DRO-210*i*
Broadband Business Gateway
User Guide

(Updated for Firmware Revision 2.1.2)

D-Link India Ltd.,
Software and R&D Center,
Bangalore.
Phone: 91-80-26788345/46/50/51
www.dlink.co.in

Table Of Contents

About This Manual

This document provides information related to the installation and configuration of DRO-210i along with a description of all its features. This document is intended for service providers and network administrators who guide the network infrastructure deployment in enterprises.

Conventions

This document uses the following notational conventions:

bold	This text format is used to give strong emphasis.
Italics	This text format is used to highlight specific keywords, notes and cautions.
Web UI	This icon is used to indicate that the Web User Interface is explained.
	This icon is used to highlight important notes regarding the router.
	This icon is used to caution the user about the adverse affects of specific router configurations.

Product Overview

DRO-210i is a part of D-Link's DRO-2XX Business Gateway series, especially designed as an all-in-one network solution for small and medium businesses. Today's network infrastructure for small and medium business calls for highly reliable connectivity, comprehensive security features and high throughput with sophisticated QoS to support Voice/Video over IP. Such a network infrastructure can be implemented with different boxes, but the cost, performance bottlenecks and interoperability issues make such an approach impractical. DRO-2XX Business Gateways are a cost-effective, all-in-one-box solution for converged network infrastructure of small and medium businesses.

Some of the key features of DRO-210i Broadband Business Gateway are:

Dual WAN Connectivity
The router supports *Dual Ethernet Ports for xDSL connectivity*. xDSL connectivity is cheap, but more susceptible to outages. With two xDSL links, DRO-210i ensures high reliability, and also the benefit of double internet capacity.

Converged Network Support
The router provides the following features to support Data, Voice and Video services over the same IP Network:

- *Application Level Gateway support for Voice/Video over IP* enables successful deployment of voice/video equipment by addressing the interoperability issues with Firewall/NAT devices.
- *QoS support* allows prioritization, bandwidth reservation and upper ceiling for each class of service. This enables optimal and dynamic utilization of bandwidth, while guaranteeing voice and video quality.

Secure Remote Management
Administrators can remotely provision the router over a secure SSL-based Web User Interface. He can also perform remote software upgrades and remote monitoring to ensure smooth operation of the network.

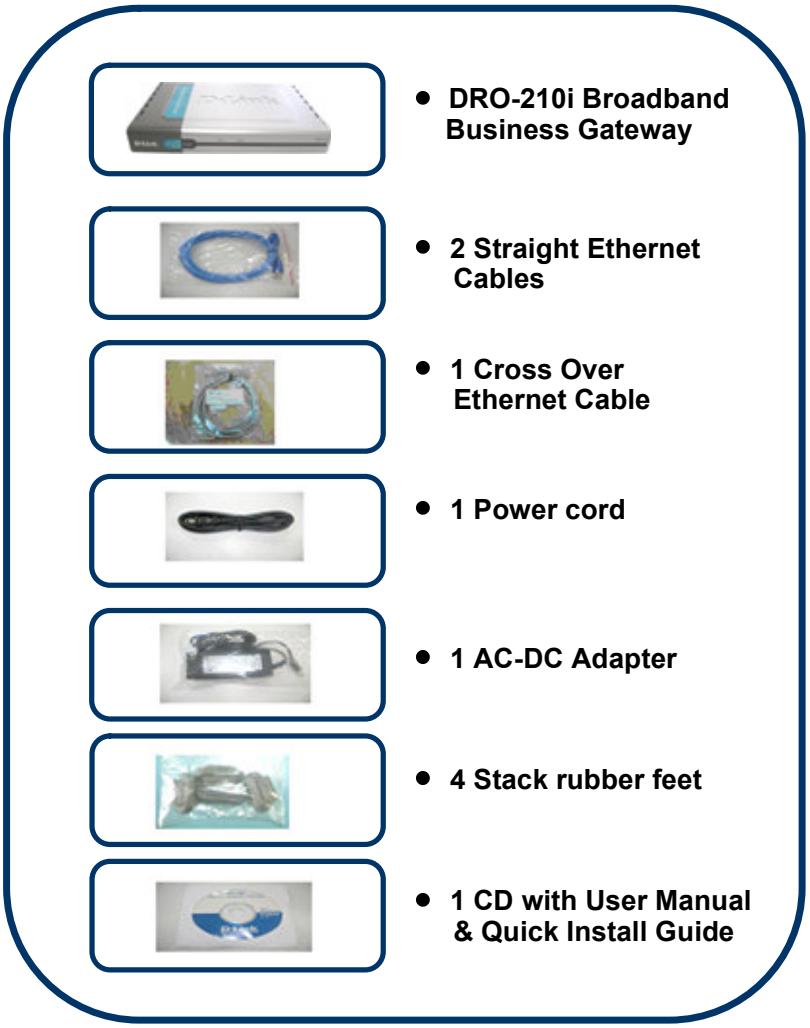
Self monitoring and Restart
This feature monitors the health of the system and automatically restarts in panic cases, without a need of intervention from the user; thus ensuring minimal system downtime in case of failures.

Built-in Hardware accelerator
The router platform uses Intel's XScale Architecture with on-board hardware crypto accelerator. The hardware accelerator enables high-performance VPN connectivity for branch offices and teleworkers requiring secure access to the corporate network resources.

1.1 Hardware Details

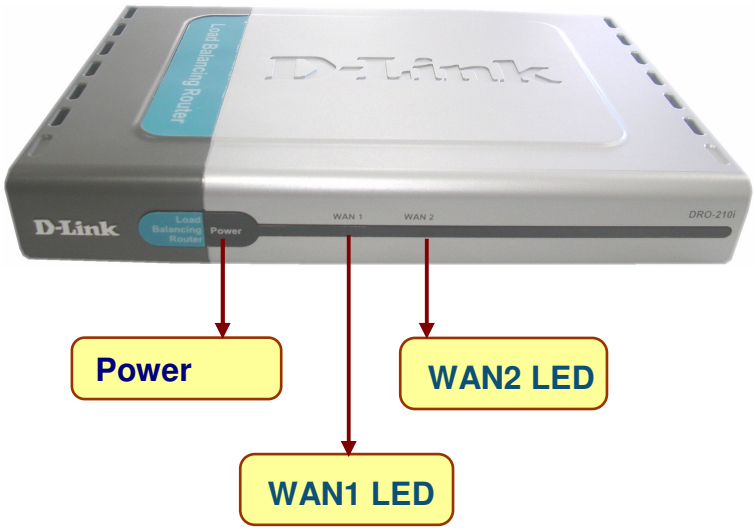
DRO-210i Package Contents

The DRO-210i package contains the following items:



Front Panel

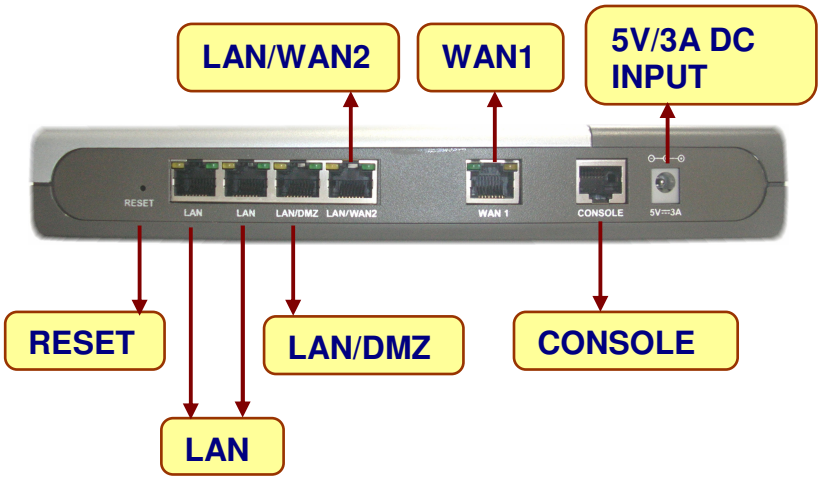
The front panel provides the LEDs to indicate the status of the router.



Module	Status	Description
Power	On	ON OFF
WAN1 LED	Ready	ON: Link and Protocol is UP OFF: Link or Protocol is DOWN
WAN2 LED	Ready	ON: Link and Protocol is UP OFF: Link or Protocol is DOWN

Rear Panel

The rear panel provides the router's ports and reset button.



Interface Description	
RESET	Restore the Factory Default Settings in the router
LAN	10/100Mbps Ethernet LAN Ports (RJ-45)
LAN/DMZ	10/100Mbps Ethernet Port (RJ-45) - configurable as LAN or DMZ Port
LAN/WAN2	10/100Mbps Ethernet Port (RJ-45) - configurable as LAN or WAN2 Port
WAN1	10/100Mbps Ethernet WAN1 Port (RJ-45)
CONSOLE	DB-9 Console Port
5V/3A DC INPUT	Input Voltage 5V, 3A DC

1.2 Software Features

The router has rich features like routing, load-balancing, auto backup, firewall access control, secure VPN connectivity, network address translation, quality of service and remote management satisfying most of the needs of the SMB market.

Routing

The router supports static, dynamic and policy-based routing.

- *Static Routing* - The network administrator can manually configure the routes according to his network topology.
- *RIP* - The Routing Information Protocol (or RIP) enables the routes to be learnt dynamically, avoiding cumbersome manual configuration. The router supports both RIPv1 and RIPv2 versions.
- *Policy-Based* - Policy-based routing helps to define custom policies for routing traffic. For example, policy routes can be defined to route all HTTP traffic through WAN1 and E-mail traffic through WAN2.

High Availability

The *Load-Balancing* feature is an ideal solution for businesses requiring uninterrupted, low cost internet connectivity. With multiple Internet connections, it effectively uses the combined bandwidth of all the internet links resulting in a significant increase in the total available bandwidth. Also if any Internet connection goes down, uninterrupted internet connectivity is provided utilizing the serviceable links.

With *Auto Backup* feature, one of the links can function as the Primary WAN Link, and the other as the Backup Link. When the Primary Link fails, the Backup Link will become operational and traffic will switchover to this link. And when the Primary Link becomes serviceable, the traffic will automatically switchback to the Primary Link.

Firewall

An integrated network security provides the following features

- Stateful Packet Inspection (SPI) Firewall performs deep packet inspection to filter out unwanted packets
- Real-time Intrusion Detection and Prevention System (IDS/IPS) detects intruders or hackers trying to damage your network and denies further access to the network by blacklisting them.
- Flexible access control policies to restrict or permit traffic based on IP Address/Port, MAC Address or Domain Name.
- URL/Content filtering of web traffic based on keywords, file extensions etc.

Network Address Translation (NAT)

NAT enables the router to act as an address translation agent between the Internet (public network) and the local (or private) network. The router supports all the combinations of NAT models like *Many to Many*, *Many to One* and *One to One* to provide internet access to LAN client. And the *Virtual Server* (or Port Forwarding) feature enables remote access to the Company Servers (HTTP/FTP etc) from WAN.

VoIP enables voice communication to use the same infrastructure as data in your network; thus resulting in significant cost reductions. Session Initiation Protocol (SIP) is widely used for VoIP calls, and does not work behind NAT. The *SIP-ALG* feature in the router will ensure that SIP calls can be successfully established, even when NAT is performed at the router. SIP-ALG overcomes the need for STUN support at VoIP end points behind NAT.

VPN

Virtual Private Networks (VPN) feature enables secure connectivity between multiple location offices (Gateway mode) and/or remote users (Dynamic VPN Mode). The IPSec VPN includes strong encryption and authentication mechanisms to encapsulate data to protect it from potential hackers. DRO Business Gateways provide high performance IP-Sec VPN tunneling with built-in Hardware Accelerator for DES, 3DES, AES crypto algorithms. Apart from Gateway mode, the router also allows roaming users in Dynamic VPN Mode, which makes it extremely useful for tele-workers and on-the-go sales force to access data on the corporate network.

Quality of Service

The router provides sophisticated Quality of Service (QoS) algorithm to effectively use the available WAN bandwidth. This feature allows prioritization and bandwidth reservation with upper ceiling for each class of service and enables optimal dynamic utilization of bandwidth while guaranteeing highest quality voice and video services.

DHCP Server

The router provides a built-in DHCP Server/Relay for assigning network settings for the LAN clients. The DHCP Server also supports reservation of IP Addresses for specific hosts (based on MAC address). The DHCP Relay in the router enables LAN clients to use a DHCP Server connected to WAN Port, by relaying the DHCP messages between the LAN and WAN subnet.

Tools

The router supports various tools to manage and monitor the device.

- *Syslog* - The Router can send the Syslog messages to the configured server to aid in network administration.
- *NTP* - The administrator can configure the system date and time manually. Or he can use NTP feature to automatically synchronize the router's time with specified global time servers.
- *Configuration upload/download* -This tool allows the administrator to download the router configuration onto the local hard disk as a backup. The same configuration can be later uploaded to restore the device to its original settings.
- *Firmware Upgrade* – The administrator can easily upgrade the router's firmware whenever a new firmware release is made available. The firmware can be upgraded from a local/remote location in a secure manner.

Secure Web-based Management

The product provides SSL-based secure, user friendly Web Pages to configure and manage the device and the network. The router also supports Secure, Remote Configuration of the device to enable easy remote monitoring and troubleshooting. In addition, it provides Comprehensive Logging, Secure Local/Remote firmware upgrade, Configuration Backup and Restoration.

The supported Web Browsers for router configuration are:

- Internet Explorer Ver 6.0 +
- Mozilla 5.0 (Release 1.5)
- Netscape 8.0
- Mozilla FireFox 1.0

Interfaces

The router provides the following interface ports:

- **LAN Ports -** The router has two dedicated 10/100 Ethernet LAN ports.
- **DMZ Port -** The router has one 10/100 Ethernet DMZ port. A DMZ port is used to connect to the company servers (e.g. Web server, FTP Server). This port can be optionally reconfigured as a regular LAN port.
- **WAN Ports -** The router has two 10/100 Ethernet WAN ports. One WAN port can be optionally reconfigured to operate as LAN Port. The WAN interface can be used to connect to the Internet using any broadband modem. The administrator has the following three choices for WAN connectivity:

  ***Static*:** The administrator can configure a Static IP Address assigned by the ISP to connect to the broadband network.

  ***Dynamic*:** The ISP assigns an IP Address dynamically using DHCP Protocol.

  PPPoE (Point to Point link over Ethernet): This option is the most common mode of WAN connectivity. Here the ISP assigns an IP Address dynamically through PPPoE Protocol.

The following sections explain these interfaces and their configuration in detail.

2.1 Port Configuration

Select **Interface → Port Config** to configure **Optional Port Configuration** as explained below.

Web UI	Optional Port Configuration
Port 1	This Port will always be **LAN**. It cannot be reconfigured.
Port 2	This Port will always be **LAN**. It cannot be reconfigured.
Port 3	This Port is **LAN** by default. It can be reconfigured as **DMZ**.
Port 4	This Port is **WAN2** by default. It can be reconfigured as **LAN**.

Caution: *Do not connect LAN & WAN2 Ports or LAN & DMZ Ports to the same switch/hub in your network.*

Disabled WAN2/DMZ

The administrator may have configured certain features like Static Routing, Virtual Server Entries, QoS Entries etc. on WAN2 or DMZ Port. At a later time when Port 3 or

Port 4 is reconfigured as LAN, the entries configured on WAN2/DMZ earlier will be displayed in **dark grey** color in the corresponding feature tables to indicate that these entries are currently invalid.

Note: *When Port 4 is configured as LAN, Load Balancing and Auto Backup features get disabled as there is only one WAN interface available.*

2.2 LAN Interface

The user systems can be connected to the LAN Interface. And the administrator can configure the router using HTTPS to this LAN Interface IP Address (i.e https://RouterLANIP). If the administrator uses http://RouterLANIP by mistake, the router will automatically redirect the Web Browser to use https.

Note: *Default LAN Interface IP Address is 192.168.100.254.*

Select **Interface → LAN** to configure **LAN Settings** as explained below.

Web UI	LAN Settings
IP Address	Enter the IP address of the LAN interface.
Subnet Mask	Enter the subnet mask of the LAN interface.

Forgot LAN IP ?

In case the administrator forgets the IP given to the LAN Port, it is possible to open the Router's Web Page by pressing the factory default switch and the settings will be restored back to default settings. Type https://192.168.100.254. User name is "admin" and password is also "admin".

2.3 DMZ Interface

DMZ stands for Demilitarized Zone. The DMZ interface is typically used for connecting servers that need to be accessible from the outside world, such as e-mail, web and DNS servers.

Typically, connections from the DMZ are only permitted to the external network, and hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

Select **Interface → DMZ** to configure **DMZ Settings** as explained below.

Web UI	DMZ Settings
IP Address	Enter the IP address of the DMZ interface
Subnet Mask	Enter the subnet mask of the DMZ interface

To add a DMZ Server in the network, the administrator can

a) Assign Private IP Addresses to the DMZ network. And configure a One-To-One NAT entry to map a Global IP Address to the Private DMZ Server IP Address. Refer NAT Configuration for more details.
b) Or assign Private IP Addresses to the DMZ network. And configure a Virtual Server entry to map a Global IP Address/Port to the Private DMZ Server IP Address/Port. Refer Virtual Server Configuration for more details.
c) Or assign Global IP Address to the DMZ network. And add a NAT Exception (i.e disable NAT) between WAN and DMZ.

Note: *To make the private DMZ Server accessible from the internet, use One-To-One NAT only when multiple services are hosted by a single DMZ Server. When only one service is provided by the DMZ Server, it is preferable to use Virtual Server feature. This would enable you to save the number of Global IP Addresses required to expose your DMZ services.*

2.4 WAN Interface

This Interface is used for WAN Connectivity through an ISP. Typically ISPs support 3 modes of WAN Connectivity – Static, Dynamic and PPPoE. The WAN Interface configurations for these modes are explained in the following sections. These configurations are explained for WAN1 interface, and the same explanation holds good for WAN2 also.

Maximum Transmission Unit:
MTU (or Maximum Transmission Unit) is the largest sized packet that can be transmitted through the internet. A higher MTU brings higher bandwidth efficiency. However large packets can block up a slow interface for some time, increasing the lag on other packets. Packets with sizes greater than the MTU will be fragmented by the router.

Caution: *Follow the ISP's advice on whether to change the default MTU value and what to change it to.*

2.4.1 Static Mode

In this mode, the ISP allocates and provides a static Global IP Address for WAN connectivity. The ISP will also provide information regarding the Default Gateway IP Address to be used for this connection.

If you have purchased multiple static Global IP Addresses from the ISP, then configure the first IP Address as the WAN Interface IP Address. And use the rest of your static IP Addresses for Many-To-Many or One-To-One NAT Configuration.

Select **Interface → WAN1** and choose **IP Setting Mode** as **Static**. Configure **IP Settings for WAN1 Interface** as explained below.

Web UI	IP Settings for WAN1 Interface
IP Address	Enter the IP address assigned for the WAN interface
Subnet Mask	Enter the subnet mask for the IP address
Default Gateway	Enter the default gateway address (in the same subnet).
MTU	Enter the MTU value for the WAN. Default value is 1500.

Click on **Detect Link Status** to configure the **Ethernet WAN Link Detection** Feature.

Note: *The default gateway field specified here will be used by Load balancing feature to route packets through this interface.*

2.4.2 Dynamic Mode

In this mode, ISP provides the Global IP address automatically using DHCP Protocol. A DHCP Client is built into router to support this mode of connectivity.

Select **Interface → WAN1** and choose **IP Setting Mode** as **Dynamic**. Configure **DHCP Settings for WAN1 Interface** as explained below.

Web UI	DHCP Settings for WAN1 Interface
Host Name (optional)	Enter the hostname assigned for the WAN interface
MAC Address	Displays the MAC address of the router's WAN Port.
MTU	Enter the MTU value for the WAN. Default value is 1500.

After entering all the information press the **Apply** button. The **DHCP Client Status** table will now show the DHCP client status at the bottom of the page.

Click on **Detect Link Status** to configure the **Ethernet WAN Link Detection** Feature.

2.4.3 PPPoE Mode

In this mode, ISP provides the Global IP address automatically using PPPoE Protocol.

PPPoE protocol is a method of transmitting PPP packets over Ethernet network. Hence PPPoE is an acronym for PPP over Ethernet. It provides the ability to connect multiple hosts at a remote site through the same customer premise access device. In addition, it provides access control, billing and type of service on a per-user, rather than a per-site, basis.

PPP has three main components:

- A method for encapsulating datagram over serial links.
- A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
- A family of Network Control Protocols (NCP) for establishing and configuring different network-layer protocols. PPP is designed to allow the simultaneous use of multiple network layer protocols.

PPPoE has two distinct stages. There is a Discovery stage and a PPP Session stage. When a Host wishes to initiate a PPPoE session, it must first perform Discovery to identify the Ethernet MAC address of the peer and establish a PPPoE SESSION_ID. While PPP defines a peer-to-peer relationship, Discovery is inherently a client-server relationship. In the Discovery process, a Host (the client) discovers an Access Concentrator (the server). Based on the network topology, there may be more than one Access Concentrator that the Host can communicate with. The Discovery stage allows the Host to discover all Access Concentrators and then select one. When Discovery completes successfully, both the Host and the selected Access Concentrator have the information they will use to build their point-to-point connection over Ethernet.

Unnumbered Interfaces:
Point-to-point links are like pipes – any traffic sent through one end will be received at the other end. So the IP Addresses of interfaces at either end of the point-to-point link can be of local significance. The PPPoE interface at the router can be configured as an unnumbered interface. In this case, the unnumbered interface can borrow the LAN IP Address, and does not require a Global IP Addresses to be assigned by the ISP.

Select **Interface → WAN1** and choose **IP Setting Mode** as **PPPoE**. Configure **PPPoE Settings for WAN1 Interface** as explained below.

Web UI	PPPoE Settings for WAN1 Interface
Unnumber Interface	Select the option to enable unnumbered mode. When this option is not selected the router obtains an IP address from the ISP for the PPPoE connection. Ensure that both ends of the PPPoE link are configured as unnumbered.
IP Address	Enter the local IP address for the PPPoE connection when Unnumbered mode is enabled. An unnumbered interface borrows the LAN IP address by default. The administrator can edit this and configure a custom IP address on the unnumbered interface. The subnet mask for an unnumbered interface is always 255.255.255.255.
User Name	Enter the PPPoE username.
Password	Enter the PPPoE password.
Authentication Type	Select the authentication protocol (**PAP, CHAP or PAP-CHAP**) to be used for authentication with the PPPoE server.
Service Name (optional)	Enter the service name provided by the ISP.
Host Name (optional)	Enter the host name of the PPPoE connection.
MTU	Enter the MTU allowed for the PPPoE connect (preferred value 1492).
LCP Echo	Select this option to enable/disable Link Control Protocol (LCP). This is used to detect PPPoE Link Failures.
Interval (sec)	Enter the time interval to send LCP Echo request from PPPoE client to PPPoE server. The minimum value of this Interval is 10 seconds and the maximum value is 90 seconds.
Maximum Failures	Enter the number of Maximum Failures for the PPPoE connection. This is the number of times for which LCP Echo requests from PPPoE client did not get response from PPPoE server. After the number of failures cross this value, the PPPoE session is disconnected. The minimum value for failure is 2 seconds and maximum value is 10 seconds.

After entering all the information press the **Apply** button and the **PPPoE Status** is displayed at the bottom of the screen. The administrator may **Connect or Disconnect** using the appropriate button.

Caution: *When NAT is enabled on an unnumbered interface, local services (such as DNS Proxy, VPN etc) may be affected. To overcome this problem, configure one of the Global IP addresses from the NAT pool as the unnumbered interface's IP address.*

DHCP, DNS and Time

3.1 DHCP

DHCP (Dynamic Host Configuration Protocol) is a method of automatically assigning IP address, subnet mask, default gateway and DNS server IP address to hosts on the LAN. This router provides an in-built DHCP Server. In addition, a DHCP Relay is available to relay the DHCP Requests to a DHCP Server on another port.

3.1.1 DHCP Server

The DHCP server assigns and manages IP addresses from a specified address pool to DHCP clients. When a DHCP server receives a request from a DHCP client, it returns the configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a unicast message format. Because the DHCP server maintains all the configurations parameters, an administrator only needs to update the central DHCP Server when any configuration parameter is to be changed.

Compared to the static assignment where the client owns the address, dynamic addressing by the DHCP server leases the address to each client for a defined period of time. During the life cycle of the lease, the client is guaranteed to have a unique IP address that can last for the entire period. If the client needs to renew the lease from the server it can do so before the expiration of the lease. The client may also decide at any time that it no longer wishes to use the IP address it was assigned, and may terminate the lease by releasing the IP address. The administrator can configure this lease time in the DHCP server.

Note: *The DHCP Server can assign up to 253 IP Addresses to the LAN Clients. For example, if the router IP address is 192.168.100.254, the DHCP Server can assign IP Addresses from 192.168.100.1 to 192.168.100.253. Please note that the addresses ending in 0 and 255 are reserved for other uses.*

Select **Misc → DHCP → DHCP Server** to configure **DHCP Server** as explained below.

Web UI	DHCP Server
DHCP Server Status	Select Enable or Disable option to activate or deactivate the DHCP Server feature on the router (default value is Enable).
Starting IP address	Enter the starting IP address from the range of IP address assigned to the DHCP Server.
Ending IP address	Enter the ending IP address from the range of IP address assigned to the DHCP Server.

Default Gateway	Enter the default gateway IP address that the router will assign to the hosts on the network.
Lease Time (sec)	Enter the length of time any host on the network can keep its DHCP settings assigned by the router. If the lease expires while the host is logged on, then that host will request for a new set of DHCP settings. The default Lease Time is 60 seconds.
Auto Configuration	Select Enable to enable the DNS Proxy in the router (the router acts as a DNS server). In this case, the router gets the DNS IP manually or from ISP. When Disable is selected, the network settings entered by the administrator will be assigned to hosts on the network. In this case the DNS server IP addresses should be specified.
Domain Name	Enter a domain name the router can assign to hosts on the network. This suffix will then be automatically added to URL requests for access to your ISP's servers.
Primary DNS Server	Enter the IP address of a DNS server on the Internet that provides the service of converting text URLs into IP address for sites on the Internet.
Secondary DNS Server (optional)	Enter the IP address of a secondary DNS server that is be used when there is a problem with the Primary DNS Server. Select the Disable checkbox to disable Secondary DNS.

After entering all the information press the **Apply** button. The **DHCP Client Table** will list the client hosts (to which IP addresses have been assigned) with their Host Name, IP Address, MAC Address, and Lease Time values.

Any IP address in the DHCP server range may be assigned as a static IP to some PC in the network. When DHCP Server tries to assign this IP address to another client, the client will send a DECLINE message to the server. This is shown in the DHCP Client Table as **DECLINED** in host name, with MAC Address of zero and lease time of one hour.

3.1.2 DHCP Static Mapping

DHCP Static Mapping (or DHCP Reservation) is a method of assigning static IP address to a defined MAC Address. System administrators can use this feature to configure a static IP address for some of the systems in the LAN. These IP addresses however need to fall within the DHCP server configured IP Address Range.

Select **Misc → DHCP → Static Mapping** to configure **DHCP Static Mapping** as explained below.

Web UI	**DHCP Static Mapping**
MAC Address	Enter the MAC Address of the system.

IP Address	Enter the IP address to be assigned to the system with the above MAC Address.

After entering all the information press the **Apply** button. The entries will now be displayed under the **DHCP Static Mapping Client Table**.

If the Static IP in the DHCP Reservation entry does not fall within the DHCP Server IP Range, then it will be treated as an invalid entry. These invalid entries will be displayed in **dark grey** color in the DHCP Static Mapping Client Table.

3.1.3 DHCP Relay

In DHCP implementations, the DHCP clients send requests to locate the DHCP server by broadcast messages. Since broadcast messages are normally limited to the local network, the DHCP server and client always need to be in the same physical network. In large networks, a server needs to exist on every LAN, which is not economical or easy to maintain. DHCP relay solves this problem.

A DHCP relay acts as an intermediary between the client in the local network and the remote DHCP server. It intercepts requests from clients and relays them to the server. The server then responds back to the relay, which then forwards the response back to the client.

This relay-agent functionality is most conveniently located in the router which interconnects the clients and servers, but may alternatively be located in a host which is directly connected to the client subnet.

Caution: *Both DHCP Server and DHCP Relay cannot be enabled in the router simultaneously. When DHCP Relay is enabled, the Server will be disabled automatically. And when DHCP Server is enabled, the Relay will be disabled.*

Select **Misc → DHCP → DHCP Relay** to configure **DHCP Relay** as explained below.

Web UI	**DHCP Relay**
Relay-Status	Select Enable or Disable to activate or deactivate the DHCP Relay.
DHCP Server IP	Enter the IP address of the DHCP Server from which LAN clients will get their IP address.

Note: *In Relay mode, the DHCP server may unicast the DHCP ACK message to the DHCP Client. So proper routes should be configured at the server to enable it to reach the DHCP Client subnet.*

3.2 DNS Proxy

DNS (Domain Name System) is the protocol used to translate Domain Names to IP Addresses. DNS is an essential component of internet use, since it allows you to attach easy-to-remember domain names (such as www.dlink.com) to hard-to-remember IP Addresses. The DNS Servers maintain the database of Domain Name to IP Address mappings. All user systems (PCs) contain a DNS Client which communicates with the DNS Server to resolve any Domain Name.

With multiple WAN links, each ISP may provide a different set of DNS Servers to be used. And it is a cumbersome task to configure all the user PCs with the correct DNS Server IP Addresses. This problem can be overcome with the use of router's DNS Proxy feature. Here, the router's LAN IP Address can be configured as the DNS server at all the end user systems. The router acts as a DNS Proxy, and communicates with the DNS Servers to resolve the domain names on behalf of the user systems.

Select **Misc → DNS Proxy** to configure **DNS Proxy Settings** as explained below.

Web UI	DNS Proxy Settings
DNS Server IP	Enter the IP address of the DNS Server provided by the ISP.
Interface	Select the Interface corresponding to the DNS Server IP address entered. If two or more interfaces have the same DNS Server, select the interface type as DEFAULT. The interface with DEFAULT type will have the highest priority.

After entering all the information press the **Apply** button. The DNS server configuration entries will show up in a table at the bottom of the page. To delete any entry press the **Delete** button next to the entry.

Note: *In the DHCP Server Setting page, Enable the* ***Auto Configuration*** *for computers on the user's network to use the DNS Proxy.*

3.3 Time

The system date and time of the router can be configured via this option. The system date and time can be configured manually, or it can be obtained automatically from a global time server using NTP.

NTP is designed to synchronize the time on a network of machines. NTP runs over the User Datagram Protocol (UDP), using port 123 as both the source and destination port. NTP Version 3 RFC 1305 is used to synchronize timekeeping among a set of distributed time servers and clients.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP Protocol is then used to distribute this time across the network. An NTP client makes a transaction with its server over its polling interval (from 64 to 1024 seconds) which dynamically changes over time depending on the network conditions between the NTP server and the client.

The list of public NTP servers is available at http://www.ntp.org.

Select **Misc → Time** to configure **System Time Settings** as explained below.

Web UI	System Time Settings
System Date Time	The current date and time at the router.
Time Zone	Select the appropriate time zone that can be used to set the system time. Administrator can select any one of the time zone to which he belongs.
Time Set Type	Select either MANUAL or SNTP setting.
SNTP Settings	
Set Type	Select either IP address or Domain Name to be used for SNTP Setting.
IP address	The IP address of the NTP Server.
Domain Name	The domain name of the NTP Server e.g. ntp1.dlink.com.
Manual Settings	
YYYY-MM-DD	Manually set the current year, month and date.
HH-MM-SS	Manually set the hour, minute and seconds.

Routing

Routing determines how to transport packets from the initiating host to the receiving host. The packet needs to determine a path through which it can travel from the sender to the receiver. The *Routing Table* in a router provides such a map to all packets. Each entry (or route) in the routing table indicates the destination address of the packet, where the next hop (or gateway) should be, which interface of the router the packet should go out to reach the destination, and hence provides a path selection. When a packet arrives at a router, it looks up the routing table to decide which path to take next. The router compares the destination address of the packet with the entries in the routing table, and finds out the associated interface and next hop from the matching route to forward the packet.

As the networks grow large and complex, the entire domain of routing can be divided into sub areas to provide better functionality and control. This routing hierarchy divides all the routers in the network into administrative regions called the *Autonomous System* (AS). Routers inside AS (i.e. intra-AS routers) run the same routing algorithm and only need to know the topology of their network. RIP and OSPF are examples of intra-AS routing algorithms. These algorithms are also referred to as Interior Gateway Routing Protocols. This router supports *RIP routing algorithm.*

In the internetworking environment there are typically more than one path connecting the two end hosts. The dynamic routing algorithm selects the “best” path that has the “least cost” for transporting. RIP uses *Path Length* routing metric to determine the best path. Path length is the sum of the costs associated with each link. Path Length is commonly known as the hop count, or the number of routing devices (i.e. routers) that a packet takes to travel from the source to its destination. The cost of a link may be determined based on the below parameters:

• *Bandwidth* – Bandwidth is the traffic capacity of a path, rated by “Mbps”.

• *Load* – Load refers to the usage of a router. The usage can be evaluated by CPU utilization and the throughput.

• *Delay* – Delay is the time it takes to move a packet from the source to the destination. The time depends on many factors, such as the bandwidth, load, and the length of the path.

In case of a device or a link failure, the router looses its “best” route (associated with that link) and relies on the routing algorithm to select the next best route available in the routing table. This is a continuous process to keep the internetworking functional and help the router select the correct path at all times.

4.1 Static Routing

When Static Routing is selected as the routing algorithm, the network administrator needs to manually configure all routes on the router. Any change in the network configuration would require the administrator to update the information in all affected routers. This can be a cumbersome task and lead to errors in case of large and complicated networks. Hence Static routing is typically used for very small networks.

Select **Routing → Static** to configure **Static Routing** as explained below.

Web UI	Static Routing
Interface Name	Select the interface name (e.g. LAN, WAN1, WAN2) on which route is to be added.
Destination Network IP address	Enter the destination network IP address for which route is to be added.
Subnet Mask	Enter the subnet mask for the destination network IP address.
Gateway IP address (optional)	Enter the Gateway IP address for the route.

After entering all the information press the **Apply** button. The routes entered will now be displayed under the **Route Entries** table. To delete a specific route press the **Delete** button next to the specific route entry. In the table, entries with **yellow** color are active routes (i.e. the corresponding interface is UP). The entries with **grey** color are inactive routes (i.e. the corresponding interface is DOWN).

Click on View Active Routes, to view the Routing Table with the active routes.

Note: *The Gateway IP Address for a static route should be disabled only in case of PPPoE WAN Link. In all other cases, the Gateway IP Address is mandatory to ensure proper ARP Resolution.*

4.2 Dynamic Routing

Unlike Static routing, Dynamic routing adapts to changes in the network topology. It automatically learns the routes from all the neighboring routers, selects the most suitable route to a destination and then spreads the routing information through periodic updates to all the other routers in the network. The routing updates due to device or link down (or up) are sent immediately to all routers in the network. The administrator does not need to manually update any information. There are also mechanisms of self-correction to avoid

other network configuration problems like routing loop. In the Internet, there are two types of dynamic routing algorithms used – Distance vector and Link State algorithm.

In the Distance Vector (DV) algorithm, each router computes the costs of its own attached links and shares the route information with its neighbor routers. The router gradually learns the least-cost path by iterative computation and knowledge exchange with its neighbors. The least-cost path in this algorithm is determined by the number of intermediate routers i.e. the hop-count. The path with the least hop-count is chosen as the best route. When the hop count reaches the maximum value of 16, the route is dropped from the table.

Routing Information Protocol (RIP) is one of the most common Distance Vector algorithms used. In case of RIP each router sends a periodic update every 30 seconds to its neighbor. When a router receives the updates from its neighbor, it first updates the entire routing table (choosing the best routes) and then sends the entire table to all the neighbors.

This router supports both versions of RIP - RIP V1 and RIP V2.

- **RIP V1:** Uses only classful routing, which means that all devices in the network must use the same subnet mask. This is because RIP version 1 does not include the subnet mask when it sends updates. RIP V1 broadcasts its routing updates.
- **RIP-V2:** Uses classless routing. RIP v2 uses multicast (224.0.0.9) to update its routing tables. For backward compatibility with RIP V1, RIP V2 messages must be broadcast instead of multicast.

Select **Routing → Dynamic** to configure **RIP Settings** as explained below.

Web UI	RIP Settings
Routing Protocol	Select **RIP** to configure dynamic routing.
RIP Version	Select **RIP2** or **RIP1**.
Redistribute	Static or Connected Routes can be redistributed into RIP table, so that these routes are also sent with the route updates.
RIP Daemon	Select Start or Stop to activate or deactivate the RIP daemon.
Enable	Select Enable to activate RIP on the corresponding interface.
Send Version	Select the RIP version to use. The interface can use the global default RIP version to send RIP messages or select a specific RIP version to use.
Receive Version	Select the RIP version to use. The interface can use the global default RIP version to receive RIP messages or select a specific RIP version to use.
V2 Broadcast	Select V2 Broadcast option, when the send RIP version for an interface is set to use RIP 2, to broadcast RIP 2 messages instead of the default multicast behavior.

4.3 Routing Table

The router maintains all the active route entries, and displays them in the Routing table. The static routes configured manually by the administrator are displayed in **grey** color. And the dynamic routes learnt via RIP are displayed in **yellow** color.

Select **Status → Route Table** to view the **Routing Table** as explained below.

Web UI	Routing Table
Destination IP address	The destination network reachable through this route.
Subnet Mask	The subnet mask for this route. When there are multiple routes to the same destination, the route with the longest subnet mask will be given preference.
Gateway IP address	This is the next hop router's IP Address to which packets matching this route will be forwarded.
Interface	This is the interface on which the route is active

4.4 Policy Based Routing

Policy Based Routing (PBR) is an extension of normal routing, which offers network administrators significant flexibility to implement their own custom policies for making routing decisions. Typically, Static/Dynamic routing defines routes based on the destination IP Address of the packet. With PBR, the administrator has more control to choose a specific path for certain traffic flows based on various criteria, such as source/destination IP Addresses, Ports and Protocol.

Policy-based routing helps to define custom policies for routing traffic. For example, policy can be defined to route all HTTP traffic through WAN1 and E-mail traffic through WAN2. These policies help to achieve efficient traffic distribution. A set of parameters (e.g. source IP address, destination IP address, inbound interface, protocol, source/destination ports) are used to identify and direct the traffic out of a specific outbound interface.

Select **Routing → Policy-Based** to configure **Policy Based Routing** as explained below.

Web UI	Policy Based Routing
Policy Based Routing	Select Enable to activate Policy based routing in the router.

Outbound Interface	The network traffic which matches with all the below policy parameters will be sent out of this interface.
Policy Parameters	
Inbound Interface	Select the interface through which the incoming traffic will come in.
Source	Select the source IP address of the traffic. Select Any when there is no specific source IP address. However if Specific is selected the administrator will be allowed to configure specific source IP address for this policy.
Destination	Select the destination IP address of the traffic. Select Any when there is no specific destination IP address. However if Specific is selected the administrator will be allowed to configure specific destination IP address for this policy.
Protocol	Select a protocol for the policy.
Source Port Number (optional)	Enter the Source Port Number to specify the type of application for this policy. Source port value of zero indicates "Any" Source Port.
Destination Port Number (optional)	Enter the Destination Port Number to specify the type of application for this policy. Destination port value of zero indicates "Any" Destination Port.

After entering all the information press the **Apply** button. The routes entered will now be displayed under the **Policy Based Routing Table.**

***Note**: Policy Based Routes will be given higher preference over Static/Dynamic routes to the same destination.*

High Availability

The *High Availability* support in the router is an ideal solution for businesses requiring uninterrupted, low cost internet connectivity. The router supports *Dual Ethernet WAN Ports for xDSL connectivity*. Though xDSL connectivity is cheap, it is more susceptible to outages. Hence with two xDSL links, DRO-210i guarantees uninterrupted internet connectivity.

High Availability is made possible through two key features in the router - Auto Backup and Load Balancing.

5.1 Auto Backup

The *Auto Backup* feature enables one of the WAN links to function as the Primary WAN Link, and the other as the Backup Link. When the Primary Link fails, the Backup Link will become operational and traffic will switchover to this link. And when the Primary Link becomes serviceable, the traffic will automatically switchback to the Primary Link.

Select **Interface → AutoBackup** to configure the **Backup Configuration** as explained below.

Web UI	Backup Configuration
Primary	The primary interface for which Auto Backup functionality can be configured.
Backup-Mode	If Enabled, the configured backup interface will be connected automatically when the Primary interface goes down.
Backup Interface	This interface will be configured as backup interface for the primary and cannot be the primary interface at any time.

When the Primary Link fails, all configurations (other than VPN and SIP-ALG) made for the Backup Interface will become active. That is, the connection type for the WAN interface, Static Routes configured on this interface, NAT configured on this interface etc. will be automatically activated on the backup interface. And when the Primary Link becomes UP, the configurations on the Backup interface will be disabled and the configurations on the Primary Interface will be made active. This switchover and switchback will occur automatically without need for user intervention.

5.2 Load Balancing

With multiple Internet connections, Load Balancing effectively uses the combined bandwidth of all the internet links resulting in a significant increase in the total available bandwidth. Also if any Internet connection goes down, uninterrupted internet connectivity is assured utilizing the serviceable links.

Based on the speed of the WAN link, the administrator can configure an appropriate percentage of internet traffic to be routed through each of the WAN Links.

Note: *The priority of route lookups is in the following order:*

a) Policy Based Routing (PBR) routes
b) Static/Dynamic routes
c) Load Balancing routes

Select **Interface → LoadBalancing** to configure the **Load Balancing Configuration** as explained below.

Web UI	Load Balancing Configuration
Load Balancing	Select to enable the load-balancing feature.
Interface	WAN interfaces between which the load must be shared.
Status	Enable/Disable load-balancing on this interface.
Weight	Percentage of the load to be sent through this interface. The sum of the weights in all enabled interfaces should be equal to 100.

Caution: *Load Balancing feature will not function as desired if default routes are added via Static Routing, since static routes will be given higher preference.*

5.3 Ethernet Link Detection

In case of Ethernet WAN Connectivity (Static and Dynamic Modes) there is no specific control protocol to detect the link status. **Ethernet WAN Link Detection** Feature in the router enables you to detect link failures through periodic transmission of ICMP/ARP messages.

Note: *When using Static/Dynamic mode of WAN Interfaces, it is imperative to enable Ethernet Link Detection for proper functionality of Load Balancing and Auto Backup features.*

Select **Interface → WAN1** and choose **IP Setting Mode** as **Static** or **Dynamic**. Click on **Detect Link Status** to configure the **Ethernet WAN Link Detection** as explained below.

Web UI	Ethernet WAN Link Detection
Interface	The WAN interface on which link detection is to be performed.
Link Detection	Select to enable Link Detection on this Interface.
Mode	Select protocol (ARP or ICMP) used to detect reachability of the default gateway IP address. If the default gateway is reachable, then the Protocol Status of the Interface will be UP, otherwise it will be DOWN.
No of Retries	Enter the number of attempts to reach the default gateway, before confirming the status (UP/DOWN) of the link.
Delay between Retries	Enter the time in seconds between retry attempts.

After entering all the information press the **Apply** button. The **Ethernet WAN Status Table** will display the list of interfaces on which Link Detection is enabled and their status.

Network Address Translation

When a computer wants to connect to the Internet, it needs a legal and unique Global IP address to traverse the internet. With the explosion of Internet, the unique IP address space available is insufficient. NAT solves this problem by allocating single or a small range of legal Global IP addresses. A NAT router translates the **unregistered local (or Private) IP addresses** to the **registered global (or Public) Internet IP addresses**.

NAT allows hosts within a private network to transparently access hosts in the external network. The NAT sessions are unidirectional, outbound from the private network. NAT does not advertise private network addresses to the external network, hence preventing direct access to the enterprises' private network from the internet. So in addition to solving the addressing problem, NAT also acts as a ***security agent***.

The router provides ***ALG (Application Level Gateway) support*** for common applications to enable smooth operation behind NAT. The ALG Support involves:

- Allowing client applications to use dynamic ephemeral TCP/ UDP ports to communicate with the server applications, even though firewall may allow only a limited number of known ports. In the absence of an ALG, either the ports would get blocked or the network administrator would need to explicitly open up a large number of ports in the firewall — rendering the network vulnerable to attacks on those ports.
- Converting the network layer address information found inside an application payload to addresses acceptable by the hosts on either side of the firewall/NAT.

6.1 NAT

6.1.1 NAT Interface Configuration

NAT can be enabled or disabled on a specific interface. Typically NAT must be enabled at the WAN interface used for internet connectivity.

Select **NAT → Interface Configuration** to configure the **NAT Interface Configuration** as explained below.

Web UI	NAT Interface Configuration
Interface Name	The interface on which NAT can be enabled/disabled.
Status	Select Enable to activate NAT on the corresponding interface.

Press the **Apply** button.

6.1.2 NAT Configuration

This router supports the following types of NAT:

- **Many-To-One** - In this case, multiple private IP addresses are mapped to one Global IP address by using different ports.
- **Many-To-Many** - In this case, multiple private IP addresses are mapped to a pool of Global IP addresses.
- **One-To-One** - In this case, one private IP address is mapped to one global IP address. This type of NAT is used to enable internal servers (e.g. Web servers) to be accessible from the Internet.

Select **NAT → NAT Configuration** to configure the **NAT Configuration** as explained below.

Web UI	NAT Configuration
NAT	Enable/Disable this NAT Configuration Entry.
WAN Interface	Select the WAN interface.
NAT Type	Select the type of NAT (One to One, Many to One or Many to Many).
Private IP address	
Start Address	This can be configured only in case of One-to-One NAT. Enter the starting IP address for the range of Private IP Addresses.
End Address	This can be configured only in case of One-to-One NAT. Enter the ending IP address for the range of Private IP Addresses. In case of a single IP, configure the same IP in both the Start and End fields.
Global IP address	
On This Interface	Select this checkbox to automatically use the WAN Interface's IP Address as the Global IP address.
Start Address	Enter the starting IP address for the range of Global IP Addresses.
End Address	Enter the ending IP address for the range of Global IP Addresses. In case of a single IP, configure the same IP in both the Start and End fields.

After entering all the information press the **Apply** button. The **NAT Configuration Table** will now be displayed at the bottom. The NAT configuration entry can be enabled or disabled by clicking the **View** button. The NAT configuration entry can be deleted by using the **Delete** button.

6.1.3 NAT Exception

NAT can be disabled between two interfaces using NAT Exception.

Consider a scenario where WAN1 is used for internet connectivity. NAT must be enabled at WAN1 to enable LAN systems to access the internet. The company's servers (Web/FTP Server) may be installed at the DMZ interface using public IP Address for direct access from the internet. NAT should not affect the traffic between DMZ and WAN1, because DMZ systems are already using public/global IP Addresses. In this case, NAT can be disabled between DMZ and WAN1.

Say WAN2 Port is used to connect some PCs or IP Phones with global IP Addresses. In this case, NAT is required only for traffic between LAN and WAN1. NAT can be disabled between WAN2 and WAN1 since WAN2 systems already use global IP Addresses.

Select **NAT → NAT Exception** to configure the **NAT Exception** as explained below.

Web UI	NAT Exception
NAT between WAN1 and WAN2	Select Disable to deactivate NAT between WAN1 and WAN2.
NAT between WAN1 and DMZ	Select Disable to deactivate NAT between WAN1 and DMZ.
NAT between WAN2 and DMZ	Select Disable to deactivate NAT between WAN2 and DMZ.

6.2 Virtual Server

Virtual Servers use NAPT (Network Address and Port Translation) to allow remote users access certain special services on the LAN, such as FTP server for file transfer and STMP or POP3 for e-mail. The administrator configures the Global IP address, TCP or UDP protocol and port number used to access the Server. The router redirects requests from the remote clients to the Internal Server running the specified service on the LAN, by translating the Global IP/Port to the Private IP/Port of the end server.

Select **NAT → Virtual Server/NAPT** to configure the **Virtual Server/NAPT** as explained below.

Web UI	Virtual Server/NAPT
Interface Name	Select the interface on which the virtual server is to be configured.
Transport Type	Select the transport protocol (TCP or UDP) that the application on the virtual server will use for its connections. The transport type is dependent on the application that is providing the service. This is mostly used for non-standard cases where the port numbers are defined by the administrator.

Protocol	Select the appropriate application from the list. This selection is equivalent to entering a correct transport type (TCP or UDP) and port number for an application. For example, when SMTP is chosen transport type TCP and port number 25 is automatically entered.
Private Settings	
IP address	Enter the private IP address of the server that will provide the service to remote users.
Port	Enter the private port number on which the server is running.
Global Settings	
IP address	Enter the global IP address of the server. External world sees this global IP address specified by the administrator.
Port	Enter the application port number (global) that is providing the service.

After entering all the information press the **Apply** button and the **Virtual Server** table will now be displayed at the bottom. Each entry can be deleted by selecting the **Delete** button next to the entry.

6.3 SIP-ALG

Session Initiation Protocol (SIP) packets have IP address embedded in the data packet. So NAT is not fully effective for such applications. SIP ALG enables SIP phones on the LAN side to make calls across the Internet when NAT is enabled.

The administrator needs to configure the port numbers used for SIP by the IP Phone or the SIP Server. A maximum of 20 SIP calls can be active simultaneously.

Caution: *If router reboots, SIP Phones need to be reregistered with the external SIP Server. This is because the router does not remember the earlier SIP Registrations on reboot.*

Select **NAT → SIP-ALG** to configure the **SIP ALG Configuration** as explained below.

Web UI	**SIP ALG Configuration**
Enable	Select **Enable** to activate the feature.
Port number	Enter the port number of the SIP Phone or SIP Server.

After entering all the information press the **Apply** button and the **SIP ALG Table** will now be displayed at the bottom. To delete an entry press the **Delete** button next to the entry.

6.4 NAT Table

The router maintains a table of sessions for which IP Address and Port Translations have been performed. This translation table can be viewed from the *NAT Table* Page.

Select **Status → NAT Table** to view the **NAT Session Table** explained below.

Web UI	NAT Session Table
Private IP address: Port	This is the IP address and port number of a host on the private LAN that has an active NAT session.
Peer IP address: Port	This is the IP address and port number of a host on the WAN that has an active connection with the router.
Mapped IP address: Port	This is the IP address and port number that will be seen by the devices on the WAN side for the corresponding private IP address and port.

Firewall

Firewall is a set of security rules that prevents intruders from gaining access to confidential and sensitive information. Its task is to ensure that only approved communication happens and unauthorized communication is blocked and logged.

The primary purpose of a firewall is to enforce a security policy stating who can communicate, with whom and in what way. The firewall accomplishes this task by examining the traffic that passes through it, comparing each packet against a set of rules programmed into it. It makes a decision based on factors such as sender address, destination address, protocol and ports. This allows businesses to use less secure applications on the protected networks and prevent all outsiders from ever gaining access to these services.

Most firewalls, including D-Link firewalls, ensure that network traffic complies with current protocol definitions. This can prevent poorly implemented services on the protected servers and client software from being exposed to unexpected data, causing them to hang or crash. In short, a firewall is the network's answer to poor host security.

7.1 Firewall Policies

7.1.1 Interface Configuration

Select **Firewall → Interface Configuration** to configure the **Firewall Interface Configuration** as explained below.

Web UI	Firewall Interface Configuration
Firewall	Select **Enable** to activate firewall feature.
Interface Name	Interface for which firewall is to be configured.
Status	Firewall can be **Enabled** or **Disabled** on a particular Interface.
Security Type	Select **Trusted** or **UnTrusted**. If the security type is set to **Trusted** then **Outbound** Policies will be applied on that interface. If the security type is set to **UnTrusted** then **Inbound** Policies will be applied on that interface.

Typically, LAN is configured as a **Trusted** Interface and WAN is configured as **UnTrusted** Interface.

Note: *If more than one interface is of same security type, then Policy database for them is same i.e if WAN1 and WAN2 are configured as* ***UnTrusted*** *then both of them will share a common Inbound Policies database.*

Caution: *If LAN is configured as* ***UnTrusted****, then Remote Access needs to be configured for getting the web-configuration. So before configuring LAN as* ***UnTrusted****, first enter the IP of the LAN PC (which is configuring the DRO-210i) in the Remote access configuration webpage.*

7.1.2 Policy Rules

A policy is a rule that can be active on the router for certain period of time according to its configuration. These rules allow/deny traffic, ensuring that the network is less vulnerable to external attacks. The rules that are added for a policy, take effect only when corresponding policy is active i.e. the administrator can activate different policies at different times by specifying the time.

Select **Firewall → Policy** to configure the **Policy Rules** as explained below.

Web UI	Policy Rules
System Date Time	Shows the current system time.
Policy Name	Alphanumeric name representing the Policy. All the policies should have a unique name.
Schedule	Select the schedule type (**Always** or **One-Time). Always** means always active. **One-Time** policy is active for certain configured period and becomes inactive after that. This Start Time and End Time fields below are applicable for One-Time Policy only. The format of time is Month: Day: Hr: Min.
Start Time	Enter the starting time of the policy.
End Time	Enter the ending time of the policy.
Status	Select E**nable** or **Disable** to activate or deactivate the policy.

After entering all the information press the **Apply** button and the **Policy Table** (shows the active period of the policy) will now be displayed at the bottom of the page. The Firewall policy configuration entry can be viewed by pressing the **View** button and can be deleted by using the **Delete** button.

Note: *An* ***Always*** *Policy exists by default with the name* ***"Default"****. This Policy cannot be disabled or deleted.*

Note: *When an active policy is disabled or deleted, another enabled policy will become active. In this case, currently ongoing sessions will no longer function if they are not permitted by the new active policy.*

7.1.3 Inbound Policies

The traffic flowing from UnTrusted to Trusted network is the Inbound traffic. By default, all network traffic going from UnTrusted network to Trusted network are blocked. Port Filter rules can be added to allow specific traffic.

Select **Firewall → Policy** to get to the **Policy Table**, and click **In** button to configure **Inbound Policies**.

Web UI	**Inbound Policies**
Port Filter	
Enabled	Select Enable to activate Inbound Port Filter. Port Filter is used to allow network packets coming from the untrusted domain. Configured inbound port filters will not take effect if this field is disabled.
Deny all services to be accessed except "Permitted Service"	Click on "Permitted Service" to configure the port filter rules.

Note: *Some old eMail and FTP Servers use IDENT protocol to automatically identify the users connecting to them. By default, the firewall in the router will block the incoming IDENT protocol at an **UnTrusted** port. This will cause eMail and FTP access to these servers to slow down. To avoid this problem, Port 113 should be opened explicitly in inbound firewall policy at the router.*

Permitted Services

Click on the link **"Permitted Services"** to get to **Permitted Services** configuration page. This page allows administrator to configure the application to be allowed from UnTrusted network to the Trusted network.

Web UI	**Inbound Policies (Permitted Services)**
Add Service Rules	
Transport Type	Select from the drop-down menu a transport type to be allowed by the router.

Protocol	Select from this drop-down menu the application. This is the equivalent of entering the correct Transport Type and the port number corresponding to a given application.
Port Range	Enter the range of port numbers for which the current policy rules will be applied. If you have only one port number to enter, enter it in both fields.
Direction	This is the direction (**Inbound)** of network traffic for which the current policy entry will be applied.

After entering all the information press the **Apply** button and the **Service Permitted Rule** table will now be displayed at the bottom of the page. Press the **Delete** button to delete the corresponding entry.

IP Permitted Rules

In **Service Permitted Rule** table, click the icon under **IP Permitted Rule** column to configure **Permitted IP Rules**.

Web UI	**Add Permitted IP Rule**
Service	Displays the Protocol and Port for which Permitted IP Rule is being configured.
Source IP	Select **Any** or **IP Range**. If **IP Range** is selected, the administrator can specify a range of IP addresses that the IP filter policy will be applied to. If you have only one IP address that you want to filter, enter this address in both the From and To fields.
Destination IP	Select **Any** or **IP Range**. If **IP Range** is selected, the administrator can specify a range of IP addresses that the IP filter policy will be applied to. If you have only one IP address that you want to filter, enter this address in both the From and To fields.
Status	Select **Enable** or **Disable** to activate or deactivate the configured entry.

After entering all the information press the **Apply** button and the **Permitted IP Table** will now be displayed at the bottom of the page. Press **View** button for viewing and **Delete** button for deleting the corresponding entry.

7.1.4 Outbound Policies

The traffic flowing from Trusted to UnTrusted network is the Outbound traffic. By default, all network traffic which flows from Trusted network to UnTrusted network is allowed. Port Filter rules can be added to block specific traffic.

Select **Firewall → Policy** to get to the **Policy Table** and click **Out** button to configure **Outbound Policies**.

Web UI	Outbound Policies
Port Filter	
Enabled	Select Enable to activate Outbound Port Filter. Port Filter is used to deny network packets coming from the trusted domain. Configured outbound port filters will not take effect if this field is disabled.
Allow all WAN service to be accessed except "Blocked Service"	Click on "Blocked Service" to configure the port filter rules.
Domain Filter	
Enabled	Select Enable to activate domain filter
Allow all WAN Domain to be accessed except "Untrusted Domain"	Click "Untrusted Domain" to configure the domain names that are to be blocked.
Deny all WAN Domain to be accessed except "Trusted Domain"	Click "Trusted Domain" to configure the domain names that are to be allowed.
Web Filter	Select the type of web filter from the list (**Java Filter, Cookie Filter, ActiveX Filter, Keyword Filter, and File Extension Filter**).
Java Filter	Select to enable Java Filter on the packets coming out from firewall enabled Interface.
Cookie Filter	Select to enable Cookie Filter on the packets coming out from firewall enabled Interface.
ActiveX Filter	Select to enable ActiveX Filter on the packets coming out from firewall enabled Interface.
Keyword Filter	Select to enable Keyword Filter on the packets coming out from firewall enabled Interface. Click on "Keyword List" to configure the keywords to be blocked.
File Extension Filter	Select to enable File Extension Filter on the packets coming out from firewall enabled Interface. Click on "File Extension List" to configure the file extensions to be blocked.
MAC Filter	
Enabled	Select to enable MAC Filter on the packets coming from trusted Interface.
Allow all LAN MAC address to access Internet except "Blocked MAC"	Click "Blocked MAC" to configure the MAC Addresses to be blocked.

Blocked Services

Click on the link **"Blocked Services"** to get to **Blocked Services** configuration page. This page allows administrator to specify the application to be blocked from Trusted network to the UnTrusted network.

Web UI	Outbound Policies (Service Blocked Rule)
Add Service Rules	
Transport Type	Select from the drop-down menu a transport type to be blocked by the router.
Protocol	Select from this drop-down menu the application. This is the equivalent of entering the correct Transport Type and the port number corresponding to a given application.
Port Range	Enter the range of port numbers for which the current policy rules will be applied. If you have only one port number to enter, enter it in both fields.
Direction	This is the direction (**Outbound)** of network traffic for which the current policy entry will be applied.

After entering all the information press the **Apply** button and the **Service Blocked Rule** table will now be displayed at the bottom of the page. Press **Delete** button for deleting the corresponding entry.

IP Blocked Rules

In **Service Blocked Rule** table, click the icon under **IP Blocked Rule** column to configure **Blocked IP Rules**.

Web UI	Add Blocked IP Rule
Service	Displays the Protocol and Port for which Blocked IP Rule is being configured.
Source IP	Select **Any** or **IP Range**. If **IP Range** is selected, the administrator can specify a range of IP addresses that the IP filter policy will be applied to. If you have only one IP address that you want to filter, enter this address in both the From and To fields.
Destination IP	Select **Any** or **IP Range**. If **IP Range** is selected, the administrator can specify a range of IP addresses that the IP filter policy will be applied to. If you have only one IP address that you want to filter, enter this address in both the From and To fields.
Status	Select **Enable** or **Disable** to activate or deactivate the configured entry.

After entering all the information press the **Apply** button and the **Blocked IP Table** will now be displayed at the bottom of the page. Press **View** button for viewing and **Delete** button for deleting the corresponding entry.

7.1.5 Domain Filter

Domain Filter feature enables the administrator to block specific domain names (or) allow only specific domain names. This feature prevents DNS resolution for the blocked domain names.

Untrusted Domain

Here, the administrators can **Allow all WAN Domain** to be accessed **except Untrusted Domain**.

In **Outbound Policies**, select **Untrusted Domain** (under Domain Filter) to go to the **Outbound Policies (Untrusted Domain)** configuration page.

Web UI **Outbound Policies (Untrusted Domain)**

Add Untrusted Domain Rules	
Domain Name	Enter the domain names to which access should be denied.

After entering all the information press the **Apply** button and the status table will now be displayed at the bottom of the page. Press **View** button for viewing and **Delete** button for deleting the corresponding entry.

Trusted Domain

Here, the administrator can **Deny all WAN Domain** to be accessed **except Trusted Domain**.

In **Outbound Policies,** select **Trusted Domain** (under Domain Filter) to go to the **Outbound Policies (Trusted Domain)** configuration page.

Web UI **Outbound Policies (Trusted Domain)**

Add Trusted Domain	
Domain Name	Enter the domain names to which access should be permitted

After entering all the information press the **Apply** button and the status table will now be displayed at the bottom of the page. Press **View** button for viewing and **Delete** button for deleting the corresponding entry.

7.1.6 Web Filter

The different types of Web Filters in the firewall are

- Java Filter
- Cookie Filter
- ActiveX Filter
- Keyword Filter
- File extension Filter

Java Filter

Java at runtime could allow the attacker to run harmful code on the victim's computer. Java Plug-in enables small web programs such as applets to run on the user's computer. A malicious webpage can run a malicious code without the user's knowledge. By Enabling the Java Filter, such Java related attacks can be prevented.

Cookie Filter

Cookies are merely text files that are placed on a user's computer by Web sites that the user visits. Cookies can be used to gain information about the surfer. Cookies are not spyware. They cannot run Trojan horse or any other malicious code on the user's computer but can provide confidential information about users to others. By enabling the Cookie Filter, the user can prevent the Cookie based attacks.

ActiveX Filter

The name "ActiveX" is sometimes used as a synonym for COM (Component Object Model), and sometimes as a general term for Microsoft's component strategy. "ActiveX" specifically means the technology that downloads and runs controls in one of the formats supported by the "Authenticode" code signing system. This corresponds to controls that can be declared from a web page using an OBJECT tag, and currently includes:

- COM controls (file types .DLL and .OCX)
- Win32 executable files (file type .EXE)
- INF set-up files, used to specify locations and versions for a collection of other files (file type .INF)
- "cabinet" files that are referred to by an OBJECT tag (file type .CAB)

By enabling the ActiveX Filter, the attacks related to ActiveX can be prevented.

Keyword Filter

HTTP Packets with specific keywords (like jobs) in the URL can be blocked using the Keyword Filter.

In **Outbound Policies** select **Keyword List** (under Web Filter) to go to the **Keyword Filter** configuration page.

Web UI	Keyword Filter
Enter the Keyword	Enter the keywords to be matched.

After entering all the information press the **Apply** button and the status table will now be displayed at the bottom of the page. Press **Delete** button for deleting the corresponding entry.

Keyword Exception

If the administrator would like to block all job sites, he can add "jobs" in the Keyword Filter. However to permit access to a Dlink Job site (http://www.dlink.com/jobsatdlink), a keyword exception "jobsatdlink" can be added.

In Keyword Filter select Exceptions to go to the Keyword Exception configuration page.

Web UI	Keyword Exception
Enter the Exception Keyword	Enter the exception keyword which should not be blocked.

After entering all the information press the **Apply** button and the status table will now be displayed at the bottom of the page. Press **Delete** button for deleting the corresponding entry.

File Extension Filter

This feature can be used to block access to specific file extensions. For example, viruses spread through VB Script (.vbs), Executables (.exe) etc. To avoid the spread of virus through these files, HTTP access of these files can be blocked by their extensions.

In **Outbound Policies,** select **File Extension List** (under Web Filter) to go to the **File Extension Filter** configuration page.

Web UI	File Extension Filter
Enter the File Extension	The file extension to be blocked.

After entering all the information press the **Apply** button and the status table will now be displayed at the bottom of the page. Press **Delete** button for deleting the corresponding entry.

7.1.7 MAC Filter

MAC Filter feature can be used to block all traffic from a specific user's system. The user's system can be uniquely identified by its MAC Address.

In **Outbound Policies,** select **Blocked MAC** (under MAC Filter) to go to the **Blocked MAC Address** configuration page.

Web UI	Add Blocked MAC Address
MAC Address	MAC Address to be blocked
DHCP Client	The MAC Address to be blocked can also be chosen from the list of DHCP Clients.

After entering all the information press the **Apply** button and the status table will now be displayed at the bottom of the page. Press **Delete** button for deleting the corresponding entry.

7.1.8 Blocking Log

This list shows what traffic has been blocked by the Firewall Policy and the reason for blocking.

Select **Status → Log Tables → Blocking Log** to view the **Blocking Log Table** as explained below.

Web UI	Blocking Log Table
Blocking Time	Displays the time when the blocking happened.
Transport Type	Displays the transport type.
Source	Displays the source IP address that was blocked.
Destination	Displays the destination IP that was blocked.
Blocking Reason	Displays the reason why the packet was blocked.

7.2 Intrusion Detection

An Intrusion is a deliberate, unauthorized attempt to access or manipulate information or system and to render them unreliable or unusable. The security architecture that detects and prevents these types of intrusion is called *Intrusion Detection and Prevention System.*

Intrusion Detection Systems (IDS) detect unwanted access to devices on the private network mainly from the public Internet. The manipulations may take the form of attacks by skilled malicious hackers or by using automated tools. IDS detect all types of malicious network traffic and computer usage that can not be detected by a conventional firewall. So Intrusion Detection is an important technology for routers to identify and prevent these threats from affecting the devices on the network.

IDS and Firewall both are ways to enhance security in a networking environment but they function differently. Firewall limits the flow of packets between networks to prevent intrusion and do not look for a pattern that signifies an attack. An IDS detects a potential security breach, logs the information and signals an alert to the operator. It matches the packets against a 'signature'. A signature is a pattern observed in a previous intrusion attack by examining the network communications and identifying heuristics of that attack.

In order to make IDS effective and reliable, the router implements three levels of processing:

- **Intrusion Detection Rules:** An Intrusion Detection Rule defines the kind of traffic should be analyzed. Filtering fields regarding source and destination interfaces, networks, ports, and protocols are also defined here. Only traffic matching this rule is passed on to the next processing level of IDS, where actual analysis takes place.
- **Pattern Matching:** In order to correctly identify an attack, pre-defined patterns called "signatures", are created that describe certain attacks. The network traffic is then analyzed by the IDS, searching for these patterns. This is also known as "misuse detection" or "signature detection".
- **Action:** If an intrusion or attack has been detected, the router logs the attack and takes an action or response. Depending on the severity of the attack, traffic can be blacklisted to prevent further attacks, or just dropped.

7.2.1 IDS Configuration

Certain sessions between computers on your LAN and the WAN have the potential to cause a disruption the functioning of your LAN computers and are blocked by the Router's IDS Engine. The signatures for these attacks are pre-defined by the factory and are the commonly used intrusion methods. The IDS feature in this router can detect and block these well-known network attacks.

Select **Firewall → IDS Configuration** to configure the **IDS Configuration** as explained below.

Web UI	IDS Configuration
Enable IDS	Select Enable to activate the IDS.
Flood Attack	Select Enable to activate all types of flood attacks available on this router i.e. SYN flood attack, ICMP flood attack, ICMP Echo storm attack. In these attacks, packets are flooded continuously on the target machine.
Ping of Death	Select Enable to activate a form of DoS (denial of service) attack. This attack consists of flood of large-sized ping requests designed to disrupt the normal activity of a system.
Boink Attack	Select Enable to activate the Boink attack. It involves the perpetrator sending corrupt UDP packets to host.
Smurf Attack	Select Enable to activate Smurf attack. This is named after its exploit program and is the most recent network intrusions against hosts.
TCP SYN Attack	Select Enable to activate TCP attacks like SYN/ACK attack, FIN attack and RESET attack. These attacks exploit the three-way TCP handshaking.
Port scan Attack	Select Enable to activate the port scan attacks like Netbus scan, Back orifice scan, Echo chargen scan, UDP echo scan, Chargen scan, IMAP scan. All ports are scanned under this attack.
Land Attack	Select Enable to activate the Land attack. In this attack the perpetrator sends spoofed packet(s) with the SYN flag set to the victim's machine on any open port that is listening. If the packet contains the same source and destination IP address as the host, the victim's machine could hang or reboot.
Winnuke Attack	Select Enable to activate Denial of service attack. This attack sends OOB data to an established connection on port 139 (NetBIOS), to any windows user using 95/NT/3.x.
XMAS-Tree Attack	Select Enable to activate the XMAS Tree attack. This attack uses the DoS technique that sets all TCP header flags to 'ON' in an attempt to gain information regarding a network.
Ascend kill Attack	Select Enable to activate the Ascend Kill attack. This attack makes the remote Ascend router reboot by sending it a UDP packet containing special data on port 9(discard).

After entering all the information press the **Apply** button. The attacks are logged on the Intrusion Log. The IP address of the attacker is blacklisted to prevent any further attacks.

Note: *To ensure the highest level of security in a network, it is recommended to enable detection of all the attacks supported by the router.*

7.2.2 Intrusion Log

When traffic matches an Intrusion signature and is blocked by the IDS engine, the blocking event is recorded in the **Intrusion Detection Log**.

Select **Status → Log Tables → Intrusion Log** to view the **Intrusion Log Table** as explained below.

Web UI	Intrusion Log Table
Intrusion Time	Displays the time when the intrusion happened.
Intrusion Type	Displays a brief statement of the type of intrusion that was attempted. The router's firewall can detect following attacks - SYN Flooding , TCP Hijacking, LAND Attack, WinNuke/OOBNuke, Christmas Tree SYN / FIN (Jackal), SYN / FIN (zero-sized DNS zone payload), BackOffice, NetBus, Smurf, Tear Drop, ICMP Flooding.
Source: port	Displays the source IP address and the TCP/UDP port that the intrusion was attempted from.
Destination: port	Displays the destination IP address and the TCP/UDP port that the intrusion was attempted to.

7.2.3 Black List

This list shows the blacklist of intruders in the "Intruder Blacklist" which are automatically blocked as soon as they are detected.

Select **Status → Log Tables → Black List** to view the **Black List Table** as explained below.

Web UI	Black List Table
Source IP	Displays the source IP address that was blacklisted.
Destination IP	Displays the destination IP that was blacklisted.
Destination Port/Transport Type	Displays the destination port and transport type of the blacklisted packet.
Blocking Duration	Displays the time of blocking in seconds.

Press **Delete** button for unblock the corresponding entry.

Virtual Private Network

VPN or virtual private networks allow multiple sites from an organization (and its clients, suppliers, etc.) to communicate securely over an insecure internet by encrypting all communication between the sites.

IPSec protocol is the Internet standard protocol for tunneling, encryption and authentication. IPSec can be used to protect the path between a pair of security gateways (***Peer-To-Peer Mode***) or between a security gateway and a host (***IPSec Server Mode***).

IPSec is designed to protect the network traffic by addressing basic issues like:

- **Access control**: This is controlling the access to the remote host machines from the local hosts. This also involves local host access control, where the system administrators can control which local hosts can communicate to the remote hosts through the local IPSec gateways.
- **Data integrity**: This makes sure that the data that is transferred from one IPSec gateway to another IPSec gateway is not tampered (changed).
- **Authentication of IPSec peers**: This ensures that an IPSec peer is communicating with the proper remote IPSec peer. So it involves authenticating the remote IPSec peer.
- **Protection against replays**: An intermediate person between any two communicating IPSec peers can spoof the packet, tamper it and then repeatedly send it to any of those IPSec gateways, thus causing Denial – of – Service attack. So IPSec has the capability to prevent this attack.
- **Traffic Confidentiality**: This involves encrypting the data so that a third person cannot peek in through the data.

IPSec provides the securing services at IP layer, offering protection for IP and upper layer protocols. The security services are provided through the use of the following protocols

- Cryptographic key management procedures and protocols, including the **Internet Security Association and Key Management Protocol (ISAKMP)** and the **Internet Key Exchange protocol (IKE)**. In order to use IPSec, both the communicating peers need to have the same protocol, encryption algorithms and keys. IKE provides the mechanism for a pair of IPSec entities to negotiate security services and their associated session authentication and encryption keys.
- Security protocols such as the **Authentication Header (AH)** and the **Encapsulating Security Payload (ESP)**. The Authentication Header (AH) addresses data origin authentication, data integrity, and replay protection. The Encapsulating Security Payload (ESP) header has the same capabilities as AH in addition to data confidentiality and encryption. IPSec uses the AH by default. If data confidentiality is desired, ESP can be used, which has the additional encryption feature.

8.1 IPSec Tunnel or Passthrough

The IPSec VPN Feature can operate in 2 modes:

- **IPSec Passthrough:**
  In this mode, the router will allow IPSec-VPN tunnels to be established between multiple LAN side IPSec clients and multiple remote IPSec servers. It can also support multiple LAN side IPSec clients to connect simultaneously to a single remote IPSec server. But the administrator cannot establish tunnels from the router to remote IPSec peers.
- **IPSec Tunnel:**
  In this mode, the administrator can establish tunnels from the router to remote IPSec peers. However, IPSec Passthrough functionality will not be available in this mode.

Note: *The router can operate in only one of the modes at a time - either IPSec Passthrough mode or IPSec Tunnel mode.*

Select **VPN → VPN-IPSec** to configure the **VPN IPSec Configurations** as explained below.

Web UI **VPN IPSec Configurations**

IPSec Passthrough	Select **Enable** to activate the Passthrough feature.
IPSec Tunnel	Select **Enable** to activate the Tunnel feature.

8.2 Peer-To-Peer

In Peer-To-Peer mode, the administrator can setup a secure tunnel between the router and a remote IPSec gateway. After the tunnel is established, the networks behind both the IPSec routers can communicate securely via the internet.

Note: *There should not be any IP Address conflict between the LAN subnets behind the IPSec routers i.e both the LAN networks should not be in the same subnet.*

Typically, the remote IPSec peer can be identified by means of its IP Address. If the peer's IP Address can vary, then the remote peer can be identified by its Domain Name.

Select **VPN → Peer-To-Peer** to configure the **Tunnel Configurations** as explained below.

Web UI **Tunnel Configurations**

Add/Modify Tunnel

Tunnel ID	Enter the alphanumeric string that identifies the remote tunnel.
Tunnel Source Interface	Select the WAN interface, which serves as the tunnel's source endpoint.
Termination Type	Select the termination type (**Domain name** or **IP address**), which a remote endpoint can use.
Termination IP/Name	Enter the remote gateway's IP address or domain name depending on the termination type selected. When Domain Name is configured, ensure that DNS Proxy is configured with the appropriate DNS Server IP address.
Shared Key	Enter the secret key that should be used on both endpoints in order to establish Phase I negotiation. The purpose of this key is for the IPSec peers to authenticate each other
Tunnel Type	Only **Public** IPSec VPN tunnels are supported.
Phase 1 Proposal	
Mode	This will allow a user to select the Phase 1 negotiation mode. User can select between **Main** and **Aggressive** modes. In the Main mode, all communications between the two endpoints of an IPSec VPN tunnel are encrypted. In Aggressive mode, there is no encryption in the Phase 1 negotiation.
DH Group	Select the DH algorithm to generate the shared keys in a secure manner. This shared key is used for deriving encryption and hash algorithm keys used during Phase 1 negotiation. • **Group 1** generates a 768-bit key • **Group 2** generates a 1024-bit key. The same DH Group must be used on both ends of an IPSec VPN tunnel.
IKE Life Duration	Enter the life duration (in seconds) of Phase 1 key. When it is expired, the two IPSec peers should trigger Phase 1 negotiation again to set up a fresh IPSec tunnel. The minimum life duration is 300 seconds and maximum life duration is 86400 seconds.
IKE Hash	Select the algorithm that will be used to ensure that the messages exchanged between the two IPSec VPN tunnel endpoints has been received exactly as it was sent. In other words, a Hash algorithm is used to generate a binary number by a mathematical operation using the entire message. The resulting number is called a message digest. The same operation is performed when the message is received, and if there has been any change in the message during transit, the resulting message digest number will be different and the message will be rejected. The options are: • **MD5** - a 128-bit message digest • **SHA** - a 160-bit message digest. User must have exactly the same IKE Hash algorithm on both ends of a VPN tunnel.
IKE Encryption	Select the encryption algorithm (**DES, 3DES**) that will be used to encrypt the messages passed between the VPN tunnel endpoints during the Phase 1 negotiation. The length of the key for the 3DES algorithm is three times

	that of DES key and hence it is more secure. User must select exactly the same IKE Encryption algorithm on both ends of a VPN tunnel.
Phase 2 Proposal	
PFS Mode	Select the mode that will be used for IPSec Perfect Forward Secrecy (PFS). (**Group 1, Group 2, Disabled**). • **Group 1** uses 768-bit prime number • **Group 2** uses 1024-bit prime number • **Disable** disables the PFS mode. User must use exactly the same PFS mode on both ends of the VPN tunnel.
IPSec Operation	Select the IPSec transform that will be applied to packets that are sent between the two endpoints of a VPN tunnel. • **ESP** - specifies that the entire packet will be encrypted (using DES, 3DES or AES algorithm, as selected in ESP Transform field) and authenticated (using MD5 or SHA algorithm, as selected in ESP Authentication field). • **AH** - specifies that only the authentication algorithm (MD5 or SHA, as selected in the AH transform field) will be used. When AH is selected, the data portion of packets sent between the two endpoints of a VPN tunnel will not be encrypted.
IPSec Life Duration	Enter the IPSec Life Duration (in seconds). It is used for life duration of Phase 2 key. When this timer expires, the two peers should trigger Phase 2 negotiation again to set up a new Phase 2 key. The minimum life duration is 180 seconds and maximum life duration is 86400 seconds.
ESP Transform	Select the ESP transform encryption algorithm (**Null, DES, 3DES and AES**) to be used when ESP is selected as the IPSec Operation. User must select the same ESP transform encryption algorithm on both ends of a VPN tunnel.
ESP Auth	Select the ESP authentication algorithm (**Null, MD5, and SHA**) to be used when ESP is selected as IPSec Operation. The user needs to use the same ESP authentication algorithm on both ends of a VPN tunnel.
AH Transform	Select the AH authentication algorithm (**MD5, SHA**) to be used when AH is selected as the IPSec Operation. The user needs to use the same AH authentication method on both ends of a VPN tunnel.
Target Host Range	
Type	Select the type of network definition for the range of IP addresses on the remote LAN that will access the VPN. Only the **Subnet** type is supported.
Target Network Address	Enter IP address range of the remote host machines that can be accessible from a VPN tunnel. This is specified as a combination of network address and the subnet mask. e.g. when the user needs to access remote machines with IP address in the range of 192.168.20.1 to 192.168.20.16 , then he/she can specify this range as 192.168.20.1/28.

Note: *The user has to specify a proper routing entry in the routing page for the remote network address. For example, if the remote network address range is 192.168.20.1 / 28 , then the user can specify the route entry with destination address*

as 192.168.20.0 with subnet mask 255.255.255.0 and outgoing device same as that of the source interface which was specified in the corresponding tunnel entry.

8.3 IPSec Server

IPSec server allows tele-workers to connect to their corporate office securely from anywhere in the world. Since the remote user's IP Address will vary based on the user's current location, the IPSec server tunnel ignores the client's address. Instead it recognizes the clients based on their remote IDs, which can be configured separately through the Remote ID page.

The IPSec Server tunnel can be configured in Main Mode or Aggressive Mode. Many Aggressive Mode Server tunnels may be added simultaneously, however only one Main Mode Server tunnel can be configured.

Select **VPN → IPSec Server → Server** to configure the **IPSec Server Configurations** as explained below.

Web UI	**IPSec Server Configurations**
Add/Modify Tunnel	
Tunnel Name	Enter the name of the IPSec server tunnel.
Tunnel Source Interface	Select the WAN interface, which serves as the tunnel's source endpoint.
Shared Key	Enter the secret key that is used to establish Phase I negotiation. This key should be entered exactly the same way on both endpoints. This key is used for the IPSec peers to authenticate each other.
Tunnel Type	Select the type of VPN Tunnel. Only **Public** IPSec VPN tunnels are supported.
Phase 1 Proposal	
Mode	Select the Phase 1 negotiation mode. User can select from: • **Main mode** - all communications between the two endpoints of an IPSec VPN tunnel are encrypted. • **Aggressive mode** - there is no encryption in the Phase 1 negotiation.
DH Group	Select the DH algorithm to generate shared keys in a secure manner. This shared key is used for deriving encryption and hash algorithm keys used during Phase 1 negotiation. • **Group 1** generates a 768-bit key • **Group 2** generates a 1024-bit key. The same DH Group must be used on both ends of an IPSec VPN tunnel.
IKE Life Duration	Enter the life duration (in seconds) of Phase 1 key. When this timer expires, the two IPSec peers should trigger Phase 1 negotiation again to set up a fresh IPSec tunnel. The minimum life duration is 300 seconds and

	maximum life duration is 86400 seconds.
IKE Hash	Select the Hash algorithm that will be used to ensure that the messages exchanged between the two IPSec VPN tunnel endpoints has been received exactly as it was sent. In other words, a Hash algorithm is used to generate a binary number by a mathematical operation using the entire message. The resulting number is called a message digest. The same operation is performed when the message is received, and if there has been any change in the message during transit, the resulting message digest number will be different and the message will be rejected. The options are: • **MD5** - a 128-bit message digest, • **SHA** - This generates a 160-bit message digest. User needs to configure exactly the same IKE Hash algorithm on both ends of a VPN tunnel.
IKE Encryption	Select the encryption algorithm (**DES, 3DES**) that will be used to encrypt the messages passed between the VPN tunnel endpoints during the Phase 1 negotiation. The length of the key for the 3DES algorithm is three times that of the DES key, and is therefore more secure. User must choose exactly the same IKE Encryption algorithm on both ends of a VPN tunnel.
Phase 2 Proposal	
PFS Mode	Select the mode that will be used for IPSec Perfect Forward Secrecy (PFS). (**Group 1, Group 2, Disabled**). • Group 1 uses 768-bit prime number • Group 2 uses 1024-bit prime number • Disable disables the PFS mode. User must use exactly the same PFS mode on both ends of the VPN tunnel.
IPSec Operation	Select the IPSec transform that will be applied to packets that are sent between the two endpoints of a VPN tunnel. • **ESP** - specifies that the entire packet will be encrypted (using DES, 3DES or AES algorithm, as selected in ESP Transform field) and authenticated (using MD5 or SHA algorithm, as selected in ESP Authentication field). • **AH** - specifies that only the authentication algorithm (MD5 or SHA, as selected in the AH transform field) will be used. When AH is selected, the data portion of packets sent between the two endpoints of a VPN tunnel will not be encrypted.
IPSec Life Duration	Enter the IPSec Life Duration (in seconds). This is the life duration of Phase 2 key. When this timer expires, the two peers should trigger Phase 2 negotiation again to set up a new Phase 2 key. The minimum life duration is 180 seconds and maximum life duration is 86400 seconds.
ESP Transform	Select the ESP transform encryption algorithm (**Null, DES, 3DES and AES**) to be used when ESP is selected as the IPSec Operation. User needs to select the same ESP transform encryption algorithm on both ends of a VPN tunnel.
ESP Auth	Select the ESP authentication algorithm (**Null, MD5 and SHA**) to be used when ESP is selected for IPSec Operation. The user needs to use the same

	ESP authentication algorithm on both ends of a VPN tunnel.
AH Transform	Select the AH authentication algorithm (**MD5, SHA**) to be used when AH is selected for the IPSec Operation. The user needs to use the same AH authentication method on both ends of a VPN tunnel.

A ***Remote ID*** needs to exist for each remote user client that wants to connect to the IPSec Server at the router.

Note: *Ensure that the remote user's VPN client is configured with the same Tunnel Parameters (Password, Phase 1 and Phase 2 algorithms) as the IPSec Server Tunnel at the router.*

Limitation:
The router requires every remote client connected to it, to have a unique IP Address. So multiple IPSec clients behind a Many-To-One NAT Router cannot connect to the IPSec Server at the router. This is because all these IPSec clients will communicate with the router using the same global source IP Address.

Select **VPN → IPSec Server → Remote ID** to configure **Tunnel Remote ID Configuration** as explained below.

Web UI	**Tunnel Remote ID Configuration**
IPSec Server Name	Select the IPSec Server Tunnel for which Remote ID is to be configured.
Remote ID Type	Select the type (IPV4 address, FQDN) of Remote ID to be configured.
Remote ID Data	Enter the Remote ID depending on the type selected.

After entering all the information press the **Apply** button and the **Remote IDs** table will now be displayed at the bottom of the page. Press **Delete** button for deleting the corresponding entry.

8.4 Tunnel Table

The Tunnel Table displays the list of tunnels configured by the administrator. The administrator can edit or delete the configured tunnels from this page.

Select **VPN → Tunnel Table** to view/edit the **Tunnel Table** as explained below.

Web UI	**Tunnel Configurations**

Tunnel Name	This is the name of the tunnel if it is a peer-to-peer configuration or it is the name of the IPSec server if it's an IPSec server configuration.
Termination IP/Domain Name	If this is a peer-to-peer tunnel, then it indicates remote peer IP address or its domain name. If it is a IPSec server then "ROAMING MODE" will be displayed.
No of Remote IDs	This indicates the number of Remote IDs corresponding to the IPSec server. For a peer-to-peer tunnel this field is not applicable since Remote IDs are not configured for a peer-to-peer tunnel.

Press **View** button for editing and **Delete** button for deleting the corresponding IPSec Peer-To-Peer or IPSec Server tunnel entry. When an IPSec server entry is deleted, all its corresponding Remote IDs are also deleted.

Note: *The total no of IPSec configuration entries includes the number of peer-to-peer tunnel along with number of IPSec servers plus its corresponding Remote IDs. For example: If there are two peer-to-peer tunnels and two IPSec servers one with three Remote IDs and the other with 4 Remote IDs, then the total no of entries will be: 2 + 3(1st IPSec server) + 4(2nd IPSec server) = 9.*

8.5 IPSec Status

IPSec status table shows the state of the tunnel along with the number of packets received and transmitted through the tunnel. Only IPSec Tunnels that are established or in the negotiation state will be displayed here, tunnels that are Idle will not be displayed in this table.

Select **Status → IPSec Status** to view the **IPSec Status** table as explained below.

Web UI	**IPSec Status**
Tunnel Name	Displays the name of each tunnel.
Termination IP/ Name	Displays the termination IP Address/name of the tunnel.
Remote ID (Server Only)	Displays the remote ID of the server.
Status	Displays the status of each connection.
Receive Packets	Displays the number of packets received through the tunnel.
Transmit Packets	Displays the number of packets transmitted through the tunnel.

8.6 IPSec Log

The router maintains a log of the IPSec protocol activities i.e Tunnel Negotiation, Establishment and Renegotiation.

Select **Status → Log Tables → IPSec Log** to view the **IPSec Log Table** as explained below.

Web UI	**IPSec Log Table**
Index	Displays the sequence of the IPSec log.
Description	Displays a brief description of the log entry, which can be used to check tunnel behavior.

Quality of Service

Traffic control in a network can be achieved by Quality of Service (QoS) algorithms, which involves guiding the packets based on some predefined rules. Traffic control classifies packets and places them in individual flows or classes. It can then **police** by limiting the number of packets transmitted and/or **schedule** the packets in different order of priority for transmission.

The QoS algorithms in the router can apply prioritization rules on traffic which are passing through the router. However, the traffic will need to be prioritized at every hop router until it reaches its destination to ensure good quality of service. This can be achieved by ensuring that the ***TOS octet*** in IP header is set appropriately. Every hop router can prioritize traffic based on the TOS octet value in the packet's IP Header.

9.1 Hierarchical Token Bucket (HTB)

HTB is a classful queuing algorithm which provides rate limiting, guaranteed bandwidth and prioritization of the traffic. HTB ensures that the amount of service provided to each class is at least the minimum of the amount it requests and the amount assigned to it. When a class requests less than the amount assigned, the remaining (excess) bandwidth is distributed to other classes which request service and which have highest priority.

To enable this feature, the administrator can configure the total interface bandwidth and different classes with the total bandwidth shared among them. Subsequently filters need to be configured to match the traffic to flow through the different classes.

9.1.1 Class Configuration

The administrator should configure a Root Node first, by specifying the interface bandwidth (upstream link bandwidth) and the default class to be used for unclassified traffic. Subsequently, Class Nodes can be added and the interface bandwidth can be distributed among these classes.

Select **QoS → HTB Configuration** to enter the **HTB QoS Configuration**. Select **Node** as **Root** to configure the **HTB Root Settings**.

Web UI	HTB QoS Configurations
Interface Name	Select the interface (**LAN, WAN1, WAN2**) on which the bandwidth control is to be added
Node	Select the node (**Root, Class)** to be configured.
HTB Root Settings	Displays when Node is selected as **Root**.

Interface Bandwidth	Enter the upstream bandwidth of the interface.
Default Class ID	Enter the default Class ID for the root class. Corresponding class needs to be added in the class configuration The unclassified traffic will be sent to the class with this default class ID.
Root ID	The Root ID (configured automatically by the device when we add a root class) is displayed. This is the parent class ID of the interface.

Select **QoS → HTB Configuration** to enter the **HTB QoS Configuration**. Select **Node** as **Class** to configure the **HTB Class Settings**.

Web UI **HTB QoS Configurations**

Interface Name	Select the interface (**LAN, WAN1, WAN2**) on which the bandwidth control is to be added
Node	Select the node (**Root, Class)** to be configured.
HTB Class Settings	Displays when Node is selected as **Class**.
Priority	Enter the priority of this node (value should be between 0 and 7). Default value is 0. Priority field value 0 has highest priority. Classes with the highest priority will get excess bandwidth first. The priority will be effective at the leaf classes only.
Guaranteed Rate	Enter the Guaranteed bandwidth (value should be between 1 and 100,000 Kbps). This value should not exceed the interface bandwidth. This is the bandwidth which the class and all its children are guaranteed.
Maximum Rate	Enter the Maximum bandwidth (value should be between 1 and 100,000 Kbps). This value should not exceed the interface bandwidth. This is the bandwidth which the class and all its children are given, when excess bandwidth is available.
Parent ID	Enter the Parent class ID value to which we are adding this child class to.
Class ID	Enter the Class ID of the class, which is currently being added.

After entering all the information press the **Apply** button and the **HTB QoS Entries** table will now be displayed at the bottom of the page. Press **Delete** button for deleting the corresponding entry.

Note:
1) The sum of child's guaranteed bandwidth should be less than or equal to the parent's guaranteed bandwidth.
2) Any child's maximum rate should be less than or equal to it's parent's maximum rate.

9.1.2 Filter Configuration

Filters in QoS help in **classification** of traffic, and assigning the traffic to a specific HTB class. These filters use IP parameters like Source IP, Destination IP, Protocol, Source Port and Destination Port. The packets that match a filter configuration is placed in the class specified with the Class ID parameter and will receive the specified traffic treatment.

Multiple filters can be configured for the same Class ID. For example, consider a scenario where the administrator wants to ensure that HTTP and Email traffic together do not exceed 100kbps. In this case, a HTB Class can be configured with a Maximum Rate of 100kbps, and two filters (one for HTTP and one for Email traffic) can be added for the same HTB Class.

Select **QoS → Filter Configuration** to configure the **QoS Filter Configuration** as explained below.

Web UI	QoS Filter Configurations
Filter Name	Enter the name of the Filter (Max 20 characters). Filter Name should be unique.
Interface Name	Select the Interface on which to apply the filter.
Source	The Source IP. • **Any** - If selected the filter will be applied for any source address. • **Subnet** - If selected the user needs to configure specific Source IP address with subnet.
IP Address	Enter the Source IP Subnet
Destination	The Destination IP. • **Any** - If selected the filter will be applied for any destination address. • **Subnet** - If selected the user needs to configure specific destination IP address with subnet.
IP Address	Enter the Destination IP Subnet
Protocol	Select the Protocol to filter the network traffic. When **Other** is selected enter the protocol number (between 1 and 255).
Source Port No	Enter the Source port number (value between 1 and 65535) to specify the type of application for which this filter is used. Source port value of zero indicates "Any" Source Port. This field is effective when TCP/UDP is selected as the Protocol.
Destination Port No	Enter the Destination port number (value between 1 and 65535) to specify the type of application for which this filter is used. Destination port value of zero indicates "Any" Source Port. This field is effective when TCP/UDP is selected as the Protocol.
Class ID	Enter the Class ID of the class, through which this traffic should flow.

After entering all the information press the **Apply** button and the **QoS Filter Entries** table will now be displayed at the bottom of the page. Press **View** button for editing and **Delete** button for deleting the corresponding entry.

Note:
1) Always configure filters to direct traffic to a leaf class (i.e class which has no children).
2) When IP Packets are fragmented, only the first fragment will contain the source/destination port fields. So if a QoS Filter is based on packet's source/destination port, the non-first fragments will NOT be matched by the filter rule, and so the QoS configuration will not apply on these fragments.

9.2 TOS/DiffServ

TOS configuration page is used to set the TOS octet in IP header for the packets that match the set of configured filters.

Select **QoS → TOS/DiffServ** to configure the **Type Of Service/DiffServ** as explained below.

Web UI	Type Of Service/DiffServ
Source	The Source IP. • **Any** - If selected the filter will be applied on the network traffic regardless of its source address. • **Subnet** - If selected the user needs to configure specific Source IP address with subnet.
IP Address	Specify the Source IP Subnet.
Destination	The Destination IP. • **Any** - If selected the filter will be applied on the network traffic regardless of its destination address. • **Subnet** - If selected the user needs to configure specific destination IP address with subnet.
IP Address	Specify the Destination IP Subnet.
Protocol	Select the Protocol to filter the network traffic. When **Other** is selected enter the protocol number (between 1 and 255).
Source Port No	Enter the Source port number (value between 1 and 65535) to specify the type of application for which this filter is used. Source port value of zero indicates "Any" Source Port. This field is effective when TCP/UDP is selected as the Protocol.
Destination Port No	Enter the Destination port number (value between 1 and 65535) to specify the type of application for which this filter is used. Destination port value

	of zero indicates "Any" Source Port. This field is effective when TCP/UDP is selected as the Protocol.
TOS/DiffServ	Enter the TOS value (8 bit binary number) to be set in the IP header of the filtered packet.

After entering all the information press the **Apply** button and the **TOS/DiffServ Table** will now be displayed at the bottom of the page. Press **Delete** button for deleting the corresponding entry.

Administration

The router provides several administrative features/tools to maintain and monitor the router. This section discusses these features and their configuration in detail.

10.1 Device Information

The current status of the router can be obtained through this page.

Select **Status → Device Info** to view **Device Information** table as explained below.

Web UI	Device Info
Device Name	Displays the device name.
Firmware Version	Displays the firmware version used by the router.
System Up Since	Displays the duration for which the router has been running.
LAN	
LAN Physical Link Status	Displays if a cable is plugged in (UP) or out (DOWN) on the LAN port.
MAC Address	Displays the MAC address of the LAN port.
IP Address	Displays the current LAN IP address.
Subnet Mask	Displays the subnet mask for the LAN IP address.
DHCP Server	Displays if the router is currently configured as a DHCP server.
WAN1	
WAN1 Physical Link Status	Displays if a cable is plugged in (UP) or out (DOWN) on the WAN port.
WAN1 Protocol Status	Displays the operational status of the WAN protocol.
Connection Type	Displays the WAN routing protocol selected (Static, Dynamic or PPPoE).
IP Address	Displays the current WAN IP address.
Subnet Mask	Displays the subnet mask for the WAN IP address.
Default Gateway	Displays the gateway IP address for this interface.
WAN2	
WAN2 Physical Link Status	Displays if a cable is plugged in (UP) or out (DOWN) on the WAN port.
WAN2 Protocol Status	Displays the operational status of the WAN protocol.

Connection Type	Displays the WAN routing protocol selected (Static, Dynamic or PPPoE).
IP Address	Displays the current WAN IP address.
Subnet Mask	Displays the subnet mask for the WAN IP address.
Default Gateway	Displays the gateway IP address for this interface.
DMZ	
DMZ Physical Link Status	Displays if a cable is plugged in (UP) or out (DOWN) on the DMZ port.
IP Address	Displays the DMZ IP address.
Subnet Mask	Displays the subnet mask for the DMZ IP address.

10.2 Traffic Statistics

The number of packets transmitted, received, errors at each interface can be obtained through the traffic statistics page. These counters will be reset when the router is rebooted.

Select **Status → Traffic** to view **Traffic Statistics** as explained below.

Web UI	**Traffic Statistics**
Interface Name	Displays the interface name.
Received	Displays the number of packets received.
Transmitted	Displays the number of packets transmitted.
Rx-Error	Displays number of error packets received.
Tx-Error	Displays number of error packets transmitted.
Dropped	Displays the number of packets dropped.

10.3 Session Log

The Session Log is used to log and display the sessions created at the router. For example, sessions will be created when hosts in the LAN accesses applications or services on the WAN.

Select **Status → Log Tables → Session Log** to view **Session Log** as explained below.

Web UI	Session Log
Start Time	Displays the starting date and time.
End Time	Displays the ending date and time.
Source: port	Displays the IP address and the TCP/UDP port number of the application that initiated the session.
Destination: port	Displays the IP address and the TCP/UDP port number of the application that responded to the session.
Type	Displays the protocol used for the session.
Terminate Reason	Displays the reason for session termination or the current status.

10.4 SysLog

The SysLog feature is used to send the System Logs to a remote server.

Select **Misc → SysLog** to configure **SysLog** as explained below.

Web UI	System Log
Sys-Log Status	Select Enable or Disable to activate or deactivate system logging.
Remote Server	Enter the IP address of the remote server where to send the log messages.
Sys Log level	Select the System Log levels (e.g. Alert, Emergency, and Critical) according to which System Log files will be generated.

Caution: *The router's performance may be affected if the Log Level is set to* ***Debug*** *Level.*

10.5 Password Change

This page allows the user to change the Password used to control access to the router configuration.

Select **Tools → Password** to configure **Change Password** as explained below.

Web UI	Change Password
Username	The username for the account should be **admin**.
Old Password	Enter the old password for the account.
New Password	Enter the new password for the account.
Confirm New Password	Enter the new password again to verify that the password has been entered correctly.

Password Recovery

If administrator misplaces the router password he/she can call Dlink Technical Support to inform the router MAC address which is on the product sticker of the router. The Technical Support will then generate and mail a <username> and <serial-key> for that router.

Once the administrator gets the username and serial key from the technical support, he/she has to go the following URL:
https://<LAN IP address>/html/Backup.html

To access the router, enter "DRO210i" as the username and the password. This web page will prompt for username and serial key. When the administrator enters the information received from the technical support, the password will be displayed for subsequent login to the router.

Note: *The <username> and <serial-key> obtained from the technical support team can be used only once i.e. it cannot be used again to recover the password from the same box. Also the set of <user name> and <serial key> cannot be used for recovering password for any other customer (with different MAC address).*

10.6 System

The administrator can save the router's configuration, restart the router and restore the router back to factory default settings.

Select **Tools → System** to configure **System** as explained below.

Web UI	System
Save Settings	Press this button to save the current settings of the router.
Save Settings and	Press this button to save the current settings and restart the router with

Restart the Device	the saved settings.
Restore to Factory Default Settings	Press this button to restore the factory default settings of the router. On reboot, the router can be accessed using LAN IP Address 192.168.100.254.
Restart the Device	Press this button to restart the router without saving current changes in the settings.

Caution: *After configuring the router, use Save Settings to save the configurations permanently. Otherwise on reboot, the router would not remember the current settings.*

10.7 Upload/Download

This feature allows the administrator to upload new configuration file, firmware or certificate to the router. The administrator can configure the device, save the configuration and download the configuration in cfg format on the local PC. Subsequently he can upload the configuration file (DRO210.cfg) on the device again whenever required.

Caution: *Ensure that the downloaded configuration is saved with the file name DRO210.cfg. Only a file of this name will be accepted by the router for configuration upload.*

Select **Tools → Upload** to configure as explained below.

Web UI	**Update Firmware/Configuration**
Update File	Select the file using the browse option. The following files can be provided for upgrade: ▪ **upgrade.tar.gz**: This is the upgrade file which will be available from Dlink Technical Support whenever any module or any feature is changed. ▪ **DRO210.cfg**: File which contains the entire configuration of DRO-210i. ▪ **cert.der**: Certificate File for SSL Configuration ▪ **pkey.der**: Private Key File for SSL Configuration
Load Configuration Files to Local Hard Drive	Click OK to download the DRO-210i configuration file onto the Local PC.

10.8 Ping Test

The **Ping Test** feature allows the user to ping to any network device from the router. This helps in checking network connectivity from the router.
Select **Tools → Ping Test** to configure **Ping Test** as explained below.

Web UI	Ping Test
Set Type	Select IP address or Domain Name to use for the ping test.
IP address	Enter the IP address of the end host, if Set Type selection was IP address.
Domain Name	Enter the Domain Name of the end host, if Set Type selection was Domain Name.
Count Number	Enter the number of packets to send for the ping test. The value should be always less than or equal to 10 (four is recommended).

Press the **Apply** button to start the ping test. When the test is over the results are shown in the text box below.

10.9 Remote Access

Remote Access enables the Administrator to remotely provision the router over a secure SSL-based Web User Interface. He can also perform remote software upgrades and remote monitoring to ensure smooth operation of the network. In case of external attacks, the administrator can use the logging provided by the router to locate what kind of attack has happened, when it has taken place and which device may have played a role in it. The administrator can then decide on what firewall policies to add to prevent future attacks (or take necessary steps to correct any internal device problem). Once the problem is corrected, the logs can be used to verify the smooth and correct operation of the router.

Select **Tools → Remote Access** to configure **Remote Access** as explained below.

Web UI	Remote Access
Remote Access Status	Select Enable or Disable to activate or deactivate this feature.
Remote IP address	Enter the IP address of the host(s), which can configure the router remotely.

If Firewall feature is enabled, only these selected IP addresses will be able to access the router remotely. However if there is no firewall configured then anyone can access the device from an external host.

Note: *If* ***NAT*** *is enabled on the remote side then the Global IP address should be entered as the remote IP address because the router will get the request from that address.*

Frequently Asked Questions

11.1 General

Q1. ***I have forgotten the router's LAN IP Address. Now how can I access the router to configure it?***

Ans: Press the **Factory Default switch** (RESET switch on the Front Panel) and the router settings will be restored to default settings. Now you can configure the router using https://192.168.100.254. User name is "admin" and password is also "admin".

Q2. ***I have forgotten my password. How do I recover it?***

Ans: Call Dlink Technical Support to inform the router's MAC address (displayed on the product sticker of the router). The Technical Support will then generate and send you a <username> and <serial-key>.

Open the router's Web Page: https://<LAN IP address>/html/Backup.html. The username and password is "DRO210i". Enter the information received from the technical support, and the old password will be displayed to you for subsequent login to the router.

Q3. ***I have a working configuration currently. I want to try out some new firewall rules. But if the new configuration does not work out, how can I easily revert back to my original configuration.***

Ans: Go to Tools → System, and click "Save" to save your working configuration. Now go to Tools → Upload, and Download your configuration to the Local Hard Disk. If your new firewall rules don't work out, you can revert back to your previous configuration by uploading the saved DRO210.cfg through Tools → Upload, Update file option.

Q4. ***I want use two subnets in my LAN. How can I do this?***

Ans: The router does not have a direct support for multiple subnets on the LAN. However if DMZ Port or WAN2 Port is unused, this Port can be used as the second subnet.

Q5. ***I am unable to access internet. What could be the problem?***

Ans: To troubleshoot this issue, follow the below steps:

- From your LAN PC, ping to the router's LAN IP Address. If this fails, then check your cable connectivity. Also, if Firewall is enabled in the router and LAN is set as **UnTrusted**, ensure that ICMP protocol is permitted in the Inbound Rules.

- Go to Status → Device Info, and check the Physical Link Status and Protocol Status of the WAN Interface. If the Physical Link Status is DOWN, check the cable connectivity. If the Protocol Status is DOWN, then go to Interfaces → WAN and connect the interface.
- Go to Tools → Ping Test, and ping to the ISP Gateway IP Address. If the ping succeeds then the WAN link connectivity is fine, otherwise contact the ISP to fix this issue.
- In Tools → Ping Test, ping to dlink.com or any other domain name. If the ping fails, then go to Misc → DNS Proxy and ensure that the DNS Server IP Addresses are configured properly.
- Now ping to a global IP Address (eg. 4.2.2.2) from your LAN PC. If this ping fails, then either NAT or Route configuration is not proper.
    - Check NAT Configuration:- Ensure that NAT is enabled on the router's WAN interface via NAT → Interface Configuration. And either Many-To-One or Many-To-Many NAT has been configured through NAT → NAT Configuration.
    - Check Route Configuration:- Verify that a default static route has been configured via the WAN Interface with the correct Gateway IP Address via Routing → Static page.
- Now ping to a domain name (e.g. dlink.com) from your LAN PC. If this ping fails, check the DNS Configuration at your PC. The DNS Server can be set to the router's IP Address. If your PC has been configured with a global DNS Server, then ensure that the DNS Server is reachable.

11.2 DHCP, DNS

Q6. ***What is the purpose of DHCP Server Auto Configuration?***

Ans: This field allows you to specify whether or not the Router will automatically assign the DNS settings to the LAN computers. If Enable Auto Configuration is chosen, the DNS Proxy is enabled in the Router. The router acts as DNS server. It gets the DNS IP manually or from ISP. If Disable Auto Configuration is chosen by the administrator, the Domain Name and DNS Server Settings entered by the administrator will be assigned to the LAN computers.

Q7. ***I want to use the router's DHCP Server for the LAN Systems. But I have some Servers (File Server, Web Server) in the LAN for which I want to assign specific IP Addresses. How can I do this?***

Ans: Use **DHCP Static Mapping** feature to reserve specific IP Addresses to the Server Systems. Go to Misc → DHCP → Static Mapping, and configure the MAC address and IP Address mappings.

11.3 Routing

Q8. ***How can I verify that the dynamic routes got exchanged using the RIP feature?***

Ans: Go to Status → Route Table. Here the list of active route entries is displayed. The routes in "Grey" color are static route entries. The entries in "Yellow" color are the routes that were received from the RIP enabled neighboring routers.

Q9. ***I am not able to see the dynamic routes ("Yellow" colored entries) in the route table even after enable RIP feature in this router and the neighboring router. What could be the problem?***

Ans: To troubleshoot this issue, follow the below steps:

- Make sure RIP is enabled on the proper interface to which the RIP enabled neighbor router is connected.
- Ensure that the RIP version matches at the Dlink Router and the neighbor router. i.e The router's RIP send version on the interface must be the same as the neighbor's receive version, and the router's receive version on the interface must be the same as the neighbor's send version.

11.4 High Availability

Q10. ***I have multiple ISP Connections, and am using the router in Load balancing / Auto Backup mode. However the router does not automatically detect ISP Connectivity failures, requiring me to manually disconnect the failed ISP link. What could be the problem?***

Ans: If the ISP Connection is Static or Dynamic WAN Mode, then ensure that Ethernet Link Detection feature is enabled. Go to Interfaces → WAN and click on "Detect Link Status" to enable this feature. It will periodically send ARP or ICMP requests to the ISP and automatically detect connectivity failures.

If the ISP Connection is PPPoE WAN Mode, then ensure that LCP Echo Feature is enabled via Interfaces → WAN, PPPoE Mode. Also ensure that the Interval and Maximum Failures is configured optimally. If the interval is 30 secs and Max Failures is 6, then it will take 30 * 3 secs, i.e 3 minutes to detect link failure.

11.5 Firewall

Q11. ***I want to block access to download of songs, movies etc. How can I do that?***

Ans: Use the router's **File Extension Filter** feature to block HTTP access to extensions like .avi, .mp3 etc. To configure File Extension Filter, enable Firewall on all the relevant LAN, DMZ and WAN interfaces. Go to Firewall → Policy, and click on Out. Enable "File Extension Filter" feature and configure the list of File Extensions to be blocked.

Q12. ***I want to block access to specific sites such as pornographic sites, job sites etc. How can I do this?***

Ans: Use the **Keyword Filter** feature to block HTTP access to specific keywords like sex, job etc. To configure Keyword Filter, enable Firewall on all the relevant LAN, DMZ and WAN interfaces. Go to Firewall → Policy, and click on Out. Enable "Keyword Filter" feature and configure the list of Keywords to be blocked.

Q13. ***I have setup Web Proxy Server and FTP Server on the DMZ Port. I want to ensure that all traffic to the internet is via my DMZ Servers only. i.e my LAN systems can access Web and FTP Traffic only via DMZ Servers and not Internet directly. And Web and FTP traffic can flow unrestricted between my DMZ Servers and internet. How do I configure this?***

Ans: To configure this, you can set all interfaces as UnTrusted and allow only desired traffic between the interfaces. The below steps will guide you through the configuration:

- Go to Firewall → Interface Configuration; disable firewall until the configuration is complete.
- In Firewall → Policy, click In and Permitted Service, and add Service Permitted Rules for Web traffic (HTTP and HTTPS) and FTP Traffic. Add the following IP Permitted Rules for each of the Service Permitted Rules:
  - Add IP Permitted Rule with Source IP as IP Range (DMZ Server's Range of IP Addresses), and Destination IP as Any. This will ensure that Web and FTP Traffic can flow from the DMZ Server to the Internet without any restriction.
  - Add IP Permitted Rule with Source IP as Any, and Destination IP as IP Range (DMZ Server's Range of IP Addresses). This will ensure that Web and FTP Traffic can flow from the LAN to DMZ, and from the Internet to DMZ only.
- In the HTTP/HTTPS Service Permitted Rule, add the below IP Permitted Rule to allow administrator to configure the router:
  - Add IP Permitted Rule with Source IP as IP Range (The LAN System IP Addresses from which router should be configurable), and Destination IP as IP Range (The router's LAN Interface IP Address). This will ensure that router's Web Page is configurable by the administrator.
- Now go to Firewall → Interface Configuration, enable Firewall and set LAN, DMZ and WAN as UnTrusted.

Q14. ***One of the LAN Systems is affected by Virus and is generating huge traffic; which is consuming the entire internet bandwidth. What can I do?***

Ans: Use the **MAC Filter** feature to temporarily block all traffic from the infected system. To configure MAC Filter, enable Firewall on the LAN interface, and set it as a Trusted Interface. Go to Firewall → Policy, and click on Out. Enable "MAC Filter" feature and configure the virus-infected system's MAC Address to be blocked.

After the infected system has been updated with the relevant anti-virus patches and is free from all viruses, remove the MAC blocking to allow internet access to that system.

Q15. ***My LAN Systems are frequently infected by virus. What measures can I take in the router to avoid this?***

Ans: A typical firewall configuration is explained below to take precautionary measures against viruses, intruder attacks etc:

- Go to Firewall → Interface Configuration, and enable Firewall on all interfaces. Set LAN and DMZ to Trusted, and WAN as UnTrusted Interface.
- Go to Firewall → Policy, click on In. Add Port Filters and Permitted IP Rules to allow access to the Company Servers at the LAN or DMZ, which are to be accessible from the internet.
- Go to Firewall → Policy, click on Out. Enable File Extension Filter feature, and block HTTP access to file extensions like .vbs, .exe etc. Files with these extensions are most likely to infect a system with virus.
- Go to Firewall → Policy, click on Out. Enable Web Filter Feature to block Java and ActiveX, since these scripts can contain malicious code that spreads virus.
- Go to Firewall → IDS Configuration, and enable Intrusion Detection for all attacks. This will safeguard the router and LAN systems from the given hacker attacks.

Q16. ***Why I am unable to access the router's Web Pages after enabling Firewall?***

Ans: This can occur due to any of the below reasons:

- You are accessing router from WAN side, but have not configured Remote Access feature to allow remote router configuration.
- You have enabled firewall on LAN interface, and have set LAN as UnTrusted. In this case, configure Remote Access or add inbould firewall policy rules to allow HTTPS access to the router.

To recover, reboot the router so that your previous settings are lost. And then ensure that Remote Access or Firewall Policy Rules are configured appropriately before enabling Firewall.

Q17. ***Can I configure the router to block messengers like skype etc?***

Ans: The router can only block messengers based on Domain names, URL Keywords, IP Addresses or Port numbers used for communication. Blocking of messengers (like skype) which cannot be identified by any of these methods is not supported by the router.

11.6 NAT

Q18. ***How do I make my web server accessible from the internet?***

Ans: The following steps will guide you through this setup:

- Connect your Web Servers to the DMZ Port and configure DMZ Systems in a specific private subnet (e.g 192.178.1.0/24).
- Go to NAT → Virtual Server/NAPT and add an entry to redirect your Server traffic (eg. HTTP, FTP) from the Global IP to the DMZ Internal Server IP Address.
- Instead of Virtual Server configuration, you can also use One-To-One NAT. Go to NAT → NAT Configuration, and configure a One-To-One NAT entry mapping the global IP Address to the Internal Server IP Address.
- If Firewall is enabled, go to Firewall → Policy and click on In. Add Port Filter and Permitted IP Rules to allow the Server traffic from WAN to LAN.

Q19. ***I am unable to access my server in the DMZ Port. What could be the problem?***

Ans: To troubleshoot this issue, follow the below steps:

- Ensure that Virtual Server or One-To-One NAT has been configured to access the DMZ Server. Specifically verify the global IP Address, private IP Address and Port Number configuration.
- If Firewall is enabled, ensure that inbound firewall policy rules have been added to allow the DMZ traffic. In the IP Permitted Rule Page, if specific IP Address has been configured, ensure that Private IP Address and not Public IP Address has been configured to allow access.
- If everything is proper but still not working, then verify Status → Log Tables → Blocking Log to see the reason why the traffic has been blocked from entering inside.

Q20. ***I am using SIP-ALG for VoIP Calls between my branch offices. But I am not able to register my phones to the SIP Server. What could be the problem?***

Ans: Follow the steps below to troubleshoot this issue:

- Verify the phone network configurations for default gateway and dns server
- Verify the phone sip configurations for user name, password and proper registration port
- If firewall is enabled, ensure that the SIP signaling port is not blocked.
- Ensure that the SIP Server IP Address is reachable by pinging to it.

Q21. ***What are the call features supported by SIP-ALG?***

Ans: The call features supported by SIP-ALG are as below:

a. Registration
b. Call Establishment
c. Attended Call transfer
d. Unattended Call transfer
e. Call Forward
f. Voice Mail
g. Conference Call

Q22. ***I am using SIP-ALG for VoIP Calls between my branch offices. My VoIP Call has been established, but I am unable to hear the voice of the other person. What could be the problem?***

Ans: This problem can occur if the SIP Phone has been registered to the Server with the private IP Address/Port. Ensure that your phone's signaling port or the SIP Server signaling port has been configured at the router via NAT → SIP-ALG.

Q23. ***I am not able to make calls after rebooting the router. Why?***

Ans: After rebooting, the router cannot remember the device registrations which happened earlier. You have to register your device again after the router reboots.

Q24. ***Can I use SIP-ALG for Video Over IP?***

Ans: Yes. SIP-ALG can be used for both Voice and Video over IP. The only requirement is that the voice/video endpoints or equipment use SIP (Session Initiation Protocol) for Call Establishment and RTP (Real-time Transport Protocol) for Voice/Video traffic.

Q25. ***Can I use TCP for SIP signaling or media traffic in DRO2xx router?***

Ans: DRO2XX routers support only UDP for both signaling and media traffic.

11.7 VPN

Q26. ***I want to use IPSec VPN for Secure Branch Office access. Will this make my access very slow?***

Ans: The router has a built-in hardware accelerator to guarantee high-speed encryption and decryption for secure VPN Connectivity. The speed of your access is more dependant on the speed of your ISP Connectivity.

Q27. ***Will the router's VPN feature offer virus protection?***

Ans: No. VPN provides security by encrypting and decrypting data that passes through a VPN connection; it does not offer protection from viruses.

Q28. ***How should I configure my VPN Tunnel to ensure maximum security?***

Ans: Configure the VPN Tunnel in the following manner to ensure maximum security:

- In Phase 1 Proposal, use **Main Mode** instead of Aggressive Mode, because Main Mode has more messages to ensure secure exchange of encryption keys.
- In Phase 2 Proposal, use **ESP** IPSec Operation instead of AH, because ESP encrypts the traffic unlike AH. And use ESP Transform of **AES** or **3DES** algorithms since they are more secure.
- In both Phase 1 and Phase 2, use DH Group/PFS Mode of **Group 2** because it uses a 1024-bit prime number, which is longer than the 768-bit prime number used by Group 1.

Q29. ***What are the different IPSec VPN solutions that have been tested with the DRO-2XX products?***

Ans: For the purpose of site-to-site VPN connectivity, the DRO-2XX has been tested & interoperating successfully with DFW-100i (Powered by Intoto's VPN implementation), OpenSwan (formerly called FreeSwan) and DFL series of routers.
For the purpose of secure remote access (i.e. Server Tunnels for Roaming Users), the product has been tested & interoperates successfully with SafeNet SoftRemote VPN client and D-Link VPN client.

Q30. ***What is the maximum number of VPN Tunnels supported by the router?***

Ans: The router supports up to 32 VPN Tunnels. This includes both Peer-To-Peer as well as Roaming User Tunnels.

11.8 QoS

Q31. ***I have a ISP Connection with 128kbps upstream bandwidth. And I want to ensure that my email traffic is always guaranteed atleast 50 kbps. How can I do this?***

Ans: Configure QoS on the WAN Interface in the following manner:

- Add a HTB Root Node with interface bandwidth as 128kbps. Set the Default Class ID as 3.
- Add a HTB Class Node (for Email Traffic) with Priority 0, Guaranteed Rate 50kbps, Maximum Rate 128kbps, Parent ID 1 and Class ID 2.
- Add another HTB Class Node (for all other traffic) with Priority 1, Guaranteed Rate 78kbps, Maximum Rate 128kbps, Parent ID 1 and Class ID 3.
- Add a HTB Filter on the corresponding WAN interface for Email Traffic. The Protocol and Destination Port Number should correspond to the Email Protocol and set the Class ID as 2.

Q32. ***My company uses a Financial Application across the internet, and I want to ensure that this traffic is prioritized over all other traffic.***

Ans: Configure HTB QoS on the WAN interface as explained in Q31. This will ensure that this router prioritizes your application over all other traffic.

To ensure that every hop router prioritizes your application, configure the TOS/DiffServ feature to appropriately set the TOS Octet in the IP Header of your application packets. For example, a TOS Value of "00111101" can be used for critical traffic which should be transmitted with low delay, high reliability and high throughput.