

Wireless AC Services Router User Manual

DSR-250V2 Version 1.00 April 07, 2022

1. D-Link Services Router	 3
1.1 User Guide	
1.1.1 Preface	
1.1.1.1 Copyright Notice	
1.1.2 Web UI Login	
1.1.3.1 Summary	
1.1.3.2 Statistics	
1.1.3.3 Event Logging Status	
1.1.3.4 Connections	
1.1.3.5 Client	 9
1.1.3.6 VPN Status	-
1.1.3.6.1 IPSec status	
1.1.3.6.2 PPTP status	
1.1.3.6.4 Openvpn/GRE status	
1.1.3.7 Routing status	
1.1.4 Chapter 2 Administration	
1.1.4.1 Event Logging	
1.1.4.2 Maintenance	
1.1.4.2.1 Firmware upgrade	
1.1.4.2.2 Backup and Restore	
1.1.4.3 Management	
1.1.4.3.1 Session Settings 1.1.4.3.2 Device Management	
1.1.4.3.3 Utility	
1.1.4.3.4 SNMP-Removed from UI	
1.1.4.3.5 License	
1.1.4.4 Certificate Management	 24
1.1.4.4.1 TLS/CRL Profiles	
1.1.4.5 Schedules	
1.1.4.6 Diagnostics	
1.1.5 Chapter 3 Authentication	
1.1.5.1.1 External auth server	
1.1.5.2 Captive Portal	
1.1.5.2.1 Login Profiles	
1.1.5.2.2 Captive Portal Configuration	
1.1.6 Chapter 4 Interface	
1.1.6.1 Port Configuration	 42
1.1.6.1.1 Network Configuration	
1.1.6.1.3 IP Aliasing	
1.1.6.2 LAN Clients	
1.1.6.2.1 IP Management	
1.1.6.2.2 DNS Host Mapping	
1.1.6.3 VLAN Settings	 57
1.1.7 Chapter 5 Network	
1.1.7.1 Routing	
1.1.7.1.1 Static Route	
1.1.7.1.3 IGMP	
1.1.7.2 Bandwidth Management	
1.1.7.2.1 Add Bandwidth management	
1.1.7.2.2 Session Limiting	
1.1.8 Chapter 6 Firewall	
1.1.8.1 Firewall Settings	
1.1.8.1.1 General	
1.1.8.1.2 Attack Check	
1.1.8.1.4 UPnP	
1.1.8.2 Firewall Policy	
1.1.8.2.1 IP Rule	
1.1.8.2.2 Port Forwarding	
1.1.8.2.3 Port Triggering	
1.1.9 Chapter 7 Security	
1.1.9.1 Web Content Filter 1.1.9.1.1 Custom Group list	
1.1.9.2 Application Control	
1.1.9.2.1 Auto Upgrade	
1.1.9.2.2 Custom Group List for Application Control	 86
1.1.10 Chapter 8 VPN	

1.1.10.1 IPsec Profiles	87
1.1.10.2 IPsec Site to Site	91
1.1.10.3 IPsec Client to Site	94
1.1.10.4 IPsec 1 to 1 mapping	97
1.1.10.5 PPTP	97
1.1.10.6 L2TP	100
1.1.10.7 OpenVPN	103
1.1.10.7.1 Server mode	103
1.1.10.7.2 Client mode	108
1.1.10.7.3 Access server-client mode	110
1.1.10.8 GRE	110

Web UI Login

Logging 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, you can manage DSR 250v2 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 you manage the router must be in the same subnet as the router (192.169.10.0/24).

Accessing the device via Web UI

- · Connect your workstation to an available router's LAN port.
- 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 https://192.168.10.1 to your pop-up blocker's allow list.

- Launch a browser, enter the IP address for the LAN interface (default = https://192.168.10.1), and then press Enter.
- Enter your username (default = admin) and your password (default = Admin\$123), then click Sign in.

B-Link I INF MAR			
	Longin (
	Press	of in	
	Ramor J		E-
	L.	- N, 18	

The web management interface opens with the **Summary** page. This page displays device information and port status. You can return to this page at any time by clicking System and status > Summary.

Chapter 1 System and Status

This chapter provides details about the port status, device information, and statistics. You can add filters for the event logging. This section of the user manual gives status about the connections, client, VPN, and Routing.

D-Link	254.75	0.12			39		lawer.	0
	Summ	nery -						
System and status								
Summers		eternation						
Sudditor	Types of	ne -	memory.					
Event function	had a board	iner'	Sector parents.					
Daviddellight.	The Party of		4					
CSW	in the second		+ == = = = = = = = = = = = = = = = = =					
YPN H	Appendix of		10.049 (115.210					
1000								
American	1.0.00		N 14-14 12 14 12 14	Gertin (1913				
Automocality	Partitio							
		100000-000-000-0-0-0-0-0-0-0-0-0-0-0-0-	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	hants	1004,444,000	-	1-8444 (Marile	1000 (1000 (1000))
		Perit Newsgel 1		1008	01111110-0111	191.101.2011	211.251.251.8	
(Childrenia)	1	Work Instant 1	tank.	+	18.11.0134.05.44	1012184.30-0	011,256,358.8	
		Med Brough L	Links.		14-10 14-16-16-16	1012104-0014	- 498-386-398-8	

This chapter covers the following topics:

• Summary

- Statistics
- Event logging
- Connections
- Client
- VPN status
- Routing

Summary

The *Device information* section provides details of the device, like the system name, serial number, hardware version, and firmware version. The Port status section displays details about the configured ports.

<u>D-Link</u>	051296	a					(G. Frank) (S
	Samme	414 -						
🖄 synam and raiku	Ensite tab							
Sumas								
S falsion	dy kan sa		×.					
Parel ingles	Long and a	n naa	1 M PROVINCE					
Concerning a	Constant of	ee (1)						
VI06	Distance	(m. 620-00						
A HS I SHA	éstan a l	s : : : : :	3					
Packs								
🚋 Abridden e	Sanat Une		District Stationals Soft					
La Automición	Part datas							
💯 televise	1.0.00	1.0 B.40 B.40	LINE VERIN	10000	10.0 ALC: NO.	1.000	1000000000	100000
st) Herada	1799) C	AT A SHARE	10. 20 M	nas ja ses Ko	6001 (2001 (2000)	Radia di Kal	2001 100 000 0 300 000 0	IK. 21.1
2 K. 100								
19 statu ny								
₩ ver								

Field	Description
	Device information
System name	It indicates the name of the device.
Serial number	It displays the serial number of your device.
Hardware version	It displays the hardware version of the device.
Firmware version	It displays the current firmware version running on the device.
System uptime	It displays the time duration since the last reboot.
Current time	It displays the present time.
	Port status
Ports	It displays the port numbers.
Interface name	It displays the interfaces of the device.
Link status	It displays whether it is uplink or downlink.
Speed	It displays the uplink or downlink speed.
MAC address	It displays the MAC address of the port.
IP address	It displays the IP address of the port.
Subnet mask	It displays the subnet mask of the port.

Statistics

This page displays detailed transmit and receive statistics for each physical port. Each interface (WAN1, WAN2/DMZ, LAN, and VLANs) has portspecific packet-level information provided for review. In addition, it also provides sent/received packets, Sent/received bytes, and packet errors for each interface. If you suspect issues with any wired ports, this table diagnoses transmit level issues with the port. The statistics table has a refresh icon that allows the display of the most current port-level data.

Portisans							
e s							
Part	Interface many	He have been	Reachered layers	Arrest lagress	Sensional posterio	Level packages	Paster reca
4.204	Contraction (Comp. 2	10.4100340	1000 CO	an entre	248	8400	10 C
1.1	V04-1	0.000, 0.02	1220000	15.190305	2000	718000	2 C

The fields available in the Port Traffic table are as follows:

Port traffic				
Field	Description			
Port	It displays the port numbers.			
Interface name	It displays the interfaces of the device.			
Link status	It displays whether it is uplink or downlink.			
Received bytes	It displays the number of bytes received by the port.			
Sent bytes	It displays the number of bytes sent by the port.			
Received packets	It displays the number of packets received by the port.			
Sent packets	It displays the number of packets sent by the port.			
Packet error	It displays the number of packets with errors.			



This section displays the speed at which the data is uploaded or downloaded from the particular WAN port for the selected time frame. You can choose the *Time frame* from the drop-down list located in the upper-right corner of the graph and then click the *Refresh* icon to update the graph with the latest readings. When the mouse hovers over the graph, it displays the upload and download speed at a particular time.



VPN usage displays the usage of the VPN tunnels for downloading and uploading the data. You can select the Time frame to display traffic over



The fields displayed on this page are as follows:

Field	Description
Resource utilization	It displays the percentage of the CPU currently consumed by the device and displays the space of memory utilized by the device.
Service port usage	It displays bandwidth usage by network segments such as LAN or VLAN.
Web usage	It displays the activity going on for web pages.
Application usage	It displays the usage (in percentage) of each application.

Event Logging Status

The router allows you to capture log messages. You can monitor the type of traffic that goes through the router, and when the router detects potential attacks or errors, it notifies you. The following sections

describe the log configuration settings and the ways you can access these logs.

D-Link	0.580,2550,0			(2) fait the	
	Event logging				
To System and status					
distanting.	$0=\tau=\pm 3$	$\{(a),b\in t\}$			
estatistica	Edites .				
Parts logging	Current logs				
Convertional	<u>+</u>				() +==1.7
Chine	1144 1711 / 12 10 11 14 17	- Leven	· Anternalized new	a Velatentetation	L CHIEF HIM H
With status		3495	MY ANT PROPAGE STOTES	\oplus if the \mathcal{T} we let \mathcal{M} due	1
- + Fry-atamous	15,245,433 1,246,27	39.0	ALLOND (*) FORMUL, STRIDS	4350 Lince Marke	stream in the figure.
70.012	1002-05-09-05-02-56	NPO .	MADNET ARRANGE REPAILS	 all light frames States 	PARTING TO BE THE
- Admitistration	3103-0203110-0233	544	and the second second second	which the control and	systematics, success
t_ Automidication				Totob+ Buy to	10. E 424
A method					
TAT - or choose of the					
C Halwark					

The fields displayed on the page are as follows:

Event logging

Field	Description
Time period	Select the time frame for which you want to schedule logging.
Filter	Click Filter to display the data.
	Current logs
Time	It displays the time when the event occurred.
Severity	It displays the severity of the logged event.
Category/Event type	It displays the category/Event type to which the entry belongs.
Event description	It displays the description of the event.
Event Details	It Displays the Event information in detail.
Download Icon	Click on Download Icon to download the logs in .csv format to PC.

Connections

This table lists the active Internet sessions through the router's firewall. In addition, it displays the session's protocol, source IP, total sessions, and port number.



The fields available on this page are as follows:

Field	Description
Source IP	It displays the source IP address at which the connection gets established.
Protocol	It displays the protocol used to establish the connection.
Total sessions	It displays the total number of sessions established at the source IP address.
Port number	It displays the port number at which the session establishes.

Client

The **Dynamic Host Configuration Protocol** (DHCP) simplifies the configuration and management of the IP address of the devices like printers, laptops, desktops, etc., present on the network. A range of IP addresses that are assigned for the devices is known as the DHCP pool. When you add a device to a network where it gets its IP address from the DHCP server dynamically, one of the IP addresses from the configured DHCP pool is assigned to the device. However, these IP addresses are given to the clients only for a limited amount of time, and this process is called a **DHCP lease**. The DHCP lease gets renewed on its own after the lease time is expired.

This page of the router details the DHCP server status and LAN clients connected to your router.



The fields available on this page are as follows:

Field Description				
DHCP server status				
Name	It displays the name of the DHCP server.			
Interface	It displays the interface on which the DHCP server is configured.			
IP range	It displays the range of IP addresses that you can assign for lease.			
Active	It displays the number of IP addresses being used.			
Utilization (%)	It displays the percentage of the utilized IP addresses.			
LAN clients				
Host name	It displays the name of the client to whom the IP address is assigned.			
IP address	It displays the IP address assigned to the client.			
MAC address	It displays the MAC address of the client for which an IP address is reserved.			
Туре	It displays the type of Internet connection used.			
Interface	It displays the interface through which the client connects.			
Expires time	It displays the date and time when the DHCP lease expires.			
Block	To stop traffic from particular LAN client(Enable/Disable)			

VPN Status

You can view the status (connect or disconnect) of the gateway's VPN associations/connections. In addition, the page lists the active VPN association/connections, the traffic details, and the tunnel state. The traffic is a cumulative measure of transmitted or received packets since the tunnel was established.

D-Link	058(230)(2			(g. mint	
	VPN status				
👔 System and status					
	Office chertal Pre-	sate constant appears	NUMBER OF STREET,		
intristics)					
Tante lagaten	Side to side VPT				
Conceptions					
EW.	How States	Relates Laur	- Barrada	theil bitrand	- Balan I - Sachiel
NTRA MINISTRA			e vand oorstoom	and the second	
a ostrin matter	Card In vie VPR				
- Authenrichtlade					22.14145
	deres:	1. Investorie		disa-are (Asso)	
Л. нанку-			a obtain problem		

This page covers the following Topics:

VPN status

- Ipsec status
- PPTP status
- L2TP status
- Openvpn/GRE status

IPSec status

An IPSec policy is between DSR-250v2 and another router and an IPSec client on a remote host. Depending on the traversed network between the two policy endpoints, the IPSec mode can be either tunnel or transport.

- **Transport**: This is used for end-to-end communication between the 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 authenticated.
- This page covers the following Topics:
 - Ipsec status
 - > Site to site VPN
 - > Client to site VPN



The fields displayed on this page are as follows:

Field	Description				
	Site to Site VPN				
Name	It displays the name of the VPN.				
Interface	It displays the interface on which the VPN tunnel is established.				
Remote gateway	It displays the IP address or the domain name of the remote peer.				
Local network	It displays the local network being used by this VPN connection.				
Remote network	It displays the remote network being used by this VPN connection.				
Sent bytes	It displays the number of bytes transmitted through the tunnel.				
Received bytes	It displays the number of bytes received through the tunnel.				
Status	It displays if the VPN connection is connected or disconnected.				
Connect	Click the icon to connect or disconnect the tunnel.				
	Client to site VPN				
Name	It displays the client name of the VPN.				
Interface	It displays the used WAN connection.				
Connections	It displays the number of connections established on that interface.				

PPTP status

This page covers the following Topics:

- PPTP status
- > PPTP Client mode
- > PPTP Active Users

It displays status of PPTP VPN i.e whether tunnel is established or not .Where we can connect or disconnect VPN for PPTP client ,In server it shows the list of active VPN's

Dilink	Constea.		(Grantha)
	VPN status	3	
J within the rates		7.000 300(7123.000	
Sannan Sadura Seatherna Ganalas	PPTP all and contain		
	Wit serve	The same of the designs.	(Marana)
Steel and a	STREAT SETT	55445	2

Field	Description	
VPN Server	It displays the VPN server (WAN) ip address.	
Client IP address It displays the Remote IP address to which the tunnel is established.		
connect	It displays the connected Status of PPTP client.	

PPTP active users

			CT (MANN
Mane reason	Assessment of the state of the second	PPTP lamoni (P	Cattoric Office
autor inv	282 198 59 30	11.0.0.8	Jam Silts
			miara aven an i a •

Field	Description
Username	It displays the PPTP user name.
Remote IP address	It displays the Remote IP address to which the tunnel is established.
PPTP tuneel IP It displays the IP address of the connected PPTP client.	
Connect time	It displays the time duration when the tunnel is up.

L2TP Status

This page covers the following Topics:

- L2TP status
- > L2TP Client mode
- > L2TP Active Users

It displays status of L2TP VPN i.e whether tunnel is established or not .Where we can connect or disconnect VPN for L2TP client ,In server it shows the list of active VPN's

D-Link	D08-250-2		S Cherry	0
C Servers and mature	VPN status			
Summativ Skatarate	and house - which we have	L20"misto		
Devent loang ng	L2TP client mode			
Districture				
Dentil	(artillapping)		Sover	
VIN status	112 (42.00.013	100.00	39	

Field	Description	
VPN Server	It displays the VPN server (WAN) ip address.	
Client IP address It displays the Remote IP address to which the tunnel is established.		
connect	It displays the connect/Disconnect status of L2TP client.	

L2TP active users

1.35: 승규 수 한 상당이 수 있는

T1.41 114715	Association of a defense	L21P (P address)	Constant Viters
admin .	192 366.09 37	10.5.2	Jrn 3de

Field	Description	
Username	It displays the L2TP user name.	
Remote IP address	It displays the Remote IP address to which the tunnel is established.	
L2TP IP address	It displays the IP address of the connected L2TP client.	
Connect time	It displays the time duration when the tunnel is up.	

Openvpn/GRE status

This page covers the following Topics:

- Openvpn/GRE status
- > OpenVPN Connection
- > OpenVPN Status
- > GRE status
- **GRE Status**

Name	Interface	sonic transmit op-	Removate 10	Status
1@#\$%^%*Ofbridgtf	WANIS	66.06.66.4	66.66.66.3	CONNECTED
			Total:1 Rems 1/1	1 5 -

You will find a list of GRE clients connected with the following details:

The fields available on this page are as follows:

Field	Description	
Name	It displays the VPN server (WAN) ip address.	
Interface	It displays the interface name to which the tunnel is established.	
GRE tunnel IP	It displays the connect/Disconnect status of GRE client.	
Remote IP	It displays the Remote IP address to which the tunnel is established.	
Status	It displays the connected Status of GRE	

OpenVPN status :

You will find a list of openVPN clients connected with the following details:

CONTRACTOR -	content to purclash	Chief P (1999)	Sant Lyres	Hardward Styles	201010389
UNDER	112152554		118	28	2001275
dependent.	132.166.53.212	10.038	1201437346	44534834	352 Adm (15)
opened	332108.85100	3.83.10	1212034436	128/0011018	128.200.388

The fields available on this page are as follows:

Field	Description	
User Name	It displays the VPN client username	
Client IP (actual)	It displays the actual IP address of the client	
Client IP(VPN)	It displays the tunnel IP of the client.	
Sent bytes	It displays the Bytes of data sent to the client.	
Received bytes	It displays the Bytes of receive from the client.	
Connect time	It displays the duration of client connectivity.	

Montaining reach basel

OpenVPN Connection

You will find the status of openVPN client connectivity.

OpenWPM Connection

Connection States

Connect

Field Description	
Connection status It displays the VPN connection status.	
Connect We can connect or disconnect VPN tunnel.	

Routing status

This chapter covers the following topics:

Routing

Active Routes

Multicast IP table D-Link	010.250-7			Q Teach	0
	Routing	D ₂			
System and states Summery Unstruction	Active fonder.				
Event Equina Linenection	107 888.13.14	1 - kanna a ana 276.02.278.0	10 (100 100 (44)	is another contract	Ballen
C said	Multicent IP table			lowit dress, and	
Routing	manual statement		 matrix to Surveying encode/land 	- Tarki	10 Januar

Field	Field Description			
	Active routes			
Destination	It displays the Destination IP address			
Subnet mask	It displays the subnet mask.			
Gateway	It displays the gateway IP address.			
Interface	Interface It displays the interface on which the route is present.			
Metric	Metric It displays the metric value of the route			
	Multicast Ip table			
Multicast channel	It displays the name of the client to whom the IP address is assigned.			
VLAN ID	It displays the IP address assigned to the client.			
Ports	It displays the MAC address of the client for which an IP address is reserved.			

Chapter 2 Administration

This chapter covers of the following sections:

- Event loggingMaintenance

- ManagementCertificate management
- Schedules
- Diagnostic

Event Logging

D-Link	$T \in \mathbb{P}_{n} \setminus \{0, 1\} \setminus \{0, 1\}$		(C. 2011)
	Event ogstop		:
) Systems and states			
 Administration 	Lives dia 10	8	
Liven: sgging	Concepty' Court Lyn	Component	
Madales Concer		Contraction of the cost	
Press, encode		 BRATY PARCE STATE 	
Certacae management			
Zider des		💽 CORRECT 💽 CORFERENCES	
Disc scale			
T Adhenikaan	ramos refu ellistinoiti		
- Inamical	factor of the	8	
S READE	Living provide	All a second s	
* Forse	\cdot for θ is the set of θ -base of	ZB - ZAN STR	
9 teacting), as in gravitation in $[\mathcal{L}_{ij}]$ is a $[\mathcal{L}_{ij}]$	ap data dara	
z vre	Conternation 4000 Land	and the states	
	contraction 2.75262-05	441 (140) (140)	

Event Logging

The router allows you to capture log messages. You can monitor the type of traffic that goes through the router, and the router detects and notifies about potential attacks or errors. In this section, you can configure the event logging feature and select the category or the event type you want to log.

The fields available in this section are as follows:

Field	Description	
Event logging	Select the checkbox to enable event logging.	
Category/Event type	Select the checkboxes of the categories that you want to log.	
Apply	Click Apply to save your settings.	
Cancel	Click Cancel to revert to the previous settings.	

Remote Logging (Syslog)

An external Syslog server collects and stores logs from the router. This remote device typically has fewer memory constraints than the local Event Viewer on the router. Therefore, it can manage many logs over a sustained period. These logs help debug network issues or monitor router traffic over a long duration.

The router supports five concurrent Syslog servers. Using the Remote Logs page, you can configure the server to receive different log facility messages of varying severity. This page also lets you send configuration logs to three email recipients.

The fields available in this section are as follows:

Field	Description	
Syslog server	Select the checkbox to enable the Syslog server.	
Syslog server 1	Enter the IP address or the FQDN to set up Syslog server 1. Repeat the fields above for each server you want to set up.	
Syslog server 2 (Optional)	Enter the IP address or the FQDN to set up Syslog server 2.	
Syslog server 3 (Optional)	Enter the IP address or the FQDN to set up Syslog server 3.	
Syslog server 4 (Optional)	Enter the IP address or the FQDN to set up Syslog server 4.	
Syslog server 5 (Optional)	Enter the IP address or the FQDN to set up Syslog server 5.	

Maintenance

This page consists of following topics:

- 1. System
- 2. Firmware upgrade
- 3. Backup & Reboot

System



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

The fields available on this page are as follows:

Field	Description		
System name	Enter a new name for the router.		
	Date and time		
Current device time	It displays the current date and time on the router.		
Time zone	Select your time zone from the drop-down menu.		
Daylight saving	Select the checkbox to enable daylight saving time.		
Set date and time	Select Auto or Manual. If you select Manual, enter date and time manually.		
NTP server	This field appears when you select <i>Auto</i> . Choose either <i>Default</i> or <i>Custom</i> . When you choose Custom, enter the primary and secondary NTP servers URL in the NTP server 1 and NTP server 2 fields respectively.		
Time to re-synchronize	Enter the time in minutes for the router to re-synch with the NTP server(s).		
Apply	Click Apply to save your settings.		
Cancel	Click Cancel to revert to the previous settings.		

Firmware upgrade

You can upgrade to a newer firmware version from the Administration web page. In the Firmware Upgrade section, to upgrade your firmware, click Browse, locate and select the firmware image on your host, and click Upgrade. After validating the new firmware image, the new image writes to flash, and the router automatically reboots with the latest firmware.

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

D-Link	NUL212.2		(a. /		$\supset \otimes$
	Maintenance			Valeet	1000
😥 Kyalan sana salah s					
As Assessments	Reference Pressant re-	s ale lindea i rivel			
investi keyyang					
Mantakance	A constitueness interact	•			
nan aga marti	 Company of the second seco	168,77			
Contribution management					
Bellinde en.	LITTLE CONTRACTOR	des 6a 14 - 0 (\$108			
ti agrosto					
FI Automotion	1997 B	An an analysis was an an an an an an			
$R_{\rm c}$ introduces					
 Mersons 	100 T				
🖾 Friend	Paratan ay yanka				
 County 					
BLARK	Transis description	1.000			
	Aver the				

Current firmware information

This section displays the current firmware running on the DSR-250v2 router.

Field	Description	
Firmware version	It displays the firmware version running on the device.	
Firmware date	It displays the date and time when it was last upgraded.	
Status	It displays whether the current firmware is the latest firmware or not.	
Check	Click the Check button to connect the router to a D-Link server to check if the recent firmware version for this router is available.	

Firmware upgrade

You can use this section for firmware upgrades via PC or USB. The fields available in this section are as follows:

Field	Description	
Browse firmware	Click Browse to locate the firmware image on your system and select the file.	
Upgrade	Click Upgrade to start the firmware upgrade.	

Backup and Restore

After you configure the router, you can backup the configuration settings. When you back up the settings, the router saves them as a file. You can then use the file to restore the settings on the same router if something goes wrong or on a different router (must be the same model) replacing the existing router.

D-Link	1 USH 2001	((#) =(+)	0
<u>e</u> =	9		

Syder and states	contraction and	Dank g. Lint on
25 Accessore	8.way	
Danloging	Steel a copy gift is with safety?	
Munitered by	Lower N.	5,000.00T
(Atragener 1		
CarSing restryment	Record and any print care	el Nai
Section	Review countries to part of	T and
Сириал.		
TT Administration	Period	
E Innina	Robert & locary default	
Sec. Barris	200 (W)	201-000
the lines		
Contra	Selico pil toto parali	- Entrait

Backup

This section allows you to save a backup file of the current configuration. The fields available in this section are as follows:

Field	Description
Save to	To save the file to your computer, click System (PC).

Restore

After using the procedure to back up a router's configuration, you can restore the settings using the following procedure. The fields available in this section are as follows:

Field	Description	
Browse saved configurations	Click Browse to select the file saved in your system. This field is available when you select the System (PC) as the Source file.	
Restore	Click Restore to start the restore process.	

Reboot & factory default

If you reset a router to its factory default settings, it returns to the state when it was new — you lose all changes you made to the default configuration. The fields available in this section are as follows:

Field	Description		
Soft reboot	Click Soft reboot to perform a power cycle and keep any customized overrides you made to the default settings.		
Reboot with factory default	Click this button to reboot the router to the original factory default.		

Management

Web GUI Access

D-Link	0.044 \$36.3					$\left(H_{n} \right) = M_{n} + M_{n}$		$(\mathbf{i}) = (\mathbf{i})$
() узын хамаалаг	Managemen	1					Ger vit	dight
25 Alex Solice	and a second second	are a stronge	ever sample en er	ng nar	1 MP IP P			
Electric applications Described and	794 B							

	-			
Kagarat				
Carl Monde in some care of	Lini of allowed Phoblecon View establish			
Artes des	1 📅			C. Strech
Dig talk	1.000 C	anaro.rga		Protected Managements of a
🗁 Acherikator	0000	They're Problem (YOU REPORT
S. Derter	C 14	Must service		2 I. Mari
< nexter		Ling of Lowerse	-	PRIVATE:
🔄 Please	· · ·			
90 George 🗰				NAME OF A DESCRIPTION O
Ç WN				

The Web GUI access page allows users to specify the user's IP address or VLAN to configure the router using the web GUI.

Field	Description
Enable	Select the check box to enable the Web GUI access feature.
Name	It displays the name of the user.
Access type	It displays the type of access used.
IP address/VLAN network	Enter the IP address or the VLAN network based on the selected access type.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Session Settings

Session Settings

On this page, you can set the timeo	ut value for admin and guest logins.

D-Link	13 8 4 5 56 28			(<u>7</u> -2a	···)
	Management				Vance 40
 System and status A, el fatte spation 	President Statements	ana kang	a ny		
Romai seguine Mainer anes	To a los callings				
материнате	And the latent	o n			
Constitute in composition of	Almain de Laws.	1	ai des		
Cohere Jern	11.2.2				
LABOR SHEE	Constitution of	4	at size		
🔄 Aal anks Sa					
A transm					
- Ş. FREVER					
22 Franci					
10 Leoney					
RT 1475					

Field	Description
Administrator	It displays the name of the admin.
Administrator timeout	Enter the timeout value in minutes for the Administrator account.
Guest	It displays the name of the guest.
Guest timeout	Enter the timeout value in minutes for the Guest account.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Device Management

Enable this feature to manage the router from a remote location, using HTTPS. Both HTTPS and access can be restricted to a subset of IP addresses. The router administrator can define a known PC, single IP address, or range of IP addresses to access the GUI with HTTPS. The opened port for SSL traffic can be changed from the default of 443 while defining the allowed remote management IP address range.

D-Link	N 01 210.2	$\left(\overline{c_{-2}}$ of $\right) = \hat{Q}$
🖞 Sveichendoirtus	Managament	varias 🥄 koje
🗻 Annahir in	Man De annexes - Sana an Francisco y - Bandan Mar e y e mar	
Pro l'agli a	Levice Valuement	
le dels como le necessorie el	LATE was welled 🛛 💽	
Ok raterak matagainana	Parada na nyamata sa ap	
Schedules Dag sails	Back of the second 1	
≥ Schertsche	n n pa	
A. Carlan	77 B	
SŞ. Artorak	····· • •	
= Heat	Analis and Anal	
S. Secoles		
± 2004		

Field	Description				
	Device management				
LAN IP access via WAN	Select the checkbox to enable this feature. This feature configures the router to provide the LAN IP Access from the WAN side.				
	Remote management setup				
Enable remote management	Select the checkbox to enable this feature.				
HTTPS port	Enter the port for HTTPS access. The default port is 443.				
SSH	Select the checkbox to enable SSH (Secure Shell) protocol to access the CLI over the network from a remote host.				
SNMP	Select the checkbox to enable SNMP for remote management.				
Allowed remote access	Select All IP Addresses, IP Address Range (enter an IP range), or Only Selected PC (enter an IP address).				
Apply	Click Apply to save your settings.				

Utility

A package is a set of files installed by the router from D-Link's repositories. This feature lets users download new drivers for supported USB devices and language packs to enable multi-lingual support for the router's management interface. In addition, multi-lingual support via the Utility page allows the user to choose a language of choice to present the entire textual content in the router's user interface in the selected language.

D-Link	$12.4 \le 5.01 \pm 3$			C. San da) (
Assignmentations	Management				Cerros esta
, An Olds Inc.	Pair Colleman	dens for Lothers.	Ex. or Management Coll a		
Brand Lag. 1 g	LIFE STREAM CONTRACT				
le dels conse					
le seguere d	< 0				G, comes
Gertilitatie	Crime	1 ipen	1 Doumiprior	1. Invation	ili nativita
menegativene	LL		construct endorse induction end, constant 3		L.
Same Called	Contraction	2	the short start	2 B	
	Except	1000	ter graden and		F
Day main	1.1.1	1.000	e e contra construir agres con contra con	1	
An international free	ski sa	Second.	CHARACTERIZATION ACCESSION OF ACCESSION	44	
l des la c				miner at 199	
A HARRIN					
-erva					
Sec.					
WH .					

The fields displayed on this page are as follows:

Field	Description
Driver	It displays the name of the installed driver.
Туре	It displays the type of the installed driver.
Description	It provides description about the driver.
Installed	It displays the version of the installed driver.
Enable	Select the checkbox of the driver you want to enable.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

SNMP-Removed from UI

License

D-Link	009/28/42	(3. sent) 🔕
El: Sontero ensimilar	Management	
A. CONTRACTOR	and a second of the second process of the se	
1 Section to		
Neimeitte Seconder	Course for	
Carringer an	han bhanga a mainting a tha Battan	Tall and Tall

n Tana an Dianach II Achardanna A Mariann A Mariann A Mariann A Mariann A Mariann A Mariann	Adhatan Artas Adhatan Artas	. Ad	or samalar occetti la rel	1. Area 1. Area 1. (10) - 1. (10)
Field			Description	
License model			It tells about model of lice	ense

Activation code	It displays the activation code of the license.
Expires	It tells about expiry time

Activation setup

We need to give activation code in license activation code and click on activate. Which will activate the license Certificate Management

This page consists of following topics:

- 1. Certificate Management.
- 2. TLS/CRL Profile
- 1. Certificate Management.

	Certificate manag					Gent
D. Symbor and Manue.	(artificate Hantgamer)	No. 2 10 Protection				
Event Inscinut Harmonica	Contribution and Reys					
Management	十合法					
Carolycene exercise	2	 Description terms Description terms 	and the second s	111.0 mm	numer on Attacement of the Ad	Pulle
Sinten	20. 100 miles	District General Sectors (1997)	erm; ersit	1,000	ananangen 1. m. ak.	
Deserver.					black lines (

Filed	Description
Profile name	It displays profile name of certificate
Common name	It displays common name of certificate
Application name	It tells about the application in which user is using the certificate
Status	It displays about the status of certificate
valid to	It displays validity of certificate
Enable	It displays enable/disable option

TLS/CRL Profiles

A certificate revocation list (CRL) is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their actual or assigned expiration date.

It is a type of blocklist that includes certificates that should no longer be trusted and is used by various endpoints, including web browsers, to verify if a certificate is valid and trustworthy.

Generating TLS/CRL profile

Field		Description		
Method		It says about how we are adding tls/crl profile		
Profilename		It displays the name of profile		
TLS key name		It tells about the key		
0 D-Link DSR-258v2 × +			- 1	8
	https://192.166.10/1/v/ach	ninistration/addTiscri	<u>Ω</u> 8	
D-Link	DSR-250v2	Q Search		
	Add TLS/CR	L Profiles	Cancel Apply	
🕄 System and status				
a Administration	Method	Generate OTLS Upload OFL Upload		
Event logging	Profile Name	Dar250		
Maintenance	TIS Key Name	sehithil123		
Management				
Certificate management				
Schedules				
Diagnostic:				
Authentication				
吊 Interface				

TLS upload

Field	Description
Method	It says about how we are adding tls/crl profile
Profile name	It displays the name of profile
upload	we need to give file and upload

D-Link DSR-258v2 × +					- • 🛽
e⇒ c 08	https://192.166.10.1/0/administ	ration/addThcrl		Ŷ	8 =
D-Link	DSR-250v2		Q Search.		0
	Add TLS/CRL P	rofiles		Cancel	Apply
🗄 System and status					
Sa Administration	Method	🔾 Generatz 🔹 TLS Upload 🔾 Of	1L Upload		
Event logging	Profile Name	Dar250			
Maintenance	Upfield	Browse operwpeá.sh	Upload		
Management					
Certificate management					
Celhadudae					



CRL upload

Field	Description
Method	It says about how we are adding tls/crl profile
Profile name	name of profile
upload	we need to give file and upload

D-Link DSR-251V2 × +					- * 🙆
e⇒ 0 0&	https://192.168.10.1/W/administry	ablom/add/Thecri		Ŷ	8 =
D-Link	DSR-250v2		Q Search		0
🕄 System and status	Add TLS/CRL Pr	ofiles		Cancel	Apply
a Administration	Method	O Generate O TLS Upload	CPL Upload		
Event logging	Profile Name	Dur250			
Maintenance	Uplicad	Browse sal_tis_prog	Upload		
Management					
Certificate management					
Schedules					
Diagnostic					
Authentication					
鼎 Interface					
🖸 D-Link DSR-251v2 🛛 🗴 🕺 Edit	: - TLSJCAL Profiles - D × +				- • 🔕
e⇒o 0&	https://192.104.10.1/%/administra	stion/certificate_menagementDective	etlact	Ŷ	Θ =
D-Link	DER SEAUS		(A same		6





Click Add icon to add a new entry to the table. This opens the Add tls/crl profile . To delete more than one entry, select the checkbox you want to delete, and click Delete icon.

Schedules

Schedule policies

The *Schedule policies* page displays all the default and configured schedule policies for the devices. These schedules are used to activate a few features of the gateway for a certain period of time. So, for features like web content filter, access control, etc., you can configure the schedules on this page, and then you can select one of these schedules from the drop-down list while configuring these features.



The fields available in the table are as follows:

Field	Description
Name	Enter the name of the configured schedule.
Start time (24 hh:mm)	Enter the start time.
End time (24 hh:mm)	Enter the stop time.
Days	Select the checkboxes of days when you want to apply the schedule policy.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Click Add (+ button) to add a new schedule. To delete multiple entries at once, select the checkboxes of the configured schedule you want to delete, and click Delete Icon. To edit schedule click on edit icon. Diagnostics



Q Search.

⊗

	Diagnostic		Gancel Apply
System and status	Ping		
Administration	ring		
Event logging	IP address / FIGON	mm gropis com Ping	
Maintenance			
Management	Traceroute		
Certificate management	IF address / FGOM	men dink com Trace code	
Schedules	System check		
Diagnostic			
Authentication	iPvi tabio	Drigitoy	
鼎. Interface	Debug logs		
	Logi	Download	
	Capture packets		
	Interface	Port group 4 -	
	Action	Þ	
	Speed test		
		PERMIT	
	r	arEasTone (S Go ()	

Ping

As part of the diagnostics tools supported by the router, you can ping an IP address or FQDN (Fully Qualified Domain Name). You can use this feature to test connectivity between the router and another device connected to the router.

Ping		
Folders *FCDN	www.google.com Ping	
Result	PING www.google.com (142.200.195.164) 64(92) bytes of a 72 bytes from mag00s47 in 14.16100.net (142.200.106.164 time=29.0 ms	
	72 bytes from maa50s47 in 14. te100.net (142,250,196,164	4): http://www.awarda.tk/

The fields available in this section are as follows:

Field	Description
IP address / FQDN	Enter the IP address or FQDN.
Ping	Click Ping to send an ICMP echo request packet to the destination using the IPv4 network.
Result	It displays the result of the IP address. If the destination IP address is active, you can see a response. A <i>response timed-out</i> message indicates that the destination is either not active or is blocking ping requests.

Traceroute

The router DSR-250v2 provides a *Traceroute* function to map the network path to a public host. In addition, it displays up to 30 "hops" between this gateway and the destination.

P address / FGDN	www.durecom	TREESENC	
försutt -	traceroute to www.dlime.com	n (104.20.90,84), 10 nops max, 50 ovte packets	
	1 10:10:1,1 (10:10:1:1) 1 2	440 ms 1 409 ms 1 355 ms	
	2 202 158 49 17 (202 159	43 17) 5 419 ms 5 439 ms 5 456 ms	
	3 202 151 46 8 6002 (53.1	0.955-447 ms 5-470 ms G 620 ms	

The fields available in this section are as follows:

Field	Description
IP address / FQDN	Enter the IP address or FQDN.
Traceroute	Click Traceroute to display all the routers present between the destination IP address and this router.
Result	This section displays the results of the Traceroute operation.

System check

As part of the diagnostics functions on the router, you can view the static and dynamic routes for IPv4.

wd table	Display							
Riouli		Kernel IP routing table						
	Destination	Gabeway	Gennask	Flaga	Metric	Ret	Use	Race
	0.0.0.0	10.10.1.1	0.0.0.0	UC	0	0	0	eth4
	10,10.0.0	0.0.0.0	265,255,0.0	U	0	0	0	eth4

The fields available in this section are as follows:

Field	Description	
IPv4 table	Click Display to display the results of the static and dynamic route of IPv4.	
Result	This section displays the results of the Traceroute operation.	

Debug logs

Debug logs	
Logs	Download

To download the debug logs, click Download. Then, select a location on your computer and save the file with the extension ".tgz."

Capture packets

The router lets you capture all packets that pass through the LAN and WAN interfaces. The packet trace's limit is 1MB of data per capture session. The router deletes the capture files exceeding 1MB creating a new capture file.

Capture packets			
Interface	Port group 4	- 0	
Action			

The fields available in this section are as follows:

Field	Description
Interface	Select an interface from the drop-down list for packet tracing.
Action	Click this button to start packet tracing. Click this button to stop packet tracing. Click this button to download the packet tracing file.

Speed test

This section allows you to check the Internet speed of your WAN connection. To check the speed, select the WAN port you want to test, and click **Go**. It displays the *Ping time, Upload speed,* and *Download speed* on the screen. Click **Again** to recheck the speed.



Chapter 3 Authentication

This chapter covers the following topics:

- User authentication status
- User data base
- Captive portal

User Authentication

					(in teast	0
	User out enforts	on i				
) system and earlier.						
Acceleration and	Used dispersion state in the					
1 Automation						
the activity date	Berley C. C.	L I MAR SMOK	Language States	[] (1) (1)	1. 1. AMPL11	
Open dis Selamon		L	2010)	A TWO PARTS	PROVINE AND	
	1.4	5.87M	Wire Drude -	VT	MD - 51-10-13	
cupora poru	K den	9.473	Addres Develope	1719	BC204, 030	
- Northers	2.0	104170	Active Lines and	 A state parts 	ment of the second	
Second .	Sec.	5.00 million	Sales Creation	0010	102 - 54 - 52 - 54	
NNU .						

This page displays the status of the authenticated users with the following details:

Field	Description
User account	It indicates the name of the user account.
User group	It displays the group's name to which the user account belongs.
Authentication server	It displays the authentication server that provides authentication to the account.
Application	It displays the name of the application.
IP address	It displays the IP address of the user.

User data base

This page covers the following topics:

User Account

External servers

User Account:

Use	e arceust	i) (si (ti fai	1997			
	đunab					
+	10					Q. Smith
+ ;	2 D		Maritar	Reactions Services	Description	Q Smith
+ ;				nter Austriand Services - Searception		

This page allows you to add user groups. The fields displayed are as follows:

Field	Description
Group name	It displays the name of the group.
Member	It displays the number of members present in the group.
Associated services	It displays the associated services with the group.
Description	It displays the description about the group.

To add a new local group, click the + icon.

D-Link	1144 5 30.2				Mar al		$> \otimes$
 Option are calls. 	Add foreal group					General	-4 π %
Z. Meridiality	C. C. C. B. C.	HI Gassies					
T Astrony	Description (Accession	Set Concern					
Den fall indiction Den Jahrens							
Capitor porta	New open en de rechtpelling						
A Portes						di Serah	
- S. Hereitek	Veries et		Annes Annes II	 Zeracieliza Veracieliza 	n - 746		
28 Chevel	here .		1421.46	Longer devicement			
19 Mars 19	162		This is a	Selected by her	_		
	14 M		and the second sec	And a second	=		
No. And	1200		1.1	Particle in the second of			
				5.3a	alara ar	1 - A - 1	a - 7
						-	

Field	Description

Group name	Enter the name of the group.
Description	Describe the group.
	Group membership list
User name	It displays the number of members present in the group.
Group	It displays the associated services with the group.
Description	It displays the description about the group.
Join	Enable to add the already existing user to the group.

Local 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 commaseparated-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.

stal unors			
120			S. Barah
DEEL MADE	11 Oncupa	The Description	
stime -	ARABI STORE AND	DE AUTI NU VORKENER	
shiir	ADER	ADVE STRATCH HOLDER	
(part)	Q EVE	CE SET ACCORD	

```
Télène e e e e e e e e
```

The fields available in this section are as follows:

Field	Description
User name	It displays the name of the user.
Groups	It displays the name of the group to which the user belongs.
Description	It displays the description.

To add a new local user, click the + icon.

D-Link				4.347		
To Designer allele en	Add (000 upper				(m.	
e e and da	+:+:+					
Advertising the	(1997) (1997)	P 25 - 5649-4	H			
	in paramit.					
for a de la	Sector La cost ()		- ad			
9000 m	5+ 4+ 30-1+1	Marin				
See.	Av a hour					
N -1	ana ita					
en lan. An N						
,	r.					

Field	Description
User name	Enter the user name.
Group	Select the checkbox of the group to which you want to add the user.
New password	Enter a password of length 1 to 64 characters.
Confirm password	Confirm the password by reentering the same password.
Description (optional)	Enter the user's description. This field is optional.
Email (optional)	Enter the email of the user. This field is optional.
Mobile (optional)	Enter the mobile number of the user. This field is optional.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

External auth server

Authentication Server

An authentication server is a network service that provides credentials to authenticated users to access the network. When a user enters these credentials into the login page, they get access to the network. In addition, the authentication server maintains a database of users or an external authentication server configuration.

This router page lists all the configured authentication servers and allows the user to configure them for the device.



The fields displayed on this page are as follows:

Field	Description
Server name	It indicates the name of the server.
Туре	It displays the type of server. It could be any of the following server types: RADIUS, LDAP, Active Directory, POP3, or NT Domain.
Primary server	It displays the IP address of the authentication server.
Port	It displays the authentication server port.
Accounting server	Enter the IP address of the RADIUS accounting server.

Port	Enter the RADIUS accounting port.
Enable	Select the checkbox to enable the server.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Click + to add an external authentication server.

Adding RADIUS server

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

D-Link.	03.5A/2			17	-1981
2 Rock and take of	Add or thendoor	ion torver			1 mi
×	10000	1			
T Call a description	S41.0.00 S1	0.000	÷		
Output the factor	News	T=118.8			
(Conset	22	1	-		
atre an	000				
	W.S. Lawrence				
1.74t	we wanted again	1140.000			
* *	5.0000	10.0			
1 0%	list.	1 of General			
	114.055	1 M	10 C		

Field	Description
Server name	Enter the name of the server.
Authentication type	Select RADIUS as the type of server.
Primary server	Enter the IP address of the authentication server.
Port	Enter the 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 the RADIUS server.
Radius accounting	Select the checkbox to enable this feature to configure Accounting Interim Interval (in seconds). The device sends the traffic statistics of a session in accounting messages to the configured Radius Server.
Accounting server	Enter the IP address of the RADIUS accounting server.
Port	Enter the RADIUS accounting port.
Secret	Enter the secret key that allows the device to get authenticated with the RADIUS accounting server. The secret authenticates all the radius accounting transactions between the client and the RADIUS accounting server.
Interim interval	Enter the interim interval in seconds. Then, the device sends the Radius Accounting (Interim- Update) packets at the interim interval. The value range is 300 - 3600. By default, it is 300.

Adding LDAP server

The LDAP authentication method uses LDAP to exchange authentication credentials between the gateway 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 different groups can be authenticated since the user information is stored hierarchically. Also, note that configuring an LDAP server on Windows or Linux servers is considerably less complex than setting up NT Domain or Active Directory servers for user authentication.

D-Link	10139.7		. n. m.	Ø
	ARALIMON	CD definer	- 201	-
- Levelare	bergen	(mainten		
Li Allenines De la latin a	and the second of	100 30		
One to care	Contraction of Contra	the second secon		
COST IN FORM	Pal	- Ann 2		
ti natua	Devis	man and facilities and		
tics the				
(Carlor)				
E VIII				
	- Q			

The fields available in this section are as follows:

Field	Description
Server name	Enter the name of the server.
Authentication type	Select LDAP as the type of server.
Primary server	Enter the IP address of the authentication server.
Port	Enter the authentication server port.
Base DN	Enter the base domain name.

Adding POP3 Server

POP3 is an application layer protocol most commonly used for email 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. A CA certificate verifies the POP3 server's certificate.

D-Link warate		(a. *
Asking the second	antatun weve	ų statistas
56- 40- m		
And Marine Conservation	N°	
Der klaser, State		
Rectand . Are		
Contract Contraction	6	
inisia Lans Lans	Not a more	


The fields available in this section are as follows:

Field	Description	
Server name	Enter the name of the server.	
Authentication type	ect POP3 as the type of server.	
Primary server	nter the IP address of the authentication server.	
Port	inter the authentication server port.	
Encryption	You can enable or disable the SSL support for POP3. If this option is enabled, it is mandatory to select a certificate authority for it.	
CA file	Select a Certificate Authority to verify the POP3 server's certificate.	

Adding Active Directory Server

Active Directory authentication is an enhanced version of NT Domain authentication. The Kerberos protocol is leveraged for authentication of users grouped in Organizational Units (OUs). 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.



The fields available in this section are as follows:

Field	Description
Server name	Enter the name of the server.
Authentication type	Select Active Directory as the type of server.
Primary server	Enter the IP address of the authentication server.
Port	Enter the authentication server port.
AD domain	

	Since Active Directory is the chosen authentication type, you must enter the Active Directory domain name. Users registered in the Active Directory database can now access the SSL VPN portal using their Active Directory username and password.
Hostname	Enter the server hostname for Active Directory.

Adding NT Domain Server

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

D-Link	n/91216.7		5 Barr		- (Q)
Superior and	Auki wili terrinde.	R: deller		1.1804	-
an terretar an 11 diseben en	Sec. and	(= resider			
One de com	(# 10 ⁻¹	1/1-11-11			
Versional A series C verse 2 Trans D An A E PD	0-1				

The fields available in this section are as follows:

Field	Description
Server name	Enter the name of the server.
Authentication type	Select Active Directory as the type of server.
Primary server	Enter the IP address of the authentication server.
Workgroup	Enter the NT workgroup name(s).

Captive Portal

A *captive portal* is a web page that appears when an unauthenticated user tries to access the Internet. Captive portal verifies and authenticates the user and then only grants internet access. It is done by entering the login credentials and accepting the terms and conditions of service. This feature helps the router monitor and control Internet usage.

The router DSR-250v2 allows its users to configure the captive portal page and provides various authentication methods. It consists of the following two sections:

- Login profiles
- Captive portal configurations

Login Profiles

The Router, allows its users to customize the login page as per their requirements, e.g., they can add a specific text and images. It allows you to create and edit login pages. Associate login profiles on VLANs separately.





The fields available on this page are as follows:

Field	Description
Name	It displays the name of the login profile.
Browser title	It displays the browser title.

Click + to add a new login profile.

R-Link	2.0058.012		$\int \Delta t = 2 \pi t r r dr$.	2 3
	Add login profile			Constr. Angle
Ryden and define				
Alexandre de	Concentration in the			
🔄 é de destra	Prov.	141 Constants		
the submits for	Converties	Test Concess of		
LIN STORES	1000000	par C. p.a.		
Capitor partial 7. latenteer		- OF ST ST ST		
al. Helenik		1 1 1 · 1 · 1		
		bala i		
🔆 F mel				
)" form the	President destation			
91 V7 V	Desker cand	Chillippe Serie		
	a construction of	1315 Sec. 1		
	Logi sere	tais a		
	Lation	ta -		
	L AN CAN	500 -		
	Logic stabilis			
		1994 I.M.		
	and the straight	Linear search		
	A constant	and an exception of the second		
	A	8		
		Autor v		

		1.1		
	All controls			
	Self-self to	847.7398	· · · ·	
	Set our	1.000		
	Particular	16 M	· · ·	
Example details				
1.0407	9			
	Sec. and			
	Part sets	in an		

The fields available on this page are as follows:

Field	Description	
General details		
Name	Enter a name for this login profile.	
Browser title	Enter the text that will appear in the title of the browser during the captive portal session.	
Background	 Choices are: Image: It displays an image as the background on the page. Use the Page Background Image field to select a background image. Color: It sets the background color on the page. Select the color from the drop-down list. 	
	Header details	
Background	 Choices are: Image: It shows a photo on the page. Use the radio buttons to select an image. Color: It shows the background color on the page. Select a background color from the drop-down list. 	
Header caption	Enter the text that appears in the header of the login page during the captive portal session.	
Font name	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 session title	Enter the text that appears in the title of the login box when the user logs in to the captive portal session.	
Welcome message	Enter the welcome message that appears when users log in to the captive session successfully.	
Error message	Enter the error message that appears when users fail to log in to the captive session successfully.	
	Advertisement details	
Enable	Select the checkbox for an advertisement on the login page.	
Ad place	Select where you want to place the advertisement. You could put it either at the top or at the bottom of the page.	
Ad content	Write the content of the advertisement.	
Font name	Select the font of the text to be displayed.	

Font size	Font size Select the size of the text font to be displaced.	
Font color	Select the color for the advertisement text.	
Footer details		
Enable	Enable Select the checkbox to enable changes to the footer content on the login page.	
Content	Enter the text that appears in the footer.	
Font color	Select the color of the text that appears in the footer.	

Captive Portal Configuration

You can enable Captive Portal on a per-VLAN basis. Then, the hosts of a particular VLAN get authentication via the Captive Portal, which may be a customized portal with special instructions and branding 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 get authentication through the selected server.

Natrie	123		
Login profile	distants	100	
Authentication server	Local user databout	(.)	U.
Local user group	default_user	85	
ide timeriut	30	10	minicites
UNIT INDIGECTION			
Urini.	news Passiblick.com		
linterwal	15	•	minister
Assign VLAN	2		
VLAN	AR	1	11

The fields available on the Captive portal configuration page are as follows:

Field	Description	
Name	Enter the captive portal name.	
Login profile	elect the configured login profile page from the drop-down list.	
Authentication server	Select the authentication server. Local Authentication: Local authentication is a method where the end-user is redirected to a page that provides options to enter username and password validated against the configured user database of the device. External authentication :If this is selected, the end-user is redirected to a page that provides options to enter username and password validated against the configured external	

	authentication server. The list of servers includes RADIUS, LDAP, POP3, Active Directory, and NT domain.
Local user group	This option appears when we select local authentication as authentication server. Select the local user group from the drop-down list.
Idle timeout	Idle timeout refers to the end of the session when no data traffic is observed for the given amount of time. The client connected to the gateway re-authenticates once the timer reaches the idle timeout to access the Internet. This value is per gateway and applicable to all the clients connected to the gateway. The range of idle timeout is between 1-1440 minutes.
URL redirection	Select the checkbox to enable URL redirection. If enabled, the user is redirected to the configured URL after the successful authentication.
URL	Enter the URL where the user gets redirected after a successful login.
Interval	Select the periodic interval when the router redirects the user to the URL mentioned in the above field.
Assign VLAN	Enable this feature if you want to assign the captive portal to any VLANs.
VLAN	Select the VLAN ID or name on which the captive portal is to be enabled.

Chapter 4 Interface

This section provides an overview of the port status. You can configure WAN, LAN, and DMZ ports on this page. The Unified services router, DSR-250v2 supports 1 WAN port and other as configurable port as WAN2 or DMZ Another feature that the router supports is Dynamic DNS (DDNS), i.e., an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. You may also configure the IP aliasing feature to associate another IP address with the interface.

The Interface section includes the following topics:

- Port configuration
 - Port settings
 - DDNS
 - IP aliasing
- LAN Clients
 - IP managment
 - DNS host mapping
- VLAN settings

Port Configuration

Port Settings

This section allows you to select the Ethernet port configuration you want to apply to each port,By default each port is connected to port group (192.168.10.x) to change this we need to change port settings.

Eg: if we give port 2 to port group 2 then device which is connected to port 2 will be in different network(192.168.11.x by default)

Note : port 4 can be used either as LAN,WAN or DMZ

Portentings					
In the Local Manual	Post 1	No.1	Parts	Parte	
For Difference 4		0	0	0	
Per Histop S	0	0	0	0	
Prof Marca 2		0	0	0	
Prof Margaria			*	*	

Click on the radio button to select the apply the configured port settings.

Network Configuration

This section allows you to configure the ports.

Network Configuration							
1							
ICONSCIENCE NAME	NUMBER OF STREET	Prior content Tour content a final	NUMBER OF SEC.	00034703	DD17 DDADLL2	87.02M	

E E E graup d	LAN .	172368-1723	200.201000.5		2
For Lign step 2	LAN	122,162,122,1	200.000-000.0		2
Profige say 2	1441	122,182,111,1	200.201200.0		2
En l'Arrige I	144	122.102.1211	200 200 200 C		2

The fields available on this page are as follows:

Field	Description
Interface name	It displays the name of the interface.
Interface type	It displays the type of the interface.
IP address	It displays the IP address of the interface.
Subnet mask	It displays the subnet mask.
Gateway	It displays the gateway IP address.
DDNS	It displays the status of the DDNS feature.
Enable	You can enable any port configuration by selecting the checkbox.

The Port Configuration section explains how to configure the following ports:

- WAN Port
- LAN Port

WAN Port

The unified services router DSR-250v2 has one WAN port to connect to the Internet or another network subnet.

D -Link	0.05-25262		
	Edit port configure	rien	
 Nysemiana maani Aominisamiani 	Lana		
🗖 Administration	Interface by a	ena -	
Z. Kostan	est of the second	-	
Proti se li paralle : L'an districi	to the store	97	• .
V Maring.	NNH cellings		
 Hearth 	a national spec	Shiki -	-
20 FINAL	5.00 Kep	8	
() secure El secu	10.00 B	14	
	A mailer 19-		
	to any state	DIRACTI	
	to a read many	20010300	
	A BUTTER OF LOOPING	DIK.L	
	transfer to the	12 K. I.	
	the second set in the second	80.04	
	Caller Antonio Constanti	an anna ana	-
	Antoniana Antonia		
	40.055	28	0.000

The fields available on this page are as follows:

Field	Description

Ports	You cannot edit this field. It is 5.
Interface type	Select the type of interface.
Interface name	Enter the interface name.
Route mode	Choose a route mode. The options are NAT and Classical.
	WAN settings
Connection type	Select a connection type from the following options: DHCP, Static IP, PPPoE, PPTP, L2TP, Russian PPPoE, Russian PPTP, and Russian L2TP.
VLAN tag	Enable or disable the VLAN tag on the configured WAN port.
VLAN ID	If the VLAN tag is enabled, enter the VLAN ID.
MAC address source	Select Use default MAC to use the MAC address from the configured WAN port to associate with your modem/ISP, or Use this MAC to enter a MAC address manually.
MAC address	If you select Use this MAC, enter the MAC address you want to associate with your ISP.
Jumbo frame	Jumbo frames are Ethernet frames with more than 1500 bytes of payload. When this feature is enabled, the LAN devices can exchange information at the Jumbo frames rate.
MTU size (byte)	The MTU (Maximum Transmit Unit) is the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 Bytes, and for PPPoE/ PPTP connections, it is 1492 Bytes. For all L2TP connections, it is 1460 Bytes.
	DHCP
Hostname	Enter the hostname if required by your ISP.
DNS Server	Select either Get dynamically from ISP or Use these DNS servers to enter DNS servers manually.
Primary DNS	If you select Use these DNS servers , enter the primary DNS server IP address.
Secondary DNS (optional)	If you select Use these DNS servers , enter the secondary DNS server IP address. It is an optional field.
	Static IP
IP address	Enter the static address that your ISP assigned to you.
IP subnet mask	Enter the IP subnet mask.
Gateway IP address	Enter the default gateway IP address.
Primary DNS	If you select Static IP as the address mode, enter the static primary DNS IP address in the respective subnet.
Secondary DNS (optional)	If you select Static IP as the address mode, enter the secondary DNS server IP address. It is an optional field.
	РРРоЕ
Address mode	Select either Dynamic IP or Static IP.
IP address	If you select Static IP, enter the IP address supplied to you by your ISP.
IP subnet mask	If you select Static IP, enter the subnet mask supplied to you by your ISP.
User name	Enter your PPPoE user name.
Password	Enter your PPPoE password.
Service (Optional)	If your ISP supports the service name, enter it here.
Authentication type	Select the type of Authentication to use (Auto-Negotiate, PAP, CHAP, MS-CHAP, or MS-CHAPv2).
Reconnect mode	Select one of the following options:
	• Always on: The connection is always on.

Primary DNS Secondary DNS (optional) Maximum idle time	Select either Get dynamically from ISP or Use DNS as below to enter DNS servers manually. If you select Use these DNS servers , enter the primary DNS server IP address. If you select Use these DNS servers , enter the secondary DNS server IP address. It is an optional field. Enter the number of minutes in the <i>Maximum idle time</i> field. This feature is useful if your ISP charges you based on the time you are connected. This field is available only when On- demand is selected. PPTP Select Dynamic IP or Static IP (IP settings supplied by your ISP).
Secondary DNS (optional) Maximum idle time	If you select Use these DNS servers , enter the secondary DNS server IP address. It is an optional field. Enter the number of minutes in the <i>Maximum idle time</i> field. This feature is useful if your ISP charges you based on the time you are connected. This field is available only when On-demand is selected. PPTP
Maximum idle time	optional field. Enter the number of minutes in the <i>Maximum idle time</i> field. This feature is useful if your ISP charges you based on the time you are connected. This field is available only when On-demand is selected. PPTP
	charges you based on the time you are connected. This field is available only when On- demand is selected.
Address mode	
Address mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).
Server address	Enter your PPTP server IP address or the domain name.
User name	Enter your PPTP user name.
Password	Enter your PPTP password.
IP address	If you select Static IP as the address mode, enter the IP address supplied by your ISP.
IP subnet mask	If you select Static IP as the address mode, enter the subnet mask supplied by your ISP.
IP gateway	If you select Static IP as the address mode, enter the gateway IP address supplied by your ISP.
	If you select Static IP as the address mode, enter the static DNS IP address in the respective subnet. It is a option field.
MPPE encryption	Enable it if the PPTP server supports this feature.
	Some ISPs may require you to pay for usage time. Select On-Demand if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select Always On to have the gateway stay connected to the Internet.
, , , , , , , , , , , , , , , , , , ,	Enter the number of minutes in the <i>Maximum Idle Time</i> field. This feature is useful if your ISP charges you based on the time that you are connected. This field is available only when Ondemand is selected.
	L2TP
Address mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).
Server address	Enter your L2TP server IP address or the domain name.
IP address	If you select Static IP as the address mode, enter the IP address supplied by your ISP.
IP subnet mask	If you select Static IP as the address mode, enter the subnet mask supplied by your ISP.
IP gateway	If you select Static IP as the address mode, enter the gateway IP address supplied by your ISP
"	If you select Static IP as the address mode, enter the static DNS IP address in the respective subnet.
User name	Enter your L2TP user name.
Password	Enter your L2TP password.
Secret (Optional)	Enter a shared secret if your ISP supports it.
	Some ISPs may require you to pay for usage time. Select On-Demand if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select Always On to have the gateway stay connected to the Internet.
	Enter the number of minutes in the <i>Maximum Idle Time</i> field. This feature is useful if your ISP charges you based on the time that you are connected. This field is available only when Ondemand is selected.
	Russian PPPoE

Address mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).
IP address	If you select Static IP as the address mode, enter the IP address supplied by your ISP.
IP subnet mask	If you select Static IP as the address mode, enter the subnet mask supplied by your ISP.
User name	Enter your Russian PPPoE user name.
Password	Enter your Russian PPPoE user name.
Service (Optional)	If your ISP supports the service name, enter it here.
Authentication type	Select the authentication type from the drop-down list.
Reconnect mode	Some ISPs may require you to pay for usage time. Select On-Demand if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select Always On to have the gateway stay connected to the Internet.
Maximum idle time	Enter the number of minutes in the <i>Maximum Idle Time</i> field. This feature is useful if your ISP charges you based on the time that you are connected. This field is available only when On-demand is selected.
	Russian PPTP
Address mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).
IP address	If you select Static IP as the address mode, enter the IP address supplied by your ISP.
IP subnet mask	If you select Static IP as the address mode, enter the subnet mask supplied by your ISP.
IP gateway	If you select Static IP as the address mode, enter the gateway IP address supplied by your ISP.
Server address	Enter your Russian PPTP server IP address or the domain name.
Static DNS IP (optional)	If you select Static IP as the address mode, enter the static DNS IP address in the respective subnet. It is a option field.
User name	Enter your Russian PPTP user name.
Password	Enter your Russian PPTP user name.
MPPE encryption	Enable it if the Russian PPTP server supports this feature.
Authentication type	Select the authentication type from the drop-down list.
Reconnect mode	Some ISPs may require you to pay for usage time. Select On-Demand if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select Always On to have the gateway stay connected to the Internet.
Maximum idle time	Enter the number of minutes in the <i>Maximum Idle Time</i> field. This feature is useful if your ISP charges you based on the time that you are connected. This field is available only when On-demand is selected.
	Russian L2TP
Address mode	Select Dynamic IP or Static IP (IP settings supplied by your ISP).
IP address	If you select Static IP as the address mode, enter the IP address supplied by your ISP.
IP subnet mask	If you select Static IP as the address mode, enter the subnet mask supplied by your ISP.
IP gateway	If you select Static IP as the address mode, enter the gateway IP address supplied by your ISP.
Server address	Enter your Russian L2TP server IP address or the domain name.
Static DNS IP (optional)	If you select Static IP as the address mode, enter the static DNS IP address in the respective subnet. It is a option field.
User name	Enter your Russian PPTP user name.
Password	Enter your Russian PPTP user name.
Secret (Optional)	Enter the shared secret if your ISP supports it.
Authentication type	Select the authentication type from the drop-down list.

Reconnect mode	Some ISPs may require you to pay for usage time. Select On-Demand if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select Always On to have the gateway stay connected to the Internet.
Maximum idle time	Enter the number of minutes in the <i>Maximum Idle Time</i> field. This feature is useful if your ISP charges you based on the time that you are connected. This field is available only when On-demand is selected.

LAN Port

By default, the router as a Dynamic Host Configuration Protocol (DHCP) server to the hosts present on the LAN network. With DHCP, PCs and other LAN devices can be assigned IP addresses and addresses for DNS servers and the default gateway. The gateway's IP address serves as the gateway address for LAN clients, with the DHCP server enabled. The PCs in the LAN are assigned IP addresses from a pool of addresses if the DHCP server is configured.

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 forward DHCP packets to get the DHCP lease information from another DHCP server on the network.

You can configure the LAN port in the *Port configuration* section. Click on the radio button to select the LAN port group and then click on **Edit** to open the respective port configuration page.

Note:

- Port interface 1 and Port interface 5 are WAN and LAN ports, respectively.
- You can configure WAN, LAN, or DMZ ports on port interface 4 only.

D-Link	058-250v2					
	Edit port config	ination		ĺ2		
C System bare status		The last				
al administration	Parts	8 <u>70</u>				
E Automotion	mentals Max	1.48				
a, interface	methics server (Part Group 1				
Portuge digeration	Didge seizert	C1				
(u.ah setting)	LAN settings					
Network	ff actions	112.040.16.1				
Testal	3-devel must	135 235 235 3		1		
U. Scentty	press from	0				
The Autor	975/ ave	-1985		la/mi		
	Alay you too LAN	-				
	DHOI wede	Ohim		• DHCF and and	DHP may	
	Desariyane Consult	334				
	Satisfied & mithere	182.160.10.3				
	Entry # attract	152188.10.54		1		
	Detault general/	100138.10.1		1		
	12005 34 4 (4)	DVS show	(i) (i)			
	Laster (gros	1405		10 million		

The fields available on this page are as follows:

Field	Description
Interface type	Select LAN to configure the port as the LAN port.
	Note: You can not edit this field for Port interface 1, 2, 3 and 5 interfaces. Port interface 5 can only be configured as a WAN port and Port interface 1, 2, 3 as a LAN port.
Interface name	Specify the name for your LAN interface.
Bridge network	Enable this field to bridge this LAN to another VLAN.
Network	Select the network from the drop-down list. This field is available when you enable the <i>Bridge network</i> field.
IP address	Enter a new IP address for the gateway.
IP subnet mask	Enter the subnet mask for your network.
DHCP mode	Select one of the following modes:
	 None - Select None to turns off DHCP. DHCP server - If this is selected, the gateway will act as the DHCP server on your network. By default, the "DHCP server" is selected as the DHCP mode. DHCP relay - If this is selected, DHCP clients on your network will receive IP address leases from a DHCP server on a different subnet.
Domain name	Enter a domain name for LAN configuration.
Starting IP address	Enter the starting IP address.
Ending IP address	Enter the ending IP address.
Default gateway	If DHCP mode is DHCP server , enter the default gateway for the DHCP server mode.
DNS server	 Select one of the following options for DNS servers for the DHCP clients: DNS Proxy: Enable or disable DNS Proxy on this VLAN. When the DNS Proxy field is selected, the gateway acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. DNS from ISP: This option sends all DNS requests to the ISP's DNS Servers. Static DNS: This option sends all DNS requests to the configured static DNS servers.
Primary DNS server	Enter the primary DNS Server IP address.
Secondary DNS server (optional)	Enter the secondary DNS Server IP address. It is an optional field.
Lease time (minutes)	Enter the duration (in minutes) for which IP addresses will be leased to clients.
Relay gateway	Enter the relay gateway IP address. This field is available when you select <i>DHCP mode</i> as D HCP relay .
Allow ping from LAN	If this option is disabled, the ping requests to the LAN interface are blocked.
DNS Proxy	When the DNS Proxy field is enabled, the gateway acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. This field is available when you select DHCP relay or None as the DHCP mode.
Jumbo frame	Jumbo frames are Ethernet frames with more than 1500 bytes of payload. When this feature is enabled, the LAN devices can exchange information at the Jumbo frames rate.
Apply	Click apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

DMZ Port

The router supports one of the physical ports to be configured as a dedicated DMZ port. A DMZ is a sub-network that is open to the public but behind the firewall. The DMZ provides security to the network, as specific services/ports exposed to the Internet on the DMZ do not get exposed to the Intranet. Therefore, it is recommended that hosts exposed to the Internet (such as web or email servers) be placed in the DMZ network. Firewall rules can permit access to specific services/ports to the DMZ from LAN or WAN. In an attack on any of the DMZ nodes, the LAN is not necessarily vulnerable. 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 router. You can configure Port interface 4 as DMZ ports in the *Port Configuration* section. Select radio button of interface type 4 for port 4 and Apply the configurations. Select interface type 4 and Click **Edit ion** to open the respective port configuration page.

	Port settings						
	provide a financia		Aug. 1	Art	Port I	1010	
	Post Grand J		0	0			
	Part Great 2						
	Perf Ormer L						
	2114					•	
D-Li	nk	055 256-2					
	1	Edit port config	uration		<		
🚊 System e	optimizations.				à		
a Administ	netwer:	Anto.	040				
🗄 Autoriti	5.0500-	energies spe	2002]		
A Interface	07	and the second second	0//3	_]		
(Pathony) (LAN) me	nguration nts	DNZ settings					
WEAN DE		Failure	122.168.128.1				
· Network	55 1	24010.000	259.259.255.0				
I frewell		Janisi hane	G1				
3) Security		Intra stare	1500	- 1	DjOH		
E. wit		Allow along from LAM					
		1902 mails	C Marine		B DICP incom	() DKF stap	
		Donas same tiptoral	DLim				
		Surray # ettrain	131318.526.3				
		Breing Platitions	100.168 129156				
		Datus papersy	1013181203				
		1001	(85-(10))	- 28	1		

The fields available on this page are as follows:

Field	Description
Interface type	Select DMZ to configure the port as the DMZ port.
Interface name	Specify the name for your DMZ interface.
IP address	Enter a new IP address for the device.
IP subnet mask	Enter the subnet mask for your network.
DHCP mode	Select one of the following modes:
	 None - Select None to turns off DHCP. DHCP server - If this is selected, the gateway will act as the DHCP server on your network. By default, the "DHCP server" is selected as the DHCP mode.

	• DHCP relay - If this is selected, DHCP clients on your network will receive IP address leases from a DHCP server on a different subnet.
Domain name	Enter a domain name for DMZ configuration.
Starting IP address	Enter the starting IP address.
Ending IP address	Enter the ending IP address.
Default gateway	If you select DHCP Server as the DHCP mode, enter the default gateway for the DHCP server mode.
DNS server	 Select one of the following options for DNS servers for the DHCP clients: DNS Proxy: Enable or disable DNS Proxy. When the DNS Proxy field is selected, the device acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. DNS from ISP: This option sends all DNS requests to the ISP's DNS Servers. Static DNS: This option sends all DNS requests to the configured static DNS servers.
Primary DNS server	Enter the primary DNS Server IP address.
Secondary DNS server (optional)	Enter the secondary DNS Server IP address. It is an optional field.
Jumbo frame	Jumbo frames are Ethernet frames with more than 1500 bytes of payload. When this feature is enabled, the LAN devices can exchange information at the Jumbo frames rate.
Lease time (minutes)	Enter the duration (in minutes) for which IP addresses will be leased to clients.
Relay gateway	Enter the relay gateway IP address. This field is available when you select <i>DHCP mode</i> as D HCP relay .
Allow ping from LAN	If this option is disabled, the ping requests to the LAN interface are blocked.
DNS Proxy	When the DNS Proxy field is enabled, the device acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. This field is available when you select DHCP relay or None as the DHCP mode.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

WAN Mode Configuration

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

To use Auto-rollover or Load Balancing, you must configure WAN link failure detection. This involves accessing DNS servers on the Internet or ping to an Internet address (user-defined). In load balancing, you can also select *None* to disable the failure detection feature. When the failure detection is enabled, specify the retry interval and the number of attempts it has to connect to the configured server. If all the attempts are failed, the WAN port is considered to be down.

This section discusses the following WAN modes:

- Primary WAN
- Auto-rollover using WAN
- Load Balancing
 - Round Robin
 - Spillover mode

Primary WAN

If you do not want to use Auto-rollover or Load balancing, select **Primary WAN** as the WAN mode and select the WAN port you want to set as the primary WAN port.

WAN mode configuration

WAN mode:

Primary WAN

Using primary WAN port



Auto-rollover using WAN

In the Auto-rollover using WAN mode, one of the WAN ports is assigned as the primary Internet link for all the Internet traffic; the secondary WAN port is used for redundancy if 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). If a failure occurs on the primary port, the Internet traffic will roll over to the backup port. When configured in Auto-rollover mode, the link status of the primary WAN port is checked at regular intervals as defined by the failure detection settings.

WAN mode configuration	Ca.		
WAN mode	Auto-rollover using WAN	14]
Auto-rollover using WAN por	t		
Primary WAN port	WANI	۲	
Secondary WAN port	Select secondary WAN port	25	
Health check	WAN DNS Servers	<u> 1</u>	
Retry interval	5		seconds
Failtowir alber	2		Natures

If you want to use Auto-rollover, select *Auto-rollover using WAN* as the WAN mode and enter the following details.

Field	Description
WAN mode	Select Auto-rollover using WAN.
Primary WAN port	Select the primary WAN port.
Secondary WAN port	Select the secondary WAN port.
Health check	 Select one of the following options for the health check: WAN DNS Servers: If you select this option, it detects the health of a WAN link using the WAN DNS servers configured in the WAN Settings pages. DNS Servers: If you select this option, it detects WAN health by using a specific DNS server. Select DNS Servers and enter the IP addresses of custom DNS servers for the primary and secondary WANs.

	• Ping IP address : If you select this option, ping to an IP address to detect WAN health. Select this option and enter the IP addresses in the fields to ping from the primary and secondary WANs. Ensure that this destination host is reliable.
Primary WAN	Enter the IP address whose health could be checked using the primary WAN port.
Secondary WAN	Enter the IP address whose health could be checked using the secondary WAN port.
Retry interval	Enter the retry time duration in seconds to check the WAN health. By default, it is every 30 seconds.
Failover after	Enter the number of failures after which the port is considered to be down.

Load Balancing

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

Load balancing is beneficial 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.

The gateway currently supports two algorithms for Load Balancing:

- Round Robin: This algorithm works in a recurring process where the packets are routed to the available WAN ports in a sequence
 irrespective of the connection speed of any WAN ports. If one packet is forwarded to one WAN port, the next packet will automatically go
 to the next WAN port. This ensures that the traffic load is distributed among all the active WAN ports.
- Spillover: If the Spillover method is selected, one WAN acts as a dedicated link until a defined bandwidth threshold is reached. After this, the next WAN will be used for new connections. Inbound connections on WAN are permitted with this mode, as the spillover logic governs outbound connections moving from one WAN to the other WAN.

You can configure spillover mode by using the following options:

- Load Tolerance: It is the percentage of bandwidth after which the gateway 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 max bandwidth load tolerance value, the gateway will spill over the next connections to the next WAN.

For example, if the maximum bandwidth of a 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 gateway will spill over new outbound connections to the next WAN. The maximum value of load tolerance is 80%, and the minimum is 20%.

Round Robin

WAN mode configuration

Round robin is an algorithm for load-balancing and is useful when the traffic load is distributed among all the WAN ports. When you select **Round-robin** as Load Balancing, configure the fields available on the page.

	101			
WAN inode		Lond bidencing	<u>.</u>	
Load balancing	U.			
Load balancing		Flound robm	C Spillment mode	
Health check		WAN DNS Servers		}
Retry interval		5		seconds
Codinate office		Č.S.		-

1.0000000

Field	Description
Load balancing	Select Round robin.
Health check	 Select any one of the following options: None: Select this option if you do not want to check the WAN health. WAN DNS Servers: Select this option to detect the health of a WAN link using the WAN DNS servers configured in the WAN Settings page. DNS Servers: Select this option to use a specific DNS server for detecting WAN health, select DNS Servers, and enter the IP addresses of custom DNS servers for the primary, secondary, and tertiary WAN ports. Ping IP address: Select this option to detect WAN health by pinging to an IP address, select this option, and enter the IP addresses in the fields to ping from the primary, secondary, and tertiary WAN ports.
Primary WAN	Enter the primary DNS server or primary IP address to ping.
Secondary WAN	Enter the secondary DNS server or secondary IP address to ping.
Retry interval	Enter the retry time duration in seconds to check the WAN health. By default, it is every 30 seconds.
Failover after	Enter the number of failures after which the port is considered to be down.

Spillover mode

WAN mode configuration

Select **Spillover mode** when you want a specific WAN to act as a dedicated link until a defined bandwidth threshold is reached. After this, the next WAN is used for new connections. When you select Spillover mode, configure the following fields.

WWN mode Load balancing τ. Load balancing 🖰 Round robin 🛛 🍵 Spillover mode i.cod balancing Health check WAN DNS Servers w. Reby interval 8 seconds Fislover after 2 folues. Load tolerance. 20, Max transferidity 512 4 hpit

Field	Description

Load balancing	Select Spillover mode.
Health check	 Select any one of the following options: None: Select this option if you do not want to check the WAN health. WAN DNS Servers: Select this option to detect the health of a WAN link using the WAN DNS servers configured in the WAN Settings page. DNS Servers: Select this option to use a specific DNS server for detecting WAN health. Select DNS Servers and enter the IP addresses of custom DNS servers for the primary, secondary, and tertiary WAN ports. Ping IP addresses in the fields to ping from the primary, secondary, and tertiary WAN ports.
Primary WAN	Enter the primary DNS server or primary IP address to ping.
Secondary WAN	Enter the secondary DNS server or secondary IP address to ping.
Retry interval is	Enter the retry time duration in seconds to check the WAN health. By default, it is every 30 seconds.
Failover after	Enter the number of failures after which the port is considered to be down.
	Spillover Configuration
Load tolerance	Enter the percentage of bandwidth, after which the gateway switches to the next WAN. The range is from 20 to 80.
Max bandwidth	This sets the maximum bandwidth tolerable by WAN for outbound traffic. The range of maximum bandwidth is from 1 to 1000 Mbps.

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. The IP aliasing section lists the configured IP aliases on the WAN interfaces. You can add a new IP alias and edit or delete the configured IP alias.

D-Link	[EAR(REA)	(C. least)	8
Alter a st	Most made coolig matter		
- Svenn ort cane	weeknots		
An and the second second	Онин самар УАХисс.		
utenia	Tready Will and		
Ean contigurator			
LANGRAM	PAssage		
VILAN SPIRAL	+ # ²⁰¹ 0000000000		C.A.M.
TRACK.	j antre i trakes	(i) demension	L B. T
int contra	Ment + 135100.001	m1285400.0	
Tease.	- wett - untitelet	201100-013	
	Contraction and Contraction	1.27 au	11

The fields displayed on the *IP aliasing* table are as follows:

Field	Description
Interface	It displays the WAN port on which the IP alias is configured.
IP address	It displays an alias IP address for the WAN interface you selected.
Subnet mask	It displays the subnet mask for the WAN interface you selected.

To delete multiple entries at once, select the checkboxes of the *IP aliasing* you want to delete, and click **Delete**. Click **Add icon** to add a new IP alias. This opens a new row to *Add IP aliasing* rule.

t d	2 years weeking	Ander Appry Victor				Q Tranki
	ant-door	11	(P) additions	11	Tritorioral	Ť
	WKNI	82	192 383 305 3	1	294-255 256-0	
2	WANT	2	195 (18590).		39-210.38-0	-
1	904001	1	at strait in m		Les mary man	

The fields available on this page are as follows:

Field	Description
Interface	Select the WAN port.
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.
Apply	Click Apply to save your settings.
Close	Click Close to revert to the previous settings.

LAN Clients

LAN clients page include IP management and DNS host mapping. You can assign IP settings to your clients on your network by adding a client's MAC address and the IP address to the DHCP server's database and assign a specific IP address to a domain name.

IP Management

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 the DHCP server's database. Whenever the gateway receives a request from a client, the MAC address of that client is compared with the MAC address list present in the database, and the corresponding IP address is assigned to the client.

Another available security measure is to allow outbound traffic (from LAN to WAN) when the LAN node has an IP address matching the MAC address bound to it. This is IP/MAC Binding. By enforcing the gateway to validate the source traffic's IP address with the unique MAC Address of the configured LAN node, the administrator can ensure traffic from that IP address is not spoofed. If a violation (i.e., the traffic's source IP address does not match up with the expected source MAC address) occurs, the packets will be dropped.

This section of LAN clients displays the IP management list.

D-Link	050 (1MNT				C.9. 1999.		Ø
	LAN clients					Grad	140
Antenan	Prezenteren 11	000710-0					
II. teaker							
Personnia Mana	+ 3	entri Alegie antietti				12.00004	
LAN CONS		1	$(1-\theta) \circ (\theta_1 \circ (\phi_1)) =$	 Jacketse, Landstation 	A BOARD	a beginning	10
ALCOLOGINE ST	B (199	a landered	100.004.13231	2			1.0
- henait					Ri-diam	40	(a) - 1
II. Incas							
S Secury							



The fields displayed in the *IP management list* table are as follows:

Field	Description
Hostname	It displays the hostname for the pair of IP and MAC addresses.
IP address	It displays the IP address you have assigned to the device.
MAC address	It displays the MAC address of the host that can connect on the configured interface and for which an IP address is reserved.
Address reservation	It displays if the DHCP reserved IP is enabled or disabled.
IP/MAC binding	It displays if the IP/MAC binding feature is enabled or disabled.
Log dropped packets	Enable this option to log dropped packets

Click Add icon to add a new entry. This opens a new row to Add IP management configuration. To delete multiple entries at once, select the checkboxes of the IP management that you want to delete, and click **Delete icon**.

	clients									Cancel	Appy
1935	topped	60())si	0								
пнср)	olting										
		etosotty	120200								
刊》	l seconda	0.0000.0								-Cl. Sewette	
世後	Hamindalar		Mill address		of salations	dilimi Interdiat	11	1942	19	12 Seette Log-bacol pactors	- 14
+ # 回 回 回	Heatinkie .		Minifaddaeee	4		dillersi.	11	PIMAG	19	log to col.	- 14

The fields available on the Add IP pool configuration page are as follows:

Field	Description
Host name	Enter the host name for the pair of IP and MAC addresses.
IP address	Enter the IP address you want to assign to this device. Note: This IP address must be in the same range as the starting/ending IP address under DHCP Settings for that interface.
MAC address	Enter the MAC address (xx:xx:xx:xx:xx format) of the host that can be connected on LAN, for which an IP address has to be reserved.
IP/MAC binding	You can enable or disable the IP/MAC binding feature. If enabled, it associates the host's information with IP/MAC Binding.
Address reservation	You can enable or disable the DHCP reserved IP feature.
Log dropped packets	Enable this option to log dropped packets
Apply	Click Apply to save your settings.
Close	Click Close to revert to the previous settings.

DNS Host Mapping

DNS Host Mapping is used to assign a specific IP address to a domain name. We can use this domain name instead of IP Address to access that particular host.

You will find a list of host names configured on the router with the following details:

D-Link	10.8-0.0<		(n
-	LAN cleans		Genel
Aline aline			
_ ourselato	- Meeting Inc.		
1 mm	+ 0		
	The second second		
tentime -	blays	IIII JP	
C. Contraction			(2.7) Sec. *
S. Anne			
2.344			

Field	Description
Host Name	It displays the host name.
IP address	It displays the IP address of the host.
Enable	Select enable or disable to activate or deactivate.

Click Add (+ button) to add a new entry. This opens a new row to Add mapping list. To delete multiple entries at once, select the checkboxes of the configured list you want to delete, and click Delete Icon.

LAN charts		
Mapping Ter		
+ 0		The second
() materia	P. W. Calman	a base a
[] [hotion	Inclusion and American Statements	2
		failure b [1] b e

Field	Description
Host Name	Enter the name of the host.
IP address	Enter the IP Address to be assigned to the Host Name.
Enable	Select enable or disable to activate or deactivate this route.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

VLAN Settings

The gateway supports virtual network isolation on the LAN by using VLANs. You can configure LAN devices to communicate in a sub-network defined by VLAN identifiers. A unique VLAN ID can be assigned for each LAN port so that traffic to and from the physical port can be isolated from the general LAN.

VLAN filtering is advantageous to limit broadcast packets of a device in a large network. In the Add VLAN profile page, define the virtual network.

VLAN Settings

The VLAN settings section displays a list of configured VLANs by name and VLAN ID. A VLAN membership can be created by clicking the Add button present above the list.

The VLAN ID value can be any number from 1 to 4094. By default, the router accepts only untagged traffic on the LAN interface. Therefore, for any tagged traffic, the user has to add a VLAN explicitly.

P-Link max	ter de la comp		(2) (140/B)	0
	VLAN settings			
C Annual Contra	VERMEN			
Attenden	+ 2 8			O. Sance
A mino			Logic Rend Laws	1.200400
Children Liftdere Stationersta Classes Classes	🔁 Wakife an Sei Sanad	() to all of () the Dr. Office and () of	Total and a line	Г. <u>Ш.</u>] С.,
in Secon _ upp.				

The fields available on the VLAN settings table are as follows:

Field	Description
Name	It displays the name of the VLAN.
VLAN ID	It displays the numeric value associated with the VLAN.
Base Interface	It displays the physical interface on which the VLAN is created.
IP address	It displays the IP address for the VLAN.
DHCP mode	It displays the selected DHCP mode for the VLAN.
IP range/ Relay server	It displays the IP range if DHCP mode is selected as DHCP server and Relay agent IP is DHCP mode is selected as DHCP relay
Captive portal	If the captive portal is enabled on the VLAN, this field displays the name of the captive portal.

Click Add icon to add a new VLAN. This opens the Add VLAN settings page. To delete multiple entries at once, select the check boxes of the configured VLANs you want to delete, and click **Delete icon**.

Add VLAN Set 11		080	404
2-8-8 0-1-9-800			
	1.0		
Transie Dame Seat	Conception		
-	generative designed and the set of the set o		
1444 (1.440 (1)	100.0010		
and reading	TRUMMON.		

 Refginer +	
 2.0	- in mult
 - E	
American .	

The fields available on the Add VLAN profile page are as follows:

Field	Description	
Name	Enter a unique name for this VLAN.	
VLAN ID	Enter a unique ID to this VLAN (1 - 4094).	
Base Interface	Select the physical interface on which VLAN is to be created.	
Intervlan routing	It allows or denies communication between VLAN networks.	
	VLAN subnet	
IP address	Enter an IP address for the VLAN subnet.	
Subnet mask	Enter the subnet mask for the VLAN subnet.	
DHCP mode	 Select one of the following modes: None: Select None to turns off DHCP. DHCP Server: If this is selected, the device will act as the DHCP server on your network. DHCP Relay: If this is selected, DHCP clients on your network will receive IP address leases from a DHCP server on a different subnet. 	
Domain name	Specify the domain name. This field is available only when DHCP Server is the <i>DHCP Mode</i> .	
Starting IP address	Enter the starting IP address.	
Ending IP address	Enter the ending IP address.	
Default gateway	If <i>DHCP mode</i> is DHCP Server , enter the default gateway for the DHCP server mode.	
DNS server	 Select one of the following options for DNS servers for the DHCP clients: DNS Proxy: Enable or disable DNS Proxy on this VLAN. If enabled, the gateway acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. DNS from ISP: This option sends all DNS requests to the ISP's DNS Servers. Static DNS: This option sends all DNS requests to the configured static DNS servers. 	
Primary DNS server	Enter the primary DNS Server IP address.	
Secondary DNS server	Enter the secondary DNS Server IP address.	
Lease time (minutes)	Enter the duration (in minutes) for which IP addresses will be leased to DHCP clients.	
Relay gateway	Enter the relay gateway IP address.	
Captive portal	You can enable or disable the captive portal feature over the VLAN.	
Captive portal name	Select the configured captive portal name from the drop-down list.	
DNS Proxy	When the DNS Proxy field is enabled, the gateway acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. This field is available when you select DHCP Relay or None as the DHCP mode.	
Apply	Click Apply to save your settings.	
Close	Click Close to revert to the previous settings.	

Chapter 5 Network

This chapter covers the following topics:

Static Route

Policy Route

RIP Configuration

OSPFv2 Configuration

Bandwidth management

Session limiting

Routing

Routing refers to the path that the packets follow from the source to the destination in the most optimum manner. This section of the Network provides you with the configuration fields required to manage the routing process in the network. Various methods are supported by the DSR-250v2 like the Static Route, Policy Route, RIP, and OSPFv2.

This section covers the following topics:

Static Route

Policy Route

RIP Configuration

OSPFv2 Configuration

Static Route

Static routing is a conventional method where the gateway uses the manually configured route path, and if any changes occur, the static route is to be reconfigured manually. Policy route allows you to configure routing policy based on certain parameters like the source address, destination address, source port, or destination port.

Static IPv4 routes:

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

Manually adding static routes to this device allows you to define the traffic path selection from one interface to another. There is no communication between this gateway 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 Static Route page displays all routes added manually by an administrator and allows several operations on the static routes.

D-Link	063-25342				S. Steel			${}_{\bigcirc}$
	And eg					1.000	- 10	TH.
ill System est state in Advintration								
A rise in sec.	Static (Perf realise							
75 History								
E REPARTS	+ 2 0							-
Walter	1. kare	 Instance Instance 	100100-0000	DRI DRI PLUTT	score and	2.	21 billion	-
Derroger					NOK (0071	34 14	11 A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A.A	311

You will find a list of static routes configured on the gateway with the following details:

Field	Description
Name It displays the name of the route.	
Destination	It displays the IP address of the static route's destination.
Subnet mask	It displays the subnet mask of the static route.
Gateway	

	It displays the IP address of the gateway through which the destination host or network can be reached.
Interface	It displays the physical network interface (WAN, DMZ, VLAN, or LAN) through which this route is accessible.
Metric	It displays a value between 2 and 15.
Enable	Select enable or disable to activate or deactivate this route.

Click Add (+ button) to add a new entry. This opens the Add static route page. To delete multiple entries at once, select the checkboxes of the configured static route you want to delete, and click **Delete Icon**.

Apply

Cancell

Add static route

Marr+	512
Desiretion Politica	199.559.20.100
Sabhad maik	256,245,237,0
Satesau (Fordosta	152,155,10 10
9.0214.0	Part Oroug 1
Meter	(a) (iii)
3. Arra	

The fields available on this page are as follows:

Field	Description
Name	Enter the name of the route.
Destination IP address	Enter the IP address of the static route's destination.
Subnet mask	Enter the subnet mask of the static route.
Gateway IP address	Enter the IP address of the gateway through which the destination host or network can be reached.
Interface	Select a physical network interface (WAN, DMZ, VLAN, or LAN) through which this route is accessible.
Metric	Enter a value between 2 and 15. It determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen.
Private	Enable this feature to make this route private. If the route is made private, the route will not be shared in a RIP.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Policy Route

Policy routes are useful when the Load Balancing feature is in use. Selecting TCP/UDP, you can assign the type of traffic to go over the specified WAN ports. The source network, source address, the destination network, a destination address, service, or protocol can be associated with a particular WAN port for increased flexibility.

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. Policy routes are only applicable when load balancing mode is enabled and more than one WAN is configured.

Policy routes 🎒

्मः स	63,9K								77
E.	maria la	Perman	1 Inchester	in magnet	1. Built Barrier	المعتم المعالا الل	touchart	a present	
17	1134	400	140,004.02.008	1 (188.8.5	141-169-10 100	4458.	NEM		
						74.67.610.0	12		

Field	Description
Name	It displays the name of the policy route.
Protocol	It displays the protocol placed in the transport layers of the Internet protocol suite.
Source network	It displays the source network. It options are Any, an IP address, and a range of IP address.
Source port	It displays a source port for which the policy route will be applicable.
Destination network	It displays the destination network. Its options are Any, an IP address, and a range of IP addresses.
Destination port	It displays a destination port for which the policy route will be applicable.
Local Gateway	It displays the WAN interface.
Enable	You can enable or disable the selected policy route.

To delete multiple entries at once, select the checkboxes of the policy route you want to delete, and click **Delete icon**. Click **Add(+ button)** to add more entries. This opens the *Add policy route* page.

Add policy rout	e.		Cancel
Name	1234		
hitseface	WWR	1	
Pranacol	AMY.	te.	
source network	132.164.10.300	0	
Source port	3.941	0	
Destination retained	192168.20106	0	

The fields available on the Add policy route page are as follows:

1003

Dedisation perf.

Field	Description
Name	Enter the name of the policy route.
Local gateway	Select the WAN interface.
Protocol	Select one of the protocols that are commonly placed in the transport layers of the Internet protocol suite.
Source network	Enter an IP address, a range of IP addresses, or Any as the source network.
Source port	A port is a communication endpoint. Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the port number. The most common protocols that use port numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Here, the <i>Source port</i> is an integer in the range of 1-65535 initiated from a specific application on the source IP. Enter a source port number.

Destination network	Enter an IP address, a range of IP addresses, or Any as the destination network.
Destination port	Destination Port is an integer in the range of 1-65535 destined to a specific application on destination IP. Enter the destination port number.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Dynamic route

Protocols that the DSR-250V2 is the Routing Information Protocol (RIP). It is a protocol that keeps a check on the number of hops a packet can make from its source to destination. Similarly, you will also learn to configure OSPFv2 in this section. OSPFv2 is a dynamic protocol that routes Internet Protocol (IP) packets solely within a single routing domain.

RIP:

Dynamic routing using the Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) common in LAN. With RIP, DSR-250V2 can exchange routing information with other supported gateways in the LAN and allow for dynamic adjustment of routing tables to adapt to modifications in the LAN without interrupting traffic flow.

D-Link	055-250v2	61	CO Series	0
Winterson Street	Routing			Sarbol
(1. System and status 	tata ante diporte cola ante			
E Autoritaican	(IP)			
🖶 maitas	+ 3			
26 Network				3,2415
(builting)	🗋 алалын таларын тананы т	August - Andrease Mar	- HUGH HUGH WHY	a makerol.
naurenem	□ P(C304	E 124	E 12245	

The fields displayed on the page are as follows:

Field	Description
Interface	It displays the interface on which the RIP is configured.
Direction	It displays in which direction the RIP packets need to be exchanged.
Version	It displays the RIP version supported by the routing devices in the selected interface.
Authentication	It displays whether the authentication is enabled or disabled for RIP-2M.
MD5 key ID	Enter the unique MD5 key ID.
MD5 Auth key	Enter the authentication key for this MD5 key.
Enable	You can enable or disable the configured RIP.

Click Add(+ button) to add a new entry to the list. This opens the Add RIP configuration page. To delete multiple entries, select the corresponding checkboxes present in the first column of the table, and click **Delete Icon**.

± 3	8		T INA TOK LITTLY HI				0500.2-
	nterfaile	meetine	weeklast op 12	unit, 11 - Mitth Aug et	6	HUR MORE LOD	
	Per cout	000	RE20 +	229	10	129m	
2	selen +	0.01	886 + I				C1 ==

The fields available on the Add RIP configuration page are as follows:

Field	Description
Interface	Select the interface where you want to configure the RIP.
Direction	The RIP direction will define how this gateway sends and receives RIP packets. Select one of the following options:
	 Both: The gateway both broadcasts its routing table and also processes RIP information received from other routers. This is the recommended setting to utilize RIP capabilities fully. In Only: The gateway accepts RIP information from other routers but does not broadcast its routing table.
Version	 The RIP version is dependent on the RIP support of other routing devices in the LAN. RIP-1: A class-based routing version that does not include subnet information. This is the most commonly supported version. RIP-2M: It includes all the functionality of RIPv1, plus it supports subnet information. RIP-2M sends data to multicast addresses.
Authentication	Select Enable to activate the authentication for RIP-2M. By default, RIP authentication is disabled.
MD5 Key ID	Enter the unique MD5 key ID.
MD5 Authentication Key	Enter the authentication key for this MD5 key.
Enable	Click checkbox to enable/Disable your settings.
Cancel	Click cancel to revert to your previous settings.
Apply	Click on Apply to save the settings.

OSPFV2:

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

Ū.	0										Q Serence 1		
	unitare u	tonia =	Printing 1	vietta ortaciónt		Crimit: Outpress()	ų,	Cast 1	Automatication	1 AnH minta	resident.	Readable (1	
0	Port through 3.	2	1	10		42		300	90001H		10	10	
	Port group 2	1.	4	10		40		38	M000011H		000	0	
	Port protect	2.	11	10		44-		10	GOODT H	÷	001	101	
U.	Port group 3	3	18	14		44		16	NONDTH	the second se	dist.	A.L.	
	WANG .		9	10 10		-40		άp.	MOAUTH	•			
										NGIO Rens UI	TI	825	

The fields displayed on the OSPFV2 Configuration table are as follows:

Field	Description
Interface	It displays the physical network interface on which OSPFv2 is enabled or disabled.
Area	It displays the area to which the interface belongs.
Priority	It displays the priority of the router to become the designated router.
Hello interval	It displays the number of seconds that the hello packet is sent.
Dead interval	It displays the time (number of seconds) that a device's hello packets must not have seen before its neighbors declare the OSPF router down.

Cost	It displays the cost of sending a packet on an OSPFv2 interface.	
Authentication	It displays the authentication type.	
LAN route exchange It displays the LAN Route Exchange status for a WAN interface.		
NSSA	It displays whether NSSA is enabled or disabled.	
Enable	You can enable or disable the respective interface.	

Click Edit to open the Edit OSPFv2 page.

D-Link	0.55-253+7			a mar	9
	Edit OSPPV2	D.			Carole Anton
(5) System and station (
E. Averaboolite	No. 401.1.1	9031			
2 Administer	-				
M. Britten	Children (Children)				
se Network	market mark	10	8. j		
score)	105-111				
Revelation (to otherwyst) (B) (
THEOREM	200	18	(E)		
i in and					
o Security	inches barris	e tat	1		
	55546(-0	- 10.			
2 WH	NO at the part when		1		
	100	80			

Field	Description
Interface	It displays the physical network interface on which OSPFv2 is enabled or disabled.
NSSA	Enable this option to allow OSPF stub areas to carry external routes.
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 should have a similar mask.
Priority	It helps to determine the OSPFv2 designated gateway for a network. The gateway 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 priority.
Hello interval	Enter the number, in seconds, when the Hello packet is to be sent. This value must be the same for all gateways attached to a common network. The default value is 10 seconds.
Dead interval	Enter the number of seconds when a device's hello packets are not 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 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	 Select one of the following authentication types: None: The interface does not authenticate OSPF packets. Simple: OSPF packets are authenticated using simple text keys. MD5: The interface authenticates OSPF packets with MD5 authentication.
Authentication Key	Enter the authentication key. This field is available when you select Simple as the <i>Authentica tion Type</i> .
MD5 Key ID	If you select MD5 as the Authentication Type, enter the MD5 key ID.

MD5 Authentication Key	If you select MD5 as the <i>Authentication Type</i> , enter the MD5 authentication key.
LAN route exchange	It displays the LAN Route Exchange status for a WAN interface.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

IGMP

IGMP Proxy:

The Internet Group Management Protocol (IGMP) is used by hosts and routers on an IP network to create multicast group memberships. The IGMP can be used for web and support applications like the online streaming of videos and games. The IGMP proxy enables the gateway to issue IGMP messages on behalf of the clients behind it. If the IGMP proxy feature is enabled, select the WAN interface on which it is to be applied.

Dillak	444 Zmc		£.
Therest subtant	Reuting	Tanal Anton	
A Contraction			
()	No.		
C behalt			
Transa a			
To Desid			
(internet			
1.00			

IGMP snooping

IGMP snooping allows the gateway to 'listen' in on IGMP network traffic through the gateway. This allows the gateway 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.

tining				Cannet	Arth
	KA#				
all gives	5				
all group					
	tanani Ny filon	12 16 4 4 10	a financia		

Field	Description
Name	It tells about vlan name
VLAN ID	It tells about vlan id
Enable	We can enable and disable by checking and unchecking the option

Bandwidth Management

The bandwidth management feature allows you to regulate the traffic flow from the LAN to WAN. 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.

This section will help you understand and configure the bandwidth control feature from the web user interface and add a profile that defines the control parameters. You can then associate the profile with a traffic selector to apply the bandwidth profile to the traffic, matching the selectors. Selectors are elements like IP addresses or services that would trigger the configured bandwidth regulation.

The bandwidth management section covers the following topics:

- Bandwidth management
- Session Limiting

Add Bandwidth management

Bandwidth management is a service-based rule to which the user can attach traffic management profiles. Once a profile has been created, it can then be associated with traffic flow from the LAN to WAN. bandwidth management selector configuration binds a bandwidth profile to a type or source of LAN traffic with the following settings.

D-Link	TWO DWWN			Q	0
	Bandwalth management				100 146
The Address from the		n na mai kata ak			
	The American Statement Statement	Contract Marine	The Sector	 Telle (More)	1 2 44- E
and the second	. – 6			1989	
.194.14					
Verbada Interaction					
- Hereit					
年 (44)					

The fields displayed in the bandwidth management table are as follows:

Field	Description
Name	It displays the name of your profile.
Policy type	It displays the policy type (Inbound or Outbound).
Interface	It displays the interface with which the profile is associated.
Bandwidth Rate Priority/session	It displays the range of bandwidth rates or priority i.e low or high
Service	It displays the service.
Traffic selector match type	It displays the traffic selector match type.
Enable	You can enable or disable the respective bandwidth management policy.

Click Add icon to add a new entry to the table. This opens the Add bandwidth management . To delete more than one entry, select the checkbox of the traffic management policies you want to delete, and click Delete.

Count

-	1609,221	
avolanajolas (Dime:	33
lene -	(iii)	33
(%)(%)(§)(8)	•	
(MICLER) AND	NM ::	
Taultia substant		
	152	3
1.01.07400000000	0102708	23

Add handwitth management.

57 (PE)	201.001.001	
Smithing	\$10.200.2007	
Adventury on the	diamont	

The fields available on the Add bandwidth management page are as follows:

Field	Description	
Name	Enter a name for your profile. This identifier is used to associate the configured profile to the traffic selector.	
Policy typeSelect the policy type (Inbound or Outbound).		
WAN Interface Select which of the available WAN interfaces you want to associate this profile with field appears when Outbound is selected as the <i>Policy type</i> .		
Interface	Select which of the available interfaces you want to associate this profile with. This field appears when Inbound is selected as the <i>Policy type</i> .	
Management type	Select either Priority or Rate .	
Priority	If you select Priority , specify the priority. It could be <i>Low</i> , <i>Medium</i> , or <i>High</i> .	
Max. bandwidth rate (Kbps)	If you select Rate, enter the maximum bandwidth rate.	
Min. bandwidth rate (Kbps)	If you select Rate, enter the minimum bandwidth rate.	
	Traffic selector	
Service Select a service from the drop-down list.		
Traffic selector match type	 This field is available when you select Outbound as the <i>Policy type</i>. Select any one of the following match types: IP address: Select this option to associate this traffic selector with an IP Address of a LAN device. Once selected, enter the IP address of the LAN device. MAC address: Select this option to associate this traffic selector with a specific MAC address on the LAN. Once selected, enter a valid MAC Address. Interface: If this option is selected, select the interface. 	
Interface	If you select Interface, select an interface from the drop-down list.	
IP address	Enter the IP address of the source associated with this profile.	
Subnet mask	Enter the subnet mask.	
MAC address	If you select MAC address , enter the MAC address of the source associated with this profile.	
Schedule policy	It allows you to define the time and day when the traffic shaping rule is to be applied.	
Apply	Click apply to save your settings.	
Cancel	Click cancel to revert to the previous settings.	

Session Limiting

The Session Limiting section displays a list of configured session limiting profiles. It allows a user to limit the number of sessions per IP address, range of IP addresses, or interface through the device. When the session limit is reached, a warning message is displayed to users for a session initiated from a web browser. Session Limiting configuration consists of profile name, source type, schedule, and maximum sessions.

Dink	104.46 (C. 194)		(second second	0
The second second	Bandwath managariem			Tana Caral
Transfer and the t				
A Alexander	+ * 0			
the defensation	The second second second second	- management in the state	 a recipient	
W rerus	2		Test and	. I. Miller.

Date 4

Acet



The fields displayed in the Session Limiting table are as follows:

Field	Description	
Name	It displays the name of the profile configured for a particular source type.	
Maximum sessions	It displays the maximum number of sessions allowed on the selected source type to limit sessions.	
Traffic Selector	It tells about traffic selector type	
Enable	You can enable or disable the policy	

Click Add icon to add a new entry to the list. This opens the Add Bandwidth management To delete more than one entry, select the check-boxes of the entries you want to delete, and click Delete icon.

	Correction -	
bene - i er	Amount Colora	24
Usama Bassa	100	
Twilling probability		
Talla princie		
011101010000	(# 9800)	τ.)
* 30 <i>1</i> ==	102106-00.01	
Q 2022 - 2040	deserve -	20

The fields available on the Add bandwidth management page are as follows:

Field	Description		
NameEnter the name of the profile to be configured for a particular Source type.			
Management Type Session limiting			
Maximum sessions	Enter the maximum number of sessions allowed on the source type to limit sessions.		
	Traffic selector		
Service	Select a service from the drop-down list.		
Traffic selector match type	 This field is available when you select session limiting as the <i>management type</i>. Select any one of the following match types: IP address: Select this option to associate this traffic selector with an IP Address of a LAN device. Once selected, enter the IP address of the LAN device. Interface: If this option is selected, select the interface. IP range: If this option is selected, enter the range of Ip addresses 		
Interface	If you select Interface, select an interface from the drop-down list.		
IP address	Enter the IP address of the source associated with this profile.		
Subnet mask	Enter the subnet mask.		

Starting IP address If you select IP range then enter the staring IP address	
Ending IP address	If you select IP range then enter the ending IP address
Schedule policy It allows you to define the time and day when the traffic shaping rule is to be applied.	
Apply Click apply to save your settings.	
Cancel	Click cancel to revert to the previous settings.

Chapter 6 Firewall

This chapter introduces you to the security features supported by the router. These features include Firewall and IPS/IDS. These are the various techniques used to block any malicious attacks from the Internet to access your network. You can also configure your own Internet policies to allow only selected web-based information.

This chapter covers the following topics:

- Firewall settings
 - Attack check
 - Application layer gateways
 - UPnP
- · Firewall policy
 - IPv4 Firewall Rules
 - Port Forwarding
 - Port Triggering

Firewall Settings

In firewall setting you can configure IPS/IDS to prevents malicious attacks from the Internet from accessing the private network and ALGs that enhance the firewall and NAT support of the Router.

General

The router's Intrusion Prevention System (IPS) prevents malicious attacks from the Internet from accessing the private network. Static attack signatures loaded to the router allow common attacks to be detected and prevented. In addition, you can enable checks between the WAN and DMZ or LAN.

D-Link	DOR-GOOLG		Or Journation	C
	Firewall setting		.12	
A spectrum was	221231010-1124			
25 7.0 m ik 414		Agriculture (press) - 1917		
17 Automation of	le trais a ciele deser parame d	ada)		
A increa	11-14-2 20-4 U.S.			
<	httm://windo/	ιζί.		
W Dave	Sector of the sector	51)		
I wait a big	PL Discission and the second			
- tapen	Lines (C.) primes	iii		
W setteres Ξ /mm		0		
	W.S. oken			
	NUTBER STREET, NO COOL	<u> </u>		

The fields available on this page are as follows:

Field	Description	
Intrusion detection/prevention		
Intrusion detection	Enable or disable intrusion detection.	

Intrusion prevention Enable or disable intrusion prevention.		
IPS/IDS checks active between		
LAN and WAN	Enable it to detect intrusions between LAN and WAN interfaces.	
DMZ and WAN	Enable it to detect intrusions between DMZ and WAN interfaces.	
IPS status		
Number of signatures loaded	It displays the number of signatures loaded.	

Attack Check

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

Additionally, you can block certain Denial-of-Service (DoS) attacks. These attacks, if uninhibited, can use up processing power and bandwidth and can prevent normal regular network services. You can also configure ICMP packet flooding, SYN traffic flooding, and Echo storm thresholds to suspect traffic from the offending source temporarily.



The fields available on this page are as follows:

Field	Description	
WAN security checks		
Stealth mode		

	If this option is enabled, the gateway will not respond to port scans from the WAN. This makes it less susceptible to discovery and attacks.		
Block TCP flood	If this option is enabled, the gateway drops all invalid TCP packets and gets protected from the TCP flood attack.		
Allow ICMP traffic	If this option is enabled, the WAN host can ping traffic to the WAN interface.		
TCP filter check			
Filter check mode	If this option is enabled, the gateway drops invalid TCP packets (FIN, RST, and ACK) going with SNAT while the connection is closed. Some of the other packets, like TCP OUT-OF-WINDOW, are also considered to be invalid. Disable this option while taking performance, as enabling this option will affect the throughput.		
	LAN security checks		
Block UDP flood	If this option is enabled, the gateway will not accept more than the configured value in <i>Accept UDP connections</i> , indicating simultaneous, active UDP connections from a single computer on the LAN.		
Accept UDP connections	Enter the number of UDP connections simultaneously accepted by the gateway from a single computer on the LAN. You can select any number between 25 to 500. This field is available when you enable <i>Block UDP flood</i> .		
	DoS Attacks		
SYN flood detect rate	Enter the rate at which the SYN flood can be detected.		
Echo storm	Enter the number of ping packets per second at which the gateway detects an Echo storm attack from the WAN and prevents further ping traffic from that external address.		
ICMP flood	Enter the number of ICMP packets per second at which the gateway detects an ICMP flood attack from the WAN and prevents further ICMP traffic from that external address.		

Application Layer Gateways

Application Level Gateways (ALGs) are security components that enhance the firewall and NAT support of the Router to seamlessly support application layer protocols. In some cases enabling the ALG will allow the firewall to use dynamic, ephemeral TCP/ UDP ports to communicate with the known ports a particular client application (such as H.323 or RTSP) requires; otherwise, the admin would have to open a large number of ports to accomplish the same support. ALG understands the protocol used by the specific application that it supports. It is a very secure and efficient way of introducing client applications through the gateway's firewall.

D-Link	Mar Pare 7 BERLINES	an adia aon	(C. 19+4	ø
· Antonio contenente	Frewall setting		Gravel	- 5552
1 Syneriteritoria 11 Accession	11-10-10-10-10-	Antication from potential		
D Harrison	8787	i ci		
ll, fanchen V Robert	10°.	ü		
. Frend	16444	0		
From Starfings	1977			
A State of the second s		0 5		
(VPN)	itt - almap	8		
	Canviel Heroley			

Field	Description
RTSP	Enable it to allow applications that use Real Time Streaming Protocol to receive streaming media from the Internet. QuickTime and Real Player are some of the common applications using this protocol.
SIP	Enable it to allow devices and applications using VoIP (Voice over IP) to communicate across NAT.
-------------------	---
H.323	Enable it to allow H.323 (specifically Microsoft Netmeeting) clients to communicate across NAT.
TFTP	Enable it to allow Trivial FTP (TFTP) clients and servers to transfer data across NAT.
SMTP	Enable it to transfer email between mail servers over the Internet and enter the port at which the SMTP packets are inspected.
IPSec Passthrough	Enable this feature to allow encrypted VPN traffic for IPSec VPN tunnel connections through the device.
L2TP Passthrough	Enable this feature to allow encrypted VPN traffic for L2TP VPN tunnel connections through the device.
PPTP Passthrough	Enable this feature to allow encrypted VPN traffic for PPTP VPN tunnel connections through the device.

E-mail filter list

The *E-mail filter list* appears only when the SMTP is enabled. Simple Mail Transfer Protocol (SMTP) is a text-based protocol used for transferring emails between mail servers over the Internet. Typically, the local SMTP server is located on a DMZ so that mail sent by remote SMTP servers traverses the router to reach the local server. Local users then use email client software to retrieve their email from the local SMTP server. SMTP is also used when clients send emails. In addition, SMTP ALG can monitor SMTP traffic originating from both clients and servers.

Firewall setting			Escol.	OODY .
Server years				
ms=	ίΞ.			
Santo	0			
40429				
TTTE	11			
SAPTP PB-1				
Phi				
+ 10 - 1. inc. icc 3	6481 Aprile 12801			
P.1 (1998)	the data (second)	2 and determine		
NATE	· 1	deal for which we		1.1

The table lists all the subjects along with email addresses that are blocked or allowed.

Field	Description
Policy	It displays the policy to allow or block the email address.
Subject	It displays the subject.
Email address	It displays the email address.

Click Add icon to open a row to Add Email filter to add a new entry. To delete multiple entries at once, select the checkboxes of the entries you want to delete, and click Delete icon.

SALAR INCOME.

9/73	-
Ret	10
$\pm \pi$	2 meye tarest terrikit Apoly Salton
- C - P	1.00

Ξ.	0.1875	5 6 1	and providing.	
190	402808	 [immass] 		

The fields available on the *Add Email filter* page are as follows:

Field	Description
Policy	Select a policy. It can be either Allow or Block .
Subject	Enter the subject. The range is from 1 to 64 characters.
Email address	Enter an email address.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

UPnP

Universal Plug and Play (UPnP) is a feature that allows the router to find the devices on the network that can communicate with the router and allow for auto-configuration. If UPnP detects a network device, the router can open internal or external ports for the traffic protocol required by that network device. If the UPnP feature is disabled, the gateway can not configure an automatic device, and you may have to manually open /forward ports to allow applications to work.

Select Enable to configure UPnP and display the UPnP port mapping list.

Frewall settin	9				Garcel Appy
3000 (need the state	1.00 (1000) - 100			
0.00	8				
Average and prove			er eft.		
An optimized in the Ar	0.0	10	P1		
UPoP port mapping)	004				
					2.047
(trobusts	Politika -	1.004.00	Paravised goals	the second second	P. Calendari
200	10	0008	0059		192.100.001
				(stold) as	0 <u>16 E</u>

The UPnP port mapping list has the details of UPnP devices that respond to the gateway's advertisements. The following information is displayed for each detected device:

Field	Description			
UPnP	You can enable or disable the UPnP feature.			
Advertisement period	Enter a value for the Advertisement period. This is the frequency that the router broadcasts UPnP information over the network. A large value will minimize the network traffic but cause delays in identifying new UPnP devices to the network. Enter a value for Advertisement time to live. This is the number of hops 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 numbers of switches.			
Advertisement time to live				
	UPnP port mapping list			
Active	It indicates if the UPnP port is still open in the device or not.			

Protocol	It displays the network protocol used by the gateway.
Internal port	It displays the internal ports opened by UPnP (if any).
External port	It displays the external ports opened by UPnP (if any).
Interface	It refers to the LAN/VLAN segment on which the UPnP option is enabled.
IP address	It displays the IP address of the UPnP device detected by the gateway.

Firewall Policy

The *Firewall* section of the Security deals with the various methods adopted by router to ensure a safe and secure network. In this section, you will learn about the Firewall rules configuration on the IPv4 networks. These are the rules defined to keep a check on the incoming and outgoing traffic of the network. You can state which traffic is to be allowed or blocked. Similarly, the Port Forwarding method can restrict access to traffic entering your network while allowing only specific outside users to access specific local resources. When you have multiple public IP addresses and multiple servers across the firewall, the 1:1 NAT method is used.

This section covers the following topics:

- IPv4 Firewall Rules
- Port Forwarding
- Port Triggering

IP Rule

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 allows access from the secure zone (LAN) to either the public DMZ or insecure WAN. On the other hand, the default outbound rule is to deny access from DMZ to insecure WAN. In addition, you can restrict VLAN to VLAN or LAN to VLAN traffic using IPv4 Firewall rules.

D-Link	And Ann									L. year			15
energiant.		out potes	Č.								i.	• 10	
37571.000	1	-	and Room										
n de la constante de la consta	\mathbf{t}_{2}	1.0											
Cherry .	1.	and the second		Contraction of the	1	Charles and service	10-10-00-00-00-00-00-00-00-00-00-00-00-0		1.000	1. 1. 1. 1 . 1	1.11	1000	
R. Carriel		.84	The second	M ²	-114	and a	in ittain	-	(BAP)				
Hered and a													
Totale:													
a													

The fields displayed in the IPv4 Firewall Rules table are as follows:

Field	Description
Priority	It specifies the priority of the configured rule.
Name	It specifies the name of the firewall rule
Source Interface	It specifies the source interface
Destination interface	It specifies the destination interface
Service	It displays the service for which the firewall rule is defined.
Source	It displays the source IP address range, a specific IP address, or Any for all IP addresses on which the firewall rule is applied.
Destination	It displays the destination IP address range, a specific IP address, or Any for all IP addresses on which the firewall rule is applied.
Schedule	It displays the schedule when the firewall rule is applied.

Enable	You can enable or disable the respective IPv4 firewall rule, except for the Default rule.
Actions	You can edit or delete the configured firewall rule except for the <i>Default rule</i> . It displays the policy applied to the particular firewall rule. It is either Deny or Permit .
Logs	You can enable or disable the logs for respective IPv4 firewall rule.

To delete multiple entries at once, select the checkboxes of the IPv4 firewall rules you want to delete, and click **Delete icon**. Click **Add icon** to add a new entry to the list. This opens the *Add IPv4 firewall rules* page.

Catter.

- 4001

Add Phile 111.04 0.044 . New Constant. in the second Search traches : 1000 intra tel portes 0 Per-Sniph. The Amazon Sciences 1010-0102 Distance: O. а, it we $\pi \pi$ 40. 12 Institution (ed.) 1000 Ð. (interaction party) 4 See. tion. Stene ÷ Westin. 144 1990 2

The fields displayed on this page are as follows:

Field	Description
Priority	Define the priority of the IPv4 firewall rule. The smaller the number, the higher the priority.
Name	Define the name of the IPv4 firewall rule
Source interface	Select the source interface from the drop down.
Destination interface	Select the Destination interface from the drop down.
Action	Select either Block or Allow .
Service	Select the protocol/service on which you want to configure the firewall rule. The options are all, TCP, UDP, TCP/UDP, ping, HTTP, HTTPs, FTP, SSH,etc.,
Source	Enter a specific IP address, a range of IP addresses, or any IP addresses from where the traffic is sent.
Source port	Specify a source port or multiple source ports where the traffic generates. This field appears only when you select TCP, UDP, or TCP/UDP protocols.
Destination	Enter a specific IP address, a range of IP addresses, or any IP addresses where the traffic is sent.
Destination port	Specify a destination port or multiple destination ports that will receive the traffic for this firewall rule. This field appears only when you select TCP, UDP, or TCP/UDP protocol.
Logs	Select Always to capture the logs and Never option to disable logs.
Schedule	Select a schedule from the drop-down list. You can define the time and day when the IPv4 firewall rule is to be applied.
Apply	Click Apply to save your settings.

Port Forwarding

Port forwarding is a process to restrict access to traffic entering your network, selectively allowing only specific outside users to access specific local resources. By default, all access from the WAN side is blocked from accessing the secure LAN, except in response to the LAN or DMZ requests. To allow outside devices to access services on the secure LAN, you must create a port forwarding rule for each service. It also supports Translation (Outbound).

D-Link	2.85 (58.7								
	Fairwall polities							1	
enter anticent	na Aranaka	Farmers							
	= 0								
helen bi	1 mm	140	- magnegic	-	Sub-red 🖷		The second s	And the second second	
	12 ···· +	Several and the second		1. 114	1.11		Concerne a	100 Mar.	-
		internet and the second s	100	1.000	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	1.0	100 (00 h h	64	
		والملكان والالالة فشيعاش كال		Contraction of the second	100000	Sec.	Carlos and	100 (C. R. 1997) (R. 1	

The fields displayed in the Port forwarding table are as follows:

Field	Description
Active	You can enable or disable the respective rule.
Allowed remote IPs	It displays the IP addresses that can accept to and from traffic.
Interface	It displays the interface on which the rule is configured.
Forward internal IP	It displays the LAN host IP address.
Local port	It displays the LAN host port numbers.
Mode	It displays the mode configured for the selected rule.
Name	It displays the name of the rule.
Protocol	It displays the protocol followed for the configured rule.
Public port	It displays the public port number.

Click Add icon to add a new entry. This opens the Add port forwarding page. To delete multiple entries, select the checkboxes that you want to delete, and click Delete icon.

		1.00	+47)	(endine)					
	-	a second		(and a			and the second		1
	International survey	107	94	545	• [(M		38114(10)	100.004.4-00	5
- 1	bermatarian da i	10	1.41	i inter	1.00	1.48	Carrowin	144	5
1.54	tradicitients -	198	$\langle \phi \rangle$	1.000	• me	1.04	22203.355	10.000 0 0.000	-
	-market download	64	4	998			Litter and		12

The fields available on the Add port forwarding page are as follows:

Field	Description

Name	Enter the name for your rule.
Mode	 Select any one of the following modes: Forwarding (Inbound): If you select this mode, traffic passes from the WAN host to the LAN host for a public destination port. Translation (Outbound): It translates the traffic from a local source port number to the configured public source port number for the LAN host to the WAN host traffic. Translation (Inbound): If you select this mode, traffic passes from the WAN host to the LAN host and translates to the destination local port when the traffic is sent on the public destination port. Note: Translation (Inbound) and Translation (Outbound) options are available only when the route mode is configured as NAT on the port configuration WAN mode page
Interface	Select the interface on which this rule will be applied.
Protocol	Select one of the following protocols: TCP, UDP, or TCP/UDP.
Public port	Enter the port number on which the applications are running on the WAN host.
Forward internal IP	Enter the LAN host IP address. For Translation (Outbound), it refers to the IP address from where the traffic will be originating. For Translation (Inbound) or Forwarding (Inbound), it refers to the IP address to which the traffic will be sent.
Local port	 Local port refers to the LAN host port numbers. For outbound, it means local source port, and for inbound, it means the destination local port for the LAN host. This field is available only when you select Translation (Outbound) or Translation (Inbound) mode. <i>Note:</i> Mapping a range of public ports to a range of local ports, the ranges must be the same length.
Allowed remote IPs	Enter the allowed remote IPs. Allowed remote IPs are the IPs that accept to (for Translation Outbound) and from traffic (for Translation Inbound and Forwarding Inbound).
Apply	Click apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Port Triggering

Port triggering allows devices on the LAN or DMZ to request one or more ports to be forwarded to them. This feature waits for an outbound request from the LAN or DMZ on one of the defined outgoing ports and then opens an incoming port for that type of traffic. This can be a form of dynamic port forwarding while an application transmits data over the opened outgoing or incoming port(s).

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

Note: This section is available only when you configure the route mode as NAT on the Port configuration -- WAN Mode page.

D-Link	manifast	(1 ····) (0
(and the second second	Preswall policy	Laws .
A spectralities	and a second	
Concession in the local division of the loca	+ =	
in the second second	11 mm mmm mmm mmm mmm mmm mmm mmm mmm m	0
Treast room	12 (ard) (24 +) (24	
() manual and		
100-000		
1000		

The fields displayed in the *Port Triggering* table are as follows:

Field	Description

Name	It displays the name of the port-triggering rule.
Protocol	It displays the protocol on which the rule is being configured. It is TCP, UDP, or TCP/UDP.
Outgoing trigger port	It displays the start and end trigger port range.
Incoming trigger port	It displays a port range that is open to receive the traffic.
Enable	You can enable or disable the port-triggering rule.
Interface	It displays the interface name

Click Add icon to add a new entry. This opens the Add port triggering page. To delete multiple entries, select the checkboxes you want to delete, and click Delete icon.

Free	sall policy							Contraction and and and and and and and and and an	16.4
1	- Internet Permission	-							
÷	ŝ.	. 1		Carrier C.					
	TEX	1000		19190			Second and the second second second	-	
	(men 1	Tor	- #£	1011	- 86	See.	H H		
8	1	1.44	12	No.	-2b	() Circ	100	1.1	
							Marginane de-	11月2日	-12.

The fields available on this page are as follows:

Field	Description
Name	Enter the name of the port-triggering rule.
Protocol	Select the protocol on which the rule is to be configured. It is TCP, UDP, or TCP/UDP.
Outgoing trigger port	Enter the start and end trigger port range.
Incoming trigger port	Enter the port range that is open to receive the traffic.
Interface	Select the WAN interface.
Enable	Select radio option to enable or disable the port-triggering rule.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Chapter 7 Security

This chapter introduces you to the security features supported by the DSR-250v2. These features include Web content filtering and Application control. These are the features used to Block/Allow only selected web-based applications.

This chapter covers the following topics:

Web content Filtering.

Application control.

Web Content Filter

The gateway offers standard web filtering options to filter out the web page displayed by the domain names. It allows you to create Internet access policies between LAN and WAN. Instead of creating policies based on the type of traffic (as is the case when using firewall rules), web-based content itself can be used to determine if the traffic is allowed or dropped.

D-Link	1219-012-2				O hann	\odot
	Web content filter	ŝ			2.94 CB	
 Antimistation 	Web contains little ratios					
2 Calmandar	- × 0					
2. Series	13.	and a	1000	11-10-100 ap	1 million	

S. April 1	<u>(1)</u> mt	 ((the factor)	RECO DEGREE	5
				Baller III TE IVE
- n-e	Caston group the			
Act restors if the	- 10			

The fields displayed in the *Web content filter list* are as follows:

Field	Description
Name	It displays the name of the policy.
Action	It displays the Action rule(Allow/Block).
Schedule	It displays the schedule selected for the policy.
Filtered by	It displays the type of information you want to filter with this policy.
Enable	You can enable or disable the policy.

Click Add(+ button) to add a new entry. This opens the *Add web content filter configuration* page. To delete multiple entries, select the checkboxes of the web content filter you want to delete, and click **Delete icon**.

D-Link	058-250+2		15
	Add new web c	ontent fliter rule	
System and status			
a Administration	Marris	124	
D Authentication	tim manapati scher	NW F	
f, intertice:	Addationarrities	Dide	
- Network	2(0)	Alter +	
(; finiwal)	Scheman.	Kouner .	
Security	Poscy scope	By Nature +	
Web content filter			
Application particul	harsen.	mortuos +	
3 YPH	Instan Lacar	Petgrapit -	
	Capital portai assi	C Elusia 🌰 Dissosc	
	10029	🔿 Shat e 🔹 Dissolo	
	1128	🗇 Deze e 🔹 Dezeke	
	Dputy/40%	O Drafé le Drafélic	
	PSec 191	🗇 İvana 🔹 Diama	
	Princes by	Category .	
		Talogay I Beaking	2.4

The fields available on the Add web content filter configuration page are as follows:

Field	Description
Name	Enter the name of the policy.
Non-managed action	This is an action to be taken for the Non-Managed Site. You can Allow or Block. By default, it is Allow.

Allow override If enabled, it allows the sites categorized under Blocked categories.				
Override timeout (seconds) Enter the time (in seconds) for which all the disallowed categories will be allowed.				
Update on access Enable the field to restart the override timer on each new access to disallowed categories				
Policy rule setup				
Policy Select the policy rule. The options are <i>Allow</i> and <i>Block</i> .				
Schedule	Select the schedule when the policy rule is to be applied. To configure a schedule, refer to the Schedule policies page			

	Policy scope setup					
Policy scope	Select either <i>Global</i> or <i>By Feature</i> as the policy scope. The global policy affects all types of traffic matching the selected application(s). If you select <i>By Feature</i> , the following additional fields will be available.					
Network	Select one of the configured network profiles. You can select None, Single, Range, or Interface.					
IP address If you select a Single as the <i>Network</i> , enter the IP address.						
Starting IP address	If you select Range as the <i>Network</i> , enter the starting IP address of the IP range.					
Ending IP address	If you select Range as the <i>Network</i> , enter the ending IP address of the IP range.					
Interface	If you select Interface as the Network, select the configured interface from the drop-down list.					
Captive portal user	Enable or disable the <i>Captive Portal user</i> option. Enabling this option allows all Captive Portal clients to follow this policy.					
РРТР	Enable or disable the PPTP VPN. Enabling this option allows PPTP traffic to follow this policy.					
L2TP	Enable or disable the L2TP VPN. Enabling this option allows L2TP traffic to follow this policy.					
OpenVPN	Enable or disable the OpenVPN. Enabling this option allows OpenVPN traffic to follow this policy.					
IPSec VPN	Enable or disable the IPSec VPN. Enabling this option allows IPSec traffic to follow this policy.					
	Content filtering					
Filtering type	 This field allows you to select the type of information you want to filter. Select any one of the following options: Default category: Select the default categories that you want to filter. URL: The URL filtering section is available on the next page. Click the Next button located in the lower right corner of the page to add URLs or keywords. Default category+URL: Select a default category from the drop-down list, and add URLs/keywords in the URL filtering section available on the next page. Custom group: Select one of the configured custom groups or create a new group. 					
URL filtering	To add a URL (HTTP or HTTPS), domain name, or a keyword, select Add URL/keyword . Click +Add to add more than one entry. If you want to add URLs or keywords at once, select Bulk import . Click Browse and select the file (in CS ¹ format) whose information you want to import into the database. You can download the sample template file here. <i>Note that the number of entries is limited to a maximum of 512 URLs</i> .					
Default category	This field is available when you select the <i>Default category</i> or <i>Default category+URL</i> as the filtering type. Select the type of categories to be filtered from the drop-down list.					
Custom group	Select any one of the configured custom groups from the drop-down list. To create a new group, click Adc custom group. This opens the Add group configuration page. For details, refer to Custom Group List					
Apply	Click Apply to save your settings.					

, pp.)	chok rippij to dave year betange.
Cancel	Click Cancel to revert to the previous settings.

Custom Group list

Users can select a particular URL or select a group to manage URLs associated with that group. This section displays groups and URLs associated with them.

ustom group list			
+00			C heat h
U Hame U Hame Mar	0.900.0	Citegery Officing	dest based
5. 14		Service Sheet	1.7
		Advortising	
			10001.03 Norms 1.62.

The fields displayed in the Custom Group List table are as follows:

Field	Description
Name	It displays the name of the group.
URLs	It displays the list of selected URLs.
Category filtering	It displays the category to which these URLs belong.
In use	It displays if that custom group is in use or not.

Click Add(+ button) to add a new group. This opens the Add group configuration page. You can edit by use edit icon or delete the group list using delete icon.

Add new group	configuration			Cancel	Appy
Group norme	10/				
Duitoin Shalling type	1191,#legwood	- 1			
	unukeyeard 🌒 ityet e	ining 🔿	roger		
	Proprioriu	www.th	cabdok.com		
Add new group ^b	configuration			Cancel	Aboy
logiane	Mad .				
anten Skalan tya	Category tasked	2			
Talopony builed bitating	Supplied lates		Selected Items		
	tevicit		hereb		
	TT Nation	l m	[]]. Russnerz		
	[] Advertiging		C Available Stat.		
	Bismess Orientes	10041			
	Computers & Redenstry Search area				
	www-tiral Stec				
	Cenpumpπ				
	E second g				
	Total 12 tarm		Selector: I terra		

The fields available on this page are as follows:

Field	Description
Group name	Enter a name for your group.
Custom filtering type	 Select one of the following types of filtering you want to apply to your group: URL: If you select this option, the URL Filtering section will be available. Category-based: If you select this option, the Category-based filtering section will be available. URL+Category-based: If you select this option, both the above sections will be available. Click the Next button located at the lower-right corner of the page to go to the Category-based filtering section.
Add URL/keyword	Select this option to add a new URL. Enter the URL in the box; 1 to 64 characters are allowed.
Bulk import	To import URLs in bulk, select "Bulk import." Next, click Browse to locate the file on your system, and then import the file in *.csv format. You can download the sample template file here. Note that the number of entries is limited to a maximum of 512 URLs.
Supported items	Select one or more checkboxes of the categories that you want to filter. Then, click the ">>" button to move it to the box of the selected item. This is available when you select either "Cat egory-based" or "URL+Category-based" filtering type.
Selected items	This box displays the items selected from the supported items list. To remove the item from the selected list, click the "<<" button. This is available when you select either " Category-based " or " URL+Category-based " filtering type.
Next	Click Next to go to the <i>Category-based filtering</i> section. This button is available only when you select URL+ Category-based filtering type.
Previous	Click Previous to go back to the <i>URL filtering</i> section. This button is available only when you select URL+ Category-based filtering type.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Application Control

Application Control is a feature that allows network administrators to allow, block, or control the traffic of applications that is transacting the traffic. It allows you to block or allow any specific applications, like Netflix, YouTube, Facebook, Twitter, etc.

This section covers the following topics:

- Auto Upgrade
- Application Control List
- Custom Group List for Application Control

Auto Upgrade

This section provides the current package version running on the device. You can enable or disable the *Auto upgrade* feature. The auto-upgrade feature allows the user to define a time interval or a schedule for the device to auto-check for the updated packages on the server.

Dilink	10.00 100 vi.		6 Aug	- 49
(and a second	Application control			
	Light trees at participa			
T American	1000-2711	100		
-		<u>.</u>		
11 1984 -	international West Production	8 3 1944		
g. Looky		er.		

Carl Carl	- Theorem Service	100 A	-*i				
	A set of the control g is $\phi = g^{2} - 11$						
)) (here) Column prosp that	8.10	1 (Filmer)	i teri	5. (m.)	1.449	11
	+ 2 2						
	1 lines			to to the second state	2. 1999		

The fields available in this section are as follows:

Field	Description	
Package version	It provides details about the running package version.	
Auto upgrade	Enable or disable the Auto upgrade option.	
Time	Select either <i>Interval</i> or <i>Schedule</i> to check for updated packages on the server. If you select <i>Interval</i> , enter the number of minutes after which the device will check for the updates. If you select <i>Schedule</i> , choose a Day and Time .	
Reboot Type	Select either manual or auto	

Application Control List

The user can select a particular app or select a group to manage applications associated with that group. This provides an administrator with more options to set up policies to control access to the applications for the selected network users, IP addresses, or network segments.

D-E.inic	the off, c					1. mar. 1	8
Westmanne -	Application control					20	- 1220
Records.	r star gover en en ansaño						
Circle and and a	(weather the second	00					
a interne	Automatics and agree	9					
le tanen	According to the						
The base of the	+22		summer of sets last data				
df 879	1	1.00	a lateration Association	Turk	A Constantion Constant Constant	1.5	
	S. d. Stragering Ball					Seattless	E = +1
	+ 2.3						11
	2 her-		1.0004	in a company of the company	18	Ξ.	



Field	Description	
Name	It displays the name of the policy.	
Policy It displays the rule for the policy.		
Schedule	It displays the schedule for your policy.	
Scope	It displays the scope of the policy, i.e., whether the policy is Global or By feature.	
Application	It displays the application type - Default group, Single APP, or Custom group.	
Enable	You can enable or disable the selected policy.	

Click **Add icon** to add a new policy. This opens the *Add application control policy configuration* page. To delete multiple entries, select the checkboxes of the application control policies you want to delete, and click **Delete icon**.



The fields available on the Add application control policy configuration page are as follows:

Field	Description			
Policy Name	Enter a name to identify the policy.			
Policy rule setup				
Policy	Select the policy rule. It could be either <i>allow</i> or <i>block</i> .			
Schedule	It allows you to set a schedule when you want to apply the policy. To configure a new schedule, refer to the Schedule section.			
	Policy scope setup			
Policy scope	Select either <i>Global</i> or <i>By feature</i> as the policy scope. The global policy affects all types of traffic matching the selected application(s). If the <i>By feature</i> is selected as the Policy type, the following fields will be available.			
Network	 Select any one of the following networks: Single: If you select this option, enter the IP address. IP range: If you select this option, enter the starting IP address and ending IP address. Interface: If you select this option, select the interface from the drop-down list. 			
IP address	Enter the IP address. This field is available when the <i>Network</i> is Single .			
Starting IP address	Enter the starting IP address of the IP range. This field is available when the <i>Network</i> is IP range .			
Ending IP address	Enter the ending IP address of the IP range. This field is available when the <i>Network</i> is IP range .			
Interface	Select the interface from the drop-down list. This field is available when the <i>Network</i> is Interf ace .			
Captive portal user	Enable or disable the Captive Portal option. Enabling this option allows all the Captive Portal clients to follow this policy.			
QoS	Enable or disable the QoS option to select Bandwidth Rate or Priority for the traffic accessing through the selected application.			
Traffic management	Select Rate or Priority for the traffic accessing through the selected application.			
Priority	Specify the priority as Low, Medium, or High.			
Max bandwidth rate (Kbps)	Enter the maximum bandwidth rate.			

Min bandwidth rate (Kbps)	Enter the minimum bandwidth rate.		
РРТР	Enable or disable the PPTP VPN. Enabling this option allows all the PPTP traffic to follow this policy.		
L2TP	Enable or disable the L2TP VPN. Enabling this option allows all the L2TP traffic to follow this policy.		
OpenVPN	Enable or disable the OpenVPN. Enabling this option allows all the OpenVPN traffic to follow this policy.		
IPSec VPN	Enable or disable the IPSec VPN. Enabling this option allows all the IPSec traffic to follow this policy.		
	Application control		
Application type	Select the application type from the drop-down list. The options are Default group, Single application, and Custom group.		
Category	This field is available when you select the option Single application as the <i>Application type</i> . Select the category of application from the drop-down list.		
Application	This field is available when you select the option Single application as the <i>Application Type</i> . Select an application from the drop-down list available for each category.		
Default group	This field is available when you select Default group as the <i>Application type</i> . Select a default group from the drop-down list.		
Custom group	This field is available when you select the Custom group as the <i>Application Type</i> . Select the configured group from the drop-down list. If you want to create a new group, click the Ad d custom group button. It will redirect you to the <i>Add group configuration</i> page.		
Apply	Click apply to save your settings.		
Cancel	Click Cancel to revert to the previous settings.		

Custom Group List for Application Control

This section allows configuring groups and associating applications with them. It displays a list of configured groups along with the application list associated with them.



The fields displayed in the Custom Group List table are as follows:

Field	Description
Name	It displays the name of the group.

Application list	It displays the list of selected applications.
In use	It displays the status of the selected application, i.e., whether the group is in use or not.

Click Add icon to configure a new group. This opens the Add group configuration page. To delete more than one group, select the corresponding checkboxes and click **Delete icon**.

n galaap kand ganadkan ganta (samajawa mineta (samajawa filo ya	New york (Marcola Control of Cont	term Har
illerie (scool Mi)	1	
ninch (Second Wei	1	
	H++1	
17 78 AL 12 84 13 79	E Free	
1 mm	~	
W.HOI	last Boost Dava	
-		
	i der i stre i stre	□ 2-579 □ 1-599 □ 1-5

The fields available on the Add group configuration page are as follows:

Field	Description		
Application list	It includes the following two boxes:		
	 Supported APPs: It lists all the applications supported by the device. Select the checkbox of the corresponding application that you want to add to the group. Click the ">>" button to add the application to the selected apps list. Selected APPs: It lists all the applications to be added to the group. Select the checkbox of the corresponding application that you want to remove from the selected apps list. Click the "<<" button to remove the application from the selected apps list. 		
Group Name	Enter the name of the group. It can be of 1 to 64 characters.		
Apply	Click apply to save your settings.		
Cancel	Click Cancel to revert to the previous settings.		

Chapter 8 VPN

VPN provides a secure communication channel ("tunnel") between two gateway routers or a remote PC client. DSR-250v2 supports the following types of tunnels:

- 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 a responder.
- PPTP server tunnel for PPTP client connections
- L2TP server tunnel for L2TP client connections
- OpenVPN server tunnel for OpenVPN client connections
- GRE tunnel

In this chapter, you will learn how to configure the VPN protocols supported by the DSR-250V2.

- Ipsec Profiles
- Ipsec site to site
- Ipsec client to site
- Ipsec 1 to 1 mapping
- **PPTP**
- L2tp
- Openvpn
- GRE

IPsec Profiles

The Ipsec profile is the central configuration in IPSec that defines most of the IPSec parameters such as the protocol, algorithms, SA lifetime, and key management protocol. In addition, it contains information related to algorithms such as encryption, authentication, and DH group for Phase I and II negotiations. This section lists all the configured ipsec profiles.

D58-250v2		O least.	8
IPsec profiles			
IPsec profiles			
+ 🖉 ili 🗇 mm			
C Atom	 Holl Introducts 		17
 OFF, crufile_de/solt 	82(11)	- The	
		Rollinera in	1 1 1 1 1

The fields displayed on the *lpsec profile* table are as follows:

Field	Description
Name	It displays the name of the configured ipsec profile.
IKE version	It displays the version of IKE that has been used.
In use	It indicates if the configured ipsec profile is being used or not.

Click + to add a new entry to the list. This opens the Add Ipsec profiles page. To delete multiple entries, select the checkboxes of the Ipsec profiles you want to delete, and click **Delete**.

Add new IKE			
Profile name	Arba Shuractera ;		
BCE version	• IKEV1 O IKEV2		
IKE phase-1 settings			
Exchange mode	Main	3 0	
NAT Traversal			
	NAT Keep Alive Frequency	50	[9]
Local Idantifian turus	-		

socal mentiles cype	FOCSI MV/M IN		
Remote identifier type	Remote WAN IP		
DH group	Group 2 (1024 bit)	3	
DH group	Group 2 (1024 bit)	-	
Encryption	3DES X AES-128 X	Ŧ	
Authentication algorithm	SHA-1 x	Ŧ	
SA lifetime	28800	© seconds	
Authentication method	Pre-shared Key	•	
Pre-shared Key		Ø	
Dead peer detection	Z		
	Detection interval	10 0	
	Reconnect after failure	3	
	VPN tunnel backup		
	Backup tunnel	Select Backup policy +	
	Failure time to primary	30 (2)	seconds
Extended authentication	Z		
	Extended authentication type	NONE	

IKE phase-2 settings

Protocol selection

.

Encryption algorithm	3DES X AES-128 X	÷]
Authentication algorithm	SHA-1 X	-]
SA lifetime	3600	$\stackrel{\wedge}{\scriptstyle_{\vee}}$	seconds
Perfect forward secrecy	✓		
DH group	Group 5 (1536 bit)	-)

The fields available on the Add Ipsec profiles are as follows:

Field	Description	
Profile name	Enter a unique name for the ipsec profile.	
IKE version	Select the version of IKE.	
IKE phase-1 settings		
Exchange mode Select the exchange mode: <i>Main</i> or <i>Aggressive</i> .		
Local identifier type	Select the local identifier type. The options are Local WAN IP, FQDN, and User-FQDN. If you select User-FQDN , enter the FQDN name in the <i>Local identifier</i> field. When you select L ocal WAN IP or FQDN , it uses the Local IP address of the WAN interface, and the FQDN name of the WAN configured on the Dynamic DNS page.	
Remote identifier type	Select the remote identifier type. The options are Remote WAN IP, FQDN, and User-FQDN. If you select FQDN or User-FQDN , enter the FQDN name in the <i>Remote identifier</i> field. When you select Remote WAN IP , it uses the remote IP address entered in the VPN policy.	
DH group	Select the DH (Diffie-Hellman) group. It defines the strength of the key used in the key exchange process.	
Encryption algorithm	Select the encryption algorithm to be followed during key exchange. You may select multiple algorithms.	
Authentication algorithm	Select the authentication algorithm from the drop-down list. You may select multiple algorithms.	
SA lifetime (sec.)	It refers to the security association lifetime, and the range varies from 300 to 604800 seconds.	
Authentication method	Select the authentication method. The options are the Pre-shared key and RSA-Signature (Certificate).	
Pre-shared key	Enter the preshared key. This field is available only when you select the Pre-shared key as the <i>Authentication method</i> .	
Certificate	Select the certificate to be used for authentication. This field is available only when you select RSA-Signature (Certificate) as the <i>Authentication method</i> .	
Dead peer detection	You can enable or disable the <i>Dead peer detection</i> feature. If enabled, it allows you to detect if the remote peer is reachable or not. If it is not reachable, this feature will make the tunnel down.	
Detection interval	Enter the interval at which you want to send peer detection packets to the peer to check its liveliness.	
Reconnect after failure		

	This is the failure count, after which it is considered the other peer as down. Enter the failure count.	
VPN tunnel backup	You can enable or disable the VPN tunnel backup feature.	
Backup tunnel	If <i>VPN tunnel backup</i> is enabled, you can use the VPN backup of the selected profile if the primary tunnel is down. When the primary tunnel is up, the backup tunnel will be turned down.	
Failure time to primary (seconds)	Specify the time after which the backup tunnel will be down.	
Extended authentication	Enable or disable the extended authentication feature.	
Extended authentication type	Select the authentication type that you want to use. The options are Local authentication, Authentication server, and IPSec host (Initiator).	
Authentication server	Select any one of the external authentication servers from the drop-down, and select the respective server.	
Username	Enter the user name. This field is available when you select the IPSec host (Initiator) as the <i>Extended authentication type</i> . The length of the user name may vary from 1 to 64 characters.	
Password	Enter the password. This field is available when you select the IPSec host (Initiator) as the <i>Extended authentication type</i> . The length of the password may vary from 8 to 63 characters.	
Local authentication	You may select one of the saved authentications on the local server. This field is available when you select Local authentication as the <i>Extended authentication type</i> .	
	IKE phase-2 settings	
Protocol selection	Select the protocol for IKE phase-2.	
Encryption algorithm	Select the encryption algorithm to be used. You may select multiple algorithms.	
Authentication algorithm	Select the authentication algorithm from the drop-down list. You may select multiple algorithms.	
SA Lifetime (sec.)	It refers to the security association lifetime, and the range varies from 300 to 604800 seconds.	
Perfect forward secrecy	If enabled, it does not allow the same key to be generated, forcing the user to use a new DH key exchange.	
DH group	Select the DH group.	
Apply	Click Apply to save your settings.	
Cancel	Click Cancel to revert to previous settings.	

IPsec Site to Site

The user can manually configure it in the *Ipsec site to site* and build IPSec VPN tunnels. This mode is useful when you try to establish a tunnel between two DSR-250v2 devices or when you try to establish a tunnel between DSR-250v2 and/or with any third-party gateway.



The fields available in the *Ipsec site to site Configuration* table are as follows:

Field	Description
Name	It displays the name of the VPN.
Remote gateway	It displays the remote IP address to which the VPN tunnel is established.
Interface	It displays the interface being used for the VPN connection.
Local subnet	It displays the local subnet being used by this VPN connection.
Remote subnet	It displays the remote subnet being used by this VPN connection.
IKE profile	It displays the IKE profile selected for the configured VPN connection.
Enable	You can enable or disable the connection.
Status	It displays if the VPN connection is connected or disconnected.

Click + to add a new VPN configuration. This opens the *Add basic configuration* page. To delete an entry or multiple entries, select the corresponding checkboxes, and click **Delete**, for edit an entry select the corresponding checkboxes to **edit**.

Connection name	spoke-1		
outgoing interface	WAN1	9 40	
lemote gateway	Static IP	Ť	
P address	192,168.98.147		1
KE profile	IKE_profile_default		0
ocal site setup			
ocal network	SUBNET	(*)	
ocal network P address	SUBNET 192.168.20.0))
	1 200 200		

IP address Subnet mask	192.168.20.0 255.255.255.0	
Subnet mask	255.255.255.0	
Remote site setup		
Remote network	SINGLE IP	Ŕ
IP address	192.168.10.2	
Basic settings Advance	ed settings	
NetBIOS broadcast		
Auto-rollover using WAN port	0	

The fields available on the Add basic configuration and Advanced configuration pages are as follows:

Field	Description	
Connection name	Enter a descriptive name for the VPN connection.	
Outgoing interface	Specify the interface to be used for the outgoing data.	
Remote gateway	Select the gateway you want to use for the connection. The options are Static IP and FQDN.	
IP address	If you select Static IP as the remote gateway, enter the IP address.	
Domain name	If you select FQDN as the remote gateway, enter the domain name.	
IKE profile	Select one of the configured IKE profiles from the drop-down list.	
Local site setup		
Local network	 Select the network access type that you want to provide over the IPSec Tunnel. Any: It specifies that the policy is for any traffic from the given local endpoint. Single IP: It limits the policy to one host. Enter the IP address of the host that will be part of the VPN. 	

	• Subnet : It allows an entire subnet to connect to the VPN. Enter the network address and subnet mask in the provided fields.	
IP address	Enter the IP address to connect to the VPN.	
Subnet mask	Enter the subnet mask for the network address.	
Remote site setup		
Remote network	 Select the network access type that you want to provide over the IPSec Tunnel. Any: It specifies that the policy is for any traffic from the given remote endpoint. Single IP: It limits the policy to one host. Enter the IP address of the host that will be part of the VPN. Subnet: It allows an entire subnet to connect to the VPN. Enter the network address and subnet mask in the provided fields. 	
IP address	Enter the IP address to connect to the VPN.	
Subnet mask	Enter the subnet mask for the network address.	
	Advanced configuration	
NetBIOS broadcast	Enable it to allow NetBIOS broadcast to travel over the VPN tunnel.	
Rollover	To enable a VPN rollover, you must have the WAN Mode set to Rollover.	
Apply	Click Save to save your settings.	
Cancel	Click Cancel to revert to the previous settings.	

IPsec Client to Site

The user can manually configure it in the *Ipsec client to site* and build IPSec VPN tunnels. This mode is useful when you try to establish a tunnel between two DSR-250v2 devices or when you try to establish a tunnel between DSR-250v2 and/or with any third-party gateway.



The fields available in the Ipsec client to site Configuration table are as follows:

Field	Description
Name	It displays the name of the VPN.
Interface	It displays the interface being used for the VPN connection.
Local subnet	It displays the local subnet being used by this VPN connection.
Enable	You can enable or disable the connection.

Basic settings Advanced settings

Connection name	bhb	
Outgoing Interface	WANI	3 9 3
Remote gateway	IP_ADDRESS	्र
IP address	2.3.24.2	
IKE profile	IKE_profile_default	1

Local site setup

Local network

ANY	2.42

÷.

Remote site setup

Remote network

ANY

Basic settings	Advanced settings	
Mode config		
Starting IP address	192.168.1.3	
Ending IP address	192.168.1.56	
Primary DNS Server	192.168.1.1	
Secondary DNS Server		

(Optional)			
Primary WINS Server (Optional)	e.g. 192.168-10.4	
Secondary WINS Serve (Optional)	н	e.g. 192.168.10.2	
Split Tunnel			
Sark Terrod	2		
Set DRS			
	+ 🖉 i		
		Things also Fill more	
	100	abc.com	
REPRIES Frontcast	Ψ.		
Auto-militater using work port	0.0		

The fields available on the Add basic configuration and Advanced configuration pages are as follows:

Field	Description	
Connection name	Enter a descriptive name for the VPN connection.	
Outgoing interface	Specify the interface to be used for the outgoing data.	
Remote gateway	Select the gateway you want to use for the connection. The options are Static IP and FQDN.	
IP address	If you select Static IP as the remote gateway, enter the IP address.	
Domain name	If you select FQDN as the remote gateway, enter the domain name.	
IKE profile	Select one of the configured IKE profiles from the drop-down list.	
	Local site setup	
Local network	 Select the network access type that you want to provide over the IPSec Tunnel. Any: It specifies that the policy is for any traffic from the given local endpoint. Single IP: It limits the policy to one host. Enter the IP address of the host that will be part of the VPN. Subnet: It allows an entire subnet to connect to the VPN. Enter the network address and subnet mask in the provided fields. 	
IP address	Enter the IP address to connect to the VPN.	
Subnet mask	Enter the subnet mask for the network address.	
	Remote site setup	
Remote network	 Select the network access type that you want to provide over the IPSec Tunnel. Any: It specifies that the policy is for any traffic from the given remote endpoint. 	
	Advanced configuration	
Mode config		

	Mode Config is similar to DHCP and is used to assign IP addresses to the remote VPN clients. You can enable or disable this feature.
Split Tunnel	Split Tunnel: It provides VPN client access to all the intranet services.
Starting IP address	Enter the starting IP address of the assigned IP range to the VPN clients.
Ending IP address	Enter the ending IP address of the assigned IP range to the VPN clients.
Primary DNS	Enter the IP address of the primary DNS.
Secondary DNS (Optional)	Enter the IP address of the secondary DNS. It is an optional field.
Starting IP address	Enter the first IP address of the DHCP IP range.
Ending IP address	Enter the last IP address of the DHCP IP range.
Subnet mask	Enter the subnet mask for the IP range.
NetBIOS broadcast	Enable it to allow NetBIOS broadcast to travel over the VPN tunnel.
Rollover	To enable a VPN rollover, you must have the WAN Mode set to Rollover.
Save	Click Save to save your settings.
Cancel	Click Cancel to revert to the previous settings.

IPsec 1 to 1 mapping

Ipsec 1 to 1 mapping is used to hide our local network by mapping it to another network.Let us see in detailed for example my lan network is in 192.168.10.0/24 and administrator want to hide this network from remote user in this case i mapped my lan network with some other network (192.168.70.0/24).

IPse	c 1 to 1 mapping							Garc	ef Antra
(Psec	1:1 mapping list								
+ t	1							18	
ġ.	Source IP range shart	ĥ	Noggetti IP comproduct	1	Barrya bergih	54	ministry		- Brieffe
0	597.199.17.2		145.998.50%		11.	30	.gobe-t	35	
						7.643	t tara 👘 in		1 5 -

The fields displayed on the *lpsec* 1 to 1 mapping are as follows:

Field	Description
Source Ip Range Start	Here we have to information regarding our local network
Mapped Ip Range Start	Here we have to information regarding to which network we have to do mapping.
RangeLength	We have to give range from 1-254
Ipsec policy name	We have to select the configured ipsec policy
Enable	You can enable or disable the configured tunnel.

Click + to add a new entry to the list. This opens the *new ipsec 1 to 1 mapping rule*. To delete multiple entries, select the checkboxes of the policies you want to delete, and click **Delete**, click on edit to edit the policy.

PPTP

Server Mode

DSR-250v2 can establish a PPTP/L2TP VPN. Once enabled, a PPTP/L2TP server is available on the gateway for the LAN and WAN PPTP/L2TP client users to access, i.e., PPTP/L2TP clients can reach the gateway's PPTP/L2TP server. Furthermore, once authenticated by the PPTP/L2TP server (the tunnel endpoint), PPTP/L2TP clients can access the LAN network managed by the gateway.

The range of IP addresses allocated to PPTP/L2TP clients should not coincide with the LAN subnet. Also, the PPTP/L2TP server will default to local PPTP/L2TP user authentication but can be configured to employ an external RADIUS authentication server should one be configured.

PPTP		
Server Client		
Enable PPTP are out	2	
PPTP routing mode	NAT C Boxter	
Starting IP address	10,0.0.2	
Ending IP address	10.0.0.102	
Authentication server	Local user-database +	
	Local user group	default_user •
	Authentication protocol	PAP x CHAP x =
Idle timeout	450	securida
Nettions		

The fields available on the *PPTP server* page for the **PPTP server** type are as follows:

Field	Description	
	PPTP Server	
Enable PPTP Server	Enable pptp server for the configuration	
Name	Enter the name of the PPTP server.	
Routing mode	Select the routing mode, either NAT or Router.	
Starting IP address	Enter the starting IP address of the IP address range to assign to your PPTP clients.	
Ending IP address	Enter the ending IP address of the IP address range to assign to your PPTP clients.	
Authentication Server	Select any one of the available authentication servers. The options are <i>Local authentication</i> , <i>RADIUS</i> , and <i>None</i> authentication.	
Radius Server	Select the RADIUS server. It is available when you select Radius as the <i>Authentication Server</i> .	
Local authentication	Select one of the saved authentications on the local server.	

Authentication protocol	Select one or multiple authentication types from the drop-down list (<i>All/PAP/CHAP/MS-CHAP/MSCHAPv2</i>).
Encryption	 This field is available only when MS-CHAP or MS-CHAPv2 is selected as the Authentication protocol. All: Select the checkbox to select all the encryption options. Mppe 40 Bit: Select the checkbox to enable Mppe 40 bit encryption. Mppe 128 Bit: Select the checkbox to enable Mppe 128 bit encryption. Stateful Mppe: Select the checkbox to enable Stateful Mppe encryption. This mode of Mppe encryption is less secure and can be used for compatibility.
Idle timeout (seconds)	Enter the amount of time in seconds, after which the connection will disconnect when idle.
Netbios	Enable it to allow NetBIOS broadcasts to travel over the VPN tunnel.
WINS server	Enter the WINS server address for Netbios. This field is available when you enable Netbios.
Apply	Click Save to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Client Mode

The DSR-250v2 can configure the PPTP/L2TP VPN Client. Using this client, we can access a remote network that is local to the PPTP/L2TP server. Once a client is enabled, it will try to auto-connect or manual connect to the server.

РРТР				
Surver Client				
Enable PPIP Client	2			
VPN server	22,23,22.3			
Tunnel type	Full Tunnel	•		
User Name	admin			
Research		2		
MPPE and system.				
Idle Unieuul	300	12 security		
Asto connect				
	Girrae	2	10	mittatas

The fields available on the *PPTPclient* page are as follows:

Field	Description

Name	Enter the name.	
VPN server	Enter the IP address or domain name of the PPTP server you want to connect to.	
Tunnel type	 Select the tunnel type. Full tunnel: If this is selected, it will access the Internet and the LAN host connected to the server device through the PPTP server once the connection is established, Split tunnel: If this is selected, it will access only the selected remote network. 	
Remote network	Enter the remote network address. This address is local for the PPTP Server.	
Remote netmask	Enter the remote network subnet mask.	
User name	Enter the user name to connect to the server.	
Password	Enter the password to connect to the server.	
MPPE	Enable or disable Microsoft Point-to-Point Encryption (MPPE).	
Auto connect	Enable the option to connect the tunnel automatically	
Time	Provide the time in how many minutes tunnel should connect	
Idle timeout (seconds)	Enter the amount of time (in seconds) that you will disconnect from the PPTP server when idle.	
Apply	Click Apply to save your settings.	
Cancel	Click Cancel to revert to the previous settings.	

L2TP

Server Mode

DSR-250v2 can establish a PPTP/L2TP VPN. Once enabled, a PPTP/L2TP server is available on the gateway for the LAN and WAN PPTP/L2TP client users to access, i.e., PPTP/L2TP clients can reach the gateway's PPTP/L2TP server. Furthermore, once authenticated by the PPTP/L2TP server (the tunnel endpoint), PPTP/L2TP clients can access the LAN network managed by the gateway.

The range of IP addresses allocated to PPTP/L2TP clients should not coincide with the LAN subnet. Also, the PPTP/L2TP server will default to local PPTP/L2TP user authentication but can be configured to employ an external RADIUS authentication server should one be configured.

L2TP server	slimt		
Enable L2TP server			
Routing mode	NAT 🕜 Route		
Starting IP address	9.9.9.0)	
Ending IP address	9.9.9.10		
Authentication server	Local user database	·	
	Local user group	default_user	•
	Authentication protocol	PAP × CHAP +	•

	Enable secret key		
Idle timeout	450	12	seconds
L2TP over IPaec			

The fields available on the *L2TP server* page for the **L2TP server** type are as follows:

Field	Description	
L2TP Server		
Enable I2tp server	Enable I2tp server to configure	
Name	Enter the name of the L2TP server.	
Routing mode	Select the routing mode, either NAT or Router.	
Starting IP address	Enter the starting IP address of the IP address range to assign to your L2TP clients.	
Ending IP address	Enter the ending IP address of the IP address range to assign to your L2TP clients.	
Authentication server	Select the authentication server. The options are <i>Local authentication</i> , <i>RADIUS</i> , and <i>None</i> a uthentication.	
Local authentication	Select one of the saved authentications on the local server. This field is available when you select Local authentication as the authentication server.	
Radius server	Select the Radius server. This field is available when you select Radius as the authentication server.	
Authentication protocol	Select any authentication types from the drop-down menu (<i>All/PAP/CHAP/MS-CHAP/MSCAPv2</i>).	
Encryption	Enable it to add a secret key.	
Enable Secret key	If the Encryption field is enabled, enter the secret key.	
Auto connect	Enable the option to connect the tunnel automatically	
Time	Provide the time in how many minutes tunnel should be connected	
Idle timeout (seconds)	Enter the amount of time in seconds that the connection will disconnect when idle.	
L2TP over IPsec	When the <i>L2TP over IPsec</i> configuration is enabled, the IPsec tunnel initiation starts automatically. Still, the establishment of the tunnel depends on the configuration at the client and the server-side and the response from the server. Select I2tp over ipsec to configure the <i>ipsecprofile</i> for IPsec. For details, refer ipsec profiles.	
Apply	Click Save to save your settings.	
Cancel	Click Cancel to revert to the previous settings.	

Client Mode

DSR-250V2 can configure the PPTP/L2TP VPN Client. Using this client, we can access a remote network that is local to the PPTP/L2TP server. Once a client is enabled, it will try to auto-connect or manual connect to the server.

LETP server L2TP client

Enable L3TP Client		
VPN server	22.22.22.3	
Turisel type	Fall Tunnel	Si -
User Name	admin	
Password		Ø
Enable secret key		
Reconnect mode	Always on	÷
MPPE		
Auto connect		
L2TP over IPsec		

The fields available on the *L2TP client* page are as follows:

Field	Description	
Name	Enter the name.	
VPN server	Enter the IP address of the L2TP server you want to connect to.	
Tunnel type	Select the tunnel type.	
	 Full tunnel: If this is selected, it will access the Internet and the LAN host connected to the server device through the L2TP server once the connection is established. Split tunnel: If this is selected, it will access only the selected remote network. 	
Remote network	Enter the remote network address. This address is local for the L2TP Server.	
Remote netmask	Enter the remote network subnet mask.	
User name	Enter the user name to connect to the VPN server.	
Password	Enter the password to connect to the VPN server.	
Enable secret key	You may enable or disable the Secret key.	
Secret key	If the Secret key is enabled, enter the secret key.	
MPPE	Enable or disable Microsoft Point-to-Point Encryption (MPPE).	
Reconnect mode	Select either Always On or On Demand.	
Maximum idle time (seconds)	Enter the idle time in seconds before the gateway disconnects from the L2TP server. This field is available only when <i>Reconnect mode</i> is On Demand .	
L2TP over IPsec	You may enable or disable this feature. If enabled, it will redirect you to the IPsec settings. Click Next to configure the <i>Ipsecprofile</i> for IPsec.	

Auto-connect .It is used to connect the tunnel automatically	
Apply	Click Save to save your settings.
Cancel Click Cancel to revert to the previous settings.	

OpenVPN

The router provides the OmniSSL feature, a customized OpenVPN, similar to the SSL VPN connectivity. OmniSSL provides an executable configuration file via a portal page (*<https://<Device WAN IP>/omnissl>*) that facilitates the client installation from the device and is an enhancement to the existing OpenVPN. In addition, this VPN tool can be used via mobile devices, thereby eliminating browser and Java dependencies typical to the SSL VPN solutions.

OpenVPN allows peers to authenticate each other using certificates or username/password. When used in a multi-client-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 gateway.

In access server-client mode, the user downloads the auto-login profile from the OpenVPN Access Server and uploads the same to connect. You can select the following modes:

- Server mode
- Client mode
- Access Server-client mode

Server mode

In this section, you will learn about the OpenVPN configuration in the Server mode.



The fields available on this page are as follows:

Field	Description		
OpenVPN	You can enable or disable the OpenVPN feature.		
OpenVPN daemon mode			
Mode	Select Server.		
	VPN setting		
VPN network	Enter the IP network for the VPN.		
VPN netmask	Enter the netmask.		
Duplicate CN	Enable it to allow the user to use the same certification to connect for multiple clients. User-based authentication is also required for this feature, and multiple clients require to have their respective user names and passwords.		

Port	Enter the port number on which the OpenVPN server runs. The default port is 1194.	
Tunnel protocol	Select either TCP or UDP to communicate with the remote host.	
Encryption algorithm	Select the encryption algorithm from the drop-down menu. The options are <i>AES-128</i> , <i>BF-CBC</i> , <i>AES-192</i> , and <i>AES-256</i> .	
Hash algorithm	Select the hash algorithm from the drop-down menu. The options are <i>SHA1</i> , <i>SHA256</i> , and <i>SHA512</i> .	
Tunnel type	Select either Full Tunnel or Split Tunnel . Full Tunnel mode sends all the traffic from the client across the VPN tunnel to the gateway. 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 to create local networks.	
Client to client	Enable this field to allow OpenVPN clients to communicate with each other in the split tunnel case. By default, it is disabled.	
User-based authentication	This option provides an additional authentication method. You can enable this field to select an authentication server.	
Local authentication	Select a configured local authentications saved on the local server. To add a new local authentication server, click the <i>Local authentication list</i> link. For more details, refer to local authentication list section.	
Certificate verification	Enable or disable certificate verification. This method does not require the client certificate; the client authenticates using the username/password only. It is enabled by default.	
Certificate	Select the profile which has a list of certificates uploaded for the configured mode server /client.	
TLS authentication key	Enabling this adds TLS authentication, which adds a layer of authentication. It can be checked only when the TLS key is uploaded. It is disabled by default.	
TLS key	Select the type of TLS certificate name.	
DH key	Select the DH key from the drop-down list.	
	Advanced settings	
Server policies	Enable or disable the <i>Server Policies</i> feature; if enabled, configure the Server policies under the Server policies section.	
Remote networks	Enable or disable the <i>Remote networks</i> feature; if enabled, configure this feature in the remote networks section.	
Local networks	Enable or disable the <i>Local networks</i> feature; if enabled, configure this feature in the Local networks section. This section is available when you select Split Tunnel as the <i>Tu nnel type</i> .	

Client List

It allows the user to generate the client's configuration. Furthermore, OmniSSL is an adaptable feature as it supports and gets installed on various operating systems following their respective procedures.

+ # + 12	Straty and a server of	神 2
T1 Oberinei.	ded	
		·····

The fields available on the *Client list* table are as follows:

Field	Description	
User name	It displays the OmniSSL client name.	
Update at	It displays the date and time when the user's certificates were last updated.	

Status	It displays the status of certificates.
Revoke	Click Revoke to validate the client certificate against the revoked certificates.
Resume	When the client is in the revocation status, the user can click Resume to resume the client, and the DSR-250V2 UI generates a new CRL.
Local authentication pool name	It displays the name of the local authentication pool where the clients belong.
Import at	It displays the date and time when the user's certificates were first imported.
Import	Click Import to import the OmniSSL Client list.
Download	Click Download to download the selected certificate and use it when required.
Actions	It allows you to view the client details.
	Note: You cannot view the client details if the status is Pending.

• Click Import to import an OmniSSL Client list. This opens the Import users from local authentication list page. Select the checkbox corresponding to the Local authentication you want to import, and click Save. Click Cancel to revert to the previous settings.

The fields available on this page are as follows:

Field	Description
Local authentication	It displays the name of the local authentication.
Access level	It displays the access level for the local authentication.
Entries	It displays the number of login credentials saved in the local authentication server.
Add local authentication	Click this button to add a local authentication. This opens the <i>Add local authentication list</i> page. For details, refer to the local authentication list
Apply	Click apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

• Click **Download** to download the OmniSSL list in the *.csv format.

OmniSSL Portal Layout

The router supports a static portal page to enable or disable authentication to the remote OmniSSL users.

Oracidal porte legest int			
+ 2 1			1
To continue	The Contract of the	The Rollins shall be sport	1. Turke
Find 1		12224_0.0028	
(herefyld) - eilant (operficiente that the			Solline [] [] [] []

Cashi25L client configuration fail:

The fields displayed in the OmniSSL Portal layout table are as follows:

Field	Description
Active	You can enable or disable the portal layout. When you enable it, the OmniSSL URL will appear above the table in the right corner.
Layout name	It displays a name for the portal layout.
Login page	It displays the portal login page link.

Server Policies

OmniSSL Server Policies are useful in permitting or denying access to specific IP addresses or IP networks. They may be defined at the user or global level.



Sa Admin stration	Second Second	and a long a					
The Article State	Spin Shrundi para						
	1.44						
010100							1 (1) (10)-10
± 145,5	11		Const.		in a second		incon .
C. Burnet				10778	0.0000	$(2\pi_{0})^{2}(1+\epsilon)$	
-/44	Firmula colora fat						
And Install	+ 2						
-	17			in a second s			
Section 201	Los private :						
1.1	100000000000000000000000000000000000000			correct and from the former PLAT	2.23		
1220							
CONT (MY)							
100							

The fields displayed in the Server policies table are as follows:

Field	Description
Name	It displays the name of the server policy.
Policy	It displays the policy applied to the IP address.
Scope	It displays the scope. It is either Global or Local authentication.
Destination	It displays the IP address to which the OpenVPN policy is applied.
Port	It displays the port number to which the policy is applied.

Click Add icon to add a new entry to the list. This opens the Add OpenVPN server policy page. To delete multiple entries, select the corresponding checkboxes, and click Delete icon.

Add	Open'	VEN	200401	P20 (77

All second second	Providence	
Platy	Price and	
Barry .	1.14L	1000
Accessing	-	
P sales		11
901	Later	0
1,54	2	

The fields available on the Add OpenVPN server policy page are as follows:

Field	Description
Policy name	Enter a name for the server policy.
Policy	Select the policy, whether to permit or deny access to the specific IP address or IP network.
Scope	Select the scope from the drop-down menu. It is either Global or Local authentication.
Local authentication	If Local authentication is selected as the <i>Scope</i> , specify the user name (client) to which this policy is to be applied.
Apply policy to	Select an accessible IP address or IP network to which the policy is applied.

SHORE STANK

IP network	Enter the IP network to which the OpenVPN policy needs to be applied.
Subnet mask Enter the subnet mask for the above IP network.	
IP address	Enter the IP address to which the OpenVPN policy needs to be applied.
Port	Enter the range of port numbers to which the policy will be applied.
ICMP	Enable it to support ICMP traffic.
Apply	Click apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Remote Networks

This section displays a list of configured remote networks. The configured IP addresses can remotely access the server through an OpenVPN tunnel.

DLink	THE NEW				15	0
(second	Openves					
er same ment	alternal strage	-				
2 Martine	Specifies server palleting					
AL contact	1.2.15					
)) inter Second	retail .	41066	and the second s		
art.ee e= 30%	Next In Institutes				Seller	e pine
Page partial /	$+ \alpha$					
THE REPORT	1 1 Participation		and an and a			
and become			a contraction of the second		the local of	e ipe ie C
Continent and and a second sec	Local protects					80.0
	The same loss transference and the	all a second design and	(α,β) is the set of	CP. 47496		
Sec.						
246						

The fields displayed on the *Remote networks* table are as follows:

Field	Description
User name	It displays the name of the remote network.
Remote networks	It displays the IP address of the remote networks.
Subnet mask	It displays the subnet mask for the IP address of the remote network.

Click Add icon to add a new entry to the list. This opens the Add OpenVPN remote network configuration page. To delete multiple entries, select the checkboxes of the remote networks you want to delete, and click **Delete** icon

(Barder)	lución			
± 0	1 mm our annih Kana anti-			
4	The selection	· · · · · · · · · · · · · · · · · · ·	- 1-0	V
0	Non-on-participae	Not take bit 1	A ANY DAME OF A CONTRACTOR	
3		Assumed box 1	Loss appendix a	
				C Theres

The fields available on the Add OpenVPN remote network configuration page are as follows:

Field	Description
user name	Enter the name of the remote network.

Remote networks Enter the IP address of the remote networks.	
Subnet mask	Enter the subnet mask for the IP address of the remote network.
Apply	Click Save to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Local Networks (Split Tunnel)

This section is available only when the **Split Tunnel** is selected as the *Tunnel type*. It displays a list of the configured OpenVPN local networks. The clients have access only to these configured local networks.

D-Link	4704-21912				to his is	3
Station .	Openint thi				ũ	
	Access Manay offer					
Tratamina -	CONSISTS SERVE CONC.00					
	+ 1 2					1.1.1.1
- David		100	11		por com	
il daana	E-main constra				an an line i	0.43
An	+ II Non-er-en-		REPRESE	and the second	1	U.
men i segne die men die die sooner segle die	Local entrocke				heime [16]]	11 0.93
in and the second se						
1						fil (13)

The fields displayed on the Local networks list are as follows:

Field	Description	
Local network	It displays the IP address of the local network.	
Subnet mask	It displays the subnet mask for the IP address of the local network.	

Click Add to add a new entry to the list. This opens the Add OpenVPN local network configuration page. To delete multiple local networks, select the checkboxes corresponding to the local networks you want to delete, and click **Delete**.

+ tr			
1072 - 11	Aurorat & Channell	11 Aread and	
1	142104-1-12	Burnhalter (
10.		• 1	

The fields available on the Add OpenVPN local network configuration page are as follows:

Field Description	
Local networks Enter the IP address of the local network.	
Subnet mask Enter the subnet mask for the IP address of the local network.	
Apply	Click apply to save your settings.
Cancel	Click Cancel to revert to the previous settings.

Client mode

In this section, you will learn about the OpenVPN configuration in the Client mode.

D-Link	min drift				(The second seco	\odot
(www.user)						Aug 1
Sector and						
La constante E seconda E seconda	Manda Anari (Mar Algori Milita Anaria	•				
a and an	100	9.54	1. C.			
a dialay	and a	Page 1				
D.95		Company in				
North Col.	Taken and California	lare .	-			
www.committee.com	Pe+	. <u>1</u> H	-			
nin johnen in Ni	Terret is seen	100.1 200.0				
		to more any				
-	2000 - 10 C	2				
	100000-10000	and a				
	Print and Print	201.	1.123			
	(Participal)	term a term				

The fields available when the *Client mode* is selected are as follows:

Field	Description		
Mode	Select Client.		
	VPN setting		
Server IP	Enter the IP address/FQDN of the OpenVPN server.		
Failover server IP	Select the type of identifier you want to provide for the failover mechanism at the Failover Server IP: IP Address or FQDN (Fully Qualified Domain Name). This feature allows configuring an additional OpenVPN server for the client, which will be used when the primary server is down. This is applicable only in client mode.		
Port	Enter the port number on which the OpenVPN server (or Access Server) runs.		
Tunnel protocol	Select either TCP or UDP.		
Encryption algorithm	Select the encryption algorithm from the drop-down menu.		
Hash algorithm	Select the hash algorithm from the drop-down menu.		
User-based authentication	This option provides an additional authentication method using a user name/password. It is disabled by default.		
User name	Enter the user name. This field is available when User-based authentication is enabled.		
Password	Enter the password. This field is available when User-based authentication is enabled.		
Certificate verification	This method enables tunnel authentication to be with certificates. It is enabled by default.		
Certificate	Select the profile which has list certificates uploaded for the configured client mode.		
TLS authentication key	Enabling this adds TLS authentication, which adds a layer of authentication. It can be enabled only when the TLS key is uploaded. It is disabled by default.		
TLS key	Select the type of TLS certificate name. When you click the <i>Certificate list</i> link, it will redirect you to the <i>Certificate Management</i> page to add a new certificate and key.		
Auto connect	we can disable and enable, if enabled give we need to give interval		

Interval	it dispalys the time interval to connect tunnel automatically	
Status	It displays the connection status of the VPN.	

Access server-client mode

Select the mode as access server-client mode. In access server-client mode, the user downloads the auto-login profile from the OpenVPN Access Server and uploads the same to connect.

D-Link	hist becoi		1 (1	0
0 monate	(Openional)			carde Electro
to alternation	harry	at an a		
	Statute Version			
(term	Oper#PH suck	Anti-with the formula		
i viati	375 setting	and on a second second second		
ISI YM Recooline	(mag)	7.4		
and the second second	(Ball, Library)	Renter of Datas		
Problemania Problemania	1.0 Automatic record control			
1000 C				
Case of a literature				

The fields available when the Access server-client mode is selected are as follows:

Field	Description	
Mode Select the Access Server-Client mode.		
Port	Port It displays the port numbers on which the client will connect with the OpenVPN server (Access Server).	
Auto connect It displays the auto connect enabled or disabled		
Interval	When auto connect enabled give time interval to auto connect	
Upload status It tells about upload status whether it is yes or no		
upload access server client	Click Browse and locate the configuration file. Click Open, and then click Apply	

GRE

GRE tunnels allow LAN broadcast traffic of the gateway to pass over the Internet and receive by the remote LAN hosts. While creating a GRE tunnel, a unique IP address should identify the GRE tunnel endpoint. It will be referenced in the other gateway'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 gateway.

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

The fields displayed in the *Configuration* table are as follows:

GRE	3					Canod Aking 1
÷,	¢ III					6 Same
	264 (11)	interface -	1 GDC surrent IP	1. Directo D	1 Status	Active
	0.00	111/22	10000	221.000/0002	4499000000000	

	3533	WEINE	364,43	10.15.14.141	13 SCORPETING	
					Just Literat	1 1 .
	Fie	d		Desc	cription	
	Name			e of the GRE tunnel.		
Interface It displays the interface with which this tunnel is created.						
GRE tunnel IP			It displays the IP address of this endpoint.			
Remote IP			It displays the WAN	IP address of the endpoi	nt gateway.	

Click + to add a new entry. This opens the Add GRE tunnel page. To delete multiple entries, select the checkboxes of the GRE tunnels you want to delete, and click **Delete**. To edit, select the checkboxes of the GRE tunnels you want to edit.

You can enable or disable the configured tunnel.

It displays the status of the GRE tunnel, i.e., whether it is connected or disconnected.

GRE tunnel name	123
Interface	WAN1 -
GRE tunnel IP	3.3.3.1
Subnet mask	255.255.255.0
Remote IP	10.10.20.54
IP address	192.168.10.0
Subnet mask	255.255.255.0
Gateway IP address	3.3.3.2

The fields available on the Add GRE tunnel page are given below.

Active

Status

Field	Description	
GRE tunnel name Enter a name for the GRE tunnel.		
Interface Select the interface to create this tunnel.		
GRE tunnel IP	Enter the IP address of this endpoint. It will be referenced in the other gateway's static route as the Gateway IP address.	

Subnet mask	Enter the subnet mask.	
Remote IP	Enter the WAN IP address of the endpoint gateway.	
Static route configuration		
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 gateway.	
Apply	Click Save to save your settings.	
Cancel	Click Cancel to revert to the previous settings.	