Perle IRG7000/5000 5G/LTE Cellular Router User’s Guide

Updated: May 17 2024
Revision: A1.05.17.2024
Document Part: 5500445-10

Preface

Intended Audience

This guide is for the individual responsible for the installation and configuration of the IRG5000 Series Router. Familiarity with networking, concepts, and terminology relating to Cellular, GNSS (GPS), WiFi, Ethernet, and LAN (local area networks) may be required.

Purpose

This guide provides the information needed to configure and manage the Perle IRG5000 Series Router. This document does not cover hardware features, installation instructions, and product specifications. This information can be found in the product specific Hardware Installation Guides.

This guide provides information about product features and guidance on configuring and using these features. Some features may not be applicable to your model or running software. For users of the WebManager, this guide also provides navigation reference. For those using the Command Line Interface (CLI), a reference guide can be download that provides detailed command information.

All guides can be downloaded from the Perle web site at https://www.perle.com/.

Document Conventions

This document contains the following conventions:

Most text is presented in the typeface used in this paragraph. Other typefaces are used to help you identify certain types of information. The other typefaces are:

Note: *Means reader take note*: notes contain helpful suggestions.

Caution: Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Perle Systems Limited.
60 Renfrew Drive
Markham, Ontario
L3R 0E1, Canada

Publishing History

Date	Revision	Update Details
Jan 22, 2020	A1.22.01.2020	Initial release of the manual.
May 2021	A1.13.05.2021	Release 2 (Rev B).
September 2021	A1.30.09.2021	Minor fixes to document.
January 2022	A1.25.01.2022	Added 5G Cellular model.
April 2022	A1.04.14.2022	Added updates for router V7.0.
May 2022	A1.05.18.2022	Fixed errors in documentation.
January 2023	A1.01.25.2023	Added container support.

February 2023	**A1.02.16.2023**	**Fixed manual con cons.**
April 2023	**A1.04.27.2023**	**Manual corrections.**
June 2023	**A1.06.21.2023**	**Release V7.2 for routers**
Oct 2023	**A1.10.30.2023**	**Added IPv6 Prefix delegation support**
May 2024	**A1.05.17.2024**	**Release V7.3 for routers**

Table of Contents

Overview

About the Perle IRG7000/5000 5G/LTE Router

The Perle IRG7000/5000 5G/LTE routers are compact, rugged, fully featured routers intended for a variety of applications. It has multiple communication ports including Serial, Ethernet, and a USB port. It supports 5G/LTE wireless solutions for both fixed and mobile applications (IoT).Also standard on all models is a USB-C port that can be used as a serial console port or in some models as an additional Ethernet interface. Some routers come with an 5G/LTE modem supporting, data, SMS, and GNSS features. Depending on the model, there are a variety of combinations of Ethernet, Serial, and I/O ports.
Some models provide LTE CAT6 connectivity with download speeds up to 300 Mbps, others provide LTE CAT12 connectivity with download speeds up to 600 Mbps. The IRG7000 5G/LTE supports peak download rates of 4.5 Gbps and uploads speeds of 660 Mbps. It offers global coverage of frequency bands, supports Cat-20 technology with automatic fall-back to 4G and 3G (HSPA+, UMTS) networks. Cellular models include integrated GNSS receiver (GPS, GLONASS, Beidou, and Galileo) satellite support. FirstNet Ready™ models run a version of the software specifically intended to meet FirstNet™ certification and operational requirements. Please see the Hardware Information Guide for your model for a detailed description of your hardware.

*Note: Some features may not be available on your firmware version or hardware model.*Please see the Hardware Installation Guide for your model for full details.

Functionality

- Gateway (IP Passthrough), Bridging, Switching, RoutingFirmware over the Air (FOTA)
- (OCI) Container Management
- DDNS, DNS Proxy/Spoofing, Relay Client Opt982
- NTP, & SNTP (Version 1,2,3,4)
- DDNS, DNS Proxy/Spoofing, Relay Client, Opt82
- DHCP/DHCPv6 server & BOOTP for automated network-based setup
- IPv6 Prefix Delegation

GPS & GNSS Reports

- GPS for tracking equipment

LAN Features

- LAN bridging and/or switching
- 802.1x
- IPv4/IPv6 DHCP Server,
- IPv4 Relay
- IPv4/IPv6 DNS Server
- DNS Forwarding / DDNS / Caching
- STP / MSTP
- VLAN / Sub-interface

- LLDP
- Virtual Modem
- Modbus Master/Slave/Gateway
- Remote Access (PPP)
- Remote Access (SLIP)

Management and Configuration Features

- Zero Touch Provisioning (ZTP), DHCP/BOOTP
- Management and Monitoring: HTTP/HTTPS, CLI, Telnet, SNMP 1/2c and 3v
- Multiple copies of firmware can be saved in the unit
- Multiple configuration files can be stored on the unit
- Automatic check for new firmware updates available over (HTTP/HTTPS, FTP, HTTP, SCP, SFTP and TFTP)
- RESTful API
- Connectivity Watchdog
- LLDP-Link Layer Discovery Protocol
- Dynamic DNS with DynDNS.org
- Initial Setup Mode

Redundancy

- Load balancing
- VPN failover
- Virtual Router Redundancy Protocol (VRRPv3).
- Primary/Backup host functionality

Routing Protocols

- RIP/RIPNg, OSPF / OSPFv3, BGP-4, NAT, IPv4/IPv6, Static Routing, IPv6 Encapsulations (GRE, 6in4), Port Routing

VLAN & VPN

- VPN, OpenVPN, VPN failover
- IPsec VPN: NAT traversal, ESP authentication protocol

Firewall Features

- Firewalls to restrict incoming and outgoing packets
- Build in Zone-Based Firewall for local security and traffic filtering
- ACL—Access Control List (list, range, and time)
- Filter based on MAC addresses, IP, port, protocol and user
- IEEE 802.1x authentication and port security can be enabled for any Ethernet ports
- Port forwarding
- BGP Communities
- Zone Firewall
- 2 Factor authentication via email or SMS
- SSHV2
- RADIUS, TACACS+ authentication, Authorization and Accounting
- Local User data
- SMNPV3

Security Features

- AAA Security via remote authentication (RADIUS, TACACS+, LDAP)
- SSHv2 client and server connections
- SSL/TLS client/server data encryption
- Local user database
- RIP authentication (via password or MD5)
- 2F authentication over Email or SMS
- Management Access Control
- Demilitarized Zone (DMZ)
- Secure HTTP/HTTPS/FTP/Telnet Authentication Proxy
- SNMPv3 Authentication and Encryption support
- Active Directory via LDAP

Logging, Reporting, and Alerts

- PerleView Central Management System
- Email alert notifications
- SMS notifications
- Syslog,
- SNMP Traps
- Configuration of Alarms
- Network Watchdog status
- Local port buffering
- External port buffering

Initial Setup

Initial Configuration using the WebManager

Your router is shipped in Factory Default mode. Your router provides a quick Setup Mode to configure the required setup fields. You can use the WebManager or the Command Line Interface (CLI) to perform this operation. To use the CLI interface for initial setup refer to the Hardware Installation Guide on the Perle Website for your model.
You can return to factory default mode at any time by resetting the router to factory mode. (See ***Reset to Factory Defaults***)

In factory default or setup mode, these inbound and outbound ports are in an open state.

TCP (inbound)

- 22 (SSH)
- 443 (HTTPS)
- 53 (DNS)

UDP (inbound)

- 53 (DNS)
- 67 (DHCP server)
- 68 (DHCP client)
- 123 (NTP)
- 161 (SNMP)
- 33815 (PerleView)

TCP (outbound)

- 443 (HTTPS)—software update check

Note: If you configure for secure web access (HTTPS), your web browser is re-directed to a secure URL following initial setup.
Note: startup config may be different depending on the model or running software.

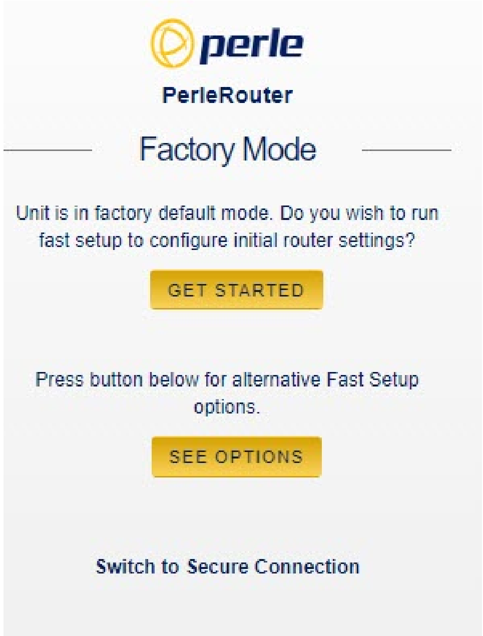
For detailed information on the CLI, please refer to the Perle IOLANCLI Command Reference Guide available for download from the Perle web site at ***https://www.perle.com***.

For details on connecting via the console port, please see your Hardware Installation Guide.

Performing the Initial Configuration using the WebManager

1. Connect power and switch the unit on.
2. Configure your PC to obtain an IP address automatically using DHCP.
3. Plug your PC into any of the Ethernet ports. This method is not available on the 5541R+ model.Connect to the wireless LAN (if available on your model) using the credentials printed on the label

4. Use a standard web browser and enter https://192.168.0.1 or http://192.168.0.1 to access your unit.On the Factory Mode Setup screen, select, Get Started or See Options.



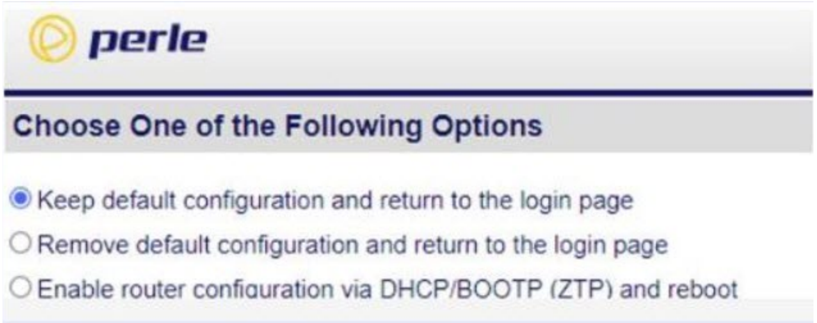
Factory Mode

Unit is in factory default mode. Do you wish to run fast setup to configure initial router settings?

Press button below for alternative Fast Setup options.

5. Once connected, fill in the required fields, apply changes to save and exit configuration. The configuration changes are immediately applied.

6. The IOLAN web configuration Login screen will now be displayed. Using the credentials you previously defined in the previous steps, you can now log in and access your units full configuration.If you select Get Started, fill in the required fields, apply the changes, then save and exit. The configuration changes will be immediately applied to the router. You can now access your router’s complete configuration using the WebManager using the credentials you supplied.
7. If you select See Options, the following screen appears.



Choose One of the Following Options

- ● Keep default configuration and return to the login page
- ○ Remove default configuration and return to the login page
- ○ Enable router configuration via DHCP/BOOTP (ZTP) and reboot

Enabling router configuration via DHCP/BOOTP (ZTP) and reboot, will cause the router to reboot and it will attempt to download either a new version of firmware and/or new configuration from a DHCP/BOOTP server.

Configuration Files

Running-config

The operates from a version of the configuration that is loaded into memory and is referred to as “running-config”. In addition, there is a copy of the configuration file stored in flash memory in text format and used every time the router is rebooted. This is referred to as the “startup-config” file. When making changes to the configuration using the WebManager, it applies all changes to both the “running-config” and the “startup-config” file when the Apply button is selected. These changes take effect immediately and are persistent (maintained after a restart of the router).
However, when using the CLI to configure your router, configuration changes are made immediately to the running configuration, but not to your startup-config, therefore, you must copy the running-config to the startup-config before you reload your router or your configuration changes are lost.

Startup-config

The “startup-config” file resides in flash memory and is used every time the router is reloaded. When making changes to the configuration using the WebManager, it applies all changes to both “running-config” and “startup-config” at the same time. All changes made in WebManager take effect immediately and are persistent (maintained after a restart of the router).The “startup-config” file is a CLI formatted text file stored in flash and can be copied to and from the router using the CLI-based “copy” command.

Default config for router

```
sdm prefer dual-ipv4-and-ipv6 default
interface eth1
ip address 192.168.0.1 255.255.255.0
controller cellular 0
no lte enable
ip nat inside source any interface cellular 0 overload
ip dns listen-address 192.168.0.1
ip dhcp pool default-pool
network 192.168.0.0 255.255.255.0 start 192.168.0.100 stop 192.168.0.200
authoritative enable
default-router 192.168.0.1
dns-server 192.168.0.1
```

System

Under System navigation, you configure the General parameters. Some configuration parameters may be different on some models or running software

General

Use this section to setup General Router information.

Identification	
System name	**Provide your router with a system name.**
Domain Name	**Provide your router with a domain name.**
Location	**Provide a location description.**
Contact	**Provide a contact name.**

Date and Time	
Set clock from PC	**Set the router's clock using your PC's clock time.**
Set Summer Time	**Set the date/recurring option.** **Set the summer time start date/day/month/time and end date/day/month/time.** **Offset in minutes**
Change Date and Time	**Manually change the router's time.**
Change Time Zone	**Manually change the router's time zone.**

IPv6

Depending on the model, IPv6 may or may not be disabled. The router's factory default link local IPv6 address is based upon its MAC Address.

For example:

For an router with a MAC Address of 00-80-D4-AB-CD-EF, the Link Local Address would be fe80::0280:D4ff:feAB:CDEF.

The router listens for IPv6 router advertisements to obtain additional IPv6 addresses. Auto configuration is enabled by default, however you can statically configure IPv6 addresses and network settings.

IPv6	
Enable IPv6	**Activate IPv6 on the next boot. Relevant configuration screens and CLI commands are added to the configuration.**

Management Access

The parameters in this section define how management access to the router is controlled. Protocol based access control is used to restrict access to either the LAN or WAN type interfaces.

Management access is enabled by default, and the default settling for the three roles are:

- LAN—all protocol enabled
- WAN—all protocols are disabled
- TRUSTED—all protocols are enabled.

From within each interface configuration screen, you can set the interface role as a WAN, LAN, or TRUSTED management connection.

Management Access	
Access Restriction	**Enable or disable access restrictions.** **Default is enabled**
Allow from LAN	**Allow management access from LAN type interfaces over these protocols.** • **HTTP—Allow non-secure Web sessions** • **HTTPS—Allow secure Web sessions** • **SSH—Allow SSH sessions** • **TELNET—Allow Telnet sessions** • **SNMP—Allow SNMP sessions** • **HTTP RESTful—Allow HTTP RESTful** • **HTTPS RESTful—Allow HTTPS RESTful** **Default all protocols are enabled.**
Allow from WAN	**Allow management access from WAN type interfaces over these protocols.** • **HTTP—Allow non-secure Web sessions** • **HTTPS—Allow secure Web sessions** • **SSH—Allow SSH sessions** • **TELNET—Allow Telnet sessions** • **SNMP—Allow SNMP sessions**

	• HTTP RESTful—Allow HTTP • HTTPS RESTFUL—Allow HTTPS RESTful Default all protocols are disabled

Allow from TRUSTED	Allow management access from TRUSTED type interfaces over these protocols. • HTTP—Allow non-secure Web sessions • HTTPS—Allow secure Web sessions • SSH—Allow SSH sessions • TELNET—Allow Telnet sessions • SNMP—Allow SNMP sessions • HTTP RESTful—Allow HTTP RESTful • HTTPS RESTful—Allow HTTPS RESTful Default all protocols are enabled

Command Line

Access Command Line	Access Command Line Mode using: • Telnet—Telnet session • SSH—SSH session • Console Port—Physical console port (only available on models with a console port) Default all access command line are enabled

Console Port

Select Port	Only available on models with a console port. • usb port—by default the USB port is used as the system console port. Note: if using the USB port in console mode, you must set up the USB Interface Mode to USB-Console. For the IRG7440 router you must match the console speed with the USB port speed on your computer's USB port • none—no console port • tty1—select tty1 to use the (RS232–DB9) serial port as the console port (model dependent). Note: if using the tty1 in console mode, you must set up the usage mode to serial-console mode.

Allow EXEC (Command line management) on this console	**Only available on models with a console port.** **Select to enable EXEC mode.**
Settings	**Outgoing Access** • **Allow outgoing telnet connections** • **Allow outgoing SSH connections** **Outgoing access is enabled** **Session (EXEC) inactivity timeout in** **days, hours, minutes, seconds** **Values are 0 to 35791 in minutes** **Default is disabled** **Login prompt response timeout in seconds.** **Values are 1–300 seconds** **Default is 120 seconds**
Terminal	**Terminal** **Enable terminal history** **Values are 0–256 buffer size** **Default is 20 buffer size** **Terminal width in columns** **Values are 0-512** **Default is 80 lines in width** **Enable terminal pausing** **Terminal length in lines** **Values are 1-512** **Default is 24 lines**

WebManager Access

Use HTTP (non-secure) or HTTPS (secure) to connect to the router using WebManager mode. If HTTPS connections are used, a certificate needs to be uploaded to the router. If a certificate is not uploaded, the router uses a self-signed certificate. You are given a warning by the browser indicating that the identify of the target web site could not be verified. You must agree to accept the Perle certifiable to connect to the router in HTTPS (secure) mode.

Note: if the protocol that is currently being used is disabled, the web session is lost after the parameters are saved.

WebManager	
WebManager HTTP	Specify protocols to be supported by the WebManager. *HTTP*—Allow non-secure Web sessions Port—Port to use for HTTP sessions Default port is 80 Values are 1025–65535
HTTPS	*HTTPS*—Allow secure Web sessions Port—Port to use for HTTPS sessions Default port is 443 Values are 1024–65535
Idle Timeout	*Idle Timeout*—Amount of time to wait before disconnecting an idle Web session. Default time is 1440 in minutes Values are 1–1440 in minutes

SNMP	
Enable SNMP	The internal SNMP server is activated. Default is enabled

RESTful API	
Cookie Max Age	Configures set-cookie based authentication. Values 1–20160 in minutes (14 days) Default is 1440 in minutes (24 hours)
Enable HTTP Client Requests	Configures the router to accept and respond to HTTP client request. Values are port number 80 or enter a number from 1025–65535 Default is port 8080
Enable HTTPS Client Requests	Configures the router to accept and respond to HTTP client request. Values are port number 443, or enter a enter from 1025–65535 Default is port 8443

JSON Web Signature	Configures RESTful API options. JSON Web Token (JWS) is an Internet standard way to securely transfer information between devices as a JSON object. This information can be verified and trusted because it is digitally signed. JSON Web Tokens (JWTs) can be signed using an algorithm or a public/private key pair.
JWS Algorithm	Select an algorithm: • none, ES256, ES384, ES512, HS256,HS384, HS512, PS256, PS384, PS512, RS256, RS384,RS512
JWS Key	Import the key via the terminal screen. To end the entry type ”quit” on a blank line.
JWT Claims	
Audience Claim	Configure the identity of the recipients that the JWT is intended for. This tends to be the “client id” or “client key” of the application that the JWT is intended to be used by. It allows the client to verify that the JWT was sent by someone who actually knows who they are.
Expiration Time Claim(s)	Configure the expiration time on and after the JWT must not be accepted for processing. Values are 1–3153600 seconds
Issued at Claim	Configure the time the JWT will start to be accepted for processing.
Issuer Claim	Configure the principal that issued the JWT.
JWT ID Claim	Configure the unique identifier of the token. (case sensitive).
Not Before Claim/s	Configure the time JWT will start to be accepted for processing. Values are 1–31536000 seconds Default is 31536000 seconds
Subject Claim	Configure the Identify the subject of the JWT.

OCI Containers

To enable or disable the OCI container management feature, you must reboot the router for the option to take affect. Disabling container management will delete all container configuration.

OCI Container Management	
After next restart	Configures the OCI container management feature. All container options will be visible after the reboot. • Enable container management • Disable container management Note: any containers set to enable will run after a router reboot

IP Passthrough

This feature provides a method for using the router as an LTE Modem. When a device, such as a PC, or another router is connected to an Ethernet port, that device is given the IP address provided by the cellular network. All data is passed straight through to and from the device to the cellular network.

When operating in this mode, most of the router configuration is ignored and some menu and options are not available to you. Routing, firewalls or other functions are not activated.

IP Passthrough is supported on either the Ethernet port or the USB-C port configured as Ethernet. A reboot is needed to enable and disable this feature.

IP Passthrough	
Enable	This enables IP passthrough mode and reboots the router. After the reboot, any non IP passthrough commands become invalid. If you issue a copy running-config to startup-config, the non IP passthrough commands are lost. You should save your current running configuration to another file for safety. This feature requires a reboot. Default is disabled
Router Management IP Address	The device connected to the Ethernet receives the address from the cellular connection. However, the router itself is still addressable for management purposes using this IP address. Default IPv4 address is 192.168.0.1
Restrict to specific MAC hardware address	If unchecked, the router passes through to the first device connected with Ethernet. If checked the router only passes through to the specified device with this MAC address. Default is disabled
MAC Address	MAC address of device in IP Passthrough mode.

Logging

The router can log event messages to:

- its local volatile "buffered" memory log
- a file stored on the router’s non-volatile flash memory
- an external Syslog server
- telnet/SSH sessions
- the console port

Logging is enabled by default.

Logging	
Enable logging	**Enable or disable the logging feature.**
General	
Include sequence number in log messages	**Whether or not to include sequence numbers in the log messages.**
Limit log rate to messages/per second	**Sets receive messages.** **Values are 1–1000 messages/second** **Default logging rate-limit is disabled**
....except messages with a severity of x or higher	• **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notification** • **Informational** • **Debugging**

Timestamp	
Include timestamp in log messages **Timestamp type**	**Enable timestamps in log messages. Select timestamp type and include information.** • **Uptime or Date/time** • **Include milliseconds** • **Include year** • **Include time zone** • **Use local time or UTC time**

Syslog	
Enable logging to Syslog hosts	**Enable/disable the sending of messages to one or more IPv4 or IPv6 Syslog servers.**

Level	- Emergency - Alert - Critical - Error - Warning - Notification - Informational - Debugging
Syslog source interface	Specify the source address in logging transactions from the drop-down list.
Syslog facility	You can append the hostname, an IP address, or a text string to Syslog messages that are sent to remote Syslog servers. - Kernel, User, Mail, Daemon, Authorization, Syslog, LPR, News, UUCP, System 9, System 10, System 11, System 12, System 13, System 14, Cron, Local 0, Local 1, Local 2, Local 3, Local 4, Local 5, Local 6, (default), Local 7
Origin ID Source	Add origin ID source. Select from the drop-down list. - None - IP - IPv6 - Hostname - Custom
Custom Origin ID	Add custom origin ID to source. Create your own custom origin ID. - hostname - IP address - text string
Append delimiter to syslog messages over TCP	Enable to add delimiter to syslog messages.
Syslog (Add, Edit, Delete)	
Hostname/IP address	Hostname or IPv4/IPv6 address.
Resolve hostnames to	- IPv4 - IPv6

Transport	Choose a transport method. • UDP • TCP
Port	Port number for the Syslog messages. Values are 1 to 65535 Default is 514

Console

Enable logging on the console port	Only available on models with a console port. Enables or disables the ability to output the log messages to the console.
Level	The default setting is enabled. • Emergency • Alert • Critical • Error • Warning • Notification • Informational (default) • Debugging

Telnet/SSH

Enable logging on Telnet/SSH sessions Level	Enables or disables the ability to log messages to the current virtual, (vty, SSH, or telnet) sessions. The default setting is enabled.Emergency • Emergency • Alert • Critical • Error • Warning • Notification • Informational (default) • Debugging

Buffered

Enable buffered logging	Enables or disables the ability to log messages to the internal RAM buffer and you can also specify the level of logging desired to be buffered and how much RAM to use.

Level	The default setting is enabled. • Emergency • Alert • Critical • Error • Warning • Notification • Informational (default) • Debugging
Maximum Size	Buffer size is 4096–32768 bytes. The default is 16384 bytes

File	
Enable logging Select from Flash: or USB Level	Enables or disables the ability to log messages to be stored on non-volatile memory (i.e. flash) . The router will only log messages to one file at a time, so if the command is repeated with a different filename, logging messages will stop being stored in the previous filename and start being stores as the new defined logging filename. The default setting is enabled. • Emergency • Alert • Critical • Error • Warning • Notification • Informational (default) • Debugging
Filename	Enter a logging file name.
Minimum Size	Configure the minimum size of the log file. Values are 1024–2147483647 bytes Default is 2048 bytes
Maximum Size	Configure the maximum size of the log file. Values are 4096–2147483647 bytes Default is 4096 bytes

EMAIL

Notifications generated by the router can be sent to one or more recipients via Email. Setting up the Email subsystem requires setting up the Email server (SMTP) and the list of recipients. Email is disabled by default.

Email	
Enable	Enables Email services.

Encryption	**Emails are to be encrypted using:** • **none** • **TLS**
From	**Configures "the from" Email address.**
SMTP Server Host	**Configures the IP Address of the SMTP host used to send the Email.**
SMTP Server Port	**Configures the SMTP host port number required for the connection.** **Values are 1 to 65535** **Default port is 25**
Username / Password	**User name and password required to authenticate with the SMTP server.**
Validate Email Certificate	**Validate the certificate provided by the SMTP server.**

Email Recipients (Add, Edit or Delete)	
Email Address	**Configures the Email address of the recipient.**
Email Subject Line	**Use the default subject line or configure your own.** **Default message is "Notification event from Perle IRG5000 Series Router".**
Notifications Sent	**List of notification categories sent to the recipient.** • **alarms, authentication, bgp, cellular-lte, lldp, bridge, entity, envmon, ipsec, openvpn, ospf, snmp, network watchdog, interface IP, software-update**
Send a TEST EMAIL message	**Configure a user email address, then press the TEST EMAIL button to send a test message to the user's email address.**

SMS

Overview

This feature is dependant on having a cellular interface which includes SMS support.

Your router supports SMS control and SMS two-factor authentication requests. Verify with your cellular provider that SMS functionality has been enabled.

SMS Control

Through SMS control, a validated user sends commands to the router and receives requested statuses. Users are validated either using a password prefixed with every request or by the phone number of the sending device used to generate the request or by both. When using email for two factor authentication, some email programs require you to set the parameter “allow less secure apps to connect” to receive SMS email messages. If the authentication method includes a password, you need to send the SMS command using this format.

<password> <command>

For example, if the user password was 54321 and you want to get a list of valid SMS command, you would send the following SMS message to the phone number of the IOLAN.

router**54321 help**

Note: SMS commands are not case sensitive and all white spaces are ignored.
The commands that are available to a user from SMS are:

SMS Commands	
help	**Returns a list of valid commands.**
Location	**Returns the GPS co-ordinates of the current device location and a Google map to the returned location.**
log	**Returns the last 16 entries of the system log file, each in a separate SMS message.**
lteconn	**Establish an LTE Data connection. The device returns an OK message to indicate the command has been performed.**
ltedisc	**Disconnects the LTE Data connection. The device returns an OK message to indicate the command has been performed. The LTE Status command indicates the current connection status.**
model	**Returns device model information.**
mreset	**Reset the modem portion of the device only. Both data and SMS connectivity are lost for up to 1 minute**
ltestatus	**Returns status specific to the LTE data connection.**
reload	**Reboots the device.**
status	**Returns general device information.**

SMS Notifications

SMS notifications generated by the router can be sent to one or more recipients via SMS.

Setting up the SMS notifications subsystem requires enabling SMS and configuring a list of users/recipients, then enabling the notifications feature for each.

SMS Settings	
Enable SMS	Enable or disable Short Message Service (SMS).
User Authentication Method	Only required for SMS control, this dictates the method used for authenticating all incoming requests. Note: all users automatically default to Admin privilege when authentication is disabled
None	No Authentication is required.
Password	User must provide a password on every text message.
Phone number	incoming messages are authenticate by the source phone number.
Both	Matching both phone number and password are required.

SMS Users (Add, Edit, Delete)	
Name	Enter a name for this SMS user. For identification only.
Privilege	Enter the User privilege. • Admin—Full SMS management user is able to reboot the router and see statuses • Restricted—User may solicit device status, but cannot reset, reload, or enable/disable cellular connections • No Admin—No router management access
Phone Number	User phone number. Only required if SMS authentication is enabled or configuring a notification recipient.
Password	User password. Only required if SMS authentication is enabled or configuring a notification recipient.

SNMP Notifications	**Notifications to be sent to this user. You may enable as many of the following notification types in the SNMP notification configuration as you want.** • **alarms** • **openvpn** • **authentication** • **ospf** • **bgp** • **snmp** • **cellular-gnss - (Model dependent)** • **cellular-lte—(model dependent)dot11—(Model dependent),** • **network-watchdog** • **interface IP** • **lldp** • **software-update** • **bridge** • **entity,** • **envmon**
Send a Test SMS Message	**Configure a user phone number, then press the TEST SMS button to send a test text to the user's cellular phone.**

Power Management

Overview

Only available on models with the Power Management Feature.

Power Management falls into 2 categories;

- Power savings while maintaining full functionality
- Standby mode to save power when communications are not required

Power savings while maintaining full functionality

The following is a list of power saving opportunities:

- **Enabling LED Low Power—**Reduces LED usage to save power.
- **Enabling Processor Low Power**—The microprocessor slows itself down when there is reduced activity on the router.
- **Ethernet Interface Disable—**Disabling, configuring at lower Ethernet speeds or enabling Energy Efficient Ethernet will use less power.
- **USB port**—disabling the USB port will use less power
- **RS232**—disabling TTY1 will use less power
- **RS485**—disabling TTY2 will use less power
- **GNSS Receiver Disable—**Shutting down the GNSS Radio saves power if location services are not needed.
- **Cellular—Radio Enable—**Disabling the cellular radio saves power.
- **Cellular—Module Power Up—**If the module is not powered up neither LTE nor GNSS functions are available. Maximum power savings if these are not needed.

Standby—When in standby mode, the router is essentially powered off. The microprocessor runs to monitor the internal and external environment to determine when to power the router back up and take it out of standby mode. When the router is in standby mode, it displays a amber System LED blip. Pressing the reset button takes the router out of standby mode and powers it up.

Power Management	
Enable Processor Low Power mode	**Enables or disables processor mode.** **The microprocessor slows itself down with reduced activity on the router.**
Enable LED Low Power	**Enables or disables LED low power mode.** **Reduces LED usage to save power.**
Power Consumption Summary	**Display current Power Consumption Summary.**
Power Operating Mode	
Mode of Operation	• **Standard** • **Ignition** • **Smart Standby**
Standard	**In this mode the router does not go into Standby mode. (Default)**
Ignition	**In this mode the router monitors an input to determine if the vehicle ignition switch is turned on or not (see Deployment documentation in the Hardware Installation Guides for information on how to make appropriate connections). When the ignition is determined to be on, the router wakes from standby, and when the ignition is determined to be off, it goes into standby mode.**
Contact	**The input used for monitoring the ignition voltage.** • **IGN–Ignition Input on power connector** • **GPIO–GPIO pin on the power connector** **Note: The GPIO pin needs to be configured to be an analog input. (See I/O section)**
Standby Delay	**If the router detects that the “contact voltage” has remained either “less then” or “greater than” the standby voltage level for this number of seconds then the router goes into “Standby” mode.** **Default is 30 seconds**

Wakeup Delay	If the router detects that the “contact voltage” has remained either “less then” or “greater than” the wakeup voltage then the router is taken out of standby and is powered back up. Default is 1 second
Change Default Voltages	
Standby when Voltage	Sets the comparison operator and “standby voltage” used for monitoring the “contact voltage”. Default is less then 9V
Wakeup when Voltage	Sets the comparison operator and “wakeup voltage” used for monitoring the “contact voltage” Default is greater then 10.8V
Smart Standby	In this mode the router can be setup to monitor 1 or 2 condition(s) to determine when to initiate and exit standby mode. These conditions can be either AND’d or OR’d
Condition Type	The type of condition monitored. • Analog–Analog input • Digital–Digital input • Schedule–The actual date and time is monitored and used to determine when this condition is true
Condition Type: Analog Input	
Contact	The input is used for monitoring the analog input. • 1–IGN (Ignition Input on power connector) • 2–GPIO (GPIO pin on the power connector) Note: the GPIO pin needs to be configured to be an analog input. See *I/O* section.
Standby Delay	If the router detects that the “contact voltage” has remained either “less then” or “greater than” the standby voltage level for this number of seconds then the router goes into “Standby” mode. Default is 30 second

Wakeup Delay	If the router detects that the "contact voltage" has remained either "less then" or "greater than" the wakeup voltage then the router is taken out of standby and is powered back up. Default is 1 second
Standby when Voltage	Sets the comparison operator and "standby voltage" used for monitoring the "contact voltage". Default is 9.0V
Wakeup when Voltage	Sets the comparison operator and "wakeup voltage" used for monitoring the "contact voltage". Default is 10.8V
Condition Type: Digital Input	
Contact	The input monitored for this condition. • GPIO—GPIO pin on the power connector Note: The GPIO pin needs to be configured to be a digital input. (See I/O section)
Wakeup Trigger	Define the digital input condition (trigger) that initiates the wakeup. The opposite value initiates going into standby. Open—Detect connected digital contact switch is open Closed—Detect connected digital contact switch is closed The default is Open
Wakeup/Standby Delay	The amount of time the trigger state must remain before waking up from or entering into standby mode. Values are 1 to 30 seconds Default is 1 second
Condition Type: Schedule	
Frequency	Sets up the base by which you would like to schedule the occurrence of change in wakeup and standby mode. • Daily: Define a daily power schedule • Hourly: Define an hourly power schedule The default is hourly
Hourly Wakeup Time	Specify the minute of the hour that the router wakes up from standby mode and the minute of the hour that the router goes into standby mode

Wakeup/Daily Standby Time	Specify the time of day using the 24 hour clock in the HH:MM format that the router wakes up from standby mode and the time of day the router goes into standby mode.
Repeat	How often to repeat the schedule in days or hours, depending on the type of schedule defined. Default is not to repeat
Condition Expression	This field exists if more than one condition is defined. It is used to determine what causes the power state change to occur. • OR—If “condition 1” or “condition 2” is true it causes the power state to change. • AND—Both “condition 1” or “condition 2” needs to be true before the power state occurs.
Low Voltage Standby	
Low Voltage Standby (LVS) is a battery saving feature to monitor the input voltage (presumably from a battery). If the voltage remains below the configured “standby voltage” for the configured “standby delay”, the router is put into standby mode. This protects the battery from further drain. If the voltage is restored, the router will take itself out of standby and power back up.	
Contact	The input for monitoring the low voltage. • IGN–Ignition Input on power connector • GPIO–GPIO pin on the power connector. Note: The GPIO pin needs to be configured for analog input. (See I/O section)
Standby Delay	If the router detects that the “contact voltage” has remained either “less then” or “greater than” the standby voltage level for this number of seconds then the router goes into “Standby” mode. Default is 30 seconds
Wakeup Delay	If the router detects that the “contact voltage” has remained either “less then” or “greater than” the wakeup voltage then the router is taken out of standby and is powered back up. Default is 1 second
Change Default Voltages	
Standby when Voltage	Sets the comparison operator and “standby voltage” used for monitoring the “contact voltage”. Default is less then 1.0V

Wakeup when Voltage	**Sets the comparison operator and "wakeup voltage" used for monitoring the "contact voltage"** **Default is greater then 9V**

I/O

Overview

Depending on the model, your router may have a combination of an analog input, digital inputs, digital outputs, and relays. This section describes the configuration parameters that can be defined for these different types of I/O's.AI (Contact 1)—On models that have this analog input, it is located on the unit with the connector marked as AI. The router monitors the differential voltages between Pin1 and Pin 4. Pin 1 (AI+) can monitor different type of input voltages coming from devices like temperature sensors, batteries and so on.

IGN (Contact 1)—On models that have this analog input, it is located on the power input connector. In a vehicular application this input would typically be used to monitor the vehicle ignition, however it can be used as a general-purpose analog input also. As an analog input, the voltage read may not always be useful. An example would be an analog input from a thermometer. A more meaningful reading in this case would be degrees Celsius or Fahrenheit. In order to transpose the read voltage to a more meaningful unit of measurement, the following formula can be used; **Transpose Value = mx + b =** coefficient * voltage read + offset

Coefficient—(- 2147483.647 – 2147483.646)

This value can be found in the guide for the equipment you have connected to the analog input.

- Value used as the coefficient m in the formula y = mx + b
- Allows fractions up to 3 decimal points, for example 23.521
- Default is 1

Offset—(- 2147483.647–2147483.646)

The difference between a 0 volt reading and the equivalent value for the units being measured. If for example we are measuring temperature in degrees Celsius, and 0 volts represents -40 degrees, the offset would be -40.

- Integer value used as the offset b in the formula y = mx + b
- Allow fractions up to 3 decimal points, for example 23.521

Default is 0

Units—string that describes the transposed value.

I/O: AI (Contact 1)

Description	A description to help you identify the equipment being monitored. Default is External alarm contact 1.
Analog Input Transformation	See formula above.
I/O: IGN (Contact 1)	
Description	A description to help you identify the equipment being monitored. Default is External alarm contact 1.
Analog Input Transformation	See formula above.

I/O: GPIO (Contact 2)	
Description	A description helps you identify the equipment being monitored. Default is External alarm contact 2
Direction	The direction can be configured as an analog or digital input contact or a digital output.

Digital Input	
Power Source	How is the input powered? • Wet—Pull-up disabled, open voltage supplied externally • Dry—Pull-up enabled, closed we supply the voltage Default is wet

Pulse Counter	
Pulse Mode	Digital Inputs can also be used as a pulse counter. The counting can be done either on complete pulses or on transitions. • Pulses—count full pulses
	• Transitions—increment the count on every transition Default is pulses
Analog Input Transformation	See formula above. Note: This parameter only applies if the input is analog and if you wish to transform the voltage read into a meaningful unit of measurement.

Contact A	
Description	AUX-IO: Digital Input
Digital Input	
Power source	How is the input powered? • Wet—Pull-up disabled, open voltage supplied externally • Dry—Pull-up enabled, closed we supply the voltage Default is wet
Pulse Counter	
Pulse Mode	Digital Inputs can also be used as a pulse counter. The counting can be done either on complete pulses or on transitions. • Pulses—count full pulses • Transitions—increment the count on every transition Default is pulses

Contact B	
Description	AUX-IO: Digital Input

Digital Input	
Power source	How is the input powered? • Wet—Pull-up disabled, open voltage supplied externally • Dry—Pull-up enabled, closed we supply the voltage Default is wet
Pulse Counter	
Pulse Mode	Digital Inputs can also be used as a pulse counter. The counting can be done either on complete pulses or on transitions. • Pulses—count full pulses • Transitions—increment the count on every transition Default is pulses

Interfaces

Introduction

Interfaces are networking communication ports for your computer. Each interface is associated with a physical or virtual networking device.Your router supports a number of different types of interfaces and each interface has its own characteristics and capabilities. Not all physical interfaces described below are available on all models and the number of interfaces for a particular interface type may vary as well. Some configuration parameters may also be different on some models or running software.

Physical Interfaces

Ethernet

Ethernet interfaces connect to devices, switches, or other routers. They are used as a gateway to a LAN or to provide WAN functionality to routers. MAC addresses for Ethernet/ SFP ports are based on the label attached to the IOLAN. SFP 1 is the first MAC address as printed on the label, SPF 2 is plus 1 of the first address, then Ethernet port 1-x, you continue to add a 1 thereafter.

See your Hardware Installation Guide for hardware features of your model.

Virtual Interfaces

VLAN

Each Ethernet interface can support sub-interfaces, which in turn support the transport and segregation of VLAN traffic. For example if Ethernet 1.51 is defined, the traffic on the sub interface is associated with and tagged as belonging to VLAN 51.

Bridge

A bridge connects several interfaces together to behave as a single Local Area Network (LAN). All devices attached to any of the interfaces in the bridge are all part of the same broadcast domain. They share a common IP address and subnet. You must remove the interface from the bridge, to use the interfaces individually.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside. PPPoE allows Internet Service Providers (ISPs) to manage access to accounts via user names and passwords. You can virtually “dial” from one node to another over an Ethernet network to establish a client to server point to point connection, then transport data packets over that connection.

Tunnels

Your router supports three types of tunnels:

- **Generic Routing Encapsulation (GRE)—**Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links or point-to-multipoint links over an Internet Protocol network.

- **OpenVPN—**uses VPN techniques to secure point-to-point and site-to-site connections.The OpenVPN protocol is responsible for handling client-server communications. Basically, it helps establish a secure “tunnel” between the VPN client and the VPN server. OpenVPN handles encryption and authentication. It also, can use either UDP (User Datagram Protocol) or TCP (Transmission Control Protocol) to transmit data.
- **6in4—**6in4 tunnels are configured between border routers or between a border router and a host. The simplest deployment scenario for 6in4 tunnels is to interconnect multiple IPv6 sites, each of which has at least one connection to a shared IPv4 network. This IPv4 network could be the global Internet or a corporate backbone.

Port Channels

Your router allows you to group multiple physical interfaces into one logical interface, thereby providing each channel a higher aggregated bandwidth, load balancing, and/or link redundancy.

VRRP

Your router supports the Virtual Router Redundancy Protocol (VRRP). This networking protocol provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP sub-network.

SFP ports

Your SFP ports and their corresponding SFP modules can facilitate high-speed data communications over extended distances in a variety of applications. They are often used to connect a 1-gigabyte network switch to another, which, in turn, increases the size and improves the functionality of a network.

(OCI) Containers

Your router supports the Open Container Initiative (OCI) software management container feature. Simply put, a software container bundles an application’s code together with the related configuration files and libraries, and all dependencies required for a application to run. By using our OCI container management system, you are able to load images, create containers, configure private registry credentials, and manage multiple containers, conveniently, and easily.

Your router allows you to deploy and run (OCI) compatible containers from both public and private container registries, such as Open Containers, GitHub and Docker Hub. Perle router’s support the following OCI container specifications:

1. the Runtime Specification (runtime-spec)
2. the Image Specification (image-spec)
3. the Distribution Specification (distribution-spec)

Perle provides a publicly available repository of sample python scripts that can be used in containers in your router. These samples can be used as a code base for you to start developing custom containers.

https://github.com/Perle-Systems-Limited/container-sample

Interface Parameters

WLAN (Wireless Radio)	
Enable	Enable or disable the wireless LAN or WIFI interface. This interface cannot be deleted. Default is enabled
Description	Provide a description for this interface.
Mode	Select Access Point or Client mode. • Access Point (Default)—This interface can used as a access point that allows LoT devices to connect to the network and also can serve as the point of interconnection between the WLAN and fired wire networks (Ethernet). • Client—Allows your router to be a client that connects to an Access Point.
Mode (Access Point)	
Region	Select the region of operation for the WiFi modem. For a complete list, please see --> *Appendix—Regions*
Radio Mode	Select: • 2.4 GHz (default) • 5GHz.
Wireless Mode	For 2.4GHz select: • 802.11 b • 802.11 g (default) • 802.11 n
Wireless Mode	For 5GHz select: • 802.11 a • 802.11 ac, • 802.11 n (default)

Channel	For 802.11 g/b/n select the channel for 2.4GHz communications the default channel is 11. Values are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (default) or least congested. For 802.11 a select channel for 5 GHz communications, the default channel is 36. Values are 36, 40, 44, 48, 149, 153, 157, 161 For 802.11 a/ac/n select channel for 5GHz communications, the default channel is 36. Values are 36, 40, 44, 48, 149, 153, 157, 161
802.11 n	
Channel width option	Select: • 40/20 MHz (Auto) • 20 MHz only
Maximum A-MSDU length	Select: • 3839 • 7935
Auto power save	Set WMM-PS unscheduled automatic power save delivery. Default is disabled
Channel width	Select: • 20 MHz • 40 MHz above primary • 40 MHz below primary
DSSS-CCK mode	Enable or disable. Default is disabled
LDPC coding capabilities	Use LDPC coding capabilities. Default is disabled
Require stations to support HT	Reject association if stations do not support HT PHY.
Short Guard interval capacity	Select short guard interface capabilities. • default • 20 • 40

Set receiving PPDU using STBC	Set receiving PPDU using STBC. Enable or disable. Default is disabled.
Set transmitting PPDU using STBC	Set transmitting PPDU using STBC. Enable or disable. Default is disabled
802.11 ac	
Set fix antenna-pattern	Set fix antenna pattern during the lifetime of an association. Enable or disable. Default is disabled
Use default VHT operating channel center frequent	VHT operating channel center frequency. Range is 1–173 Default is 42
LDPC coding capabilities	Use LDPC coding capabilities.
Maximum MPDU length	Select: • 3839 (default) • 11454 • 7991
Maximum MPDU-exp length	Select maximum mpdu-exp length. Range is 0–7 Default is 0
Require stations to support VHT	Enable if stations must support VHT.
Short guard interval capabilities	Set short guard interval capabilities. • 20 • 40 • 80
Set receiving PPDU using STBC	Set receiving PPDU using STBC. Default is disabled.
Set transmitting PPDU using STBC	Set transmitting PPDU using STBC. Enable or disable. Default is disabled

Mode (Client)	
Region	See “Access Point Region” above.
SSID profile	Select SSID or create a new profile. Provide a description for this interface. Name can be up to 32 characters long. Maximum profiles is 16.
Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
DHCP Client	For detailed parameter descriptions see *DHCP Client*
DHCP Server	For detailed parameter descriptions see *DHCP Server*
IPv6 Neighbor Discovery	
Router preference	Set the default router preference. A High value means this router will be preferred. • High • Medium • Low Default is medium
Managed config flag	Hosts should use DHCP for address config. Enable or disable config flags. Default is disabled
Other config flag	Hosts should use DHCP for non-address config. Enable or disable config flags. Default is disabled
DAD attempts	To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1

Reachable time	**Specify the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation Default is 0 (unspecified by this router) Range is 0-360000 milliseconds**
Retransmission time	**The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 1–3600000 in milliseconds Default is 0**
IPv6 Routing Prefix Advertisement	
Add Prefix	
Address	**Configure an IPv6 address.**
Prefix length	**Configure the prefix length. Range is 0–128**
Valid lifetime	**This value applies to the device's usefulness as a default router. It does not apply to other information contained in the RA message. IPv6 hosts receiving the RA message should install the default route with an expiry time set to the lifetime. A lifetime of 0 indicates that the router is not a default router anymore and associated default route should be discarded from host's routing table. Range is 1–4294967294 in seconds or infinite Default is 259200 in seconds (30 days)**
Preferred lifetime	**Specify how long the prefix generated by stateless autoconfiguration remains preferred. Range is 1–4294967294 seconds or infinite Default is 604800 (7 days)**
Do not use prefix for onlink determination	**A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off**
Do not use prefix for autoconfiguration	**The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Enable or disable prefix for autoconfiguration. Default is off**
IPv6 Routing Advertisement Control	

Suppress IPv6 router advertisement	Enable or disable IPv6 Router advertisements. Default is sent router advertisements
Hop limit	The hop-limit option—Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
RA interval	The maximum time interval between sending unsolicited multicast router advertisements from the interface, in seconds. Max range is 4–1800 in seconds Default is 600 seconds
Minimum interval	The minimum time interval between sending unsolicited multicast router advertisements from the interface, in seconds. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 3–1350 in seconds
RA lifetime	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router, it does not apply to information contained in other message fields or options. Range is 4–9000 seconds Default is 1800 seconds
Add DNS	
Address	Add IPv6 address of a DNS server.
General Settings	
Role	Used for controlling admin access. Options: • LAN • WAN • TRUSTED Default is LAN

MTU size	Optional: provide an MTU size. Range is 64–9000 Default is 1500
Wireless Network	
Interface type—Wireless Network SSID:	
Enable	Enable wireless network.
Description	Description of this wireless network profile.
Enable Hotspot	
Settings	
Address	Enter the hotspot name on the subscriber network.
Mask	Enter the netmask.
Location	Configure the location name.
Organization Name	Configure an organization name.
Limit bandwidths uploads	Configure maximum bandwidth upstream in bps (bytes per second). Values are 1–4294967295
Maximum idle time	Re-authenticate the user if idle for x minutes. Value 1–240 in minutes
Maximum Session time	Re-authenticate the user after x minutes. Value 1–240 in minutes
Authentication	Authentication method • None • Local • RADIUS • UAM
DNS server 1	DNS server address 1.
DNS server 2	DNS server address 2.

RADIUS settings	
RADIUS server 1	Configure the address of the RADIUS server.
RADIUS server 2	Configure the address of the second RADIUS server.
RADIUS secret	Configure shared secret between the RADIUS server and your router.
UDP port for accounting requests	Configure the UDP port number to use for radius accounting messages. Values are 1–65535 Default port is 1813
UDP port for authentication requests	Configure the UDP port number to use for RADIUS authenticating requests. Values are 1–65535 Default port is 1812
UAM settings	
Login URL	Configure login URL to use on UAM server. Default is https://customer.hotspotsystem.com/customer/hotspotlogin.php
NAS ID	Your ID on the UAM server.
TCP port for authentication clients	Enter the TCP port for authenticating clients. Values are 1025–64435 Default is 3990
TCP Port for embedded content	Port to bind for serving embedded content. Values are 1025–65535 Default is 4990
UAM shared secret	Enter the shared secret between the UAM server and the router.

Heartbeat settings	When enabled, the heartbeat is sent: • mac—the MAC address of your router • nasid—the NAS/Gateway ID of the router which should be entered in the UAM • os_date—in string format the type of router and firmware version running • uptime—the uptime and system load average of your router
Interval to send the heartbeat	Configure the interval value for heartbeat information to be sent to the configured URL. Values are 15–60 minutes. Default is 60 minutes.
Heartbeat URL	Sent heartbeat information to this URL.
Users	
Username	Configure a user to add to the hotspot users database.
Password	Configure a password for this hotspot user.
Allowed MAC Addresses	
MAC address	Allow these MAC addresses without authentication. Value is xxxx.xxxx.xxxx
Files	
Footer	Specify—the file to use for the footer that displays below every page.
Icon	Specify—the file that contains the icon image 123px by 39px.
Login message	Specify—the file that contains the login message between the header and the form on the login page.
Login footer message	Specify—the file that contains the login footer between the form the footer on the login.
Title	Specify—the file that contains the title for the page.

TOS	Specify—the file that contains the Terms of Service agreement (TOS).
Allowed Host and Domains	
Domain	Configure a domain name to add.
URL	Configure a URL to add.
Enable IP Address	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
IPv6 Neighbor Discovery	
Manage config flags	Hosts should use DHCP for address config. Enable or disable config flags. Default is disabled
Manage other config flags	Hosts should use DHCP for non-address config. Enable or disable config flags. Default is disabled
DAD attempts	To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
Reachable time	Specify the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation. Default is 0 (unspecified by this router) Range is 0-360000 milliseconds
Retransmission time	The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 1–3600000 in milliseconds Default is 0
IPv6 Routing Prefix Advertisement	

Add Prefix	
Address	Configure an IPv6 address.
Prefix length	Configure the prefix length. Range is 0–128
Valid lifetime	This value applies to the router's usefulness as a default router. It does not apply to other information contained in the RA message. IPv6 hosts receiving the RA message should install the default route with an expiry time set to the Lifetime. A Lifetime of 0 indicates that the router is not a default router anymore and associated default route should be discarded from host's routing table. Range is 1–4294967294 in seconds or infinite Default is 259200 in seconds (30 days)
Preferred lifetime	Specify how long the prefix generated by stateless autoconfiguration remains preferred. Range is 1–4294967294 in seconds or infinite Default is 604800 (7 days)
Do not use prefix for onlink determination	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
Do not use prefix for autoconfiguration	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Enable or disable prefix for autoconfiguration. Default is off
IPv6 Routing Advertisement Control	
Suppress IPv6 router advertisement	Enable or disable IPv6 router advertisements. Default is sent router advertisements
Hop limit	hop-limit—Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64

RA interval	The maximum time interval between sending unsolicited multicast router advertisements from the interface, in seconds. Maximum range is 4–1800 in seconds Default is 600 seconds
Minimum interval	The minimum time interval between sending unsolicited multicast router advertisements from the interface, in seconds. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 3–1350 in seconds
RA lifetime	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn't appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message. fields or options. Range is 4–9000 seconds Default is 1800 seconds
Add DNS	IPvv6 address of DNS server.
Role	Used for controlling admin access. Options: • LAN • WAN • TRUSTED Default is LAN
MTU size	Optional: provide an MTU size. Range is 64–9000 Default is 1500
Log the following events	• Link status • IP Address Change
Send SNMP traps for the following event	• Link status • IP Address Change

Ethernet Interface	
Enable/Disable	Enabled or disabled this interface. Default is enabled.
Description	Provide a description for this interface.
Ethernet Options	
Link negotiation	Auto—negotiation of Ethernet parameters. Fixed—select if your setup requires a fixed speed and duplex settings. Not configurable on USB-Ethernet port.
Fixed speed (Mbps)	Select a speed of 10, 100, 1000. Both ends of the connection must be set to the same speed. Not configurable on USB-Ethernet ports.
Fixed duplex	Select half or full duplex to match the connection on both ends. Not configurable on USB-Ethernet port.
IPv4 address	
DHCP	Your IP address is assigned from a DHCP server.
Static	Provide an IPv4 address and netmask for this interface.
IPv4 Secondary Addresses	Provide additional IPv4 addresses and network masks for this interface.
DHCP Client	
Hostname	This can be any string. By default, this is the device name.
Default Route Distance	Default route distance is a value that your router uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. A static route is normally set too 1. The smaller the default route distance, the more reliable the protocol. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown. Default: 210 Values: 1-255

Class ID	Specify Class ID: • Auto • Specify Specify a Class-id string, truncated to 200 characters. The same string or text is configured on the server side associated with an address to give the client. Default: Auto
Client ID	This can be configured as Ethernet, ASCII text, Auto, or HEX value. Ethernet values 1-5 option—60—Vendor class identifier <oem-name>:<model>:<serial#> in ASCIIRouter example: Perle:IRG5541:350-01T00003
DHCP Server	Enable or disable the DHCP server.
Pool name	Configure a pool name.
Network	Configure a network name for this DHCP pool.
Netmask	Configure a network mask.
Start	Configure the start address for this pool.
Stop	Configure the end address for this pool.
Default Gateway	Configure the default gateway.
DNS	Configure a DNS server.
Select how to obtain the IPv6 address: Note: not all interfaces support all addressing methods for IPv6	
IPv6 address	
DHCP	• DHCP—obtain an IPv6 address using DHCP

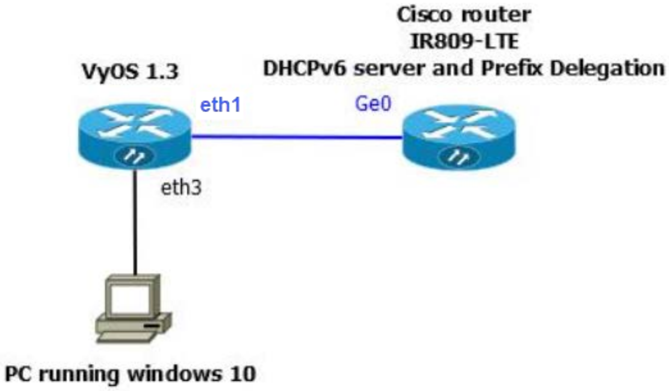
IPv6 (Request prefix delegation)	• Prefix delegation— • PD name—configure a name for this prefix • PD ID#—specify a unique instance (0-65535) • Prefix length—length of prefix (48-64)
IPv6 address (Auto configuration)	• Obtain an address using Auto Configuration.
IPv6 address (Delegated)	• PD name—select PD name from the drop-down box • SLA length—interface site-level aggregator (SLA) length • SLA-ID—specify a decimal integer which fits in the length of the SLA length • address used to form the IPv6 interface address or EUI-64 EUI-64 is the Default
IPv6 address (Static)	• Add static addresses for this interface • Address—in format X:X:X:X::X
IPv6 Neighbor Discovery	Select the router's default preference. A high value means this route will be preferred. • High • Medium • Low Default is Medium
Manage config flag	Hosts should use DHCP for address config. Enable or disable config flags. Default is disabled
Manage other config flag	Hosts should use DHCP for non-address config. Enable or disable config flags. Default is disabled

DAD attempts	To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
Reachable time	Configure the length in time (milliseconds) a node assumes a neighbor is reachable after receiving a reachability confirmation. Default is 0 (unspecified by this router) Range is 0–360000 milliseconds
Retransmission time	Configure the retransmission timer to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 1–3600000 in milliseconds Default is 0
IPv6 Routing Prefix Advertisement	
Add Prefix	
Address	Configure an IPv6 address.
Prefix length	Configure the prefix length. Range is 0–128
Valid lifetime	This value applies to the device usefulness as a default router. It does not apply to other information contained in the RA message. IPv6 hosts receiving the RA message should install the default route with an expiry time set to the Lifetime. A Lifetime of 0 indicates that the router is not a default router anymore and associated default route should be discarded from host's routing table. Range is 1–4294967294 in seconds Default is 259200 in seconds (30 days) Infinite—lifetime never expires
Preferred lifetime	Configure how long the prefix generated by stateless autoconfiguration remains preferred. Range is 1–4294967294 seconds Default is 604800 (7 days) Infinite—lifetime never expires

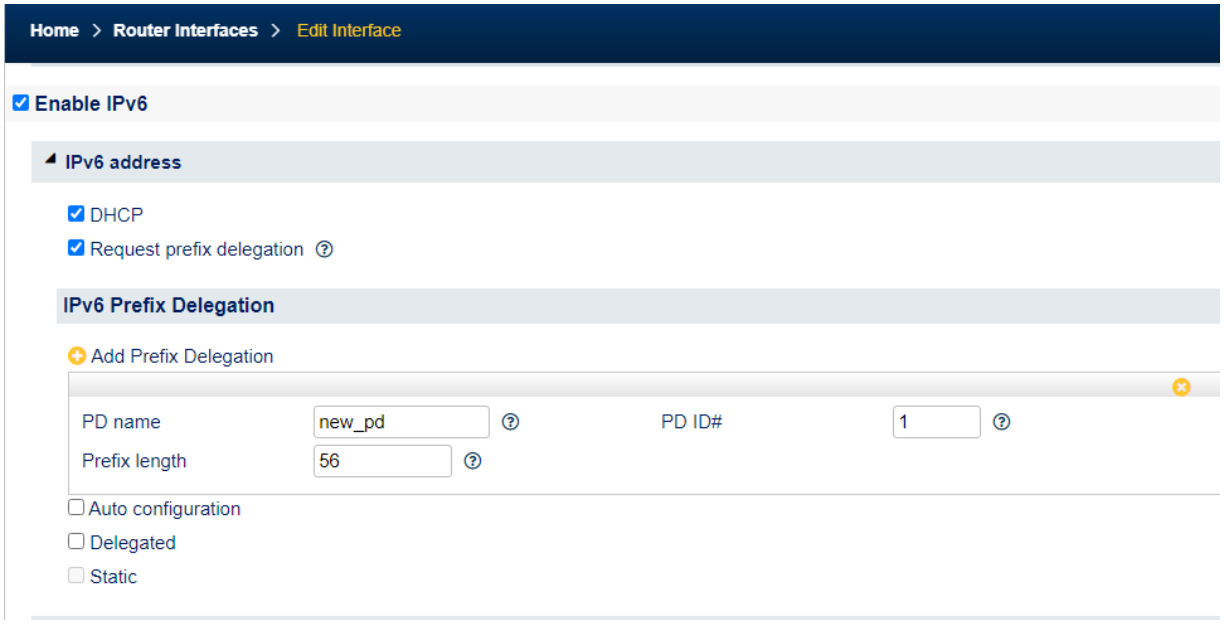
Do not use prefix for onlink determination	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
Do not use prefix for autoconfiguration	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Enable or disable prefix for autoconfiguration. Default is off
IPv6 Routing Advertisement Control	
Suppress IPv6 router advertisements	Enable or disable IPv6 router advertisements. Default is “enable” (send router advertisements)
Hop limit	Configure the hop count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
RA interval	Configure the maximum time interval between sending unsolicited multicast router advertisements from the interface, in seconds. Max range is 4–1800 in seconds Default is 600 seconds
Minimum interval	Configure the minimum time interval between sending unsolicited multicast router advertisements from the interface. Range is 3–1350 in seconds Default is 198 seconds
RA lifetime	Configure the lifetime associated with the default route. A value of 0 indicates that the route is not a default route and doesn’t appear on the default route list. The route lifetime applies only to the route's usefulness as a default route; it does not apply to information contained in other message fields or options. Range is 4–9000 in seconds Default is 1800 in seconds
Add DNS	Configures the address of the Domain Name Server (DNS).
Address	Add IPv6 address of DNS server.

Role	Configure the role for this interface. • WAN • LAN • TRUSTED Default is LAN
MTU size	Provide an Maximum Transmission Unit (MTU) size. Values are 1280-9000 Default is 1500
Log the following events	• Link status • IP address change
Send SNMP traps for the following events	• Link status • IP address change

IPv6 Prefix Delegation example configuration



Configuration Parameters for Eth1 interface



☑ Enable IPv6

IPv6 address

☑ DHCP

☑ Request prefix delegation

IPv6 Prefix Delegation

Add Prefix Delegation

PD name: new_pd

PD ID#: 1

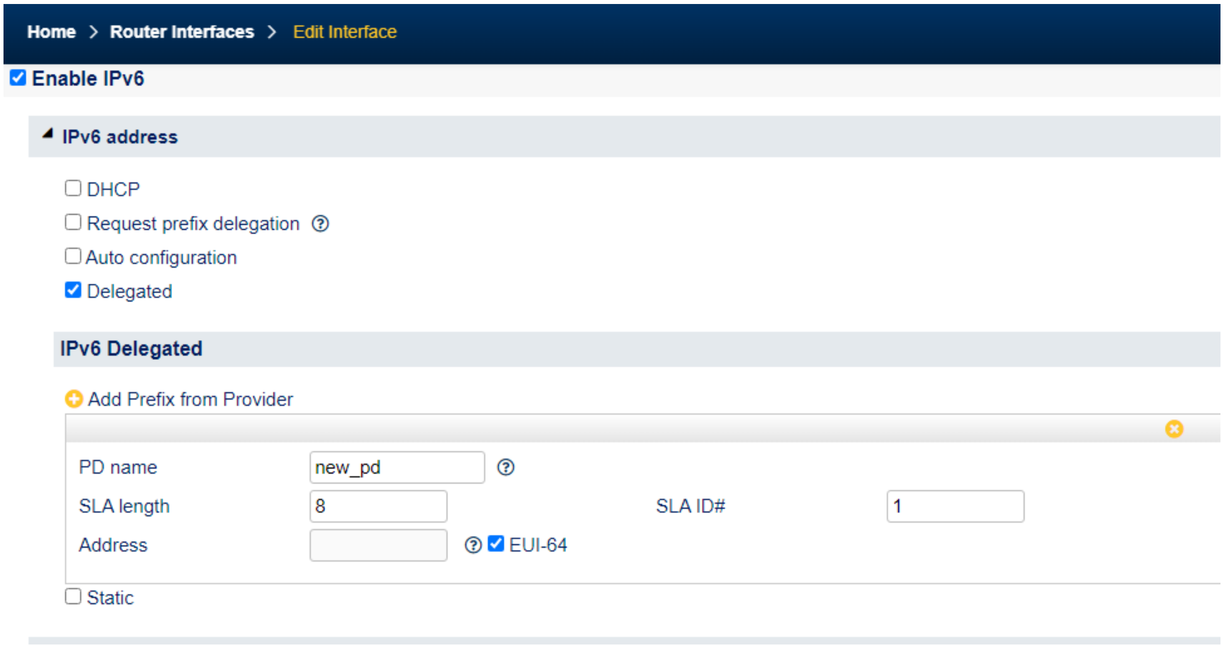
Prefix length: 56

□ Auto configuration

□ Delegated

□ Static

Configuration Parameters for Bridge interface



☑ Enable IPv6

IPv6 address

□ DHCP

□ Request prefix delegation

□ Auto configuration

☑ Delegated

IPv6 Delegated

Add Prefix from Provider

PD name: new_pd

SLA length: 8

SLA ID#: 1

Address: ☑ EUI-64

□ Static

Configuration on Cisco router as a dhcpv6 server and PD

```
ipv6 dhcp pool test6
prefix-delegation pool pd-test6
address prefix 2001:2::/40
dns-server 2001:DB8:3000:3000::42
domain-name example.com
!
```

```
ipv6 local pool pd-test6 2001:78::/40 56
interface GigabitEthernet0
ipv6 address 2001:2::80/40
ipv6 enable
ipv6 nd other-config-flag
ipv6 dhcp server test6
```

```
PerleRouter#show ipv6 interface
Interface   IPv6 Address                      Admin        Status      Link
Status  Description
------------------------------------------------------------------------------------------
lo       fe80::200:ff:fe00:0/64                  up           up
         ::1/128
eth1    2001:1::240:2ff:fe00:450/64              up           up
         fe80::240:2ff:fe00:450/64
eth2    fe80::240:2ff:fe00:452/64                up           up
eth3       -                                     up           up
eth4       -                                     up           up
wwan0      -                                     up           up
br1      2001:78:0:b00::40/64                    up           up
         fe80::240:2ff:fe00:453/64
```

The windows client gets a IPv6 address with prefix length of 64 by delegation from the Cisco router (2001:78::/56).

Cellular Interface	
Enable LTE	**Select Enable LTE to enable this interface. This interface can not be deleted.** • **Disabling this interface also disables SMS messaging.** • **Power savings if no connections** **Default is disable**
Module Power Up	**Module must be powered up for LTE connection.**
Radio Enable	**Enable LTE radio** **Disable Radio to achieve better power savings.**
LTE, Module Power Up and Radio Enabled must be selected in order to use LTE	
Description	**Provide a description for this profile.** **Name can be up to 32 characters long.** **Maximum profiles is 16.**

Connect on Startup	Connect LTE on modem power up or reset.
Primary Profile	Select the primary profile to use for this connection. Default is Auto
Alternate Profile	Select the alternative profile to use for this connection. Default is Auto
NAT Enable	Creates an auto NAT rule on interface wlm0.
Connection	
Diversity Antenna Enabled	Use both antennas to improve the quality and reliability of link.
Connect On Demand	The connect on-demand feature is only applicable for the cellular interface. If the cellular connection drops due to inactivity (based on the idle timer), then the connection is re-established after any outbound routed traffic is detected on the cellular interface. The idle time and monitor direction are configurable. The connection can also be configured to start connected or disconnected on system bootup.
Maintain connection on traffic type	Specify the connection traffic type. • Transmit • Receive • Receive and Transmit Default is transmit
Drop connection after inactivity	If no activity then drop the connection. Range is 1–60 minutes. Default is 5 minutes
Enable Failover	Allows a configured redundant profile (link) to be used when the primary link fails. The configured alternate profile is be used. Feature is available on some models.
Reconnect attempts	Number of times to attempt to reconnect to the alternate cellular profile. Range is 1-100 times Default is 5 times

Switch profiles if signal goes below (dBm)	Switch profile if power level goes below configured dBm value. Range is -150-0 dBms Default is -110 dBm
Wait period before switching profiles	Wait until switching profiles. Range is 1–60 minutes Default is 1 minute
Attempt to revert back to primary profile after	Wait the configure time to try to revert back to primary profile. Range 1–1500 minutes Default is 1 minute
IPv6 address	
IPV6 address (Auto configuration)	Obtain an address using Auto Configuration
IPv6 (request prefix delegation)	Prefix delegation PD name—configure a name for this prefix
Role	WLAN for cellular interface.
MTU size	Set the maximum transmission unit size. Range is 64–9000 Default is 1460
Log the following events	• Link status • IP Address Change
Send SNMP traps for the following event	• Link status • IP Address Change
VLAN Interface	
Enable	Enabled or disabled this interface. Default is enabled
Ethernet/SFP	Select the Ethernet interface. Range 5

VLAN ID:	Select the Ethernet interface to be associate with the VLAN ID. Values are 1–4000
Description	Provide a description for this interface.
Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
DHCP Client	For detailed parameter descriptions see *DHCP Client*
DHCP Server	For detailed parameter descriptions see *DHCP Server*
Role	Configure the role for this interface for admin access. Default is LAN Options: • LAN • WAN • TRUSTED
MTU size	Optional: provide an MTU size. Default is 1500 Range is 64–9000
Log the following events	• Link status • IP Address Change
Send SNMP traps for the following event	• Link status • IP Address Change

Bridge Interface

Enable/Disable Interface	Enabled or disabled this interface. Default is enabled.
Bridge ID	Provide a number for bridge ID. Range is 1–9999
Description	Provide a description for this interface.

Select interfaces	Select the interfaces from the drop-list to associate with this bridge.
Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
DHCP Client	For detailed parameter descriptions see *DHCP Client*
DHCP Server	For detailed parameter descriptions see *DHCP Server*
Role	Configure the role for this interface for admin access. Default is LAN Options: • LAN • WAN • TRUSTED
MTU size	Optional: provide an MTU size. Default is 1500 Range is 64–9000
Log the following events	• Link status • IP Address Change
Send SNMP traps for the following event	• Link status • IP Address Change

Port-Channel	
Enable	Enable or disable port channel (bonding).
Port Channel ID	Number for the port channel. Values are 1-13
Description	Description for this port channel.

Mode—Active LACP mode	Active LACP— port channel in LACP mode enables a number of ports to be manually configured to form a single logical connection of higher bandwidth. • Hash Policy • IP port—transmits hash policy using IP and Port addresses • Mac—transmit hash policy using • Mac-ip—transmit hash policy using MAC and IP addresses
Mode—Active Standby	Active-Standby—port channel in Active-standby mode allows the redundancy of port channels grouped together to be used as "fail-back" should the primary interface fail. • Select Interface • Primary • Backup Interface
Mode—Static	Static—the router treats the aggregation as effectively a single port, and uses policy for its hashing algorithm to share data across whichever member ports are link-up. • Policy • adaptive • round-robin • transmit • xor-hash
Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
DHCP Client	For detailed parameter descriptions see *DHCP Client*
DHCP Server	For detailed parameter descriptions see *DHCP Server*
IPv6 (Request prefix delegation)	• Prefix delegation— • PD name—select name from the drop-down box • PD ID#—specify a unique instance id (0-65535) • Prefix length—length of prefix (48-64)

IPv6 address (Auto configuration)	• Obtain an address using Auto Configuration.
IPv6 address (Delegated)	• PD name—select PD name from the drop-down list • SLA length—interface site-level aggregator (SLA) length • SLA-ID—specify a decimal integer which fits in the length of the SLA length • address used to form the IPv6 interface address or EUI-64 • EUI-64 is the Default
Static	• Address X:X:X:X::X • Prefix length—length of prefix (48-64) or EUI-64 • EUI-64 is the Default
MTU size	Values are 64-1500 Default 1500

PPPoE Interface

Enable/disable interface	Enabled or disabled this interface. Default is enabled
PPPoE ID	The ID for this PPPoE connection. Values are 0–15
Interface	Select the interface from the drop-list to associate with this interface.
Description	Provide a description for this interface.
Encapsulation	Set to PPP
CHAP user name	Enter a username for this connection.
CHAP password	Enter a password for this connection.
Idle timeout	Drop the connection after idle timer expires. Values 1–4294967 in seconds

Access concentrator	Specify the name for the access concentrator.
Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
DHCP Client	For detailed parameter descriptions see *DHCP Client*
DHCP Server	For detailed parameter descriptions see *DHCP Server*
MTU size	Configure the Maximum Transmission Unit (MTU) Default is 1492 Range is 64–9000
Log the following events	• Link status • IP Address Change
Send SNMP traps for the following event	• Link status • IP Address Change

Tunnels Interface

Tunnel type	Select the tunnel type: • GRE • OpenVPN • 6in4 Default is GRE
Enable/Disable Interface	Enabled or disabled this interface. Default is enabled
OpenVPN mode	Select tun or tap.
Tunnel ID	Provide a tunnel ID.
Description	Provide a description for this interface.

Source IP address	Provide the source IP address. • IP Based • Interface based Eth 1–5 wlan 0-4,wlm0
Destination IP address	Provide the destination IP address.
Type of service	This value is written into the ToS byte in tunnel packet IP headers (the carrier packet). The range is 0 to 99, where 0 means tunnel packets copy the ToS value from the packet being encapsulated (the passenger packet). Values 0–99 The default is 0
Time to live	This value is written into the TTL field in tunnel packet IP headers (the carrier packet). The range is 0 to 255, where 0 means tunnel packets copy the TTL value from the packet being encapsulated (the passenger packet). Values are 1-255 The default is 255.
Set multicast operation over tunnel	Enable or disable multicast operation over the tunnel.
Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
IPv6 Neighbor Discovery	
Router Preference	Select the router's default preference for discovering IPv6 neighbors. A High value means this router will be preferred. • High • Medium • Low The default is medium
Manage config flags	Hosts should use DHCP for address config. Enable or disable config flags. Default is disabled

Manage other config flags	Hosts should use DHCP for non-address config. Enable or disable config flags. Default is disabled
DAD attempts	To check the uniqueness of an IPv6 address, a node sends Neighbor Solicitation messages. Use this command to specify the number of consecutive Neighbor Solicitation messages (dad_attempts) to be sent before this address can be configured. Range 1–600 Default is 1
Reachable time	Specify the length in time a node assumes a neighbor is reachable after receiving a reachability confirmation. Default is 0 (unspecified by this router) Range is 0-360000 milliseconds
Retransmission time	Configure the retransmission timer to control the time between retransmissions of neighbor solicitation messages from the user equipment (UE). Range 1–3600000 in milliseconds Default is 0
IPv6 Routing Prefix Advertisement	
Add Prefix	
Address	Configure an IPv6 address.
Prefix length	Configure the prefix length. Range is 0–128
Valid lifetime	This value applies to the router's usefulness as a default router. It does not apply to other information contained in the RA message. IPv6 hosts receiving the RA message should install the default route with an expiry time set to the Lifetime. A Lifetime of 0 indicates that the router is not a default router anymore and associated default route should be discarded from host's routing table. Range is 1–4294967294 Default is 259200 in seconds (30 days) Infinite—lifetime never expires
Preferred lifetime	Specify how long the prefix generated by stateless autoconfiguration remains preferred. Range is 1–4294967294 Default is 604800 (7 days) Infinite—lifetime never expires

Do not use prefix for onlink determination	A prefix is onlink when it is assigned to an interface on a specified link. Enable or disable prefix for onlink determination. Default is off
Do not use prefix for autoconfiguration	The sending router can indicate that a prefix is to be used for address autoconfiguration by setting the autonomous flag and specifying a nonzero Valid Lifetime value for the prefix. Enable or disable prefix for autoconfiguration. Default is off
IPv6 Routing Advertisement Control	
Suppress IPv6 router advertisement	Enable or disable IPv6 router advertisements. Default is “enable” (send router advertisements)
Hop limit	hop-limit—Specifies the Hop Count field of the IP header for outgoing (unicast) IP packets. Range is 1–255 Default is 64
RA interval	The maximum time interval between sending unsolicited multicast router advertisements from the interface, in seconds. Max range is 4–1800 in seconds Default is 600 seconds
Minimum interval	The minimum time interval between sending unsolicited multicast router advertisements from the interface, in seconds. Range of minimum is 3 to *0.75 max (dynamic range) Default maximum 600 seconds, minimum is 0.33*max Range is 3–1350 in seconds
RA lifetime	The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and doesn’t appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields, or options. Range is 4–9000 Default is 1800
Add DNS	

Address	Add IPv6 address of DNS server.
Role	Used for controlling admin access • LAN • WAN • TRUSTED Default is TRUSTED
MTU size	Optional: provide an MTU size. Default is 1476 Range is 1280–9000
Log the following events	• Link status • IP address change
Send SNMP traps for the following event	• Link status • IP Address Change

VRRP Interface

Enable VRRP	Enable or disable VRRP. Default is enabled
Interface	Select the Ethernet interface to be associate with this VRRP. The select Ethernet interface must be unbridged and have a configured ip address. Values are Ethernet. Values are Ethernet 1–5
Group	Create VRRP group number between 1–255.
Description	Specify a name for this VRRP group.
Version	Specify the version number. Values are 2–3 Default is 3
Priority	The priority value for the VRRP router that owns the IP address(es) associated with the virtual router. Values are 1–255 Default is 100
Peer address	Specify the unicast peer address.

Authentication/password	Configure VRRP authentication parameters. Configure the VRRP authentication clear text/cipher password for the VRRP group on this interface. If this option is not set, the interface is not required to authenticate to the VRRP group.
VRRP advertisement interval	Specify the time interval between the advertisement packets sent to other Virtual Router Redundancy Protocol (VRRP) routers in the same group. Values are 10–255000 milliseconds Default is 1000 milliseconds
Add this VRRP group to a sync group	Add this sync VRRP group to a sync group. Sync groups are used to link VRRP groups together in order to propagate transition changes from one group to another group. To clarify, in a VRRP synchronization group (“sync group”) are synchronized such that, if one of the interfaces in the group fails over to backup, all interfaces in the group fail over to backup. Note: VRRP groups in a sync group must have similar priority and preemption configurations. Before enabling a sync-group you should verify that one router is master of both groups and the other is backup of both groups. If both sides think they are master of the same group, then enabling a sync group can cause endless transitioning to get in sync.
Sync group name	Provide a name for the sync group.
Enable preemption of lower priority master	An important aspect of the VRRP redundancy scheme is the ability to assign each VRRP router a VRRP priority. The VRRP priority must express how efficiently a VRRP router would perform as a backup to a virtual router defined in the VRRP router. If there are multiple backup VRRP routers for the virtual router, the priority determines which backup VRRP router is assigned as master if the current master fails. • Enabled—When a VRRP router is configured with higher priority than the current master is up, it replaces the current master. • Disabled—Even if a VRRP router with a higher priority than the current master is up, it does not replace the current master. Only the original master (when it becomes available) replaces the backup. By default, the preemptive feature is enabled.

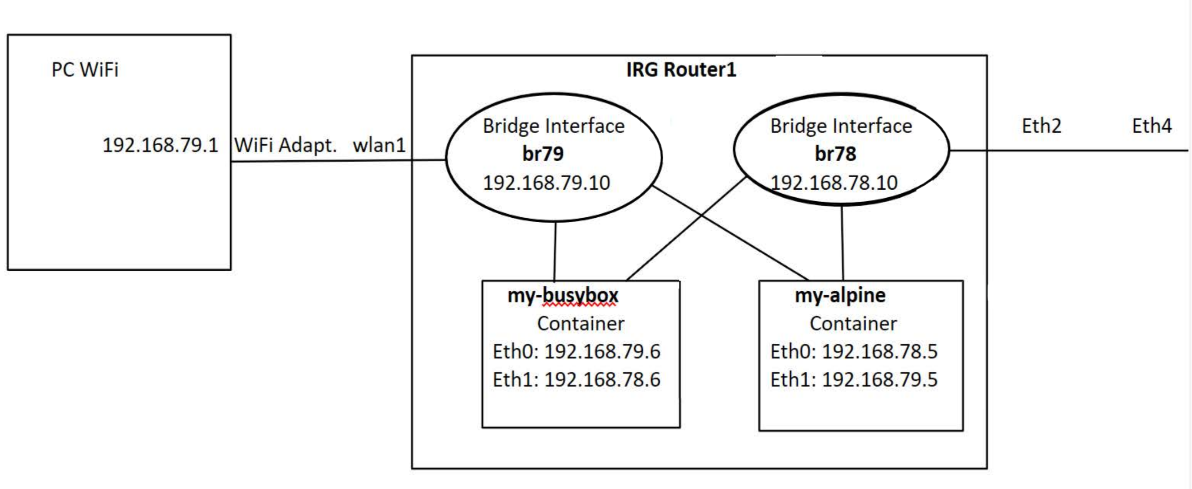
Delay at least this long	The time to delay before switching back to a master when detecting. Delay is 0–1000 in seconds Default is 0
Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
Role	Used for controlling admin access • LAN • WAN • TRUSTED Default is TRUSTED
MTU size	Optional: provide an MTU size. Default is 1500 Range is 64–9000
Log the following events	• Link status • IP Address Change
Send SNMP traps for the following event	• Link status • IP Address Change

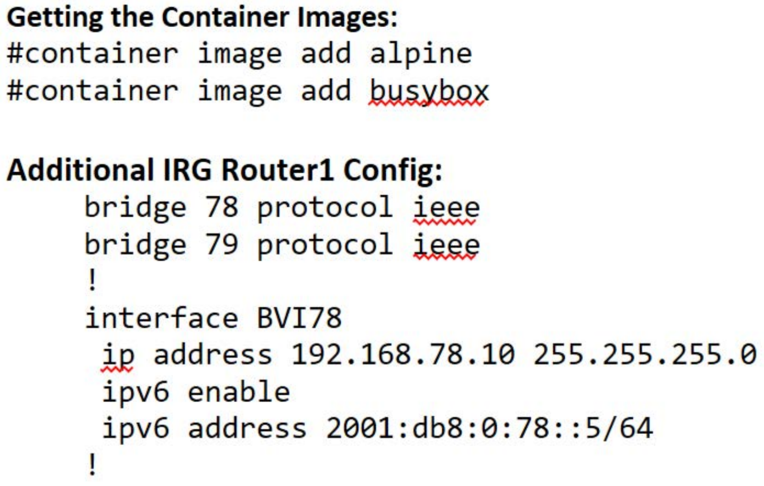
OCI Container	
Enable	Enable or disable this container instance. Default is disable
Container name	The container name. Max is 256 characters
Description	Description for this container. Max is 32 characters
Automatically add container image if not present	When enabled, you must enter the image to be upload From image box.

From image	Select the image you want in this container from the drop-down list. Container images are downloaded using the Container Management feature -> *Container Management*
Assign container network(s) to container	
Network	From the drop-down list, select the network that this container will be part of.
Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
Memory	Enter the amount of memory to use for this container. Value is 6-512 Default is 256
Restart -policy	• no—do not restart container on exit • on-failure—restart containers when they exit with a non-zero exit code, retrying <0-9999> times. Default is on failure 100 retries, 0 for infinite.
	• always—restart containers when they exit, regardless of status exit code, retrying indefinitely
Maximum restart attempts	Values are 0-9999 Default is 100 attempt 0 for infinite
Clean-restart	On bootup or restart, the container will be removed first before starting. Default is disabled
Maximum log size	Size of the log file before the file is rolled over and new entries replace older entries. Values 100–10000 KB Default is 100 KB
Log compress	Turn on compression of rotating log files. Default is compress log files
Container environment	

Name	Add custom environment variables
Value	Specify the environment option value.
Container Argument	
Number	Specify a argument number. Values 1-40
Argument	Specify the action to be done in the container when it is started.
Import changes from [Flash:]	Enter the filename in flash to import changes from.

OCI Container example configuration for IOLAN and Router models



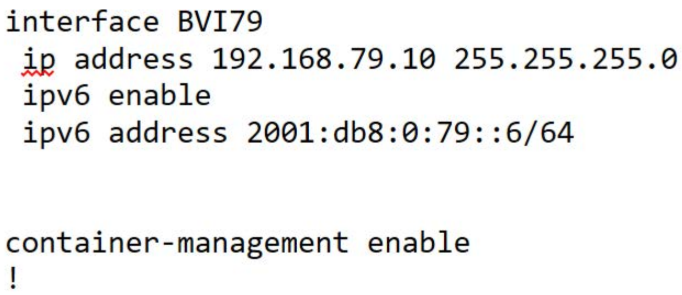

Getting the Container Images:

```
#container image add alpine
#container image add busybox
```

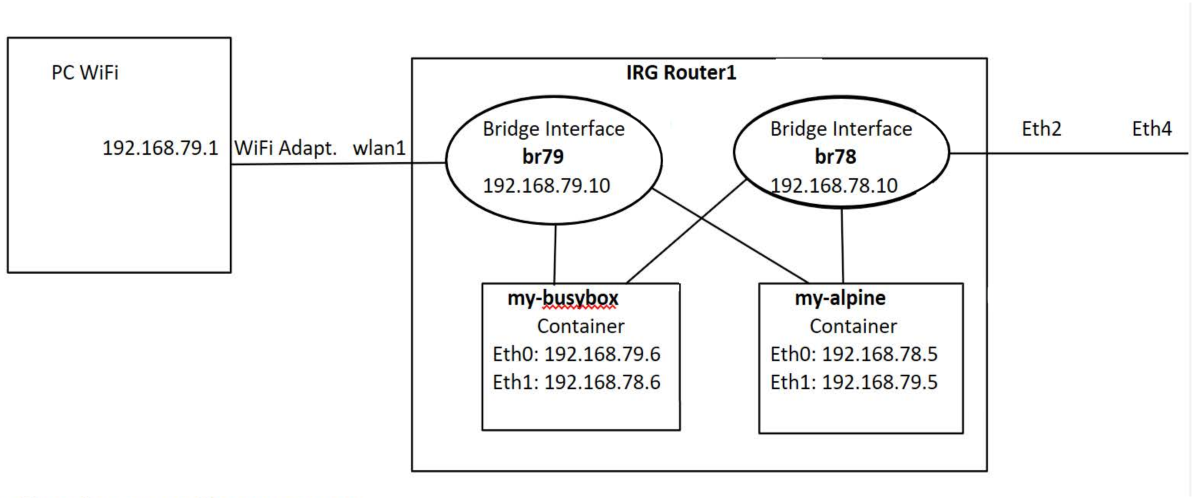
Additional IRG Router1 Config:

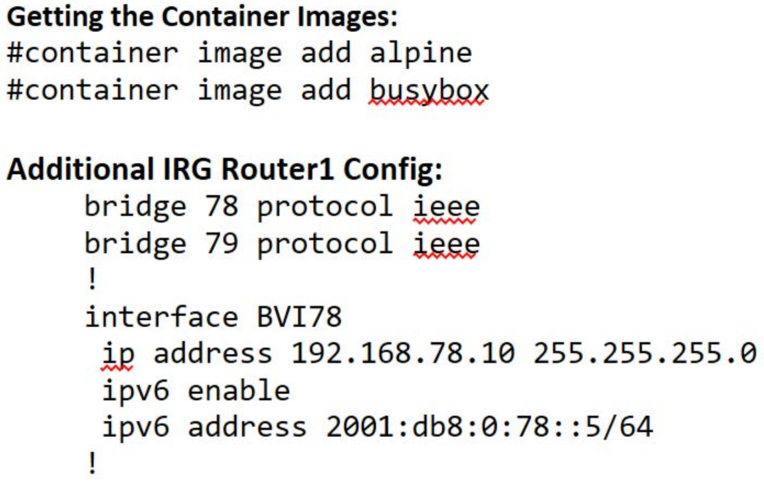
```
     bridge 78 protocol ieee
     bridge 79 protocol ieee
     !
     interface BVI78
      ip address 192.168.78.10 255.255.255.0
      ipv6 enable
      ipv6 address 2001:db8:0:78::5/64
     !
```

OCI Container example configuration for IOLAN and Router models



```
interface BVI79
 ip address 192.168.79.10 255.255.255.0
 ipv6 enable
 ipv6 address 2001:db8:0:79::6/64


container-management enable
!
```



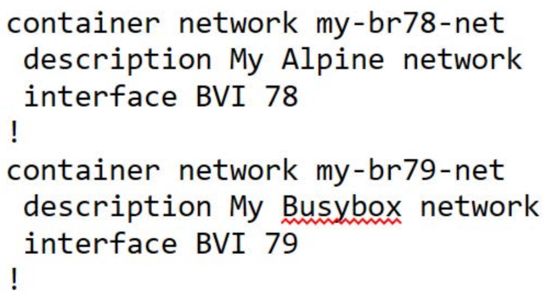


Getting the Container Images:

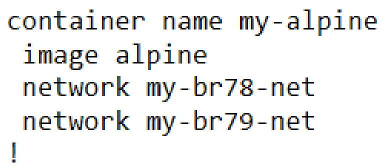
```
#container image add alpine
#container image add busybox
```

Additional IRG Router1 Config:

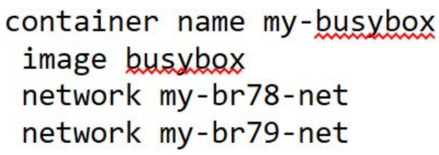
```
     bridge 78 protocol ieee
     bridge 79 protocol ieee
     !
     interface BVI78
      ip address 192.168.78.10 255.255.255.0
      ipv6 enable
      ipv6 address 2001:db8:0:78::5/64
     !
```



```
container network my-br78-net
 description My Alpine network
 interface BVI 78
!
container network my-br79-net
 description My Busybox network
 interface BVI 79
!
```

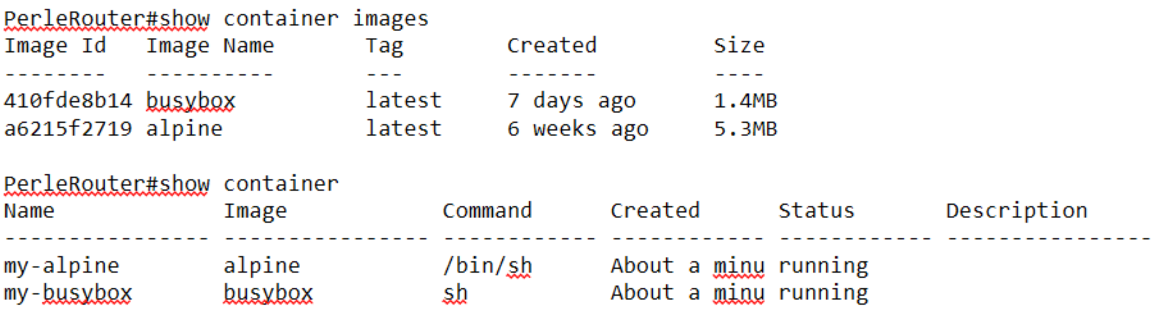


```
container name my-alpine
 image alpine
 network my-br78-net
 network my-br79-net
!
```

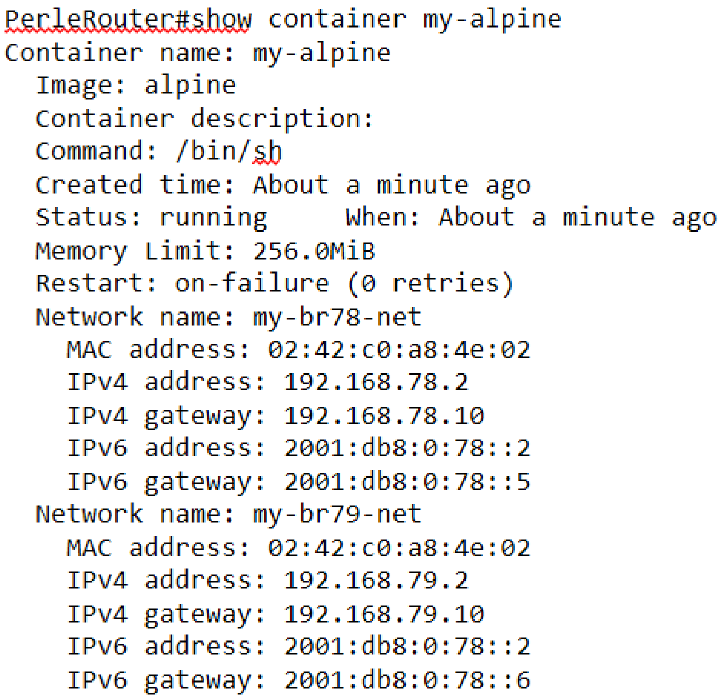


```
container name my-busybox
 image busybox
 network my-br78-net
 network my-br79-net
```

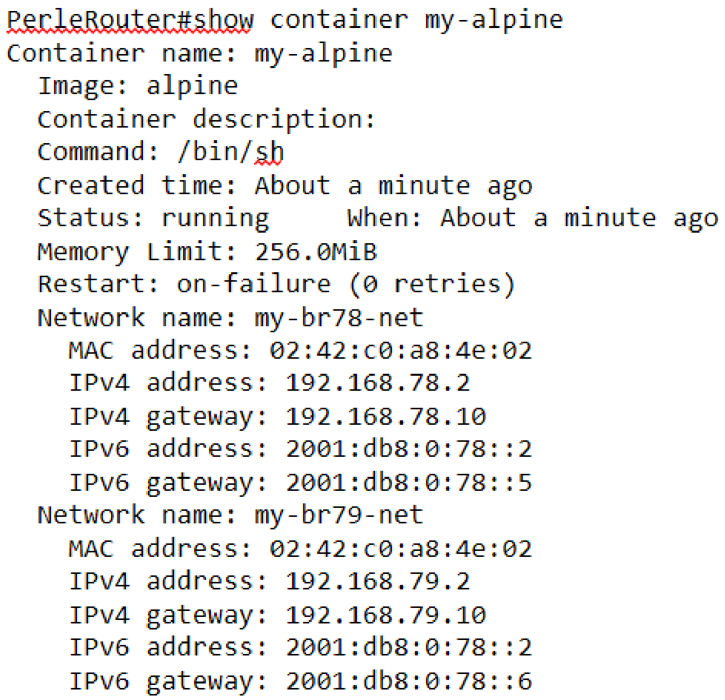
Container show command output for above Configuration:



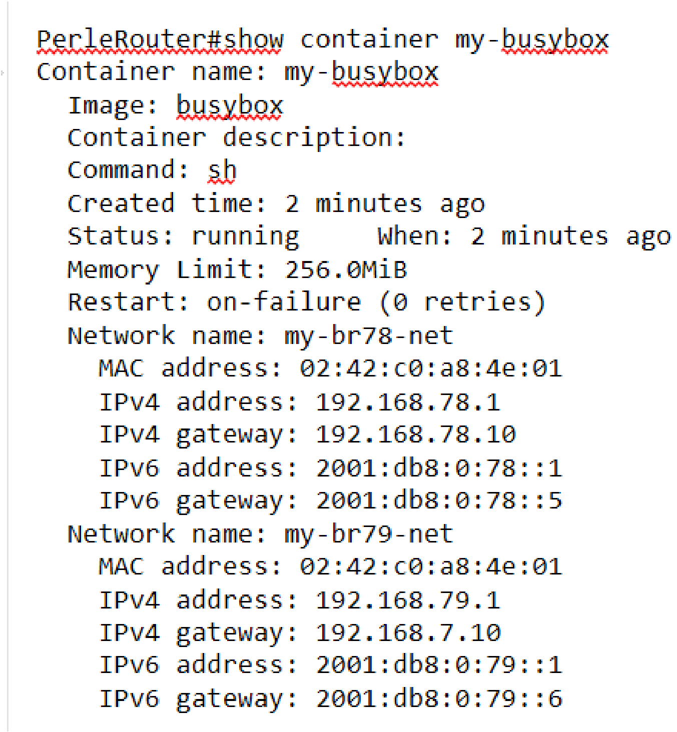
```
PerleRouter#show container images
Image Id   Image Name       Tag        Created         Size
--------   ----------       ---        -------         ----
410fde8b14 busybox          latest     7 days ago      1.4MB
a6215f2719 alpine           latest     6 weeks ago     5.3MB

PerleRouter#show container
Name             Image            Command      Created      Status       Description
---------------- ---------------- ------------ ------------ ------------ ----------------
my-alpine        alpine           /bin/sh      About a minu running
my-busybox       busybox          sh           About a minu running
```



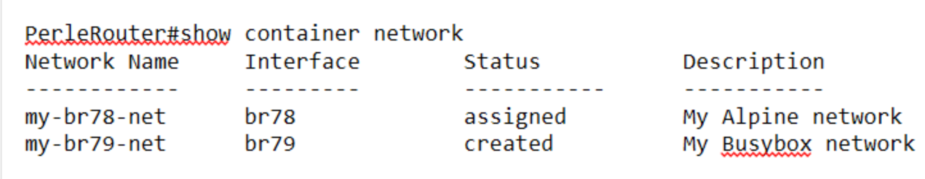
```
PerleRouter#show container my-alpine
Container name: my-alpine
  Image: alpine
  Container description:
  Command: /bin/sh
  Created time: About a minute ago
  Status: running     When: About a minute ago
  Memory Limit: 256.0MiB
  Restart: on-failure (0 retries)
  Network name: my-br78-net
    MAC address: 02:42:c0:a8:4e:02
    IPv4 address: 192.168.78.2
    IPv4 gateway: 192.168.78.10
    IPv6 address: 2001:db8:0:78::2
    IPv6 gateway: 2001:db8:0:78::5
  Network name: my-br79-net
    MAC address: 02:42:c0:a8:4e:02
    IPv4 address: 192.168.79.2
    IPv4 gateway: 192.168.79.10
    IPv6 address: 2001:db8:0:78::2
    IPv6 gateway: 2001:db8:0:78::6
```



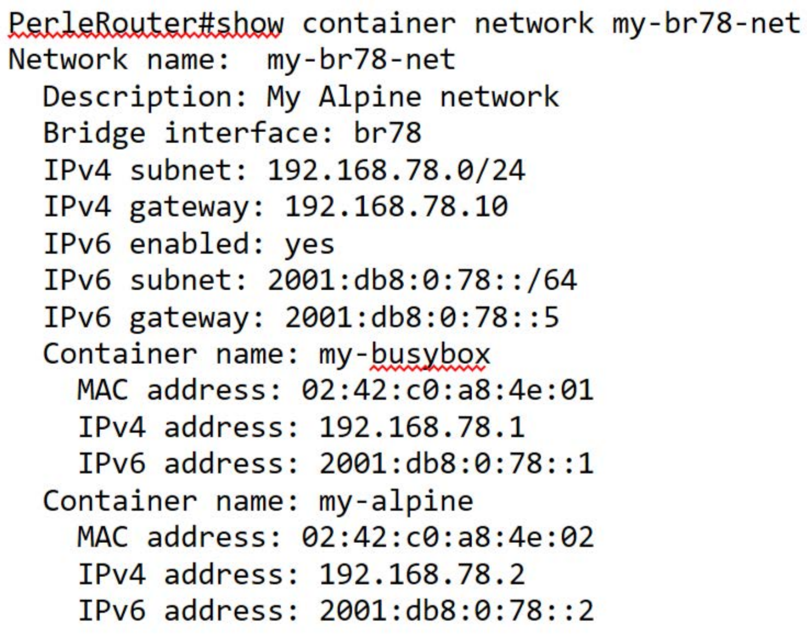
```
PerleRouter#show container my-alpine
Container name: my-alpine
  Image: alpine
  Container description:
  Command: /bin/sh
  Created time: About a minute ago
  Status: running     When: About a minute ago
  Memory Limit: 256.0MiB
  Restart: on-failure (0 retries)
  Network name: my-br78-net
    MAC address: 02:42:c0:a8:4e:02
    IPv4 address: 192.168.78.2
    IPv4 gateway: 192.168.78.10
    IPv6 address: 2001:db8:0:78::2
    IPv6 gateway: 2001:db8:0:78::5
  Network name: my-br79-net
    MAC address: 02:42:c0:a8:4e:02
    IPv4 address: 192.168.79.2
    IPv4 gateway: 192.168.79.10
    IPv6 address: 2001:db8:0:78::2
    IPv6 gateway: 2001:db8:0:78::6
```



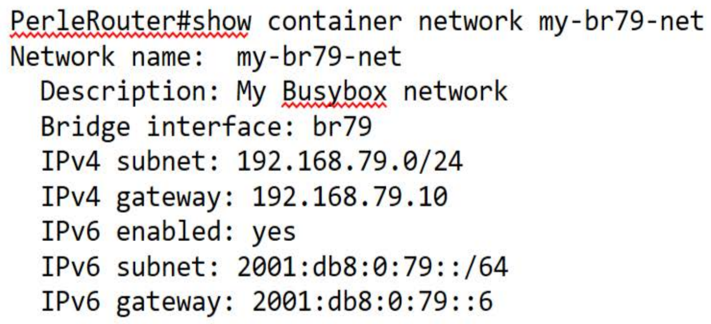
```
PerleRouter#show container my-busybox
Container name: my-busybox
  Image: busybox
  Container description:
  Command: sh
  Created time: 2 minutes ago
  Status: running     When: 2 minutes ago
  Memory Limit: 256.0MiB
  Restart: on-failure (0 retries)
  Network name: my-br78-net
    MAC address: 02:42:c0:a8:4e:01
    IPv4 address: 192.168.78.1
    IPv4 gateway: 192.168.78.10
    IPv6 address: 2001:db8:0:78::1
    IPv6 gateway: 2001:db8:0:78::5
  Network name: my-br79-net
    MAC address: 02:42:c0:a8:4e:01
    IPv4 address: 192.168.79.1
    IPv4 gateway: 192.168.7.10
    IPv6 address: 2001:db8:0:79::1
    IPv6 gateway: 2001:db8:0:79::6
```



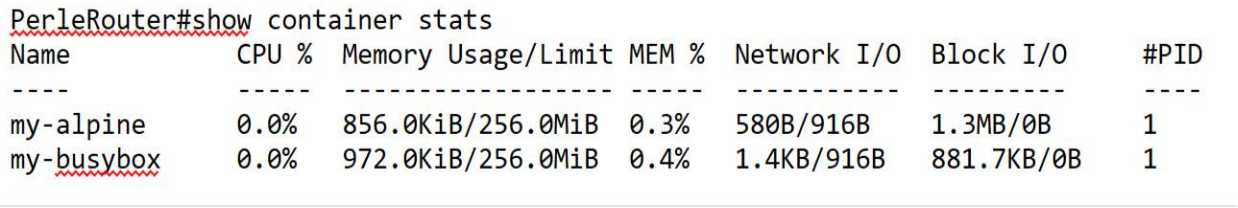
```
PerleRouter#show container network
Network Name     Interface        Status          Description
------------     ---------        -----------     -----------
my-br78-net      br78             assigned        My Alpine network
my-br79-net      br79             created         My Busybox network
```



```
PerleRouter#show container network my-br78-net
Network name:  my-br78-net
  Description: My Alpine network
  Bridge interface: br78
  IPv4 subnet: 192.168.78.0/24
  IPv4 gateway: 192.168.78.10
  IPv6 enabled: yes
  IPv6 subnet: 2001:db8:0:78::/64
  IPv6 gateway: 2001:db8:0:78::5
  Container name: my-busybox
    MAC address: 02:42:c0:a8:4e:01
    IPv4 address: 192.168.78.1
    IPv6 address: 2001:db8:0:78::1
  Container name: my-alpine
    MAC address: 02:42:c0:a8:4e:02
    IPv4 address: 192.168.78.2
    IPv6 address: 2001:db8:0:78::2
```



```
PerleRouter#show container network my-br79-net
Network name:  my-br79-net
  Description: My Busybox network
  Bridge interface: br79
  IPv4 subnet: 192.168.79.0/24
  IPv4 gateway: 192.168.79.10
  IPv6 enabled: yes
  IPv6 subnet: 2001:db8:0:79::/64
  IPv6 gateway: 2001:db8:0:79::6
```



```
PerleRouter#show container stats
Name           CPU %  Memory Usage/Limit MEM %  Network I/O  Block I/O    #PID
----           -----  ------------------ -----  -----------  ---------    ----
my-alpine      0.0%   856.0KiB/256.0MiB  0.3%   580B/916B    1.3MB/0B     1
my-busybox     0.0%   972.0KiB/256.0MiB  0.4%   1.4KB/916B   881.7KB/0B   1
```

Serial	
Serial-line (applicable to RS232 interface	
The Usage mode	**Select how this interface is used.** • **Disabled—disabled** • **Serial-Line—serial mode operation** • **Serial Console—used as console** • **Serial-GNSS— used for GNSS output**
Service	**Select the service you wish to run on this port.** **Valid options for RJ-45 port are:** • **Console Management** • **Trueport** • **TCP sockets** • **UDP sockets** • **Terminal** • **Printer** • **Serial Tunneling** • **Virtual Modem** • **Modbus Gateway** • **Remote Access (PPP)** • **Remote Access (SLIP)** **More models with USB serial ports the valid options are:** • **Console Management** • **Trueport** • **TCP sockets** **For a detailed description of the above services please see** ***Services***
Hardware settings-Serial Line	
	Configure speed: • **300** • **600** • **1200** • **1800** • **2400** • **4800** • **custom** • **19200** • **28800** • **38400** • **57600** • **115200** • **230400**

Parity	Configure parity: • None • Even • Odd • Mark • Space
Data bits	Configure databits: • 5 • 6 • 7 • 8
Stop bits	Configure stop bits: • 1 • 2
Enable CTS Toggle	Configure the Toggle CTS Feature if your application needs this signal to be raised during character transmission.
Initial Delay	Configure the time (in ms) between the time the CTS signal is raised and the start of character transmission. This delay only applies if this port is not running hardware flow control. If hardware flow control is used, the transmission occurs as soon as RTS is raised by the modem.
Final Delay	Configure the time (in ms) between the time of character transmission and when CTS is dropped.
Flow control	
Enable Inbound Flow Control	Configure if input flow control is to be used. Default is enabled
Enable Outbound Flow Control	Configure if output flow control is to be used. Default is enabled
Enable DTR-DSR monitor	The serial doesn’t go active until DTR-DSR are both active.
Discard Characters Received with errors	When enabled, the router discards characters received with a parity framing error. Default is disabled

Enable Echo Suppression	This parameter applies only to EIA-485 Half Duplex mode. All characters are echoed to the user and transmitted across the serial ports. Some EIA-485 applications require local echo to be enabled in order to monitor the loopback data to determine that line contention has occurred. If your application cannot handle loopback data, echo suppression should be enabled. Default is Disabled
Enable Line Termination	Enable or disable

Serial Console (RS232)	
Speed	Configure speed: • 9600 • 19200 • 38400 • 57600 • 115200
Parity	Configure parity: • None • Even • Odd
Data bits	Configure databits: • 7 • 8
Stop bits	Configure stop bits: • 1 • 2

Serial GNSS	
Speed	Configure speed: • 4800 • 9600 • 19200 • 38400 • 57600 • 115200 • 230400
Parity	Configure parity: • None • Even • Odd • Mark • Space
Data bits	Configure databits: • 7 • 8
Stop bits	Configure stop bits: • 1 • 2
Interface Type: USB-Ethernet	
USB usage mode	Select how the USB interface is used. • USB-Console—set this mode when using the serial port as a console port. • USB Ethernet—select this mode to use the USB port as an Ethernet port. • USB-GNSS—select this mode to send GNSS output to the USB port. Disabled

USB Ethernet	
Description	Add a description for the USB port.

Enable IP addresses	
Enable IPv4 address	For detailed parameter descriptions see *IPv4 address*
Enable IPv6 address	For detailed parameter descriptions see *IPv6 address*
DHCP Client	For detailed parameter descriptions see *DHCP Client*
DHCP Server	For detailed parameter descriptions see *DHCP Server*

Serial Interfaces

Each router serial port can be connected to a serial device.
Note: Some configuration parameters may be different on some models or running software.
The following are the serial profile types:

- **Console Management—**The Console Management profile configures a serial port to provide network access to a console or administrative port. This profile sets up a serial port to support a TCP socket that listens for a Telnet or SSH connection from the network.
- **Trueport—**The Trueport profile configures a serial port to connect network servers or workstations running the TruePort software to a serial device as a virtual COM port. This profile is ideal for connecting multiple serial ports to a network system or server.
- **TCP Sockets—**The TCP Sockets profile configures a serial port to allow a serial device to communicate over a TCP network. The TCP connection can be configured to be initiated from the network, from a serial device connected to the serial port, or both. This is sometimes referred to as a raw connection or a TCP raw connection.
- **UDP Sockets—**The UDP Sockets profile configures a serial port to allow communication to/from the network and to connect serial devices to the router using the UDP protocol.
- **Terminal—**The Terminal profile configures a serial port to allow network access from a terminal connected to the router's serial port. This profile is used to access predefined hosts on the network from the terminal.
- **Printer—**The Printer profile configures a serial port to support a serial printer that can be accessed by the network.
- **Serial Tunneling—**The Serial Tunneling profile configures a serial port to establish a virtual link over the network to a serial port on another Perle router. Both router serial ports must be configured for Serial Tunneling (typically one serial port is configured as a Tunnel Server and the other serial port as a Tunnel Client).
- **Virtual Modem—**The Virtual Modem profile configures a serial port to simulate a modem. When the serial device connected to the router initiates a modem connection, the router start up a TCP connection to the other router configured with a virtual Modem serial port or to a host running a TCP application.
- **Modbus—**The Modbus Gateway profile configures a serial port to act as a Modbus Master Gateway or a Modbus Slave Gateway.
- **Remote Access (PPP)—**The Remote Access (PPP) profile configures a serial port to allow a remote user to establish a PPP connection to the router's serial port. This is typically used with a modem for dial-in or dial-out access to the network.
- **Remote Access (Slip)—**The Remote Access (SLIP) Profile configures a serial port to allow a remote user to establish a SLIP connection to the router's serial port. This is typically used with a modem for dial-in.

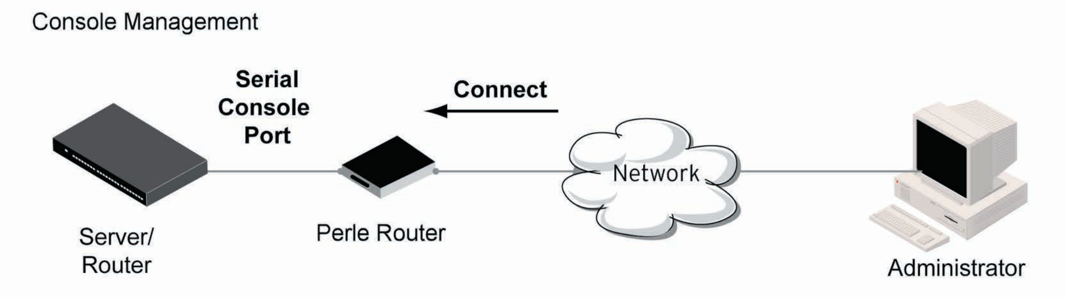
Common Serial Port Profiles Functions:

- Enable the serial port, enter description, then select service. See ***Serial Interfaces***
- Hardware— Configure the physical serial line parameters. ***Serial Interfaces***
- Packet Forwarding—Configure data packet parameters.See ***Packet Forwarding***
- SSL/TLS—Configure SSL/TLS encryption options for the serial port. See ***SSL/TLS***
- Port Buffering—Configure serial port data buffering preferences. See ***Local Port Buffering***
- Trueport Baud Rate. Map your Trueport baud rate (running on the application software) to the Actual baud rate (on the serial port). See ***Trueport***
- Advanced Serial Options. See ***Advanced Serial Options***

Services

Console Management

The Console Management profile provides access through the network via Telnet or SSH to a console or administrative port of a server or device attached to the router's serial port. Use the Console Management profile when you are configuring users who need to access a serial console from the network.Trueport



Console Management	
Enable	**Enable or disable interface**
Description	**Provide a description for this interface.**
Service	**Select a service type for this interface from the drop-down box.**
Hardware Settings	**See *Hardware settings-Serial Line***
Enable IP aliasing	**Check this box to enable IP aliasing.**

IP address	Enter the IP alias address for this serial port.
Settings	
Protocol	Specify the connection method that users use to communicate with a serial device connected to the router through the network. • SSH • Telnet Default is SSH
Listen For Connections on TCP Port	The TCP port number the router will listen on for incoming TCP connections. Note: If more then one serial port has the same TCP port number assignment, this creates a hunt group scenario. You must configure all operating parameters for each serial port the same. Default: 10001, depending on the serial port number
Advanced	
Authenticate User	Enables/disables login/password authentication for users connecting from the network. Default is disabled
Enable TCP Keepalive	Enables the per-connection TCP keep-alive feature. After the configured number of seconds, the connection sends a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized. This parameter is used in conjunction with the Monitor Connection Status Interval parameter found under the Advanced Setting *Advanced Serial Options* configuration. The interval specifies the inactivity period before “testing” the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port. Default is disabled.
Enable Message of the Day (MOTD)	Enables/disables the display of the message of the day. Default is disabled
Session Timeout	Use this timer to forcibly close the session/connection when the Session Timeout expires. Default is 0 seconds so the port will never timeout Range is 0–4294967 seconds (about 49 days)

Idle Timeout	Use this timer to close a connection because of inactivity. When the idle Timeout is reached, the router will end the connection. Range is 0–4294967 seconds (about 49 days) Default is 0 seconds so the port will never timeout
Multisession	The number of extra network connections available on a serial port, in addition to the single session that is always available. Enabling multisessions permits multiple users to monitor the same console port. The maximum number of multisessions is 8.
Dial Options	Configures Dial in and Dial Out parameters. See *Dial Options*
Session Strings	Configures session control for Send at Start, End and Delay after parameters. See *Session Strings*
Break Handing	Specifies how a break is interpreted. • None—The router ignores the break key and it is not passed through to the host • Local—The router interprets the break locally. If the user is in a session, the break key has the same effect as a hot key • Remote—When the break key is pressed, the router translates this into a telnet break signal then sends it to the host machine • Break interrupt—On some systems such as SunOS, XENIX and AIX, a break received from the peripheral is not passed to the client properly. Set this if the client wants to make the break act like an interrupt key (for example, when the stty options ignbrk and brkintr are set)
None	The router ignores the break key and it is not passed through to the host.
Local	Local—The router interprets the break locally. If the user is in a session, the break key has the same effect as a hot key.
Remote	Remote—When the break key is pressed, the router translates this into a telnet break signal then sends it to the host machine

Break Interrupt	On some systems such as SunOS, XENIX and AIX, a break received from the peripheral is not passed to the client properly. Set this if the client wants to make the break act like an interrupt key (for example, when the stty options ignbrk and brkintr are set)
Packet Forwarding	Packet forwarding can be used to control/define how and when serial port data packets are sent from the routerto the network. See *Packet Forwarding*

Trueport

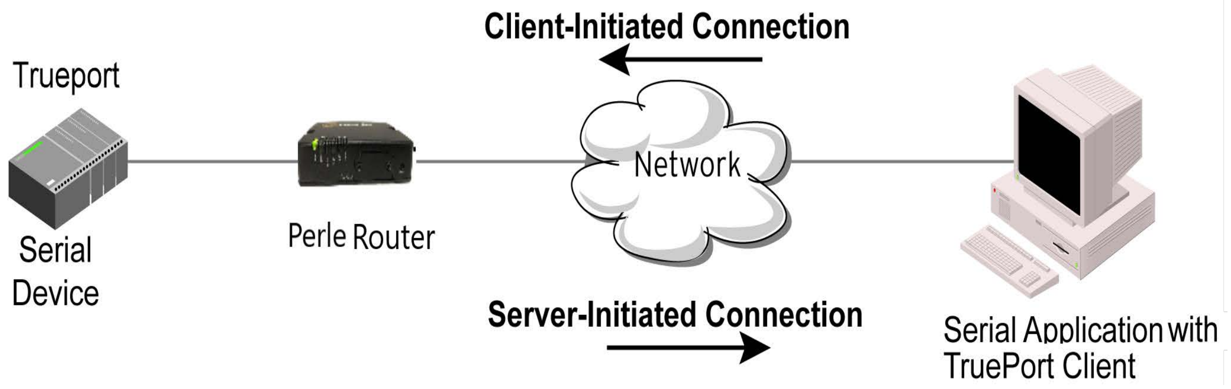
TruePort is a COM port redirector client utility that is installed and run on your PC. It can be run in two modes (the mode is selected on the client software when it is configured). In client mode the software is installed to listen for connections from the router to establish a connection. In server mode, the client PC sends a connection request to the router. router

Trueport can also be configured on the client to run in Full mode that allows complete control and operates as if the com port was directly connected to the Workstation/Server's local serial port. It provides a complete COM port interface between the attached serial device and the network. All serial controls, baud rate, control, etc., are sent to the router and replicated on its associated serial port.

Alternatively, Trueport can be configured to run in Lite mode where it provides a simple raw data interface between the application and the remote serial port. Although the port will operate as a Com port, control signals are ignored.

See the Trueport User's Guide for more information.

Client Services



Trueport	
Enable	Enable or disable interface

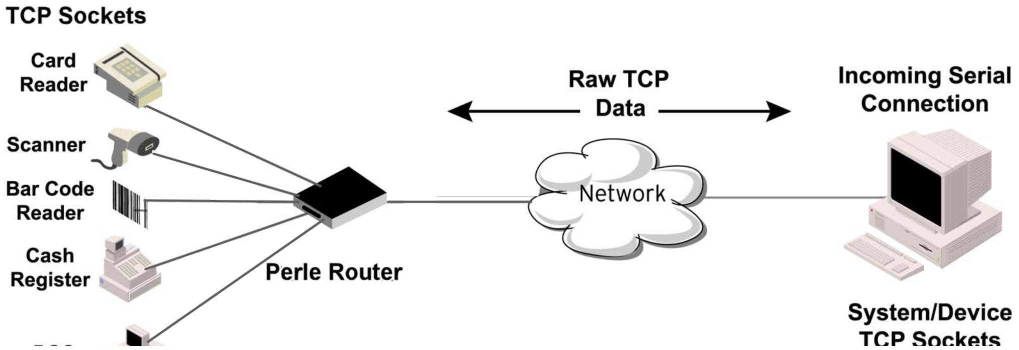
Description	Provide a description for this interface.
Service	Select a service type for this interface from the drop-down box.
Hardware Settings	See *Hardware settings-Serial Line*
Service Settings	
Server Initiated	
Connection	Connection determines how the TruePort connection is initiated and then sets up the appropriate connection parameters. • Server Initiated—The router will initiate the connection to the client. • Client Initiated—The client will initiate the connection to the router. Default is Client initiated
Host	The configured host that the router will connect to (must be running TruePort).
TCP Port	The TCP port that the router will use to communicate through to the Trueport client. Default—10001 for serial port 1, then increments by one for each serial port
Connect to multiple hosts	When this option is enabled, multiple hosts can connect to the serial device connected to this serial port. Note: These multiple clients (Hosts) need to be running TruePort in Lite mode. Default is disabled
Send name on connect	When enabled, the port name is sent to the host upon session initiation. This is done before any other data is sent or received to/from the host. Default is disabled
Client Initiated	
TCP Port	The TCP port that the client uses to communicate through to the Trueport Service Default—10001 for serial port 1, then increments by one for each serial port

Client allow multiple connections (Trueport Lite mode)	When this option is enabled, define all the hosts for the client to connect to. Default is enabled Note: These multiple clients (Hosts) need to be running TruePort in Lite mode.
Advanced	Configure parameters that are applicable to specific environments. See *Advanced Serial Options*
Raise Signals when not under Trueport control	This option has the following impact based on the Trueport mode.
TruePort Lite Mode	When enabled, the EIA-232 signals remain active before, during, and after the TruePort connection is established. When disabled, the EIA-232 signals remain inactive during and after the Trueport connection is established.
TruePort Full Mode	When enabled, the EIA-232 signals remain active before and after the TruePort connection and the TruePort client will control the state of the signals during the established TruePort connection. When disabled, the EIA-232 signals remain inactive before and after the TruePort connection and the TruePort client will control the state of the signals during the established TruePort connection. Default is enabled
Enable Message of the Day (MOTD)	Enables/disables the display of the message of the day (MOTD). Default is disabled
Enable TCP Keepalive	Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection sends a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized. This parameter is used in conjunction with Monitor Connection status interval parameter found in the Serial, Advanced, Advanced Settings. The interval specifies the inactivity period before testing the connection. Default: disabled

Enable Data Logging (Trueport Lite Mode)	When enabled, serial data is buffered if the TCP connection is lost. When the TCP connection is re-established, the buffered serial data is sent to its destination. If using the Trueport profile, data logging is only supported in Lite Mode. Default Note: a kill line or a reboot of the router causes all buffered data to be lost Some profile features are not compatible with the data logging feature. See *Data Logging Feature*
Session Timeout	Use this timer to forcibly close the session/connection when the Session Timeout expires. Default is 0 seconds so the port will never timeout Range is 0–4294967 seconds (about 49 days)
Idle Timeout	Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the router ends the connection. Range is 0–4294967 seconds (about 49 days) Default is 0 seconds so the port will never timeout
Dial Options	Configures Dial in and Dial Out parameters. See *Dial Options*
Session Strings	Configures Send at Start, End and Delay after parameters for session control. See *Session Strings*
Packet Forwarding	Packet forwarding is used to control/define how and when serial port data packets are sent from the router to the network. See *Packet Forwarding*
SSL/TLS	You can create an encrypted connection using SSL/TLS for the following profiles: Trueport, TCP Sockets, Terminal (the user's service must be set to SSL_RAW), Serial Tunneling, Virtual Modem and Modbus. When configuring SSL/TLS, the following configuration options are available • You can set up the router to act as an SSL/TLS client or server. • There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection See *SSL/TLS*

TCP Sockets

The TCP Socket profile allows for a serial device to communicate over a TCP network. The TCP connection can be initiated from a host on the network and/or a serial device. This is typically used with an application on a Workstation or Server that communicates to a device using a specific TCP socket. This is often referred to as a RAW connection. The TCP Socket profile permits a raw connection to be established in either direction, meaning that all the connection can be initiated by ether the Workstation/Server or the router.



TCP Sockets	
Enable	Enable or disable interface
Description	Provide a description for this interface.
Service	Select a service type for this interface from the drop-down box.
Hardware Settings	See *Hardware settings-Serial Line*
Service Settings	
Settings	• Listen for connection—the router is listening for a connection from the server • Connect to—the router is initiating a connection to the server
	• Bidirectional Connection—both sides can initiate or respond to the connection
TCP Port	When enabled, the router listens for a connection to be established by the Workstation/Server on the network. Default is enabled
Connect to Multiple Hosts	When this option is enabled, multiple hosts can connect to the serial device that is connected to this serial port. Default is disabled

IP address	Users can access serial devices connected to the router through the network by the specified Internet Address (or host name that can be resolved to the Internet Address in a DNS network). Field format is IPv4 or IPv6 address
Advanced Options	Configures those parameters that are applicable to specific environments. See *Advanced Serial Options*
Authenticate User	Enables/disables login/password authentication for users connecting from the network. Default is disabled
Enable Message of the Day (MOTD)	Enables/disables the display of the message of the day (MOTD). Default is disabled
Enable TCP Keepalive	Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized. This parameter is used in conjunction with Monitor Connection status interval parameter found in the Serial, Advanced, Advanced Settings. The interval specifies the inactivity period before testing the connection. Default: disabled
Enable Data Logging	When enabled, serial data is buffered if the TCP connection is lost. When the TCP connection is re-established, the buffered serial data is sent to its destination. If using the Trueport profile, data logging is only supported in Lite Mode. Default is disabled Note: a kill line or a reboot of the router causes all buffered data to be lost Some profile features are not compatible with the data logging feature. See *Data Logging Feature*
Session Timeout	Use this timer to forcibly close the session/connection when the Session Timeout expires. Default is 0 seconds so the port will never timeout Range is 0–4294967 seconds (about 49 days)
Idle Timeout	Use this timer to close a connection because of inactivity. When the idle Timeout expires, the router will end the connection. Range is 0–4294967 seconds (about 49 days) Default is 0 seconds so the port will never timeout

Dial Options	**Configure Dial in and Dial Out parameters. See *Dial Options***
Session Strings	**Configure session control for Send at Start, End and Delay after parameters. See *Session Strings***
Packet Forwarding	**Packet forwarding is used to control/define how and when serial port data packets are sent from the router to the network.** **See *Packet Forwarding***
SSL/TLS	**You can create an encrypted connection using SSL/TLS for the following profiles: Trueport, TCP Sockets, Terminal (the user's service must be set to SSL_RAW), Serial Tunneling, Virtual Modem and Modbus.** **When configuring SSL/TLS, the following configuration options are available** **• You can set up the router to act as an SSL/TLS client or server.** **• There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection** **See *SSL/TLS***

UDP Sockets

The UDP profile configures a serial port to send or receive data to/from the LAN using the UDP protocol.When you configure UDP, you are setting up a range of IP addresses and the port numbers that are used to send UDP data to or receive UDP data from.You can use UDP profile in the following two basic modes. The first is to send data coming from the serial device to one or more UDP listeners on the LAN. The second is to accept UDP datagrams coming from one or more UDP senders on the LAN and forward this data to the serial device. You can also configure a combination of both which will allow you to send and receive UDP data to/from the LAN.

When you configure UDP for **LAN to Serial**, the following options are available:

To send to a single IP address, leave the **End IP Address** field at its default value of (0.0.0.0)

The IP address can be auto learned if both start/end IP address are left blank/default.

If the **Start IP Address** field is set to 255.255.255.255 and the **End IP Address** is left at its default value (0.0.0.0), the router will accept UDP packets from any source address.

Four individual entries are provided to allow you greater flexibility to specify how data will be forwarded to/from the serial device. All four entries support the same configuration parameters. You can configure one or more of the entries as needed.

The first thing you need to configure for an entry is the **“Direction”** of the data flow. The following options are available;

- **Disabled—**UDP service not enabled.
- **LAN to Serial—**This setting will allow UDP data to be received from one or more hosts on the LAN and forwarded to the serial device attached to this serial port.
- **Serial to LAN—**This setting will allow data originating from the serial device attached to this serial port to be sent to one or more hosts on the LAN using UDP datagrams.
- **Both—**Allows for data to flow from the serial device to the LAN and from the LAN to the serial device.

The role of each of the configurable parameters in an entry depends on the **Direction** selected. When the direction is **LAN to Serial** the role of the additional parameters is as follow;

- **Start IP Address—**This is the IP address of the host from which the UDP data will originate. If the data will originate from a number of hosts, this becomes the starting IP address of a range.
- **End IP Address—**If you wish to receive data only from the single host defined by Start IP address, leave this entry as is (0.0.0.0). If you wish to accept data from a number of hosts, this address will represent the upper end of a range starting from Start IP address. Only data originating from this range will be forwarded to the serial port.
- **UDP port**—This is the UPD port from which the data will originate. There are two options for this parameter.
    - **Auto Learn—**The first UDP message received will be send to define which UDP port we are going to accept

UDP data from. Once learned, only data from this UDP port will be accepted. The data must also originate from a host which is in the IP range defined for this entry.

- **Port—**Only data originating from the UDP port configured here as well as originating from a host in the IP range defined for this entry will be accepted.

When the direction is **Serial to LAN** the role of the additional parameters is as follow;

- **Start IP Address—**This is the IP address of the host to which the serial data will be sent using UDP datagrams. If the serial data is to be sent to more than one host, this becomes the starting IP address of a range.
- **End IP Address—**If you wish to send serial data to a single host, leave this entry as is (0.0.0.0). If you wish to send the serial data to a number of hosts, this address will represent the upper end of a range starting from **Start IP Address**.
- **UDP port—**This is the UPD port to which the serial data will be forwarded. For a direction of **Serial to LAN**, you must specify the port to be used.

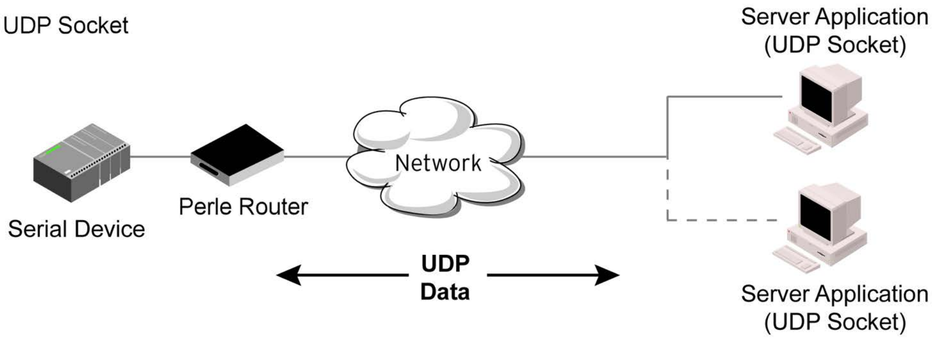
When the direction is **Both** the role of the additional parameters is as follow;

- **Start IP Address—**This is the IP address of the host to which the serial data will be sent using UDP datagrams. It is also the IP address of the host from which UDP data coming from the LAN will be accepted from. If the data is to be sent to or received from more than one host, this becomes the starting IP address of a range.
- **End IP Address—**If you wish to send serial data to a single host and only receive data from the single UDP host, leave this entry as is (0.0.0.0). If the data is to be sent to or received from more than one host, this address will represent the upper end of a range starting from **Start IP Address.** Only data originating from this range will be forwarded to the serial port.
- **UDP Port—**This is the UPD port to which the serial data will be forwarded as well as the UPD port from which data originating on the LAN will be accepted from. For a direction of **Both**, there are two valid option for the UDP Port as follows;
- **Auto Learn—**The first UDP message received will be used to define which port we are going to accept UDP data from. Once learned, only data from this UDP port will be accepted and serial data being forwarded to the LAN will be sent to this UDP port. Until the port is learned, data from the serial port intended to be sent to the LAN will be discarded.
- **Specific/Port—**Serial data being forwarded to the LAN from the serial device will sent to this UDP port. Only data originating from the UDP port configured here (as well as originating from a host in the IP range defined for this entry) will be forwarded to the serial device.

Special values for Start IP address

- **0.0.0.0—**This is the **auto learn IP address** value which is valid only in conjunction with the LAN to Serial setting. The first UDP packet received for this serial port will set the IP address from which we will accept future UDP packets to be forwarded to the serial port. For this setting, leave the **End IP Address** as 0.0.0.0.

- **255.255.255.255—**This selection is only valid in conjunction with the **LAN to Serial** setting. It will accept all UDP packets received for this serial port regardless of the originating IP address.For this setting, leave the **End IP Address** as 0.0.0.0.
- **Subnet directed broadcast—**You can use the **Start IP Address** field to enter a subnet directed broadcast address. This is done by specifying the subnet address with the host portion filled with 1s. For example, if you are on the subnet 172.16.x.x with a subnet mask of 255.255.254.0 than you would specify an IP address of 172.16.1.255 (all ones for host portion). For this setting, leave the **End IP Address** as 0.0.0.0. For any LAN to Serial ranges you have defined for this serial port, you must ensure that IP address of this router is not included in the range. If your IP address is within the range, you will receive the data you send via the subnet directed broadcasts as data coming in from the LAN.



UDP Sockets

Enable	**Enable or disable interface**
Description	**Provide a description for this interface.**
Service	**Select a service type for this interface from the drop-down box.**
Hardware Settings	**See** ***Hardware settings-Serial Line***
Service Settings	
Listen for Connections on UDP Port	**The router listens for UDP packets on the specified port. Default is 1000+ port-number. (for example, 10001 for serial port 1)**

Direction	The direction in which information is received or relayed:
Disabled	UDP service not enabled.
LAN to Serial	This setting allows UDP data to be received from one or more hosts on the LAN and forwarded to the serial device attached to this serial port.
Serial to LAN	This setting allows data originating from the serial device attached to this serial port to be sent to one or more hosts on the LAN using UDP datagrams.
Both	Allows for data to flow from the serial device to the LAN and from the LAN to the serial device.
Start IP address	The first host IP address int he range of IP addresses (for IPv4 and IPv6) that the router will listen for messages from and/or send messages to. Field Format is IPv4 or IPv6 address
End IP address	The last host IP address in the range of IP addresses (for IPv4, not supported for IPv6) that the router will listen for messages from and/or send messages to. Field Format is IPv4 or IPv6 address
UDP Port	Determines how the router's UDP port that will send/receive UDP messages is defined: • Auto Learn—The router will only listen to the first port that it receives a UDP packet from. Applicable when Direction is set to LAN to Serial or Both. UDP Port determines how the router's UDP port will send/ receive UDP messages. • Auto Learn—The router will only listen to the first port that it receives a UDP packet from. Applicable when Direction is set to LAN to Serial or Both. • Port—The port that the router will use to relay messages to servers/hosts. This option works with any Direction except disabled. The router will listen for UDP packets on the port configured by the Listen for connection on UDP port parameter. Default is Auto Learn
Session Strings	Configures Send at Start, End and Delay after parameters for session control. See *Session Strings*

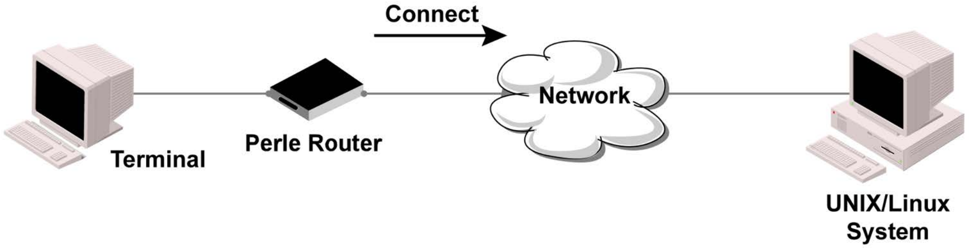
Packet Forwarding	**Packet forwarding can be used to control/define how and when serial port data packets are sent fro the router to the network.** **See *Packet Forwarding***

Terminal

The Terminal profile allows network access from a terminal connected to the router’s serial port. Use this profile to access pre-defined hosts on the network from the terminal. This profile can be configured for users:

- who must be authenticated by the router first and then a connection to a host can be established
- who are connecting through the serial port directly to a host.

Terminal



Terminal	
Enable	**Enable or disable interface**
Description	**Provide a description for this interface.**
Service	**Select a service type for this interface from the drop-down box.**
Hardware Settings	**See *Hardware settings-Serial Line***
Service Settings	
Terminal Type	**Type of terminal attached to this serial port.** • **Dumb, WYSE60, VT100, TVT100, ANSI, VT925 IBM3151, VT320, HP700** **Default is Dumb**

Mode	When users access the router’s serial ports, they must be authenticated, using either the local user database or an external authentication server. After a user has been successfully authenticated, the router connects to the specified host using the specified protocol according to: • the User Serial Service parameter for locally configured users • TACACS+/RADIUS for externally authenticated users where the target host is passed to the router
	Default: enabled See User Service settings • See *Login* • See *Telnet* • See *RLogin* • See *SSL/TLS* • See *fred * wilma Remote Access (SLIP)* • See *Remote Access (PPP)* • See *SSL/TLS*
Connect to Remote System	
Host	Select the remote host you want to connect to.
Port	The TCP Port that the router will use to connect to the host. Default: Telnet-23, SSH-22, Rlogin-513

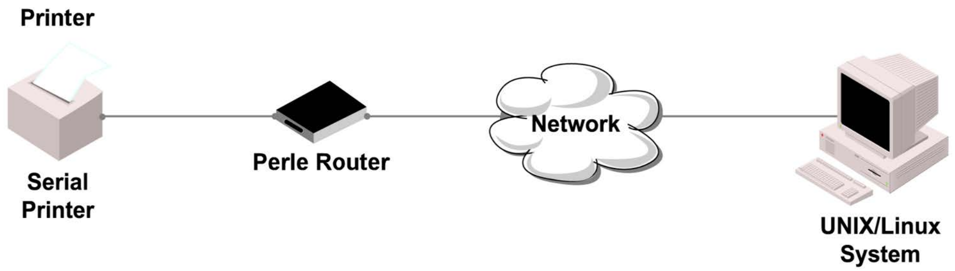
Initiate Connection	• Automatically—If the serial port hardware parameters have been setup to monitor DTR-DSR, the host session will be started once the signals are detected. • If no hardware signals are being monitored, the router will initiate the session immediately after being powered up. • Any Data Received—Initiates a connection to the specified host when any data is received on the serial port. • Specify a character—Initiates a connection to the specified host only when the specified character is received on the serial port • Connect when following character is received (Hex 00-ff) Default: disabled
Protocol	Specify the protocol used to connect to the specified host. Options—Telnet, SSH, Rlogin Default—Telnet See *Telnet* See *RLogin* See *SSH*
Enable Local Echo	Toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter is used only when Enable Line Mode is enabled. Default is disabled
Enable Line Mode	When enabled, keyboard input is not sent to the remote host until Enter is pressed, otherwise input is sent every time a key is pressed. Default is disabled
Map CR to CR/LF	When enabled, maps carriage returns (CR) to carriage return line feed (CRLF). Default is disabled
Control Characters	
Interrupt	Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal. Default is 3 (ASCII value ^C)

Quit	Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal. Default is 1c (ASCII value FS)
EOF	Defines the end-of-file character. When Enable Line Mode is enabled, entering the EOF character as the first character on a line sends the character to the remote host. This value is in hexadecimal. Default is 4 (ASCII value ^D)
Erase	Defines the erase character. When Line Mode is Off, typing the erase character erases one character. This value is in hexadecimal. Default is 8 (ASCII value ^H)
Echo	Defines the echo character. When Line Mode is On, typing the echo character echoes the text locally and sends only completed lines to the host. This value is in hexadecimal. Default is 5 (ASCII value ^E)
Escape	Defines the escape character. Returns you to the command line mode. This value is in hexadecimal. Default is 1d (ASCII value GS)
Advanced	
Enable Message of the Day (MOTD)	Enables/disables the display of the message of the day (MOTD). Default is disabled
Reset Terminal on Disconnect	When enabled, resets the terminal definition connected to the serial port when a user logs out. Default is disabled
Allow Port Locking	When enabled, you can lock your terminal with a password using the Hot Key Prefix (default Ctrl-a) ^a l (lowercase L). The router prompts you for a password and a confirmation. Default is disabled

Hot Key Prefix	The prefix that a user types to lock a serial port. Data Range: - ^a l—(Lowercase L) Locks the serial port until the user unlocks it. The user is prompted for a password (any password, excluding spaces) to lock the serial port. Next, the user must retype the password to unlock the serial port. You can use the Hot Key Prefix key to lock a serial port only when the Allow Port locking is enabled. Default is Hexadecimal 01 (Ctrl-a, ^a)
Session Timeout	Use this timer to forcibly close the session/connection when the Session Timeout expires. Default is 0 seconds so the port never timeout. Range is 0–4294967 seconds (about 49 days)
Idle Timeout	Use this timer to close a connection because of inactivity. When the Idle Timer times out, the router ends the connection. Range is 0–4294967 seconds (about 49 days) Default is 0 seconds so the port never times out
Packet Forwarding	Packet forwarding is used to control/define how and when serial port data packets are sent to and from the network. See *Packet Forwarding*
SSL/TLS	You can create an encrypted connection using SSL/TLS for the following profiles: Trueport, TCP Sockets, Terminal (the user's service must be set to SSL_RAW), Serial Tunneling, Virtual Modem and Modbus. When configuring SSL/TLS, the following configuration options are available - You can set up the router to act as an SSL/TLS client or server - There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection See *SSL/TLS*

Printer

The Printer profile allows for the serial port to be configured to support a serial printer device that can be access by the network.

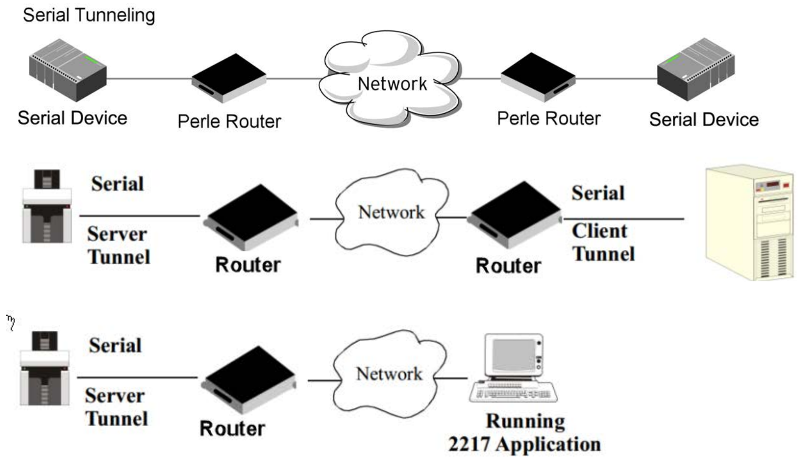


Printer	
Enable	Enable or disable interface
Description	Provide a description for this interface.
Service	Select a service type for this interface from the drop-down box.
Hardware Settings	See *Hardware settings-Serial Line*
Service Settings	
Map CR to CR/LF	The default end-of-line terminator as CR/LF (ASCII carriage-return line-feed) when enabled. Default is disabled
Session Strings	Configures session control for Send at Start, End and Delay after parameters. See *Session Strings*
Packet Forwarding	Packet forwarding is used to control/define how and when serial port data packets are sent from the router to the network. See *Packet Forwarding*

Serial Tunneling

The Serial Tunneling profile allows two routers to be connected back-to-back over the network to establish a virtual link between two serial ports based on RFC 2217.The serial device that initiates the connection is the **Tunnel Client** and the destination is the **Tunnel Server**, although once the serial communication tunnel has been successfully established, communication can go both ways **Tunnel Server**, although once the serial communication tunnel has been successfully established, communication can go both ways.

A more detailed implementation of Serial Tunneling.



The Server Tunnel will also support Telnet Com Port Control protocol as detailed in RFC 2217.

Serial Tunneling	
Enable	**Enable or disable interface**
Description	**Provide a description for this interface.**
Service	**Select a service type for this interface from the drop-down box.**
Hardware Settings	**See** ***Hardware settings-Serial Line***

Service Settings

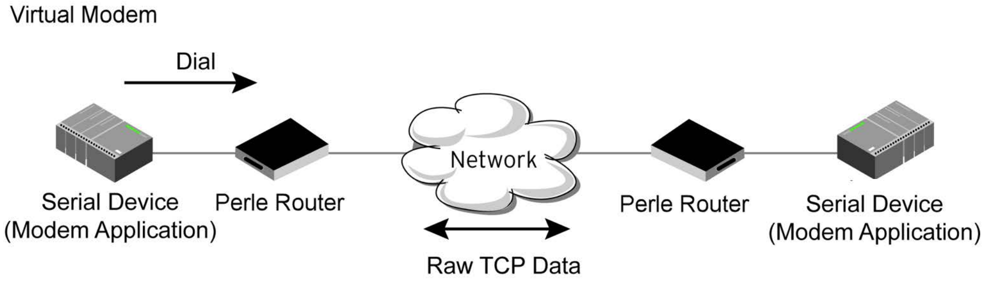
Act as a	• Tunnel Server—The router will listen for an incoming connection request on the specified Internet Address on the specified port. Default: enabled • Tunnel Client—The router will initiate the connection the Tunnel Server. Default: disabled
Listen for connection on TCP Port	The TCP port the router will listen for incoming connection. Default—10000+serial port number; so serial port 1 is 10001.
Enable TCP Keepalive	Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection sends a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized. This parameter is used in conjunction with Monitor Connection status interval parameter found in the Serial, Advanced, Advanced Settings. The interval specifies the inactivity period before testing the connection. Default: disabled
Advanced	
Break Length	When the route receives a command from its peer to issue a break signal, this parameters defines the length of time the break condition will be asserted on the serial port. Default is 1000ms (1 second)
Delay After Break	This parameter defines the delay between the termination of a a break condition and the time data will be sent out the serial port. Default is 0ms (no delay)
Packet Forwarding	Packet forwarding can be used to control/define how and when serial port data packets are sent from the router to the network. See *Packet Forwarding*

SSL/TLS	**You can create an encrypted connection using SSL/TLS for the following profiles: Trueport, TCP Sockets, Terminal (the user's service must be set to SSL_RAW), Serial Tunneling, Virtual Modem and Modbus. When configuring SSL/TLS, the following configuration options are available** • **You can set up the router to act as an SSL/TLS client or server.** • **There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection** **See *SSL/TLS***

Virtual Modem

Virtual Modem (Vmodem) is a router feature that provides a modem interface to a serial device. It responds to AT commands and provides signals in the same way that a serially attached modem would. This feature is typically used when you are replacing dial-up modems with the router in order to provide Ethernet network connectivity.

The serial port will behave in exactly the same fashion as it would if it were connected to a modem. Using AT commands, it can configure the modem and the issue a dial-out request (ATTD). The router then translate the dial request into a TCP connection and data will be begin to flow in both directions. The connection can be terminated by "hanging" up the phone line. You can also manually start a connection by typing ATD <ip_address,<port_number> and end the connection by typing +++ATH. The IP address can be in IPv4 or IPv6 format and is the IP address of the receiver. For example, ATD123.34.23.43,10001 or you can use ATD12303402304310001. You do need to add zeros where there are not three digits presents, so that the IP address is 12 digits long.



Virtual Modem	
Enable	**Enable or disable interface**
Description	**Provide a description for this interface.**
Service	**Select a service type for this interface from the drop-down box.**

Hardware Settings	See *Hardware settings-Serial Line*
Service Settings	
Listen on TCP Port	The router TCP port that the router will listen on. Default is 10000 + serial port number (for example, serial port 1 defaults to 10001)
Connection—Connect Automatically	When enabled, automatically establishes the virtual modem connection when the serial port becomes active. Default is enabled
Connection—Manually	When enabled, the virtual modem requires an AT command before it establishes a connection. Specify this option when your modem application sends a phone number or other AT command to a modem. The serial device can supply an IP address directly or it can provide a phone number that will be translated into an IP address by the router using the mapping table. Default is disabled When your modem application provides a phone number in an AT command string, you can map that phone number to the destination host. Add a phone number • Phone number • Host • TCP Port
Host	The pre-configured target host name.
TCP Port	The port number the target host is listening on for messages. Default is 0 (zero)
Send Connection Status as	When enabled, the connection success/failure indication strings are sent to the connected device, otherwise these indications are suppressed. This option also determines the format of the connection status results that are generated by the virtual modem. Default is enabled

Numerical Code	When enabled, the connection status is sent to the connected device using the following numeric codes: • 0 OK • 1 CONNECTED • 2 RING • 3 NO CARRIER • 4 ERROR • 6 ITERFACE DOWN • 7 CONNECTION REFUSED • 8 NO LISTENER
Verbose String	When enabled, the connection status is sent by text strings to the connected device. • Success—String that is sent to the serial device when a connection succeeds. Default is CONNECT <*speed*>, for example, Connect 9600 • Failure—String that is sent to the serial device when a connection fails. Default is NO CARRIER
Advanced	
Echo characters in command mode	When enabled, echoes back characters that are typed in (equivalent to ATE0/ATE1 commands). Default is disabled
Hardware Signal Assignment	
DTR Signal Always On	Specify this option to make the DTR signal always act as a DTR signal. Default is enabled
DTR Signal Acts as DCD	Specify this option to make the DTR signal always act as a DCD signal. Default is disabled
DTR Signal Acts as RI	Specify this option to make the DTR signal always act as a RI signal. Default is disabled

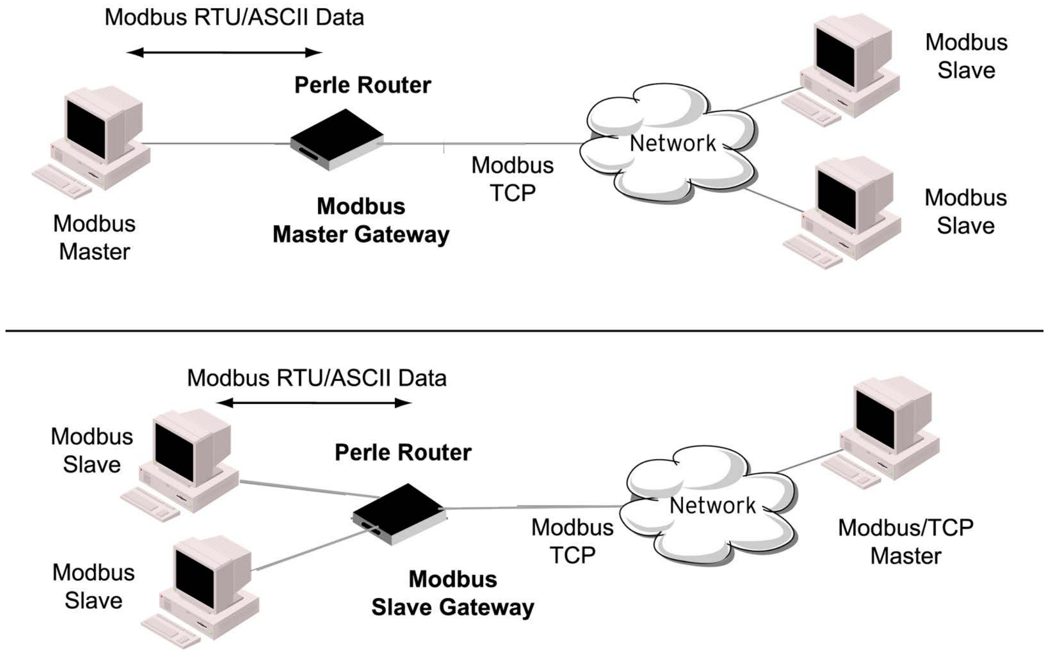
DTR Signal Acts as RI	Specify this option to make the DTR signal always act as a RI signal. Default is disabled
RTS Signal Always On	Specify this option to make the RTS signal always act as a RTS signal. Default is enabled
Additional Modem Initialization	You can specify additional modem commands that will affect how the modem starts. The following commands are supported: ATQn, ATVn, ATEn, +++ATH, ATA, ATI0, ATI3, ATS0, AT&Z1, AT&Sn, AT&Rn, AT&Cn, AT&F, ATS2, ATS12, ATO (ATD with no phone number), and ATDS1.
Enable Message of the Day (MOTD)	Enables/disables the display of the message of the day. Default is disabled
Enable TCP Keepalive	Enables a per-connection TCP keep-alive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized. This parameter needs to be used in conjunction with the Monitor Connection Status Interval parameter found under the Advanced Setting *Advanced Serial Options* configuration. The interval specifies the inactivity period before “testing” the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port. Default is disabled.
AT Command Response Delay	The amount of time, in milliseconds, before an AT response is sent to the requesting device. Default is 250 ms
Session Strings	Configures Send at Start, End and Delay after parameters for session control. See *Session Strings*
Packet Forwarding	Packet forwarding can be used to control/define how and when serial port data packets are sent fro the router to the network. See *Packet Forwarding*

SSL/TLS	**You can create an encrypted connection using SSL/TLS for the following profiles: Trueport, TCP Sockets, Terminal (the user's service must be set to SSL_RAW), Serial Tunneling, Virtual Modem and Modbus. When configuring SSL/TLS, the following configuration options are available** • **You can set up the router to act as an SSL/TLS client or server.** • **There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection** **See** ***SSL/TLS***

Modbus Gateway

The Modbus Gateway profile configures a serial port to act as a Modbus Master Gateway or a Modbus Slave Gateway. Each serial port can be configured as either a Modbus Master or gateway depending on your configuration and requirements.

Modbus



Modbus Gateway	
Enable	**Enable or disable interface**
Description	**Provide a description for this interface.**

Service	**Select a service type for this interface from the drop-down box.**
Hardware Settings	**See *Hardware settings-Serial Line***
Service Settings	
Modbus Mode - Slave	**Typically, the Modbus Master is accessing the router through the network to communicated to Modbus Slaves connected to the router's Serial Ports.**
UID Range	**You can specify a range of UIDs (1-247), in addition to individual UIDs.** **Field Format—Comma delimited; for example, 2–35, 50, 100–103**
Advanced Slave Settings	
TCP/UDP Port	**The network port number that the Slave Gateway will listen on for both TCP and UDP messages.** **Default is 502**
Next Request Delay	**A delay, in milliseconds, to allow serial slave(s) to re-enable receivers before issuing the next Modbus Master request.** **Range is 0–1000** **Default is 50 ms**
Enable Serial Modbus Broadcast	**When enabled, a UID of 0 (zero) indicates that the message will be broadcast to all Modbus Slaves.** **Default is disabled**
Request Queuing	**When enabled, allows multiple, simultaneous messages to be queued and processed in order of reception.** **Default is enabled**
UID Address mode	• **Embedded—When this option is selected, the address of the slave Modbus device is embedded in the message header.** **Default is enabled** • **Remapped—Used for single device/port operation. Older Modbus devices may not include a UID in their transmission header. When this option is selected, you can specify the UID that will be inserted into the message header for the Modbus slave device. This feature supersedes the Broadcast feature.** **Default is disabled**

Remap UID	Specify the UID to be inserted into the message header for the Slave Modbus serial device. Range is 1–247 Default is 1
Enable SSL/TLS	When enabled, Modbus Slave Gateway messages to remote TCP Modbus Masters are encrypted via SSL/TLS. Default is disabled
Protocol	• Modbus/RTU—Select this option when the Modbus/RTU protocol is being used for communication between the Modbus Master and Slave. Default is disabled
Protocol	• Modbus/ASCII—Select this option when Modbus/ASCII protocol is being used for communication between the Modbus Master and Slave. Default is enabled • Append CR/LF—When Modbus/ASCII is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. Default is enabled
Modbus Mode (Master)	
Add Slave Mapping	
UID Start	When Destination is set to Host and you have sequential Modbus Slave IP addresses (for example, 10.10.10.1, 10.10.10.2, 10.10.10.3, etc.), you can specify a UID range (not supported with IPv6 addresses) and the router will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and therouter will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100. Range is 1–247 Default is 0 (zero)

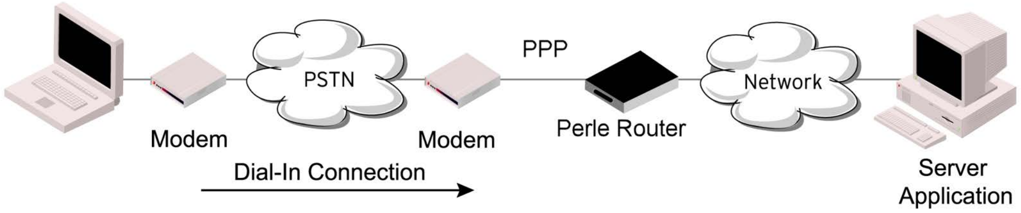
UID End	When Destination is set to Host and you have sequential Modbus Slave IP addresses (for example, 10.10.10.1, 10.10.10.2, 10.10.10.3, etc.), you can specify a UID range (not supported with IPv6 addresses) and the router will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the router will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1–10.10.10.100. Range is 1–247 Default is 0 (zero)
Type	Specify the configuration of the Modbus Slaves on the network. Data Options: • Host—The IP address is used for the first UID specified in the range. The last octet in the IPv4 address is then incremented for subsequent UID's in that range. • Gateway—The Modbus Master Gateway will use the same IP address when connecting to all the remote Modbus slaves in the specified UID range. Default is Host
Start IP Address	The IP address of the TCP/Ethernet Modbus Slave. Field Format IPv4 or IPv6 address
End IP Address	Displays the ending IP address of the TCP/Ethernet Modbus Slaves, based on the Start IP address and the UID range (not supported for IPv6 addresses). Field Format is IPv4 address or IPv6 address
Protocol	Specify the protocol that is used between the Modbus Master and Modbus Slave(s). Data Options are TCP or UDP Default is TCP
UDP/TCP Port	The destination port of the remote Modbus TCP Slave that the router will connect to. Range is 0–65535 Default is 502
Advanced	

Idle Timeout	This timer closes a connection because of inactivity. When the idle timeout expires, the router ends the connection.
	Range 0–4294967 seconds (about 49 days) Default is 0 (zero), no timeout, the connection is permanently open
Character Timeout	Used in conjunction with the Modbus RTU protocol, specifies how long to wait, in milliseconds, after a character to determine the end of frame. Range 10–10000 Default 30 ms
Message Timeout	Time to wait, in milliseconds, for a response message from a Modbus TCP or serial slave (depending if the Modbus Gateway is a Master Gateway or Slave Gateway, respectively) before sending a Modbus exception. Range 10–10000 ms Default is 1000 ms
Enable Modbus Exceptions	When enabled, an exception message is generated and sent to the initiating Modbus device when any of the following conditions are encountered: • there is an invalid UID, • the UID is not configured in the Gateway • there is no free network connection • there is an invalid message • the target device is not answering the connection attempt. Default is enabled
Session Strings	Configures Send at Start, End and Delay after parameters for session control. See *Session Strings*
Packet Forwarding	Packet forwarding can be used to control/define how and when serial port data packets are sent fro the router to the network. See *Packet Forwarding*
SSL/TLS	You can create an encrypted connection using SSL/TLS for the following profiles: Trueport, TCP Sockets, Terminal (the user's service must be set to SSL_RAW), Serial Tunneling, Virtual Modem and Modbus. When configuring SSL/TLS, the following configuration options are available. • You can set up the router to act as an SSL/TLS client or server.

	• **There is an extensive selection of SSL/TLS ciphers that you can configure for your SSL/TLS connection** **See *SSL/TLS***

Remote Access (PPP)

The Remote Access (PPP) profile configures a serial port to allow a remote user to establish a PPP connection to the router's serial port. This is typically used with a modem for dial-in or dial-out access to the network.



There are two options for PPP user authentication:

1. You can configure a specific user/password and a specific remote user/password per serial port.
2. You can create a secrets file with multiple users and their passwords that will globally authenticate users on all serial ports.
3. You can use configure PPP authentication in the configuration or in the secrets file, but not both.
4. If you want to use a secrets file, you must download the secrets file to the router for CHAP or PAP authentication: the files must be downloaded to the router using the names chap-secrets and pap-secrets, respectively. The file can be downloaded to the router under the Administration, Key and Certificates, download other file.

In the Remote Access (PPP) profile, you must also specify the Authentication option as PAP or CHAP on the under Authentication, but you must leave the User, Password, Remote User and Remote Password fields blank.

An example of the CHAP secrets file follows:

```
#Secrets for authentication using CHAP
# clients                serversecret acceptable local IP addresses
barney                   fredwilma192.168.43.1
fred                     barneyflintstone1234567890192.168.43.2

#Secrets for authentication using PAP
# clients                serversecret acceptable local IP addresses
barney                   *flintstone1234567890
```

fred *wilmaRemote Access (SLIP)

Remote Access (PPP)	
Enable	Enable or disable interface
Description	Provide a description for this interface.
Service	Select a service type for this interface from the drop-down box.
Hardware Settings	See *Hardware settings-Serial Line*
Service Settings	
IPv4	
Local IP address	The IPV4 IP address of the router end of the PPP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the router's (main) IP address in this field; if you do so, routing will not take place correctly.
IPv4 Remote IP Address	The IPv4 address of the remote end of the PPP link. Choose an address that is part of the same network or subnetwork as the router. If you set the PPP parameter IP Address Negotiation to On, the router will ignore the remote IP address value you enter here and will allow the remote end to specify its IP address. If your user is authenticated by RADIUS and the RADIUS parameter framed-address is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here. The exception to this rule is a Framed-address value in the RADIUS file of 255.255.255.255; this value allows the router to use the remote IP address value configured here.
IPv4 Subnet Mask	The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS and the RADIUS parameter Framed-netmask is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here.

Negotiation IP addresses automatically	Specifies whether or not IP address negotiation will take place. IP address negotiation is where the router allows the remote end to specify its IP address. When On, the IP address specified by the remote end will be used in preference to the remote IP Address set for a Serial Port, When Off, the remote IP address for the Serial Port will be used. Default is disabled
Dial	
Connection Method Connect—select the connection method.	
Dial In	The device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default is disabled
Dial Out	If you want the modem to dial a number when the serial port is started, enable this parameter. Default is disabled
Dial in/Dial Out	Dial in/Dial Out—Enable this option when you want the serial port to do either of the following: • accept a call from a modem or ISDN TA • dial a number when the serial port is started. Default is disabled
MS Direct	• MS Direct Host—Specify this option when the serial port is connected to a Microsoft Guest device. Default is enabled • MS Direct Guest—Enable this option when the serial port is connected to a Microsoft Host device. Default is disabled
Dial Timeout	The number of seconds the router will wait to establish a connection to a remote modem. Range is 1–99 Default is 45 seconds
Dial Retries	The number of times the router will attempt to re-establish a connection with a remote modem. Range is 0–99 Default is 2

Modem init string	You can specify additional modem commands that will affect how the modem starts. The following commands are supported: ATQn, ATVn, ATEn, +++ATH, ATA, ATI0, ATI3, ATS0, AT&Z1, AT&Sn, AT&Rn, AT&Cn, AT&F, ATS2, ATS12, ATO (ATD with no phone number), and ATDS1.
Phone number	The phone number to use when Dial Out is enabled.
Authentication	The type of authentication that will be done on the link. You can use PAP or CHAP(MD5-CHAP, MS-CHAPv1 and MS-CHAPv2) to authenticate a user or client on the router. When setting either PAP and CHAP, make sure the router and the PPP peer, have the same setting. For example, if the router is set to PAP, but the remote end is set to CHAP, the connection will be refused.
None	No authentication will be preformed.
PAP	PAP is a one time challenge of a client/device requiring that it responds with a valid username and password. A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated.
CHAP	CHAP—challenges a client/device at regular intervals to validate itself with a username and a response, based on a hash of the secret (password). A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated. MD5-CHAP and Microsoft MS-CHAPv1/MS-CHAPv2 are supported. The router will attempt MS-CHAPv2 with MPPC compression, but will negotiate to the variation of CHAP, compression and encryption that the remote peer wants to use. Default is CHAP

User	Complete this field only if you have specified PAP or CHAP (security protocols) in the Authentication field, and you wish to dedicate this line to a single remote user, who will be authenticated by the router or you are using the router back-to-back with another router. When Connect is set to Dial Out or both Dial In/Dial Out are enabled, the User is the name the remote device will use to authenticate a port on this router. The remote device will only authenticate your router's port when PAP or CHAP are operating. You can enter a maximum of sixteen alphanumeric characters; for example, tracy201. When connecting together two networks, enter a dummy user name; for example, DS_HQ. Note: If you want a reasonable level of security, the user name and password should not be similar to a user name or password used regularly to login to the router. External authentication can not be used for this user. Field Format is you can enter a maximum of 254 alphanumeric characters.
Password	Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field and: • you wish to dedicate this serial port to a single remote user, who will be authenticated by the router or • you are using the router back-to-back with another router Password means the following: • When PAP is specified, this is the password the remote device will use to authenticate the port on this router. • When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges shall be based. Field Format is you can enter a maximum of 16 alphanumeric characters.

Remote User	Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, and • you wish to dedicate this line to a single remote user, who will be authenticated by the router, or • you are using the router back-to-back with another router When Dial In or Dial In/Dial Out is enabled, the Remote User is the name the router will use to authenticate the port on the remote device. Your router will only authenticate the port on the remote device when PAP or CHAP are operating. When connecting together two networks, enter a dummy user name; for example, DS_SALES. Note: If you want a reasonable level of security, the user name and password should not be similar to a user name or password used regularly to login to the router. This option does not work with external authentication. Field Format is you can enter a maximum of 254 alphanumeric characters
Remote Password	Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, and • you wish to dedicate this serial port to a single remote user, and this user will be authenticated by the router • you are using the router back-to-back with another router Remote password means the following: • When PAP is specified, this is the password the router will use to authenticate the remote device. • When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges will be based. Remote password is the opposite of the parameter Password. Your router will only authenticate the remote device when PAP or CHAP is operating. Field format is you can enter a maximum of 16 alphanumeric characters
Authentication Timeout	The timeout, in minutes, during which successful PAP or CHAP authentication must take place (when PAP or CHAP are specified). If the timer expires before the remote end has been authenticated successfully, the link will be terminated. Range is 1–255 minutes Default is 1 minute

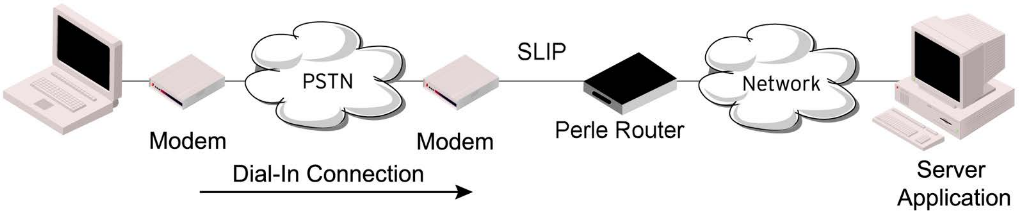
CHAP Challenge Interval	The interval, in minutes, for which the router will issue a CHAP re-challenge to the remote end. During CHAP authentication, an initial CHAP challenge takes place, and is unrelated to CHAP re-challenges. The initial challenge takes place even if rechallenges are disabled. Some PPP client software does not work with CHAP rechallenges, so you might want to leave the parameter disabled in the router. Range is 0–255 Default is 0 (zero), meaning CHAP re-challenge is disabled
Enable Roaming Callback	A user can enter a telephone number that the router will use to callback him/her. This feature is particularly useful for a mobile user. Roaming callback can only work when the User Enable Callback parameter is enabled. Enable Roaming Callback therefore overrides (fixed) User Enabled Callback To use Enable Roaming Callback, the remote end must be a Microsoft Windows OS that supports Microsoft's Callback Control Protocol (CBCP). You are allowed 30 seconds to enter a telephone number after which the router ends the call. Default is disabled
Routing	Determines the routing mode (RIP, Routing Information Protocol) used on the PPP interface. This is the same function as the Framed-Routing attribute for RADIUS authenticated users. Default is None
Data Options: None	None—Disables RIP over the PPP interface.
Send	Sends RIP over the PPP interface.
Listen	Listens for RIP over the PPP interface.
Send and Listen	Send and Listen—Sends RIP and listens for RIP over the PPP interface.

ACCM	Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream. The Field Formats is entered as a 32-bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped. The bits are specified as the most significant bit first and are numbered 31-0. Thus if bit 17 is set, the 17th character should be escaped, that is, 0x11 (XON). The value 000a0000 will cause the control characters 0x11 (XON) and 0x13 (XOFF) to be escaped on the link, thus allowing the use of XON/XOFF (software) flow control. If you have selected soft Flow Control on the Serial Port, you must, you must enter a value of at least 000a0000 for the ACCM. Default is 00000000, which means no characters will be escaped
MRU	The Maximum Receive Unit (MRU) parameter specifies the maximum size of PPP packets that the router's port will accept. If your user is authenticated by the router, the MRU value will be overridden if you have set a MTU value for the user. If your user is authenticated by RADIUS and the RADIUS parameter Framed-MTU is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here. Range is 64–1500 bytes Default is 1500
Configure Request Retries	The maximum number of times a configure request packet will be re-sent before the link is terminated. Range is 0–255 Default is 10 seconds
Configure Request Timeout	The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a configure request packet to have been lost. Range is 1–255 Default is 3 seconds
Terminate Request Retries	The maximum number of times a terminate request packet will be re-sent before the link is terminated. Range is 0–255 Default is 3 seconds

Terminate Request Timeout	The maximum time, in seconds, that LCP (Link Control Protocol) will wait before it considers a terminate request packet to have been lost. Range is 1–255 Default is 3 seconds
Echo Request Retries	The maximum number of times an echo request packet will be re-sent before the link is terminated. Range is 0–255 Default is 3
Echo Request Timeout	The maximum time, in seconds, between sending an echo request packet if no response is received from the remote host. Range is 0–255 Default is 30 seconds
Configure NAK	The maximum number of times a configure NAK packet will be re-sent before the link is terminated. Range is 0–255 Default is 10 seconds
Enable Address/ Control Compression	This determines whether compression of the PPP Address and Control fields take place on the link. For most applications this should be enabled. Default is enabled
Enable Protocol Compression	This determines whether compression of the PPP Protocol field takes place on this link. Default is enabled
VJ Compression	When enabled, Van Jacobson Compression is used on this link. If your user is authenticated by the router, this VJ compression value will be overridden if you have enabled the User, Enable VJ Compression parameter. If the user is authenticated by RADIUS and the RADIUS parameter Framed Compression is set in the value configured here. Default is enabled
Enable Magic Negotiation	Determines if a line is looping back. If enabled (On), random numbers are sent on the link. The random numbers should be different, unless the link loops back. Default is disabled

Idle Timeout	Use this timer to close a connection because of inactivity. When the idle timeout expires, the router will end the connection. Range is 0–4294967 seconds (about 49 days) Default is 0 (zero), which does not timeout, so the connection is permanently open
Session Strings	See *Session Strings*
Packet Forwarding	Packet forwarding is used to control/define how and when serial port data packets are sent from the router to the network. See *Packet Forwarding*

The Remote Access (SLIP) profile configures a serial port to allow a remote user to establish a SLIP connection to the uter's serial port. This is typically used with a modem for dial in or dial out access to the network.



Remote Access (SLIP)	
Enable	Enable or disable interface
Description	Provide a description for this interface.
Service	Select a service type for this interface from the drop-down box.
Hardware Settings	See *Hardware settings-Serial Line*
Service Settings	
IPv4	

Local IP address	The IPV4 IP address of the router end of the SLIP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the router's (main) IP address in this field; if you do so, routing will not take place correctly.
IPv4 Remote IP Address	The IPv4 address of the remote end of the SLIP link. Choose an address that is part of the same network or subnetwork as the router. If your user is authenticated by the router, this remote IP address will be overridden if you have set a Framed IP Address for the user. If your user is authenticated by RADIUS and the RADIUS parameter Framed -Address is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here.
IPv4 Subnet Mask	The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS and the RADIUS parameter Framed-netmask is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here.
MTU	The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the router. Enter a value between 256 and 1006 bytes; for example, 512. The default is 256. If your user is authenticated by the router, this MTU value will be over-ridden when you are a Framed-MTU value set for the user. If your user is authenticated by RADIUS and the RADIUS parameter Framed-MTU is set in RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here. Default is 256
Routing	Determines the routing mode (RIP, Routing Information Protocol) used on the SLIP interface. This is the same function as the Framed-Routing attribute for RADIUS authenticated users. Data Options: • None—Disables RIP over the SLIP interface. • Send—Sends RIP over the SLIP interface. • Listen—Listens for RIP over the SLIP interface. • Send and Listen—Sends RIP and listens for RIP over the SLIP interface. Default is none

VJ Compression	When enabled, Van Jacobson Compression is used on this link. If your user is authenticated by the router, this VJ compression value will be overridden if you have enabled the User, Enable VJ Compression parameter. If the user is authenticated by RADIUS and the RADIUS parameter Framed Compression is set in the value configured here. Default is enabled
Dial Options	Select the connection method. • Direct Connect—Specify this option when a modem is not connected to this serial port. Default is enabled • Dial In—If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default is disabled
	• Dial Out—If you want the modem to dial a number when the serial port is started, enable this parameter. Default is disabled • Dial in/Dial Out—Enable this option when you want the serial port to do either of the following: • accept a call from a modem or ISDN TA • dial a number when the serial port is started. Default is disabled
Modem init string	You can specify additional modem commands that will affect how the modem starts. The following commands are supported: ATQn, ATVn, ATEn, +++ATH, ATA, ATI0, ATI3, ATS0, AT&Z1, AT&Sn, AT&Rn, AT&Cn, AT&F, ATS2, ATS12, ATO (ATD with no phone number), and ATDS1.
Phone number	The phone number to use when Dial Out is enabled.
Session Strings	Configures Send at Start, End and Delay after parameters for session control. See *Session Strings*
Packet Forwarding	Packet forwarding can be used to control/define how and when serial port data packets are sent from the router to the network. See *Packet Forwarding*

Dial Options

Dial in	If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter. Default is disabled
Dial out	If you want the modem to dial a number when the serial port is started, enable this parameter. Default is disabled
Dial Timeout	The number of seconds the router waits to establish a connection to a remote modem. Range is 1–99 Default is 45 seconds
Dial Retries	The number of times the router attempts to re-establish a connection with a remote modem. Range is 0–99 Default is 2
Modem Init String	You can specify additional modem commands that affect how the modem starts.
Phone Number	Specify the phone number your modem application sends to the modem. Note: The router does not validate the phone number, so it must be entered in the exact way the application will send it. For example, if you enter 555-1212 in this table and the application sends 5551212, the router will not match the two numbers. Spaces will be ignored.
Session Strings	
Send at Start	Session Strings Controls the sending of ASCII strings to serial device at session start as follows; Send at Start—If configured, this string will be sent to the serial device on power-up of the router, or when a kill line command is issued on this serial port. If the monitor DTR-DSR option is set, the string will also be sent when the monitored signal is raised. Range is 0–127 alpha-numeric characters Range is hexadecimal 0-FF

Send at End	If configured, this string is sent to the serial device when the TCP session on the router is terminated. If multihost is configured, this string will only be send in listen mode to the serial device when all multi-host connections are terminated. Range is 0–127 alpha-numeric characters. Non printable ASCII character must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3).
Delay after Send	If configured, this command will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated. Default is 10 ms

Packet Forwarding

Packet forwarding can be used to control/define how and when serial port data packets are sent from the router to the network.

Define how the data received on the serial port with be forwarded to the network.

Minimize Latency	This option ensures that all application data is immediately forwarded to the serial device and that every character received from the serial device is immediately sent on the network. Select this option for timing-sensitive applications. Default is disabled
Optimize Network Throughput	This option provides optimal network usage while ensuring that the application performance is not comprised. Select this option when you want to minimize overall packet count, such as when the connection is over a WAN. Default is disabled
Prevent Message Fragmentation	This option detects the message, packet or data blocking characteristics of the serial data and preserves it through the communication. Select this option for message-based application or serial devices that are sensitive to inter-character delays within these messages. Default is disabled
Delay Between Messages	• Minimize Latency • Optimize Network Throughput • Prevent Message Fragmentation • Custom Packet Forwarding

Custom Packet Forwarding	This option allows you to define forwarding rules based on the packet definition or the frame definition. Default is disabled
Packet Definition	When enabled, this group of parameters allows you to set a variety of packet definition options. The first criteria that is met causes the packet to be transmitted. For example, you set a Force Transmit Timer of 1000 ms and a packet size of 100 bytes, whichever criteria is met first is what will cause the packet to be transmitted. Default is disabled
Packet Size	The number of bytes that must be received from the serial port before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Range is 0–1024 bytes Default is 0
Idle Time	The amount of time, in milliseconds, that must elapse between characters before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Range is 0–65535 ms Default is 0
End Trigger1 Character	When enabled, specifies the character that when received will define when the packet is ready for transmission. The actual transmission of the packet is based on the Trigger Forwarding Rule. Range Hexadecimal 0–FF Default is 0
End Trigger2 Character	When enabled, creates a sequence of characters that must be received to specify when the packet is ready for transmission (if the End Trigger1 character is not immediately followed by the End Trigger2 character, the router waits for another End Trigger1 character to start the End Trigger1/End Trigger2 character sequence). The actual transmission of the packet is based on the Trigger Forwarding Rule. Range Hexadecimal 0–FF Default is 0
Frame Definition	When enabled, this group of parameters allows you to control the frame that is transmitted by defining the start and end of frame character(s). If the internal buffer (1024 bytes) is full before the EOF character(s) are received, the packet will be transmitted and the EOF character(s) search will continue. Default is disabled

SOF1 Character	When enabled, the Start of Frame character defines the first character of the frame, any character(s) received before the Start of Frame character is ignored. Range Hexadecimal 0–FF Default is 0
SOF2 Character	When enabled, creates a sequence of characters that must be received to create the start of the frame (if the SOF1 character is not immediately followed by the SOF2 character, the router waits for another SOF1 character to start the SOF1/SOF2 character sequence). Range Hexadecimal 0–FF Default is 0
Transmit SOF Character(s)	When enabled, the SOF1 or SOF1/SOF2 characters will be transmitted with the frame. If not enabled, the SOF1 or SOF1/SOF2 characters will be stripped from the transmission. Default is 0
EOF1 Character	Specifies the End of Frame character, which defines when the frame is ready to be transmitted. The actual transmission of the frame is based on the Trigger Forwarding Rule. Range Hexadecimal 0–FF Default is 0
EOF2 Character	When enabled, creates a sequence of characters that must be received to define the end of the frame (if the EOF1 character is not immediately followed by the EOF2 character. The router waits for another EOF1 character to start the EOF1/EOF2 character sequence), which defines when the frame is ready to be transmitted. The actual transmission of the frame is based on the Trigger Forwarding Rule. Range Hexadecimal 0–FF Default is 0
Trigger Forwarding Rule	Determines what is included in the Frame (based on the EOF1 or EOF1/EOF2) or Packet (based on Trigger1 or Trigger1/Trigger2). Choose one of the following options: Default is Trigger
Strip-Trigger	Strips out the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings.
Trigger	Includes the EOF1, EOF1/EOF2, Triggr1 or Trigger/Trigger2 depending on your settings.

Trigger+1	Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/ Trigger2,depending on your settings, plus the first byte that follows the trigger.
Trigger+2	Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the next two bytes received after the trigger.
SSL/TLS	
Enable	Enable or disable SSL/TLS.
SSL/TLS Version	Select version of SSL/TLS. Some TLS versions may not be available on some firmware versions or models. • Any • Suite B TLS • TLS v1.2 • TLS v1.3
SSL/TLS Type	• Client • Server
Add Cipher	
Encryption	• Any • AES • 3DES • DES • ARCTWO • ARCFOUR • AES-GCM
Minimum Key Size	• 40 • 56 • 64 • 128 • 168 • 256

Maximum Key Size	• 40 • 56 • 64 • 128 • 168 • 256
Key Exchange	• Any • RSA • EHD-RSA • EDH-DSS • ADH • ECDH-ECDSA
HMAC	• Any • SHA1 • MD5 • SHA256 • SHA384
Validate Peer Certificate	This is the SSL/TLS passphrase used to generate an encrypted RSA/DSA private key. This private key and passphrase are required for both HTTPS and SSL/TLS connections, unless an unencrypted private key was generated, then the SSL passphrase is not required. Make sure that you download the SSL private key and certificate if you are. If both RSA and DSA private keys are downloaded to the router, they need to be generated using the same SSL passphrase for both to work. Enable this option when you want the Validation Criteria to match the Peer Certificate for authentication to pass. If you enable this option, you need to download an SSL/TLS certificate authority (CA) list file to the router. Default is Disabled
Country	A country code; for example, US. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data option is two characters
State/Province	An entry for the state/province; for example, IL. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Option is Maximum 128 characters

Locality	An entry for the location; for example, Chicago. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Option is Maximum 128 characters
Organization	An entry for the organization; for example, Accounting. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Option is maximum 64 characters
Organizational Unit	An entry for the unit in the organization; for example, Payroll. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Option is maximum 64 characters
Common Name	An entry for common name; for example, the host name or fully qualified domain name. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Option is Maximum 64 characters
Email	An entry for an email address; for example, acct@anycompany.com. This field is case sensitive in order to successfully match the information in the peer SSL/TLS certificate. Data Option is maximum 64 characters

Terminal User Service Settings

Login	
Terminal Type	Type of terminal attached to this serial port. • ansi, dumb, hp700, ibm3151TE, tvi925, vt100, vt320, wyse60
Mode	
Limit Connection to User	Makes the serial port dedicated to the specified user. The user won't need to enter their login name - just their password.
Terminal Pages	The number of video pages the terminal supports. Range: 1–7 Default is 5 pages

Telnet	
Enable Local Echo	Toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter can be used only when enable Line Mode is enabled. Default is disabled
Enable Line Mode	When enabled, keyboard input is not sent to the remote host until Enter is pressed, otherwise input is sent every time a key is pressed. Default is disabled
Map CR to CR/LF	When enabled, maps carriage returns (CR) to carriage return line feed (CRLF). D Default is disabled
Control Characters	
Interrupt	Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal. Default: is (ASCII value ^C)
Quit	Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal. Default is 1c (ASCII value FS)
EOF	Defines the end-of-file character. When enabled Line Mode, entering the EOF character as the first character on a line sends the character to the remote host. This value is in hexadecimal. Default is 4 (ASCII value ^D)
Erase	Defines the erase character. When Line Mode is Off, typing the erase character erases one character. This value is in hexadecimal. Default: is 8 (ASCII value ^H)
Echo	Defines the echo character. When Line Mode is On, typing the echo character echoes the text locally and sends only completed lines to the host. This value is in hexadecimal. Default: 5 (ASCII value ^E)

Escape	Defines the escape character. Returns you to the command line mode. This value is in hexadecimal. Default: 1d (ASCII value GS)

RLogin	
Terminal Type	Type of terminal attached to this serial port; for example, ANSI or WYSE60.
SSH	
Terminal Type	Type of terminal attached to this serial port.
	• ansi, hp700, ibm3151TE, tvi925, vt100, vt320,wyse60 Default is dumb
Verbose Mode	When enabled, displays debug messages on the terminal. Default is disabled
Enable Compression	When enabled, requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down things on fast networks. Default is disabled
Strict Host Checking	When enabled, a host public key (for each host you want to ssh to) must be downloaded into the router. Default: is enabled
Login Automatically	When enabled, creates an automatic SSH login, using the name and Password values. Default is enabled
Name	The name of the user logging into the SSH session. Field Format: Up to 20 alphanumeric characters, excluding spaces.
Password	The user’s password when auto login is enabled. Format: Up to 20 alphanumeric characters, excluding spaces.
Protocol	

SSH2 Cipher	• 3DES • Blowfish • AES-CBC • CAST • ARCFOUR • AES-CTR • AES-GCM • ChaCha20-Poly1305
Authentica tion	• RSA • DSA • Keyboard-interactive
Keyboard Authentication	When enabled, the user types in a password for authentication. Default is enabled
SLIP	
Local IP address	The IPV4 IP address of the router end of the SLIP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the router's (main) IP address in this field; if you do so, routing will not take place correctly.
IPv4 Remote IP Address	The IPv4 address of the remote end of the SLIP link. Choose an address that is part of the same network or subnetwork as the router. If your user is authenticated by the router, this remote IP address will be overridden if you have set a Framed IP Address for the user. If your user is authenticated by RADIUS and the RADIUS parameter Framed -Address is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here.
IPv4 Subnet Mask	The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS and the RADIUS parameter Framed-netmask is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here.

MTU	The Maximum Transmission Unit (MTU) parameter restricts the size of individual SLIP packets being sent by the router. Enter a value between 256 and 1006 bytes; For example, 512. The default value is 256. If your user is authenticated by the router, this MTU value will be overridden when you have set a Framed-MTU value for the user. If your user is authenticated by RADIUS and the RADIUS parameter Framed-MTU is set in the RADIUS file, therouter will use the value in the RADIUS file in preference to the value configured here. Default is 256
PPP	
Settings IPv4	
Local IP address	The IPV4 IP address of the router end of the PPP link. For routing to work, you must enter a local IP address. Choose an address that is part of the same network or subnetwork as the remote end; for example, if the remote end is address 192.101.34.146, your local IP address can be 192.101.34.145. Do not use the router's (main) IP address in this field; if you do so, routing will not take place correctly.
IPv4 Remote IP Address	The IPv4 address of the remote end of the PPP link. Choose an address that is part of the same network or subnetwork as the router. If you set the PPP parameter IP Address Negotiation to On, the router will ignore the remote IP address value you enter here and will allow the remote end to specify its IP address. If your user is authenticated by RADIUS and the RADIUS parameter framed-address is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here. The exception to this rule is a Framed-address value in the RADIUS file of 255.255.255.255; this value allows the router to use the remote IP address value configured here.
IPv4 Subnet Mask	The network subnet mask. For example, 255.255.0.0. If your user is authenticated by RADIUS and the RADIUS parameter Framed-netmask is set in the RADIUS file, the router will use the value in the RADIUS file in preference to the value configured here.
Enable IP Address Negotiation	Specifies whether or not IP address negotiation will take place. IP address negotiation is where the router allows the remote end to specify its IP address. When On, the IP address specified by the remote end will be used in preference to the remote IP Address set for a Serial Port, When Off, the remote IP address for the Serial Port will be used. Default is disabled

Authentication	
Authentication Type	The type of authentication that will be done on the link. You can use PAP or CHAP(MD5-CHAP, MS-CHAPv1 and MS-CHAPv2) to authenticate a user or client on the router. When setting either PAP and CHAP, make sure the router and the PPP peer, have the same setting. When setting either PAP and CHAP, make sure the router and the PPP peer, have the same setting. For example, if the router is set to PAP, but the remote end is set to CHAP, the connection will be refused. Default is CHAP
None	No authentication will be preformed.
PAP	PAP is a one time challenge of a client/device requiring that it respond with a valid username and password. A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated.
CHAP	CHAP challenges a client/device at regular intervals to validate itself with a username and a response, based on a hash of the secret (password). A timer operates during which successful authentication must take place. If the timer expires before the remote end has been authenticated successfully, the link will be terminated.
MD5-CHAP	MD5-CHAP and Microsoft MS-CHAPv1/MS-CHAPv2 are supported. The router will attempt MS-CHAPv2 with MPPC compression, but will negotiate to the variation of CHAP, compression and encryption that the remote peer wants to use. Default is CHAP

User	Complete this field only if you have specified PAP or CHAP (security protocols) in the Authentication field, and you wish to dedicate this line to a single remote user, who will be authenticated by the router or you are using the router as a router (back-to-back with another router). When Connect is set to Dial Out or both Dial In/Dial Out are enabled, the User is the name the remote device will use to authenticate a port on this router. The remote device will only authenticate your router's port when PAP or CHAP are operating. You can enter a maximum of sixteen alphanumeric characters; for example, tracy201. When connecting together two networks, enter a dummy user name; for example, DS_HQ. Note: If you want a reasonable level of security, the user name and password should not be similar to a user name or password used regularly to login to the router. External authentication can not be used for this user. Field Format: you can enter a maximum of 254 alphanumeric characters.
Password	Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field and: • you wish to dedicate this serial port to a single remote user, who will be authenticated by the router or • you are using the router (back-to-back with another router) Password means the following: • When PAP is specified, this is the password the remote device will use to authenticate the port on this router. • When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges shall be based. • Field Format maximum of 16 alphanumeric chars.

Remote User	Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, and • you wish to dedicate this line to a single remote user, who will be authenticated by the router, or • you are using the router back-to-back with another router When Dial In or Dial In/Dial Out is enabled, the Remote User is the name the router will use to authenticate the port on the remote device. Your router will only authenticate the port on the remote device when PAP or CHAP are operating. When connecting together two networks, enter a dummy user name; for example, DS_SALES. Note: If you want a reasonable level of security, the user name and password should not be similar to a user name or password used regularly to login to the router. This option does not work with external authentication. Field Format is you can enter a maximum of 254 alphanumeric characters
Remote Password	Complete this field only if you have specified PAP or CHAP (security protocols) in the Security field, and • you wish to dedicate this serial port to a single remote user, and this user will be authenticated by the router, or • • you are using the router back-to-back with another router Remote password means the following: • When PAP is specified, this is the password the router will use to authenticate the remote device. • When CHAP is specified, this is the secret (password) known to both ends of the link upon which responses to challenges will be based. Remote password is the opposite of the parameter Password. Your router will only authenticate the remote device when PAP or CHAP is operating. Field format is you can enter a maximum of 16 alphanumeric characters
Authentication Timeout	The timeout, in minutes, during which successful PAP or CHAP authentication must take place (when PAP or CHAP are specified). If the timer expires before the remote end has been authenticated successfully, the link will be terminated. Range is 1–255 Default is 1 minute

CHAP Challenge Interval	The interval, in minutes, for which the router will issue a CHAP re-challenge to the remote end. During CHAP authentication, an initial CHAP challenge takes place, and is unrelated to CHAP re-challenges. The initial challenge takes place even if rechallenges are disabled. Some PPP client software does not work with CHAP re-challenges, so you might want to leave the parameter disabled in the router. Range is 0–255 Default is 0 (zero), meaning CHAP re-challenge is disabled
Enable Roaming Callback	A user can enter a telephone number that the router will use to callback him/her. This feature is particularly useful for a mobile user. Roaming callback can only work when the User Enable Callback parameter is enabled. Enable Roaming Callback therefore overrides (fixed) User Enabled Callback To use Enable Roaming Callback, the remote end must be a Microsoft Windows OS that supports Microsoft's Callback Control Protocol (CBCP). The user is allowed 30 seconds to enter a telephone number after which the router ends the call. Default is disabled
Advanced	
Routing Data Options:	Determines the routing mode (RIP, Routing Information Protocol) used on the PPP interface. This is the same function as the Framed-Routing attribute for RADIUS authenticated users. Default is None
None	Disables RIP over the PPP interface.
Send	Sends RIP over the PPP interface.
Listen	Listens for RIP over the PPP interface.
Send and Listen	Sends RIP and listens for RIP over the PPP interface.

ACCM	**Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream. The Field Formats is entered as a 32-bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped.** **The bits are specified as the most significant bit first and are numbered 31-0. Thus if bit 17 is set, the 17th character should be escaped, that is, 0x11 (XON). The value 000a0000 will cause the control characters 0x11 (XON) and 0x13 (XOFF) to be escaped on the link, thus allowing the use of XON/XOFF (software) flow control. If you have selected soft Flow Control on the Serial Port, you must, you must enter a value of at least 000a0000 for the ACCM.** **Default is 00000000, which means no characters will be escaped**

Network

Cellular Profiles	
Cellular profile name	Provide a description for this interface. Name can be up to 32 characters long. Maximum profiles is 16.
SIM slot	Depending on the model. 1 or 2 Default is 1
Radio technology	• Auto • LTE (4G) • UMTS (3G) • 5g
Roaming allowed	Allow roaming on the cellular network. Select enabled to allow your router to roam outside of your provider's coverage area. If your router moves outside of your provider's coverage and registers on a new LTE network: • The router's LTE connection stays disconnect until the router re-enters the provider' coverage area. • If LTE Failover is configured, then failover to the alternate profile may occur. If disconnected due to roaming the router may stay registered to the network which means that SMS may be possible and charges may occur.
Modem firmware	• SIM-Based • Generic • ATT • Verizon • Specific Other • Carrier name

Cellular bands	**Select the cellular band. (Depending on the firmware version or model)** • auto • 1 • 2 • 3 • 4 • 57 • 8 • 9 • 12 • 13 • 14 Public Safety • 17 • 18 • 19 • 26 Public Safety • 28 Public Safety • 29 • 30 • 32 • 4142 CBRS • 43 CBRS • 46 • 48 CBRS • 66 • 1800 GSM • 1900 GSM • 850 GSM • 900 GSM
5g bands	**Select the cellular band.** • auto • 1 • 2 • 3 • 4 • 5 • 28 • 41

	• 66 • 71 • 77 • 78
Carrier Aggregation	Enabled to acquire successively higher peak data rates as well as better broadband experience across the coverage area. Default is enabled
PIN	Maximum 4–8 digits either encrypted or unencrypted.
APN	Maximum of 16 cellular profiles can be created.
Use default APN	Enabled by default.
Advanced	
Data APN Settings	Specific the APN to use for this connection.
APN	
PDP type	Specify the PDP type • IPv4 • IPv6 • IPv4/IPv6 Default is IPv4
Context identifier	Range 1–16 Default is 1 Note: This is an internal slot number not the SIM slot.
Authentication Type	Specify the authentication type • None • CHAP • PAP
Mobile Data Monitor	
Monthly Data Limit (MB)	Maximum is 100,000
Billing Day	1–31 (days in the month)
Alert at (% used)	0–99%—send an alert/trap when percentage is reached

Alert when data limit is reached	Send an alert • None • Disconnect LTE Default is None
Wireless Profiles	
Network name (SSID)	Provide a description for this interface. Name can be up to 32 characters long. Maximum profiles are 16.
Security Type	Select the security type • opened • WEP • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise • WPA1/2 Personal • WPA1/2 Enterprise • 802.1x
	To use WPA-Enterprise you must create a RADIUS server. Default is opened
WEP Key	Hex-string of 10, 27, or 32 characters long
Encryption Type	Depending on the security type selected. • TKIP • CCMP • CCMP/TKIP
Security Key	Values are 8–62 characters in length
Hidden SSID	Select hidden SSID if you do not want to broadcast your network name. Default is not hidden
Prevent low level bridging of frames between associated clients	Dot not allow bridge between clients. Default is off

Management frame protection	**Set management frame protection (MFP).** • **Disabled—no MFP negotiated** • **Mandatory—clients must support MFP** • **Optional—clients are allowed to associate only if MFP is negotiated (that is, if WPA2 is configured on the router and the client supports CCXv5 MFP and is also configured for WPA2)**
Max Number of Clients	**Set the number of clients that can connect at the same time to this ssid.** **Values are 1–2007** **Default is 2007**

DNS

Overview

The DNS (Domain Name Service) protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. This enables you to substitute the hostname for the IP address within all local IP commands, such as ping and telnet. The IP address of the DNS server can be obtained from either a DHCP server or manually configured on your router.

The local Host Table in your router provides the same function of converting a name to an IP address to that of using an external DNS server but uses a local database manually configured by you on your router.

Feature details / Application notes

- Configure an external DNS server to resolve name to IP address
- Configure a local host table with a database of names to IPv4 addresses
- The host table is examined before doing a lookup via a DNS server

DNS Global Setting

DNS Servers	
Enable DNS	**Enabled or disabled DNS.** **Default is enabled**
IPv4 Address (Add, Delete)	**Enter an IPv4 address for your DNS server. Select the + symbol to add more.**

IPv6 DNS Servers	
Enable DNS	**Enabled or disabled DNS.** **Default is enabled**

IPv6 DNS Servers (Add, Delete)	Enter an IPv6 address for your DNS server. Select the + symbol to add more DNS servers.

DNS Forwarding

Cache Size	By setting the cache size, this allows the router to store frequently used resolved DNS queries. This allows clients to resolve DNS queries locally rather then remotely from a global DNS server. DNS server 0–10000 Default is 10000
Seconds to Cache NVDOMAIN entries	Cache “Name Error" entries for specified seconds. Also know as Negative caching. It can be useful to reduce the response time for negative answers. It also reduces the number of messages that have to be sent between resolvers and name servers hence overall network performance. Range is 0–7200 Default is 3600 seconds
Ignore IP Host Tables	Do not check the IP host table for host resolution.
Use DNS Servers received from DHCP servers for the following interfaces	Select the interfaces that meets this criteria.

DNS Listeners

IPv4 address	Enter an IPv4 address to listen for DNS requests.

DNS Domain Forwarding

Domain	This server receives domain requests.
IPv4/IPv6 Address	Forward domain request to this server. Select the + symbol to add more.

Dynamic DNS

Host Groups (Add, Edit or Delete)	Configure a Group name.
Add Hostname/IP entries	Add hosts to be added to this group. Select the + symbol to add more.
Add DDNS to interface	
Interface	Select from the drop-down list, the interface to add DDNS functionality.
Web Check to obtain external IP	This field should be left blank.
Service used for Dynamic DNS	
Service	Set to DynDNS.
Login	Specify a username to use for logging into the DynDNS Host server.
Password	Specify a password to use for logging into the DynDNS host server.
Registered DNS service	Specify whether you are providing a host name or a host group name.
Host name or Host group name	Specify either a host name or a host group name.

IP Host Tables

The Host table contains the list of hosts to be accessed by an IP address or Fully Qualified Domain Name (FQDN) from the router. This local database contains a symbolic names for the hosts as well as its IP address or FQDN configured by you. When a host entry is required elsewhere in the configuration, this symbolic name is used. The local Host Table provides the same function of converting a name to an IP address to that of using an external DNS server but uses a local database manually configured by you on the router.

Overview

Add host to IP address relationships.

Feature details / Application notes

IP addresses can be configured manually or via an external DHCP server.

IP Host Tables

Hostname (Add)	**Enter a hostname.**
Add IPv4/IPv6 Address	**Add the IPv4 or IPv6 address.**

routerWAN

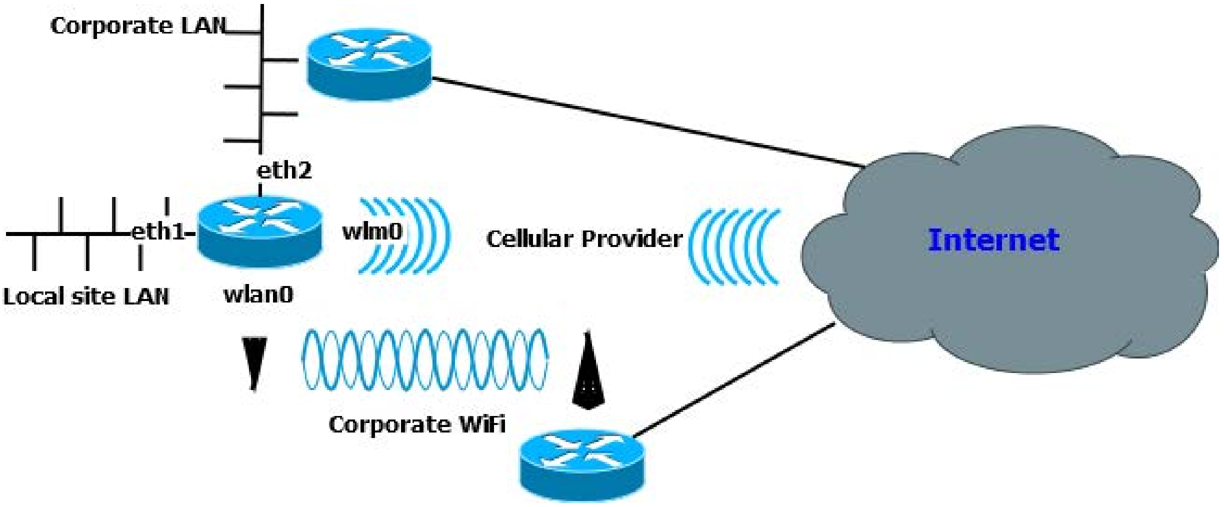
Overview

Your router has the ability to determine the health status of its interfaces. By configuring ping and traceroute tests, you can determine whether an interface can send and receive data, if the interface fails, then a backup action can be taken.**High Availability example**

Health Profiles	
Profile (Add, Edit, delete)	
Name	**Enter a profile name.**
Mark as failed after	**Specify the number of failed tests.** **Value is 1–10** **Default is 1** **If more than one test is defined, the failure count applies to EACH test.**
Mark as active after	**Specify the number of successful tests.** **Value is 1–10** **Default is 1**
Tests (Add, Edit, Delete)	
Test priority	**Enter a numerical value for the priority for this test. Tests are (order dependent with 1 being first test to run and 100 being the last).**
Target	**Enter a target IPv4 address or hostname.**
Type	**Select the type of test to run.** • **ping** • **traceroute**
Response	**Select the response timeout between pings.**

Test Limit	Enter a numerical value from 1–254

configuration



The above diagram shows an example of where a customer wants all his local site LAN traffic on eth1 to by default over his Corporate LAN on eth2, but if that fails, they want all the traffic to go through the Corporate WiFi on wlan0 and if that fails go through the Cellular connection on wlm0 in that order of priority. This means that if both eth2 and wlan0 network connections comes back up it would switch back to the corporate LAN eth2.
Before configuring the WAN high availability fail-over feature, all 3 network connection need to configured and tested first by bringing them up 1 at a time and being sure you can ping a public IP address line "ping www.google.com"

In this example the eth2's IP address is statically configured, so the following two static configurations are required so that unknown addresses are routed through the eth2. Also note the administrative distance for the static route needs to match the other 2 WAN interfaces, in this case 210.

Using the WebManager configure,

Under Interfaces/Add/Edit, the following interfaces.
Eth1
Description – Local site LAN
IPv4 address 172.16.23.9 255.255.0.0

Eth2
Description – Corporate LAN
DHCP

wlm0

Enable

wlan0
Mode – client
SSID Profile – select default SSID of router (example: IRG5521+/2200)
DHCP

Under General Routing/Static route
Add static route
Destination Prefix 0.0.0.0
Destination Prefix Netmask 0.0.0.0
Route via forwarding
Router Address 192.168.23.1
Administrative Distance 210

Under Network/WAN/Health Profiles
Add Health profile testfailover
Mark as failed after 3
Mark as active after 3
Add Tests
Target 8.8.8.8
Type ping
Response is timeout

Under Network/WAN
High Availability
Mode Failover
Source interface eth1
Add WAN interface
Eth2 priority 40
wlan0 priority 30
wlm0 priority 20

Under WAN
Interface IP Health/Add
eth2
Profile testfailover
Nexthop IP
IP address 192.168.23.1
wlan0
Profile testfailover
Nexthop IP
ip address 192.168.0.1
wlm0
Profile testfailover

Nexthop DHCP

Under Routing/NAT/ALG
NAT rules /Add
ACL 1
Global Address
Interface eth2
ACL 2
Global Address
Interface wlan0
ACL 3
Global Interface
Interface wlm0

Under Network/DNS/Add
ip address 8.8.8.8

Under Routing/Access Control List/Add
standard list 1 permit any
standard list 2 permit any
standard list 3 permit any

To verify the connections, select Command line in the left navigation panel.
At the command prompt type the following commands.

```
PerleRouter#show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [210/0] via 192.168.0.1, wlan0
  *                   via 192.168.23.1, eth2
  *                   via 10.19.136.213, wlm0
C>* 10.19.136.208/29 is directly connected, wlm0
C>* 127.0.0.0/8 is directly connected, lo
C>* 172.16.0.0/16 is directly connected, eth1
C>* 192.168.0.0/24 is directly connected, wlan0
C>* 192.168.23.0/24 is directly connected, eth2
```

Show wan failover with all network connections up

```
WAN Failover Source Interfaces:
======================================
  eth1

WAN Failover Interfaces:
=============================
  eth2        Priority: 40
  wlan0       Priority: 30
  wlm0        Priority: 20
WAN Failover Primary Active Interface:
=========================================
  eth2

WAN Load Failover Interfaces Health Status:
==============================================
Interface:  eth2
  Status:  active
  Last Status Change:  Mon Mar  2 09:52:46 2020
  +Test:  ping Target: 8.8.8.8
    Last Interface Success:  0s
    Last Interface Failure:  1m7s
    # Interface Failure(s):  0

Interface:  wlan0
  Status:  active
  Last Status Change:  Mon Mar  2 09:53:11 2020
  +Test:  ping Target: 8.8.8.8
    Last Interface Success:  0s
    Last Interface Failure:  43s
    # Interface Failure(s):  0

Interface:  wlm0
  Status:  active
  Last Status Change:  Mon Mar  2 09:52:55 2020
  +Test:  ping Target: 8.8.8.8
    Last Interface Success:  0s
    Last Interface Failure:  57s
    # Interface Failure(s):  0

Show wan failover with eth2 network connections down
WAN Failover Source Interfaces:
=================================
  eth1

WAN Failover Interfaces:
==========================
  eth2        Priority: 40
  wlan0       Priority: 30
  wlm0        Priority: 20

WAN Failover Primary Active Interface:
=========================================
  wlan0

WAN Load Failover Interfaces Health Status:
================================================
Interface:  eth2
  Status:  failed
  Last Status Change:  Mon Mar  2 09:54:53 2020
  -Test:  ping Target: 8.8.8.8
    Last Interface Success:  1m8s
    Last Interface Failure:  0s
    # Interface Failure(s):  6

Interface:  wlan0
  Status:  active
  Last Status Change:  Mon Mar  2 09:53:11 2020
  +Test:  ping Target: 8.8.8.8
    Last Interface Success:  0s
    Last Interface Failure:  2m32s
    # Interface Failure(s):  0

Interface:  wlm0
  Status:  active
  Last Status Change:  Mon Mar  2 09:52:55 2020
  +Test:  ping Target: 8.8.8.8
    Last Interface Success:  0s
    Last Interface Failure:  45s
    # Interface Failure(s):  0
```

Show wan failover with eth2 and wlan0 network connections down

```
WAN Failover Source Interfaces:
===================================
  eth1

WAN Failover Interfaces:
===========================
  eth2       Priority: 40
  wlan0       Priority: 30
  wlm0        Priority: 20

WAN Failover Primary Active Interface:
==========================================
  wlm0

WAN Load Failover Interfaces Health Status:
================================================
Interface:  eth2
```

```
  Status:  failed
  Last Status Change:  Mon Mar  2 09:54:53 2020
  -Test:  ping Target: 8.8.8.8
    Last Interface Success:  3m45s
    Last Interface Failure:  0s
    # Interface Failure(s):  20

Interface:  wlan0
Status:  failed

  Last Status Change:  Mon Mar  2 09:57:19 2020

  -Test:  ping Target: 8.8.8.8

    Last Interface Success:  1m18s

    Last Interface Failure:  0s

    # Interface Failure(s):  7

Interface:  wlm0
  Status:  active
  Last Status Change:  Mon Mar  2 09:52:55 2020
  +Test:  ping Target: 8.8.8.8
    Last Interface Success:  0s
    Last Interface Failure:  3m22s
    # Interface Failure(s):  0
```

Show wan failover with eth2 network connection back up but wlan0 network connections still down

```
WAN Failover Source Interfaces:
================================
  eth1

WAN Failover Interfaces:
========================
  eth2        Priority: 40
  wlan0       Priority: 30
  wlm0        Priority: 20
WAN Failover Primary Active Interface:
======================================
  eth2

WAN Load Failover Interfaces Health Status:
===========================================
Interface:  eth2
  Status:  active
  Last Status Change:  Mon Mar  2 10:00:06 2020
  +Test:  ping Target: 8.8.8.8
    Last Interface Success:  1s
    Last Interface Failure:  34s
    # Interface Failure(s):  0

Interface:  wlan0
  Status:  failed
  Last Status Change:  Mon Mar  2 09:57:19 2020
  -Test:  ping Target: 8.8.8.8
    Last Interface Success:  3m21s
    Last Interface Failure:  1s
    # Interface Failure(s):  18

Interface:  wlm0
  Status:  active
  Last Status Change:  Mon Mar  2 09:52:55 2020
  +Test:  ping Target: 8.8.8.8
    Last Interface Success:  1s
    Last Interface Failure:  5m25s
    # Interface Failure(s):  0
```

ARP Management

Overview

The ARP table holds information on the association between IP addresses and MAC addresses. This table is maintained by the management software and is used strictly for management functions. It is used for mapping a network address (e.g. IPv4 address) to a physical address which in the case of Ethernet is call a MAC address.

Age-out

- Entries have an age-out timeout associated with them. This is the length of time the entry is maintained in the ARP table. This time is refreshed whenever a message is received from the IP address matching an entry in the table.

Feature details / Application notes

The ARP table can consist of "static" and "dynamic" entries.

- Static entries are configured by you
- Dynamic entries are learned by the software

Dynamic entries age out if we have not seen a message from that device in the time specified by the ARP timeout parameter. Static entries do not timeout.

Configuring an ARP entry in the *router*IOLAN prevents the software from "arping" for a hostname or IP address.

Terminology

ARP—Address Resolution Protocol

ARP is used for mapping a network address (e.g. IPv4 address) to a physical address which in the case of Ethernet is call a MAC address.

Age-out

- Entries have an age-out timeout associated with them. This is the length of time the entry is maintained in the ARP table. This time is refreshed whenever a message is received from the IP address matching an entry in the table.

Feature details / Application notes

The ARP table can consist of "static" and "dynamic" entries.

- Static entries are ones configured by you
- Dynamic entries are learned by the software

Dynamic entries age out if no messages from that device in the time specified by the ARP timeout parameter. Static entries do not timeout. Configuring an ARP entry in the routerIOLAN prevents the software from "arp'ing" for a hostname or IP address.

Static ARP	
IPv4 address	**Enter the IPv4 address you want to add to the ARP table as a static entry.**
MAC address	**Enter an MAC address associated with the IPv4 address.**
Interface	**Select the interface that this ARP entry to be associated with.**

ARP Timeout	
ARP Timeout	**If an ARP entry is not used for a specific amount of time the entry is removed from the caching table.**
Disable ARP filter	**If enabled the router responds to the same ARP requests coming from multiple interfaces.**
Enable ARP Accept	**Define the behavior for gratuitous ARP frames who's IP is not already present in the ARP table:** • **0—don't create new entries in the ARP table** • **1—create new entries in the ARP table**
Enable ARP Announce	**Define different restriction levels for announcing the local source IP address from IP packets in ARP requests sent on interface** • **0—(default) Use any local address, configured on any interface** • **1—Try to avoid local addresses that are not in the target's subnet for this interface.**

Enable ARP Ignore	Enable arp-ignore on this interface • 0 (default): reply for any local target IP address, configured on any interface • 1 reply only if the target IP address is local address configured on the incoming interface
Enable Proxy ARP	Enable Proxy ARP if you need your router to respond to local networks with its MAC address. Default is Disabled

Interface IP Health

Interface	Select the interface that you want to add a health profile to.
Profile	Select the pre-defined profile from the drop-down list. Defining a source interface/originating traffic will be included in the dynamic WAN high-availability feature failover feature.
NextHop	Select: • IP • DHCP
IP Address	The IP address of the next hop.
Priority (good status)	VRRP priority when IP health is good. 1-255
Priority (bad status)	VRRP priority when IP health is bad. 1-255

High Availability

Mode	Select: • Disable • Failover • Load Sharing
Failover	
Source Interface	
Interface	Configure a source interface.

WAN Interface	
Add WAN Interface	Select the interface from the drop-down list.
Priority	Specify the priority for load-sharing. Values are 1–255
Failover	Failover is defined as a mode where 2 or more WAN interfaces are configured, but only 1 interface is active at a time. Once IP HEALTH has detected that a WAN interface no longer has Internet connectivity, it "failovers" to the next active (via IP HEALTH status) WAN interface.
Load Sharing	Load Sharing is defined as a mode where you define how routed traffic can be sent over one or more defined active WAN interfaces. Unlike failover, mode where ALL routed traffic is cut over to the next highest priority active WAN interface, this mode defines how specific or all traffic is to be shared/divided over multiple active WAN interfaces. Each load-sharing rule allows the user to define: • a SINGLE source interface • MULTIPLE WAN interfaces (each with a weighting value that determines percentage output relative to all WAN interfaces).
Enable flushing connections on WAN interface outage	If WAN interface goes down, flush connections. Default is enabled
Include local traffic	Include all local traffic in the rule. Default is enabled
Enable source address translation on this rule	Apply any source NAT to this rule. Default is disabled
Enable inbound connection tracking	Track inbound connections. Default is enabled
Rules	
Rule Number	Supply a rule number.

Description	Description of this rule.
Enable excluding of matching rules load sharing	Check for rule matching.
Enable per-packet load-sharing	Enable Load-sharing based at packet level.
Source interface	Select interface from the drop-down list.
Add WAN interface	
Interface	Select an interface from the drop-down list.
Weight	Configure a weight value. Example of weighting value on each WAN interface: Wan interface 1's weighting = 10, results in 10/ (10+20+40) = 1/7 output of this rule Wan interface 3's weighting = 40, results in 40/(10+20+40) = 4/7 output of this rule optional source packet matching rules based on protocol, source/destination IP, port, etc. Note: Load sharing requires at least one valid rule to enable it.
Enable matching protocol	Select the protocol to match.
Match	Select to match all protocols.
Match all except Protocol	Select the protocols not to match. • ah, dccp, dsr, egp, eigp, encap, esp, etherip, ggp, gre, hmp, icmp, idrc, igmp, igp, ip, ipip, ipv6, ipv6-frag, ipv6-icmp, ipv6-nonxt

Match all except Protocol	• ipv6-opts, ipv6-route, isis, l2tp, manet, mpls-in-ip, narp, ospf, pim, rdp, roch, rsvp, sctp, sdrp, shim6, skip, tcp, udp, udplite, vrrp, xns-idp • protocol number <1-255>
Limit	
Burst	Configure the number of packets that match the criteria allowed out the WAN interface based on the rate calculation window. Values are 0-4294967295 packets
Rate calculation window	Select calculate the rate as: • hour • minute • second
Rate	Number of packets that match the criteria allowed out the WAN interface based on number of packets. Values are 0-4294967295 packets
Threshold behavior for limit	Configure to apply the threshold limit behavior: • Above • Below

Network Watchdog

Overview

The network watchdog feature monitors the health status of your modem or router. The watchdog feature runs continuous ping tests. Each ping test is comprised of one or more ping attempts. If all of the ping's in a test fail, the test failed, if one ping test passes, the test is considered to have passed.
The watchdog feature only gets triggered once there is a successful connection which is defined as one successful ping. At that point it begins running the tests as configure. Should any of the ping tests fail, the router and modem can be set to notify you, or reset or both.

Feature details / Application notes

Once the maximum number of consecutive failed tests occurs the router will:

1. Start a 2 minute countdown timerto reset the modem or to re-boot therouter .
2. A message is displayed in the WebManager notifying you the watchdog timer is activated due to failed tests.
3. When you get this message it allows you to cancel the reboot within this 2 minute interval timer.

4. If the 2 minute interval timer expires without your intervention, the reset/reboot occurs.

After the reset, or reboot, the watchdog feature begins to monitor the connection and modem for health status again.

Network Watchdog	
Enable	Enable or disable the Network Watchdog feature.
Fail Action	Fail-action • notify only • notify and reboot
Ping	Ping count for each test. Values are 1–10
Interval	Time interval between tests. Values are 1–180 in minutes
Response	Ping response timeout. Timeout 1–3600 in seconds
Threshold	Consecutive failed tests count to trigger reset.
Target	Test the target host IP, IPv6 or name.
Interface	Interface for ping test. BVI (1-9999) Cellular (0–0) Dialer (0–15) Dot11Radio (0–4) Ethernet (1–5) OpenVPN-Tunnel (0–999) Tunnel (0–999)

Modem Watchdog	
Enable	Enable or disable the Modem Watchdog feature.
Fail Action	Specify what the router does on failure. • notify only • notify and reset

Ping	Ping count for each test. Values are 1 - 10
Interval	Time interval between tests. Values are 1 - 180 in minutes
Response	Ping response timeout. Timeout 1- 3600 in seconds
Threshold	Consecutive failed tests count to trigger reset.
Target	Test the target host IP or name.
Interface	Interface for ping test. BVI (1-9999) Cellular (0-0) Dialer (0–15) Dot11Radio (0–4) Ethernet (1–5) OpenVPN-Tunnel (0–999) Tunnel (0–999)

Cellular Profiles	
Cellular profile name	Provide a description for this interface. Name can be up to 32 characters long. Maximum profiles is 16.
SIM slot	Depending on the model. 1 or 2 Default is 1
Radio technology	• Auto • LTE (4G) • UMTS (3G)

Roaming allowed	Allow roaming on the cellular network. Select enabled to allow your router to roam outside of your provider’s coverage area. If your router moves outside of your provider’s coverage and registers on a new LTE network: • The router’s LTE connection stays disconnect until the re-enters the provider’ coverage area. • If LTE Failover is configured, then failover to the alternate profile may occur. If disconnected due to roaming the routermay stay registered to the network which means that SMS may be possible and charges may occur.
Enable Carrier Aggregation	Enabled to acquire successively higher peak data rates as well as better broadband experience across the coverage area. Default is enabled
Modem firmware	Select the modem firmware. • SIM-Based • Generic • ATT • Verizon • Specific Other • Carrier name
Cellular bands	Select the cellular band. (Depending on the firmware version or model) • auto • 1 • 3 • 4 • 5 • 7 • 8 • 12 • 14 • 13 • 17 • 18 • 19 • 25 • 26 Public Safety • 28 Public Safety • 29 • 30 • 32 • 34 • 38 • 39 • 40 • 41 • 42 CBRS • 46 • 66 • 71

PIN	Maximum 4–8 digits either encrypted or unencrypted.
APN	Maximum of 16 cellular profiles can be created.
Use default APN	Enabled by default.
Advanced	
Data APN Settings	Specific the APN to use for this connection.
APN	
PDP type	Specific the PDP type. • IPv4 • IPv6 • IPv4/IPv6 Default is IPv4
Context identifier	Range 1–16 Default is 1 Note: This is an internal slot number not the SIM slot.
Authentication Type	Specific the authentication type. • None • CHAP • PAP
Username	Specific the username for authentication.
Password	Specific the password for the username.
Mobile Data Monitor	
Monthly Data Limit (MB)	Specific the maximum data limit. Maximum is 100,000
Billing Day	Specific the number of billing days. 1–31 (days in the month)
Alert at (% used)	Specific the percentage on when to send the alert. 0–99%—send an alert/trap when percentage is reached

Alert when data limit is reached	**Specific the alert to send when data limit is reached.** • **None** • **Disconnect LTE** **Default is None**

Routing

This section describes how to configure routing features on your router. Some configuration parameters may be different on some models or running software.

Default Gateway

The default gateway specifies the IP address of a node to which traffic should be sent if the routing engine does not know which interface to use to reach a given IP address. This can be manually configured by the user or automatically setup via protocols such as DHCP.

Static Routing

Static routing occurs when you manually configure a routing entry in the routing table, rather than information collected from dynamic routing traffic.
Use Static routing to:

- define an exit point from the router when no other routes are available or necessary. This is called a default route.
- define static routes for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- as a complement to dynamic routing to provide a failsafe backup in the event that a dynamic route is unavailable.
- help transfer routing information from one routing protocol to another (routing redistribution).

Restrictions / Limitations

Static routing is not fault tolerant. This means when there is a change in the network or a failure occurs between two statically defined devices, traffic is not re-routed. As a result, the network is unusable until the failure is repaired or the static route is manually reconfigured by an administrator. One important fact to remember is the router on the other side (destination) must have a route back to the source. If it is not aware of the source network there will never be a response. Just like if you don't put a return address on an envelope

Terminology

Dynamic Routes—Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes.

Your router supports these networking routing techniques.
RIP—See ***RIP*** for more information
BGP—See ***BGP*** for more information
OSPF—See ***OSPF*** for more information

Static Routing	
Static Routing (Add, Edit, Delete)	
Destination prefix	The prefix for the destination network.
Destination prefix mask	The prefix mask for the destination network.
Route	
Route via:	The interface the traffic is to leave by: • Gateway—The IP address of the forwarding router • Interface—The interface to use for this route • Null—Select null to discard IP packets (used to prevent routing loops from occurring in your network)
Default Gateway for Interface obtained by DHCP	Enable if you want this interface to obtain default gateway though DHCP.
Administrative Distance	Enter an Administrative Distance. (AD) is a value that your router uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too 1. The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown
IPv6	
Enable IPv6 Unicast Routing	Enable unicast routing if your router needs to route IPV6 traffic AND to participate in IPv6 IGPs (Interior Gateway Protocols).
IPv6 Static Routing (Add, Edit, Delete)	
Destination prefix	The prefix for the destination network.

Destination prefix mask	The prefix mask for the destination network. Value is 0–128
Route	
Route via:	The interface the traffic is to leave by: • Gateway—The IP address of the forwarding router • Interface—The interface to use for this route • Null—Select null to discard IP packets (used to prevent routing loops from occurring in your network)
Administrative Distance	Enter an Administrative Distance. (AD) is a value that your router uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too 1. The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown

NAT/ALG

Network Address Translation (NAT) allows a network device—usually a firewall—to assign a public address to a computer (or group of computers) inside a private network. NAT helps limit the number of public IP addresses an organization or company uses for economic and security purposes.

To configure NAT, you make at least one interface on the router—NAT outside and another interface on the router—NAT inside.

Port Forwarding

Port forwarding or port mapping redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

Port forwarding is an excellent way to preserve public IP addresses. It protects servers and clients from unwanted access. It "hides" the services and servers available on a network, and limits access to and from a network. Port forwarding is transparent to the end user and adds an extra layer of security to networks.Your IOLAN supports ninety-nine port forwarding rules.

NAT
Destination NAT Port Forwarding

Protocol	• TCP • UDP • TCP+UDP
Inbound interface	Select the inbound interface from the drop down list.
Inbound interface global port	Enter inbound interface global port number. Values are 1-65535
Destination address	Enter destination IPv4 address.
Destination address local port	Enter destination address local port number. Values are 1-65535
Destination NAT IP Forwarding	
Mapping type	• 1-to-1 • 1-to-multiple / multiple-to-1
Inbound interface	Select the inbound interface from the drop-down list.
Inside/Local IP address	Enter the IP address to use as the inside or local address.
Outside/Global address	Enter the IP address to use as the outside or global address.
Source NAT Forwarding	
ACL	Select the access control list (ACL) to use from the drop-down list.
Global address	• Interface • Pool
Interface	Select the interface to use from the drop-down list.
Do not turn on firewall to drop invalid connections	Enable or disable. Default is disabled
Source NAT Forwarding (Add, Edit, Delete)	

Add NAT Pool	
Pool name	Configure the name for this pool.
Start IP Address	Configure the start address of this pool.
End Address	Configure the end address of this pool.
Netmask	Configure netmask for this pool.
Add Nat66 Rules	
Inside Prefix	Configure the inside prefix for this rule.
Inside Prefix Length	Configure a prefix length. Value is 0–128
Outside Prefix	• Prefix • Any
Outside Prefix Length	Configure the prefix length. Values are 0-128
Outside Interface	Select the outside interface from the drop-down list for this rule.
Do not turn on firewall to drop invalid connections	By default connections are not dropped by the firewall.

ALG	
Enable certain protocols to transverse NAT and Firewalls. Some protocols may not be available on some firmware versions.	
Select the protocols to enable	By default all protocols are enabled, to disable uncheck the check-box • ftp, gre, h323, nfs, pptp, sip, sqlnet, tftp

Access Control Lists (ACLs)

Access Control Lists (ACLs) control the traffic entering your network. They control the access to and denial of services. On network devices such as routers and firewalls, they act as filters for network traffic, packet storms, services, and host access. Configured

ACLs provide security for your network as well as controls network traffic based on the TCP port number.

Uses for access lists

- Limits network traffic to increase network performance.
- ACLs provides traffic flow control by restricting the delivery of routing updates.
- It can be used as additional security.
- Controls which type of traffic are forwarded or blocked by the router.
- Ability to control which areas a client access.

Terminology

Standard access-list

Standard access lists create filters based on source addresses and are used for server-based filtering. Address-based access lists distinguish routes on a network you want to control by using network address number (IP).

Extended access lists

Extended access lists create filters based on source addresses, destination addresses, protocol, port number and other features and are used for packet-based filtering for packets that traverse the network.

Feature details / Application notes

The list is processed from the top down. As soon as a match is found on the IP address attempting access, the processing of the list stops and the corresponding allow or deny is applied. If the list is fully processed and no match is found for the IP address in question, access will be denied.

Access Control Lists	
ACL Type	**Specify the type of ACL.** • **Standard** • **Extended**
ACL number	**Enter an ACL number for this entry.** • **Standard range is 1-99** • **Extended range is 1300-1999**
Sequence number	**Specify the sequence number. Entries will be read from lowest to highest. It is best practice to leave gaps between sequence numbers such as 10, 20, 30, so that further entries can be inserted.**
Action	**Permit or denies the IP packet from the specified source (host/address)** • **Permit** • **Deny**

Source Type	**Specify the source type for matching** • **Any** • **Host** • **Wildcard**
Source hostname/ address	**IPv4 address or hostname**
IPV6 Access Control Lists	
ACL Number	**Enter an ACL number for this entry.** • **Standard range is 1-99** • **Extended range is 1300-1999**
Sequence number	**Specify the sequence number. Entries will be read from lowest to highest. It is best practice to leave gaps between sequence numbers such as 10, 20, 30, so that further entries can be inserted.**
Action	**Permit or denies the IP packet from the specified source (host/address)** • **Permit** • **Deny**
Source Type	**Specify the source type for matching** • **Any** • **Prefix**
IPv6 Prefix	**Specify an IPv6 prefix**
Prefix Length	**Specify a prefix length**
Exact Match	**Match exactly on the prefix**

Prefix List

Prefix-list is mainly used to filter the routes – not user traffic. Therefore it is used in routing protocols only.The main difference in access-list and prefix-list is that access-list only matches the bits specified by a wildcard mask but prefix-list can also match sub-net mask and you can specify a range of subnet masks which need to be matched to be permitted or denied.

Prefix lists work very similarly to access lists; a prefix list contains one or more ordered entries which are processed sequentially. As with access lists, the evaluation of a prefix against a prefix list ends as soon as a match is found.

Feature details / Application notes

Two keywords can be optionally appended to a prefix list entry: minimum prefix length (less than or equal to) and maximum prefix length (greater than or equal to). Without either, an entry will match an exact prefix.

Prefix-List	
Name	Name of this prefix list.
Description	Description of this prefix list.
Sequence number	Specifies the number to order entries in the prefix list. Entries will be read from lowest to highest. It is best practice to leave gaps between sequence numbers such as 10, 20, 30, so that further entries can be inserted between numbers. Range is 1-65535
Action	• Permit—Allows routes or IP packets that match the prefix list • Deny—Rejects routes or IP packets that match the prefix list.
Prefix	Specify a IPv4 prefix.
Mask	Specify a subnet mask.
Minimum Prefix length	Specify minimum prefix length (less than or equal to). Range is 1–32
Maximum Prefix length	Specify maximum prefix length (less than or equal to). Range is 1–32
Prefix IPv6	
Name	Name of this prefix list.
Description	Description of this prefix list.
Sequence number	Specifies the number to order entries in the prefix list. Entries will be read from lowest to highest. It is best practice to leave gaps between sequence numbers such as 10, 20, 30, so that further entries can be inserted between numbers. Range is 1-65535

Action	• Permit—Allows routes or IP packets that match the prefix list • Deny—Rejects routes or IP packets that match the prefix list.
Prefix	Specify a IPv6 prefix.
Prefix length	Specify a subnet mask.
Minimum Prefix length	Specify minimum prefix length (less than or equal to). Range is 1–32
Maximum Prefix length	Specify maximum prefix length (less than or equal to). Range is 1–32

Route Maps

Route maps provide a way for your router to evaluate optimum routes for forwarding packets or suppressing the routing of packets to particular destinations.

Compared to access lists, route maps support enhanced packet-matching criteria. In addition, route maps can be configured to permit or deny the addition of routes to the routing table and make changes to routing information dynamically as defined through route-map rules.The router compares the rules in a route map to the attributes of a route. The rules are examined in ascending order until one or more of the rules in the route map are found to match one or more of the route

Feature details / Application notes

- When a single matching match-* rule is found, changes to the routing
- information are made as defined through the configured rules.
- If no matching rule is found, no changes are made to the routing information.
- When more than one match-* rule is defined, all of the defined match-* rules must evaluate to TRUE or the routing information is not changed.
- If no match-* rules are defined, the router makes changes to the routing information only when all of the default match-* rules happen to match the attributes of the route.

Route Maps	
Route Maps (Add, Edit, Delete)	
Name	Specify a name for this route map rule.

Rule Number	Specify a rule number. Entries will be read from lowest to highest. It is best practice to leave gaps between rule numbers such as 10, 20, 30, so that further entries can be inserted between rule numbers. Range is 1–65535.
Description	Enter a description for this rule.
Set Operation	Set the operation mode on whether this rule is an Permit (accept) rule or a Deny (reject rule) • Permit • Deny
Match Values from Routing Table Add Traffic Match	
Select Matching Criteria	• AS Path, BGP Community List, BGP/VPN Extended, Community List, IP Address route, Next-hop address of route, IP source route, IPv6 address, IPv6 next hop, Metric of Route, BGP Origin Code, Tag of Route, Interface, Peer address
Set Values in Destination Routing Protocol Set Attribute	
Select Set Criteria	• BGP Aggregator, Transform BGP AS-Path, BGP, Atomic Aggregate, Delete BGP community list, BGP Community, BGP Extended Community, IP (next hop), IPv6 (next hop), BGP Local Preference, Metric, Metric Type, BGP Origin Code, BGP, Originator ID, Source Address for Route, Tag of route, BGP Weight
Jump to another Route-map after match+set	
Route Map	Specify the route map to jump to after match.
Continue to a different entry within the route-map	Select a rule from the drop-down list.
Rule List	Select a rule from the drop-down list.
Exit policy on matches	What action to take when rule matches. • none • Next • Goto

Community List (Add, Edit, Delete)	By using the BGP communities attribute, BGP speakers with common routing policies can implement inbound or outbound route filters based on the community tag, rather than consult long lists of individual permit or deny statements. A communities attribute can contain multiple communities. A BGP community list is used to create groups of communities to use in a match clause of a route map.
Community List Type	Select the type of list: • Standard • Expanded
Community List Sequence number	Configure a sequence number. Entries will be read from lowest to highest. It is best practice to leave gaps between sequence numbers such as 10, 20, 30, so that further entries can be inserted between them. Range is 1–65535
Community List Rules	
Sequence number	Specify a sequence number. Entries will be read from lowest to highest. It is best practice to leave gaps between rule numbers such as 10, 20, 30, so that further entries can be inserted between rule numbers. Range is 1–65535.
Action	What action will be taken with this route. • Permit • Deny
Community	Select how the BGP routes will the advertised to the community • internet—advertise this route to the Internet community; by default, all prefixes are members of the Internet community • local-AS—routes are advertised to only peers that are part of the local autonomous system • no-advertise—do not advertise this to any other routers • no-export—do not advertise to external neighbors, but it is ok to advertise to internal neighbors.

Ext-Community List (Add, Edit, Delete)	By using the BGP communities attribute, BGP speakers with common routing policies can implement inbound or outbound route filters based on the community tag, rather than consult long lists of individual permit or deny statements. A communities attribute can contain multiple communities. A BGP community list is used to create groups of communities to use in a match clause of a route map.
Community List Type	Select the type of list. • Standard • Expanded
Community List Sequence number	Specify a sequence number. Entries will be read from lowest to highest. It is best practice to leave gaps between sequence numbers such as 10, 20, 30, so that further entries can be inserted between sequence numbers. Range is 1–65535
Action	Action to take with this route. • Permit • Deny
Type	Select how the BGP routes will the advertised to the community Route Target • VPN Extended Community (ASN.nn) Site of Origin • VPN Extended Community (ASN.nn) An autonomous system number (ASN) is a unique number that's available globally to identify an autonomous system and which enables that system to exchange exterior routing information with other neighboring autonomous systems. The number of autonomous system numbers is limited. Your service provider will assign you the first three digit for ASN, the last two digits should be unique. The number of autonomous system numbers is limited. Your service provider will assign you the first three digit for ASN, the last two digits should be unique

AS-Paths

The AS path is one of the BGP attributes, it’s a well-known mandatory attribute which means that it’s included with all prefixes that are advertised through BGP.

When a BGP router advertises a prefix, it will include its own AS number to the left of the AS path attribute. The AS path allows us to see through which autonomous systems we have to travel to get to a certain destination and is also used in BGP for loop prevention. When the router sees its own AS number in the AS path, it will not accept the prefix.

AS-Paths	
Name	**Configure an AS-path name.**
Sequence number	**Specifies the number to order entries. Entries will be read from lowest to highest. It is best practice to leave gaps between rule numbers such as 10, 20, 30, so that further entries can be inserted between them.** **Range is 1 to 65535**
Action	**Action to take when rule matches.** • **Permit** • **Deny**
Regular Expression	**Enter a text string.**

Policy Routing

Policy-based routing overrules your routing table and changes the next hop IP address for traffic meeting your configured specifications.

By default, the router forwards packets based on the main routing table. Policy-based routing allows you to create a Route Policy to match packets and have them use a separate route policy to forward the packets. Policy-based routing allows you to apply policies based on source IPv4 address, source MAC-address, destination IPv4 address, protocol, fragment, IPSEC, recent and state. The resulting actions can include dropping matched packets or assigning packets to a static routing table.

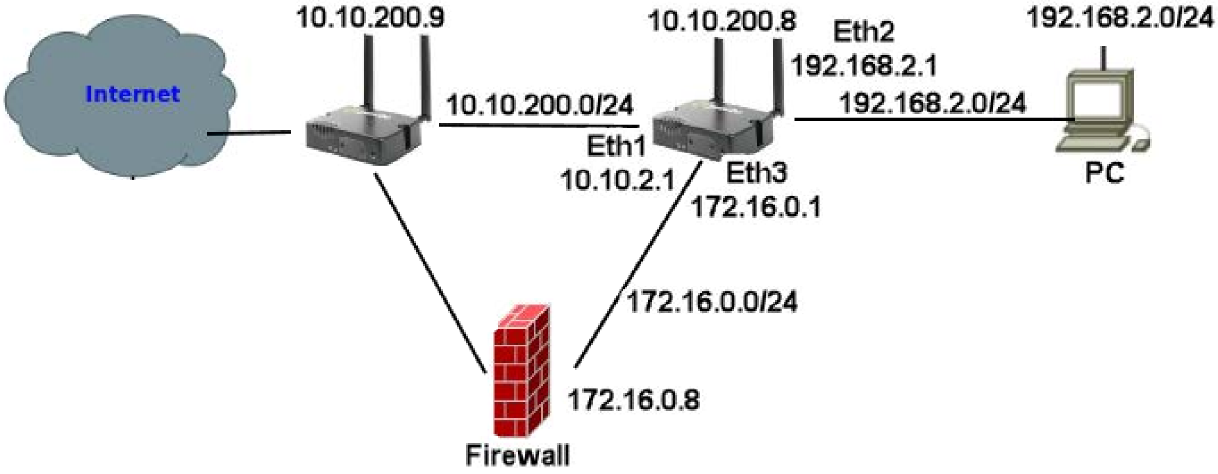
Policy Routing	
Policy Routes—Add, Edit, Delete	
Name	**Name of this policy.**
Description	**Configure a description for this policy.**
Rule Number	**Configure a rule number.** **Range is 1–9999**
Enable	**Enable or disable this policy.**

Log packeting matching this rule	Log the packets that match this rule.
Traffic Match	
Select Matching Criteria	• Source IPv4-address • Source MAC address • Source port (TCP/UPD) • Destination IPv4-address • Destination port (TCP/UDP) • Protocol • Fragment • IPsec • Recent • State
Policy Action	• Drop matched packets • Route
Assign to routing table (default static)	Matching packets should be assigned to this default routing table.
Schedule	• Use UTC • Enable Schedule Select Schedule Type • Date • Weekdays • Days of Month
Interface Policy—Add, Edit, Delete	
Interface	Select interface.
Policy	Add policy to this interface.
Policyv6 Routes—Add, Edit, Delete	
Name	Name of this policy.
Description	Configure a description for this policy.
Rule Number	Configure a rule number. Range is 1–9999

Enable	Enable or disable this policy.
Log packeting matching this rule	Log the packets that match this rule.
Traffic Match	
Select Matching Criteria	• Source IPv6-address • Source MAC address • Source port (TCP/UPD) • Destination IPv6-address • Destination port (TCP/UDP) • Protocol • Fragment • IPsec • Recent • State
Policy Action	• Drop matched packets • Route
Assign to routing table (default static)	Matching packets should be assigned to this default routing table.
Schedule	• Use UTC • Enable Schedule Select Schedule Type • Date • Weekdays • Days of Month
Interface-Policyv6	
Select interface	Add policy to this interface.
Policy	Select policy name.

Example

This example uses policy-based routing to route all HTTP traffic protocol TCP, destination port 80 through a route policy named http-firewall.



1. Create a static route as ip route 0.0.0.0 0.0.0.0 10.10.200.9
   Create a route table entry (2) as 0.0.0.0 0.0.0.0 172.16.0.8
   Create a route policy named http-firewall, under this create a rule (2)
2. Create a traffic match for criteria matching protocol tcp and destination port 80 >
3. Under interfaces assign an IP address of 192.168.2.1 255.255.255.0 to interface Ethernet 2.
4. Under Routing/Routing Policy/Interface/ Assign Policy Route http-firewall to Ethernet interface 2.

Route Tables

Policy based routing can be used to overrule your routing table and change the next hop IP address for traffic meeting certain requirements.

Policy-based routing provides a tool for forwarding and routing data packets based on policies defined by you. It is a way to have the policy override routing protocol decisions. Policy-based routing includes a mechanism for selectively applying policies based on source IPv4 address, source mac-address, destination IPv4 address, protocol, fragment, IPSEC, recent and state. The resulting actions can include dropping matched packets or assigning packets to a static routing table.RIP

Route Tables	
Route Tables (Add, Edit, Delete)	
Destination prefix	**Configure a destination prefix.**

Destination prefix mask	Configure a destination prefix mask.
Route	
Route via:	• Forwarding Address • Interface • Null
Interface	Select the interface from the drop-down list.
Router Address	Configure the address of the forwarding router.
Default Gateway for Interface obtained by DHCP	Select this option to use the default gateway obtained by DHCP. Default is off
Administrative Distance	Enter an Administrative Distance. (AD) is a value that your router uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too 1. The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown
IPv6 Route Tables (Add, Edit, Delete)	
Destination prefix	Specify a destination prefix.
Destination prefix mask	Specify a destination prefix mask.
Route	
Route via:	• Forwarding Address • Interface • Null
Interface	Select the interface.
Router address	Specify the address of the forwarding router.

Administrative distance	**Enter an Administrative Distance.** **(AD) is a value that your** router **uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too 1. The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network.** **Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown**

RIP

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.

RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. RIP messages use the User Datagram Protocol on port 520 and all RIP messages exchanged between routers are encapsulated in a UDP segment. The routing metric used by RIP counts the number of routers that need to be passed to reach a destination IP network. The hop count 0 denotes a network that is directly connected to your router. A network is unreachable at 16 hops according to the RIP hop limit.

RIP	
Enable RIP	**Enable or disabled RIP.** **Default is disabled**
Administrative Distance	**Enter an Administrative Distance.** **(AD) is a value that your** router **uses to select the best path when there are two or more different routes to the same destination from two different routing protocols.** **Administrative distance is the reliability of a routing protocol. A static route is normally set too 1. The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network.** **Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown** **Value is 1-255** **Default is 120**
Metric	**Metric (hop count) is the number of routers through which data must pass from source network to reach the destination.** **Range is 1–60** **Default is 1**

Originate Default-information	Using originate default-information will advertise a default route, if there is one in the routing table. Default is no
Timers	
Update	Rate (in seconds) at which routing updates are sent. Range is 1–2147483 Default is 30 seconds
Invalid	The number of seconds since we received the last valid update. It should be at least three times the value of the update argument. A route becomes invalid when no updates refresh the route. The route then enters into a hold-down state where it is marked as inaccessible and advertised as unreachable. However, the route is still used to forward packets. Range is 1–2147483 Default is 180 seconds
Flush	Amount of time (in seconds) that must pass before the route is removed from the routing table. Range is 1–2147483 Default is 120 seconds
Passive Interfaces, Networks and Neighbors	
Passive Interface (Add, Delete)	Suppress routing updates on these interfaces. Select an interface from the drop-down list.
Network (Add, Delete)	Specify the Network’s IPv4 address and netmask. • IPv4 Address • IPv4 Mask
Neighbors (Add, Delete)	Specify the Neighbor address • IPv4 Address
Distributed and Redistributed Lists	
Distributed (Add, Delete)	
Filter	Filter the packets based on: • ACL • Prefix Default is ACL

ACL List or Prefix List	Select ACL list from the drop-down list. Select a Prefix List from the drop-down box
Direction	Select the direction to apply the ACL list to: • In • Out
Specify Interface	Apply the ACL/Prefix list to this interface. Select the interface from the drop-down box.
Redistributed (Add, Edit, Delete)	
Type	Type of routing protocol to redistribute to another routing protocol. It includes advertising your static routes and default routes also. • BGP • Connected • Kernel • OSPF • Static
Metric	Metric (hop count) is the number of routers through which data must pass from source network to reach the destination. Range is 1–16 Default is 1
Interface RIP (Edit)	
Interface	Select the interface to add authentication.
Mode	To specify the type of authentication used in the Routing Information Protocol (RIP) Version 2 packets • null • text <password> • md5 <key-chain>
Enable Split Horizon	Enable split horizon to prevent a routing loop in your network. Basically, information about the routing for a particular packet is never sent back in the direction from which it was received. Default is enabled

Enable Poison reverse for split-horizon	Enabling poison reverse for split-horizon sets therouter to actively advertise routes as unreachable from the interface over which they were learned by—setting the router's metric to infinite (16 for RIP). The effect of such an announcement is to immediately remove most looping routes before they can propagate through the network. The main disadvantage of poison reverse is that it can significantly increase the size of routing announcements in certain fairly common network topologies, but it allows for the improvement of the overall efficiency of the network in case of faults. Default is disabled.
Key Chain (Edit, Delete)	Specify the set of keys that can be used on an interface for RIP authentication.
Name	Add a key chain name.
Add Key ID	Configure the Key ID. ID for this key. Range is 1–2147483647
Password	Configure a password for key ID. This password is encrypted.

OSPF

OSPF (Open Shortest Path First) is a router protocol used to find the best path for packets as they pass through a set of connected networks.
Some of the most important reasons for implementing OSPF protocol are:

- Reducing routing overheads for companies
- Achieving network redundancy
- Optimizing performance of local area networks (LAN)

Terminology

OSPF (Open Shortest Path First)
Open Shortest Path First (ospf) is a protocol used to find the best paths for packets as they pass through a set of connected networks. OSFP was designed to replace the RIP protocol as it optimizes the updating up of the routing table. OSPF should be enabled on your router.

BGP (Broader Gateway Protocol)
BGP is an independent routing protocol that is used exclusively for the Internet. If using your router to connect to the Internet, BGP should be enabled.

Feature details / Application notes

Areas are a logical collection of routers that carry the same Area ID or number inside of an OSPF network, the OSPF network itself can contain multiple areas, the first and main

Area is called the backbone area “Area 0”, all other areas must connect to Area 0.

Area Type
Normal area By default, when you use a multiple area design, your created area’s will be considered “normal” area’s. This just means that these area’s support the flooding of all standard LSA types (1,2,3,4,5). Your backbone is considered a “normal” area. The main problem with “normal” area’s are they must carry all redistributed routes, including the redistributed routes instability. So to limit the amount of routing information into area’s, besides summarization, different “stubbie” area types are available.

Stub areas are areas through which or into which AS external advertisements are not flooded. You might want to create stub areas when much of the topological database consists of AS external advertisements. Doing so reduces the size of the topological databases and therefore the amount of memory required on the internal routers in the stub area. Stub areas are shielded from external routes but receive information about networks that belong to other areas of the same OSPF domain. You can define totally stubby areas. Routers in totally stubby areas keep their LSDB-only information about routing within their area, plus the default route.

Not-so-stubby areas (NSSAs) are an extension of OSPF stub areas. Like stub areas, they prevent the flooding of AS-external link-state advertisements (LSAs) into NSSAs and instead rely on default routing to external destinations. As a result, NSSAs (like stub areas) must be placed at the edge of an OSPF routing domain. NSSAs are more flexible than stub areas in that an NSSA can import external routes into the OSPF routing domain and thereby provide transit service to small routing domains that are not part of the OSPF routing domain.

OSPF Router ID is an IPv4 address (32-bit binary number) assigned to each router running the OSPF protocol. OSPF Router ID should not be changed after the OSPF process has been started and the OSFP neighborships are established.

OSPF Reference Bandwidth. OSPF uses a simple formula to calculate the OSPF cost for an interface with this formula: cost = reference bandwidth / interface bandwidth

Administrative distance determines what route to take when there are identical entries in the routing table. OSPF uses three different administrative distances: **intra-area**, **inter-area,** and **external**. Routes within an area are intra-area; routes from another area are inter-area; and routes injected by redistribution are external. The default administrative distance for each type of route is 110.

Border router is a router with interfaces in two (or more) different areas. An area border router is in the OSPF boundary between two areas. Both sides of any link always belong to the same OSPF area.

Virtual Links All areas in an OSPF autonomous system must be physically connected to the backbone area 0). In some cases where this physical connection is not possible, you can use a virtual link to connect to the backbone through a non-backbone area.

SPF – Shortest Path First

Interface – OSPF

- A **broadcast** interface behaves as if the routing device is connected to a LAN.
- A **point-to-point** interface provides a connection between a single source and a single destination (there is only one OSPF adjacency).
- A point-to-multipoint interface provides a connection between a single source and multiple destinations.
- **Non-broadcast** type is used on networks that have no broadcast/multicast capability, such as frame-relay, ATM, SMDS, & X.25

OSPF	
Enable OSPF	**Enable or disabled OSPF.** **Default is disabled**
Router ID	**Configure a global OSPF router ID. If this command is not configured, OSFP chooses an IPv4 address as the router ID from one of its interfaces. If this command is used on an OSPF instance that has neighbors, OSFP uses the new router ID at the next reload or restart of OSFP.**
Enable auto cost	**Enable auto-cost and configure a reference bandwidth to use to dynamically calculate OSPF interface cost.** **Default is disabled**
Reference bandwidth	**Directs the router to use reference bandwidth method for calculating administrative costs.** **Default reference bandwidth is 108 Mbps.**
Enable RFC 1583 compatibility	**Indicates whether handing of AS external routes should comply with RFC 1583.** **Default is disabled**
Enable opaque capability	**Enables support for opaque link-state advertisement as described in RFC2370.** **Default is disabled**
Distance	

Administrative Distance	Enter an Administrative Distance. (AD) is a value that your router uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too 1. The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown Value is 1-255 Default is 110
OSPF External	Sets the OSPF for routes injected by redistribution. Range is 1–255 Default is 110
OSFP inter-area routes	Sets the OSPF administrative distance by route type. Routes from another area are inter-area. Range is 1–255 Default is 110
OSFP intra-area routes	Sets the OSPF administrative distance by route type. Routes within an area are intra-area. Range is 1–255 Default is 110
Specify Default Metric	Configure a default metric to be applied to routes being distributed into OSPF. Range is 0–16777214 Default is none
Original default-information	Sets the characteristics of an external default route originated into an OSPF routing domain. Default is off
Max-Metric	Enables or disables the OSFP maximum / infinite-distance metric. Range is 0–16777215

Administrative	Enter an Administrative Distance. (AD) is a value that your router uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. A static route is normally set too 1. The smaller the administrative distance value, the more reliable the protocol. Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown Value is 1-255 Default is 110
On shutdown	Advertise stub-router prior to full shutdown of OSPF. Range is 5–86400 seconds Default is 600 seconds
On startup	Configures the router to advertise a maximum metric at startup. Range is 5–86400 seconds Default is 600 seconds
Refresh timer	The router automatically updates link-state information with its neighbors. Only an obsolete information is updated when age has exceeded a specific threshold. Range is 10–1800 seconds Default is 1800 seconds
Throttle Timers	Delay between receiving a change to SPF calculation in milliseconds. Range is 1–600000 milliseconds Default is 1 Delay between first and second SPF calculation. Range is 1–600000 milliseconds Default is 1 Maximum wait time in milliseconds for SFP calculations. Range is 1–600000 milliseconds Default is 1
OSPF Area	
Select Area ID format	Configure a unique number or IP address to identify this area • Number ID (use 0 to specify a backbone area) • IP address (use 0.0.0.0 to specify a backbone area)

ID	Enter the ID number or IP address as selected under Select Area ID format.
Area type	• normal • Stub—do not send summary LSA into stub area • NSSA—do not interject inter-area routes into NSSA
Default Authentication	Configure a password used by neighboring routers for simple password authentication. It can be any continuous string of up to eight characters. There is no default value. • None—no password • Message-digest—(Optional) Identifies the key ID and key (password) used between this device and neighboring routers for MD5 authentication. The default is none.
Default cost	Cost for the default summary route used for a stub or NSSA. Range is from 0–16777215
Shortcut	This parameter allows to "shortcut" routes (non-backbone) for inter-area routes. • enable—use this area for shortcutting • disable—never use this are for route shortcutting. • default—use this area for shortcutting—only if the ABR does not have a link to the backbone area or this link was lost
Virtual Link (Add, Edit, Delete)	
IP Address	IPv4 address of this virtual link.
Hello Packet Interval	Configure the hello packet time interval for hello packets sent on an interface. The default is 10 seconds.
Dead Router Detection Time	Configures the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down (dead).) As with the hello interval, this value must be the same for all routers attached to a common network. Default is 4 times the hello interval Default is 40 seconds
LSA retransmit Interval	Configure the time between link-state advertisement (LSA) retransmissions for adjacencies that belong to the virtual link. Default is 5

LSA transmission Delay	Before a link-state update packet is propagated out of an interface, the routing device increases the age of the packet. The transit delay sets the estimated time required to transmit a link-state update on the interface. By default, the transit delay is 1 second. You should never have to modify the transit delay time. To avoid LSAs from aging out during transmission, set an LSA retransmission delay especially for low speed links. The default is 5 seconds.
Authentication	Configure a password used by neighboring routers for simple password authentication. It can be any continuous string of up to eight characters. There is no default value. • None—no password • Text—Configure an authentication key • Message-digest—(Optional) Identifies the key ID and key (password) used between this device and neighboring routers for MD5 authentication. The default is none.
Authentication key	Configure the authentication key. Value is maximum 8 characters
Ranges	
Prefix length	Configure a prefix specified as IP address.
Mask	Configure a subnet mask
Mode	Advertise—sets the address range status to advertise and generates a Type 3 summary LSA. Not-advertise—sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed and the component networks remain hidden from other networks. Substitute (network prefix to be announced instead of range). The default is advertise
User Specified Cost	Configure the metric for this area range. Range is 0–16777215
Passive Interfaces, Network and Neighbors	
Passive Interfaces	Suppresses routing updates on these interfaces.
Add IP Network	

IPv4 Address	Configure IPv4 network address.
IPv4 Wildcard	Configure IPv4 wildcard address.
Select Area ID format	Configure a unique number or IP address to identify this area • Number ID (use 0 to specify a backbone area) • IP address (use 0.0.0.0 to specify a backbone area)
ID	Enter the ID number or IP address as selected under Select Area ID format.
Add Neighbor	
IPv4 Neighbor Address	Configure IPv4 Neighbor Address.
Poll Interval	Configure the dead-router polling interval for non-broadcast neighbor. Values are 1-65535 in seconds Default is 120 in seconds
Priority	Priority of non-broadcast neighbor. Values are 0-255 Default is 1
Distributed List (Add, Edit, Delete)	
ACL List	Specify the access list to filter networks in routing updates. With extended ACL, only the source is used for filtering, the destination must be set to any.
Type	Select the type of route: • BGP • Connected (directly attached subnet or host) • Kernel • OSPF • Static
Redistribution List (Add, Edit, Delete)	

Type	Select the type of route: • BGP • Connected (directly attached subnet or host) • Kernel • OSPF • Static
Router Map	Select the router map from the drop-down list.
Metric	Configure the metric for this redistribution list. Values are 1-16 Default is 1
Metric Type	Set metric type to: 1—OSPF External Type 1 2—OSPF External Type 2
Interface—OSPF (Edit)	
Network Type	• broadcast—a designated router and backup designated router are elected using OSPF multicasting capabilities. (most common type) • non-broadcast—use this type of network on networks having no broadcast/multicast capability, such as frame-relay, ATM, SMDS, & X.25. The key point is that these layer 2 protocols are unable to send broadcasts/multicasts. • point-to-multipoint— configures selected routers with neighbor/cost parameters, identifying a specific cost for the connection to the specified peer • point-to-point—there are only two neighbors and multicast is not required. Routers on an interface becoming neighbors should match the network type all.
Disable MTU mismatch detection	By default, OSPF checks whether neighbors are using the same MTU on a common interface. Use this command to disable this check and allow adjacencies when the MTU value differs between OSPF neighbors. OSPF will not establish adjacencies if the receiving MTU is higher than the IP MTU configured on the incoming interface. Default is disabled.

Router Priority	**A router with a high priority will always win the DR/BDR election process** **Priority Range is 0-255** **Default is 1**
Interface cost	**OSPF uses "Cost" as the value of metric and uses a Reference Bandwidth of 100 Mbps for cost calculation. The formula to calculate the cost is Reference Bandwidth divided by interface bandwidth.** **For example, in the case of 10 Mbps Ethernet, OSPF Metric Cost value is 100 Mbps / 10 Mbps = 10**
Dead interval	**Configures the interval during which at least one hello packet must be received from a neighbor before the device declares that neighbor as down (dead).) As with the hello interval, this value must be the same for all** routers **attached to a common network.** **Range is 1–65535 seconds** **Default is 4 times of hello interval in seconds**
Hello interval	**Configure the time between Hello packets.) Time in seconds between the hello packets that the** router **software sends on an interface. The** **value must be the same for all** routers **attached to a common network.** **Range is 1–65535** **Default is 10 seconds**
Retransmit interval	**Configure the time between retransmitting lost link state advertisements.) Time in seconds between link state advertisement retransmissions for adjacencies belonging to the interface. The expected round-trip delay between any two** routers **on the attached network.** **Range is 1–65535** **Default is 5 seconds**
Transmit delay	**Configure the transmit delay. The estimated time in seconds required to transmit a link state update packet on the interface. Link state advertisements in the update packet have their age incremented by this amount before transmission** **Range is 1–65535** **Default is 1 seconds**
Authentication	

Mode	Enable authentication in OSPF to exchange secure routing update information. • null—configures authentication type as • plaintext and assign a password to be used by neighboring routers that are using OSPF simple password authentication. • md5—the most secure OSPF authentication mode. Configure the entire area with the same authentication mode
Authentication key	Configure the text authentication mode key.
Message Digest	
Add Key	
ID	Configure ID for md5 authentication mode.
Key	Configure the md5 key.
OSPFv3	
Enable OSPFv3	Enable or disabled OSPFv3. Default is disabled
Router ID	Configure a global OSPF router ID. If this command is not configured, OSFP chooses an IPv4 address as the router ID from one of its interfaces. If this command is used on an OSPF instance that has neighbors, OSFP uses the new router ID at the next reload or restart of OSFP.
Select area ID format	Configure a unique number or IP address to identify this area • Number ID (use 0 to specify a backbone area) • IP address (use 0.0.0.0 to specify a backbone area)
Export list	Select list from the drop-down box.
Import list	Select list from the drop-down box.
Specify OSPFVv3	Stub—do not send summary LSA into stub area NSSA—do not interject inter-area routes into NSSA
Add range	

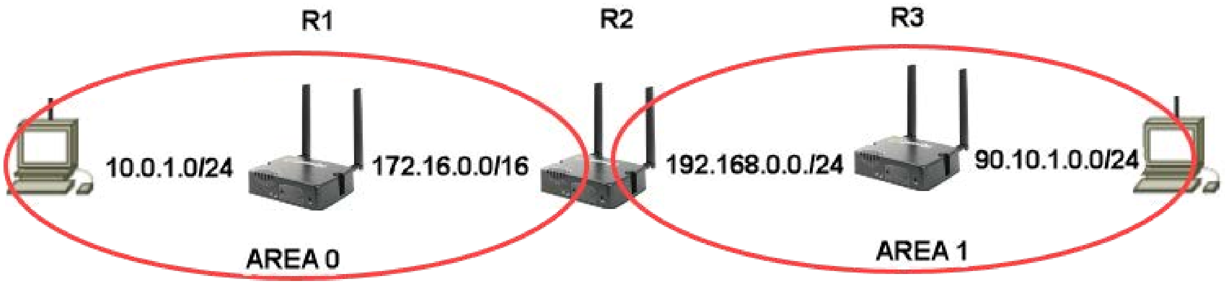
Range	Specify the ip address range.
Prefix Length	Specify the prefix length.
Add Redistribution List	• BGP • Connected • Kernel • RIP • Static
Router Map	Select from the drop-down list.
Interface—OSPFv3 (Edit)	
Network Type	• broadcast—a designated router and backup designated router are elected using OSPF multicasting capabilities. (most common type) • non-broadcast—use this type of network on networks having no broadcast/ multicast capability, such as frame-relay, ATM, SMDS, & X.25. The key point is that these layer 2 protocols are unable to send broadcasts/multicasts. • point-to-multipoint— configures selected routers with neighbor/cost parameters, identifying a specific cost for the connection to the specified peer • point-to-point—there are only two neighbors and multicast is not required. Routers on an interface becoming neighbors should match the network type all.
OSPFv3 area this interface belong to	Enter OSPFv3 area ID. Values are format 0,429496729 or format 0.0.0.1
Passive interface, no adjacency will be formed on this interface	Passive interface only, do not form adjacencies. Enable or Disable Default is disabled
Disable MTU mismatch detection	By default, OSPF checks whether neighbors are using the same MTU on a common interface. Use this command to disable this check and allow adjacencies when the MTU value differs between OSPF neighbors. OSPF will not establish adjacencies if the receiving MTU is higher than the IP MTU configured on the incoming interface. Default is disabled

Router Priority	A router with a high priority will always win the DR/BDR election process Priority Range is 0-255 Default is 1
Instance ID	Enter an instance between 0-255.
Interface MTU	Enter the MTU for this interface. Values are 1-65535
Interface Cost	To help maximize efficiency on your network, you can manually specify a different cost. Values are 1-65535
Dead interval	Configures the interval during which at least one hello packet must be received from a neighbor before the device declares that neighbor as down (dead).) As with the hello interval, this value must be the same for all routers attached to a common network. Range is 1–65535 seconds Default is 4 times of hello interval in seconds
Hello interval	Configure the time between Hello packets.) Time in seconds between the hello packets that the router software sends on an interface. The value must be the same for all routers attached to a common network. Range is 1–65535 Default is 10 seconds
Retransmit interval	Configure the time between retransmitting lost link state advertisements.) Time in seconds between link state advertisement retransmissions for adjacencies belonging to the interface. The expected round-trip delay between any two routers on the attached network. Range is 1–65535 Default is 5 seconds
Transmit delay	Configure the transmit delay. The estimated time in seconds required to transmit a link state update packet on the interface. Link state advertisements in the update packet have their age incremented by this amount before transmission Range is 1–65535 Default is 1 seconds

Network Type	• **broadcast—a designated router and backup designated router are elected using OSPF multicasting capabilities. (most common type)** • **point-to-point—there are only two neighbors and multicast is not required. routers on an interface becoming neighbors should match the network type all.** • **auto—automatically selects network type**

OSFP Configuration Example

In this example, we will configure a multi area OSPF network. We have two OSPF areas—area 0 and area 1. Area 0 consists of routers R1 and area 1 consists of router R3. R2 connects to both areas and therefore makes him a ABR (Area Border Router). Our goal is to advertise the subnets directly.



Configuration for Router **R1**

1. Under Routing/OSPF/Enable OSFP manually configure the Router ID to 1.1.1.1. The OSPF process uses this RID (router-id) to communicate to other OSPF neighbors.
2. Under OSPF Area add area 0.
3. Under OSPF/Passive Interfaces/ Network and Neighbors, Add Network 10.0.1.0 0.0.0.255 area 0, then add Network 172.16.0.0 0.0.225.255 area 0

Configuration for Router **R3**

1. Under Routing/OSPF/Enable OSFP manually set the Router ID to 3.3.3.3 The OSPF process uses this RID (router-id) to communicate to other OSPF neighbors.
2. Under OSPF Area add area 1.
3. Under OSPF/Passive Interfaces/ Network and Neighbors, Add Network 192.168.0.0 0.0.0.255 area 1, then add Network 90.10.0.0 0.0.0.255 area 1

Configuration for Router **R2**

Because R2 is an ABR, we need to establish neighbor relationship with both R1 and R3. To do that, we need to specify different area ID for each neighbor relationship, 0 for R1 and 1 for R2.

1. Under Routing/OSPF/Enable OSFP manually set the Router ID to 2.2.2.2. The OSPF process uses this RID (router-id) when communicating to other OSPF neighbors.
2. Under OSPF/Passive Interfaces/ Network and Neighbors, Add Neighbor 172.16.0.0 0.0.255.255 area 0, then add Neighbor 192.168.0.0 0.0.0.255 area 1.

R2 now has a neighbor relationship with both R1 and R3.

Use the show command on R2 to verify.

```
Router#ip ospf neighbor<cr>

Neighbor ID Pri State        Dead Time Address            Interface  RXmtL RqstL DBsmL
1.1.1.1                      1Full/BRD00:00:22172.16.0.1    Ethernet             1000
3.3.3.3                      1Full/BRD00:00:26192.168.0.2  Ethernet             2000
```

NOTE: R1 and R3 will never establish a neighbor relationship because they reside in different areas.

BGP

Border Gateway Protocol (BGP) is one of the key protocols used to achieve Internet connection redundancy and optimization. It is designed as a standardized exterior gateway protocol to exchange routing and reachability information among autonomous systems (AS) on the Internet. BGP makes routing decisions based on paths, network policies, or rule-sets configured by you.

When you connect your network to two different Internet service providers (ISPs), it is called multihoming. When running BGP with more than one service provider, you run the risk that your autonomous system (AS) will become a transit AS. Internet traffic can pass through your AS and potentially consume all of the bandwidth and resources on the CPU of your router. See the example below for setting up BGP with multihoming.

Terminology

BGP (Border Gateway Protocol) is a routing protocol that makes routing decisions across the Internet—usually externally rather than internally. BGP works towards changing routing information between gateway hosts in a network of autonomous systems—it establishes routing between users and allows for peer and carrier networks to connect.
AS (Autonomous System)—is a set if internet routable IP prefixes belonging to a network or a collection of networks that are all managed and controlled by a single organization.

BGP	
BGP (Add, Edit, Delete)	**Some BGP parameters may not be available on some firmware versions or models.**
ASN	**An autonomous system number (ASN) is a unique number that's available globally to identify an autonomous system and which enables that system to exchange exterior routing information with other neighboring autonomous systems.** **Your service provider will assign you the first three digit for ASN, the last two digits should be unique.** **Values are 1–4294967295**
Administrative Distance	
Remote Addresses (Add, Delete))	
Distance (Administrative)	**Enter an Administrative Distance.** **(AD) is a value that your router uses to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance is the reliability of a routing protocol. Administrative distance is the reliability of a routing protocol. A static route is normally set to 1. The smaller the administrative distance value, the more reliable the protocol.**

	Administrative Distance is locally significant, it is not advertised to the network. Range is 1-255 (with 1 being the most reliable) and 255 is route not used or unknown
IP Source	Configure the IP source prefix.
IP Mask	Configure the IP source prefix mask.
BGP Distance	
Distance for external routes to AS	Configure the administrative distance (AS) for external routes. Values are 1–255 Default is 20
Distance for internal routes to AS	Configure the administrative distance (AS) for internal routes. Values are 1–255 Default is 200
Distance for local routes	Configure the administrative distance (AS) for local routes. Values are 1–255 Default is 200
Timers	
Keep Alive	Configure a keepalive time. Range is 0–65535 Default is 60 seconds
Hold Time	Configure a hold time. Default is 180 seconds
Neighbor List (Add)	
Redistribution List	Select the type of route for redistribution. • BGP • Connected (directly attached subnet or host) • Kernel • OSPF • Static

Router Map	A route map consists of a series of statements that check to see if a route matches the policy, to permit or deny the route Select a router map from the drop-down list.
Metric	This is a measure used by the routing protocol to calculate the best path to a given destination, if it learns multiple paths to the same destination. Metric is the primary metric on all routes sent to peers. Value range is 1-4,294,967,295
Neighbors (Add, Edit, Delete)	
IPv4 neighbor address	IPv4 address of a neighbor peer.
BGP neighbor	Configures a BGP neighbor also called peer.
Enable neighbor	Enable this BGP neighbor. Default is enabled
Description of the neighbor	Configure a description of this neighbor.
Advertisement interval	Configure the minimum time between sending BGP routing updates. Values 0-600 seconds Default eBGP is 30 seconds Default iBGP peers is 5 seconds
Accept as-path with my AS occurrence	Accept AS-path with my own AS present in it. Allows or disallows receiving BGP advertisements containing the AS path of the local router Default readvertisement is disabled Values are 1 to 10. Default is 3
Override match AS-number when sending updates	Overrides ASN's in outbound updates if AS–path equals remote. Only applies to eBGP neighbor. Default is disable
All BGP attributes are propagated unchanged to this neighbor	Allows the router to send updates to a neighbor with unchanged attributes. Default is on

Specify BGP attribute is propagated unchanged to this neighbor	Allows the router to send updates to a neighbor with these unchanged attributes. • AS-path • MED • Next-hop Default is on
Advertise capability to the peer	Advertises support for Outbound Route Filtering (OFR) for updating BGP capabilities advertised and received from this neighbor. Dynamic • ORF receive • ORF transmit • ORF both Default is OFR transmit Default is session is brought up with minimal capability on both sides
Originate default route to this neighbor	Enables or disables forwarding of the default route to a BGP neighbor. Default is off
One-hop away EBGP peer using loopback address	Enables a directly connected eBGP neighbor to peer using a loopback address without adjusting the default TTL of 1. Default is off
Do not perform capability negotiation	Disables BGP capability negotiation Default is capability negotiation is performed
Allow EBGP neighbors not on directly connected networks	Allows you to establish eBGP peer relationships between routers that aren't directly connected to one another. Default is off.
Filter outgoing updates	Filter outgoing packet updates from neighbors. You must create the access list before it can be selected here. Default is off
Filter incoming routes	Limit inbound BGP routes according to the specified access list. You must create the access list before it can be selected here. Default is off.

Filter outgoing routes	Limit outbound BGP routes according to the specified access list. You must create the access list before it can be selected here. Default is off.
Specify local as number	Using a local AS number permits the routing devices in an acquired network to appear to belong to the former AS. This is useful if you cannot immediately modify your peer arrangements or configuration during a transition period of assigning a new AS number.
Allow a maximum number of prefixes accepted from this peer	Specify the number of prefixes that have been received from a peer has exceeded the maximum prefix limit. Default is off
Disable the next hop calculation for this neighbor	This command will change next hop attribute for received updates to its own IP address. Default is off
Override capability negotiation result	Use configured capabilities regardless of what capabilities have been negotiated. Default is off
Don’t send open messages to this neighbor	Configure the routing device to be passive, the routing device will wait for the peer to issue an open request before a message is sent. Default is off
Set a password	MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Default is off
Neighbor’s BGP port (TCP)	Specify the TCP port that BGP peers will use to exchange BGP information. Values 1-65535 ports Default is 179 port
Filter incoming routes	Allow incoming routes to be filtered. Default is off
Filter outgoing routes	Allow outgoing routes to be filtered. Default is off

Remove private AS number from outbound updates	Select this option to remove private ASNs from the AS path if you have been using private ASNs and you want to access the global Internet. Default is off
Apply map incoming routes	Apply route map to incoming routes.
Apply map outgoing routes	Apply route map to outgoing routes.
Configure a neighbor as Route Reflector client	Configure the BGP peer to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors.
Configure a neighbor as Route Server client	Configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.
Send Community attribute to this neighbor	• Extended • Standard • Both Default is both
Allow inbound soft reconfiguration for this neighbor	Enables you to generate inbound updates from a neighbor, change and activate BGP policies without clearing the BGP session.
Strict capability negotiation for this neighbor	By default, your router will bring up peering with minimal common capability for the both sides. For example, local router has unicast and multicast capabilities and remote router has unicast capability. In this case, the local router will establish the connection with unicast only capability.
Keepalive interval	How often the router sends out keepalive messages to neighbor routers to maintain those sessions. Values are 1–65535 Default is 60
Hold Time	How long th e router will wait for a keepalive message before declaring a router off-line. A shorter time will find an off-line router faster. Values are 1–65535 Default is 180

Connect Timer	How long in seconds the router will try to reach this neighbor before declaring it off-line. Values are 1–65535 Default is 120
Specify the maximum number of hops to the BGP peer	Enable, then specify the number of hops for not directly connected EBGP neighbors. Values are 1–254
Route-map to selectively unsuppressed suppressed routes	Use this command if a BGP neighbor requires some of the granular routes within the route-map summary. Default is off
Set source of routing updates	Select the source for routing updates. • IP based • Interface based
IP address	Specify an IP address for IP based source routing updates.
Set default weight for routes from this neighbor	Weight is not exchanged between BGP routers. Weight is only local on the router. The path with the highest weight is preferred. Values are 1–65535
IPv4 Family	Select the address family mode. Select IPv4 or IPv6.
Maximum Path	Configure the maximum paths to forward packets over. Values are 1–64 Default is 1
IBGP Maximum Path	Configure the maximum paths to forward IBGP packets over. Default is 1 Values are 1–64
BGP Settings	
BGP Router ID	Configure a BGP router ID to identify to BGP-speaking peers. The BGP router ID is a 32-bit value that is often represented by an IPv4 address. Default is 0.0.0.0

Compare MED from different neighbors	Allow comparing MED from different sources. Default is off
Best Path (AS-path)	
Compare a path lengths including confederation set and sequences	Compare path lengths including confederation when selecting a route. Default is off
Ignore AS-Path Length	Do not consider AS-path length with selecting a route. Default is off
MED Attribute	
Compare MED among confederation paths	Consider matching of confederation paths. Default is off
Treat missing MED as the least preferred one	Treats a route without an MED as the worst possible available route due to expected unreliability. Default is off
Compare router-id for identical EGBP paths/labels	Check router-id for identical EGBP paths. Default is off
Configure client to client route reflection	Select whether this BGP entity reflects routes received from a client to another client. Default is on
Cluster-ID	Configure Route-Reflector client cluster-id. Default is 0

Confederation	Configure a confederation identifier. In network routing, BGP confederation is a method to use Border Gateway Protocol (BGP) to subdivide a single autonomous system (AS) into multiple internal sub-AS's, yet still advertise as a single AS to external peers. The intent is to reduce iBGP mesh size. Default is 0
Identifier	Configure an confederation identifier. Value range is 1-4294967295
Dampening	A flapping route is unstable and continually transitions down and up (see RFC 2439). When a prefix flaps it's assigned a penalty of 1000 and moved into the dampening state. Each flap incurs another penalty (of 1000), which is applied cumulatively. If the penalty reaches the suppress-limit, the route is dampened, meaning it won't be advertised to any neighbors. Once a route is dampened, the penalty must be reduced to a value lower than the reuse limit in order to be advertised once again. Enable or disable (by default)
Half-life	The half-life timer is a calculation to determine when the route is stable again and is advertised. After a penalty is assigned and the prefix is stable again, the half-life timer starts. Values are 1-45 minutes Default is 15 minutes
Value to Start re-using a route	A dampen route begins to be advertised to neighbors when it recovers to this value. Values 1–20000 Default is 750
Value to start suppress-ing a route	Specify a value, when reached, the route is no longer advertise this route to any neighbors. Values are 1–20000 Default is 2000
Max duration to suppress a stable route	The maximum suppress-limit ensures the prefix doesn't get dampened indefinitely. Values are 1-255 Default is 60
Activate IPv4-unicast	Activate ipv4-unicast for a peer by default. Default is off

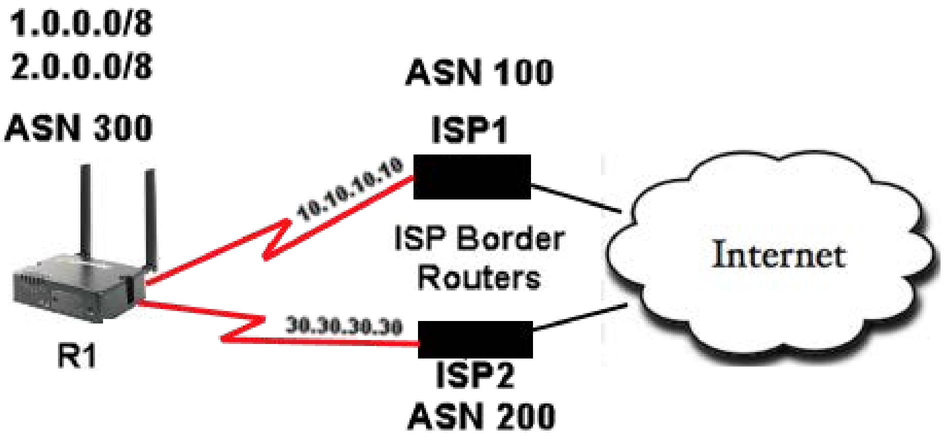
Default Local Preference	Configure a local preference level. The higher value is more preferred. Values are 0–4294967295 Default is 100
Pick the best-MED path among paths advertised from the neighboring AS	Determine the best MED-path from paths advertised from the neighboring AS. Default is off
Enforce the first AS for EBGP routes	Enforce the first (left-most) autonomous system number (ASN) is the AS-path in the previous neighbor's ASN. Default is off
Immediately reset session if a link to a directly connected external, peer goes down	Immediately reset the session information associated with BGP external peers if the direct link to reach them goes down. Default is on
Graceful Restart capability parameters	The routing device informs its neighbors when it is performing a restart. Default is off
Set the max time to hold onto restarting peer’s stale paths	Configure the time to hold stale paths of restarting neighbors Value is 1–3600 seconds. Default is 360 seconds
Log neighbor up/down and reset reason	Log reason for neighbor up/down/reset state. Default is off
Check BGP network route exists in IGP	Check if the BGP network route exists in IGP. Default is on

Background scanner interval	Configure a time for BGP tolls to go through the routing table to ensure the next-hop address of all the BGP prefixes are reachable through an IGP. Values are 5-60 seconds Default is 60 seconds
Aggregate Address	BGP Route Aggregation reduces the number of BGP entries that have to be stored and exchanged with other BGP peers.
IPv4 Address	Configure an IPv4 aggregation address. This address is used to summarize a set of networks into a single prefix
IPv4 Mask	Configure the netmask for the aggregate address.
Generate AS set path information	Creates an aggregate address with a mathematical set of autonomous systems (ASs). This AS-set argument summarizes the AS_PATH attributes of all the individual routes.
Filter more specific routes from update	Filter longer prefixes inside of the aggregate address before sending BGP updates.
Networks (Add, Edit, Delete)	
IPv4 neighbor address	IPv4 address of a neighbor peer.
Mask	Configure the mask for the neighbor peer.
Specific a BGP backdoor route	Specify to use a backdoor route Default is off
Route Map	Select a route map from the drop-down list.
Redistribute List (Add, Edit, Delete)	
Type	Select route type for redistribution. • BGP • Connected (directly attached subnet or host) • Kernel • OSPF • RIPng • Static
Router Map	A route map consists of a series of statements that check to see if a route matches the policy, to permit or deny the route A route map must be predefined.

Metric	**This is a measure used by the routing protocol to calculate the best path to a given destination, if it learns multiple paths to the same destination.**
IPv6 Address Family	
Aggregate Address (Add, Edit, Delete)	
IPv6 Address	**Specify the IPv6 address.**
IPv6 Mask	**Specify the IPv6 mask.**
Filter more specific routes from update	**Filter longer-prefixes inside of the aggregate address before sending BGP updates.**
Networks (Add, Edit, Delete)	
IPv6 address	**Add a IPv6 peer network.**
Prefix Length	**Specify a prefix length for this network**
Route Map	**A route map consists of a series of statements that check to see if a route matches the policy, to permit or deny the route A route map must be predefined.**
Redistribute List (Add, Edit, Delete)	
Type	**Select route type for redistribution.** • **BGP** • **Connected (directly attached subnet or host)** • **Kernel** • **OSPFv3** • **RIPng** • **Static**
Router Map	**A route map consists of a series of statements that check to see if a route matches the policy, to permit or deny the route A route map must be predefined.**
Metric	**This is a measure used by the routing protocol to calculate the best path to a given destination, if it learns multiple paths to the same destination.**

BGP Multihoming Example

Network Diagram



This configuration allows Router (R1) to peer with BGP speakers in other autonomous systems. The **route-map localonly** command allows only the locally generated routes to be advertised to both of the ISPs. This prevents Internet routes from one ISP to the other ISP and prevents the risk that your AS becomes a transit AS for Internet traffic.

Configuration to receive directly-connected routes.
R1
Current configuration

```
router bgp 300
        network 1.0.0.0
        network 2.0.0.0
        neighbor 10.10.10.10 remote-as 100
        neighbor 10.10.10.10 route-map localonly out
        * outgoing policy route-map the filters routes to ISP1*
        neighbor 30.30.30.30 remote-as 200
        neighbor 30.30.30.30 route-map localonly out
        * outgoing policy route-map the filters routes to ISP2*
```

This AS-path access list will only allow locally originated BGP routes:

```
        ip as-path access-list permit 10 permit ^$
```

This route-map command uses the as-path access list to filter the routes advertised to the external neighbors in the ISP networks.

```
        route-map localonly permit 10
        match as-path 10
```

Configuration to receive directly-connected routes.
R1
Current configuration

router bgp 300

```
        network 1.0.0.0
        network 2.0.0.0
        neighbor 10.10.10.10 remote-as 100
        neighbor 10.10.10.10 route-map localonly out
```

*** outgoing policy route-map the filters routes to ISP1***

```
        neighbor 10.10.10.10 route-map as100only in
```

incoming policy route-map that filters routes to ISP1*

```
        neighbor 30.30.30.30 remote-as 200
        neighbor 30.30.30.30 route-map localonly out
```

*** outgoing policy route-map the filters routes to ISP2***

```
        neighbor 30.30.30.30 remote-as as200only in
```

incoming policy-map that filters routes from ISP2

You want to accept routes that are directly connected to the ISPs, therefore you must filter the routes that they send to you, as well as the routes that you advertise. Do you that use this access-list and route map command.

```
        ip as-path access-list 10 10 permit ^$
        route-map localonly permit 10
        match as-path 10
```

Use these access-list and route-map commands to filter out anything that is not sourced within ISP1—filter the routes that are learned from ISP1.

```
        ip as-path access-list 20 permit ^100$
        route-map as100only permit 10
        match as-path 20
```

Use this access-list and route-map commands to filter out anything that is not sourced within ISP2—filter the routes that are learned from ISP2.

```
        ip as-path access-list 30 permit ^100$
        route-map as100only permit 10

        match as-path 20
```

Configure two default routes that are distributed back into the rest of your network, one pointed to each of the ISP provider entry points.

```
        ip route 0.0.0.0 0.0.0.0 10.10.10.10
        ip route 0.0.0.0 0.0.0.0 20.20.20.20
```

Configuration to receive default routes only
R1
Current configuration

router bgp 300

```
network 1.0.0.0
network 2.0.0.0

neighbor 10.10.10.10 remote-as 100
neighbor 10.10.10.10 route-map localonly out
```

*** outgoing policy route-map that filters routes to ISP1***

```
neighbor 10.10.10.10 prefix-list filterroute in

neighbor 30.30.30.30 remote-as 200
neighbor 30.30.30.30 route-map localonly out
```

*** outgoing policy route-map that filters routes to ISP2***

```
neighbor 30.30.30.30 prefix-list filterroute in
ip prefix-list ABC seq 5 permit 0.0.0.0/0
```

*** Prefix list to allow only default route updates and no other networks form ISP1 and ISP2***

Apply the prefix-list on the inbound updates on individual BGP neighbors like this

```
neighbor 10.10.10.10 prefix-list filterroute in
neighbor 30.30.30.30 prefix-list filterroute in
```

Services

Telnet/SSH

Set routerVTY session, SSH client, and SSH server configuration parameters in this section.

Terminal	
Enable terminal history size	Enter the size of the terminal history. Range is 1—256 Default is 20
Terminal width	Specify the width of the terminal Values are 1—512 columns Default is 80 columns
Enable terminal pausing	Pause the terminal at end of screen.
Terminal length	Specify the terminal length in line. Range is 1—512 Default is 24
Session EXEC inactivity timeout	Specify the days, hours, minutes, and seconds for the timeout on EXCEC sessions.
SSH	
Client	
Enable strict host key checking (install host keys)	When enabled, a host public key—for each host you SSH to—must be downloaded into the router. Default is enabled
Configure MACs for the SSH2 client in order of preference	Data Options: • UMAC-64-ETM • UMAC-128-ETM • HMAC-SHA2-256-ETM • HMAC-SHA2-512-ETM • HMAC-SHA1-ETM • UMAC-64 • UMAC-128 • HMAC-SHA2-256 • HMAC-SHA2-512 • HMAC-SHA1

Server	
Login timeout	The login timeout. Range 0—150 seconds Default is 120 seconds
Authentication retries	The user is locked out after x incorrect authentication attempts. Range is 1—5 Default is 3
Authentication	• public key • keyboard interactive • password
Configure allowed ciphers	• ChaCha20-Poly1305, AES128-CTR, AES192-CTR, AES256-CTR, AES128-GCM, AES256-GCM, AES128-CBC, AES-192-CBC, AES-256-CBC, RIJNDEL-CBC, ARCFOUR, ARCFOUR128, ARCFOUR256, CAST128-CBC, BLOWFISH-CB, 3DES-CBC
Configure allowed MACs for the SSH-2 server	• UMAC-64-ETM, UMAC-128-ETM, HMAC-SHA2-256-ETM, HMAC-SHA2-512-ETM, HMAC-SHA1-ETM, HMAC-SHA1-96-ETM, UMAC-64, UMAC-128, HMAC-SHA2-256, HMAC-SHA2-512, HMAC-SHA1, HMAC-SHA-96, HMAC-MD5, HMAC-MD5-96

DHCP Server

The Perle router can act as a DHCP server to devices connected to its Ethernet ports or devices which can access the network. A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients Your router can act as a DHCP server so that clients can obtain addresses from its DHCP pool. Your router has a predefined default pool with a network address of 192.168.0.0 and a pool from 192.168.0.100 to 192.168.0.200.

To use DHCP/BOOTP, edit the bootp file with router configuration parameters. You can use DHCP/BOOTP to perform the following actions on a single or multiple routers on boot up:

- auto-configure with minimal information; for example, only an IP address
- auto-configure with basic setup information (IP address, subnet/prefix bits, etc.)
- download a full configuration file

DHCP/BOOTP is particularly useful for multiple installations: you can do all your Perle router configuration in one DHCP/BOOTP file, rather than configure each router manually.

Another advantage of DHCP/BOOTP is that you can connect your router to the network, turn on its power and let autoconfiguration take place. All the configuration is carried out for you during the DHCP/BOOTP process.

DHCP Parameters

The following parameters can be set in the DHCP/BOOTP bootp file:

- **SW_FILE**—The full path, pre-fixed by hostname/IP address (IPv4 or IPv6), and file name of the software update.
- **CONFIG_FILE**—The full path, pre-fixed by hostname/IP address (IPv4 or IPv6), and file name of the configuration file.
- **GUI_ACCESS**—Access to the router from the HTTP or HTTPS-WebManager. Values are on or off.
- **AUTH_TYPE**—The authentication method(s) employed by the router for all users. You can specify the primary and secondary authentication servers, separated by a comma. This uses the following numeric values for the authentication methods.
  - **0**—None (only valid for secondary authentication)
  - **1**—Local
  - **2**—RADIUS
  - 4—LDAP/Microsoft Active Directory
  - **5**—TACACS+
- **SECURITY**—Restricts router access to devices listed in the routers host table. Values are yes or no.
- **TFTP_RETRY**—The number of TFTP retries before aborting. This is a numeric value, for example, 5.
- **TFTP_TMOUT**—The time, in seconds, before retrying a TFTP download/ upload. This is a numeric value, for example, 3.

Terminology

DHCP Pool

A predefined grouping of IP addresses from which the DHCP server can assign IP addresses to clients.

DHCP lease

- A DHCP lease defines the duration for which a valid IP address is assigned to a DHCP client.
- When the lease expires, the DHCP client will not be able to use the IP assigned to it unless the DHCP reassigned that IP address.

DHCP Relay Agent

A DHCP relay agent is a device which forwards DHCP requests from clients to a DHCP server. This often is used if a central DHCP server is being used. The DHCP clients make the local DHCP requests and these requests are forwarded by the Relay Agent to the DHCP server which is not available on the local network.

DHCP Server

Enable DHCP Server	Enable or disabled DHCP Server. Default is enabled.
Description	Enter a description for this DHCP pool.
DHCP Pools (Add)	
DHCP Basic Settings	
Network subnet	Specify the DHCP network subnet.
Network mask	Specify the DHCP network mask.
Specify Address Range within Network	The router's DHCP pool will assign addresses to clients starting at X.X.X.X with an end address of X.X.X.X.
Lease Duration	• Infinite: The DHCP lease will not expire • Limited: Set the time for the DHCP lease to expire, thereby releasing the address back to the DHCP pool
Default Gateway	Specify the default gateway. This will normally be the IP address of your router.
DNS Server	Specify the DNS addresses to be used by the clients.
Use Static Route	
Destination Network Prefix	Specify a destination network prefix for this static route.
Destination Network Mask	Specify a destination network mask for this static route.
Gateway Address	Specify a the gateway for this static route.
Reserved Addresses	Enter reserved addresses (IP addresses that will not be served from this pool) and their corresponding MAC addresses.

Options	Enter an option number. Range is–254 Enter option data. • ASCII • Hex • IP addresses
Advanced	
Enable Authoritative Mode	Enable Authoritative is defaulted to On. This allows our router to respond to all DHCP requests on the network. If the network has no authoritative DHCP server present, all DHCP servers will ignore client requests and the client will potentially get into an unstable state. At least one DHCP server must be set to Authoritative on the network.
Bootfile	Specify the name of the bootfile to use.
Domain Name	Specify the Domain name of the server that has the bootfile.
DHCP Exclude Addresses (Add)	
Excluded Address	Specify addresses to exclude from the DHCP pool.
DHCPv6 Pools (Add, Edit, Delete)	
Pool name	Specify a pool name.
Lifetime	Configures the device lifetime value in IPv6 router advertisements on an interface. • Default valid lifetime Range is 0–4294967294 • Maximum valid lifetime Range is 0–4294967294 • Minimum valid lifetime Range is 0–4294967294
IPv6 Subnet Allocation	
Network Subnet	Enter the Network subnet for this network.
Network Mask	Enter the Network Mask for this network.
IPv6 Address Allocation (Add)	

Address	IPv6 address
Prefix Length	The number of bits in a prefix.
IPv6 Address Lease Range	
Start	Enter the start range for IPV6 leased addresses. Format: X:X:X:X::X
Stop	Enter the stop range for IPV6 leased addresses. Format: X:X:X:X::X
DNS Servers	Specify the DNS server addresses to be used by the clients.
SNTP Servers	Specify the SNTP server addresses to be used by the clients.
NIS Servers	Specify the NIS domain and server addresses to be used by clients.
NISP Servers	Specify the NISP domain and servers addresses to be used by clients.
SIP Servers	IPv6 address of SIP outbound proxy server. Domain name of the SIP outbound proxy server.
Domain	Specify the domain servers to be used by clients
Add Host	Hostname—Specify a client hostname Client ID—Specify the client ID to use. (In DHCPv6 it consists of two parts: a DHCP Unique Identifier (DUID) and an Identity Association Identifier (IAID)) Address—Specify client IPv6 address

DHCP Relay

The router is able to act as a DHCP relay agent. The DHCP relay agent forwards DHCP requests between the DHCP clients residing on the local subnet and a remote DHCP server which resides outside the local physical subnet.

Terminology

DHCP Relay Agent

A Relay agent is a device which forwards DHCP requests from clients to a DHCP server. This is often used if a central DHCP server is being used. The DHCP clients make local DHCP requests and these requests are forwarded by the relay agent to the DHCP server which is not available on the local network.

Feature details / Application notes

The DHCP Relay agent does not transparently forward DHCP requests to the DHCP server. It receives the DHCP request from the client and generates a new request which is forwarded to the DHCP server. The relay agent will include additional information in the DHCP request which provides the remote DHCP server with information on where the request is coming from so that the correct IP address can be assigned to the DHCP client.

DHCP Relay	
Enable DHCP Relay Agent	**Enable or disabled DHCP Relay Agent.** **Default is enabled**
Relay information forwarding policy	**If your router receives a packet which already contains an option 82 field, it can take one of the following actions;** • **Replace the option 82 information and forward the frame (default action).** • **Drop—The frame is discarded.** • **Keep—The frame is forwarded with the received option 82 information.** • **Encapsulate—The relay agent is allowed to append its own relay information to a received DHCP packet, disregarding relay information already present in the packet.**
Hop Count	**Set the maximum hop count before packets are discarded.** **Range is 0–255** **Default is 10**
Packet size	**Set maximum size of DHCP packets including relay agent information. If a DHCP packet size surpasses this value it will be forwarded without appending relay agent information.** **Range is 64–1400** **Default is 1400**
Port	**Set the port used to relay DHCP client messages. Range 1–65535** **Default port is 67**
DHCP Relay Interfaces	
Interface	**Select the DHCP relay interface from the drop-down list.**
DHCP Server	**Specify the DHCP server associated with this relay interface.**

GNSS/GPS

Overview

GNSS/GPS allows real-time location tracking of remote devices.

Terminology

GNSS – *Global Navigation Satellite System*
Profile – Defines the data content (language, sentences) and frequency
Streams – Define how, when and to whom the data will be sent using a particular profile

GNSS/GPS	
Enable Location and Steaming Functions	Enable or disable GNSS/GPS functions. Default is disabled
Receiver Disable	Saves power—forces a modem reset causing temporary loss of LTE connection.
GNSS Constellations	• GPS • Galileo • Glonass • Default is GPS
Antenna Select	• GNSS (Dedicated) • Diversity (Shared)
Antenna Type	• Active • Passive Default is Passive
GNSS Data Steaming	
Stream Output Rate	Value is 1–10 Default is 1
Maximum Streaming Connections	Value is 1–64 Default is 10
Vehicle ID	Value is 1–9999 Default is 10
System ID	Used in NMEA stream profiles
Streaming Profile (Add, Edit or Delete)	

ID	Value is 1–16 Default is 1
Name	Specify a name for this profile
Sentence Definition	
Language	• NMEA • TAIP • CSV
Sentences to be Streamed	• NMEA • GGA • RMC • VTG • GLL • GSA • ZDA • GSV • GNS • TAIP • AL • CP • ID • LN • PV (off by default) • ST • TM • CSV • GGA • RMC • VTG • GLL
Include System ID Sentence (NMEA)	Default is enabled

Prepend System ID to all streamed Sentences (NMEA)	Prefix system ID to all streams sentences. Default is disabled
Vehicle ID Reporting (TAIP)	Default is enabled
Sentence Checksum Reporting (TAIP)	Default is enabled
Prepend Newline to all streamed sentences (TAIP)	Default is enabled
Include Column Headers (CSV)	Default is enabled
Movement Triggers	
Moving Time Interval	Specify a moving distance interval. (0 means disabled) Value is 1–3600 seconds Default is 1
Stationary Time Interval	Specify a stationary time interval. Value is 1–3600 seconds Default is 1
Movement Resumption	Specify a movement resumption event. Value is 1–3600 Default is 20 min
Moving Distance Event (M)	Specify a moving distance event. Value is 0–3600 Default is 0 min

Configuration over DHCP (Zero Touch Provisioning)

Zero Touch Provisioning (ZTP) allows your router to be provisioned with configuration and/or software during their initial boot, from a DHCPv4 server. You must configure boot host dhcp under administration to enable ZTP on the router.

Below are the DHCP options used for defining the TFTP server IP address.

DHCP Option	
150	TFTP server IP address. Only the first IP address is used.
66	TFTP server name

siaddr	BOOTP/DHCP header
54	Server Identifier

Note: in decreasing order of precedence

The DHCP options used for the router configuration file.

DHCP Option	
67	Bootfile name
Bootfile name	BOOTP/DHCP header

Note: in decreasing order of precedence

The DHCP option is used for the router ***software and protocol selection.***

DHCP Option			
125	Specify: 1. Software file name to be download 2. Protocol to use to retrieve the bootfile (start-up config)		
Enterprise #	0x00 0x00 0x07 0xae In network byte order (1966 decimal; Perle's Enterprise #)	4 bytes	
Data Length	Length of remaining fields not including this length type	1 byte	
Sub option optional fields			
Sub option code	0x05	1 byte	Software filename to download
Sub option data length	Length of software file name not including this length byte	1 byte	

Software file name	**Name of the file containing the source parameter of an archive download-sw formatted command** **This file contains the source parameter of an archive download-sw formatted command to download the software image. Example:tftp://174.16.21.1/ Router-4.5.G4.img**	**x byte**	
Sub option code	**0x10**	**1 byte**	**Protocol to use when retrieving the bootfile (startup config) and the software file (option 125 sub option 5)**
Sub option data length	**Must be 1**	**1 byte**	**Set this option to 1**
Protocol			**Startup-config filename/ path is specified by option 67 or bootfile in the DHCP header (see above for order of precedence)**
	0=TFTP	**1 byte**	**TFTP:** **Default if no protocol selected** **HTTPS:** **When using HTTPS, you must either disable server certificate validation (no http-client verify server) or load CA certificates on the router.**
	1=HTTP **2=HTTPS**	**1 byte**	**HTTP/HTTPS:** **When using HTTPS, you must either disable server certificate validation (no http-client verify server) or load CA certificates on the router.**

	3=FTP	1 byte	FTP: When using FTP, username is anonymous and the password is <serial# of the unit>@<oem-name>.com Examples Router example: Perle:IRG5541:350-01T0003

DHCP requests including the following options.

DHCP Option	
60 Vendor class identifier	<oem-name>:<serial#> in ASCII Example: Perle:IRG5541:350-01T0003
61 Client identifier	<mac-addr> <ifname> in ASCII Example: 0040.0200.00c0-eth1

SNMP

Simple Network Management Protocol is a standard management protocol which you can use to monitor or configure all aspects of your router.

The router supports configuration and management through SNMP. SNMP Management tools (SNMP client/MIB browser software) can be used to set router configuration parameters and/or view router statistics.

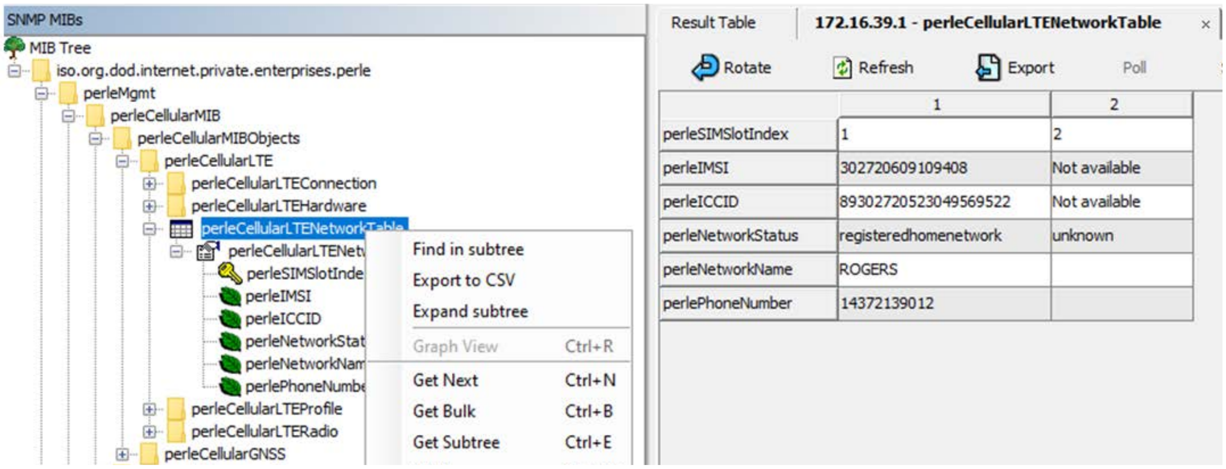
Using SNMP

Before you can connect to the router through an SNMP Management tool or MIB browser, you need to set the following components through another configuration method.

1. Configure a known IP address on the router.
2. Configure the enable check-box for 1/2c, if you are using 1/2c.
3. Configure a user for SNMP version 3 or a community for SNMP version 2c on the router.

Using the SNMP MIB

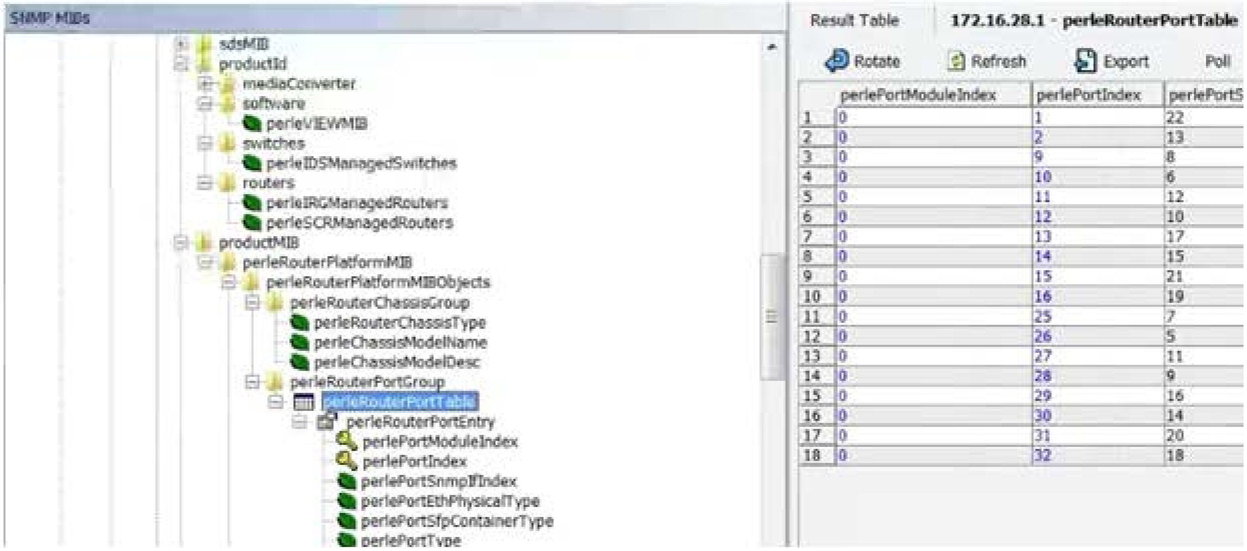
After you have successfully accessed to the router through your SNMP Management tool or MIB browser, load the desired MIB in the MIB browser, expand the MIB folder to see the router's parameter folders.



172.16.39.1 - perleCellularLTENetworkTable

	1	2
perleSIMSlotIndex	1	2
perleIMSI	302720609109408	Not available
perleICCID	89302720523049569522	Not available
perleNetworkStatus	registeredhomenetwork	unknown
perleNetworkName	ROGERS	
perlePhoneNumber	14372139012	

Pre-requisites



172.16.28.1 - perleRouterPortTable

	perlePortModuleIndex	perlePortIndex	perlePortS
1	0	1	22
2	0	2	13
3	0	9	8
4	0	10	6
5	0	11	12
6	0	12	10
7	0	13	17
8	0	14	15
9	0	15	21
10	0	16	19
11	0	25	7
12	0	26	5
13	0	27	11
14	0	28	9
15	0	29	16
16	0	30	14
17	0	31	20
18	0	32	18

- You must load the Perle supplied SNMP MIBs. The router MIBs can be found on the Perle web site.

Terminology

Communities

These are used to define the access level to different groups.

Traps

This is the message which SNMP uses to inform management software when an event has occurred on a managed entity.

- Inform traps are traps which require acknowledgment from the receiver.

Inform

Since SNMP operates over UDP, there is usually no guarantee that a message has been received by the intended recipient. Inform is a type of SNMP trap which requires the receiving host to acknowledge the fact that it has been received and therefore giving the sending entity a confirmation that the message was correctly received.

MIB

Management Information Base. This defines the parameters which SNMP can operate on.

SNMP	
Enable SNMP	Enable or disable service. Default is disabled
Location	Define the SNMP location of your router. Maximum length is 32 characters
Contact	Defines the SNMP contact of your router. Maximum length is 14 characters
Enable SNMP versions 1/ 2c	Enable support for versions 1/2c
SNMP Community (Add, Edit or Delete)	
Name	Name of the community. Maximum length is 63 characters
Permission	Select the permission rights for this community. • Readwrite (rw)—read/write access with this community string • Readonly (ro)—readonly access with this community string

Access	Select the access rights for this community. • Any (Default)—allow access from any IP address • Access—access specified from specific host IP address or network subnets • Add hostname/ IP address • Add network Default is Any
SNMP Listening Address	
Address	By specify an IP address that matches one of your interfaces, you would only be allowing SNMP requests to come on that interface or bridged interface. Enter the IPv4 address.
UDP Port	Enter listening UDP port. Range is 1–65535 Default is 162
Add SNMP Host	
Community User	Add the community user name.
Add Hostname/IP address	IPv4 address/hostname/network of SNMP client/s allowed to contact this router. Note: the host name must exist in the host table within your router.
UDP port	Enter the UDP port number. Range is 1–65535 Default is 162
SNMP version	Select SNMP version. • v2c • v3

Enable Traps and Notifications	
SNMP Notifications	**Notifications to be sent to this user. You may enable as many of the following notification types in the SNMP notification configuration as you want.** • alarms • openvpn • authentication • ospf • bgp • snmp • cellular-gnss - (Model dependent) • network-watchdog • interface IP • lldp • software-update • bridge • entity, • envmon • cellular-gnss • cellular-lte (supported on some models)
SNMP Target Hosts	**Define the SNMP hosts to send traps to.** **IPv4 or IPv6 address of host.** **Type of notification trap or inform.** **Version of trap (v2c or v3)**
Community User	**Name of community user.**
Hostname/IP address	**Specify hosts or host name to receive notifications.**
UDP port	**UDP port the trap host is listening on. (default is 162).**
SMNP Version	**Version of trap:** • v2c • v3 **Default is v2c**
Add View	
OID	**Add OID for this view.**
Include	**Specify fields to include in this view.**
Exclude (optional)	**Exclude this fields from this view.**
Add Group	
Name	**Add the name of the group.**

Authentication Level	Select Authentication Level. • None • Authentication/no privacy • Authentication/privacy
View Access	Select whether this group has View access. • Read-Only • Read-Write
Write View	Specify a write view name.
Add User	
Username	Specify the V3 user.
Group	Specify the group this user belongs to.
Authentication algorithm	• MD5 • SHA
Privacy algorithm	• AES • DES
Authentication/ privacy passwords	Set whether to use password or localized keys for this user.
Authentication password	Enter a authentication password.
Privacy password	Enter a privacy password.
Default Engine ID	The default SNMP engine ID is a unique string used to identify this device. You do not need to specify an engine ID for the device. A default string is generated using Perle's enterprise number and the mac address of your router.
Custom Default Engine ID	Specify your own custom Engine ID for your router.

Alarm Manager

The router can monitor for global and individual port conditions. These alarms can be configured to send alert messages to an;

- External Syslog server
- SNMP trap server
- External alarm device such as a bell, light or other signaling device via the router’s built-in dry contact alarm relay.
- contact alarm relay

Port Status Monitoring Alarms

- Link Fault Alarm (ie: loss of signal)
- Port not operating alarm (failure upon start up tests)

Global Status Monitoring Alarms

Internal temperature alarm***Alarm Relay***

The alarm relay is an additional method for indicating that an alarm condition exists. Utilizing the router’s built-in dry contact alarm relay, a circuit can be designed that drives a light or speaker when the contacts on the alarm are open or closed. The router’s contact relay has a default alarm state which is either a normally open or closed condition. Please refer to the hardware installation guide for your particular model.

The router upon power up, remains in this default alarm state until the boot process has completed. Once the boot cycle has completed and finds that no error conditions exist, the router’s OS “energizes” the relay. Should an alarm condition occur, the router’s OS will “de-energize” the relay. You also have the ability to change the setting of the default alarm condition to either “de-energize” (default) or “energize”.

For each alarm, there is an associated severity level as follows:

Critical—Severity 1

- Syslog equivalent is “Emergency”

Major—Severity 2

- Syslog equivalent is “Error”

Minor—Severity 3

- Syslog equivalent is “Warning”

Informational—Severity 4

- Syslog equivalent is “Informational”

Common Settings	
Alarm Action Settings	
Relay (major)	• **Energized** • **De-energized**

Relay (minor) (only apples to models that support GPIO - GPIO must be set to output)	• Energized • De-energized
Port Alarms	
Port Alarms (Add, Edit or Delete)	
Profile Name	Provide a alarm profile name.
Selected Alarm Relay	• none • major • minor
Not Operational	
Monitor	Enable or disable to monitor for not operational alarms.
Action	Should this action occur: • Send a Syslog message • Send a Trap messageSend a Relay message
Link Fault	
Monitor	Enable or disable to monitor for not operational alarms.
Action	Should this action occur: • Send a Syslog message • Send a Trap messageSend a Relay message
Not Forwarding	
Monitor	Enable or disable to monitor for not operational alarms.
Action	Should this action occur: • Send a Syslog message • Send a Trap messageSend a Relay message
Assign Alarm Profiles to Ports	Assign interfaces to Alarm profiles.
Facilities	

IGN Contact 1 - (supported on IRG 5521/5521+, 5410/5410+ and 5540/40+/5541/5541+)	
Description	**DC-POWER: IGN**
Severity Level	• **None** • **major** • **minor**
Analog	
Enable Alarm	**Enable alarm for analog operations.**
Actions	**Monitor for these conditions.** • **LTE Data Disconnect** • **Syslog** • **Trap** **Action for Relay on these conditions** • **none** • **major** • **minor**
High Threshold	**Set high threshold 0–2147483.647**
Low Threshold	**Set low threshold 0–2147483647**
GPIO (Contact 2)	
Description	**DC-POWER: GPIO**
Severity Level	• **None** • **major** • **minor**
Analog	
Enable Alarm	**Enable alarm for analog operations**

Actions	Monitor for these conditions. • LTE Data Disconnect • Syslog • Trap Action for Relay on these conditions • none • major • minor
High Threshold	Set high threshold value. Values 0–2147483.647
Low Threshold	Set low threshold value. Values 0–2147483647
Digital	
Enable Digital Contact Alarm	Enable digital contact alarm
Trigger	Monitor for Trigger condition • Open • Closed Action for on Trigger condition • LTE Data Disconnect • Syslog • Trap Relay • none • major • minor
Pulse Counter	
Enable Alarm	Enable alarm for Pulse Counter operations
Starting Trigger	Enter the start trigger value. Value from 1–65535
Repeat Trigger	Enter the repeat trigger value. Value from 1–65535

Actions	Action for on Trigger condition • LTE Data Disconnect • Syslog • Trap Relay • none • major • minor
Description	AUX-IO: Digital Input B
Severity Level	• None • major • minor
Digital	
Enable Digital Contact Alarm	Enable digital contact alarm
Trigger	Monitor for Trigger condition • Open • Closed Action for on Trigger condition • LTE Data Disconnect • Syslog • Trap
Pulse Counter	
Enable Alarm	Enable alarm for Pulse Counter operations.
Starting Trigger	The start trigger is how many pulses or transitions you want before the alarm is triggered. If you just have this set then it will be a one time alarm, until you manually clear the counter.
Repeat Trigger	You can optionally enable the Repeat Trigger, which means whatever count you put here, it will trigger an alarm every n occurrences after the starting trigger count.

Actions	Action for on Trigger condition • LTE Data Disconnect • Syslog • Trap Relay • none • major • minor
Standby Mode	
Enable Alarm	Enable the alarm if standby condition exists.
Actions	Specify a actions for Standby condition. • LTE Data Disconnect • Syslog • Trap
	Relay • none • major • minor
Facilities	
LED	When enabled, the power LED will display an orange light if the power supply is not working or powered off.
Action	Should this action occur: • Send a Syslog message • Send a Trap message • Send a Relay message
Internal Temperature	
Primary Range	
High Threshold	Set the high threshold. -150°C—300°C
Low Threshold	Set the low threshold. -150°C—300°C

Action	Should this action occur: - LTE Data Disconnect - Send a Syslog message - Send a Trap message
Selected Alarm Relay	- none - major - minor
Secondary Range	
High Threshold	Set the high threshold. -150°C—300°C
Low Threshold	Set the low threshold. -150°C—300°C
Action	Should this action occur: - LTE Data Disconnect - Send a Syslog message - Send a Trap message
Selected Alarm Relay	- none - major - minor
Standby Mode	
Enable Alarm	Enable or disable the alarm.
Action	Should this action occur: - LTE Data Disconnect - Send a Syslog message - Send a Trap message
Selected Alarm Relay	- none - major - minor

QOS (Quality of Service)

By default, your router treats all internet traffic equally—all users, ports, applications, sources, and destinations. However, there may be times when it is necessary to prioritize the internet traffic for specific users or devices. Quality of Service (QoS) technologies accomplishes this by providing differentiated handling and capacity allocation to specific flows in network traffic—it manages network resources to reduce packet loss as well as lower network jitter and latency. A policy map essentially defines a policy stating what happens to traffic that has been classified using class maps and ACLs.

Your router provides you with three mechanisms for configuring QOS.
1) Priority-queuing—packets are placed in queues, high priority packets are sent first.
2) Rate-control—rate control is a classless policy that limits the packet flow to a set rate. Traffic is filtered based on the expenditure of tokens. Tokens roughly correspond to bytes. Short bursts can be allowed to exceed the limit. On creation, the Rate-Control traffic is stocked with tokens which correspond to the amount of traffic that can be burst in one go. Tokens arrive at a steady rate, until the bucket is full.
3) Traffic-limiting—traffic limiting is a mechanism that can be used to "police" incoming traffic. The mechanism assign each traffic flow a bandwidth limit. All incoming traffic within a flow in excess of the bandwidth is dropped.This policy can be applied to both ingress and egress packets.

With QoS, you can change your network so that certain traffic is preferred over other traffic when it comes to bandwidth—the speed of the link in bits per second, delay—the time it takes for a packet to get from a source to the destination and back, jitter—the variation of one-way delay in a stream of packets and loss—the amount of lost data when packets get dropped. What you need to configure, however really depends on the applications that you use. Applications that benefit from defining QOS rules are those that rely on the timely delivery of real–time data packets, for example:

- Video-on-demand
- Voice over IP (VoIP)
- Internet Protocol television (IPTV)
- Streamed media
- Video conferencing
- Online gaming

Feature Details / Application Notes

The traffic classification process consists of these steps:
1. Create a class map by configuring an ID, description, and associated match commands for that class map. A set of match commands are match criteria related to Layer 3 and Layer 4 traffic classifications or Layer 7 protocol classifications.
2. Create a policy map which refers to the class map and identifies a series of actions to perform based on the traffic match criteria.
3. Activate the policy map, then attach it to a specific interface by using the service-policy command.

Terminology

A class map defines a traffic classification—a network that is of interest to you.
Class Map—contains the following components:

- Class ID
- Description

- One or more match commands that define the match criteria for the class map
- Instructions on how your router will evaluates match commands when you specify more than one match command in a class such as match any, match-all
- match criteria related to Layer 3 and Layer 4 traffic classifications or Layer 7 protocol classifications

Policy Map— refers to the class maps and identifies a series of actions to perform based on the traffic match criteria.

Service Policy—assigns a traffic policy to an interface.

QOS	
Class Maps (Add, Edit and Delete)	
ID	**Configure a class number.** **Values are 1-4094** **Priority queues use classes 1 -7**
Description	**Configure a description for this class.**
Match Rules	
Class Map Name	**Configure a name for this classification.** **Classification is the separation of packets into traffic classes.** **Configure your router to take a specific action on the specified classified traffic, such as policing, marking down and other actions.**
Class Map Description	**Specify a class-map match-name description.**
Match Type—Other	• **Match** • **Mark—Mark applied bu policy-routing, Values are (1-4294967295)** • **Vlan (1-4000)**

Match Type—Interface	**• Match interface** **◦ BVI <1–9999>** **◦ wwan0** **◦ wlan1** **◦ wlan2** **◦ Dialer <0–15>** **◦ Ethernet <1–5>** **◦ OpenVPN-Tunnel <0–999>** **◦ Tunnel <0–999>**
Match Type—Ethernet	**• Match** **◦ Ethernet source—MAC address** **◦ Ethernet destination—MAC address** **◦ Type—(1–65535)**
Match Type—IP	**• IP** **◦ source IP address and wildcard bits** **◦ IP source port TCP/UDP (1–65535)** **◦ destination IP address and wildcard bits** **◦ destination port TCP/UDP (1-65535)** **◦ IP protocol** **◦ IP Max Length** **◦ dscp—default, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef, dscp, default, (0-63)**

Match Type—IP	**• max length (0-65535)** **• protocol** **•ah, dccp, dsr, egp, eigrp, encap** **• esp, etherip, ggp, gre, hmp, icmp, idpr, igmp, igp, ip, ipip, ipv6, ipv6-frag, ipv6-icmp, ipv6-nonxt, opts, ipv6-route, isis, l2tp, manet, mpls-in-ip, narp, osfo, pim, rdp, roch, rsvp, sctp, osfo, pim, rdp, roch, rsvp, sctp, sdrp, shim6, skip, tcp, udp, udplite, vrrp, xns-idp, IP protocol number <0–255>** **• tcp-flags** **• ACK** **• SYN** **• VLAN 1-4000>** **• Mark 1-214748748364**
Match Type—IPv6	**• source IPv6 address and netmask** **• IPv6 source port (1–65535)** **• destination IPv64 address and netmask** **• destination port (TCP/UDP)** **• dscp—default, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef**
Match Type—IPv6	**• dscp** **• default** **• (0-63)** **• max length (0-65535)** **• protocol** **• ah, dccp, dsr, egp, eigrp, encap, esp, etherip, ggp, grep, hmp, icmp, idpr, igmp, igp, ip, ipip, ipv6, ipv6-frag, ipv6-icmp, ipv6-nonxt, opts, ipv6-route, isis, l2tp, manet, mpls-in-ip, narp, osfo, pim, rdp, roch, rsvp, sctpdrp, shim6, skip, tcp, udp, udplite, vrrp, xns-idp, 0-255,** **• tcp-flags** **• ACK** **• SYN** **• VLAN 1-4000>** **• Mark 1-214748748364**

Policy Map	
Policy map name	Configure the policy map name.
Policy Map Type	Configure the policy map type. • default • priority queue • rate-control • traffic limit
Description	Configure a description for this policy map.
Bandwidth (Kbps)	Configure the available bandwidth in Kbps for this policy. Default Auto: matching interface speed
Policy Map Class (Add, Edit, Delete)	
Class	Configure a name for this classification. Classification is the separation of packets into traffic classes. You configure your router to take a specific action on the specified classified traffic, such as policing, marking down and other actions. Values <1-4096>
Description	Description for this policy.
Bandwidth (kbps)	Specifies the base guaranteed bandwidth for a traffic class in Kbps or in percent. Default 100 % of bandwidth specified for the whole policy or 100% physical interface rate.
Burst (kbps)	Set the burst size for a traffic class in kbytes. Default is 15 Kbytes
Ceiling (kbps)	Set bandwidth limit for this class, the maximum amount of bandwidth a traffic class ca consume when excess bandwidth is available. (1-200,000 kbps) or percent (1-100)
Number of flows	Specify the queue type. Values are (1-4294967295) Default is 1024

Delay interval	Interval in milliseconds to measure the delay. Values are (1-4294967295) Default 100ms
Byte deficit	The byte deficit in bytes. Values are (1-4294967295) Default 1514 bytess
Enable min. queue delay	The minute queue delay in milliseconds Values are (1-4294967295) milliseconds
Priority	Priority for queue. Values are 0-7
Max. queue size packets	Maximum for queue size in packets. Values are (1-4294967295) packets
Queue type	Specify the queue type: • First-In-First-Out • Stochastic fair queue • Flow queue codel • Priority queue (DSCP) • Random early detection
DSCP	DSCP value is 0-63
Interface Policy Map	
Map policies to Interfaces (Add, Edit, Delete)	Select interface from the drop-down box
Policy map to input of interface	Select interface from the drop-down box
Policy map to output of interface	Select interface from the drop-down box

LLDP (Link Layer Discovery Protocol)

LLDP, defined in the IEEE 802.1AB standard, is a Layer 2 protocol that allows network devices to advertise their identity and capabilities on a LAN. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers, and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP should be enabled in a multi-vendor network.

Feature Details / Application Notes

LLDP provides the following benefits:

- simplifies the use of network management tools in a multi-vendor environment
- accurate discovery of physical networks allows for easier troubleshooting
- enables discovery of devices in multi-vendors environments
- LLDP uses standard TVLs attributes that contain a type, length, and value descriptions.

LLDP	
Enable LLDP	Enable or disable LLDP.
Enable neighbor discovery logging	Enable LLDP neighbor discovery logging. Default is off.
Tx Hold Multiplier	Configure a value for the LLDP hold multiplier. This is the time to cache learned LLDP information before discarding, measured in multiples of the Timer parameter. For example, if the Timer is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds. Default is 4 Values 2-10
Min interval between successive LLDP SNMP notifications	Minimum interval between LLDP SNMP notifications. Default is 5 seconds Value is 5-3600 seconds
Delay for LLDP initialization on any interface	Sets the delay (in sec) for LLDP initializations on any interface. Default is 2 seconds Value 1–10 seconds
Rate at which LLDP packets are sent (secs)	Specify the rate at which LLDP packets are sent. This parameter is used with the TX Hold multiplier parameter to determine when LLDP packets are discarded. Default is 30 seconds Values are 5–32768 seconds
Delay between successive LLDP frame transmissions (sec)	Configure the amount of time in seconds that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB. Default is 30 seconds Values are 1-8192 seconds

Selection for LLDP TLVs to send	Select the LLDP TLVs to send. • MAC PHY configuration and status TLV • Port Description TLV • System Name TLV • Management Address TLV • System Capabilities TLV • Maximum frame size TLV • System Description TLV Default is all TLVs are sent Maximum management addresses are 8. First default management addressees for IPv4 and IPv6 are automatically selected by LLDP.
LLDP Interface Settings	
Enable LLDP Transmission	Enable LLDP transmission on this interface.
Enter LLDP Reception	Enable LLDP reception on this interface.
Max number of LLDP neighbors	Specify maximum number of LLDP neighbors for this interface.
Selection for LLDP TLVs to send	Select the TLVs to send. • MAC PHY configuration and status TLV • Port Description TLV • System Name TLV • Management Address TLV • System Capabilities TLV • Maximum frame size TLV • System Description TLV

STP (Spanning Tree Protocol)

Spanning Tree is a protocol that ensures a loop free topology for an Ethernet local area network.If loops are detected, the protocol blocks one of the paths so that the loop is eliminated.

Feature Details / Application Notes

Spanning Tree Protocol (STP)—A layer 2 protocol which identifies and eliminates loops in your network. It is detailed in the IEEE
RSTP Rapid Spanning Tree Protocol (RSTP)—RSTP (IEEE 802.1w) is inter-operable with STP and takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree. Reconfiguration of the spanning tree can occur in less than 1 second

Multiple Spanning Tree Protocol (MSTP)—MSTP Originally defined in IEEE 802.1s and now incorporated IEEE 802.1Q-2014, defines an extension to RSTP for use with VLANs. The Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

STP	
Bridge Spanning Tree Settings	
Mode	**• RSTP • MSTP • STP Default is disabled**
Enable Loopguard by default on all ports	**Configures the Spanning Tree Protocol (STP) loop guard feature which provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. Default is Disabled**
Forward time	**Configures the forward delay timer. The forward delay timer is the time interval spent in the listening and learning state. Values are 4–30 seconds Default is 15 seconds**
Hello time	**Configures the hello timer. The hello timer is the time between each bridge protocol data unit (BPDU) sent on a port. Values are 1–10 seconds Default is 2 seconds.**
Maximum age	**Configures the max age timer to control the maximum length of time that passes before a bridge port saves its configuration BPDU information. Value are 10–100000 seconds Default is 20 seconds**

Priority	Every router participating in a Spanning Tree Protocol (STP) network is assigned with a numerical number called a bridge priority value. Priority values decide who will be elected as root.
	You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. You set the priority value argument to 0 to make therouter root. Default is 32768
Configure router as root	Configures the root bridge.The root bridge is the bridge with the smallest (lowest) bridge ID.
Transmit hold count	Controls the number of BPDUs sent before pausing for 1 second. Range is 1–10 seconds Default is 6 seconds
Maximum hops	Configures the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded. Value are 6–40 Default is 20
Aging Time	Configures the timeout period in seconds, for aging out dynamically learned forwarding information. Values are 1–1000000 in seconds Default is 300 seconds
Multiple Spanning Tree—MSTP	
Set MST configuration name and revision	Enables or disables name and revision.
Configuration name	Configures the name of the region.
Configuration revision	Configures the revision. This setting must be the same for all MSTP switches in the same MST region.

MST instance (Add, Edit, Delete)	Configures MST instances for the region. Each region can have multiple instances. Map VLANs to an MST instance (0-63).
	Instance 0 cannot be deleted and is used to map/unmapped VLANs to instance 0. Each instance has a VLAN or range of VLANs which is associated with it. Values are 0-4000
Cost	Configures the spanning tree port cost for an instance. You assign lower values to interfaces that you want selected first. Values are 0–200000000
Port priority	Configures the spanning tree port priority for an instance. If a loop occurs, MST uses the port priority when selecting an interface to put into the forwarding state. Assign lower priority values to the interfaces you want selected first. Values are 1-240 (in increments of 16) Default is 128
Bridge Spanning Tree Settings	
Enable BPDU guard	Don’t accept BPDUs on this interface. Default is Disabled
Enable BPDU filter	Don’t send or receive BPDUs on this interface. Default is Disabled
Enable Mcheck	Automatically transition to STP mode from RSTP/MTSP
Guard mode	• None • Root • Loop • Topology change Default is none
Link Type	• Auto—this interface is point to point if configured for full duplex • Point-to-point • Shared Default is Auto

Portfast mode	A spanning tree normal port is one that functions in the default manner for spanning tree. Under normal circumstances it will transition from the Listening, Learning, Forwarding stages based on the default timers.
Portfast mode	PortFast mode causes a port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states. STP enabled ports that are connected to devices such as a single switch, workstation, or a server can access the network only after passing all these STP states. Some applications need to connect to the network immediately, else they will timeout. Disable—go through normal learning/forwarding and blocking states. (Default) Network—Interface goes into forward state immediately. Portfast network protects against loops by detecting unidirectional links in the STP topology. Edge—is used to configure a port on which an end device is connected such as a PC. All ports directly connected to end devices cannot create bridging loops in the network. Therefore, the edge port directly transitions to the forwarding state, and skips the listening and learning stages. However, the specific command configures a port such that if it receives a BPDU, it immediately loses its edge port status and becomes a normal spanning-tree port.
Port Priority	Configures the spanning tree port priority for an instance. If a loop occurs, STP uses the port priority when selecting an interface to put into the forwarding state. Assign lower priority values to the interfaces you want selected first. Values are 1-240 (in increments of 16). Default is 128
Port path cost	Configures the spanning tree port cost for an instance. You assign lower values to interfaces that you want selected first. Values are 0–200000000

Local Port Buffering

The Local Port Buffering feature allows you to see data received on the IOLAN’s serial ports.

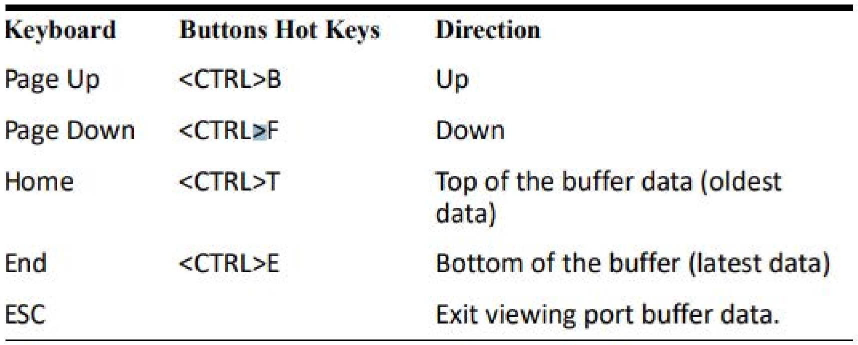
To view the local port buffer for a particular serial port, you must:

Connect to the device on that serial port by Telnet or SSH.

The serial port(s) must be set to the Console Management profile

Once you have established a connection to a device, you can enter the View Buffer String at any time to switch the display to the content of the port buffer for that particular serial port. To return to communicating to the device, press the ESC key and the communication session will continue from where you left off.

To navigate through the port buffer data, the following chart illustrates the keyboard keys or “hot keys”
that can be used to view the port buffer data. Press the ESC key and to continue to communicate with the
device on that particular serial port.



Keyboard	Buttons Hot Keys	Direction
Page Up	<CTRL>B	Up
Page Down	<CTRL>F	Down
Home	<CTRL>T	Top of the buffer data (oldest data)
End	<CTRL>E	Bottom of the buffer (latest data)
ESC		Exit viewing port buffer data.

Remote Port Buffering

The Remote Port Buffering feature allows data received from serial ports on the IOLAN to be sent to a remote server on the LAN. The remote server, supporting Network File System (NFS), allows administrators to capture and analyse data and messages from the serial device connected to the IOLAN serial port. Remote Port Buffering data can be time stamped. The data is transmitted to an NFS server where a unique remote file is created for each serial port using the configured serial port Name for the file name. If the serial port Name parameter is left blank, the IOLAN will create unique files using the IOLAN’s Ethernet MAC address and serial port number. It is recommended that a unique NFS directory and serial port name be configured if multiple IOLANs use the same NFS host for Remote Port Buffering.

The filenames will be created on the NFS host with a .DAT extension.

The data that is sent to the remote buffer file is appended to the end of the file, so you will want to create a size limit on the file on your remote NFS host, to keep the buffer file size from becoming too large for your system.

Pre-requisites

- When using Trueport Service Type, Trueport client software must be installed on the client PC.

Restrictions / Limitations

- Port Buffering is not supported on all Service Types.

Port Buffering

Serial Port Data Buffering

Enable Local Buffering	Enables/disables local port buffering on the router. Default is disabled
View Buffer string	The string used by a a session connected to a serial port to display the port buffer for that particular serial port. Data Options are up to an 8 character string. You can specify control (unprintable) codes by putting the decimal value in angle brackets < > (for example, Escape b is <027>b). Default is ~view
Enable Remote (NFS) Buffering	Enables/disables port buffering on a remote system. When you enable this option, you have the ability to save the buffered data to a file(s) (one file is created for each serial port) and/or send it to the Syslog host for viewing on the Syslog host's monitor. Default is Disable
NFS Host	The NFS host that the router will send data to for its Remote Port Buffering feature. The router will open a file on the NFS host for each serial port configured for Console Management, and will send serial port data to be written to that file(s). Default is None
NFS Directory	The directory and/or subdirectories where the Remote Port Buffering files will be created. For multiple routers using the same NFS host, it is recommended that each router have its own unique directory to house the remote port log files. Default is device_server/portlogs
Enable Port Buffering to Syslog	When enabled, buffered data is sent to the syslog host to be viewed on the host's monitor.
Level	Choose the event level that will be associated with the "port buffer data" in the syslog. Data options are Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug. Default Level is Info Default is disabled
Advanced Port Buffering	
Add Time Stamp	Enable/disable time stamping of the serial port buffer data. Default is disabled
Enable Key Stoke Buffering	When enabled, key strokes that are sent from the network host to the serial device on the router's serial port are buffered. Default is disabled

Remapping of Trueport Baud Rate

Trueport Baud Rate	
Mapping	
Trueport	**Actual Baud Rate**
50	**300 or above** **Default is 57600**
75	**300 or above** **Default is 75**
110	**300 or above** **Default is 115200**
134	**300 or above** **Default is 230400**
150	**300 or above** **Default is 150**
200	**300 or above** **Default is 200**
300	**300**
600	**600**
1200	**1200**
1800	**1800**
2400	**2400**
4800	**4800**
9600	**9600**
19200	**19200**
38400	**38400**

Advanced—Configures those parameters that are applicable to specific environments. You will find modem and Trueport configuration options, in addition to others, here.

Advanced Serial Options	
Process Break Signals	Enables/disables proprietary inband SSH break signal processing, the Telnet break signal, and the out-of-band break signals for TruePort. Default is disabled
Flush Data Before Closing Serial Port	When enabled, deletes any pending outbound data when a port is closed. Default is disabled
Deny Multiple Network Connections	Allows only one network connection at a time per serial port. Application accessing a serial port device across a network will get a connection (socket) refused until: • All data from previous connections on that serial port has drained • There are no other connections • Up to a 1 second interconnection poll timer has expired Enabling this feature automatically enables a TCP keep-alive mechanism which is used to detect when a session has abnormally terminated. The keep-alive is sent after 3 minutes of network connection idle time. Applications using this feature need to be aware that there can be some considerable delay between a network disconnection and the port being available for the next connection attempt, allowing any data sent on prior connections to be transmitted out of the serial port. Application network retry logic needs to accommodate this feature. Default is disabled
Data Logging	When enabled, serial data will be buffered if the TCP connection is lost. When Logging the TCP connection is re-established, the buffered serial data will be sent to its destination. If using the Trueport profile, data logging is only supported in Lite Mode. Default is disabled Note: A kill line or reboot of the router causes all buffered data to be lost.
Buffer Size	Buffer size is 1–2000 Mb. Default size is 4 Mb

Monitor Connection Status	
Status Interval	**Specify how often, in seconds, the router will send a TCP keep-alive to services that support TCP keep-alive.** **Default is 180 seconds**
Retry Interval	**The seconds between interval attempts.** **Default is 5 seconds**
Retry (attempts)	**The number of TCP keep-alive retries before the connection is closed.** **Retries 1-32767** **Default is 5**

NTP Server

Network Time Protocol (NTP) is used as a method of distributing and maintaining synchronization of time information between nodes in a network. NTP server uses UTC (Universal Coordinated Time). When initially launched, it can take NTP as much as 5 minutes to obtain an accurate time.This is due to the algorithm used to determine what NTP master(s) your router should synchronize with. NTP will not synchronize with nodes whose time is significantly different even if its stratum is lower. During this “settling” period, your router may not have the correct time.

Terminology

SNTP—Simple Network Time Protocol

A subset of NTP

Uses the same protocol.

SNTP can only receive the time from NTP servers and cannot be used to provide time services to other systems.

NTP Server

A node with an accurate clock source which is used to disseminate the time information to the other nodes in the network. A network may contain multiple NTP servers. The client will attempt to determine what the best clock source is and use it.

NTP Client

A node which receives its time information from an NTP Server (or an NTP peer).

UDP—User Datagram Protocol

This is the underline protocol used by NTP and SNTP for packet transmission.

Stratum

This defines the NTP. The highest stratum is 1. It is reserved for atomic clocks, GPS clocks or radio clock which generates a very accurate time. This type of time source is defined as the “Authoritative time source”. The stratum defines how many hops a node is from the “authoritative time source”. Stratum x nodes are synchronized to stratum x-1 nodes. Stratum numbers range from 1 to 15.

NTP Settings	
Enable NTP (Network Time Protocol	**Some parameters may not be available on some versions of the firmware or models.** **By default NTP is disabled globally.**
Internal Time Sources	**Select the time sources.** • **Cellular system time** • **GNSS (GPS)GNSSGNSS**
Enable NTP on management Interfaces	**Select interfaces from the drop-down list.**
Advanced NTP Settings	
Authentication time sources	**Authenticate with the time sources.**
Enable logging	**NTP messages will be logged.**
Auto-negotiate broadcast delay	**By default, your router will set broadcast delay to Auto-negotiate. Select the auto-negotiate broadcast delay off if you wish to set your own broadcast delay time in microseconds.**
Broadcast delay (ms)	**Broadcast delay time is the estimated round-trip delay between the broadcast NTP server and your router. Microseconds are from 1-999999.**
Act as a master NTP clock	**Sets your router to act as the master clock source providing time to NTP clients.**
Stratum	**Specify how far your router is away from the Authoritative Time Source.** **The highest stratum is 1. It is reserved for atomic clocks, GPS clocks or radio clock which generates a very accurate time. This type of time source is defined as the “Authoritative time source”. The stratum defines how many hops a node is from the “authoritative time source”. Stratum x nodes are synchronized to stratum x-1 nodes.** **Stratum numbers range from 1 to 15**

NTP Server / IP address

Hostname / IP address	Enter the hostname or IPv4/IPv6 address of the NTP Server/ Peer. • IPv4—A.B.C.D • IPv6—1:2:3:4::5
Resolve hostnames to	• IPv4 or IPv6 • IPv4 • IPv6 Default is IPv4 or IPv6
Type	Server, a reliable clock source that is used to provide time to NTP clients. Peer command is set between two clients. The assumption is that neither one has authority (equal, peering) to know what time it is, but the two will work on getting in sync. Both sides will actually shift their clock (maximum jump of two minutes at a time, so if clocks are way different then it'll take a while to sync towards each other. However, if there is no NTP server configured on the network for the peer clients to get the correct time, the time will be wrong. NTP peer mode is intended for configurations where a group of clients operate as mutual backups for each other. If one of the devices loses a reference source, the time values can flow from the surviving peers to all the others. Each client operates with one or more primary reference sources, or a subset of reliable NTP secondary servers. When one of the clients lose all reference sources or simply cease operation, the other peers automatically reconfigures so that time values can flow from the surviving peers to others.
Use authentication key	Configure an authentication key that will be used between the server and NTP clients. You must configure the same authentication key on your NTP clients.
Add key	Index—add index (1-65534) Key—add numeric value for key Trust this key—enable or disable
Prefer this server/ peer	Select this option to prefer this NTP source over another. A preferred server/peer's responses are discarded only if they vary greatly from the other time sources. Otherwise, the preferred server/peer is used for synchronization without consideration of the other time sources.
Advanced Options	

NTP version	Version 1–4 are supported. Default is 4
Minimum poll interval	4(16s), 5(32 s), 6 (1m, 4s), 7(2m,8s), 8(4m, 16s), 9(8m, 32s), 10 (17m, 4s), 11 (34m, 8s). Default is 6
Maximum poll interval	4(16s), 5(32 s), 6 (1m, 4s), 7(2m, 8s), 8(4m,16s), 9(8m, 32s), 10 (17m, 4s), 11 (34m, 8s). Default is 10
NTP Authentication Keys	
Index	Specify a index number from 1 to 65534.
Authentication algorithm	• SHA256 • SHA512 • SHA1 • MD5
Key	Specify a key. Value 1-65534
Trust this key	Enable or disable to trust this key.
NTP Broadcast / Multicast	
Client	
Authentication peers	Enable to authenticate peers.
Broadcast Client Select Management interfaces	Configure the router’s NTP broadcast client to receive broadcasts from other devices.
Multicast Client Select Management VLAN interfaces	Configure the router’s NTP multicast clients to receive multicasts from other devices.
Add Multicast address Interface	
Multicast address	Specify a IPv4 or IPV6 multicast address
Server	

Select an interface	
Add Broadcast/Multicast Address	
Type	• Broadcast server • Multicast server
Broadcast address	Enter a broadcast address to broadcast to the entire local network.
Use authentication key	Enter a number from 1 to 65534.
NTP version	Version 1–4 are supported. Default is 4
Minimum poll interval	4(16s), 5(32 s), 6 (1m, 4s), 7(2m,8s), 8(4m, 16s), 9(8m, 32s), 10 (17m, 4s), 11 (34m, 8s). Default is 6

Container Management

Your router supports software management containers. Simply put, a software container bundles application’s code together with the related configuration files and libraries, and all dependencies required for a application to run. By using our container management system, you are able to create, deploy, and scale containers within your router.

Container Management	
Container Network (Add, Edit, Delete)	
Network Name	Enter the container network name.
Description	Enter a description for this container network
Bridge Interface	Select the bridge interface that is associated with the container network.
DHCP Option	Select to use DCHP option or disabled. • Disabled • DHCP • DHCPv6
Add Container Private Registry Credential	

Private Registry Type	**• Secure • Insecure Secure—Private registries incorporate security and privacy into enterprise container image storage. Insecure-Add to list of registries which do not require certificates or authorization. Note: Setting registry as Insecure means that container management will disregard any security for your registry. This is very insecure and is not recommended. It exposes the registry to trivial man in the middle (MITM) attacks. Only use this setting for isolated testing or in a tightly controlled environment.**
Username	**Enter the username for access to this container.**
Password	**Enter the password for this container.**
Import Certificates and Keys	
Transfer method	**Select transfer method from: • Browser • FTP • HTTP • HTTPS • SCP • SFTP • TFTP**
Registry	**Use (-) dash to use the default docker registry**
File type	**Specify the type of certificate to import: • CA Certificate • Certificate for IOLAN • Private Key for IOLAN**
Start Import	**Select the file to import.**
Installed Files	**Delete or view installed files.**

Security

User Accounts

In order to manage the router users have to login. One of the methods which can be used to login involves a username and password. Add names to the router's internal users' database or if using an external authentication service such as RADIUS or TACACS+, add the user names there. Some user account configuration parameters may be different on some models or running software.
The user will be assigned one of two authorization levels.

- User EXEC—Able to perform most monitoring functions but not allowed to perform configuration of the router.
- Privileged EXEC—Is able to perform all supported operations on your router.

Another method you can use is two factor authentication which will require you to input a verification code to be sent to you either as a SMS message or an email after you have logged in. Some email programs require that you create a third party app password to be used on the router as the email user password. See the documentation for your email program on how to create a password to be used on less secure apps or third party apps. When using SSH with two factor authentication, you must select Keyboard Interactive as the first method of Authentication.

User Sessions

The Sessions tab is used to configure specific connections for users who are accessing the network through the 's serial port. Users who have successfully logged into the router (User Service set to DSprompt) can start up to four login sessions on network hosts. Multiple sessions can be run simultaneously to the same host or to different hosts. Users can switch between different sessions and also between sessions on the router using Hotkey commands. Users with Admin or Normal privileges can define new sessions and use them to connect to Network hosts; they can even configure them to start automatically on login into the router.

Feature details / Application notes

Passwords can be up to 25 characters long. Blank passwords are also supported. Passwords will be stored in the local database using encryption. This is a one way encryption scheme. There is no way to extract the clear password from the stored value. When viewing the text configuration of your router, the password will be displayed in its encrypted form in ASCII printable characters. A user can cut and paste this information into the configuration of another router. This allows the administrator to copy users from one router to another without knowing what their passwords are.

Advanced User Session features are Serial Services, Advanced features such as session length, the hot key for switching between sessions, callback etc, Lastly, Serial port Access for assigning read, write and read/write access to your serial ports.

Users

Add, Edit, Delete User	Specify a username.
Privilege Level	- No Admin, CLI only - Operator - Dashboard - Diagnostics - Logging - Monitor Statistics - Reset - RESTful API - Admin/Web User
Password	Passwords can be up to 25 characters long. Blank passwords are also supported.
Enable OpenVPN for this user	Enable or disable OpenVPN for this user.
User Access Schedule	Enter can access the routerIOLAN at these days and times. Schedule 1–10 Enter Start time/End time/Days of the week
Two Factor authentication	Enable Two Factor authentication. You can specify whether to use SMS or Email for authentication. If you use EMAIL, you must enable and configure email settings under System/Email. If you use SMS, you must configure (SMS) under System/SMS.
Format	- SMS - Email
Phone Number	Specify the phone number to receive the verification code.
Email address	Specify the email address to send the verification code.

Serial Configuration	
Service	• DSPrompt • Telnet • Connect Host • TCP port (default 23) • SSH • Connect Host • TCP port (default 22) • Rlogin • Connect Host • TCP port (default 513) • SLIP • IPv4 address • IPv4 subnet mask • MTU • Routing • Enable VJ compression • PPP • IPv4 address • IPv4 subnet mask • IPv6 interface identifier • MTU • Routing • Enable VJ compression • TCP-Clear • Connect Host • TCP port • SSL-Raw • Connect Host • TCP port
Advanced	
Idle Timeout	The amount of time, in seconds, before the router closes a connection due to inactivity. The default value is 0 (zero), meaning that the Idle Timer will not expire (the connection is open permanently). The User Idle Timeout will override all other Serial Port Idle Timeout parameters. Range is 0–4294967 Default is 0

Session Timeout	The amount of time, in seconds, before the router forcibly closes a user’s session (connection). The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The User Session Timeout will override all other Serial Port Session Timeout parameters. Range is 0-4294967 Default is 0
Enable Callback	When enabled, enter a phone number for the router to call the user back (the Enable Callback parameter is unrelated to the Serial Port Remote Access PPP profile Dial parameter. Note: the router will allow callback only when a user is authenticated. If the protocol over the link does not provide authentication, there will be no callback. Therefore, when the Serial Port profile is set to Remote Access (PPP), you must use either PAP or CHAP because these protocols provide authentication. The router supports another type of callback, Roaming Callback, which is configurable when the Serial Port profile is set to Remote Access (PPP). Default is disabled
Phone Number	The phone number the router will dial to callback the user (you must have set Enable Callback enabled). Restrictions enter the number without spaces.

Hot Key Prefix	The prefix that a user types to control the current session. Data Options: ^a number—To switch from one session to another, press ^a (Ctrl-a) and then the required session number. For example, ^2 would switch you to session 2. Pressing ^a 0 will return you to the router Menu. • ^a n—Display the next session. The current session will remain active. The lowest numbered active session will be displayed. • ^a p—Display the previous session. The current session will remain active. The highest numbered active session will be displayed. • ^a m—To exit a session and return to the router. You will be returned to the menu. The session will be left running. • ^a l—(Lowercase L) Locks the serial port until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and the serial port is locked. The user must retype the password to unlock the serial port. • ^r—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always Ctrl R, regardless of the Hotkey Prefix. The User Hotkey Prefix value overrides the Serial Port Hotkey Prefix value. You can use the Hotkey Prefix keys to lock a serial port only when the serial port's Allow Port locking parameter is enabled. Default is Hex 01 (Ctrl -a or ^a)
Sessions (1-4)	You can configure up to four (4) sessions that the user can select from to connect to a specific host after that user has successfully logged into the router (used only for serial ports configured for the Terminal profile).
Service	Select the service for this session. • Off—no connection is configured for this session • Telnet—For information on the Telnet connection see *Telnet* • SSH—*SSH* • Rlogin—*RLogin*
Host	Select the host you want to connect to from the pre-defined drop down list.

Port	Specify the TCP port that you will connect to for this session.
Connect Automatically	Specify whether or no the session(s) will start automatically when the user logs into the router.

Login

Configure Login settings	
Set enable password	Enable password is used to access privileged mode.
Enable user lockout	• Maximum failed attempts before lockout • Value is 1 to 65535 • Maximum failed logins before disconnection • Value is 1 to 65535 • Minimum length of a username • Value is 1 to 32
On successful login	• Send syslog • Send trap • on every occurrence (1-65535)
On failed login	• Send syslog • Send trap • on every occurrence (1-65535)
Login banner Message of the day Login prompt timeout banner	Use this command to configure a banner or message of the day to display to users. Configure a delimiting character to indicate the start and end of the message. It cannot be a character that you use in the message. Do not use " or % as a delimiting character. No white space characters are allowed. Banner applies to all consoles and vty sessions Use this command to configure a banner or message of the day to display to users. delimiter character—indicates the start and end of the message and is not a character that you use in the message. Do not use " or % as a delimiting character. White space characters do not work. banner text—the text is alphanumeric, case sensitive, and can contain special characters. It cannot contain the delimiter character you have chosen. The text has a maximum length of 80 characters and a maximum of 40 lines.

	The banner has special macros that are inserted into the banner. They are: $(hostname) which is the hostname you configured on the switch and $(domain) which is the domain name you configured on the IOLAN. login—set login banner motd—set message of the day (motd) prompt-timeout—login authentication timeout

SSL/TLS	
Configure SSL setting for file transfers and HTTPS web server	
SSL Cipher Suite	• Any • Suite B TLS • TLS v1.2 • TLS v1.3

AAA (Authentication, Authorization, and Accounting)

This section describes how you set up AAA on your router.
First you must define the servers and methods which you will use with AAA and then assign these servers to access methods available on your router.

Terminology

AAA
Stands for Authentication, Authorization and Accounting. The three functions which are associated with security.

Authentication
The act of verifying that a user is who they say they are.

Authorization
The act of assigning a valid user with a privilege level.

Accounting
The act of recording when users access your router to manage it. It also involves recording when your router is re-booted.

RADIUS—Remote Authentication Dial-In User Service
A network protocol which provides AAA management for users or devices that connect to your router.

TACACS+—Terminal Access Controller Access-Control System Plus
A network protocol developed by Cisco which provides AAA management for users or devices that connect to your router.

Feature details / Application notes
AAA involves the following steps;
Defining methods for performing authentication, authorization and accounting.
Assign methods to be used for each management access method;

- Console
- Telnet/SSH (TTY access)
- Web browser

AAA—Login	
Authentication	
Add, Edit, Delete Group	**Specify a group name.**
Group	**Select the type of group;** • **Local** • **RADIUS** • **TACACS+** • **LDAP**
Authorization	
Add, Edit, Delete Group	**Specify a group name.**
Group	**Select the type of group;** • **Local** • **If-Authenticated** • **RADIUS** • **TACACS+**
Accounting	
Add, Edit, Delete Group	**Specify a group name.**
List name	**Select the type of group; RADIUS or TACACS+.**

Accounting type	Select the type of messages you want to log; None, Start-Stop (login and log out) or Stop (logout).
AAA—802.1X	
Accounting and Authentication	
Authentication	**Select:** • None • RADIUS
Accounting	**Select:** • None • RADIUS • TACACS+
AAA—System	
Accounting Settings	**Select the type of messages you want to log; None, Start-Stop (login and log out) or Stop (logout).** • None • Start/Stop
Broadcast Methods (Add Group)	
Group	**Select the type of group:** • RADIUS • TACACS+
AAA—Management	
HTTP/HTTPS Management	
Authentication method list	**Select the list to be used for authentication.**
Accounting method list	**Select the list to be used for accounting.**
Enable console authorization	

Authorization method list	Select the list to be used for authorization.
Accounting method list	Select the list to be used for accounting

AAA—Two Factor Settings

PIN Size	Size of the PIN. Values are 4–6 Default is 6
Number of PIN Tries	Number of new two-factor PIN codes retries before failing authentication. Values are 1–10 Default is 3
Number of PIN Attempts	Number of two-factor PIN attempts before trying a new PIN. Values are 1–10 Default is 3

AAA—Password Expiry & Restriction

Password Reuse	The number of times a password can be changed before it can be reused. Value 1-32 times.
Password Expiry	Configures when the password will expire. Value is 1-999 days
Enable Password Restriction	Configures password restrictions. Password cannot be the same as User name Cannot have 3 consecutive characters in the same password No password is not allowed
Group	
Min. Lower Case Characters required	Configures the minimum number of lowercase. numeric numbers. Values are is 1–5

Min. Numeric Characters required	Configures the minimum number of special character that are non alphanumeric character. Values are is 1–5
Min. Special Characters required	Configures the minimum number of special characters. Values are 1–5
Min. Upper Case Characters required	Configures the minimum number of uppercase characters. Values are is 1–5
Password Max Length	Configures the maximum length of the password. Values are 1–128 in length
Password Min. Length	Configures the maximum length of the password. Values are 1–128 in length

RADIUS

A RADIUS server can be used to provide authentication and accounting security for your router. Your router supports User parameters that can be sent to the RADIUS server; see ***Radius and TACACS+*** for more information on the User parameters.

Pre-requisites

Basic AAA has been configured on your router.

Terminology

RADIUS—Remote Authentication Dial-In User Service

A network protocol which provides AAA management for users or devices that connect to your router.

AAA—Stands for Authentication, Authorization and Accounting. The three functions which are associated with security

Feature details / Application notes

RADIUS can be used with your router to provide the following functions;

- Authenticate users logging into your router.
- Provide authorization information for users logging into your router.
- Returned via attribute "Service-Type"
- 1 (login) = User Exec
- 6 (administrative) = Privileged Exec
- Any other value is determined by User Exec.
- Provide accounting information for users and or devices logging in and out of your router.
- Provide AAA functions for devices accessing a port configured for 802.1x.

The following ports are used by default;

- Authentication—1812

- Accounting—1813
- These can be changed on a per RADIUS host basis via configuration.
- User can assign different servers (if desired) for authentication, authorization and accounting.

Radius	
RADIUS Servers (Add, Edit, Delete)	
Name	The name of this RADIUS host.
Hostname/IP address	Defines which IP address will be used when originating RADIUS messages from this router. The interface must be a management interface (i.e. has an IP address assigned).
	Hostname or IPv4/IPv6 IPv4—A.B.C.D IPv6—X:X:X:X::X
Authentication Port	Set the UDP authentication port for the requests to be received on the RADIUS host. Both your router and RADIUS server must match. Default is 1812.
Accounting Port	Set the udp accounting port for the requests to be received on the RADIUS host. Both your router and RADIUS server must match. Default is 1813.
Override Global RADIUS Settings	You can override the global settings for the following three parameters for this RADIUS host.
Secret	Encryption key shared between the router and the RADIUS host/s.
Timeout	Delay between unresponsive attempts. Range is 1–1000 seconds. Default is 5 seconds
Retries	Number of attempts to reach host. Range is 1–100 Default is 3

TACACS+

A TACACS+ server can be used to provide external security to your router.

Pre-requisites

Basic AAA has been configured on your router.

Terminology

TACACS+ - Terminal Access Controller Access-Control System Plus

A network protocol developed by Cisco which provides Authentication, Authorization and Accounting services for users or devices that connect to your router.
TACACS+ is not backwards compatible with the much older TACACS protocol.

AAA

Stands for Authentication, Authorization and Accounting. The three functions which are associated with security.

Feature details / Application notes

TACACS+ can be used with your router to provide the following functions.

- Authenticate users logging into your router.
- Provide authorization information for users logging into your router.
- Provide accounting information for users logging in and out of your router.
- Provide accounting for devices connecting on 802.1x ports.
- The following ports are used by default; Authentication = 1812, Accounting = 1813

TACACS+	
Secret (Global)	Encryption key shared between the router and the TACACS+ host.
Timeout in seconds (Global)	Delay between unresponsive attempts. Range is 1–1000 Default is 5 seconds
Skip non-responsive servers (Global)	How long to ignore non-responsive servers.
IPv4 source interface	Select the source interface from the drop-down list.
IPv6 source interface	Select the source interface from the drop-down list.
TACACS+ Server (Add, Edit, Delete)	
Name	The name of this TACACS+ server.
Hostname / IP address	Defines which IP address will be used when originating TACACS+ messages from this router. The interface must be a management interface (i.e. has an IP address assigned). Hostname or IPv4/IPv6

Override Global RACACS+ Settings	
Secret	The encryption key for this TACACS+ server. This overrides the global secret.
Timeout	Delay between unresponsive attempts. Range is 1–1000 Default 5 seconds This overrides the global parameter for timeout.
TACACS+ Groups (Add, Remove)	Add one or more TACACS+ server(s) to the group. Group can be assigned to authentication, authorization and/or accounting functions.
Group Name	The name of this TACACS+ Server Group
Add a TACACS+	Select a TACACS+ server from the drop-down list to add to the server group.

LDAP	
Server Name	Enter a name for this LDAP server.
Enable Secure Server Mode	
Base DN	root-dn bind root-dn
IPv4/IPv6 Address	Configure the IPv4/IPv6 address of th LDAP server.
Search filter	Configure the name for the search filter.
Retransmission Timeout	Configure a retransmission timeout. Range is 1-65535 seconds Default is 30 seconds
Transport Port	Server listening port. Range is 1-65535 Default is 389

Bind Authentication Parameters

Username	**Configure a user name.**
Password	**Configure the password.**
Secure Options	
Ciphers	**Configure the cipher:** • **adh, dh, dss, edh, high, medium, rsa, sslv3**
Listening Port	**Server listening port.** **Range is 1-65535** **Default is 636**
Trustpoint Name	**Configure the trustpoint name for this LDAP server.**
Add LDAP Server Group	
Name	**Configure the name of the LDAP Server group.**
Add a LDAP server	**Select a LDAP server from the drop-down list.**

Firewall

A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely.

Your router provides global settings for all source packet validation based on state policies. In addition, your router allows you to configure firewall rules and zones which can then be applied to interfaces within your router.

Source validation (strict, loose, disabled) for the following source packets types;

- IPv4 ping
- Broadcast Ping
- Handle IPv4 packet with source router option
- Handle received ICMPv6 redirected messages
- Handle IPv6 packet with routing ext-header
- Log IPv4 with invalid address
- Receive IPv4 redirect messages
- Send IPv4 redirected messages
- SYN Cookies
- RFC1337 TCP time-wait hazard protection

Incoming packet state;

- Established—the incoming packets are associated with an already existing connection),
- Invalid—the incoming packets do not match any of the other states
- Related—the incoming packets are new, but associated with an already existing connection.

These incoming packets can be:

- accept—allow the traffic through
- drop—block the traffic and send no reply
- reject—block the traffic but reply with an “unreachable” error

Feature details / Application notes

As mentioned above, network traffic that traverses a firewall is matched against rules to determine if it should be allowed through or not. A default policy should always be configured as firewall rules do not explicitly cover every possible condition.

Firewall	
Source validation	**Policy for source validation by reversed path (IPv4 only).** **• Disable—no source validation is performed** **• Loose—enable loose reverse path forwarding as defined by RFC3704** **• Strict—enable strict reverse path forwarding as defined in RFC3704** **Default is Disabled**
Packet Handling Policies	
IPV4 ping	**Policy for handling IPv4 ICMP Echo requests.** **Enable—system responses to IPv4 ICMP Echo requests.** **Disable—system does not respond to IPv4 ICMP Echo requests** **Default is disabled**
Broadcast Ping	**Policy for handling IPv4 ICMP Echo and timestamps requests.** **Enable—system responses to broadcast IPv4 ICMP Echo and Timestamp requests** **Disable—system does not respond to IPv4 Echo and Timestamp requests** **Default is disabled**
Handle IPv4 packet with source route option	**Policy for handing IPv4 packets with source route option.** **Default is disabled**

Handle received ICMPv6 redirected messages	Policy for handing received IPv6 ICMP redirect messages. Default is disabled
Handle IPv6 packet with routing ext-header	Policy for handling IPv6 packets with routing extension header. Default is disabled
Log IPv4 packet with invalid address	Policy for logging Ipv4 packets with invalid addresses. Default is enabled
Receive IPv4 redirect messages	Policy for handing received IPv4 ICMP redirect messages. Permits or denies IPv4 ICMP redirect messages. Default is disabled
Send IPv4 redirected messages	Policy for sending IPv4 only redirect messages. Default is enabled
SYN cookies	Policy for using TCP SYN cookies with IPv4. Default is enable
TIME_WAIT assassination hazards protection per RFC 1337	Policy for TIME_WAIT assassinations hazards protection.
State Policy	
Based on Session States	Established—accept, drop or reject Invalid—accept, drop or reject Related—accept, drop or reject
Firewall Rule	
Name	Configure a name for this firewall rule.
Description	Configure a description for this firewall rule.
Log packets hitting default action	Log packets for default action.
Default Action	• accept • drop • reject
Traffic Match (Add)	

Enable	Enable this traffic rule.
Rule Number	Configure a rule number.
Description	Configure a description for this rule.
Log packets matching this rule.	Log packets for default action.
Select Matching Criteria	
Source IPv4 address	Accept IPv4 address or exclude IPv4 address • address and wildcard Use range of addresses • start and stop addresses
Source MAC address	Accept MAC address or exclude MAC address • address and wildcard Use range of MAC addresses • start and stop addresses
Source Port (TCP/UDP)	Accept packets from this source port (TCP/UDP) port.
Destination IPv4 Address	Accept IPv4 address or exclude IPv4 address • address and wildcard Use range of addresses • start and stop addresses
Destination Port (TCP/UDP)	Accept packets from this destination port (TCP/UDP) port.
Recent	Count (Source Addresses sen more the N times. Value 1–255 Time (Source Addresses seen in last N seconds) Value 1-4294967295
State	• Established • Invalid • New • Related

Fragment	• fragment • non fragment
IPSEC	• ipsec • non ipsec
Protocol	• ah, dccp, dsr, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr, igmp, igp, ip, ipip, ipv6, ipv6-frag, ipv6-icmp, ipv6-nontxt, ipv6-opts, ipv6-route, isis, l2ip6-route, isis, l2tp, manet, mpls-in-ip, narp, ospf, pim, rdp, roch, rsvp, sctp, sdrp, shim6, skip, tcp, udp, udplite, vrrp, xns-idp, protocol number 0–255
Firewall Action- Rule	• accept • drop • reject
Schedule	• Use UTC • Enable Schedule
Enable Schedule	• Start time/End Time (hh:mm:ss—24 hour clock)
Select Schedule Type	• Date—Start date - end date (Month/Day/Year) • Weekdays—M, T, W, T, F, S, S, or All • Days of the month—1-31 or All
IPv6 Firewall	
Handle received ICMPv6 redirected messages	Enable or disable.
Handle IPv6 packet with routing ext-header	Enable or disable.
Policies Based on Session States	Established—accept, drop or reject Invalid—accept, drop or reject Related—accept, drop or reject
Firewall Rule	
Name	Configure a name for this firewall rule.

Description	Configure a description for this firewall rule.
Log packet hitting default action	Log the packets that match the default action.
Default Action	• accept • drop • reject
Traffic Match (Add)	
Enable	Enable this traffic rule.
Rule Number	Configure a rule number.
Description	Configure a description for this rule.
Log packets matching this rule.	Log packets for default action.
Traffic Match	
Source IPv6 address	Accept IPv6 address or exclude IPv6 address • address and wildcard Use range of addresses • start and stop addresses
Source MAC address	Accept MAC address or exclude MAC address • address and wildcard Use range of MAC addresses • start and stop addresses
Source Port (TCP/UDP)	Accept packets from this source port (TCP/UDP) port.
Destination IPv6 Address	Accept IPv6 address or exclude IPv6 address • address and wildcard Use range of addresses • start and stop addresses
Destination Port (TCP/UDP)	Accept packets from this destination port (TCP/UDP) port.

Recent	Count (Source Addresses sen more the N times. Value 1–255 Time (Source Addresses seen in last N seconds) Value 1-4294967295
State	• Established • Invalid • New • Related
Fragment	• fragment • non fragment
IPsec	• ipsec • non ipsec
Protocol	Match all or match all except • ah, dccp, dsr, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr, igmp, igp, ip, ipip, ipv6, ipv6-frag, pv6-icmp, ipv6-nontxt, ipv6-opts, ipv6-route, isis, l2ip6-route, l2tp, manet, mpls-in-ip, narp, ospf, pim, rdp, roch, rsvp, sctp, sdrp, shim6, skip, tcp, udp, udplite, vrrp, xns-idp, protocol number 0–255
Firewall Action	• accept • drop • reject
Schedule	• Use UTC • Enable Schedule Start time End Time (hh:mm:ss—24 hour clock)
Type	• Date—Start date - end date (Month/Day/Year) • Weekdays—M, T, W, T, F, S, S, or All • Days of the month—1-31 or All
Zones based Firewall (Add, Edit, Delete)	
Name	Name of the zone.
Description	Description of the zone.

Local Zone	A local zone is the router itself, including interfaces on the router. All packets constructed on and actively sent from the router are regarded as from the local area.
Log packets hitting default action	Enable or disable.
Default Action	• Drop • Reject
Zones Pair (Add, Edit, Delete)	• From what zone • To what zone • Firewallv6 • Firewall
Firewall Interfaces (IPv4/IPv6)	
Assign Firewall and Zones to existing Interfaces	• Select interface • Inbound Firewall • Local Firewall • Outbound Firewall

MAC Filtering

MAC filtering is a security method based on access control. Every hardware device has a unique 48-bit MAC address, Using these MAC addresses, you can filter MAC addresses to the list and either deny or that you don’t want on your network by adding them to the filter list.

Feature details / Application notes

MAC address filtering should not be the only method of securing and protecting large networks. Overall MAC filtering should be viewed as an more of an administration function rather then a security measure. MAC filtering is useful in filtering out unintentional or intentional packet flooding thereby filtering out packets before inspection by firewall or access-list filtering. In fact, MAC addresses are easily spoofed, making MAC address filtering a poor method of security. Every packet from a client device includes their unique MAC address, thereby enabling a third party with a spoofing program to pull off the MAC address of the client device, thus enabling them to then change their own MAC address to match that of the allow client device.

MAC Filtering	
Name	Enter the name of the access list.
Description	Enter a description for this access list.

MAC Addresses	
Add	
Import	**Import formats are;** • **xxxx.xxxx.xxxx—Cisco format where xxxx is 1-4 digits** • **xx:xx:xx:xx:xx:xx—where xx is 1-2 digits** • **aabbccddeeff** • **import from supported interface** • **ethernet interfaces** • **sub-ethernet (VLANs) interfaces** • **dot11radio (SSID 1-4 in AP mode)** • **bridge interfaces**
Export	**Export the MAC access-list to a server.**

802.1X

802.1X defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to the router's Ethernet ports.

Pre-requisites

This feature requires a RADIUS host to perform the authentication for the device. The configuration and setup of this host is beyond the scope of this document.

Restrictions / Limitations

- 802.1x is only supported on access ports.
- Not supported on VLANs or sub-interfaces

Terminology

dot1x

This is a term that is used to refers to the 802.1x feature.

Supplicant

This refers to the device which is requesting access to the network.

Authenticator

Your router acts as the intermediary between the supplicant and the authenticating server.

Authenticating Server

This is the server which provides the actual authentication for the supplicant.

EAP—Extensible Authentication Protocol

This is the protocol that is used to perform the basic authentication function.

For messages between the supplicant and the authenticator, this is encapsulated in EAPoL. (EAP over LAN)

For messages between the authenticator and the authenticating server, the EAP is encapsulated within the RADIUS messages.

MAB—MAC Authentication Bypass

This feature allows devices which do not support 802.1x to be authenticated on your router. The authentication is done by using the MAC address of the device as both the username and password. The authenticating server would need to have this information configured as a valid user.

Feature details / Application notes

The RADIUS host needs to support EAP extensions in order to perform the 802.1x authentication function Your router supports a RADIUS host as the authenticating server. Your router can act as both a supplicant or an authenticator. You can configure this option on a port-by-port basis.

The port is in an “unauthorized” state if the device attempting access has not authenticated.

In this state the following applies;

- The port does not allow any traffic except for EAPOL.
- If the port is configured as a VOICE VLAN port, the port allows VoIP traffic as well.
- Any static addresses configured are not written to your router until the port is authorized.

802.1X Authenticator and Suppliant

Selecting the 802.1x role for a port.

802.1x enabled ports can perform one of two roles;

Authenticator

- Port will authenticate 802.1x supplicants which are connected to it.

Supplicant

- The port will authenticate with its peer which acts as the 802.1X authentication.

802.1X	
Enable 802.1X authentication	**Select Enable to enable this feature.**
Test 802.1X Readiness	**The 802.1x readiness check monitors 802.1X activity on all the router port/s and displays information about the devices connected to the ports that support 802.1X. You can use this feature to determine if the devices connected to the router ports are 802.1x-capable.**

Initialize	• This command re-initialize the port to an unauthorized state and attempts to authenticate the device(s) on the port. This test be done on a per port basis or across all ports.
Re-authenticate	This command will re-authenticate all 802.1X port(s).
Advanced	
Enable 802.1X logging	Send 802.1X messages to a preconfigured syslog server.
802.1X test timeout	Timeout for device EAPOL capabilities test. Range is 1-65535 seconds Default is 10 seconds

Mode	
Supplicant	Port will authenticate with peer which is the authenticator.
Authenticator	Port will authenticate the device/devices (supplicants) connecting on the port.
Authenticator Settings	
Port control	• Auto—the port is locked expecting authentication from either a connected 802.1X client or if MAB is enabled, it will authenticate the MAC to the RADIUS server. • Force authorized—the port is unsecure/unlocked meaning normal operation where no 802.1X client or MAB authentication via RADIUS is required. This is the default setting.
	• Force unauthorized – the port is secured/locked and will NEVER allow any traffic to ingress into our Ethernet port/s.

Host Mode	Single host - Only one device can authenticate and connect on the port. - This is the default mode of operation. Multiple host - Unlimited number of devices can connect on the port once a single device has been authenticated on the port. This single device must be a data (as opposed to voice) device. Multiple authentication - Each device connecting to your router is required to authenticate. - No limit as to the number of devices which can authenticate on the port.
MAB (MAC Authentication Bypass)	Allows devices which do not support 802.1X to be authenticated on your router. The authentication is done by using the MAC address of the device as both the username and password. The authenticating server would need to have this information configured as a valid user. Disabled–no MAB enabled Fallback–MAB is enabled, 802.1X is enabled - Use EAP - Enable periodic reauthentication Standalone–MAB is enabled, 802.1X is disabled
Enable periodic reauthentication	When enabled, the supplicant will be asked to re-authenticated based on the Advanced setting -> re-authentication timeout value.
Advanced Settings	
Supplicant response timeout	Sets the amount of time that the authenticator will wait for the supplicant to reply to all 802.1x messages. Supplicant will time out after this period of waiting. Range is 1-65535 seconds Default is 30
Transmit timeout	The tx-period timer is the time before a port will begin the next method of authentication, and begin the MAB process for non-authenticating devices. Default is 30 seconds

Quiet period timeout	Configure the number of seconds the interface remains in the wait state following a failed authentication attempt by a supplicant before reattempting authentication. Range is 1-65535 seconds Default is 60 seconds
Restart timeout	Interval in seconds after which an attempt should be made to authenticate an unauthorized port. If the parameter “server” is specified, the time is derived from the “Session-Timeout value” (RADIUS Attribute 27) Range is 1-65535 seconds Default is 60 seconds
Maximum authentication retries	Set the number of times the authenticator will retransmit an EAP message to the supplicant. Range is 1-10 seconds Default is 2 seconds
Maximum re-authentication retries	Set the number of times the authenticator will attempt to re-authenticate a supplicant. Range is 1-10 seconds Default is 2 seconds
Credential Profile (Add, Edit, Delete)	Credential profiles are a username and password which will be used by supplicants to authenticate on 802.1X authenticators. Creating a profile allows you to assign this profile to individual ports as needed.
Profile Name	Enter a profile name.
Username	Enter a username.
Password	Enter the password.
EAP Profile (Add, Edit, Delete)	
Profile Name	Enter the profile name.
PKI trustpoint	Enter the PKI trustpoint name.

Methods	• EAP-MD5 • EAP-MSCHAPV2 • EAP-GTC • EAP-TLS • TTLS-MSCHAP • TTLS-MSCHAPV2 • TTLS-CHAP • TTLS-EAP-MSCHAPv2 • TTLS-EAP-GTC • PEAP-MD5 • PEAP-EAP-MSCHAPv2 • PEAP-GTC

IPSEC

A Virtual Private Network (VPN) creates a secure, dedicated communications network tunnelled through to another network.When an IPsec tunnel becomes active, you are requiring that all access to the router go through the configured IPsec tunnel(s), so you must configure any exceptions first. for more information on exceptions) or you will not be able to access the router through the network unless you are configured to go through the IPsec tunnel (you can still access the router through the Console port).

You can configure the router for:

- a host-to-host Virtual Private Network (VPN) connection
- a host-to-network VPN connection
- a network-to-network VPN connection
- or host/network-to-router VPN connection (allowing serial devices connected to the router to communicate data to a host/network).

IPSEC	
Enable IPSEC	Enable or disable IPSEC.
Enable NAT Traversal	Enable or disable NAT Traversal.
NAT Network	Specify the network for NAT transversal.
Client Name	Enter the name for this client connection.

Connection Type	When defining peer VPN gateways, one side should be defined as Initiate (start) and the other as Respond (listen). VPN gateways take longer when both gateways are set to initiate, as both will attempt to initiate the same VPN connection. • Disable—no connection (default) • Initiate—connection will be initiated by the client • Respond—the client will listen for a connection
Any Local Address	Use any local address for the tunnel or the IP address of the router. You should select Any when the IP address of the router is not always known (for example, when it gets it's IP address from DHCP). When Any is used, a default gateway must be configured under Routing/General Routing/Default Gateway Field Format is IPv4 address, IPv6 address, FQDN.
IKE Group	Select an IKE group or use the default_ IKE group.
Authentication	
Identity	The tunnel IP address of a specific host, or the network address that the router will provide a VPN connection to. Field Format is IPv4 address, IPv6 address, FQDN, @IPSEC Key-id
Remote Identity	The subnet mask of the local tunnel IPv4 network. Keep the default value when you are configuring a host-to-host VPN connection. Default is 255.255.255.255
Authentication	• None—no authentication • PSK—A pre-shared key is a string of characters that is used as an authentication key. Pre-shared keys have to be distributed beforehand to all devices that use it. • x509—x.509 certificates are used to authenticate the IPsec tunnel. When using this authentication method, you must include the Peer ID and Trust Point name (pem file).
Tunnel ID	Enter an ID for this tunnel.
ESP Group	Select the Default ESP group or select one from the drop down list.

Local Address Family	Select either IPv4 or IPv6 for this tunnel connection. Default is IPv4
Local Address/ Netmask	The IP address and netmask of your router.
Remote Address Family	Select either IPv4 or IPv6 for this tunnel connection. Default is IPv4
Remote Address/ Netmask	The IP address of a specific host or the network address that the router will provide a VPN connection to. If the IPsec tunnel is listening for connections (Respond) and the connection type is checked for ANY local address then any VPN peer with a private remote network/host will be allowed to use this tunnel if it successfully authenticates.
IKE Groups	
Profile Name	Name of this IKE profile.
Aggressive mode	Aggressive mode takes part in fewer packet exchanges. Aggressive mode does not give identity protection of the two IKE peers, unless digital certificates are used. This means VPN peers exchange their identities without encryption (clear text). It is not as secure as main mode, but the advantage to aggressive mode is that it is faster than Main mode. You must use aggressive mode if one or both peers have dynamic external IP addresses or if you need Network Address Translation Traversal (NAT-T) Default is off
IKE Version	Select 1, 2 or both. Proposal IKEv1 • Proposal ID— enter an ID number • Diffe-Hellman group—2, 5, 14, 15, 16, 17, 18,19,20, 21,22, 23, 24, 25, 26 • Encryption—3des, aes128, aes128gcm128, aes256, aes256gcm128, chacha20poly1305 • Hash—SHA1,MD5, SHA1, SHA256, SHA384, SHA512 Proposal IKEv2 • Proposal ID—enter an ID number • Diffe-Hellman group—2, 5, 14, 15, 16, 17, 18,19,20, 21,22, 23, 24, 25, 26 • Encryption—3des, aes128, aes128gcm128, aes256, aes256gcm128, chacha20poly1305

	• Diffe-Hellman group—2, 5, 14, 15, 16, 17, 18,19,20, 21,22, 23, 24, 25, 26 • Encryption—3des, aes128, aes128gcm128, aes256, aes256gcm128, chacha20poly1305 • Hash—MD5, SHA1, SHA256, SHA384, SHA512 Default is Version 2
Keep-alive lifetime	Time to keep connection alive. Range is 30–86400 Default is 3600 seconds
Dead Peer Detection (DPD)	DPD is a method of detecting a dead Internet Key Exchange (IKE) peer. This method uses IPsec traffic patterns to minimize the number of messages required to confirm the availability of a peer. DPD is used to reclaim the lost resources in case a peer is found dead.
Action	• Clear—terminate the VPN connection over the detection timeout. You must manually re-initiate the VPN connection. We recommend that you use Clear when the remote peer uses dynamic IP address. • Hold—traffic from your local network to the remote network can trigger the router to re-initiate the VPN connection over the detection timeout. We recommend that you use Hold when the remote peer uses a static IP address • Restart—re-initiate the VPN connection for three times over the detection timeout. Default Action is Hold Interval is 30 seconds Timeout is 120 seconds
Interval	Enter the value of delay time in seconds between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when IPsec traffic is idle. Range is 2–86400 Default is 30 seconds
Timeout	Enter the value of detection timeout in seconds. If no response and no traffic over the timeout, declare the peer dead. Range is 10–86400 Default is 120 seconds

Add IKE Proposals	
Proposal ID	ID of this proposal. Values are 1–65535
Diffe-Hellman Group	• 2–1024-bit MODP Group (RFC6989) • 5–1536-bit MODP Group (RFC6989) • 14–2048-bit MODP Group (RFC6989) • 15–3072-bit MODP Group (RFC6989) • 16–4096-bit MODP Group (RFC6989) • 17–6144-bit MODP Group (RFC6989) • 18–8192-bit MODP Group (RFC6989) • 19–256-bit random ECP group (RFC6989) • 20–384-bit random ECP group (RFC6989) • 21–521-bit random ECP group (RFC6989) • 22–1024-bit MODP Group with 160-bit Prime Order Subgroup (RFC6989) • 23–1536-bit MODP Group with 224-bit Prime Order Subgroup (RFC6989) • 24–1536-bit MODP Group with 256-bit Prime Order Subgroup (RFC6989) • 25–192-bit Random ECP Group (RFC6989) • 26–224-bit Random ECP GroupMODP Group (RFC6989) Default is 2
Encryption	• 3des • aes128 • aes128gcm128 • aes256gcm128 • chacha20poly1305 Default is aes256
Hash	• MD5 • SHA1 • SHA256
	• SHA384 • SHA512 Default is SHA1

Add ESP Groups	
Profile Name	Add a name for this ESP profile.
Compression for IPSEC Connection	Use compression for this IPsec connection.
Perfect Forward Secrecy	PFS on will improve security forcing a new key exchange for each new session. Both sides of the VPN tunnel must be able to support this option. Enabling PFS by renewing keys more often will have a little performance impact but provide further security.
Keep-alive lifetime	The tunnel will expires after no activity. Range is 30–86400 Default is 1800 seconds
ESP Mode	Sets the tunnel mode. Transport mode—payload encrypted; headers clear Transport mode—both headers and payload encrypted. Default is tunnel
Restrict IPSEC on interface	Restrict IPsec to these interface. If no interfaces selected then all interface will listen for IPsec packets.
L2TP Settings	Note: NAT traversal and NAT Network must be enabled and configure for L2TP connections.
Client IP Pool Address	Define the pool from which the clients are assigned addresses
Start	Define the start address of the pool.
Stop	Define the end address of the pool.
DNS Server 1	Define a DNS server for clients.
DNS Server 2	Define a DNS server for clients.
Outside Address	The IP address of the remote host.
Pre shared key	Enter the pre shared key for this connection. This must match the server side.
L2TP Username	Enter the username to be used for this connection.
L2TP password	Enter the password to be used for this connection.

OpenVPN

OpenVPN is a virtual private network (VPN) system that implements techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It implements both client and server applications.
Note: to create a connection, a tunnel must exist.

OpenVPN	
Enable OpenVPN	
RESTART AND ENABLE OPENVPN	
Connections (Add, Edit, Delete)	
Enable connection	
Connection name	Give a name to this connection.
Enable the use of config Template (advanced configuration)	Select the name of the template from the drop-down box of the connection you want to use.
Tunnel (tun/tap)	tun—is a virtual point-to-point IP link (L3 layer) tap—is a virtual Ethernet adapter (L2 layer) Note: simple tun is the most common configuration.
Authentication	• Pre-Shared key • TLS certificates
Pre-shared key	Select the pre-shared key from the drop-down box.
TLS Certificates	
TLS authorization PSK	See *Manage Files* files to import keys and certificates.
CA certificate	Indicate the format of the certificate. Indicate whether you will use the terminal (type or paste the certificate) or file transfer from a url. If the certificate was encrypted using a passphrase, it must be entered here. See *Manage Files* files to import keys and certificates.
Certificate for router	The PKI certificate used for this secure connection. See *Manage Files* files to import keys and certificates.

Private Key for router	The PKI private key used for this secure connection. See *Manage Files* files to import keys and certificates.
Act as	• TLS Client • TLS Server
Port	Enter a port value. Range is 1-65535 Default is 1194
Set Different Remote/ Local ports	Remote port. Range is 1–65535 Default is 1194 Local port. Range is 1–65535 Default is 1194
Remote Addresses	
Hostname/IP	Add the hostname or IP address for the remote side.
Port	Add the port number for the remote side. Range is 1–65535 Default is 1194
Protocol	Select to use: • UDP • TCP
Connection Settings	
Local IP Address	Defines the local side and should be a private IPv4 or IPv6 address or hostname. IP Address (local)
Remote Address	Defines the remote side and should be a private IPv4 or IPv6 address or hostname. IP Address (remote) Note: If using a tap device then this parameter will be a netmask.
Enable compression control	• yes • no • adaptive

Enable client to client	Enable client to client mode.
Enable KeepAlive	Enable keepalive timers.
Keepalive interval	Check for connection up every (interval time). Range is 1–65535
Timeout	Check for connection up every (interval time). Range is 1–65535
Enable keepalive	Set keepalive interval Range is 1–65535 seconds Set timeout Range is 1–65535 seconds
Ciphers	Select the ciphers. • aes-128-cbc, aes-192-cbc, aes-256-cbc, bf-cbc, camellia-128-cbc, camellia-192-cbc, camellia-256-cbc, cast-5-cbc, des-cbc, des-ede-cbc, des-ede3-cbc, desx-cbc, rc2-40-cbc, rc2-64-cbc, rc2-cbc, seed-cbc
Verbosity (Logging Level)	This sets the logging level for this connection and messages will be prepended with %OVPN-XXX where the XXX is the connection name in uppercase. • 0, 1, 2, 3, 4, 5, 6, 7,8, 9, 10, 11
Preserve Tunnel Settings between Restarts	Maintain tunnel connection between router restarts.
Advanced–Template	Use template.
Manage Files	
Define Pre-shared secret key	
Name of new key	• enter the name of the new key • generate secret key

Import Certificates, Keys and Parameters	
Transfer Method	• Browser • FTP • HTTP • HTTPS • SCP • SFTP • TFTP
File Type	• CA certificate • certificate for router • Diffie-Hellman parameters • Private key for routers • Pre-Shared Secret Key • Template
Destination file name	Name of destination file.
Start Import	
Installed Files	Delete or View the installed files.

LDAP

Lightweight Directory Access Protocol (LDAP) user authentication is the process of validating a username and password combination with a directory server such MS Active Directory, OpenLDAP or OpenDJ. LDAP directories are standard technology for storing user, group, and permission information and serving that to applications in the enterprise.Lightweight Directory Access Protocol (LDAP) must be integrated into IRG5000 software as an authentication, authorization, and accounting (AAA) protocol alongside the existing AAA protocols such as RADIUS and TACACS+. The AAA framework provides tools and mechanisms such as method lists, server groups, and generic attribute lists that enable an abstract and uniform interface to AAA clients irrespective of the actual protocol used for communication with the AAA server.

As such the router LDAP must support authentication and authorization functions for AAA. Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP. It is also used as a method of authenticating users. Microsoft Active Directory is an LDAP-like directory

LDAP	
Server Name	Enter a name for this LDAP server.

Enable Secure Server Mode	
Base DN	**root-dn** **bind root-dn**
IPv4/IPv6 Address	**Configure the IPv4/IPv6 address of th LDAP server.**
Search filter	**Configure the name for the search filter.**
Retransmission Timeout	**Configure a retransmission timeout.** **Range is 1-65535 seconds** **Default is 30 seconds**
Transport Port	**Server listening port.** **Range is 1-65535** **Default is 389**
Bind Authentication Parameters	
Username	**Configure a user name.**
Password	**Configure the password.**
Secure Options	
Ciphers	**Configure the cipher:** • **adh, dh, dss, edh, high, medium, rsa, sslv3**
Listening Port	**Server listening port.** **Range is 1-65535** **Default is 636**
Trustpoint Name	**Configure the trustpoint name for this LDAP server.**
Add LDAP Server Group	
Name	**Configure the name of the LDAP Server group.**
Add a LDAP server	**Select a LDAP server from the drop-down list.**

SSL/TLS

Configure SSL setting for file transfers and HTTPS web server

SSL Cipher Suite	• **Any** • **Suite B TLS** • **TLS v1.2** • **TLS v1.3**

Monitor and Stats

You can view statistics for your router with either the WebManager or through the Command Line Interface (CLI). Some viewing options may be different on some models or running software.

Administration

Your router provides a comprehensive range of management services.
Some parameters and/or features may not be on your version of firmware or product model.
Administration services may include;

- **Software Management—**including checking for updates, viewing software versions, automatically updating software, and creating backup software.
- **Configuration—**including backing up/restoring your configuration and booting from a configuration file using DHCP/BOOTP.
- **Keys and Certificate—**including importing and exporting of HTTPS, Server, SSH and SSL host/client/user keys and certificates.
- **Flash/NVRAM Files—**including exporting and importing files to/from flash.
- **Reboot/Reset—**including resuming power standby mode, timed reboots, resetting to factory defaults (removing all containers) and shutting down your router.
- **Container Management—**including adding, updating, and deleting local container images, as well as configuring container private registry credentials and displaying container storage information.adding, updating, and deleting local container images. Also view container-storage information

Note: Some administrator services may be different on some models or running software.

Software Management

This section describes how to manage the Perle router software (images) files.
Terminology

- Startup software is the software that is stored in flash and will run the next time the router is rebooted.
- Current running software is the actual software image that is executing on your router.
- Backup software is the software that is stored in backup. A new backup is created in the routerrouterevery time the software is updated.
- Revert to backup software, will delete your present software and use the saved backup software at next reboot.
- SCP (Secure Copy Protocol) uses Secure Shell (SSH) for data transfer, authentication and encryption.
- TFTP (Trivial File Transfer Protocol) is a common File Transfer Protocol which allows a client to get a file from or put a file onto a remote host)
- SFTP (Secure File Transfer Protocol) is a common File Transfer Protocol which allows a client to get a file from or put a file onto a remote host
- FTP is similar to TFTP, but requires user authentication
- HTTP (Hypertext Transfer Protocol) is an application layer protocol used to transfer a file between devices using the HTTP protocol
- HTTPS is the secure form of HTTP, which means that traffic or data is encrypted by Transport Layer Security (TLS)

- Internal Flash is the internal flash storage within the router

Automatically Check for updates option—if enabled, the router checks the Perle repository every 7 days then informs you if your router needs a software update.

Check now option—immediately checks the Perle repository for new software updates. If a new software image is found:

- it can be downloaded directly from the Perle repository using the Update Software button/Direct Download feature
- it can be copied directly from our website using Direct download, Browser, FTP, HTTP, HTTP, SCP, SFTP, or TFTP and saved to an external server to be updated to your router at a later date. Internet access is required to obtain the latest software images from the Perle web site at https://www.perle.com/downloads/

The download function can be cancelled at any time during the download, and the router will use the current software image.

Automatically download software if new version found during check (Firmware over the Air (FOTA))—our FOTA software feature allows enterprises to efficiently and securely update FOTA supported Perle devices in large scale deployments. By default, FOTA is enabled, allowing operators to remotely and seamlessly perform upgrades of the devices' software versions to add new features and fix software issues.

Process:

1. The router software automatically checks the central repository for software updates.
2. The check is done every 7 days, regardless of the frequency of reboots.
3. If an update is available an automatic download will be initiated.
4. If the download fails—retries will be scheduled every hour for 24 retries. If still not successful after the 24 attempts, the process will begin again on the next "check for updates".
5. Until a successful download has happened—the current version of software will continue to be the "next boot" version.
6. Once the software has been successfully downloaded, it will be made the "next startup" version and will take effect at the time of the next boot.
7. Once the software has been successfully downloaded, what was the "currently running software" now becomes the "backup" boot software.

Router Software Versions

Software Information on Next Startup, Currently Running and Backup software images.

- Name
- Version
- Date created
- Size of the software file

LTE Modem Firmware

- Your router comes pre-installed with LTE firmware for the most popular cellular carriers. In most cases, you will not need to download new LTE modem firmware unless directed by Perle Systems Technical support. An Update button allows you to maintain the latest LTE modem software on your router.

Manage Configuration Files

The configuration files can be backed up or restored from the router browser option or to a FTP, HTTP, HTTPS, SCP, SFTP or TFTP server.
Choose the method to backup and restore device configuration files.

Boot Configuration File

Specify the BOOTP server name that contains the boot file and the time-out value. Configure DHCP Client parameters per interface. See ***Network***.

Download configuration file using DHCP/BOOTP	**Specify the name of the BOOTP server that contains the BOOTP file.**
Timeout	**Timeout in seconds waiting for response from the BOOTP server.** **Default is 600** **Value is 600–65535**

Keys and Certificates

This feature allows for the management of keys and certificates on your router. Keys and certificates are used to identify users and hosts for secure connections such as SSH and HTTPS.

Terminology

Strict Host Checking

The client is attempting to establish an SSH or HTTPS connection to a server must validate the identity of that server using keys and certificates. If the server fails to authenticate using this method, the connection is not established.

Feature details / Application notes

We support the following certificates/keys in our router.

Server SSH key

This RSA key is used to identify the server when a client connects via SSH to your router. When your router boots, if there is no SSH server key present, then your router will automatically generate a SSH2. You can optionally import your own key.
The public portion of the key can then be exported from your router so that the host key can be put on SSH clients who are using strict host key checking to connect via SSH2.
The private portion of the key can be exported as well. This can be done to backup this private key. If the original router is reset to factory default or is replaced, this key can be downloaded to your router so that the SSH clients see the same SSH host as before. Only

the private key is saved. The public portion can always be generated from the private portion so it does not need to be saved.
To protect the private key, if you export it out of your router you must enter a passphrase which is used to encrypt the key. This passphrase is required when restoring the key to your router and protects if from unauthorized usage.

SSH Host keys
When your router attempts an SSH2 session to an SSH server and strict host checking is enabled, there needs to be an SSH host key for this host present on your router. This is the public portion of the SSH2 host key
Note: The key needs to be an RSA key in OpenSSH format.

SSH User keys
If SSH2 clients choose key authentication, then each user needs to have a key on your router which identifies them.
Note: The key needs to be an RSA key in OpenSSH format.

Server CA Certificate
A CA certificate is used when you use HTTPS to transfer a file to an HTTPS host. You configure the CA certificate with a name known as a trustpoint. The CA certificate validates certificates presented by the HTTPS host. It can also be used to identify a RADIUS authentication server to your router when the port is acting as an 802.1x supplicant.

SSL Client key

- Used by 802.1x supplicant
- The key is used to encrypt the data exchange between the suppliant and the RADIUS host.
- This is a global client key which is used as the credentials for your router.
- The user imports the public key into our router.

SSL Client Certificate

- Used by 802.1x supplicant
- The certificate is used by the RADIUS host to validate that we are who we say we are.
- This is a global client certificate which is used as the credentials for your router.
- The user imports the certificate into our router.

Managing the HTTPS Certificate

- This is the certificate which identifies our router to clients which use HTTPS to access our router and need the certificate to validate our identity.
- This certificate/key is also used by the TTY services that have SSL/TLS enabled.
- Your router is shipped with a generic certificate signed by Perle Systems Limited. This certificate can be replaced by you with a certificate from a signed authorized certificate authority.

Managing SSH server key

- Your router is shipped with an auto generated SSH server key.
- This key can be exported for safe keeping or to be imported on to SSH clients that are using "strict host checking".
- Once exported for safe keeping, the key can be restored to your router (i.e. after a reset to factory or if your router was replaced due to a service issue). This would allow all the existing clients to continue to treat your router as they did before.

Manage HTTPS Certificate	
Import HTTPS Certificate for the WebManager	
	• Browser • FTP • HTTP • HTTPS • SCP • SFTP • TFTP • USB
Your routerhas a built-in self signed certificate. **To use your own HTTPS Certificate, you need to download a signed version of a .pfx certificate from a CA authority**router**. You also need to set the SSL passphrase parameter with the same password that was used to generate the key.**	
Type	• PEM • PKCS#12
Passphrase	**Enter the passphrase to use with the certificate.**
Import HTTPS Certificate File	**Select the certificate to be imported into the** router**.**
Manage Server SSH Key	
Import and Export server SSH-2 RSA Key. This key is used to identify the router **to incoming SSH clients.**	
Public Key	**OpenSSH**
Private Key	**PEM**
Method	• Browser, FTP, HTTP, HTTPS, SCP, SFTP, TFTP

Transfer server SSH key directly through your web browser.
Import Options

Passphrase	Enter the passphrase to be used with this private server SSH key. Import the private server SSH key.
Key size	Specify a key size in bits. Range is 1024-4096
Manage SSH Host Keys	
Import SSH-2 RSA host public keys in OpenSSH format. These keys are used to authenticate other SSH servers for outgoing SSH connections.	
Method	• Browser, FTP, HTTP, HTTPS, SCP, SFTP, TFTP
Transfer SSH host keys directly through your web browser	
SSH Hostname/IP address	Enter the host name or IP address where the SSH host key resides.
	Select SSH Host Key to import to the routerrouterrouterrouter.
Installed Keys	You can view/delete installed keys.
Manage SSH User Keys	
Import SSH-2 RSA user public keys in OpenSSH format. These keys are used to authenticate users for incoming SSH connections.	
Method	• Browser, FTP, HTTP, HTTPS, SCP, SFTP, TFTP
Transfer SSH user keys directly through your web browser	
SSH User	Enter the name of the SSH user.
	Import SSH User Key for this user.
Installed Keys	You can view/delete installed keys.
Manage Server/CA Certificates	

This option is used to validate HTTPS certificates presented by hosts which we perform HTTPS transfers to/from. It can also be used to validate the RADIUS authentication server if your router is acting as an 802.1x supplicant. Import server/CA Certificates	
Method	• Browser, FTP, HTTP, HTTPS, SCP, SFTP, TFTP
Transfer server/CA Certificate directly though your web browser	
Type	• PEM • PKCS#12
Passphrase	Enter the passphrase to use with the certificate
Import Server/ CA Certificate	Select the certificate to be imported into the router.
Installed Certificates	You can view/delete installed certificates.
Manage SSL Client Key	
Key pair is generated externally to your router and the public portion of the key is imported to your router. Import server/CA Certificates	
Method	• Browser, FTP, HTTP, HTTPS, SCP, SFTP, TFTP
Transfer SSL key directly through your web browser.	
Type	• PEM • PKCS#12
Passphrase	Enter the passphrase to use with your SSL client key.
Import SSL Client Key	Select the SSL Client Key to be imported into the router.
Manage SSL Client Certificate	
Import SSL Client Certificate	
Method	• Browser, FTP, HTTP, HTTPS, SCP, SFTP, TFTP
Transfer SSL Client Certificate directly through your web browser.	

Type	• **PEM** • **PKCS#12**
Passphrase	**Enter the passphrase to use with your SSL client certificate.**
Import SSL Client Key	**Select the SSL Client Certificate to be imported into the** router.
Password Encryption	
Manage Password Encryption Key	
Default Key Currently in use	**Encrypt current passwords with new encryption keys. You can generate, delete, upload and export keys.The default key is currently in use.** • **Generate new key** • **Upload key**

Managing Flash/NVRAM Files

Export and Import file from flash or NVRAM.

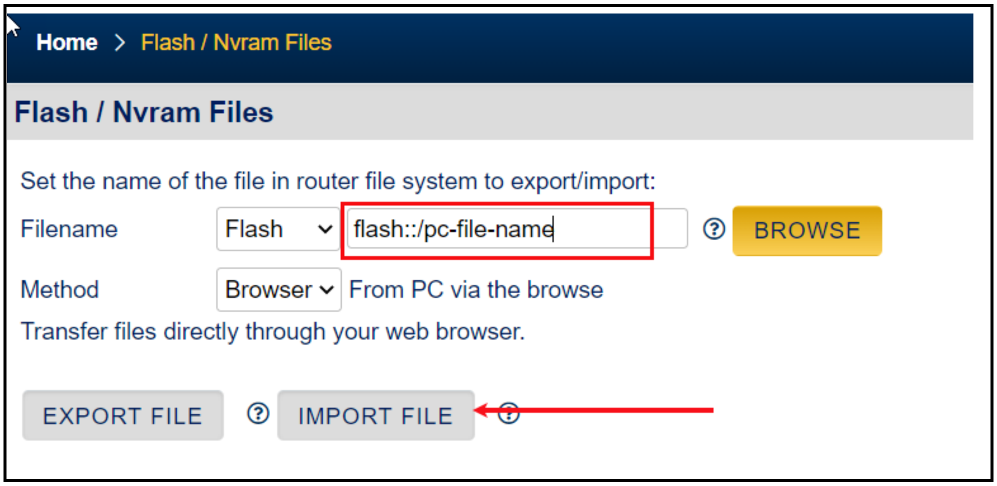
Pre-requisites

- TFTP, FTP, HTTP, SFTP, HTTPS, SCP server/s, USB or the web browser.

Features details / Application notes

- Export flash/NVRAM file to PC via web browser
- Export flash/NVRAM file to FTP server
- Export flash/NVRAM file to HTTP server
- Export flash/NVRAM file to HTTPS server
- Export flash/NVRAM file to SCP server
- Export flash/NVRAM file to SFTP server
- Export flash/NVRAM file to TFTP server
- Export flash/NVRAM file from the USB drive
- Importing flash/NVRAM file from PC via web browser
- Importing flash/NVRAM file from FTP server
- Importing flash/NVRAM file from HTTP server
- Importing flash/NVRAM file from HTTPS server
- Importing flash/NVRAM file from SCP server
- Importing flash/NVRAM file from SFTP server
- Importing flash/NVRAM file from TFTP server
- Importing flash/NVRAM file from the USB drive

Example:
Import a file on your PC to the router flash file system.



Set the name of the file in router file system to export/import:

Filename: Flash, flash::/pc-file-name

Method: Browser, From PC via the browse

Transfer files directly through your web browser.

Reboot/Reset

Enables you to reboot the router based on:

- reboot now
- reboot in hours/minutes

You can manually reboot the router by, pressing the reset button and holding for 10 seconds. You can manually reset the router by holding the reset button while powering the unit up.

Reboot/Reset	
Reboot	**Reboot now**
Reboot in	**Schedule a time to reboot in hours and minutes.**
Resume Power Management	
Standby	**Depending on power management setting this may cause the router to enter Standby Mode.** • **Resume** **Note: not all models support Standby mode, see the Hardware Installation Guide on the Perle Website to see if your model supports this feature.**

Reset to Factory Defaults	
Reset to Factory **Remove all container management images**	**Reset all configuration, operational information, and certificates to factory default settings. Ethernet settings are 192.168.0.1. with DHCP enabled.** • **Reset now** • **remove container management images** • **Delete all container images from the router**
Shutdown the router	
Shutdown	**This will shutdown the router. without engaging any of the standby modes.. The Reset button will power the router back up.** • **Shutdown now** **Note: not all models support Standby mode, see the Hardware Installation Guide on the Perle Website to see if your model supports this feature.**

Container Management

Enables you to add, update, delete, and view local container storage images and information. **Note:** By default, the router will pull the images from docker’s public registry at *https://hub.docker.com/*

Local Container Images	
Add container image from:	**Registry—add an image from a repository** **Image name—specify the image name** • **tag—if no TAG is specified, TAG latest will be used**
Add Container image tarball	**Container image tarball—enter the flash:/path and filename to add this container image.** **Note: you must upload the image tarball into flash: before trying to add this image into the container image storage area.**
Update	**Update container image specified.**
Delete	**Delete the specified image from storage.**
Container-storage information	**View container storage information.**

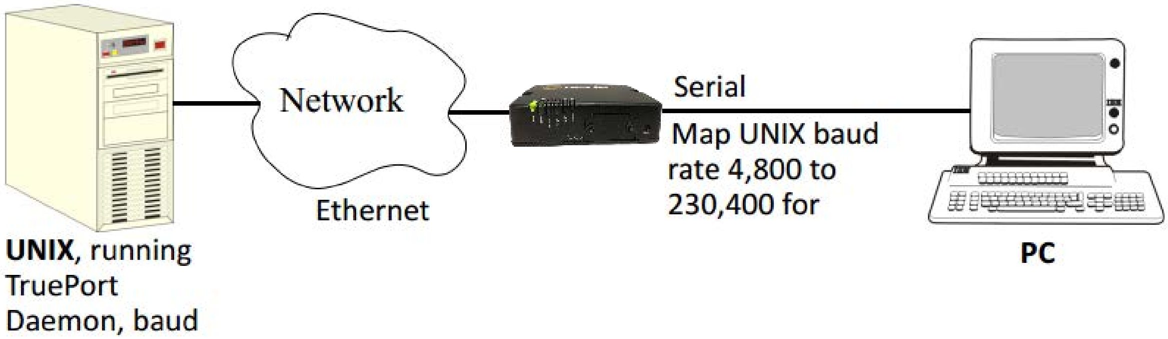
Trueport

This chapter provides information on TruePort Redirect utility.

Trueport is a com port redirector utility for the router. It can be run in two modes:

- **Trueport Full Mode—**This mode allows complete device control and operates exactly like a directly connected serial port. It provides a complete COM port interface between the attached serial device and the network.
- **TruePort Lite mode**—This mode provides a simple raw data interface between the device and the network. Although the port will still operate as a COM port, control signals are ignored. In this mode, the serial communications parameters must be configured on the router.

You use TruePort when you want to connect extra terminals to a server using the router rather than a multi-port serial card. TruePort is especially useful when you want to improve data security, as you can enable an SSL/TLS connection between the TruePort host port and the router. When run on UNIX, TruePort allows you to print directly from a terminal to an attached printer (transparent printing). You can also remap the slow baud rate of your UNIX server to a faster baud rate.


Network
Ethernet
Serial
Map UNIX baud rate 4,800 to 230,400 for
PC
UNIX, running TruePort Daemon, baud

For a complete list of the supported operating systems, see the Perle website.

PerleView

Managing large numbers of deployed network equipment poses unique challenges to the network administrator. It requires a centralized solution with efficiencies found in a platform that uses standard client tools, databases and protocols.

PerleVIEW Device Management System is an Enterprise-grade, multi-user, Windows server-based centralized management package that simplifies the configuration, software upgrade, administration, monitoring, and troubleshooting of devices managed by Perleview in medium to large-scale deployments. Network Administrators, using their Internet Browser, can securely access PerleVIEW and manage 10’s, 100’s or thousands of Perle supported devices from a centralized server.

PerleView can be used to:

- See all network problems at a glance and take appropriate action
- Track inventory and display how the devices are performing
- Gather statistics and run reports from network data stored in the SQL database
- Schedule, or issue on-demand, mass deployment of software updates and configuration files
- Backup and restore configuration
- Automatically check the latest software levels

For more information please go to https://www.perle.com/products/perleview.shtml

Modbus Remapping Feature

This appendix provides additional information about the Modbus Remapping feature.

Modbus Remapping Feature

The Modbus remapping feature allows a TCP Modbus Master to poll a Modbus slave device and have the router translate the UID to a different UID for the slave device. The Master UID has to be unique on the router. The Slave UID must be unique on each serial port. The translate rules are controlled by a file downloaded to the router.

The following procedure will allow you to use the Modbus remapping feature:
Create a configuration file

- **The file must be called "modbus. remap"**
- **One translate rule per line**
- **The fields on a line are separated by a comma**

Line format for one UID is:

- **port,master_uid,slave_uid**
- **port: is therouter port number that the slave is connected to**
- **master_uid: is the UID that the TCP Modbus Master uses**
- **slave_uid: is the UID that the Modbus slave uses**

Line format for UID ranges is:

- **port,master_start-master_end,slave_start-slave_end**
- **port: is therouter port number that the slave is connected to**
- **master_start: is the first master UID in the range**
- **master_end: is the last master UID in the range**
- **slave_start: is the first slave UID in the range**
- **slave_end: is the last slave UID in the range**

Configuring the Modbus UID Remapping Feature

1. On the serial port Modbus Gateway, configure Modbus slave. Configuration parameters such as “UID range” and UID Address Mode will be ignored in this mode of operation.
2. Download the "modbus_remap" file to the router’s flash using the copy command.
3. With the WebManager use the Administration/Manage Flash Files page.

Valid SSL/TLS Ciphers

This appendix contains a table that shows valid SSL/TLS cipher combinations.Some configuration parameters may be different on some models or running software.

Full Name	Key-Exchange	Auth	Encryption	Key-Size	HMAC
EDCHE-ECDSA-AES256-GCM-SHA384	Kx=ECDH	Au=ECDSA	Enc=AES-GCM	256	Mac=SHA384
ECDHE-ECDSA-AES256-SHA384	Kx=ECDH	Au=ECDSA	Enc=AES	256	Mac=SHA384
ECDHE-ECDSA-AES256-SHA	Kx=ECDH	Au=ECDSA	Enc=AES	256	Mac=SHA1
EDH-DSS-AES256-GCM-SHA384	Kx=DH	Au=DSS	Enc=AES-GCM	256	Mac=SHA384
EDH-RSA-AES256-GCM-SHA384	Kx=DH	RSA	Enc=AES-GCM	256	Mac=SHA384
EDH-RSA-AES256-SHA256	Kx=DH	RSA	Enc=AES	256	Mac=SHA256
AES256-GCM-SHA384	Kx=RSA	RSA	Enc=AES-GCM	256	Mac=SHA384
AES256-SHA256	Kx=RSA	RSA	Enc=AES	256	Mac=SHA256
EDH-DSS-AES256-SHA256	Kx=DH	DSS	Enc=AES	256	Mac=SHA256
EDH-RSA-AES256-SHA	Kx=DH	RSA	Enc=AES	256	Mac=SHA1
EDH-DSS-AES256-SHA	Kx=DH	DSS	Enc=AES	256	Mac=SHA1
ADH-AES256-GCM-SHA384	Kx=DH	None	Enc=AES-GCM	256	Mac=SHA384
ADH-AES256-SHA256	Kx=DH	None	Enc=AES	256	Mac=SHA256
ADH-AES256-SHA	Kx=DH	None	Enc=AES	256	SHA1
AES256-SHA	Kx=RSA	Au=RSA	Enc=AES	256	Mac=SHA1
ECDHE-RSA-AES128-GCM-SH256	Kx=ECDH	Au=RSA	Enc=AES-GCM	128	Mac=SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	Kx=ECDH	Au=ECDSA	Enc=AES-GCM	128	SHA256
ECDHE-ECDSA-AES128-SHA256	Kx=ECDH	Au=ECDSA	Enc=AES	128	SHA256
ECDHE-ECDSA-AES128-SHA	Kx=ECDH	Au=ECDSA	Enc=AES	128	SHA1
EDH-DSS-AES128-GCM-SH256	Kx=DH	Au=DSS	Enc=AES-GCM	128	SHA256
EDH-RSA-AES128-GCM-SHA256	Kx=DH	Au=RSA	Enc=AES-GCM	128	SHA256
EDH-RSA-AES128-SHA256	Kx=DH	Au=RSA	Enc=AES	128	SHA256
EDH-DSS-AES128-SHA256	Kx=DH	Au=DSS	Enc=AES	128	SHA256
EDH-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES	128	SHA1

Full Name	Key-Exchange	Auth	Encryption	Key-Size	HMAC
EDH-DSS-AES128-SHA	Kx=DH	Au=DSS	Enc=AES	128	SHA1
ADH-AES128-SHA256	Kx=DH	Au=None	Enc=AES	128	SHA256
ADH-AES128-SHA	Kx=DH	Au=None	Enc=AES	128	SHA1
AES128-GCM-SHA256	Kx=RSA	Au=RSA	Enc=AES-GCM	128	SHA256
AES128-SHA256	Kx=RSA	Au=RSA	Enc=AES	128	SHA256
AES128-SHA	Kx=RSA	Au=RSA	Enc=AES	128	SHA1
RC2-CBC-MD5	Kx=RSA	Au=RSA	Enc=RC2	128	MD5
ADH-RC4-MD5	Kx=DH	Au=None	Enc=RC4	128	MD5
RC4-SHA	Kx=RSA	AU=RSA	Enc=RC4	128	SHA1
RC54-MD5	Kx=RSA	Au=RSA	Enc=RC4	128	MD5
ECDHE-ECDSA-DES-CBC3-SHA	Kx=ECDH	Au=ECDSA	Enc=3DES	168	SHA1
EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES	168	SHA1
EDH-DSS-DES-CBC3-SHA	Kx=DH	Au=DSS	Enc=3DES	168	SHA1
ADH-DES-CBC3-SHA	Kx=DH	Au=None	Enc=3DES	168	SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES	168	SHA1
DES-CBC3-MD5	Kx=RSA	Au=RSA	Enc=3DES	168	MD5
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES	56	SHA1
EDH-DSS-DES-CBC-SHA	Kx=DH	Au=DSS	Enc=DES	56	SHA1
ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES	56	SHA1
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES	56	SHA1

Diagnostics

These diagnostic tools are available on your router.

Email/SMS Test

The email test utility allows you to test the email function.

Specify the email address you want to send the email message to. If successful, you will receive an email with the heading of ”Test Message from “your host name” with a body text of “Hello World”.

The SMS test utility allows you to test the SMS function.

Specify the phone number to send a text message to. If successful, you will receive a text message”.

Ping

The ping utility accepts the following parameters.

- Host (this is the destination host)
  - Specified as;
    - Name (resolvable via DNS or host table)
    - IPv4 address
    - IPv6 address
- Count (number of repetitions)
  - 1–2147483647
- Datagram size
  - Valid range is 36–8024 bytes
  - Default is 56 bytes
- Data pattern
  - Hexadecimal pattern

If a name is specified, the utility attempts to resolve the name to an IP address. If unsuccessful, an error message is given. Next, the utility attempts to send the ICMP message to the destination host. If this is received by the host, the host responds to the sender. The send / response sequence is considered one repetition of the ping command. Each repetition is timed. This information is displayed for each successful request. After the requested number of repetitions is completed, the utility provides a summary of how many requests were sent, how many responses were received and the min/avg/max round-trip times.

Traceroute

This utility displays each hop on the path to the final destination including the time it took to reach that hop and return. If the destination is not reachable, the utility displays how far the message travelled. Traceroute displays the path taken by a packet travelling from the host on which the command is execute to a destination normally reachable via IP routing, It uses ICMP messages to do this. This utility helps identify at what point the routing to the destination failed This information can be used to provide Perle Technical support information on your router.

The traceroute utility accepts a single parameter which is the destination address. This parameter is specified as;

- Name
- IPv4
- IPv6

If a name is specified, the utility resolves the name to an IP address. If unsuccessful, an error message is given.

It then attempts to communicate with the next hop in the path (i.e. default router/ gateway). If this is successful, it will attempt to communicate with the next hop in the path. This is repeated until it either reaches the end destination or fails to reach one of the hops on the way. As each attempt is made, the utility displays the results of that attempt—including the timing information.

The utility displays an "*" to indicate a hop is unreachable.

Enabling debug messages

Log debug messages to collect debugging information. Debug commands do not survive a re-boot.

- add 802.1X authenticator
- add 802.1X supplicant
- add alarm manager
- add command line parser
- add Device Manager
- add DHCP client
- add DHCP relay agent
- add DHCP server
- add INIT
- add kernel
- add LLDP
- add logging manager
- add SNMP
- add trap
- add VTY
- add RESTful API
- add VRRP
- add dot11 station
- add dot11 access-point
- add BGP RIB
- add BGP updates
- add BGP keepalives
- add BGP FSM
- add BGP filters
- add BGP events

- add WAN High availability
- add email
- add IPSEC
- add OSPF RIB
- add OSPF packets
- add OSPF NSSA
- add OPSF NSM
- add OSPF ISM
- add LTE
- add GNSS
- add NTP
- add BGP messages
- add IP Passthrough
- add TTY
- add Dialer
- add RIP packets
- add RIP Events
- add RIP RIB
- add WAN Interface Manager
- add OSPF Events

Radius and TACACS+

RADIUS

RADIUS can be used strictly for external authentication, it can also be used to configure line and user parameters. Therefore, when a user is being authenticated using RADIUS, it is possible that the user's configuration is a compilation of the parameters passed back from RADIUS, and from the router if the user has also been set up as a local user in the router, and the Default User's parameters for any parameters that have not been set by either RADIUS or the user's local configuration.

Supported Radius Parameters

This section describes the attributes which will be accepted by the router from a RADIUS server in response to an successful authentication request.

Table 0–1

Type	Name		Description
1	User-Name	Request	The name of the user to be authenticated.
2	User-Password	Request	The password of the user to be authenticated.
4	NAS-IP-Address	Response	The router's IPV4 address.
5	NAS-Port	Response	If the user is connected to a physical port then the port number of the port is sent. If the user is connected to the router itself then a port number of 0 is sent.
6	Service-Type	Response	Indicates the service to use to connect the user to the router. A value of 6 indicates administrative access to the router. Supported values are: ● 1—Login ● 3—Callback-Login Equivalent to the router **User Service** set by Type 15, Login-Service. ● 2—Framed ● 4—Callback-Framed Equivalent to the router **User Service** set by Type 7, Framed-Protocol. ● 7—NAS prompt ● 9—Callback NAS-prompt Equivalent to router **User Service DSLogin**. ● 6—Administrative User ● 11—Callback Administrative User Equivalent to router **User Service DSLogin** and the User gets Admin privileges.
7	Framed-Protocol	Response	The link layer protocol to be used by this user. Determines the User Service when Service-Type is set to Framed or Callback-Framed. Supported values are: ● 1—PPP ● 2—SLIP

Table 0–1

Type	Name		Description
8	Framed-IP-Address	Response	The IP Address to be assigned to this user for PPP or SLIP.
9	Framed-IP-Netmask	Response	The subnet to be assigned to this user for PPP or SLIP.
12	Framed-MTU	Response	Attribute indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means such as PPP.
13	Framed-Compression	Response	Indicates a compression protocol to be used for the PPP or SLIP link. Supported value is: ● 1—Van Jacobson TCP/IP compression.
14	Login-Host	Response	Indicates the host with which the user can connect to when the Service-Type is set to `1` (Login) or `3` (Callback-Login).
15	Login-Service	Response	Indicates the **User Service** to use to connect the user a a host. Supported values are: ● 0—Telnet ● 1—Rlogin ● 2—TCP Clear ● 5—SSH ● 6—SSL Raw
16	Login-TCP-Port	Response	Indicates the TCP port with which the user is to be connected when the Service-Type is set to `1` (Login) or `3` (Callback-Login).
19	Callback-Number	Response	Specifies the callback phone number. This is the same implementation as `20` (Callback-ID), but takes precedence if `20` is set.
20	Callback-ID	Response	Specifies the callback phone number. This is the same implementation as `19` (Callback-Number), but `19` takes precedence if both are set.
22	Framed-Route	Response	When the PPP IPv4 interface comes up, the router will add routes to the user's PPP interface in the same order they were received
25	Class	Response	Received attributes are send in the Accounting Reply messages.
26	Vendor-Specific	Response	Perle's defined attributes for line access rights and user level. Line Access Rights for port ***n*** (where ***n*** is the line number): **Name:** Perle-Line-Access-Port-***n*** Type: 100 + ***n*** Data Type: Integer Value: Disabled (0), ReadWrite(1), ReadInput(2), ReadInputWrite (3), ReadOutput (4), ReadOutputWrite (5), ReadOutputInput (6), ReadOutputInputWrite (7) **Name:** Perle-User-Level Type: 100 Data Type: Integer Value: Admin(1), Normal(2), Restricted(3), Menu(4) **Name:** Perle-Clustered-Port-Access Type: 99 Data Type: Integer Value: Disabled(0), Enabled(1)
27	Session-Timeout	Response	Maximum number of seconds the user will be allowed to stay logged on.

Table 0–1

Type	Name		Description
28	Idle-Timeout	Response	Use this timer to close a connection because of inactivity. When the Idle-Timeout expires, the router will end the connection. The maximum value is 4294967 seconds (about 49 days). A value of 0 (zero) means the Idle-Timeout will not expire, so the connection is permanently open.
31	Calling-Station-Id	Response	For reverse telnet and reverse ssh the IP address of the client will be sent. All other server type do not send this field.
32	NAS-Identifier	Response	If the identifier is configured then this field will be sent.
61	NAS-Port-Type	Response	For reverse telnet and reverse ssh connections, a type of Virtual (5) will be sent. For a PPP connection type a type of Async (0) will be sent. For all direct connect service types a type of Async (0) will be sent.
87	NAS-Port-Id	Response	For sessions originating from the serial port: <line-name> or “SERIAL:xx”, where xx starts at serial port 1. For reverse Telnet and SSH Ethernet sessions: “ETH:REVSESS:xx”, where xx is the serial port being accesses, otherwise 00 for a routermanagement session. For HTTP sessions: “HTTP”
95	NAS-IPv6-Address	Response	The IPv6 address of the router.
96	Framed-Interface-Id	Response	The remote IPv6 interface identifier for the remote end of the PPP link.
98	Login-IPv6-Host	Response8	For LOGIN and CALLBACK service types, the IPv4 address of the login host is sent to the RADIUS accounting host.
99	Framed-IPv6-Route	Response	When the PPP IPv6 interface comes up, the router will add routes to the user’s PPP interface in the same order they were received.

Accounting Message

This section describes the attributes which will be included by the Routerrouterwhen sending an accounting message to the RADIUS server.

Type	Name	Description
1	User-Name	The name of the user to be authenticated.
4	NAS-IP-Address	IP Address of the routerinterface.
5	NAS-Port	If the user is connected to a physical port then the port number of the port is sent. If the user is connected to the router itself then a port number of 0 is sent.

Type	Name	Description
6	Service-Type	Indicates the service to use to connect the user to the router. A value of 6 indicates administrative access to the router. Supported values are: ● 1—Login ● 3—Callback-Login Equivalent to the **User Service** set by Type 15, Login-Service. ● 2—Framed ● 4—Callback-Framed Equivalent to the **User Service** set by Type 7, Framed-Protocol. ● 7—NAS prompt ● 9—Callback NAS-prompt Equivalent to **User Service DSPrompt**. ● 6—Administrative User ● 11—Callback Administrative User Equivalent to **User Service DSPrompt** and the User gets Admin privileges.
14	Login-IP-Host	For LOGIN and CALLBACK service types, the IPv4 address of the login host is sent to the RADIUS accounting host.
31	Calling-Station-Id	For reverse telnet and reverse ssh the IP address of the client will be sent. All other server type do not send this field.
32	NAS-Identifier	If the identifier is configured then this field will be sent.
40	Acct-Status-Type	Indicates if this is the beginning or end of a session. Supported values are: 1 = Start 2 =Stop.
42	Acct-Input-Octets	Number of bytes which were received from the user during this session.
43	Acct-Output-Octets	Number of bytes where were transmitted to the user during this session.
44	Acct-Session-ID	A string which identifies the session. The same string must be used in the start and stop messages.
45	Acct-Authentic	Indicates how the user was authenticated. Supported values are: 1 = Local 2 = RADIUS.
46	Acct-Session-Time	Number of seconds for which the user has been connected to a specific session.
47	Acct-Input-Packets	Number of packets which were received from the user during this session.
48	Acct-Output-Packets	Number of packets which were transmitted to the user during this session.
49	Acct-Terminate-Cause	Indicates how the session was terminated: Supported values include: 1 = User Request 2= Lost Carrier 3=Lost Service 4= Idle Timeout 5= Session Timeout 14 = Port Suspended 16 = Callback.
61	NAS-Port-Type	For reverse telnet and reverse ssh connections, a type of Virtual (5) will be sent. For a PPP connection type a type of Async (0) will be sent. For all direct connect service types a type of Async (0) will be sent.
77	Connect-Info	.For reverse telnet, reverse ssh and direct serial connections the serial port baud rate is send to the RADIUS accounting server.

Type	Name	Description
87	NAS-Port-Id	For sessions originating from the serial port: <line-name> or “SERIAL:xx”, where xx starts at serial port 1. For reverse Telnet and SSH Ethernet sessions: “ETH:REVSESS:xx”, where xx is the serial port being accesses, otherwise 00 for a routerrouter management session. For HTTP sessions: “HTTP”
95	NAS-IPv6-Address	The IPv6 address of the router
98	Login-IPv6-Host	For LOGIN and CALLBACK service types, the IPv4 address of the login host is sent to the RADIUS accounting host.

Mapped RADIUS Parameters to Router Parameters

When authentication is being done by RADIUS, there are several Serial Port and User parameters that can be set by the RADIUS server. Any parameters sent by that RADIUS server that are not supported by the router are discarded. Below is a list of the RADIUS parameters and their router parameters:

RADIUS Parameter	
Service-Type	This has no router field, although it needs to be set to **`Framed-User`** in the RADIUS server if the port is set for PPP or SLIP. For a Console Management profile set the RADIUS Service-Type to NAS prompt.
Framed-Protocol	Set to SLIP or PPP service.
Framed-Address	Remote IP Address field under either SLIP or PPP. *Caution:* the exception to the above rule is a **`Framed-Address`** value of 255.255.255.254. When this value is specified in the RADIUS file, the unit will use the Remote IP address configured for a PPP line in the router.
Framed-Netmask	**IPv4 Subnet Mask** field under either **SLIP** or **PPP**.
Framed-Compression	**VJ Compression** field under either **SLIP** or **PPP**.
Framed-MTU	**MTU** field under **SLIP**. **MRU** field under **PPP**.
Idle-Timeout	**Idle Timeout** under the serial port **Advanced** settings.
Login-Service	Corresponds to one of the following **User Service** parameters: **Telnet**, **Rlogin**, **TCP Clear**, **SSH**, or **SSL Raw**.
Session-Timeout	**Session Timeout** under the serial port **Advanced** settings.
Callback-Number	Combination of the **Enable Callback** and **Phone Numbe**r fields under **User**, **Advanced** settings.
Callback-ID	Combination of the **Enable Callback** and **Phone Numbe**r fields under **User**, **Advanced** settings.

Perle RADIUS Dictionary Example

The Router has defined Vendor Specific RADIUS attributes in order for the RADIUS server to be configured to support the router features of Line Access Rights and User Level. These attributes have been defined in ***Supported Radius Parameters*** to allow the RADIUS server to be configured for RADIUS users to have this level of configuration.

See below for an example of the Perle defined attributes for the RADIUS server for an router.

```
# Perle dictionary.
#
#       Perle Systems Ltd.
#       http://www.perle.com/
#
#       Enable by putting the line "$INCLUDE dictionary.perle" into
#       the main dictionary file.
#
# Version:  1.30  21-May-2008  Add attribute for clustered port access
# Version:  1.20  30-Nov-2005  Add new line access right values for ports
#                              up to 49.
# Version:  1.10  11-Nov-2003  Add new line access right values
# Version:  1.00  17-Jul-2003  original release for vendor specific field
support
#

VENDOR  Perle       1966

#   Perle Extensions

ATTRIBUTE   Perle-User-Level            100 integer Perle
ATTRIBUTE   Perle-Line-Access-Port-1    101 integer Perle
ATTRIBUTE   Perle-Line-Access-Port-2    102 integer Perle
ATTRIBUTE   Perle-Line-Access-Port-3    103 integer Perle
ATTRIBUTE   Perle-Line-Access-Port-4    104 integer Perle
.................

#   Perle User Level Values

VALUE   Perle-User-Level    Admin           1
VALUE   Perle-User-Level    Normal          2

#   Perle Line Access Right Values

VALUE   Perle-Line-Access-Port-1    Disabled                0
VALUE   Perle-Line-Access-Port-1    Read-Write              1
VALUE   Perle-Line-Access-Port-1    Read-Input              2
VALUE   Perle-Line-Access-Port-1    Read-Input-Write        3
VALUE   Perle-Line-Access-Port-1    Read-Output             4
VALUE   Perle-Line-Access-Port-1    Read-Output-Write       5
VALUE   Perle-Line-Access-Port-1    Read-Output-Input       6
VALUE   Perle-Line-Access-Port-1    Read-Output-Input-Write 7

VALUE   Perle-Line-Access-Port-2    Disabled                0
VALUE   Perle-Line-Access-Port-2    Read-Write              1
VALUE   Perle-Line-Access-Port-2    Read-Input              2
VALUE   Perle-Line-Access-Port-2    Read-Input-Write        3
VALUE   Perle-Line-Access-Port-2    Read-Output             4
VALUE   Perle-Line-Access-Port-2    Read-Output-Write       5
VALUE   Perle-Line-Access-Port-2    Read-Output-Input       6
VALUE   Perle-Line-Access-Port-2    Read-Output-Input-Write 7

VALUE   Perle-Line-Access-Port-3    Disabled                0
VALUE   Perle-Line-Access-Port-3    Read-Write              1
VALUE   Perle-Line-Access-Port-3    Read-Input              2
VALUE   Perle-Line-Access-Port-3    Read-Input-Write        3
VALUE   Perle-Line-Access-Port-3    Read-Output             4
VALUE   Perle-Line-Access-Port-3    Read-Output-Write       5
VALUE   Perle-Line-Access-Port-3    Read-Output-Input       6
VALUE   Perle-Line-Access-Port-3    Read-Output-Input-Write 7

VALUE   Perle-Line-Access-Port-4    Disabled                0
VALUE   Perle-Line-Access-Port-4    Read-Write              1
VALUE   Perle-Line-Access-Port-4    Read-Input              2
VALUE   Perle-Line-Access-Port-4    Read-Input-Write        3
VALUE   Perle-Line-Access-Port-4    Read-Output             4
VALUE   Perle-Line-Access-Port-4    Read-Output-Write       5
VALUE   Perle-Line-Access-Port-4    Read-Output-Input       6
VALUE   Perle-Line-Access-Port-4    Read-Output-Input-Write 7

..........
```

TACACS+

Although TACACS+ can be used strictly for external authentication, it can also be used to configure Serial Port and User parameters. Therefore, when a user is being authenticated using TACACS+, it is possible that the user's configuration is a compilation of the parameters passed back from the TACACS+ authentication server, the User's router parameters if the user has also been set up as a local user in the router, and the Default User's parameters for any parameters that have not been set by either TACACS+ or the User's local configuration.

User and Serial Port parameters can be passed to the router after authentication for users accessing the router from the serial side and users accessing the router from the Ethernet side connections.

Accessing the Router through Serial Port Users

This section describes the attributes which will be accepted by the router from a TACACS+ server in response to an authentication request for Direct Users.

Name	Value(s)	Description
priv-lvl	1-user EXEC only 10-Web only 11-RESTful API 15-Privileged EXEC and Web	The router privilege level.
Perle_User_Service	0 (Telnet) 1 (Rlogin) 2 (TCP_Clear) 3 (SLIP) 4 (PPP) 5 (SSH) 6 (SSL_Raw)	Corresponds to the User Service setting in the router. If no value is specified, DSPrompt is the default User Service.

Name	Value(s)	Description
service = telnet		Settings when Perle_User_Service is set to 0.
{		
addr =	IPv4 or IPv6 address	
port =	TCP port number	
}		
service = rlogin		Settings when Perle_User_Service is set to 1.
{		
addr =	IPv4 or IPv6 address	
}		
service = tcp_clear		Settings when Perle_User_Service is set to 2.
{		
addr =	IPv4 or IPv6 address	
port =	TCP port number	
}		
service = slip		Settings when Perle_User_Service is set to 3.
{		
routing =	true (Send and Listen) false (None)	
addr =	IPv4 or IPv6 address	
}		
service = ppp		Settings when Perle_User_Service is set to 4.
{		
routing =	true (Send and Listen) false (None)	
addr =	IPv4 or IPv6 address	
port =	TCP port number	
ppp-vj-slot-compression	true or false	
callback-dialstring	phone number, no punctuation	
}		
service = ssh		Settings when Perle_User_Service is set to 5.
{		
addr =	IPv4 or IPv6 address	
port =	TCP port number	
}		
service = ssl_raw		Settings when Perle_User_Service is set to 6.
{		
addr =	IPv4 or IPv6 address	
port =	TCP port number	
}		

Accessing the Router Through a Serial Port User Example Settings

The following example shows the parameters that can be set for users who are accessing the router from the serial side. These settings should be included in the TACACS+ user configuration file.

```
Service = EXEC
{
priv-lvl = x              # x = 1 (User EXEC only)
                          # x = 10 (Web only)
```

```
                        # x = 11(RESTful API)
                        # x = 15(Priviledged EXEC and WEB)

timeout=x                        # x = session timeout in minutes

idletime=x                       # x = Idle timeout in minutes

Perle_User_Service = x           # x = 0 Telnet
                                 # x = 1 Rlogin
                                 # x = 2 TCP_Clear
                                 # x = 3 SLIP
                                 # x = 4 PPP
                                 # x = 5 SSH
                                 # x = 6 SSL_RAW
                                 # If not specified, command prompt
}

#  Depending on what Perle_User_Service is set to

service = telnet
{
addr = x.x.x.x       # ipv4 or ipv6 addr
port = x             # tcp_port #
}

service = rlogin
{
addr = x.x.x.x        # ipv4 or ipv6 addr
}

service = tcp_clear
{
addr = x.x.x.x       # ipv4 or ipv6 addr
port = x             # tcp_port #
}


service = slip
{
routing = x         # x = true (Send and Listen)
                  # x = false (None)
addr = x.x.x.x    # ipv4 addr
}
service = ppp
{
routing = x       # x = true (Send and listen)
                  # x + false (None)
addr = x.x.x.x    # ipv4 or ipv6 addr
ppp-vj-slot-compression = x # x =true or false
callback-dialstring = x # x = number to callback on
}
service = ssh
{
addr = x.x.x.x   # ipv4 or ipv6 addr
port = x         # tcp_port
}
service  = ssl_raw
addr = x.x.x.x   # ipv4 or ipv6 addr
port = x         # tcp_port #
```

```
}

port = x              # tcp_port #
}
```

Accessing the Router from the Network Users

This section describes the attributes which will be accepted by the router from a TACACS+ server in response to an authentication request for Reverse Users. The TACACS+ **`service`** needs to be set to **`EXEC`**/**`raccess`** or just **`raccess`** on the well known port.

Name	Value(s)	Description
priv-lvl	1- (User Exec only) 10- (Web only) 11- (RESTful API only) 15- (Privileged EXEC and Web)	The router privilege level.
Perle_Line_Access_#	# = port number 0 (Disabled) 1 (ReadWrite) 2 (ReadInput) 3 (ReadInputWrite) 4 (ReadOuptut) 5 (ReadOutputWrite) 6 (ReadOutputInput) 7 (ReadOuputWrite)	For the specified line, provides the User's Line Access rights.
timeout	0-4294967	Session timeout in minutes.
idletime	0-4294967	Idle timeout in minutes.

Accessing the Router from the Network User Example Settings

The following example shows the parameters that can be set for users who are accessing the router from the Ethernet side. These settings should be included in the TACACS+ user configuration file.

```
# Settings for telnet/SSH access
service = raccess
{
priv-lvl = x             # x = 1 (User EXEC only)
                         # x = 10 (Web only)
                         # x = 11 (RESTful API only)
                         # x = 15 (Priviledge EXEC and Web)


Perle_Line_Access_i=x   # i = port number
                        # x = 0 (Disabled)
                        # x = 1 (Read/Write)
                        # x = 2 (Read Input)
                        # x = 3 (Read Input/Write)
                        # x = 4 (Read Output)
                        # x = 5 (Read Output/Write)
                        # x = 6 (Read Output/Input)
                        # x = 7 (Read Output/Write)
timeout=x               # x = session timeout in minutes

idletime=x              # x = Idle timeout in minutes
```

Note: Users who are accessing the router through WebManager and are being authenticated by TACACS+ must have the Admin privilege level and the TACACS+ service level must be set to EXEC.

```
# Settings for WebManager access
service=EXEC
{
priv-lvl = x             # x = 1 (User EXEC only)
                         # x = 10 (Web only)
                         # x = 11 (RESTful API only)
                         # x = 15 (Priviledge EXEC and Web)



Perle_Line_Access_i=x   # i = port number
                        # x = 0 (Disabled)
                        # x = 1 (Read/Write)
                        # x = 2 (Read Input)
                        # x = 3 (Read Input/Write)
                        # x = 4 (Read Output)
                        # x = 5 (Read Output/Write)
                        # x = 6 (Read Output/Input)
                        # x = 7 (Read Output/Write)
}
```

Data Logging Feature

This appendix provides additional information about our Data Logging Feature.

Trueport Profile

The following features are not compatible when using the Data Logging feature.

- Allow Multiple Hosts to connect
- Connect to Multiple Hosts
- Monitor DTR-DSR
- Signals high when not under Trueport client control
- Message of the day
- Session timeout

TCP Socket Profile

The following features are not compatible when using the Data Logging feature.

- Allow Multiple Hosts to connect
- Connect to Multiple Hosts
- Monitor DTR-DSR
- Permit connections in both directions
- Authenticate user
- Message of the day
- Session timeout

RESTful API

You can use the Perle's RESTful API to manage your router as an alternative to configuring and managing selected features using the Command Line Interface (CLI), WebManager, or our other configuration methods.
See ***Initial Configuration using the WebManager***f configuring your router for the first time.

Your routerneeds to have an IP address and REST API enabled before you can use the RESTful API feature.

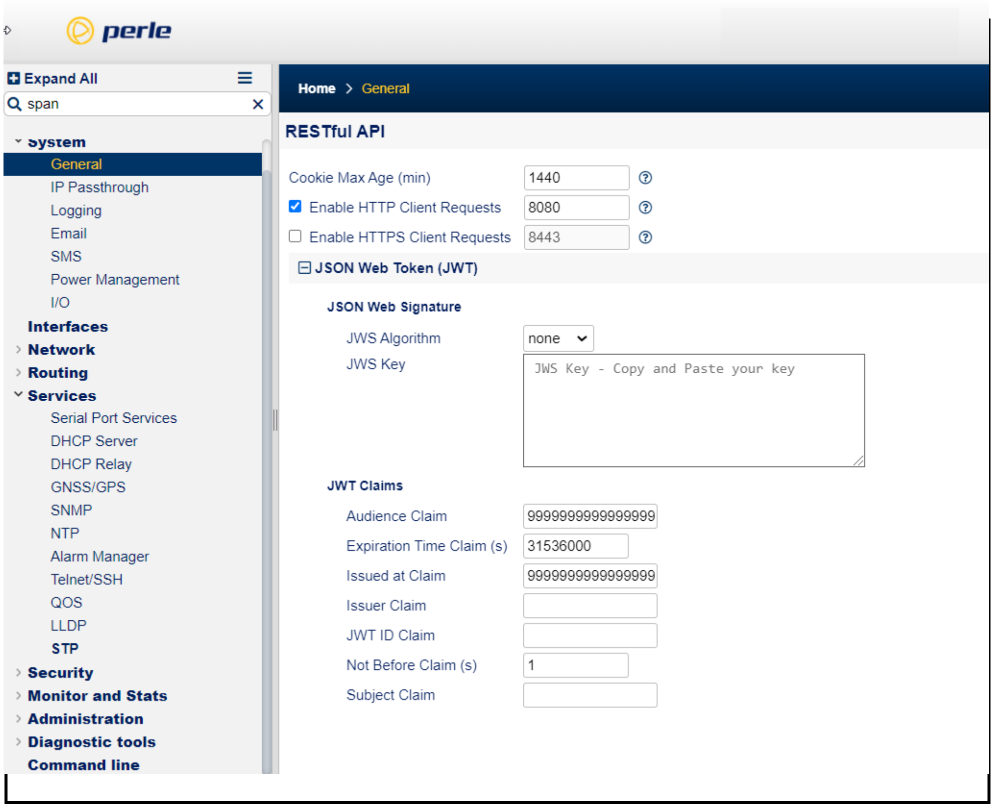
Enabling Restful API Support using CLI

From the PerleRouter command prompt type:

1. PerleRouter>enable
2. PerleRouter#configure terminal
3. PerleRouter(config)#remote-management
4. PerleRouter(config-remote-mgmt)#restful-api http

Enabling Restful API Support using the WebManager

1. From the WebManager left navigation panel, select System, then General.
2. Under Remote Management/RESTful API, configure the parameters for RESTful-API.



RESTful API

Cookie Max Age (min) 1440

☑ Enable HTTP Client Requests 8080

□ Enable HTTPS Client Requests 8443

⊟ JSON Web Token (JWT)

JSON Web Signature

JWS Algorithm none

JWS Key: JWS Key - Copy and Paste your key

JWT Claims

Audience Claim 9999999999999999

Expiration Time Claim (s) 31536000

Issued at Claim 9999999999999999

Issuer Claim

JWT ID Claim

Not Before Claim (s) 1

Subject Claim

Authentication and Authorization Requests

The Perle RESTful API feature supports three authentication methods:

- Basic Authorization
- Cookie Authentication
- JWT Token based Authentication

Basic Authorization

The client sends HTTP requests with the Authorization header that contains the word Basic followed by a space and a base64-encoded string username:password. Basic Authorization is not secure and is recommended only for RESTful APIs over HTTPS secure connections.

Example Authorization: Basic <token>

Cookie Authentication

1. The client sends a login request to the server.
2. On successful login, the router responds with the Set-Cookie header that contains the cookie name, value, expiry time and some other info.

Here is an example that sets the cookie named JSESSIONID: Set-Cookie: JSESSIONID=abcde12345; HttpOnly

3. The client sends this cookie in the Cookie header in all subsequent requests to the server. Cookie: JSESSIONID=abcde12345

4.On logout, the router sends the Set-Cookie header back to the server which then causes the cookie to expire.

Example: Client will need to use "POST http://{{server}}/login" with JSON message body {"username":"name","password":"pwd"} to get the cookie from router. Use the "POST http://{{server}}/logout" request to the router, to log out of the router and delete the cookie.

JWT Token based Authentication

1. The client sends a request "POST http://{{server}}/Session" with the JSON message body {"username":"name","password":"pwd"} to get JWT token.
2. If the login is successful, the router will return the response with a JWT token in message body.

3. The client will send this JWT token in the Authorization header in all subsequent requests to the router.

Example: Authorization: Bearer <jwt token>

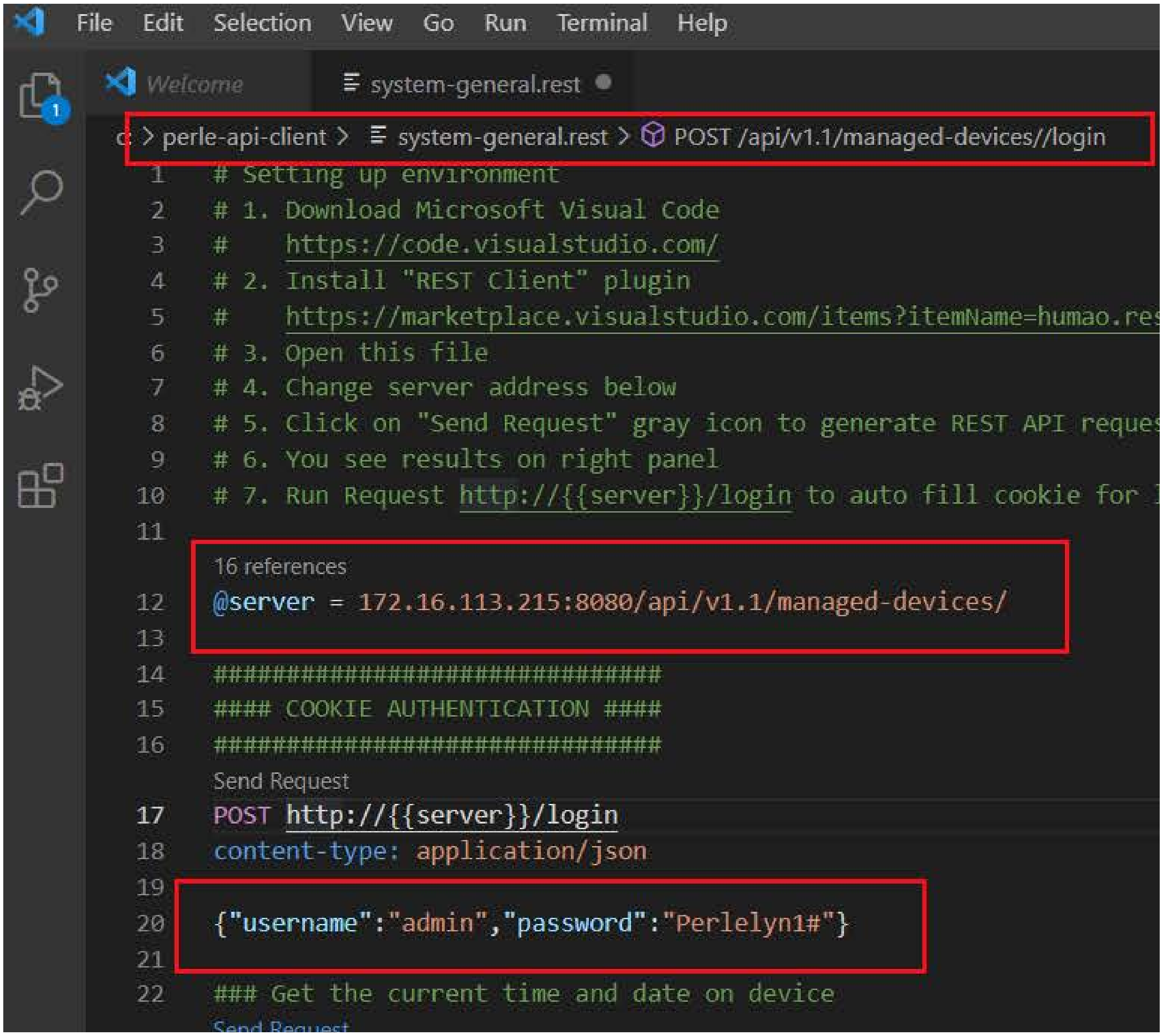
Verifying RESTful API using Windows Visual Studio

To verify and familiarize yourself with our RESTful api feature, do the following:

1. Download and install Visual Studio Code from here -> ***https://code.visualstudio.com/***
2. Download and install the Rest Client from here ->***https://www.perle.com/downloads/software/restful-api/restful-api-client-examples.zip***
3. Download from the Perle Web at ***https://www.perle.com/downloads/software/restful-api/managed-devices.zip*** the yaml restful-api/managed-devices.zip file.

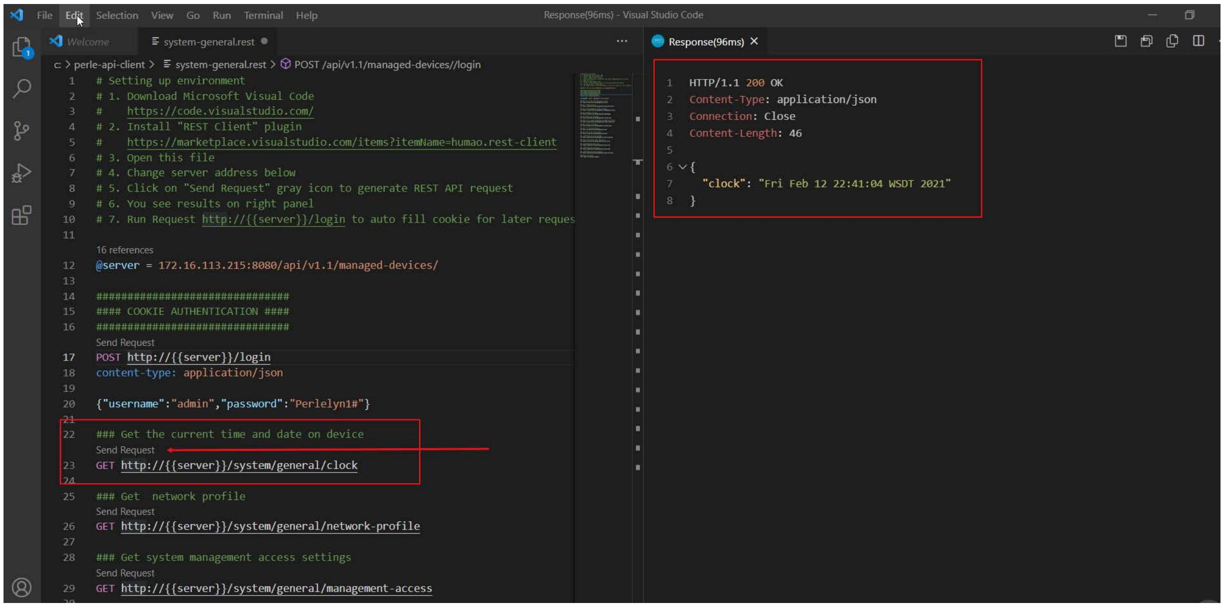
For Example:

1. Open from the Visual Studio Code, select File -> Open file, then select the system-general file from the list of available api files.
2. The file is loaded into Visual Studio Code.
3. Change the @server = localcode:8000/api/v1.1/managed-devices/ line to reference your own IPRouter address.
4. Change the {“myUserName”:”admin”,”myPassword”:”Perlelyn1#”} line to your own username and password.
5. Once you have changed the username and password, click on the grayed out “Send Request” link just above the “Post http://{{server}}/login”. You will see the result on the right hand panel—if the request was successful you will see the response code 200 OK.


File
Edit
Selection
View
Go
Run
Terminal
Help
Welcome
system-general.rest
1
c > perle-api-client > system-general.rest > POST /api/v1.1/managed-devices//login

```
# Setting up environment
# 1. Download Microsoft Visual Code
#    https://code.visualstudio.com/
# 2. Install "REST Client" plugin
#    https://marketplace.visualstudio.com/items?itemName=humao.res
# 3. Open this file
# 4. Change server address below
# 5. Click on "Send Request" gray icon to generate REST API reques
# 6. You see results on right panel
# 7. Run Request http://{{server}}/login to auto fill cookie for 

16 references
@server = 172.16.113.215:8080/api/v1.1/managed-devices/

################################
#### COOKIE AUTHENTICATION ####
################################
Send Request
POST http://{{server}}/login
content-type: application/json

{"username":"admin","password":"Perlelyn1#"}

### Get the current time and date on device
Send Request
```

6. For example to get the current time and date from your Router, select “Send Request”, the result will be displayed in the right column on the screen.



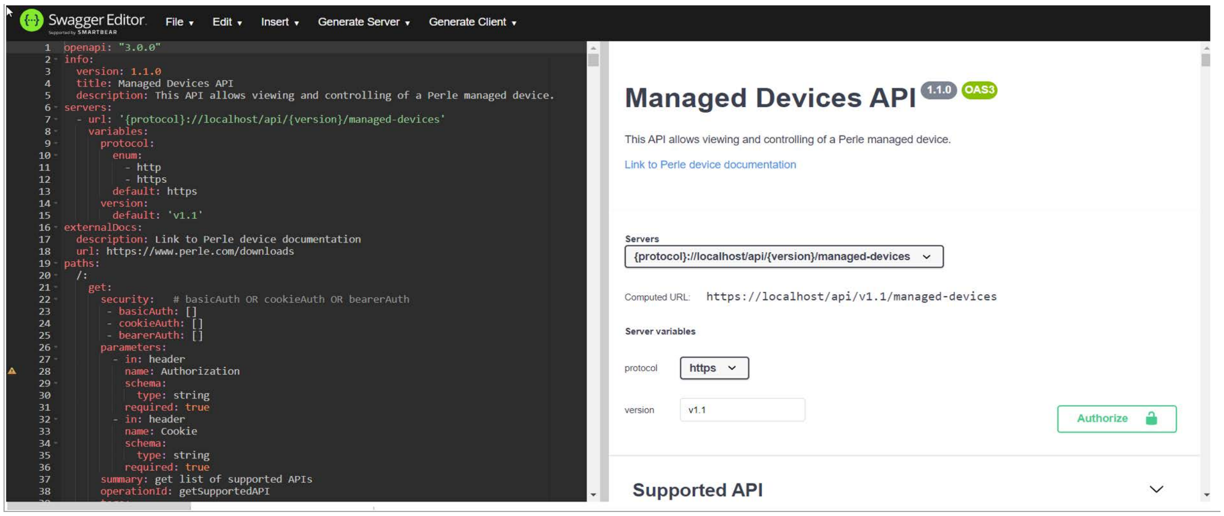
File Edit Selection View Go Run Terminal Help
Response(96ms) - Visual Studio Code
Welcome
system-general.rest
Response(96ms)
c: > perle-api-client > system-general.rest > POST /api/v1.1/managed-devices//login

```
# Setting up environment
# 1. Download Microsoft Visual Code
#    https://code.visualstudio.com/
# 2. Install "REST Client" plugin
#    https://marketplace.visualstudio.com/items?itemName=humao.rest-client
# 3. Open this file
# 4. Change server address below
# 5. Click on "Send Request" gray icon to generate REST API request
# 6. You see results on right panel
# 7. Run Request http://{{server}}/login to auto fill cookie for later reques

16 references
@server = 172.16.113.215:8080/api/v1.1/managed-devices/

################################
#### COOKIE AUTHENTICATION ####
################################
Send Request
POST http://{{server}}/login
content-type: application/json

{"username":"admin","password":"Perlelyn1#"}

### Get the current time and date on device
Send Request
GET http://{{server}}/system/general/clock

### Get  network profile
Send Request
GET http://{{server}}/system/general/network-profile

### Get system management access settings
Send Request
GET http://{{server}}/system/general/management-access
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Connection: Close
Content-Length: 46

{
  "clock": "Fri Feb 12 22:41:04 WSDT 2021"
}
```

Viewing Perle RESTful API Documentation

1. Download the Perle managed-devices.yaml file either from the Perle Website or directly from the routerfolder at flash:managed-devices.yaml.
2. Go to Swagger Editor website at **https://editor.swagger.io/** to import the managed-devices.yaml file downloaded in Step 1.
3. The Perle managed-devices.yaml file is loaded into the Swagger Editor.
4. You are now able to view the Perle RESTful API documentation.



```
openapi: "3.0.0"
info:
  version: 1.1.0
  title: Managed Devices API
  description: This API allows viewing and controlling of a Perle managed device.
servers:
  - url: '{protocol}://localhost/api/{version}/managed-devices'
    variables:
      protocol:
        enum:
          - http
          - https
        default: https
      version:
        default: 'v1.1'
externalDocs:
  description: Link to Perle device documentation
  url: https://www.perle.com/downloads
paths:
  /:
    get:
      security:   # basicAuth OR cookieAuth OR bearerAuth
       - basicAuth: []
       - cookieAuth: []
       - bearerAuth: []
      parameters:
        - in: header
          name: Authorization
          schema:
            type: string
          required: true
        - in: header
          name: Cookie
          schema:
            type: string
          required: true
      summary: get list of supported APIs
      operationId: getSupportedAPI
```

Managed Devices API 1.1.0 OAS3

This API allows viewing and controlling of a Perle managed device.

Link to Perle device documentation

Servers: {protocol}://localhost/api/{version}/managed-devices

Computed URL: https://localhost/api/v1.1/managed-devices

Server variables

protocol: https

version: v1.1

Appendix—Regions

The following is the complete list of the regions which are supported on the WiFi interface.

- **Canada**
- **United Kingdom**
- **US (default)**
- **Andorra**
- **United Arab Emirates**
- **Afghanistan**
- **Anguilla**
- **Albania**
- **Armenia**
- **Argentina**
- **American Samoa**
- **Austria**
- **Australia**
- **Aruba**
- **Azerbaijan**
- **Bosnia and Herzegovina**
- **Barbados**
- **Bangladesh**
- **Belgium**
- **Burkina Faso**
- **Bulgaria**
- **Bahrain**
- **Saint Bartholemy**
- **Bermuda**
- **Brunei**
- **Bolivia**
- **Brazil**
- **Bahamas**
- **Bhutan**
- **Belarus**
- **Canada**
- **Central Africa Republic**
- **Cote d'Ivoire**
- **Chile**
- **China**
- **Colombia**
- **Costa Rica**

- **Cuba**
- **Christmas Island**
- **Cyprus**
- **Czech Republic**
- **Germany**
- **Denmark**
- **Dominica**
- **Dominican Republic**
- **Algeria**
- **Ecuador**
- **Estonia**
- **Egypt**
- **Spain**
- **Ethiopia**
- **Finland**
- **Micronesia**
- **France**
- **France**
- **United Kingdom**
- **Grenada**
- **Georgia**
- **French Guiana**
- **Ghana**
- **Greenland**
- **Greece**
- **Guatemala**
- **Guam**
- **Guyana**
- **Hong Kong**
- **Honduras**
- **Croatia**
- **Haiti**
- **Hungary**
- **Indonesia**
- **Ireland**
- **Israel**
- **India**
- **Iran**
- **Iceland**
- **Italy**

- **Jamaica**
- **Jordan**
- **Japan**
- **Kenya**
- **Cambodia**
- **Saint Kitts and Nevis**
- **North Korea**
- **South Korea**
- **Cayman Islands**
- **Kazakhstan**
- **Lebanon**
- **Saint Lucia**
- **Liechtenstein**
- **Sir Lanka**
- **Lesotho**
- **Lithuania**
- **Latvia**
- **Morocco**
- **Monaco**
- **Moldova**
- **Montenegro**
- **Saint Martin**
- **Marshall Islands**
- **Macedonia**
- **Mongolia**
- **Macau**
- **Northern Mariana Islands**
- **Mauritania**
- **Malta**
- **Mauritius**
- **Maldives**
- **Malawi**
- **Mexico**
- **Malaysia**
- **Nigeria**
- **Nicaragua**
- **Netherlands**
- **Norway**
- **Nepal**
- **New Zealand**

- Oman
- Panama
- Peru
- French Polynesia
- Papua New Guinea
- Philippines
- Pakistan
- Poland
- Saint Pierre and Miquelon
- Puerto Rico
- Portugal
- Palau
- Paraguay
- Reunion
- Romania
- Serbia
- Russia
- Rwanda
- Saudi Arabia
- Sweden
- Singapore
- Slovenia
- Slovakia
- Senegal
- Suriname
- El Salvador
- Syria
- Turks and Caicos Islands
- Chad
- Togo
- Thailand
- Tunisia
- Turkey
- Trinidad and Tobago
- Taiwan
- Tanzania
- Ukraine
- Uganda
- United States
- Uruguay

- **Uzbekistan**
- **Saint Vincent and the Grenadines**
- **Venezuela**
- **U.S. Virgin Islands**
- **Vietnam**
- **Vanuatu**
- **Wallis and Futuna**
- **Samoa**
- **Yemen**
- **Mayotte**
- **South Africa**
- **Zimbabwe**