Perle IRG5000 Series Routers User's Guide

Updated: Jan 21, 2020
Revision: A.21.01.2020
Document Part: 5500445-10

Preface

Audience

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

Purpose

This guide provides the information needed to configure and manage the Perle IRG5000 router. This document does not cover hardware features, installation instruction 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. 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.

Publishing History

Date	Revision	Update Details
Jan 22/2020	A.22.01.2020	Initial release of the manual.

Table of Contents

Overview

About the Perle IRG5000 Router Series

The Perle IRG5000 series of routers are compact, rugged, fully featured routers intended for a variety of applications. All routers come standard with an LTE modem supporting, data, SMS and GNSS features. Also standard on all models is a USB-C port that can be used as a serial console port or as an additional Ethernet interface. Depending on the model, there are a variety of combinations of Ethernet, Serial, I/O ports as well as a server/client Wireless LAN (WLAN) interface.

Some models provide LTE CAT6 connectivity with download speeds up to 300 Mbps and some provide LTE CAT12 connectivity with download speeds up to 600 Mbps.

General Features

- LTE coverage supporting 21 or 30 LTE bands (depending on the model)
- Dual SIMs with automatic failover
- Auto APN
- WAN and VPN Fail-over
- Active GPS supporting standard GPS protocols
- Selection of Power Operating Modes
- Routing Protocols including RIP, OSPF, BGP
- Firewall
- WAN Traffic Load Balancing
- IP Passthrough Mode
- IPv6 Support

Management Features

- Web User Interface (WebManager)
- CLI via USB or Serial (model dependent) Console or via SSH/Telnet
- SNMP
- PerleVIEW central management software
- SMS Status and Control
- Alarm and Alert Reporting including SMS and Email
- Auto Software Update Checking

LAN Features

- Gigabit Ethernet on all models
- LAN bridging and/or switching
- 802.1x
- DHCP Server, Client and Relay
- DNS Server / Forwarding / DDNS / Caching
- VLAN / Sub-interface

WLAN Features (model dependent)

- 802.11 a/b/g/n/ac
- Server or Client Mode
- Bridging to Ethernet LAN

- WPA2
- Multiple SSIDs
- DNS Server / Forwarding / Caching

Serial Features (model dependent)

- Full Device Server, Terminal Server and Console server functionality
- Virtual modem emulation
- Serial Redirector using Perle's TruePort utility
- Modbus master/slave/gateway support
- Remote access support via PPP
- Serial port tunneling with other Routers or Perle Device, Terminal or Console Servers.

Hardware Features

- Gigabit Ethernet interfaces – all models
- I/O's and relay for alarm signaling or Power Management Control
- Ignition monitoring for in-vehicle installation
- Low power operating modes (model dependent)
- IP54 or DIN enclosures

Security Features

- OpenVPN
- IPSEC
- SSL and HTTPS support
- Two factor authentication for Web and CLI
- Radius and TACACS+

Initial Setup

Hardware Installation

The following steps provide a simplified method of doing an initial setup. Detailed instructions for each of these steps can be found in the Hardware Installation Guide.

1. SIM Installation

In order to access LTE services, an activated SIM will be required. Wireless providers offer a variety of plans including voice, data and SMS. To use the LTE modem on the router, the plan must have “data”. If you wish to make use of the router’s ability to send or receive text messages, you need to ensure that the plan also include the “SMS” services. The router does not make use of any “voice” services. Once an activated SIM has been provisioned by the wireless provider it can be used in the router. A second SIM can also be installed for failover or roaming purposes. The carrier will provide you with the preferred APN to use. However, if this is not initially available, the router will attempt to determine the best APN to use based on the SIM.

Refer to the Hardware Installation Guide for instructions on inserting the SIM(s).

2. Antennas

Refer to the Hardware Installation Guide for instructions on connecting antennas for LTE, GNSS and WLAN.

3. LAN Connection

From the factory the router comes with the Ethernet connectors bridged together as a single LAN, with an IP address of 192.168.0.1. On this LAN connection the router is acting as a DHCP server to provide IP addresses to any connected devices.

Warning: Do not connect any of the routers Ethernet ports to an existing network, since the DHCP service on the router may interfere with existing DHCP services on the network. The default configuration would have to be changed before this connection can be made.

It is recommended that a single PC is connected to one of the Ethernet ports for doing the initial setup.

4. USB Connection

If you plan to configure the router using the Command Line Interface (CLI), the recommended method for initial setup is to use the USB console port.

5. Connect the power source

See the Hardware Installation Guide for instructions and guidelines on connecting the power. Once power has been applied to the router the “Power” LED will begin to flash with the colour Amber. When the Power LED flashes green, the router has completed its power up cycle. Flashing green indicates that it is still running the factory default configuration. Once the unit has been setup the LED will be solid green.

Configuration

Performing initial configuration using the WebManager

1. Connect your PC

If using a wireless interface on your PC, use the SSID (Network Name) and password printed on the label on the bottom of the router to connect to the router.

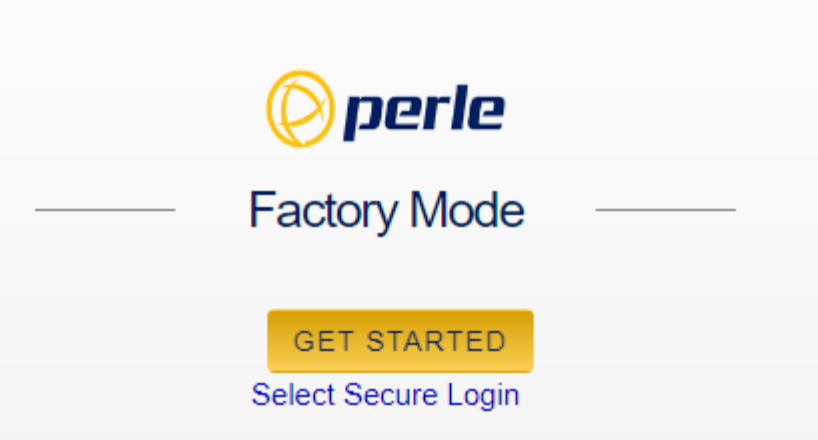
2. If using a wired interface on your PC, you can connect to any of the Ethernet ports and proceed to Step 3.

3. IP Address

Ensure the PC is setup to obtain an IP address automatically (DHCP).

4. Web Browser

From a web browser, enter the IP address 192.168.0.1. The Fast Mode Setup screen will be displayed.



Fast Setup mode

This mode is available when the router is in “Factory Default” mode. Once the router is configured, it is no longer in this mode. You can return to this mode anytime by resetting the router to factory defaults.

Fill in the required fields, apply changes to save and exit. The configuration changes will be immediately applied to the router.

Note: If you have selected to only allow secure web access (HTTPS) your web browser will be re-directed to the appropriate sign on screen following Fast Setup.

5. Sign-in to Access full configuration

Once Fast Setup has been completed, you will now have an administrators UserID and Password. These can now be used to sign-in to the full configurator.

Performing Initial Configuration using the Console

1. IP Connected PC's

If CLI is to be accessed using Telnet or SSH, follow the same steps as above for connecting the PC to the wired or wireless network

2. Console Port Access

If the CLI is to be accessed using the console port follow the instructions listed here.

- Connect a USB to USB-C cable between the router's USB port and a USB port on your PC.
- From the Windows PC choose Start > Control Panel > Systems. Click the Hardware tab and choose Device Manager to identify the COM port created.
- From a terminal-emulation program (such as Putty or SecureCRT) use the COM port identified above (ex. COM6).
- From the emulation window, press the <enter> key on your keyboard until you see "Configure basic operating parameters for the router"?(yes/no)

Type "yes" to begin the Fast Setup process. Once this is complete you can proceed to detailed configuration if required.

Managing the Router

Using the WebManager

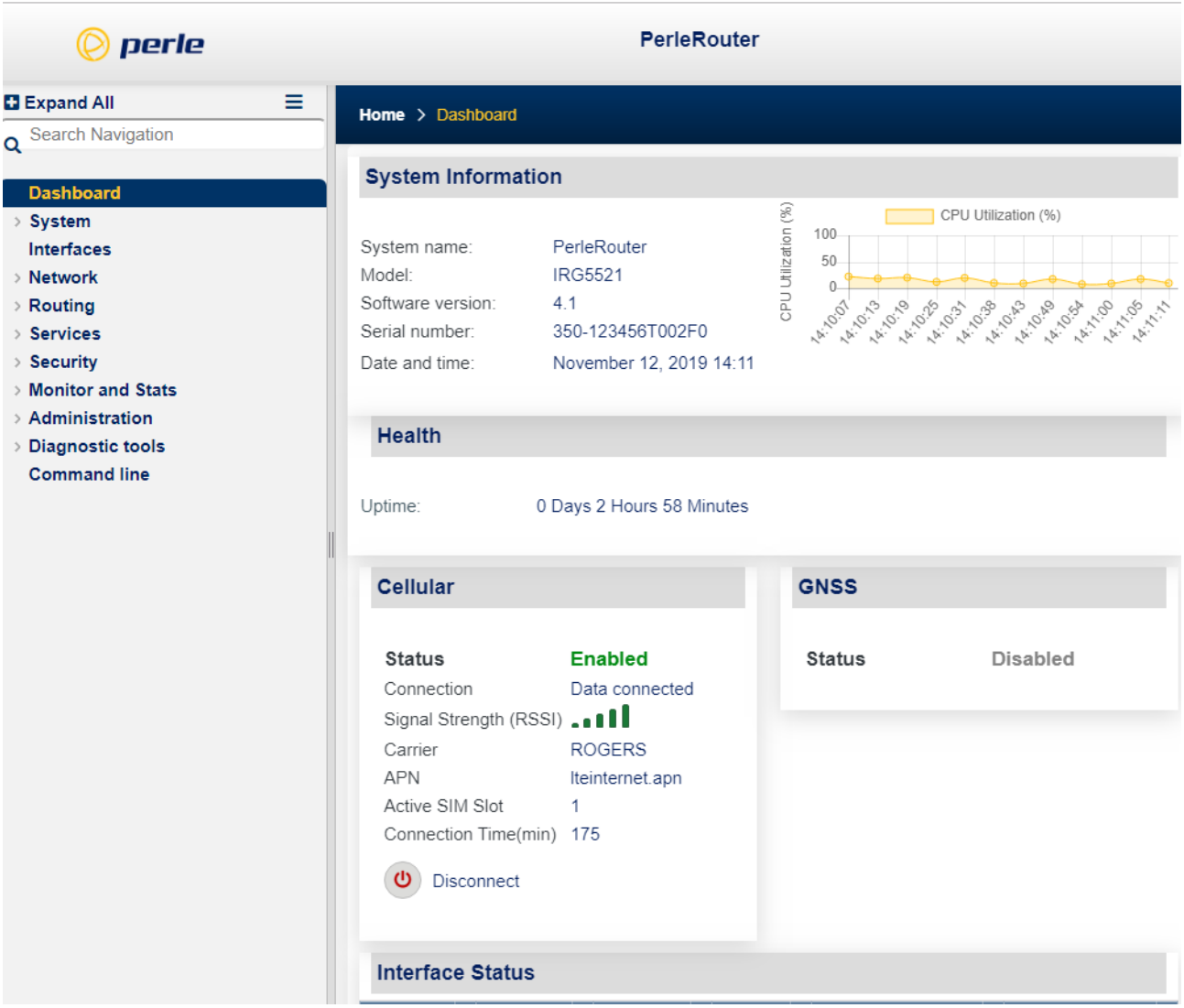
The Perle WebManager is an embedded Web based application that provides an easy to use browser interface for configuring and managing your router. The WebManager is accessible through any standard desktop web browser either through a secure or non-secure connection.

Navigating the WebManager

WebManager uses expandable/collapsible sections in the navigation panel. Expandable sections are indicated by the ">" symbol.

Search Navigation

A search tool is provided on the top of the navigation panel to facilitate finding a specific keyword in the navigation panel.



Using the CLI (Command Line Interface)

A familiar text-based Command Line Interface based on accepted industry standard syntax and structure is provided. This interface which is ideal for network industry certified engineers, is available on the router console or IP based sessions like SSH or Telnet.

Note: If using CLI to perform the initial configuration of the router (also known as “fast setup”), you must connect to the router via the console port.

CLI via the USB port

All models of the router come standard with a USB port featuring a USB-C connector. By default this port is configured to run the console. Connecting to a PC will generate a COM port on the PC that can be used by a terminal emulation program such as Putty or SecureCRT to manage the router.

CLI via the Serial Port

On models that are equipped with a serial port (DB9-RS232), this port can be configured to run the console instead of running it on the USB port. If this option is chosen, the port communication parameters of the PC will need to be setup to match those on the router's serial port. Using the serial port for console can be handy if the USB port has been re-purposed to be an additional Ethernet port.
The default parameters for the serial port are;

- tty 1 mode console
- line console 0
- media-interface tty 1
- 9600 Baud
- 8 Data bits
- 1 Stop bit
- No Parity
- No flow control

See the Perle IRG5000 Series Router CLI Reference Guide to see how to set these parameters using the CLI commands.

Configuration Files

The router 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 which is stored in flash memory and used every time the router is rebooted. This is referred to as the "startup-config".

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 (with only a few exceptions) take effect immediately and will be persistent (maintained after a restart of the router).

When making changes to the configuration using the CLI, these changes are applied to the "running-config" and take effect immediately. To make these changes persistent, the running-config file will need to be copied to the "startup-config".
For detailed information on the CLI, please refer to the Router, CLI Reference Guide available for download from the Perle web site at *https://www.perle.com*.

System

General

This section allows you to setup general router information.

Identification	
System name	**Provide your router with a 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 clock time.**
Change Date and Time	**Manually change the router's time.**
Change Time Zone	**Manually change the router's time zone.**

IPv6

By default, the router ships with IPv6 turned off. Enabling or Disabling IPv6 will require a system reboot. The router has a factory default link local IPv6 address 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 will listen for IPV6 router advertisements to obtain additional IPV6 addresses. No configuration is required, however, you can manually configure IPV6 addresses and network settings.

IPv6	
Enable IPv6	**Activate IPv6 on the next boot. This will add relevant configuration screens and CLI commands.**

Management Access

The parameters in this section define how management access to the router is controlled. In addition, protocol based access control is used to restrict access by interface. The router will, by default, allow management access for LAN type interfaces (e.g. Ethernet), and deny access for WAN type interfaces (e.g. Cellular). From within each interface configuration screen you can instruct the router to treat that interface as a WAN or as a LAN.

Management Access	
Access Restriction	**Enable or disable access restrictions.**
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** **Default for LAN interfaces is allow.**
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** **Default for WAN interfaces is not allow.**

Command Line	
Access Command Line	**When a connection is made with any of these methods, you effectively get a console to the router. This option determines which of these methods allow CLI access.** • ***Telnet*** **– Telnet session** • ***SSH*** **– SSH Session** • ***Console*** **– Physical console port**

Console Port	
Select Console Port	• ***USB*** **– USB port will be the console port. Note: if using the USB port in console mode, you must set up the USB Interface Mode to USB-Console. See *Select how the USB interface will be used.*** • ***None*** **– no console port** • **tty1 – select tty1 to use this port as a serial (RS232) port (model dependent) Note: if using the tty1 in console mode, you must set up the usage mode to serial-console mode. See *TTY Usage mode* for setting the port to serial-line mode.**

WebManager Access

WebManager can be accessed by HTTP (non-secure) or HTTPS (secure). If HTTPS connections are used, a certificate will need to be uploaded to the router. If a certificate is not uploaded, the router will use a self-signed certificate. You will be given a warning by the browser indicating that the identify of the target web site could not be verified.

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

WebManager	
WebManager	**Specify protocols to be supported by the WebManager.** • ***HTTP*** **- Allow non-secure Web sessions** • ***HTTPS*** **- Allow secure Web sessions** • ***Port – Port to use for HTTPS sessions*** • ***Idle Timeout*** **– Amount of time to wait before disconnecting an idle Web session**

SNMP	
Enable SNMP	**The internal SNMP server will be activated.** **Note: When enabling SNMP you must ensure that the "From LAN" and "From WAN" match the interface access that is desired**

IP Passthrough

Overview

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 will be given the IP address provided by the cellular network. All data will be pass straight through to and from the device to the cellular network.

When operating in this mode, most of the router configuration will be ignored. Routing, firewalls or other functions will not be activated. IP Passthrough is supported on either the Ethernet port or the USB-C port configured as Ethernet.

To enable and disable this feature a reboot is needed.

IP Passthrough	
Enable	**This enables IP passthrough mode and reboots the router. After the reboot, any non IP passthrough commands become invalid. If you user issues a copy running-config to startup-config, the non IP passthrough commands will be lost. You should save your current running configuration to another file for safety. This feature will require a reboot. Default is disabled**
Router Management IP Address	**The device connected to the Ethernet will receive the address from the cellular connection. However, the router itself will still be addressable for management purposes using this IP address. Default IPv4 address is 192.168.0.1**
Restrict to specific MAC hardware address	**If this option is not checked, the router will passthrough to the first device that connects on the Ethernet. If checked the router will only passthrough to the device whose MAC has been specified. Default is disabled**
MAC Address	**MAC address of device to be used in IP Passthrough mode.**

Logging

The router has the ability to communicate and log event messages such as monitored alarms:

- to its local volatile "buffered" memory log
- to a file stored on the router's non-volatile flash memory
- to an external Syslog server
- telnet sessions

- or the serial console port

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	**Set messages per second.** **1 - 1000 per messages/second**
....except messages with a severity of x or higher	• **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notification** • **Informational** • **Debugging**
Timestamp	
Include timestamp in log messages	**Enable timestamps in log messages. Select timestamp type and include information.**
Timestamp type	• **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 interface for sending messages to syslog from the drop-down list.**
Syslog facility	• **Local7** • **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** • **Local 7**

Origin ID Source	• None • IP • IPv6 • Hostname • Custom
Custom Origin ID	You can append the hostname, an IP address, or a text string to Syslog messages that are sent to remote Syslog servers.
Append delimiter to syslog messages over TCP	Add line feed delimiter to Syslog messages.
Syslog (Add, Edit, Delete)	
Hostname/IP address	Hostname or IPv4/IPv6 address.
Transport	Choose a transport method. • UDP • TCP
Port	Port number for the syslog message. Default is 514
Console	
Enable logging on the console port	This command turns console logging on and specifies the level of logging to be directed to the console. (The default setting is enabled.).
Level	• Emergency • Alert • Critical • Error • Warning • Notification • Informational • Debugging
Telnet/SSH	
Enable logging on Telnet/SSH sessions	This command copies monitor logging messages to the current virtual, (vty, SSH or telnet session).Enable or disable logging for the console port.

Level	• Emergency • Alert • Critical • Error • Warning • Notification • Informational • Debugging
Buffered	
Enable buffered logging	This command enables sending logging messages to the an internal RAM buffer and you can also specify the level of logging desired to be buffered and how much RAM to use.
Level	• Emergency • Alert • Critical • Error • Warning • Notification • Informational • Debugging
Maximum Size	Buffer size is <4096-32768> (Default is 16384 bytes).
File	
Enable file logging	Enables sending logging messages to a file 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 message will stop being stored in the previous filename and start being stored in the new defined logging filename. (The default setting is disabled.)

Level	• **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notification** • **Informational** • **Debugging**
Filename	**Enter the name for the log file.**
Minimum Size	**Enter the minimum size of the log file.** **Values: 1024 – 2147483647** **Default: 2048**
Maximum Size	**Enter the minimum size of the log file.** **Values are 4096 – 2147483647** **Default is 4096**

Email

Overview

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	
Enable	**Enabling Email notifications.**
Encryption	**Emails are to be encrypted using;** • **None** • **SSL** • **TLS**
From	**Specify the Email address that the Email will appear to be From.**
SMTP Server Host	**IP Address of the SMTP host that will be used to send the Email.**
SMTP Server Port	**Port number on the SMTP host required for the connection.**

Username / Password	**Username and password required to authenticate with the SMTP server.**
Validate Email Certificate	**Validate the certificate provided by the SMTP server.**
Email Recipients	
Email Address	**Email address of the recipient.**
Email Subject Line	**Subject line that will be contained in the Email.**
Notifications Sent	**List of events that this recipient will receive.**

SMS Settings

Overview

The router supports SMS control and SMS Notifications. In order to use this function, verify with your cellular provide to ensure that SMS functionality has been enabled.

SMS Control

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

<password> <command>

For example, if the user password was 54321 and they wanted to get a list of valid SMS commands, they would send the follow SMS Message to the phone number of the router.

54321 help

You will receive a list of valid commands with any invalid command.
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 the valid commands.**

Reload	**Reboot the router.**
Status	**Returns a general router status.**
LTEStatus	**Returns status specific to the LTE data connection.**
Model	**Information about the router.**
MReset	**Reset the modem portion of the router only. Both data and SMS connectivity will be lost for up to 1 minute.**
Log	**Returns the last 16 entries of the system log file, each in a separate SMS message.**
LTEDisc	**Disconnect the LTE Data connection. Will return OK to indicate that the message is being acted upon. LTEStatus will indicate the current connection status.**
LTEConn	**Establish an LTE Data connection. Will return OK to indicate that the message is being acted upon. LTEStatus will indicate the current connection status.**
Location	**Returns the GPS co-ordinates of the current location, if there is a location fix.**

SMS Notifications

Notifications generated by the router can be sent one or more recipients via SMS. Setting up the SMS notifications subsystem requires enabling SMS and configuring a list of users/recipients and enabling the notifications feature on each.

SMS Control / Notifications	
Enable	**Enabling SMS.**

User Authentication Method	**Only required for SMS control, this dictates the method used for authenticating all incoming requests.** • ***None*** **– No Authentication Required** **Note: all users automatically default to Admin privilege when authentication is disabled.** • ***Password*** **– User must provide a password on every text message** • **Phone *Number* – Incoming messages will be authenticate by the source phone number** • ***Both*** **– Both matching phone number and password are required**
SMS Users	
Name	**User Name - for identification only**
Privilege	**User Privilege** • ***Admin*** **– Full SMS management allowed** • ***Restricted*** **– May solicit router 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 needed if required for authentication.**
Notifications	**Notifications to be sent to this user. You may enable as many of the following notification types in the SNMP notification configuration as they wish;** **Alarms, authentication, cellular-gnss, bgp, dot11, cellular-lte, envmon, entity, ipsec, openvpn etc**

Power Management

Overview

Power Management falls into 2 categories;

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

1. Power savings while maintaining full functionality

Following is a list of items that can be employed for power savings:
Interface Disable – Each physical interface can be disabled.
GNSS Receiver Disable – Shutting down the GNSS Radio will save power if location services are not needed.
Cellular – Radio Enable – Disabling the cellular radio will save power if LTE data services are not required and will not have an effect on the GNSS radio.
Cellular – Module Power Up – If the module is not powered up neither LTE nor GNSS functions will be available. Maximum power savings if these are not needed.
LED Low Power – Reduces LED usage to save power.
Processor Low Power – The microprocessor will slow itself down when there is reduced activity on the router.

2. Power Operating Modes

Standby – When in standby mode, the router is essentially powered off. However, there are a few low power circuits that are kept running in order to monitor the internal and external environments in order to determine when to power the router back up and take it out of standby mode.

When the router is in standby mode, a low frequency LED blip is displayed. If there is need to power up the router, even though the power up conditions are not met, this can be done by pressing the reset button. This will take the router out of standby mode and power it up, enabling configuration changes to be made. After 12 minutes the router will return to the state dictated by the power operating mode configuration. If the delay is no longer necessary, The Standby Resume can be initiated from the Administration Reboot/Reset screen.

Note: If the router is about to enter standby mode and there an active WebManager session, a pop-up window will be displayed for 120 seconds. You will be given the option to delay standby by 6 minutes, at which time this process will repeat.

3. Low Voltage Standby (LVS)

LVS is a battery saving feature. This is used to monitor the input voltage (presumably from a battery) and if the voltage dips below a certain threshold, the router is put into standby mode. This protects the battery from further drain. If the voltage is restored, the router can be configured to take itself out of standby and power back up.

Low Voltage Standby	
Contact	**The input that will be used for monitoring the voltage. Since the actual input power connection cannot be monitored, this contact will need to be connected to the power input.** • ***IGN*** **- Ignition Input on power connector** • ***GPIO*** **- GPIO Pin on the power connector**

Standby Delay	**If the router detects that the "contact voltage" has dropped below the "standby voltage" level, it will wait this number of seconds. If the voltage is still below this level, the router will go into "Low Voltage Standby" mode.** **Default is 30 seconds**
Wakeup Delay	**If the router detects that the "contact voltage" has gone above the "wakeup voltage", it will wait this number of seconds. If the voltage is still above this level the router will be taken out of standby and will power back up.** **Default is 1 second**
Standby Voltage	**When the "contact voltage" goes below this setting, the router will begin initiating low voltage standby mode, following the "Standby Delay".** **Default is 9V**
Wakeup Voltage	**When the "contact voltage" goes above this setting, the router will initiate the power up sequence following the "Wakeup Delay".** **Default is 10.8V**

Standard – In this mode the router will not go into standby mode.
Ignition – In this mode the router will monitor an input to determine if the vehicle ignition switch has been turned on or not (see Deployment documentation in the Hardware Installation Guides for information on how to make the appropriate connections). When the ignition is determined to be on the router will power up and come out of standby, and when ignition is off, it will go into standby.

Ignition	
Contact	**The input that will be used for monitoring the ignition voltage.** • ***IGN*** **- Ignition Input on power connector** • ***GPIO*** **- GPIO Pin on the power connector.** **Note: The GPIO pin will need to be configured to be an analog input. (See I/O section)**

Standby Delay	**If the router detects that the "contact voltage" has dropped below the "standby voltage" level, it will wait this number of seconds. If the voltage is still below this level, the router will go into "Standby" mode.** **Default is 30 seconds**
Wakeup Delay	**If the router detects that the "contact voltage" has gone above the "wakeup voltage", it will wait this number of seconds. If the voltage is still above this level the router will be taken out of standby and will power back up.** **Default is 1 second**
Standby Voltage	**When the "contact voltage" goes below this setting, the router will begin initiating low voltage standby mode, following the "Standby Delay".** **Default is 1.0V**
Wakeup Voltage	**When the "contact voltage" goes above this setting, the router will initiate the power up sequence following the "Wakeup Delay".** **Default is 9V**

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.

Smart Standby	
Condition Type	**The type of condition monitored.** • ***Analog*** **– Analog input** • ***Digital*** **– Digital input** • ***Schedule*** **– The actual date and time will be monitored and used to determine when this condition is true**
Condition Type: Analog Input	
Contact	The input that will be used for monitoring the analog input. • ***IGN*** **– Ignition Input on power connector** • ***GPIO*** **– GPIO Pin on the power connector.**

Standby Delay	**If the router detects that the "contact voltage" has moved beyond the "standby voltage" (below or above depending on user configuration), it will wait this number of seconds and if the voltage level is still beyond the "standby voltage", the router will go into "Standby" mode. Default is 1 second**
Wakeup Delay	**If the router detects that the "contact voltage" has moved beyond the "Wakeup voltage" (below or above depending on user configuration), it will wait this number of seconds and if the voltage is still beyond the "Wakeup voltage", the router will be taken out of standby and will power back up. Default is 1 second**
Standby When Voltage Condition	**Select the condition to apply to the "Standby voltage" level.** • ***Greater than*** **- Take action when the "contact voltage" level goes above the "Standby voltage".** • ***Less than*** **- Take action when the "contact voltage" level goes below the "Standby voltage".**
Standby When Voltage	**When the "contact voltage" meets the "condition" defined above, the router will apply the "Standby delay" and then will begin initiating low voltage standby mode.**
Wakeup When Voltage Condition	**Select the condition to apply to the "Wakeup voltage" level.** ***Greater than*** **- Take action when the "contact voltage" level goes above the "Wakeup voltage".** ***Less than*** **- Take action when the "contact voltage" level goes below the "Wakeup voltage".** **Note: The condition is not configurable. It is always set to the opposite of the "Standby When Voltage" condition.**
Wakeup When Voltage	**When the "contact voltage" meets the "condition" defined above, the router will apply the "Wakeup delay" and then will begin initiating the power up sequence.**

Condition Type: Digital Input	
Contact	**The input that will be monitored for this condition.** • ***GPIO*** **- GPIO Pin on the power connector** **Note: The GPIO pin will need to be configured to be a digital input. (See I/O section)** • **I/O (A or B) - Some models have two additional I/O pins. These can also be used as the contact to monitor**
Wakeup Trigger	**Define the digital input condition (trigger) that will initiate the wakeup. The opposite value will initiate going into standby.** **Open - Detect connected digital contact switch is open**
Wakeup/Standby Delay	**The amount of time to wait before changing between the two states.**
Condition Type: Schedule	
Frequency	**This is used to set up a schedule that will make this condition true for initiating standby.** • ***Daily: Define a daily power schedule*** • ***Hourly: Define an hourly power schedule***
Daily Wakeup Time	**Time of day that the router will wakeup and come out of standby. Specify using the 24 hour clock in the HH:MM format.**
Daily Standby Time	**Time of day that the router will go into Standby. Specify using the 24 hour clock in the HH:MM format.**
Hourly Wakeup Time	**Minutes within the hour that the router will wakeup and come out of standby. Specify the minute.**
Hourly Standby Time	**Minutes within the hour that the router will go into Standby. Specify the minutes.**
Repeat	**How ofter to repeat the schedule in days or hours depending on the type of schedule defined.**
Conditional Expression	

Condition Expression	**This field exists if more than one condition is defined. It is used to determine what will cause the power state change to occur.** • ***OR* – Either "condition 1" or "condition 2" being true will cause the power state change.** • ***AND – Both "condition 1" or "condition 2" will need to be true before the power state will occur.***

Overheat Standby

If the temperature remains above the high threshold for 5 minutes, the router will go into Standby and remain in Standby until the temperature returns to the normal operating range. The high threshold can be configured within Alarm Manager /Primary/High Threshold menu.

I/O

Overview

Depending on the model, the router will have a combination of 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

IGN – On models that have this analog input, it is located on the power input connector. In vehicular applications this input would typically be used to monitor the vehicle ignition, however it can be used as a general-purpose analog input. 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 convert from voltage to a more meaningful unit of measurement, the following formula can be used;
Units = coefficient * voltage read + offset

Units – Meaningful units for measurement

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**
- Will allow 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**
- Will allow fractions up to 3 decimal points, for example 23.521

- Default is 0

I/O: IGN	
Description	**A description which will help you identify the equipment being monitored.**
Analog Input Transformation	**See formula above.**
I/O: GPIO	
Description	**A description which will help you identify the equipment being monitored.**
Direction	• ***Input*** **– Digital input** • ***Output*** **– Digital output**
Digital Input	
Power Source	**How is the input powered?** • ***Wet*** **– Connected device is providing the power** • ***Dry*** **– Router high side pull-up will be engaged** **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.**
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.**

Interfaces

Introduction

Fundamentally the router works with interfaces. Any routing rules, firewalls, Natting all relate back to interfaces. The router support a number of different types of interfaces and each my have it own characteristics and capabilities. There are a few very basic types of interfaces that will be used in most applications and there are some more advanced also discussed in this section.

Ethernet

The Ethernet interfaces are one of the basic elements of the router. These interfaces the connecting of devices or switches or other routers. They can be used as a gateway to a LAN or to provide WAN functionality to the routers.

An Ethernet interface can be:

- Included into a bridge
- Configured to support VLANs using sub-interfaces
- Used as a LAN or a WAN

VLAN

Each Ethernet interface can support sub-interfaces with enable the transport and segregation of VLAN traffic. For example if Ethernet 3.51 is defined, the traffic on the sub interface would be associated with and tagged as belonging to VLAN 51.

Bridge

A bridge is a way of connecting several interfaces and having the behave as a single Local Area Network (LAN). When configured this way all devices attached to any of the interfaces in the bridge are all part of the same broadcast domain. Be default the router comes configured with all of the Ethernet ports and with the wireless LAN network (WiFi) configured into one bridge. In order to use any of these interfaces on it own, it must first be removed from the bridge.

Cellular

The cellular interface (wlm0) provides the connection to the cellular network. In order to setup a connection, at least one SIM card will be required. For simple connections a the router will automatically attempt to establish a connection. In order to establish a connection an APN will be required. If no cellular profile has been defined the router will set an APN based on the SIM card detected or will attempt to get one from the network. If the carrier requires a specific APN, this can be configured in a cellular profile.

PPPoE

PPPoE allows Internet Service Providers to manage access to accounts via user names and passwords. By using PPPoE, you can virtually “dial” from one node to another over an Ethernet network to establish a point to point connection between client and server and then transport data packets over the connection.

Tunnels

Your router supports three types of tunnels.
They are:

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, Open 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.

Wireless Radio Settings	
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.**
Add Wireless Interface	
SSID Profile	**Select Wireless Profile (1-16)**
Wireless Interface	**Select wlan 1 – 4**
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.**

Access Point – Radio Band	Select 2.4GHz (default) or 5GHz.
Access Point – Wireless Mode	For 2.4GHz select 802.11 b, 802.11 g (default), 802.11 n. For 5GHz select 802.11 a, 802.11 ac, 802.11 n (default).
Access Point – Channel	For 802.11 g/b select the channel for 2.5GHz communications. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (default) or least congested. 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 1, 2 , 3, 4, 5, 6, 7, 8, 9, 10, 11 (default) or least congested. For 5 GHz communications the default channel is 36. Values are 36, 40, 44, 48, 149, 153, 157, 161
802.11 ac	
Set fix antenna-pattern	Enable or disable. Default is disabled
Use default VHT operating channel center frequent	Range is 1 – 173 Default is 42
Auto power save	Select power save enable or disable. Default is disabled
Channel Width option	Select either: • 40/20 MHz (Auto) • 20 MHz only
Maximum A-MSDU length	Select either • 3839 • 7935
Auto power save	Select power save enable or disable. 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 capabilites	Enable or disable. Default is disabled
Require stations t support HT	Enable or disable. Default is disabled.
Short Guard interval capacity	Select: • default • 20 • 40
Set receiving PPDU using STBC	Enable or disable. Default is disabled.
Set transmitting PPDU using STBC	Enable or disable. Default is disabled
802.11 n	
Channel Width option	Select either: • 40/20 MHz (Auto) • 20 MHz only
Maximum A-MSDU length	Select either • 3839 • 7935
Auto power save	Select power save enable or disable. 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	Enable or disable. Default is disabled

Require stations t support HT	Enable or disable. Default is disabled.
Short Guard interval capacity	Select: • default • 20 • 40
Set receiving PPDU using STBC	Enable or disable. Default is disabled.
Set transmitting PPDU using STBC	Enable or disable. Default is disabled
Region	Select region. US/CA default), EU or Japan. Depending on the model you purchased, the Radio Band can be US/Canada, EU or Japan. See the *Perle IRG5400 series Router Hardware Guide* for more information.
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 IPv4 address	
Enable DHCP	Your IP address will be assigned from a DHCP server.
Enable Static	Provide a IP address and network mask for this interface.
Enable DHCP Server	***Using DHCP Server***

Enable IPv6	Select how to obtain the IPv6 address:
	• Auto configuration
	• DHCP
	• Static
	  • Address
	  • Prefix
	  • eui-64

IPv6 Neighbor Discovery	**Router Preference** • **High** • **Medium** • **Low**
Manage config flags	**Enable or disable config flags.** **Default is disabled**
Manage other config flags	**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	**Value of the reachable time field of the IPv6 router advertisement messages.** **Range 1 – 3600000** **Default is 0**
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** **Default is 0**
IPv6 Routing Prefix Advertisement	
Add Prefix	
Address	**Specify an IPv6 address.**
Prefix Length	**Specify the prefix length.** **Range is 0 – 128**
Valid Lifetime (secs)	**Range is 1 – 4294967294 or infinite** **Default is 2591800**
Preferred Lifetime (secs)	**Range is 1 – 4294967294 or infinite** **Default is 604800**

Do not use prefix for online determination	**Enable or disable prefix for online determination.** **Default is off**
Do not use prefix for autoconfiguration	**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 off**
Hop Limit	**Range is 1-255** **Default is off**
RA Interval (secs)	**Range is 1 – 1800** **Defaults is 600**
Minimum Interval (secs)	**Range is 1 – 1350** **Default is 132**
RA Lifetime (secs)	**Range is 1 – 9000** **Default is 1800**
Add DNS	
	Add address of DNS server.
Role	**Used for controlling admin access.** **Default is LAN** **Options:** • **LAN** • **WAN** • **TRUSTED**
MTU Size	**Optional: provide an MTU size.** **Default is 1500** **Range is 64 – 9000**

Ethernet Interface	
Enable/Disable	**Enabled or disabled.** **Default is enabled.**

Description	**Provide a description for this interface.**
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.**
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 port.**
Duplex	**Select half or full duplex to match the connection on both ends.** **Not configurable on USB-Ethernet port.**
Energy Efficient Ethernet	**Select EEE to allow your router to set low-power idle mode on this Ethernet interface when there is no data to send.** **Not configurable on USB-Ethernet port.**
Enable IPv4 address	
Enable DHCP	**Your IP address will be assigned from a DHCP server.**
Enable Static	**Provide a IP address and network mask for this interface.**
Enable DHCP Server	***Using DHCP Server***
Enable IPv6	
Enable DHCP	**Your IPv6 address will be assigned from a DHCP server.**
Enable Static	**Provide a IPv6 address and network mask for this interface.**

Enable IPv6	**Select how to obtain the IPv6 address:**
	• **Auto configuration**
	• **DHCP**
	• **Static**
	  • **Address**
	  • **Prefix**
	  • **eui-64**

IPv6 Neighbor Discovery	**Router Preference** • **High** • **Medium** • **Low**
Manage config flags	**Enable or disable config flags.** **Default is disabled**
Manage other config flags	**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 is 1 – 600** **Default is 1**
Reachable time	**Value of the reachable time field of the IPv6 router advertisement messages.** **Range is 1 – 3600000** **Default is 0**
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 is 1 – 3600000** **Default is 0**
IPv6 Routing Prefix Advertisement	
Add Prefix	
Address	**Specify an IPv6 address.**
Prefix Length	**Specify the prefix length.** **Range is 0 – 128**
Valid Lifetime (secs)	**Range is 1 – 4294967294 or infinite** **Default is 2591800**
Preferred Lifetime (secs)	**Range is 1 – 4294967294 or infinite** **Default is 604800**

Do not use prefix for online determination	**Enable or disable prefix for online determination.** **Default is off**
Do not use prefix for autoconfiguration	**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 off**
Hop Limit	**Range is 1-255** **Default is off**
RA Interval (secs)	**Range is 1 – 1800** **Defaults is 600**
Minimum Interval (secs)	**Range is 1 – 1350** **Default is 132**
RA Lifetime (secs)	**Range is 1 – 9000** **Default is 1800**
Role	• **WAN** • **LAN** • **TRUSTED** **Default is LAN**
MTU size	**Provide an Maximum Transmission Unit (MTU) size.** **Default is 1500**

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 from 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.
Alternate Profile	Select the alternative profile to use for this connection.
NAT Enable	Enabling Network Address Translation (NAT) allows your private network to access a public network.
Connection	
Diversity Antenna Enabled	Use both antennas to improve the quality and reliability of link.
Connect on Demand	The on-demand feature is only applicable for the cellular interface. If the cellular connection is dropped due to inactivity when the idle time has expired, then the connection will be 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.
Establish Connection on Traffic Type	• Transmit • Receive • Receive and Transmit
Drop Connection after inactivity	• Transmit • Receive • Receive and Transmit Default is 5 minutes, range 1-60 minutes

Enable Failover	**Allows a configured redundant profile (link) to be used when primary link fails. The configured alternate profile will be used.**
Reconnect Attempts	**Number of times to attempt to reconnect to the alternate cellular profile.** **Default is 5 times, range 1-100 times**
Switch Profiles if signal goes below (dBm)	**Switch profile if power level goes below configured dBm value.** **Default is -110 dBm, range -150-0 dBms**
Wait period before switching profiles	**Wait until switching profiles.** **Default is 1 minute, range 1-60 minutes**
Attempt to revert back to primary profile after	**Wait the configure time to try to revert back to primary profile.** **Default is 1 minute, range 1-1500 minutes**
Enable IPv6	
Auto configuration	**Enable or disable.** **Default is disabled**
Role	**WLAN for cellular interface.**
MTU Size	**Set the maximum transmission unit size.** **Default is 1280** **Range is 1280 – 9000**

VLAN Interface	
Enable	**Enabled or disabled interface.** **Default is enabled**
Ethernet	**Select the Ethernet interface.** **Range 1-4**
VLAN ID:	**Select the Ethernet interface to be associate with the VLAN ID.**
Description	**Provide a description for this interface.**

Enable IPv4 address	
Enable DHCP	**Your IP address will be assigned from a DHCP server.**
Enable Static	**Provide a IP address and network mask for this interface.**
Enable DHCP Server	***Using DHCP Server***
Enable IPv6	
Enable DHCP	**Your IPv6 address will be assigned from a DHCP server.**
Enable Static	**Provide a IPv6 address and network mask for this interface.**

Enable IPv6	**Select how to obtain the IPv6 address:**
	• **Auto configuration**
	• **DHCP**
	• **Static**
	  • **Address**
	  • **Prefix**
	  • **eui-64**

IPv6 Neighbor Discovery	**Router Preference** • **High** • **Medium** • **Low**
Manage config flags	**Enable or disable config flags.** **Default is disabled**
Manage other config flags	**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	Value of the reachable time field of the IPv6 router advertisement messages. Range 1 – 3600000 Default is 0
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 is 1 – 3600000 Default is 0
IPv6 Routing Prefix Advertisement	
Add Prefix	
Address	Specify an IPv6 address.
Prefix Length	Specify the prefix length. Range is 0 – 128
Valid Lifetime (secs)	Range is 1 – 4294967294 or infinite Default is 2591800
Preferred Lifetime (secs)	Range is 1 – 4294967294 or infinite Default is 604800
Do not use prefix for online determination	Enable or disable prefix for online determination. Default is off
Do not use prefix for autoconfiguration	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 off
Hop Limit	Range is 1-255 Default is off
RA Interval (secs)	Range is 1 – 1800 Defaults is 600
Minimum Interval (secs)	Range is 1 – 1350 Default is 132

RA Lifetime (secs)	Range is 1 – 9000 Default is 1800
Add DNS	
	Add address of DNS server.
Role	Used for controlling admin access. Default is LAN Options: • LAN • WAN • TRUSTED
MTU Size	Optional: provide an MTU size. Default is 1500 Range is 64 – 9000

Bridge Interface	
Enable/Disable Interface	The interface will be enabled or disabled. Default – 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 that you want to associate with this bridge.
Enable IPv4 address	
Enable DHCP	Your IP address will be assigned from a DHCP server.
Enable Static	Provide a IP address and network mask for this interface.
Enable DHCP Server	*Using DHCP Server*

Enable IPv6	**Select how to obtain the IPv6 address:**
	• **Auto configuration**
	• **DHCP**
	• **Static**
	  • **Address**
	  • **Prefix**
	  • **eui-64**

IPv6 Neighbor Discovery	**Router Preference** • **High** • **Medium** • **Low**
Manage config flags	**Enable or disable config flags.** **Default is disabled**
Manage other config flags	**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	**Value of the reachable time field of the IPv6 router advertisement messages.** **Range 1 – 3600000** **Default is 0**
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** **Default is 0**
IPv6 Routing Prefix Advertisement	
Add Prefix	
Address	**Specify an IPv6 address.**

Prefix Length	Specify the prefix length. Range is 0 – 128
Valid Lifetime (secs)	Range is 1 – 4294967294 or infinite Default is 2591800
Preferred Lifetime (secs)	Range is 1 – 4294967294 or infinite Default is 604800
Do not use prefix for online determination	Enable or disable prefix for online determination. Default is off
Do not use prefix for autoconfiguration	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 off
Hop Limit	Range is 1-255 Default is off
RA Interval (secs)	Range is 1 – 1800 Defaults is 600
Minimum Interval (secs)	Range is 1 – 1350 Default is 132
RA Lifetime (secs)	Range is 1 – 9000 Default is 1800
Role	Used for controlling admin access. Default is LAN Options: • LAN • WAN • TRUSTED
MTU Size	Optional: provide an MTU size. Default is 1500 Range is 64 – 9000

PPPoE Interface	
Enable/Disable Interface	Enabled or disabled interface. Default is enabled
PPPoE ID	The ID for this PPPoE connection
Interface	Select an available Ethernet interface.
Description	Provide a description for this interface.
Encapsulation	Set to PPP.
User Name	Enter a username for this connection.
Password	Enter a password for this connection.
Idle Timeout	Drop the connection after set idle time.
Access Concentrator	Specify the name for the access concentrator.
Enable IPv4 address	
Enable DHCP	Your IP address will be assigned from a DHCP server.
Enable Static	Provide a IP address and network mask for this interface.
Enable DHCP Server	*Using DHCP Server*

Tunnels (Interface)	
Tunnel Type	• GRE • OpenVPN • 6in4 Default is GRE
Enable/Disable Interface	Enabled or disabled 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.**
Destination IP Address	**Provide the destination IP address**
Enable IPv4 address	
Enable DHCP	**Your IP address will be assigned from a DHCP server.**
Enable Static	**Provide a IP address and network mask for this interface.**

Enable IPv6	**Select how to obtain the IPv6 address:**
	• **Auto configuration**
	• **DHCP**
	• **Static**
	  • **Address**
	  • **Prefix**
	  • **eui-64**

IPv6 Neighbor Discovery	**Router Preference** • **High** • **Medium** • **Low**
Manage config flags	**Enable or disable config flags.** **Default is disabled**
Manage other config flags	**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	**Value of the reachable time field of the IPv6 router advertisement messages.** **Range 1 – 3600000** **Default is 0**

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 Default is 0
IPv6 Routing Prefix Advertisement	
Add Prefix	
Address	Specify an IPv6 address.
Prefix Length	Specify the prefix length. Range is 0 – 128
Valid Lifetime (secs)	Range is 1 – 4294967294 or infinite Default is 2591800
Preferred Lifetime (secs)	Range is 1 – 4294967294 or infinite Default is 604800
Do not use prefix for online determination	Enable or disable prefix for online determination. Default is off
Do not use prefix for autoconfiguration	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 off
Hop Limit	Range is 1-255 Default is off
RA Interval (secs)	Range is 1 – 1800 Defaults is 600
Minimum Interval (secs)	Range is 1 – 1350 Default is 132
RA Lifetime (secs)	Range is 1 – 9000 Default is 1800

Role	**Used for controlling admin access.** **Default is TRUSTED** **Options:** • **LAN** • **WAN** • **TRUSTED**
MTU Size	**Optional: provide an MTU size.** **Default is 1500** **Range is 64-9000**

Profiles (Cellular and Wireless)

Wireless Profiles	
Network name (SSID)	Provide a description for this interface. Name can be up to 32 characters long. Maximum profiles is 16.
Security Type	• opened • WEP • WPA-Personal • WPA-Enterprise • WPA2-Personal • WPA2-Enterprise • WPA1/2 Personal • WPA1/2 Enterprise • 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	8-62 characters in length
Hidden SSID	Select hidden SSID if you do not want to broadcast your network name. Default is not hidden
Max Number of Clients	1-2007 Default is 2007

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	1 or 2 Default is 1

Radio Technology	• **Auto** • **LTE (4G)** • **UMTS (3G)**
Roaming Allowed	**Allow roaming on the wireless network.** **Once registered to the network, if roaming is disabled, the router will either stay disconnected until such time as we are no longer roaming or will do failover if that is enabled.** **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**
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	
Attach APN Settings	**Specific the APN to use for this connection.**
APN	
PDP type	• **IPv4** • **IPv6** • **IPv4/IPv6** **Default is IPv4**
Modem Slot number	**Range 1-16** **Default is 1** **Note: This is an internal slot number not the SIM slot.**
Data APN Settings	

Same as Attach APN	**Use the same settings as set for APN.**
APN	**Specify the APN to use for this connection.**
PDP Type	• **IPv4** • **IPv6** • **IPv4/IPv6** **Default is IPv4**
Modem Slot number	**Range 1-16** **Default is 1** **Note: This is an internal slot number not the SIM slot.**
Roaming Allowed	**Allow roaming to other networks** **Default is On**
Use DNS offering from Carrier	**Use the DNS offered by the carrier** **Default is On**
Use Default Gateway offering from Carrier	**Use the default gateway offered by the carrier** **Default is On**
Maximum MTU	**Values are 64-9000** **Default is 1500**
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**
Action when Maximum MB reached	• **Turn off (that SIM) when limit reached and send a trap message** • **None** **Default is None**

Serial Interface (tty)	
TTY Usage mode	**Select how this interface will be used.** • **Serial-Line – configure parameters for the serial line (see below). Select tty mode here -> *Console Port* if you want to use this port as a console port.** • **Serial-Console – set this mode when using the serial port as a console port. See *Console Port*** • **Serial-GNSS – see *Serial-GNSS* to set line parameters** • **Disabled – the interface is disabled**
Serial Line	
Speed	**Configure speed:** • **300** • **600** • **1200** • **1800** • **2400** • **4800** • **9600** • **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 for CTS 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 will occur 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	**Determines if input flow control is to be used.** **Default: Enabled**
Enable Outbound Flow Control	**Determines if output flow control is to be used.** **Default: Enabled**
Enable DTR-DSR monitor	**The serial will not go active until DTR-DSR are both active.**
Discard Characters Received with errors	**When enabled, the IOLAN will discard characters received with a parity of framing error.** **Default is disabled**

Enable Echo Suppression	**This parameter applies only to EIA-485 Half Duplex mode. All characters will be 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**
Serial Console	
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	**Select the 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
USB Console	
USB usage mode	**Select how the USB interface will be used.** • **USB-Console – set this mode when using the serial port as a console port. See *Select Console Port*** • **USB Ethernet – select this mode to use the USB port as an Ethernet port. See *USB Ethernet*** • **USB-GNSS – select this mode to send GNSS output to the USB port. See *Serial-GNSS*** • **Disabled**
USB Ethernet	
Description	**Add a description for the USB port.**
Enable IPv4 address	
Enable DHCP	**Your IPv4 address will be assigned from a DHCP server.**
Enable Static	**Provide a IPv4 address and network mask for this interface.**
Enable DHCP Server	***Using DHCP Server***

Enable IPv6	**Select how to obtain the IPv6 address:**
	• **Auto configuration**
	• **DHCP**
	• **Static**
	  • **Address**
	  • **Prefix**
	  • **eui-64**

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 Settings

DNS	
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 (Add, Delete)	**Enter an IPv6 address for your DNS server. Select the + symbol to add more.**
DNS Forwarding	
Cache Size	**By setting the cache size, this will allow the router to store frequently used resolved DNS queries, thereby allowing 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 meet this criteria.
DNS Listeners	
IPv4 address	Enter an IPv4 address to listen for DNS requests.
DNS Domain Forwarding	
Domain	This server will receive domain requests.
IPv4 Address	Forward domain request to this server.
Dynamic DNS	
Host Groups (Add, Edit or Delete)	Specify a Group name.
Add Hostname entries	Add hosts that will be added to this group.
Add DDNS to interface	
Interface	Select from the drop-down list, the interface to add DDNS functionality.
Web Check to obtain external IP	Enter the URL that you want to obtain an IP address from. This will allow the router to be seen on the internet as a public address.
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 will be 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 that will be accessed by an IP address or Fully Qualified Domain Name (FQDN) from the router. This table will contain a symbolic name for the host as well as its IP address or FQDN. When a host entry is required elsewhere in the configuration, the symbolic name will be used. The local Host Table in the 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 the router.

Overview

- Add host to IP address relationships.

Restrictions / Limitations

- Only IPv4 addresses are supported

Feature details / Application notes

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

IP Host Tables	
Host (Add)	**Enter a hostname to IPv4/IPv6 address association you want to add to the host table.**

WAN

Overview

Your router has the ability to determine the health status of any interface. By configuring ping and traceroute tests you can determine whether an interface is still able to send and receive data. Every interface can be configured to run these tests and if the interface fails, then a backup action can be taken.

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 will apply 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**

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.
NextHop	• IP • DHCP
IP Address	The IP address of the next hop.

High Availability	
Mode	• Disable • Failover • Load Sharing
Failover	Specify the source interface to fall over to.
WAN Interface	
Interface	Specify WAN interface.
Priority	Specify the priority for load-sharing. Values are 1-255
Load Sharing	Note: Load sharing requires at least one valid rule to enable it.
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.
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	Load-sharing based at packet level.
WAN	
Interface	Specify a WAN interface.
Weight	Specify a weight.
Enable Matching Protocol	Select protocol to match.
Limit	
Burst	Number of packets that match the criteria allowed out the WAN interface based on the rate calculation window.
Rate calculation window	• hour • minute • second
Rate	Number of packets that match the criteria allowed out the WAN interface based on number of packets.
Threshold behavior for limit	• above • below

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.

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 will be 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 will 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 will prevent 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 will be 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 will 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 will prevent the software from "arping" 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 you added.**
Interface	**Select the interface that this ARP entry will 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 router will respond to same ARP requests coming from multiple interfaces**
Enable ARP Accept	**Define 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**

Routing

Default Gateway	
	Enter the default gateway for your router.

Static Routing

Static routing is a form of routing that occurs when you manually configure a routing entry in the routing table, rather than information collected from dynamic routing traffic.

Overview

Use Static routing to:

- define an exit point from a 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 that when there is a change in the network or a failure occurs between two statically defined devices, traffic will not be 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 that 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 two networking routing techniques.
RIP – See ***RIP*** for more information
BGP – See ***BGP*** 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	**(AD) is a value that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative Distance counts the reliability of a routing protocol. A static route is normally set to 1** **Default is 1** **Range is 1-255 (with 1 being the most reliable)** **255 is route not used or unknown**
IPv6	
Enable IPv6 Unicast Routing	**Enable unicast routing if your router needs to be able to route IPV6 traffic AND to participate in IPv6 IGPs (Interior Gateway Protocols)**

Port Forwarding

Port forwarding or port mapping is an application of network address translation (NAT) that 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.

Overview

Port forwarding is an excellent way to preserve public IP addresses. It can protect servers and clients from unwanted access, "hide" the services and servers available on a network, and limit access to and from a network. Port forwarding is transparent to the end user and adds an extra layer of security to networks.Your router supports 99 port forwarding rules.

Port Forwarding

Protocol	**Set the protocol to be used for this rule.** • **TCP** • **UDP**
Inbound Interface	**Select the inbound interface.** • **Br (bridge)** • **Eth1 - Eth4 (Ethernet)** • **wlm0 - cellular** • **wlan0 - wireless 1** • **wlan1 - wireless 2** • **tunnel** • **openvpn-tunnel**
Inbound port	**Specify the port number for the incoming data.** **Range is 1-65535**
Destination address	**Specify the IPv4 address of the end device receiving the data.**
Destination port	**Specify the port number for the end device receiving the data.** **Range is 1-65535**

NAT/ALG

NAT is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

Overview

Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. In order to configure NAT, you need to make at least one interface on a router (NAT outside) and another interface on the router (NAT inside).

NAT	
NAT Rules (Add, Edit, Delete)	
ACL List	**Set the ACL from the drop-down list to be used with the specified interface.**

Global Address	
Interface or Pool	• Select the pool from the drop-down list • Select the interface from the drop-down list
ALG	
Enable certain protocols to transverse Nat and Firewalls	
Select the protocols to enable	• ftp • gre • h323 • nfs • pptp • sip • sqlnet • tftp

Access Control Lists

An ACL or Access control list is a common means by which access to and denial of services is controlled. Access control lists (ACLs) control the traffic entering a network. On network devices such as Rruters and firewalls, they act as filters for network traffic, packet storms, services and host access. The most important reason to configure ACLs is to provide security for your network. ACLs can also be configured to control network traffic based on the TCP port being used.

Overview

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.dadsaadada

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.

ACL	
ACL Type	**Specify the type of ACL.** • **Standard** • **Extended**
ACL number	**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**
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 tries 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	**Specify the hostname or IPv4 address. e.g. 192.168.1.0**
Source wildcard	**Specify the source wildcard to match. e.g. 0.0.0.255**

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.

Overview

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	
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 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**

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. attributes.

Overview

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** • **Interface** • **IP Address Route** • **Next-hop Address of route** • **match-iproutesource** • **match-ipv6address** • **match-ipv6nexthop** • **Metric of Route** • **BGP Origin Code** • **Peer Address** • **Tag of Route**
Set Values in Destination Routing Protocol **Set Attribute**	

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 • 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 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	Specify 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	**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 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	**Specify 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	**What action will be taken 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.**

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.

Overview

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 a router sees its own AS number in the AS path, it will not accept the prefix.

AS-Paths	
Name	**Specify a 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 sequence numbers.** **Range is 65535**
Action	**What action to take when rule matches.** • **Permit** • **Deny**

Regular Expression	**Enter a text string**

Policy Routing

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

Overview

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.

Policy Routing	
Enable	**Enabled or disabled Policy routing.** **Default is disabled**
Rule Number	**Specify a rule number.** **Range is 1-9999**
Description	**Enter a description for this rule.**
Log packeting matching this rule	**Log the packets that match this rule.**
Traffic Match	
Select Matching Criteria	• **Source IPv4-address** • **Source MAC address** • **Destination IPv4-address** • **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**

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.

Overview

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.

Route Tables	
Route Tables (Add, Edit, Delete)	
Destination Prefix	**Specify a destination prefix.**
Destination Network Mask	**Specify a destination prefix mask.**
Route	
Route via:	• **Forwarding Address** • **Interface** • **Null**
Router Address	**Specify the address of the forwarding router.**
Default Gateway for Interface obtained by DHCP	**Select this option if you want to use the default gateway obtained by DHCP.** **Default is off**

Administrative Distance	**Enter an Administrative Distance.** **(AD) is a value that routers use in order to select the best path when there are two or more different routers 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 anywhere.** **Values are 1-255**

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.

Overview

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 the router. 16 hops denote a network that is unreachable, according to the RIP hop limit.

RIP	
Enable RIP	**Enable or disabled RIP.** **Default is disabled**
Distance	**Enter an administrative distance.** **(AD) is a value that routers use in order to select the best path when there are two or more different routers 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 anywhere.** **Values are 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. Default is 30 seconds Range is 1 to 2147483**
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. Default is 180 seconds Range is 1 to 2147483**
Flush	**Amount of time (in seconds) that must pass before the route is removed from the routing table. Default is 120 seconds Range is 1 to 2147483**
Passive Interfaces, Networks and Neighbors	
Passive Interface (Add, Delete)	**Select an interface from the drop-down list**
Network	**Specify the Network's IPv4 address and netmask. • IPv4 Address • IPv4 Mask**
Neighbors	**Specify the Neighbor address • IPv4 Address**
Distributed and Redistributed Lists	

Filter	• ACL • Prefix Default is ACL
ACL List **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	Select an interface to apply the ACL list to. Only defined interfaces will be shown.
Add Redistributed List	
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 • md5

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 the router to actively advertise routes as unreachable over the interface over which they were learned by setting the router 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 (Add, 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	**Specify the Key ID and Password.** • **ID for this key.** **Range is 1-2147483647** • **Password** **password will be encrypted**

OSPF

Overview

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. If the router has limited memory or CPU capabilities this would impact performance. 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	**Router-id for this OSPF process.**
Enable Auto cost	**Enable Auto-cost and specify a reference bandwidth that will be used to dynamically calculate OSPF interface cost.** **Default is no**
Reference Bandwidth	**Default reference bandwidth is 100 Mbps.**
Enable RFC 1583 compatibility	**Enable for RFC 1583 compatibility.**
Enable Opaque Capability	**Enable for Opaque capability**
Distance	

Administrative	**Enter an administrative distance. (AD) is a value that routers use in order to select the best path when there are two or more different routers 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 anywhere. Values are 1-255 Default is 110**
OSPF External	**Routes injected by redistribution. Range is 1 – 255 Default is 110**
OSFP inter-area routes	**Routes from another area are inter-area. Range is 1 – 255 Default is 110**
OSFP intra-area routes	**Routes within an area are intra-area. Range is 1-255 Default is 110**
Specify Metric	**Metric is the best route. Metric is dependent on the other routers (neighbors) along the path, and it is advertised between neighbors. Range is 0 – 16777214**
Original Default-Information	**Default is off**
Max-Metric	
Administrative	**Advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations.**
On Shutdown	**Advertise stub-router prior to full shutdown of OSPF. Range is 5 – 86400 Default is 600**
On Startup	**Configures the router to advertise a maximum metric at startup. Range is 5 – 86400 Default is 600**

Refresh Timer	**The router automatically updates link-state information with its neighbors. Only an obsolete information is updated which age has exceeded a specific threshold. Range is 10 -1800 seconds**
Throttle Timers	• **Delay between receiving a change to SPF calculation in milliseconds.** **Range is 1-600000** • **Delay between first and second SPF calculation.** **Range is 1-600000** • **Maximum wait time in milliseconds for SFP calculations.** **Range is 1-600000** **Default is off**
OSPF Areas (Add, Edit, Delete)	
Select Area Id format	**Specify 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)**
Area Type	• **normal areas – can contain LSAs of type 1, 2, 3, 4, and 5, and may contain an ASBR. The backbone is considered a standard area** • **stub – can contain type 1, 2, and 3 LSAs. A default route is substituted for external routes** • **nssa – Not-so-stubby areas implement stub or totally stubby functionality yet contain an ASBR. Type 7 LSAs generated by the ASBR are converted to type 5 by ABRs to be flooded to the rest of the OSPF domain**
Default Authentication	**Select the method for authentication.** • **None** • **Text** • **Message Digest** **Default is no authentication**

Default cost	Cost for the default summary route used for a stub or NSSA. Range is from 0 to 16777215
Shortcut	This parameter allows to "shortcut" routes (non-backbone) for inter-area routes. • enable – the area will be used for shortcutting every time the route that goes through it is cheaper • disable – this area is never used by ABR for routes shortcutting. • default – this area will be used for shortcutting only if 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	(Optional) Specifies the time (in seconds) between the hello packets that your router sends on an interface. The value must be the same for all routers and access servers attached to a common network. The default is 10 seconds.
Dead Router Detection Time	Specifies the time (in seconds) that must pass without hello packets being seen before a neighboring router declares the router down. Default is 4 times the hello interval Default is 40
LSA retransmit Interval	Specify 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 must increase 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	Specifies the password used by neighboring routers for simple password authentication. It is any continuous string of up to eight characters. There is no default value. • None – no password • Text – text • Message-digest –(Optional) Identifies the key ID and key (password) used between this router and neighboring routers for MD5 authentication. The Default is none.
Area Range (Add, Edit, Delete)	
Prefix	Specify a prefix specified as IP address.
Mask	Specify a subnet mask
Mode	• sets the address range status to advertise and generates a Type 3 summary LSA • 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) Default is advertise
User Specified Cost	Specify the metric for this area range. Range is 0-16777215
Substitute Prefix	Specify the substitute prefix when mode set to substitute.
Substitute Mask	Specify the substitute mask when mode set to substitute.
Distributed and Redistributed Lists	
Distributed List (Add, Edit, Delete)	
ACL List	Select ACL (Access Control List) from drop-down list.

Direction	**Out – the distributed list out option works only on the routes being redistributed by the ASBR into the OSFP. It can only be applied to external type 2 and external type 1 routes but not to intra-area and inter area routes.** **In – The distribute-list in command filters routes only from entering the routing table, but it doesn't prevent link-state packets (LSP) from being propagated.**
Type	**Select the type of route** • **BGP** • **Connected (directly attached subnet or host)** • **Kernel** • **OSPF** • **Static**
Redistributed List (Add, Edit, Delete)	
Type	**Select the type of route** • **BGP** • **Connected (directly attached subnet or host)** • **Kernel** • **OSPF** • **Static**
Metric	**Specify the metric for this redistribution list**
Metric Type	**Set metric type to;** **1 – OSPF External Type 1** **2 – OSPF External Type 2**
Interface – OSPF	

Network Type	• **broadcast – a designated router and backup designated router are elected which uses OSPF multicasting capabilities. (most common type)** • **non-broadcast – use this type of network on networks that have 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 – allows you to configure selected routers with neighbor / cost commands, identifying a specific cost for the connection to the specified peer** • **point-to-point – there are only two neighbors and multicast is not required. For routers on an interface to become neighbors, the network type for all should match.**
Disable MTU mismatch detection	**Use the disable MTU mismatch detection on an interface if the receiving MTU is higher than the IP MTU configured on the incoming interface, OSPF will not establish adjacencies. 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.** **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	**Sets the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down (dead).** **Range is 1 – 65535 seconds** **Default is 40 seconds**

Hello interval	**Specify the time between HELLO packets.** **Range is 1 – 65535** **Default is 10 seconds**
Retransmit interval	**Set the time between retransmitting lost link state advertisements.** **Range is 1 – 65535** **Default is 5 seconds**
Transmit delay	**Transmit-delay is 1 – 65535** **Range is 1 – 65535** **Default is 5 seconds**
Authentication	
Mode	**Enable authentication in OSPF in order to exchange routing update information in a secure manner.** • **md5 – the most secure OSPF authentication mode. You must configure an entire area with the same type of authentication** • **text – plain text (a password) will be used for authentication** • **null – no authentication will be used**

BGP

Overview

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.

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 peering and carrier networks to connect.

BGP	
BGP (Add, Edit, Delete)	

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. 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. Values are 1-4294967295
Administrative Distance	
Remote Addresses (Add)	
Distance (Administrative)	Enter an administrative distance. (AD) is a value that routers use in order to select the best path when there are two or more different routers 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 anywhere. Values are 1-255
IP Source	You must specify the IP addresses of the peers in order to establish a BGP session. Specify the network.
IP Mask	Specify a network mask for this network.
BGP Distance	
Distance for external routes to AS	Specify the administrative distance for external routes. Values are 1-255 Default is 20
Distance for internal routes to AS	Specify the administrative distance for internal routes. Values are 1-255 Default is 200
Distance for local routes	Specify the administrative distance for local routes. Values are 1-255 Default is 200
Timers	

Keep Alive	Specify a keepalive time. Range is 0-65535 Default is 60 seconds
Hold Time	Specify a hold time. Default is 180 seconds
Redistribution List (Add)	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
IPv4 Family	Enter address family mode. Select IPv4 or IPv6.
Maximum Path	Specify the maximum paths to forward packets over. Default is 1
IBGP Maximum Path	Sets the number of equal-cost multipath iBGP routes or paths that are selected. Specify the maximum paths to forward IBGP packets over. Default is 1
BGP Settings	
BGP Router ID	BGP uses a router ID to identify 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.**
Treat missing MED as the least preferred one	**Treats a route without an MED as the worst possible available route due to expected unreliability.**
Compare router-id for identical EGBP paths/labels	**Check router-id for identical EGBP paths.**
Configure client to client route reflection	**Specifies whether this BGP entity reflects routes received from a client to another client. Default is enabled.**
Cluster-ID	**Configure Route-Reflector client cluster-id. Default is 0**
Confederation	**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. Specify a confederation identifier. Default is 0**
Peers	**Specify confederation peers.**

Dampening	Enable or disable (by default) route-flap dampening on all BGP routes. A flapping route is unstable and continually transitions down and up (see RFC 2439).When a prefix flaps it will be assigned a penalty of 1000 and moved into the dampening state “history”. 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 has been dampened, the penalty must be reduced to a value lower than the reuse limit in order to be advertised once again.
Half-life	The half-life timer is a calculation to determine when the route has become stable again and can be advertised. After a penalty has been assigned and the prefix has become 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 will begin to be advertised to neighbors when it recovers to this value. Values 1-20000 Default is 750
Value to start suppressing a route	Specify a value, when reached will 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 is used to ensure 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	Specify a local preference level. The higher 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 that the first (left-most) autonomous system number (ASN) in AS-path is 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 link used to reach them goes down. Default is on
Graceful Restart capability parameters	The GR feature provides a routing device with the capability to inform its neighbors when it is performing a restart. Default is off
Set the max time to hold onto restarting peer's stale paths	Set the time to hold stale paths of restarting neighbors Value is 1 to 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	Specify a time for BGP toll go through the routing table to make sure that the next-hop address of all the BGP prefixes are reachable through an IGP. 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	Specify a IPv4 aggregation address. This address can be used to summarize a set of networks into a single prefix
IPv4 Mask	Specify 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.

Neighbor (Add)	
IPv4 neighbor address	IPv4 address of a neighbor peer.
BGP neighbor	Configure a BGP neighbor also called peer.
Enable neighbor	Enable this BGP neighbor. Default is enabled
Description of the neighbor	Provide a description of this neighbor.
Advertisement interval	Specify a minimum time between sending BGP routing updates. Values are 0 – 600 seconds Default is 30 seconds
Accept as-path with my AS occurrence	Accept AS-path with my own AS present in it. Values are 1-10 Default is 3
Override match AS-number when sending updates	Override matching AS-numbers when sending updates.
All BGP attributes are propagated unchanged to this neighbor	Send BGP attributes unchanged. Default is enabled
Specify BGP attribute is propagated unchanged to this neighbor	• AS-path • MED • Next-hop
Advertise capability to the peer	• Dynamic • ORF receive • ORF transmit • ORF both Default is OFR Transmit
Originate default route to this neighbor	Send default route to this neighbor.
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.

Do not perform capability negotiation	Set this option on if you need to control advertisement of BGP capabilities to peers. Default is off
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 (IPv4). 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 (IPv4). 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.
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.
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.
Neighbor's BGP port (TCP)	Specify the TCP port that BGP peers will use to exchange BGP information. Default is 179
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 incoming 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 the router will wait for a keepalive message before declaring a router offline. 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 offline. 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
Network (Add)	
IPv4 Address	Specify a IPv4 address for this network.

Mask	Specific the network mask
Specify a BGP backdoor route	Specify a route map to be used in order for an interior gateway routing protocol (IGP) to take precedence over an eBGP route.
Route Map	Use this route map as a backdoor.
IPv6 Address Family	
Aggregate Address	
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)	
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 prefined.
Redistribute List (Add)	
Type	
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 prefined.
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.

Services

Serial Port Services

Overview

Each router serial port can be connected to a serial device. From the main Serial Ports screen you will see the tty serial interfaces that are installed. Select the tty interface, then select the Edit button to configure.

Select the service type from the drop down menu.

The following are the serial profiles:

- **Console Management** – The console Management profiles 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** – This 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, 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** – UDP Sockets profile configures a serial port to allow communication the network and serial devices connected 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 SLI P connection to the router's serial port. This is typically used with a modem for dial-in.

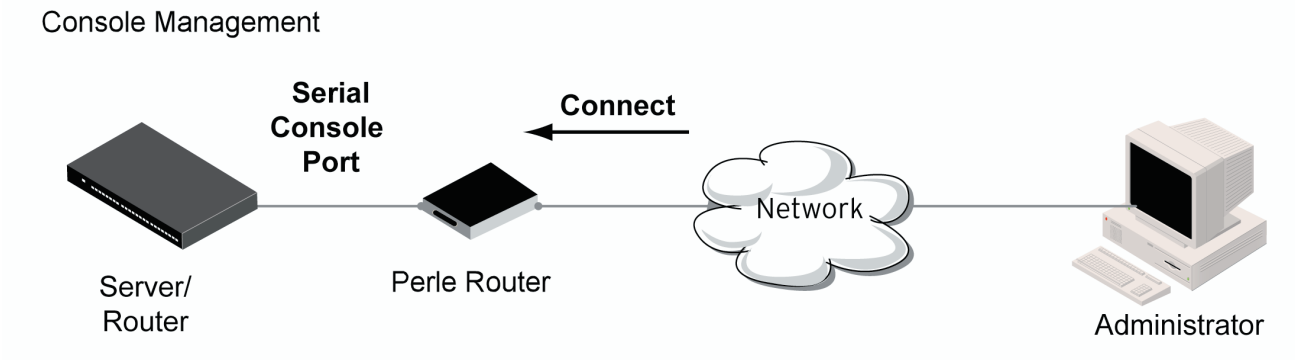
Common Serial Port Profiles Functions:

- Enable the serial port, enter description, then select service. See ***Serial Port***
- Hardware – Configure the physical serial line parameters.
- Packet Forwarding – Configure data packet parameters. ***Packet Forwarding***
- SSL/TLS – Configure SSL/TLS encryption options for the serial port. See ***SSL/TLS***
- Port Buffering – Configures serial port data buffering preferences. See ***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 Baud Rate***
- Advanced Serial Options. See ***Advanced Serial Options***

Serial Port	
Name	**Specify a name for this serial port.**
Enable	**Enable this serial port.**
Service	**Select a service type.**

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 router 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.



Console Management
Settings

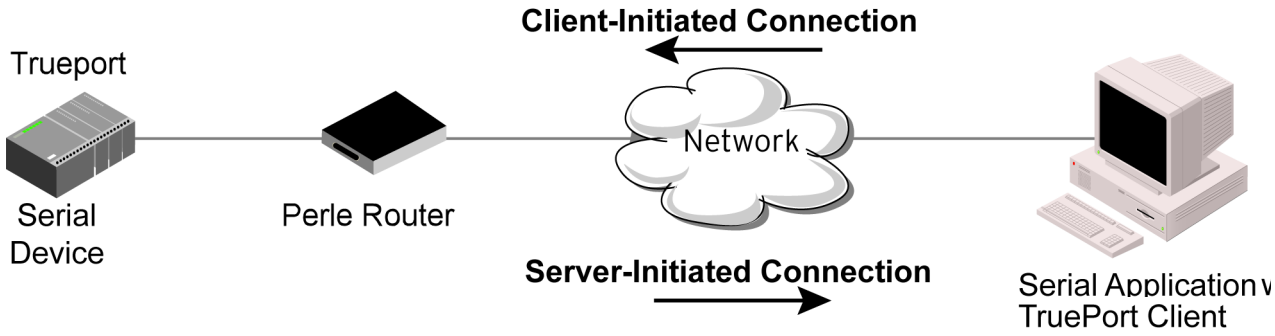
Protocol	Specify the connection method that users will use to communicate with a serial device connected to the router through the network. • SSH • Telnet Default is Telnet
Listen For Connections on TCP Port	The port number that the router will listen on for incoming TCP connections. Note: If more then one serial port has the same TCP port number assignment, this would create a hunt group scenario. However, all operating parameters for each serial port configuration need to be the same. Default: 10001, depending on the serial port number
Enable IP Aliasing IP Address	Enables/disables the ability to access a serial device connected to the serial port by an IP address (or host name that can be resolved to the Internet Address in a DNS network) instead of the router's IP address and port number. Default is Disabled
Advanced	
Authenticate User	Enables/disables login/password authentication for users connecting from the network. Default is Disabled
Enable 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.
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 , 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	**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***
Break Handing	**Specifies how a break is interpreted.** • **None –The router ignores the break key completely and it is not passed through to the host** • **Local – The router deals with 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 which it sends 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. If the client wishes 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 router to the network.** **See *Packet Forwarding***

Trueport

TruePort is a COM port redirector client utility that is 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.

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 as this 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 details about Trueport Client software.

Trueport	
Settings	
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 server.** **Default is Client initiated**
Server 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 a serial device that is 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 will be sent to the host upon session initiation. This will be 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 will use 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 Host for the client to connect to. Default is enabled Note: These multiple clients (Hosts) need to be running TruePort in Lite mode.
Advanced	Configures those parameters that are applicable to specific environments. See *Advanced Serial Options*

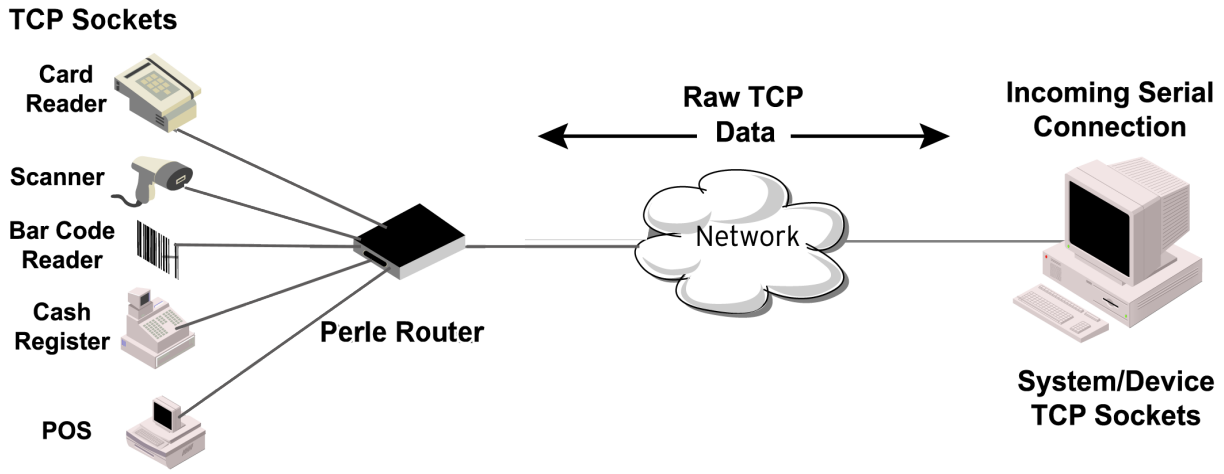
Raise Signals when not under Trueport control	**This option has the following impact based on the state of the TruePort connection:** • **TruePort Lite Mode –When enabled, the EIA-232 signals remain active before, duri ng, and after the TruePort connection is established. When disabled, the EIA-232 signals 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.** **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 needs to be 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 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** **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 , 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	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 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*

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 the connection can be initiated by either the Workstation/Server or the router.



TCP Sockets	
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**
Enable IP Aliasing	**Enables/disables the ability to access a serial device connected to a serial port by an IP address (or host name that can be resolved to the Internet Address in a DNS network) instead of the router's IP address and port number. 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. 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 needs to be 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 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 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 , 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	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 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*

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 you will use 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 IPaddress", 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.

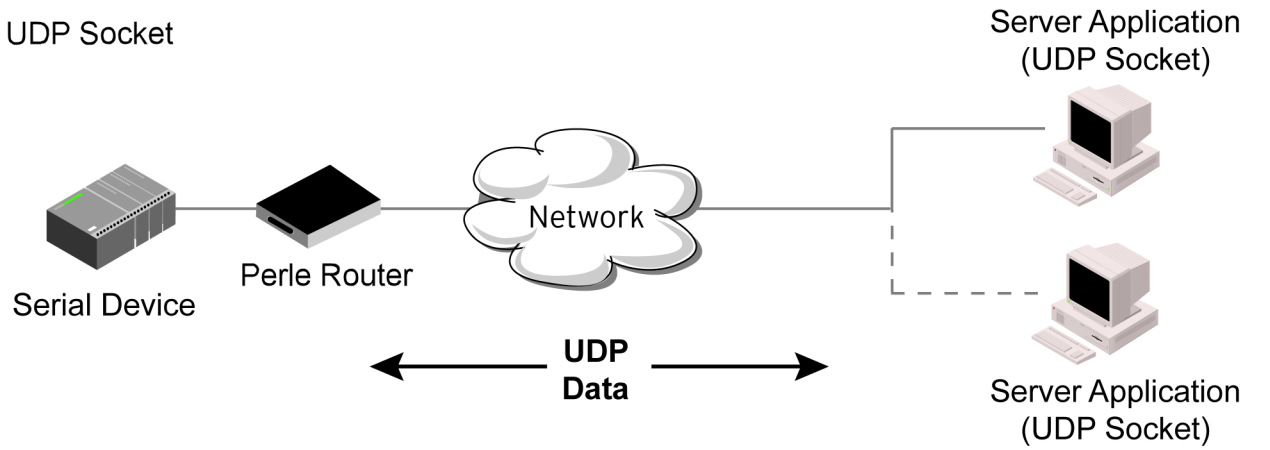
When the direction is "Both" the role of the additional parameters is as follow;

- **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	
Listen for Connections on UDP Port	**The router will listen 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 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.**
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**

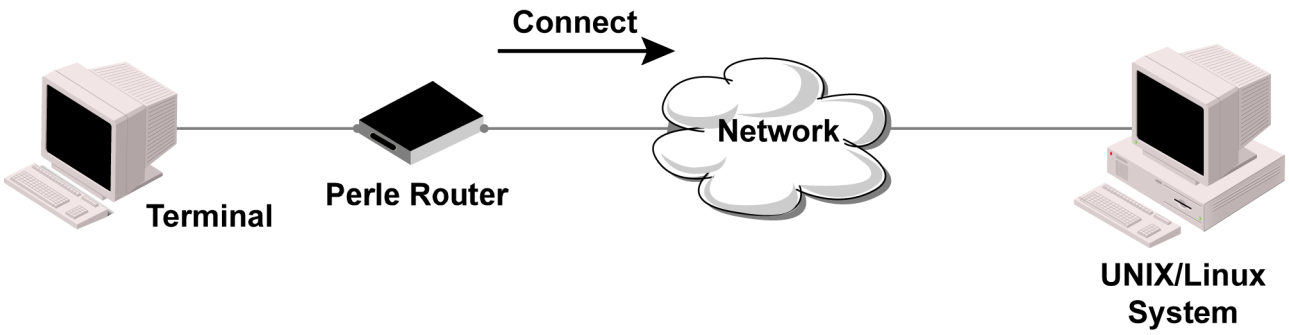
Port	**The UDP port to use.** **Default is 0 (zero)**
Session Strings	**Configures Send at Start, End and Delay after parameters for session control. See *Session Strings***
Packet Forwarding	**Packet forwarding can be used to control/define how and when serial port data packets are sent fro the router to the network.** **See *Packet Forwarding***

Terminal

The Terminal profile allows network access from a terminal connected to the router's serial port. This profile is used 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
Settings

Terminal Type	Type of terminal attached to this serial port. For user defined term types 1, 2, 3, you must copy the term type into the router's falsh. Dumb • WYSE60 • VT100 • ANSI • YVI925 • IBM3151TE • VT320 • HP700 • term 1 • term 2 • term 3 Default is Dumb
Mode	When users access the router the serial port, they must be authenticated, using either the local user database or an external authentication server. After a user has been successfully authenticated, the router will connect to the specified host using the specified protocol according to: • the User Service parameter for locally configured users • the Default User Service parameter for users who are externally authenticated • 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 *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 that will be used to connect to the specified host. Options – Telnet, SSH, Rlogin Default –Telnet See *Telnet* See *RLogin* See *SSH*
Terminal Type	Type of terminal attached to this serial port. For user defined term types 1, 2, 3, you must copy the term type definition into the router's flash. • Dumb • WYSE60 • VT100 • ANSI • TVI925 • IBM3151TE • VT320 (specifically supporting VT320-7) • (HP700 (specifically supporting HP700/44) • Term 1 • Term 2 • Term 3 Default is Dumb

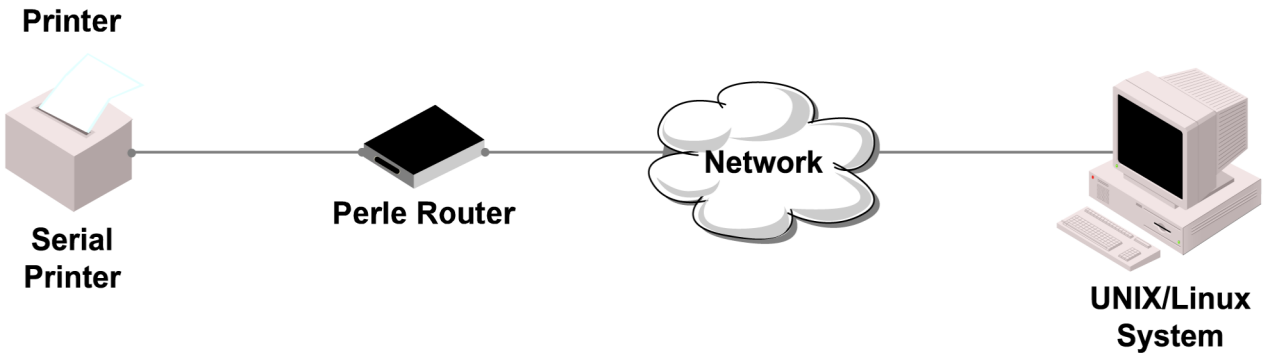
Enable Local Echo	Toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter can be used only when Enable 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). 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 remotehost. 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. 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 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 Timer times out, the router will end the connection. Range is 0-4294967 seconds (about 49 days) Default is 0 seconds so the port will never timeout

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*

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	
Map CR to CR/LF	The default end-of-line terminator as CR/LF (ASCII carriage-return line-feed) when enabled. Default: Disabled
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***

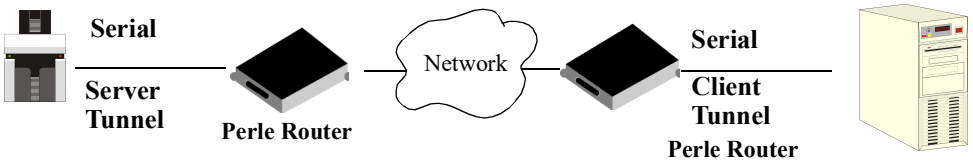
Serial Tunneling

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.

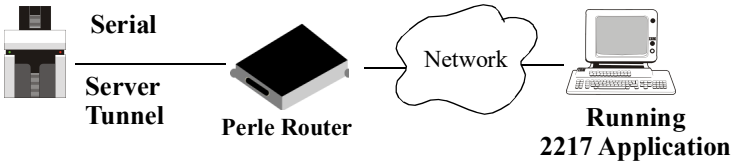
Serial Tunneling	
Settings	
Act as a	• **Tunnel Server – The router will listen for an incoming connection request on the specified Internet Address on the specified port.** **Default: Enabled** • **Tunnel Client – The router will initiate the connection the Tunnel Server.** **Default: Disabled**
Listen for connection on TCP Port	**The TCP port that the router will listen for incoming connection on.** **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 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 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 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***

A more detailed implementation of the Serial Tunneling profile is as follows:



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

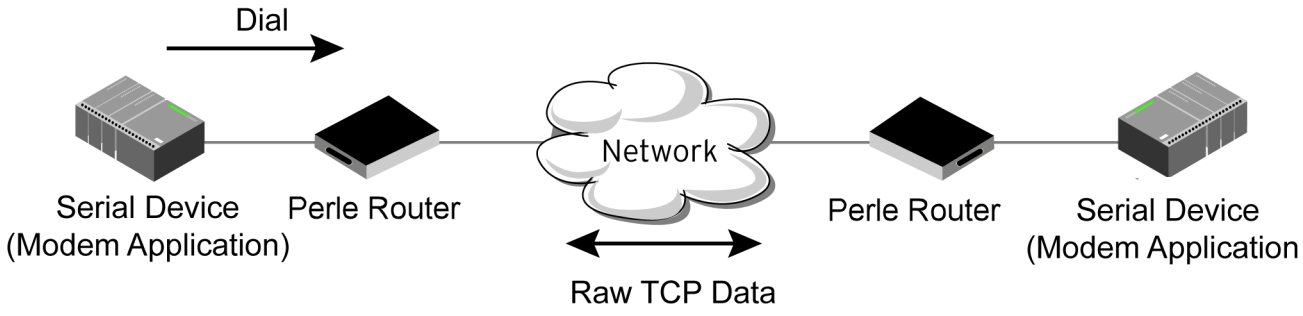


The routers serial port signals will also follow the signals on the other serial port. If one serial port receives DSR then it will raise DTR on the other serial port. If one serial port receives CTS then it will raise RTS on the other serial port. The CD signal is ignored.

Virtual Modem

Virtual Modem (Vmodem) is a feature of the router that provides a modem interface to a serial device. It will respond to AT commands and provide 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 will 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 formats and is the IP address of the receiver. For example, ATD123.34.23.43,10001 or you can use ATD12303402304310001, without any punctuation (although you do need to add zeros where there are not three digits presents, so that the IP address is 12 digits long).

Virtual Modem



Virtual Modem

Settings	
Listen on TCP Port	The router TCP port that the router will listen on. Default: 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: Enabled • 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: 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 preconfigured target host name.
TCP Port	The port number the target host is listening on for messages. Default: 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: 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
	Default: Enabled
	• 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 – CONNECT <*speed*>, for example, Connect 9600
	  • Failure – String that is sent to the serial device when a connection fails.
	Default – 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
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*

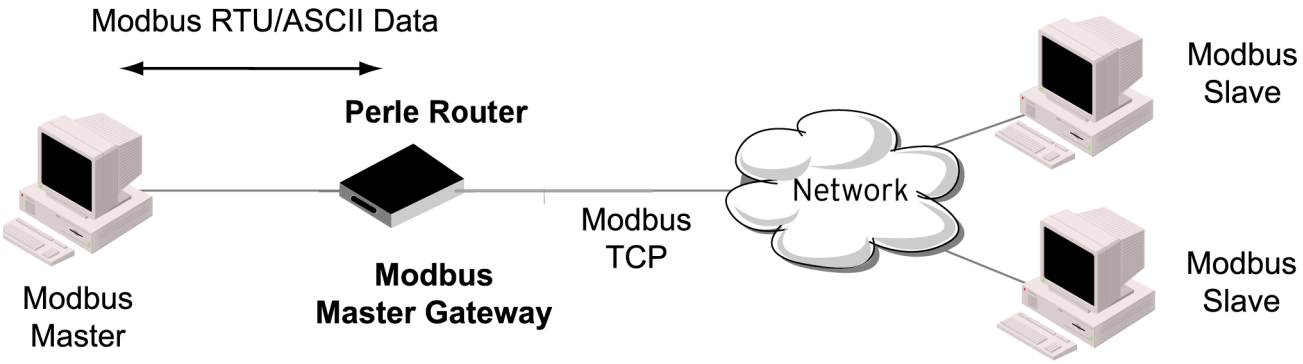
	You can create an encrypted connection using SSL/TLS for the following profiles: Trueport, TCP Sockets, Terminal (the user's service must be set to SSL_RAW), Serial Tunneling, Virtual Modem and Modbus. When configuring SSL/TLS, the following configuration options are available • **You can set up the 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***

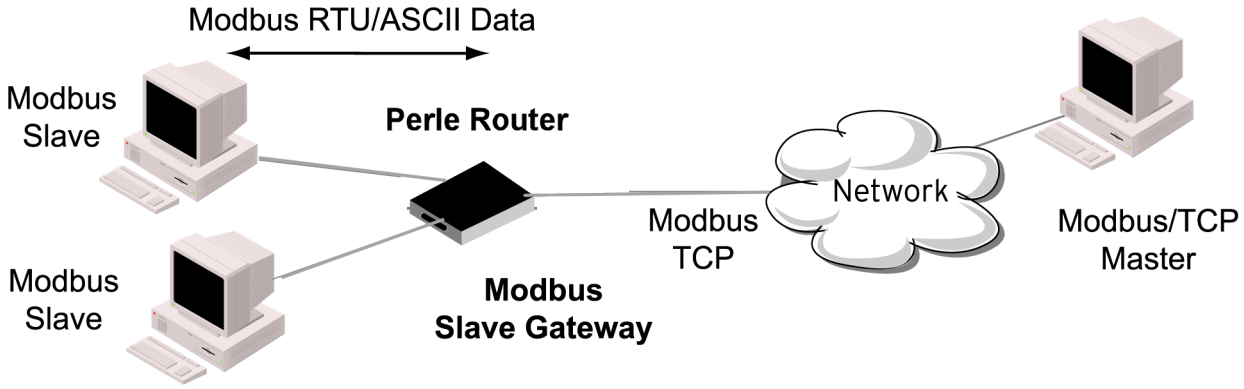
Modbus Gateway

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 gateway or a Modbus Slave gateway, depending on your configuration and requirements.

Modbus





Modbus Gateway	
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: 502**

Next Request Delay	**A delay, in milliseconds, to allow serial slave(s) to re-enable receivers before issuing 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 – 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 that will be inserted into the message header for the Slave Modbus serial device.** **Range is 1 – 247** **Default is 1**
Enable IP Aliasing	**When enabled, allows for multiple requests to serial slaves (from an Ethernet Master/s) to be processed simultaneously.** **Default is Off**
IP Address	**IP Address – Set the IP address to be used for this serial port when using the IP Aliasing feature.**
Enable SSL/TLS	**When enabled, Modbus Slave Gateway messages to remote TCP Modbus Masters are encrypted via SSL/TLS.** **Default: Disabled**

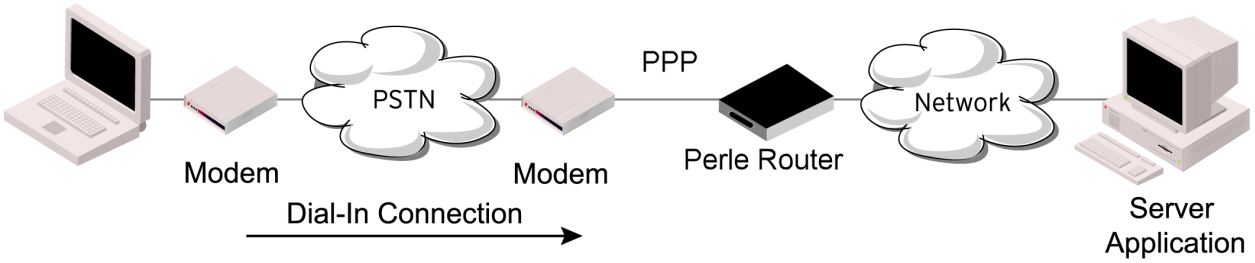
Protocol	• **Modbus/RTU – Select this option when the Modbus/RTU protocol is being used for communication between the Modbus Master and Slave.** **Default: Disabled** • **Modbus/ASCII – Select this option when Modbus/ASCII protocol is being used for communication between the Modbus Master and Slave.** **Default: 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: 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 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)**
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	**Use this timer to close a connection because of inactivity. When the idle Timeout expires, the router will end the connection.** **Range 0 – 4294967 seconds (about 49 days)** **Default is 0 (zero), which does not timeout, so 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** **Default 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, or 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 erial 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 leag 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
barneyfredwilma192.168.43.1
fredbarneyflintstone1234567890192.168.43.2

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

Remote Access (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**

Connection Method	**Connect – 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
	MS Direct – select whether the MS-Direct is by Host or Guest.
	• **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	
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. 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 – 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 – 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 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 as a 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, 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 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.** **Data Options:** • **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.** **Default is None**

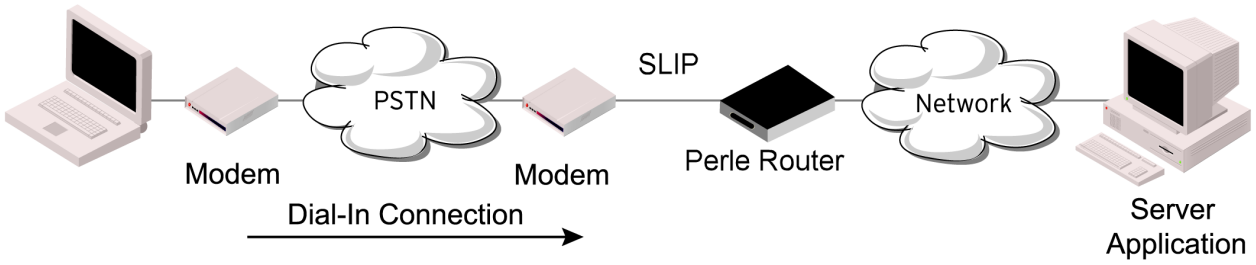
ACCM	**Specifies the ACCM (Asynchronous Control Character Map) characters that should be escaped from the data stream.** **The Field Formats is entered as a 32-bit hexadecimal number with each bit specifying whether or not the corresponding character should be escaped. The bits are specified as the most 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 Serila 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 to 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 can be used to control/define how and when serial port data packets are sent from the router to the network.** **See *Packet Forwarding***

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 or dial-out access to the network.



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 tfor 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 route 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.
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	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 will be 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 fro 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** **Custom Packet Forwarding** • **This option allows you to define forwarding rules based on the packet definition or the frame definition.** **Default is disabled**
Delay Between Messages	• **Minimize Latency** • **Optimize Network Throughput** • **Prevent Message Fragmentation** • **Custom Packet Forwarding**

Custom Packeting Forwarding	**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 etwork. 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: • 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. Default is Trigger
Use Global Settings	SSL/TL Version • Any • TLSv1 • TLSv1.1 • TLSv1.2
SSL/TLS	
Enable	Enable or disable SSL/TLS.
SSL/TLS Version	Select version of SSL/TLS. • Any • TLSv1 • TLSv1.1 • TLSv1.2
SSL/TLS Type	• Client • Server
Add Cipher	
Encryption	• Any • AES • 3DES • 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 • MF5 • 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	
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	
Terminal Type	**Type of terminal attached to this serial port. For user defined term types 1, 2, 3, you must copy the term type definition into the router's flash.** • **ansi** • **dumb** • **hp700** • **ibm3151te** • **tvi925** • **vt100** • **vt320** • **wyse60** • **term1** • **term2** • **term3**
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: 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.**
User	**This name is passed on to the specified host for the Rlogin session, so that the user is only prompted for a password.**

SSH	
Terminal Type	Type of terminal attached to this serial port. For user defined term types 1, 2, 3, you must copy the term type definition into the router's flash • ansi • hp700 • ibm3151te • tvi925 • vt100 • vt320 • wyse60 • term 1 • term 2 • term 3 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
Authentication	• 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 therouter, 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, the router 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. 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 – 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 – 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 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 as a 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, 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	**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.** **Data Options:** • **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.** **Default is None**

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 Serila Port, you must, you must enter a value of at least 000a0000 for the ACCM.** **Deafult 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 to 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**
Send at Start	**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**
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**
SSL/TLS	
Enable SSL/TLS	
SSL/TLScipher	• **Any** • **TLSv1** • **SSLv3** • **TLSv1.1** • **TLSv1.2**
Type	**Select whether the mode is client or server.** • **client** • **server**
Protocol	

SSH2 Cipher	• **3DES** • **Blowfish** • **AES-CBC** • **CAST** • **ARCFOUR** • **AES-CTR** • **AES-GCM** • **ChaCha20-Poly1305**
Authentication	• **RSA** • **DSA** • **Keyboard-interactive**
Advanced Options	**See *Advanced Serial Options***
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***

Port Buffering

The Remote Port Buffering feature allows data received from serial ports on the router to be sent to a remote server on the LAN. The remote server, supporting Network File System (NFS), allows administrators to capture and analyze data and messages from the serial device connected to the router 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 router will create unique files using the router's Ethernet MAC address and serial port number. It is recommended that a unique NFS directory and serial port name be configured if multiple routers 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 (even through router reboots), 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 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**

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 to 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.** **Default is 5** **Retries 1-32767**

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

Using 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 routers' 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 firmware 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
  - **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 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.

DHCP Server	
Enable DHCP Server	**Enable or disabled DHCP Server. Default is enabled.**
DHCP Pools (Add, Edit or Delete)	

Pool Name	**Enter a name for this DHCP pool.**
Description	**Enter a description for this DHCP pool.**
Network address	**Specify the DHCP network.**
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.**
Static Route	
Destination Address	**Specify a destination address for this static route.**
Destination Mask	**Specify a destination route 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 1-254** **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.
Bootp Server Name	Specify the name of the bootp server that contains the bootp file.
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.

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**
SIP Servers	**Specify the SIP domain and servers addresses to be used by clients.**

DHCP Relay

Overview

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 DHCP 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 Server	
Enable DHCP Relay Agent	**Enable or disabled DHCP Relay Agent.** **Default is enabled**
Relay information reforwarding 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.** • **Drop – The frame is discarded. (default action)** • **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. After setting a different port, requests are still accepted on port 67 but replies are forwarded to 255.255.255.255 port 0 instead of 68** **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/GPDS 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**

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**

SNMP

Overview

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.

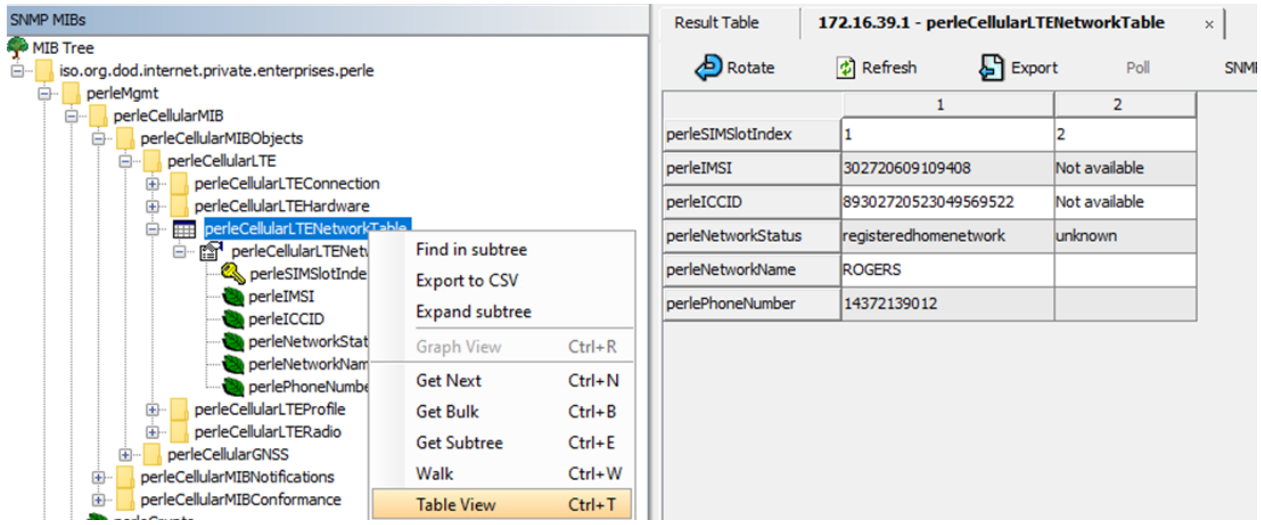
Connecting to the router Using SNMP

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 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. Below is an example of table view from perleCellularLTE MIB. In this example, you select perleCellularLTENetworkTable and click "Table View" using iReasoning MIB Browser.



Pre-requisites

- You must load the Perle supplied SNMP MIBs. The IRG5000 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.

Configuring SMNP parameters

SNMP	
Enable SNMP	**Enable or disable service.** **Default is disabled**
Location	**Define the SNMP location of your router.** **Max length is 32 characters**
Contact	**Defines the SNMP contact of your router.** **Max length is 14 characters**
SNMP Community (Add, Edit or Delete)	
Name	**Name of the community.** **Max length is 63 characters**
Permission	**Select the permission rights for this community.** • **ip-access – restrict access to IP address (host or network as defined)** • **ro – readonly access with this community string** • **rw – read-write 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** **Default is Any**
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	
Notifications	Individually enable/disable what conditions would generate a notification. • alarms • bgp • cellular-gnss • ipsec • openvpn • ospf • snmp • entity • authentication • envmon • cellular-lte • dot11
SNMP Notification	• coldstart • authentication • linkdown • linkup • warmstart
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 (v2 or v3c)
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/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.**
Authentication key	**Enter a authentication key.**
Privacy key	**Enter a privacy key.**
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.**

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 even if its stratum is lower. During this "settling" period, your router may not have the correct time. NTP can usually achieve time synchronization between two systems in the order of a few milliseconds. This can be achieved with a time transmission rate of as little as one packet per minute.

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.

Feature Details / Application Notes

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

than the other nodes, even if its stratum is lower. During this “settling” period, your router may not have the correct time.
NTP can usually achieve time synchronization between two systems in the order of a few milliseconds. This can be achieved with a time transmission rate of as little as one packet per minute.

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.

Feature Details / Application Notes

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 than the other nodes, even if its stratum is lower. During this “settling” period, your router may not have the correct time. NTP can usually achieve time synchronization between two systems in the order of a few milliseconds. This can be achieved with a time transmission rate of as little as one packet per minute.

NTP Settings	
Enable NTP (Network Time Protocol	**By default NTP is disabled globally. See reference for NTP per interface.**
Internal Time Sources	**Select the time sources.** • **Cellular System Time** • **GNSS (GPS)**

Advanced NTP Settings	
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/Peer	
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::5:6
Resolve hostnames to	• IPv4 or IPv6 • IPv4 • 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.**
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 (17,m, 4s), 11 (34,m,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 (17,m, 4s), 11 (34,m,8s)** **Default is 10**

Alarm Manager

Overview

The switch can monitor global switch 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 builtin 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

Feature details / Application notes

Alarm Relay

The alarm relay is an additional method for indicating that an alarm condition exists. Utilizing the switch's builtin 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 switch'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**
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 message** • **Send 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 message** • **Send a Relay message**

Facilities	
IGN (Contact 1)	
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
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	
Repeat Trigger	
Actions	Action for on Trigger condition • LTE Data Disconnect • Syslog • Trap Relay • none • major • minor
Contact B	
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	
Repeat Trigger	
Actions	**Action for on Trigger condition** • LTE Data Disconnect • Syslog • Trap **Relay** • none • major • minor
internal Temperature	
Primary	

High Threshold	**Specify a high threshold.** **Action on High Threshold condition** • **LTE Data Disconnect** • **Syslog** • **Trap** **Relay** • **none** • **major** • **minor**
Low Threshold	**Specify a low threshold.** **Action on low Threshold condition** • **LTE Data Disconnect** • **Syslog** • **Trap** **Relay** • **none** • **major** • **minor**
Secondary	
High Threshold	**Specify a high threshold.** **Action on High Threshold condition** • **LTE Data Disconnect** • **Syslog** • **Trap** **Relay** • **none** • **major** • **minor**

Low Threshold	**Specify a low threshold.** **Action on low Threshold 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**

Telnet/SSH

Terminal	
Enable terminal history size	Enter the size of the terminal history. Range is 1 – 256 Default is 20
Terminal width and length	Specify the width of the terminal 80 columns
Terminal width	Specify the terminal length in line. Range is 1 – 512 Default is 80
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	
Strict Host Key Checking	When enabled, a host public key (for each host you wish to ssh to) must be downloaded into the router. Default is Enabled
Configure ciphers in order of preference	Data Options: • ChaCha20-Poly1305 • AES128-CTR • AES192-CTR • AES256-CTR • AES128-GCM • AES192-GCM • AES128-CBC • AES-256-CBC • 3DES-CBC

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	After this many incorrect retires the user will be locked out. Range is 1 – 5 Defaults is 3
Configure allowed ciphers for incoming ssh2 users	• 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 • 3DES-CBC

Configure allowed MACs for incoming ssh2 users	• **UMAC-64-ETM** • **UMAC-128-ETM** • **HMAC-SHA2-256-ETM** • **HMAC-SHA2-512-ETM** • **HMAC-SHA1-ETM** • **HMAC-SHA1-96-ETM** • **HMAC-RIPEMD160-ETM** • **HMAC-MD5-ETM** • **HMAC-MD5-96-ETM** • **UMAC-64** • **UMAC-128** • **HMAC-SHA2-256** • **HMAC-SHA2-512** • **HMAC-SHA1** • **HMAC-SHA-96** • **HMAC-RIPEMD160** • **HMAC-MD5** • **HMAC-MD5-96**

Security

User Accounts

Overview

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.
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 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 that will be sent to you either as a SMS message or an email after you have logged in. When using email for two factor authentication, some email programs require that you set the parameter "allow less secure apps" in order to receive SMS email messages. When using SSH with two factor authentication, you must select Keyboard Interactive as the first method of Authentication. See ***SMS Settings***.

User Sessions

The Sessions tab is used to configure specific connections for users who are accessing the network through the router'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 (see ***Hot Key Prefix***) for more information. 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 to 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 MD5 encryption. This is a one way encryption scheme. There is no way to extract the clear password from the stored value. User password validation is performed by taking the password supplied by the user and encrypting it using the MD5 algorithm and comparing the result to the value stored in the database.
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 allow 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 • Admin/Web User
Password	Passwords can be up to 25 characters long. Blank passwords are also supported.
Two Factor Authentication	
Two Factor authentication	Enable Two Factor authentication. You must also enable and configure email settings under System/Email. See ***Email*** for these settings.
Format	• SMS • Email
Phone Number	Specify the phone to receive the verification code.
Email address	Specify the email address to send the verification code.
Serial Configuration	
Service	• Dslogin • Telnet • SSH • Rlogin • SLIP • PPP • TCP-Clear • SSL-Raw
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)	
Serial Port Access	

AAA (Authentication, Authorization and Accounting)

Overview

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

Configuring AAA Method

Login	
Authentication	
Add, Edit, Delete Group	**Specify a group name.**
Group	**Select the type of group; Local, Radius or TACACS+.**
Authorization	
Add, Edit, Delete Group	**Specify a group name.**
Group	**Select the type of group; Local, Radius or TACACS+**
Accounting	
Add, Edit, Delete Group	**Specify a group name.**
Accounting type	**Select the type of messages you want to log; None, Start-Stop (login and log out) or Stop (logout).**
Group	**Select the type of group; RADIUS or TACACS+.**
802.1X	
Accounting and Authentication	
Authentication	**Select a None or RADIUS.**
Accounting type	**Select the type of messages you want to log; None, Start-Stop (login and log out) or Stop (logout).**
System	
Accounting and Authentication	
Authentication	**Select a None or RADIUS.**
Accounting type	**Select the type of messages you want to log; None, Start-Stop (login and log out) or Stop (logout).**
Group	**Select the type of group; RADIUS or TACACS+.**

Radius

Overview
A RADIUS server can be used to provide authentication and accounting security for your router.

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	
Secret	**Encryption key shared with RADIUS hosts.**
Timeout (seconds)	**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**
Skip non -responsive servers	**How long to ignore non-responsive servers.**
IPv4 source interface	**Select the source interface from the drop-down list.**
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 with RADIUS hosts.**
Timeout (seconds)	**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+

Overview

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

your router supports User parameters that can be sent to the TACACS+ server; see ***Radius External Parameters*** for more information on the User parameters

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 with all TACACS+ configured servers.**
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.**
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
Secret	The encryption key for this TACACS+ server. This overrides the global secret.
Timeout in seconds	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.

802.1X	
Enable	Select to enable 802.1X on your router. Default: off
Timeout in seconds (Global)	Delay between unresponsive attempts. 1-1000 default 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.
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** **IPv4 - A.B.C.D** **IPv6 - X:X:X;X::X**
Secret	**The encryption key for this TACACS+ server. This overrides the global secret.**
Timeout in seconds	**Delay between unresponsive attempts.** **Range is 1-1000** **Default is 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.**

Firewall

Overview

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	• **IPV4 ping** • **Broadcast Ping** • **Handle IPv4 packet with source route option** • **Handle received ICMPv6 redirected messages** • **Handle IPv6 packet with routing ext-header** • **Log IPv4 packet with invalid address** • **Receive IPv4 redirect messages** • **Sen IPv4 redirected messages** • **SYN cookies** • **RFC1337 TCP time-wait hazard protection**
State Policy	**disable – no source validation** **loose – meaning any route (even default)** **strict – must match the inbound interface**
Firewall Rule (Add, Edit, Delete)	
Name	**Enter the name for this firewall rule.**

Description	Enter 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)	

Select Matching Criteria	Source IPv4-address
	• Accept addresses or exclude addresses
	• Use a range of addresses
	• address and wildcard
	Source MAC address
	Source Port (TCP/UDP)
	Destination IPv4-address
	Destination Port (TCP/UDP)
	Protocol
	• ah
	• dccp
	• egp
	• eigrip
	• ggp
	• gre
	• hmp
	• icmp
	  • Protocol
	  • Match by ICMP
	  • Type Value
	• TCMP Code
	• idpr
	• igmp
	• ipv6-frag
	• ipv6-icmp
	• ipv6nonxt

Select Matching Criteria	• ipv6-opts
	• ipv6-route
	• isis
	• i2tp
	• manet
	• mpls-in-ip
	• narp
	• ospf
	• pim
	• rdp
	• rohc
	• rsvpsctp
	• sdrp
	• shim6
	• skip
	• tcp
	  • ack
	  • fin
	  • psh
	  • rst
	  • syn
	  • urg
	• udp
	• udplite
	• vrrp
	• xns-idp
	• IP Protocol number
	  • IP Protocol Number

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 (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 pro actively sent from the router are regarded as from the local area.**
Default Action	• **Drop** • **Reject**
Zones Pairs (Add, Edit, Delete)	• **From** • **To** • **Firewall**
Firewall and Zone Interfaces	
Assign Firewall to Interface	• **Select interface** • **Inbound Firewall** • **Local Firewall** • **Outbound Firewall**
Assign Zones to Interfaces	• **Select interface** • **Zone**

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 to use 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 its 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/Netmask	The IP address and netmask of your router.
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. Field Format is IPv4 or IPv6 address
IKE Proposal	
Profile Name	Name of this 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 to use Network Address Translation Traversal (NAT-T)** **Default is off**
IKE Version	**Select 1 or 2.** **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** • **SHA1,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.**
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 Proposal	
Proposal ID	**ID of this proposal.**

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 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	• **tunnel** • **transport** **Default is tunnel**
ESP Proposal	
Proposal ID	**Add a name for this proposal ID.**
Encryption	• **3des** • **aes128** • **aes128gcm128** • **aes256gcm128** • **chacha20poly1305** **Default is aes256**
Hash	• **MD5** • **SHA1** • **SHA256** • **SHA384** • **SHA512** **Default is SHA1**

OpenVPN

Overview

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).

Note: to create a connection, a tunnel must exist.

OpenVPN	
Enable OpenVPN	**Enables OpenVPN**
Connections (Add, Edit, Delete)	
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.**
Port	**Port to use for both sides of the connection.** **Range is 1-65535** **Default is 1194**
Set Different Remote/Local ports	**Remote port to use.** **Range is 1 – 65535** **Local port to use.** **Range is 1 – 65535**
Remote Addresses	
Local Address	**Defines the remote tunnel local side and should be a private IPv4 or IPv6 address or hostname.** **IP Address (local)**
Remote Address	**Defines the remote tunnel local 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.**

Ciphers	• aes-128-cbc • aes-128-gcm • aes-192-cbc • aes-192-gcm • aes-256-cbc • aes-256-gcm • bf-cbc • camellia-128-cbc • camellia-192-cbc • camellia-256-gcm • cast-5-cbc • des-cbc • des-ede-cbc • des-ede3-cbc • desx-cbc • rc2-40-cbc • rc2-64-cbc • seed-cbc
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

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.
Keys and Certificates	
PSK	A pre-shared key (PSK) 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. See ***Manage Files*** files to import keys and certificates.
PKI CA TrustPoint	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.
PKI Certificate	The PKI certificate to use for this secure connection. See ***Manage Files*** files to import keys and certificates.
PKI Private Key	The PKI private key to use for this secure connection. See ***Manage Files*** files to import keys and certificates.
Advanced – Template	Use template.

Manage Files	
Import File	
Method	• **Browser** • **FTP** • **HTTP** • **HTTPS** • **SCP** • **SFTP** • **TFTP**
File Type	• **CA** • **CERT** • **Diffie-Hellman** • **PKI Key** • **Pre-Shared Secret Key** • **Template**
Name	**Name of certificate/key to download**
Import File	**Select the file to import to the router**
Installed Files	**The installed certificate and keys in the router.**

802.1X

Overview

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
This refers to your router which the supplicant is attempting to connect to. Your router will act 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 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 chip 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 authenticator.

802.1X	
Enable 802.1X authentication	**Select Enable to enable this feature.**

Selected Port/all	• **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. This test be done on a per port basis or across all ports. If the test is successful then a syslog message is sent to the syslog server. If not no message is sent.** • **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.**

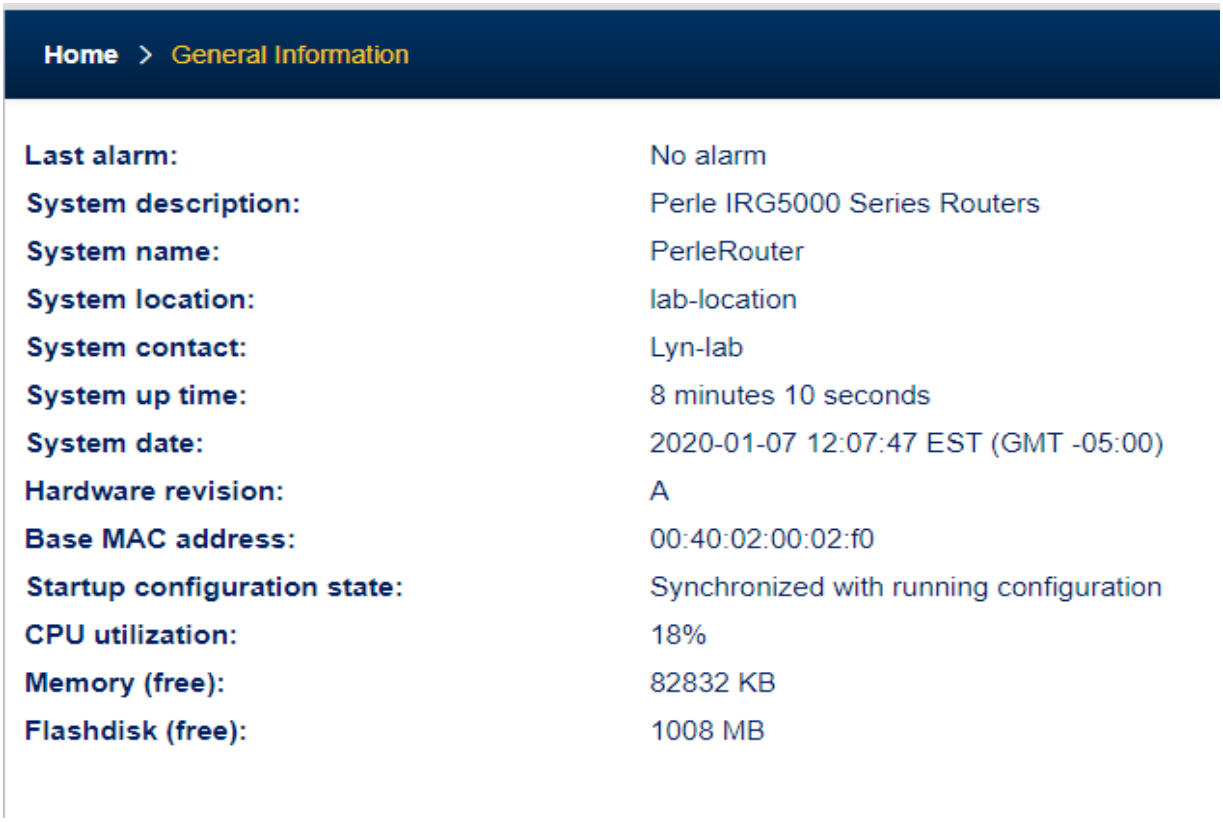
Profile Name	Enter a profile name.
Username	Enter a username.
Password	Enter the password.
EAP Profile (Add, Edit, Delete)	
Profile Name	Enter the profile name.
PKI trustpoint	Enter the PKI trustpoint name.
Methods	• EAP-MD5 • EAP-MSCHAPV2 • EAP-GTC • EAP-TLS • TTLS-MSCHAP • TTLS-MSCHAPV2 • TTLS-CHAP • TTLS-EAP-MSCHAPv2 • TTLS-EAP-GTC • PEAP-MD5 • PEAP-EAP-MSCHAPv2 • PEAP-GTC

Monitor and Statistics

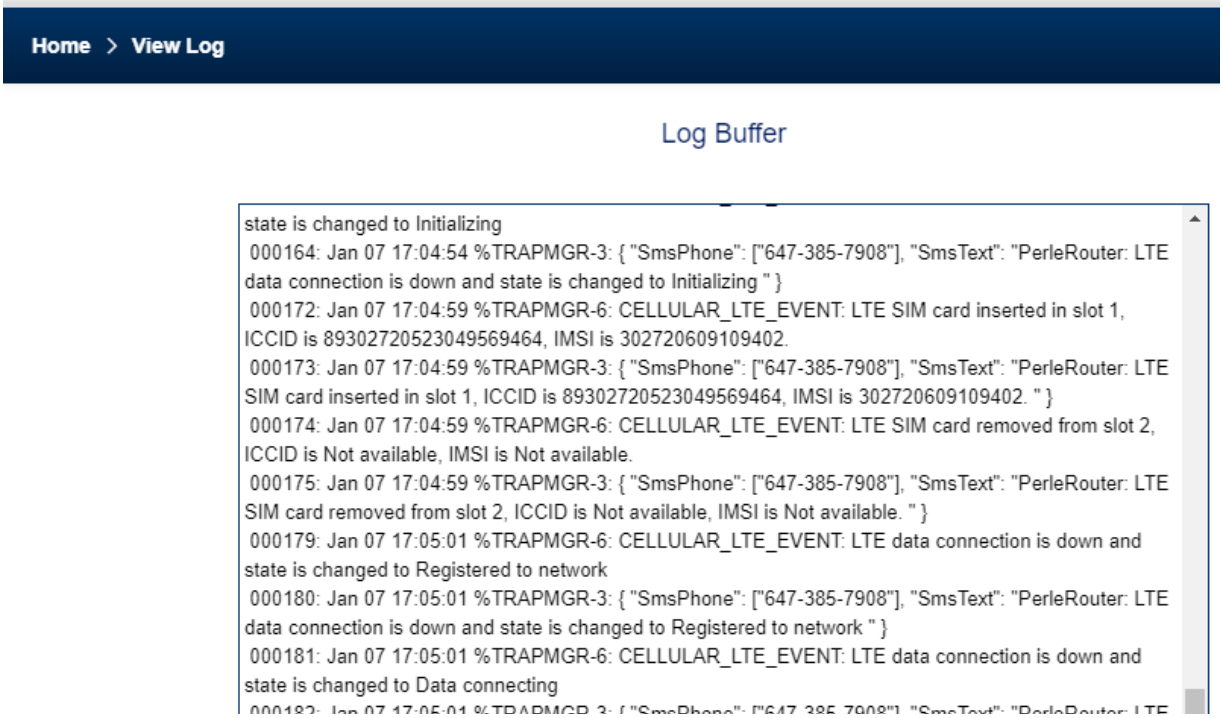
Your router can allow you to view statistics for general information about your router, view the logs, interface statuses and Alarms and I/O.

System

General Information

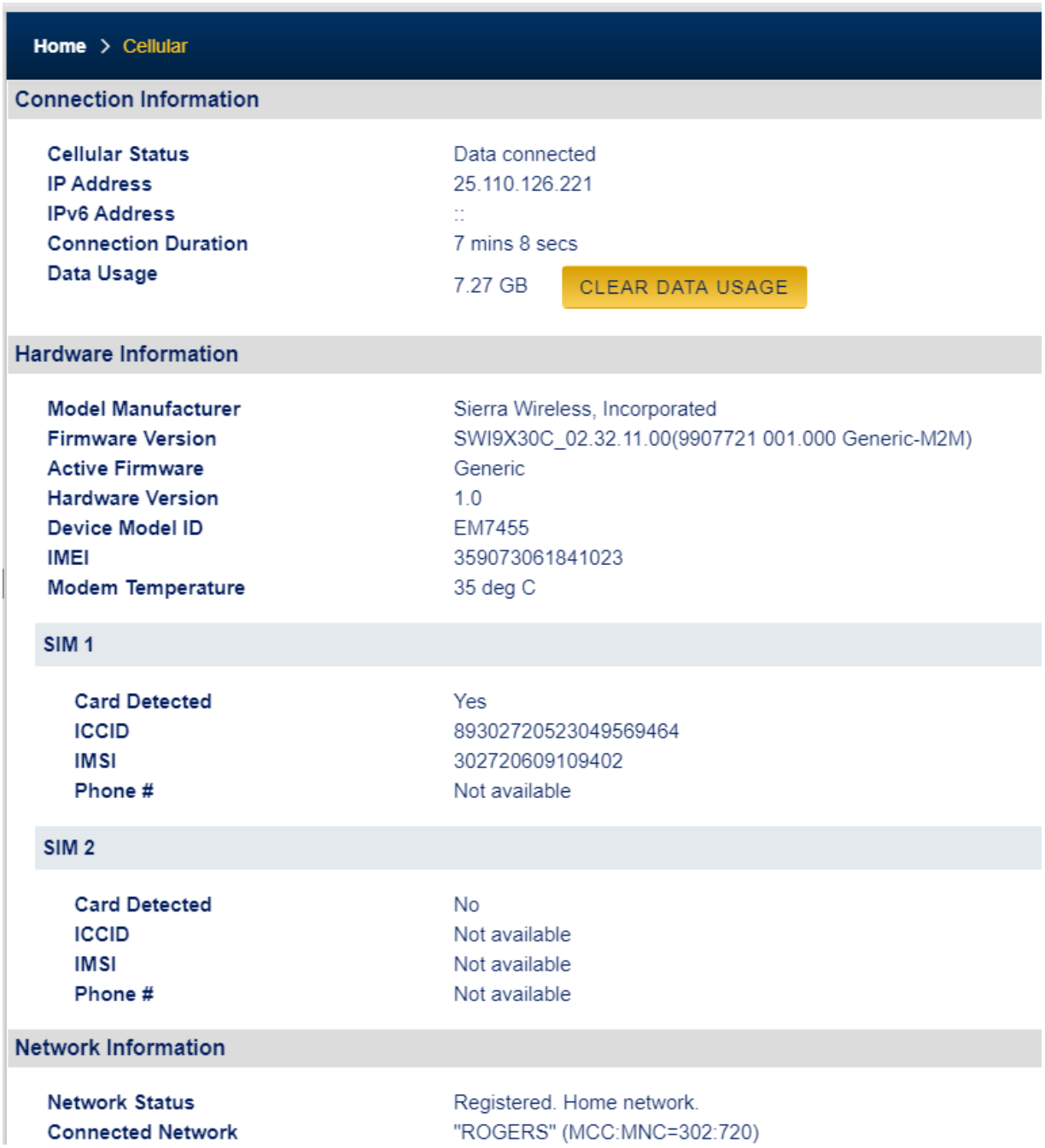


View Logs



Interface Status

Cellular



Alarms and I/O

Global Monitoring

Use global monitoring to check Interface Statuses, Network Statuses, Routing, Service and Security on your router.

Administration

Your router provides a comprehensive range of services.
These services include;

- **Software Management** including: checking for updates, viewing software versions, updating software and creating backup software.
- **Configuration** including backing up/restoring your configuration and booting from a configuration file.
- **Import Keys and Certificates** including importing and exporting of HTTPS, Server, SSH and SSL host/client/user keys and certificates.
- **Managing Flash Files** including exporting and importing files to/from flash.
- **Reboot/Reset** your router including resuming power standby mode, resetting to factory defaults and shutting down your router.

Software Management

Updating Router Software Versions

Overview

This section describes how to manage the Perle router software (images) files.
To check for new software updates, select the Check Now button or select the automatically check for updates checkbox. By enabling these features, the router will check the Perle repository and inform you if your router software is up-to-date. The software image can then be downloaded directly from the Perle repository using the Update Software button/Direct Download feature or alternatively, the software can be copied directly from our website to an external TFTP, SFTP, FTP, or HTTP, HTTPS and then update to your router at a later date. The current image can be replaced with a new one or kept in flash memory after a download as a backup.

Pre-requisites

- TFTP, SFTP, FTP, or HTTP, HTTPS or SCP server for downloading/uploading image files
- Internet access is required to obtain the latest software images from the Perle web site at https://www.perle.com/downloads/

Terminology

- Startup software is the software that is stored in flash and will run the next time the router is rebooted.
- Currently 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 router every 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

Router Software Versions

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

- Name
- Version
- Date created
- Size of the software file
- Source (where it was loaded from)
- Date downloaded (installed)

Create Backup of Startup Software

The Backup software image can be stored locally on your router overwriting the Startup software image or can be backed up offline to a FTP, HTTP, HTTPS, SCP, SFTP or TFTP server.

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. A Check for Update button allows you to maintain the latest LTE modem software on your router.

Keys and Certificates

Overview

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 ADIUS 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	
Method	• **Browser** • **FTP** • **HTTP** • **HTTPS** • **SCP** • **SFTP** • **TFTP**

Your router has a built-in self signed certificate. **To use your own HTTPS Certificate, you need to download the SSL/TLS private key and certificate to the router. You also need to set the SSL Passphrase parameter with the same password that was used to generate the key.** **Note: Your router has a built-in self signed certificate.**	
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.
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 router.
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 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.**

Managing Flash Files

Overview

Export and Import file from flash.

Pre-requisites

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

Features details / Application notes

- Export flash file to PC via web browser
- Export flash file to FTP server
- Export flash file to HTTP server
- Export flash file to HTTPS server
- Export flash file to SCP server
- Export flash file to SFTP server

- Export flash file to TFTP server
- Importing flash file from PC via web browser
- Importing flash file from FTP server
- Importing flash file from HTTP server
- Importing flash file from HTTPS server
- Importing flash file from SCP server
- Importing flash file from SFTP server
- Importing flash file from TFTP server

Reboot/Reset

Overview

Enables you to reboot the router based on:

- reboot now
- reboot in hours/minutes

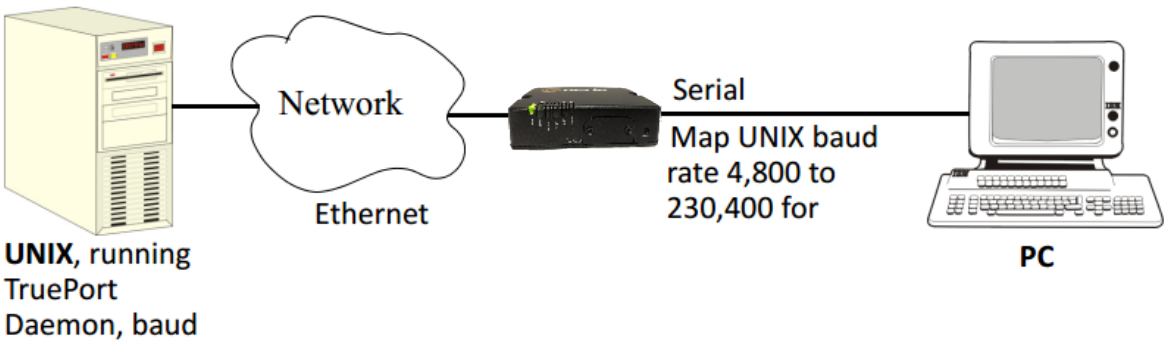
Reboot/Reset	
Reboot	**Reboot now**
Reboot in	**Schedule a time to reboot in hours and minutes**
Resume Power Management	
Standby	**Depending on power management setting this may cause the router to enter Standby Mode** • **Resume**
Reset to Factory Defaults	
Reset to Factory	**This will reset all configuration, operational information and certificates to factory default settings. Ethernet settings are 192.168.0.1. with DHCP enabled** • **Reset Now**
Shutdown the router	
Shutdown	**This will shutdown the router without engaging any of the standby modes. The Rest button will power the router backup up.** • **Shutdown now**

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, as shown below.



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 Industrial Switches 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 switches from a centralized server. There is no user client software required to be installed on administrator's PCs.

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 the router 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 the router 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 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.

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

Full Name	Key-Exchange	Auth	Encryption	Key-Size	HMAC
EDH-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES	128	SHA1
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

The following diagnostic tools are available in your router.

Ping

The ping utility will accept the following parameters.

- Host (this is the destination host)
  - Can be 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 - 18024 bytes
  - Default is 56 bytes
- Data pattern
  - Hexadecimal pattern

If a name was specified, the utility will first attempt to resolve the name to an IP address. If this can't be done, an error message is provided. Next, the utility will attempt to send the ICMP message to the destination host. If this is received by the host, the host will respond to the sender. The send / response sequence is one repetition of the ping command. Each repetition is timed. This information is displayed for each successful request. After the requested number of repetitions has been 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

Traceroute

This utility displays each hop on the path to the final destination including the time it took to reach that hope and return. If the destination is not reachable, the utility will display how far the message was able to travel. Traceroute displays the path which is 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. It is used in cases where the destination can't be reached. This utility will help identify at what point the routing to the destination fails. 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 your router is attempting to reach.

This parameter can be specified as;

- Name
- IPv4
- IPv6

If a name was specified, the utility will first attempt to resolve the name to an IP address. If this can't be done, an error message is provided.

It will then attempt 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 destination or fails to reach one of the hops on the way. As the attempts are being made, the utility displays the results of each attempt including timing information.
The utility will display an "*" to indicate a hop can't be reached.

Enabling debug messages
You can enable debug on specific code modules in order to collect more debugging information. Debug commands do not survive a re-boot.

- alarmgr – add alarm messages to logging
- all – add all debugging messages to logging (this will serious degrade the performance of your router)
- bgp – add bgp messages to logging
- cellular-gnss –add gnss messges to logging
- cellular-lte – add cellular messages to logging
- clpd – add command line parser
- dialer – add dial on demand debugging to logging
- dot11-ap – IEEE 802.11 AP and authentication messages to logging
- dot11-station – IEEE 802.11 Client and authentication messages to logging
- dot1x-authenticator – add 802.1x authenticator messages to logging
- dot1x-supplicant – add 802.1x supplicant messages to logging
- drmgrd – Device Remote Manager daemon messages to logging
- email – add email messages to logging
- init – add init messages to logging
- ip – add ip messages to logging
- ip-passthrough – add ip passthrough messages to logging
- ipsec – add ipsec messages to logging
- kernel – add kerne messages to logging
- logging = debug logging manager
- ntp - add ntp messages to logging
- snmp - add snmp messages to logging
- trapmgr – add trap manager messages to logging
- tty – add tty port (line tty) messages to logging
- vty – add vty messages to logging
- wan-highavail – add high available and health debugging to logging
- wanifmgr – WAN Interface Manager messages to logging

Radius External Parameters

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, 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.

Table 0–1

Type	Name		Description
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
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 router **User Service** to use to connect the user 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

Table 0–1

Type	Name		Description
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. See ***Perle RADIUS Dictionary Example*** for an example of this file. 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.
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.

Table 0–1

Type	Name		Description
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 ILOAN management session. For Device manager sessions: "DEVMGR" 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	Response 8	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 router when 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 router LAN interface.
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 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 DSPrompt**. • 6—Administrative User • 11—Callback Administrative User Equivalent to router **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.

Type	Name	Description
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.
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 ILOAN management session. For Device manager sessions: "DEVMGR" 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	router 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 a 4-port router (although the dictionary can contain 48 ports, even if they are not all defined):

```
# 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	12-15 (Admin) 8-11 (Normal)	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 = 12-15 (Admin)
                        # x = 8-11  (Normal)

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 #
}
```

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	12-15 (Admin) 8-11 (Normal)	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 = 12-15 (Admin)
                        # x = 8-11 (Normal)

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 = 12           # x = 12-15 (Admin)

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 the 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