

# Unified Services Router User Manual

Wireless N Service Router

DSR-250NB1 DSR-150/150N/250/250N/500/500N/1000/1000N Version 2.01 | November 17, 2014

# Preface

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.

#### **Manual Revisions**

Revision	Date	Description
2.00	July 31, 2014	DSR Products with firmware version 2.00
2.01	November 17, 2014	add License Update section

## Trademarks/Copyright Notice

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

© 2014 D-Link Corporation, All Rights Reserved

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.

#### **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, DLINK 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.

## **Safety Instructions**

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

#### **Safety Cautions**

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions:

- Observe and follow service markings.
  - Do not service any product except as explained in your system documentation.
  - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
  - Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - The power cable, extension cable, or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets.

- These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

#### **Protecting Against Electrostatic Discharge**

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

- 1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- 2. When transporting a sensitive component, first place it in an antistatic container or package.
- 3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.

#### **Power Usage**

This device is an Energy Related Product (ErP) with High Network Availability (HiNA), and automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed.

DSR-250N/DSR-250NB1 Network Standby:7.8336 watts Switched Off: 0.1301 watts

DSR-250 Network Standby: 7.8588 watts Switched Off: 0.1290 watts

DSR-150N Network Standby: 8.2317 watts Switched Off: 0.1283 watts

DSR-150 Network Standby: 6.9133 watts Switched Off: 0.12661 watts

DSR-1000N Network Standby: 10.969 watts Switched Off: 0.0 watts

DSR-1000 Network Standby: 10.912 watts Switched Off: 0.0 watts

DSR-500N Network Standby: 11.487 watts Switched Off: 0.0 watts

DSR-500 Network Standby: 9.744 watts Switched Off: 0.0 watts

# **Table of Contents**

Preface	i
Manual Revisions	i
Trademarks/Copyright Notice	i
Limitations of Liability	i
Safety Instructions	ii
Safety Cautions	ii
Protecting Against Electrostatic Discharge	iv
Power Usage	V
Introduction	1
Installation	
Before you Begin	
Connect to your Network	
Basic Configuration	
#1 Log in to the Web UI	
#2 Change LAN IP Address	
#3 Configure DHCP Server	7
#4 Set Time and Date	
#5 Internet Connection Setup	
#6 Wireless Network Setup	
#7 Create Users	
#8 Security/VPN Wizard	
#9 Dynamic DNS Wizard	
LAN Configuration	
LAN Settings	
DHCP Server	
DHCP Relay	
DHCP Reserved IPs	21
IGMP Setup	
UPnP Setup	23
Jumbo Frames	24
VLAN	25
VLAN Settings	25
Captive Portal	27
Port/Wireless VLAN	
Connect to the Internet	
Dynamic IP	

Static IP	
PPPoE	
PPTP	
L2TP	
Japanese PPPoE	
Russian PPPoE	
Russian PPTP	
Russian L2TP	
WAN2 Settings	
WAN	
DMZ	40
WAN3 (3G Internet)	41
WAN Mode	
Single WAN Port	
Auto-Rollover using WAN IP	
Load Balancing	
Round Robin	45
Spillover	
Routing Mode	47
NAT or Classical	47
Transparent	
Bridge	
IP Aliasing	
DMZ Settings	
DMZ LAN DHCP Reserved IPs	
Dynamic DNS Settings	53
Traffic Management	
Bandwidth Profiles	
Traffic Shaping	
Routing	
Static Routes	
RIP	
OSPF	
Protocol Binding	
IPv6	
IP Mode	
WAN Settings	64
Dynamic IP	
Static IP	65
PPPoE	
Static Routing	67
OSPFv3	
6 to 4 Tunneling	71

ISATAP	
LAN Settings	
DHCPv6 Server	
IPv6 Address Pools	
IPv6 Prefix Length	
Router Advertisement	
Advertisement Prefixes	
IPv6 Tunnels Status	
Wireless Settings	
Access Points	
Profiles	
Radio Settings	
WMM Settings	
WDS	
Advanced Settings	
WPS	
VDN	90
IPSec VPN	
Policies	
Tunnel Mode	
Split DNS Names	
DHCP Range	
Certificates	
Trusted Certificates	
Active Self Certificates	
Self Certificate Requests	
Easy VPN Setup	
PPTP VPN	
Server	
Client	
PPTP Active Users List	
L2TP VPN	
Server	
Client	
L2TP Active Users List	
SSL VPN	
Server Policies	
Portal Layouts	
Resources	
Add New Resource	
Port Forwarding	
Client	

Client Routes	
Open VPN	
Settings	
Server	
Client	
Access Server Client	
Local Networks	
Remote Networks	
Authentication	
GRE	
Security	
Groups	
Login Policies	
Browser Policies	
IP Policies	
Users	
User Management	
Import User Database	
Create a User Database (CSV File)	
External Authentication Servers	
RADIUS Server	
POP3 Server	
POP3 Trusted Server	
LDAP Server	
AD Server	
NT Domain Server	
Login Profiles	
Web Content Filtering	
Static Filtering	
Approved URLs	
Blocked Keywords	
Dynamic Filtering	
Firewall	
Firewall Rules	
Schedules	
Custom Services	
ALGs	
SMTP ALGs	
Approved Mail IDs	
Blocked Mail IDs	
Mail Filtering	
VPN Passthrough	
Dynamic Port Forwarding	

Application Rules	
Attack Checks	
Intel <sup>®</sup> AMT	
IPS	
Maintenance	
System Settings	
Date and Time	
Session Settings	
License Updates	
USB Share Ports	
SMS Service	
Inbox	
Create SMS	
Package Manager	
Set Language	
Web GUI Management	
Remote Management	
SNMP	
SNMP User List	
SNMP Trap List	
Access Control	
SNMP System Info	
Diagnostics	
Ping an IP Address/Domain Name	
Using Traceroute	
Performing DNS Lookups	
Capture Packets	
System Check	
Power Saving	
Firmware Upgrade	
Check Update	
Using PC	
Using USB	
Configuration Files	
Backup	
Restore	
Configuration Settings	
Soft Reboot	
Reset to Factory Default Settings	
Log Settings	
Defining What to Log	
Routing Logs	

System Logs	
Remote Logs	
Syslog Server	
Event Logs	
IPv6 Logs	
Status and Statistics	
Dashboard	200
Manage Dashboard	201
System	
LAN Info	
WAN1	
WAN2	205
WAN3	
Wireless	
All Logs	
Current Logs	
Firewall Logs	
IPSec VPN Logs	
SSL VPN Logs	211
USB Status	212
Network Information	213
DHCP Leased Clients	213
Active Sessions	214
Active VPNs	215
Interface Statistics	216
View Wireless Clients	217
Device Stats	218
Wireless Statistics	219
View LAN Clients	220
Troubleshooting	221
Internet Connection	221
Date and time	223
Pinging to Test LAN Connectivity	224
Testing the LAN path from your PC to your router	224
Testing the LAN path from your PC to a remote device	225
Restoring factory-default configuration settings	226
Appendix A - Glossary	227
Appendix B - Factory Default Settings	229
Appendix C - Standard Services for Port Forwarding & Firewall Configuration	230

Appendix D - Log Output Reference	231
Appendix E - RJ-45 Pin-outs	294
Appendix F - New Wi Fi Frequency table ( New appendix section )	295
Appendix G - Product Statement	

## Introduction

D-Link 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 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 solution supports configuring a port as a dedicated DMZ port allowing you to isolate servers from your LAN.

*Note:* The DSR-150/150N/250/250N products have a single WAN interface, and thus do not support Auto Failover or 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 support, 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.

Note: The DSR-150N, DSR-250N, and DSR-500N support 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-150/150N/250/250N, DSR-500/500N and DSR-1000/1000N are capable of simultaneously managing 5, 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-150/150N, DSR-250/250N, DSR-500/500N, and DSR-1000/1000N support 10, 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 Wi-Fi 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.

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

## Installation

This section provides information and steps on how to connect your DSR router to your network.

### **Before you Begin**

Observe the following precautions to help prevent shutdowns, equipment failures, and injuries:

- Ensure that the room in which you operate the device has adequate air circulation and that the room temperature does NOT exceed 40°C (104°F).
- Allow 1 meter (3 feet) of clear space to the front and back of the device.
- Do NOT place the device in an equipment rack frame that blocks the air vents on the sides of the chassis. Ensure that enclosed racks have fans and louvered sides.
- Before installation, please correct these hazardous conditions: moist or wet floors, leaks, ungrounded or frayed power cables, or missing safety grounds.

#### **Connect to your Network**

This section provides basic information about physically connecting the DSR-250 to a network.

- 1. Connect an Ethernet cable from the port labeled WAN to the external router or modem. The port WAN is pre-allocated to the WAN network segment.
- 2. Connect an Ethernet cable from one of the LAN ports to a switch or a computer in the LAN network segment.
- 3. Connect an RJ45-to-DB9 cable from the console port for CLI (Command Line Interface) management access (optional).

**Note:** Refer to the Quick Installation Guide included with your router for more information on network connectivity, port, and LED information.

# **Basic Configuration**

After you install the router, perform the basic configuration instructions described in this section which includes:

- "#1 Log in to the Web UI" on page 5
- "#2 Change LAN IP Address" on page 6
- "#3 Configure DHCP Server" on page 7
- "#4 Set Time and Date" on page 8
- "#5 Internet Connection Setup" on page 9
- "#6 Wireless Network Setup" on page 12
- "#7 Create Users" on page 13
- "#8 Security/VPN Wizard" on page 14
- "#9 Dynamic DNS Wizard" on page 16

## #1 Log in to the Web UI

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. Access the router's Web user interface (Web UI) for management by using any web browser, such as Internet Explorer, Firefox, Chrome, or Safari.

Note: The workstation from which you manage the router must be in the same subnet as the router (192.169.10.0/24).

To access the device with the Web UI:

- 1. Connect your workstation to an available LAN port on the router.
- 2. Ensure your workstation has DHCP enabled or is assigned a static IP address within the 192.168.10.0/24 subnet.

**Note:** Disable pop-up blocking software or add the management IP address http://192.168.10.1 to your pop-up blocker's allow list.

3. Launch a browser, enter the IP address for the LAN interface (default = http://192.168.10.1), and then press **Enter**.



4. Enter your username (default = admin) and your password (default = admin), then click Login.

Username	1		
Password			
	Login		

5. The web management interface opens with the Status > Dashboard page. This page displays general, LAN, and WLAN status information. You can return to this page at any time by clicking Status > Dashboard.

## **#2 Change LAN IP Address**

To change the LAN IP address of the router, follow the steps below:

- 1. Log in to the router.
- 2. Click **Network** > **LAN** > **LAN Settings**. The LAN Settings page will appear.

D-Link Unified Services Router - DSR-1000N		Logged in a Serial:	Logged in as: admin (ADMIN)   Language: English [US] O Logout Serial: Q8281A3000007   Firmware: 1,108006E_WW Wizard System Search 9.		
🖾 Status	🛜 Wireless 🛛 📃 Networ	rk CB VPN	Security	<b>O</b> <sup>o</sup> Maintenance	
Network » LAN » LAN Setting The LAN Configuration page a affect all devices connected hosts to be in the same subno LAN Settings	is Nows you to configure the LAN interfac to the router's LAN switch and also wir and use the new address to access t	ce of the router inclu reless LAN clients. No this GUI.	uding the DHCP Server w te that a change to the	which runs on it and Changes here LAN IP address will require all LAN	
IP Address Setup					
IP Address	192.168.10.1				
Subnet Mask	255.255.255.0				
DHCP Setup					
DHCP Mode	DHCP Server	•			
Starting IP Address	192.168.10.100				
Ending IP Address	192.168.10.254	1			
Default Gateway	192.168.10.1				
Domain Name	DLink				
Lease Time	24 [Rar	nge: 1 - 262800) Hours			
Configure DNS / WINS	OFF				

- 3. Under IP Address Setup, enter a new IP address for the router.
- 4. Enter a new subnet mask if needed.
- 5. Click **Save** at the bottom of the page.

**Note:** If you change the IP address and click Save, the Web UI will not respond. Open a new connection to the <u>new</u> IP address and log in again. Be sure the LAN host (the machine used to manage the router) has obtained an 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.

## **#3 Configure DHCP Server**

To change the DHCP settings of the router, follow the steps below:

- 1. Log in to the router.
- 2. Click **Network** > **LAN** > **LAN Settings**. The LAN Settings page will appear.

D-Link Unified Services Router - DSR-1000N		Logged in as: Serial: QB	admin ( ADMIN )   La 281 A3000007   Firmv	nguage: English [US] 💽 Legout vare: 1.108006E_WW Vizard System Search Q
🖾 Status 🗧	Wireless 📃 Network	CA VPN	Security	O <sup>o</sup> Maintenance
Network » LAN » LAN Settings The LAN Configuration page allows y affect all devices connected to the hosts to be in the same subnet and LAN Settings	ou to configure the LAN interface o router's LAN switch and also wireles use the new address to access this	f the router includin ss LAN clients. Note 1 GUI.	g the DHCP Server w that a change to the	Hich runs on it and Changes here LAN IP address will require all LAN
IP Address Setup	100 100 10 1	_		
Subnet Mask	255.255.255.0			
DHCP Setup				
DHCP Setup DHCP Mode	DHCP Server	×		
DHCP Setup DHCP Mode Starting IP Address	DHCP Server 192.168.10.100			
DHCP Setup DHCP Mode Starting IP Address Ending IP Address	DHCP Server 192.168.10.100 192.168.10.254			
DHCP Setup DHCP Mode Starting IP Address Ending IP Address Default Gateway	DHCP Server 192 168.10.100 192 168.10.254 192 168.10.1			
DHCP Setup DHCP Mode Starting IP Address Ending IP Address Default Gateway Domain Name	DHCP Server 192 168.10.100 192 168.10.254 192 168.10.1 DLink			
DHCP Setup DHCP Mode Starting IP Address Ending IP Address Default Gateway Domain Name Lease Time	DHCP Server 192.168.10.100 192.168.10.254 192.168.10.1 DLink 24 [Ranger	1 - 262800) Hours		

3. From the *DHCP Mode* drop-down menu under *DHCP Setup*, select **None** (disable), **DHCP Server** (enable), or **DHCP Relay**.

**Note:** DHCP Relay will allow DHCP clients on the LAN to receive IP address leases and corresponding information from a DHCP server on a different subnet. When LAN clients make a DHCP request it will be passed along to the server accessible via the Relay Gateway IP address you enter.

4. If enabled, fill in the following fields:

Field	Description
Starting IP Address	Enter the starting IP address in the DHCP address pool. Any new DHCP cli- ent joining the LAN is assigned an IP address within the starting and end- ing IP address range. Starting and ending IP addresses should be in the same IP address subnet as the wireless controller's LAN IP address.
Ending IP Address	Enter the ending IP address in the DHCP address pool.
Default Gateway	By default this setting is router's LAN IP address. It can be customized to any valid IP within the LAN subnet, in the event that the network's gateway is not this router. The DHCP server will give the configured IP address as the Default Gateway to its DHCP clients.
Domain Name	Enter a domain name.
Lease Time	Enter the time, in hours, for which IP addresses are leased to clients.
Configure DNS/WINS	Toggle to <b>On</b> and enter DNS and/or WINS server IP address(es).

5. Click **Save** at the bottom of the page.

#### #4 Set Time and Date

- 1. Log in to the router.
- 2. Click **Wizard** in the upper-right side of the page. If you want to manually configure your date/time settings, refer to "Date and Time" on page 162.
- 3. Click **Run** in the *Date and Time Wizard* box.



4. Click the continent from the map and then next to *City*, select your time zone from the drop-down menu. Toggle Daylight Saving to **ON** if it applies to you and then click **Next**.



- 5. Toggle NTP server to ON to use a time server or toggle to OFF to manually enter the time and date.
- 6. If you selected ON, select either **Default** or **Custom** from the drop-down menu. If you selected Custom, enter a primary and secondary NTP server address.
- 7. Enter the time to synchronize with the NTP server and click **Save**.

ate and Time Wi	ard	×
	Current NTP Server is ON	
Obtain Time from	Network	
NTP Server	CH	
NTP Server Type	Default	
Time to Synchronize	120	

8. A summary page will appear. Verify your settings and then click **Finish**.

#### **#5 Internet Connection Setup**

This router has two WAN ports that can be used to establish a connection to the internet. 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. Supported Internet connection types include Dynamic, Static, PPPoE, PPTP, L2TP, Japanese PPPoE, and Russian PPPoE/PPTP/L2TP.

To configure your router to connect to the Internet, follow the steps below:

- 1. Log in to the router.
- 2. Click **Wizard** in the upper-right side of the page. If you want to manually configure your Internet settings, refer to "Connect to the Internet" on page 30.



3. Click **Run** in the Internet Connection Wizard box.



4. Toggle **On** next to either *DHCP* or *Static IP Address* and click **Next**. If your connection type is not listed, refer to "Connect to the Internet" on page 30.



a. If you selected **DHCP**, complete the fields below:

nternet Connectio	n Wizard	×
	DHCP Connection Details	
DHCP Connection	Dynamic IP Address)	
MAC Address Source	Use Default Address 💌 Host Name	
DNS settings		
DNS Server Source	Get Dynamically from IS	
Step: [2 of 2]		Previous Save

Field	Description	
	This MAC address will be recognized by your ISP. Select from the following three options:	
MAC Address Source	• Use Default Address - Uses the default MAC address of the router.	
	<ul> <li>Clone your PC's MAC Address - Select to use the MAC address of the computer you are currently connecting with.</li> </ul>	
	<ul> <li>Use this MAC Address - Select to manually enter a MAC address and enter the address in the box.</li> </ul>	
Host Name	Enter a host name if required by your ISP.	
	Select from the following two options:	
DNS Server Source	• Get Dynamically from ISP - Select to use the DNS servers assigned by your ISP.	
	<ul> <li>Use these DNS Servers - Select to manually enter a primary and secondary DNS server address(es).</li> </ul>	

Skip to Step 5 on the bottom of the next page.

b. If you selected **Static**, complete the fields below:

Internet Connection Wizard	0
Static IP Con	nection Details
IP Address Gateway IP Address DNS settings	IP Subnet Mask
Primary DNS Server	Secondary DNS Server
Step: [2 of 2]	Previous Save

Field	Description	
IP Address	Enter the IP address assigned by your ISP.	
Gateway IP Address	Enter the gateway IP address assigned by your ISP.	
IP Subnet Mask	sk Enter the subnet mask assigned by your ISP.	
Primary DNS Server	Enter the primary DNS server IP address assigned by your ISP.	
Secondary DNS Server	Enter the secondary DNS server IP address assigned by your ISP.	

5. Click **Save**. The router will reboot and attempt to connect to your ISP. Please allow one to two minutes to connect.

#### **#6 Wireless Network Setup**

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".

- 1. Log in to the router.
- 2. Click Wizard in the upper-right side of the page.
- 3. Click **Run** in the Wireless Wizard box.

Internet Connection Wizard This wizard will guide you in connecting your new D-Unk Unified Services Router to the Internet. Res	Security Wizard This weard will guide you in configuring default Quibound Policy, VPN Passihraugh and VPN Network Settings.
Wirelss Wizard This wizard will gaide you through common and way steps to configure your routers: alrelacs interface.	Users Wizard This Wizard publics you in creating a new user.
Dynamic DNS Wizard. This Wizard helps in configuring Dynamic DNS WANI 1 or WAN 2 settings.	Date and Time Wizard This Wizard helps you in configuring Date and Time sotting.

- 5. Enter a SSID, which is the name of your wireless network.
- 6. Next to Network Key Type, select Manual.
- 7. Enter a password for the wireless network. Wireless devices connecting to this network must enter this password to connect. The password is case-sensitive.
- 8. Click Save.
- 9. A window will appear with a summary of your settings. Click **Finish**.

#### **#7 Create Users**

The Users Wizard allows you to create user account that you can assign to groups. Refer to "Users" on page 129 for more information. You may want to create Groups before users so you may assign them to groups as you create them. To create groups, refer to "Groups" on page 125.

To create new users, follow the steps below:

- 1. Log in to the router.
- 2. Click **Wizard** in the upper-right side of the page.
- 3. Click **Run** in the Users Wizard box.

Internet Connection Wizard	Security Witzard
This wizard will guide you in connecting	This waard will guide you in configuring
your new D-Unit Unified Services Router to	default Quibound Policy, VFN Pasthrough
the Internet.	and VFN Network Settings.
Wirelss Wizard This wized will golde you through common and way teep; to configure your routers wireless interface.	USETS Wizard This Wizerd guides you in creating a new ster:
Dynamic DNS Wizard.	Date and Time Wizard
This Wizard helps in configuring Dynamic DNS	This Wizard helps you in configuring Date
WAN 1 or WAN Z settings.	and Time settings.

Users Wizard				×
		Add a N	ew User	
User Configurati	ion			
New User Name New Password			Group Type Confirm Password	ADMIN
Step: [1 of 1]				Previous Save

- 5. Enter a unique user name.
- 6. Select the group type from the drop-down menu. For more information on groups, refer to "Groups" on page 125.
- 7. Enter a password for the user.
- 8. Enter the password again for confirmation.
- 9. Click Save.

## #8 Security/VPN Wizard

The Security Wizard allows you to enable VPN passthrough and create a VPN.

Follow the steps below:

- 1. Log in to the router.
- 2. Click **Wizard** in the upper-right side of the page.
- 3. Click **Run** in the *Security Wizard* box.

Internet Connection Wizatd This wizard will guide you in connecting rour new D-Unk Unified Services Router to the Internet. First	Security Witzard This waard will guide you in configuring default Quibound Policy, VPN Passihrough and VPN Network Settings.
Wirelss Wizard This wizard will golde you through commun- and wasy steps to configure your routers. Atrained instarface.	Users Wizard This Wizard guides you in creating a new user.
Dynamic DNS Wizard Nis Wizard helps in configuring Dynamic DNS WANI 1 or WAN 2 settings.	Date and Time Wizard This Wand helps you in configuring Date and Time setting:

	Current Outbo	und Policy is Allow	
Default Outb	ound Policy for IPv4		
Always	Allow		
VPN Passthro	ugh		
IPSec	OH	PPTP	ON
Enable this to allo route.	ow IPsec tunnels to pass through the	Enable this to allow PPTP tunnels to pass router. To make this work, enable PPTP	through the ALG also.
L2TP	NR		
Enable this to allo router.	ow L2TP tunnels to pass through the		
ten: [1 of 3]		Previo	Next

- 5. Select the default outbound policy from the drop-down menu.
- 6. Toggle which type(s) of VPN you want allowed to pass through the router to **ON** and click **Next**.

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

	Configure VPN 1	Type and Remote & Local Addresse:	5
Select VPN Type fo	r your VPN Network	Connection Name	
IP Protocol Version	lpv4	Pre-Shared key	
IKE Version	IKEv1	Local Gateway	WAN1
Remote & Local WA	N Addresses		
Remote Gateway Type	1P Address	Remote WAN's IP	
Local Gateway Type	IP Address	Address / FQDN	
		Local WAN's IP	
		Address / FQDN	

- 8. From the Select VPN Type drop-down menu, select either Site to Site or Remote Access.
- 9. Next to Connection Name, enter a name for this VPN connection.
- 10. Next to IP Protocol Version, select either IPv4 or IPv6.
- 11. Next to IKE Version, select the version of IKE.
- 12. Next to Pre-Shared Key, enter the pre-shared key used.
- 13. Next to Local Gateway, select which WAN port used for the local gateway.
- 14. Next to Remote Gateway Type and Local Gateway Type, select either IP Address or FQDN.
- 15. Enter the Remote and Local WAN IP Address or FQDN and click **Next**.

	entre entre and a second state	
	Secure Connection Accessibility	
Configure Secure Connection Ac	ccessibility	
Remote Network IP	Remote Network	
Address	Subnet Mask	
Local Network IP	Local Network Subnet	
Address	Mask	

- 16. Enter the remote network IP address and subnet mask.
- 17. Enter the local network IP address and subnet mask.
- 18. Click Save.

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

## **#9 Dynamic DNS Wizard**

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. Refer to "Dynamic DNS Settings" on page 53 for more information.

Follow the steps below:

- 1. Log in to the router.
- 2. Click **Wizard** in the upper-right side of the page.
- 3. Click **Run** in the *Dynamic DNS Wizard* box.

Internet Connection Wizard	Security Witzard
This wizard will golde you in connecting	This weard will give you in configuring
your new Dillnk Unified Services Router to	default Quibound PoBcy, VPN Pauthrough
the Internet.	and VPN Hetwork Settings.
Wirelss Wizard	Users Wizard
This wized will golde you through common	This Wizard
and way throu to configure your routers	This Wizard guides you in creating a new
wirelast interface.	user.
Dynamic DNS Wizard.	Date and Time Wizard
This Wizard helps in configuring Dynamic DNS	This Ward helps you in configuring Date
WAN 1 or WAN 2 settings.	and Time setting.

ynamic DNS Wiz	ard				X
	c	urrently WAN1 is	not configured		
Dynamic DNS					
Dynamic DNS	WAN 1				
Dynamic DNS WAN	11				
DNS Server Type	DynDNS		Domain Name		
User Name			Password		
Allow Wildcards	OFF		Update Periodically	OFF	(30 Days)
tent [1 of 1]				Pres	ious Save

- 5. Next to Dynamic DNS, select WAN1 or WAN2.
- 6. Select the DNS Server Type from the drop-down menu.
- 7. Depending on your service, enter your DDNS user name, password, and domain name.
- 8. Toggle *Allow Wildcards* to **ON** if required by your DDNS service.
- 9. Toggle Update Periodically to **ON** to auto update every 30 days.
- 10. Click Save.

# LAN Configuration

By default, the router functions as a Dynamic Host Configuration Protocol (DHCP) server to the hosts on the LAN and WLAN 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 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 DHCP server on the network. 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 host names. 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.

### **LAN Settings**

Path: Network > LAN > LAN Settings

To configure the LAN settings on the router:

#### 1. Click **Network** > **LAN** > **LAN Settings**.

D-Link Ibitly d Services Router - 1550, 10000			Logged In as: schwin ( 201401 )   Language: English (US) Serlat: clissific3coccol   Permivare: ( 1.000002 www W Witzard, System Search 9.		
🙆 Status	😤 Wineless	Network	CAL VON	Security	OP Maintenance
etwork + LAN = LAN Setting be LAN Configuration page a ffect all devices connected outs to be in the same subm AN Settings	p Nows you to configure to the router's LAN so it and use the new ad	the LAN interface of itch and also wireless dress to access this G	the router Includi LAN clients, Note UI	ing the DHCP Server w that a change to the	bich runs on it and Changes here LAN IP address will require all LA
IP Address Setup IP Address Subnet Mask		192 168 10 1 255 255 255 0			
DHCP Setup DHCP Mode	1	DHCP Server			
Ending IP Address Default Gateway		192.168.10.254	3		
Domain Name Loise Time		DLink 24 (Kitmum )	Hittill() Hours		
Configure DNS / WINS DNS Host Name Mapping	1	( Date			
Host Name			@ Add(es)	-	
LAN Proxy Activate DNS Proxy			-		

2. Complete the fields in the table below and click **Save**.

Field	Description
IP Address	Enter an new IP address for the router. Default is 192.168.10.1.
Subnet Mask	Enter the subnet mask for your network. Default is 255.255.255.0.
DHCP Mode	<ul> <li>Select one of the following modes:</li> <li>None - Turns off DHCP.</li> <li>DHCP Server (default) - The router will act as the DHCP server on your network.</li> <li>DHCP Relay - DHCP clients on your network will receive IP address leases from a DHCP server on a different subnet.</li> </ul>

#### **DHCP Server**

1. Select **DHCP Server** from the drop-down menu.

DHCP Mode	DHCP Server	
Starting IP Address	192.168.10.100	
Ending IP Address	192.168.10.254	
Default Gateway	192.168.10.1	
Domain Name	DLink	
Lease Time	24 [Range: 1 - 262800] Hours	
Configure DNS / WINS	OFF	

2. Complete the fields in the table below and click **Save**.

Field	Description
DHCP Mode	Select <b>DHCP Server</b> from the drop-down menu.
Starting IP Address	Enter the starting IP address in the DHCP address pool. Any new DHCP client joining the LAN is assigned an IP address within the starting and ending IP address range. Starting and ending IP addresses must be in the same IP address subnet as the router's LAN IP address.
Ending IP Address	Enter the ending IP address in the DHCP address pool.
Default Gateway	Enter the default gateway IP address you want to assign to your DHCP clients. This IP is usually the router's LAN IP address (default is 192.168.10.1).
Domain Name	Enter a domain name.
Lease Time	Enter the time, in hours, for which IP addresses are leased to clients.
Configure DNS/WINS	Toggle to <b>On</b> to manually enter DNS and/or WINS server IP address(es). If set to <b>Off</b> , your router's LAN IP address will be assigned the DNS server to your clients and the router will get the DNS information from your ISP.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

#### **DHCP** Relay

1. Select **DHCP Relay** from the drop-down menu.

DHCP Mode	DHCP Relay
Domain Name	DLink.
Gateway	

2. Complete the fields in the table below and click **Save**.

Field	Description
DHCP Mode	Select <b>DHCP Relay</b> from the drop-down menu.
Domain Name	Enter the domain name of your network.
Gateway	Enter the relay gateway IP address.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

#### **DHCP** Reserved IPs

```
Path: Network > LAN > LAN DHCP Reserved IPs
```

The router's DHCP server can assign IP settings to your clients on your network by adding a client's MAC address and the IP address to be assigned. Whenever the router receives a request from a client, the MAC address of that client is compared with the MAC address list present in the database. If an IP address is already assigned to that computer or device in the database, the customized IP address is configured otherwise an IP address is assigned to the client automatically from the DHCP pool.

To create DHCP reservations:

1. Click Network > LAN > LAN DHCP Reserved IPs.

D-Link Unified Services Route	r - DSR-1000N	Logged in as: admin ( ADMIN Serial: QB2B1A3000007	N)   Language: English [US] O Logout   Firmware: 1.108006E_WW   Wizard System Search. 9
🙆 Status	🛜 Wireless 📃 Network	🕼 VPN 🔒 Secu	rity 🗘 Maintenance
his page allows user to co eceive the same IP addres e assigned to the matchin AN DHCP Reserved IF	nfigure the reserved IP Addresses for the DR s when DHCP is enabled on the LAN, bind the g MAC address. 's List	ICP Server configuration.In order t b LAN device's MAC address to a pr	io ensure certain LAN devices always eferred IP address. This IP address will onl
Show 10 💌 entries	[Right click on record to get more options]		٩
Host Name	O MAC Address	0 IP Address	e Status e
	No data	available in table	
Showing 0 to 0 of 0 entries			First    Previous    Next >   Last >
Add New DHCP Reser	ved IP		

- 2. Click Add New DHCP Reserved IP.
- 3. Enter the following information and click **Save**.

Host Name		
IP Address		
MAC Address		
Associate with	OFF	
IP /MAC Binding		

Field	Description
Host Name	Enter a host name for this device. Do not use spaces.
IP Address	Enter the IP address you want to assign to this device. Note that this IP address must be in the same range as the starting/ending IP address under DHCP Settings.
MAC Address	Enter the MAC address of this device (xx:xx:xx:xx:xx:format). This is not case-sensitive.
Associate with IP/MAC Binding	Toggle <b>ON</b> to associate this device's information with IP/MAC binding.
Save	Click <b>Save</b> to save and activate your settings.

## **IGMP Setup**

Path: Network > LAN > IGMP Setup

IGMP snooping (IGMP Proxy) allows the router to 'listen' in on IGMP network traffic through the router. This then allows the router to filter multicast traffic and direct it only to hosts that need this stream. This is helpful when there is a lot of multicast traffic on the network where all LAN hosts do not need to receive this multicast traffic.

To enable IGMP Proxy:

- 1. Click **Network** > **LAN** > **IGMP Setup**.
- 2. Toggle *IGMP Proxy* to **On**.
- 3. Click Save.



### **UPnP Setup**

Path: Network > LAN > UPnP

Universal Plug and Play (UPnP) is a feature that allows the router to discover 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. If disabled, the router will not allow for automatic device configuration and you may have to manually open/forward ports to allow applications to work.

To configure the UPnP settings:

- 1. Click **Network** > **LAN** > **UPnP**.
- 2. Toggle *Activate UPnP* to **On**.
- 3. Select a VLAN from the LAN Segment drop-down menu.
- 4. Enter a value for *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.
- 5. Enter a value for *Advertisement Time to Live*. 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 a few number of switches.
- 6. Click Save.
- 7. Your entry will be displayed in the UPnP Port Map List. To edit or delete, right-click an entry and select the action from the menu. Repeat steps 2-6 to add multiple entries.

D-Link Unified Services Router - DSR-1000N			Logged in as: Serial: Q	Logged in as: admin ( ADMIN )   Language: English [US] O Logout Serial: Q8Z81A3000007   Firmware: 1.108006E_WW			
			🦮 Wizard System Search ۹				
🖾 Status	🛜 Wireless	Network	CB VPN	🔒 Security	O <sup>o</sup> Maintenance		
twork » LAN » UPnP					-	00	
ned without user interve reby don't require corres nP	ition. The UPnP Port A ponding application (p	Λap Table has the d ort forwarding) rule	etails of UPnP device as to be configured.	s that respond to the	router's advertisement	s, and	
IPnP Setup							
Activate UPnP		ION					
LAN Segment		VLAN1					
Advertisement Period	[	1800 [Range	e: 1 - 86400] Seconds				
Advertisement Time To	Live	4 [Rang	e: 1 - 2551 Hops				
	-						
		Save	Cancel				
JPnP Port Map List							
Show 10 - entries	[No right click option	s]				q	
Active O IP A	ddrost A	Protocol	A Internal Por	et A	External Port	9	
HUNNE ET IF P	0	No dat	a available in table	U. I.	and a second a second s	0	
Showing 0 to 0 of 0 entries					int   Previous Next	Last of	
					The second second second	The still	
# Jumbo Frames

Path: Network > LAN > Jumbo Frames

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.

To enable jumbo frames:

- 1. Click Network > LAN > Jumbo Frames.
- 2. Toggle Activate Jumbo Frames to **On**.
- 3. Click **Save**.

nified Services Router -	DSR-1000N		Serial: Q	8281A3000007   Firmw	are: 1.108006E_WW
🖾 Status	🛜 Wireless	📃 Network	CA VPN	Security	O° Maintenance
s page allows user to enab fic containing Jumbo Fram <b>mbo Frame</b>	le/disable jumbo fram nes on LAN side Device	es and set MTU for ju es.	mbo frames in the	router.Jumbo Frames	option is available to exchange
Activate Jumbo Frames		OK BT			
		Save	Cancel		

# VLAN

The router supports virtual network isolation on the LAN with the use of VLANs. LAN devices can be configured to communicate in a sub network 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 enabled 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.

# **VLAN Settings**

Path: Network > VLAN > VLAN Settings

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

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.

To create a new VLAN:

- 1. Click **Network** > **LAN** > **VLAN Settings**.
- 2. Click **Add New VLAN** at the bottom.
- 3. Enter the following required information from the table on the next page.

0						
<u>can</u> S	Status	🛜 Wireless	📃 Network	Ca VPN 🔒	Security 🗘 🗘	Maintenance
router support ined by VLAN ide AN List	s virtual netw entifiers. tries [Ri	ork isolation on th ight click on record to	e LAN with the use of get more options]	VLANs. LAN devices can be	configured to communi	icate in a subnetwork
ame Q VLA	AN ID \varTheta	IP Address	⊖ Subnet Mask	⊖ Captive Portal	⊖ Authenticati	ion Server
efault 1		192.168.10.1	255.255.255.0	Free	None	
	- Andrea				THE R. LANSING	

/LAN Configuration		X
VLAN ID	[Default: 1, Range: 2 - 4093]	
Name		
Captive Portal		
Captive Portal	OFF	
Activate InterVLAN Routing	OFF	
Multi VLAN Subnet		
IP Address		
Subnet Mask		
DHCP		
DHCP Mode	None O DHCP Server O DHCP Relay	
LAN Proxy		
Enable DNS Proxy	OFF	

Field	Description
VLAN ID	Enter a number between 2 and 4053.
Name	Enter a name for your VLAN.
Captive Portal	Toggle <b>ON</b> to enable Captive Portal (refer to the next page for more information).
Activate InterVLAN Routing	Toggle <b>ON</b> to allow routing between multiple VLANs or <b>OFF</b> to deny communication between VLANs.
IP Address	Enter the IP address for the VLAN.
Subnet Mask	Enter the subnet mask for the VLAN.
DHCP Mode	<ul> <li>Select one of the following modes:</li> <li>None - Turns off DHCP for your VLAN.</li> <li>DHCP Server (default) - The router will act as the DHCP server for your VLAN.</li> <li>DHCP Relay - DHCP clients on your VLAN will receive IP address leases from a DHCP server on a different subnet.</li> </ul>
Enable DNS Proxy	Toggle <b>ON</b> to enable the router to act as a proxy for all DNS requests and communicate with the ISP's DNS servers.
Save	Click <b>Save</b> to save and activate your settings.

#### **Captive Portal**

**Note:** The DSR-150/150N/250/250N routers do not have support for the Captive Portal feature. Captive Portal is available for LAN users only and not for DMZ hosts.

Captive Portals can be enabled on a per-VLAN basis. Hosts of a particular VLAN can be directed to authenticate via the Captive Portal, which may be a customized portal with unique instructions and branding as compared to another VLAN. The most critical aspect of this configuration page is choosing the authentication server. All users (VLAN hosts) that want to gain internet access via the selected Captive Portal will be authenticated through the selected server.

To enable Creative Portal to a specific VLAN:

- 1. Click **Network** > **LAN** > **VLAN Settings**.
- 2. Click Add New VLAN at the bottom or right-click an existing VLAN and select Edit.
- 3. Toggle *Captive Portal* to **ON**.
- 4. Next to Authentication Server, select an authentication server from the drop-down menu.
- 5. Next to *Login Profile Name*, select a profile from the drop-down or click **Create a Profile** to create a new one.
- 6. Select either HTTP or HTTPS for the redirect type.
- 7. If you want users to enter a CAPTCHA challenge at login, toggle to **ON**.
- 8. If you would like communication between VLANs, toggle Activate InterVLAN Routing to **ON**.
- 9. Make any other changes/selections and click **Save**.

aptive Portal	and the second s	
Captive Portal	DH TT	
Authentication Server	Local User Database	
Login Profile Name	default	Create a Profile
Redirect Type	HTTP O HTTPS	
Enable captcha challenge	OFF	
for login		
Activate InterVLAN	OFF	
Routing		

# Port/Wireless VLAN

Path: Network > VLAN Settings > Port VLAN

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

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**.

D-Link Unified Services Router - DSR-1000N					Logged in as: admin (ADMIN)   Language: English [US] O Logout Serial: QB2B1A3000007   Firmware: 1.10B006E_WW Wizard System Search ٩			
🙆 Status	<u>ې</u> ۷	/ireless	📮 Net	work	C VPN	Security	OP Maintenance	
Network » VLAN » Port VLAN This page allows user to config specific LAN port with a VLAN I that port and VLAN membership Port VLANs List	ure the p D, you c informa	oort VLANs. A an associate tion. Go to 1	A user can cl a VLAN to a the Available	noose port physical p VLAN page	ts and can add ort. The VLAN a to configure	them into a VLAN.In ord Port table displays the p a VLAN membership that	er to tag all traffic thro ort identifier, the mod can then be associated	ough a e setting for I with a port
								٩
Port Name	Q	Mode	θ	PVID	Θ	VLAN Membership		Ð
Port1		Access		1		1		
Port2		Access		1		1		
Port3		Access		1		1		
Port4		Access		1		1		
Showing 1 to 4 of 4 entries								
Wireless VLANs List								
							-	٩
Port Name	Ô	Mode	θ	PVID	Θ	VLAN Membership		θ
DSR-1000N_1		Access		1		1		
Test01		Access		1		1		
Showing 1 to 2 of 2 entries								

To edit, right-click on the port and select **Edit**. The edit page offers the following configuration options:

- Mode: The mode of this VLAN can be General, Access (default), or Trunk. Refer to the next page for more information on the different modes.
- Select PVID for the port when 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.

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.

Port VLAN Configuration

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.

For example, if Port 3 is a General port with PVID 3, then the 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.

*Note:* The DSR-150/150N do not support General mode due to hardware limitations.

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.



ort VLAN Configuration		0
Port Name	Port1	
Mode	General	
PVID	1 IDMANU 1, Damps 7, 40711	
/LAN Membership Configurat	ion	
YLAN Membership		
		Sitvo

# **Connect to the Internet**

This router has two WAN ports that can be used to establish a connection to the internet. 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.

# **Dynamic IP**

Path: Network > Internet > WAN1 Settings

Select **Dynamic IP** (DHCP) to obtain IP address information automatically from your Internet Service Provider.

								System Search.	. ૧
🖾 Status	🛜 Wireless	📃 Networ	k	C VPN			•	Maintenance	
twork » Internet » WAN1 Setti	ngs								0
is page allows you to set up yo	ur Internet connec	tion. Ensure tha	t you hav	ve the Interne	t connec	tion informat	ion such	as the IP Addres	sses,
count Information etc. This inf	ormation is usually (	provided by you	r ISP or r	network admin	istrator.				
v4 WAN1 Settings									
WAN1 Setup									
Connection Type	D	ynamic IP	F	•					
	_								
Dynamic IP (DHCP)	1			-					
nostnamo	-		_	_					
DNS Servers (Domain Name	System)	Got Dunamical	lu from 19	n @ 11co T	bace DN	Conver			
		oec bynamical	ty from t.	or e use i	nese pri	3 Servers			
Primary DNS Server	0	0.0.0							
Secondary DNS Server	0	0.0.0							
MAC Address									
MAC Address Source	C	Use Default M	AC O	Clone your PO	C's MAC	Use this	MAC		
MAC Address	Q	0:00:00:00:00:00							
Port Setup									
MTU Size	e	Default @	Custom						
	1	500 (Rai	nge: 1200 t	o 1500) Bytes					
Custom MTU									
Custom MTU	1.	1.0		-					

Field	Description
Host Name	Enter a host name if required by your ISP.
DNS Server Source	Select either <b>Get Dynamically from ISP</b> or <b>Use These DNS Servers</b> to manually enter DNS servers
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.
MAC Address Source	Select <b>Use Default MAC</b> to use the MAC address from the WAN1 port to associate with your modem/ISP, <b>Clone your PC's MAC</b> to use the MAC address of the computer you are currently using to associate with your modem/ISP, or <b>Use this MAC</b> to manually enter a MAC address.
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.
MTU Size	Select to use the default MTU value (1500) or select <b>Custom</b> to enter your own value.
Custom MTU	Enter a MTU value to optimize performance with your ISP.
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .
Save	Click <b>Save</b> to save and activate your settings.

# **Static IP**

Path: Network > Internet > WAN1 Settings

Select **Static IP** to manually enter the Internet settings supplied by your Internet Service Provider.

C20 Status	ኛ Wireless 📃 Network 👍 VPN 🗮 Security 🗭 Maintenance
twork » Internet » WAN1 Sett	lêz (
is page allows you to set up y	ur Internet connection. Ensure that you have the Internet connection information such as the IP Addresses
count Information etc. This in	ormation is usually provided by your ISP or network administrator.
v4 WAN1 Settings	
WAN1 Setup	
Connection Type	Static IP
connection Type	
Static IP	
IP Address	0.0.0.0
IP Subnet Mask	0.0.0
Gateway IP Address	0.0.0.0
Damain Nama Sustam (DNS	Former
Primary DNS Server	0.0.0 0
Secondary DNS Server	0.0.0.0
Secondary bits server	0.0.0.0
MAC Address	
MAC Address Source	U use Default MAC U Clone your PC's MAC Use this MAC
MAC Address	00:00:00:00:00
Port Setup	
	Default @ Custom
MTU Size	
MTU Size Custom MTU	1500 [Range: 1200 to 1500] Bytes

Field	Description
IP Address	Enter the IP address supplied by your ISP.
IP Subnet Mask	Enter the subnet mask supplied by your ISP.
Gateway IP Address	Enter the gateway IP address supplied by your ISP.
DNS Server Source	Select either <b>Get Dynamically from ISP</b> or <b>Use These DNS Servers</b> to manually enter DNS servers.
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.
MAC Address Source	Select <b>Use Default MAC</b> to use the MAC address from the WAN1 port to associate with your modem/ISP, <b>Clone your PC's MAC</b> to use the MAC address of the computer you are currently using to associate with your modem/ISP, or <b>Use this MAC</b> to manually enter a MAC address.
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.
MTU Size	Select to use the default MTU value (1500) or select <b>Custom</b> to enter your own value.
Custom MTU	Enter a MTU value to optimize performance with your ISP.
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .
Save	Click <b>Save</b> to save and activate your settings.

### PPPoE

Path: Network > Internet > WAN1 Settings

Select **PPPoE** to enter the PPPoE Internet settings supplied by your Internet Service Provider.

D-Link Unified Services Router - DSR 100	Logged In Jac. Jahnin ( KUMW )   Language: English (In)   Serbis: 0(22016/0700107   Firmware: 1 (1000662, WW	Inecut
🙆 Status 🛛 😤	Instess 🔜 Network 🖾 VPN 🔒 Security 📭 Maintenance	,
Network = Internet - WAN1 Settings	unet connection. Torure that you have the intercast connection information such as the IP Address on is county, avoided by your IC or generate administrates	<b>O</b> (
Pv4 WAN1 Settings		
WAH1 Setup		
Connection Type	₹₽₽₽aE	
PPPoE Profile Configuration Address Made	Dynamic IP     Static IP	
User Name	dink.	
Password		
Service	Sp 6-mail.	
Authentication Type	Auss-megolitate -	
Reconnect Mode	# Always On E On Domand	
Domain Name System (DNS) Serv DNS Server Source	rs ① Get Dynamically from ISP 🔹 Use These DNS Servers	
Primary DNS Server	0.0.0.0	
Secundary DNS Server	0.0.0.0	
MAC Address MAC Address Source	🗇 Use Defauls MAC 👘 Cloime your PCs MAC 🔎 Use this MAC	
MAL Address	00.00.00.06.00.00	
Port Setup MTU Size	B Default O Custom	
Port Speed	Auto Sense	
	Save	

Field	Description		
Address Mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).		
User Name	Enter your PPPoE user name.		
Password	Enter your PPPoE password.		
Service	Enter if your ISP requires it.		
Authentication Type	Select the authentication type from the drop-down menu.		
Reconnect Mode	Some ISPs may require you to pay for usage time. Select <b>On Demand</b> if this is the case. This will have the router connect to the Internet only when you initiate an Internet connection. Select <b>Always On</b> to have the router stay connected to the Internet.		
IP Address	If you selected Static IP, enter the IP address supplied by your ISP.		
IP Subnet Mask	If you selected Static IP, enter the subnet mask supplied by your ISP.		
Gateway IP Address	If you selected Static IP, enter the gateway IP address supplied by your ISP.		
DNS Server Source	Select either <b>Get Dynamically from ISP</b> or <b>Use These DNS Servers</b> to manually enter DNS servers.		
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.		
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.		
MAC Address Source	Select <b>Use Default MAC</b> to use the MAC address from the WAN1 port to associate with your modem/ISP, <b>Clone your PC's MAC</b> to use the MAC address of the computer you are currently using to associate with your modem/ISP, or <b>Use this MAC</b> to manually enter a MAC address.		
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.		
MTU Size	Select to use the default MTU value (1500) or select <b>Custom</b> to enter your own value.		
Custom MTU	Enter a MTU value to optimize performance with your ISP.		
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .		
Save	Click <b>Save</b> to save and activate your settings.		

### PPTP

Path: Network > Internet > WAN1 Settings

Select **PPTP** to enter the PPTP Internet settings supplied by your Internet Service Provider.

D-Link Unified Services Router - 058-000	Logged In as: Juliun ( ADAH)   Language: Konflich (m) ( Draymin Serial: Coldnis-Wood /   Firmware: 1, Lobolic, ww Serial: Coldnis-Wood /   Firmware: 1, Lobolic, ww Serial: Coldnis-Witzard (System Search
🙆 Status 🎅 (	Arcless 🗮 Network 🕼 (PH ) 🔒 Security 🗘 Malatomerice
Network - Internet - WAN1 Settings	0.0
This page allows you to set up your inte Account information etc. This informati	rnet connection. Ensure that you have the Internet connection information such as the IP Addresses, on is usually provided by your ISP or network administrator.
IPv4 WAN1 Settings	
WANT Setup	
Connection Type	PPTP .
PPTP Address Made	Cynamic IP     Static IP
Server Address	0.0,0,0
User Name	dini.
Password	*****
MPPE Encryption	TO
Split Tunnel	00
Reconnect Mode	· Atways On O On Demand
Domain Name System (DNS) Serve DNS Server Source	es ● Get Dynamically from ISP □ Use These DBS Servers
MAC Address	
MAC Address Source	Dise Default MAC D Clune your PC's MAC . Use this MAC
MAE Address	66,00,00,08,09,00
Port Setup	12 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
MTU Size	Default Custon
Eustom MTU	1500 [Ranger 1300 be 1500] Bytan
Port Speed	Auty Sense .
	Save

Field	Description		
Address Mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).		
Server Address	Enter your PPTP server address.		
User Name	Enter your PPTP user name.		
Password	Enter your PPTP password.		
MPPE Encryption	Toggle to <b>ON</b> and select the level of MPPE encryption.		
Split Tunnel	Toggle to <b>ON</b> to use split tunnelling. This will allow you to connect to a VPN and Internet using the same physical connection.		
Reconnect Mode	Some ISPs may require you to pay for usage time. Select <b>On Demand</b> if this is the case. This will have the router connect to the Internet only when you initiate an Internet connection. Select <b>Always On</b> to have the router stay connected to the Internet.		
IP Address	If you selected Static IP, enter the IP address supplied by your ISP.		
IP Subnet Mask	If you selected Static IP, enter the subnet mask supplied by your ISP.		
Gateway IP Address	If you selected Static IP, enter the gateway IP address supplied by your ISP.		
DNS Server Source	Select either Get Dynamically from ISP or Use These DNS Servers to manually enter DNS servers.		
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.		
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.		
MAC Address Source	Select Use Default MAC to use the MAC address from the WAN1 port to associate with your modem/ISP, Clone your PC's MAC to use the MAC address of the computer you are currently using to associate with your modem/ISP, or Use this MAC to manually enter a MAC address.		
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.		
MTU Size	Select to use the default MTU value (1500) or select <b>Custom</b> to enter your own value.		
Custom MTU	Enter a MTU value to optimize performance with your ISP.		
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .		
Save	Click <b>Save</b> to save and activate your settings.		

## L2TP

Path: Network > Internet > WAN1 Settings

Select **L2TP** to enter the L2TP Internet settings supplied by your Internet Service Provider.

D-Link Unified Services Router - Dier 10004	Cogged in as: Admin (ADMIN ) Language: English (US) () Theorem Sectal: Coggeta Scotter / Firmware: () Annows, you Share a state of the scotter of the state of the state of the scotter of
🖾 Status 🎅 Wieda	ss 🔄 Network 🖓 VPN 🖴 Security 🗢 Malittenance
Network - Internet - WANI Settings This page allows you to set up your Internet Account Information etc. This Information is IPv4 WANI Settings	onnection. Ensure that you have the Internet connection information such as the IP Addresses, usually provided by your ISP or network administrator.
WAN1 Satur	
Cannection Type	L2TF
LTTP Address Mode Server Address	# Dynamic IP ID Static IP [0.9.2.0
User Name	dink
Password	*****
Secret	[17 tornal
Split Tunnel	041
Reconnect Mode	· Always On O On Demand
Domain Name System (DNS) Servers DNS Server Source	🗢 Get Dynamically from ISP 🔹 Use These DHS Servers
Primary DHS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
MAC Address MAC Address Source	🗇 Use Default MAC 🗢 Clane your PC's MAC 🔹 Use this MAC
MAC Address	00.00.00.00.00
Port Setup MTU Size	· Default O Custom
Port Speed	Auta Sense
	Sava

Field	Description			
Address Mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).			
Server Address	Enter your PPTP server address.			
User Name	Enter your PPTP user name.			
Password	Enter your PPTP password.			
Secret	Enter a shared secret if required.			
Split Tunnel	Toggle to <b>ON</b> to use split tunnelling. This will allow you to connect to a VPN and Internet using the same physical connection.			
Reconnect Mode	Some ISPs may require you to pay for usage time. Select <b>On Demand</b> if this is the case. This will have the router connect to the Internet only when you initiate an Internet connection. Select <b>Always On</b> to have the router stay connected to the Internet.			
IP Address	If you selected Static IP, enter the IP address supplied by your ISP.			
IP Subnet Mask	If you selected Static IP, enter the subnet mask supplied by your ISP.			
Gateway IP Address	If you selected Static IP, enter the gateway IP address supplied by your ISP.			
DNS Server Source	Select either Get Dynamically from ISP or Use These DNS Servers to manually enter DNS servers.			
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.			
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.			
MAC Address Source	Select Use Default MAC to use the MAC address from the WAN1 port to associate with your modem/ISP, Clone your PC's MAC to use the MAC address of the computer you are currently using to associate with your modem/ISP, or Use this MAC to manually enter a MAC address.			
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.			
MTU Size	Select to use the default MTU value (1500) or select <b>Custom</b> to enter your own value.			
Custom MTU	Enter a MTU value to optimize performance with your ISP.			
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .			
Save	Click <b>Save</b> to save and activate your settings.			

# Japanese PPPoE

Path: Network > Internet > WAN1 Settings

Select Japanese PPPoE to enter the PPPoE Internet settings supplied by your Internet Service Provider.

State     S	D-Link	Kogged in as: Serial: 0	Copped in ac. admin ( 30540)   Language: Coptol (U) Serial: 00081.0000007   Firmware: (.100007, ww W Witawid   System Search   S				
Minute - Multi Setting:         This page allows you to not up your Internet connection. Information such as the IP Address         Access that normation +tc. This information is usually provided by your GP or network administrator.         IPv4 WANT Setting:         WANT Setting:         WANT Setting:         WANT Setting:         WANT Setting:         User Name         Japonese PPPoE         -Address Mode         Passend         Service         Automicision Tupe         Automicision Tupe <th></th> <th>😤 wweles</th> <th>Network</th> <th>C YPH</th> <th></th> <th>O<sup>o</sup> Maintenance</th> <th></th>		😤 wweles	Network	C YPH		O <sup>o</sup> Maintenance	
This sage allows you to any your internet cannet time. Source that you have the internet cannet time internet cannet the IP Address WAVE Setting:  WAVE Setting:  WAVE Setting:  WAVE Setting:  User Name  Autombic sites Type  Autombic sites  Autombic sites Type  Autombic sites  Autombic site	letwork - Internet - WA	il Settings					0
WANI Setting:         WANI Setting:         WANI Setting:         Sencetion Type         Japanese PPPOE         Address Mode         Duer Name         Passeriel         Service         Authenitication Type         Authenitication Type         Authenitication Type         Authenitication Type         Authenitication Type         Bis Server Source         Address Mode         Authenitication Type         Service         Authenitication Type         Authenitication Type         Authenitication Type         Authenitication Type         Authenitication Type         Descencer Mode         Secondary PPPOE Domain Name System (DMS) Servers         Dis Server Source       Northenitication Type         Daviantion Fremains Mane System (DMS) Servers <td< td=""><td>his page allows you to set</td><td>t up your Internet canne</td><td>ction. Insure that yo</td><td>a have the Interne</td><td>t connection informat</td><td>ion such as the IP Addres</td><td></td></td<>	his page allows you to set	t up your Internet canne	ction. Insure that yo	a have the Interne	t connection informat	ion such as the IP Addres	
WARI Serupi         Connection Type         Japanese PPPOE         Adverse Mode         Adverse Mode         Passord         Service         Service         Antonoginate         Primary PPOE Domain Name System (DNIS Servers)         Dissord         Dissord         Service         Adverse Source         Service         Adverse Source         Service         Service         Service         Adverse Source         Service	Pv4 WAN1 Settings	The Information is dealer	, promote al jour co	ar network down			
Sennettion Type     digenerse PPPGE       Japanese PPPGE        Adverse Mode        Duer Name        Passes        Passes        Service        Automotive Mode        Primary PPPGE Domain Name System (DMS) Servers        December Mode        Pairses        Primary PPPGE Domain Name System (DMS) Servers        December Mode        Service        Adverse Mode        Service        Adverse Mode        Service        Adverse Mode        Service        Automotive Mode        Service        Automotive Mode        Service        Dis Server Source        Service        Service        Service        Dis Server Source        Service        Dis Server Source        Secondary PPDeD Domain Name System (DHS) Servers       Mode Caddrests        Mode Caddrest        Mode Caddrests        Mode Caddrest <td>WANT Setup</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	WANT Setup						
Japanese PPDE Advess Wede	Connection Type		Japanese PPEoE	1.1			
Address Work Address Work Service Address Work Address Wo	Innanara DDDaF						
User Name Password Service Authentication Type Mathemication Type Service DMS Server Source Service Authonitication Type Authonitication Type Service Serv	Address Made		. Dynamic # 0 :	tatic IP			
Pasword Service Authentication Type Authentication Type Authentication Type Beconnect Mode Authentication Type Beconnect Mode Beconnect Beconnect Beconnect Mode Beconnect Becon	User Name		dire.				
Service  Authentication Tupe Beisoness Mode Beisone	Password						
Authentication Type Autorspitate  Reconnect Mode  Autorspitate  Reconnect Mode  Autorspitate  Reconnect Mode  Autorspitate  Auto	Service			Genne			
Always Color Conservers     Advances     Always Color Conservers     Advances     Adva	Authentication Type		Auto-mappible	-			
Primary PPPOE Domain Name System (DNS) Servers       DNS Server Source	Reconnect Mode		· Always On 12 0	n Demand			
In the provide a second system (Dec) 5 dec Opnamizable (runs 15P ) the These DNS Servers Secondary PPDeE Profile Configuration Address Mode   Dec Name  Personna  Personna Personna Personna Personna Personna Personna Personna Personna Personna Personna Personna Personna Personna Personna Personna Personn	Primary PDPoF Domai	n Nome Sustem (DMS)	Cerners				
Secondary PPPoE Profile Configuration Address Mode   Uner Name  Uner Name  Uner Name  Duer Name D	DNS Server Source	in House System Invest.	. Get Dynamically Ir	un tie 🗇 tim 1	bese DNS Servers		
Address Mode	Secondary PPPoE Proj	Ille Configuration					
Uner Name debit Pesremend debit Service Authenstication Type Automophies (Conservers) Reconnect Mode (Conservers) MAC Address MAC Address	Address Mode		# Dynamic IP 🔲 3	itatic IP			
Pesmand  Service  Automopolatis  Aut	User Name		diek				
Service Authentication Type Authentication Type Authentication Type Authentication Type Authentication Type Automotivation (IIII) Service (IIIII) Services (IIIII) Services (IIIIII) Services (IIIIIII) Services (IIIIIIIII) Services (IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Passeord						
Authentication Type Indonegolade Internet Mede Internet Mede Internet Mede Internet Mede Internet Mede Internet Mane System (DISS) Servers On Demand Secondary PPOE Domain Name System (DISS) Servers Internet Mac Address Internet	Service						
Reconnect Mode # Always On © On Dewand Secondary PPPOE Damain Name System (DIS) Servers DKS Server Source # Get Dynamically from ISP © Use These DHS Servers MAC Address MAC Address Source # Use Default MAC © Clone your PC's MAC © Use this MAC Port Secup	Authantication Type		Auto megoliate	-			
Secondary PPPOE Damain Name System (DNS) Servers DKS Server Source B Get Dynamically from ISP C Use These DHS Servers MAC Address MAC Address Source B Use Default MAC C Clone your PC's MAC D Use this MAC Port Secup	Reconnect Mode		· Always On 10 C	n Demand			
MAC Address MAC Address Une Default MAC Done your PC's MAC D Use the MAC Port Setud	Secondary PPPoE Dam DHS Server Source	aln Name System (DN)	S) Servers	um ISP E Use T	Hese DHS Servers		
Port Setup	MAC Address MAC Address Source		. Use Default MAT	O Clone your Pd	AMAE O Des This	MAE	
a state a state	Port Setup		a construction of the second				

Field	Description		
Address Mode	Select <b>Dynamic IP</b> or <b>Static IP</b> (IP settings supplied by your ISP).		
User Name	Enter your PPPoE user name.		
Password	Enter your PPPoE password.		
Service	Enter if your ISP requires it.		
Authentication Type	Select the authentication type from the drop-down menu.		
Reconnect Mode	Some ISPs may require you to pay for usage time. Select <b>On Demand</b> if this is the case. This will have the router connect to the Internet only when you initiate an Internet connection. Select <b>Always On</b> to have the router stay connected to the Internet.		
IP Address	If you selected Static IP, enter the IP address supplied by your ISP.		
IP Subnet Mask	If you selected Static IP, enter the subnet mask supplied by your ISP.		
Gateway IP Address	If you selected Static IP, enter the gateway IP address supplied by your ISP.		
Primary PPPoE DNS Servers	Select either <b>Get Dynamically from ISP</b> or <b>Use These DNS Servers</b> to manually enter DNS servers.		
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.		
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.		
Secondary PPPoE Profile	You may create a secondary PPPoE profile.		
MAC Address Source	Select <b>Use Default MAC</b> to use the MAC address from the WAN1 port to associate with your modem/ISP, <b>Clone your PC's MAC</b> to use the MAC address of the computer you are currently using to associate with your modem/ISP, or <b>Use this MAC</b> to manually enter a MAC address.		
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.		
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .		
Save	Click <b>Save</b> to save and activate your settings.		

### **Russian PPPoE**

Path: Network > Internet > WAN1 Settings

Select **Russian PPPoE** to enter the PPPoE Internet settings supplied by your Internet Service Provider.

D-Link Datied Services Rooter DSR-1000	Logged in as: minin (ADAUH)   Language: frightin [US] O Konsul Seriul: 0(201)/3000 // Firmwarg: (1100006.ww/ Witzurd Sythem Search. %			
🖾 Status 🔶 V	Troless 🔜 Network 🕼 VPN 🔒 Security 🗢 Maintenance			
Network - Internet - WAN1 Settings	0 0			
This page allows you to set up your inte Account Information etc. This information	rmmt connection. Ensure that you have the internet connection information such as the IP Addresses. on is usually provided by your ISP or network administrator.			
IPv4 WAN1 Settings				
WANT Setup				
Connection Type	Russian PPPoE			
Russian PFPoE Address Mode	🕷 Dynamic IV 🗇 Static IP			
User Name	dink			
Password				
Service	Cyptianal			
Authentication Type	Automegotiate			
Reconnect Made	always On Do On Demand			
Domain Name System (DNS) Serve DNS Server Source	rs 🗰 Get Dynamically from JSP 🔿 Use These DHS Servers			
MAC Address	W Has Balant Mart - D Province Mrs Mart - D Day Mrk Mar			
MAC Address source	a one denote wat to clame your he's wat to use the wat			
Address Made	E Dynamiz IP 🖾 Static IP			
WAN2 Physical Setting Damain Nat	me System			
DNS Server Source	Get Dynamically from ISP ID Use These DNS Servers			
Port Setup	and a state of the			
MID SIZe	e Default 🗊 Cuitom			
Purt Speed	Auto Sense			
	Save Cancel			

Field	Description		
Address Mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).		
User Name	Enter your PPPoE user name.		
Password	Enter your PPPoE password.		
Service	Enter if your ISP requires it.		
Authentication Type	Select the authentication type from the drop-down menu.		
Reconnect Mode	Some ISPs may require you to pay for usage time. Select <b>On Demand</b> if this is the case. This will have the router connect to the Internet only when you initiate an Internet connection. Select <b>Always On</b> to have the router stay connected to the Internet.		
IP Address	If you selected Static IP, enter the IP address supplied by your ISP.		
IP Subnet Mask	If you selected Static IP, enter the subnet mask supplied by your ISP.		
Gateway IP Address	If you selected Static IP, enter the gateway IP address supplied by your ISP.		
DNS Server Source	Select either Get Dynamically from ISP or Use These DNS Servers to manually enter DNS servers.		
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.		
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.		
MAC Address Source	Select <b>Use Default MAC</b> to use the MAC address from the WAN1 port to associate with your modem/ISP, <b>Clone your PC's MAC</b> to use the MAC address of the computer you are currently using to associate with your modem/ISP, or <b>Use this MAC</b> to manually enter a MAC address.		
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.		
WAN2 Physical Setting	Select <b>Dynamic IP</b> or <b>Static IP</b> (IP settings supplied by your ISP). If you select Static IP, enter the IP settings supplied by your ISP.		
WAN2 Physical DNS	Select either Get Dynamically from ISP or Use These DNS Servers to manually enter DNS servers.		
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .		
Save	Click <b>Save</b> to save and activate your settings.		

### **Russian PPTP**

Path: Network > Internet > WAN1 Settings

Select **Russian PPTP** to enter the PPTP Internet settings supplied by your Internet Service Provider.

D-Link Darred Nandces Router, 1958 (1980)	Logged in at: admin (allows)   Language: Anglinh (int) O Legison Secul: Collari Administr   Elementer: 1-) Imming_vice W Without System System System			
🙆 Status <table-cell> Ver</table-cell>	eless. 🗖 Network			O <sup>o</sup> Maintenance
etwork – Internet – WAN1 Settings				0
his page allows you to set up your intern	et connection, Ensure that yo	u have the Internet	connection Informat	ion such as the IP Addresses,
Pv4 WAN1 Settings				
WANI Setup				
Connection Type	Human Pete	1		
Russian PPTP Address Mode	· Dynamic IP	Statle IP		
Server Address	0.00.0			
User Hame	pith -			
Password				
MPPE Encryption	1000			
Split Tunnel	1000			
Reconnect Mode	# Always On D	Je Demand		
Domain Name System (DNS) Servers DNS Server Source	. Gat Dynamically (	rain ISP D Use T	Nase DHS Servers	
MAC Address Source	· Une Default MAC	Clame your PC		MAC
Port Setup MTU Size	· Default © Cus	ten		
Port Spend	Auto Serve			
	Sava	Cancel		

Field	Description		
Address Mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).		
Server Address	Enter your PPTP server address.		
User Name	Enter your PPTP user name.		
Password	Enter your PPTP password.		
MPPE Encryption	Toggle to <b>ON</b> and select the level of MPPE encryption.		
Split Tunnel	Toggle to <b>ON</b> to use split tunnelling. This will allow you to connect to a VPN and Internet using the same physical connection.		
Reconnect Mode	Some ISPs may require you to pay for usage time. Select <b>On Demand</b> if this is the case. This will have the outer connect to the Internet only when you initiate an Internet connection. Select <b>Always On</b> to have the router stay connected to the Internet.		
IP Address	If you selected Static IP, enter the IP address supplied by your ISP.		
IP Subnet Mask	If you selected Static IP, enter the subnet mask supplied by your ISP.		
Gateway IP Address	If you selected Static IP, enter the gateway IP address supplied by your ISP.		
DNS Server Source	Select either Get Dynamically from ISP or Use These DNS Servers to manually enter DNS servers.		
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.		
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.		
MAC Address Source	Select Use Default MAC to use the MAC address from the WAN1 port to associate with your modem/ISP, Clone your PC's MAC to use the MAC address of the computer you are currently using to associate with your modem/ISP, or Use this MAC to manually enter a MAC address.		
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.		
MTU Size	Select to use the default MTU value (1500) or select <b>Custom</b> to enter your own value.		
Custom MTU	Enter a MTU value to optimize performance with your ISP.		
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .		
Save	Click Save to save and activate your settings.		

# **Russian L2TP**

Path: Network > Internet > WAN1 Settings

Select **Russian L2TP** to enter the L2TP Internet settings supplied by your Internet Service Provider.

D-Link Unified Solvices Router - 05R-1000N			Logged In as: advin ( ADMA)   Langoage: English [US] () () () () () () () () () () () () ()			
🙆 Status	😤 Wireless	Retwork	A VPN	Security	O° Maintenance	
Network - Internet - WANT	iettings				90	
This page allows you to set u	your Internet conne	ection. Ensure that you	have the Interne	t connection informat	tion such as the IP Addresses,	
IPv4 WAN1 Settings						
WAN1 Setup						
Connection Type		Russian L2TP				
Durelan 13TD						
Address Mode		· Dynamic IP	itatic IP			
Server Address		0.0.0.0				
User Name		dick				
Password			-			
Secret			Deitauit			
5-111 T 1						
Spire Tunnel		- I der	Second Second			
Reconnect Mode		Always On C C	n Demand			
Domain Name System (D	NS) Servers	and the second second	and a second			
DNS Server Source		Get Dynamically fro	om ISP 🗈 Use 1	hese DNS Servers		
MAC Address						
MAC Address Source		B Use Default MAC	Clone your PC	TA MAC Use this	MAC	
Port Setup						
MTU Size		@ Default @ Cust	0 m			
Port Speed		Auto Sense	-			
		Save	Cancel			

Field	Description
Address Mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).
Server Address	Enter your PPTP server address.
User Name	Enter your PPTP user name.
Password	Enter your PPTP password.
Secret	Enter a shared secret if required.
Split Tunnel	Toggle to <b>ON</b> to use split tunnelling. This will allow you to connect to a VPN and Internet using the same physical connection.
Reconnect Mode	Some ISPs may require you to pay for usage time. Select <b>On Demand</b> if this is the case. This will have the router connect to the Internet only when you initiate an Internet connection. Select <b>Always On</b> to have the router stay connected to the Internet.
IP Address	If you selected Static IP, enter the IP address supplied by your ISP.
IP Subnet Mask	If you selected Static IP, enter the subnet mask supplied by your ISP.
Gateway IP Address	If you selected Static IP, enter the gateway IP address supplied by your ISP.
DNS Server Source	Select either Get Dynamically from ISP or Use These DNS Servers to manually enter DNS servers.
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.
MAC Address Source	Select Use Default MAC to use the MAC address from the WAN1 port to associate with your modem/ISP, Clone your PC's MAC to use the MAC address of the computer you are currently using to associate with your modem/ISP, or Use this MAC to manually enter a MAC address.
MAC Address	If you selected Use this MAC, enter the MAC address you want to associate with your ISP.
MTU Size	Select to use the default MTU value (1500) or select <b>Custom</b> to enter your own value.
Custom MTU	Enter a MTU value to optimize performance with your ISP.
Port Speed	Select a value from the drop-down menu. The default value is <b>Auto-Sense</b> .
Save	Click Save to save and activate your settings.

# WAN2 Settings

Path: Network > Internet > WAN2 Settings

Select **WAN** and select the Internet connection type. Please refer to the previous pages (41-49) for more information. If you want to set WAN2 port to **DMZ**, skip to the next page.

#### WAN

D-Linč Unified Services Router - DSR-1000N			Logged in as: admin ( ADMIN )   Language: English [US] O Logout Serial: Q8281A3000007   Firmware: 1.108006E_WW Wizard System Search ۹		
🙆 Status	🛜 Wireless	📃 Network	CA VPN	Security	O° Maintenance
etwork » Internet » WAN2	DMZ Setting				0
ns page allows you to set u count Information etc. Thi	your internet connet information is usually g	rton. Ensure that yo provided by your ISP	or network admini	strator.	on such as the IP Addresses,
Configurable Port Setup					
Configurable Port		WAN ODMZ			
WANZ Setup					
Connection Type	[	Dynamic IP			
Dynamic IP (DHCP)					
Host Name	[		Optional		
DNS Servers (Domain No	me System)				
DNS Server Source		<ul> <li>Get Dynamically fr</li> </ul>	om ISP 🔘 Use T	hese DNS Servers	
MAC Address					
MAC Address Source		Use Default MAC	Clone your PC	"s MAC 💿 Use this	MAC
Port Setup					
MTU Size		🖲 Default 🔘 Cus	tom		
Port Speed	F	Auto Sense			
		Save	Cancel		

# DMZ

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 sub network 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.

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.

**Note:** For the DSR-500N and 1000N, in order to configure a DMZ port, the router's configurable port must be set to DMZ in the **Network** > **Internet** > **DMZ Settings** page.

1. Click Network > Internet > WAN2 / DMZ Settings.



2. Select **DMZ** and click **Save**.

# WAN3 (3G Internet)

Path: Network > Internet > WAN3 Settings

This router supports the use of 3G Internet access. Cellular 3G internet access is available on WAN3 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 > WAN3 Status) and Enable the WAN3 link to establish the 3G connection.

*Note:* A 3G USB modem can be configured as the third WAN in DSR-1000 and DSR- 1000N.

		Wizard System Search 🤗			
🙆 Status 🛜 Wireless	📃 Network	CA VPN	Security	© Maintenance	
work » Internet » WAN3 Settings					0
AN3 Settings					
NAN3 (3G Internet)					
Reconnect Mode	C Always On 🔍 On Der	mand			
Maximum Idle Time	5. [Range: 1 - 99	991			
3G Internet Connection Type					
User Name		Optional			
Password		Dptional			
Dial-In Number	*99#				
Authentication Protocol	None	•			
APN Required	04				
APN	wap.isp.com				
Domain Name System (DNS) Servers					
DNS Server Source	© Get Dynamically from I	SP   Use Thes	e DNS Servers		
Primary DNS Server	0.0.0.0				
Secondary DNS Server	0.0.0.0				
Port Setup					
MTU Size	🗇 Default 🔍 Custom				
	4500				

Field	Description
Reconnect Mode	Some ISPs may require you to pay for usage time. Select <b>On Demand</b> if this is the case. This will have the router connect to the Internet only when you initiate an Internet connection. Select <b>Always On</b> to have the router stay connected to the Internet.
Maximum Idle Time	Enter the idle time in minutes before the router disconnects from the Internet (On Demand only).
User Name	Enter your 3G account user name.
Password	Enter your 3G account password.
Dial-in Number	Enter the phone number to access your Internet.
Authentication Protocol	Select one of following protocols from the drop-down menu: None, PAP or CHAP.
APN Required	Toggle to ON if your ISP requires APN to connect.
APN	Enter the APN (Access Point Name) provided by the ISP.
DNS Server Source	Select either Get Dynamically from ISP or Use These DNS Servers to manually enter DNS servers.
Primary DNS Server	If you selected "Use These DNS Servers", enter the primary DNS server IP address.
Secondary DNS Server	If you selected "Use These DNS Servers", enter the secondary DNS server IP address.
MTU Size	Select to use the default MTU value (1500) or select <b>Custom</b> to enter your own value.
Custom MTU	Enter a MTU value to optimize performance with your ISP.

# WAN Mode

Path: Network > Internet > WAN Mode

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.

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.

# **Single WAN Port**

If you do not want to use Auto Failover or Load Balancing, select **Single WAN Port** from the *WAN Mode* drop-down menu and select the WAN port you want to set. Click **Save**.



### Auto-Rollover using WAN IP

In this mode one of your WAN ports is assigned as the primary internet link for all internet traffic and 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.

1. Click Network > Internet > WAN Mode.

D-Link Unified Services Router - DSR-1000N	Logged in as: admin ( ADMIN )   Language: English [US] O Logout Serial: QB2B1A3000007   Firmware: 1.106006E_WW Wizard System Search. Q			
🖾 Status 🛜 Wi	reless 📃 Network	CAS VPN	Security	O° Maintenance
letwork » Internet » WAN Mode				0 0
ot excessively overloaded. Auto-Rollover /ption fails for any reason. VAN Mode	uses a backup link to preserve	nternet connecti	vity for the LAN if the	e main ISP configured on the primar
WAN Mode Setup				
WAN Mode	Auto-Rollover Using WAN	Pd		
WAN Mode Auto-Rollover using WAN Port Use Primary WAN Port	Auto-Rollover Using WAN     WAN1	Ø WAN3		
WAN Mode Auto-Rollover using WAN Port Use Primary WAN Port Use Secondary WAN port	Auto-Rollover Using WAN WAN1 © WAN2 WAN2	© WAN3		
WAN Mode Auto-Rollover using WAN Port Use Primary WAN Port Use Secondary WAN port WAN health check	Auto-Rollover Using WAN WAN1 © WAN2 WAN2 DNS Servers	© WAN3		
WAN Mode Auto-Rollover using WAN Port Use Primary WAN Port Use Secondary WAN port WAN health check WAN1	Auto-Rollover Using WAN              WAN1          WAN2          UNS Servers	P WAN3		
WAN Mode Auto-Rollover using WAN Port Use Primary WAN Port Use Secondary WAN port WAN health check WAN1 Retry Interval is	Auto-Rollover Using WAN WAN1 © WAN2 WAN2 DNS Servers	P(x) © WAN3 x  10, Range: 5 - 999] Set	conds	

2. Complete the fields from the table below and click **Save**.

Field	Description
WAN Mode	Select Auto-Rollover Using WAN IP from the drop-down menu.
Use Primary WAN Port	Select which WAN port is the primary.
Use Secondary WAN Port	Select which port to use if the primary port fails.
WAN Health Check	<ul> <li>DNS lookup using WAN DNS Servers: DNS Lookup of the DNS Servers of the primary link is used to detect primary WAN connectivity.</li> <li>DNS lookup using DNS Servers: DNS Lookup of the custom DNS Servers can be specified to check the connectivity of the primary link.</li> <li>Ping these IP addresses: These IP's will be pinged at regular intervals to check the connectivity of the primary link.</li> <li>Retry Interval is: The number tells the router how often it should run the above configured failure detection method.</li> <li>Failover after: This sets the number of retries after which failover is initiated.</li> </ul>
WAN1/WAN2/WAN3	Enter the DNS server or IP address to ping.
Retry Interval	Enter the time in seconds to initiate the WAN health check. Default is every 30 seconds.
Failover After	Enter the number of failures before the router will enable the failover process.

*Note:* The DSR-1000, DSR-1000N, DSR-500, DSR-500N, DSR-250, DSR-250N, DSR-150, and DSR-150N routers support 3G USB Modem as a failover link when the internet access is lost.

# Load Balancing

Path: Network > Internet > WAN Mode

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.

This router currently supports 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.

**Spillover:** If Spillover method is selected, the primary WAN acts as a dedicated link until a defined bandwidth threshold are reached. After this, the secondary WAN will be used for new connections. Inbound connections on the secondary WAN are permitted with this mode, as the spillover logic governs outbound connections moving from the primary to secondary WAN. You can configure spillover mode by using following options:

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

If the link bandwidth of outbound traffic goes above the load tolerance value of max bandwidth, the router will spillover the next connections to secondary WAN.

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

*Note:* The DSR-1000, DSR-1000N, DSR-500, and DSR-500N routers support the traffic load balancing between physical WAN port and a 3G USB Modem.

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.

#### **Round Robin**

1. Click **Network** > **Internet** > **WAN Mode**.

D-Link Unified Services Router - DSR-1000N		Logged in as: admin ( ADMIN )   Language: English [US] O Logout Serial: QB2B1A3000007   Firmware: 1.10B006E_WW Wizard System Search. 9.			Logout Q	
🖾 Status	🛜 Wireless	🖳 Network	CAS VPN	Security	O <sup>o</sup> Maintenance	
This page allows user to conf router to access the internet not excessively overloaded. A Option fails for any reason.	ope igure the policies on th t. Load balancing allows uuto-Rollover uses a bac	te two WAN ports fo traffic to and from kup link to preserve	r Internet connect the internet to be internet connecti	ion.By configuring bol shared across both c vity for the LAN if the	h WANs, there are two wa onfigured links to ensure c main ISP configured on th	ys for the one ISP is e primary
WAN Mode						
WAN Mode Setup	L	oad Balancing	•			
Load Balancing Setup						
Load Balancing	(6	Round Robin	Spillover Mode			
WAN health check	٨	lone				
		Save	Cancel			

Field	Description
WAN Mode	Select Load Balancing from the drop-down menu.
Load Balance	Select Round Robin.
WAN Health Check	<ul> <li>DNS lookup using WAN DNS Servers: DNS Lookup of the DNS Servers of the primary link is used to detect primary WAN connectivity.</li> <li>DNS lookup using DNS Servers: DNS Lookup of the custom DNS Servers can be specified to check the connectivity of the primary link.</li> <li>Ping these IP addresses: These IP's will be pinged at regular intervals to check the connectivity of the primary link.</li> <li>Retry Interval is: The number tells the router how often it should run the above configured failure detection method.</li> <li>Failover after: This sets the number of retries after which failover is initiated.</li> </ul>
Save	Click to save and activate your settings.

### Spillover

1. Click **Network** > **Internet** > **WAN Mode**.

D-Link Unified Services Rauter - DSR-1000N		Logged in as Serial: (	Logged in as: admin ( ADMIN )   Language: English [US] () Logout Serial: QB2B1A3000007   Firmware: 1.108006E_WW Wizard System Search. Q		
🙆 Status	🛜 Wireless	🖳 Network	CA VPN	Security	🗘° Maintenance
Network » Internet » WAN M Ihis page allows user to conf outer to access the internet not excessively overloaded. A Option fails for any reason.	ode igure the policies on t t. Load balancing allow uto-Rollover uses a ba	he two WAN ports 's traffic to and fr ckup link to prese	for Internet connec om the internet to be rve internet connect	tion.By configuring bot e shared across both cr ivity for the LAN if the	h WANs, there are two ways for the onfigured links to ensure one ISP io main ISP configured on the primar
AN Mode					
WAN Mode Setup	-				
WAN Mode		Load Balancing			
Load Balancing Setup					
Load Balancing		C Round Robin	Spillover Mode		
WAN health check		WAN DNS Servers	•		
Retry Interval is	[	30 (Defa	ult: 30, Range: 5 - 999] Se	aconds	
Failover After	E	4 [Defa	ult: 4, Range: Z - 999] Fai	lures	
Spillover Configuration	Setup				
Load Tolerance	[	80 [Defa	ult: 80, Range: 20 - 80]		
Max Bandwidth	Ē	8192 [Defa	ult: 8192, Range: 512 - 61	92]	
	10	Save	Cancel		

Field	Description
WAN Mode	Select Load Balancing from the drop-down menu.
Load Balance	Select <b>Spillover Mode</b> .
WAN Health Check	<ul> <li>DNS lookup using WAN DNS Servers: DNS Lookup of the DNS Servers of the primary link is used to detect primary WAN connectivity.</li> <li>DNS lookup using DNS Servers: DNS Lookup of the custom DNS Servers can be specified to check the connectivity of the primary link.</li> <li>Ping these IP addresses: These IP's will be pinged at regular intervals to check the connectivity of the primary link.</li> <li>Retry Interval is: The number tells the router how often it should run the above configured failure detection method.</li> <li>Failover after: This sets the number of retries after which failover is initiated.</li> </ul>
Retry Interval is	Enter the time in seconds to initiate the WAN health check. Default is every 30 seconds.
Failover After	Enter the number of failures before the router will enable the failover process.
Load Tolerance	Enter the percentage of bandwidth after which the router switches to the secondary WAN.
Max Bandwidth	This sets the maximum bandwidth tolerable by the primary WAN for outbound traffic.
Save	Click to save and activate your settings.

## **Routing Mode**

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.

#### **NAT or Classical**

Path: Network > Internet > Routing Mode

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

NAT is a technique which allows several computers and devices on your local network 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/devices that connect through the router will need to be assigned IP addresses from a private subnet.

1. Click Network > Internet > Routing Mode.



Field	Description
Routing Settings	Select NAT or Classical.
NAT with WAN1	Toggle to <b>ON</b> to use NAT with WAN1 or <b>OFF</b> for classical.
NAT with WAN2	Toggle to <b>ON</b> to use NAT with WAN2 or <b>OFF</b> for classical.
Save	Click to save and activate your settings.

#### Transparent

When Transparent Routing Mode is enabled, NAT is not performed on traffic between the LAN and WAN interfaces. 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.

**Note:** NAT routing has a feature called "NAT Hair -pinning" that allows internal network users on the LAN and DMZ to access internal servers (e.g., 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.

1. Click **Network** > **Internet** > **Routing**.

D-Link Unified Services Router - DSR-1000N		Logged in as: admin (ADMIN)   Language: English [US] Logout Serial: QB2B1A3000007   Firmware: 1.108006E_WW Wizard System Search. 9.		
🙆 Status 🛜	Wireless 📃 Network	CA VPN	Security	Ø <sup>o</sup> Maintenance
Network » Internet » Routing This page allows user to configure di handled when received on one physi addresses from internet devices. Tra Routing Mode	ifferent routing modes like NAT, Class cal interface. NAT is the most commo nsparent mode does not perform NAT	sical Routing and T on application for T and lets you bric	Transparent.The Routi most routers, and allo ge traffic between th	In the second
Routing Settings Routing Settings	NAT or Classical	Transparent	🔊 Bridge	
	Jave	Gancer		

Field	Description
Routing Settings	Select <b>Transparent</b> .
Save	Click to save and activate your settings.

#### Bridge

When Bridge Mode routing is enabled, the first physical LAN port and secondary WAN/DMZ (port 2) interfaces are bridged together at Layer 2, creating an aggregate network. The other LAN ports and the primary WAN (WAN1) are not part of this bridge, and the router asks as a NAT device for these other ports. With Bridge mode for the LAN port 1 and WAN2/DMZ interfaces, L2 and L3 broadcast traffic as well as ARP / RARP packets are passed through. When WAN2 receives tagged traffic the tag information will be removed before the packet is forwarded to the LAN port 1 interface.

Note: Bridge mode option is available on DSR-500/500N/1000/1000N routers only.

1. Click **Network** > **Internet** > **Routing**.

Unified Services Router - DSR-1000N		Logged in as: Serial: Q	admin ( ADMIN )   La 18281A3000007   Firmw	nguage: English [US] () Logout are: 1.108006E_WW /izard () System Search. 9,
🙆 Status 🛜 Wire	eless 📃 Network	CAS VPN	Security	OP Maintenance
twork » internet » kouting is page allows user to configure differen indled when received on one physical int idresses from internet devices. Transpare outling Mode	nt routing modes like NAT, Clas terface. NAT is the most comm ent mode does not perform NA	sical Routing and T on application for T and lets you brid	fransparent.The Routi most routers, and allo Ige traffic between th	ng mode determines how traffic is ws you to hide internal LAN IP e LAN and Option.
acing mode				
Routing Settings Routing Settings	NAT or Classical	C Transparent	Bridge	
Routing Settings Routing Settings Bridge Mode Setup	MAT or Classical	© Transparent	Ø Bridge	
Routing Settings Routing Settings Bridge Mode Setup Bridge Interface IP Address	NAT or Classical 0.0.0	© Transparent	Bridge	
Routing Settings Routing Settings Bridge Mode Setup Bridge Interface IP Address DMZ interface IP Address	NAT or Classical 0.0.0.0 172.17.100.254	C Transparent.	Bridge	
Routing Settings Routing Settings Bridge Mode Setup Bridge Interface IP Address DMZ interface IP Address Subnet Mask	<ul> <li>NAT or Classical</li> <li>0.0.0.0</li> <li>172.17.100.254</li> <li>255.255.255.255</li> </ul>	C Transparent	Bridge	
Routing Settings Routing Settings Bridge Mode Setup Bridge Interface IP Address DMZ interface IP Address Subnet Mask NAT vs Classical routing for each W. NAT with WAN1	<ul> <li>NAT or Classical</li> <li>0.0.0.0</li> <li>172.17 100.254</li> <li>255.255.255</li> <li>255</li> </ul>	Transparent.	Bridge	

Field	Description
Routing Settings	Select <b>Bridge</b> .
Bridge Interface IP Address	Enter the bridge interface IP address.
DMZ Interface IP Address	Enter the DMZ interface IP address.
Subnet Mask	Enter the subnet mask.
NAT with WAN1	Toggle <b>ON</b> to turn NAT on WAN1 or <b>OFF</b> for classical.
Save	Click to save and activate your settings.

# **IP Aliasing**

Path: Network > Internet > IP Aliasing

A single WAN Ethernet port can be accessed via multiple IP addresses by adding an alias to the port. This is done by configuring an IP Alias address. To edit or delete any existing aliases, right-click the alias and select either **Edit** or **Delete**.

To create a new alias:

1. Click **Network** > **Internet** > **IP Aliasing**.

						lizard System Search	٩
		😤 Wheless	Network	C VPN	Security	© Maintenance	
		ina					0 (
twork = Intern	er = ir anos						1000
twork = Intern is page displays n be accessed	s the configu	red IP Allases on Opt P addresses by addin	tion interfaces . User c g a alias to the port. T	an also add, delet his is done by con	e and edit the IP Alias figuring IP Alias.	s also.A single Option Ethe	ernet po
twork = Intern is page displays n be accessed Alliasing Lis	et = 10 Anas s the configu via multiple   t	red IP Allases on Op P addresses by addin	tion interfaces . User c g a allas to the port. T	an also add, delet his is done by con	e and edit the IP Allas figuring IP Alias.	s also.A single Option Ethe	ernet po
twork = Intern is page displays be accessed Aliasing Lis how 10 • #	et = P Allas s the configu via multiple   t mtries	ired IP Allases on Op Addresses by addin [Right click on record t	tion interfaces . User c g a alias to the port. T o get more options]	an also add, delet his is done by con	e and edit the IP Alias figuring IP Alias.	s also.A single Option Ethe	ernet po
twork = Intern is page displayin the accessed Aliasing Lis how 10 + a	et - P Anas s the configu via multiple   t mbries	red IP Allases on Op P addresses by addin [Right click on record t IP Address	tion interfaces . User c g a allas in the port. T w get more options]	an also add, delet his is done by con B Sub	e and edit the IP Alias figuring IP Alias. net Mask	s also. A single Option Ethe	ernet po
twork = Intern is page displays her accessed Aliasing Lis how 10 (*) = fort	et = P allos s the configu via multiple   st mtries	red IP Allases on Op P addresses by addin (Right click on record t IP Address	tion interfaces . User c g a alias in the port. T w get more options] No data ev	an also add, delet his is done by con e Sub allable in table	e and edit the IP Alias figuring IP Alias. net.Mask	s also. A single Option Ethe	ernet po

- 2. Click Add New IP Aliasing.
- 3. Enter the following information and click **Save**.

Aliasing Configuration		
Interface IP Address Subnet Mask	WAN1     WAN2	

Field	Description
Interface	Select either WAN1 or WAN2.
IP Address	Enter an alias IP address for the WAN interface you selected.
Subnet Mask	Enter a subnet mask for the WAN interface you selected.
Save	Click to save and activate your settings.

# **DMZ Settings**

Path: Network > Internet > DMZ Settings

If you set WAN2 port to DMZ, you will need to configure the port here.

To configure the DMZ Settings:

1. Click Network > Internet > DMZ Settings.

Unified Services Router - DSR	8-1000N		Logged in as: Serial: Q	admin ( ADMIN )   La 8281A3000007   Firmw \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	nguage: English [US] () are: 1.108006E_WW izard System Search	Logout
🖾 Status	🕈 Wireless	📃 Network	C VPN	Security	O <sup>o</sup> Maintenance	
etwork » Internet » DMZ Setting:	5	-				0
ost servers and give public access he LAN, and firewall/VPN policies hternet, such as FTP or mail serve	s to them.DMZ setup s can be customized ers.	on compared to the o is similar to the LAI for the DMZ. The DM	A TCP/IP options. Z is typically use	The network subnet d for network device:	of the DMZ can be diffe for the DMZ can be diffe that you wish to expose	e used rent fro to the
DMZ IP Address						
IP Address	172	2.17.100.254				
Subnet Mask	255	5.255.255.0				
DHCP for DMZ						
DHCD Made	0	None () DHCP Se	rver O DHCP	Relay		
DHCF MODE						
Starting IP Address	172	2.17.100.100				
Starting IP Address	172	2.17.100.100	=			
Starting IP Address Ending IP Address Default Gateway	172 172 172	2.17.100.100 2.17.100.253 2.17.100.254	3			
Starting IP Address Ending IP Address Default Gateway Domain Name	172 172 172 DLi	2.17.100.100 2.17.100.253 2.17.100.254 ink				
Starting IP Address Ending IP Address Default Gateway Domain Name Lease Time	172 172 172 172 172 172 172 172 172	2.17.100.100 2.17.100.253 2.17.100.254 ink [Range: 1 -	262800) Hours			
Starting IP Address Ending IP Address Default Gateway Domain Name Lease Time Enable DNS Proxy	172 172 172 172 172 172 172 172	2.17.100.100 2.17.100.253 2.17.100.254 ink [Range: 1 -	262800] Hours			
Starting IP Address Ending IP Address Default Gateway Domain Name Lease Time Enable DNS Proxy Primary DNS Server	172 172 172 DL 24	2:17.100.100 2:17.100.253 2:17.100.254 mk [Range: 1 -	262800] Hours			
Starting IP Address Ending IP Address Default Gateway Domain Name Lease Time Enable DNS Proxy Primary DNS Server Secondary DNS Server	172 172 172 174 174 174 174	2:17.100.100 2:17.100.253 2:17.100.254 mk [Range: 1 -	262800) Hours			

Field	Description
IP Address	Enter an IP address for the DMZ interface.
Subnet Mask	Enter the subnet mask for the DMZ interface.
DHCP Mode	<ul> <li>Select one of the following modes:</li> <li>None - Turns off DHCP.</li> <li>DHCP Server (default) - The router will act as the DHCP server on your network.</li> <li>DHCP Relay - DHCP clients on your network will receive IP address leases from a DHCP server on a different subnet.</li> </ul>
DHCP Server	Refer to "DHCP Server" on page 19 for more information.
DHCP Relay	Refer to "DHCP Relay" on page 20 for more information.
Enable DNS Proxy	Toggle to <b>On</b> to manually enter DNS and/or WINS server IP address(es). If set to <b>Off</b> , your router's LAN IP address will be assigned the DNS server to your clients and the router will get the DNS information from your ISP.
Primary DNS Server	If DNS Proxy is set to ON, enter the primary DNS server IP address.
Secondary DNS Server	If DNS Proxy is set to ON, enter the secondary DNS server IP address.
WINS Server	If DNS Proxy is set to ON, enter the WINS server IP address.
Save	Click to save and activate your settings.

#### DMZ LAN DHCP Reserved IPs

The router's DHCP server can assign IP settings to your DMZ clients on your network by adding a client's MAC address and the IP address to be assigned. Whenever the router receives a request from a client, the MAC address of that client is compared with the MAC address list present in the database. If an IP address is already assigned to that computer or device in the database, the customized IP address is configured otherwise an IP address is assigned to the client automatically from the DMZ DHCP pool.

To create DHCP reservations:

1. Click Network > Internet > DMZ LAN DHCP Reserved IPs.

					Wizard	System Search	٩
🖾 Status	🛜 Wireless	📃 Network	CAS VPN	Security	0°	Maintenance	
stwork » Internet » DMZ is page allows user to co	DHCP Reserved IPs	Addresses for the DHC	P Server configur	ation.In order to ens	ure certain	DMZ devices alv	🕜 🤇
twork » Internet » DMZ is page allows user to co ceive the same IP address ly be assigned to the mai MZ DHCP Reserved IF how 10 • entries	DHCP Reserved IPs nfigure the reserved IP A s when DHCP is enabled a tching MAC address. Ps List [Right click on record to	Addresses for the DHC on the DMZ, bind the get more options]	P Server configur DMZ device's MAC	ation.In order to ens address to a prefer	ure certain red IP addre	DMZ devices alv ss. This IP addre	(2) (2 ways ess will
twork » Internet » DMZ is page allows user to co ceive the same IP address (ly be assigned to the main MZ DHCP Reserved IF how 10 • entries	DHCP Reserved IPs nfigure the reserved IP A s when DHCP is enabled o tching MAC address. Ps List [Right click on record to	Addresses for the DHC on the DMZ, bind the get more options]	P Server configur. DMZ device's MAC	ation.In order to ens address to a prefer	ure certain red IP addre	DMZ devices alv	Image: ways     ess will
twork » Internet » DMZ is page allows user to co ceive the same IP address (y be assigned to the main MZ DHCP Reserved IF how 10 • entries P Address	DHCP Reserved IPs nfigure the reserved IP / when DHCP is enabled of kching MAC address. Ps List [Right click on record to	Addresses for the DHC on the DMZ, bind the get more options] MAC Address	P Server configur DMZ device's MAC	ation.In order to ens address to a prefer	ure certain red IP addre	DMZ devices alv	ays ess will

- 2. Click Add New DMZ DHCP Reserved IP.
- 3. Enter the following information and click **Save**.

DMZ DHCP Reserved IPs Con	figuration	$\bigotimes$
DMZ DHCP Reserved IP Enable IP Address MAC Address		
		Save

Field	Description
DMZ DHCP Reserved IP Enable	Toggle to <b>ON</b> to enable this reservation.
IP Address	Enter the IP address you want to assign to this device. Note that this IP address must be in the same range as the starting/ending IP address under DHCP Settings.
MAC Address	Enter the MAC address of this device (xx:xx:xx:xx:xx format).
Save	Click <b>Save</b> to save your reservation.

# **Dynamic DNS Settings**

Path: Network >	Internet >	Dynamic DN	٩S
-----------------	------------	------------	----

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.

To configure DDNS:

- 1. Click **Network** > **Internet** > **Dynamic DNS**
- 2. Click the tab on top to select which WAN port you want to configure DDNS to.
- 3. Next to Dynamic DNS Service Type, select your DDNS service.

D-Link Inified Services Router - DSR-	1000N	Logged in as: Serial: QB	admin ( ADMIN )   La 281 A 3000007   Firmv	vare: 1.108006E_WW	) Logout
🖾 Status	Wireless 📃 Network	CA VPN	Security	Vizard System Search.	
twork » Internet » Dynamic DNS	» Dynamic DNS WAN1 Settings				00
Dynamic DNS WAN1 Settings	Dynamic DNS WAN2 Settings Dyna	amic DNS WAN3 Set	tings		_
namic DNS (DDNS) is an Internet : NS, you must setup an account v	service that allows routers with varyin with a DDNS provider such as DynDNS.c	ng public IP addresse com, DlinkDDNS.com (	s to be located usin or Oray.net.	ıg İnternet domain names.	. To use
namic DNS WAN1 Settings					
WAN Mode					
Current WAN Mode	use only single WAN po	ort WAN1			
VANT					
Dynamic DNS Service Type	DynDNS ORA	Y O DLINKDONS	O None		
User Name					
Domain Name					
Status					
	1				
Password					
Password	orr				
Password Allow Wildcards	OFF				
Password Allow Wildcards Update Periodically	OFF 30 Days				
Password Allow Wildcards Update Periodically	OFF 30 Days	Consel			

4. Enter the following information and click **Save**. The information below is for DynDNS. Other services will have similar fields.

Field	Description
User Name	Enter your DDNS user name.
Domain Name	Enter the domain name.
Password	Enter your DDNS password.
Status	Displays the current connection status.
Allow Wildcards	Toggle to <b>ON</b> to allow wildcards.
Update Periodically	Toggle to <b>ON</b> to set a forced update.
Save	Click <b>Save</b> to save your reservation.

### Traffic Management Bandwidth Profiles

Path: Network > Internet > 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.

To edit, delete, or create a new bandwidth profile:

- 1. Click Network > Internet > Traffic Management > Bandwidth Profiles.
- 2. Toggle Enable Bandwidth Profiles to ON and click Save.



3. Click Add New Bandwidth Profile.

hilled Sinylans Ra	otel (159) 1000N		serial: Uni	BLA3000007   Firmw	are: ).TIMODIC_WY	
	n 🛜 Wireless	Network	CD VPH	A Security	O <sup>o</sup> Maintenance	
work - Internet -	Traffic Management - Randwid	th Profiles				0
	-	Operati	m Succeeded	-		
Eandwidth Profile	Traffic Shaning	-	_	-		
		Save	Concel			
landwidth Profiles	List					_
Shaw 10 . matri	rs (Right click on record	to get more options)				9
Name	O Dandwidth Re	te I Priority				
-		No data a	ailable in table			
Showing 0 to 0 of 0 em	ples				ef     Insurance Band in	
	and the second se					

4. Enter the following information and click **Save**.

lame	name1	
olicy Type	Outbound	
AN Interface	Dedicated WAN	
rofile Type	Rate	
Ainimum Bandwidth Rate	[Range: 1 - 9999999]	
Maximum Bandwidth Rate	[Range: 100 - 1000000] Kbps	

Field	Description
Name	Enter a name for your profile. This identifier is used to associate the configured profile to the traffic selector.
Policy Type	Select the policy type (Inbound or Outbound) from the drop-down menu.
WAN Interface	Select which WAN interface you want to associate this profile with.
Profile Type	Select either <b>Priority</b> or <b>Rate</b> from the drop-down menu.
Priority	If you selected <i>Priority</i> , select <b>Low</b> , <b>Medium</b> , or <b>High</b> .
Minimum Bandwidth Rate	If you selected <i>Rate</i> , enter the minimum bandwidth rate.
Maximum Bandwidth Rate	If you selected <i>Rate</i> , enter the maximum bandwidth rate.
Save	Click <b>Save</b> to save your reservation.

#### **Traffic Shaping**

Path: Network > Internet > Traffic Management > Traffic Shaping

Once a profile has been created it can then be associated with a traffic flow from the LAN to WAN. Traffic selector configuration binds a bandwidth profile to a type or source of LAN traffic with the following settings.

To create a traffic selector:

1. Click Network > Internet > Traffic Management > Traffic Shaping.

D-Linck Logged In as: sidnik (ADMH)   Language: En Unified Services Broster (ISB-1005M Serial: QBERTA3000007   Elementer 1.100 X Wizard					nguage: English (US) ( are: 1.108066_WW 'izard (System Souch	nglish (US) (Dengenit) 10565_WW System Sourch (School)	
2 Status	🔋 Wireless	Network	GB VPH	Security	O <sup>o</sup> Maintenance		
Network = Internet = Traffic Bandwidth Profflés	Management = Traffic S affic Shaping	haping				00	
This page shows a list of traf Traffic Selectors List	fic selectors. Traffic se	Hectors are service bi	used rules to which	h user can attach ban	dwidth profiles.		
Show 10 • entries	[Right click on record to	get more options]				٩	
Service Q Tr	affic Selector Match	Туре		Bandwidth	Profile	Ø	
		No data avi	ailable in table				
Showing 0 to 0 of 0 entries				(4)	First Presson Beat		
Add New Traffic Select	br -						

2. Click Add New Traffic Selector.

affic Selector Configuration		(
Available Profiles	band Itest	
Service	AIM	
Fraffic Selector Match Type	JP 💌	
P Address		
Subnet Mask		
		Save

Field	Description
Available Profiles	Select a bandwidth profile from the drop-down menu.
Service	Select a service from the drop-down menu.
Traffic Selector Match Type	Select IP or MAC Address.
IP Address	If you selected IP, enter the IP address of the source associated with this profile.
Subnet Mask	If you selected IP, enter a subnet mask.
MAC Address	If you selected MAC, enter the MAC address of the source associated with this profile.
Save	Click to save and activate your settings.

# **Routing** Static Routes

Path: Network > Routing > Static Routes

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.

To create a new static route:

1. Click Network > Routing > Static Routes.

Security Of Maintenance		D-Link Unified Services Router - DSR-1000N		
	COS VPM	💂 Network	🛜 Wireless	🙆 Status
l edit the configured routes.Use this page to d configured static route. The Interface dropdov	an also add, ray and metric options.	on the router. User ss, subnet mask, gate aces on the router as	atic routes configured er a destination addre onfigured wired inter	te shows the list of st outes. Be sure to entr ill show all available c Routes List
	1	get more options]	Tragar cack on record a	iu entries
⊖ Metric ⊖ Active ⊖ Private	/ ⊖ Int	sk ⊖ Gatewa No data av	⊖ Subnet Ma	Destination
First   Previous Nest / Las				g 0 to 0 of 0 entries
⊖ Me	/ ⊖ In t ailable in table	sk ⊖ Gatewa No data av	⊖ Subnet Ma	Destination

#### 2. Click Add New Static Route.

3. Complete the fields in the table on the next page and click **Save**.

tatic Route Configuration		X
Route Name Active Private Destination IP Address IP Subnet Mask Interface	OFF	
Metric	[Range: 715]	Savo

#### Section 5 - Connect to the Internet

Field	Description
Route Name	Enter a name for your route.
Active	Toggle to <b>ON</b> to activate this route or to <b>OFF</b> to deactivate.
Private	Toggle to <b>ON</b> to make this route private. If the route is made private, then the route will not be shared in a RIP broadcast or multicast.
<b>Destination IP Address</b>	Enter the IP address of the static route's destination.
IP Subnet Mask	Enter the subnet mask of the static route.
Interface	The physical network interface (WAN1, WAN2, WAN3, DMZ or LAN), through which this route is accessible.
Gateway IP Address	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.
Save	Click Save to save your route.

### RIP

Path: Network > Routing > RIP

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.

Note: The DSR-150/150N/250/250N routers do not support RIP.

To configure RIP:

1. Click Network > Routing > RIP.

Unified Services Router - DS		Serial: Q8281A3000007   Firmware: 1,108006E_WW		
🖾 Status	🛜 Wireless 🛛 💂	Network 🔝	VPN 🔒 Security	C <sup>o</sup> Maintenance
twork » Routing » RIP is page allows to configure the IP	RIP (Routing Information P	rotocol).		0
RIP Setup Direction Version	None RIP-1	🔊 In Only 🔘 Ou	t Only 🔘 Both	
	Sav	e Cancel		
			-	

Field	Description
Direction	<ul> <li>The RIP direction will define how this router sends and receives RIP packets. Select one of the following:</li> <li>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.</li> <li>Out Only: The router broadcasts its routing table periodically but does not accept RIP information from other routers.</li> <li>In Only: The router accepts RIP information from other routers, but does not broadcast its routing table</li> </ul>
	<ul> <li>None: The router neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.</li> </ul>
Version	<ul> <li>The RIP version is dependent on the RIP support of other routing devices in the LAN.</li> <li>Disabled: This is the setting when RIP is disabled.</li> <li>RIP-1: A class-based routing version that does not include subnet information. This is the most commonly supported version.</li> <li>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.</li> <li>Note: 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.</li> </ul>
Save	Click Save to save your settings.
### OSPF

Path: Network > Routing > OSPF

OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain. It gathers link state information from available routers and constructs a topology map of the network.

OSPF version 2 is a routing protocol which described in RFC2328 - OSPF Version 2. OSPF is IGP (Interior Gateway Protocols). OSPF is widely used in large networks such as ISP backbone and enterprise networks.

Note: The DSR-150/150N/250/250N routers do not support OSPFv2.

To configure OSPF:

1. Click **Network** > **Routing** > **OSPF**.

D-Link Logg Unified Services Router - DSR-1000N Si					Logged in as: admin ( ADMIN )   Language: English [US] O Logoul Serial: Q8281A3000007   Firmware: 1.108006E_WW Wizard System Search. 9			
	🙆 Status	🛜 Wireless	Retwork	CAS VPN	Security	O° Maintenance		
A DATE OF THE PARTY OF THE PART	Contraction of the second s							
nis page sh SPFv2 Li: ihow 10	ows the OSPFv2 p st • entries	arameters configurer [Right click on record 1	d on the router.User ca to get more options]	an also edit the OSPFv	2 configured param	neters.	٩	
nis page sh SPFv2 Lis ihow 10 Status (C	ows the OSPFv2 p st ▼ entries > Port ⊖ Ar	arameters configured [Right click on record 1 ea ⊖ Priority	d on the router.User ca to get more options] Ə Hello Interval	an also edit the OSPFo ⊖ Dead Interval	2 configured param ⊖ Cost ⊖	Authentication Type	٩	
nis page sh SPFv2 Lis ihow 10 Status ( XSABLED	ows the OSPFv2 p st entries Port $\Theta$ Ar LAN	arameters configured [Right dick on record t ea ⊖ Priority 1	d on the router.User ca to get more options] O Hello Interval 10	an also edit the OSPFv ⊖ Dead Interval 40	2 configured param O Cost O 10	Authentication Type None	٩,	
nis page sh SPFv2 Lis Show 10 Status ( XSABLED XSABLED	ows the OSPFv2 p st entries Port $\Theta$ Ar LAN WAN1	(Right click on record t ea O Priority 1	d on the router.User ca to get more options] O       Hello Interval         10       10         10       10	an also edit the OSPFv ⊕ Dead Interval 40 40	2 configured param O Cost O 10 10	Authentication Type None None	Q. 6	
nis page sh SPFv2 Lis Show 10 Status C NSABLED NSABLED NSABLED	entries	arameters configured [Right click on record t ea ⊖ Priority 1 1 1	d on the router.User ca to get more options] Hello Interval 10 10 10 10	<ul> <li>edit the OSPF</li> <li>⊕ Dead Interval</li> <li>40</li> <li>40</li> <li>40</li> </ul>	2 configured param	Authentication Type None None None	٩)	

- 2. Right-click the port you want to edit (LAN/WAN1/WAN2/WAN3) and select Edit.
- 3. Complete the fields in the table on the next page and click **Save**.

OSPFv2 Configuration			×
OSPFv2 Enable	DN		
Interface	WAN1		
Area		[Range: 0 - 200]	
Priority	1	[Default:1, Range: 0 - 255]	
Hello Interval	10	[Default:10, Range: 1 - 65535]	
Dead Interval	40	[Default:40, Range: 1 - 65535]	
Cost	10	[Default:10, Range: 1 - 65535]	
Authentication Type	Md5		
Md5 Key ID		[Range: 1 - 255]	
Md5 Authentication Key			
			Save

Field	Description
OSPFv2 Enable	Toggle <b>ON</b> to enable OSPF.
Interface	Displays the physical network interface on which OSPFv2 is Enabled/Disabled.
Area	Enter the area to which the interface belongs. Two routers having a common segment; their interfaces have to belong to the same area on that segment. The interfaces should belong to the same subnet and have similar mask.
Priority	Helps to determine the OSPFv2 designated router for a network. The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0 makes the router ineligible to become Designated Router. The default value is 1. Lower the value means higher the priority.
Hello Interval	The number of seconds for Hello Interval timer value. Enter the number in seconds that the Hello packet will be sent. This value must be the same for all routers attached to a common network. The default value is 10 seconds.
Dead Interval	The number of seconds that a device's hello packets must not have been seen before its neighbors declare the OSPF router down. This value must be the same for all routers attached to a common network. The default value is 40 seconds. OSPF requires these intervals to be exactly the same between two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment.
Cost	Enter the cost of sending a packet on an OSPFv2 interface.
Authentication Type	<ul> <li>Select one of the following authentication types:</li> <li>None: The interface does not authenticate OSPF packets.</li> <li>Simple: OSPF packets are authenticated using simple text key.</li> <li>MD5: The interface authenticates OSPF packets with MD5 authentication.</li> </ul>
Md5 Key ID	If MD5 authentication is selected, enter the MD5 key ID.
Md5 Authentication Key	If MD5 authentication is selected, enter the MD5 authentication key.
Save	Click Save to save your settings.

## **Protocol Binding**

Path: Network > Routing > Protocol Binding

Protocol bindings are useful when the Load Balancing feature is in use. Selecting 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.

To add, edit, or delete a protocol binding entry:

1. Click Network > Routing > Protocol Binding.



- 2. Right-click a current entry and select Edit or Delete. To add a new entry, click Add New Protocol Binding.
- 3. Complete the fields in the table below and click **Save**.

Carulca	ANY	
Service		
Local Gateway	WAN1 O WAN2 O WAN3	
Source Network	🛇 Any 🙁 Single Address 🔍 Address range	
Start Address		
End Address		
Destination Network	🔿 Any 🖲 Single Address 💿 Address range	
Start Address		

Field	Description
Service	Select a service from the drop-down menu.
Local Gateway	Select a WAN interface.
Source Network	Select the source network: <b>Any</b> , <b>Single Address</b> , or <b>Address Range</b> . If Single Address or Address Range is selected, enter the IP address or IP range.
Destination Network	Select the destination network: <b>Any</b> , <b>Single Address</b> , or <b>Address Range</b> . If Single Address or Address Range is selected, enter the IP address or IP range.
Save	Click Save to save your settings.

## IPv6 IP Mode

#### Path: Network > IPv6 > IP Mode

This page allows you to configure the IP protocol version to be used on the router. In order to support IPv6 on your local network (LAN), you must set the router to be in IPv4 / IPv6 mode. This mode will allow IPv4 nodes to communicate with IPv6 devices through this router.

To enable IPv6 on the router:

1. Click **Network** > **IPv6** > **IP Mode**.

🖾 Status	🛜 Wireless	Network	CO VPN	🗟 Security	Maintenance
work » IPv6 » IP Mode					0
s page allows user to configu	ure the IP protocol w	ersion to be used or	the router in orde	er to support IPv6 on	the LAN you must set the rout.
in IPv4 / IPv6 mode. This mod	te will allow IPv4 nod	es to communicate	with IPv6 devices th	rough this router.	the LAN, you must set the rout
Mode					
10 44 - 4-			10.10.4		
IP Mode	(	🖲 IPv4 Only 🔘 IP	v4 & IPv6		
IP Mode	(	) IPv4 Only @ IP Save	v4 & IPv6 Cancel		
IP Mode	l	D IPv4 Only @ IP Save	v4 & IPv6 Cancel		
1P Mode		D IPv4 Only ● IP Save	v4 & IPv6 Cancel		
1P Mode		9 IPv4 Only @ IP Save	v4 & IPv6 Cancel		
IP Mode		IPv4 Only ® IP	v4 & IPv6 Cancel		

- 2. Select IPv4 & IPv6.
- 3. Click Save.

### WAN Settings

Path: Network > IPv6 > WAN1 Settings

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.

#### **Dynamic IP**

To configure a dynamic (DHCP) IPv6 Internet connection:

1. Click Network > IPv6 > WAN1 Settings.

D-Link Unified Services Router, DSR 1888H			Logged in as: Serial: Q	Logged In as: admin ( ADMIN )   Language: English (US) ( Loguer Serial: 0007014/000007   Firmware: f.100004E, WW Withard ( System Senich. )			
🙆 Status	😤 Wieless	Network	CAS VPN	Security	Ø <sup>o</sup> Maintenance		
his page allows user to 19% en configured as a DHCPv6 client or tateful. If a stateful client is so in a DHCPv6 server available at 1 Pv6 Wan 1 Settings	aled Option1 confl connect to ISP us lected the gatewa he ISP, rather ICM	gurations. This router ing username and pas v will connect to the Pvé discover messages	can have a static li word (PPPoE). The ISP's DHCPv6 server will originals from	Pv6 address or receive DICDv6 client on the for a leased address. this gateway and will	connection information pateway can be either a For stateless DHCP there be used for auto configu	when tatelets or i need not ration.	
IPv6 WAN I Setup							
Connection Type	4	DHCPv6	*				
DHCPv6							
DHCPvé Auto Configuration		B Stateless Address	C Stateful Add	1442			
Prefix Delegation		28. 140					
		Save	Cancel				

Field	Description
Connection Type	Select <b>DHCPv6</b> from the drop-down menu.
DHCPv6 Auto Configuration	Select either Stateless Address or Stateful Address.
Prefix Delegation	Select this option to request router advertisement prefix from any available DHCPv6 servers available on the ISP, the obtained prefix is updated to the advertised prefixes on the LAN side. This option can be selected only in Stateless Address Auto Configuration mode of DHCPv6 Client.
Save	Click <b>Save</b> to save your settings.

#### Static IP

To configure a static IPv6 Internet connection:

1. Click Network > IPv6 > WAN1 Settings.

D-Link Unified Services Router - DSR-1000N			Logged in as: admin (ADMIN)   Language: English [US] O Logout Serial: 08281A3000007   Firmware: 1,108006E_WW Vizard System Search			
🖾 Status	🛜 Wireless	🖳 Network	CAS VPN	Security	©° Maintenance	
letwork 😐 IPv6 🐭 WAN1 Setti	ings				G	0
his page allows user to IPv6 onfigured as a DHCPv6 client tateful. If a stateful client is e a DHCPv6 server available i Pv6 Wan 1 Settings	related Option1 config or connect to ISP us: selected the gateway at the ISP, rather ICMP	gurations.This router ing username and pas will connect to the Pv6 discover messages	can have a static IP sword (PPPoE). The ISP's DHCPv6 server will originate from	v6 address or receive DHCPv6 client on the for a leased address, this gateway and will	e connection information whe gateway can be either statel For stateless DHCP there nee be used for auto configuration	n ess or ed not on.
IPv6 WAN 1 Setup						
Connection Type		Static				
Static						
IPv6 Address						
IPv6 Prefix Length		[Default:	64, Range: 1 - 128]			
Default IPv6 Gateway						
Primary DNS Server						
Secondary DNS Server						
		Save	Cancel			

Field	Description
Connection Type	Select Static.
IPv6 Address	Enter the IP address supplied by your ISP.
IPv6 Prefix Length	Enter the IPv6 prefix length supplied by your ISP.
Default IPv6 Gateway	Enter the IPv6 gateway address supplied by your ISP.
Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter the secondary DNS server IP address.
Save	Click <b>Save</b> to save and activate your settings.

#### PPPoE

To configure a dynamic (DHCP) IPv6 Internet connection:

1. Click Network > IPv6 > WAN1 Settings.

Wireless  Work + IPv6 + WANI Setting  is page allows user to IPv6 related Option1 contin  filtgured as a DHCPv6 client or connect to DP uses a OHCPv6 server available at the DP, rather ICM v6 WAN 1 Settings  IPv6 WAN 1 Setup Connection Type	Igurations. This roots sing username and p will connect to th thys discover messag	er can have assword (PP re ISP's DHCI res will origi	a static li Pot). The Pv6 server inate from	Pv6 addres DHCPv6 c for a leas this gates	Security is or receive lient on the ied address, way and will	e connec e galeway . For stab t be used	Maintenanc tion informati - can be eithe eless DHCP th for auto conf	an when r stateless ere need n figuration.
twork + IPvå + WANI Settings is page allows user to IPv6 related Option1 confi infigured as a DHCPv6 client or connect to ISP us telvit. If a stateful client is selected the gatewa a DHCPv6 server available at the ISP, rather ICM v6 Wan 1 Settings IPv6 WAN 1 Setup Connection Type	igurations. This routs sing username and p vy will connect to th Uvé discover messag	er can have assword (PP re ISP's DHCI res will origi	a static 19 PoE). The Pv6 server nate from	Pv6 addres DHCPv6 c for a leas this gates	s or receive lient on the sed address, way and will	e connes e galeway . Fur slat l be used	tion informati can be eithe eless DHCP th for auto conf	on when r stateless ere need n liguration.
is page allows user to 1946 related Option1 confi nfigured as a DHCP46 tilent or connect to CP us teleful. If a stateful client is selected the gatewa a DHCP46 server available at the ISP, rather ICM v6 Wan 1 Settings IPv6 WAN 1 Setup Connection Type	iguratiuns. This routs sing username and p by will connect to th the discover messag	er can have assword (PP re ISP's DHCI res will origi	a static IS PoE), The Pv6 server inate from	Pv6 addres DHCPv6 c for a leas this gates	is or receive lient on the lied address, way and will	e connec e galeway . For stat 1 be used	tion informati can be eithe eless DHCP th for auto conf	on when r stateless ere need n figuration.
Connection Type	PPPoE							
and the second								
14/2	10000	1995						
PPoE User Name	-							
Password		_						
Authentication Type	Auto negatiate	123						
DHCRek Dations	Disable DMCRef	121						
Polyment DNC Contract		120						
Formation DUC Second		-						
Secondary bits server		-						

Field	Description
Connection Type	Select PPPoE.
User Name	Enter your PPPoE user name.
Password	Enter your PPPoE password.
Authentication Type	Select the authentication type from the drop-down menu (Auto-negotiate/PAP/CHAP/MS-CHAP/MS-CHAPv2).
DHCPv6 Options	Select the mode of DHCPv6 client that will start in this mode (Disable dhcpv6/Stateless dhcpv6/Stateful dhcpv6/Stateless dhcpv6 with prefix delegation.
Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter the secondary DNS server IP address.
Save	Click <b>Save</b> to save and activate your settings.

### **Static Routing**

Path: Network > 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.

To create a new static route:

1. Click Network > IPv6 > Static Routing.

D-Link	Couter - DSR-1000N			Logged i Seria	n as: admin I: Q8281A30	(ADMIN)   La 100007   Firmw	inguage: Englisi vare: 1.108006E Vizard Syst	n [US] 🕐 _ww em Search	Logout Q
🙆 Sta	itus 🛜 Win	eless 📃	Network	CB VPN	8		🗭 Mair		1
Network » IPv6 » St This page shows a list IPv6 Static Routin Show 10 • entrie	atic Routing of IPv6 static routes ng List ss [Right click of	added. A user car	add, delete	and edit the	routes also.				00
								1	~
Name 🖸 I	Destination	\varTheta Gatew	ay	⊖ Interf	ace	\varTheta Met	ric \varTheta	Active	θ
			No data ava	lable in table					
Showing 0 to 0 of 0 ent	ries						First     Previo	sus Next là	Last H
Add New IPv6 St	atic Route								

- 2. Click Add New IPv6 Static Route.
- 3. Complete the fields in the table on the next page and click **Save**.

Route Name		
Active	OFF	
Pv6 Destination		
Pv6 Prefix Length	[Range: 0 - 128]	
nterface	🖲 WAN1 🔘 WAN2 🔘 sitü Tunnel 🔘 LAN	
Pv6 Gateway		
Metric	[Range: 2 - 15]	

#### Section 5 - Connect to the Internet

Field	Description
Route Name	Enter a name for your route.
Active	Toggle to <b>ON</b> to activate this route or to <b>OFF</b> to deactivate.
IPv6 Destination	Enter the IP address of the static route's destination.
IPv6 Prefix Length	Enter the prefix length of the static route.
Interface	The physical network interface (WAN1, WAN2, WAN3, DMZ or LAN), through which this route is accessible.
IPv6 Gateway	IPv6 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.
Save	Click Save to save your route.

### OSPFv3

Path: Network > IPv6 > OSPFv3

OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain. It gathers link state information from available routers and constructs a topology map of the network.

Open Shortest Path First version 3 (OSPFv3) supports IPv6. To enable an OSPFv3 process on a router, you need to enable the OSPFv3 process globally, assign the OSPFv3 process a router ID, and enable the OSPFv3 process on related interfaces.

Note: The DSR-150/150N/250/250N routers do not support OSPFv3.

To configure OSPF:

1. Click **Network** > **IPv6** > **OSPFv3**.

Inified Ser	rvices Router -	DSR-1000N		Serial: QB2B1	43000007   Firmwa	re: 1.108006E_WW zard System Sea	irch
1	🙆 Status	🛜 Wireless	Network	AS VPN	Security	Q° Maintenan	
le page che	we the OSDEv2 a	aramators configurad	on the router liner can	also adit the OSDEN	configurad param	ators OSBE/Open Sh	artart Dath
is page sho st) version uting inform res.OSPF ca SPFv3 List	ws the OSPFv3 p 3 is a routing pr mation within a s an be used to de t	ranameters configured rotocol for IPv6 Netwo single Autonomous Syst esign and build large an IRight click on record to	on the router.User can rks (OSPFv3) described i tem. Compared with RIP, nd complicated network:	also edit the OSPFv3 1 RFC2740.OSPF is an OSPF can provide sc	configured param IGP (Interior Gate alable network sup	eters.OSPF(Open Sh eway Protocol) used pport and faster con	ortest Path to distribut wergence
is page sho st) version uting inform nes.OSPF ca SPFv3 List how 10	ws the OSPFv3 p 3 is a routing pr mation within a s an be used to de t entries	Arrameters configured rotocol for IPv6 Netwo ingle Autonomous Syst ssign and build large an [Right click on record to	on the router.User can rks (0SPFv3) described i tem. Compared with RIP, nd complicated network: pget more options]	also edit the OSPFv3 n RFC2740.OSPF is an OSPF can provide sc	configured param IGP (Interior Gate alable network sup	eters.OSPF(Open Sh away Protocol) used pport and faster cor	ortest Path to distribut wergence
is page sho st) version uting inform nes.OSPF ca SPFv3 List how 10 [ itatus	ws the OSPFv3 p 3 is a routing p mation within a s an be used to de t entries Port LAN	Arameters configured rotocol for IPv6 Netwo ingle Autonomous Syst esign and build large an [Right click on record to Priority	on the router.User can rks (0SPFv3) described i tem. Compared with RIP, nd complicated network: o get more options] Hello Interv 10	also edit the OSPFv3 n RFC2740. OSPF is an OSPF can provide sc	configured parame IGP (Interior Gate alable network sup Dead Interval	eters.OSPF(Open Sh away Protocol) used pport and faster cor	ortest Path to distribut wergence Cost
is page sho st) version uting inform nes.OSPF ca SPFv3 List how 10 [] itatus WSABLED	ws the OSPFv3 p 3 is a routing p mation within as an be used to de t entries Port LAN WAN1	Arameters configured rotocol for IPv6 Netwo ingle Autonomous Syst ssign and build large an [Right click on record to O Priority 1	on the router.User can rks (0SPFv3) described i tem. Compared with RIP, nd complicated networks o get more options] Hello Interv 10 10	also edit the OSPFv3 n RFC2740.OSPF is an OSPF can provide sc	configured parame IGP (Interior Gate alable network sup Dead Interval 40 40	eters, OSPF(Open Sh away Protocol) used pport and faster cor	ortest Path to distribut wergence Cost 10 10

- 2. Right-click the port you want to edit (LAN/WAN1/WAN2) and select Edit.
- 3. Complete the fields in the table on the next page and click **Save**.

PFv3 Configuration		6
OSPFy3 Enable		
Interface	WANT	
Priority	1 (34(eL(2)), Renet: 0 - 135)	
lello Interval	10 [Decembrid: Hanger 1 AAA38]	
Dead Interval	40 (Defaulti40 Range 1 (5535)	
Cost	th (Derivativity, Danger 1 (45536)	
		Save

Field	Description
OSPFv3 Enable	Toggle <b>ON</b> to enable OSPFv3.
Interface	Displays the physical network interface on which OSPFv3 is Enabled/Disabled.
Priority	Helps to determine the OSPFv3 designated router for a network. The router with the highest priority will be more eligible to become Designated Router. Setting the value to 0 makes the router ineligible to become Designated Router. The default value is 1. Lower the value means higher the priority.
Hello Interval	The number of seconds for Hello Interval timer value. Enter the number in seconds that the Hello packet will be sent. This value must be the same for all routers attached to a common network. The default value is 10 seconds.
Dead Interval	The number of seconds that a device's hello packets must not have been seen before its neighbors declare the OSPF router down. This value must be the same for all routers attached to a common network. The default value is 40 seconds. OSPF requires these intervals to be exactly the same between two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment.
Cost	Enter the cost of sending a packet on an OSPFv3 interface.
Save	Click <b>Save</b> to save your settings.

### 6 to 4 Tunneling

Path: Network > IPv6 > 6 to 4 Tunneling

6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network. Select the check box to Enable Automatic Tunneling and allow traffic from an IPv6 LAN to be sent over an IPv4 Option to reach a remote IPv6 network.

To enable 6 to 4 tunneling:

1. Click Network > IPv6 > 6 to 4 Tunneling.



- 2. Toggle Activate Auto Tunneling to **ON**.
- 3. Click Save.

### ISATAP

Path: Network > IPv6 > 6 to 4 Tunneling

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network. ISATAP specifies an IPv6-IPv4 compatibility address format as well as a means for site border router discovery. ISATAP also specifies the operation of IPv6 over a specific link layer - that being IPv4 used as a link layer for IPv6.

To add, edit, or delete a ISATAP entry:

1. Click **Network** > **IPv6** > **ISATAP**.

					/izard System Search	٥
🖾 Status	🛜 Wireless	Retwork	CA VPN	Security	<b>©°</b> Maintenance	
work » IPv6 » ISATAP Tun	inels					
spage shows the list of an inectivity between IPv6 no I <mark>TAP Tunnels List</mark>	railable ISATAP tunnels. A u des within the LAN, as it t	user can also add, treats the IPv4 net	delete and edit IS work as a single IF	ATAP tunnels from thi Pv6 local link.	s page.ISATAP is available t	to pro
s page shows the list of av nectivity between IPv6 no NTAP Tunnels List now 10 • entries	railable ISATAP tunnels. A under within the LAN, as it to get [Right click on record to get	user can also add, treats the IPv4 net more options]	delete and edit IS work as a single IF	ATAP tunnels from thi v6 local link.	s page.ISATAP is available t	to pro
s page shows the list of av nectivity between IPv6 nc ATAP Tunnels List ow 10 • entries ocal Endpoint	railable ISATAP tunnets. A u des within the LAN, as it t [Right click on record to get	user can also add, treats the IPv4 net more options] O ISATAP No data av	delete and edit IS work as a single IF Subnet Prefix ailable in table	ATAP tunnels from thi V6 local link.	s page.ISATAP is available t	to pro

- 2. Right-click a current entry and select Edit or Delete. To add a new entry, click Add New ISATAP Tunnel.
- 3. Complete the fields in the table below and click **Save**.

ISATAP Tunnels Configuratio	n	X
ISATAP Subnet Prefix End Point Address IPv4 Address	LAN Other IP	
		Save

Field	Description
ISATAP Subnet Prefix	This is the 64-bit subnet prefix that is assigned to the logical ISATAP subnet for this intranet. This can be obtained from your ISP or internet registry, or derived from RFC 4193.
End Point Address	This is the endpoint address for the tunnel that starts with this router. The endpoint can be the LAN interface (assuming the LAN is an IPv4 network), or a specific LAN IPv4 address.
IPv4 Address	The end point address if not the entire LAN.
Save	Click <b>Save</b> to save your settings.

### LAN Settings DHCPv6 Server

Path: Network > IPv6 > LAN Settings > IPv6 LAN Settings

In IPv6 mode, the LAN DHCP server is disabled 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.

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.

To configure IPv6 LAN settings on the router:

1. Click Network > IPv6 > LAN Settings > IPv6 LAN Settings.

D-Link Unified Services Rout	ter – DSR-1000N		Logged in as: a Serial: QB2	admin (ADMIN)   Lan B1A3000007   Firmwa Nit	guage: English [US] () Logout re: 2.008001E_WW zard System Search. Q
🖾 Status	🛜 Wireles	s 📃 Network	CA VPN	A Security	🗘 Maintenance
letwork » IPv6 » LAN Se	ettings » IPv6 LAN Set	tings			0 0
IPv6 LAN Settings	IPv6 Address Pools	IPv6 Prefix Length Ro	uter Advertisement	Advertisement Pre	fixes
Pv6 LAN Settings					
LAN TCP/IP Setup IPv6 Address		fec0::1			
IPv6 Prefix Length		64 (Range:	0 - 128)		
DHCPv6					
Status		ON DOLL			
Mode		Stateless Stateless	ateful		
Domain Name		dlink.com			
Server Preference		255 (Range;	0 - 255)		
DNS Servers		Use DNS Proxy			
Lease / Rebind Time	et.a.	86400 (Range:	0 - 604800] Seconds		
		OH THE			
		OH STOR			

2. Complete the fields in the table on the next page and click **Save**.

#### Section 5 - Connect to the Internet

Field	Description
IPv6 Address	Enter the IPv6 LAN address for the router.
IPv6 Prefix Length	Enter the prefix length.
Status	Toggle to <b>ON</b> to enable DHCPv6.
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.
Domain Name	Enter a domain name (optional).
Server Preference	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.
DNS Servers	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).
Lease / Rebind Time	Enter the duration of the DHCPv6 lease from this router to the LAN client.
Prefix Delegation	Toggle to <b>ON</b> to enable prefix delegation in DHCPv6 server. This option can be selected only in Stateless Address Auto Configuration mode of DHCPv6 server.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

#### **IPv6 Address Pools**

Path: Network >	IPv6 >	I AN	Settings >	IPv6	Address	Pools
	11 VO /		Jettings /	11 00	Address	1 0013

This feature allows you to define the IPv6 delegation prefix for a range of IP addresses to be served by the router'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.

To add, edit, or delete a IPv6 address pool entry:

1. Click **Network** > **IPv6** > **LAN Settings** > **IPv6 Address Pools** tab.

					and the second s	-
🙆 Status	🛜 Wireles	s 📃 Network	Ca VPN	Security	O <sup>o</sup> Maintenanc	
rtwork » IPvó » LAN Se	ttings » IPv6 Address	Pools				0
Contractor of the local division of the						
IPv6 LAN Settings	IPv6 Address Pools eate/add/delete/ed	IPv6 Prefix Length	Router Advertisement	Advertisement Pr	efixes	
IPv6 LAN Settings is Page allow user to co v6 Address Pools L show 10   entries	IPv6 Address Pools reate/add/delete/ed ist [Right click on rec	IPv6 Prefix Length It Address Pools List for ord to get more options]	Router Advertisement r IPv6 configuration.	Advertisement Pr	efixes	
IPv6 LAN Settings is Page allow user to cr iv6 Address Pools L ihow 10 r entries Start Address	IPv6 Address Pools reate/add/delete/ed ist [Right click on rec	IPv6 Prefix Length It Address Pools List for ord to get more options]	Router Advertisement	Advertisement Pr	efixes	
IPv6 LAN Settings is Page allow user to cirv6 Address Pools L show 10 r entries Start Address	IPv6 Address Pools reate/add/delete/ed ist [Right click on rec	IPv6 Prefix Length it Address Pools List for ord to get more options] O End Address No dat	Router Advertisement r IPv6 configuration. ta available in table	Advertisement Pr	efixes	

- 2. Right-click a current entry and select Edit or Delete. To add a new entry, click Add New Address Pool.
- 3. Complete the fields in the table below and click **Save**.

v6 Address Pools Configu	ration	X
Start IPv6 Address End IPv6 Address Prefix Length	[Range: Ù - 128]	
		Save

Field	Description
Start IPv6 Address	Enter the starting IPv6 LAN address.
End IPv6 Address	Enter the ending IPv6 LAN address.
Prefix Length	Enter the prefix length.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

#### **IPv6 Prefix Length**

Path: Network > IPv6 > LAN Settings > IPv6 Prefix Length

To add, edit, or delete a IPv6 prefix length entry:

1. Click Network > IPv6 > LAN Settings > IPv6 Prefix Length tab.

					Vizard System S	earch ۹
🙆 Statu	is 🛜 Wireles	ss 📃 Network	CA VPN	Security	O° Mainten	
twork » IPv6 » LAN	Settings » IPv6 Prefix Lo	ength				0
IPv6 LAN Settings is Page allow user to	IPv6 Address Pools create/add/delete/ed	IPv6 Prefix Length Roui	ter Advertisement 6 configuration.	Advertisement Pr	efixes	
IPv6 LAN Settings is Page allow user to v6 Prefix Length how 10 • entries	IPv6 Address Pools create/add/delete/ed List [Right click on rec	IPv6 Prefix Length Row it Prefix Length List for IPv6 ord to get more options]	ter Advertisement 6 configuration.	Advertisement Pr	efixes	0
IPv6 LAN Settings is Page allow user to v6 Prefix Length how 10 • entries trefix Address	IPv6 Address Pools create/add/delete/ed List [Right click on rec	IPv6 Prefix Length Rou it Prefix Length List for IPv6 ord to get more options]	ter Advertisement 6 configuration. Q Prefix Length	Advertisement Pr	efixes	e
IPv6 LAN Settings is Page allow user to v6 Prefix Length how 10 , entries refix Address	IPv6 Address Pools create/add/delete/ed List [Right click on rec	IPv6 Prefix Length Rout it Prefix Length List for IPv6 ord to get more options] No data and	ter Advertisement 6 configuration. O Prefix Length ailable in table	Advertisement Pr	efixes	¢

- 2. Right-click a current entry and select Edit or Delete. To add a new entry, click Add New Prefix Length.
- 3. Complete the fields in the table below and click **Save**.

Pv6 Prefix Length Config	uration	X
Prefix Prefix Length	(Ranger 0 - 128)	
		Save

Field	Description
Profile	Enter a name for this profile.
Prefix Length	Enter the prefix length.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

#### **Router Advertisement**

Path: Network > IPv6 > LAN Settings > Router Advertisement

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 router will listen on the LAN for router solicitations and respond to these LAN hosts with router advisements.

To configure router advertisement settings:

1. Click **Network** > **IPv6** > **LAN Settings** > **Router Advertisement** tab.

D-Link	Logged in account ( Lonex)   Language: Premix (H) Serble: Classicianist?   Finnsaire: 2 Journalis, Wi Vitcord: Sphere Sauce 9
A States 🕈 Wireles	Network 🖾 (19) 🔒 Security 📭 Maintenance
wark = IPv6 = LAN Settings = Router Advert	iseemt 🔮
IPsi LAH Sattlings Bris Address Fools	B's Fronte Longth Boulor Advertisement advertisement Fratiens
ster Advertisement outer Advertisement Daemon Setup	
Status	
Advertice Mode	Unicational Multicast     Unicast Gety
versions included	10 Integer 10 Hills
RA Flogs Managed	
Other	
Router Preference	10 Leve 10 Maniful # High
MTU	1500 - Human Lumi House
Router Lifetime	3400

2. Complete the fields in the table on the next page and click **Save**.

Field	Description
Status	Toggle to <b>ON</b> to enable this feature.
Advertise Mode	Select <b>Unsolicited Multicast</b> 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 <b>Unicast only</b> .
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.
Managed	Toggle to <b>ON</b> to use the administered/stateful protocol for address auto-configuration. If set to <b>OFF</b> , the host uses administered/stateful protocol for non-address auto configuration.
Other	Toggle to ON to use administered/stateful protocol of other (i.e., non-address) information auto configuration.
Router Preference	This parameter (low/medium/high) 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 auto-configured by the router. The default is 1500.
Router Lifetime	This value is present in RAs 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.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

#### **Advertisement Prefixes**

Path: Network >	IPv6 >	LAN Settings >	Advertisement Prefixe	s
				-

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.

To add, edit, or delete an advertisement prefix entry:

1. Click **Network** > **IPv6** > **LAN Settings** > **Advertisement Prefixes** tab.

				W.W.	zand System Sear	ch. 9.
2 Status	😵 Wireless	Retwork	CES VPN	🔒 Security	O <sup>P</sup> Maintenant	
6 – LAN Settin	ngs Advertisement Pr	efixes				0 0
Sattings IP	Address Pools	vé Profix Longth Rou	tet Advertisement	Advertisement Pre	fixes	
ent Prefixes	List	to part spaces and there?			_	
Control Bridgers	THORNE CONTRACTOR	The second second second second second				
entries	LeoBut-crice ou vectua i	to Ker more optimist				٩
entries.	C IPvs	Prefix Leagth			fe Time	٩
entries.	Q IPys	Profix Longth No data an	ailable in table	9 u	le Time	٩
	5 - LAN Settin Settings IPu rs user to con- this router to llow the route ent Prefixer	LAN Settings - Advertisement Pr     Settings   Pvs: Address Pools   P     suser to configure IPv6 prefixes w     this router to inform hasts how to     liow the router to determine neigh     ent Prefixes List	A Standard Control Contro	AAN Settings	A - LAN Settings Advertisement Prefixes      Lattings   IPv6. Address Paols   IFv6. Prefix Length   Router Advertisement   Advertisement Pre     suser to configure IPv6 prefixes which will be used while advertisement. The router advertisement     which router to determine neighbors and whether the host is on the same link as the router,     ant Prefixes List	A divertisement Prefixes     Advertisement Prefixes

- 2. Right-click a current entry and select **Edit** or **Delete**. To add a new entry, click **Add New Advertisement** Length.
- 3. Complete the fields in the table below and click **Save**.

Advertisement Prefix Config	guration	adv.	ertisement Prefix Confi	guration	0
IPv6 Pretts Type SLA ID Pretts Lifetime	Store Colored / Local / L	10 12 17 7	vê Overîn, Type vê Overîn vê Overîn, Longth efîn Lîfetîme	(1) Sand, Clabel (Lacel/ISATAP	

Field	Description
IPv6 Prefix Type	To ensure hosts support IPv6 to IPv4 tunnel select the <b>6to4</b> prefix type. Selecting <b>Global/Local/ISATAP</b> will allow the nodes to support all other IPv6 routing antions.
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.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

#### IPv6 Tunnels Status

Path: Network > IPv6 > IPv6 Tunnels Status

This page displays the current status of IPv6 Tunnels.

D-Link Unified Services Router - DSR-1000N			Logged in as: admin ( ADMIN )   Language: English [US] Obeou Serial: 082B1A3000007   Firmware: 1.108006E_WW Wizard System Search			
🙆 Status	🛜 Wireless	📃 Network	Cas VPN	🔒 Security	OP Maintenance	
Network » IPv6 » IPv6 Tunne This page shows the status of IPv6 Tunnels Status	ls Status f IPvé tunnels.				0 0	
Show 10 💌 entries	[No right click options]				٩	
Tunnel Name		Ŷ	IPv6 Addresses		θ	
sit0-WAN1						
Showing 1 to 1 of 1 entries				He	st   Previous     Next >   Last >	

# **Wireless Settings**

The Wireless Network Setup Wizard is available for users new to wireless networking. By going through a few configuration pages you can enable a Wi-Fi<sup>™</sup> network on your LAN and allow supported 802.11 clients to connect to the configured Access Point. To run the wizard, refer to "#6 Wireless Network Setup" on page 12.

## **Access Points**

Path: Wireless > General > Access Points

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.

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.

**Note:** 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.

To add, edit, or delete an access point entry:

1. Click Wireless > General > Access Points.

Unified Se	<b>ink</b> ervices Router	+ DSR-1000N		Logge Se	ed in a erial:	s: admin ( ADMIN QB2B1A3000007	)   L Firm	Language: Engl Iware: 1.10800 Wizard Sy	ish [L 6E_W stem	Search	
	🖾 Status	🛜 Wirele	ess 💻 Netwo	ork 🕼 V	PN	Secur	ity	💇 Ma		nance	
he List of A Il radios) ca	available Access an be reviewed	Points table lists and AP parameter	the configured Acces configuration setting	ss Points (AP) for t s can be accessed	this d d.	evice, From this :	umm	ary list, the st	atus	of each AP (ov	/er
Show 10	entries	[Right click on re	ecord to get more option:	s]					-		a
Show 10	ints List ▼ entries Virtual AP	[Right click on re ∂ SSID	ecord to get more option:	s] Profile Name	Θ	Active Time	0	Start Time	•	Stop Time	٩ 0
Access Po Show 10 Status Q Enabled	ints List  entries  Virtual AP ap1	[Right click on re ⊖ SSID DSR-1000N_1	ecord to get more option: <ul> <li>Broadcast</li> <li>1</li> </ul>	s] Profile Name default1	Θ	Active Time No (Turn-off)	θ	Start Time	Ð	Stop Time	م ()
Access Po Show 10 Status O Enabled Showing 1 to	entries virtual AP ap1 1 of 1 entries	[Right click on re ⊖ SSID DSR-1000N_1	cord to get more option:	s] Profile Name default1	θ	Active Time No (Turn-off)	0	Start Time	<b>∂</b>	Stop Time	Q) 0

2. Right-click a current entry and select Edit or Delete. To add a new entry, click Add New Access Point.

ccess Point Configuration		×
AP Name	ap 1	
Profile Name	default1	
Active Time	DK	
Schedule Control	OFF	
Start Time	Hour Minute AM	
Stop Time	Hour Minute AM	
WLAN Partition	OFF	
		_
		Save

Field	Description
AP Name	Enter a name for your virtual access point.
Profile Name	Select a profile from the drop-down menu to associate this access point with. If you do not want to use the default profile, create a profile (refer to the next page) and then create an access point.
Active Time	Toggle to <b>ON</b> to "turn on" this access point.
Schedule Control	Toggle to <b>ON</b> if you want to specify a time to have this access point turned on.
Start/Stop Time	Enter a start and stop time.
WLAN Partition	Toggle to <b>ON</b> to prevent associated wireless clients from communicating with each other.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

## Profiles

Path: Wireless > General > Profiles

Creating a 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, and WPA2.

To add, edit, or delete a profile:

Unified Services Ro	uter - D5R-1000N		Logged	f in as: admin (ADMIN)   rial: QBZB1A3000007   Fi	Language: English [US] Language: Logode Logo	ogout Q
🙆 Stat	us 🔶 Wire	eless 💻 Ne	twork	PN 🔂 Security	🗘 Maintenance	
ireless a General a i						
profile is a grouping onfiguration page. The rofiles List	of wireless settings v profile allows for e [Right click on	which can be shared easy duplication of SS record to get more opt	across multiple APs. A iDs, security settings ions]	AP specific settings are o , encryption methods, cl	configured on the Access Point lient authentication, etc. acros	ss APs.
profile is a grouping onfiguration page. The rofiles List Show 10 💽 entries Profile Name	of wireless settings v profile allows for e [Right click on Q SSID	which can be shared asy duplication of SS record to get more opt O Broadcast	across multiple APs, J IDS, security settings ions] Ə Security	AP specific settings are of encryption methods, cl	configured on the Access Point lient authentication, etc. acros	ss APs.
profile is a grouping onfiguration page. The rofiles List Show 10 • entries Profile Name default1	of wireless settings v profile allows for e [Right click on <u>Q</u> SSID DSR-1000N_1	which can be shared easy duplication of SS record to get more opt	across multiple APs. A IDs, security settings ions] OPEN	AP specific settings are o encryption methods, cl O Encryption NONE	Configured on the Access Point lient authentication, etc. acros	ss APs.

1. Click Wireless > General > Profiles.

- 2. Right-click a current entry and select Edit or Delete. To add a new entry, click Add New Access Point.
- 3. Complete the fields in the table on the next page and click **Save**.

rofile Name	Profile Test 1		
SID	Test01	[Length: 1 -32]	
roadcast SSID	ON		
ecurity	WPA+WPA2		
ncryption	TKIP+CCMP		
uthentication	PSK		
/PA Password			

Field	Description
Profile Name	Enter a name for your profile.
SSID	Enter a name for your wireless network (SSID).
Broadcast SSID	Toggle to <b>ON</b> if you want your SSID broadcast openly or toggle to <b>OFF</b> to hide it. Clients will have to know the SSID to connect.
Security	<ul> <li>Select what kind of wireless security you want to use:</li> <li>Open: Select this option to create a public "open" network to allow unauthenticated devices to access this wireless gateway.</li> <li>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.</li> <li>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 preshared 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.</li> <li>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.</li> <li>WPA + WPA2: This uses both encryption algorithms, TKIP and CCMP. WPA clients will use TKIP and WPA2 clients will use CCMP encryption algorithms.</li> </ul>
Encryption	<ul> <li>Select the encryption type:</li> <li>WEP - Select <b>Open</b> or <b>Shared</b>.</li> <li>WPA - Select <b>TKIP</b> or <b>TKIP+CCMP</b>.</li> <li>WPA2 - Select <b>CCMP</b> or <b>TKIP+CCMP</b>.</li> <li>WPA+WPA2 - <b>TKIP+CCMP</b> will be the only option.</li> </ul>
Authentication	<ul> <li>Select the authentication type:</li> <li>WEP - Select 64-bit or 128-bit.</li> <li>WPA/WPA2/WPA+WPA2 - Select PSK (passphrase), RADIUS (RADIUS server), or PSK+RADIUS (both).</li> </ul>
WEP Passphrase/Key (1-4)	If you selected WEP, enter a passphrase or up to four hexadecimal keys (a-f, 0-9, A-F).
WPA Password	If you selected WPA, WPA2, or WPA+WPA2, enter a WPA password.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

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, refer to "Access Points" on page 80. After setting the AP name, the profile drop-down menu is used to select one of the configured profiles.

## **Radio Settings**

Path: Wireless > General > Radio Settings

You may configure the channels and power levels available for the AP's enabled on the router. 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.

The ratified 802.11n support on this radio requires selecting the appropriate broadcast 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 40MHz 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.

To configure the radio settings:

1. Click Wireless > General > Radio Settings.



Field	Description
Operating Frequency	Select <b>2.4GHz</b> or <b>5GHz</b> .
Mode	Select the 802.11 mode: • 2.4GHz - <b>g and b</b> , <b>g only</b> , <b>n and g</b> , or <b>n only</b> . • 5GHz - <b>a only</b> , <b>n and a</b> , or <b>n only</b> .
Channel Spacing	Select the Channel Width: <b>Auto 20/40</b> - This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices. <b>20MHz</b> - Select if you are not using any 802.11n wireless clients.
Control Side Band	Select Upper or Lower. Available for 802.11n only.
Current Channel	Displays the current channel.
Channel	Select the channel you want to use.
Default Transmit Power	Enter the default transmit power (0-31).
Transmit Power	Displays the current transmit power.
Transmission Rate	Select a transmission rate from the drop-down menu. This will lock the transmission rate of your wireless connection. It is strongly recommended to use <b>Best (Automatic)</b> .
Save	Click <b>Save</b> at the bottom to save and activate your settings.

## WMM Settings

Path: Wireless > Advanced > WMM

Wi-Fi Multimedia (WMM) provides basic Quality of Service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background.

To configure the radio settings:

1. Click Wireless > Advanced > WMM.

					Izand System Search	۵,
🕰 Status	💎 Wireless	Network	CB VPH	Security	O <sup>o</sup> Maintenance	
reless = Advanced = WMM					-	0
s page allows you to configure	the WI-FI Multin	nedia(WMM) configura	tion parameters.			
WM Settings						
WI-FI Multimedia Configura	tion	Craw I				
Profile Name		default 1				
Enable WMM		/ One	-			
Default Class Of Service		Beckground.				
IP TOS/DiffServ Mapping						_
Show 10 entries	Ha right click optic	niz)				٩
IP DSCP / TOS		0	Class Of Service			
0			Default			
1			Default			
1			Default			
3			Default			
4			Default			
5			Default			
ė			Default			
1			Defaulte			
8			Default			
9			Defaulte			
					In the local of the second	1000

Field	Description
Profile Name	Select the profile to associate this configuration to from the drop-down menu.
Enable WMM	Toggle to <b>ON</b> to enable WMM.
Default Class of Service	Select an available access category (voice, video, best effort, or background) to assign as "default".
IP DSCP / TOS	Under Class of Service, select a service and map it to the IP DSCP / TOS value.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

## WDS

#### Path: Wireless > Advanced > WDS

Wireless Distribution System (WDS) is a system enabling the wireless interconnection of access points in a network. This feature is only guaranteed to work between devices of the same type (i.e., using the same chipset/driver).

When you enable WDS, use the same security configuration as the default access point. The WDS links do not have true WPA/WPA2 support, as in there is no WPA key handshake performed. Instead the Session Key to be used with a WDS Peer is computed using a hashing function (similar to the one used for computing a WPA PMK). The inputs to this function are a PSK (configurable by an administrator from the WDS page) and an internal "magic" string (non-configurable).

In effect the WDS links use TKIP/AES encryption, depending on the encryption configured for the default AP. In case the default AP uses mixed encryption (TKIP + AES). The WDS link will use the AES encryption scheme.

Note: For a WDS link to function properly the Radio settings on the WDS peers have to be the same.

To configure the radio settings:

1. Click Wireless > Advanced > WDS.

D-Link Ontfleet Tansfors Reactor - 1950-10604			Logged In as: solver ( statur )   Language: stratus (cl.) () Language Sertal: GETE (2000007   Fittmeare: 2.000001E (WW 2% (V)Card System Search S			
🙆 Status	Wireless	Herverk.		🚊 security	O <sup>n</sup> Maintenance	
Mireless - Advanced - WDS						
This page allows you to configure th	he Wireless Distr	ibution System (WDS)	configuration para	meters.		
VDS Settings						
WDS Enable						
WDS Encryption	т	NIP+COMP				
WDS Security	W	EATWHAT				
WDS Authentication	P	SK				
WDS Passahrase	0					
System MAC Address	D	0:18:17:CD:69:78				
		Save	Carrent			
WDS Peer HAC Address Ust						
Show 10 - anteles. [Nig	At click on record	to get move options]				4
MAC Address						0
		No data ini	allable in table			
Observations in Ass. 20 and 20 conclusions						100.2

Field	Description
WDS Enable	Toggle to <b>ON</b> to enable WDS and click <b>Save</b> .
WDS Encryption	Displays the current wireless encryption used.
WDS Security	Displays the current security type.
WDS Authentication	Displays the current authentication type.
WDS Passphrase	Enter the WDS passphrase (if WEP, WPA, WPA2, or WPA+WPA2 is enabled).
System MAC Address	Displays the system MAC address.
Add New WDS	Once you enabled WDS (and clicked Save), click Add New WDS and enter the MAC address of a WDS peer. You can add up to four WDS peers.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

## **Advanced Settings**

Path: Wireless > Advanced > Advanced Settings

You can modify the 802.11 communication parameters in this page. Generally, the default settings are appropriate for most networks.

1. Click Wireless > Advanced > Advanced Settings.

				-16		System Search	٩
🖾 Status <table-cell> 🛜 Wi</table-cell>	ireless 📃		CA VPN	Security	0	Maintenance	
less » Advanced » Advanced Settings							0
page is used to specify advanced co	nfiguration settings	for the radio.					-
vanced Wireless Settings							
Beacon Interval	100	[Default: 10]	0, Range: 40 - 3500	Milliseconds			
Dtim Interval	2	[Default: 2,	Range: 1 - 255 ]				
Dtim Interval RTS Threshold	2 2346	[Default: 2,	Range: 1 - 255 ] 46, Range: 256 - 234	6.]			
Dtim Interval RTS Threshold Fragmentation Threshold	2 2346 2346	[Default: 2, [Default: 23] [Default: 23]	Range: 1 - 255 ] 46, Range: 256 - 234 46, Range: 257 - 234	e1 e1			
Dtim Interval RTS Threshold Fragmentation Threshold Preamble Mode	2 2346 2346 Long	[Default: 2, [Default: 23] [Default: 23]	Range: 1 - 255 ] 46, Range: 256 - 234 46, Range: 257 - 234	e ] e 1			
Dtim Interval RTS Threshold Fragmentation Threshold Preamble Mode Protection Mode	2 2346 2346 Long None	[Default: 2, [Default: 23] [Default: 23]	Range: 1 = 255 ] 46, Range: 256 - 234 46, Range: 257 - 234	e 1 e 1			

Field	Description
Beacon Interval	Beacons are packets sent by an Access Point to synchronize a wireless network. The default value is 100.
DTIM Interval	(Delivery Traffic Indication Message) 3 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
RTS Threshold	This value should remain at its default setting of 2432. If inconsistent data flow is a problem, only a minor modification should be made.
Fragmentation Threshold	The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.
Preamble Mode	Select either <b>Long</b> or <b>Short</b> . The Preamble Type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. High network traffic areas should use Short preamble type.
Protection Mode	Select either <b>None</b> or <b>CTS-to-Self Protection</b> . Select the CTS-to-Self Protection to enable CTS-to-Self protection mechanism, which is used to minimize collisions among stations in a mixed 802.11b & g environment. The default selection is <b>None</b> .
Power Save Enable	Toggle to <b>ON</b> to enable the Unscheduled Automatic Power Save Delivery (also referred to as WMM Power Save) feature that allows the radio to conserve power.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

## WPS

Path: Wireless > Advanced > 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 drop-down menu 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:

- **Personal Identification Number (PIN):** The wireless device that supports WPS may have an alphanumeric PIN, if it does 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 the WPS button for two seconds, and then press the WPS button (or initiate WPS via GUI) on your wireless client within two minutes. The AP will detect the wireless device and establish a secure link to the client.

To enable and connect clients using WPS:

- 1. Click Wireless > Advanced > WPS.
- 2. Select which VAP you want to perform the WPS process from the drop-down menu.
- 3. Toggle *WPS Status* to **ON** and click **Save**.

<b>D-Link</b> Unified Services Router - DS		Logged in as: admin ( ADMIN )   Language: English [US] () Logout Seriat: Q8281A3000007   Firmware: 2.008001E_WW Witzard () System Search					
🖾 Status	🛜 Wireless	Retwork	(a) VPN	Security	O <sup>o</sup> Maintenance		
fireless » Advanced » WPS						00	
his page allows you to define an /PS Settings	id modify the Wi-Fi Pri	otected Setup (WI	PS) configuration pa	rameters.			
WPS Configuration							
Select VAP	ap1	1	•				
WPS Status		OFF					
WPS Current Status							
Security	N/A						
Authentication	N/A						
Encryption	N/A						
Encryption	N/A						
Encryption WPS Setup Method Session Status	N/A						
Encryption WPS Setup Method Session Status	N/A	_					

4. Once enabled the following screen will appear.

D-Link Jnified Services Router - DSR-100	ION	Logged in as: admin ( ADMIN )   Language: English [US] O Logont Serial: QB2B1A3000007   Firmware: 2.00B001E_WW Wizard System Search. Q						
🖾 Status 🎅	Wireless 📃 Network	CAS VPN	Security	O <sup>o</sup> Maintenance				
ireless » Advanced » WPS			_	0 0				
	• Operat	tion Succeeded						
is page allows you to define and mo PS Settings	dify the Wi-Fi Protected Setup (W	(PS) configuration para	meters.					
WPS Configuration								
Select VAP	ap 1							
WPS Status	ON T							
WPS Current Status								
Security	WPA+WPA2							
Authentication	PSK							
Encryption	TKIP+CCMP							
WPS Setup Method								
Station PIN								
	Configure Via Pl	IN Configure Vi	a PBC					
Session Status	Enabling WPS							
	Save	Cancel						
		and the second se						

- 5. Under WPS Setup Method, decide to either use PIN or PBC (Push Button).
- 6. If you want to use PIN method, enter the PIN next to *Station PIN* and click **Configure Via PIN**. You will need to enter the PIN on your wireless client and start the WPS process within one minute.
- 7. If you want to use push button method, click **Configure Via PBC**. This will initiate the WPS session. You will need to press the WPS button (or initiate through an interface) on your client within one minute.
- 8. Allow up to two minutes to connect. Check the Session Status to see if it successfully connected.

# 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.

## IPSec VPN Policies

Path: VPN > IPSec VPN > Policies

An IPsec policy is between this router and another gateway or this router and an 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.

To configure the radio settings:

1. Click **VPN** > **IPSec VPN** > **Policies**.

D-Link Unified Services Rauter - DSR-1000N							Logged in as: admin ( ADMIN )   Language: English [U5] O Logout Serial: Q8281A3000007   Firmware: 1.108006E_WW Wizard System Search. Q								ut Q	
C	🛯 Status		ኛ Wireless		<u>п</u> и			ക v	PN			0	<b>o</b> Mainte			
VPN » IPSec VI This page show policies from t IPSec Polici	PN » Policies vs the list of c his page. es List	configu	ured IPsec VP	N polic	cies on th	te rou	ter. A us	er can	also add, d	elete	, edit, enab	ile, disab	le and ex	port I	Psec VPI	•
Show 10 -	entries	[Rigi	nt click on reco	rd to ge	et more of	ptions]										9
Status	A Name	θ	Backup Tunnel Name	۲	Туре	θ	IPSec Mode	θ	Local	⇔	Remote	Θ	Auth	⇔	Encr	÷
						No da	ata availabl	e in tabl	e							
Showing 0 to 0 Add New I	of 0 entries PSec Policy	1										First	Previous	Hex	t) Les	4 21
Backup Poli	cies List															0
	1															2
Status	Name	Ð	Primary Tunnel Name	θ	Туре	θ	IPSec Mode	θ	Local	Θ	Remote	θ	Auth	۲	Encr	Ð
_						No da	ata availabl	e in tabl	e							
Showing 0 to 0	of 0 entries											First	( Previous	Nex	t) La	K.z

2. Click **Add new IPSec Policy**. Fill out the General section which you will name the VPN, select policy type, define the tunnel type, and define endpoints.

IPSec Policy Configuration		8
General		
Policy Name		
Policy Type	Auto Policy	
IP Protocol Version	1Pv4	
IKE Version	IKEv1	
IPSec Mode	Tunnel Mode	
Select Local Gateway	WAN1	
Remote Endpoint	IP Address	
IP Address / FQDN		
Enable Mode Config	OFF	
Enable NetBIOS	OFF	
Enable RollOver	OFF	
Protocol	ESP	
Enable DHCP	OFF	
Local IP	Subnet	
Local Start IP Address		
Local Subnet Mask		
Remote IP	Subnet	
Remote Start IP Address		
Remote Subnet Mask		
Enable Keepalive	OFF	

Field	Description
Policy Name	Enter a unique name for the VPN Policy. This name is not an identifier for the remote WAN/client.
Policy Type	<ul> <li>Select either Manual or Auto.</li> <li>Manual: All settings (including the keys) for the VPN tunnel are manually input for each end point. No third-party server or organization is involved.</li> <li>Auto: Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN Endpoints.</li> </ul>
IP Protocol Version	Select either IPv4 or IPv6.
IKE Version	Select the version of IKE.
IPSec Mode	Select either <b>Tunnel</b> or <b>Transport</b> . IPsec tunnel mode is useful for protecting traffic between different networks, when traffic must pass through an intermediate, untrusted network. Tunnel mode is primarily used for interoperability with gateways, or end-systems that do not support L2TP/IPsec or PPTP connections. Transport mode is the default mode for IPsec, and it is used for end-to-end communications (for example, for communications between a client and a server).
Select Local Gateway	In the event that two WAN ports are configured to connect to your ISP, select the gateway that will be used as the local endpoint for this IPsec tunnel.
Remote Endpoint	Select the type of identifier that you want to provide for the router at the remote endpoint (either <b>IP Address</b> or <b>FQDN</b> [Fully Qualified Domain Name])
IP Address/FQDN	Enter the identifier for the router.
Enable Mode Config	Toggle to <b>ON</b> to enable. Mode Config is similar to DHCP and is used to assign IP addresses to the remote VPN clients.
Enable NetBIOS	Toggle to <b>ON</b> to allow NetBIOS broadcasts to travel over the VPN tunnel
Enable RollOver	Toggle to <b>ON</b> to enable VPN rollover. You must have the WAN Mode set to Rollover.
Protocol	Select a protocol from the drop-down menu.
Enable DHCP	Toggle to <b>ON</b> to allow VPN clients that are connected to your router over IPsec to receive an assigned IP using DHCP.
Local IP/Remote IP	<ul> <li>Select the type of identifier that you want to provide for the endpoint:</li> <li>Any: Specifies that the policy is for traffic from the given end point (local or remote). Note that selecting Any for both local and remote end points is not valid.</li> <li>Single: Limits the policy to one host. Enter the IP address of the host that will be part of the VPN.</li> <li>Range: Allows computers within an IP address range to connect to the VPN. Enter the Start IP Address and End IP Address in the provided fields.</li> <li>Subnet: Allows an entire subnet to connect to the VPN. Enter the network address and subnet mask in the provided fields.</li> </ul>
Enable Keepalive	Toggle to <b>ON</b> to periodically send ping packets to the host on the peer side of the network to keep the tunnel alive.

3. 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.

Phase1(IKE SA Parameters) Exchange Mode	Main			
Direction / Type	Both	F		
Nat Traversal	011			
NAT Keep Alive Frequency	20	1	Seconds	
Local Identifier Type	Local Was	IP E		
Denote Identifier Ture	Remote We	- IP 🖸		
Kemote identifier Type	nemote wa	n. iP		
Encryption Algorithm DES	OFF	3DES		OFF
AE5-128	OH CON	AES-192		OFF
AES -256	OFF			
BLO WFISH	OFF			
CAST128	OFF			
Authentication Algorithm MD5	Ott	SHA-1	0	
SHA2-256	OFF	SHA2-384		OFF
SHA2-512	OFF			
Authentication Method	Pre-Shared	Key		
Pre-Shared Key			[Length: 8 - 49]	
Diffie-Hellman (DH) Group	Group 2 (16	124 bit)		
SA-Lifetime	28800	IDefault: 28800 Ra	nee: 308 - 2147483647) Secon	
Fnable Dead Peer Detection	OFF			
Extended Authentication	None			
Dhanes (Auto Dellas Decembras	10000			
SA Lifetime	3600	Seconds 💌		
Encryption Algorithm				
DES	OFF	NONE		OFF
3DES	OFF	AES-128	0	
AES-192	OFF	AES-256		OFF
AES-CCM	OFF	AES-G CM		OFF
TWOFISH (128)	OFF	TWOFISH (192)		OFF
TWOFISH (256)	OFF			
BLOWFISH	OFF			
CAST128	OFF			
Integrity Algorithm MD5	OFF	SHA-1		
SHA2-224	OFF	SHA2-256		OFF
SHA2-384	OFF	SHA2-512		OFF

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

**Note:** Once you have created an IPSec policy, you may right-click the policy and select Export to save as a file. You can then upload this to another DSR router or keep as a backup. To upload a saved policy, refer to "Easy VPN Setup" on page 101.

### **Tunnel Mode**

Path: VPN > IPSec VPN > Tunnel Mode

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. You can also define a single IP address, a range of IPs, or a subnet on both the local and remote private networks that can communicate over the tunnel.

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 client access to specific private networks, thereby allowing access control over specific LAN services.

D-Link Unified Services Router - DSR-1000		Logged in as: admin (ADMIN)   Language: English [US] Coout Serial: Q8281A3000007   Firmware: 1.108006E_WW Wizard System Search					
🖾 Status 🎅 Wi	reless 📃 Network	CB VPN	Security	O <sup>o</sup> Maintenance			
N » IPSec VPN » Tunnel Mode Tunnel Mode Split DNS Names is page allows you to define the IP add	iress range for clients connectin	g using Mode Conf	ïg.		00		
ode Config	0 Full Frank Or						
Start ID Address	192 168 12 100	pur runnet					
End IP Address	192.168.12.254						
Primary DNS							
Secondary DNS							
Primary WINServer							
Secondary WINServer							
	Save	Cancel					

1. Click **VPN** > **IPSec VPN** > **Tunnel Mode**.

Field	Description
Tunnel Mode	Select either <b>Full Tunnel</b> or <b>Split Tunnel</b> .
Start/End IP Address	Enter the starting and ending IP addresses.
Primary/Secondary DNS	Enter the primary and secondary DNS server addresses.
Primary/Secondary WINS	Enter the primary and secondary WINS server addresses.
Save	Click <b>Save</b> to save and activate your settings.
## **Split DNS Names**

In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.

To add a DNS name:

1. Click VPN > IPSec VPN > Tunnel Mode > Split DNS Names tab.

Anned Services Router - Osh-Town		Senai: Q	8281A3000007   FIIMM	/izard System Search	h C
🖾 Status 🛜 Wireless	Retwork	CA VPN	Security	O° Maintenance	
> IPSec VPN >> Tunnel Mode >> Split DNS Names					0
Tunnel Mode Split DNS Names					
Tunnel Mode Split DNS Names	ovided in Dynamic IP	Range page to res	olve this domain name	e. This is applicable only	in case
Tunnet Mode Split DNS Names s clients connected to this device use the DNS pr it tunnel.	rovided in Dynamic IP	Range page to res	olve this domain name	e.This is applicable only	in case
Tunnet Mode Split DNS Names e clients connected to this device use the DNS pr it tunnel. Iti DNS Names List	rovided in Dynamic IP	Range page to res	olve this domain name	e.This is applicable only	in case
Tunnet Mode     Split DNS Names       e clients connected to this device use the DNS prit tunnet.       lit DNS Names List       tow     10 entries   [Right click on record to prime click on prima click on prime click on prim	rovided in Dynamic IP get more options]	Range page to res	olve this domain name	e.This is applicable only	in case
Tunnet Mode Split DNS Names e clients connected to this device use the DNS pr it tunnel. lit DNS Names List tow 10 • entries [Right click on record to provide the second to	rovided in Dynamic IP get more options]	Range page to res	olve this domain name	s.This is applicable only	in case
Tunnet Mode     Split DNS Names       e clients connected to this device use the DNS prit tunnet.       lit tunnet.       lit DNS Names List       tow     10 entries       (Right click on record to promain Names)	rovided in Dynamic IP get more options] No data av	Range page to res ailable in table	olve this domain name	a.This is applicable only	in case
Tunnet Mode     Split DNS Names       e clients connected to this device use the DNS prit tunnet.       lit DNS Names List       now     10 entries       (omain Names       nowling 0 to 0 of 0 entries	rovided in Dynamic IP get more options] No data av	Range page to res ailable in table	olve this domain name	a.This is applicable only	in case

2. Click Add New Split DNS name. You can right-click any created entries to edit or delete.



3. Enter a domain name and click **Save**.

## **DHCP** Range

This page displays the IP range to be assigned to clients connecting using DHCP over IPsec. By default the range is in 192.168.12.0 subnet.

To configure the *DHCP over IPSec* DHCP server settings:

1. Click **VPN** > **IPSec VPN** > **DHCP Range**.

nified Services Route	- DSR-1000N		Serial: QI	8281A3000807   Firmw	are: 1.10B006E_WW izard System Search
🖾 Status	🛜 Wireless	📃 Network	A VPN	Security	O° Maintenance
s page allows you to def ver on the LAN. ICP Range	ine the IP address rang	ge for clients connectin	ng using DHCP over	IPsec, Note: To suppo	ort DHCP over IPsec, enable DHCP
Starting IP Address		192.168.12.100			
Ending IP Address		192.168.12.254			
Subnet Mark		255.255.255.0			
Subnet mask					

2. Complete the fields in the table below and click **Save**.

Field	Description
Starting IP Address	Enter the starting IP address to issue your clients connecting using DHCP over IPSec.
Ending IP Address	Enter the ending IP address.
Subnet Mask	Enter the subnet mask.
Save	Click <b>Save</b> to save and activate your settings.

## Certificates

This router uses digital certificates for IPsec VPN authentication. You can obtain a digital certificate from a wellknown Certificate Authority (CA) such as VeriSign, or generate and sign your own certificate using functionality available on this gateway.

The router 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.

### **Trusted Certificates**

The certificates menu allows you to view a list of certificates (both from a CA and self-signed) currently loaded on the router. 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

To upload a certificate:

1. Click VPN > IPSec VPN > Certificate > Trusted Certificates tab.

D-Link Jnified Services Router - DSR-1000N			Logged in as Serial: C	: admin ( ADMIN 18281A3000007	)   Langua Firmware:	age: English [US] ( 1.108006E_WW rd System Searc	Logout
🖾 Status	🛜 Wireless	Network	CA VPN	Secu		O° Maintenance	
PN » IPSec VPN » Certificat	es » Trusted Certificates						0 0
Trusted Certificates	Active Self Certificates	Self Certificate	Requests				
rusted Certificates or CA co trusted organization or au ient presents a digital cert ne Trusted CA certificates	ertificates are used to v hority called the Certifi ificate, the authenticat are used in this authent	erify the validity of icate Authority. The ion process verifies ication process.	certificates signed table contains the that the presented	by them. When certificates o certificate is	a certific f each CA.V issued by c	ate is generated, it When a remote VPN one of the trusted a	is signed by gateway or uthorities.
rusted Certificates or CA co trusted organization or au lient presents a digital cert he Trusted CA certificates <b>rusted Certificates (C</b>	ertificates are used to v hority called the Certifi ificate, the authenticat are used in this authent A Certificate) List	erify the validity of icate Authority. The ion process verifies ication process.	certificates signed table contains the that the presented	by them. When certificates o certificate is	a certifica f each CA.V issued by c	ate is generated, it When a remote VPN one of the trusted a	is signed by gateway or wthorities.
rusted Certificates or CA co trusted organization or au lient presents a digital cert he Trusted CA certificates rusted Certificates (C Show 10 • entries	ertificates are used to v thority called the Certifi dificate, the authenticat are used in this authent A Certificate) List [Right click on record to g	erify the validity of icate Authority. The ion process verifies ication process. get more options]	certificates signed table contains the that the presented	by them. When certificates o d certificate is	a certifica f each CA.V issued by c	ate is generated, it When a remote VPN one of the trusted a	is signed by gateway or wthorities.
rusted Certificates or CA c trusted organization or au lient presents a digital cert he Trusted CA certificates rusted Certificates (C Show 10 v entries CA Identity (Subject Nai	ertificates are used to v thority called the Certifi ificate, the authenticat are used in this authent A Certificate) List [Right click on record to g ne)	erify the validity of icate Authority. The ion process verifies ication process. get more options] Q. Iss	certificates signed table contains the that the presented uer Name	by them. When certificates o d certificate is $\Theta$ Exp	i a certifici f each CA.V issued by c	ate is generated, it When a remote VPN one of the trusted a t Time	is signed by gateway or uthorities. Q
rusted Certificates or CA co trusted organization or au liont presents a digital corr ne Trusted CA certificates rusted Certificates (C Show 10 , entries CA Identity (Subject Nar	ertificates are used to v thority called the Certifi tificate, the authenticat are used in this authent A Certificate) List [Right click on record to g ne)	erify the validity of icate Authority. The ion process verifies dcation process. get more options] O Iss No data a	certificates signed table contains the that the presented uer Name vailable in table	by them. When certificates o d certificate is ⊖ Exp	i a certific; f each CA.V issued by c	ate is generated, it When a remote VPN one of the trusted a	is signed by gateway or uthorities. Q.
rusted Certificates or CA co trusted organization or au lient presents a digital cert ne Trusted CA certificates rusted Certificates (C Show 10 ) entries CA Identity (Subject Nau Showing 0 to 0 of 0 entries	ertificates are used to v hority called the Certifi ficate, the authenticat are used in this authent A Certificate) List [Right click on record to g me]	erify the validity of icate Authority. The ion process verifies deation process. get more options] Q Iss No data a	certificates signed table contains the that the presented uer Name valiable in table	by them. When certificates o d certificate is $\Theta$ Exp	n a certifici f each CA.V issued by c iry-Date 8	ate is generated, it When a remote VPN one of the trusted a t Time	is signed b gateway or uuthorities.

- 2. Click the **Browse** button. Locate your certificate and click **Open**.
- 3. Click **Upload**.



### **Active Self Certificates**

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 router. 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.

**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 upload a certificate:

1. Click VPN > IPSec VPN > Certificate > Active Self Certificates tab.

Unified Servic	ces Router -	D5R-1000N		Seria	il: QB2B1A3000607   Fi	rmware: 1. Wizard	108006E_WW	٩
		🛜 Wireless	Network	A VPN	Security	0	• Maintenance	
PN » IPSec VPN	» Certificate	s » Active Self Certificat	es					0 0
Trusted Cer	tificates A	ctive Self Certificates	Self Certificate R	equests				
			ertificates, rui each	certificate, t	he following data is dis	played:		
show 10	ertificates entries	List [Right click on record to p	get more options]	certificate, t	he following data is di:	played:		Q
Show 10 💽	ertificates entries Subject N	List [Right click on record to g	get more options]	certificate, t	he following data is dis	played: ⊖	Expiry Time	٩
Show 10 💽	ertificates entries Subject N	List [Right click on record to plane $\Theta$	get more options] Serial Number No data ava	certificate, ti ⊖ ailable in table	he following data is dis Issuer Name	played: ⊖	Expiry Time	٩

- 2. Click the **Browse** button. Locate your certificate and click **Open**.
- 3. Click **Upload**.

ate	
Browse_ No file selected.	
	Browse_ No file selected.

### Self Certificate Requests

To request a self certificate to be signed by a CA, you can generate a Certificate Signing Request from the router 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.

To generate a certificate signing request:

1. Click VPN > IPSec VPN > Certificates > Self Certificate Requests.

					Izard System Search	٩
🖾 Status	😤 Wireless	Retwark	CAS VPN	Security	C <sup>o</sup> Maintenance	
N = IPSec VPN = Certificates	- Self Certificate Rec	puests			-	0
Trusted Certificates	tive Sall Certificate	s Self Certificate R	equests			
e Self Certificate Requests t	able displays a list of	f all the certificate re-	quests made.			
If Certificate Requests	List					
If Certificate Requests	List Right click on record to	get more options]				q
If Certificate Requests	List Right click on record to	get more options]	tatus			q
If Certificate Requests how 10 • entries (1 fame	List Right click on record to	get more options]	tatus ilable in table		_	q

- 2. Click New Self Certificate.
- 3. Complete the fields in the table below and click **Save**.

enerate Self Certificate Re	quest	×
Name		
Subject		
Hash Algorithm	MD5	
Signature Key Length	512	
Application Type	Https	
IP Address		
Domain Name		
Email Address		
		Save

Field	Description
Name	Enter a name (identifier) for the certificate.
Subject	This field will populate the CN (Common Name) entry of the generated certificate. Subject names are usually defined in the following format: CN= <device name="">, OU=<department>, O=<organization>, L=<city>, ST=<state>, C=<country>. For example: CN=router1, OU=my_company, O=mydept, L=SFO, C=US.</country></state></city></organization></department></device>
Hash Algorithm	Select the algorithm from the drop-down menu. Select either <b>MD5</b> or <b>SHA-1</b> .
Signature Key Length	Select the signature key length from the drop-down menu. Select either 512, 1024, or 2048
Application Type	Select the application type from the drop-down menu. Select either HTTPS or IPSec.
IP Address	Enter an IP address (optional).
Domain Name	Enter a domain name (optional).
Email Address	Enter your email address.
Save	Click <b>Save</b> to save and activate your settings.

## **Easy VPN Setup**

To upload an exported IPSec VPN policy:

- 1. Click VPN > IPSec VPN > Easy VPN Setup.
- 2. Click **Browse** and navigate to the policy file you want to upload. Select it and click **Open**.
- 3. Click Upload.



4. Once uploaded, go to **VPN** > **IPSec VPN** > **Policies** and the loaded VPN will be listed. Right-click it to edit or delete.

# PPTP VPN Server

Path: VPN > PPTP VPN > 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.

The range of IP addresses allocated to PPTP clients can coincide with the LAN subnet. As well the PPTP server will default to local PPTP user authentication, but can be configured to employ an external authentication server should one be configured.

To create a PPTP VPN server:

- 1. Click VPN > PPTP VPN > Server.
- 2. Complete the fields in the table below and click **Save**.



Field	Description
Enable PPTP Server	Select either <b>IPv4</b> or <b>IPv6</b> .
PPTP Routing Mode	Select either NAT or Classical.
Starting/Ending IP Address	Enter the IP address range to assign your PPTP clients.
IPv6 Prefix	If you selected IPv6, enter the IPv6 prefix.
IPv6 Prefix Length	If you selected IPv6, enter the IPv6 prefix length.
Authentication	Select the authentication type from the drop-down menu.
Authentication Supported	Toggle which type of authentication you want to enable to <b>ON</b> .
Idle TimeOut	Enter the amount of time in seconds that the connection will disconnect when idle.
NetBIOS	Toggle to <b>ON</b> to allow NetBIOS broadcasts to travel over the VPN tunnel.
Save	Click to save your settings.

## Client

Path: VPN > PPTP VPN > Client

PPTP VPN Client can be configured on this router. Using this client you can access remote network which is local to PPTP server. Once client is enabled, the user can access Status > Active VPNs page and establish PPTP VPN tunnel clicking Connect.

To configure the router as a PPTP VPN client:

- 1. Click **VPN** > **PPTP VPN** > **Client** tab.
- 2. Toggle *Client* to **ON** and complete the fields in the table below.

fied Services Router - DSR-10	000N	Serial Q	.// W	zard System Search	٩
🖾 Status 🎅	Wireless 📃 Network	CA VPN	Security	© Maintenance	
» PPTP VPN » Client				0	
VPN Client can be configured o	on this router. Using this client we c	an access remote n	etwork which is local	to PPTP server.	
P Client					
lient	OK T				
Server IP	0.0.0.0				
Server IP Remote Network	0.0.0.0				
Server IP Remote Network Remote Netmask	0.0.0.0 0.0.0.0 0 [Range: 0	9 - 32]			
ierver IP Remote Network Remote Netmask Jsername	0.0.0.0 0.0.0.0 0 [Range: 0 dlink	J - 32]			
ierver IP Remote Network Remote Netmask Jsername Password	0.0.00 0.0.00 0 [Range: 0 dlink	0 321			
server IP Remote Network Remote Netmask Username Assword Mppe Encryption	0.0.0 0.0.0 0 [Range: ( dlink •••••	) - 32]			
ierver IP Remote Network Remote Netmask Jsername Password Mppe Encryption dle Time Out	0.0.0 0.0.0 0 [Range: ( dlink ••••• 0 [Range: ] 0 [Range: ]	) - 32]			

Field	Description
Client	Toggle to <b>ON</b> to enable PPTP client.
Server IP	Enter the IP address of the PPTP server you want to connect to.
Remote Network	Enter the remote network address. This address is local for the PPTP Server.
Remote Netmask	Enter the remote network subnet mask.
Username	Enter your PPTP user name.
Password	Enter your PPTP password.
MPPE Encryption	Toggle to ON to enable Microsoft Point-to-Point Encryption (MPPE).
Idle Time Out	Enter the amount of time (in seconds) that you will disconnect from the PPTP server when idle.
Save	Click <b>Save</b> to save and activate your settings.

### **PPTP Active Users List**

A list of PPTP connections will be displayed on this page. Right-click the connection to connect and disconnect.

D-Link Unified Services Router	DSH 1000N		Logged in as: Seriat Off	admin (ADMIN)   Lanij 20143000007   Firmva 20143000007   Firmva	guage: English (US) re: 1.108006E.wW zord System Search	y Leput
🙆 Status	💎 Wireless	Network	CA VPN		O <sup>o</sup> Maintenance	
Active PPTP tunnels connect PPTP Active Users List	tions are listed here, as l	LAN VPH clients are	active PPTP users,			00
Show 10 + entries	(No right dick options)					۹.
User Name	0	Remote IP.		8 PPTP	(P	e
and the second se		No data a	vailable in table		_	_
Showing 0 to 0 of 0 entries					Int <sup>(1</sup> ) Insection	S. Markill

# L2TP VPN Server

#### Path: VPN > L2TP VPN > 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, PPTP 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.

The range of IP addresses allocated to L2TP clients can coincide with the LAN subnet. As well the L2TP server will default to local L2TP user authentication, but can be configured to employ an external authentication server should one be configured.

To create a L2TP VPN server:

- 1. Click VPN >L2TP VPN > Server.
- 2. Complete the fields in the table below and click **Save**.



Field	Description
Enable L2TP Server	Select either IPv4 or IPv6.
L2TP Routing Mode	Select either <b>NAT</b> or <b>Classical</b> .
Starting/Ending IP Address	Enter the IP address range to assign your L2TP clients.
IPv6 Prefix	If you selected IPv6, enter the IPv6 prefix.
IPv6 Prefix Length	If you selected IPv6, enter the IPv6 prefix length.
Authentication	Select the authentication type from the drop-down menu.
Authentication Supported	Toggle which type of authentication you want to enable to <b>ON</b> .
Idle TimeOut	Enter the amount of time in seconds that the connection will disconnect when idle.
NetBIOS	Toggle to <b>ON</b> to allow NetBIOS broadcasts to travel over the VPN tunnel.
Save	Click to save your settings.

## Client

L2TP VPN Client can be configured on this router. Using this client we can access remote network which is local to L2TP server. Once client is enabled, the user can access Status > Active VPNs page and establish L2TP VPN tunnel clicking Connect.

To configure the router as a L2TP VPN client:

- 1. Click **VPN** > **L2TP VPN** > **Client** tab.
- 2. Toggle *Client* to **ON** and complete the fields in the table below.

ified Services Router - DSR-10	000N	Serial: Q	281A3000007   Firmwa	izard System Search
🖾 Status 🎅	Wireless 📃 🖳 Network	CA VPN	Security	O <sup>o</sup> Maintenance
» L2TP VPN » Client				0
VPN Client can be configured o	n this router. Using this client we c	an access remote n	etwork which is local	to L2TP server.
P Client				
Client	OK T			
Client Server IP	0.0.0.0			
Client Server IP Remote Network	0.0.0.0			
Client Server IP Remote Network Remote Netmask	он 0.0.0.0 0.0.0.0 0.0.0.0 [Range:	0 - 32]		
Client Server IP Remote Network Remote Netmask Username	он 0.0.0.0 0.0.0.0 0 [Range: dlink	0 - 32]		
Client Server IP Remote Network Remote Netmask Username Password	Сн 0.0.0.0 0.0.0.0 0 [Range: I dlink	0 - 32]		
Client Server IP Remote Network Remote Netmask Username Password Reconnect Mode	0.0.0.0 0.0.0.0 0 [Range: I dlink •••••	0 - 32]		
Client Server IP Remote Network Remote Netmask Username Password Reconnect Mode Enable MPPE	0.0.0.0 0.0.0.0 0 [Range: I dlink ••••• @ Always On © On	0 - 32)		

Field	Description
Client	Toggle to <b>ON</b> to enable L2TP client.
Server IP	Enter the IP address of the L2TP server you want to connect to.
Remote Network	Enter the remote network address. This address is local for the L2TP Server.
Remote Netmask	Enter the remote network subnet mask.
Username	Enter your L2TP user name.
Password	Enter your L2TP password.
Reconnect Mode	Select Always On or On Demand.
MPPE Encryption	Toggle to <b>ON</b> to enable Microsoft Point-to-Point Encryption (MPPE).
Save	Click <b>Save</b> to save and activate your settings.

### L2TP Active Users List

A list of L2TP connections will be displayed on this page. Right-click the connection to connect and disconnect.

D-Link Darfled Services Router - DSR-1000N		Logged in as: Serial: QD1	admin ( ADAVIA )   Lan 19143000007   Firmwa 19143000007   Kirmwa	re:   108006E WW	) Lugout
🙆 Status 🛜 Wireless	Network	Ca VPN	Security	© <sup>o</sup> Maintenance	
Active L2TP tunnels connections are listed here, as LA L2TP Active Users List	N VPN clients are a	active L2TP users.			00
Show 10 💌 entries [No right click options]					٩
User Name Ö	Remote IP		e L2TP	IP	e
	No data av	ailable in table			-
Showing 0 to 0 of 0 entries			111	The of Printers ( Hear)	k ( Gest ki

# SSL VPN Server 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 IP 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).

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.

**Note:** You must enable Remote Management. Refer to "Remote Management" on page 172.

To create a new SSL VPN policy:

- 1. Make sure you have enabled remote management and have created user(s) and group(s) to assign to this policy.
- 2. Click VPN > SSL VPN > SSL VPN Server Policy.
- 3. Click Add New SSL VPN Server Policy.

Unified S	ink ervices Router -	DSR-1000N		Logged in a Serial:	as: admin (ADMIN)   La Q8281A3000007   Firmv	anguage: English [US] 0 L vare: 2.008001E_WW /izard System Search	ogout Q
	🖾 Status	🛜 Wireless	Retwork	CA VPN	Security	<b>©</b> <sup>o</sup> Maintenance	
N N SSL	/PN » SSL VPN Ser	ver Policy					00
sources, I as already SL VPN S	P addresses, or IF configured over a erver Policies	nables Option users networks. They may ill addresses and ove List Flight click on record	to use SSLVPN function y be defined at the user ir all services/ports	uity.Policies are	al level. By Default, a gl	ny access to specific netwo	olayed)
SL VPN S	P addresses, or IF configured over a erver Policies	nables Option users in retworks. They may ill addresses and ove List [Right click on record	to use SSLVPN functions y be defined at the user ir all services/ports to get more options]	htty.Policies are	al level. By Default, a gl	ny access to specific netwo	olayed) Q
sources, I as already SL VPN S Show 10 Name	erver Policies	nables Option users ' networks. They may ill addresses and ove List [Right click on record ce $\Theta$	to use SSLVPN function; ye defined at the user or all services/ports to get more options] Destination	uty.Poucies are , group or globa ⊖	Permission	eccess to specific netwo obal PERMIT policy (net disp ecception of the specific network) ecception of the specific network of	olayed) Q
sources, I as already SL VPN S Show 10 Name	Paddresses, or IF configured over z erver Policies entries	nables Option users ' networks. They may ill addresses and ove List [Right click on record ce $\widehat{\Theta}$	to use SLVPN function, ybe defined at the user r all services/ports to get more options] Destination No data av	uty.Poucies are , group or globa ⊜ aïlable in table	Permission	ny access to specific netwo obal PERMIT policy (not disp Ə Scope	olayed) م
SL VPN S Show 10 Name Showing 0 to	Paddresses, or li configured over a erver Policies ervier S Servier of 0 of 0 entries	nables Option Users in networks. They may ill addresses and ove List [Right click on record ce 0	to use SLUPP function, ybe defined at the user r all services/ports to get more options] Destination No data av	alty.Policies are , group or globa allable in table	Permission	erit i Previus Hext -	Q Q Lest //

4. Complete the fields from the table below and click **Save**.

SSL VPN Server Policies Confi	puration	SSL VPN Server Policies C	onfiguration	8
Policy Type SSL VPN Policy Apply Policy to Policy Name ICMP Port Range / Port Number Defined Resources Permission	Olsbai O Group O Oser      Hetmore Resyster      Tor      Perest O Deny:	Policy Type SSL VPH Policy Apply Policy Ta Policy Name IP Address ICMP Part Range / Part Number Pegin End Service Permission	Global © Group © User      PAddress      Demons F - 15523      Demons F - 15523      VPH Tunnet © Port Forwarding © 48      Peruit © Dery	
		Sam		Sove

Network Resource

IP Addres	s
-----------	---

Field	Description
Policy Type	Select Global, Group, or User.
Available Groups/Users	If you selected Group, select a group from the drop-down menu. If you selected User, select a user from the drop-down menu.
Apply Policy To	Select Network Resource, IP Address, IP Network, or All Addresses.
Policy Name	Enter a unique name for this policy.
IP Address	If you selected IP Address or IP Network, enter the IP address.
Mask Length	If you selected IP Network, enter the mask length (0-32).
ICMP	Toggle to <b>ON</b> to include ICMP traffic.
Begin/End	Enter a port range or leave blank to include all TCP and UDP ports. These fields are not available when selecting Network Resource.
Defined Resources	If you selected Network Resource, select the resource for the <i>Defined Resource</i> drop- down menu. If you have not created a resource, refer to "Resources" on page 112 to create a defined resource.
Service	Select either <b>VPN Tunnel</b> , <b>Port Forwarding</b> , or <b>All</b> . This field is not available when selecting Network Resource.
Permission	Select either <b>Permit</b> or <b>Deny</b> .
Save	Click to save your settings.

## **Portal Layouts**

Path: VPN > SSL VPN > Portal Layouts

You may create a custom page for remote VPN users that is viewed during authentication. You may include login instructions, services, and other details. Note that 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 web UI.

To create a new portal layout:

- 1. Click VPN > SSL VPN > Portal Layouts.
- 2. Click Add New SSL VPN Portal Layout.

Unified Services Router -	DSR-1000N		Logged in Serial:	as: admin ( Al QB2B1A30000	DMIN)   Lan 107   Firmwa 1107 Wi	nguage: English [US]	) Logout
🖾 Status	🛜 Wireless	🖳 Network	CA VPN	B s	ecurity	O° Maintenance	
PN » SSL VPN » Portal Layo	uts		-				00
re specific to a domain are a	useful to present on th	e authentication por	tal. Portals are	assigned to th	ne user dom	ain.	curts criac
re specific to a domain are SL VPN Portal Layouts Show 10 💽 entries	useful to present on th List [Right click on record to	e authentication por get more options]	tal. Portals are :	assigned to th	ie user dom	ain,	Q
re specific to a domain are SL VPN Portal Layouts Show 10 • entries Layout Name	useful to present on th List [Right click on record to O Use Cour	e authentication port get more options] nt	al. Portals are	assigned to t	ie user dom	ain.	مین و
re specific to a domain are of SL VPN Portal Layouts Show 10 rentries Layout Name SSLVPN	useful to present on th List [Right click on record to O Use Cour 0	e authentication port get more options] nt é	<ul> <li>Portal uRL</li> <li>https://0.0.0.</li> </ul>	assigned to th D:443/portal/SS	ie user dom <u>VPN</u>	ain.	۹.
re specific to a domain are in SL VPN Portal Layouts Show 10 rentries Layout Name SSLVPN Showing 1 to 1 of 1 entries	useful to present on th List [Right click on record to OUse Cour 0	e authentication por get more options] nt é	<ul> <li>Portal URL</li> <li>https://0.0.0.</li> </ul>	assigned to tl 0:443/portal/SS	VPN	z   -   Preńous   1   Next.)	Q ( ) Lest ()

Note: You may right-click a layout from the list and edit or delete a layout.

3. Complete the fields from the table on the next page and click **Save**.

#### Section 7 - VPN

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

Field	Description
Portal Layout Name	Enter a name for this portal. This name will be used as part of the path for the SSL portal URL. Only alphanumeric characters are allowed for this field.
Login Profile View	Select a login profile from the drop-down menu.
Portal Site Title	Enter 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	Enter a message you want to display.
Display Banner Message on Login Page	Toggle to <b>ON</b> to display the banner title and message or <b>OFF</b> to hide the banner title and message.
HTTP Meta Tags for Cache Control	Toggle to <b>ON</b> or <b>OFF</b> . This security feature prevents expired web pages and data from being stored in the client's web browser cache. It is recommended to toggle to ON.
Active X Web Cache Cleaner	Toggle to <b>ON</b> or <b>Off</b> . An ActiveX cache control web cleaner can be pushed from the gateway to the client browser whenever users login to this SSL VPN portal.
Authentication Type	Select the type of authentication from the drop-down menu.
Group	Select what group to include from the drop-down menu.
VPN Tunnel Page	Toggle to <b>ON</b> to allow remote users to view this page.
Port Forwarding	Toggle to <b>ON</b> to allow remote users to view this page.
Save	Click to save your settings.

### Resources

Path: VPN > SSL VPN > 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.

### Add New Resource

To add a new resource:

- 1. Click VPN > SSL VPN > Resources.
- 2. Click Add New Resource.



3. Complete the fields from the table on the next page and click Save.

SL VPN Resources Configuration	1	X
SSL VPN Resources		
Resource Name		
Service	VPN Tunnel O Port Forwarding O All	
Resource Object Configuration		
ICMP	OFF	
Object Type	IP Network	
Object Address		
Mask Length	[Ranges 0 - 32]	
Port Range / Port Number		
Begin	[Range: 0 - 65535]	
End	[Range: 0 - 65535]	

Field	Description
Resource Name	Enter a unique name for this resource.
Service	Select VPN Tunnel, Port Forwarding, or All.
ICMP	Toggle to <b>ON</b> to include ICMP traffic.
Object Type	Select Single IP Address or IP Network.
Object Address	Enter the IP address.
Mask Length	If you selected IP Network, enter the mask length (0-32).
Begin/End	Enter a port range for the object.
Save	Click to save your settings.

### 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 tunnelled.

To add a port forwarding rule:

- 1. Click **VPN** > **SSL VPN** > **Resources**.
- 2. Click **Add New Rule** under either *Port Forwarding List for Configured Applications* (TCP Port) or under *Port Forwarding List for Configured Host Names* (FQDN).
- 3. Enter the IP address of the local server.
- 4. Next enter either the TCP port number or the domain name (FQDN).
- 5. Click Save.

Port Forwarding List for Con	figured Applications	0	Port Forwarding List for Host Configuration	0
Local Server IP Address TCP Pors Humber	Propri (1-2023)		Local Server IP Address Futty Qualified Opmain Name	
		Śnie		Sove

### Client

Path: VPN > SSL VPN > 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 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.

To configure client mode:

1. Click VPN > SSL VPN > SSL VPN Client.

D-Link Unified Services Router - DSR-1000N		Logged in as: admin (ADMIN)   Language: English [US] Services Router - DSR-1000N Serial: OB281A3000007   Firmware: 2.008001E_WW Wizard System Sear			nguage: English [US] O Logout are: 2.006001E_WW /izard System Search 9,
🖾 Status	🛜 Wireless	🖳 Network	CA VPN	A Security	O Maintenance
PN » SSL VPN » SSL VPN Client pr n SSL VPN tunnel client pr sunched from the user por pplications to talk to servi	lient ovides a point-to-point tal, a "network adapter" ces on the private netw	connection between 'with an IP address, E ork without any speci	the browser-side ma NNS and WINS settin ial network configu	achine and this devic gs is automatically cr ration on the remote	e. When a SSL VPN client is eated, which allows local SSL VPN client machine.
Full Tunnel Support DNS Suffix	I	204			
Primary DNS Server Secondary DNS Server Client Address Range B	egin	192.168.251 1			
Client Address Range E LCP Timeout	nd	192.168.251.254 60 [Range:	1 - 999999] Seconds		
		Save	Cancel		

- 2. Toggle Full Tunnel Support to ON to support full tunnel or OFF to enable split tunnel.
- 3. Enter a DNS suffix to assign to this client (optional).
- 3. Enter a primary and secondary DNS server addresses (optional).
- 4. Enter the range of IP addresses clients will be assigned (DHCP).
- 5. Next to LCP Timeout, set the value for LCP echo interval (in seconds).
- 6. Click **Save**.

## **Client Routes**

Path: VPN > SSL VPN > SSL VPN Client

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 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.

#### To configure a client route:

- 1. Click **VPN** > **SSL VPN** > **Client Routes**.
- 2. Click Add New Client Route.

VPN	Security	Q <sup>o</sup> Maintenance	00
			00
tion subnet or	n this device.		q
0.54			
O Sup	net Mask		4
able			
	by the SSL VP ected using th ent. For exam tion subnet or O Sub	by the SSL VPN Client such that excted using the hosts (SSL VPN of ent. For example if the SSL VPN i tion subnet on this device.	by the SSL VPN Client such that only traffic to these de excted using the hosts (SSL VPN Client) native network i ent. For example if the SSL VPN Client wishes to access tion subnet on this device.

- 3. Enter the destination network and subnet mask.
- 4. Click **Save**.

5L VPN Client Route Config	uration	
Destination Network Subnet Mask		
		Save

# Open VPN Settings

#### VPN > OpenVPN > Settings

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/ password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. An OpenVPN can be established through this router.

You can select server mode, client mode, or access server client mode. In access server client mode, the user has to download the auto login profile from the OpenVPN Access Server and upload the same to connect.

#### Server

To configure the router as an OpenVPN Server:

- 1. Click VPN > OpenVPN > Settings.
- 2. Toggle *OpenVPN* to **ON** and complete the fields in the table below.

D-Link UNITed Bergstan Admited Berg (1968)			Logged in at: (((())) (((()))) (()) ((())) (()) (()		
	P wieles	Hetwark-	C VPH		O <sup>o</sup> Maintenance
/PN - OpenVPN - Setzings					0
	186	Please Enable R	equired Certifica	tes	
OpenVPN configuration page al OpenVPN Settings	lives the user to co	ifigure OpenVPN as a se	erver or client.		
OpenVPH					
Mode		· Server @ Client	C Access Server	Client	
VPN Network		128.10.0.0			
VPN Netwask		255 258 0 D			
Post		1154 (Detaut)	114/ Barger 1214 - ANTE		
Tunnel Pratocal		10 TOP # 1004			
Terrentles Househing		BF-CBC	12		
Encryption Algorithm					
Hash Algorithm		SHAL			
Hash Algorithm		Full Tunnel C Si	elit Tunnel		
Hash Algorithm Tunnel Type Certificates		SHAL Full Tunnel Si	plit Tunnel		

Field	Description
Mode	Select Server.
VPN Network	Enter the IP network for the VPN.
VPN Netmask	Enter the netmask.
Port	Enter what port to use. The default port is 1194.
Tunnel Protocol	Select either <b>TCP</b> or <b>UDP</b> .
Encryption Algorithm	Select the encryption algorithm from the drop-down menu.
Hash Algorithm	Select the hash algorithm from the drop-down menu.
Tunnel Type	Select either <b>Full Tunnel</b> or <b>Split Tunnel</b> . 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. If you select Split Tunnel, refer to "Local Networks" on page 120 to create local networks.
Save	Click <b>Save</b> to save and activate your settings.

### Client

To configure the router as an OpenVPN client:

- 1. Click VPN > OpenVPN > Settings.
- 2. Toggle *OpenVPN* to **ON** and complete the fields in the table below.

	Wireless 📃 Network (	🚯 VPN 🔮 Security	O° Maintenance
» OpenVPN » Settings			0
	Please Enable Requ	ired Certificates	
nVPN configuration page allows	the user to configure OpenVPN as a server	or client.	
enVPN Settings			
OpenVPN			
Mode	Client 0	Access Server Client	
Server IP			
Best	1194		
Port	TUSA [Default: 1194,1	Kange: 1024 - 66535]	
Tunnel Protocol		1	
Encryption Algorithm			
Hash Algorithm	SHAT		
Certificates			

Field	Description
Mode	Select Client.
Server IP	Enter the IP address of the OpenVPN server.
Port	Enter what port to use. The default port is 1194.
Tunnel Protocol	Select either <b>TCP</b> or <b>UDP</b> .
<b>Encryption Algorithm</b>	Select the encryption algorithm from the drop-down menu.
Hash Algorithm	Select the hash algorithm from the drop-down menu.
Save	Click <b>Save</b> to save and activate your settings.

### **Access Server Client**

To configure the router as an OpenVPN access server client:

- 1. Click **VPN** > **OpenVPN** > **Settings**.
- 2. Toggle *OpenVPN* to **ON** and complete the fields in the table below.

	<ul> <li>Wireless</li> </ul>	📃 Network	C VPN	Security	Maintenance	
• • OpenVPN • Settings						2
enVPN configuration page	allows the user to con	nfigure OpenVPN as a se	rver or client.			
enVPN Settings						
OpenVPN		CH				
Mode		Server O Client	Access Serve	er Client		
Port		1194 [Default: 1	194. Range: 1024 - 655.	15]		
Jpload Access Server C	lient Configuration					
Upload Status		No				
File		Browse No file selected				
		Upload				
		opioud				
Certificates			1		1	
certificates	and the second se					

Field	Description
Mode	Select Access Server Client.
Port	Enter what port to use. The default port is 1194.
Upload Status	Displays if a configuration file has been uploaded.
File	Click Browse and locate the configuration file. Click Open and then click Upload.
Save	Click <b>Save</b> to save and activate your settings.

## **Local Networks**

If you selected Split Tunnel (from OpenVPN Server), you can create a local network by following the steps below:

- 1. Click VPN > OpenVPN > Local Networks.
- 2. Click Add New OpenVPN Local Network.



- 3. Enter a local IP network.
- 4. Enter the subnet mask.
- 5. Click **Save**.

OpenVPN Local Network	onfiguration	0
Local Network Subnet Mask		
		Save

## **Remote Networks**

To create remote networks:

- 1. Click VPN > OpenVPN > Remote Networks.
- 2. Click Add New OpenVPN Remote Network.

D-Link Unified Services Router - DSR-1000N			Logged in as: admin (ADMIN)   Language: English [US] O Logout Serial: QB2B1A3000007   Firmware: 2.006001E_WW Wizard System Search. Q.			Logout
🙆 Status	🛜 Wireless	📃 Network	CB VPN	Security	<b>©</b> <sup>o</sup> Maintenance	
2N » OpenVPN » Remote Ne	etworks	e user can also add.	lelete and edit ne	tworks from this page		0 0
penVPN Remote Netwo	orks List					
penVPN Remote Netwo	orks List [Right click on record to	get more options]				٩
penVPN Remote Netwo	Porks List [Right click on record to Q R	get more options] emote Network		⊖ Subn	et Mask	٩.
penVPN Remote Netwo Show 10 • entries Common Name	Porks List [Right click on record to Q R	get more options] emote Network No data av	ailable in table	e Subne	et Mask	م 6
penVPN Remote Netwo Show 10 rentries Common Name Showing 0 to 0 of 0 entries	orks List [Right click on record to O R	get moré options] eemote Network No data av	ailable in table	e Subri	et Mask	Q e Last y

- 3. Enter a name of the remote network.
- 4. Enter a local IP network.
- 5. Enter the subnet mask.
- 6. Click **Save**.

onfiguration	
	Save
	ontiguration

### Authentication

This page will allow you to upload certificates and keys. Click **Browse** and select the file you want to upload. Click **Open** and then click **Upload**.

Unified Services Router - DSR-1000N		Logged in as: admin (ADMIN)   Language: English [US] Router - DSR-1000N Serial: Q8281A3000007   Firmware: 2.008001E_WW Wizard System Sear		nguage: English [US] (O Logout are: 2,008001E_WW izard System Search Q		
	🖾 Status	🛜 Wireless	📃 Network	CAS VPN	Security	O <sup>o</sup> Maintenance
N » ( penvpn penVl	OpenVPN » Authentical provides authenticat PN Authentication	tion ion using certificate	s. This page allows you	to upload required	i certificates and key	o (
Trust	ed Certificate (CA ) tificate Status	Certificate)	No			
Brow	wse Certificate File		Browse_ No file selected	4.		
Serve Cert Brot	er / Client Certifica tificate Status wse Certificate File	te	No Browse_No file selected Upload	ł.		
Serve	er / Client Key Status		No			
Brow	wse Key File		Browse_ No file selecter	d.		
DH Ke	۶y		Upload			
Key Broy	Status wse Key File		Na Browse No file selecter	d		
TIS Au Key	uthentication Key Status		Upload			
Brow	wse Key File		Browse No file selected	d.		
			Upload			

# GRE

VPN > VPN Settings > GRE

GRE tunnels allow for broadcast traffic on the LAN of the router to be passed over the internet and received by remote LAN hosts. This is primarily useful in the D-Link Discovery Protocol (DDP) application where broadcast traffic from one LAN host is to be received by all LAN hosts in the local subnets of the GRE endpoints.

Note the following limits for the number of supported GRE tunnels per product:

- DSR-150/150N: 5
- DSR-250/250N: 10
- DSR-500/500N: 15
- DSR-1000/1000N: 20

There are two simple steps involved in establishing a GRE tunnel on the router:

- 1. Create a GRE tunnel from the GUI
- 2. Setup a static route for the remote local networks using the GRE tunnel

When creating the GRE tunnel, the IP Address should be a unique address that identifies that GRE tunnel endpoint. It will be referenced in the other router's static route as the Gateway IP address. The Remote End Address in the GRE tunnel configuration page is the WAN IP address of the other endpoint router.

Once the tunnel is established, a static route on the router can be made using the interface set to the configured GRE tunnel name. The destination IP address of the static route is the remote LAN subnet, and the route's gateway IP address will be the GRE tunnel IP of the terminating router (the same router that manages the remote LAN subnet). Once these two steps are completed, all DDP broadcast traffic can flow between remote LAN subnets via the GRE Tunnel.

To create a GRE tunnel:

- 1. Click **VPN** > **GRE** > **GRE Tunnels**.
- 2. Click Add New GRE Tunnel.

<b>D-Link</b> Unified Services Route	Logged in as Serial: (	Logged in as: admin ( ADMIN )   Language: English [US] O Logout Serial: QB2B1A3000007   Firmware: 2.008001E_WW Wizard System Search Q		
🖾 Status	🛜 Wireless 📃 Ne	etwork 🚯 VPN	Security	🍄 Maintenance
PN » GRE » GRE Tunnels his page allows user to ad GRE Tunnels List Show 10 v entries	d/edit GRE tunnel configuration.	tions]		00
	t spectral contract of ground of			4
Tunnel Name	🔂 Inte	erface	⊖ Remote	IP \varTheta
		No data available in table		
Showing 0 to 0 of 0 entries				First   Previous Next > Last >
Add New GRE Tunnel				

3. Complete the fields in the table below and then click **Save**.

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

Field	Description
GRE Tunnel Name	Enter a name for the tunnel.
IP Address	Enter the IP address of this endpoint. It will be referenced in the other router's static route as the Gateway IP address.
Subnet Mask	Enter the subnet mask.
Interface	Select the interface to create this tunnel with from the drop-down menu.
Remote End Address	Enter the WAN IP address of the endpoint router.
Enable DDP Broadcast	Toggle to <b>ON</b> to enable DDP broadcasting.
IP Address	Enter the destination IP address of the static route from the remote LAN subnet.
Subnet Mask	Enter the subnet mask.
Gateway IP Address	Enter the IP address of the termination router.
Save	Click <b>Save</b> to save and activate your settings.

# Security Groups

Path: Security > Authentication > User Database > Groups

The group page allows creating, editing, and deleting groups. The groups are associated to set of user types.

To edit/delete an existing group, or add a new group:

1. Click Security > Authentication > User Database > Groups tab.

D-Link Liathed Services Router - 058-7000H		Logged In as: John ( AMM )   Language: Logist (0) () () () topol Serial: Josef Added - Finnware: 1.150504.ww System Secon. 9.			(Lagoul)	
	P Wielen	🔟 Network		e security	OP Maintenance	
curity = Authentication =	User Database - Groups					00
tis page shows the list of a roups List Show 10 + entries	(Right dick on record to	ter. The user can add get more options)	l, delete and adli I	ke groups also.		q
Group Name			Description			
ADMIN	-		Admin Group			-
GUEST			Guest Group			
Shinwing 1 to 2 of 2 entries					- 11 Bl	
Add New Group						

- 2. Right-click a group entry and select either Edit or Delete. To add a new group, click Add New Group.
- 3. Complete the fields in the table below and click **Save**.

Group Configuration		Group Configuration	
Group Name		Group Name	
Description		Description	
User Type User Type	* Admin O Herwark O Frank Deck D Guest	User Type User Type	O Adam # Network O Front Desk O Guest
PPTP User	- INI	PPTP User	- M
LITP User		L2TP User	
SSLVPN User	34	Xauth User	( W)
Captive Portal Uses	an l	SSEWPH User	an l
Idle Timenut	10 (Section 11, manual 11, manual section)	Capitive Portal User	
		idle Timeout	10 (Settion: 10, January 1, 319) Molecular
	Sav		4

Admin User Type

Network User Type

Field	Description
Group Name	Enter a name for the group.
Description	Enter a description for the group.
User Type	<ul> <li>Select the user type:</li> <li>Admin - Grants all users in this group super-user privileges. By default, there is one admin user.</li> <li>Network - Grants the next level of privileges.</li> <li>Front Desk - Grants permissions to create temporary users who can Internet/network access (Hotspot).</li> <li>Guest - Guest users will only have read access.</li> <li>Network and Admin users can toggle <b>ON</b> PPTP, L2TP, Xauth (Network only), SSLVPN, and Captive Portal.</li> </ul>
Idle Timeout	Enter the number of minutes of inactivity that must occur before the users in this user group are logged out of their web management session automatically. Entering an Idle Timeout value of 0 (zero) means never log out.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

### **Login Policies**

Path: Security > Authentication > Internal User Database > Groups

Using the following procedure, you can grant or deny a user group login access to the web management interface.

1. Click Security > Authentication > Internal User Database > Groups tab.

Show 10 • entries			Q
Group	Û	Status	θ
ADMIN		Allow	
GUEST		Deny	
Showing 1 to 2 of 2 entries			First    Previous    Next > Last >

2. Click Add Login Policies.

gin Policies Configuration		
Group Name Disable Login Deny Login from Option Interface	ADMIN OFF OFF	
		Save

3. Complete the fields from the table below and click **Save**.

Field	Description
Group Name	Select the group you want to configure.
Disable Login	Toggle <b>ON</b> to deny login access to the web management interface for all users in this user group. Toggle <b>OFF</b> will allow users to log in.
Deny Login from Option Interface	Toggle <b>ON</b> to deny login access to the web management interface from the WAN2/DMZ Port for all users in this user group. Toggle <b>OFF</b> will allow users.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

### **Browser Policies**

Path: Security > Authentication > Internal User Database > Groups

Use this feature to allow or deny users in a selected group from using a particular web browser to log in to the router's web management interface.

1. Click Security > Authentication > Internal User Database > Groups tab.

Show 10 💌 er	ntries			٩
Group	🗘 🛛 Added Client B	Browsers	⊖ Status	
		No data available in table		
Showing 0 to 0 of 0	entries		First    Previous    Next	Last >

#### 2. Click Add Browser Policies.

Browser Policies Configurati	on	8
Group Name Add Defined Browser Client Browser	ADMIN	
		Save

3. Complete the fields from the table below and click **Save**.

Field	Description
Group Name	Select the group you want to configure from the drop-down menu.
Client Browser	Select a web browser from the drop-down menu.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

4. Your policy will now be in the browser policies list. By default the status will be set to deny. If you want to set the status to allow, right-click the policy and select **Allow**.

## **IP Policies**

Path: Security > Authentication > Internal User Database > Groups

Use this feature to allow or deny users in a user group to log in to the router's web management interface from a particular network or IP address.

#### 1. Click Security > Authentication > Internal User Database > Groups tab.

Show 10	▼ entries					Q
Group	Source Address Type	θ	Network Address / IP Address	Θ	Mask Length	\varTheta Status 🤤
			No data available in table			_
Showing 0	to 0 of 0 entries				First   Previo	aut Next & Last 2

2. Click Add IP Policies.

Porteies contributation		0
Group Name	ADMIN	
efined Address Configuration Source Address Type	IP herwork	
Retwork Address / IP Address		
Mask Length	32 (Tolernit hings: 0)	

in policies configuration		0
Group Name	ADMON	
Defined Address Configuration Source Address Type	IP Address	
Network Address / IP Address		

3. Complete the fields from the table below and click **Save**.

Field	Description
Group Name	Select the group you want to configure from the drop-down menu.
Source Address Type	Select either <b>Network</b> to specify a IP network or <b>IP Address</b> to specify a specific IP address.
Network Address/IP Address	Enter the network address or IP address.
Mask Length	If you selected <i>Network</i> , enter the mask length.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

# Users User Management

Path: Security > Authentication > Internal User Database > Users

After you add user groups, you can add users to the user groups. Users can be added individually, or they can be imported from a comma-separated-value (CSV) formatted file. After you add users, you can edit them when changes are required or delete users when you no longer need them.

To edit/delete existing users, or add a new user:

1. Click Security > Authentication > Internal User Database > Users tab.

					Native System Search	٩
🖾 Status	😤 Wireless	Hetwork		A Security	OP Maintenance	
ecurity - Authentication	- User Database - Users	1				
Gies Uxer Die Group	Users					
Bet User DE Groups his page shows a list of a n users.	vailable users in the sys	tem: A user can add, de	lete and edit the	ucers also. This page	can also be used for setti	ing polici
Bot User De Group his page shows a list of a n users. sers List	vallable users in the sys	tem. A uter can add, de	lete and edit the	users also. This page	can also be used for setti	ing palle
tion User Diff Group his page shows a list of a n users. Isers List Thow 10 • entries	Users valiable users in the sys (Right click on record)	ten: A user can add, de In gel more uptions]	lete and edit the	users also. This page	can also be used for setti	ing polici
Bet User All Group his page shows a list of a users List how 10 e	(Right dick on record)	tem: A user can add, de Ingel nore spilons] 1	lete and edit the	usørs also. This page	can also be used for settl	ing polici
Bot User DE Group his page shoes a list of a sers. Sers List Door <u>10 e</u> entries User Name admin	Digits chick on recent	ten: A user can add, de In get mure uptium) 1 É	ete and edit the	users also. This page habing (OPTION)	can also be used for setti	ing polici
Bet Vien PE Group his page shows a list of a nears. sens List Drive 16 entries Uter Hame selon punt	Payers wallable users in the sys (Right rick on record -O. Group Nam Azwan GUIST	ten: A user can add, de In gel mure spilum)	lete and edit the A Login Statu Enabled (LNI) ( Disabled (LNI) (	uters also. This page nabled (OPTION) Robled (OPTION)	can also be used for cetti	ing polici

2. Right-click a group entry and select either Edit or Delete. To add a new group, click Add New User.

User Name		
First Name		
Last Home		
Select Group	TestGraus)	
Password		
Confirm Patsword		

3. Complete the fields from the table below and click **Save**.

Field	Description
User Name	Enter the user name for this user. This name is a unique identifier
First Name	Enter the user's first name.
Last Name	Enter the user's last name.
Select Group	Select the group you want to assign this user to from the drop-down menu.
Password	Enter a case-sensitive login password that the user must specify at the login prompt to access the web management interface. For security, each typed password character is masked with a dot (•).
Confirm Password	Enter the password to confirm.
Save	Click <b>Save</b> at the bottom to save and activate your settings.

## Import User Database

Path: Security > Authentication > Internal User Database > Get User DB

The DSR administrator can add users to the local built-in database directly via an appropriately-formatted comma separated value (CSV) file. The advantage of this feature is to allow for a large number of users to be added to the system with one operation, and the same file can be uploaded to multiple DSR devices as needed. Once uploaded the specific users in the local user database can be modified via the GUI as needed.

To import a user database:

1. Click Security > Authentication > Internal User Database > Get User DB tab.

D-Link Unified Services Router- DSN-1000N		Logged In as: admite ( ADMIN )   Language: English [US] () Legnist Serial: 2020(A3000007   Firmware: 1.1080005_WW Witzard System Search 9				
🙆 Status	🛜 Wireless	Network	CA VPN	Security	O <sup>o</sup> Maintenance	1
Security = Authentication = Get User DB Groups	User Database = Get Un	er D6				
This page allows user to imp Get User DB	ort a CSV formatted us	er database to the rou	ter.			
Select User DB File		Browse. ] No file selecte	d.			

- 2. Click Browse and locate the file you want to upload. Select it and click Open.
- 3. Click **Upload**.
- 4. Once completed, go to **Security** > **Authentication** > **User Database** > **Users** and your imported users will be displayed in the Users List.
- 5. From the list you can right-click the user to edit or delete.

## Create a User Database (CSV File)

The following parameters must be used to define the User database CSV file.

- 1. Create an empty text file with a .csv extension.
- 2. Each line in the file corresponds to a single user entry. Every line should end with carriage return equivalent of CRLF. Do not add comments or other text in this file.
- 3. Formatting rules:
  - a) All the fields must be enclosed within double quotes.
  - b) Consecutive fields are separated by commas.
  - c) There should be no leading or trailing spaces in a line.
  - d) There should be no spaces between fields.

Each line in the CSV user database file should follow the following format:

"UserName","FirstName","LastName","GroupName","MultiLogin","Password"

The above sample has fields that can assume the following values:

- Username (text field): Name of the user and identifier in the DSR's database, and so it must be unique in the local user database.
- FirstName (text field): This is a user detail and need not be unique.
- LastName (text field): This is a user detail and need not be unique.
- GroupName (text field): The group that is associated with this user.
- MultiLogSup (Boolean value): With this enabled ("1"), then multiple users can share a single username and password.
- Password (text field): password to assign for this username
- The Group for a corresponding user ("GroupName" in the CSV) must be created via the GUI in advance of the User Database CSV upload action.
- None of the above fields can be left empty or NULL in the User Database CSV.
# External Authentication Servers RADIUS Server

Path: Security > Authentication > External Auth Server > RADIUS Server

A RADIUS server can be configured and accessible by the router to authenticate client connections.

To configure the router to connect to your RADIUS server:

1. Click Security > Authentication > External Auth Server > RADIUS Server tab.

D-Link		Legged in acc. which ( Addets / 1 Language: English (1/2) () Legent Gerlah: Coloris Lancely   Formany: 1 Classich, nor V <sup>6</sup> Witcold () (Spraw Spare), 0		
🙆 Status 🗣 W	nekas 💻 Herverk		Security	O <sup>p</sup> Maintenance
ity - Authentication - External Aut	h Server — Radius Server			0
	Conception and the local division of the	THE OWNER ADDRESS	-	
Lege configures the RADIUS servers anments. If a RADIUS server is confi ded by this device. If the first/pris is server for user authentication. Its Server Configuration.	to be used for authentication. A ipured in the LAN, it can be used any KADBUS server is not accessib	RACOUS server ma for authentication of at any time, th	intains a detabase of s guisers that want to c en the device will atte	oter accounts used in larger connect to the wireless network empt to contact the secondary
ierres Chazk	Server Checking			
Authentication Server IP Address	192 168 1.2			
Authentication Port	1812 (Pargar (	1.0.10		
incret		1		
Devenue	HOmmer 1	And Personal		
Desenant Lefeter	2 (Borns)	A Common		
Omensuk Refeks Authentication Server IP Address	1 Horner 1 2 (Bregg) ) 192,368.3.2	A Second		
Normal Refres Authentication Server IP Address Authentication Port	1 (former) 2 (former) 192,168,1.3 1612 (filmare)			
Omenaus Lefries Inuthentication Server (P. Address Inuthentication: Port Ieccet	1 (100mm) 2 (192,161,1,3 192,161,1,3 161,2 (00mm)	4)		
Owenus Lefrjes huthentikation Server (P Address huthentikation Port lefret Dimout	1			
Daenaus Lefryes Luthentication Server IP Address Luthentication Port Secret Daenaus Lebries	1         00mm           2         (prop)           192.161.1.3         (0mm)           192.2         (0mm)           1         (0mm)           2         (0mm)			
Dienzus Karlten Nuthentication Server IP Address Nuthentication Port Secret Dienzus Karles Nuthentication Server IP Address	1         00mm i           2         (0mm i)           192.168.1.3         (0mm i)           1012         (0mm i)           1         (0mm i)	4) ( 4.455) ( 19)		
linenan Ledrei Luithentication Server IP Address Luithentication Part Incont Ledrei Luithentication Server IP Address Luithentication Part	1 000000 2 1990apt) 1923-1613.2 1932-2 1932-2 1932-2 1932-2 1932-2 1932-2 1932-2 1932-2 1932-2 1932-2 1932-2 1932-2 1932-2 1930-2 19 19 19 19 19 19 19 19 19 19 19 19 19 1			
Dieneus) Refries Nathentication Port Secret Diecout Lebries Nathentication Server IP Address Nathentication Port	1 (00000) 2 (00000) 190-2162-1.3 190-2162 1 (00000) 2 (000000) 2 (000000) 2 (000000) 1902-144.14 1902-1010000 1902-101000 1902-100	in a second seco		
Tuenau) Refres Authentication Server IP Address Authentication Port Secret Tuerou! Authentication Server IP Address Authentication Port Secret Tuerou!	1         (0 count)           2         (0 reg)           192.168.1.3         (0 source)           1         (2 source)           2         (0 source)           192.168.1.4         (2 source)           192.168.1.4         (2 source)           1         (2 source)           1         (3 source)			

2. Complete the RADIUS server information from the table below and click **Save**. You can configure up to three servers.

Field	Description
Authentication Server IP Address	Enter the IP address of your RADIUS server.
Authentication Port	Enter the RADIUS authentication server port.
Secret	Enter the secret key that allows the device to log into the configured RADIUS server. It must match the secret on RADIUS server.
Timeout	Set the amount of time in seconds that the router should wait for a response from the RADIUS server.
Retries	This determines the number of tries the controller will make to the RADIUS server before giving up.
Save	Click <b>Save</b> at the bottom to save and activate your settings.
Server Check	Click to test the connection(s) to your RADIUS Server(s).

### **POP3 Server**

Path: Security > Authentication > External Auth Server > POP3 Server

POP3 is an application layer protocol most commonly used for e-mail over a TCP/IP connection. The authentication server can be used with SSL encryption over port 995 to send encrypted traffic to the POP3 server. The POP3 server's certificate is verified by a user-uploaded CA certificate. If SSL encryption is not used, port 110 will be used for the POP3 authentication traffic.

To configure the router to connect to your POP3 server:

1. Click Security > Authentication > External Auth Server > POP3 Server tab.

DELINK Ined Services Router DIR-1000N	Logged in as: admin (ADMRV) Language: English [US] Serual: QT281A3000007 Firmware: 1,00004E,WV W <sup>®</sup> V/tzard System See	O Logout
🙆 Status 😤 Wirele	a 🗮 Network 🚓 VPN 🖨 Security 👁 Maintenan	
rity = Authentication = External Auth Serve	r = POP3 Server	0 0
Radius Server POP3 Server POP3 Tr	sted CA LDAP Server AD Server HT Domain	
<sup>13</sup> Server Configuration		
Server Check	Server Checking	
Authentication Server1 (Primary)		
Authentication Port	110 (Default: 110, Alexand ( + 65535)	
SSL Enable	or core	
Authentication Server2 (Secondary)	Cintinnal	
Authentication Port	110 (Default: 110. Rangel, 1 (4553))	
SSL Enable	or	
Authentication Server3	(antiqC)	
Authentication Port	[110 [Deflault: 170] Parente 7 + 62535)	
SSL Enable	COT	
Timeout	(Range: 4 - 991) Seconds	
Retries	Hanger V 91	
	and the second se	

2. Complete the POP3 server information from the table below and click **Save**. You can configure up to three servers.

Field	Description
Authentication Server IP Address	Enter the IP address of your POP3 server.
Authentication Port	Enter the POP3 authentication server port.
SSL Enable	Toggle to <b>ON</b> to enable SSL support for POP3. If this option is enabled, it is mandatory to select a certificate authority for it.
CA File	Certificate Authority to verify POP3 server's certificate.
Timeout	Set the amount of time in seconds that the router should wait for a response from the POP3 server.
Retries	This determines the number of tries the controller will make to the POP3 server before giving up.
Save	Click <b>Save</b> at the bottom to save and activate your settings.
Server Check	Click to test the connection(s) to your POP3 Server(s).

### **POP3 Trusted Server**

Path: Security > Authentication > External Auth Server > POP3 Trusted CA

A CA file is used as part of the POP3 negotiation to verify the configured authentication server identity. Each of the three configured servers can have a unique CA used for authentication.

To configure:

1. Click Security > Authentication > External Auth Server > POP3 Trusted CA tab.

CCA Status	🛜 Wireless	Network	CB VPN	Security	<b>O</b> <sup>o</sup> Maintenance	
urity » Authentication »	External Auth Server	POP3 Trusted CA				0 0
Radius Server POP3	Server POP3 Trusted	CA LDAP Server A	D Server NT Domai	n		
s page shows the list of	POP3 CA Files.					
P3 CA Files List						
					-	
iow 10 💌 entries	[Right click on record to	get more options]				Q
now 10 💌 entries A File	[Right click on record to	get more options]				٩
now 10 💽 entries A File	[Right click on record to	get more options] No data ava	ailable in table			٩

2. Click Add CA File.

CA File Configuration		8
CA File	Browse_ No file selected.	
		Upload

3. Click **Browse** and select a CA file. Click **Open** and then click **Upload**.

### LDAP Server

Path: Security > Authentication > External Auth Server > LDAP Server

The LDAP authentication method uses LDAP to exchange authentication credentials between the router and an external server. The LDAP server maintains a large database of users in a directory structure, so users with the same user name but belonging to different groups can be authenticated since the user information is stored in a hierarchal manner. Also of note is that configuring a LDAP server on Windows or Linux servers is considerably less complex than setting up NT Domain or Active Directory servers for user authentication.

The details configured on the controller will be passed for authenticating the router and its hosts. The LDAP attributes, domain name (DN), and in some cases the administrator account & password are key fields in allowing the LDAP server to authenticate the controller.

To configure the router to connect to your LDAP server:

1. Click Security > Authentication > External Auth Server > LDAP Server tab.

D-Link	Knighed in asc Seriale in	Secular communications ( Adams )   Language: Trends (47)   (a) Language: Secular communications (17)   Fernication (17)   (b) Language (17)   Secular (17)   (b) Language (17)   (b) Langu			
🙆 States 🔶 Wi	eles. 📃 Netron	1 @ VTH	A Security	O <sup>o</sup> Maintenance	
ecurity - Authentication - External Auth	ierver - LDAP Server				
Radius Server POPS Server POP	TIUSTER CA LOAP SHIVE	Ale Salver HT De	main		
his page allows a user to configure authority	mtication servers for COMP.	authentication.			
DAP Server Configuration					
Server Cheza	Server Check	Hu			
Authentication Server 1	1				
Authentitation Server 2		Spiller			
Authentication Semar 2		Gammage			
LDAP Attribute 1	1	Opthical			
LDAP Attribute 2		Cational			
LDAP Astribute 3	E	(Drilling)			
LDAP Attribute 4		(press)			
LDAP Base DH	1				
Second LDAP Base DN	L	E-(Rima)			
Third LDAP Bess DH	L	Quitmit			
Timeout	. (Pair				
Retries	2 0.0	part of the second s			
First Administrator Account	admin	10000			
Password		Entimal			
Second Administrator Account	1	Sprinsie			
Pastword		(Divisional)			
Third Administrator Account	1	G-D (Type-4)			

2. Complete the LDAP server information from the table below and click **Save**. You can configure up to three servers.

Field	Description
Authentication Server (1-3)	Enter the IP address of your primary LDAP server.
LDAP Attribute (1-4)	These are attributes related to LDAP users configured in LDAP server. These may include attributes like SAM account name, associated domain name etc. These can be used to distinguish between different users having same user name.
LDAP Base DN	Enter the base domain name.
Timeout	Set the amount of time in seconds that the router should wait for a response from the LDAP server.
Retries	This determines the number of tries the controller will make to the LDAP server before giving up.
Save	Click <b>Save</b> at the bottom to save and activate your settings.
Administrator Account	Enter the admin account information that will be used when LDAP authentication is required for PPTP/ L2TP connection.
Server Check	Click to test the connection(s) to your LDAP Server(s).

### **AD Server**

Path: Security > Authentication > External Auth Server > AD Server

Active Directory authentication is an enhanced version of NT Domain authentication. The Kerberos protocol is leveraged for authentication of users, who are grouped in Organizational Units (OUs). In particular the Active Directory server can support more than a million users given is structure while the NT Domain server is limited to thousands. The configured Authentication Servers and Active Directory domain(s) are used to validate the user with the directory of users on the external Windows based server. This authentication option is common for SSL VPN client users and is also useful for IPsec / PPTP / L2TP client authentication.

To configure the router to connect to your AD server:

1. Click Security > Authentication > External Auth Server > AD Server tab.

ied Services Router - DSR-1000N		Serial: Q	32B1A3000007   Firmw	are: 1.108006E_WW
🖓 Status 🛜 Wire	less 📃 Network	CAS VPN	Security	0° Maintenance
y » Authentication » External Auth Se	rver » AD Server			
adius Server POP3 Server POP3 '	Trusted CA LDAP Server	AD Server NT Dor	main	
age allow to configure Active Directo	ry authentication servers.			
e Directory Configuration				
erver Check	Server Checking			
uthentication Server 1				
uthentication Server 2		Optional		
uthentication Server 3		Optional		
ctive Directory Domain				
econd Active Directory Domain		Optional		
hird Active Directory Domain		Optional		
meout	[Range:	- 999] Seconds		
etries	2 (Range:	1 - 9}		
rst Administrator Account		Optional		
assword		Optional		
rst Server Hostname		Optional		
cond Administrator Account	1	Optional		
ssword	[	Optional		
cond Server Hostname	1	Optional		
nird Administrator Account		Ontional		
ssword		Optional		
aird Convor Hortoomo	[	optional		
ing server nostname		Uptional		

2. Complete the AD server information from the table on the next page and click **Save**. You can configure up to three servers.

#### Section 8 - Security

Field	Description
Authentication Server (1-3)	Enter the IP address of your AD server(s).
Active Directory Domain (1-3)	Enter the active directory domain name(s).
Timeout	Set the amount of time in seconds that the router should wait for a response from the AD server.
Retries	This determines the number of tries the controller will make to the AD server before giving up.
Administrator Account	Enter the admin account information that will be used when authentication is required for PPTP/L2TP connection.
Save	Click <b>Save</b> at the bottom to save and activate your settings.
Server Check	Click to test the connection(s) to your AD Server(s).

### **NT Domain Server**

Path: Security > Authentication > External Auth Server > NT Domain

The NT Domain server allows users and hosts to authenticate themselves via a pre-configured Workgroup field. Typically Windows or Samba servers are used to manage the domain of authentication for the centralized directory of authorized users.

To configure the router to connect to your NT domain server:

1. Click Security > Authentication > External Auth Server > NT Domain tab.

D-Link Mod Services Rouger - 1958, 1000N	Loggod in ass Sertal: 0	Logged in az: -almin   Alahin     Langvage: Exclubit(US) O Liopial Serial: 19891(Alapino07)   Firmware: 1.198004E, WW Vitzard   System Search			
🕰 Stalus <table-cell> Wire</table-cell>	rless 📃 Metwork	GS VPH	Security	O <sup>p</sup> Maintenance	
rity - Authentication - External Auth S	erver = NT Domain			0	
Radius Server   POP3 Server   POP3	Insted CA LDA# Server	AD Servel NT Do	math		
Supervision in the second second	Construction Providence of the	and the second s			
page allow you to configure NT Dumain	r servers.				
Domain Configuration					
Server Check	Salver Sherkin				
Authentication Server 1					
Audiendeation Server 2	-	Optionie			
Authentication Server 1	-	Optimut			
Workgroup					
Second Workgroup		Optimal			
Third Workgroup	-	Dpliom4			
Timeout	(Raip	e 1 [mil] Sacanda			
Retries	2 (ILaug	n f - 91 Secondy			
First Administrator Account		Plananat			
Password		Optimus			
First Server Hostname		Optional			
Second Administrator Account		Optinosi			
Password		Optimon			
Second Server Hostname	Ē.	Detimal			
Third Administrator Account		Dirtional			
Password		Clatimut			
Third Campy Havings	ñ				
A MARK OF THE REAL PROPERTY OF		LAC DOMES			

2. Complete the NT server information from the table below and click **Save**. You can configure up to three servers.

Field	Description
Authentication Server (1-3)	Enter the IP address of your NT server(s).
Workgroup (1-3)	Enter the NT workgroup name(s).
Timeout	Set the amount of time in seconds that the router should wait for a response from the AD server.
Retries	This determines the number of tries the controller will make to the AD server before giving up.
Administrator Account	Enter the admin account information that will be used when authentication is required for PPTP/L2TP connection.
Save	Click <b>Save</b> at the bottom to save and activate your settings.
Server Check	Click to test the connection(s) to your AD Server(s).

# Login Profiles

Path: Security > Authentication > Login Profiles

When a wireless client connects to the SSIDs or VLANs, the user sees a login page. The Login Profile and SLA page allows you to customize the appearance of that page with specific text and images. The wireless router supports multiple login and SLA pages. Associate login page or SLAs on SSIDs or VLANs separately.

To add, delete, or edit login profiles:

1. Click Security > Authentication > Login Profiles tab.

D-Link Unified Services Router - DSR-1000N		Logged in as: Similati 🧃	Logged in as: #dmln ( ADANI )   Language: English (US) () Logo Sietals (2078) 43000007   Firmware: (1.08008F_WW Witzard () System Search.		
🙆 Status 🎅	Wireless 📕 Network	CA VPN	Security	OP Maintenance	
incurity = Authentication = Login Pro The table lists all the available Login ogin Profiles List Store 10	files Profiles in the system, This Logic	page is used for auth	mentication on Captive	Portal enabled interfa	e O
Profile Name	O Browser Title			e Status	9
default	D-link Unified Services Rou	ter		Not in Use	
default2	D-link Unified Services Rou	ter		Not In Use	
Showing 1 to 2 of 2 entries				LI Previous 1 mext	(cana) ( c
Add New Login Profile					

2. Right-click an entry and select either Edit or Delete. To add a new group, click Add New Login Profile.

rogin Promis configuration		C C
General Details Profile Name		
Brawser Title		
Background	· Image · Color	
Page Background Image		
	Default and Add and Add Add	
Minimal Page for Mobile Devices		
Header Details Background	🖲 image 👘 Cotor	
Header Background Image		
	Perform add add add add add	
	Add Add Add Add Add	
Header Caption		
Caption Font	Tahona .	
Font Size	5mail	
Font Color	Red	
Login Details Login Section Title	Fonal Login	
Welcome Message	Please Login1	
Error Message	Invalid UserName/Password	
Footer Details Change Footer Content		
Foater Content		
Footer Font Color	White	

3. Complete the fields from the table on the next page and click **Save**.

#### Section 8 - Security

Field	Description
	General Details
Profile Name	Enter a name for this captive portal profile. The name should allow you to differentiate this captive profile from others you may set up.
Browser Title	Enter the text that will appear in the title of the browser during the captive portal session.
Background	<ul> <li>Select whether the login page displayed during the captive portal session will show an image or color. Choices are:</li> <li>Image: Displays an image as the background on the page. Use the Page Background Image field to select a background image.</li> <li>Color: Sets the background color on the page. Select the color from the drop-down menu</li> </ul>
Page Background Image	If you set <i>Background</i> to <b>Image</b> , upload the image file by clicking <b>Add</b> > <b>Browse</b> . Select an image, click <b>Open</b> and then click the <b>Upload</b> button. The maximum size of the image is 100 kb.
Page Background Upload	Choose the file you want to upload.
Page Background Color	If you set <i>Background</i> to <b>Color</b> , select the background color of the page that will appear during the captive portal session from the drop-down menu.
Custom Color	If you choose Custom on Page Background Color, enter the HTML color code.
Minimal Page for Mobile Devices	Toggle to <b>ON</b> to allow the web page to be properly viewed from a mobile device.
	Header Details
Background	<ul> <li>Select whether the login page displayed during the captive portal session will show an image or color. Choices are:</li> <li>Image: Show image on the page. Use the Header Background Color field to select a background color. The maximum size of the image is 100 kb.</li> <li>Color: Show background color on the page. Use the radio buttons to select an image.</li> </ul>
Header Background Image	If you set <i>Background</i> to <b>Image</b> , upload the image file by clicking <b>Add</b> > <b>Browse</b> . Select an image, click <b>Open</b> and then click the <b>Upload</b> button. The maximum size of the image is 100 kb.
Header Background Upload	Choose the file you want to upload.
Header Background Color	If you set <i>Background</i> to <b>Color</b> , select the header color from the drop-down menu.
Custom Color	If you choose Custom on Page Background Color, you can choose particular color by filling in the HTML color code.
Header Caption	Enter the text that appears in the header of the login page during the captive portal session.
Caption Font	Select the font for the header text.
Font Size	Select the font size for the header text.
Font Color	Select the font color for the header text.

	Login Details
Login Section Title	Enter the text that appears in the title of the login box when the user logs in to the captive portal session. This field is optional.
Welcome Message	Enter the welcome message that appears when users log in to the captive session successfully. This field is optional.
Error Message	Enter the error message that appears when users fail to log in to the captive session successfully. This field is optional.
	Footer Details
Change Footer Content	Enables or disables changes to the footer content on the login page.
Footer Content	If Change Footer Content is checked, enter the text that appears in the footer.
Footer Font Color	If Change Footer Content is checked, select the color of the text that appears in the footer.

External Payment Gateway					
Enable External Payment Gateway	Enables or disables external payment gateway and online wireless service purchasing from on the login page.				
Session Title 1	Enter the text that appears in the title of the online purchasing login box when the user logs in to the captive portal session.				
Message	Enter the text appears in the online purchasing login box when the user logs in to the captive portal session.				
Session Title 2	Enter the text that appears in the title of the message box while online purchasing is complete.				
Success Message	Enter the text that appears in the message box while online purchasing is complete.				
Session Title 3	Enter the text that appears in the title of the message box while online purchasing is fail.				
Failure Message	Enter the text that appears in the message box while online purchasing is fail.				
Enable Billing Profile	Select the billing profile which will be shown on the login page. The table only listed the billing profiles which are set Unit Price. Enable the billing profile by switch ON on STATUS.				
Service Disclaimer Text	Enter the service disclaimer text which is shown before user select and purchase wireless service.				
Payment Server	Select the payment received account and its payment agent.				

# Web Content Filtering Static Filtering

Path: Security > Authentication > Static Filtering

You may block access to certain Internet services.

To block or allow a service:

1. Click Security > Web Content Filter > Static Filtering tab.

Status	S VPN t sites. Up to RLs and Bloci	Security 9.32 key words in the ked Keywords page.	© <sup>©</sup> Maintena e site's name (web si	ince (2) (2) (2) (2) (2) (3) (4) (4) (4) (4) (4) (5) (4) (4) (4) (4) (4) (4) (4) (4
Web Content Filter  Static Filtering Approved URL Blocked Keywords Atent filtering option allows the user to block access to certain Interne d, which will block access to the site. To setup URLs, go to Approved U Filtering	t sites. Up to RLs and Bloci	o 32 key words in th ked Keywords page.	e site's name (web si	(9) (9) te URL) can be
tic Filtering Approved URL Blocked Keywords Nent filtering option allows the user to block access to certain Interne d, which will block access to the site. To setup URLs, go to Approved U Filtering	t sites. Up to RLs and Bloc	o 32 key words in th ked Keywords page.	e site's name (web si	te URL) can be
itent filtering option allows the user to block access to certain Interne d, which will block access to the site. To setup URLs, go to Approved U Filtering	t sites. Up to IRLs and Block	o 32 key words in th ked Keywords page.	e site's name (web si	te URL) can be
stent Filtering ON				
a OFF				
:iveX OFF				
wser Cookies				
Save Cance	el			

- 2. Toggle Content Filtering to **ON**.
- 3. Toggle the service to **ON** to block. Toggle to **OFF** to allow.
- 4. Click Save.

### Approved URLs

Path: Security > Web Content Filter > Static Filtering > Approved URL

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

Importing/exporting from a text or CSV file is also supported.

To add/import/export URLs to the approved list:

1. Click Security > Web Content Filter > Static Filtering > Approved URL tab.



2. To import a list from a text/CSV file, click **Upload URLs List from File**. If you want to export the current list, click **Export URLs List to File**. To add a new URL, click **Add New Approved URL**.



3. Enter a URL and click **Save**.

### **Blocked Keywords**

Path: Security > Web Content Filter > Static Filtering > 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 a 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 is also supported.

To add/import/export URLs to the approved list:

1. Click Security > Web Content Filter > Static Filtering > Blocked Keywords tab.

D-Link Unified Services Rou	ter - DSR-1000N		Logged in as: Serial: Q	admin ( ADMIN )   La 8281A3000007   Firmw 💦 W	nguage: English [US]	Logout
🙆 Statu	s 🛜 Wireless	Retwork	CA VPN	Security	O <sup>o</sup> Maintenance	
Static Filtering A Static Filtering A You can block access to characters in the URLs o Blocked Keywords L	ilter » Static Filtering » B pproved URL Blocked Ke websites by entering comp r the page contents. The l ist	ocked Keywords ywords slete URLs or keyword able lists all the Bloc	s. Keywords prever ked keywords and a	it access to websites illows several operatio	that contain the specifie	0 0 d
Show 10 💌 entries	[Right click on record to	get more options]				Q
Keyword			Status			0
		No data av	vailable in table			
Showing 0 to 0 of 0 entries					First   Previous   Hext >	Last 划
Add New Keyword	Upload Keywords L	ist from File	xport Keywords L	ist to File		

2. To import a list from a text/CSV file, click **Upload Keywords List from File**. If you want to export the current list, click **Export Keywords List to File**. To add a new URL, click **Add New Keyword**.



3. Enter a keyword and click **Save**.

### **Dynamic Filtering**

Path: Security > Web Content Filter > Dynamic Filtering

Dynamic Filtering will allow you to filter content from a list of categories. The router must be upgraded with the WCF license and then the Content Filtering option, which allows the user to filter out internet sites, needs to be enabled. When enabled, access to a website belonging to one of these configured categories will be blocked with an error page.

To add/import/export URLs to the approved list:

1. Click Security > Web Content Filter > Dynamic Filtering.

D-Link	<u>56 (600)</u>		Logged In as: Samid (Adam)   Language; Fuglish (IIS) () Linguid: Serial: 010/14/000007   Flormware: 1/100045 WW Witzard () System Search. (4)			
🙆 Status	😤 Wirelass	I detwork	CB VPN	Security	O <sup>o</sup> Maintenance	
urity - Web Content Filter - Is page displays the list of ca mamic Filtering	Dynamic Filtering tegories to be blo	cked.				C
Global Filtering						
Adult	01	News	047	Job Search	OFT	
Gambling	CHI	Travel/Tourism	DIE	shopping	(D41)	
Entertainment	OFT	Chat Rooms/IMs	017	Dating Siles	OFF	
Game Sites	1 (87	Investment Sites	(Cra	E-Banking	041	
Crime Terrorism	DIE .	Personal Bellefs/Cults	OR	Politics	( DATE	
Sports	OFF	www.E.Mail Sites	07	Visience/Undesi	rable	
Maticious	047	Search Sites	(Des	Health Sites	Ga1	
Clubs and Societies	CHE	Music/Videe	CNT	Business Oriente	at For	
Government Blocking List	OFF	Educational	OFF	Advertising	Ore	
Drugs/Alcobal	- DET	Computing/IT	OIT	Swinzuit/Lingeri	e/Models.	
Remote Control/Desktop	104					
		Sove Ga	inciil			

- 2. Toggle Global Filtering to **ON** to enable dynamic filtering.
- 3. Toggle any of the listed categories to **ON** to block. Toggle to **OFF** to allow.
- 4. Click **Save**.

# Firewall Firewall Rules

Path: Security > Firewall > Firewall Rules > IPv4 Firewall Rules or IPv6 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. On other hand the default outbound rule is to deny access from DMZ to 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.

To create a new firewall rule:

1. Click Security > Firewall > IPv4 Firewall Rules tab or IPv6 Firewall Rules tab.

D-Lin	<b>ik</b> 15 Router - D	SR-1000N		Logged in a Serial:	as: admin ( A QB2B1A3000	DMIN )   Lan 007   Firmwa Wi	guage: English ire: 1.108096E zard Syste	[US] O Logout _ww m Search Q
@		🛜 Wireless	Retwork	CAS VPN		security	🗘° Main	
urity » Firewal	I » Firewall F	lules Firewall Rules						0
ewall Rules Default Outbo Always	und Policy f	or IPv4	Allow O Bloc Save	k				
Pv4 Firewall	Rules List							
Show 10 👻	entries	[Right click on reco	rd to get more options]					٩
Status O Fr	om <sub>e</sub> To Ine Zone	e Service e A	lock / O Source O Hosts	Destination ⊖ Hosts	Local Server $\Theta$	Internet Destinatio	en e Loge	Rule Priority 🗧
			No data	available in table				
Showing 0 to 0 o	f 0 entries					(k) Fire	st / Previous	Next ) Last )
Add New IP	v4 Firewall F	Rule						

2. Right-click an entry and select either **Edit** or **Delete**. To add a new group, click **Add New IPv4/IPv6** Firewall Rule.

#### Section 8 - Security

To Zone     ThisECURE (Debased WA)       Service     ANT       Action     Antro       Source Hosts     Antro       Source Hosts     Andress Range       Source Hosts     Andress Range       Destination Hosts     Andress Range       Log     Hener C Alward       Gos Priority     Remain Source	From Lone	SECURE (LAN)	From Zone	SECURE (LAN)	
Service     Atr       Action     Marges Blone       Surce Notics <ul> <li>Address Blone</li> <li>Address Blone</li> <li>Surce Hosts</li> <li>Any</li> <li>Single Address</li> <li>Address Blone</li> <li>Source Hosts</li> <li>Any</li> <li>Single Address</li> <li>Address Range</li> <li>Source Hosts</li> <li>Source Hosts</li> <li>Any</li> <li>Single Address</li> <li>Address Range</li> <li>Source Hosts</li> <li>Any</li> <li>Source Hosts</li> <li>Source Hosts</li> <li>Source Hosts</li> <li>Any</li> <li>Source Hosts<td>To Zone</td><td>INSECURE (Dedicated WAN</td><td>To Zone</td><td>INSECURE (Dedealed WAX)</td><td></td></li></ul>	To Zone	INSECURE (Dedicated WAN	To Zone	INSECURE (Dedealed WAX)	
Action     Brank Always       Source Hotts        • Any        • Source Hotts         Source Hotts        Source Hotts         • Any        • Source Hotts         • Any        • Source Hotts        Destination Hosts         • Any        • Source Hosts         • Any        • Source Hosts        Los         • Any         • Source Hosts         • Any       • Source Hosts        Los         • Any         • Source Hosts         • Any        Cos         • Monte         • Address Range         • Address        Cos         • Monte         • Monte         • Address	Service	ANY	Service	ANT	
Source Hosts <ul> <li>Any</li> <li>Single Address Range</li> </ul> Source Hosts <ul> <li>Address Range</li> <li>Source Hosts</li> <li>Source Hosts</li> <li>Any</li> <li>Single Address Range</li> <li>Destination Hosts</li> <li>Any</li> <li>Single Address Range</li> <li>Destination Hosts</li> <li>Address Range</li> <li>Log</li> <li>Hereet</li> <li>Address Range</li> <li>Log</li> <li>Hereet</li> <li>Address Range</li> /ul>	Action	Aways Block	Action	Black Alwart	
Destination Hosts     # Any     Single Address Range       Lot     # Never     Address Range       QoS Priority     Nemel Service	Source Hosts	🗢 Any 👘 Single Address 👫 Address Range	Source Hosts	Any Single Address SAddress Ranne	
Log Mexer O Always Ocs Priority Nemai Service •	Destination Hosts	* Any D Single Address D Address Range	Destination Hosts	R Any Single Address C Address Range	
Qo5 Priority Nemai Service	Los	W Never C Abraid	Log	· Hever O Always	
	Qa5 Prinrity	Nomal Service			

3. Complete the fields from the table below and click **Save**.

Field	Description
From Zone	Select the source of originating traffic: either secure LAN, public DMZ, or insecure WAN. For an inbound rule WAN should be selected.
To Zone	Select 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.
Service	Select a service from the drop-down menu. ANY means all traffic is affected by this rule.
Action	Select an action from the drop-down menu.
Source Hosts	Select a source host. If you select Single Address or Address Range, you will need to enter the IP address or IP range.
Destination Hosts	Select a Destination host. If you select Single Address or Address Range, you will need to enter the IP address or IP range.
Log	Select whether to log firewall traffic or not.
QoS Priority (IPv4 only)	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=16