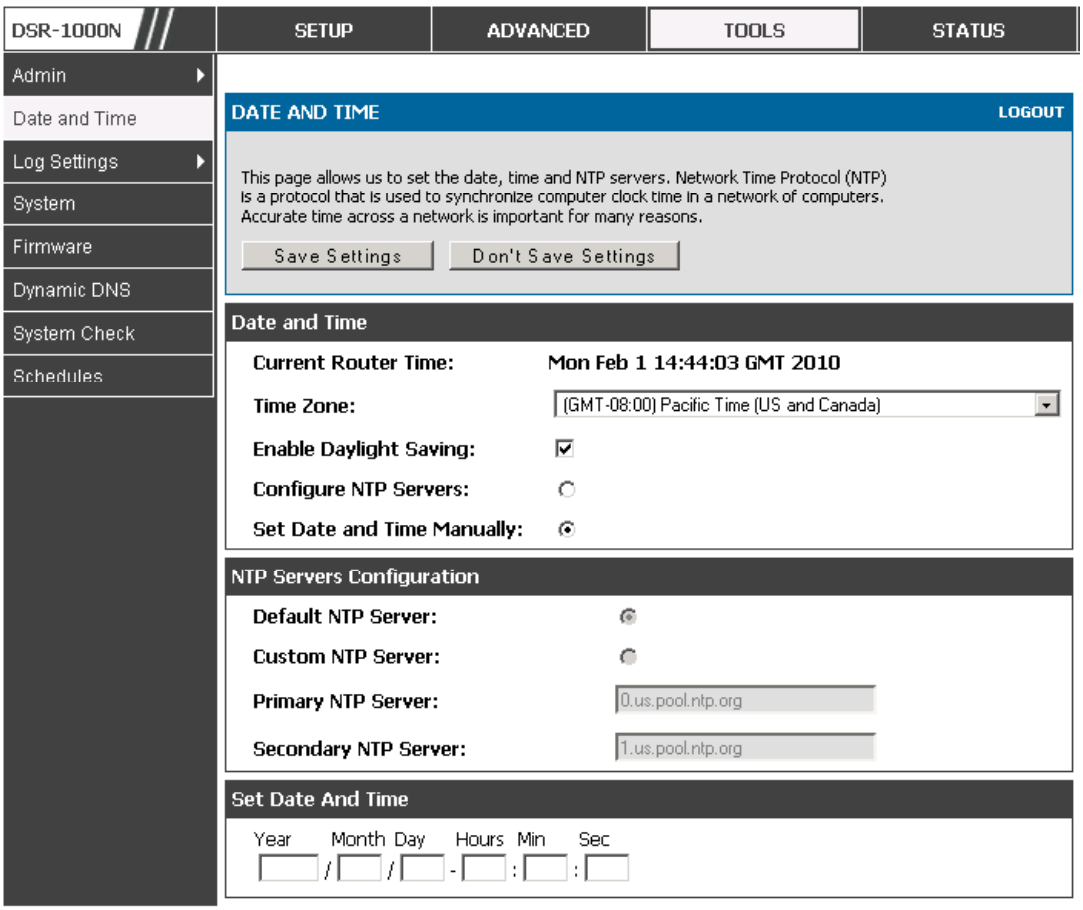
You can configure your time zone, whether or not to adjust for Daylight Savings Time, and with which Network Time Protocol (NTP) server to synchronize the date and time. You can choose to set Date and Time manually, which will store the information on the router's real time clock (RTC). If the router has access to the internet, the most accurate mechanism to set the router time is to enable NTP server communication.

Accurate date and time on the router is critical for firewall schedules, Wi-Fi power saving support to disable APs at certain times of the day, and accurate logging.

Please follow the steps below to configure the NTP server:

1. Select the router's time zone, relative to Greenwich Mean Time (GMT).
2. If supported for your region, click to Enable Daylight Savings.
3. Determine whether to use default or custom Network Time Protocol (NTP) servers. If custom, enter the server addresses or FQDN.

**Figure 79: Date, Time, and NTP server setup**




# 9.4 Log Configuration

This router allows you to capture log messages for traffic through the firewall, VPN, and over the wireless AP. As an administrator you can monitor the type of traffic that goes through the router and also be notified of potential attacks or errors when they are detected by the router. The following sections describe the log configuration settings and the ways you can access these logs.

## 9.4.1 Defining What to Log

***Tools > Log Settings > Logs Facility***

The Logs Facility page allows you to determine the granularity of logs to receive from the router. There are three core components of the router, referred to as Facilities:

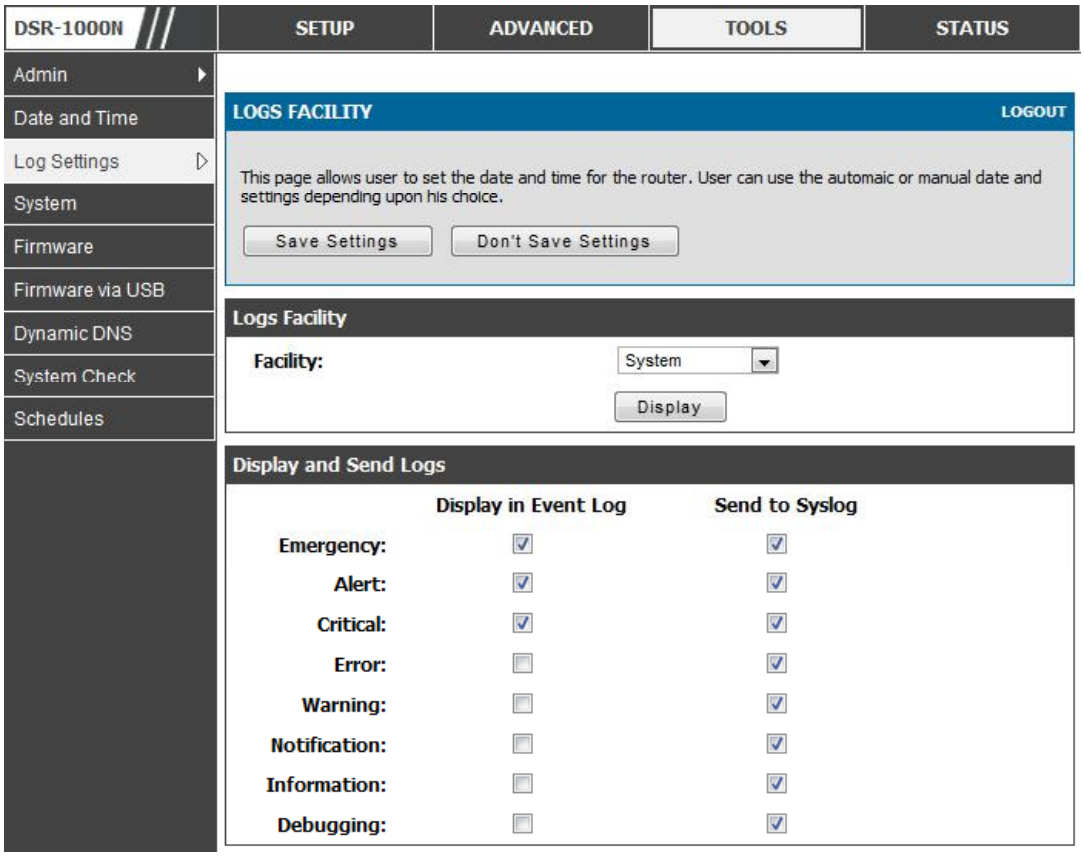
- Kernel: This refers to the Linux kernel. Log messages that correspond to this facility would correspond to traffic through the firewall or network stack.

- System: This refers to application and management level features available on this router, including SSL VPN and administrator changes for managing the unit.
- Wireless: This facility corresponds to the 802.11 driver used for providing AP functionality to your network.
- Local1-UTM: This facitlity corresponds to IPS (Intrusion Prevension System) which helps in detecting malicious intrusion attempts from the WAN.

For each facility, the following events (in order of severity) can be logged: Emergency, Alert, Critical, Error, Warning, Notification, Information, Debugging. When a particular severity level is selected, all events with severity equal to and greater than the chosen severity are captured. For example if you have configured CRITICAL level logging for the Wireless facility, then 802.11 logs with severities CRITICAL, ALERT, and EMERGENCY are logged. The severity levels available for logging are:

- EMERGENCY: system is unusable
- ALERT: action must be taken immediately
- CRITICAL: critical conditions
- ERROR: error conditions
- WARNING: warning conditions
- NOTIFICATION: normal but significant condition
- INFORMATION: informational
- DEBUGGING: debug-level messages

**Figure 80: Facility settings for Logging**




The display for logging can be customized based on where the logs are sent, either the Event Log viewer in the GUI (the Event Log viewer is in the ***Status > Logs*** page) or a remote Syslog server for later review. E-mail logs, discussed in a subsequent section, follow the same configuration as logs configured for a Syslog server.

### *Tools > Log Settings > Logs Configuration*

This page allows you to determine the type of traffic through the router that is logged for display in Syslog, E-mailed logs, or the Event Viewer. Denial of service attacks, general attack information, login attempts, dropped packets, and similar events can be captured for review by the IT administrator.

Traffic through each network segment (LAN, WAN, DMZ) can be tracked based on whether the packet was accepted or dropped by the firewall.

Accepted Packets are those that were successfully transferred through the corresponding network segment (i.e. LAN to WAN). This option is particularly useful when the Default Outbound Policy is "Block Always" so the IT admin can monitor traffic that is passed through the firewall.

- Example: If Accept Packets from LAN to WAN is enabled and there is a firewall rule to allow SSH traffic from LAN, then whenever a LAN machine tries to make an SSH connection, those packets will be accepted and a message will be logged. (Assuming the log option is set to Allow for the SSH firewall rule.)

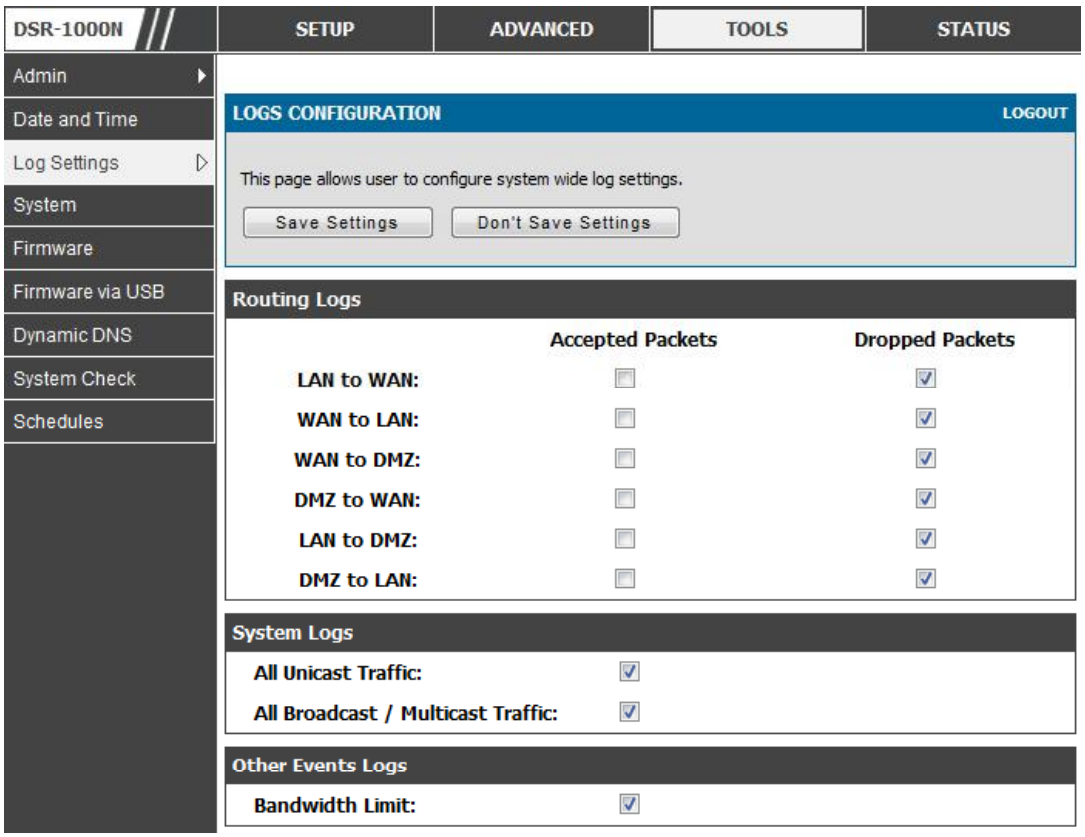
Dropped Packets are packets that were intentionally blocked from being transferred through the corresponding network segment. This option is useful when the Default Outbound Policy is "Allow Always".

- Example: If Drop Packets from LAN to WAN is enabled and there is a firewall rule to block ssh traffic from LAN, then whenever a LAN machine tries to make an ssh connection, those packets will be dropped and a message will be logged. (Make sure the log option is set to allow for this firewall rule.)

Enabling accepted packet logging through the firewall may generate a significant volume of log messages depending on the typical network traffic. This is recommended for debugging purposes only.

In addition to network segment logging, unicast and multicast traffic can be logged. Unicast packets have a single destination on the network, whereas broadcast (or multicast) packets are sent to all possible destinations simultaneously. One other useful log control is to log packets that are dropped due to configured bandwidth profiles over a particular interface. This data will indicate to the admin whether the bandwidth profile has to be modified to account for the desired internet traffic of LAN users.

**Figure 81: Log configuration options for traffic through router**




## 9.4.2 Sending Logs to E-mail or Syslog

***Tools > Log Settings > Remote Logging***

Once you have configured the type of logs that you want the router to collect, they can be sent to either a Syslog server or an E-Mail address. For remote logging a key configuration field is the Remote Log Identifier. Every logged message will contain the configured prefix of the Remote Log Identifier, so that syslog servers or email addresses that receive logs from more than one router can sort for the relevant device's logs.

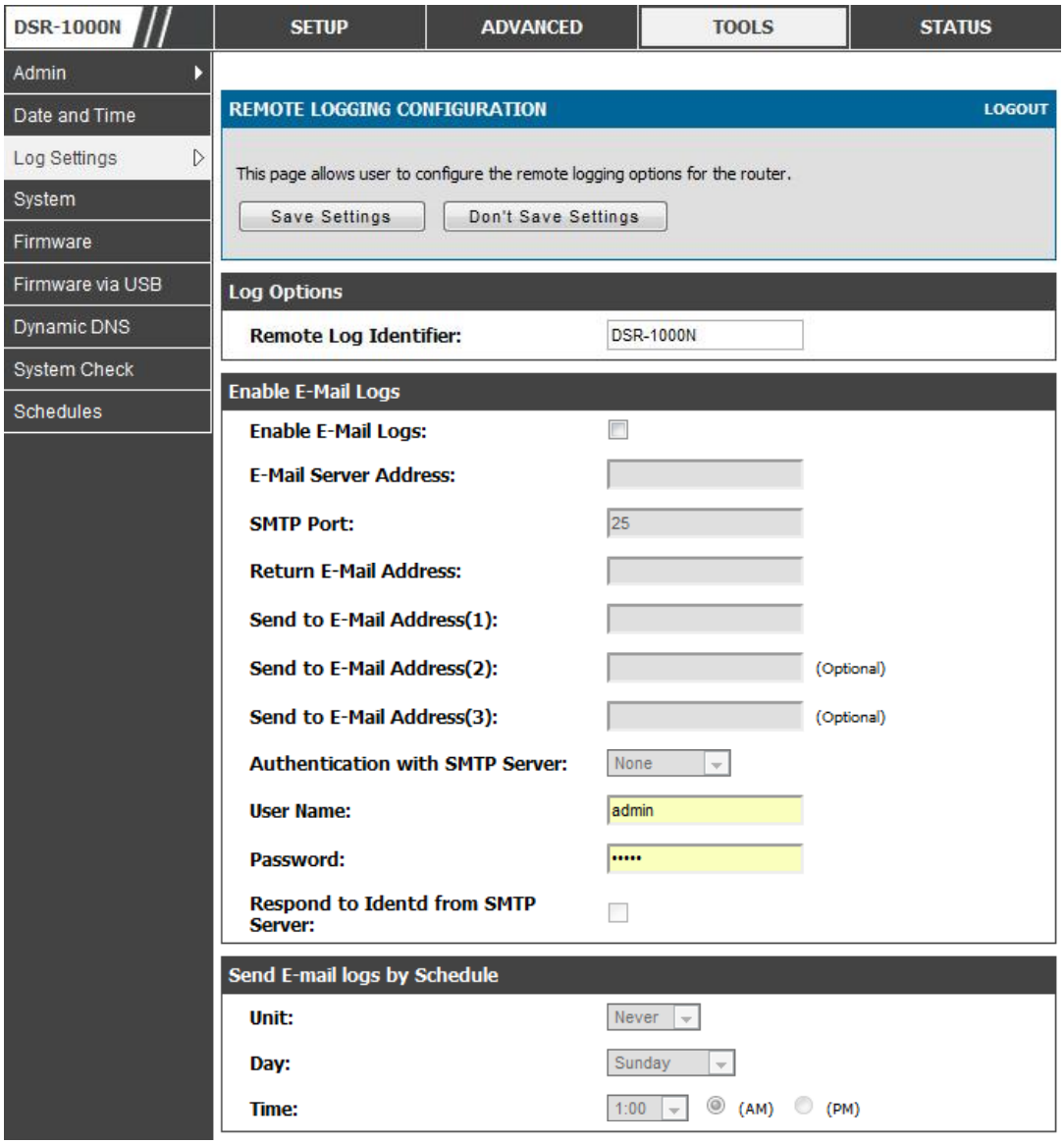
Once you enable the option to e-mail logs, enter the e-mail server's address (IP address or FQDN) of the SMTP server. The router will connect to this server when sending e-mails out to the configured addresses. The SMTP port and return e-mail addresses are required fields to allow the router to package the logs and send a valid e-mail that is accepted by one of the configured "send-to" addresses. Up to three e-mail addresses can be configured as log recipients.

In order to establish a connection with the configured SMTP port and server, define the server's authentication requirements. The router supports Login Plain (no encryption) or CRAM-MD5 (encrypted) for the username and password data to be sent to the SMTP server. Authentication can be disabled if the server does not have

this requirement. In some cases the SMTP server may send out IDENT requests, and this router can have this response option enabled as needed.

Once the e-mail server and recipient details are defined you can determine when the router should send out logs. E-mail logs can be sent out based on a defined schedule by first choosing the unit (i.e. the frequency) of sending logs: Hourly, Daily, or Weekly. Selecting Never will disable log e-mails but will preserve the e-mail server settings.

**Figure 82: E-mail configuration as a Remote Logging option**

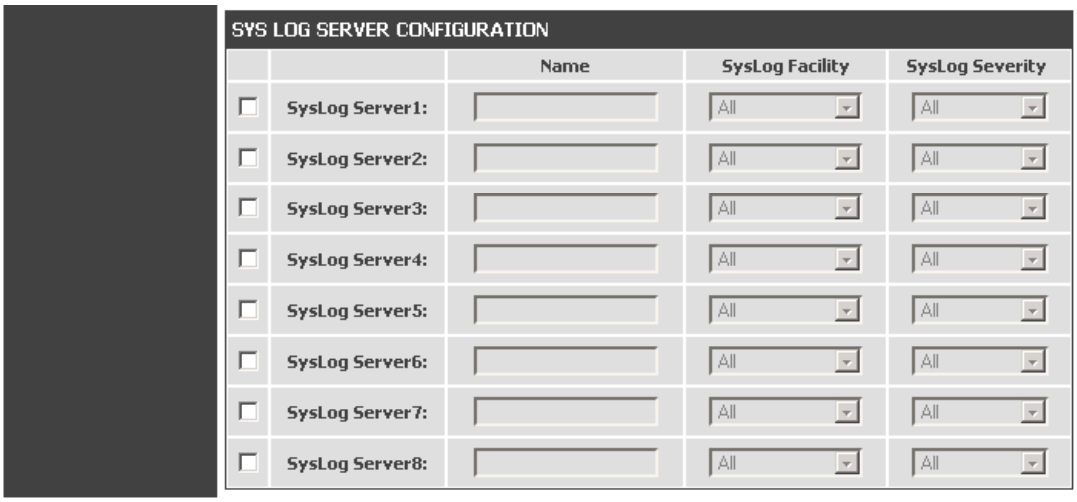



An external Syslog server is often used by network administrator to collect and store logs from the router. This remote device typically has less memory constraints than

the local Event Viewer on the router's GUI, and thus can collect a considerable number of logs over a sustained period. This is typically very useful for debugging network issues or to monitor router traffic over a long duration.

This router supports up to 8 concurrent Syslog servers. Each can be configured to receive different log facility messages of varying severity. To enable a Syslog server select the checkbox next to an empty Syslog server field and assign the IP address or FQDN to the Name field. The selected facility and severity level messages will be sent to the configured (and enabled) Syslog server once you save this configuration page's settings.

**Figure 83: Syslog server configuration for Remote Logging (continued)**




## 9.4.3 Event Log Viewer in GUI

***Status > Logs > View All Logs***

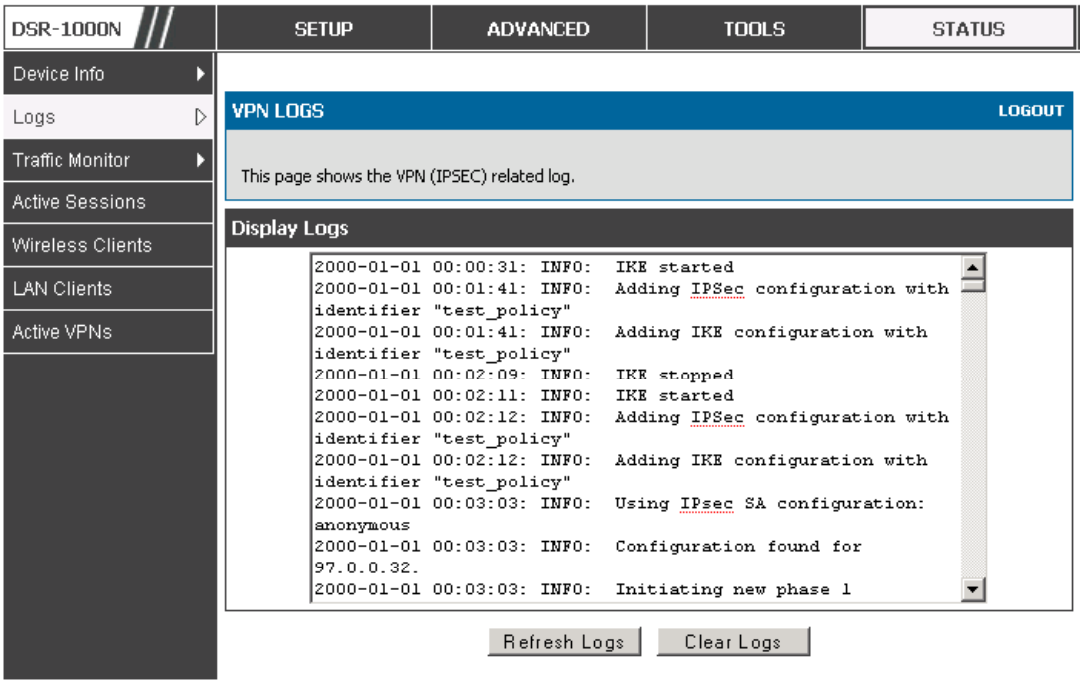
The router GUI lets you observe configured log messages from the Status menu. Whenever traffic through or to the router matches the settings determined in the ***Tools > Log Settings > Logs Facility*** or ***Tools > Log Settings > Logs Configuration*** pages, the corresponding log message will be displayed in this window with a timestamp.

It is very important to have accurate system time (manually set or from a NTP server) in order to understand log messages.

***Status > Logs > VPN Logs***

This page displays IPsec VPN log messages as determined by the configuration settings for facility and severity. This data is useful when evaluating IPsec VPN traffic and tunnel health.

**Figure 84: VPN logs displayed in GUI event viewer**




# 9.5 Backing up and Restoring Configuration Settings

### *Tools > System*

You can back up the router's custom configuration settings to restore them to a different device or the same router after some other changes. During backup, your settings are saved as a file on your host. You can restore the router's saved settings from this file as well. This page will also allow you revert to factory default settings or execute a soft reboot of the router.

> **IMPORTANT!** During a restore operation, do NOT try to go online, turn off the router, shut down the PC, or do anything else to the router until the operation is complete. This will take approximately 1 minute. Once the LEDs are turned off, wait a few more seconds before doing anything with the router.

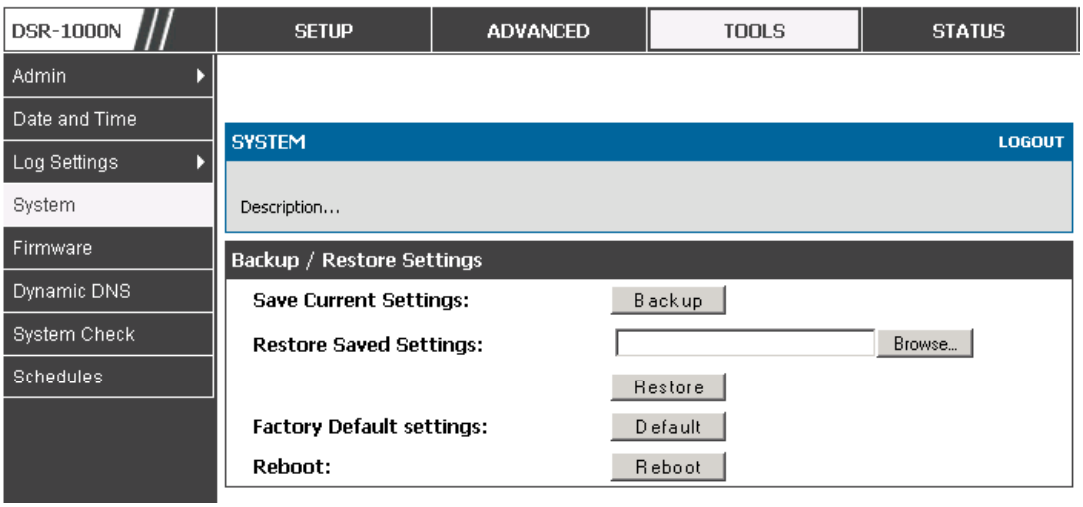
For backing up configuration or restoring a previously saved configuration, please follow the steps below:

1. To save a copy of your current settings, click the Backup button in the Save Current Settings option. The browser initiates an export of the configuration file and prompts to save the file on your host.

2. To restore your saved settings from a backup file, click Browse then locate the file on the host. After clicking Restore, the router begins importing the file's saved configuration settings. After the restore, the router reboots automatically with the restored settings.

3. To erase your current settings and revert to factory default settings, click the Default button. The router will then restore configuration settings to factory defaults and will reboot automatically. (See Appendix B for the factory default parameters for the router).

**Figure 85: Restoring configuration from a saved file will result in the current configuration being overwritten and a reboot**



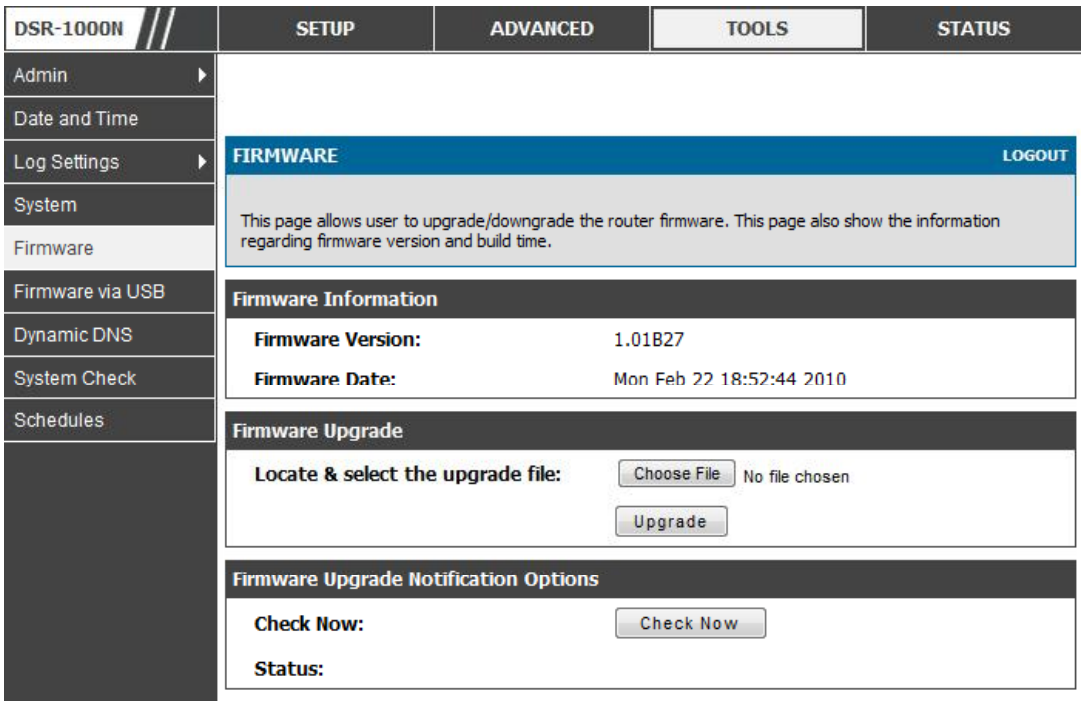

# 9.6 Upgrading Router Firmware

***Tools > Firmware***

You can upgrade to a newer software version from the Administration web page. In the Firmware Upgrade section, to upgrade your firmware, click Browse, locate and select the firmware image on your host, and click Upgrade. After the new firmware image is validated, the new image is written to flash, and the router is automatically rebooted with the new firmware. The Firmware Information and also the ***Status > Device Info > Device Status*** page will reflect the new firmware version.

**IMPORTANT!** During firmware upgrade, do NOT try to go online, turn off the DSR, shut down the PC, or interrupt the process in anyway until the operation is complete. This should take only a minute or so including the reboot process. Interrupting the upgrade process at specific points when the flash is being written to may corrupt the flash memory and render the router unusable without a low-level process of restoring the flash firmware (not through the web GUI).

**Figure 86: Firmware version information and upgrade option**




This router also supports an automated notification to determine if a newer firmware version is available for this router. By clicking the Check Now button in the notification section, the router will check a D-Link server to see if a newer firmware version for this router is available for download and update the Status field below.

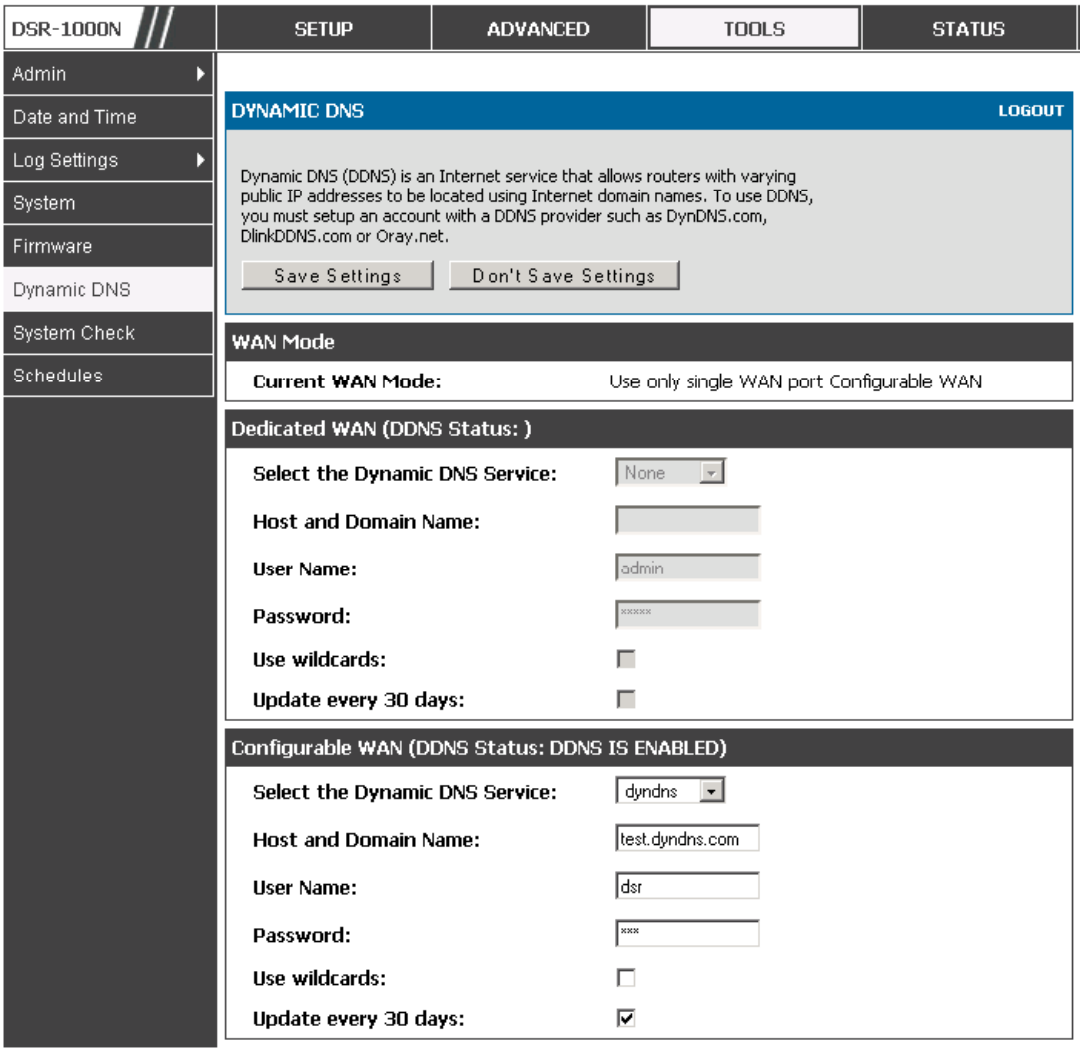
# 9.7 Dynamic DNS Setup

### *Tools > Dynamic DNS*

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org, D-Link DDNS, or Oray.net.

Each configured WAN can have a different DDNS service if required. Once configured, the router will update DDNS services changes in the WAN IP address so that features that are dependent on accessing the router's WAN via FQDN will be directed to the correct IP address. When you set up an account with a DDNS service, the host and domain name, username, password and wildcard support will be provided by the account provider.

**Figure 87: Dynamic DNS configuration**

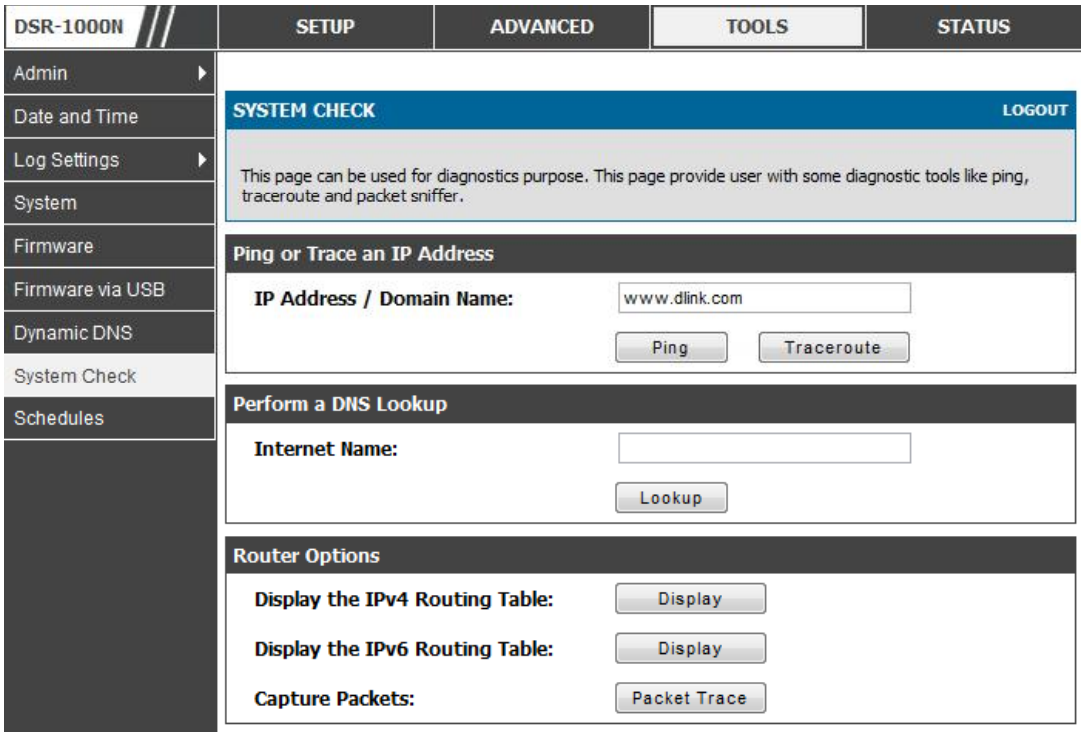



# 9.8 Using Diagnostic Tools

### *Tools > System Check*

The router has built in tools to allow an administrator to evaluate the communication status and overall network health.

**Figure 88: Router diagnostics tools available in the GUI**



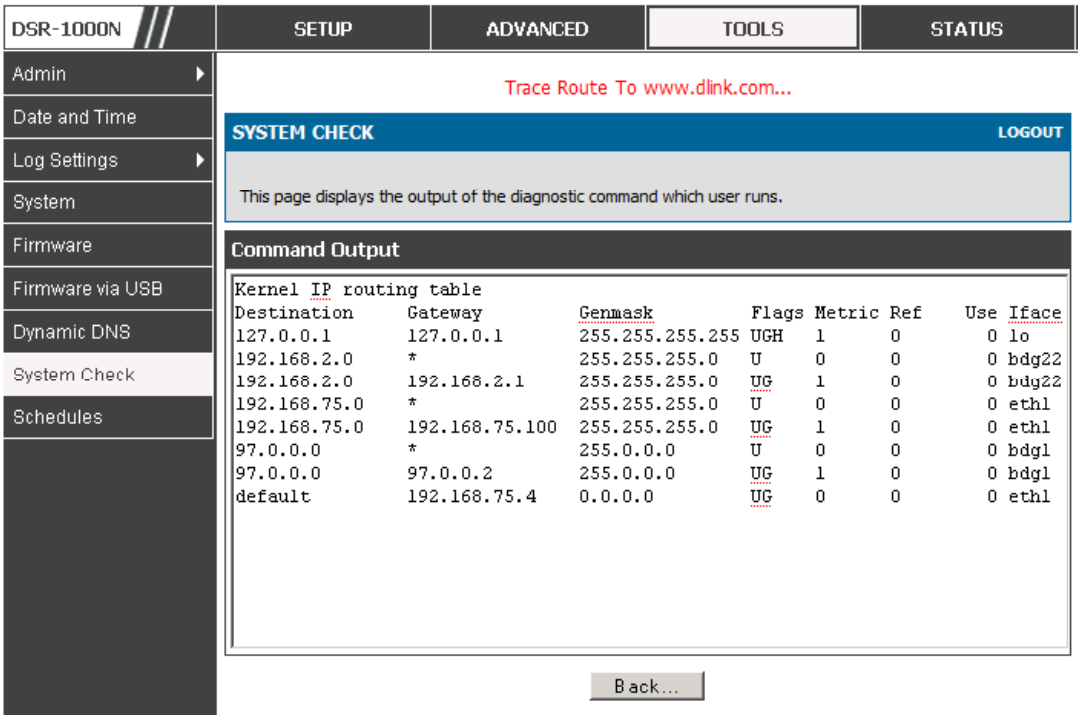

## 9.8.1 Ping

This utility can be used to test connectivity between this router and another device on the network connected to this router. Enter an IP address and click PING. The command output will appear indicating the ICMP echo request status.

## 9.8.2 Trace Route

This utility will display all the routers present between the destination IP address and this router. Up to 30 "hops" (intermediate routers) between this router and the destination will be displayed.

**Figure 89: Sample traceroute output**




## 9.8.3 DNS Lookup

To retrieve the IP address of a Web, FTP, Mail or any other server on the Internet, type the Internet Name in the text box and click Lookup. If the host or domain entry exists, you will see a response with the IP address. A message stating "Unknown Host" indicates that the specified Internet Name does not exist.

This feature assumes there is internet access available on the WAN link(s).

## 9.8.4 Router Options

The static and dynamic routes configured on this router can be shown by clicking Display for the corresponding routing table. Clicking the Packet Trace button will allow the router to capture and display traffic through the DSR between the LAN and WAN interface as well. This information is often very useful in debugging traffic and routing issues.

# Chapter 10. Router Status and Statistics

## 10.1 System Overview

The Status page allows you to get a detailed overview of the system configuration. The settings for the wired and wireless interfaces are displayed in the DSR Status page, and then the resulting hardware resource and router usage details are summarized on the router's Dashboard.

### 10.1.1 Device Status

***Status > Device Info > Device Status***

The DSR Status page gives a summary of the router configuration settings configured in the Setup and Advanced menus. The static hardware serial number and current firmware version are presented in the General section. The WAN and LAN interface information shown on this page are based on the administrator configuration parameters. The radio band and channel settings are presented below along with all configured and active APs that are enabled on this router.

**Figure 90: Device Status display**

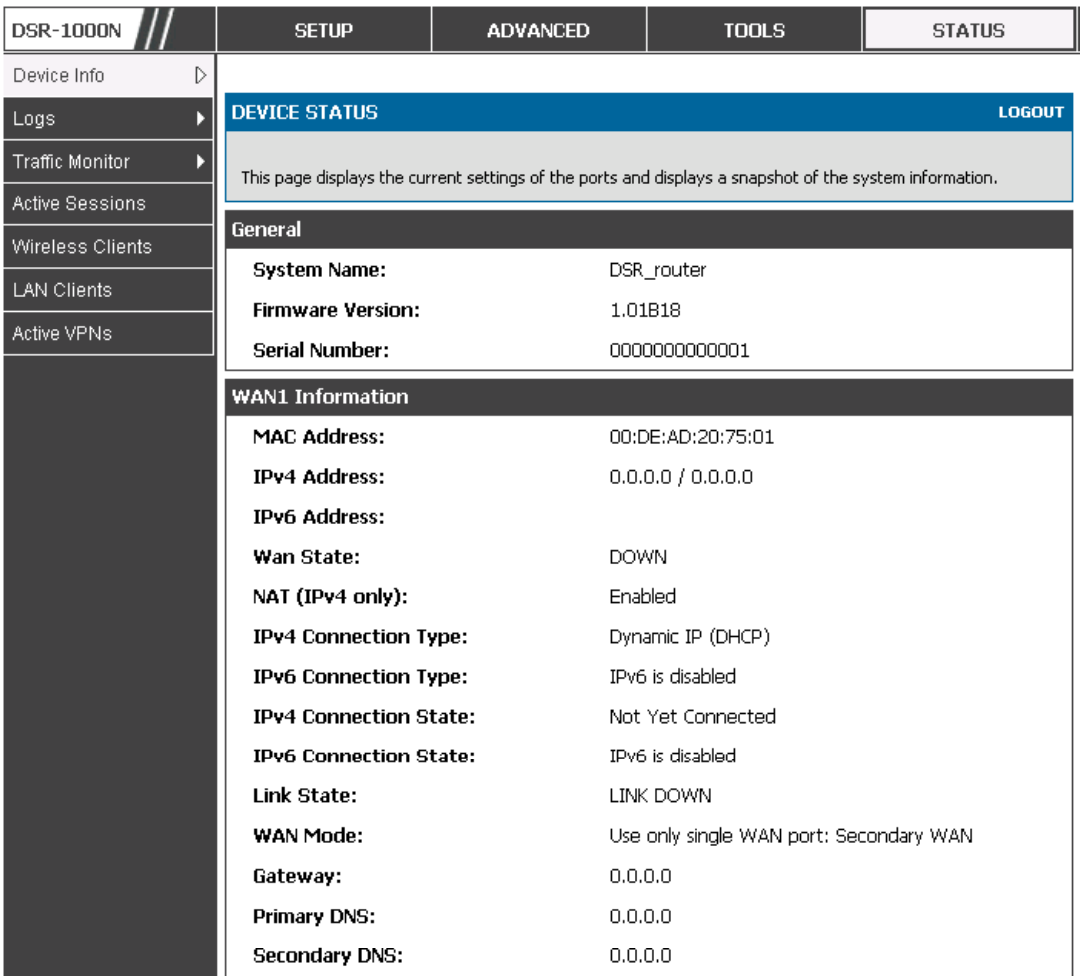
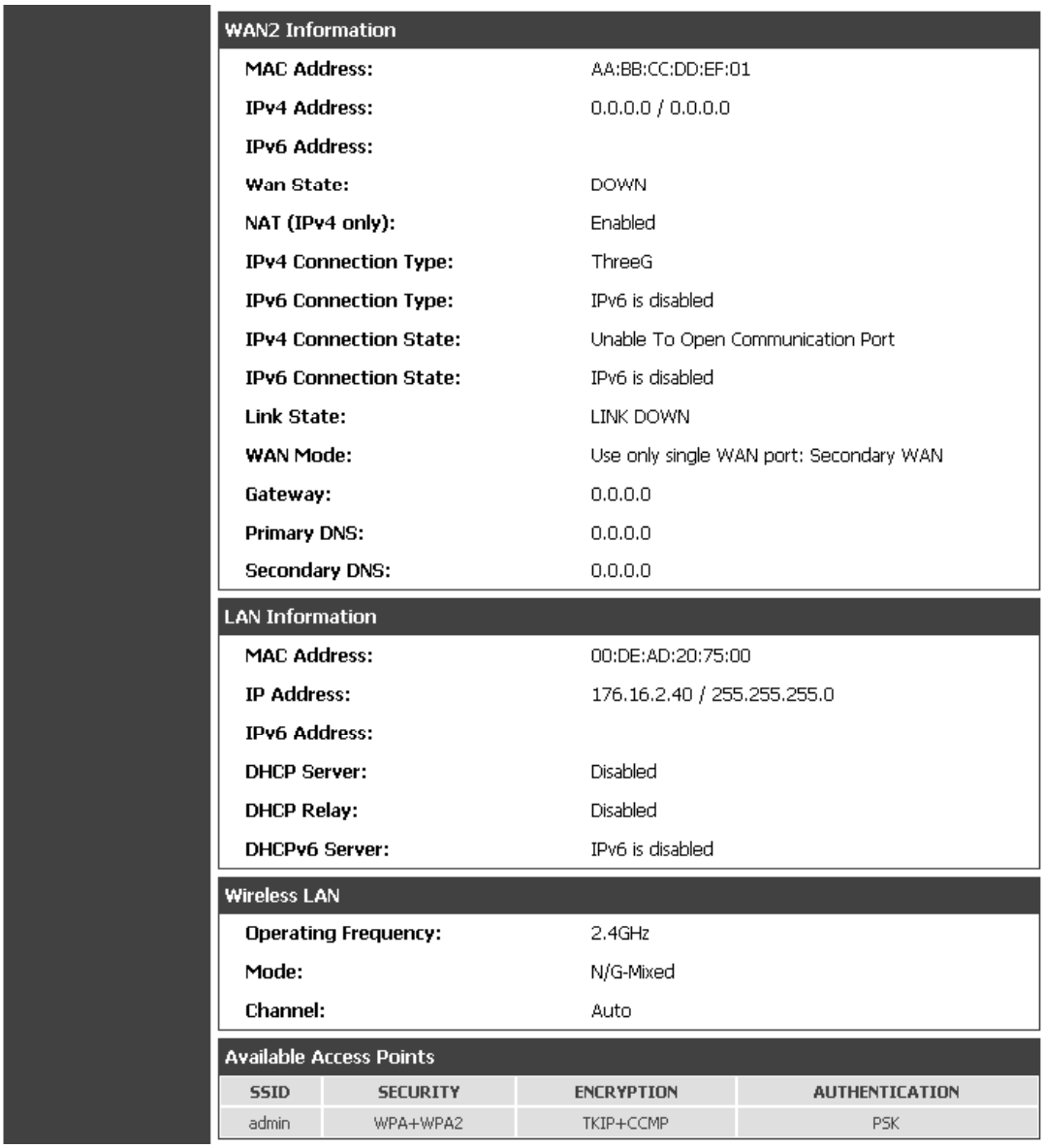


**Figure 91: Device Status display (continued)**




## 10.1.2 Resource Utilization

***Status > Device Info > Dashboard***

The Dashboard page presents hardware and usage statistics. The CPU and Memory utilization is a function of the available hardware and current configuration and traffic through the router. Interface statistics for the wired connections (LAN, WAN1, WAN2/DMZ, VLANs) provide indication of packets through and packets dropped by the interface. Click refresh to have this page retrieve the most current statistics.

**Figure 92: Resource Utilization statistics**

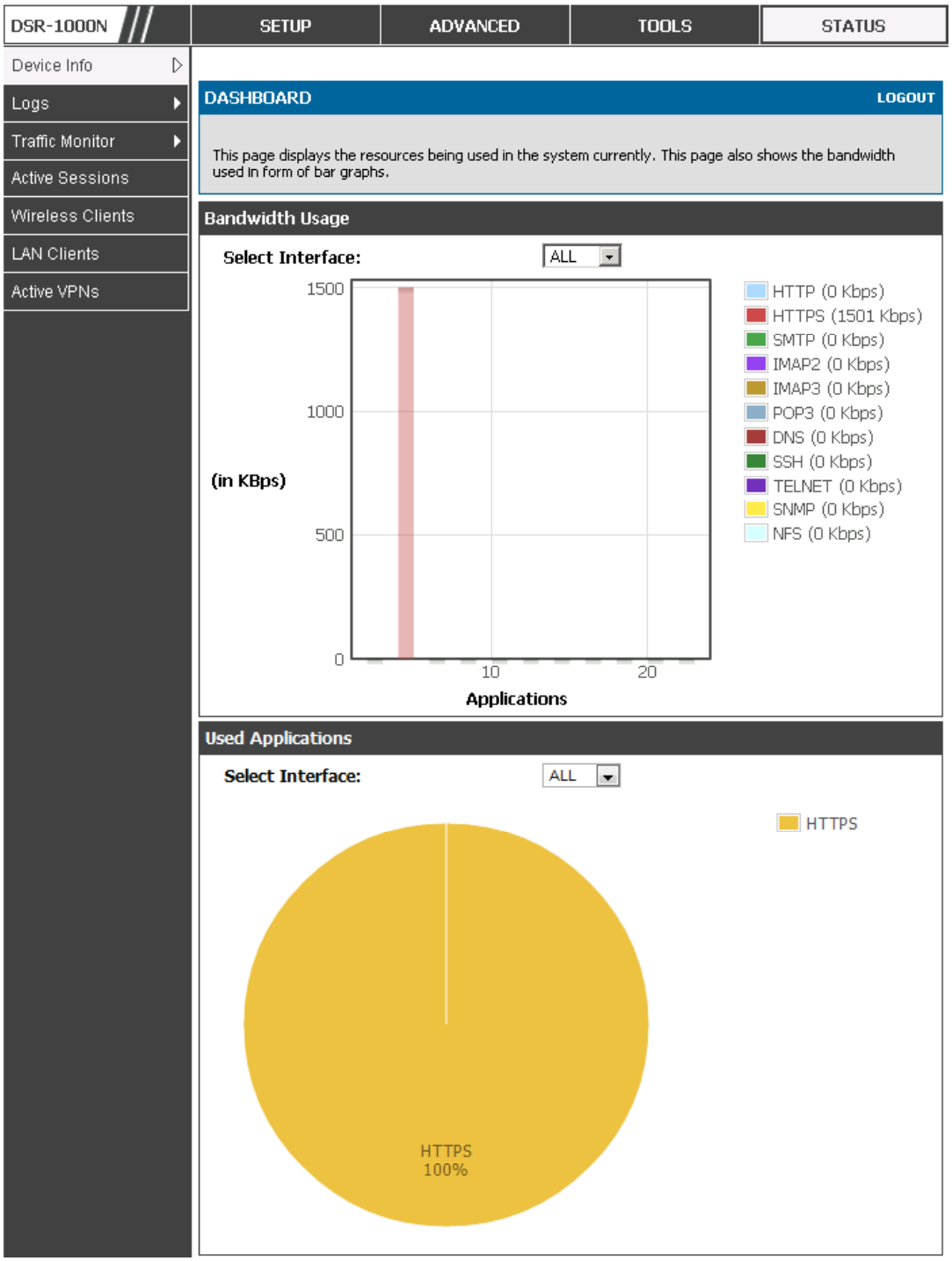
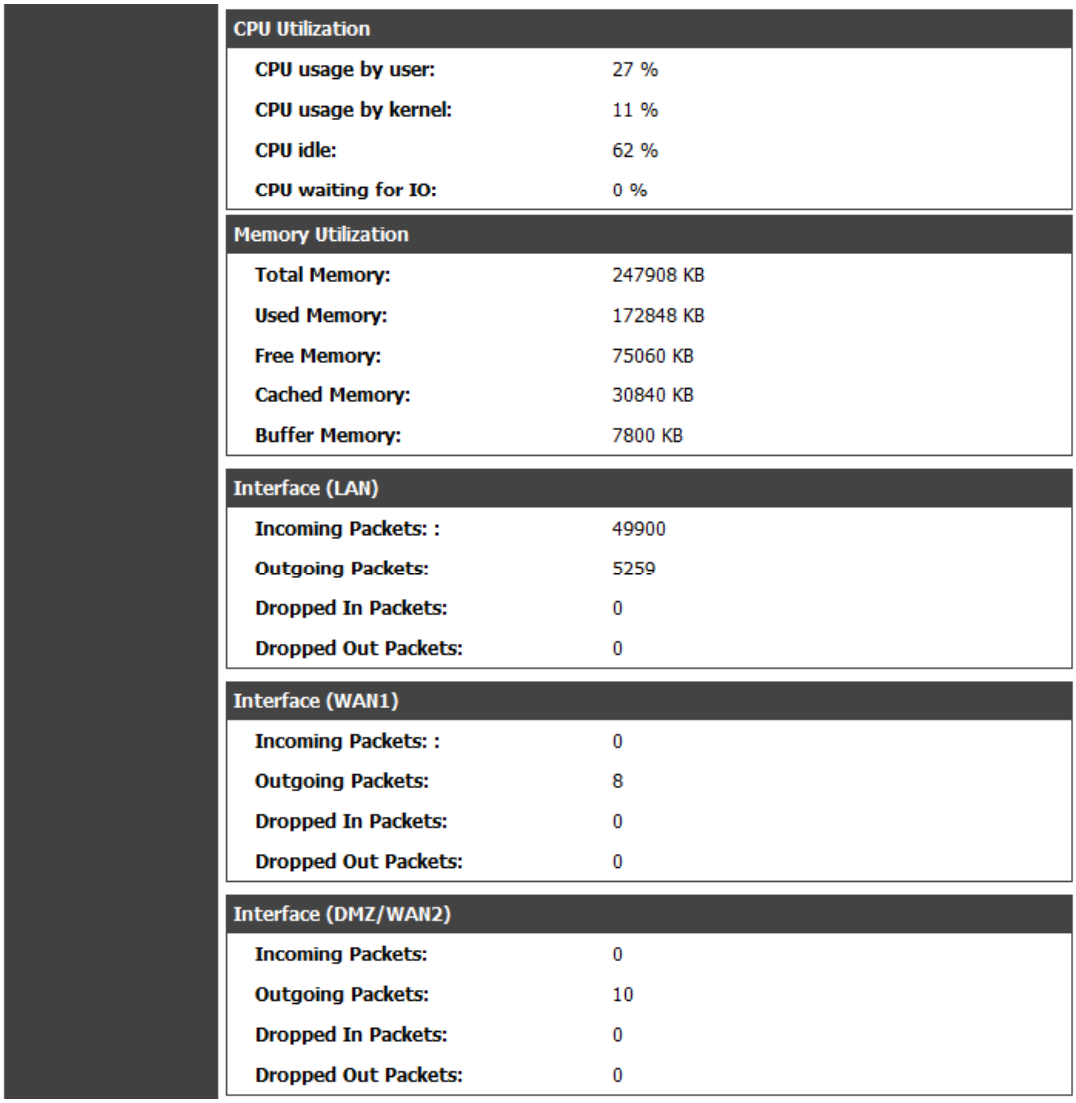


**Figure 93: Resource Utilization data (continued)**



| CPU Utilization | |
|---|---|
| CPU usage by user: | 27 % |
| CPU usage by kernel: | 11 % |
| CPU idle: | 62 % |
| CPU waiting for IO: | 0 % |

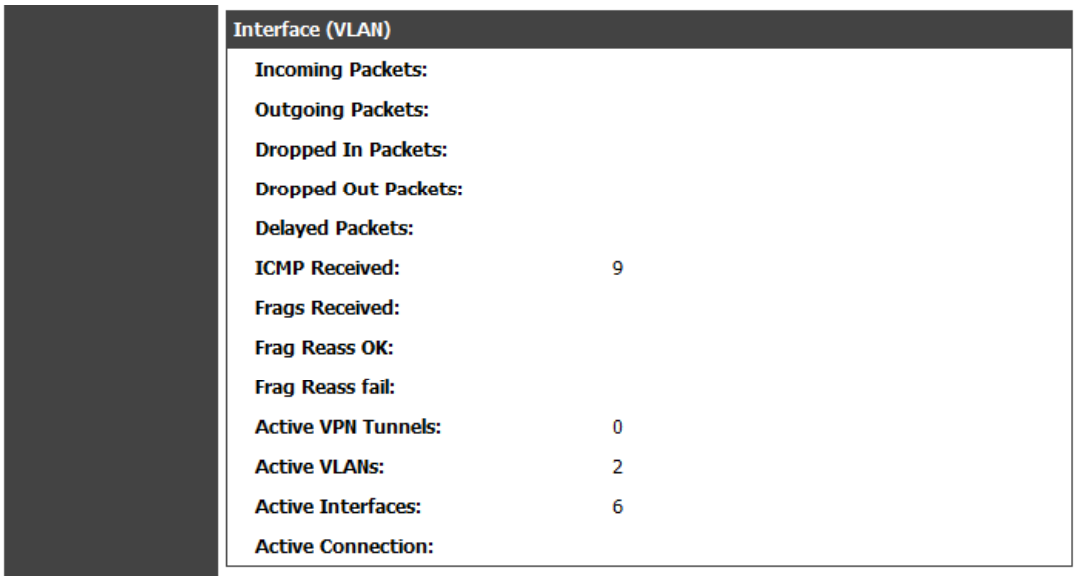
| Memory Utilization | |
|---|---|
| Total Memory: | 247908 KB |
| Used Memory: | 172848 KB |
| Free Memory: | 75060 KB |
| Cached Memory: | 30840 KB |
| Buffer Memory: | 7800 KB |

| Interface (LAN) | |
|---|---|
| Incoming Packets: : | 49900 |
| Outgoing Packets: | 5259 |
| Dropped In Packets: | 0 |
| Dropped Out Packets: | 0 |

| Interface (WAN1) | |
|---|---|
| Incoming Packets: : | 0 |
| Outgoing Packets: | 8 |
| Dropped In Packets: | 0 |
| Dropped Out Packets: | 0 |

| Interface (DMZ/WAN2) | |
|---|---|
| Incoming Packets: | 0 |
| Outgoing Packets: | 10 |
| Dropped In Packets: | 0 |
| Dropped Out Packets: | 0 |

**Figure 94: Resource Utilization data (continued)**




# 10.2 Traffic Statistics

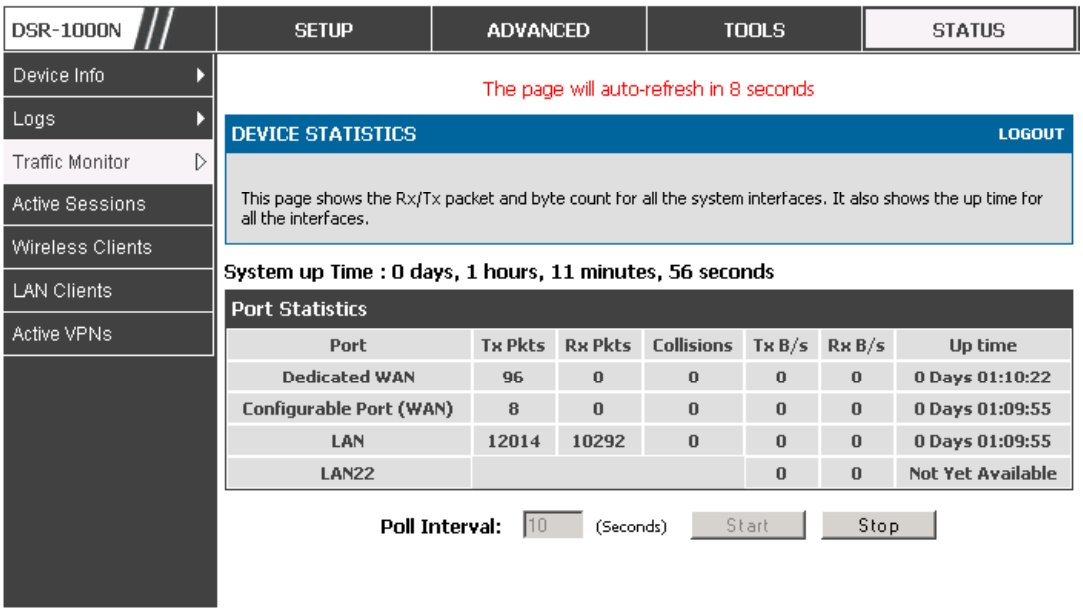
## 10.2.1 Wired Port Statistics

***Status > Traffic Monitor > Device Statistics***

Detailed transmit and receive statistics for each physical port are presented here. Each interface (WAN1, WAN2/DMZ, LAN, and VLANs) have port specific packet level information provided for review. Transmitted/received packets, port collisions, and the cumulating bytes/sec for transmit/receive directions are provided for each interface along with the port up time. If you suspect issues with any of the wired ports, this table will help diagnose uptime or transmit level issues with the port.

The statistics table has auto-refresh control which allows display of the most current port level data at each page refresh. The default auto-refresh for this page is 10 seconds.

**Figure 95: Physical port statistics**



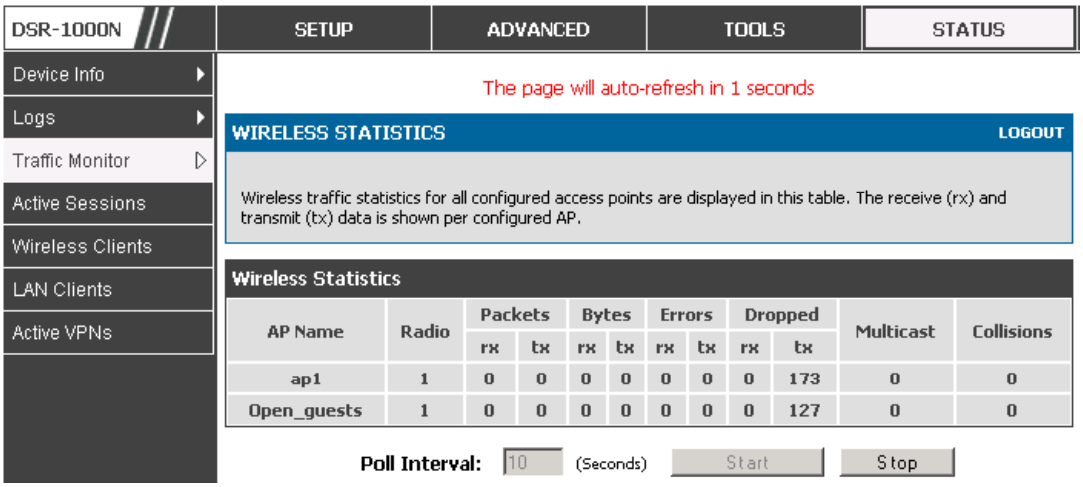

## 10.2.2 Wireless Statistics

***Status > Traffic Monitor > Wireless Statistics***

The Wireless Statistics tab displays the incrementing traffic statistics for each enabled access point. This page will give a snapshot of how much traffic is being transmitted over each wireless link. If you suspect that a radio or VAP may be down, the details on this page would confirm if traffic is being sent and received through the VAP.

The clients connected to a particular AP can be viewed by using the Status Button on the list of APs in the ***Setup > Wireless > Access Points*** page. Traffic statistics are shown for that individual AP, as compared to the summary stats for each AP on this Statistics page. The poll interval (the refresh rate for the statistics) can be modified to view more frequent traffic and collision statistics.

**Figure 96: AP specific statistics**



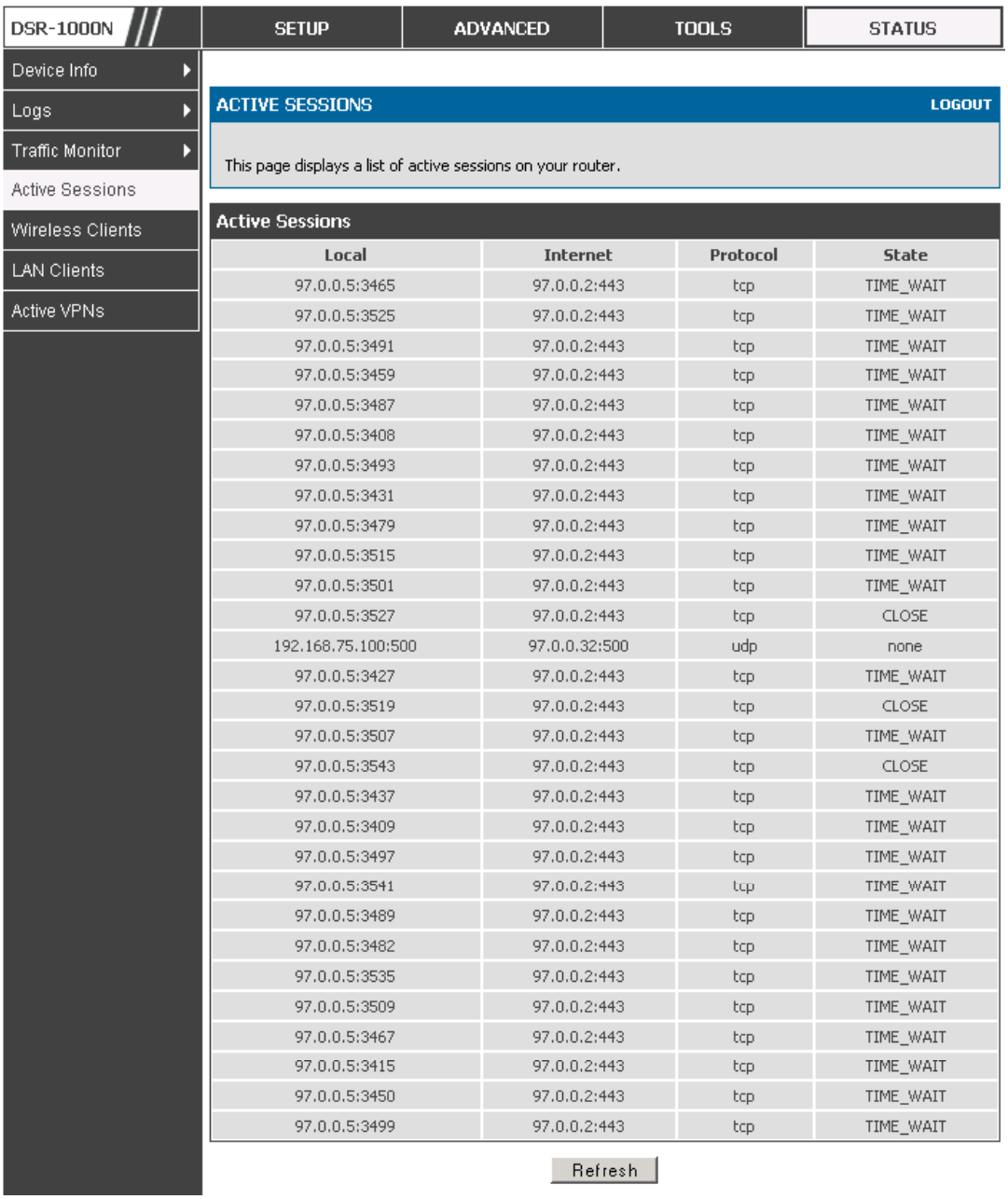

# 10.3 Active Connections

## 10.3.1 Sessions through the Router

***Status > Active Sessions***

This table lists the active internet sessions through the router's firewall. The session's protocol, state, local and remote IP addresses are shown.

**Figure 97: List of current Active Firewall Sessions**



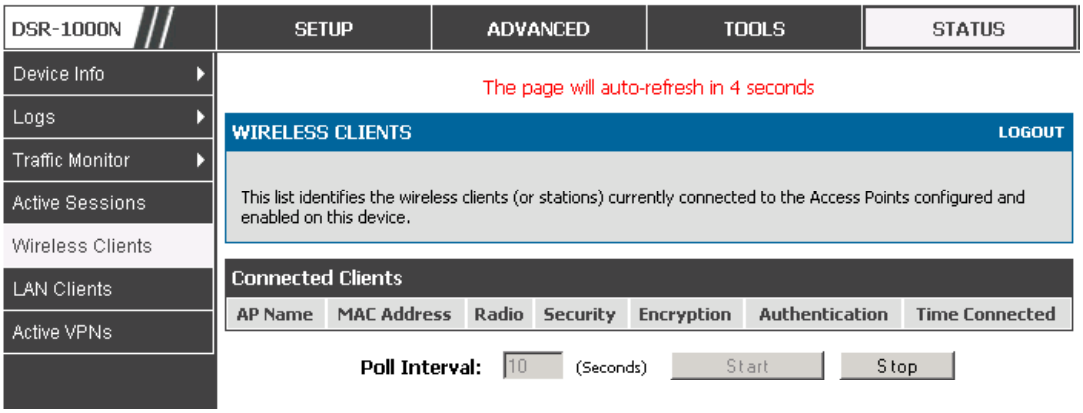
# 10.3.2 Wireless Clients

***Status > Wireless Clients***

The clients connected to a particular AP can be viewed on this page. Connected clients are sorted by the MAC address and indicate the security parameters used by the wireless link, as well as the time connected to the corresponding AP.

The statistics table has auto-refresh control which allows display of the most current port level data at each page refresh. The default auto-refresh for this page is 10 seconds.

**Figure 98: List of connected 802.11 clients per AP**

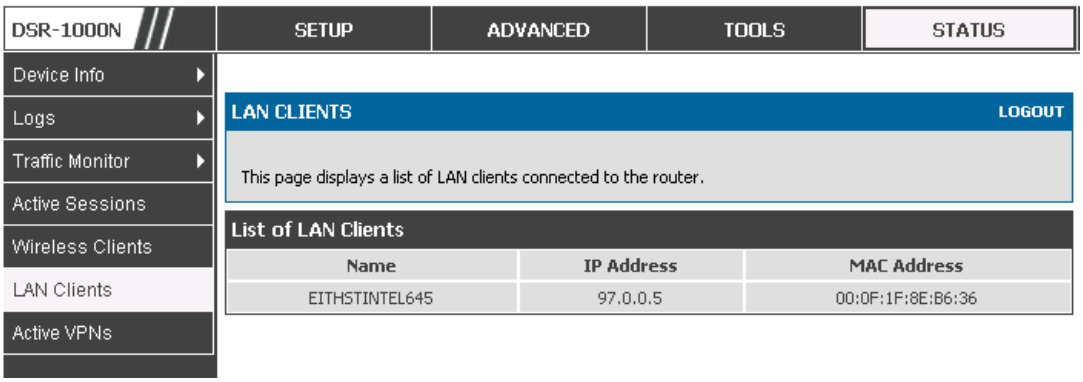



# 10.3.3 LAN Clients

***Status > LAN Clients***

The LAN clients to the router are identified by an ARP scan through the LAN switch. The NetBios name (if available), IP address and MAC address of discovered LAN hosts are displayed.

**Figure 99: List of LAN hosts**




## 10.3.4 Active VPN Tunnels

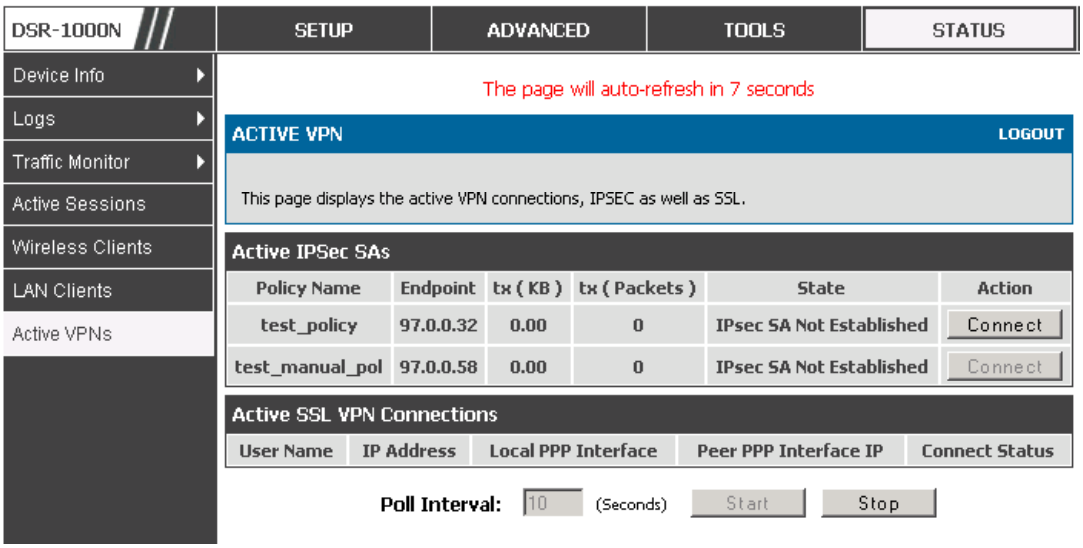
### *Status > Active VPNs*

You can view and change the status (connect or drop) of the router's IPsec security associations. Here, the active IPsec SAs (security associations) are listed along with the traffic details and tunnel state. The traffic is a cumulative measure of transmitted/received packets since the tunnel was established.

If a VPN policy state is "IPsec SA Not Established", it can be enabled by clicking the Connect button of the corresponding policy. The Active IPsec SAs table displays a list of active IPsec SAs. Table fields are as follows.

| Field | Description |
|---|---|
| Policy Name | IKE or VPN policy associated with this SA. |
| Endpoint | IP address of the remote VPN gateway or client. |
| Tx (KB) | Kilobytes of data transmitted over this SA. |
| Tx (Packets) | Number of IP packets transmitted over this SA. |
| State | Status of the SA for IKE policies: Not Connected or IPsec SA Established. |

**Figure 100: List of current Active VPN Sessions**




All active SSL VPN connections, both for VPN tunnel and VPN Port forwarding, are displayed on this page as well. Table fields are as follows.

| Field | Description |
|---|---|
| User Name | The SSL VPN user that has an active tunnel or port forwarding session to this router. |
| IP Address | IP address of the remote VPN client. |
| Local PPP Interface | The interface (WAN1 or WAN2) through which the session is active. |
| Peer PPP Interface IP | The assigned IP address of the virtual network adapter. |
| Connect Status | Status of the SSL connection between this router and the remote VPN client: Not Connected or Connected. |

# Chapter 11. Trouble Shooting

## 11.1 Internet connection

**Symptom:** You cannot access the router's web-configuration interface from a PC on your LAN.

**Recommended action:**

1. Check the Ethernet connection between the PC and the router.
2. Ensure that your PC's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your PC's address should be in the range 192.168.10.2 to 192.168.10.254.
3. Check your PC's IP address. If the PC cannot reach a DHCP server, some versions of Windows and Mac OS generate and assign an IP address. These auto-generated addresses are in the range 169.254.x.x. If your IP address is in this range, check the connection from the PC to the firewall and reboot your PC.
4. If your router's IP address has changed and you don't know what it is, reset the router configuration to factory defaults (this sets the firewall's IP address to 192.168.10.1).
5. If you do not want to reset to factory default settings and lose your configuration, reboot the router and use a packet sniffer (such as Ethereal™) to capture packets sent during the reboot. Look at the Address Resolution Protocol (ARP) packets to locate the router's LAN interface address.
6. Launch your browser and ensure that Java, JavaScript, or ActiveX is enabled. If you are using Internet Explorer, click Refresh to ensure that the Java applet is loaded. Close the browser and launch it again.
7. Ensure that you are using the correct login information. The factory default login name is admin and the password is password. Ensure that CAPS LOCK is off when entering this information.

**Symptom:** Router does not save configuration changes.

**Recommended action:**

1. When entering configuration settings, click Apply before moving to another menu or tab; otherwise your changes are lost.
2. Click Refresh or Reload in the browser. Your changes may have been made, but the browser may be caching the old configuration.

**Symptom:** Router cannot access the Internet.

**Possible cause:** If you use dynamic IP addresses, your router may not have requested an IP address from the ISP.

**Recommended action:**

1. Launch your browser and go to an external site such as www.google.com.
2. Access the firewall's configuration main menu at http://192.168.10.1.
3. Select ***Monitoring > Router Status***.
4. Ensure that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP. See the next symptom.

**Symptom:** Router cannot obtain an IP address from the ISP.

**Recommended action:**

1. Turn off power to the cable or DSL modem.
2. Turn off the router.
3. Wait 5 minutes, and then reapply power to the cable or DSL modem.
4. When the modem LEDs indicate that it has resynchronized with the ISP, reapply power to the router. If the router still cannot obtain an ISP address, see the next symptom.

**Symptom:** Router still cannot obtain an IP address from the ISP.

**Recommended action:**

1. Ask your ISP if it requires a login program — PPP over Ethernet (PPPoE) or some other type of login.
2. If yes, verify that your configured login name and password are correct.
3. Ask your ISP if it checks for your PC's hostname.
4. If yes, select ***Network Configuration > WAN Settings > Ethernet ISP Settings*** and set the account name to the PC hostname of your ISP account.
5. Ask your ISP if it allows only one Ethernet MAC address to connect to the Internet, and therefore checks for your PC's MAC address.
6. If yes, inform your ISP that you have bought a new network device, and ask them to use the firewall's MAC address.
7. Alternatively, select ***Network Configuration > WAN Settings > Ethernet ISP Settings*** and configure your router to spoof your PC's MAC address.